

# ACS 5.x和以后：与Microsoft Active Directory配置示例的集成

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[背景信息](#)

[配置](#)

[配置ACS 5.x应用程序部署引擎\(ADE-OS\)](#)

[加入ACS 5.x对AD](#)

[配置访问服务](#)

[验证](#)

[相关信息](#)

## 简介

本文提供一配置示例集成Microsoft Active Directory用思科安全访问控制系统(ACS) 5.x和以后。ACS使用Microsoft Active Directory (AD)，外部标识存储存储资源例如用户、机器、组和属性。ACS利用AD验证这些资源。

## 先决条件

### 要求

尝试进行此配置之前，请确保满足以下要求：

- Windows是活动目录的域用于的需要是充分地配置和可操作的。
- 请使用Microsoft Windows服务器2003域、MS Windows服务器2008年域或者MS Windows服务器2008 R2域，ACS支持这些5.x。**注意：**MS Windows服务器2008 R2域的集成与ACS的从ACS 5.2及以上版本支持。

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Secure ACS 5.3
- Microsoft Windows服务器2003域

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。

## 规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

## 背景信息

Windows活动目录提供在每天网络使用使用的许多功能。ACS 5.x的集成与AD的允许使用现有AD用户、机器和他们的组映射。

ACS 5.x集成与AD提供这些功能：

1. 计算机验证
2. 授权的属性检索
3. EAP-TLS验证的证书检索
4. 用户和计算机帐户限制
5. 计算机访问限制
6. 拨入许可检查
7. 拨入用户的回叫选项
8. 拨入支持属性

## 配置

### 配置ACS 5.x应用程序部署引擎(ADE-OS)

在您集成ACS 5.x对AD前，请保证时区、伊达市&时刻在ACS配比与那在AD主域名控制器。并且，请定义在ACS的DNS服务器为了能解决从ACS 5.x的域名。完成这些步骤为了配置ACS 5.x应用程序部署引擎(ADE-OS)：

1. 对ACS设备的SSH和输入CLI凭证。
2. 发出**clock timezone**命令在配置模式如命令配置ACS的时区所显示为了匹配与那在域控制器。  
`clock timezone Asia/Kolkata` 注意：亚洲/加尔各答是用于本文的时区。您能由EXEC模式找到您的特定时区显示时区命令。
3. 万一位于您的网络的您的AD域控制器与Ntp server同步，是高度推荐的使用在ACS的同样Ntp server。如果没有Ntp server，则请跳到步骤4。这些是配置Ntp server的步骤：Ntp server可以配置与NTP server> in命令配置模式的ntp server < IP地址如显示。  
`ntp server 192.168.26.55`  
The NTP server was modified.  
If this action resulted in a clock modification, you must restart ACS. 参考的[ACS 5.x : 与Ntp server配置示例的Cisco ACS同步](#)关于NTP配置的更多信息。
4. 为了配置日期和时间请手工请使用**clock set**命令在EXEC模式。示例如下所示：  
`clock set Jun 8 10:36:00 2012`  
Clock was modified. You must restart ACS.  
Do you want to restart ACS now? (yes/no) yes  
Stopping ACS.  
Stopping Management and View.....  
Stopping Runtime.....  
Stopping Database....  
Cleanup.....

Starting ACS ....

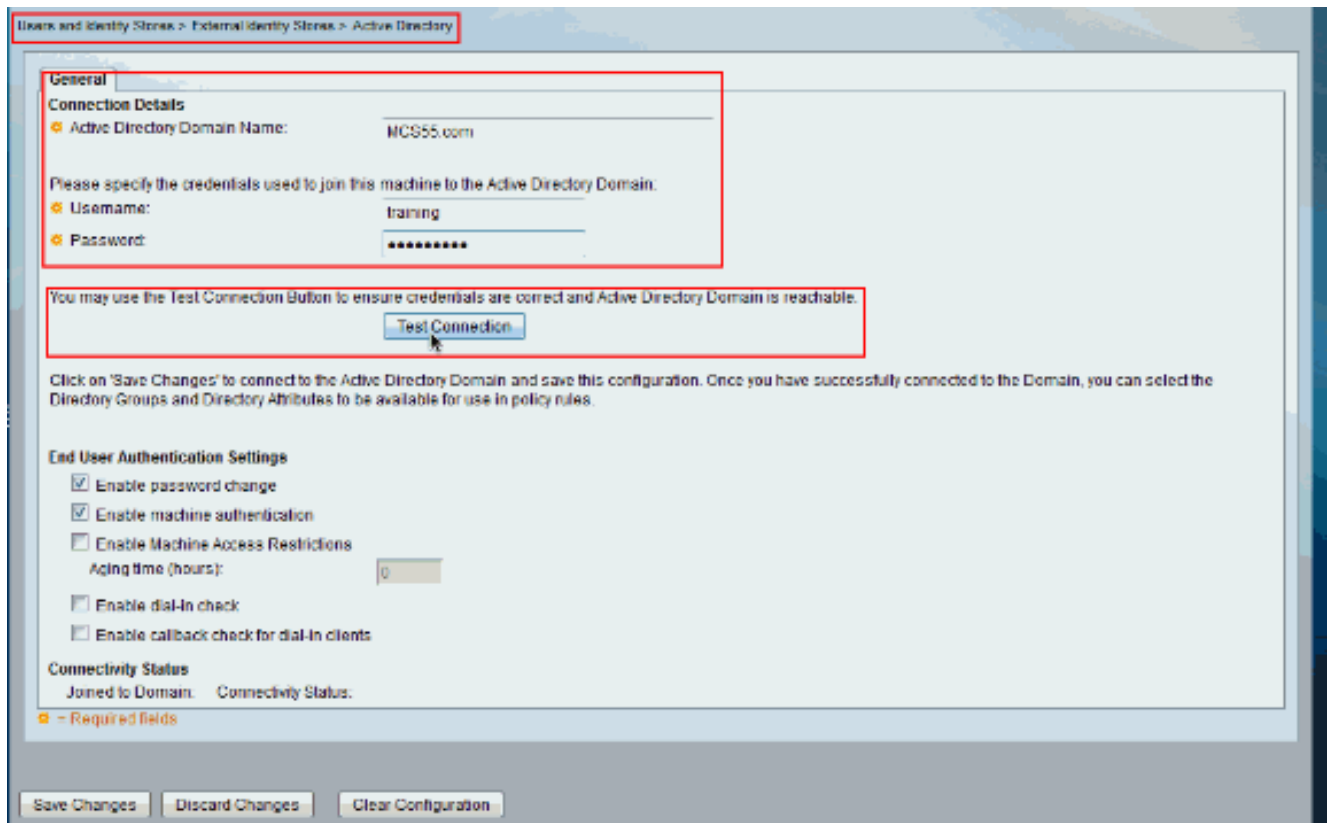
To verify that ACS processes are running, use the 'show application status acs' command.

5. 现在请验证时区，日期和时间用show clock命令。输出show clock命令显示此处：`acs51/admin# show clock` Fri Jun 8 10:36:05 IST 2012
6. 配置在ACS的DNS与<ip DNS> in命令配置模式的name-server < IP地址如显示此处：`ip name-server 192.168.26.55`注意：DNS IP地址由您的Windows域管理员提供。
7. 发出nslookup <域名>命令为了验证域名可接通性如显示。`acs51/admin#nslookup MCS55.com`  
Trying "MCS55.com" ; ; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60485 ; ; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1 ; ; QUESTION SECTION: ;MCS55.com. IN ANY ; ; ANSWER SECTION: MCS55.com. 600 IN A 192.168.26.55 MCS55.com. 3600 IN NS admin-zq2ttn9ux.MCS55.com. MCS55.com. 3600 IN SOA admin-zq2ttn9ux.MCS55.com. hostmaster.MCS55.com. 635 900 600 86400 3600 ; ; ADDITIONAL SECTION: admin-zq2ttn9ux.MCS55.com. 3600 IN A 192.168.26.55 Received 136 bytes from 192.168.26.55#53 in 0 ms 注意：如果答案部分是空的，则与您的windows域管理员联系发现域的正确DNS服务器。
8. 发出ip domain-name <域名>命令为了配置DOMAIN-NAME在ACS如显示此处：`ip domain-name MCS55.com`
9. 发出主机名<hostname>命令为了配置在ACS的主机名如显示此处：`hostname acs51`注意：由于NETBIOS限制，ACS主机名必须包含小于或等于15个字符。
10. 发出write memory命令为了保存配置到ACS。

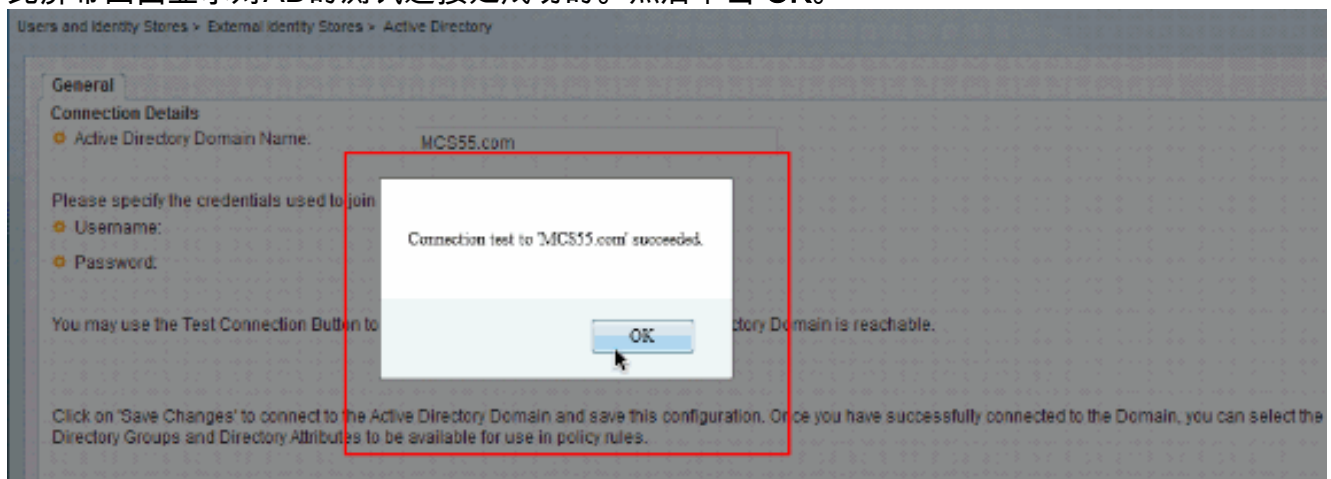
## [加入ACS 5.x对AD](#)

完成这些步骤为了加入ACS5.x到AD：

1. 选择用户，并且标识存储>外部标识存储>活动目录并且提供域名、AD帐户(用户名)和其密码并且点击测试连接。注意：要求的AD帐户在ACS的域访问的应该有这些之一：添加工作站在对应的域的域用户右边。创建计算机对象或删除计算机在ACS计算机帐户在加入对域的ACS计算机前创建的对应的计算机容器的对象权限。注意：思科建议您禁用ACS帐户的中断策略并且配置AD基础设施发送警报到admin，如果一个错误的密码使用该帐户。这是因为，如果输入一个错误的密码，ACS不创建或修改其计算机帐户，当是必要的时并且可能拒绝所有认证。注意：Windows AD帐户，加入ACS对AD域，在其自己的组织单位(OU)可以安置。它位于其自己的OU二者之一，当帐户创建或稍后与设备名称必须匹配AD帐户的名称的限制时。

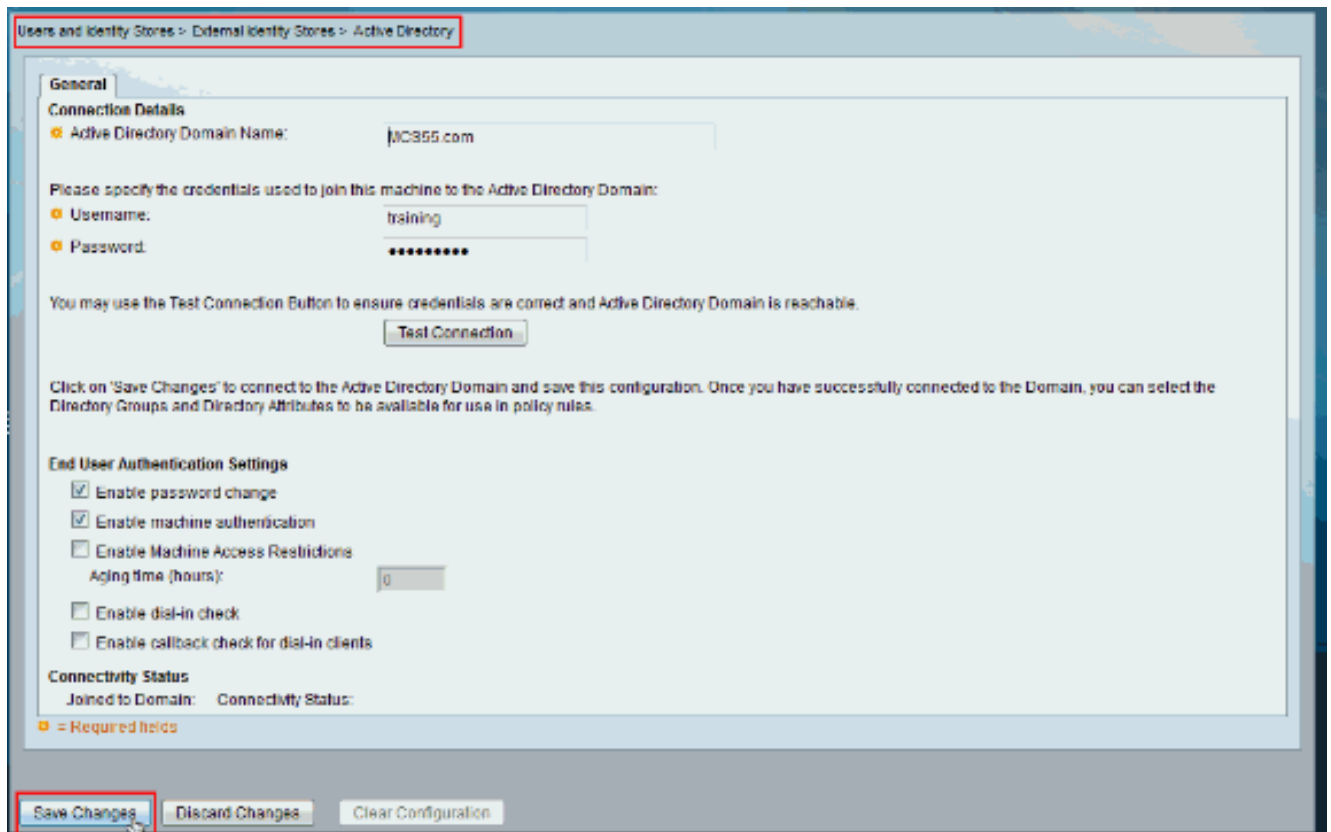


2. 此屏幕画面显示对AD的测试连接是成功的。然后单击 OK。

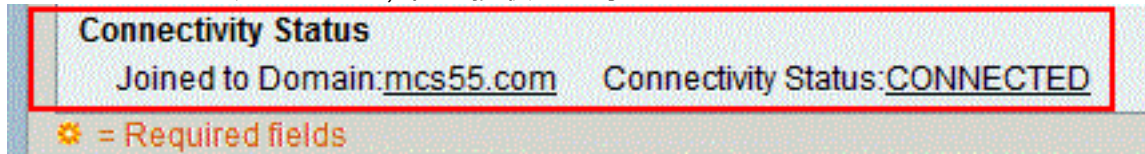


**注意：**Centrify配置受影响和有时断开，当有从服务器的一慢作用，当您测试与AD域时的ACS连接。然而，它良好工作与其他应用程序。

3. 点击ACS的保存更改加入AD。



4. 一旦ACS顺利地加入AD域，在连接状态显示。

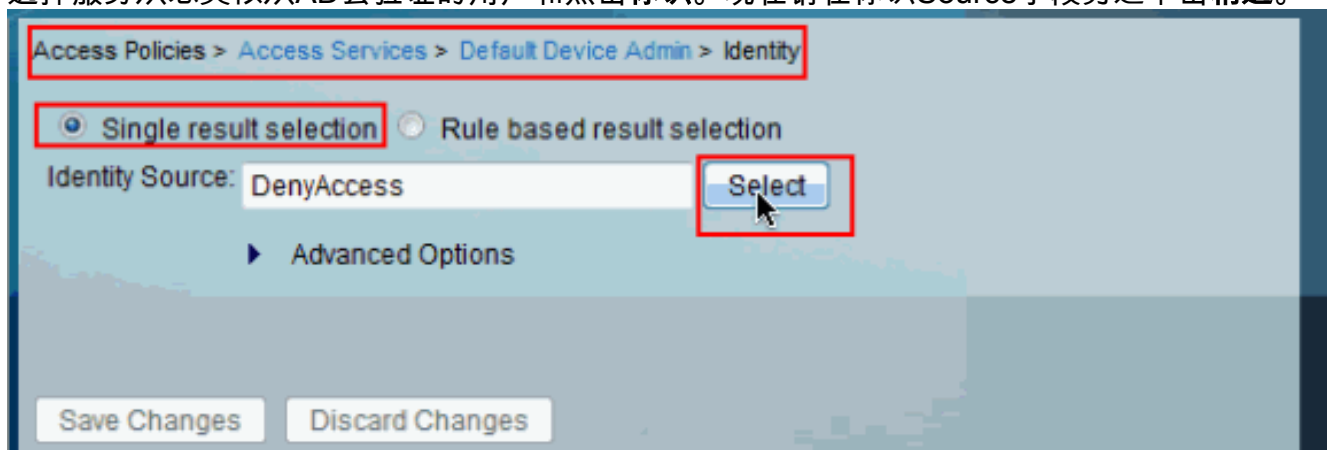


注意：当您配置AD标识存储时，ACS也创建：该存储的一个新的字典有两个属性的：ExternalGroups和另一个属性从目录属性页获取的任何属性的。新团体，IdentityAccessRestricted。您能手工创造此属性的自定义条件。组映射的一个自定义情况从ExternalGroup属性;自定义条件名是AD1:ExternalGroups和另一个自定义情况在目录属性页选择的每个属性的，例如，AD1:cn。

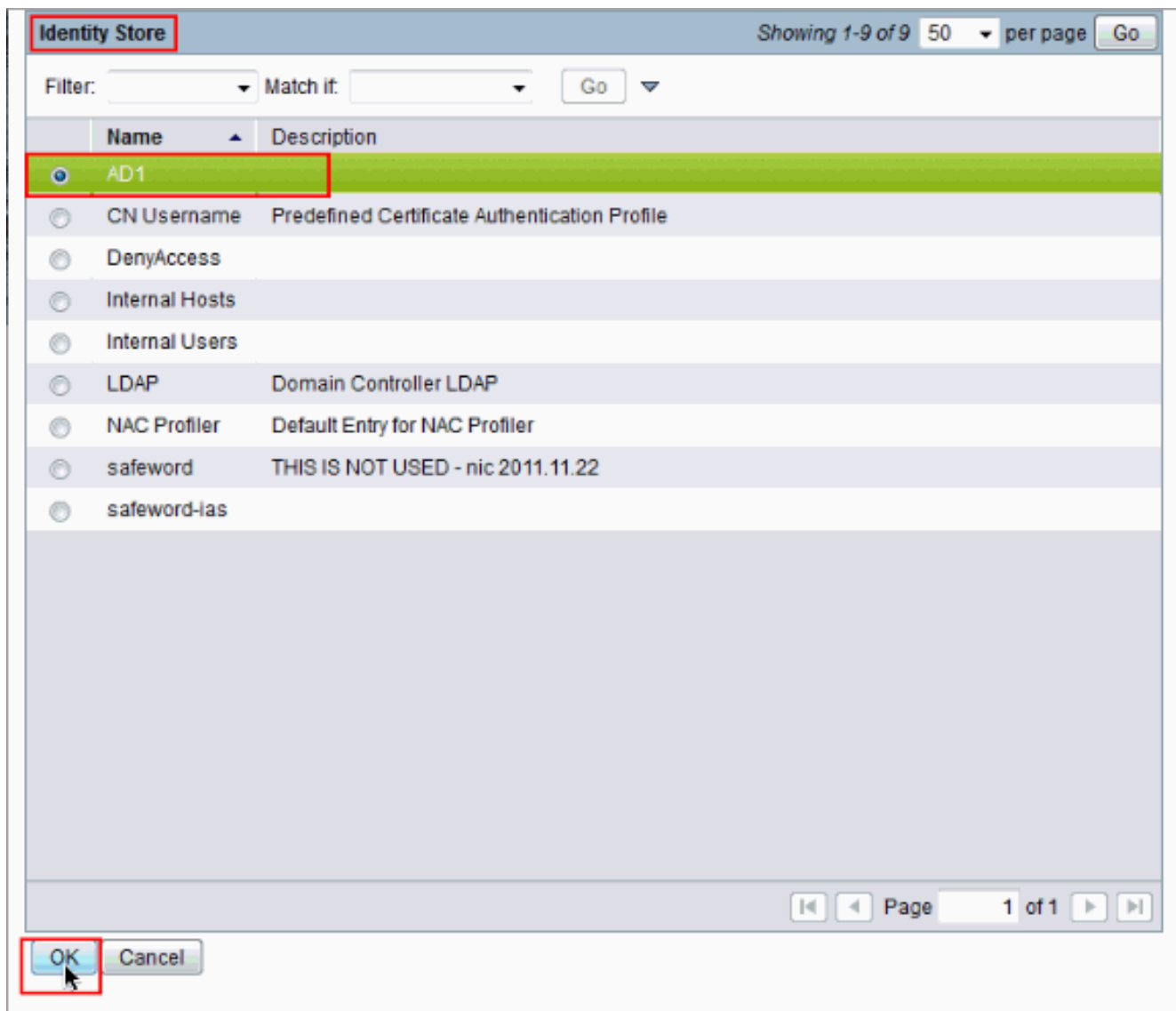
## 配置访问服务

完成这些步骤为了完成访问服务配置，以便ACS能使用最近配置的AD集成。

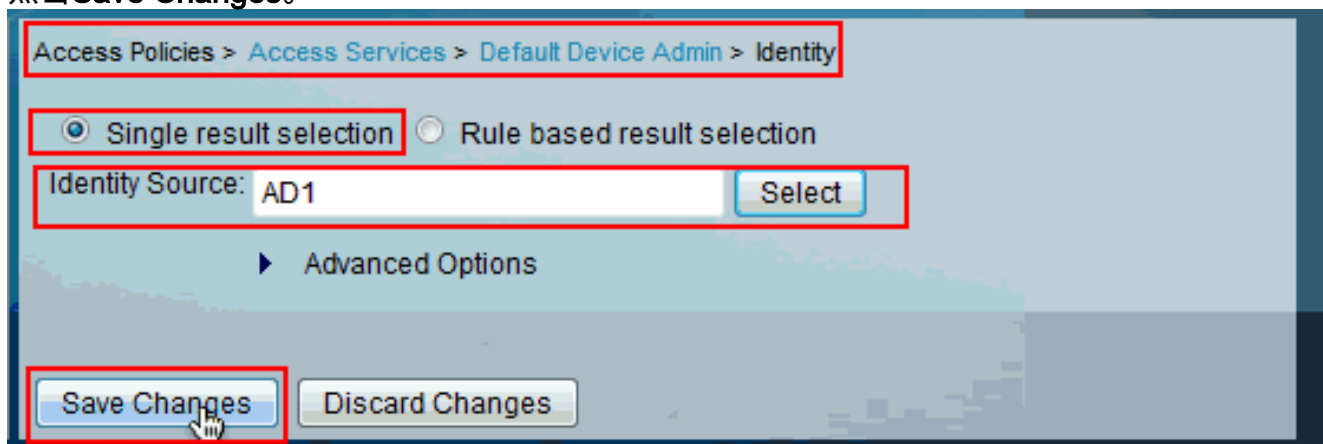
1. 选择服务从您类似从AD会验证的用户和点击标识。现在请在标识Source字段旁边单击**精选**。



2. 选择AD1并且点击OK键。



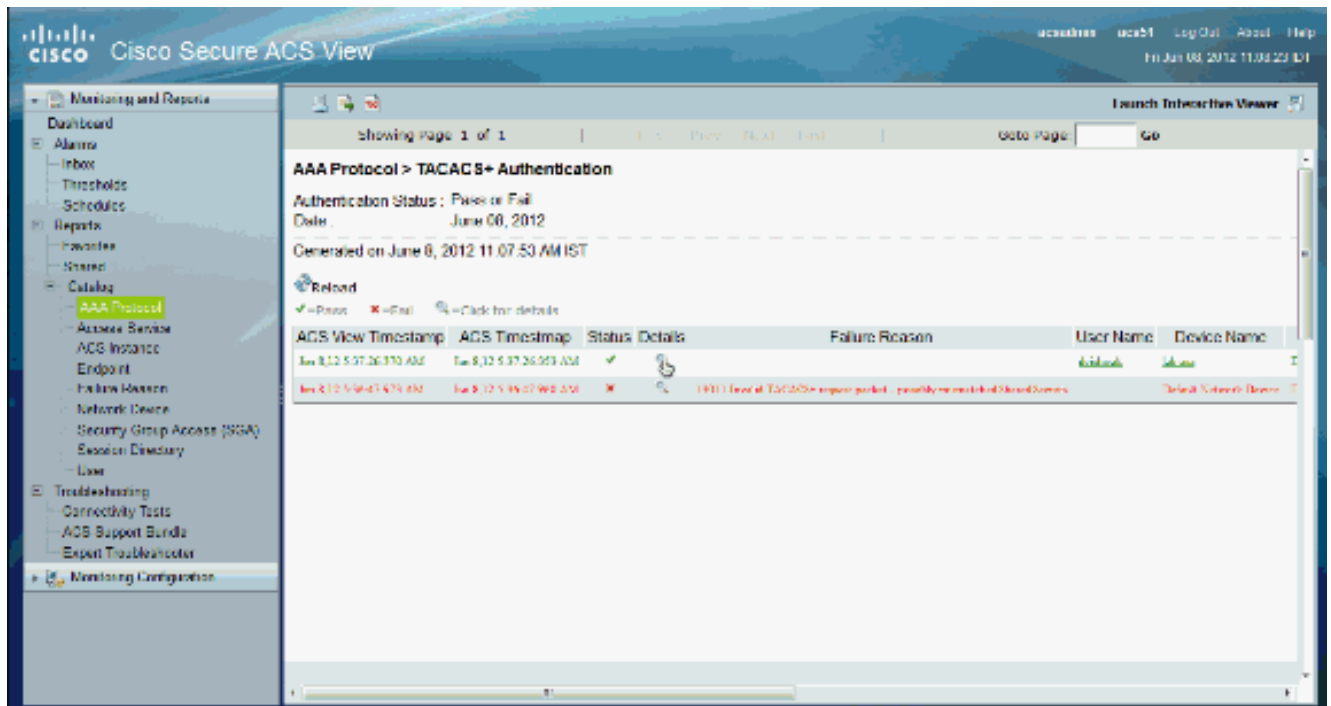
3. 点击Save Changes。



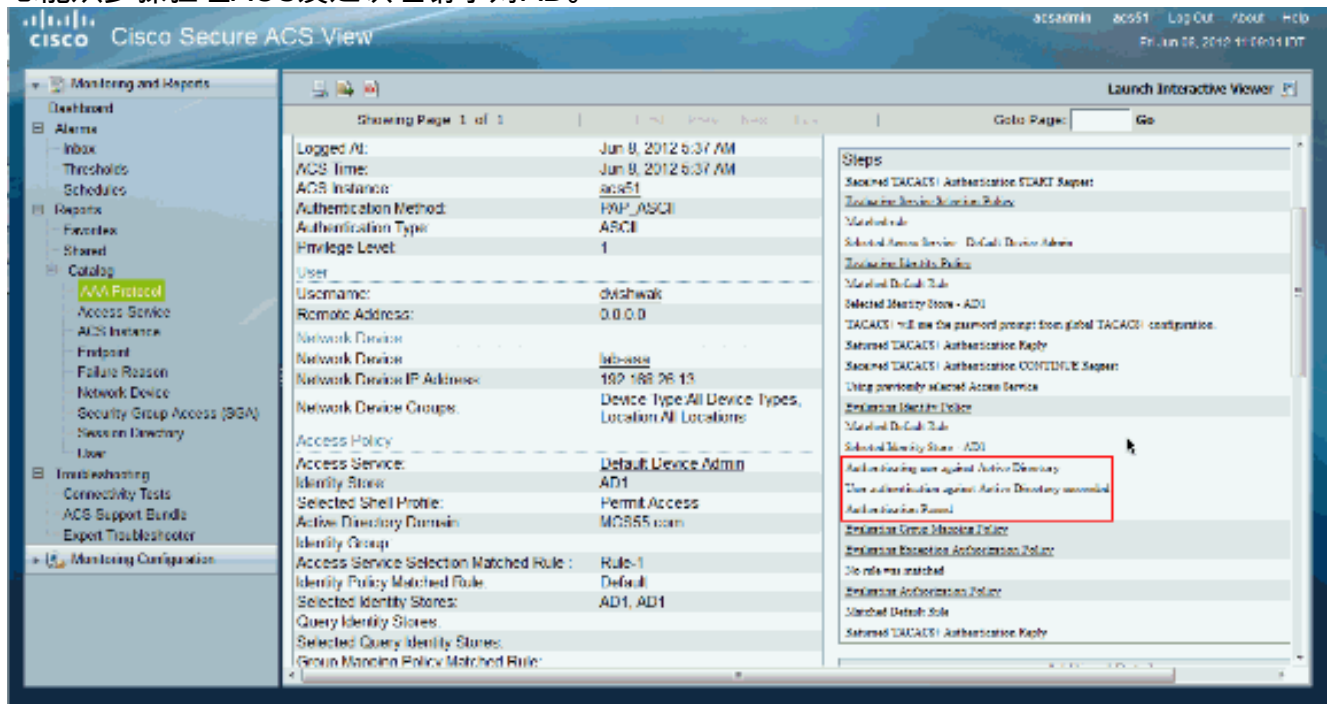
## 验证

为了验证AD验证，请发送从的认证请求与AD凭证的NAS。保证NAS在ACS配置，并且请求将由在前面部分配置的访问服务处理。

1. 在从NAS的成功认证登录ACS GUI并且选择**监听**，并且以后报告**>AAA协议>TACACS+Authentication**。识别从列表的合格验证并且点击**放大镜**符号如显示。



2. 您能从步骤验证ACS发送认证请求对AD。



## 相关信息

- [思科安全访问控制系统](#)
- [技术支持和文档 - Cisco Systems](#)