配置Cisco VPN 3000 系列集中器来支持带有RADIUS服务器的NT 密码到期功能

目录

简介

本文档包括有关如何配置Cisco VPN 3000系列集中器以支持使用RADIUS服务器的NT密码过期功能的分步说明。

要了解有关Internet身份验证服务器(IAS)的相同方案的详细信息，请参阅使用Microsoft Internet Authentication Server的具有过期功能的VPN 3000 RADIUS。

先决条件

要求

- 如果您的RADIUS服务器和NT域身份验证服务器位于两台独立的计算机上，请确保您已在两台计算机之间建立IP连接。
- 确保已建立从集中器到RADIUS服务器的IP连接。如果RADIUS服务器指向公共接口，请不要忘记在公共过滤器上打开RADIUS端口。
- 确保您可以使用内部用户数据库从VPN客户端连接到集中器。如果未配置，请参阅配置IPSec - Cisco 3000 VPN客户端到VPN 3000集中器。

注意：密码到期功能不能用于Web VPN或SSL VPN客户端。

使用的组件

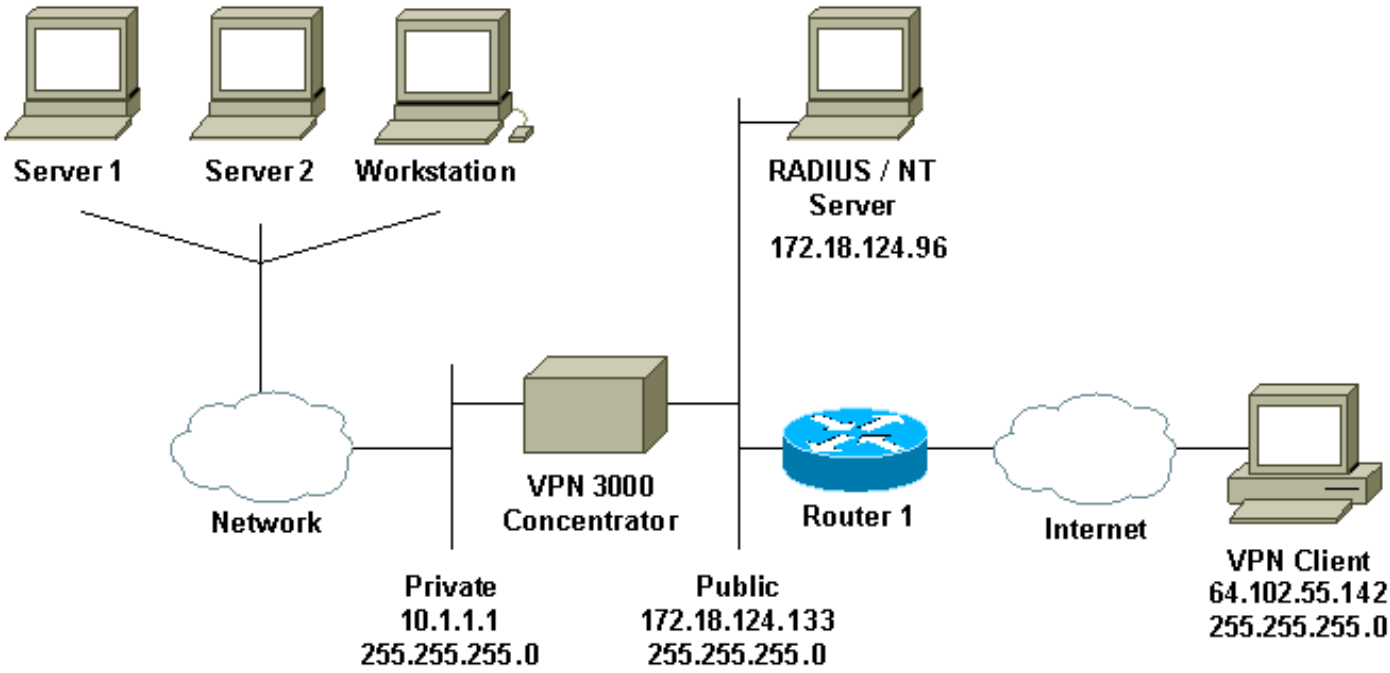
此配置使用下面软件和硬件版本开发并且被测试。

- VPN 3000集中器软件版本4.7
- VPN客户端版本3.5
- Cisco Secure for NT(CSNT)3.0版Microsoft Windows 2000 Active Directory服务器，用于用户身份验证

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。

网络图

本文档使用以下网络设置：



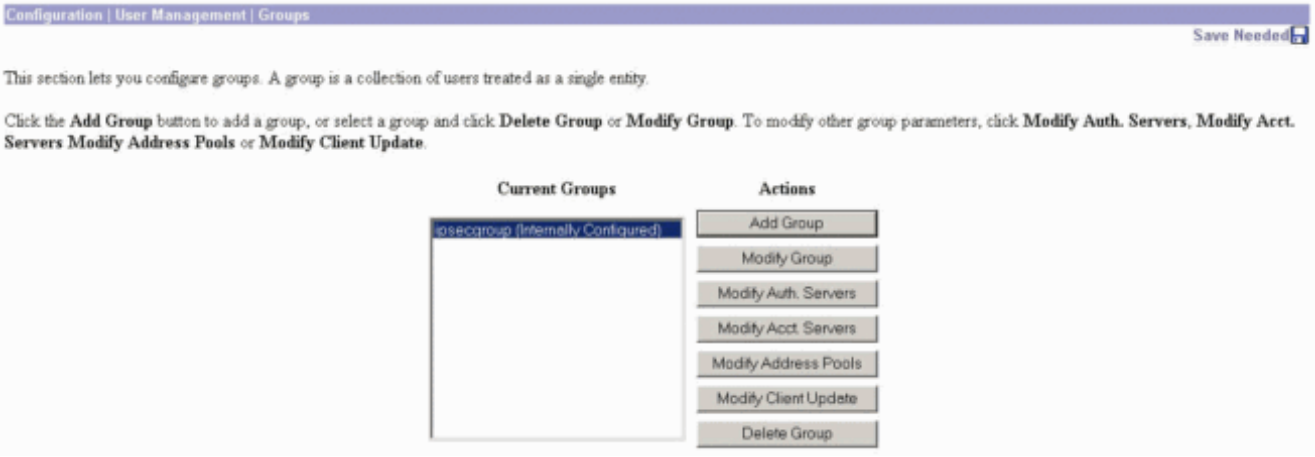
图表 注释

1. 此配置中的RADIUS服务器位于公共接口上。如果这是您特定设置的情况，请在公共过滤器中创建两个规则以允许RADIUS流量进入和离开集中器。
2. 此配置显示CSNT软件和NT域身份验证服务在同一台计算机上运行。如果配置需要，这些元素可以在两台独立的计算机上运行。

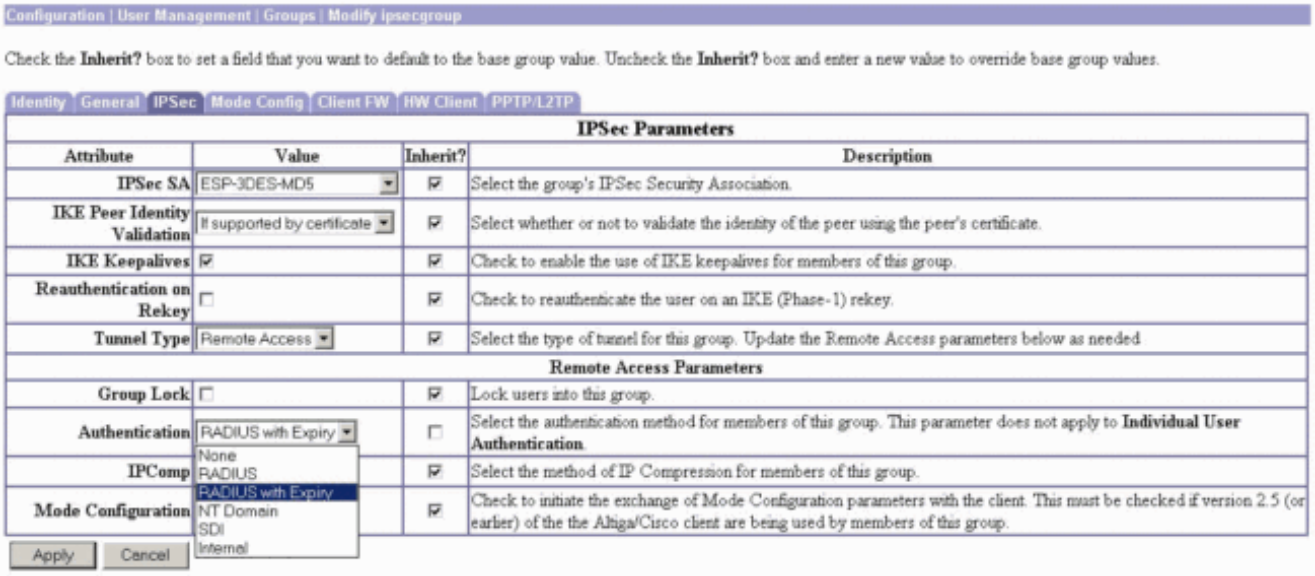
配置 VPN 3000 集中器

组配置

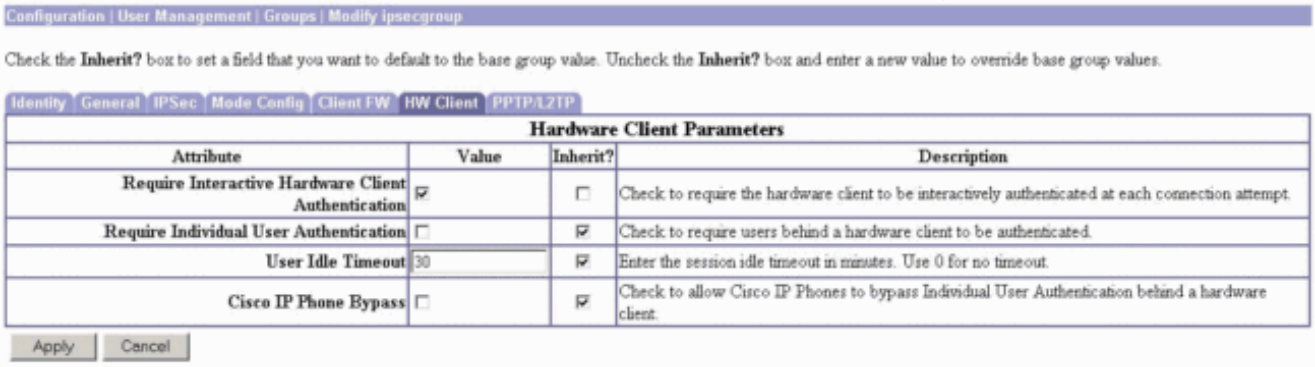
1. 要将组配置为接受来自RADIUS服务器的NT密码到期参数，请转到**Configuration > User Management > Groups**，从列表中选择您的组，然后单击**Modify Group**。以下示例显示如何修改名为“ipsecgroup”的组。



2. 转到“**IPSec**”**选项**卡，确保为“**身份验证**”**属**性选择了“RADIUS with Expiry”。

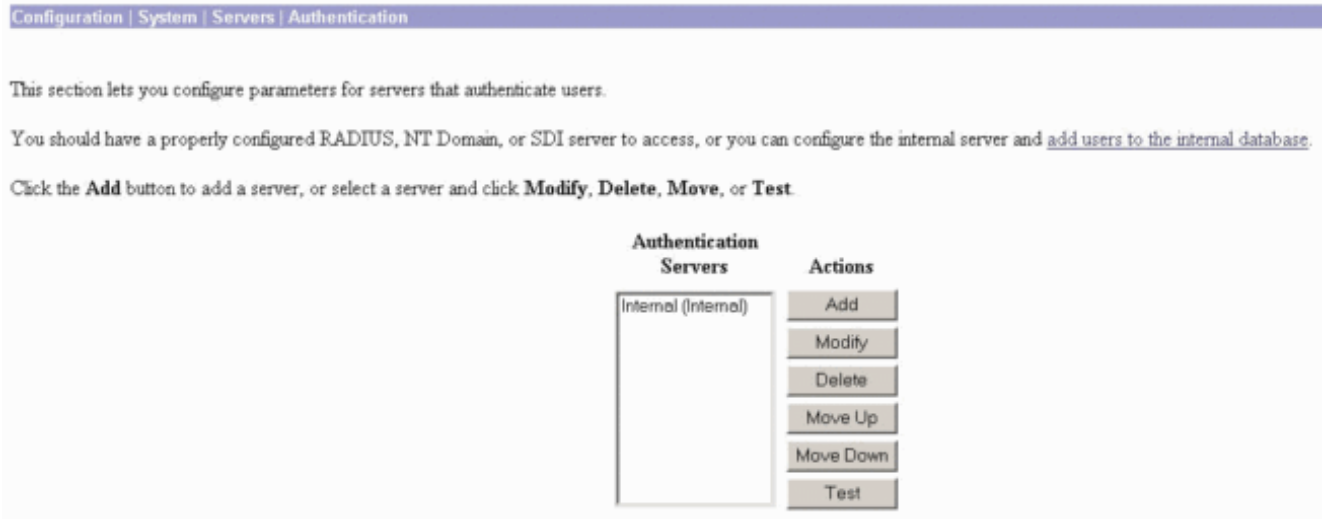


3. 如果希望在VPN 3002硬件客户端上启用此功能，请转到**HW Client**选项卡，确保已启用**Require Interactive Hardware Client Authentication**，然后单击**Apply**。



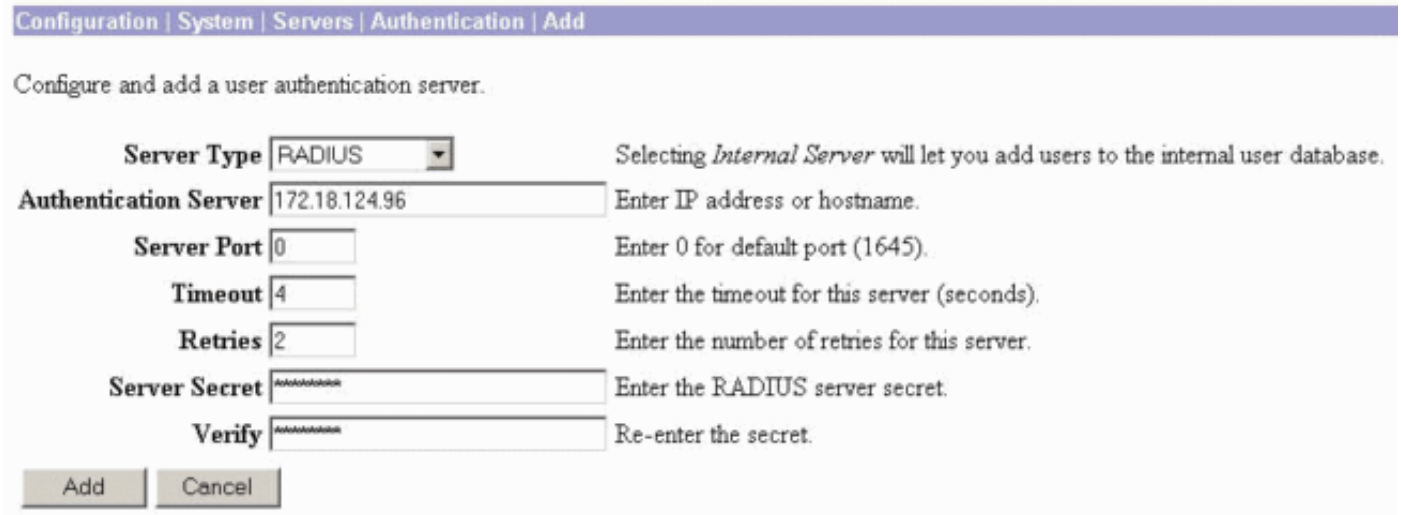
RADIUS 配置

1. 要在集中器上配置RADIUS服务器设置，请转到Configuration > **System** > Servers > Authentication > Add。



2. 在“添加”屏幕上，键入与RADIUS服务器对应的值，然后单击“添加”。以下示例使用以下值。

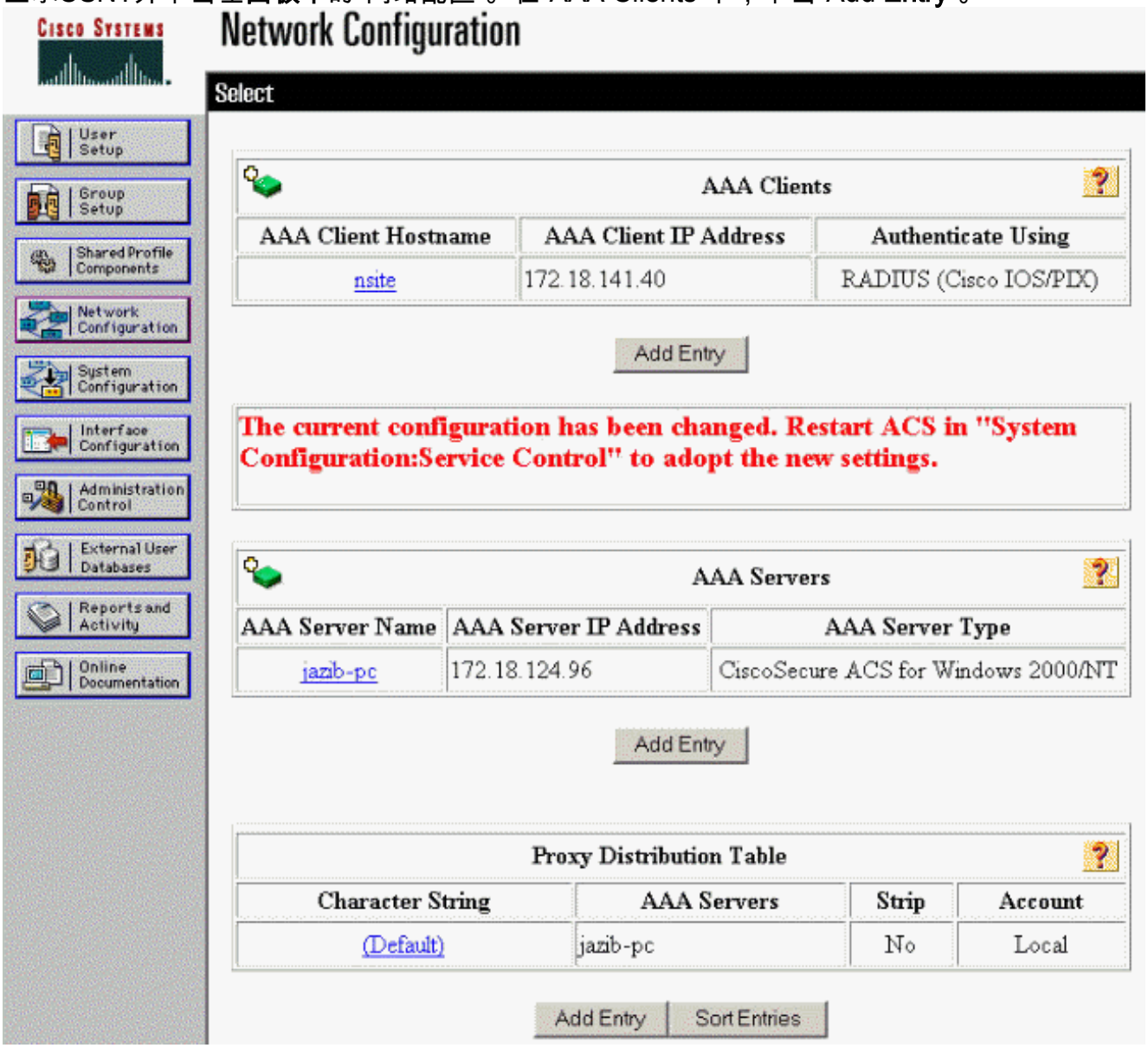
```
Server Type: RADIUS


Authentication Server: 172.18.124.96


Server Port = 0 (for default of 1645)

Timeout = 4


Reties = 2


Server Secret = cisco123


Verify: cisco123
```



配置 Cisco Secure NT RADIUS 服务器

为 VPN 3000 集中器配置条目

1. 登录CSNT并单击左**面板中**的“网络配置”。在“AAA Clients”下，单击“Add **Entry”**。



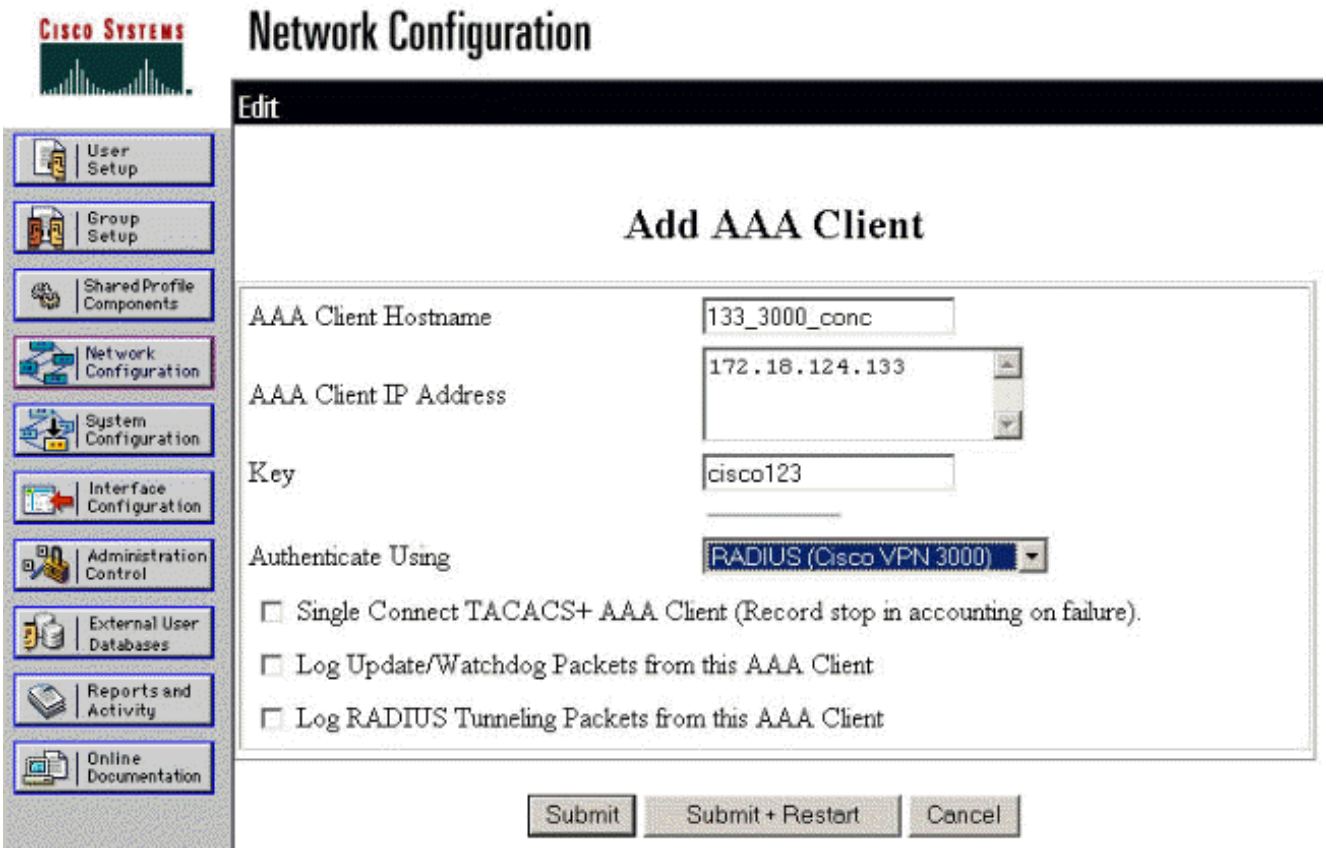
2. 在“Add AAA Client”（添加AAA客户端）屏幕上，键入适当的值以将集中器添加为RADIUS客户端，然后单击**Submit + Restart**。以下示例使用以下值。

AAA Client Hostname = **133_3000_conc**

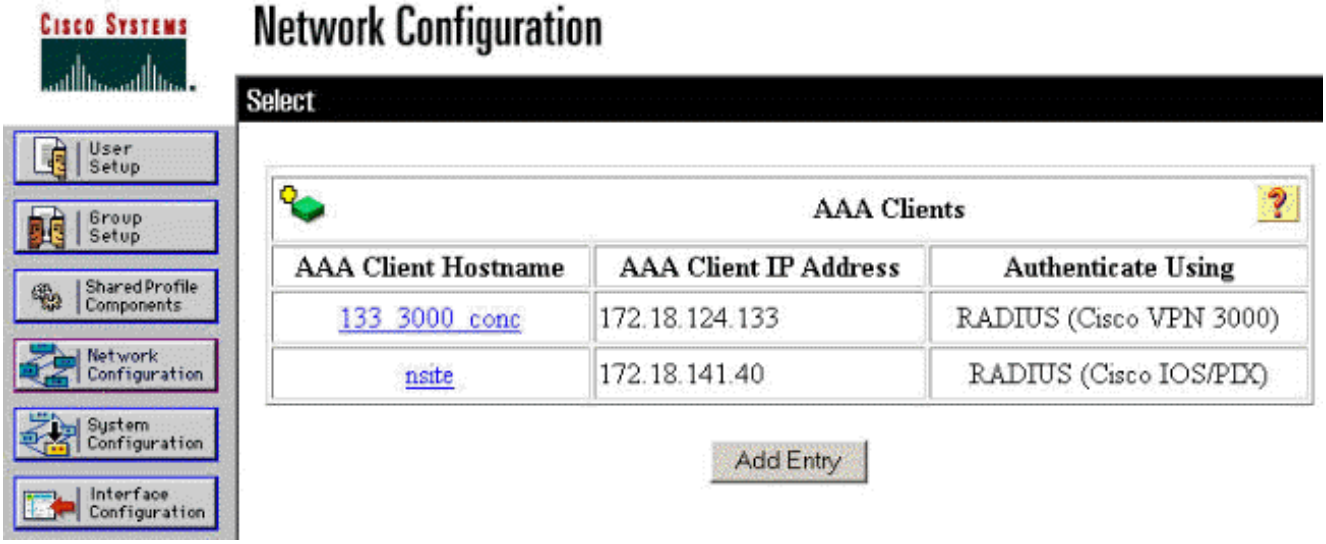
AAA Client IP Address = **172.18.124.133**

Key = **cisco123**

Authenticate using = **RADIUS (Cisco VPN 3000)**

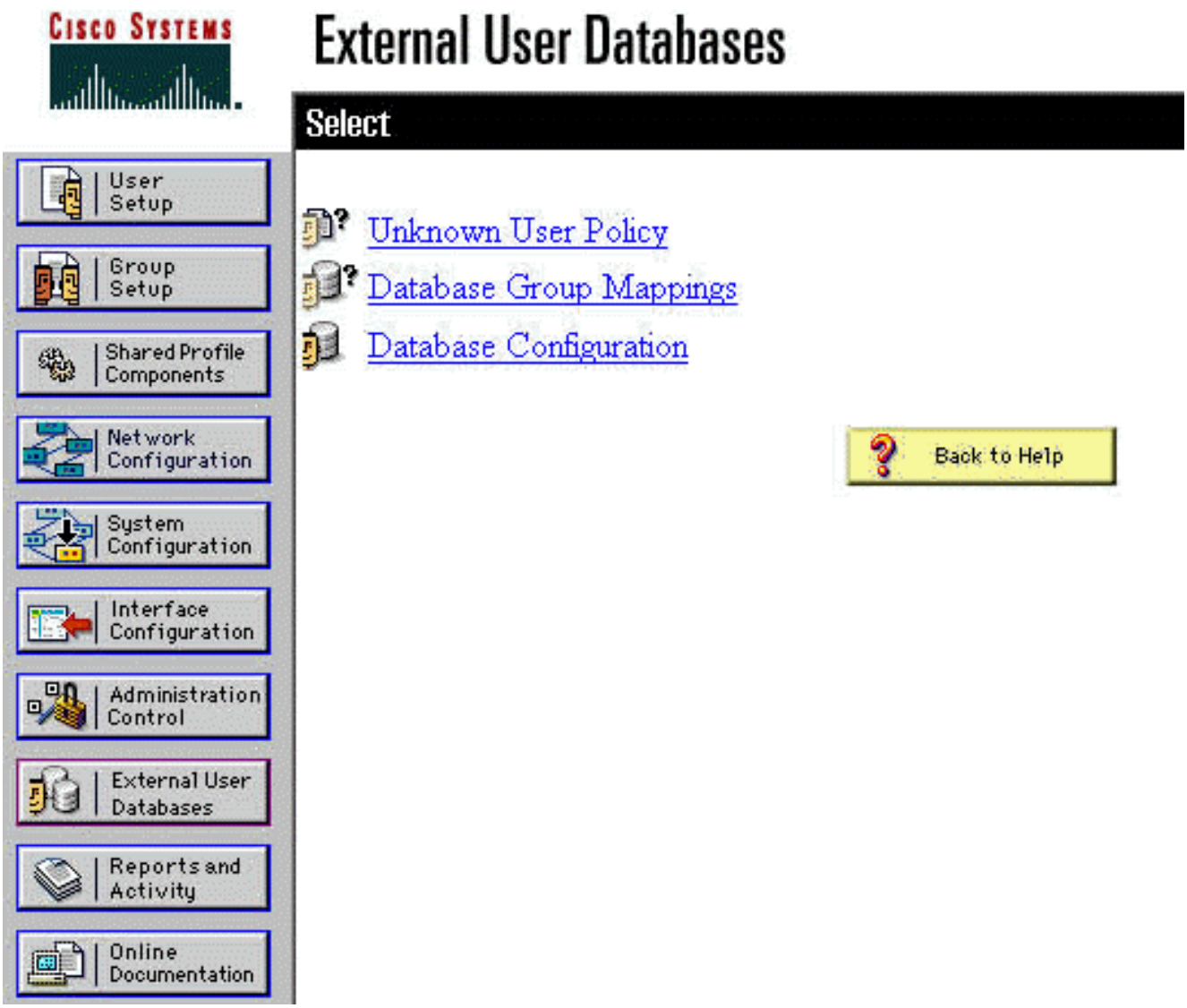


3000集中器的条目将显示在“**AAA Clients**”部分下。

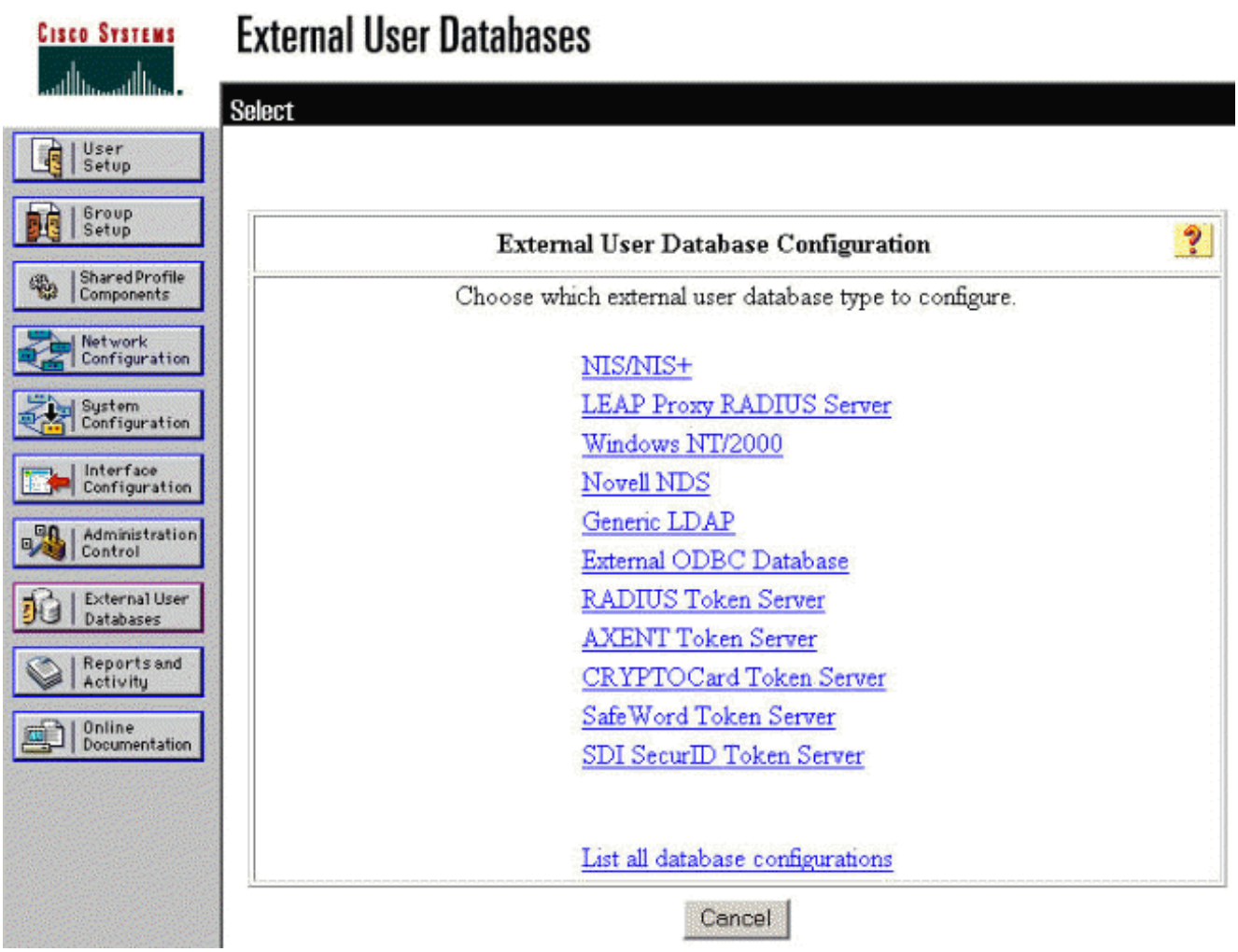


为 NT 域验证配置未知用户策略

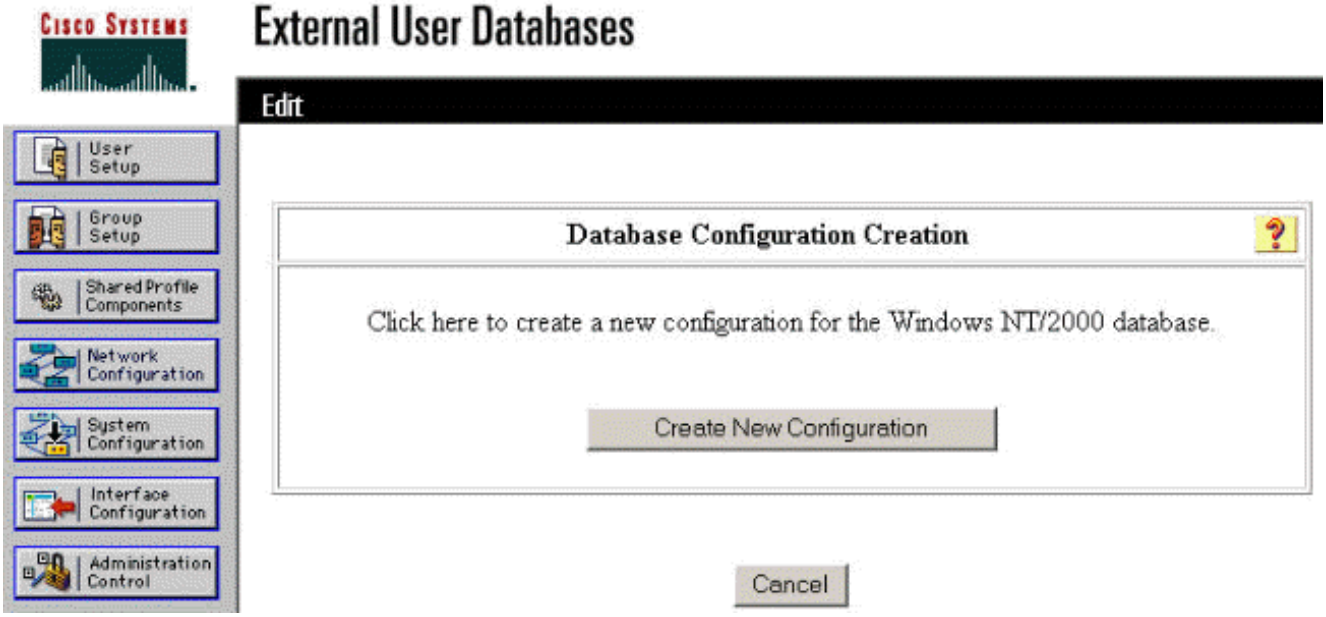
1. 要将RADIUS服务器上的用户身份验证配置为未知用户策略的一部分，请单击左面板中的**外部用户**数据库，然后单击数据库配置**的链接**。



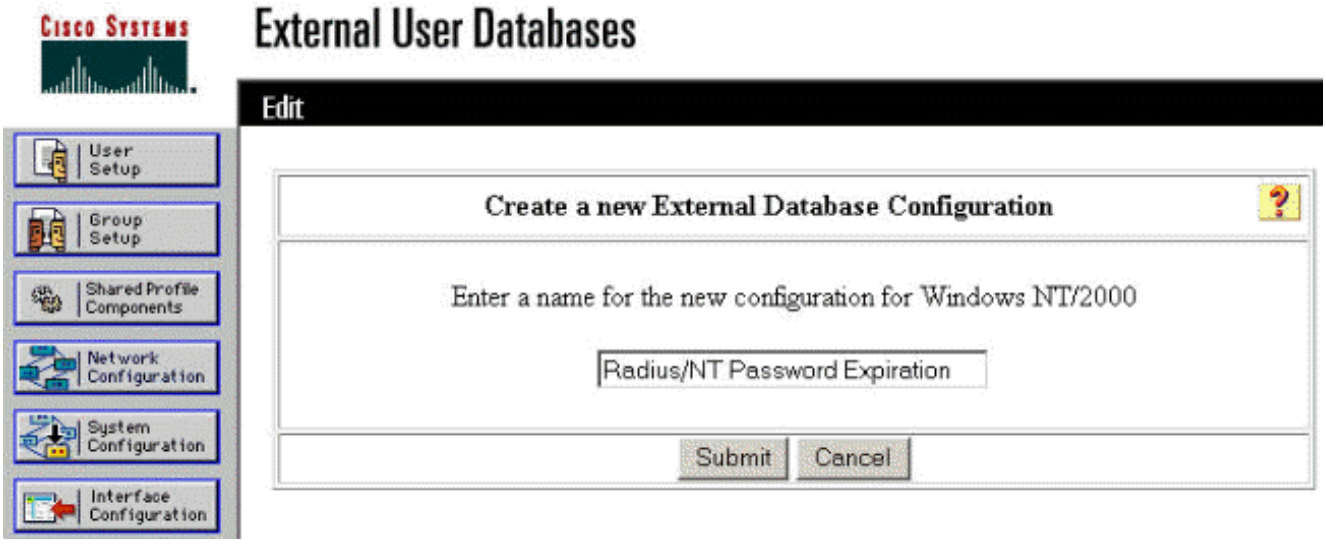
2. 在“External User Database Configuration（外部用户数据库配置）”下，单击**“Windows NT/2000”**。



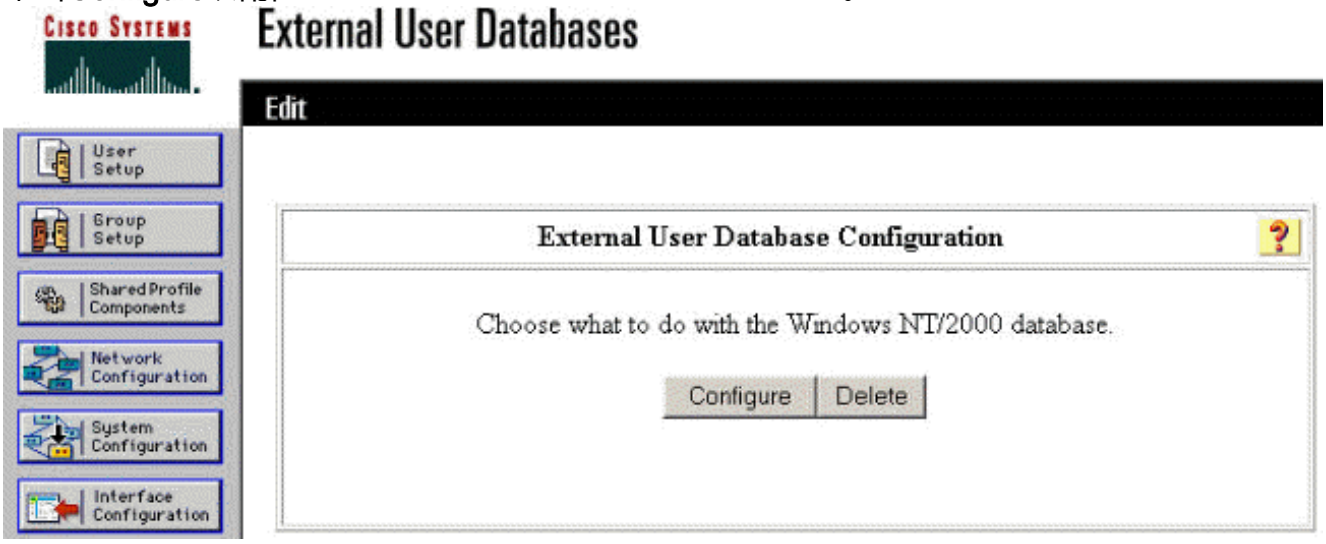
3. 在“数据库配置创建”屏幕上，单击**创建新配置**。



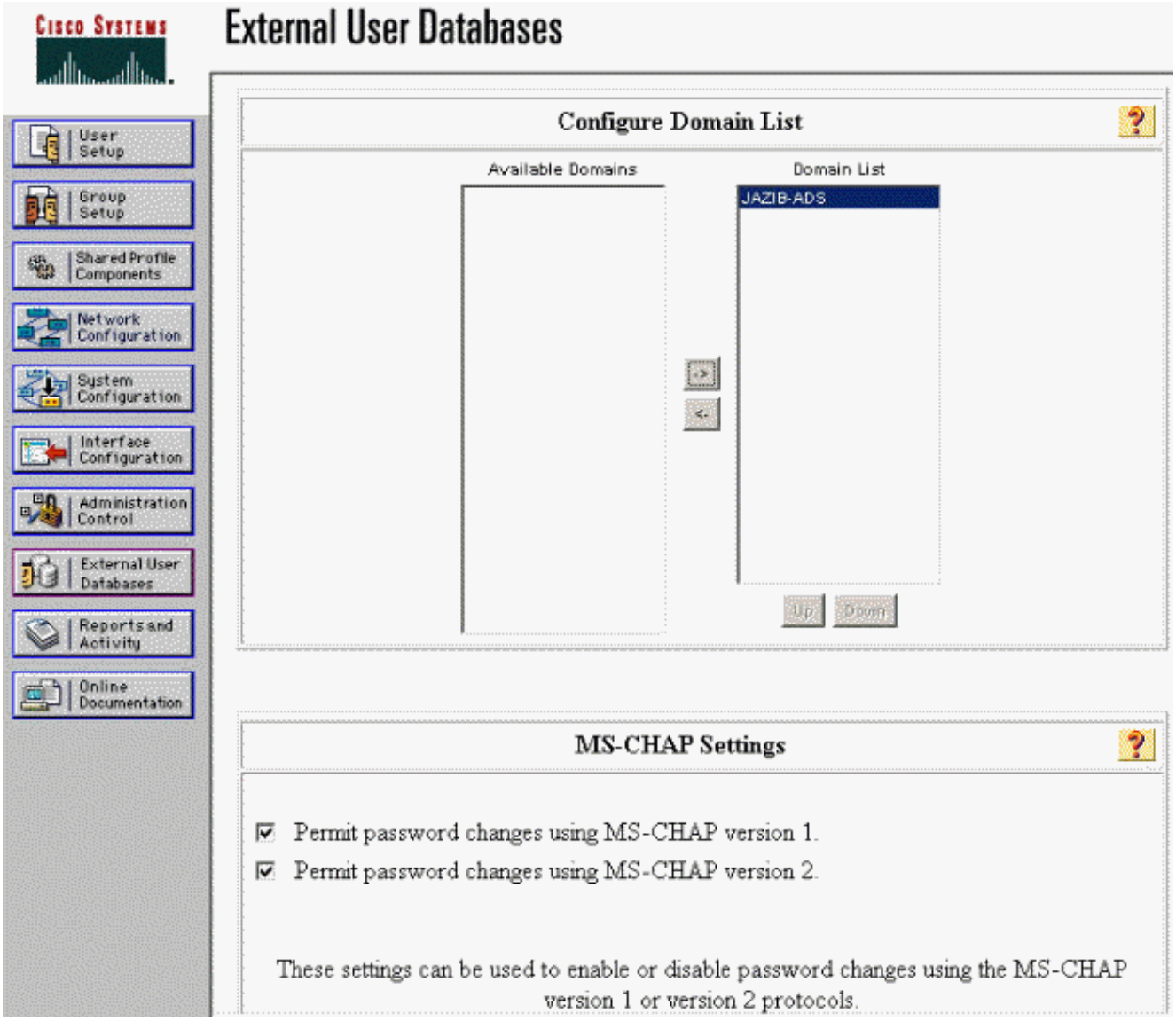
4. 出现提示时，键入NT/2000身份验证的名称，然后单击**Submit**。以下示例显示名称“Radius/NT Password Expiration”。



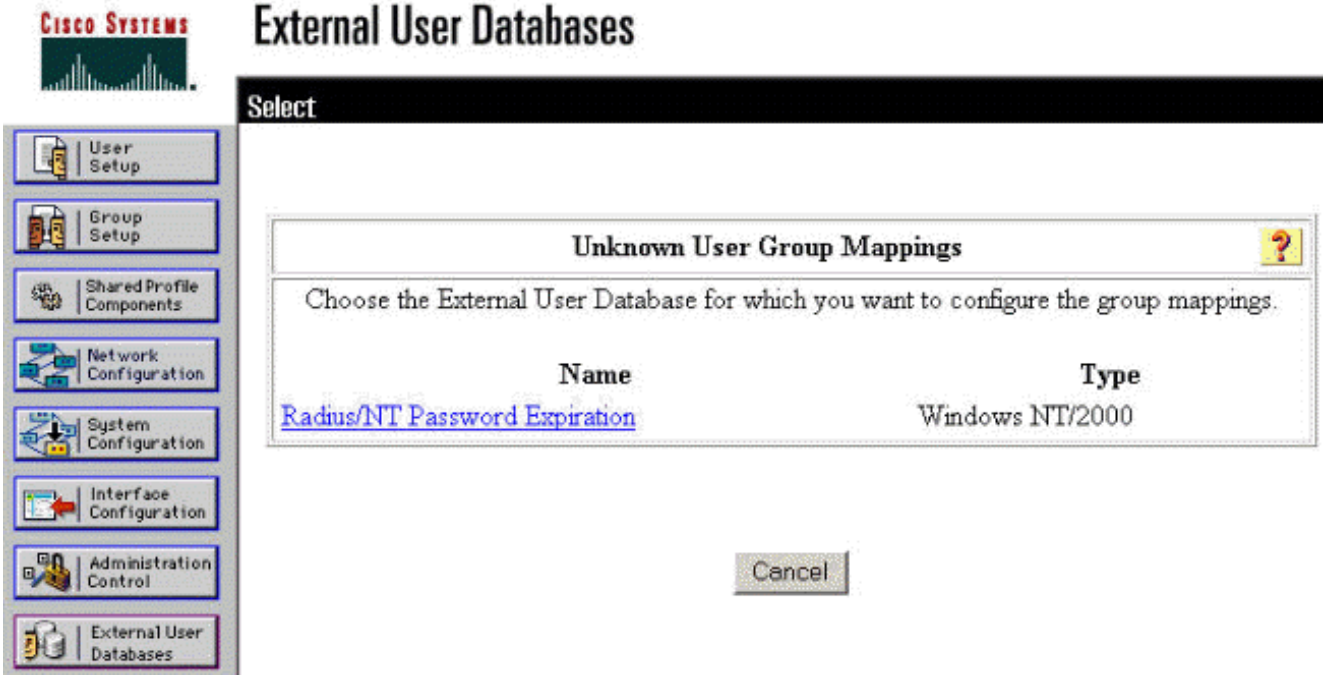
5. 单击**Configure**以配置Domain Name for User Authentication。



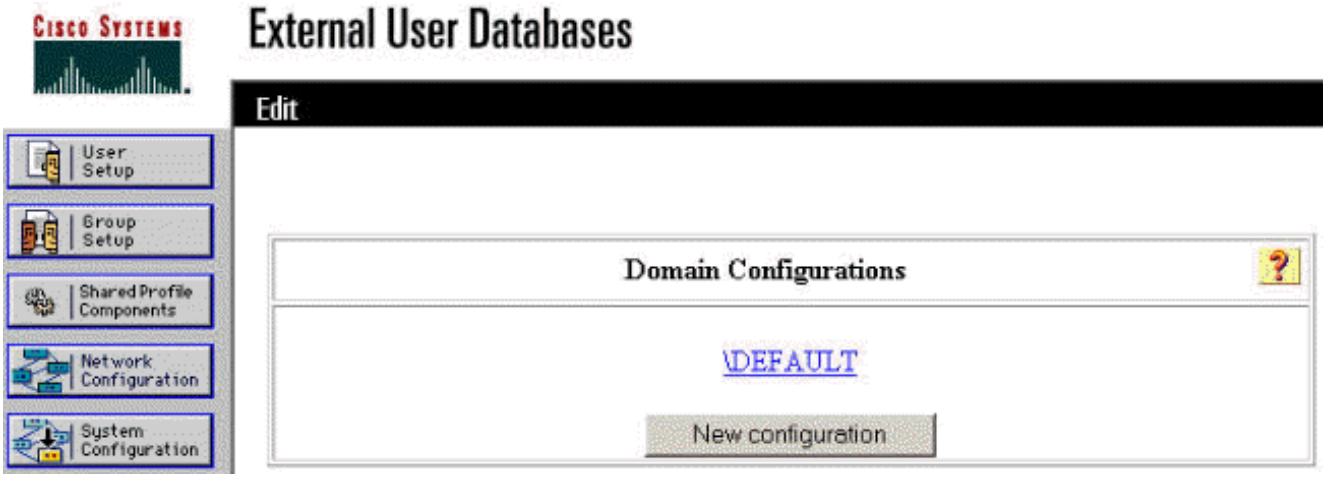
6. 从“可用域”(Available Domains)中选择NT域，然后点击右箭头按钮将其添加到“域列表”(Domain List)。 在“MS-CHAP设置”下，确保选中了“使用MS-CHAP版**本1和版本2允许密**码更**改”**选项。完成后，单击 **Submit。**



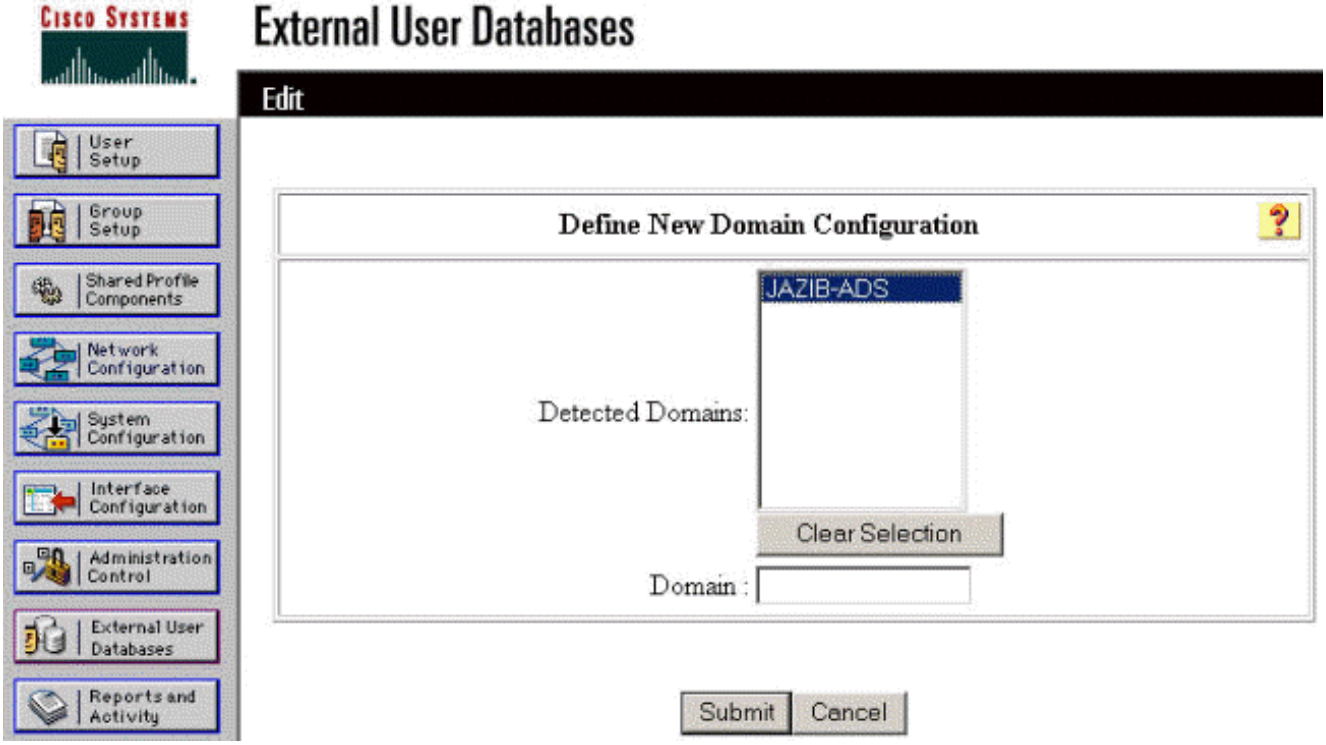
7. 单击左**面板中的**外部用户数据库，然后单击数据库组映**射的链**接(如本例所示)。 您应该看到之前配置的外部数据库的条目。以下示例显示“Radius/NT密码过期”的条目，该数据库是我们刚配置的。



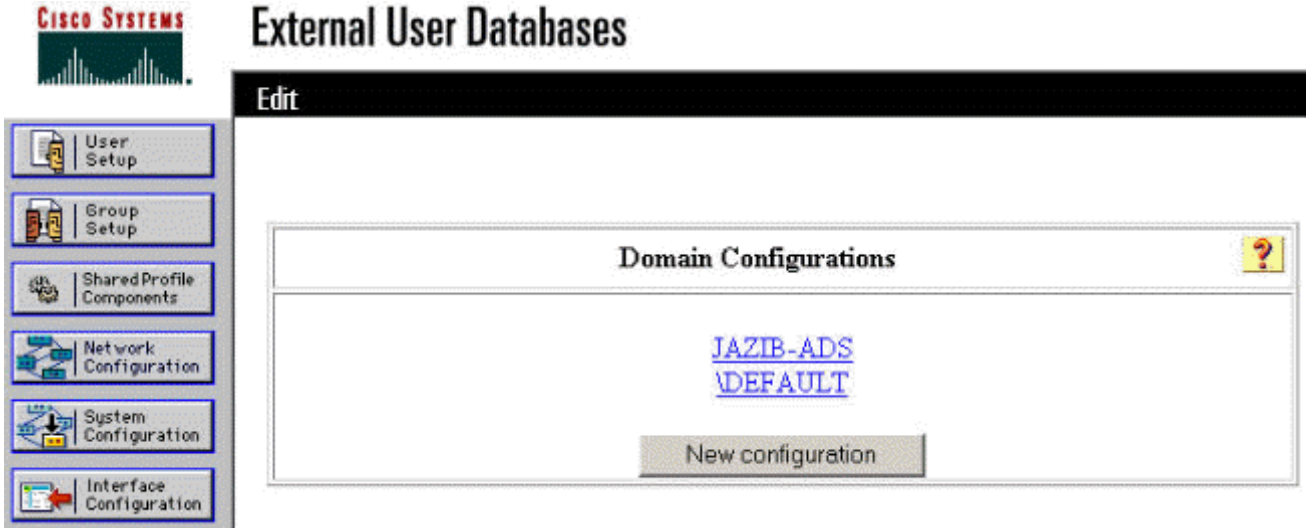
8. 在“域配置”屏幕上，单击“新**建配置**”以添加域配置。



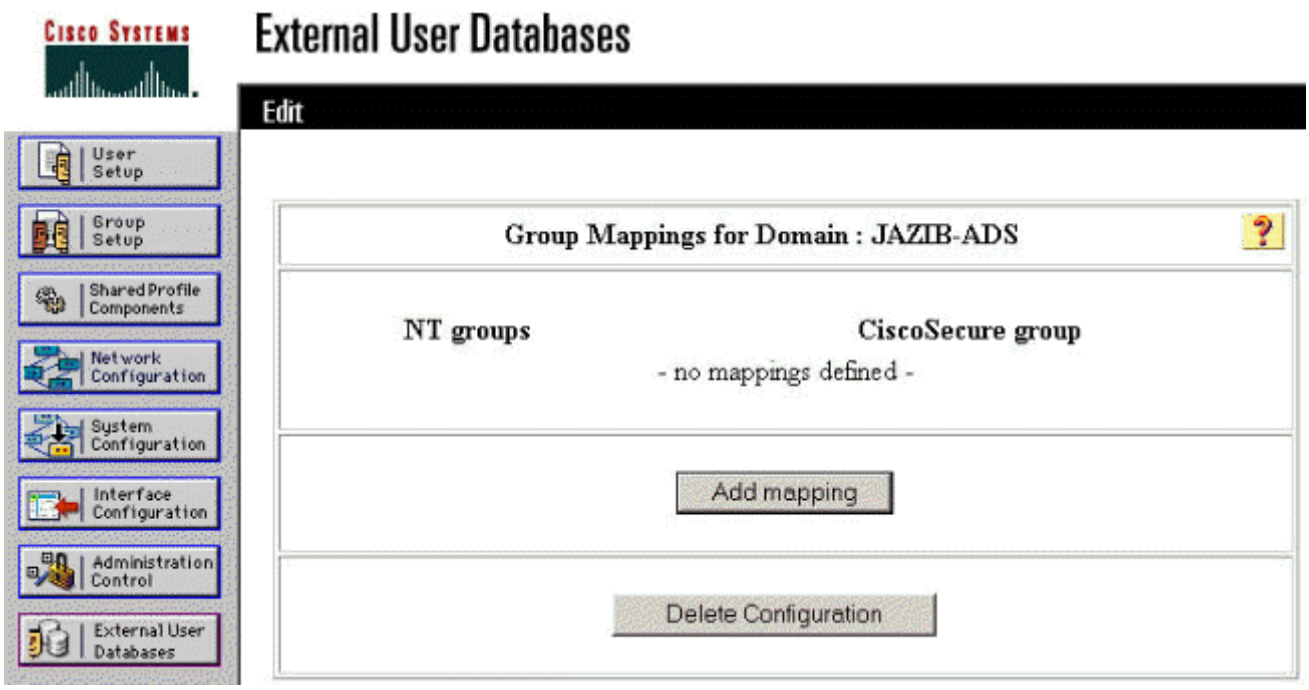
9. 从“检测到的域”列表中选择域，然后单击“提**交**”。以下示例显示名为“JAZIB-ADS”的域。



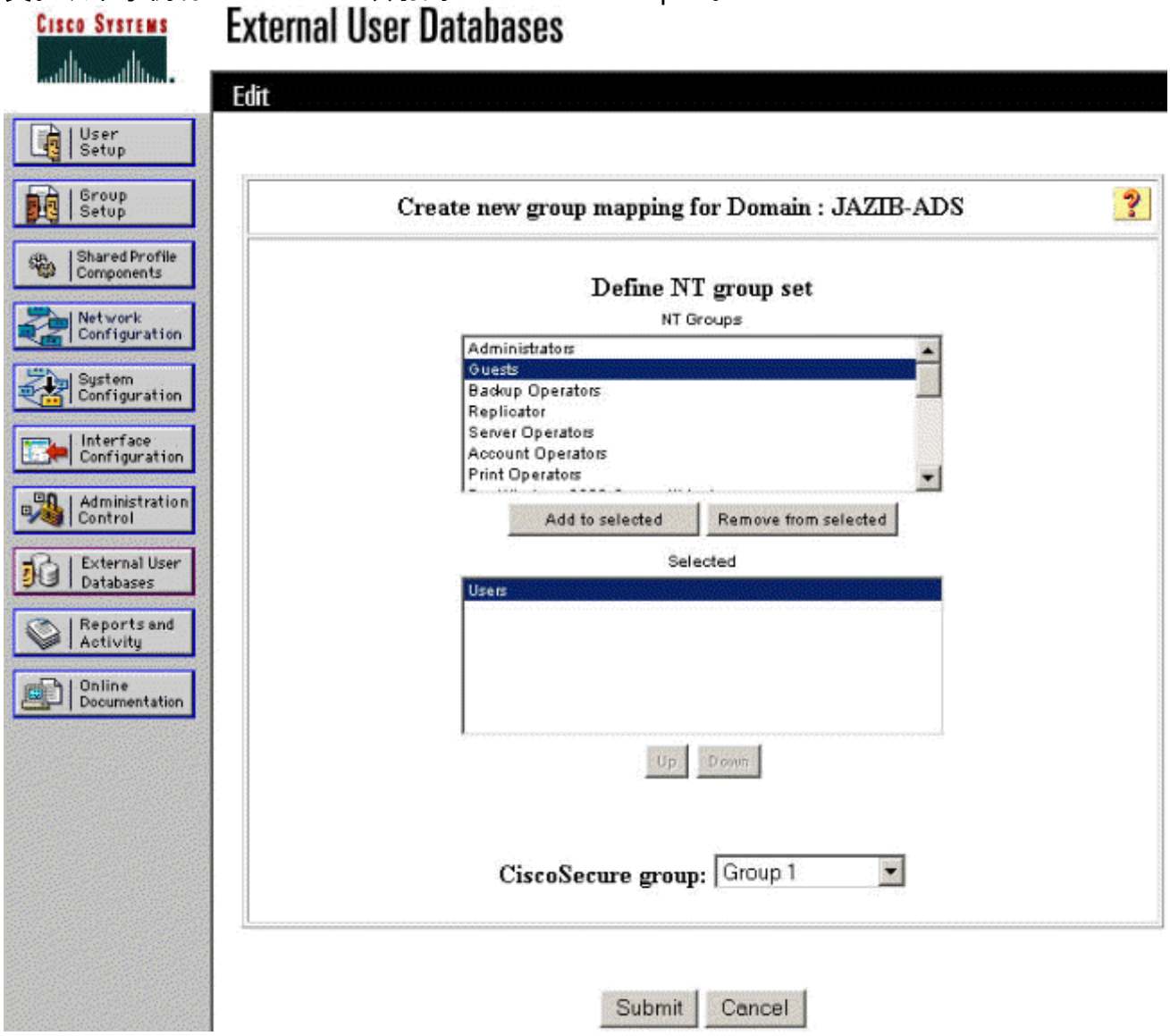
10. 单击域名以配置组映射。此示例显示域“JAZIB-ADS”。



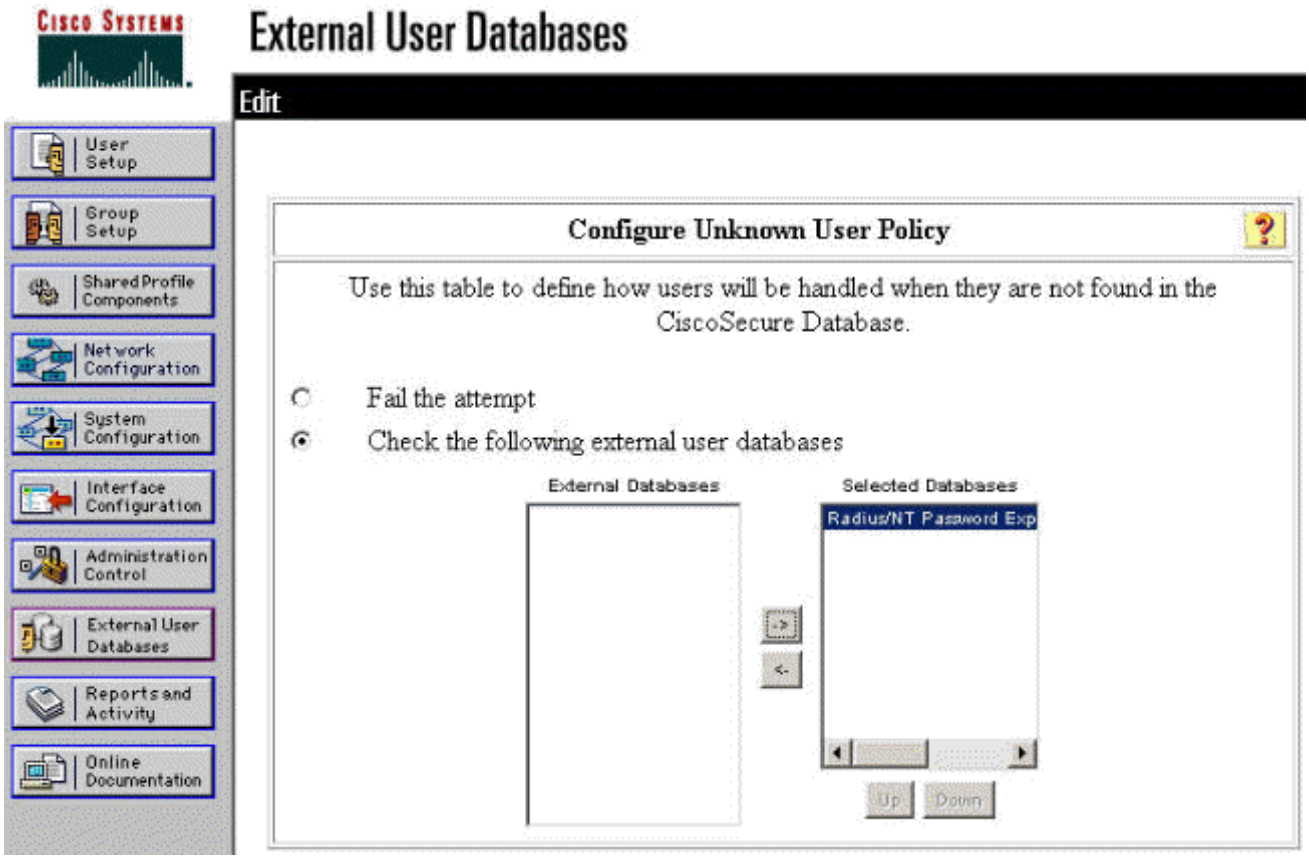
11. 单击**添加映**射以定义组映射。



12. 在“创建新组映射”屏幕上，将NT域上的组映射到CSNT RADIUS服务器上的组，然后单击**提交**。以下示例将NT组“Users”映射到RADIUS组“Group 1”。



13. 单击左**面板中的**外部用户数据库，然后单击未知用**户策略**的链接(如本例所示)。 确保选中了“检查以**下外部用户数据库”**选项。单击右箭头按钮，将先前配置的外部数据库从“外部数据库”列表移动到“选定数据库”列表。



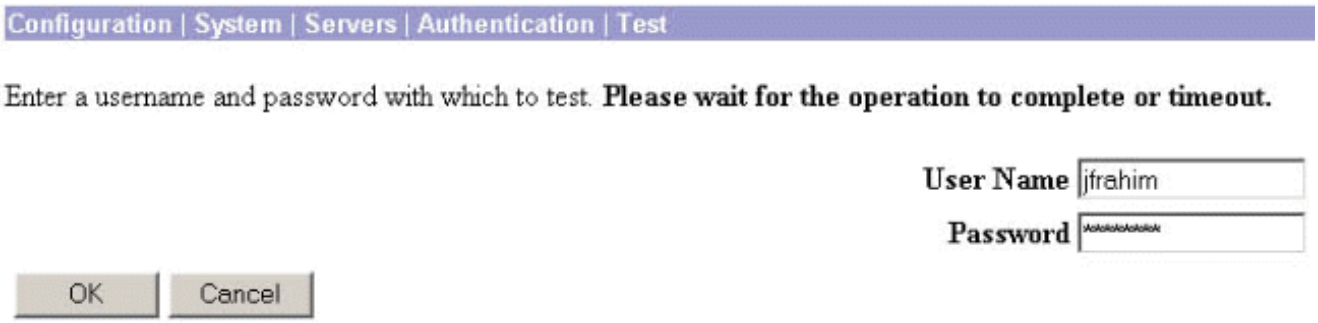
测试 NT/RADIUS密码到期功能

集中器提供测试RADIUS身份验证的功能。要正确测试此功能，请确保仔细执行这些步骤。

测试 RADIUS 验证

1. 转至**Configuration > System > Servers > Authentication**。选择您的RADIUS服务器并单击**测试**。

2. 出现提示时，键入NT域用户名和密码，然后单击**OK**。以下示例显示在NT域服务器上配置的用户名“jfrahim”，口令为“cisco123”。

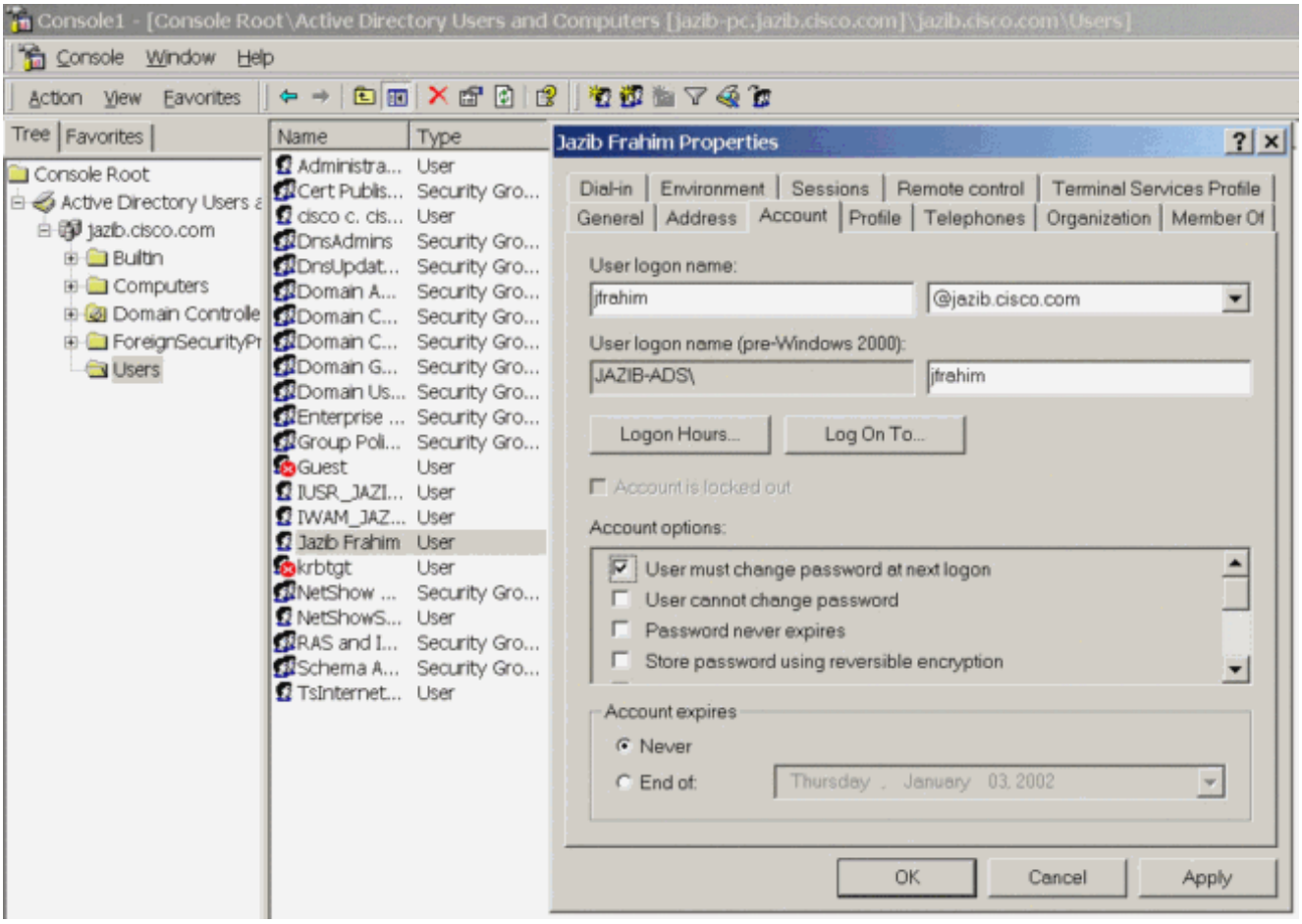


3. 如果身份验证设置正确，您应收到一条消息，指出“身份验证成功”。

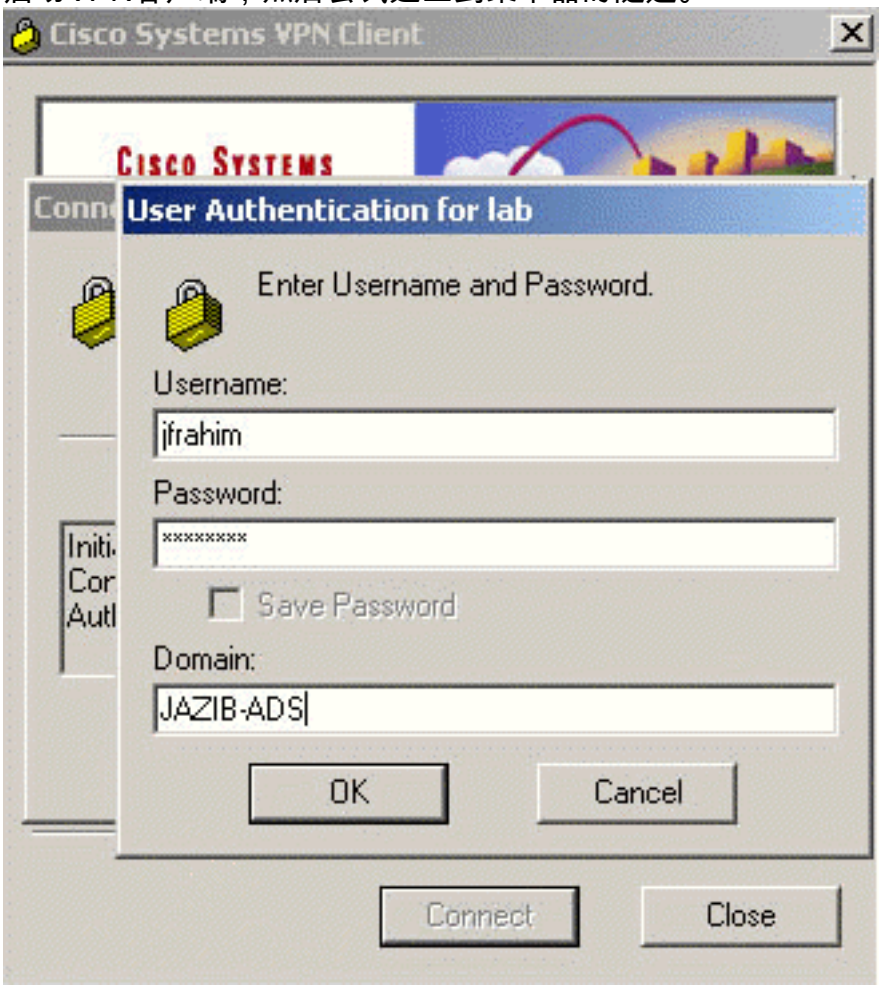
如果您收到除上面所示消息以外的任何消息，则会出现配置或连接问题。请重复本文档中概述的配置和测试步骤，以确保正确设置所有设置。另请检查设备之间的IP连接。

使用 RADIUS 代理测试密码到期功能时的实际的 NT 域验证

1. 如果用户已在域服务器上定义，请修改属性，以便在下次登录时提示用户更改密码。转到用户属性对话框的“帐户”选项卡，选择“用户必须在下次登录时更改密码”选项，然后单击“确定”。



2. 启动VPN客户端，然后尝试建立到集中器的隧道。



3. 在用户身份验证期间，应提示您更改密码。

相关信息

- Cisco VPN 3000 系列集中器
- IPsec
- 用于 Windows 的 Cisco 安全访问控制服务器
- RADIUS
- 请求注解 (RFC)