

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](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[网络图](#)

[配置 VPN 3000 集中器](#)

[组配置](#)

[RADIUS 配置](#)

[配置 Cisco Secure NT RADIUS 服务器](#)

[为 VPN 3000 集中器配置条目](#)

[为 NT 域验证配置未知用户策略](#)

[测试 NT/RADIUS密码到期功能](#)

[测试 RADIUS 验证](#)

[使用 RADIUS 代理测试密码到期功能时的实际的 NT 域验证](#)

[相关信息](#)

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

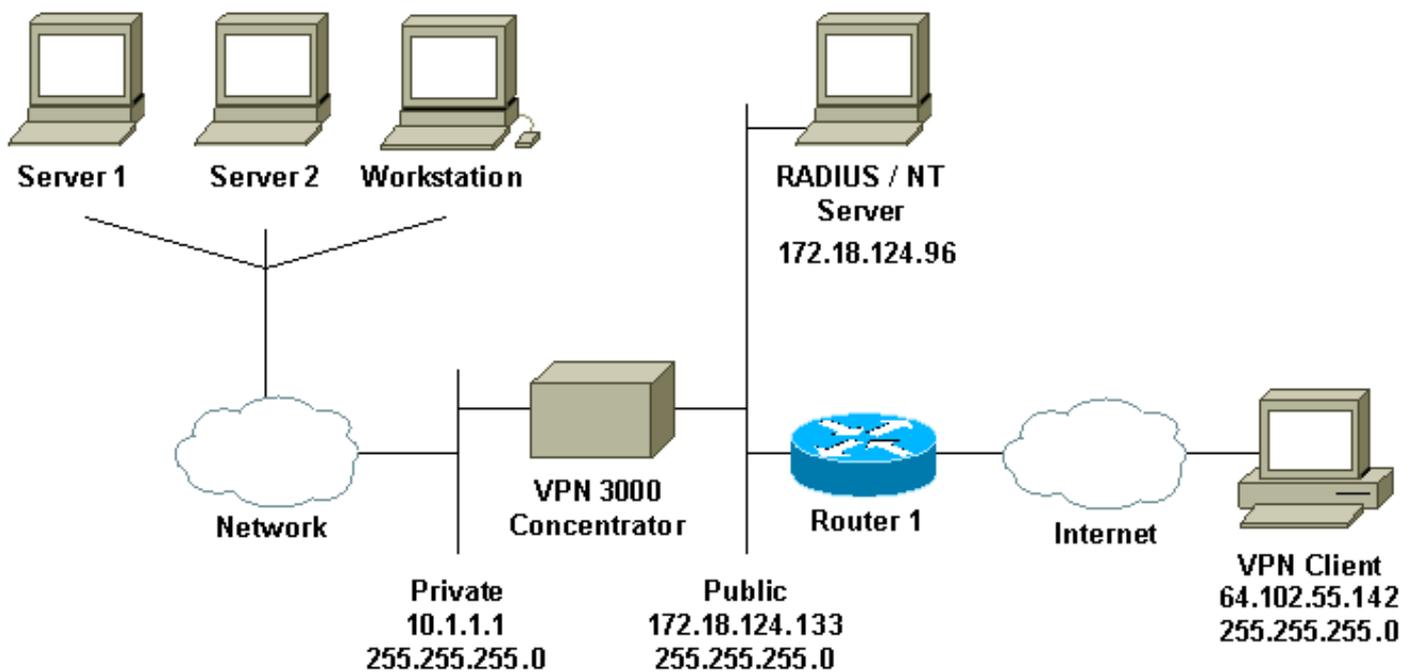
此配置使用下面软件和硬件版本开发并且被测试。

- 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。

This section lets you configure groups. A group is a collection of users treated as a single entity.

Click the **Add Group** button to add a group, or select a group and click **Delete Group** or **Modify Group**. To modify other group parameters, click **Modify Auth. Servers**, **Modify Acct. Servers**, **Modify Address Pools** or **Modify Client Update**.

Current Groups	Actions
ipsecgroup (Internally Configured)	Add Group
	Modify Group
	Modify Auth. Servers
	Modify Acct. Servers
	Modify Address Pools
	Modify Client Update
	Delete Group

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

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

IPSec Parameters			
Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5	<input checked="" type="checkbox"/>	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	<input checked="" type="checkbox"/>	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable the use of IKE keepalives for members of this group.
Reauthentication on Rekey	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to reauthenticate the user on an IKE (Phase-1) rekey.
Tunnel Type	Remote Access	<input checked="" type="checkbox"/>	Select the type of tunnel for this group. Update the Remote Access parameters below as needed.
Remote Access Parameters			
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Lock users into this group.
Authentication	RADIUS with Expiry	<input type="checkbox"/>	Select the authentication method for members of this group. This parameter does not apply to Individual User Authentication .
IPComp	None	<input checked="" type="checkbox"/>	Select the method of IP Compression for members of this group.
Mode Configuration	RADIUS with Expiry	<input checked="" type="checkbox"/>	Check to initiate the exchange of Mode Configuration parameters with the client. This must be checked if version 2.5 (or earlier) of the the Aliga/Cisco client are being used by members of this group.

Apply Cancel

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。

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Hardware Client Parameters			
Attribute	Value	Inherit?	Description
Require Interactive Hardware Client Authentication	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Check to require the hardware client to be interactively authenticated at each connection attempt.
Require Individual User Authentication	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to require users behind a hardware client to be authenticated.
User Idle Timeout	30	<input checked="" type="checkbox"/>	Enter the session idle timeout in minutes. Use 0 for no timeout.
Cisco IP Phone Bypass	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow Cisco IP Phones to bypass Individual User Authentication behind a hardware client.

Apply Cancel

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。

This section lets you configure parameters for servers that authenticate users.

You should have a properly configured RADIUS, NT Domain, or SDI server to access, or you can configure the internal server and [add users to the internal database](#).

Click the **Add** button to add a server, or select a server and click **Modify**, **Delete**, **Move**, or **Test**.

Authentication Servers	Actions
Internal (Internal)	Add
	Modify
	Delete
	Move Up
	Move Down
	Test

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**

Retries = **2**

Server Secret = **cisco123**

Verify: **cisco123**

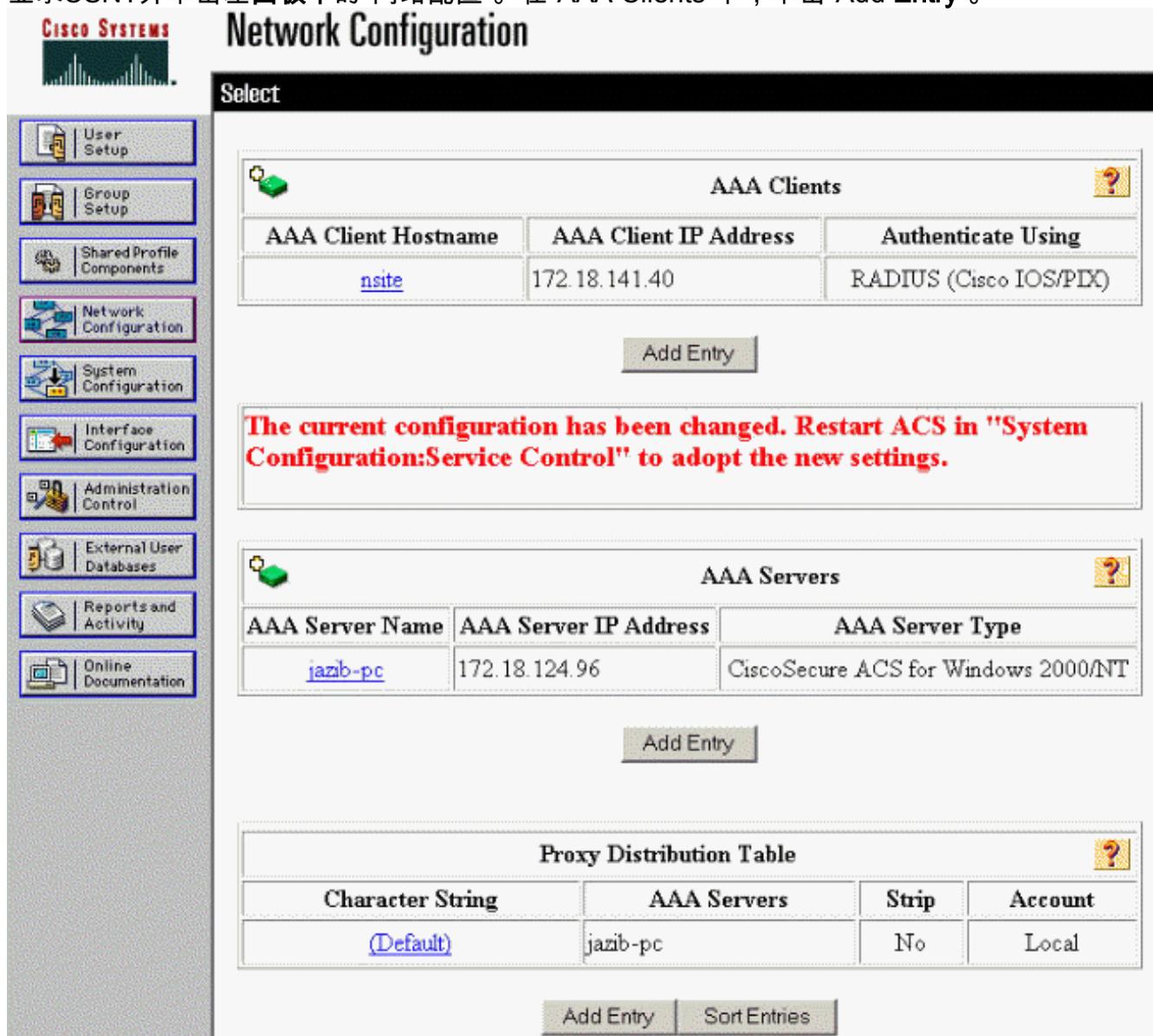
Configure and add a user authentication server.

Server Type	<input type="text" value="RADIUS"/>	Selecting <i>Internal Server</i> will let you add users to the internal user database.
Authentication Server	<input type="text" value="172.18.124.96"/>	Enter IP address or hostname.
Server Port	<input type="text" value="0"/>	Enter 0 for default port (1645).
Timeout	<input type="text" value="4"/>	Enter the timeout for this server (seconds).
Retries	<input type="text" value="2"/>	Enter the number of retries for this server.
Server Secret	<input type="password" value="*****"/>	Enter the RADIUS server secret.
Verify	<input type="password" value="*****"/>	Re-enter the secret.

[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”。



Network Configuration

Select

AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
nsite	172.18.141.40	RADIUS (Cisco IOS/PIX)

Add Entry

The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings.

AAA Servers

AAA Server Name	AAA Server IP Address	AAA Server Type
jazib-pc	172.18.124.96	CiscoSecure ACS for Windows 2000/NT

Add Entry

Proxy Distribution Table

Character String	AAA Servers	Strip	Account
(Default)	jazib-pc	No	Local

Add Entry Sort Entries

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)**



Network Configuration

Edit



Add AAA Client

AAA Client Hostname	<input type="text" value="133_3000_conc"/>
AAA Client IP Address	<input type="text" value="172.18.124.133"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="text" value="RADIUS (Cisco VPN 3000)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	

3000集中器的条目将显示在“AAA Clients”部分下。



Network Configuration

Select



AAA Clients		
AAA Client Hostname	AAA Client IP Address	Authenticate Using
133_3000_conc	172.18.124.133	RADIUS (Cisco VPN 3000)
nsite	172.18.141.40	RADIUS (Cisco IOS/PIX)

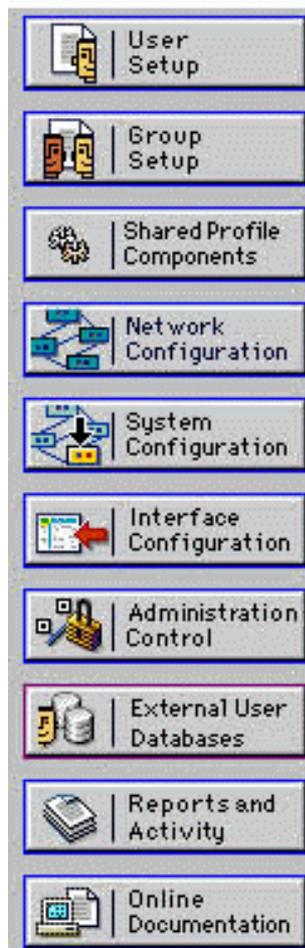
[为 NT 域验证配置未知用户策略](#)

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连接。

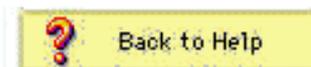


External User Databases

Select



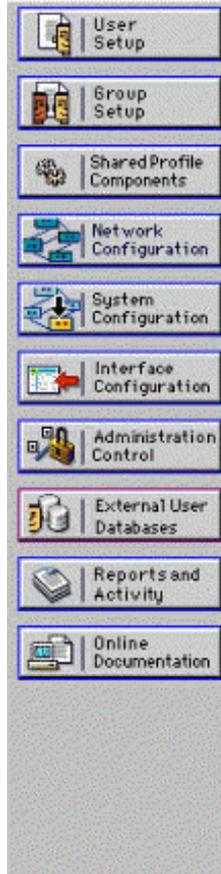
- [Unknown User Policy](#)
- [Database Group Mappings](#)
- [Database Configuration](#)



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



External User Databases



Select

External User Database Configuration

Choose which external user database type to configure.

- [NIS/NIS+](#)
- [LEAP Proxy RADIUS Server](#)
- [Windows NT/2000](#)
- [Novell NDS](#)
- [Generic LDAP](#)
- [External ODBC Database](#)
- [RADIUS Token Server](#)
- [AXENT Token Server](#)
- [CRYPTOCARD Token Server](#)
- [SafeWord Token Server](#)
- [SDI SecurID Token Server](#)

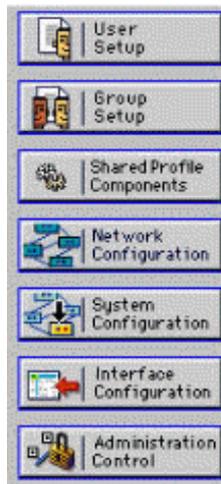
[List all database configurations](#)

Cancel

3. 在“数据库配置创建”屏幕上，单击**创建新配置**。



External User Databases



Edit

Database Configuration Creation

Click here to create a new configuration for the Windows NT/2000 database.

Create New Configuration

Cancel

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”。



External User Databases

Edit



Create a new External Database Configuration 

Enter a name for the new configuration for Windows NT/2000

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



External User Databases

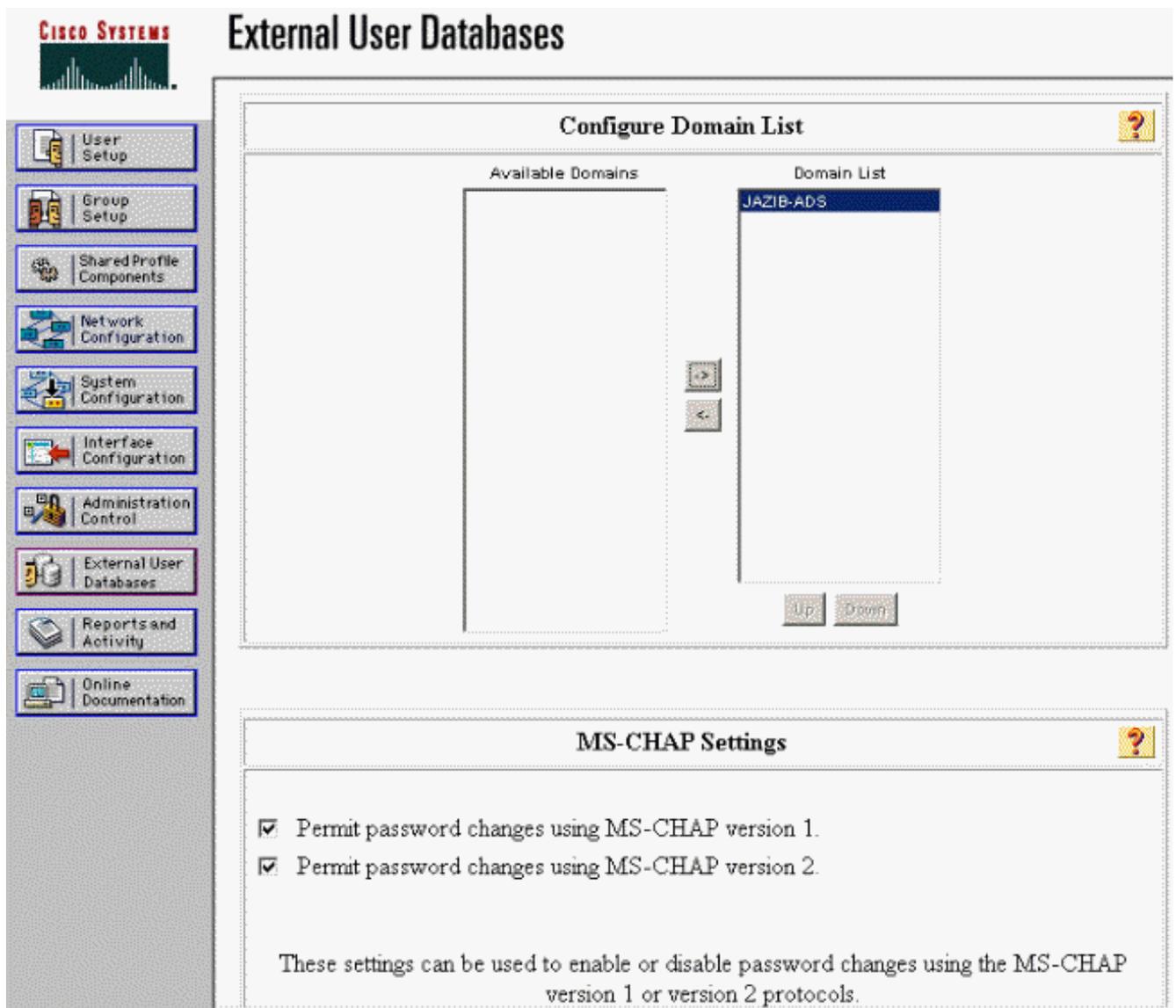
Edit



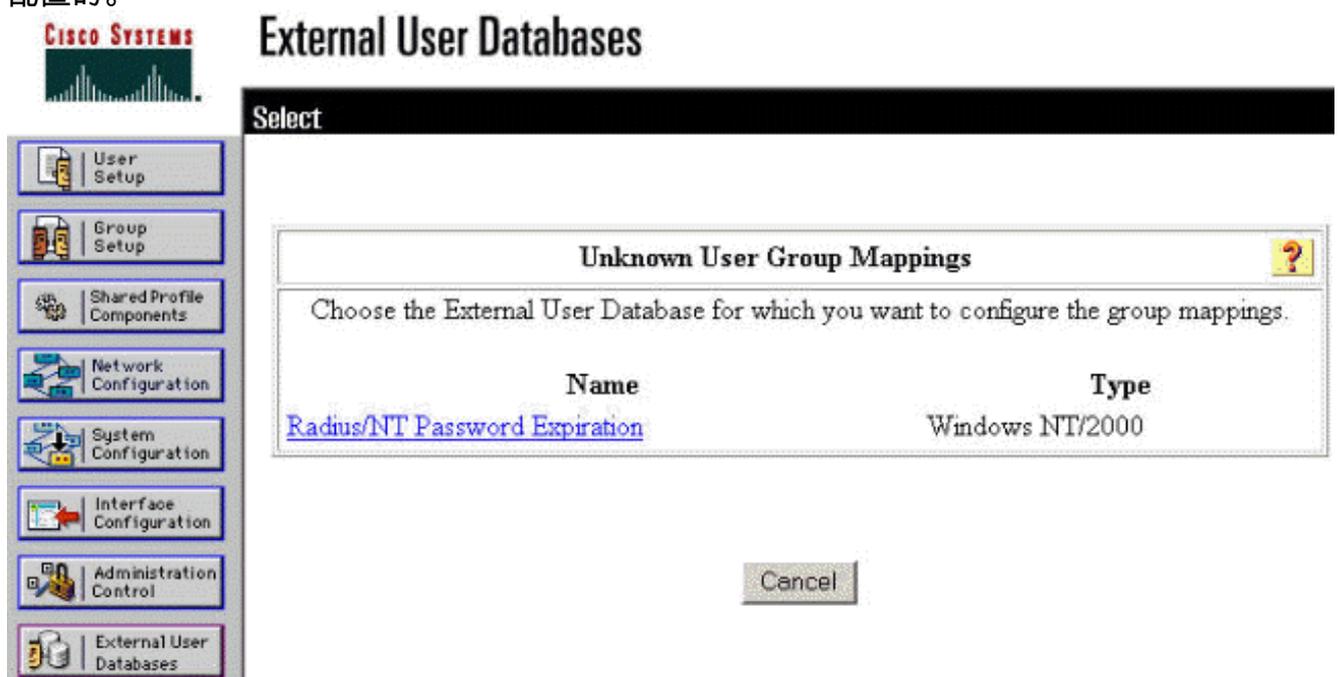
External User Database Configuration 

Choose what to do with the Windows NT/2000 database.

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。



External User Databases



Edit

Domain Configurations 

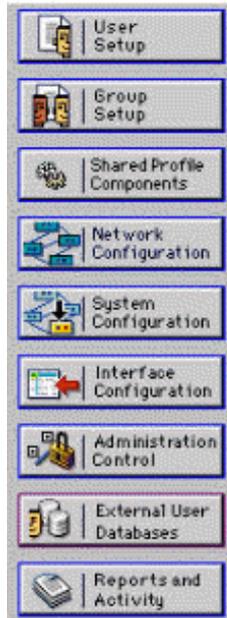
[DEFAULT](#)

New configuration

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。



External User Databases



Edit

Define New Domain Configuration 

Detected Domains:

[JAZIB-ADS](#)

Clear Selection

Domain:

Submit Cancel

10. 单击域名以配置组映射。此示例显示域“JAZIB-ADS”。



External User Databases



Edit

Domain Configurations 

[JAZIB-ADS](#)

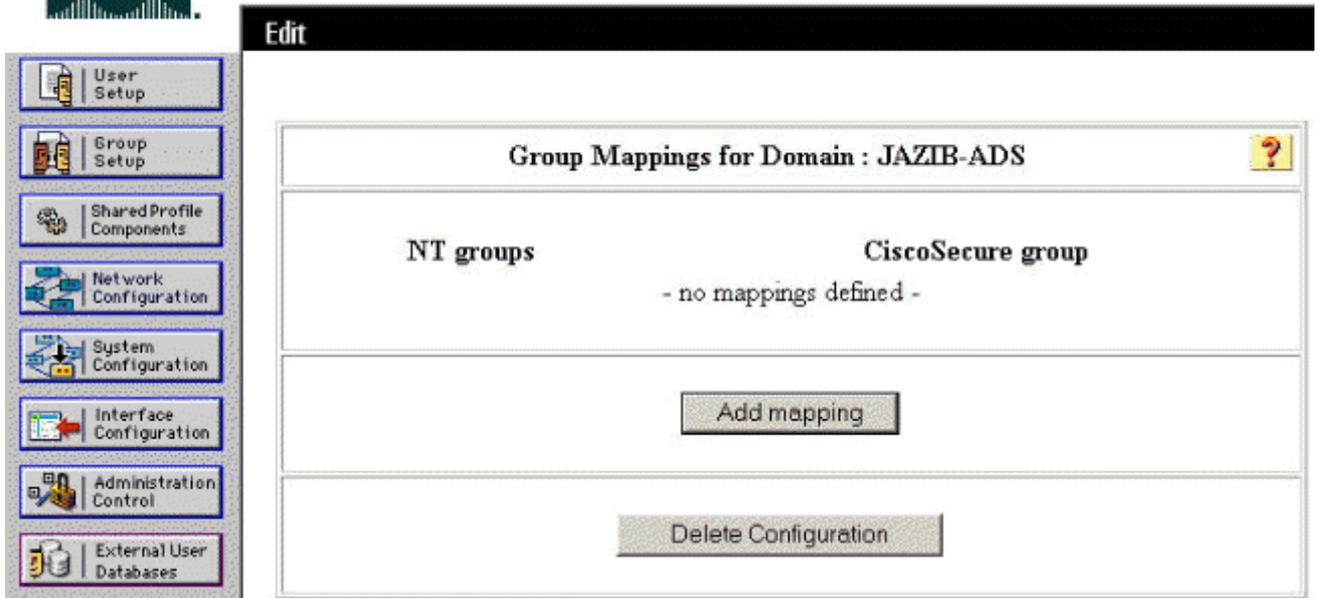
[DEFAULT](#)

New configuration

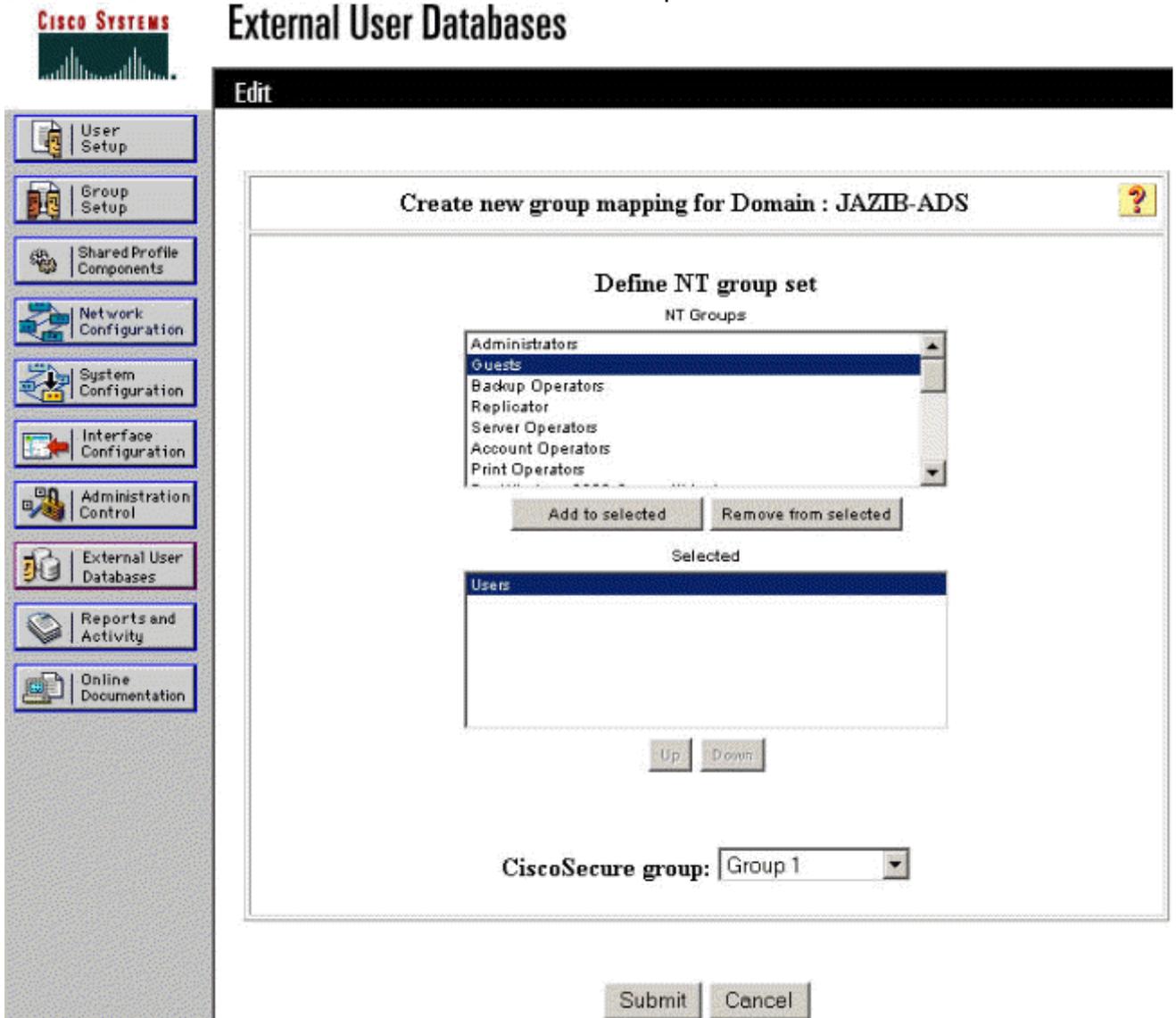
11. 单击添加映射以定义组映射。



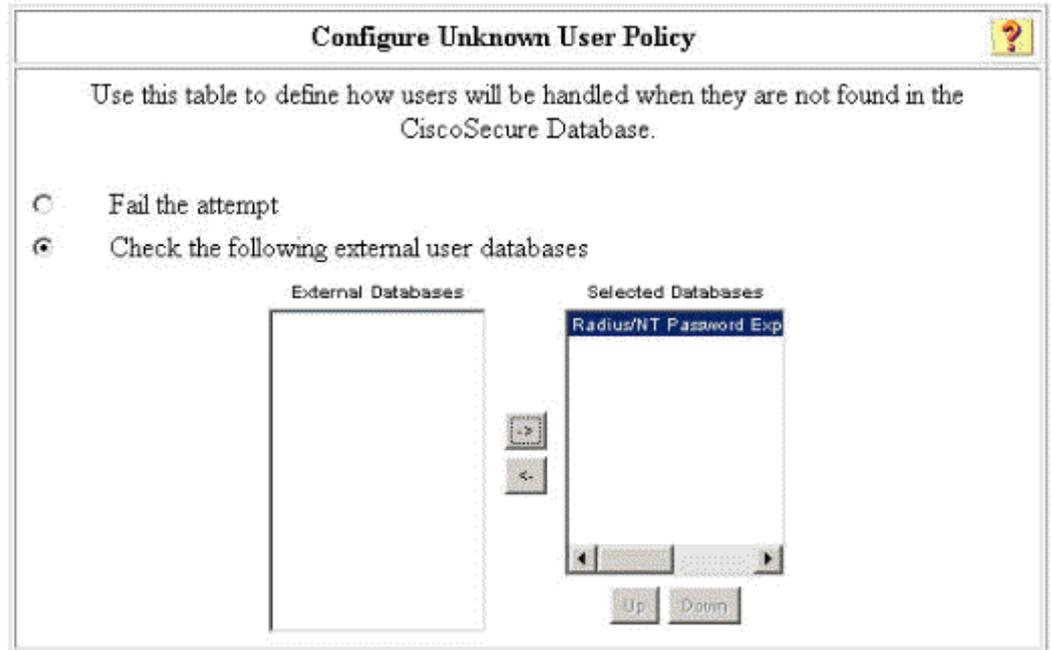
External User Databases



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。

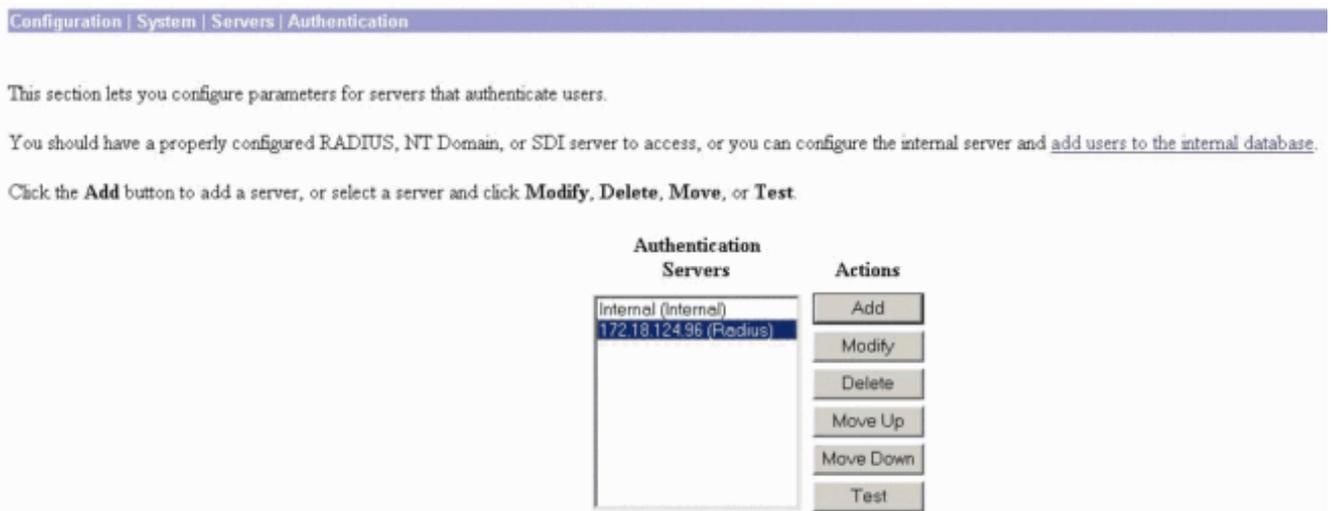


测试 NT/RADIUS密码到期功能

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“jfracim”，口令为“cisco123”。

Enter a username and password with which to test. **Please wait for the operation to complete or timeout.**

User Name
Password

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”。

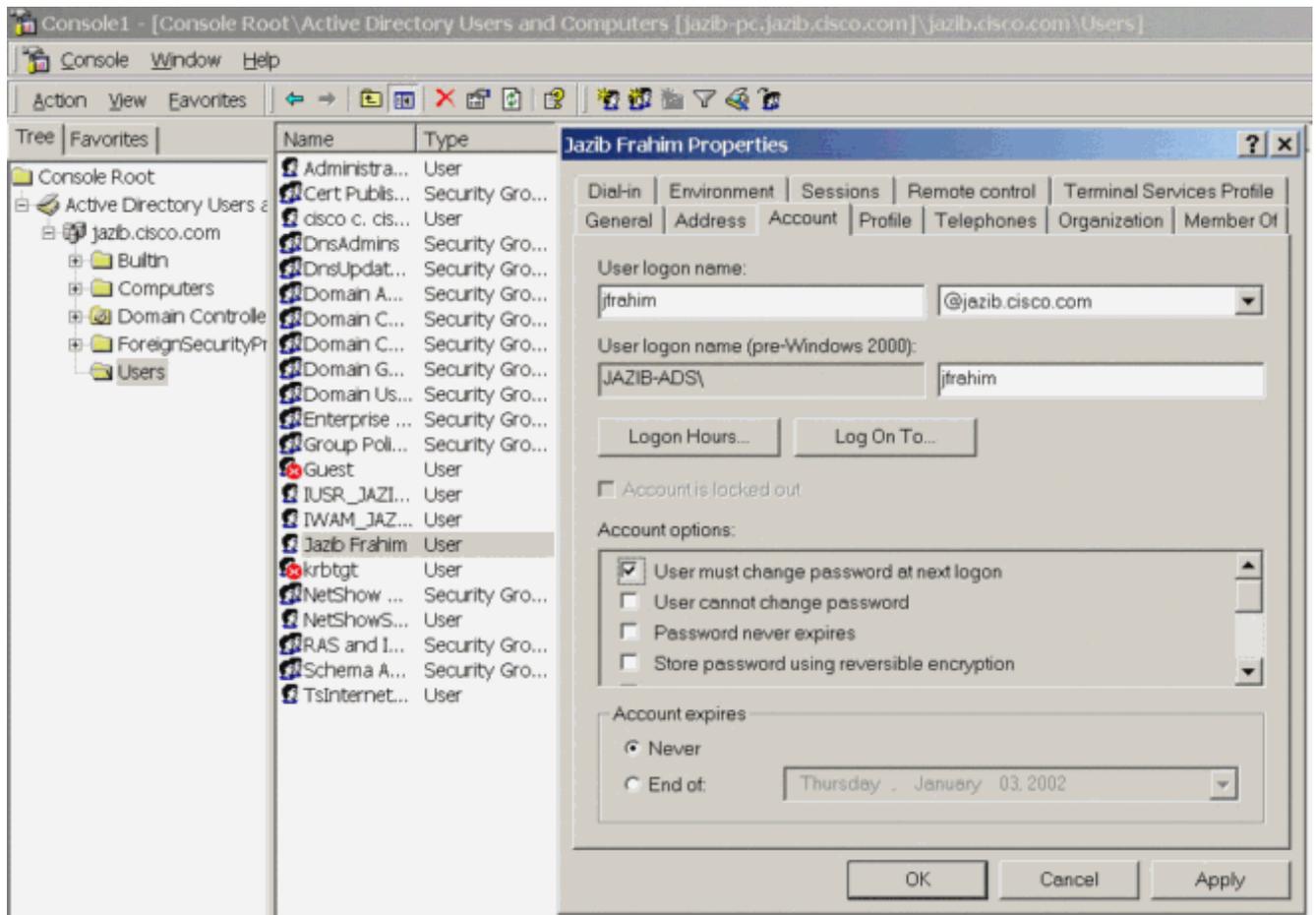
Success

 Authentication Successful

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](#)

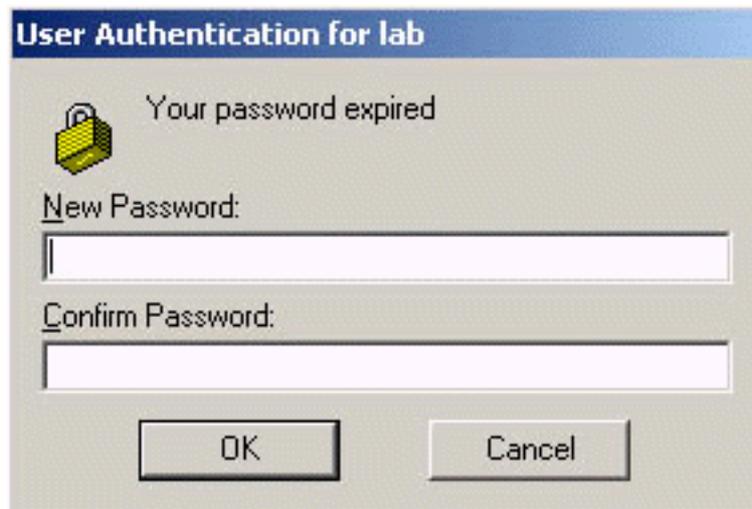
1. 如果用户已在域服务器上定义，请修改属性，以便在下次登录时提示用户更改密码。转到用户属性对话框的“帐户”选项卡，选择“用户必须在下次登录时更改密码”选项，然后单击“确定”。



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 \(RFC\)](#)