

# 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

使用RADIUS服务器，本文包括关于如何的逐步指导配置Cisco VPN 3000系列集中器支持NT口令有效期功能。

参考的[VPN3000 RADIUS with Expiry功能使用Microsoft互联网验证服务器](#)为了学习与互联网认证服务器(IAS)的更加大致同样的案例。

## 先决条件

### 要求

- 如果您的RADIUS服务器和NT域验证服务器在两个独立的机器，请确保您设立了在两台机器之间的IP连通性。
- 确保您设立了从集中器的IP连通性到RADIUS服务器。如果RADIUS服务器是往公共接口，请勿忘记打开公共过滤器的RADIUS端口。
- 保证您能连接到从使用内部用户数据库的VPN客户端的集中器。如果这没有配置，请参考[配置Ipssec- Cisco 3000 VPN客户端对VPN 3000集中器](#)。

**注意：** 密码到期功能不可能与Web VPN或SSL VPN客户端一起使用。

## 使用的组件

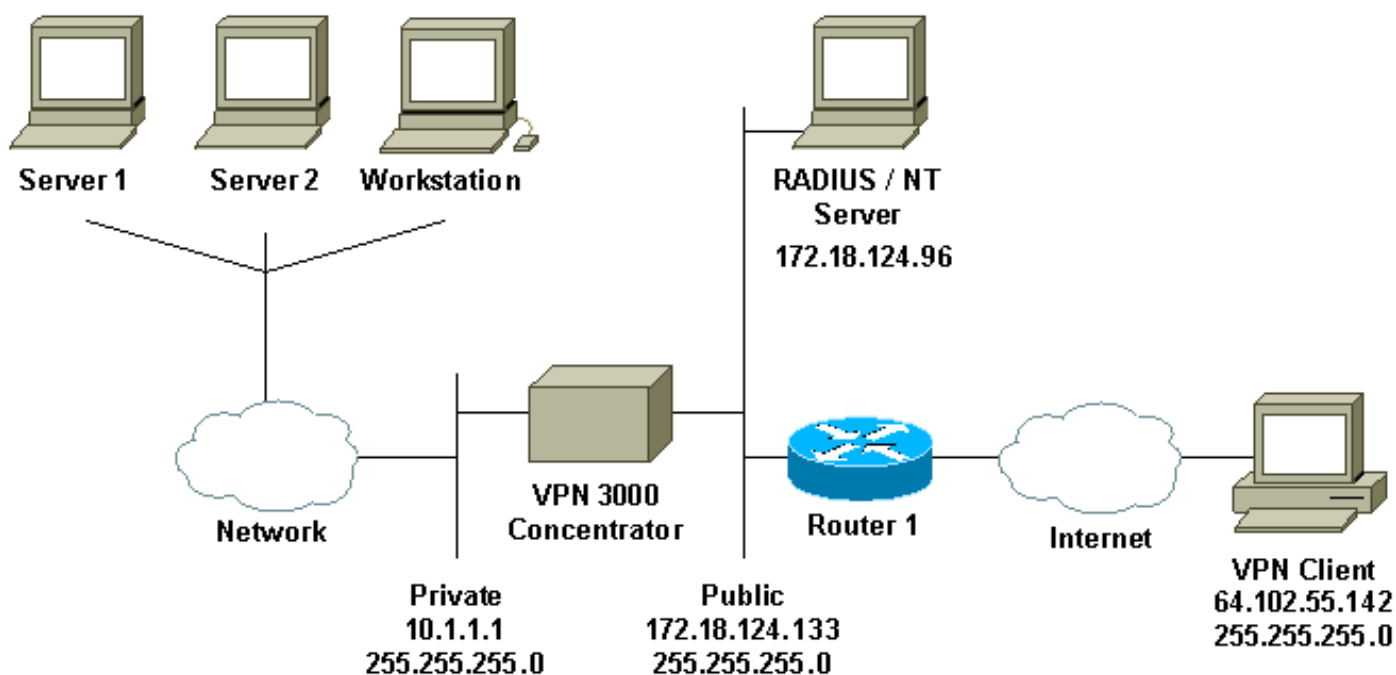
此配置使用下面软件和硬件版本开发并且被测试。

- VPN 3000集中器软件版本4.7
- VPN客户端版本3.5
- NT (CSNT)版本3.0 Microsoft Windows 2000激活目录服务器的Cisco Secure用户认证的

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. RADIUS服务器在此配置方面在公共接口。如果这是有您的特定设置的实际情形，请创建在您的公共过滤器的两个规则允许RADIUS流量输入和留下集中器。
2. 此配置显示运行在同样计算机的CSNT软件和NT域验证服务。这些元素在两个独立的机器可以如果必须由您的配置负责。

## 配置 VPN 3000 集中器

### 组配置

1. 要配置组接受从RADIUS服务器的NT口令有效期参数，去**Configuration > User Management > Groups**，选择您的从列表的组，和点击**修改组**。下面的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. 去IPSec选项，确保，RADIUS with Expiry为验证属性选择。

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 <b>Individual User Authentication</b> .
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.

## 3. 如果在VPN 3002 Hardware Clients希望此功能启用，请去HW Client选项，确保，Require Interactive Hardware Client Authentication启用，则单击应用。

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.

## RADIUS 配置

### 1. 要配置在集中器的RADIUS服务器设置，请去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

- 在**Add**屏幕上，请键入对应于RADIUS服务器并且单击**添加**的值。下面的示例使用以下值。  
 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.
<input type="button" value="Add"/> <input type="button" value="Cancel"/>		

## 配置 Cisco Secure NT RADIUS 服务器

### 为 VPN 3000 集中器配置条目

- 登录CSNT并且点击**网络配置**在左面板中。在“AAA客户端下”，请点击**Add**条目。

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Reports and Activity
- Online Documentation

AAA Clients		
AAA Client Hostname	AAA Client IP Address	Authenticate Using
<a href="#">nsite</a>	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
<a href="#">jazib-pc</a>	172.18.124.96	CiscoSecure ACS for Windows 2000/NT

Add Entry

Proxy Distribution Table			
Character String	AAA Servers	Strip	Account
<a href="#">(Default)</a>	jazib-pc	No	Local

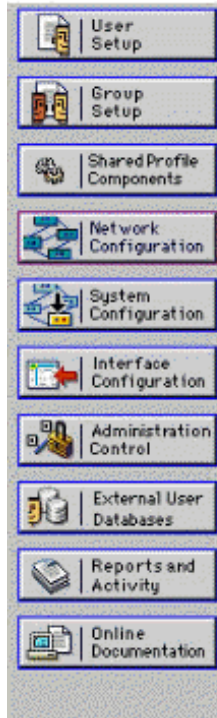
Add Entry    Sort Entries

2. 在“请添加AAA客户端”屏幕，输入适当的值添加集中器作为RADIUS客户端，然后点击 **Submit+Restart**。下面的示例使用以下值。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

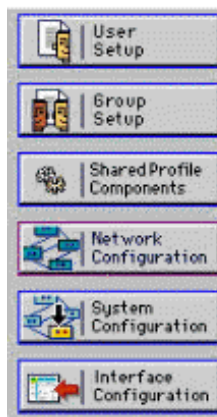
AAA Client Hostname	<input type="text" value="133_3000_conc"/>
AAA Client IP Address	<input type="text" value="172.18.124.133"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="text" value="RADIUS (Cisco VPN 3000)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (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	

您的3000集中器的一个条目将出现在“AAA客户端”部分下。



## Network Configuration

Select



AAA Clients		
AAA Client Hostname	AAA Client IP Address	Authenticate Using
<a href="#">133_3000_conc</a>	172.18.124.133	RADIUS (Cisco VPN 3000)
<a href="#">nsite</a>	172.18.141.40	RADIUS (Cisco IOS/PIX)

### [为 NT 域验证配置未知用户策略](#)

1. 要配置在RADIUS服务器的用户认证作为未知用户策略的部分，请点击外部用户数据库在左面板中，然后点击数据库配置的链路。




# External User Databases

## Select

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Reports and Activity
- Online Documentation

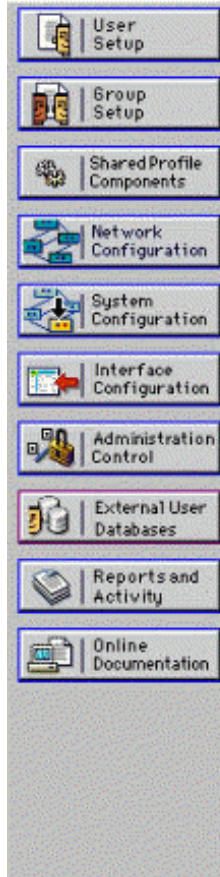
- [Unknown User Policy](#)
- [Database Group Mappings](#)
- [Database Configuration](#)

 [Back to Help](#)

2. 在“外部用户数据库配置下”，请点击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](#)

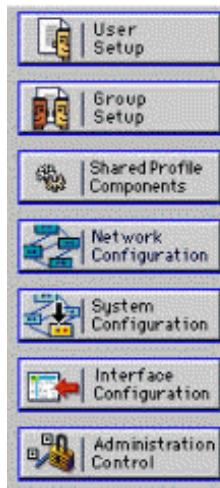
[List all database configurations](#)

Cancel

3. 在“数据库配置创建”屏幕，请单击创建新的配置。



## 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. 当提示，请键入一名称对于NT/2000验证并且单击提交。下面的示例显示命名“Radius/NT密码到期”。






## External User Databases

Edit



**Create a new External Database Configuration** 

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


5. 单击**配置**配置用户认证的域名。



## External User Databases

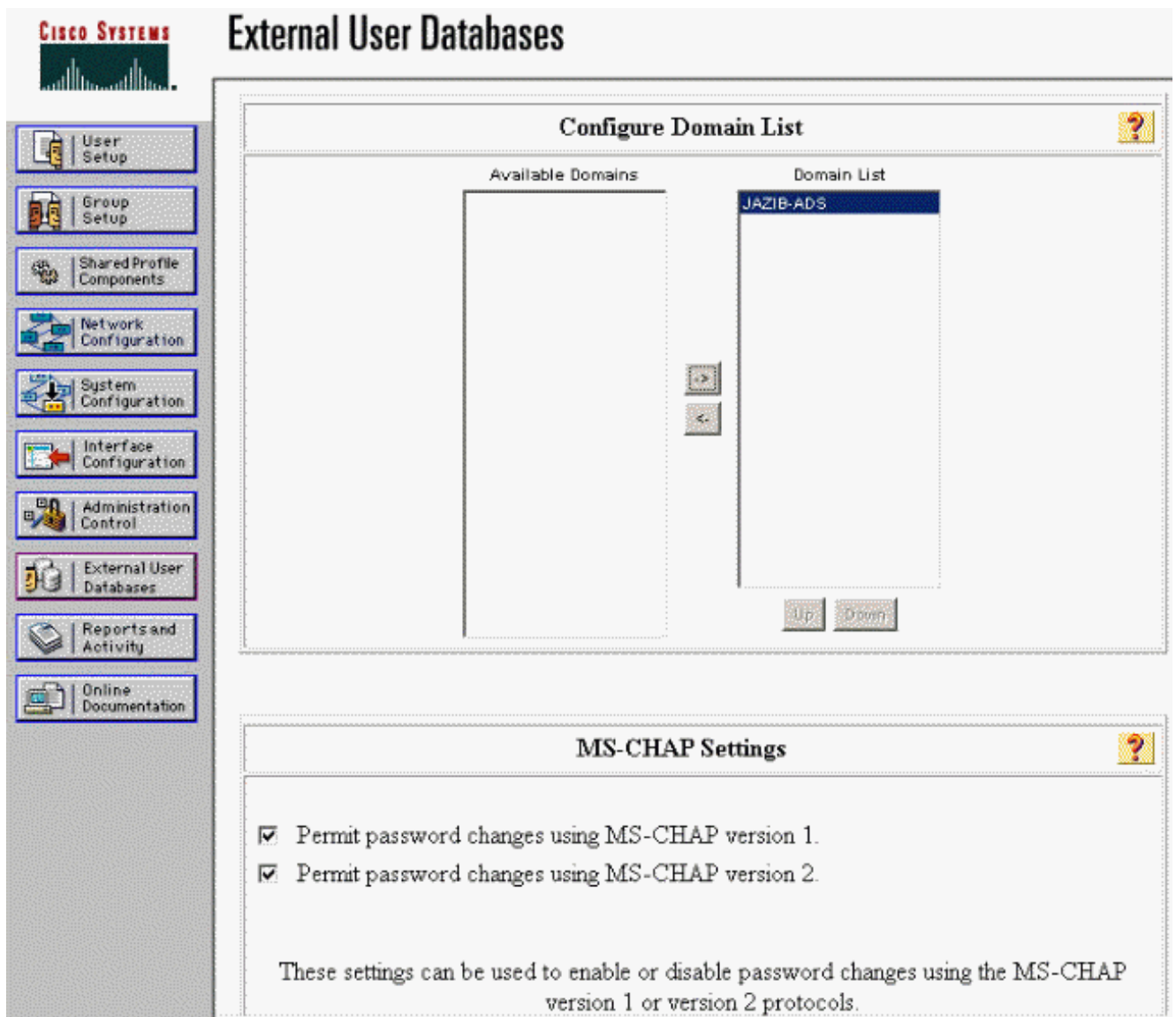
Edit



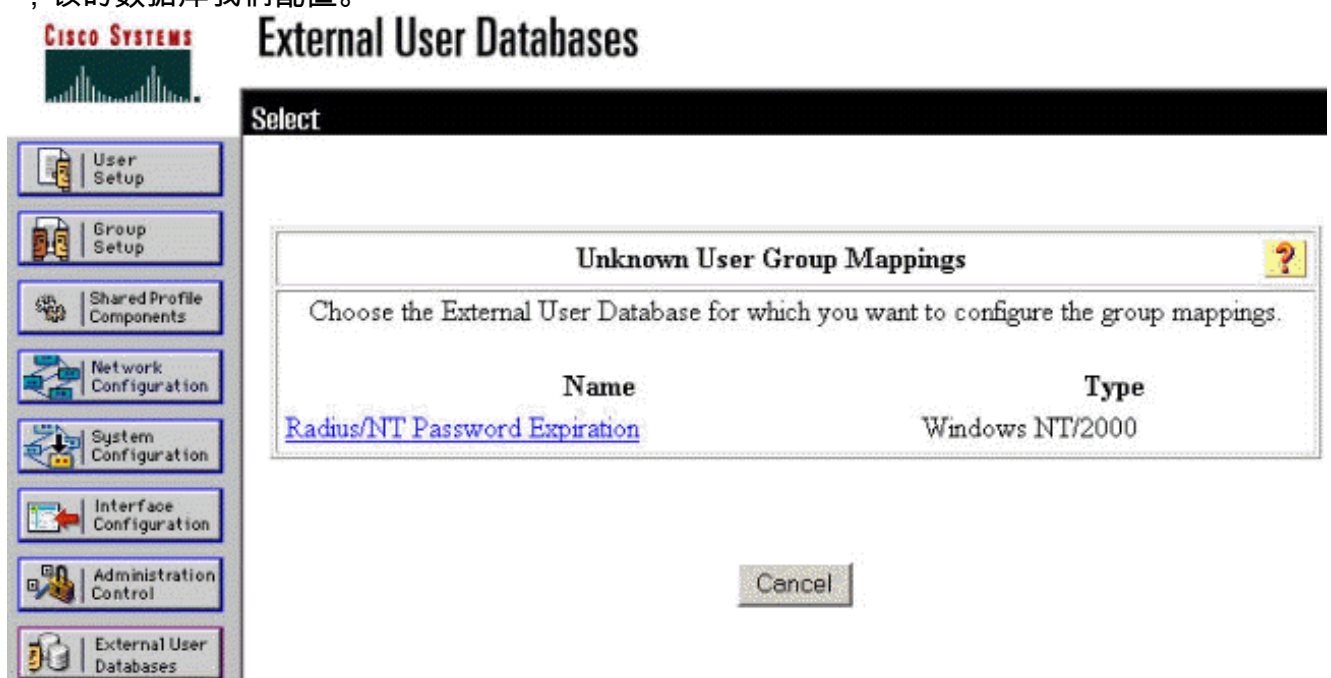
**External User Database Configuration** 

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

6. 选择您的从“可用的域的NT域”，然后单击右箭头按钮添加它对“域列表”。在“MS-CHAP设置下”，请保证**Permit**密码更改使用**MS-CHAP版本1**和**版本2**的选项选择。完成后，单击 **Submit**。



7. 点击外部用户数据库在左面板中，然后点击数据库组映射的链路(如在此[示例中看到](#))。您应该为您的以前已配置的外部数据库看到条目。下面的示例显示“Radius/NT密码到期”的一个条目”，该的数据库我们配置。



8. 在“域配置”请筛选，点击新的配置添加域配置。



## External User Databases



Edit

Domain Configurations 

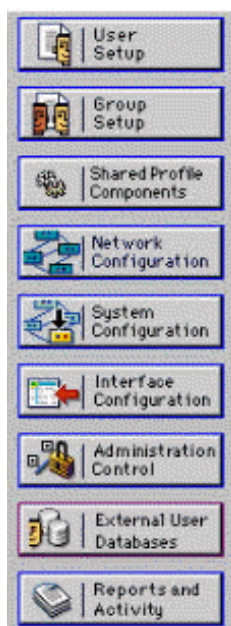
[\DEFAULT](#)

New configuration


9. 选择您的从“检测的域”列表的域并且单击提交。下面的示例显示名为“JAZIB-ADS的域”。



## External User Databases



Edit

Define New Domain Configuration 

Detected Domains:

[JAZIB-ADS](#)

Clear Selection

Domain:

Submit Cancel


10. 点击您的域名配置组映射。此示例显示域“JAZIB-ADS”。



## External User Databases



Edit

Domain Configurations 

[JAZIB-ADS](#)

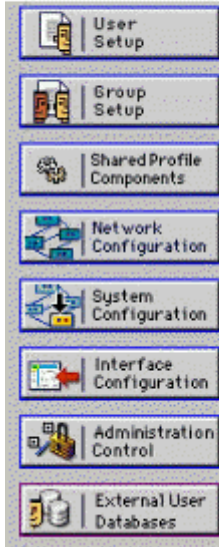
[\DEFAULT](#)

New configuration

11. 单击添加映射定义组映射。



## External User Databases



Edit

Group Mappings for Domain : JAZIB-ADS

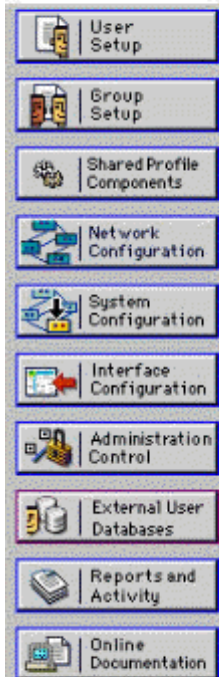
NT groups	CiscoSecure group
	- no mappings defined -
<input type="button" value="Add mapping"/>	
<input type="button" value="Delete Configuration"/>	

12. 在“创建新的组映射”屏幕，映射NT域的组给CSNT RADIUS服务器的一组，然后单击提交。示例下面的地图NT组“用户” RADIUS组的“组

1.”



## External User Databases



Edit

Create new group mapping for Domain : JAZIB-ADS

Define NT group set

NT Groups

- Administrators
- Guests**
- Backup Operators
- Replicator
- Server Operators
- Account Operators
- Print Operators

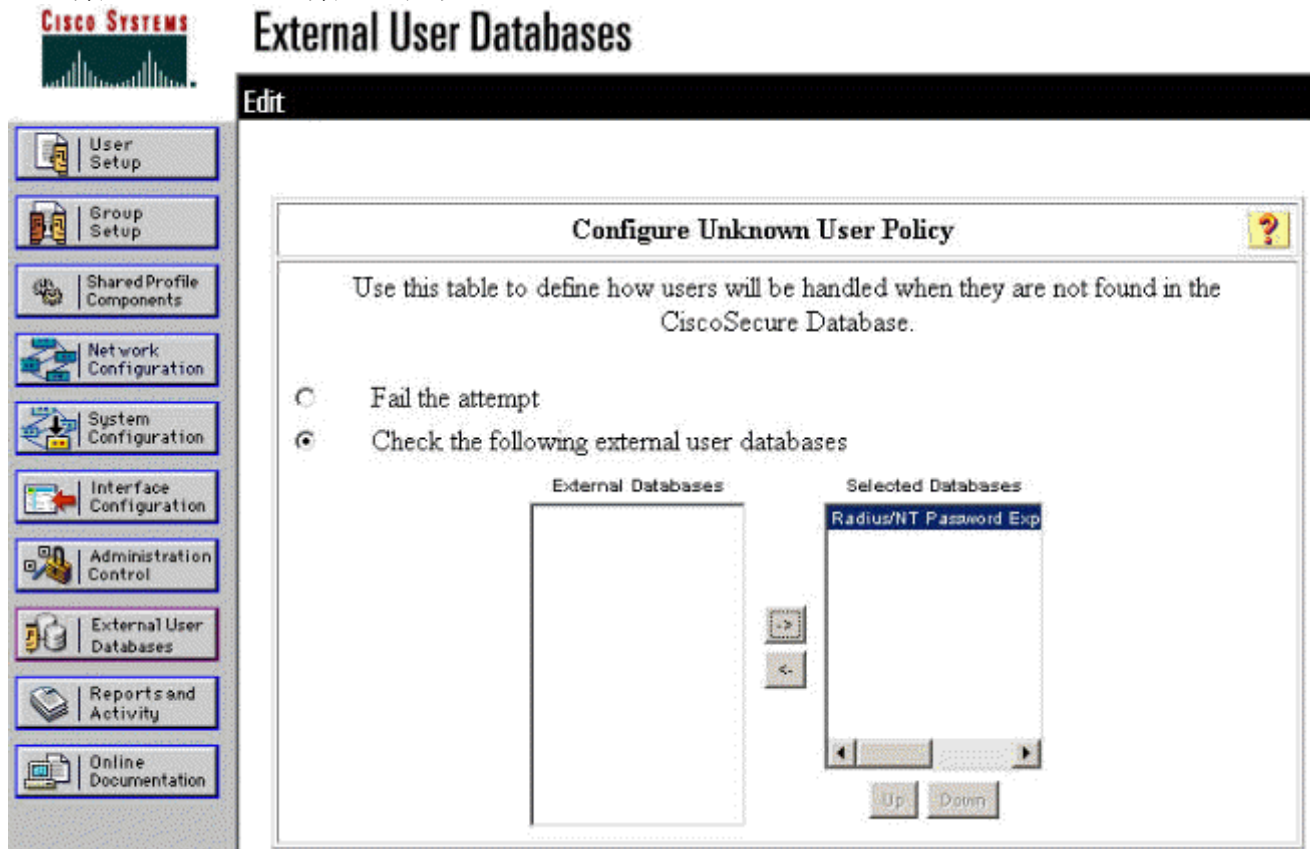
Selected

- Users**

CiscoSecure group:

13. 点击外部用户数据库在左面板中，然后点击未知用户策略的链路(如在此[示例中看到](#))。确保检查的选项以下外部用户数据库选择。点击右箭头按钮移动从“外部数据库”列表的以前已配置的

外部数据库向“所选的数据库列表”。

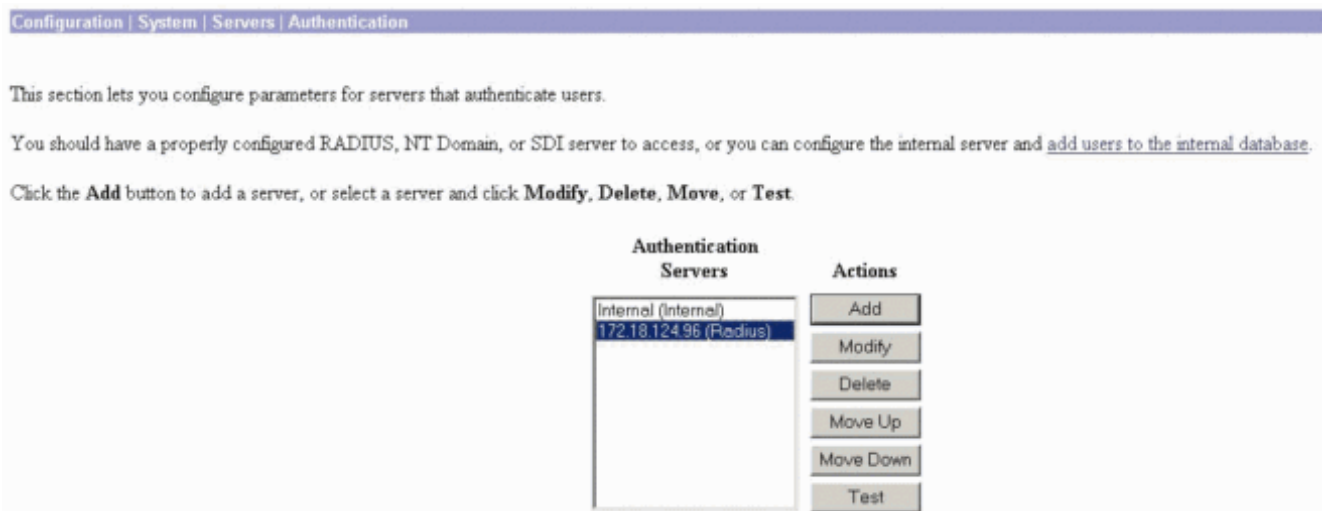


## 测试 NT/RADIUS密码到期功能

集中器提供功能测试RADIUS验证。要正确测试此功能，请确保您仔细遵从这些步骤。

### 测试 RADIUS 验证

1. 去Configuration > System > Servers > Authentication。选择您的RADIUS服务器并且点击测试。




2. 当提示，请键入您的NT域用户名和密码，然后点击OK键。下面的示例显示用户名“在有“cisco123”的NT域服务器”配置的jfracim作为密码。

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

User Name   
Password

3. 如果您的验证适当地设置，您应该收到消息陈述“验证成功”。

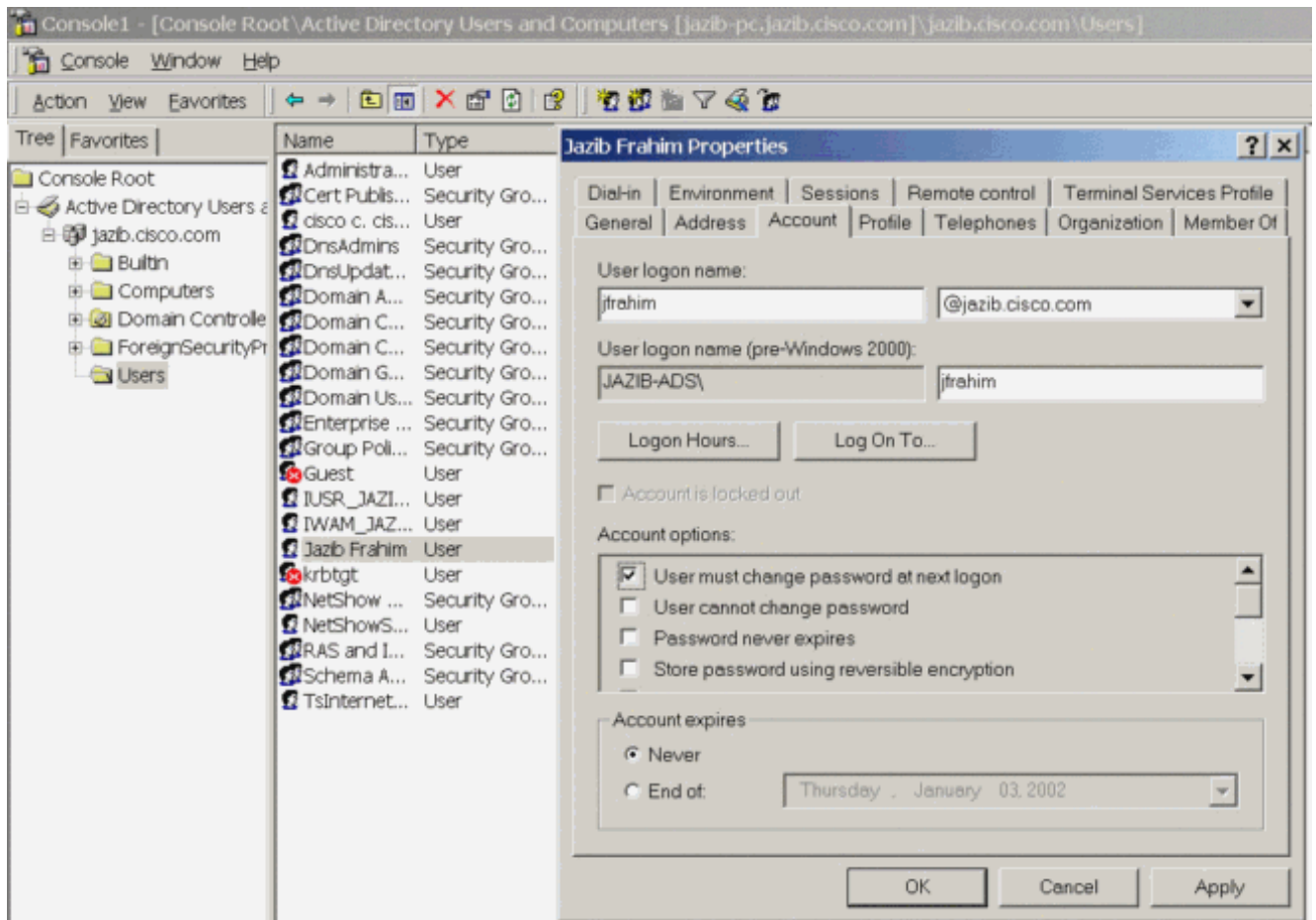
Success

 Authentication Successful

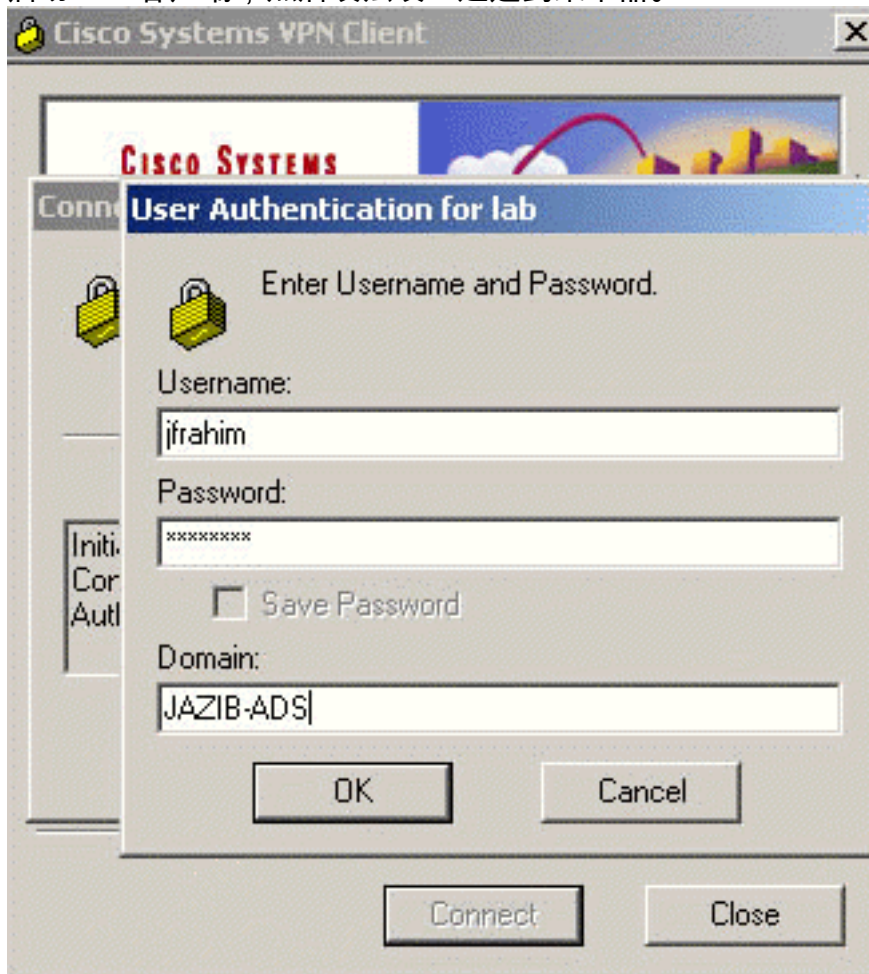
如果收到任何消息除显示的那个之外如上，有某个配置或连接问题。请重复在本文和测试的步骤略述的配置保证所有设置适当地做。并且请检查在您的设备之间的IP连通性。

### [使用 RADIUS 代理测试密码到期功能时的实际的 NT 域验证](#)

1. 如果用户在域服务器已经定义，请修改属性，以便将提示用户更改密码在下登录。去用户的 Properties对话框的“帐户”选项卡，选择用户的选项**必须更改密码在下登录**，然后点击OK键。



2. 启动VPN客户端，然后设法设立通道到集中器。





3. 在用户认证时，应该提示您更改密码。

## [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 \(RFC\)](#)