

配置Cisco VPN 3000系列集中器以支援RADIUS伺服器的NT密碼過期功能

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[網路圖表](#)

[配置VPN 3000集中器](#)

[組配置](#)

[RADIUS組態](#)

[配置Cisco Secure NT RADIUS伺服器](#)

[配置VPN 3000集中器的條目](#)

[為NT域身份驗證配置未知使用者策略](#)

[測試NT/RADIUS密碼到期功能](#)

[測試RADIUS驗證](#)

[使用RADIUS代理測試密碼到期功能的實際NT域身份驗證](#)

[相關資訊](#)

簡介

本文檔包含有關如何使用RADIUS伺服器配置Cisco VPN 3000系列集中器以支援NT密碼到期功能的逐步說明。

請參閱[使用Microsoft Internet Authentication Server的VPN 3000 RADIUS到期功能](#)，以瞭解有關Internet Authentication Server(IAS)相同方案的詳細資訊。

必要條件

需求

- 如果您的RADIUS伺服器和NT域身份驗證伺服器位於兩台單獨的電腦上，請確保您已在兩個電腦之間建立IP連線。
- 確保已建立從集中器到RADIUS伺服器的IP連線。如果RADIUS伺服器朝向公共介面，不要忘記開啟公共過濾器上的RADIUS埠。
- 確保可以使用內部使用者資料庫從VPN客戶端連線到集中器。如果尚未配置，請參閱[將IPSec - Cisco 3000 VPN客戶端配置為VPN 3000集中器](#)。

注意：密碼過期功能不能用於Web VPN或SSL VPN客戶端。

採用元件

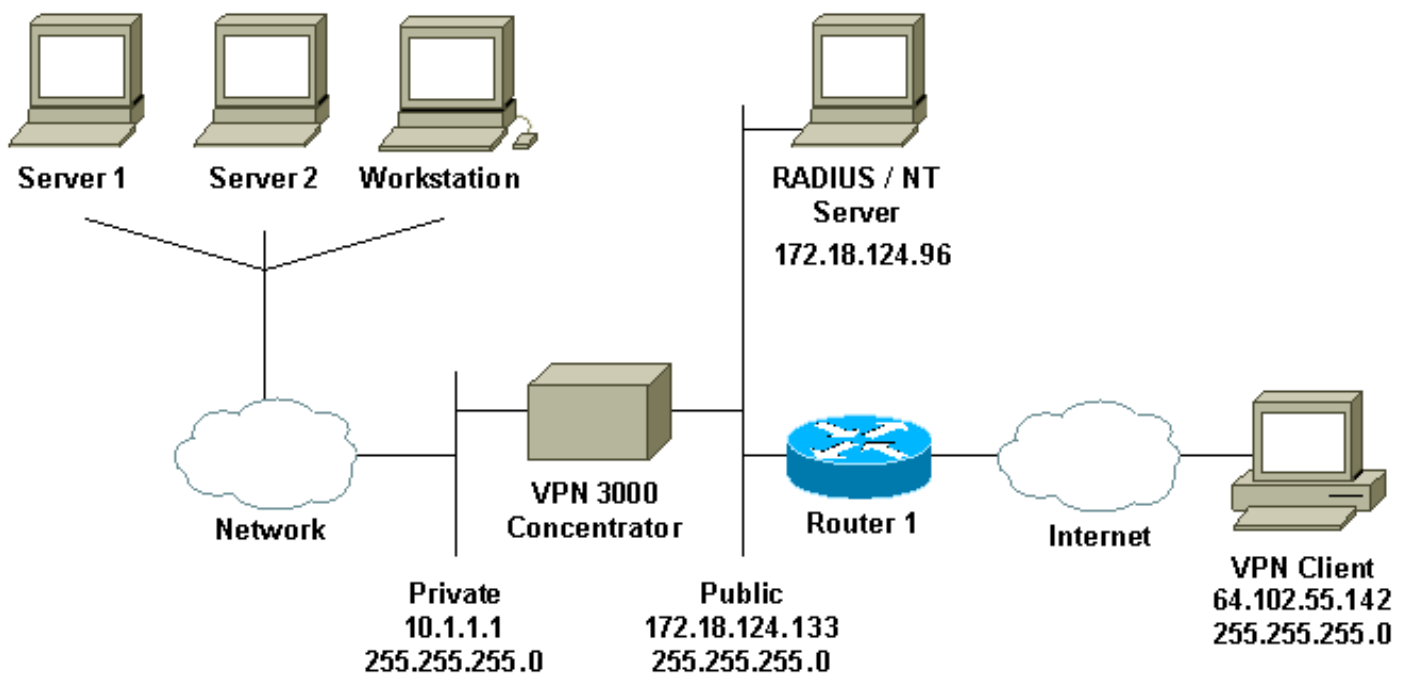
此配置是使用下面的軟體和硬體版本開發和測試的。

- VPN 3000集中器軟體版本4.7
- VPN使用者端版本3.5
- Cisco Secure for NT(CSNT)3.0版Microsoft Windows 2000 Active Directory Server，用於使用者身份驗證

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

網路圖表

本檔案會使用以下網路設定：



圖說明

1. 此配置中的RADIUS伺服器位於公共介面上。如果您的特定設定發生這種情況，請在公共過濾器中建立兩個規則，以允許RADIUS流量進入並離開集中器。
2. 此配置顯示CSNT軟體和NT域身份驗證服務在同一台電腦上運行。如果配置需要，可以在兩台單獨的電腦上運行這些元素。

配置VPN 3000集中器

組配置

1. 要將組配置為接受來自RADIUS伺服器的NT密碼到期引數，請轉到**Configuration > User Management > Groups**，從清單中選擇您的組，然後按一下**Modify Group**。以下示例顯示如何修改名為「ipsecgroup」的組。

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. 轉到IPSec頁籤，確保已為Authentication屬性選擇了Expiry的RADIUS。

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. 如果您希望在VPN 3002硬體客戶端上啟用此功能，請轉到HW Client頁籤，確保已啟用Require Interactive Hardware Client Authentication，然後按一下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組態

1. 要在集中器上配置RADIUS伺服器設定，請轉到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「Add」螢幕上，鍵入與RADIUS伺服器對應的值，然後按一下Add。以下示例使用以下值

o

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**

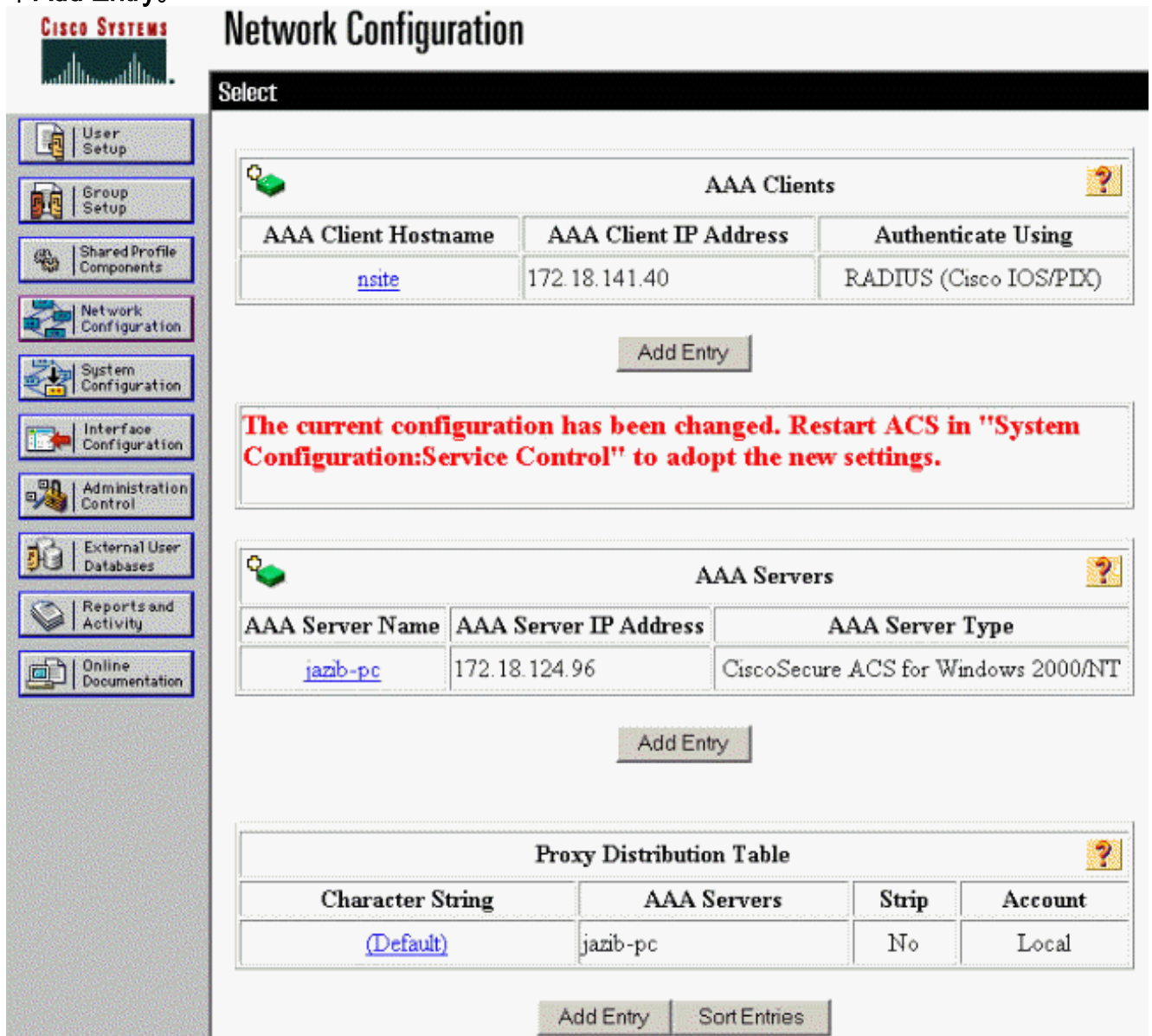
Configure and add a user authentication server.

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伺服器

配置VPN 3000集中器的條目

1. 登入到CSNT，然後按一下左側面板中的Network Configuration。在「AAA Clients」下，按一下Add Entry。



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「新增AAA客戶端」螢幕上，鍵入相應的值以新增集中器作為RADIUS客戶端，然後按一下提交+重新啟動。以下示例使用以下值。

AAA Client Hostname = **133_3000_conc**

AAA Client IP Address = **172.18.124.133**

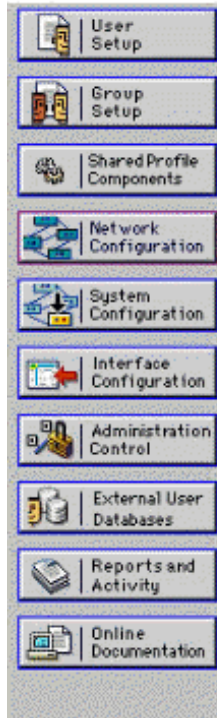
Key = **cisco123**

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	

您的3000集中器的條目將出現在「AAA客戶端」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)

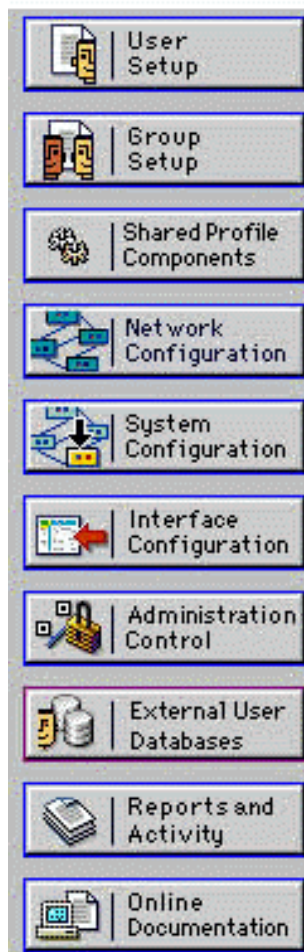
[為NT域身份驗證配置未知使用者策略](#)

1. 要將RADIUS伺服器上的使用者身份驗證配置為未知使用者策略的一部分，請在左側面板中按一下External User Database，然後按一下Database Configuration的連結。

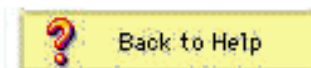


External User Databases

Select



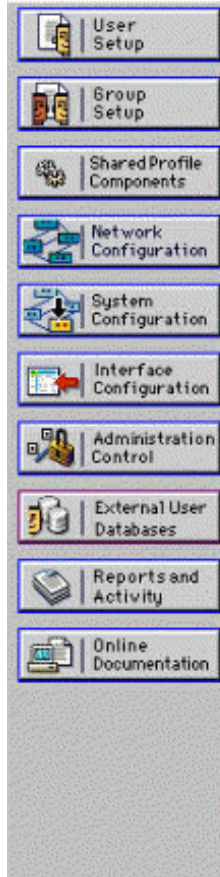
- [Unknown User Policy](#)
- [Database Group Mappings](#)
- [Database Configuration](#)



2. 在「外部使用者資料庫配置」下，按一下Windows NT/2000。



External User Databases



Select

External User Database Configuration

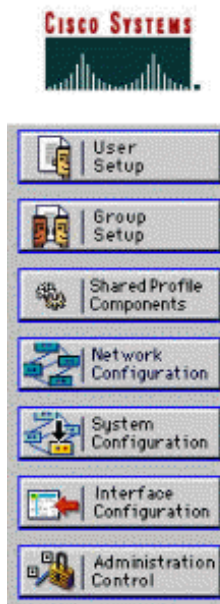
Choose which external user database type to configure.

- [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「資料庫配置建立」螢幕上，按一下**建立新配置**。



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. 出現提示時，鍵入NT/2000身份驗證的名稱，然後按一下**Submit**。以下範例顯示名稱「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. 按一下**Configure**以配置用於使用者身份驗證的域名。



External User Databases




Edit

External User Database Configuration 

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

6. 從「可用域」中選擇您的NT域，然後按一下右箭頭按鈕將其新增到「域清單」。在「MS-CHAP設定」下，確保已選中允許使用MS-CHAP版本1和版本2更改密碼的選項。完成後按一下**Submit**。



External User Databases

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

Configure Domain List ?

Available Domains		Domain List
	<input type="button" value="→"/> <input type="button" value="←"/>	<div style="background-color: #000080; color: white; padding: 2px;">JAZIB-ADS</div>
		<input type="button" value="Up"/> <input type="button" value="Down"/>


MS-CHAP Settings ?

Permit password changes using MS-CHAP version 1.

Permit password changes using MS-CHAP version 2.

These settings can be used to enable or disable password changes using the MS-CHAP version 1 or version 2 protocols.

7. 在左面板中按一下外部使用者資料庫，然後按一下Database Group Mappings的連結(如本例所示)。您應該看到以前配置的外部資料庫的條目。以下範例顯示我們剛設定的資料庫「Radius/NT密碼過期」的專案。



External User Databases

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases

Select

Unknown User Group Mappings ?

Choose the External User Database for which you want to configure the group mappings.

Name	Type
Radius/NT Password Expiration	Windows NT/2000


8. 在「域配置」螢幕上，按一下New configuration以新增域配置。



External User Databases



Edit

Domain Configurations 

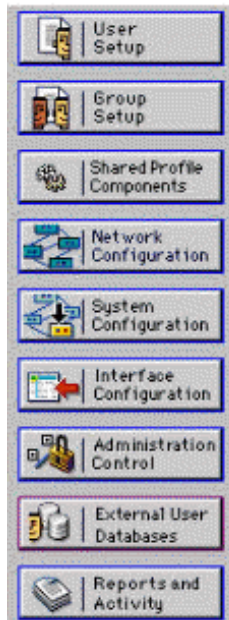
[\DEFAULT](#)

New configuration


9. 從「檢測到的域」清單中選擇您的域，然後按一下提交。以下示例顯示名為「JAZIB-ADS」的域。



External User Databases



Edit

Define New Domain Configuration 

Detected Domains:

[JAZIB-ADS](#)

Clear Selection

Domain:

Submit Cancel


10. 按一下您的域名以配置組對映。此示例顯示域「JAZIB-ADS」。



External User Databases



Edit

Domain Configurations 

[JAZIB-ADS](#)

[\DEFAULT](#)

New configuration

11. 按一下Add mapping以定義組對映。



External User Databases

Edit

Group Mappings for Domain : JAZIB-ADS

NT groups	CiscoSecure group
- no mappings defined -	

12. 在「建立新組對映」螢幕上，將NT域上的組對映到CSNT RADIUS伺服器上的組，然後按一下**提交**。以下示例將NT組「Users」對映到RADIUS組「Group 1」。

CISCO SYSTEMS

External User Databases

Edit

Create new group mapping for Domain : JAZIB-ADS

Define NT group set

NT Groups

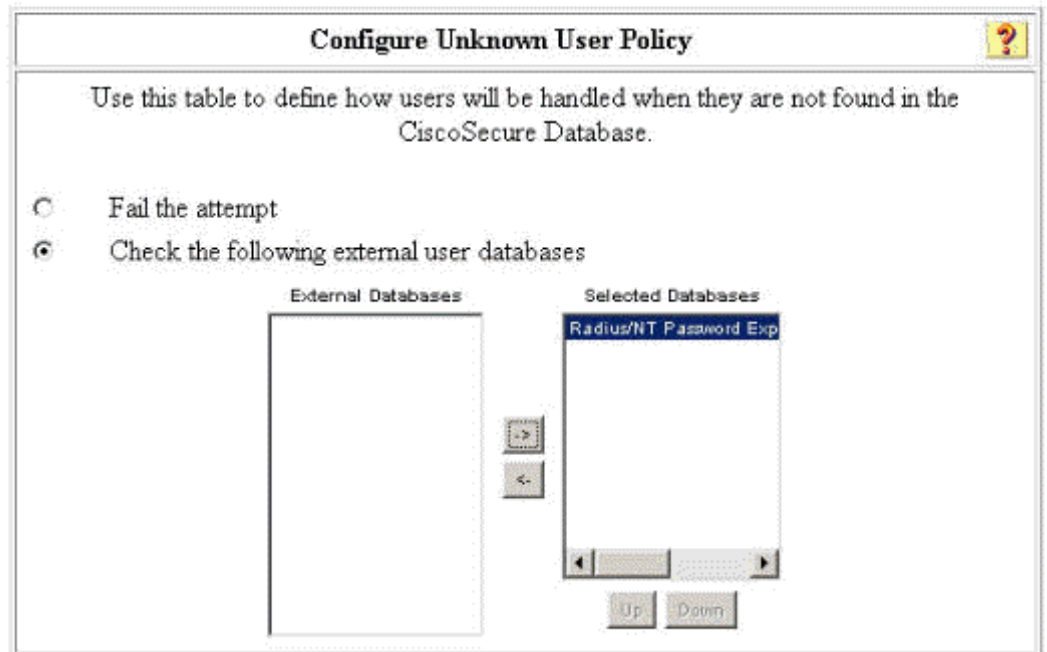
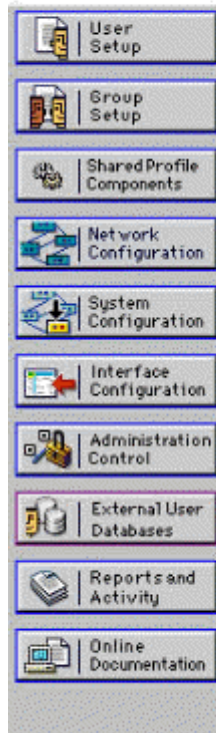
- Administrators
- Guests**
- Backup Operators
- Replicator
- Server Operators
- Account Operators
- Print Operators

Selected

- Users**

CiscoSecure group:

13. 在左側面板中按一下**External User Database**，然後按一下**Unknown User Policy**的連結(如本示例所示)。確保選中**Check the following external user databases**選項。按一下右箭頭按鈕將以前配置的外部資料庫從「外部資料庫」清單移動到「所選資料庫」清單。

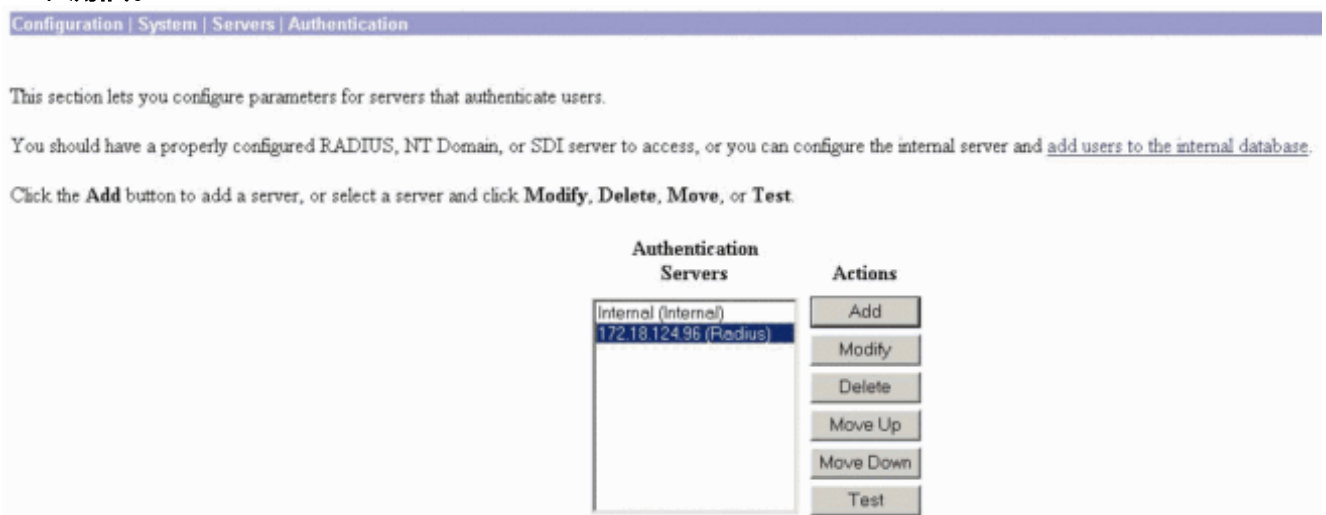


測試NT/RADIUS密碼到期功能

集中器提供測試RADIUS身份驗證的功能。要正確測試此功能，請確保您仔細執行這些步驟。

測試RADIUS驗證

1. 前往 **Configuration > System > Servers > Authentication**。選擇您的RADIUS伺服器，然後按一下**測試**。




2. 出現提示時，鍵入您的NT域使用者名稱和密碼，然後按一下**OK**。以下示例顯示在NT域伺服器上配置的使用者名稱「jbrahim」，密碼為「cisco123」。

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

User Name
Password

3. 如果身份驗證設定正確，您應該收到一條消息「Authentication Successful」（身份驗證成功

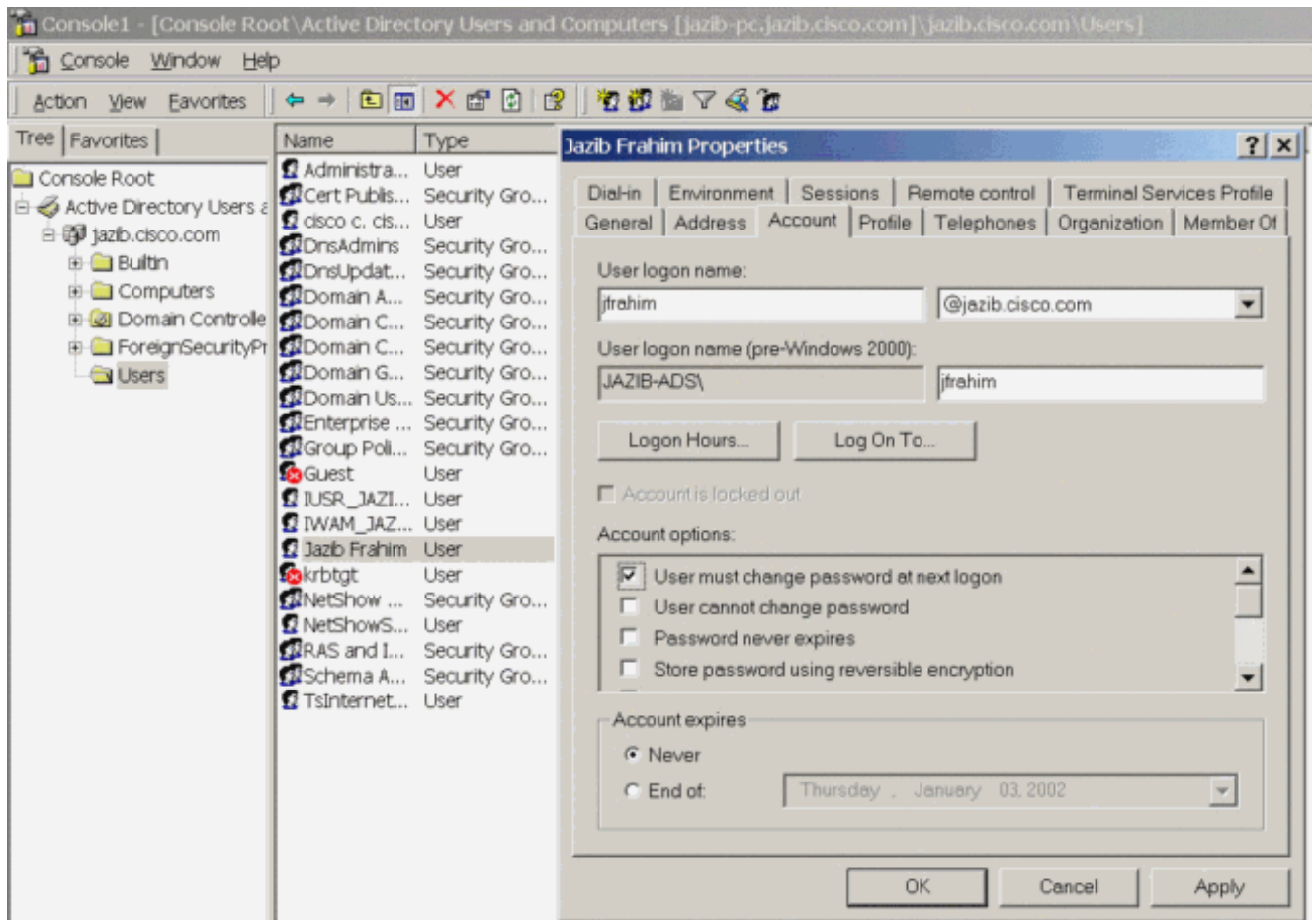
Success

 Authentication Successful

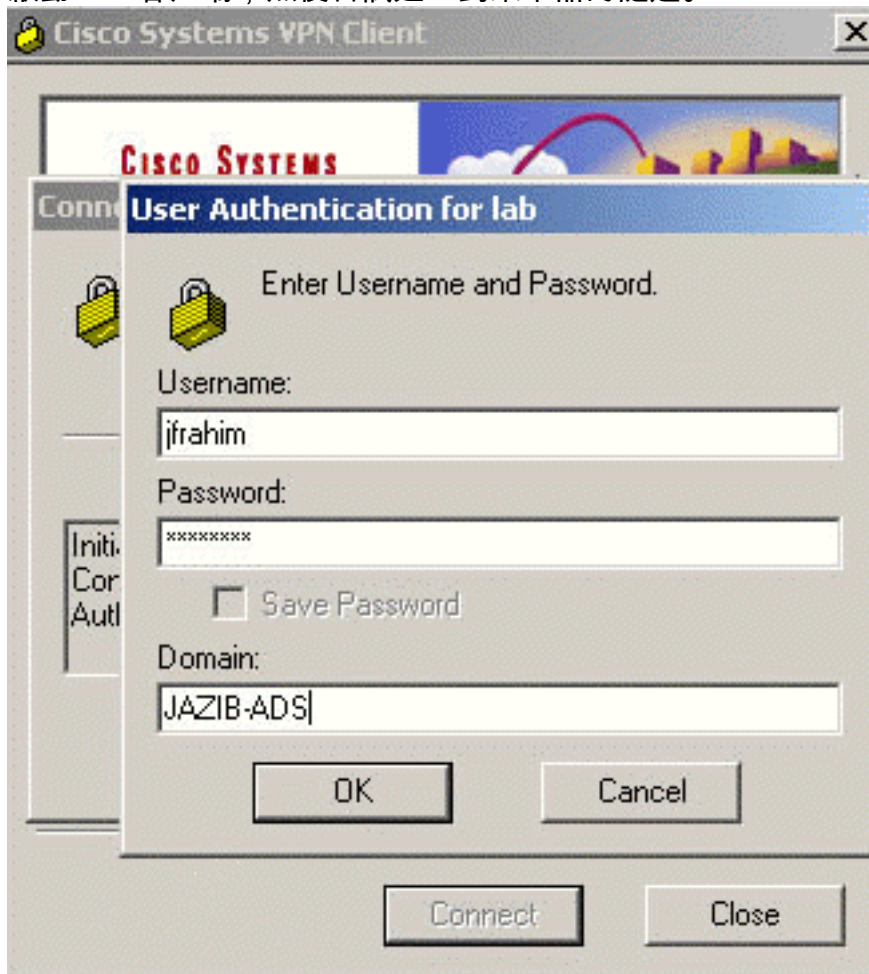
)。如果您收到的消息不是上面顯示的消息，則表明存在某些配置或連線問題。請重複本文檔中概述的配置和測試步驟，以確保正確設定所有設定。還要檢查裝置之間的IP連線。

[使用RADIUS代理測試密碼到期功能的實際NT域身份驗證](#)

1. 如果已在域伺服器上定義使用者，請修改屬性，以便在下次登入時提示使用者更改密碼。轉至使用者屬性對話方塊的「帳戶」頁籤，選擇User must change password at next logon (使用者下次登入時必須更改密碼) 選項，然後單擊「OK」(確定)。



2. 啟動VPN客戶端，然後嘗試建立到集中器的隧道。



3. 在使用者身份驗證期間，系統應提示您更改密碼。



相關資訊

- [Cisco VPN 3000系列集中器](#)
- [IPSec](#)
- [思科安全存取控制伺服器 \(Windows專用 \)](#)
- [RADIUS](#)
- [要求建議 \(RFC\)](#)