

# Configure el Concentradores Cisco VPN de la serie 3000 para soportar la característica de vencimiento de contraseña de NT con el servidor de RADIUS

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Diagrama de la red](#)

[Configuración del concentrador VPN 3000](#)

[Configuración del grupo](#)

[Configuración RADIUS](#)

[Configuración del servidor de Cisco Secure NT RADIUS](#)

[Configuración de una entrada para el concentrador VPN 3000](#)

[Configuración de la política de usuario desconocido para la autenticación de dominio NT](#)

[Prueba de la característica de vencimiento de contraseña de NT/RADIUS](#)

[Prueba de autenticación de RADIUS.](#)

[Autenticación de dominio NT real mediante el proxy de RADIUS para probar la característica de vencimiento de contraseña](#)

[Información Relacionada](#)

## [Introducción](#)

Este documento incluye las instrucciones paso a paso en cómo configurar el Concentradores Cisco VPN de la serie 3000 para soportar la característica de vencimiento de contraseña de NT usando el servidor de RADIUS.

Refiera a [VPN 3000 RADIUS con la función de vencimiento usando el Servidor de autenticación de Internet de Microsoft](#) para aprender un scenerio más casi igual con el Internet Authentication Server (IAS).

## [prerrequisitos](#)

### [Requisitos](#)

- Si servidor su servidor de RADIUS y autenticación de dominio de NT están en dos máquinas distintas, asegurese que usted ha establecido la conectividad del IP entre las dos máquinas.

- Asegúrese que usted ha establecido la conectividad del IP del concentrador al servidor de RADIUS. Si el servidor de RADIUS está hacia la interfaz pública, no olvide abrir el puerto RADIUS en el Filtro público.
- Asegure ese usted puede conectarse al concentrador del usando la base de datos de usuarios interna del cliente VPN. El si esto no está configurado, refiere por favor a [configurar el IPSec - Cliente VPN del Cisco 3000 al concentrador VPN 3000](#).

**Nota:** La característica de vencimiento de contraseña no se puede utilizar con la red VPN o los clientes VPN SSL.

## Componentes Utilizados

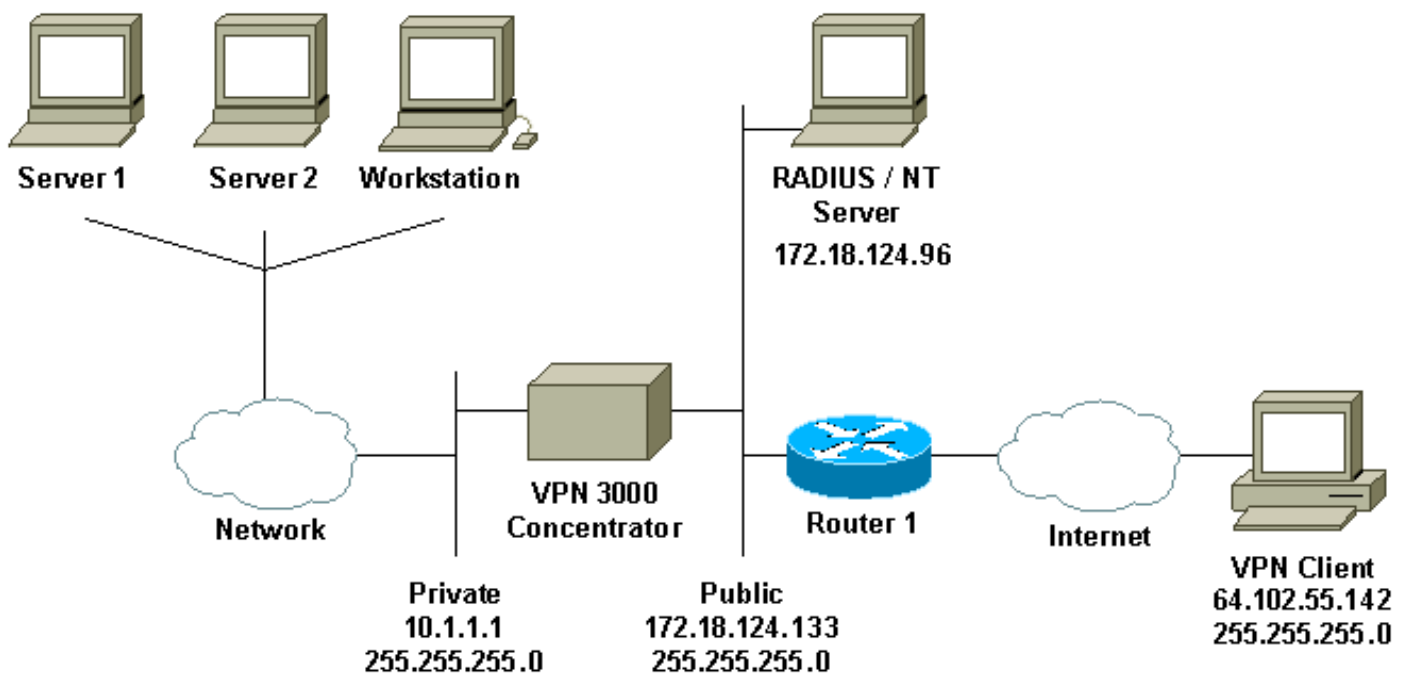
Esta configuración fue desarrollada y probada utilizando las versiones de software y hardware indicadas a continuación.

- Versión de software concentradora VPN 3000 4.7
- Versión 3.5 del cliente de VPN
- Cisco seguro para el servidor Active Directory del Microsoft Windows 2000 de la versión 3.0 de NT (CSNT) para la autenticación de usuario

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Diagrama de la red

En este documento, se utiliza esta configuración de red:



### Notas de diagrama

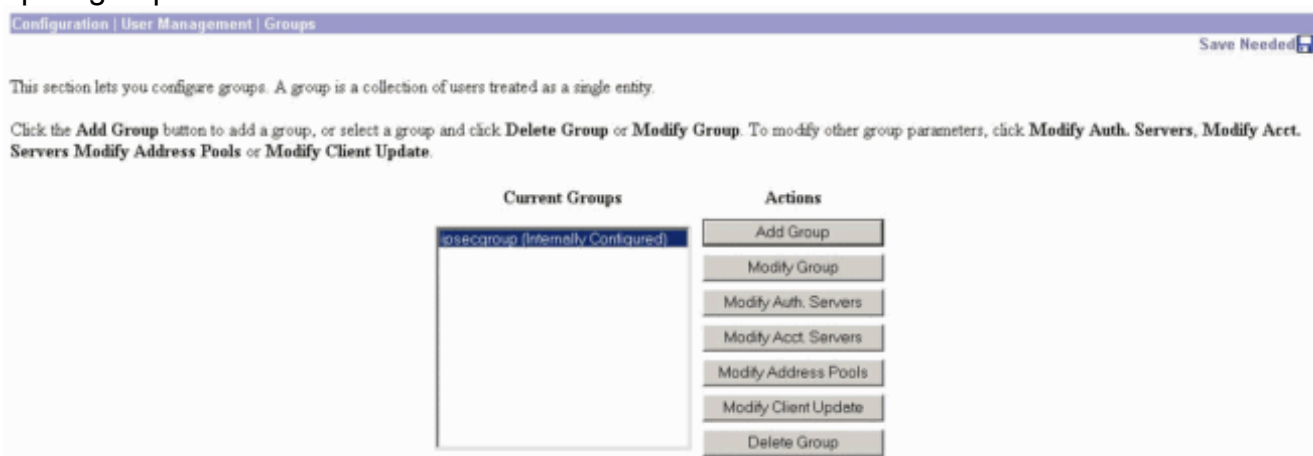
1. El servidor de RADIUS en esta configuración está en la interfaz pública. Si éste es el caso con su configuración específica, cree por favor dos reglas en su Filtro público para permitir que el tráfico de RADIUS ingrese y que deje el concentrador.

- Este configuración muestra el software CSNT y servicios de autenticación de dominio de NT que se ejecutan en la misma máquina. Estos elementos se pueden funcionar con en dos máquinas distintas si se requiere por parte de su configuración.

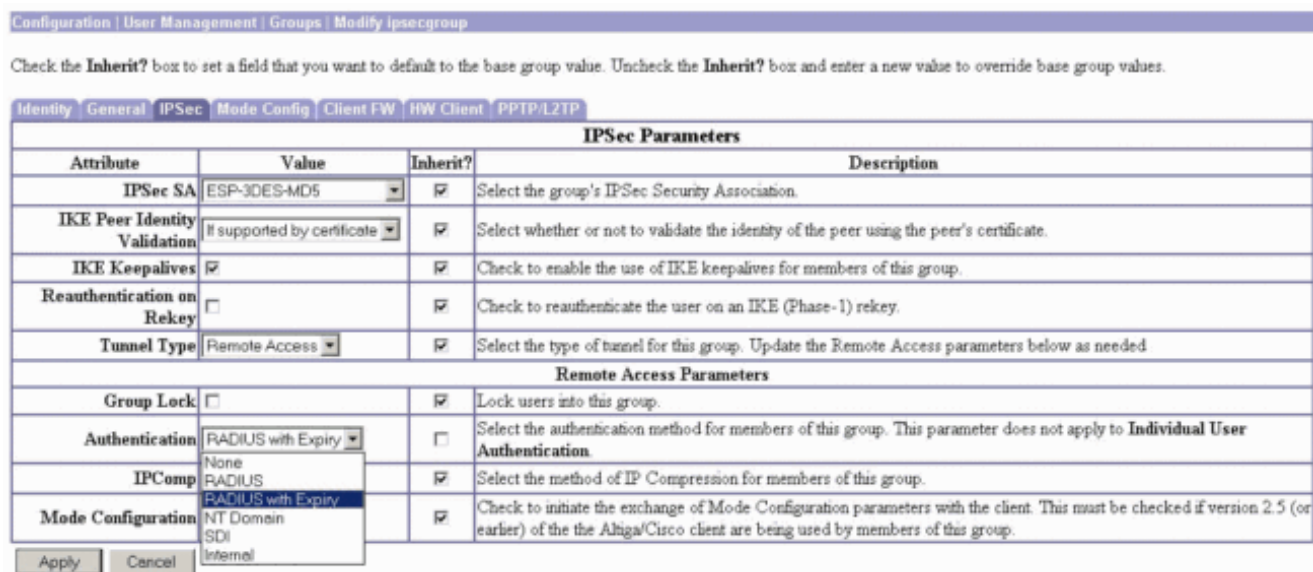
## Configuración del concentrador VPN 3000

### Configuración del grupo

- Para configurar al grupo para validar los parámetros del vencimiento de contraseña de NT del servidor de RADIUS, ir al **Configuration (Configuración)>User Management (Administración del usuario) >Groups (Grupos)**, seleccionar su grupo de la lista, y el tecleo **modifica al grupo**. El ejemplo debajo de las demostraciones cómo modificar a un grupo nombró el “ipsecgroup.”



- Va a la lengüeta del **IPSec**, se asegura que el **RADIUS con el vencimiento** está seleccionado para el atributo de la **autenticación**.



- Si usted quisiera que esta característica fuera habilitada en el VPN 3002 Hardware Clients, vaya a la lengüeta del **cliente HW**, se asegura que el **Require Interactive Hardware Client Authentication** está habilitado, después hacer clic se **aplica**.

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

## Configuración RADIUS

1. Para configurar las configuraciones del servidor de RADIUS en el concentrador, vaya al **Configuration (Configuración) > Sytem (Sistema) > Servers (Servidores) > Authentication (Autenticación) >**

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. En la pantalla Add, teclee adentro los valores que corresponden al servidor de RADIUS y al haga click en Add. El ejemplo abajo utiliza los valores siguientes.

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.

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

Add Cancel

## Configuración del servidor de Cisco Secure NT RADIUS

## Configuración de una entrada para el concentrador VPN 3000

1. Registro en el CSNT y configuración de red del teclado en el panel izquierdo. Bajo los "clientes AAA," el teclado agrega la entrada.

The screenshot shows the Cisco ACS Network Configuration interface. On the left is a navigation menu with options like User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main area is titled "Network Configuration" and has a "Select" dropdown menu. Below this, there are three sections: "AAA Clients", "AAA Servers", and "Proxy Distribution Table".

**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](#)

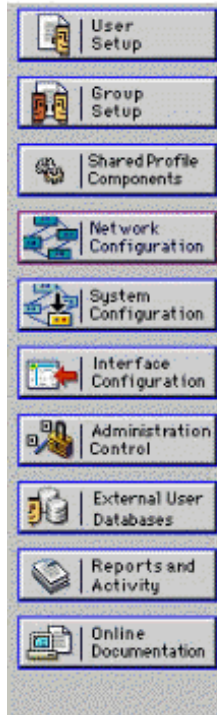
2. En "agregue la pantalla al cliente AAA", teclee adentro los valores apropiados para agregar el concentrador como el cliente RADIUS, después haga clic **Submit + Restart**. El ejemplo abajo utiliza los valores siguientes. AAA Client Hostname = 133\_3000\_conc AAA Client IP Address = 172.18.124.133 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	

Una entrada para su concentrador 3000 aparecerá bajo sección de los “clientes AAA”.



## 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)

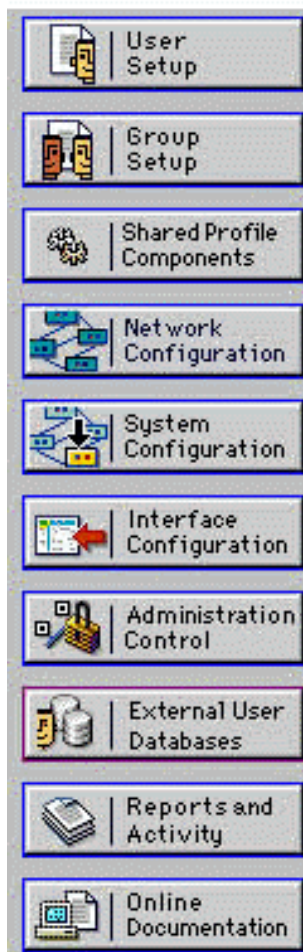
### [Configuración de la política de usuario desconocido para la autenticación de dominio NT](#)

1. Para configurar la autenticación de usuario en el servidor de RADIUS como parte de la Política de usuario desconocido, **Base de datos de usuarios externa del teclado** en el panel izquierdo, entonces para hacer clic el link para la **configuración de la base de datos**.

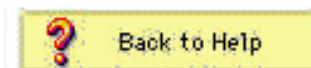


# External User Databases

Select



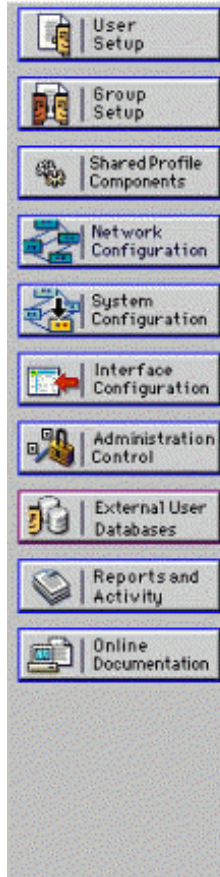
- [Unknown User Policy](#)
- [Database Group Mappings](#)
- [Database Configuration](#)



2. Bajo "Configuración de base de datos de usuarios externa," tecleo **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](#)

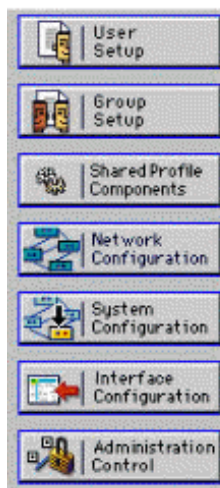
[List all database configurations](#)

Cancel

3. En “la pantalla de la creación de la configuración de la base de datos”, el tecleo **crea la nueva configuración**.



## 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. Cuando se le pregunte, teclee un nombre para la autenticación NT/2000 y el tecleo **somete**. El ejemplo abajo muestra el nombre “vencimiento de contraseña Radius/NT.”





## External User Databases



**Edit**

**Create a new External Database Configuration** ?

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

5. Hacen clic la configuración para configurar el Domain Name para la autenticación de usuario.



## External User Databases



**Edit**

**External User Database Configuration** ?

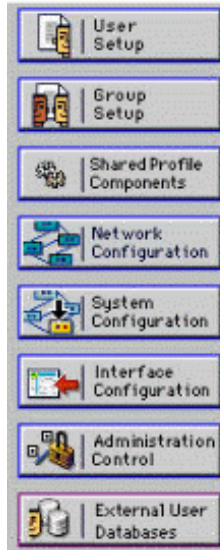
Choose what to do with the Windows NT/2000 database.

6. Seleccionan su dominio de NT de los “dominios disponibles,” entonces hacen clic el botón de la flecha correcta para agregarlo al “lista de dominio.” Bajo “configuraciones MS-CHAP,” asegúrese de que las opciones para los **cambios de la contraseña del permiso usando la versión MS-CHAP 1** y la **versión 2** estén seleccionadas. El tecleo **somete** cuando le hacen.


7. Haga clic la **Base de datos de usuarios externa** en el panel izquierdo, después haga clic el link para los **Mapeo de grupo de base de datos** (como se ve en este [ejemplo](#)). Usted debe ver una entrada para su base de datos externa previamente configurada. El ejemplo abajo muestra una entrada para el “vencimiento de contraseña Radius/NT,” la base de datos que acabamos de configurar.



## External User Databases



Select

**Unknown User Group Mappings** 

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

Name	Type
<a href="#">Radius/NT Password Expiration</a>	Windows NT/2000


8. En las “configuraciones del dominio” defienda, haga clic la **nueva configuración** para agregar las configuraciones del dominio.



## External User Databases



Edit

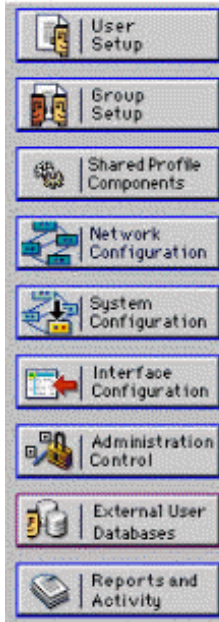
**Domain Configurations** 

[DEFAULT](#)

9. Seleccione su dominio de la lista de “detectó los dominios” y el tecleo **para someter**. El ejemplo abajo muestra un dominio nombrado “JAZIB-ADS.”



## External User Databases



Edit

### Define New Domain Configuration

Detected Domains:

JAZIB-ADS

Clear Selection

Domain:

Submit Cancel

10. Hacen clic en su Domain Name para configurar los mappings del grupo. Este ejemplo muestra el dominio "JAZIB-ADS."



## External User Databases



Edit

### Domain Configurations

[JAZIB-ADS](#)

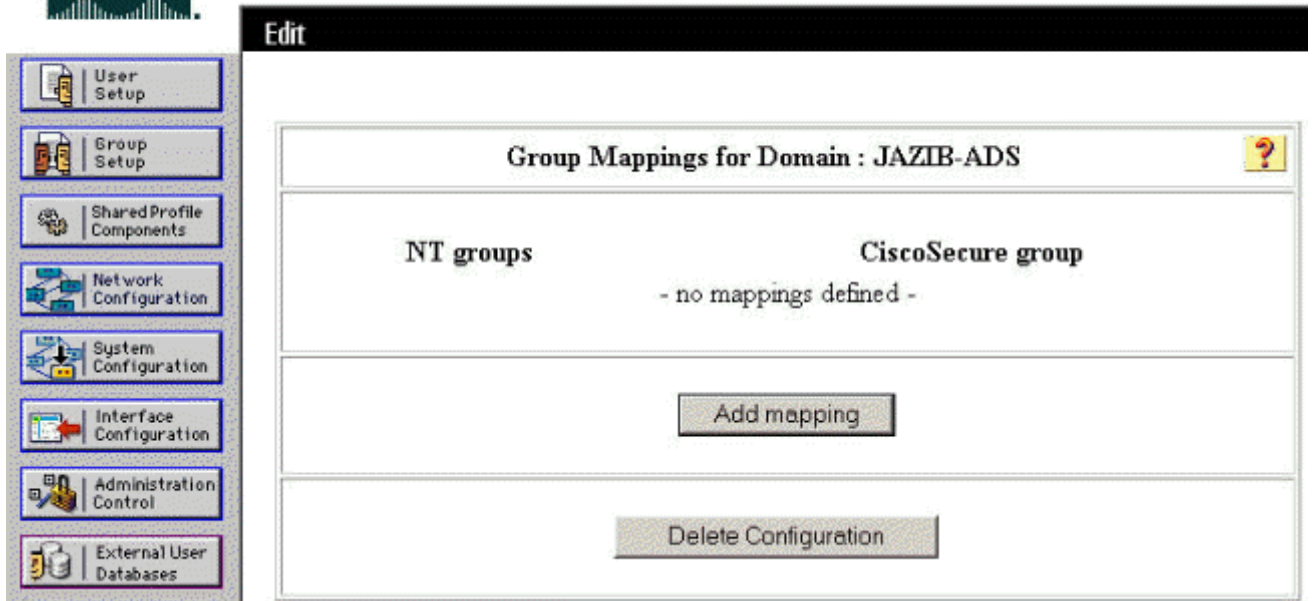
[\DEFAULT](#)

New configuration

11. El tecleo **agrega la asignación** para definir las asignaciones del grupo.



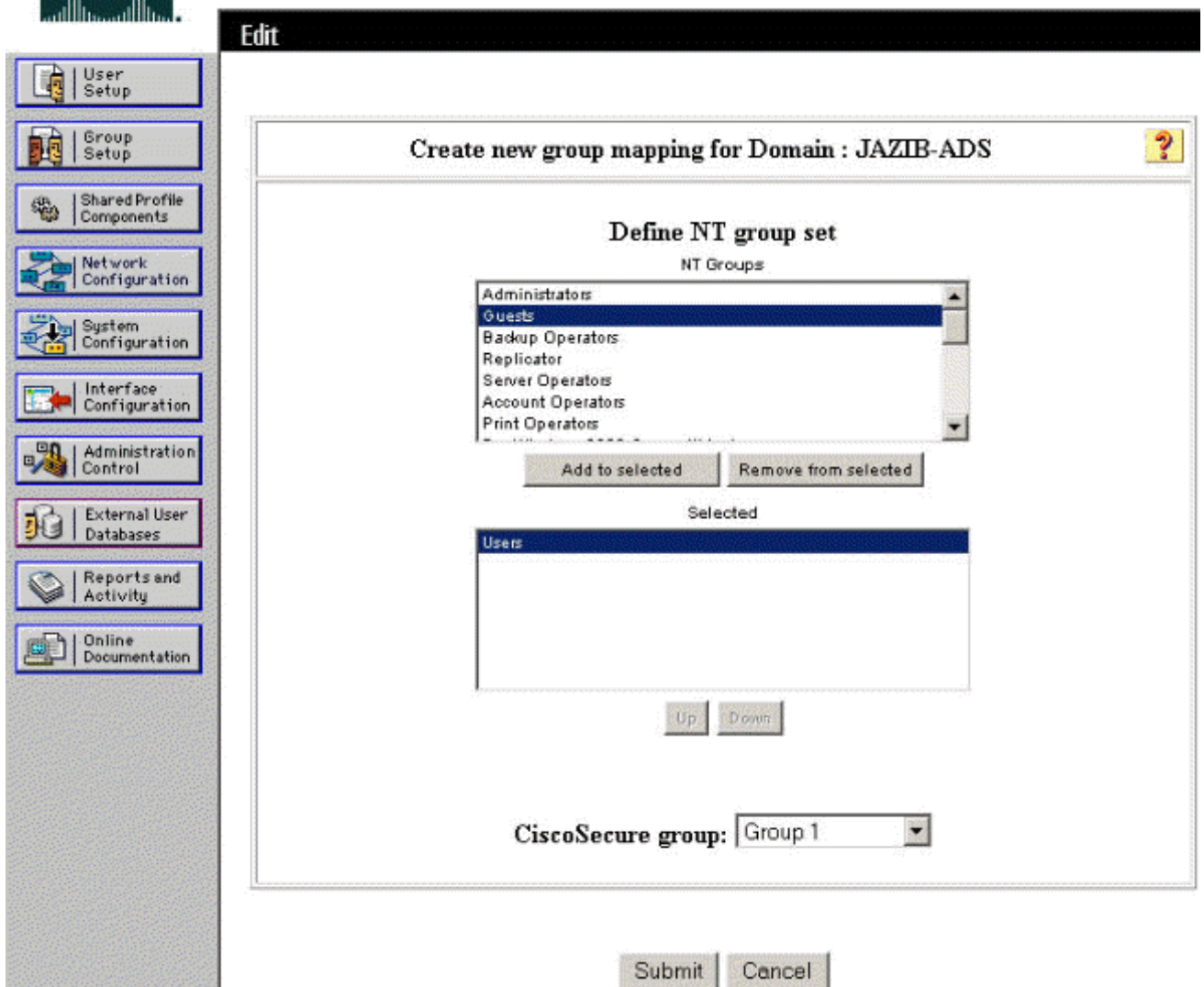
## External User Databases



12. En “ Cree la pantalla de la nueva asignación del grupo”, asocie al grupo en el dominio de NT a un grupo en el servidor del CSNT RADIUS, después haga clic **some**te. Las correspondencias abajo del ejemplo “usuarios” del grupo de NT grupo 1.” al grupo RADIUS



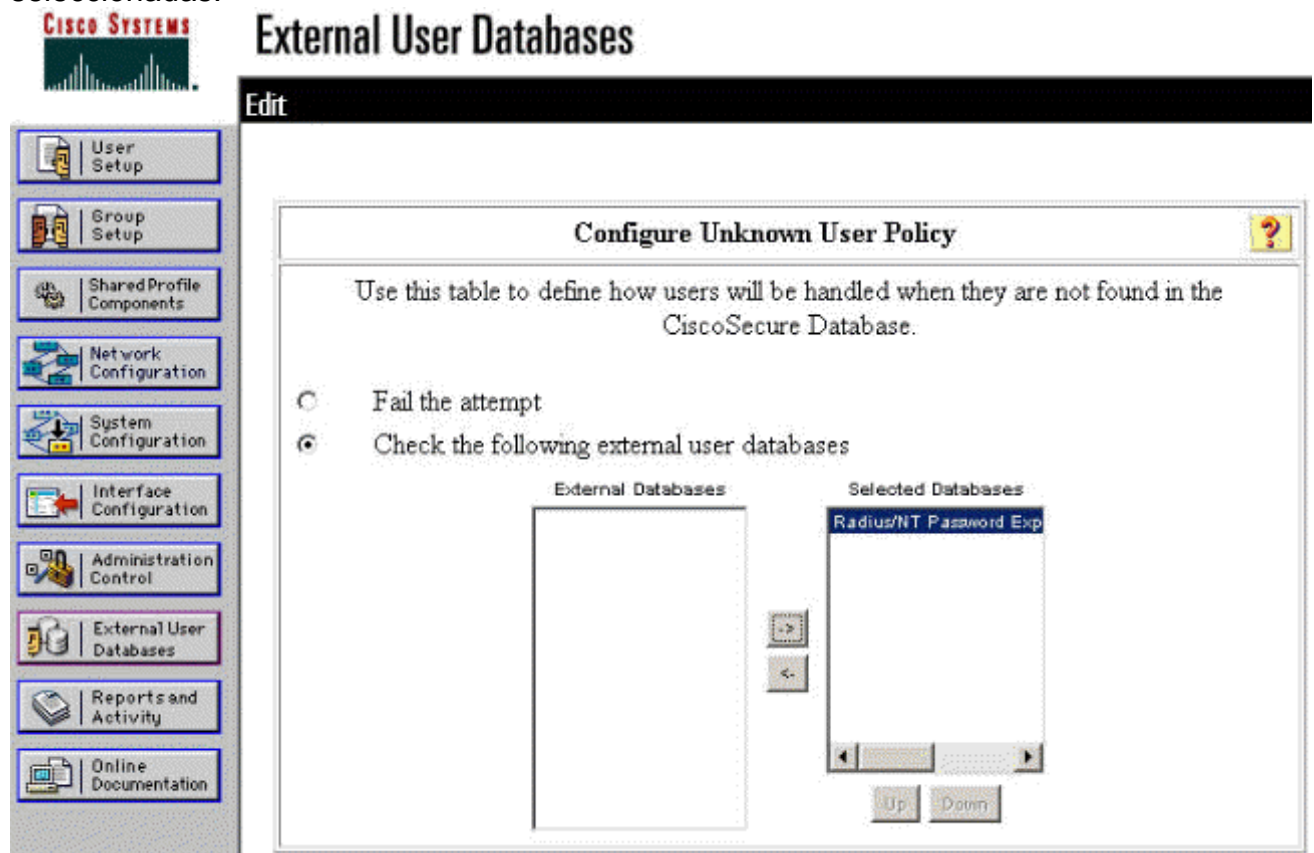
## External User Databases



13. La Base de datos de usuarios externa del teclado en el panel izquierdo, entonces hace clic



el link para la **Política de usuario desconocido** (como se ve en este [ejemplo](#)). Asegúrese que la opción para el **control las Bases de datos de usuarios externas siguientes** está seleccionada. Haga clic el botón de la flecha correcta para mover la base de datos externa previamente configurada desde la lista de “bases de datos externas” a la lista de “bases de datos seleccionadas.”



## [Prueba de la característica de vencimiento de contraseña de NT/RADIUS](#)

El concentrador ofrece una función para probar la autenticación de RADIUS. Para probar esta característica correctamente, asegúrese que usted sigue los siguientes pasos cuidadosamente.

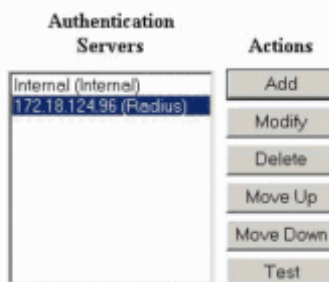
### [Prueba de autenticación de RADIUS.](#)

1. Vaya al **Configuration (Configuración) > Sytem (Sistema) > Servers (Servidores) > Authentication (Autenticación)**. Seleccione a su servidor de RADIUS y haga clic la prueba.

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**.



2. Cuando se le pregunte, teclee su nombre de usuario de dominio de NT y contraseña, y después haga clic la **AUTORIZACIÓN**. El ejemplo debajo del Nombre de usuario "jbrahim" de las demostraciones configuró en el servidor del dominio de NT con el "cisco123" como la contraseña.

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

User Name

Password

3. Si su autenticación se configura correctamente, usted debe conseguir un mensaje que expone la "autenticación

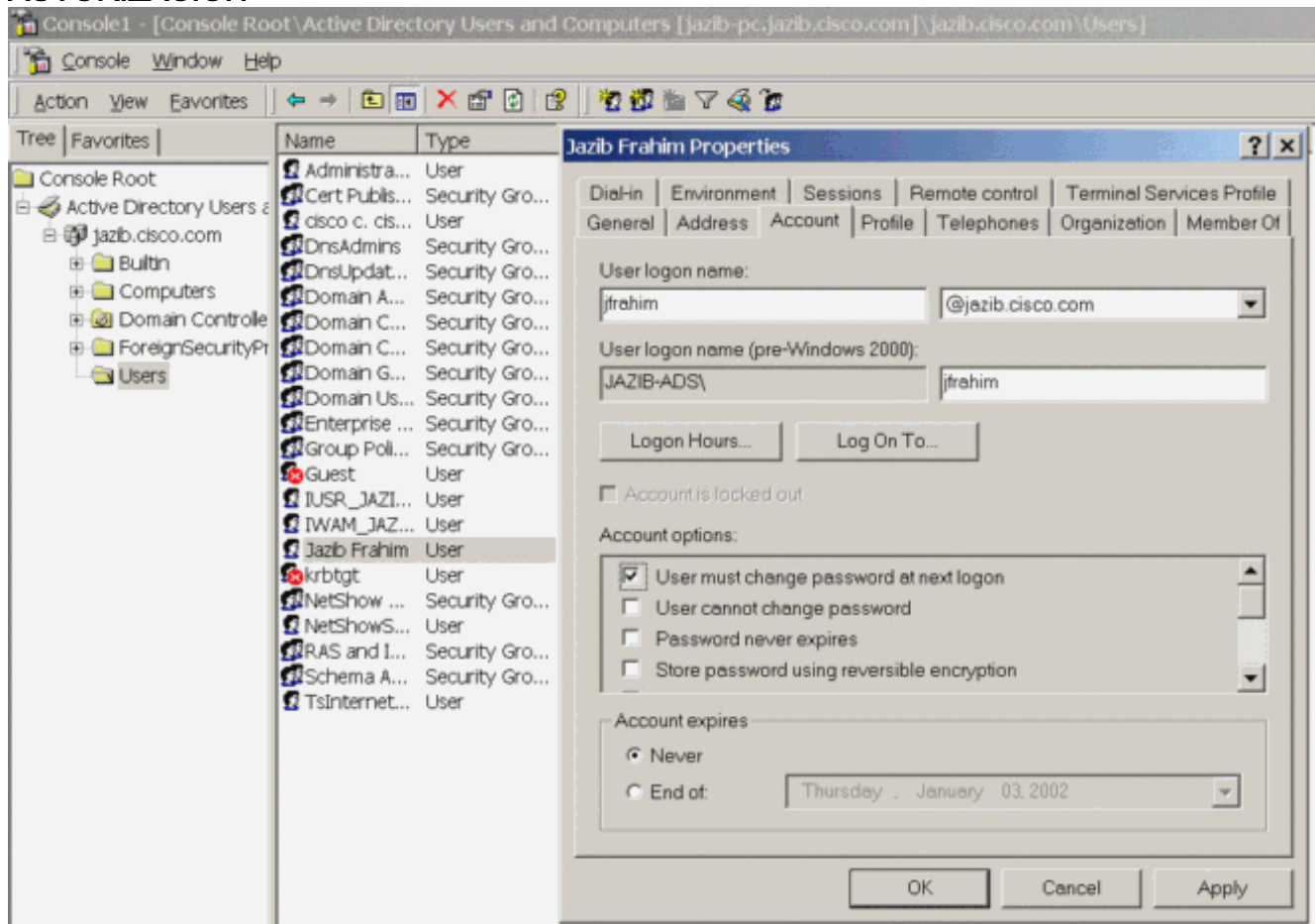


acertado.” Si usted recibe cualquier mensaje con excepción del que está mostrado arriba, hay cierta configuración o Problema de conexión. Relance por favor la configuración y los pasos de prueba delineados en este documento para asegurarse de que todas las configuraciones fueron hechas correctamente. También verifique la conectividad IP entre sus dispositivos.

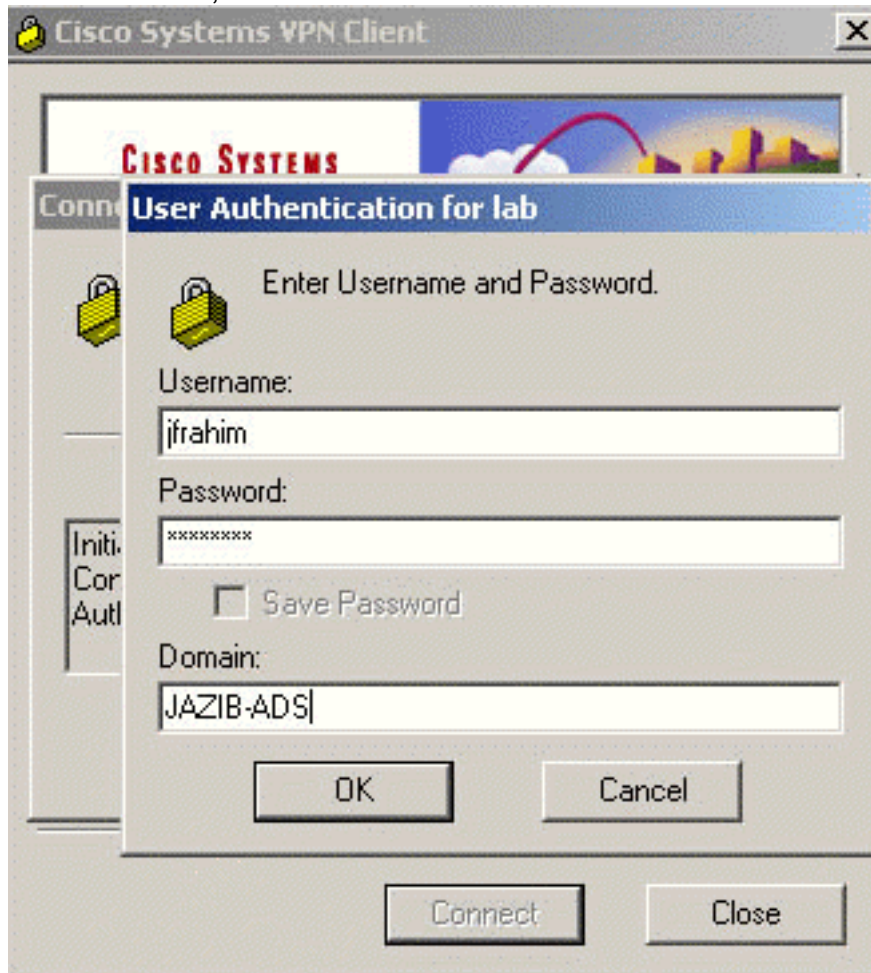
### [Autenticación de dominio NT real mediante el proxy de RADIUS para probar la característica de vencimiento de contraseña](#)

1. Si definen al usuario ya en el servidor del dominio, modifique las propiedades de modo que se indique al usuario que cambie la contraseña en el inicio siguiente. Vaya a la lengüeta de la "cuenta" del cuadro de diálogo de las propiedades de usuario, seleccionan la opción para

usuario debe cambiar la contraseña en el inicio siguiente, después hace clic la **AUTORIZACIÓN**.



2. El Ejecute el cliente de VPN, entonces intenta establecer el túnel al



concentrador.

3. Durante la autenticación de usuario, a le debe indican que cambie la



contraseña.

## [Información Relacionada](#)

- [Concentrador Cisco VPN serie 3000](#)
- [IPSec](#)
- [Cisco Secure Access Control Server para Windows](#)
- [RADIUS](#)
- [Solicitudes de Comentarios \(RFC\)](#)