

Configure los Cisco VPN 3000 Series Concentrators para Soportar la Función NT Password Expiration con el Servidor RADIUS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[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 instrucciones paso a paso sobre cómo configurar los Cisco VPN 3000 Series Concentrators para soportar la función NT Password Expiration usando el servidor RADIUS.

Consulte [Función RADIUS VPN 3000 con vencimiento mediante Microsoft Internet Authentication Server](#) para obtener más información sobre el mismo escenario con Internet Authentication Server (IAS).

Prerequisites

Requirements

- Si el servidor RADIUS y el servidor de autenticación de dominio NT están en dos equipos independientes, asegúrese de que ha establecido la conectividad IP entre los dos equipos.
- Asegúrese de que ha establecido la conectividad IP del concentrador al servidor RADIUS. Si el servidor RADIUS se dirige a la interfaz pública, no olvide abrir el puerto RADIUS en el filtro

público.

- Asegúrese de que puede conectarse al concentrador desde el cliente VPN mediante la base de datos de usuario interna. Si esto no está configurado, consulte [Configuración de IPSec - Cisco 3000 VPN Client a VPN 3000 Concentrator](#).

Nota: La función de caducidad de la contraseña no se puede utilizar con clientes VPN Web o SSL.

Componentes Utilizados

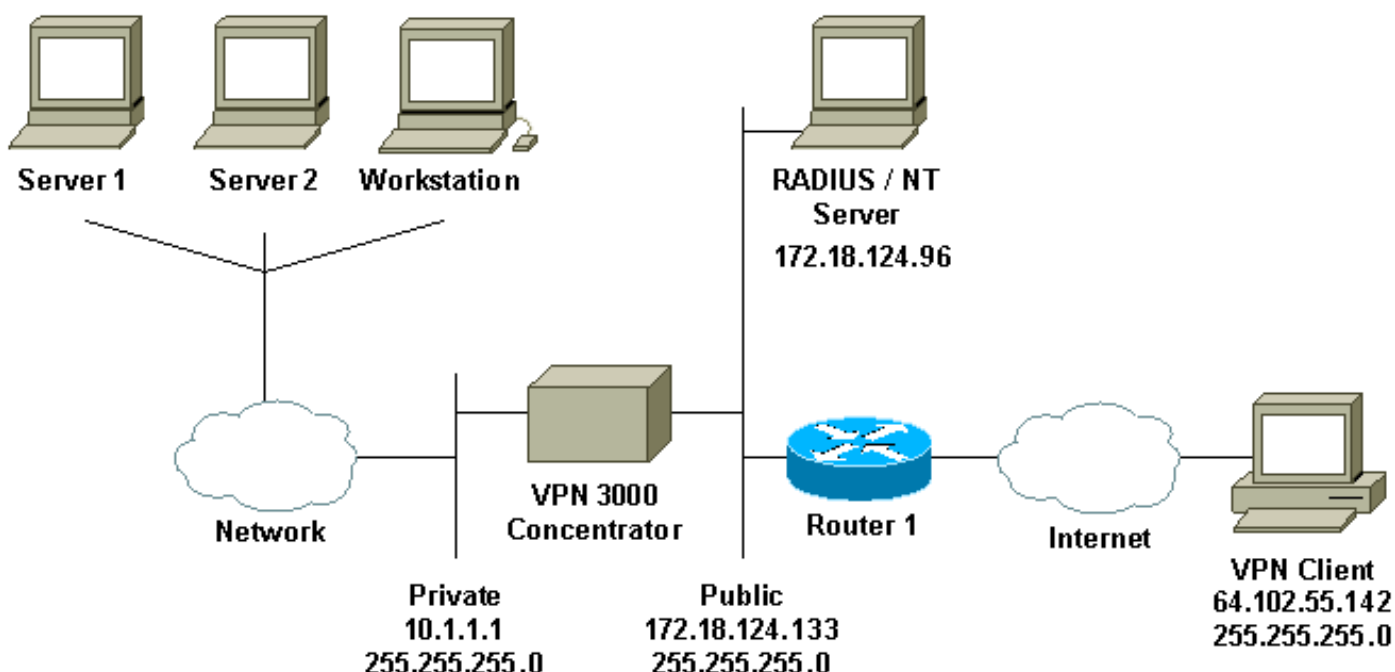
Esta configuración fue desarrollada y probada utilizando las versiones de software y hardware indicadas a continuación.

- Versión 4.7 del software del concentrador VPN 3000
- Versión 3.5 de VPN Client
- Cisco Secure para NT (CSNT) versión 3.0 Microsoft Windows 2000 Active Directory Server para autenticación de usuario

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



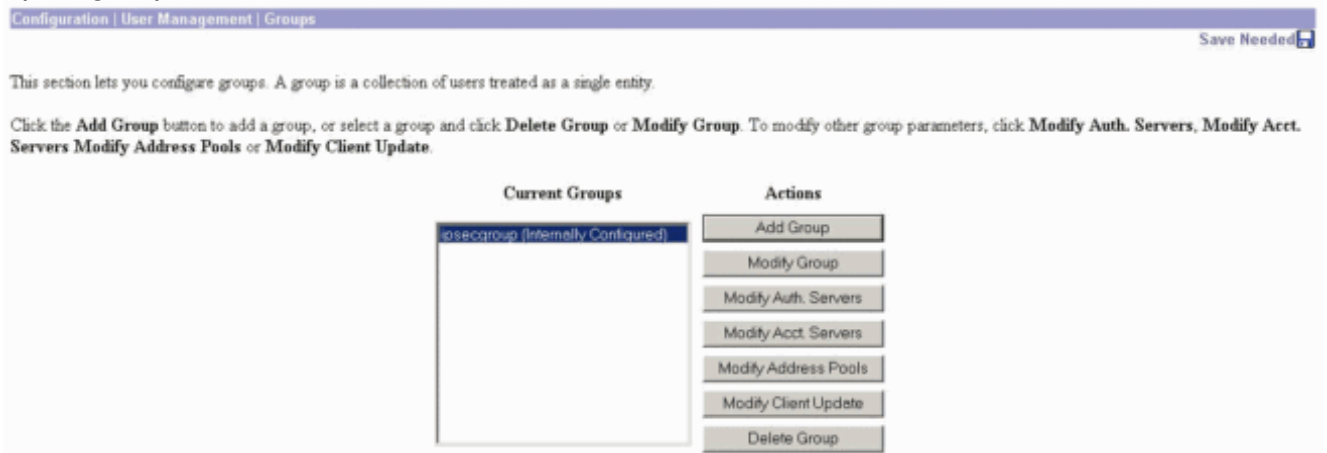
Notas de diagrama

1. El servidor RADIUS en esta configuración está en la interfaz pública. Si este es el caso con su configuración específica, cree dos reglas en su filtro público para permitir que el tráfico RADIUS entre y salga del concentrador.
2. Esta configuración muestra el software CSNT y los Servicios de autenticación de dominio NT ejecutándose en la misma máquina. Estos elementos se pueden ejecutar en dos máquinas independientes si así lo requiere la configuración.

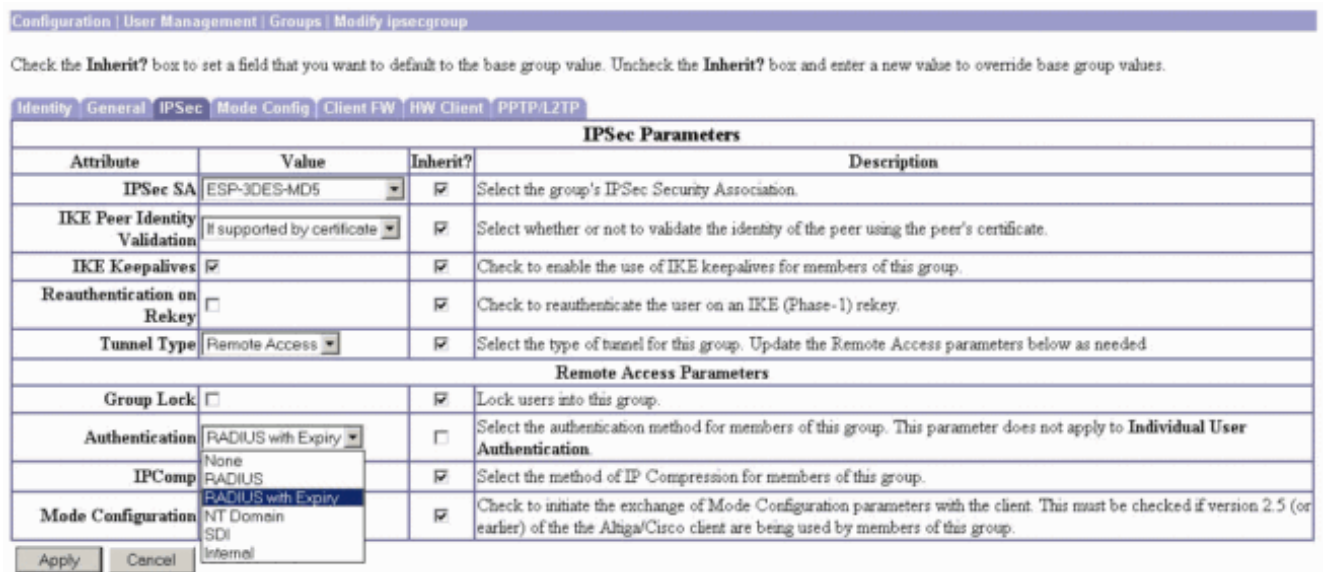
Configuración del concentrador VPN 3000

Configuración del grupo

1. Para configurar el grupo para que acepte los Parámetros de Vencimiento de Contraseña NT del Servidor RADIUS, vaya a **Configuración > Administración de Usuario > Grupos**, seleccione su grupo de la lista y haga clic en **Modificar Grupo**. El siguiente ejemplo muestra cómo modificar un grupo denominado "ipsecgroup".



2. Vaya a la pestaña **IPSec**, asegúrese de que **RADIUS con vencimiento** esté seleccionado para el atributo **Authentication**.



3. Si desea que esta función se habilite en los clientes de hardware VPN 3002, vaya a la pestaña **Client**, asegúrese de que **Require Interactive Hardware Client Authentication** esté habilitado y haga clic en **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

Configuración RADIUS

1. Para configurar la configuración del servidor RADIUS en el concentrador, vaya a 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)	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Test"/>

2. En la pantalla **Add**, escriba los valores que corresponden al servidor RADIUS y haga clic en **Add**. El ejemplo siguiente 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.

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"/>		

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

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

1. Inicie sesión en CSNT y haga clic en **Configuración de red** en el panel izquierdo. En "Clientes AAA", haga clic en **Agregar entrada**.

CISCO SYSTEMS Network Configuration

Select

AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
nsize	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. En la pantalla "Add AAA Client" (Agregar cliente AAA), escriba los valores adecuados para agregar el concentrador como RADIUS Client y, a continuación, haga clic en **Submit + Restart**. El ejemplo siguiente utiliza los valores siguientes.

AAA Client Hostname = **133_3000_conc**

AAA Client IP Address = **172.18.124.133**

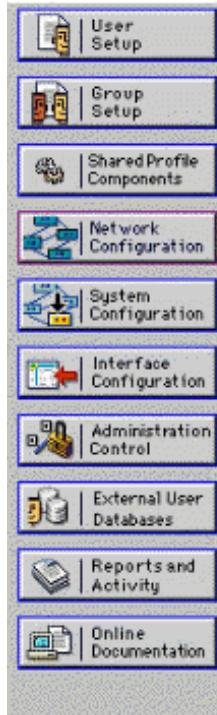
Key = **cisco123**

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	

Aparecerá una entrada para su concentrador 3000 en la sección "Clientes AAA".



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)

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

1. Para configurar la autenticación de usuario en el servidor RADIUS como parte de la política de usuario desconocida, haga clic en **Base de datos de usuario externa** en el panel izquierdo y luego haga clic en el enlace **Configuración de base de datos**.

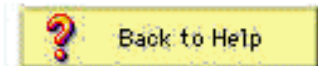


External User Databases

Select

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

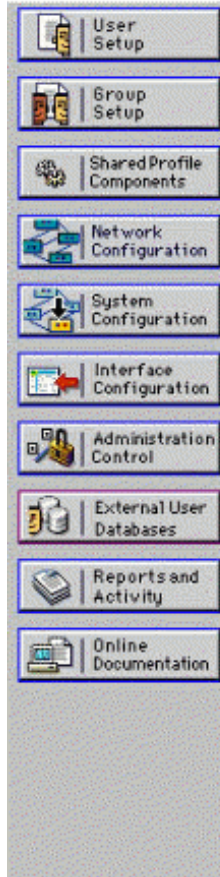
- [Unknown User Policy](#)
- [Database Group Mappings](#)
- [Database Configuration](#)



2. En "Configuración de base de datos de usuario externa", haga clic en **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](#)

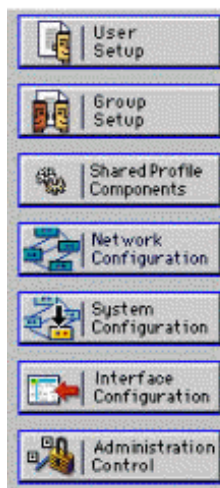
[List all database configurations](#)

Cancel

3. En la pantalla "Database Configuration Creation" (Creación de la configuración de la base de datos), haga clic en **Create New Configuration** (Crear 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 solicite, escriba un nombre para la autenticación NT/2000 y haga clic en **Enviar**. El siguiente ejemplo muestra el nombre "Expiración de contraseña de Radius/NT".



External User Databases



Edit

Create a new External Database Configuration ?

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

5. Haga clic en **Configurar** para configurar el nombre de dominio para la autenticación de usuario.



External User Databases



Edit

External User Database Configuration ?

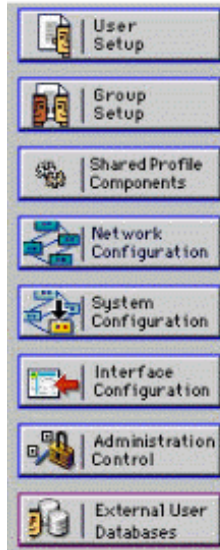
Choose what to do with the Windows NT/2000 database.

6. Seleccione su dominio NT en "Available Domains" (Dominios disponibles) y, a continuación, haga clic en el botón de flecha derecha para agregarlo a la "Domain List" (Lista de dominios). En "MS-CHAP Settings," asegúrese de que las opciones para **Permit password changes using MS-CHAP version 1** y **version 2** estén seleccionadas. Haga clic en **Enviar** cuando haya terminado.


7. Haga clic en **Base de datos de usuario externa** en el panel izquierdo y, a continuación, haga clic en el vínculo para **Asignaciones de grupo de base de datos** (como se muestra en este [ejemplo](#)). Debería ver una entrada para su base de datos externa configurada previamente. El siguiente ejemplo muestra una entrada para "Expiración de contraseña de 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
Radius/NT Password Expiration	Windows NT/2000


8. En la pantalla "Domain Configurations" (Configuraciones de dominio), haga clic en **New configuration** para agregar las configuraciones de dominio.



External User Databases



Edit

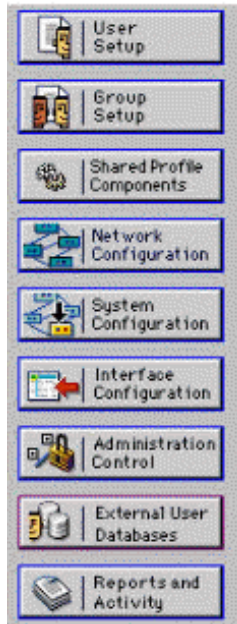
Domain Configurations 

[DEFAULT](#)

9. Seleccione su dominio de la lista de "Dominios detectados" y haga clic en **Enviar**. El siguiente ejemplo muestra un dominio llamado "JAZIB-ADS".



External User Databases



Edit

Define New Domain Configuration

Detected Domains:

JAZIB-ADS

Clear Selection

Domain:

Submit Cancel

10. Haga clic en su nombre de dominio para configurar las asignaciones de grupo. Este ejemplo muestra el dominio "JAZIB-ADS".



External User Databases



Edit

Domain Configurations

[JAZIB-ADS](#)

[DEFAULT](#)

New configuration

11. Haga clic en **Agregar asignación** para definir las asignaciones de grupo.



External User Databases

Edit

Group Mappings for Domain : JAZIB-ADS

NT groups	CiscoSecure group
	- no mappings defined -

Add mapping

Delete Configuration

12. En la pantalla "Crear asignación de grupo nuevo", asigne el grupo en el dominio NT a un grupo en el servidor RADIUS CSNT y, a continuación, haga clic en **Enviar**. El siguiente ejemplo asigna el grupo NT "Users" al grupo RADIUS "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

Add to selected Remove from selected

Selected

- Users

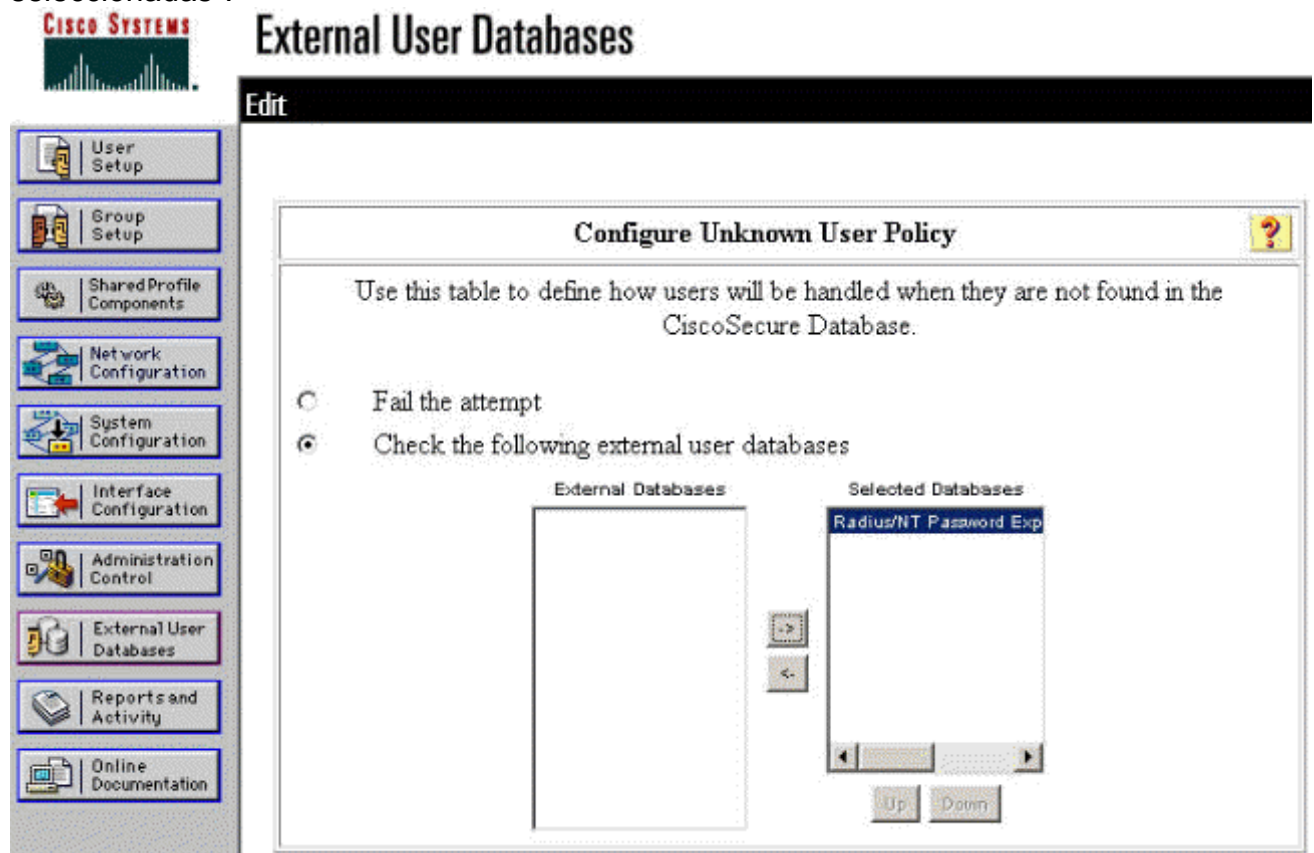
Up Down

CiscoSecure group: Group 1

Submit Cancel

13. Haga clic en **Base de datos de usuario externa** en el panel izquierdo y, a continuación,

haga clic en el vínculo **Política de usuario desconocida** (como se muestra en este [ejemplo](#)). Asegúrese de que la opción para **Verificar las siguientes bases de datos de usuario externas** esté seleccionada. Haga clic en el botón de flecha hacia la derecha para mover la base de datos externa configurada previamente de la lista "Bases de datos externas" a la lista "Bases de datos seleccionadas".



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

El concentrador ofrece una función para probar la autenticación RADIUS. Para probar esta función correctamente, asegúrese de seguir estos pasos con cuidado.

[Prueba de autenticación de RADIUS.](#)

1. Vaya a **Configuration > System > Servers > Authentication**. Seleccione su servidor RADIUS y haga clic en **Test**.

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
172.18.124.96 (Radius)	Modify
	Delete
	Move Up
	Move Down
	Test

2. Cuando se le solicite, escriba su nombre de usuario y contraseña de dominio NT y, a continuación, haga clic en **Aceptar**. El siguiente ejemplo muestra el nombre de usuario "jfracim" configurado en el servidor de dominio NT con "cisco123" como contraseña.

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

User Name

Password

3. Si la autenticación está configurada correctamente, debe recibir un mensaje que diga "Autenticación

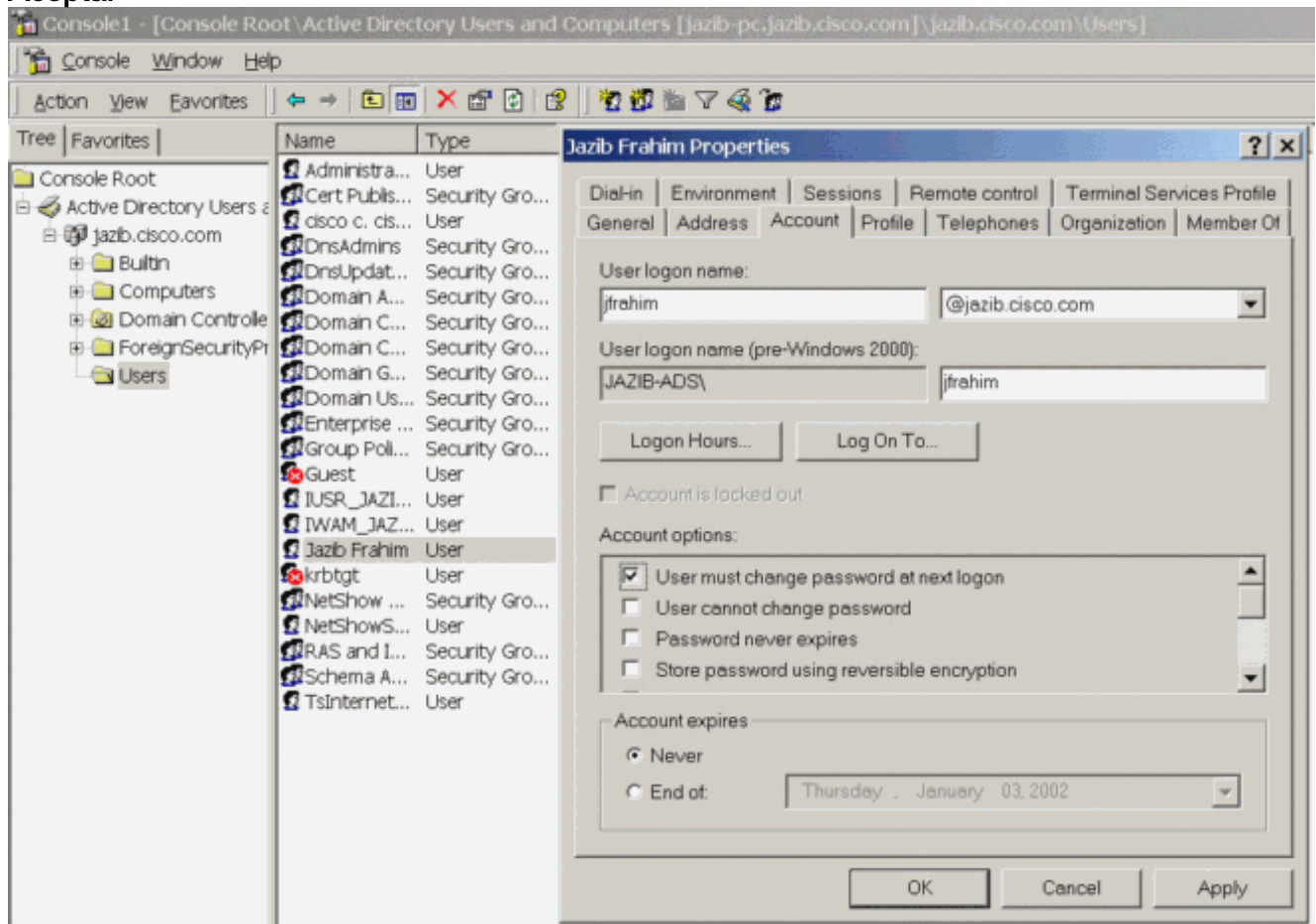


correcta". Si recibe algún mensaje que no sea el que se muestra arriba, hay algún problema de configuración o conexión. Repita los pasos de configuración y prueba descritos en este documento para asegurarse de que todos los parámetros se hayan realizado correctamente. Compruebe también la conectividad IP entre los dispositivos.

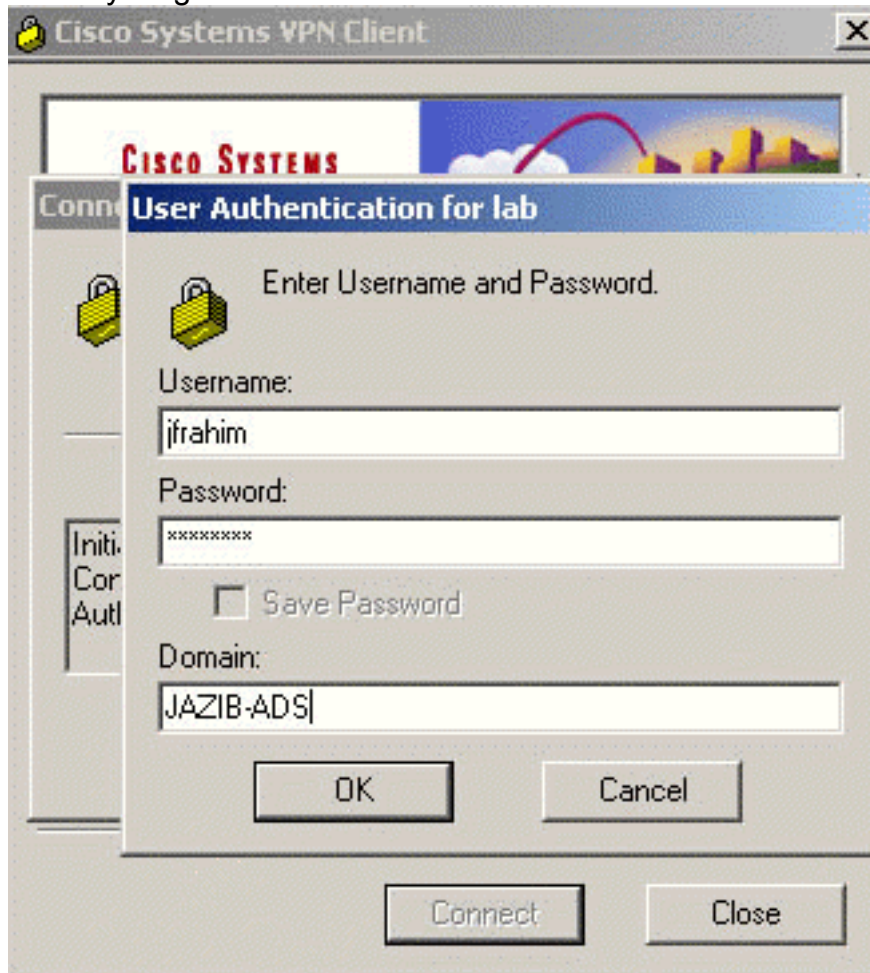
[Autenticación de dominio NT real mediante el proxy de RADIUS para probar la característica de vencimiento de contraseña](#)

1. Si el usuario ya está definido en el servidor de dominio, modifique las propiedades para que se le pida al usuario que cambie la contraseña en el próximo inicio de sesión. Vaya a la ficha "Cuenta" del cuadro de diálogo de propiedades del usuario, seleccione la opción para **EI**

usuario debe cambiar la contraseña en el siguiente inicio de sesión y haga clic en **Aceptar**.



2. Inicie el cliente VPN y luego intente establecer el túnel al



concentrador.

3. Durante la autenticación de usuario, se le solicitará que cambie la



contraseña.

[Información Relacionada](#)

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