

Configuratie van Cisco VPN 3000 Series Concentrators om de NT Password Expiration-functie met de RADIUS-server te ondersteunen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Netwerkdigram](#)

[De VPN-concentratie configureren 3000](#)

[Configuratie van groepen](#)

[RADIUS-configuratie](#)

[De Cisco Secure NT RADIUS-server configureren](#)

[Een ingang voor VPN 3000 Concentrator configureren](#)

[Het onbekende gebruikersbeleid voor NT Domain Authentication configureren](#)

[De NT/RADIUS-wachtwoordverloopfunctie testen](#)

[RADIUS-verificatie testen](#)

[Feitelijke NT-domeinverificatie met RADIUS-proxy om de wachtwoordverloopfunctie te testen](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document bevat stap-voor-stap instructies voor het configureren van de Cisco VPN 3000 Series Concentrators om de NT Password Expiration-functie te ondersteunen via de RADIUS-server.

Raadpleeg [VPN 3000 RADIUS met verloopfunctie met Microsoft Internet Authentication Server](#) om meer te weten te komen over hetzelfde scenario bij de Internet Verificatie Server (IAS).

[Voorwaarden](#)

[Vereisten](#)

- Als uw RADIUS-server en NT-domeinverificatieserver op twee afzonderlijke machines staan, zorg er dan voor dat u IP-connectiviteit tussen de twee machines hebt gerealiseerd.
- Zorg dat u IP-connectiviteit hebt ingesteld van de concentrator naar de RADIUS-server. Als de RADIUS-server naar de openbare interface is gericht, vergeet dan niet de RADIUS-poort op het openbare filter te openen.

- Verzeker dat u met de concentrator van de VPN client kunt verbinden met behulp van de interne gebruikersdatabase. Als dit niet is ingesteld, raadpleegt u [IPSec - Cisco 3000 VPN-client configureren naar VPN 3000 Concentrator](#).

N.B.: De wachtwoordverloopfunctie kan niet worden gebruikt voor VPN-clients van Web of SSL VPN.

Gebruikte componenten

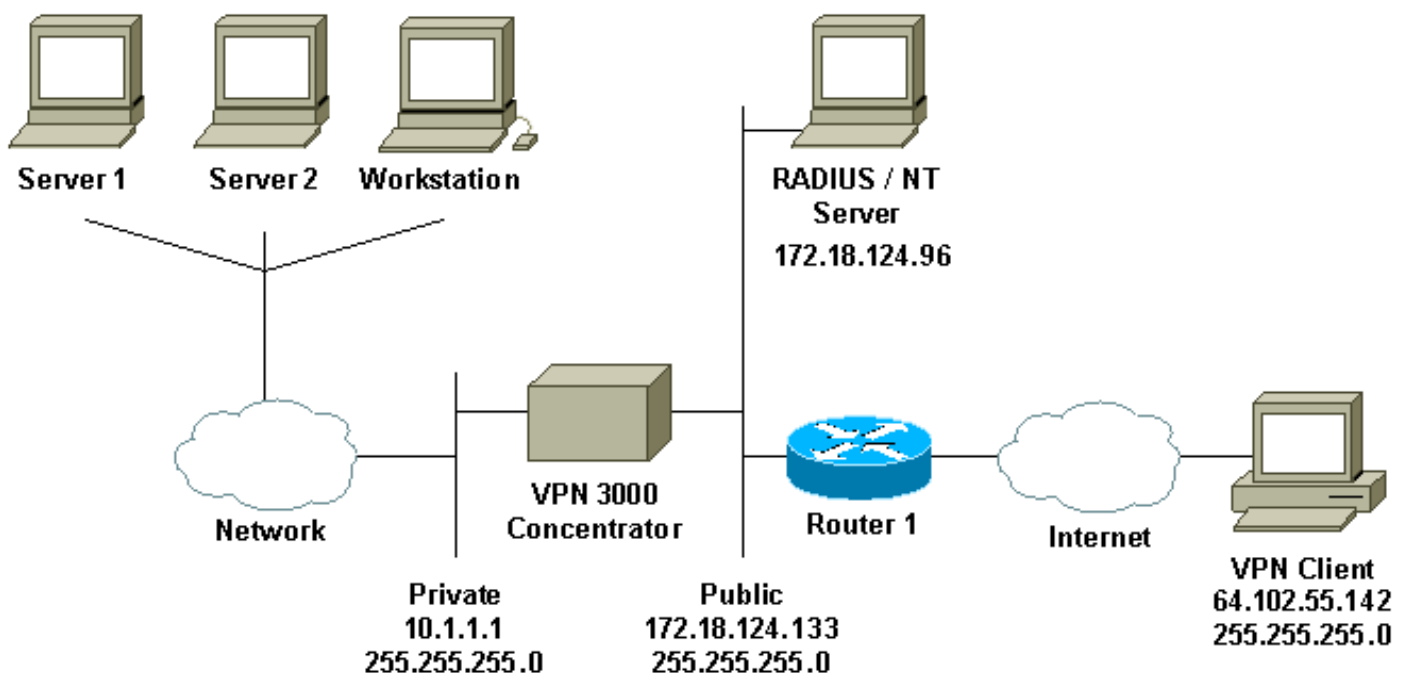
Deze configuratie is ontwikkeld en getest met behulp van de onderstaande software- en hardwareversies.

- Software voor VPN 3000 Concentrator, versie 4.7
- VPN-clientrelease 3.5
- Cisco Secure voor NT (CSNT) versie 3.0 Microsoft Windows 2000 Active Directory Server voor gebruikersverificatie

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



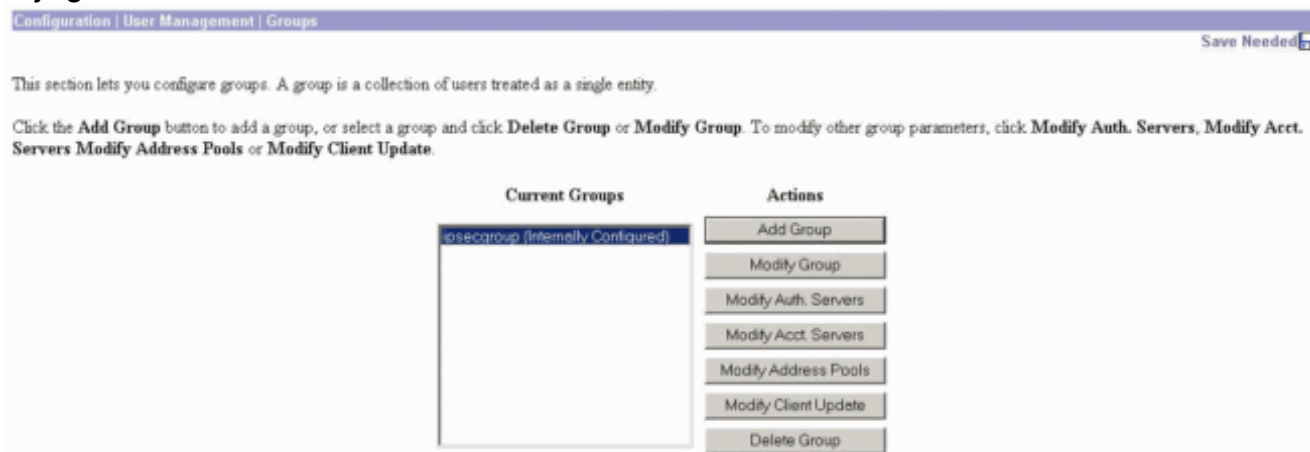
Opmerkingen bij diagrammen

1. De RADIUS-server in deze configuratie bevindt zich in de openbare interface. Als dit met uw specifieke instelling het geval is, maakt u twee regels in uw openbare filter zodat RADIUS-verkeer de concentrator kan binnengaan en verlaten.
2. Deze configuratie toont CSNT-software en NT-domeinverificatieservices op dezelfde machine. Deze elementen kunnen indien nodig op twee afzonderlijke machines worden uitgevoerd.

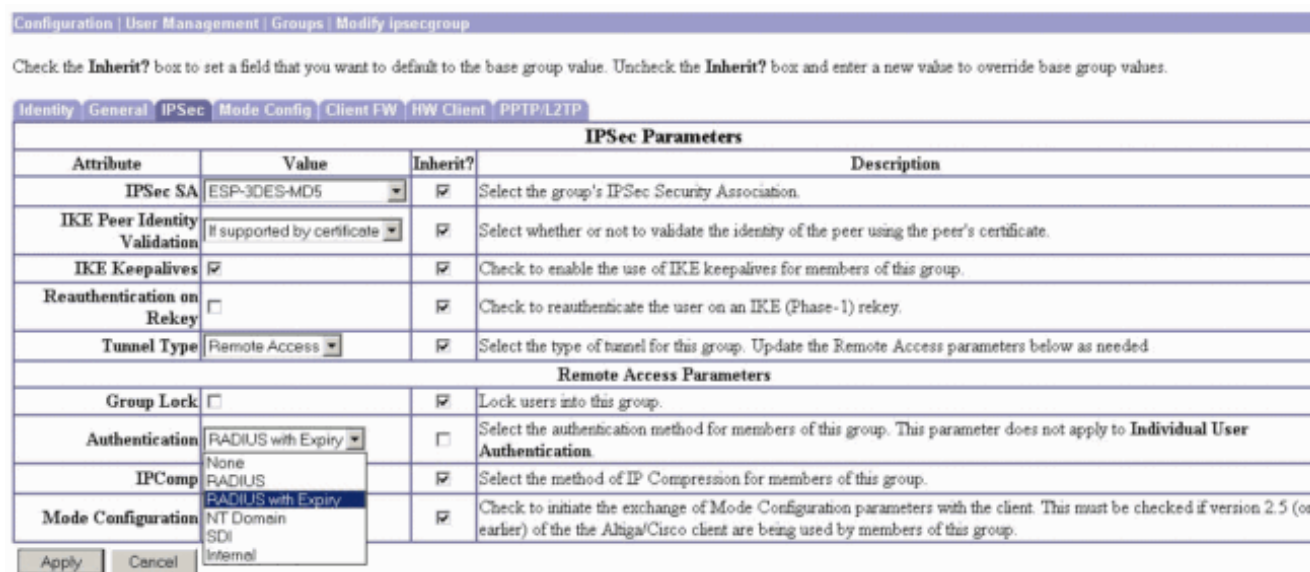
De VPN-concentratie configureren 3000

Configuratie van groepen

1. Om de groep te configureren die de NT Password EXpiration parameters accepteert vanaf de RADIUS-server, gaat u naar **Configuration > User Management > Group**, selecteert u uw groep in de lijst en klikt u op **Wijzigen**. Het onderstaande voorbeeld toont hoe u een groep met de naam "ipsecgroup" kunt wijzigen.



2. Ga naar het tabblad **IPSec**, zorg ervoor dat **RADIUS met Verlopen** is geselecteerd voor de eigenschap **Verificatie**.



3. Als u wilt dat deze optie ingeschakeld is op de VPN 3002-hardwareclients, gaat u naar het tabblad **HW-client**, zorg er dan voor dat **de verificatie van interactieve hardware** is ingeschakeld en klik vervolgens op **Toepassen**.

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-configuratie

1. Om de RADIUS-serverinstellingen op de concentrator te configureren gaat u naar **Configuration > System > Server > Verificatie > 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. Typ in het scherm **Add** de waarden die overeenkomen met de RADIUS-server en klik op **Add**. Het onderstaande voorbeeld gebruikt de volgende waarden.

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.

[De Cisco Secure NT RADIUS-server configureren](#)

[Een ingang voor VPN 3000 Concentrator configureren](#)

1. Log in op CSNT en klik op **Netwerkconfiguratie** in het linker paneel. Klik onder "AAA-clients" op **Toevoegen**.

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. Typ in het scherm "AAA-client toevoegen" de juiste waarden om de concentrator aan de RADIUS-client toe te voegen en klik vervolgens op **Inzenden + Herstarten**. Het onderstaande voorbeeld gebruikt de volgende waarden.

AAA Client Hostname = **133_3000_conc**

AAA Client IP Address = **172.18.124.133**

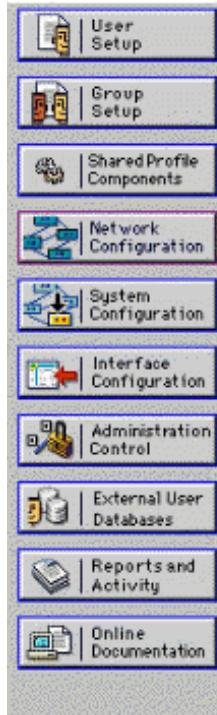
Key = **cisco123**

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	

Een punt voor uw 3000 concentrator verschijnt onder het gedeelte "AAA-clients".



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)

[Het onbekende gebruikersbeleid voor NT Domain Authentication configureren](#)

1. Om gebruikersverificatie op de RADIUS-server te configureren als onderdeel van het Onbekende gebruikersbeleid, klikt u op **Externe gebruikersdatabase** in het linker paneel en vervolgens klikt u op de link voor **Databaseconfiguratie**.




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

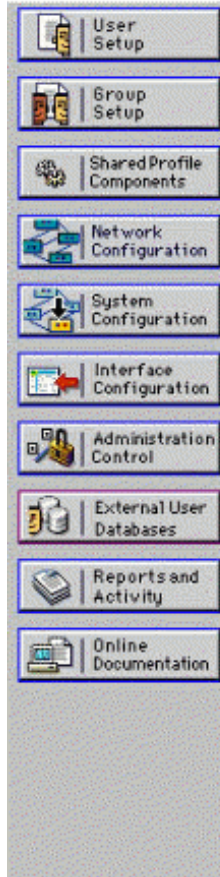
- [Unknown User Policy](#)
- [Database Group Mappings](#)
- [Database Configuration](#)

 [Back to Help](#)

2. Klik onder "Externe gebruikersdatabase Configuration" op **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](#)

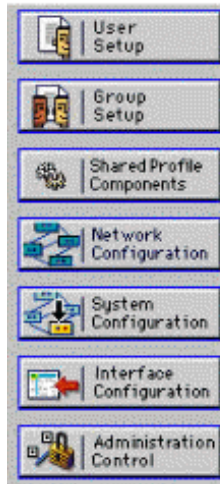
[List all database configurations](#)

Cancel

3. Klik in het scherm "Database Configuration Creation" op **New Configuration**.



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. Typ desgevraagd een naam voor de NT/2000-verificatie en klik vervolgens op **Indienen**. Het voorbeeld hieronder toont de naam "Straal/NT Wachtwoord Verlopen."



External User Databases



Edit

Create a new External Database Configuration ?

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

5. Klik op Configureren om de domeinnaam voor gebruikersverificatie te configureren.



External User Databases



Edit

External User Database Configuration ?

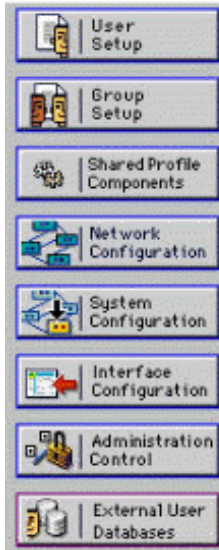
Choose what to do with the Windows NT/2000 database.

6. Selecteer uw NT-domein van de "Beschikbare domeinen" en klik vervolgens op de knop naar rechts om het toe te voegen aan de "Domain List". Zorg er onder "MS-CHAP Settings" voor dat de opties voor **wachtwoordwijzigingen met behulp van MS-CHAP versie 1** en **versie 2** zijn geselecteerd. Klik op **Inzenden** als u klaar bent.


7. Klik op **Externe gebruikersdatabase** in het linker paneel en klik vervolgens op de link voor **Databasegroep Mappings** (zoals in dit [voorbeeld](#) wordt gezien). U dient een bestandsindeling te zien voor de eerder ingestelde externe database. Het voorbeeld hieronder toont een ingang voor "Straal/NT Wachtwoord Verlopen", de gegevensbestand dat wij net vormden.



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. Klik op het scherm "Domain Configuration" op **New Configuration** om de domeinconfiguraties toe te voegen.



External User Databases



Edit

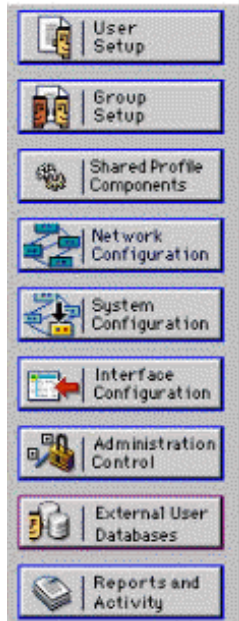
Domain Configurations 

[DEFAULT](#)

9. Selecteer uw domein in de lijst met "Geheime velden" en klik op **Indienen**. Het voorbeeld hieronder toont een domein genaamd "JAZIB-ADS".



External User Databases



Edit

Define New Domain Configuration

Detected Domains:

JAZIB-ADS

Clear Selection

Domain:

Submit Cancel

10. Klik op de naam van uw domein om de groepstoewijzing te configureren. Dit voorbeeld toont het domein "JAZIB-ADS".



External User Databases



Edit

Domain Configurations

[JAZIB-ADS](#)

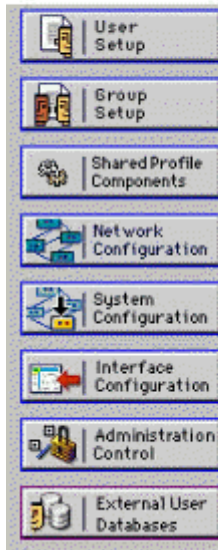
[\DEFAULT](#)

New configuration

11. Klik op **Add mapping** om de groepstoewijzing te definiëren.



External User Databases



Edit

Group Mappings for Domain : JAZIB-ADS

NT groups	CiscoSecure group
	- no mappings defined -

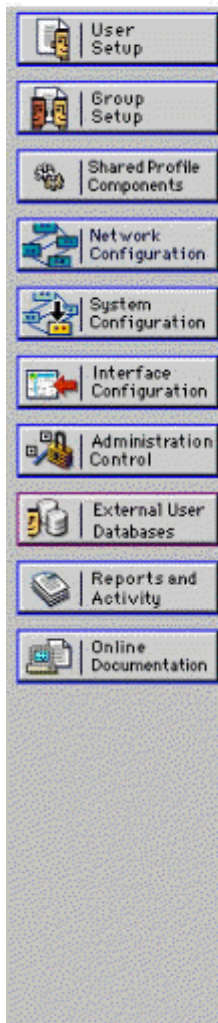
Add mapping

Delete Configuration

12. Stel in het scherm "Create new group mapping" de groep op het NT-domein in op een groep op de CSNT RADIUS-server en klik vervolgens op **Inzenden**. Het voorbeeld hieronder brengt de NT-groep "Gebruikers" in kaart aan de RADIUS-groep "Groep 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

Add to selected Remove from selected

Selected

- Users

Up Down

CiscoSecure group: Group 1

Submit Cancel

13. Klik op **Externe gebruikersdatabase** in het linker paneel en klik vervolgens op de link voor

Onbekend gebruikersbeleid (zoals in dit [voorbeeld](#) wordt gezien). Zorg ervoor dat de optie voor de volgende externe gebruikersdatabases is geselecteerd. Klik op de knop pijl-rechts om de eerder ingesteld externe database van de lijst van "Externe databases" te verplaatsen naar de lijst van "Geselecteerde databases".

The screenshot shows the Cisco Systems configuration interface for External User Databases. The sidebar on the left contains various configuration options, with 'External User Databases' highlighted. The main window is titled 'External User Databases' and features a 'Configure Unknown User Policy' section. This section includes a description: 'Use this table to define how users will be handled when they are not found in the CiscoSecure Database.' There are two radio button options: 'Fail the attempt' and 'Check the following external user databases', with the second option selected. Below these options are two lists: 'External Databases' (currently empty) and 'Selected Databases' (containing 'Radius/NT Password Exp'). Navigation buttons for moving items between lists and 'Up/Down' buttons are also visible.

[De NT/RADIUS-wachtwoordverloopfunctie testen](#)

De concentrator biedt een functie om de RADIUS-verificatie te testen. Om deze optie goed te testen, moet u deze stappen voorzichtig uitvoeren.

[RADIUS-verificatie testen](#)

1. Ga naar **Configuratie > Systeem > servers > Verificatie**. Selecteer uw RADIUS-server en klik op **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. Typ desgevraagd uw NT-naam en -wachtwoord en klik vervolgens op **OK**. Het onderstaande voorbeeld toont de gebruikersnaam "jfracim" ingesteld op de NT-domeinserver met "cisco123" als het wachtwoord.


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

User Name

Password

3. Als uw authenticatie goed is ingesteld, dient u een bericht te krijgen met de titel "Verificatie

Success

 Authentication Successful

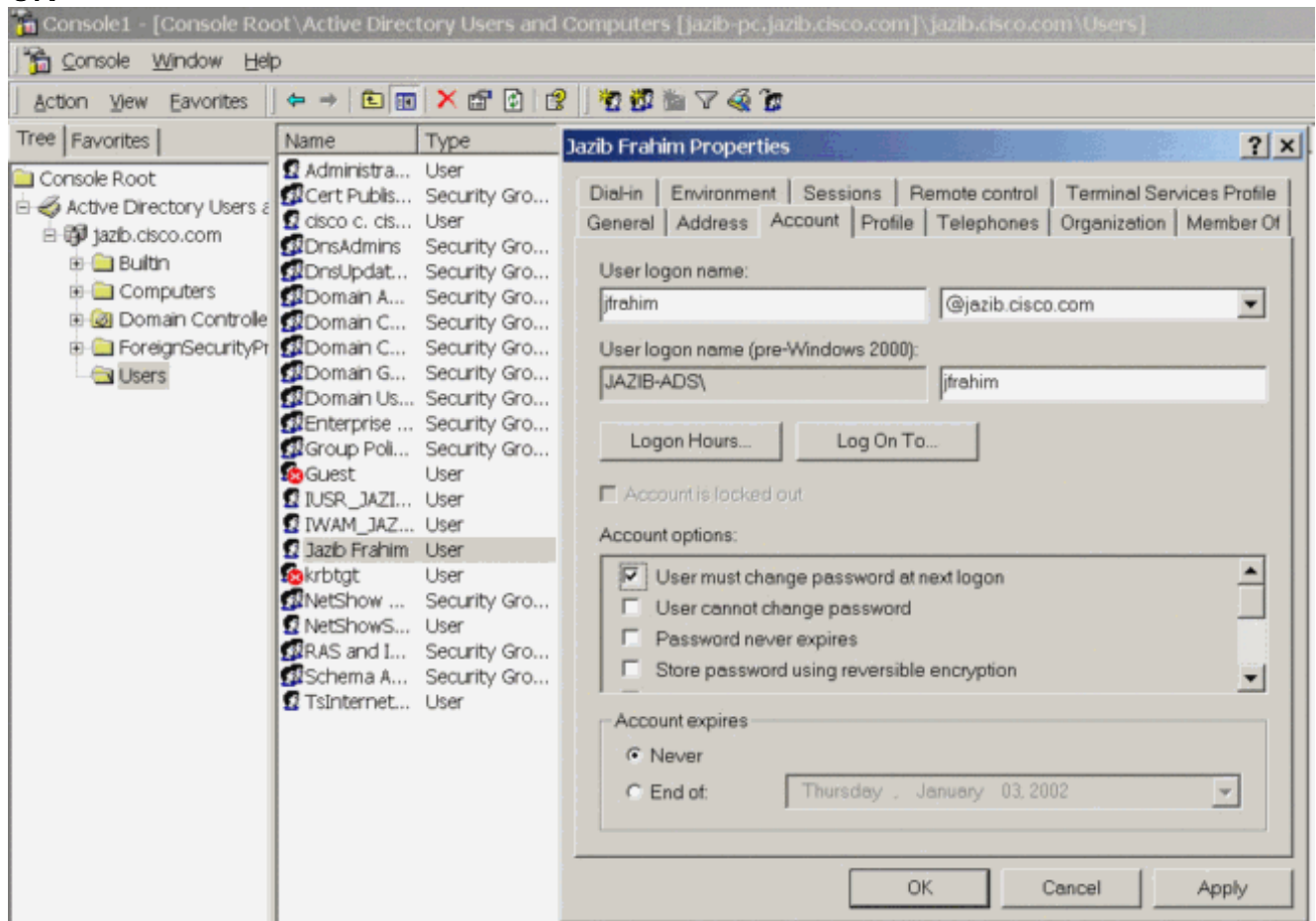
succesvol".

Als u een ander bericht ontvangt dan het bericht dat hierboven wordt getoond, is er een probleem met de configuratie of verbinding. Herhaal de configuratie- en teststappen die in dit document zijn beschreven om er zeker van te zijn dat alle instellingen correct zijn uitgevoerd. Controleer ook de IP-connectiviteit tussen uw apparaten.

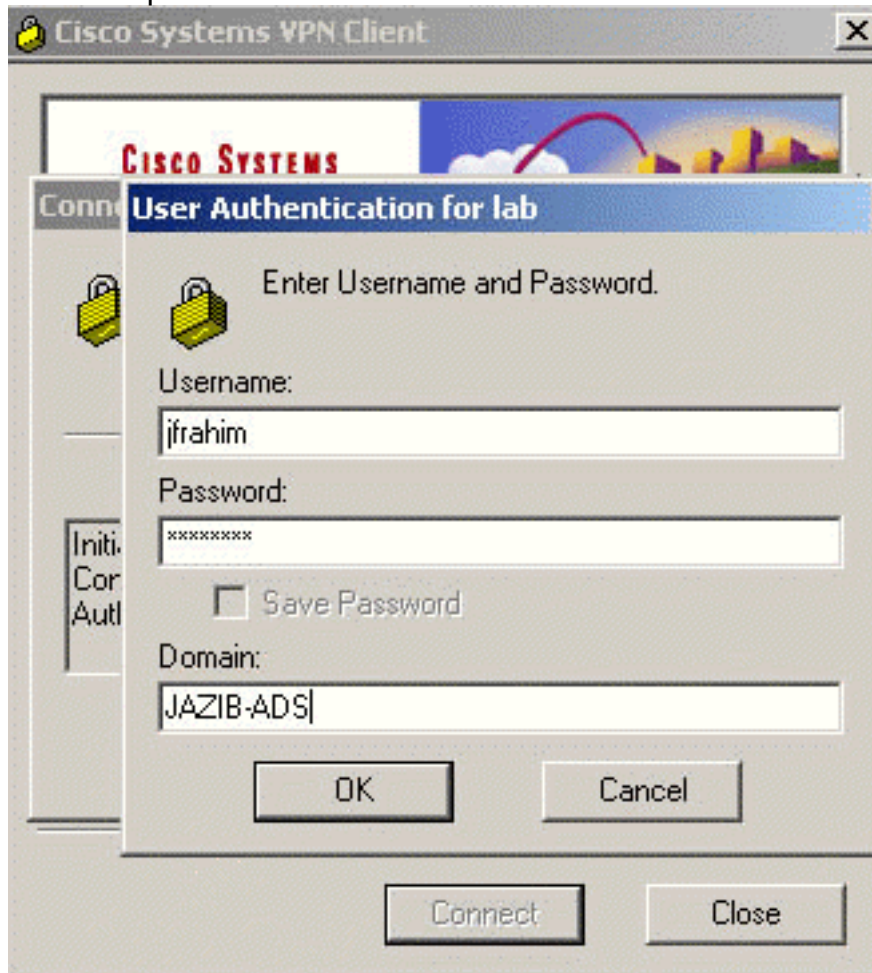
[Feitelijke NT-domeinverificatie met RADIUS-proxy om de wachtwoordverloopfunctie te testen](#)

1. Als de gebruiker al op de domeinserver is gedefinieerd, kunt u de eigenschappen wijzigen, zodat de gebruiker wordt gevraagd het wachtwoord bij de volgende aanmelding te wijzigen. Ga naar het tabblad "Account" van het dialoogvenster eigenschappen van de gebruiker, selecteer de optie voor **gebruiker om wachtwoord te wijzigen bij de volgende aanmelding** en

klik vervolgens op
OK.



2. Start de VPN-client en probeer dan de tunnel in te stellen naar de



concentrator.

3. Tijdens de gebruikersverificatie moet u worden gevraagd het wachtwoord te



wijzigen.

[Gerelateerde informatie](#)

- [Cisco VPN 3000 Series Concentrator](#)
- [IPsec](#)
- [Cisco Secure Access Control Server voor Windows](#)
- [RADIUS](#)
- [Verzoeken om opmerkingen \(RFC's\)](#)