

Konfigurieren Sie die Cisco VPN Concentrators der Serie 3000, um die Funktion zum Ablauf eines NT-Kennworts mit dem RADIUS-Server zu unterstützen.

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Netzwerkdigramm](#)

[Konfigurieren des VPN 3000-Konzentrators](#)

[Gruppenkonfiguration](#)

[RADIUS-Konfiguration](#)

[Konfigurieren des Cisco Secure NT RADIUS-Servers](#)

[Konfigurieren eines Eintrags für den VPN 300-Konzentrator](#)

[Konfigurieren der unbekanntes Benutzerrichtlinie für die NT-Domänenauthentifizierung](#)

[Testen der NT/RADIUS-Kennwortablauffunktion](#)

[Testen der RADIUS-Authentifizierung](#)

[Tatsächliche NT-Domänenauthentifizierung mithilfe des RADIUS-Proxys zum Testen der Funktion zum Ablauf des Kennworts](#)

[Zugehörige Informationen](#)

[Einführung](#)

Dieses Dokument enthält schrittweise Anweisungen zur Konfiguration der Cisco VPN Concentrators der Serie 3000 für die Unterstützung der NT Password Expiration-Funktion unter Verwendung des RADIUS-Servers.

Unter [VPN 300 RADIUS mit Ablauffunktion unter Verwendung des Microsoft-Internet-Authentifizierungsservers](#) finden Sie weitere Informationen zum gleichen Szenario mit dem Internet Authentication Server (IAS).

[Voraussetzungen](#)

[Anforderungen](#)

- Wenn sich Ihr RADIUS-Server und Ihr NT Domain Authentication-Server auf zwei verschiedenen Computern befinden, stellen Sie sicher, dass Sie eine IP-Verbindung zwischen

den beiden Systemen hergestellt haben.

- Stellen Sie sicher, dass Sie die IP-Verbindung vom Konzentrator zum RADIUS-Server eingerichtet haben. Wenn sich der RADIUS-Server in Richtung der öffentlichen Schnittstelle befindet, vergessen Sie nicht, den RADIUS-Port im öffentlichen Filter zu öffnen.
- Stellen Sie sicher, dass Sie über den VPN-Client mithilfe der internen Benutzerdatenbank eine Verbindung zum Konzentrator herstellen können. Wenn dies nicht konfiguriert ist, lesen Sie die Informationen zur [Konfiguration von IPSec - Cisco 3000 VPN Client zum VPN 3000 Concentrator](#).

Hinweis: Die Kennwortablauffunktion kann nicht mit Web-VPN- oder SSL-VPN-Clients verwendet werden.

Verwendete Komponenten

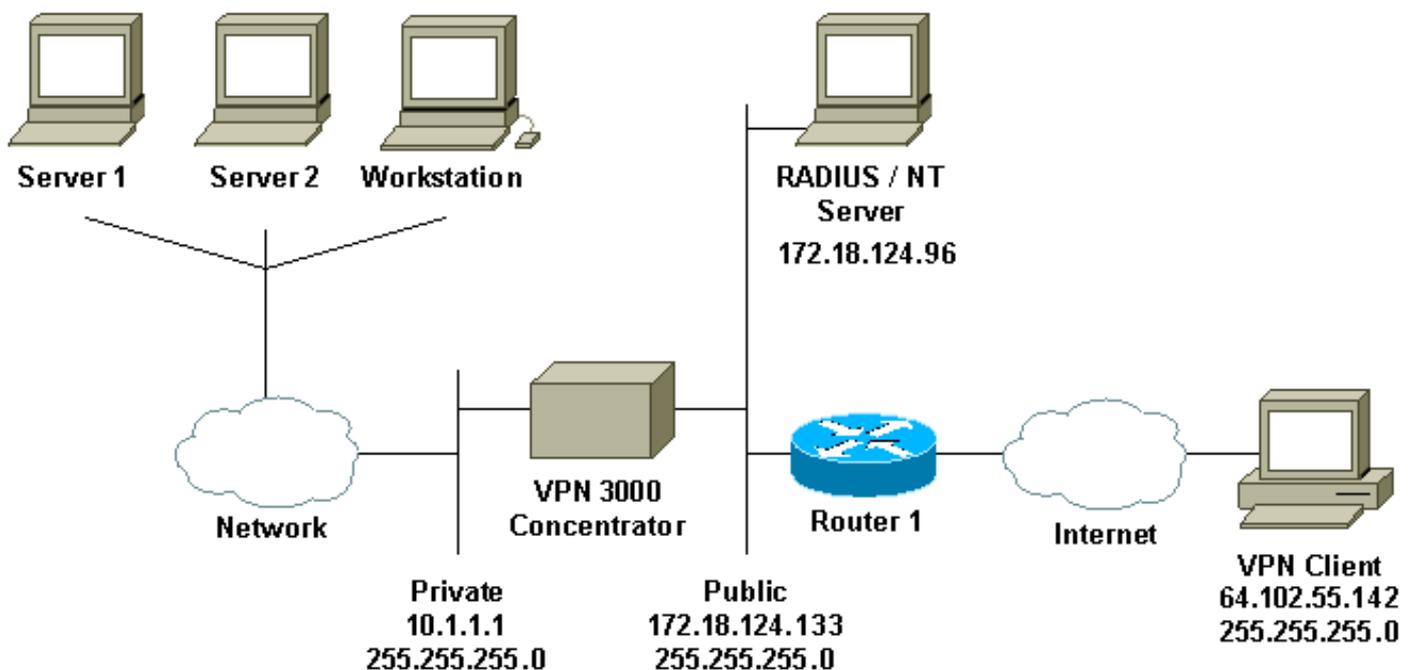
Diese Konfiguration wurde mit den unten stehenden Software- und Hardwareversionen entwickelt und getestet.

- VPN 3000 Concentrator Software Version 4.7
- VPN-Client Version 3.5
- Cisco Secure for NT (CSNT) Version 3.0 Microsoft Windows 2000 Active Directory Server für die Benutzerauthentifizierung

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Diagrammnotizen

1. Der RADIUS-Server in dieser Konfiguration befindet sich auf der öffentlichen Schnittstelle.

Wenn dies bei Ihrer spezifischen Konfiguration der Fall ist, erstellen Sie bitte zwei Regeln in Ihrem öffentlichen Filter, damit der RADIUS-Datenverkehr in den Konzentrator eintritt und diesen verlässt.

- In dieser Konfiguration werden CSNT-Software und NT-Domänenauthentifizierungsdienste angezeigt, die auf demselben Computer ausgeführt werden. Diese Elemente können auf zwei verschiedenen Computern ausgeführt werden, wenn die Konfiguration dies erfordert.

Konfigurieren des VPN 3000-Konzentrators

Gruppenkonfiguration

- Um die Gruppe so zu konfigurieren, dass sie die NT-Kennwort-Ablaufparameter vom RADIUS-Server akzeptiert, gehen Sie zu **Konfiguration > Benutzerverwaltung > Gruppen**, wählen Sie Ihre Gruppe aus der Liste aus, und klicken Sie auf **Gruppe ändern**. Im folgenden Beispiel wird veranschaulicht, wie eine Gruppe mit dem Namen "ipsecgroup" geändert wird.

- Wechseln Sie zur Registerkarte **IPSec**, und stellen Sie sicher, dass **RADIUS mit Ablaufdatum** für das **Authentication**-Attribut ausgewählt ist.

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 Altiga/Cisco client are being used by members of this group.

- Wenn Sie diese Funktion auf den VPN 3002-Hardware-Clients aktivieren möchten, gehen Sie zur Registerkarte **HW Client**, stellen Sie sicher, dass **Interaktive Hardware-Client-Authentifizierung** aktiviert ist, und klicken Sie dann auf

Apply.

Configuration | User Management | Groups | Modify ipsecgroup

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.

Identity | General | IPsec | Mode Config | Client FW | HW Client | PPTP/L2TP

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-Konfiguration

1. Um die RADIUS-Servereinstellungen für den Konzentrator zu konfigurieren, gehen Sie zu **Configuration > System > Servers > Authentication > Add.**

Configuration | System | Servers | Authentication

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. Geben Sie im Bildschirm **Add** die Werte ein, die dem RADIUS-Server entsprechen, und klicken Sie auf **Hinzufügen**. Im folgenden Beispiel werden die folgenden Werte verwendet.
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"/>		

[Konfigurieren des Cisco Secure NT RADIUS-Servers](#)

[Konfigurieren eines Eintrags für den VPN 300-Konzentrator](#)

1. Melden Sie sich bei CSNT an, und klicken Sie im linken Bereich auf **Netzwerkconfiguration**. Klicken Sie unter "AAA-Clients" auf **Eintrag hinzufügen**.

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. Geben Sie im Bildschirm "Add AAA Client" (AAA-Client hinzufügen) die entsprechenden Werte ein, um den Konzentrator als RADIUS-Client hinzuzufügen, und klicken Sie dann auf **Senden + Neu starten**. Im folgenden Beispiel werden die folgenden Werte verwendet.

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

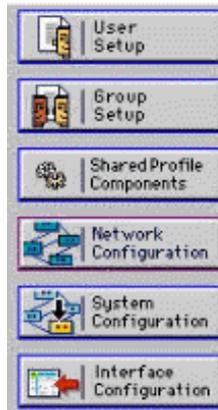
AAA Client Hostname	<input type="text" value="133_3000_conc"/>
AAA Client IP Address	<input type="text" value="172.18.124.133"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="text" value="RADIUS (Cisco VPN 3000)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client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

Ein Eintrag für Ihren 3000 Konzentrator wird im Abschnitt "AAA Clients" angezeigt.



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)

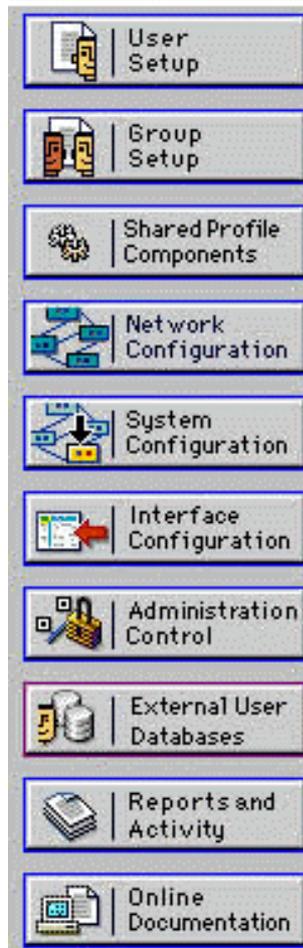
Konfigurieren der unbekanntem Benutzerrichtlinie für die NT-Domänenauthentifizierung

1. Um die Benutzerauthentifizierung auf dem RADIUS-Server als Teil der Richtlinie für unbekannte Benutzer zu konfigurieren, klicken Sie im linken Bereich auf **Externe Benutzerdatenbank** und dann auf den Link für **Datenbankkonfiguration**.



External User Databases

Select



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



2. Klicken Sie unter "Konfiguration der externen Benutzerdatenbank" auf **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](#)

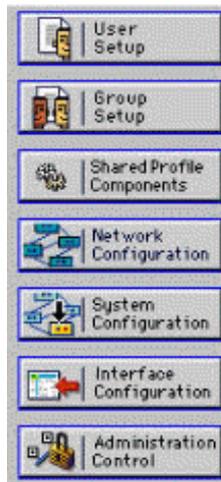
[List all database configurations](#)

Cancel

3. Klicken Sie im Bildschirm "Database Configuration Creation" auf **Create 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. Geben Sie bei Aufforderung einen Namen für die NT/2000-Authentifizierung ein, und klicken Sie auf **Senden**. Im folgenden Beispiel wird der Name "Radius/NT Password Expiration" angezeigt.



External User Databases



Edit

Create a new External Database Configuration ?

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

5. Klicken Sie auf **Konfigurieren**, um den Domännennamen für die Benutzerauthentifizierung zu konfigurieren.



External User Databases



Edit

External User Database Configuration ?

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

6. Wählen Sie Ihre NT-Domäne aus der Liste "Verfügbare Domänen" aus, und klicken Sie dann auf den Pfeil nach rechts, um sie der "Domänenliste" hinzuzufügen. Stellen Sie unter "MS-CHAP-Einstellungen" sicher, dass die Optionen für **Kennwortänderungen mit MS-CHAP Version 1** und **Version 2** ausgewählt sind. Klicken Sie abschließend auf **Senden**.



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. Klicken Sie im linken Bereich auf **Externe Benutzerdatenbank** und dann auf den Link für **Datenbankgruppenzuordnungen** (siehe [Beispiel](#)). Es sollte ein Eintrag für Ihre zuvor konfigurierte externe Datenbank angezeigt werden. Das Beispiel unten zeigt einen Eintrag für "Radius/NT Password Expiration", die Datenbank, die wir gerade konfiguriert haben.



External User Databases

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

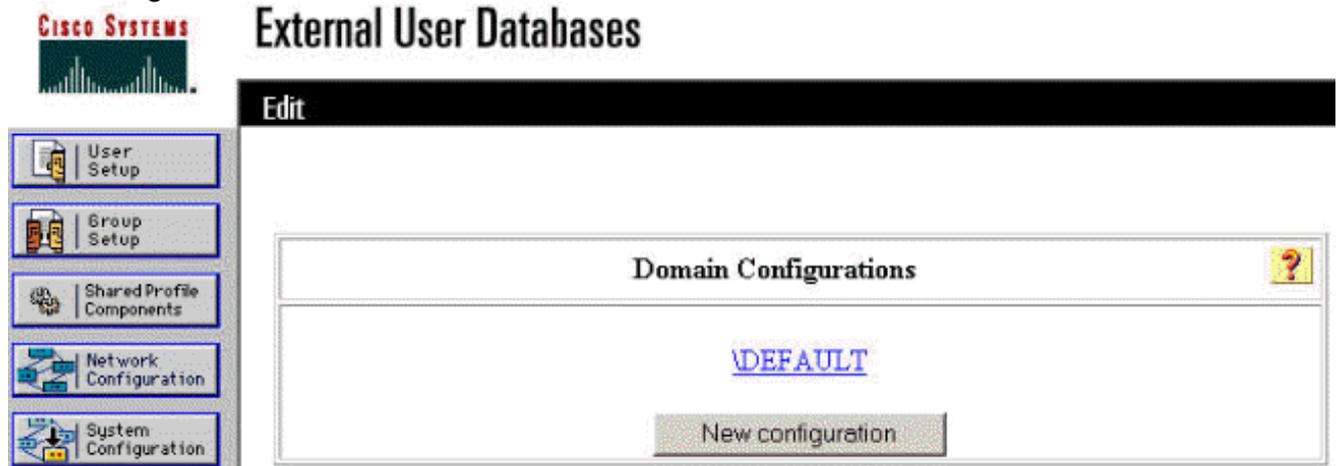
Select

Unknown User Group Mappings ?

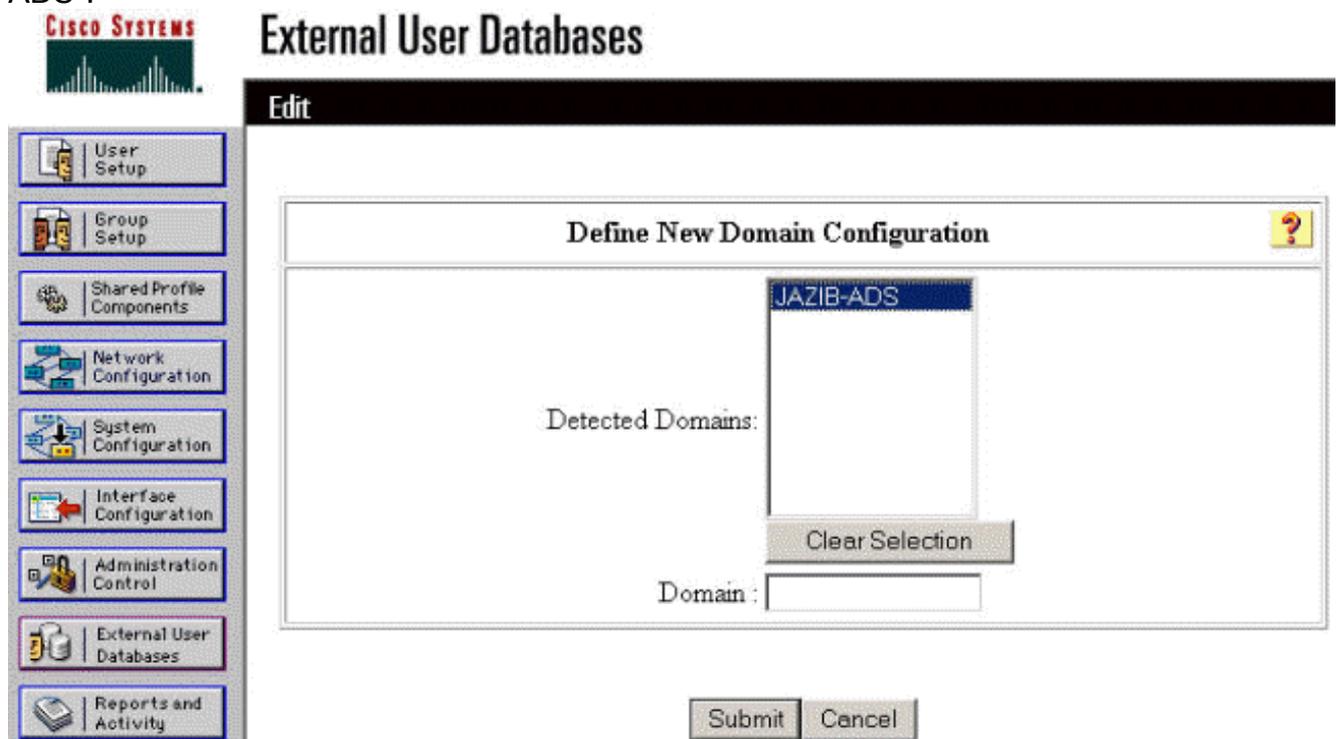
Choose the External User Database for which you want to configure the group mappings.

Name	Type
Radius/NT Password Expiration	Windows NT/2000

8. Klicken Sie im Bildschirm "Domänenkonfigurationen" auf **Neue Konfiguration**, um die Domänenkonfigurationen hinzuzufügen.



9. Wählen Sie Ihre Domäne aus der Liste "Erkannte Domänen" aus und klicken Sie auf **Senden**. Das nachfolgende Beispiel zeigt eine Domäne mit dem Namen "JAZIB-ADS".



10. Klicken Sie auf Ihren Domännennamen, um die Gruppenzuordnungen zu konfigurieren. Dieses Beispiel zeigt die Domäne "JAZIB-ADS".



External User Databases

Edit

Domain Configurations 

[JAZIB-ADS](#)
[DEFAULT](#)

New configuration

11. Klicken Sie auf **Zuordnung hinzufügen**, um die Gruppenzuordnungen zu definieren.



External User Databases

Edit

Group Mappings for Domain : JAZIB-ADS 

NT groups	CiscoSecure group
- no mappings defined -	

Add mapping

Delete Configuration

12. Ordnen Sie im Bildschirm "Create new group mapping" (Neue Gruppenzuordnung erstellen) die Gruppe in der NT-Domäne einer Gruppe auf dem CSNT RADIUS-Server zu, und klicken Sie dann auf **Submit (Senden)**. Im folgenden Beispiel wird die NT-Gruppe "Benutzer" der RADIUS-Gruppe "Gruppe 1" zugeordnet.

Edit

Create new group mapping for Domain : JAZIB-ADS ?

Define NT group set

NT Groups

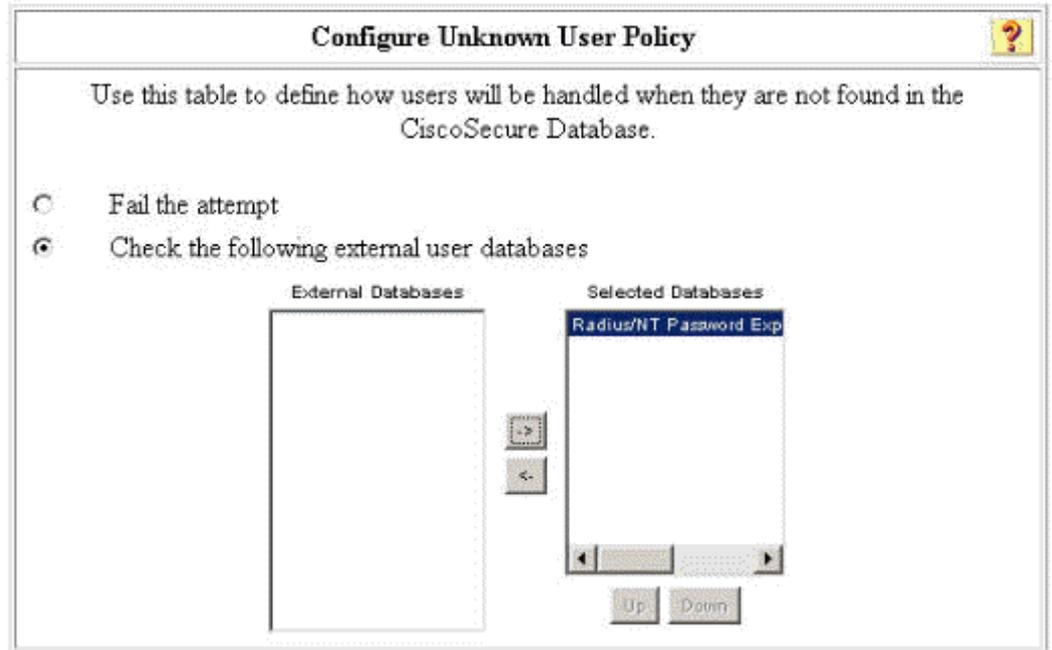
Administrators
Guests
 Backup Operators
 Replicator
 Server Operators
 Account Operators
 Print Operators

Selected

Users

CiscoSecure group:

13. Klicken Sie im linken Bereich auf **Externe Benutzerdatenbank** und dann auf den Link für **Unbekannte Benutzerrichtlinie** (wie in diesem [Beispiel](#) gezeigt). Stellen Sie sicher, dass die Option **Folgende externe Benutzerdatenbanken überprüfen** aktiviert ist. Klicken Sie auf den Pfeil nach rechts, um die zuvor konfigurierte externe Datenbank aus der Liste "Externe Datenbanken" in die Liste "Ausgewählte Datenbanken" zu verschieben.

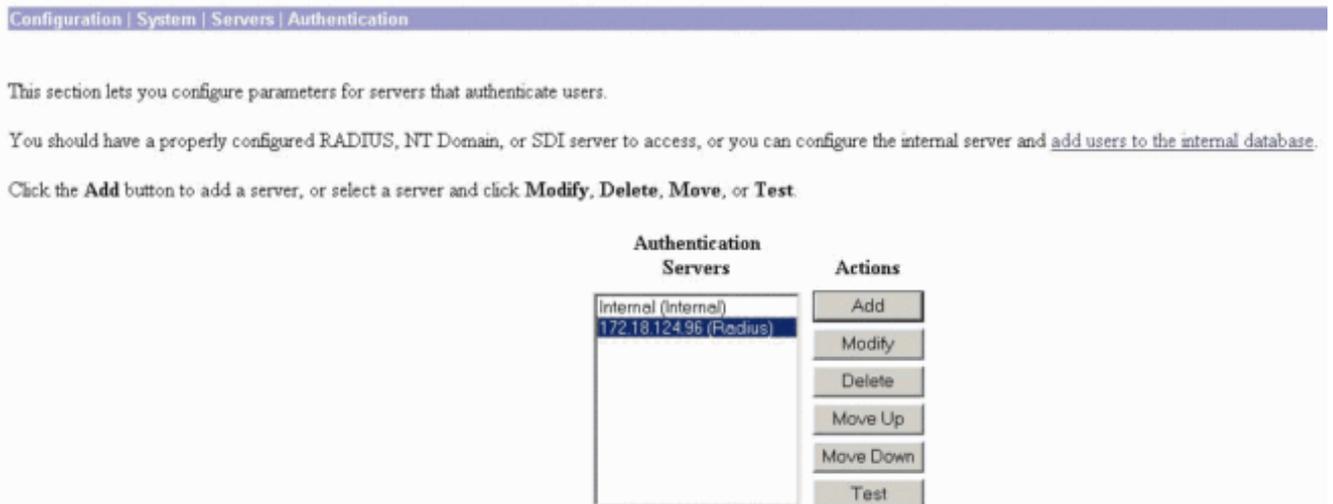


Testen der NT/RADIUS-Kennwortablauffunktion

Der Konzentrator bietet eine Funktion zum Testen der RADIUS-Authentifizierung. Um diese Funktion ordnungsgemäß zu testen, sollten Sie diese Schritte sorgfältig durchführen.

Testen der RADIUS-Authentifizierung

1. Gehen Sie zu **Configuration > System > Servers > Authentication**. Wählen Sie Ihren RADIUS-Server aus, und klicken Sie auf **Test**.



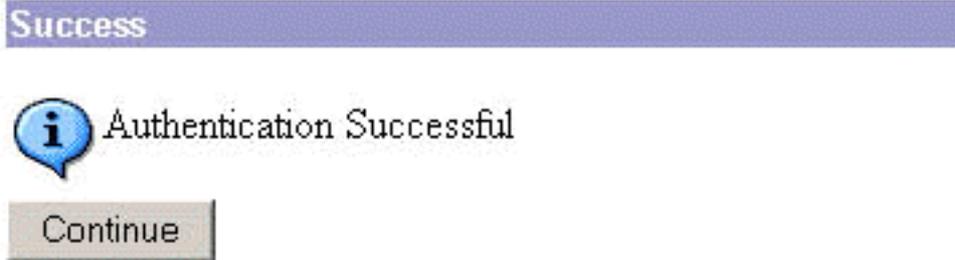
2. Wenn Sie dazu aufgefordert werden, geben Sie Ihren NT-Domännennamen und Ihr Kennwort ein, und klicken Sie dann auf **OK**. Das nachfolgende Beispiel zeigt den Benutzernamen "jfracim", der auf dem NT-Domänenserver mit dem Kennwort "cisco123" konfiguriert ist.

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

User Name

Password

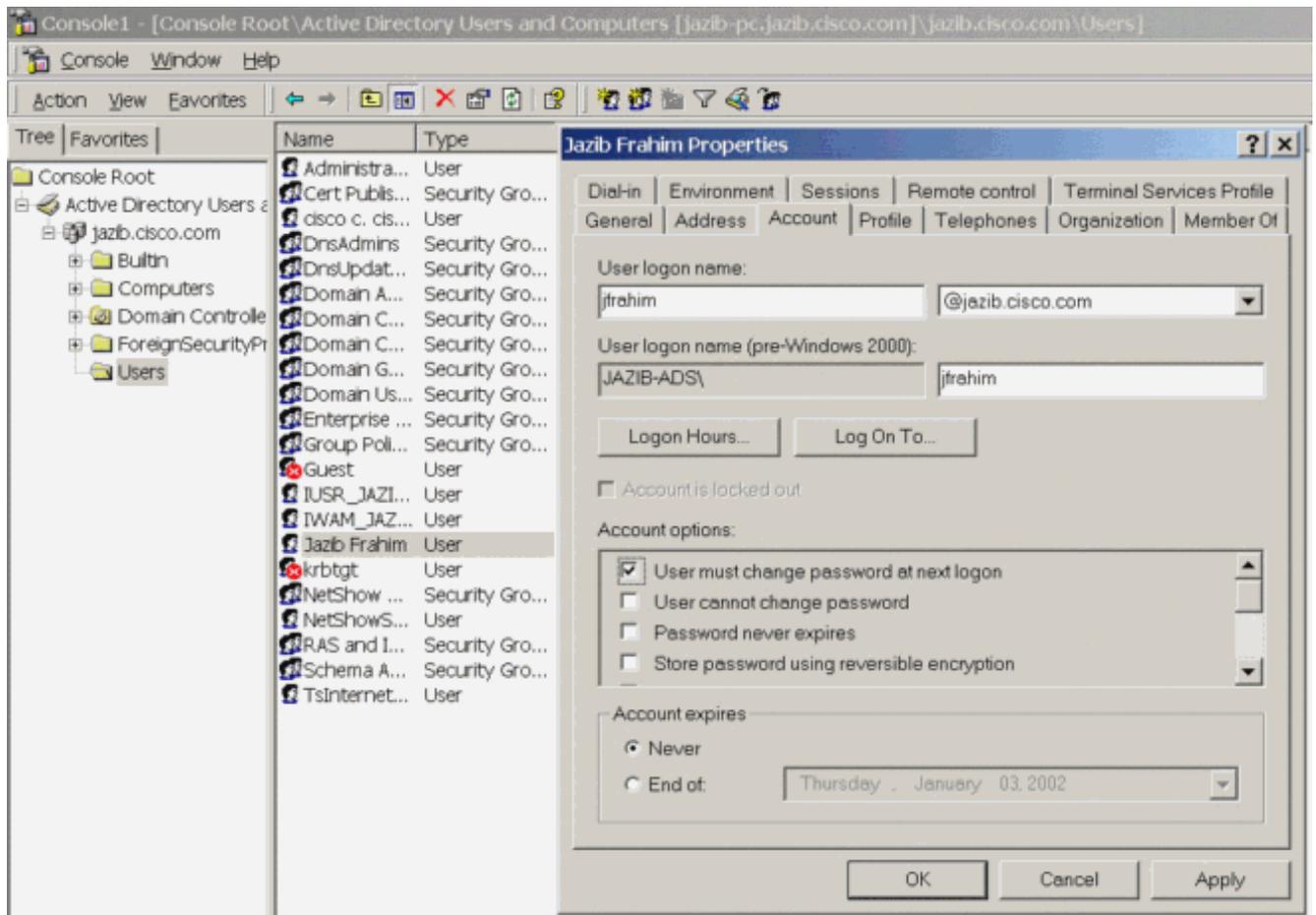
3. Wenn Ihre Authentifizierung ordnungsgemäß eingerichtet ist, erhalten Sie die Meldung "Authentication Successful" (Authentifizierung



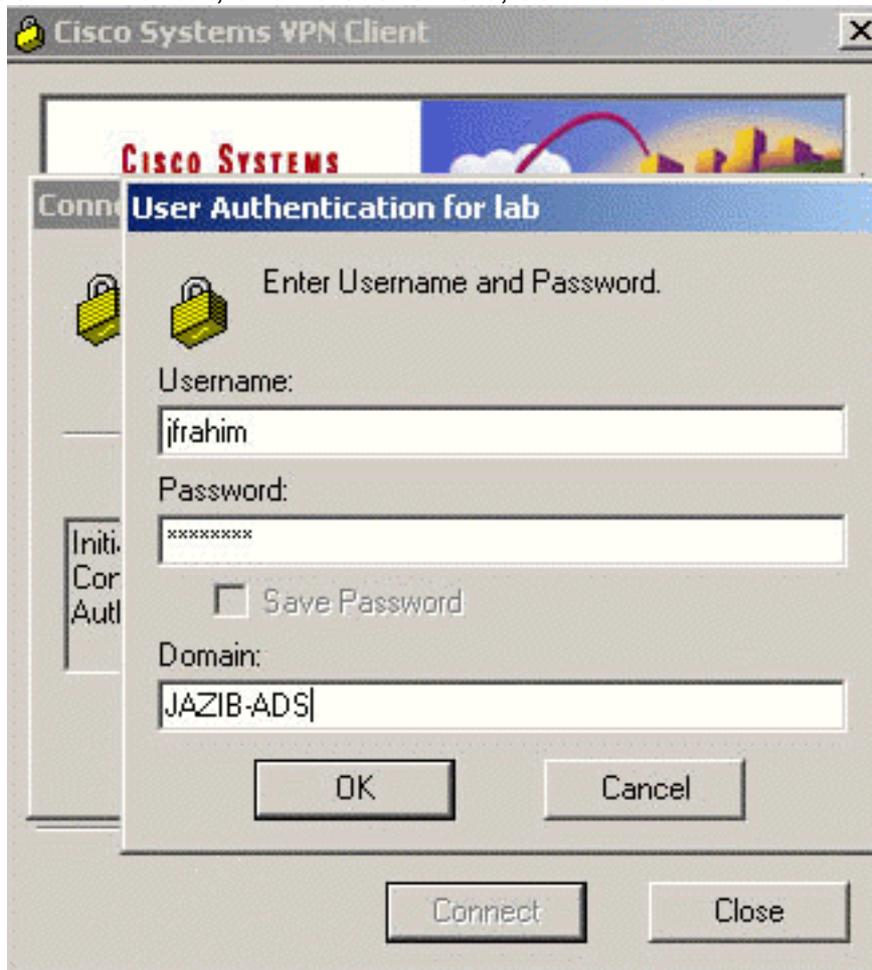
erfolgreich). Wenn Sie eine andere Meldung als die oben abgebildete erhalten, liegt ein Konfigurations- oder Verbindungsproblem vor. Wiederholen Sie die in diesem Dokument beschriebenen Konfigurations- und Testschritte, um sicherzustellen, dass alle Einstellungen ordnungsgemäß vorgenommen wurden. Überprüfen Sie auch die IP-Verbindung zwischen Ihren Geräten.

[Tatsächliche NT-Domänenauthentifizierung mithilfe des RADIUS-Proxys zum Testen der Funktion zum Ablauf des Kennworts](#)

1. Wenn der Benutzer bereits auf dem Domänenserver definiert ist, ändern Sie die Eigenschaften so, dass der Benutzer bei der nächsten Anmeldung aufgefordert wird, das Kennwort zu ändern. Gehen Sie zur Registerkarte "Konto" des Eigenschaftendialogfelds des Benutzers, wählen Sie die Option **Benutzer muss Kennwort bei der nächsten Anmeldung ändern**, und klicken Sie dann auf **OK**.



2. Starten Sie den VPN-Client, und versuchen Sie, den Tunnel zum Konzentrador



einzurichten.

3. Während der Benutzerauthentifizierung sollten Sie aufgefordert werden, das Kennwort zu



ändern.

Zugehörige Informationen

- [Cisco VPN Concentrator der Serie 3000](#)
- [IPSec](#)
- [Cisco Secure Access Control Server für Windows](#)
- [RADIUS](#)
- [Anforderungen für Kommentare \(RFCs\)](#)