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

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

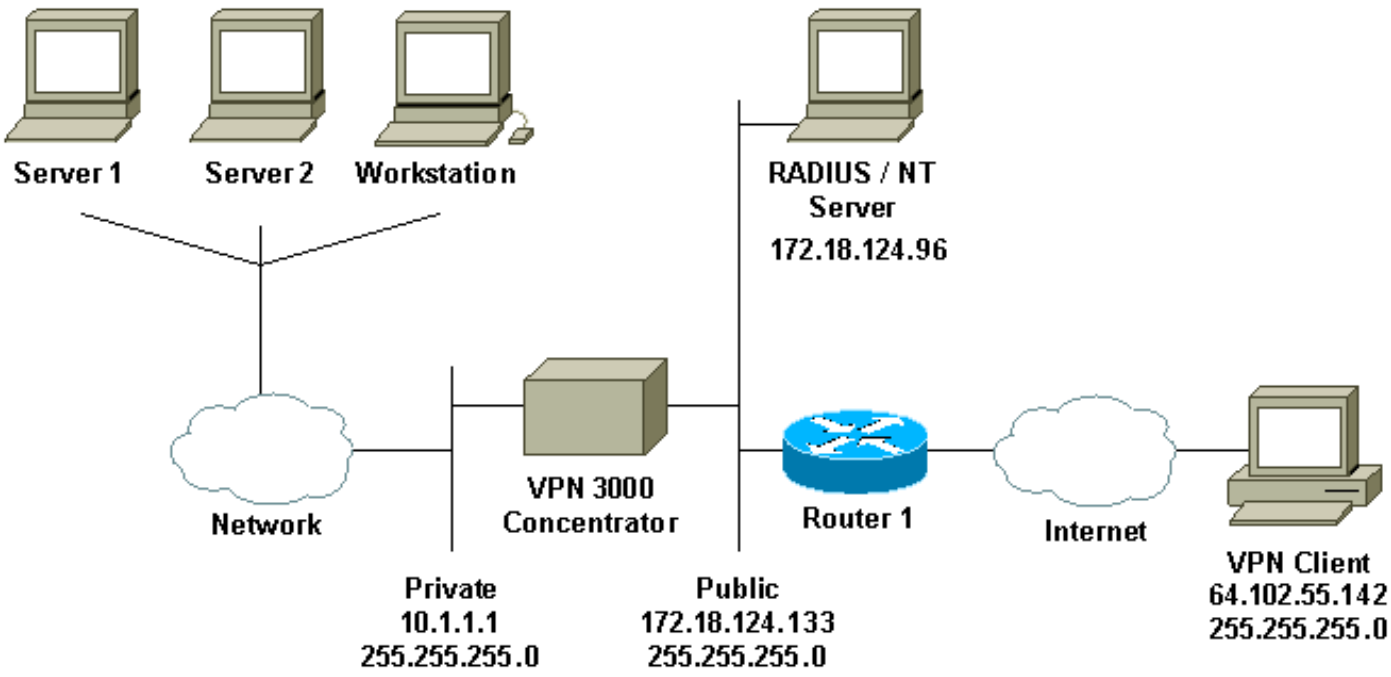
Diese Konfiguration wurde mit den unten stehenden Software- und Hardwareversionen entwickelt und getestet.

- 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.

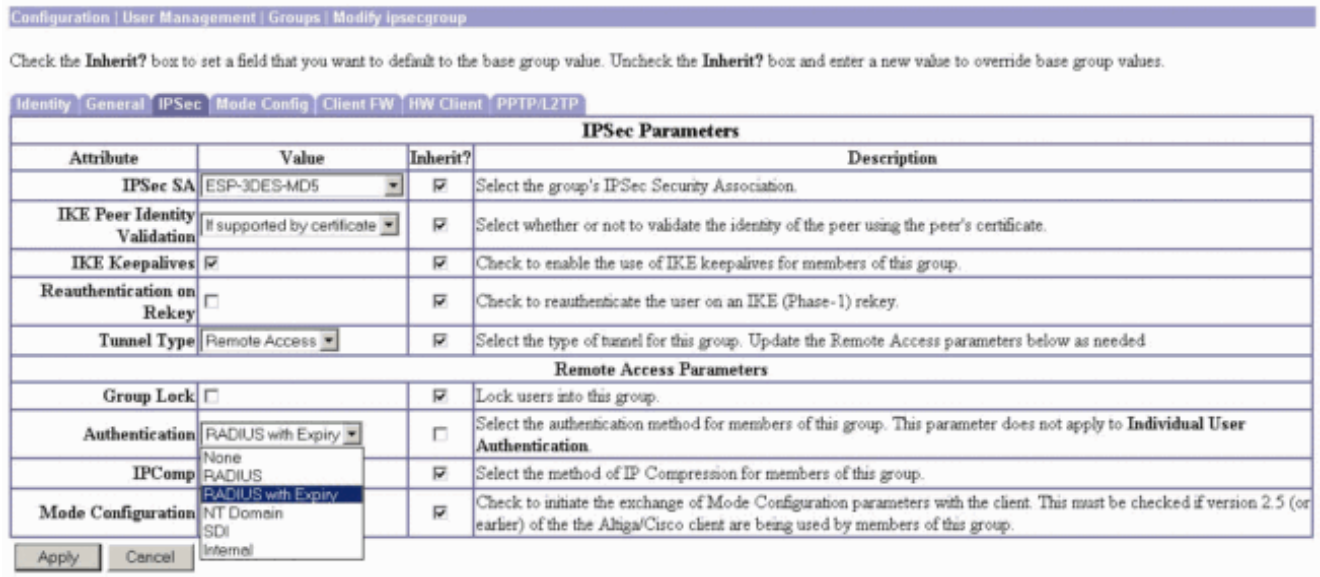
2. In dieser Konfiguration werden CSNT-Software und NT-Domänenauthentifizierungsdienste angezeigt, die auf demselben Computer ausgeführt werden. Diese Elemente können auf zwei verschiedenen Computern ausgeführt werden, wenn die Konfiguration dies erfordert.

Konfigurieren des VPN 3000-Konzentrators

Gruppenkonfiguration

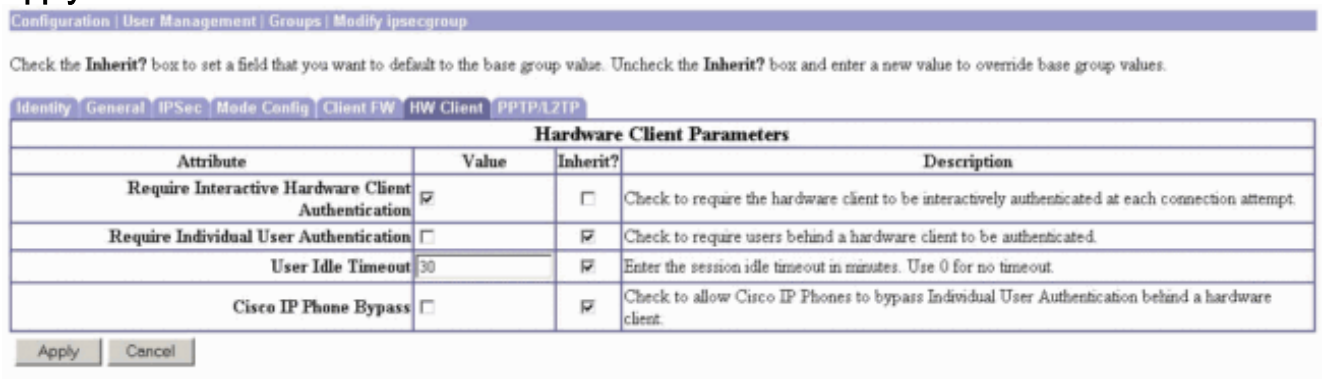
1. Um die Gruppe so zu konfigurieren, dass sie die NT-Kennwort-Ablaufparameter vom RADIUS-Server akzeptiert, gehen Sie zu **Konfiguration > Benutzerverwaltung > Gruppen**, wählen Sie Ihre Gruppe aus der Liste aus, und klicken Sie auf **Gruppe ändern**. Im folgenden Beispiel wird veranschaulicht, wie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

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



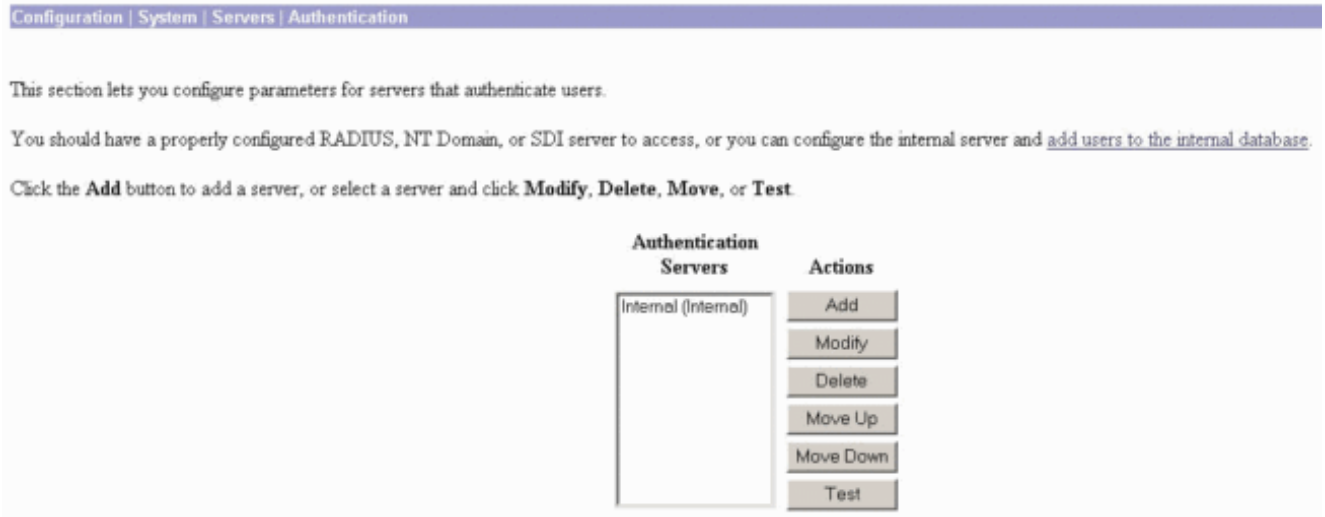
3. Wenn Sie diese Funktion auf den VPN 3002-Hardware-Clients aktivieren möchten, gehen Sie zur Registerkarte **HW Client**, stellen Sie sicher, dass **Interaktive Hardware-Client-Authentifizierung** aktiviert ist, und klicken Sie dann auf

Apply.



RADIUS-Konfiguration

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



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`**

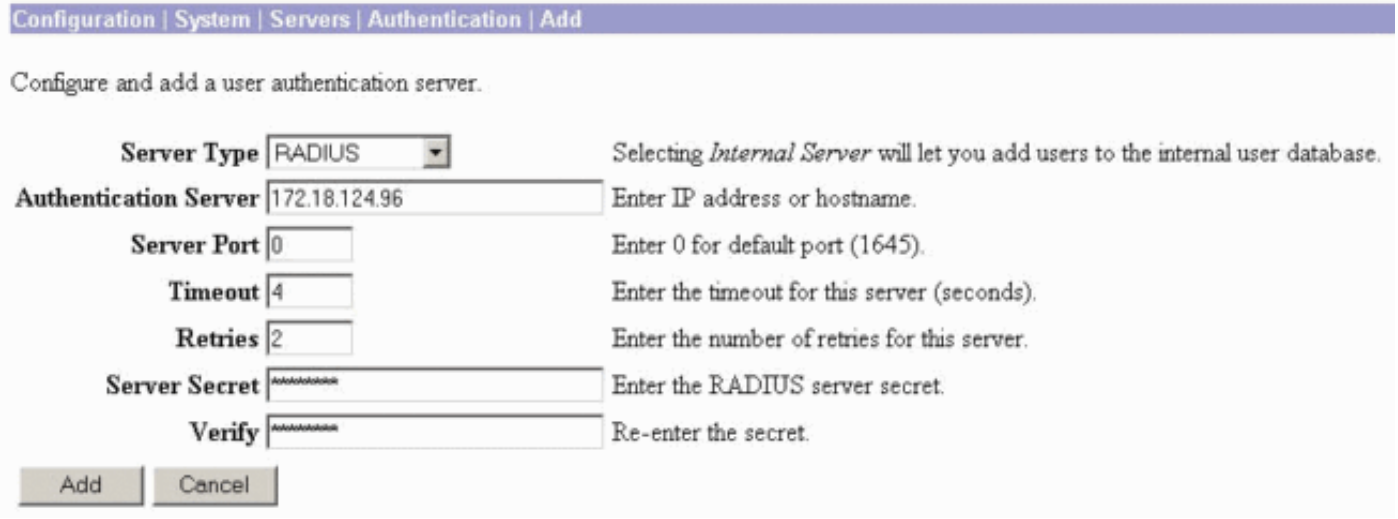
   `Server Port =` **`0`** `(for default of 1645)`

   `Timeout =` **`4`**

   `Reties =` **`2`**

   `Server Secret =` **`cisco123`**

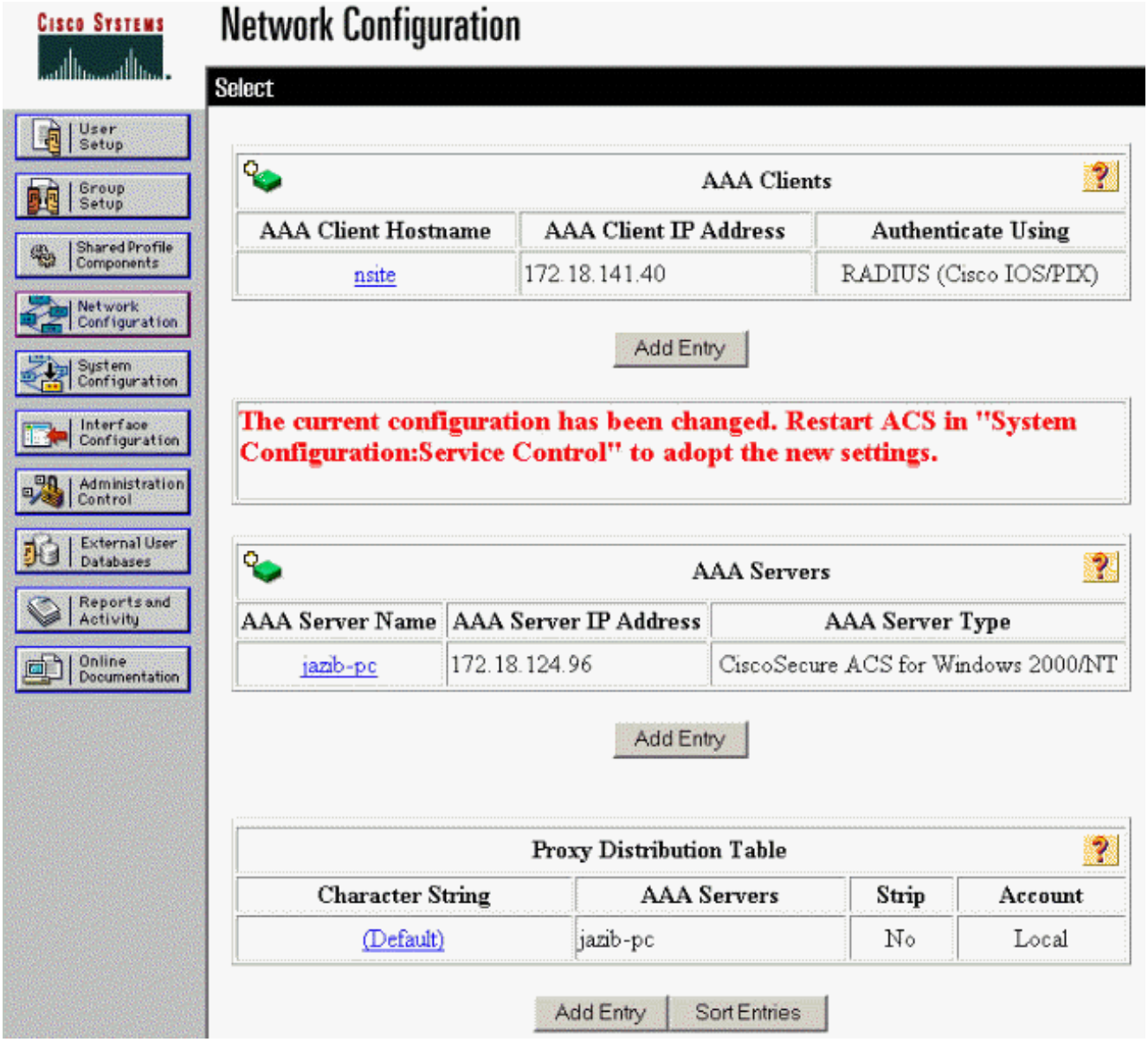
   `Verify:` **`cisco123`**



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 **Netzwerkkonfiguration**. Klicken Sie unter "AAA-Clients" auf **Eintrag hinzufügen**.

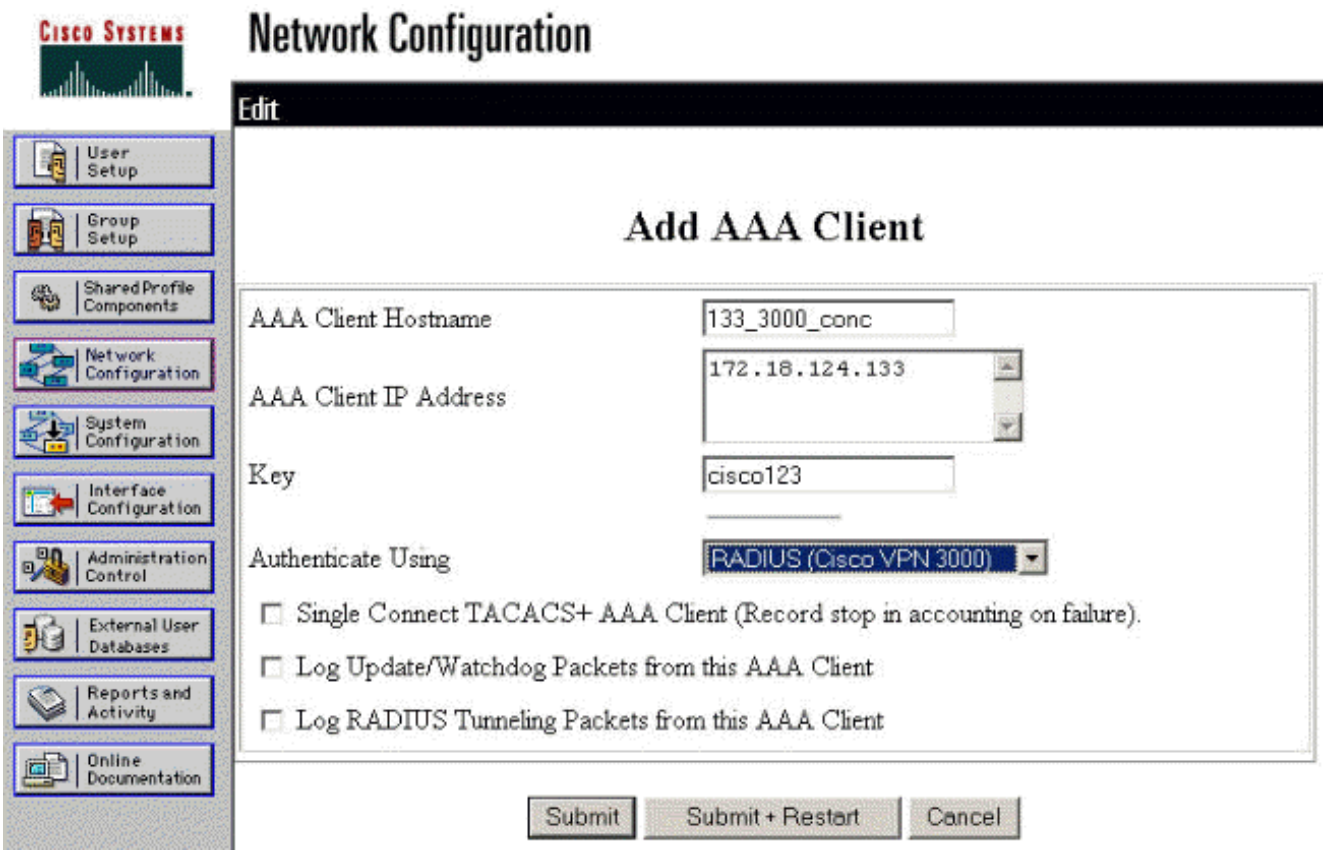


2. Geben Sie im Bildschirm "Add AAA Client" (AAA-Client hinzufügen) die entsprechenden Werte ein, um den Konzentrator als RADIUS-Client hinzuzufügen, und klicken Sie dann auf **Senden + Neu starten**.Im folgenden Beispiel werden die folgenden Werte verwendet.
   AAA Client Hostname = **133_3000_conc**

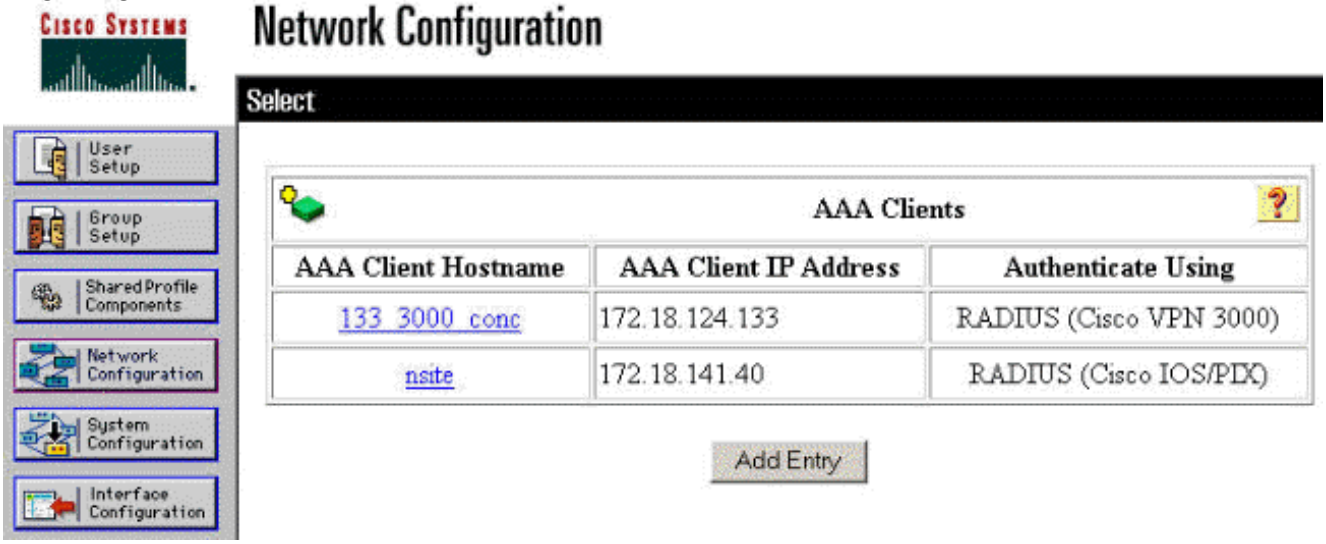
   AAA Client IP Address = **172.18.124.133**

   Key = **cisco123**

   Authenticate using = **RADIUS (Cisco VPN 3000)**

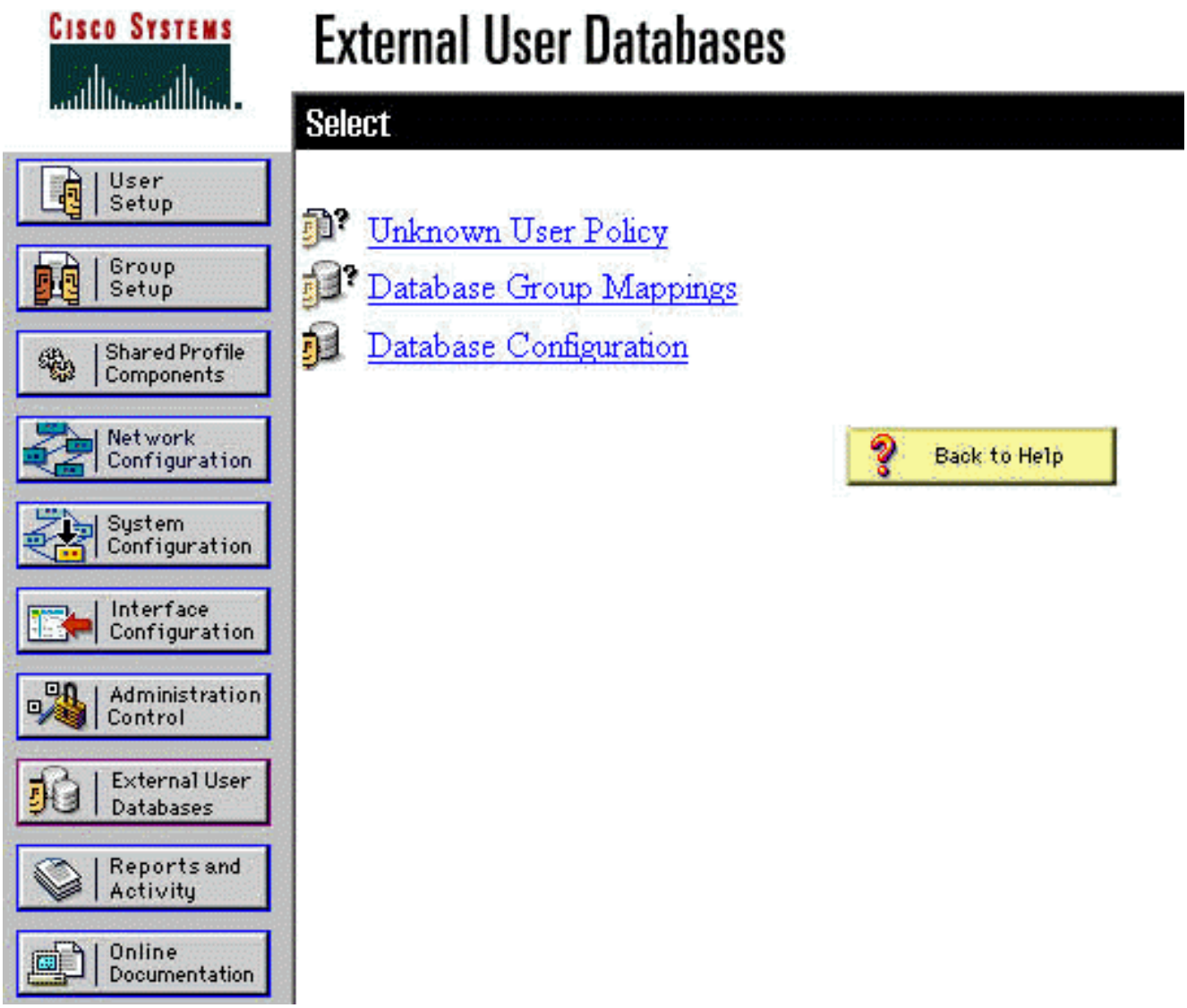


Ein Eintrag für Ihren 3000 Konzentrator wird im Abschnitt "**AAA Clients**" angezeigt.

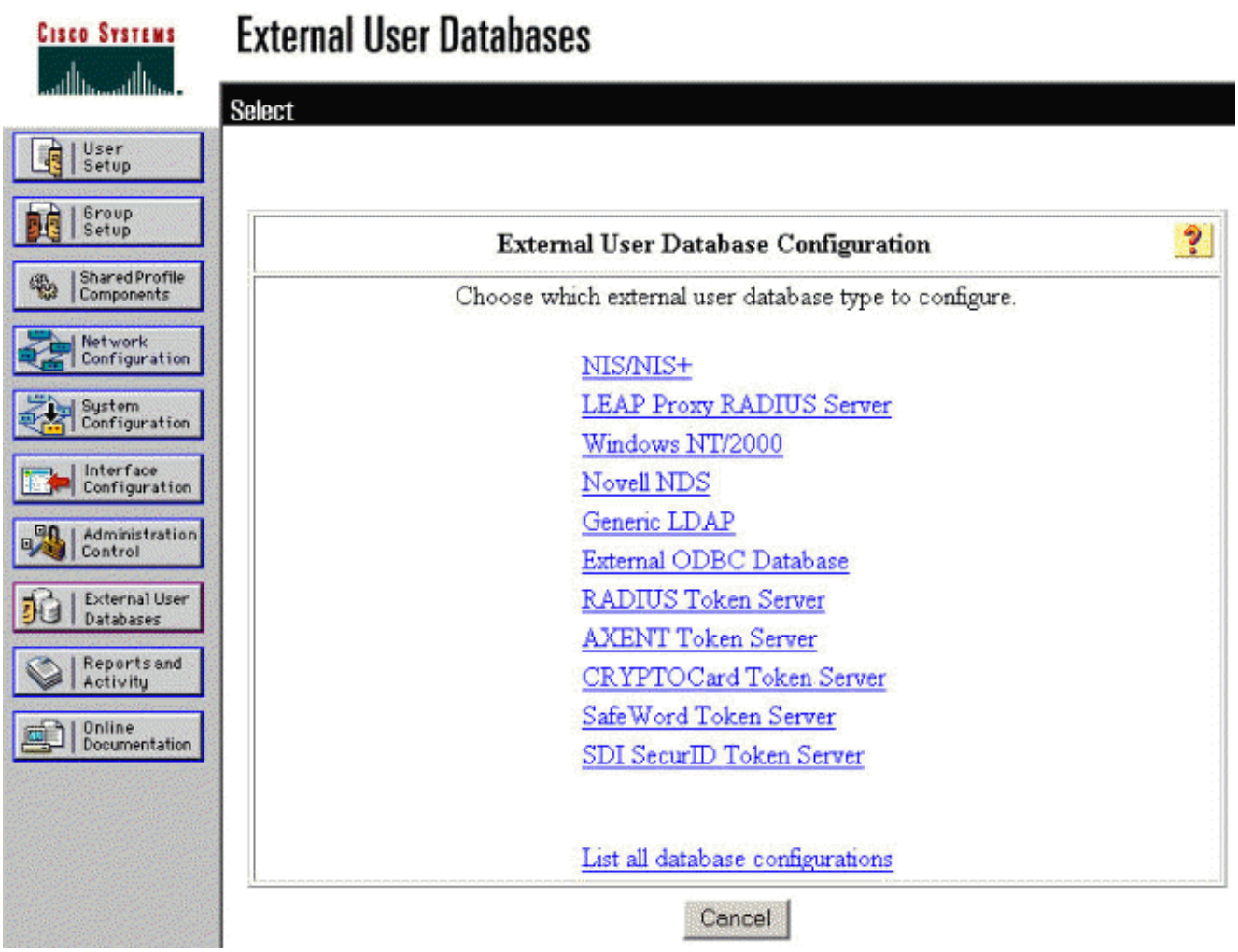


Konfigurieren der unbekannten Benutzerrichtlinie für die NT-Domänenauthentifizierung

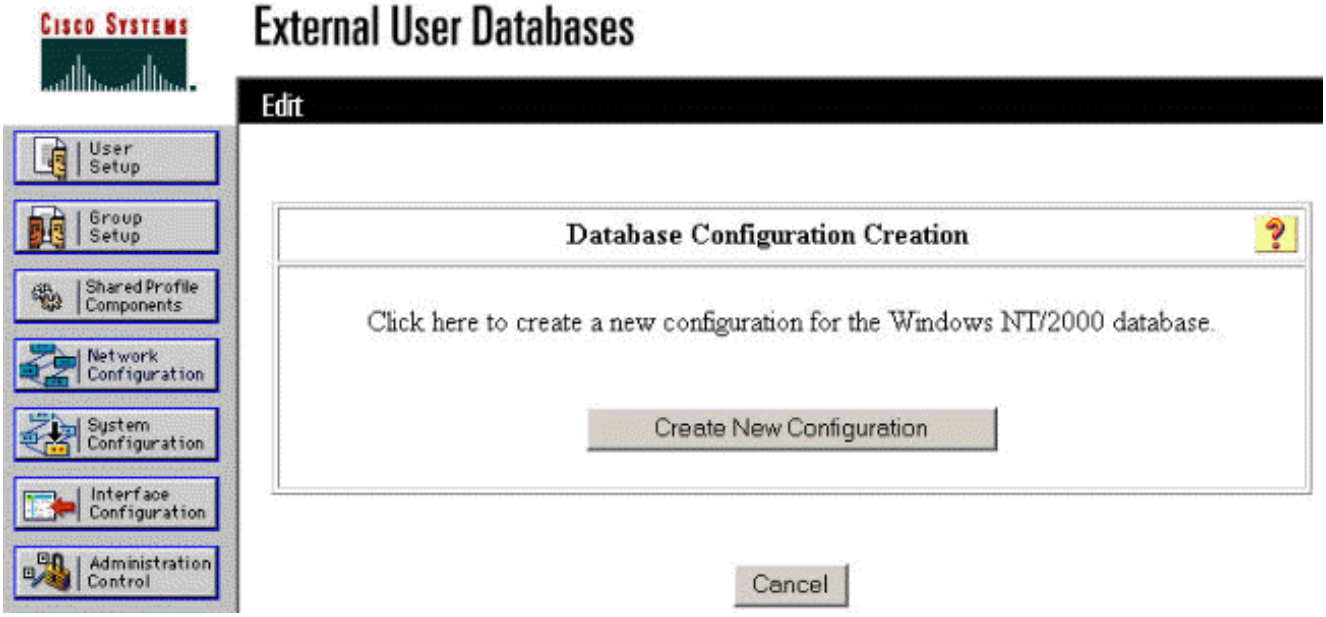
1. Um die Benutzerauthentifizierung auf dem RADIUS-Server als Teil der Richtlinie für unbekannte Benutzer zu konfigurieren, klicken Sie im linken Bereich auf **Externe Benutzerdatenbank** und dann auf den Link für **Datenbankkonfiguration**.



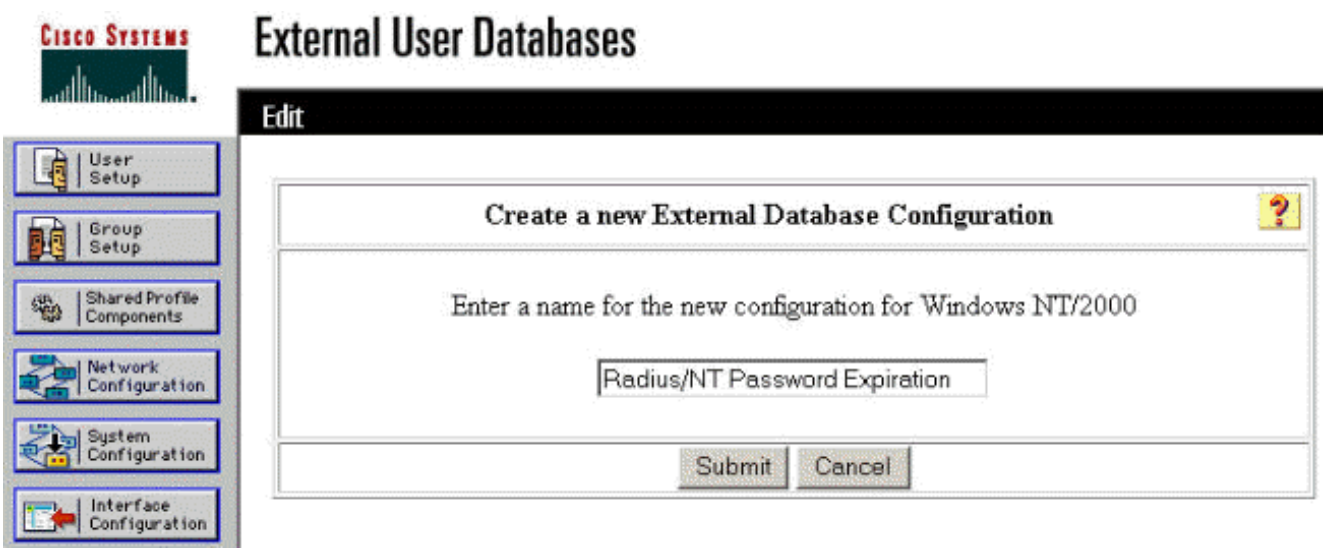
2. Klicken Sie unter "Konfiguration der externen Benutzerdatenbank" auf **Windows NT/2000**.



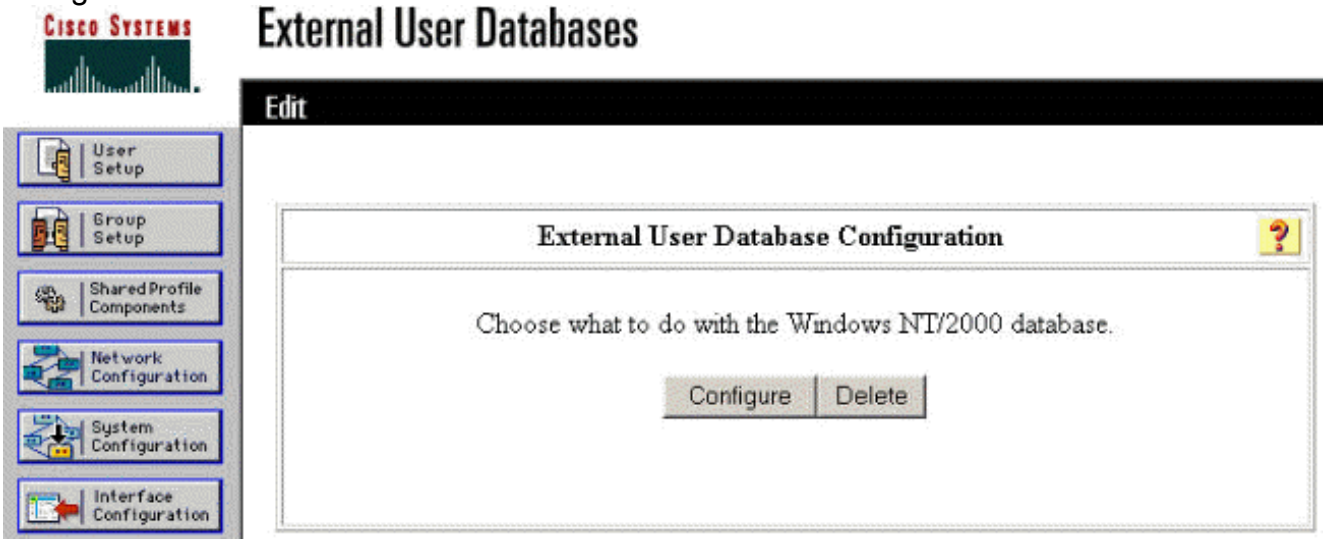
3. Klicken Sie im Bildschirm "Database Configuration Creation" auf **Create New Configuration**.



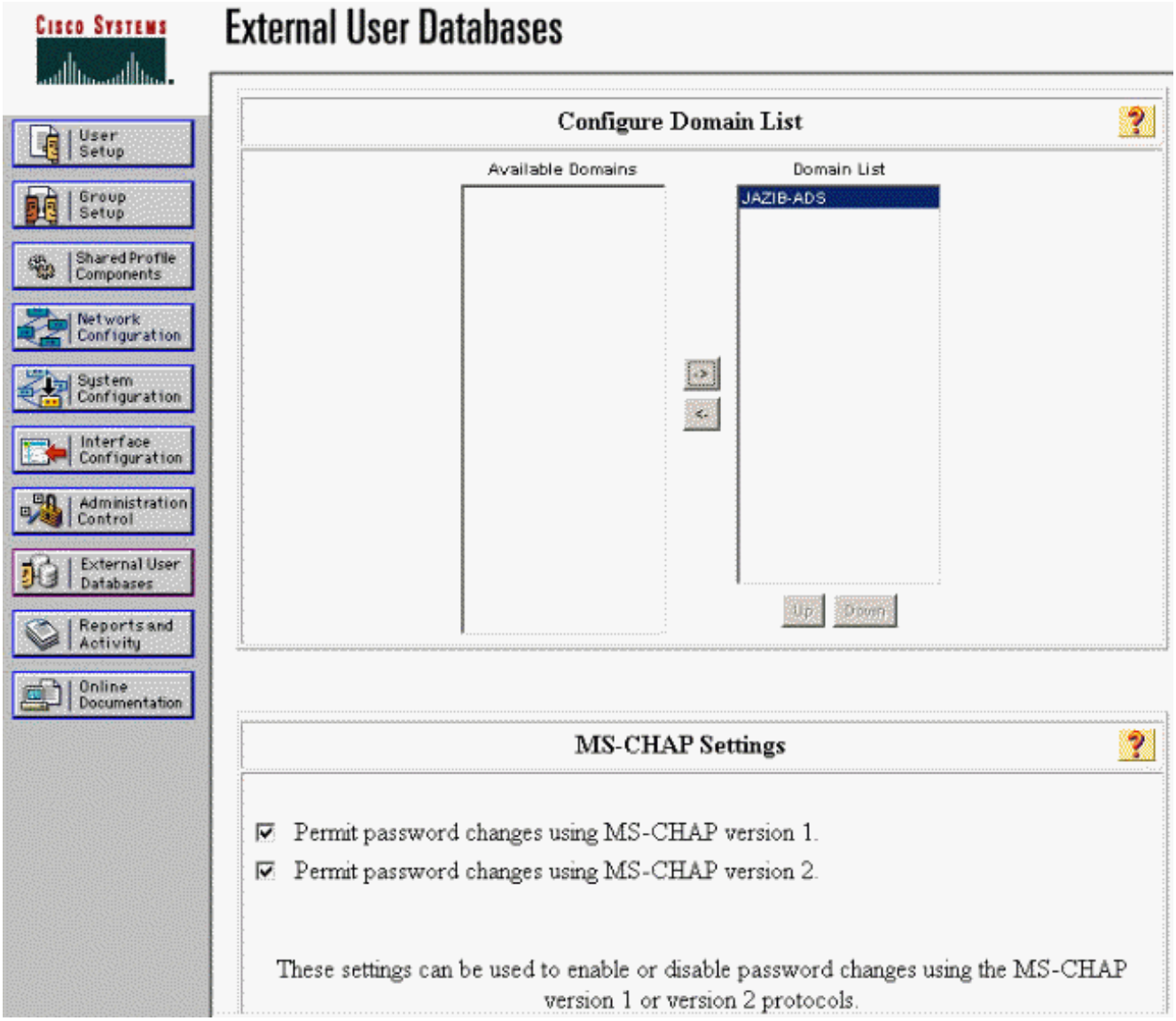
4. Geben Sie bei Aufforderung einen Namen für die NT/2000-Authentifizierung ein, und klicken Sie auf **Senden**. Im folgenden Beispiel wird der Name "Radius/NT Password Expiration" angezeigt.



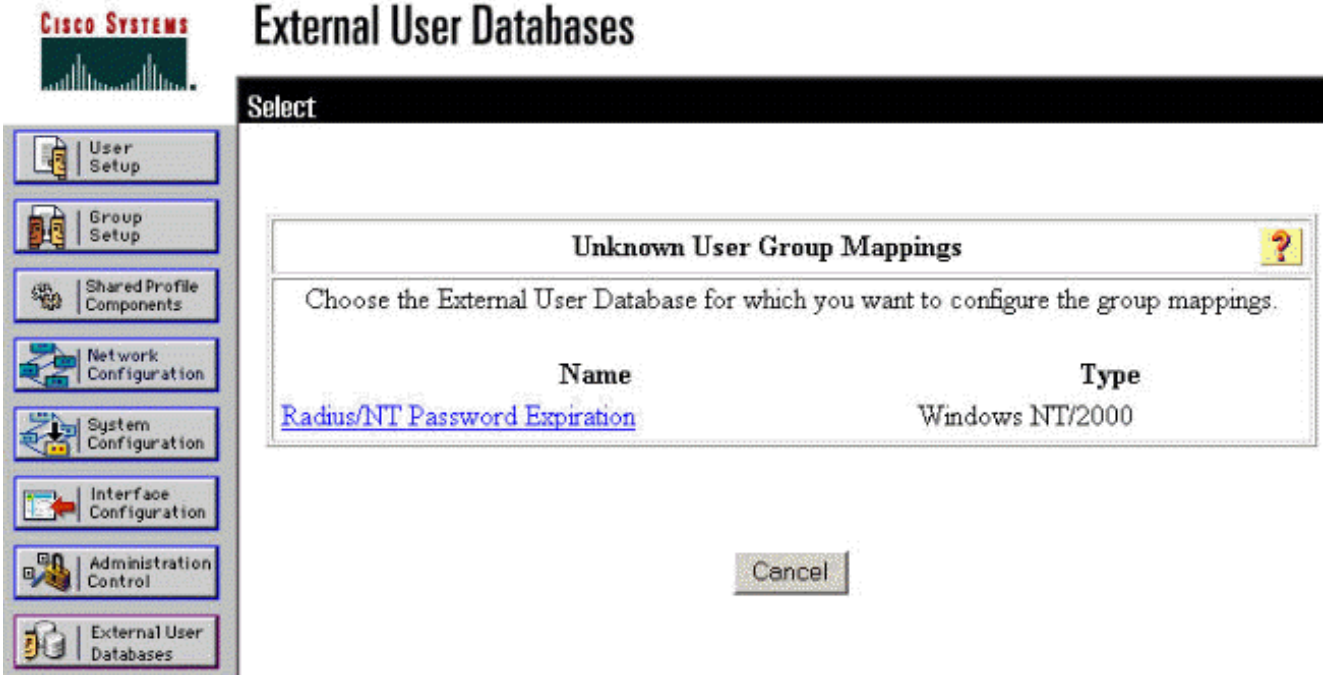
5. Klicken Sie auf **Konfigurieren**, um den Domänennamen für die Benutzerauthentifizierung zu konfigurieren.



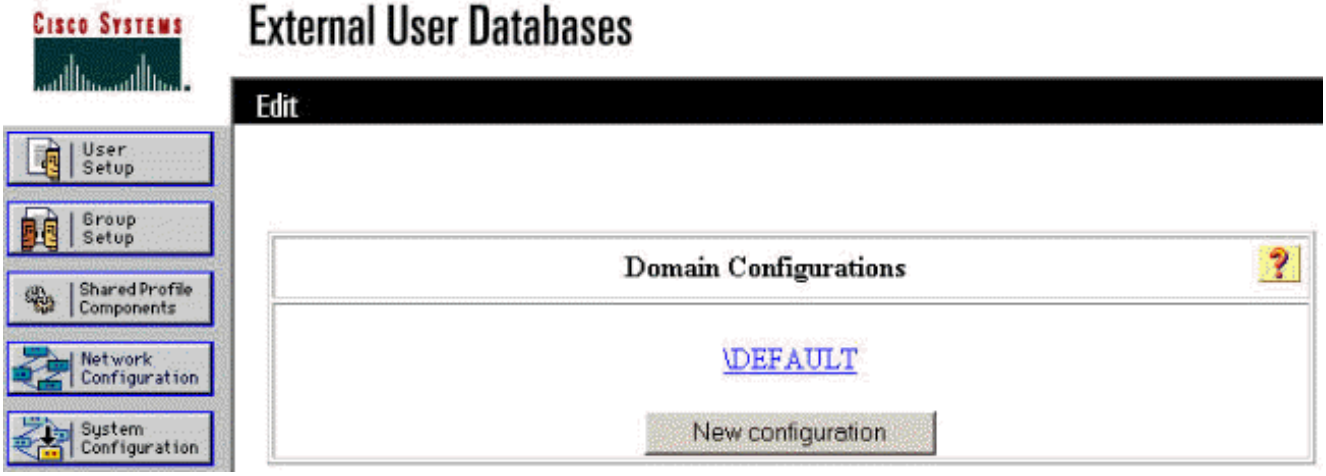
6. Wählen Sie Ihre NT-Domäne aus der Liste "Verfügbare Domänen" aus, und klicken Sie dann auf den Pfeil nach rechts, um sie der "Domänenliste" hinzuzufügen. Stellen Sie unter "MS-CHAP-Einstellungen" sicher, dass die Optionen für **Kennwortänderungen mit MS-CHAP Version 1** und **Version 2** ausgewählt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



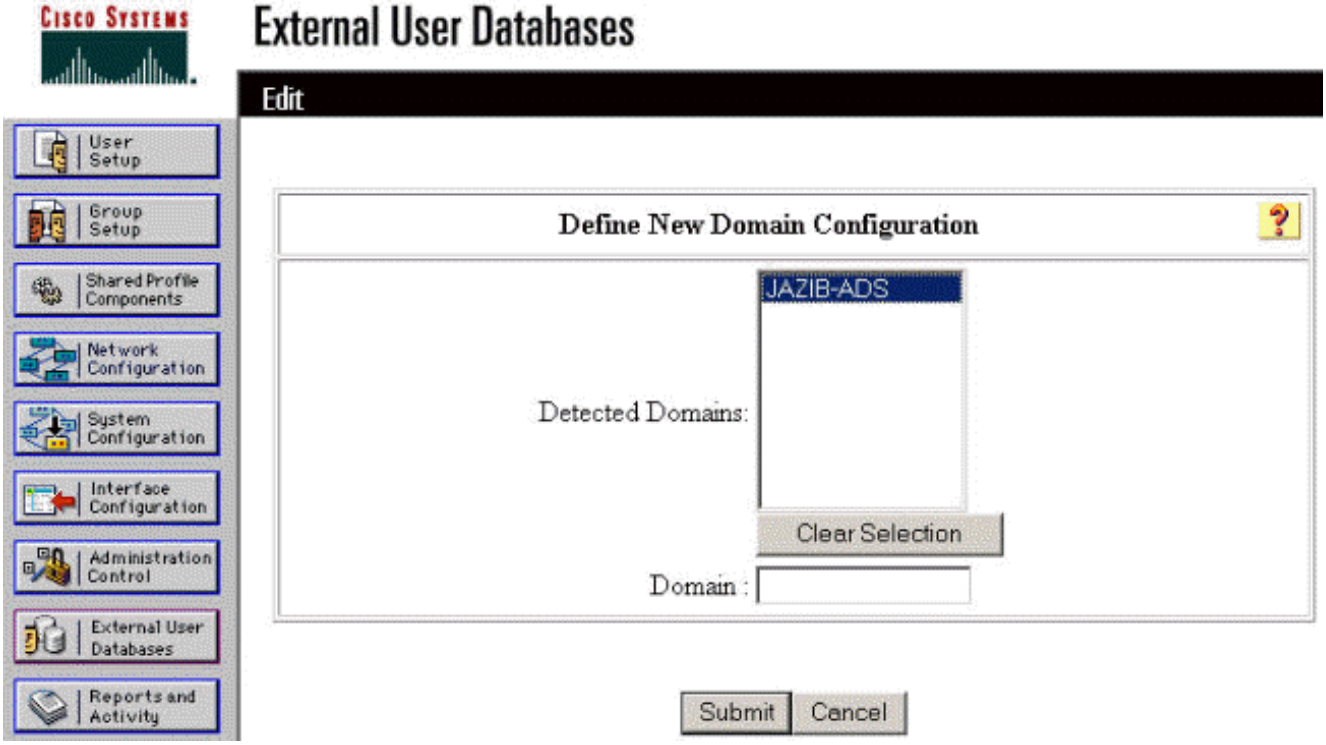
7. Klicken Sie im linken Bereich auf **Externe Benutzerdatenbank** und dann auf den Link für **Datenbankgruppenzuordnungen** (siehe Beispiel). Es sollte ein Eintrag für Ihre zuvor konfigurierte externe Datenbank angezeigt werden. Das Beispiel unten zeigt einen Eintrag für "Radius/NT Password Expiration",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



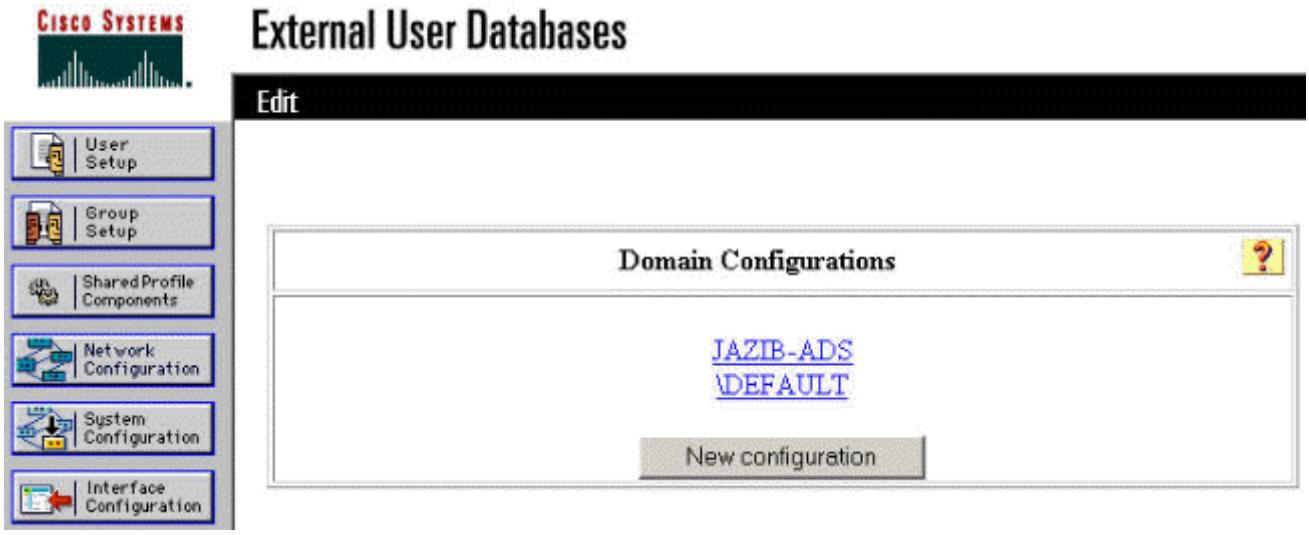
8. Klicken Sie im Bildschirm "Domänenkonfigurationen" auf **Neue Konfiguration**, um die Domänenkonfigurationen
hinzuzufügen.



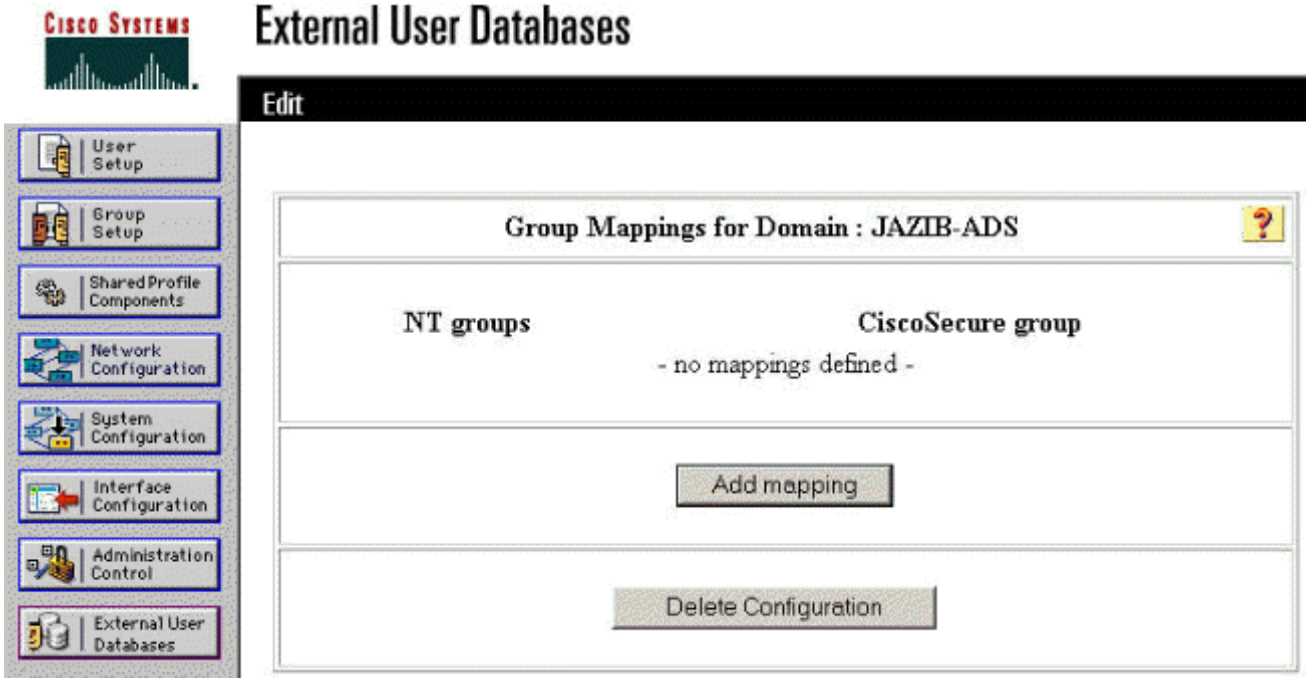
9. Wählen Sie Ihre Domäne aus der Liste "Erkannte Domänen" aus und klicken Sie auf **Senden**. Das nachfolgende Beispiel zeigt eine Domäne mit dem Namen "JAZIB-ADS".



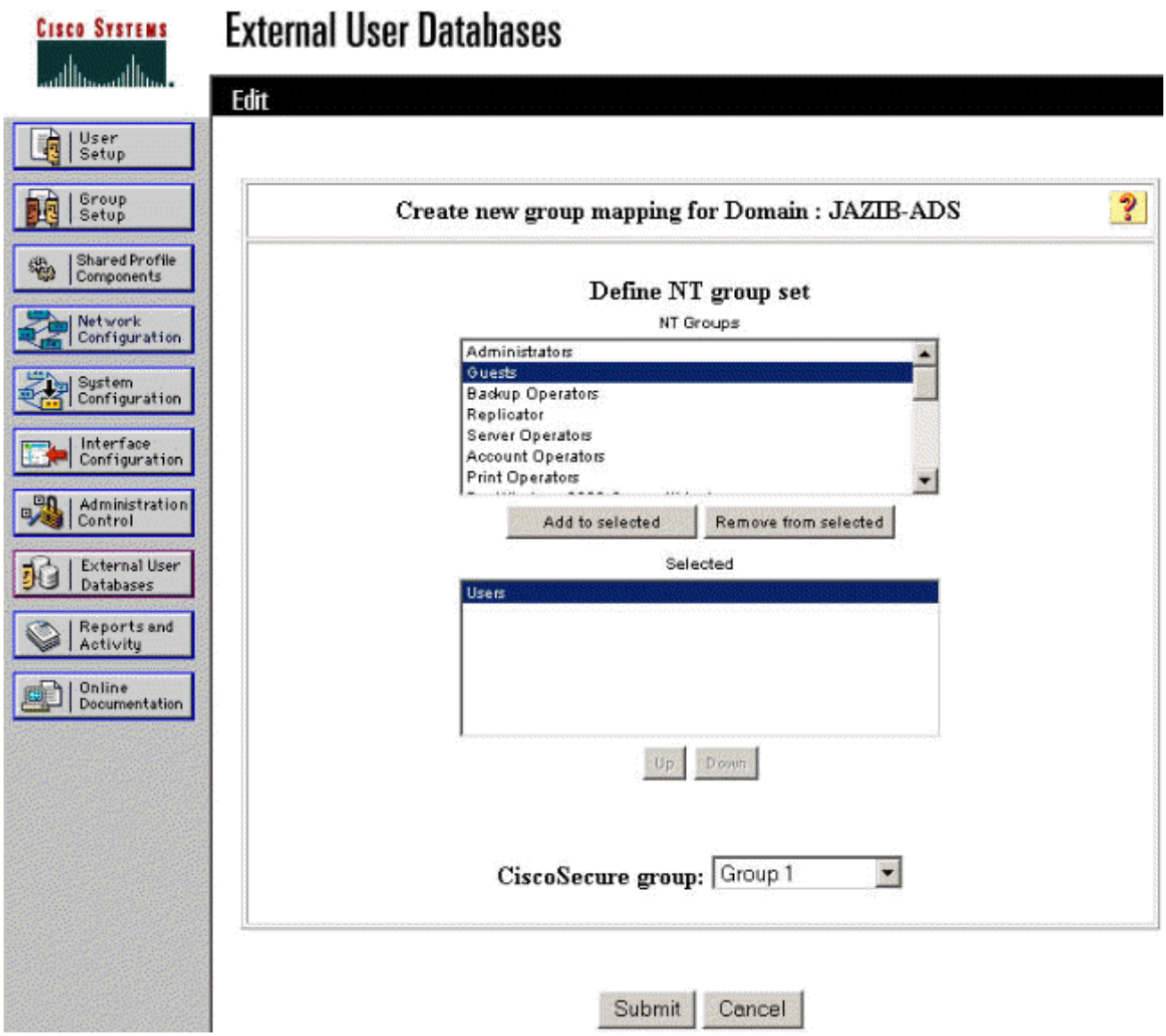
10. Klicken Sie auf Ihren Domänennamen, um die Gruppenzuordnungen zu konfigurieren. Dieses Beispiel zeigt die Domäne "JAZIB-ADS".



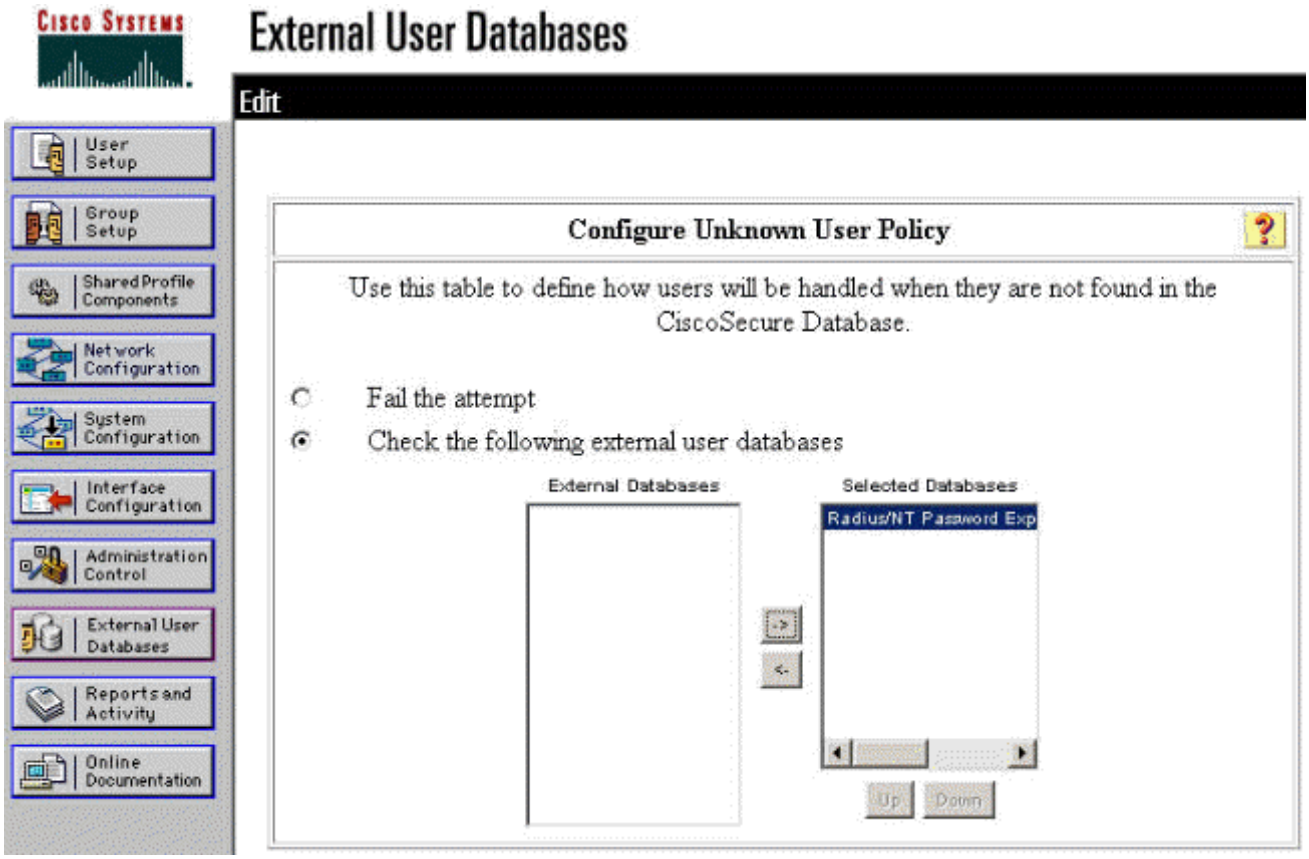
11. Klicken Sie auf **Zuordnung hinzufügen**, um die Gruppenzuordnungen zu definieren.



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.



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.

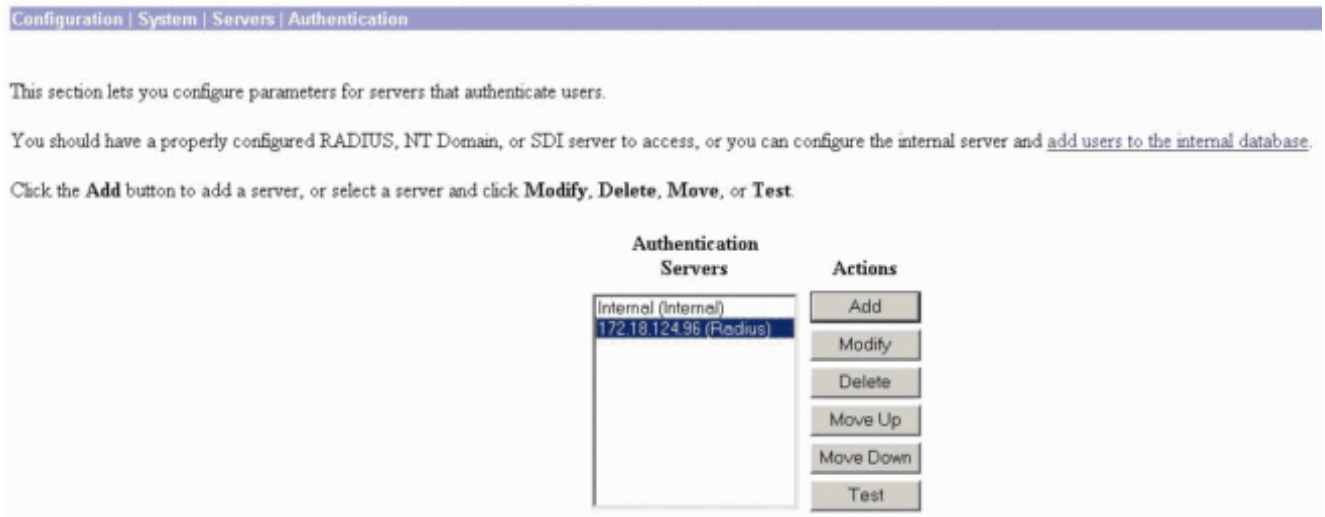


Testen der NT/RADIUS-Kennwortablauffunktion

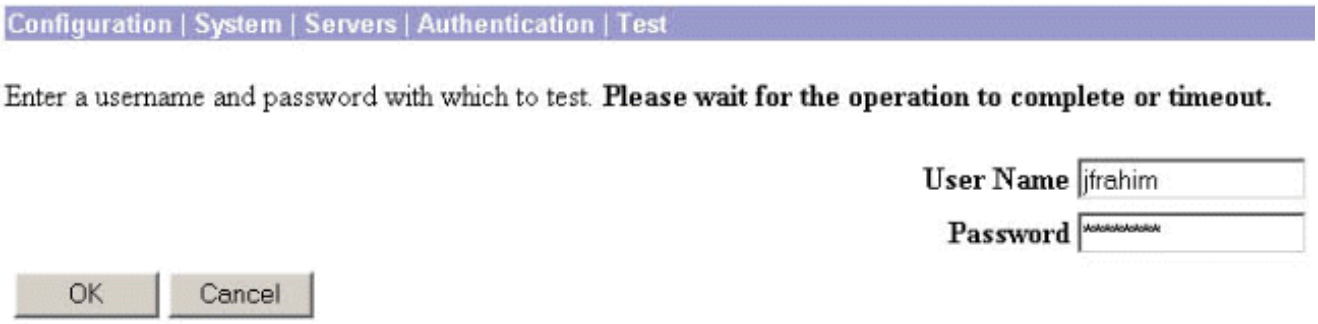
Der Konzentrator bietet eine Funktion zum Testen der RADIUS-Authentifizierung. Um diese Funktion ordnungsgemäß zu testen, sollten Sie diese Schritte sorgfältig durchführen.

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-Domänennamen und Ihr Kennwort ein, und klicken Sie dann auf **OK**. Das nachfolgende Beispiel zeigt den Benutzernamen "jfrahim", der auf dem NT-Domänenserver mit dem Kennwort "cisco123" konfiguriert ist.

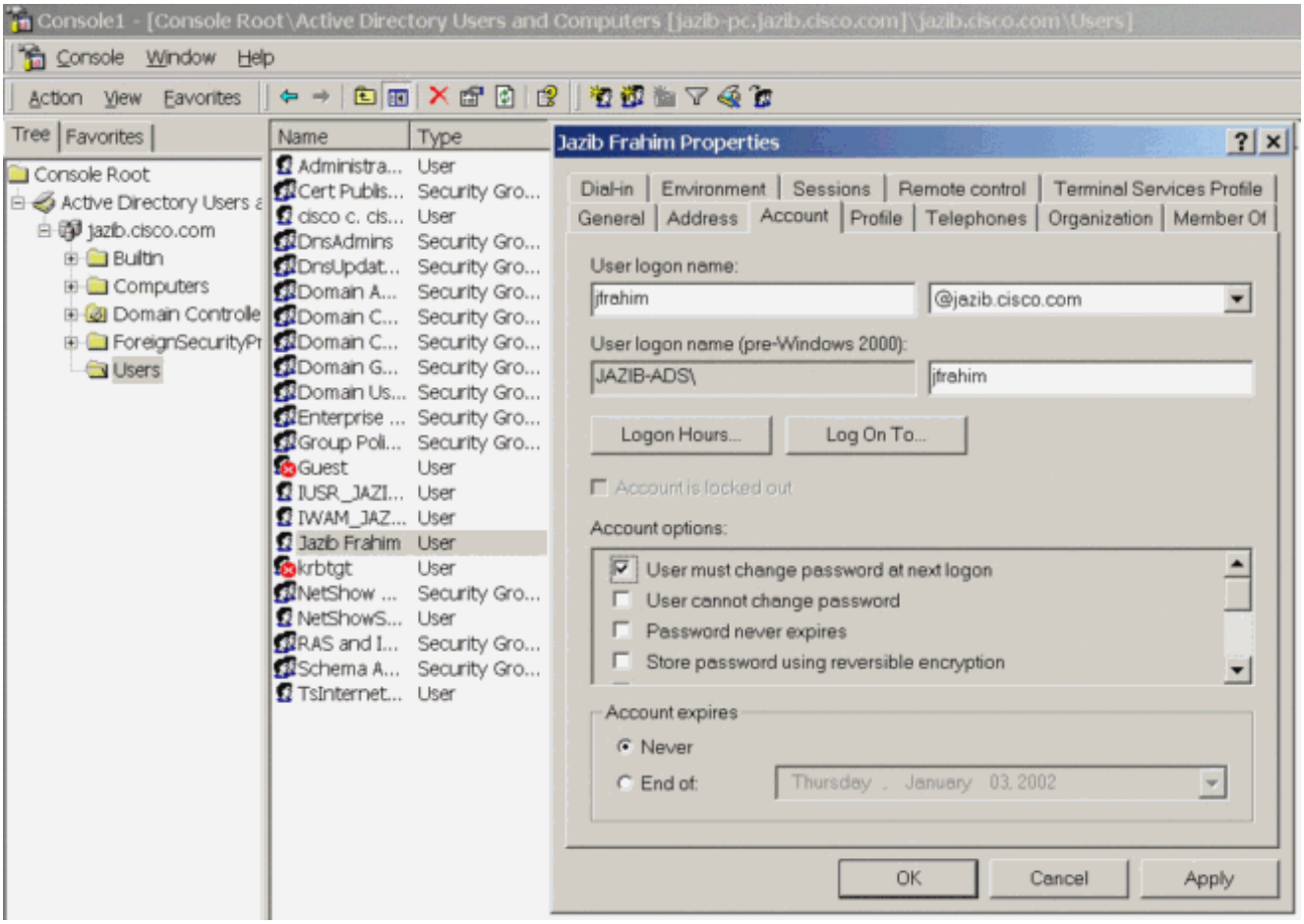


3. Wenn Ihre Authentifizierung ordnungsgemäß eingerichtet ist, erhalten Sie die Meldung "Authentication Successful" (Authentifizierung

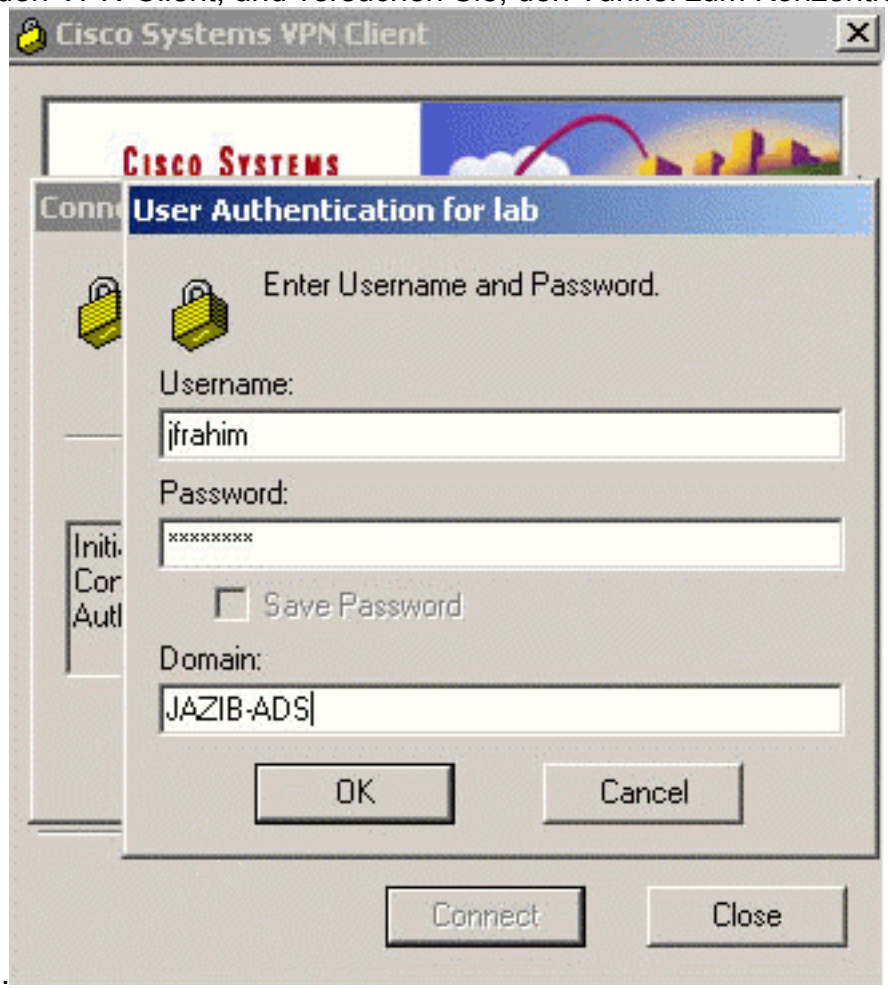
erfolgreich). Wenn Sie eine andere Meldung als die oben abgebildete erhalten, liegt ein Konfigurations- oder Verbindungsproblem vor. Wiederholen Sie die in diesem Dokument beschriebenen Konfigurations- und Testschritte, um sicherzustellen, dass alle Einstellungen ordnungsgemäß vorgenommen wurden. Überprüfen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



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)