

Configurare i Cisco VPN serie 3000 concentrator per supportare la funzione di scadenza password di NT con il server RADIUS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Esempio di rete](#)

[Configurazione di VPN 3000 Concentrator](#)

[Configurazione gruppo](#)

[Configurazione RADIUS](#)

[Configurazione di Cisco Secure NT RADIUS Server](#)

[Configurazione di una voce per il concentratore VPN 3000](#)

[Configurazione del criterio utente sconosciuto per l'autenticazione del dominio NT](#)

[Test della funzionalità di scadenza delle password NT/RADIUS](#)

[Test di autenticazione RADIUS](#)

[Autenticazione del dominio NT effettiva tramite proxy RADIUS per verificare la funzionalità di scadenza password](#)

[Informazioni correlate](#)

Introduzione

In questo documento vengono fornite istruzioni dettagliate su come configurare i Cisco VPN serie 3000 concentrator in modo da supportare la funzione di scadenza della password NT con il server RADIUS.

Per ulteriori informazioni sullo stesso scenario con il server di autenticazione Internet (IAS, Internet Authentication Server), fare riferimento alla [VPN 3000 RADIUS con funzionalità di scadenza](#) che [utilizza](#) il server di autenticazione Internet (Internet Authentication Server).

Prerequisiti

Requisiti

- Se il server RADIUS e il server Autenticazione dominio NT si trovano su due computer distinti, accertarsi di aver stabilito la connettività IP tra i due computer.
- Accertarsi di aver stabilito la connettività IP tra il concentratore e il server RADIUS. Se il server RADIUS è rivolto verso l'interfaccia pubblica, non dimenticare di aprire la porta

RADIUS sul filtro pubblico.

- Accertarsi di poter connettersi al concentratore dal client VPN utilizzando il database degli utenti interni. Se non è configurata, consultare il documento sulla [configurazione di IPsec - Cisco 3000 VPN Client su VPN 3000 Concentrator](#).

Nota: non è possibile usare la funzione di scadenza password con client VPN Web o SSL.

Componenti usati

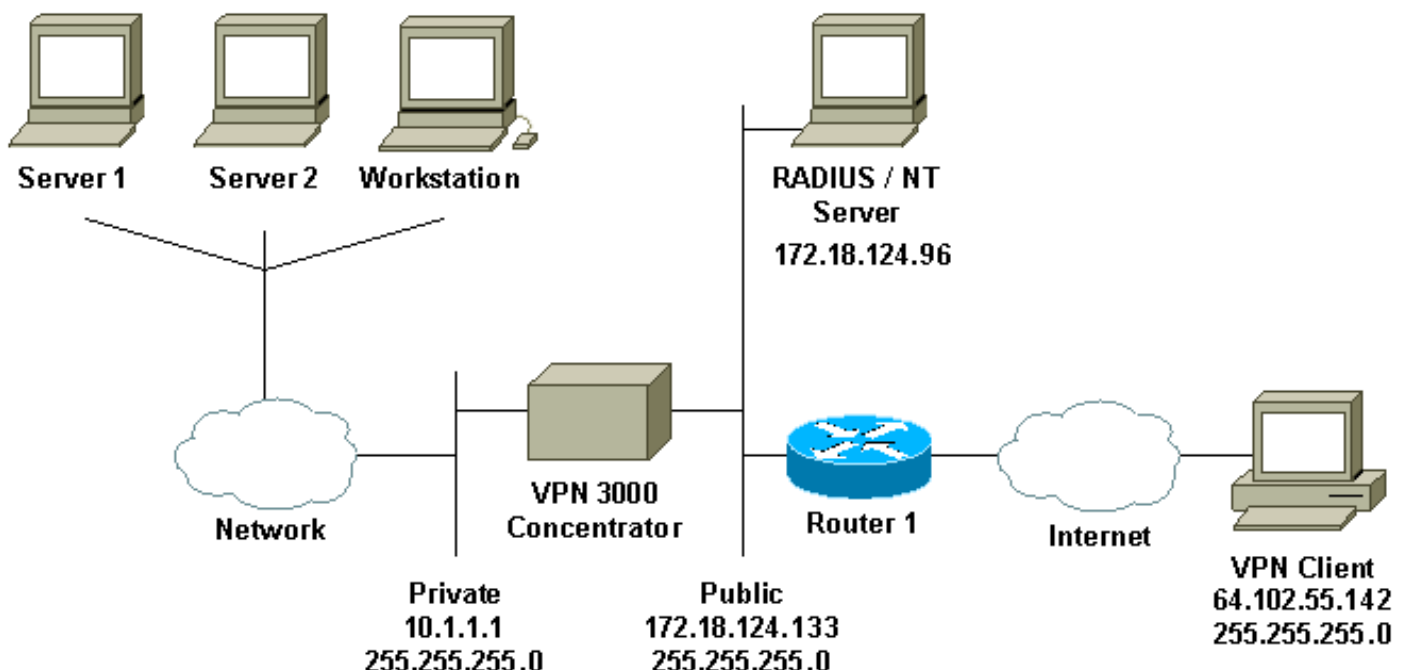
Questa configurazione è stata sviluppata e testata utilizzando le versioni software e hardware riportate di seguito.

- VPN 3000 Concentrator Software versione 4.7
- VPN Client release 3.5
- Cisco Secure for NT (CSNT) versione 3.0 Microsoft Windows 2000 Active Directory Server for User Authentication

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



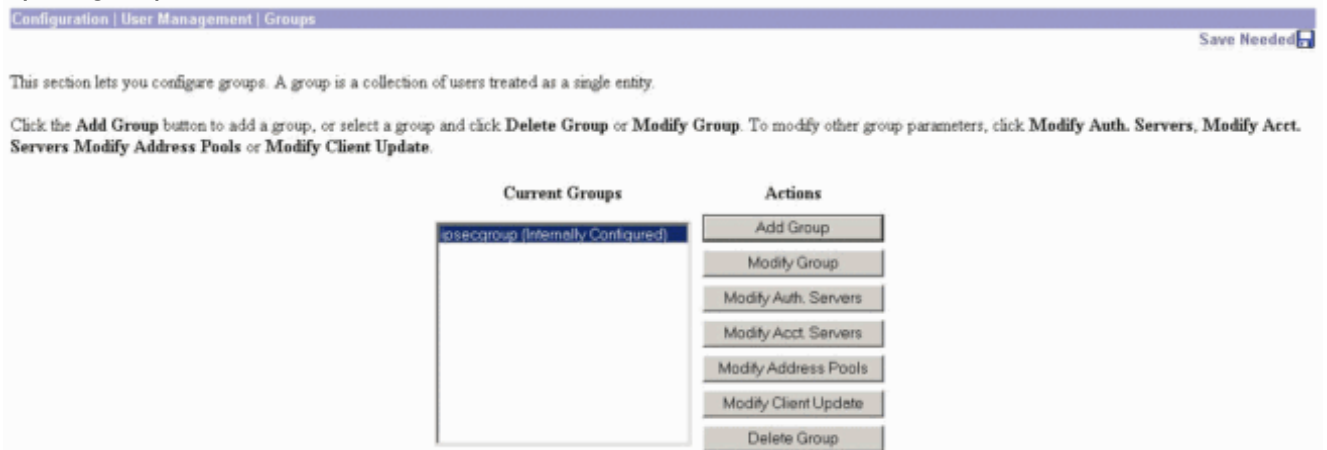
Note diagramma

1. Il server RADIUS in questa configurazione si trova nell'interfaccia pubblica. In questo caso, creare due regole nel filtro pubblico per consentire al traffico RADIUS di entrare e uscire dal concentratore.
2. Questa configurazione mostra il software CSNT e i servizi di autenticazione di dominio NT in esecuzione sullo stesso computer. Questi elementi possono essere eseguiti su due computer separati se richiesto dalla configurazione.

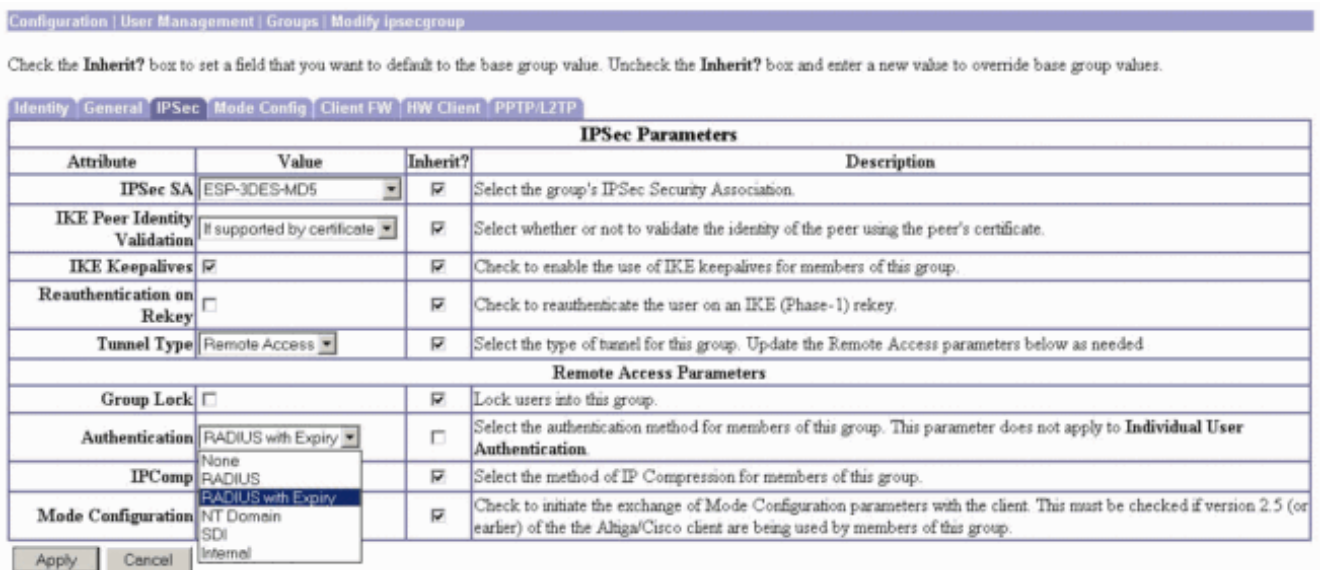
Configurazione di VPN 3000 Concentrator

Configurazione gruppo

1. Per configurare il gruppo in modo che accetti i parametri di scadenza password NT dal server RADIUS, andare a **Configurazione > Gestione utente > Gruppi**, selezionare il gruppo dall'elenco e fare clic su **Modifica gruppo**. Nell'esempio seguente viene illustrato come modificare un gruppo denominato "ipsecgroup".



2. Andare alla scheda **IPSec** e verificare che per l'attributo **Authentication** sia selezionato **RADIUS con scadenza**.



3. Se si desidera abilitare questa funzionalità sui client hardware VPN 3002, passare alla scheda **Client hardware**, verificare che **Richiedi autenticazione client hardware interattivo** sia abilitato, quindi fare clic su **Applica**.

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

Configurazione RADIUS

1. Per configurare le impostazioni del server RADIUS sul concentratore, selezionare Configurazione > Sistema > Server > Autenticazione > **Aggiungi**.

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. Nella schermata **Aggiungi**, immettere i valori che corrispondono al server RADIUS e fare clic su **Aggiungi**. Nell'esempio seguente vengono utilizzati i valori seguenti.

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"/>		

[Configurazione di Cisco Secure NT RADIUS Server](#)

[Configurazione di una voce per il concentratore VPN 3000](#)

1. Accedere a CSNT e fare clic su **Configurazione di rete** nel pannello sinistro. In "Client AAA", fare clic su **Add Entry** (Aggiungi voce).

CISCO SYSTEMS Network Configuration

Select

AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
nsite	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. Nella schermata "Add AAA Client" (Aggiungi client AAA), immettere i valori appropriati per aggiungere il concentratore come client RADIUS, quindi fare clic su **Submit (Invia) + Riavvia (Riavvia)**. Nell'esempio seguente vengono utilizzati i valori seguenti.

AAA Client Hostname = **133_3000_conc**

AAA Client IP Address = **172.18.124.133**

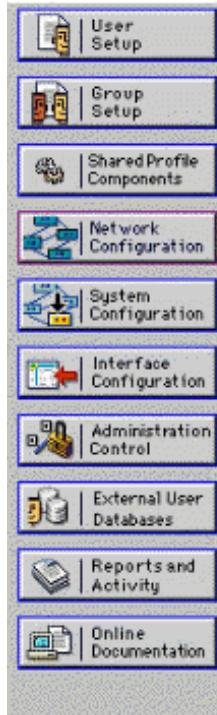
Key = **cisco123**

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	

Nella sezione "Client AAA" verrà visualizzata una voce relativa al concentratore 3000.



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)

[Configurazione del criterio utente sconosciuto per l'autenticazione del dominio NT](#)

1. Per configurare l'autenticazione utente sul server RADIUS come parte del criterio utente sconosciuto, fare clic su **Database utente esterno** nel riquadro sinistro, quindi fare clic sul collegamento **Configurazione database**.




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

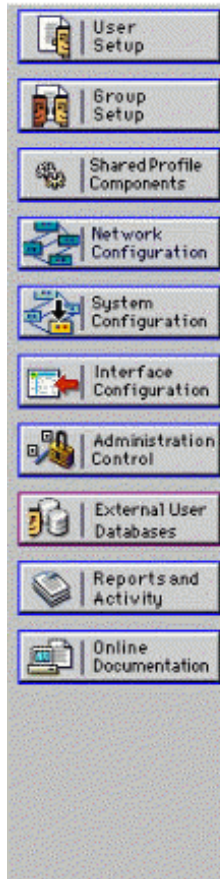
- [Unknown User Policy](#)
- [Database Group Mappings](#)
- [Database Configuration](#)

 [Back to Help](#)

2. In "Configurazione database utenti esterni", fare clic su **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](#)

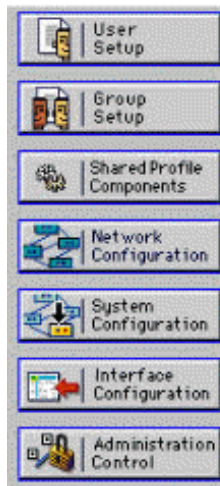
[List all database configurations](#)

Cancel

3. Nella schermata "Creazione della configurazione del database", fare clic su **Crea nuova configurazione**.



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. Quando richiesto, digitare un nome per l'autenticazione NT/2000 e fare clic su **Invia**.
Nell'esempio seguente viene illustrato il nome "Radius/NT Password Expiration" (Scadenza password Radius/NT).



External User Databases



Edit

Create a new External Database Configuration 

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


5. Fare clic su **Configura** per configurare il nome di dominio per l'autenticazione utente.



External User Databases




Edit

External User Database Configuration 

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

6. Selezionare il proprio dominio NT da "Domini disponibili", quindi fare clic sul pulsante freccia destra per aggiungerlo all'elenco dei domini. In "MS-CHAP Settings" (Impostazioni MS-CHAP) verificare che le opzioni per **Permit password changes using MS-CHAP version 1 and version 2** (Consenti modifiche password utilizzando MS-CHAP versione 1 e versione 2) siano selezionate. Al termine, fare clic su **Submit** (Invia).



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. Fare clic su **Database utente esterno** nel pannello a sinistra, quindi fare clic sul collegamento per i **mapping dei gruppi di database** (come mostrato nell'[esempio](#)). Verrà visualizzata una voce per il database esterno configurato in precedenza. L'esempio seguente mostra una voce per "Radius/NT Password Expiration", il database appena configurato.



External User Databases

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

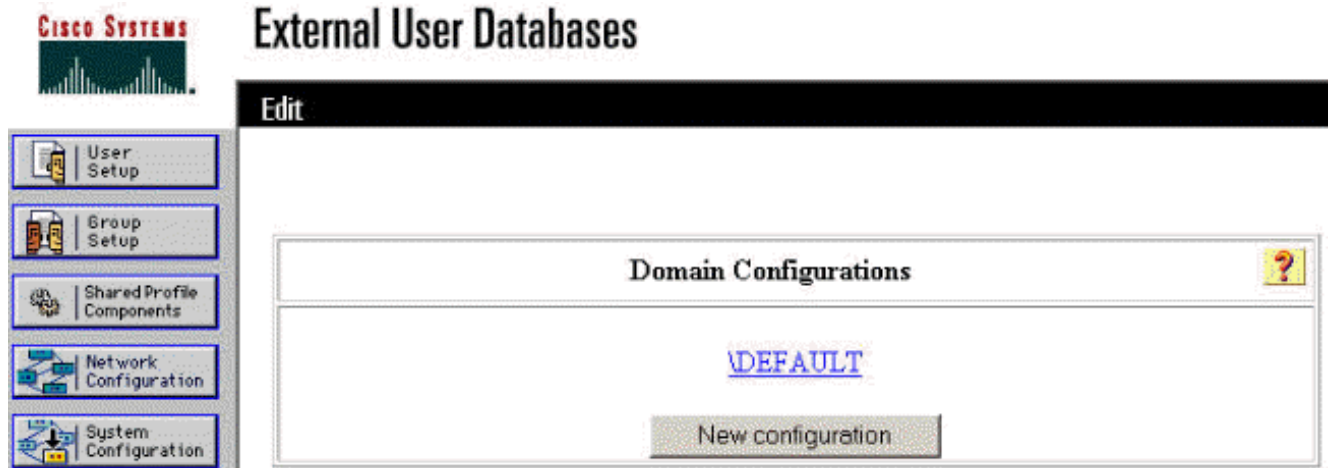
Select

Unknown User Group Mappings ?

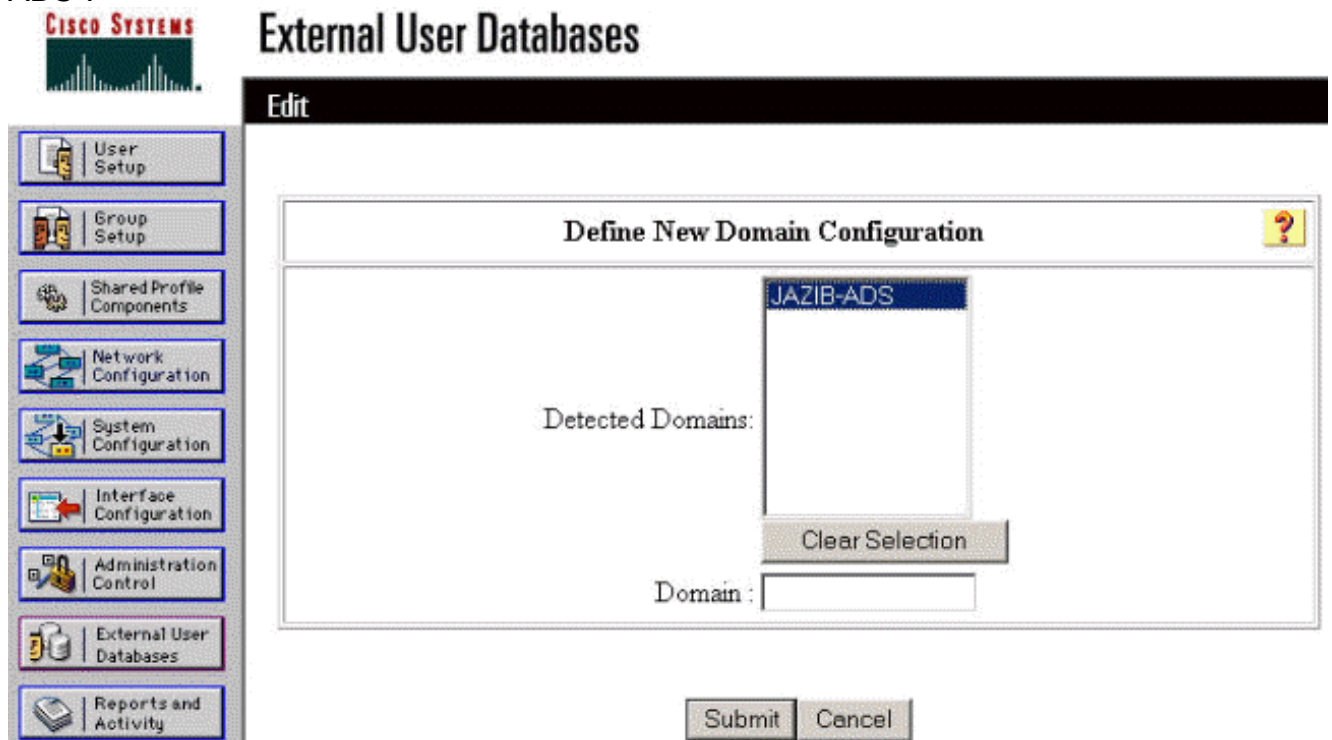
Choose the External User Database for which you want to configure the group mappings.

Name	Type
Radius/NT Password Expiration	Windows NT/2000

8. Nella schermata "Domain Configurations" (Configurazioni dominio), fare clic su **New configuration** (Nuova configurazione) per aggiungere le configurazioni di dominio.



9. Selezionare il proprio dominio dall'elenco "Domini rilevati" e fare clic su **Invia**. Nell'esempio seguente viene illustrato un dominio denominato "JAZIB-ADS".




10. Fare clic sul nome di dominio per configurare i mapping dei gruppi. Nell'esempio viene mostrato il dominio "JAZIB-ADS".



External User Databases

Edit

Domain Configurations 

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


New configuration

11. Fare clic su **Aggiungi mapping** per definire i mapping dei gruppi.



External User Databases

Edit

Group Mappings for Domain : JAZIB-ADS 

NT groups	CiscoSecure group
- no mappings defined -	

Add mapping

Delete Configuration

12. Nella schermata "Crea nuova mappatura gruppo", mappare il gruppo sul dominio NT a un gruppo sul server RADIUS CSNT, quindi fare clic su **Invia**. Nell'esempio seguente il gruppo NT "Users" viene mappato al gruppo RADIUS "Group 1".

Edit

Create new group mapping for Domain : JAZIB-ADS ?

Define NT group set

NT Groups

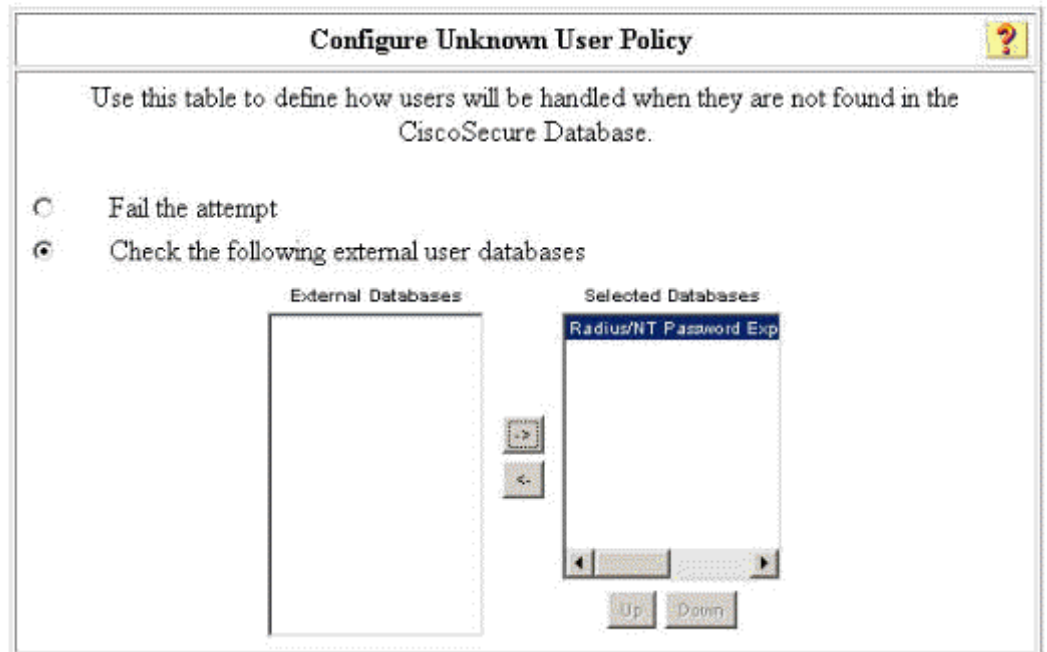
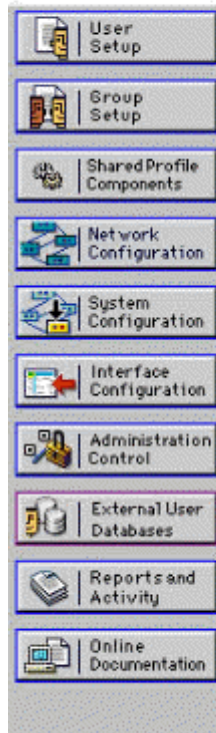
Administrators
Guests
 Backup Operators
 Replicator
 Server Operators
 Account Operators
 Print Operators

Selected

Users

CiscoSecure group:

13. Fare clic su **Database utenti esterni** nel pannello a sinistra, quindi fare clic sul collegamento per **Criteri utente sconosciuti** (come illustrato in questo [esempio](#)). Assicurarsi che l'opzione **Controlla i seguenti database utenti esterni** sia selezionata. Fare clic sul pulsante freccia destra per spostare il database esterno configurato in precedenza dall'elenco "Database esterni" all'elenco "Database selezionati".



Test della funzionalità di scadenza delle password NT/RADIUS

Il concentratore offre una funzione per testare l'autenticazione RADIUS. Per verificare correttamente questa funzionalità, eseguire la procedura descritta di seguito.

Test di autenticazione RADIUS

1. Andare a **Configurazione > Sistema > Server > Autenticazione**. Selezionare il server RADIUS e fare clic su

Test.



2. Quando richiesto, digitare il nome utente e la password di dominio NT e quindi fare clic su **OK**. L'esempio seguente mostra il nome utente "jfracim" configurato sul server di dominio NT con "cisco123" come password.

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

User Name
Password

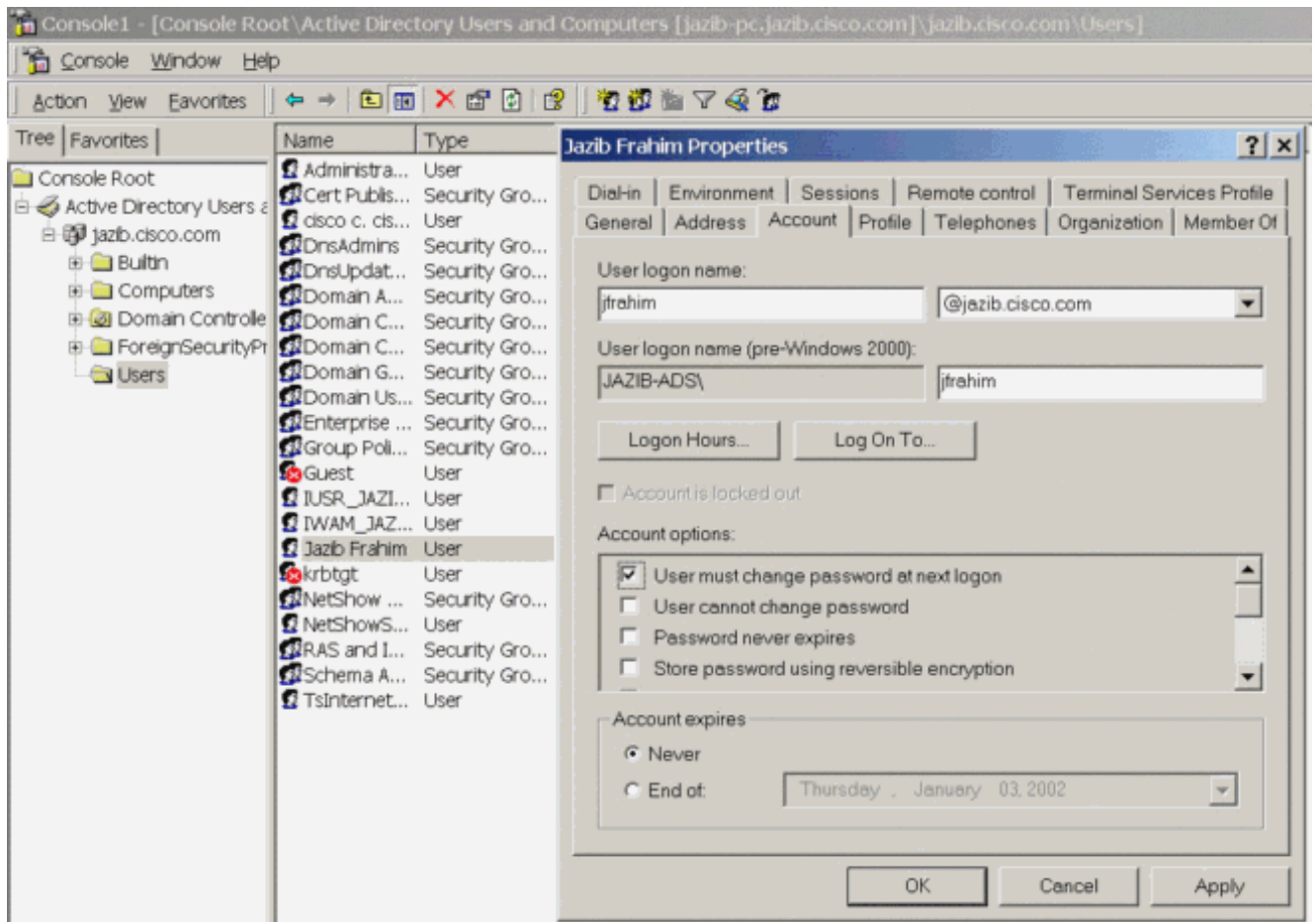
3. Se l'autenticazione è configurata correttamente, dovrebbe essere visualizzato il messaggio "Autenticazione



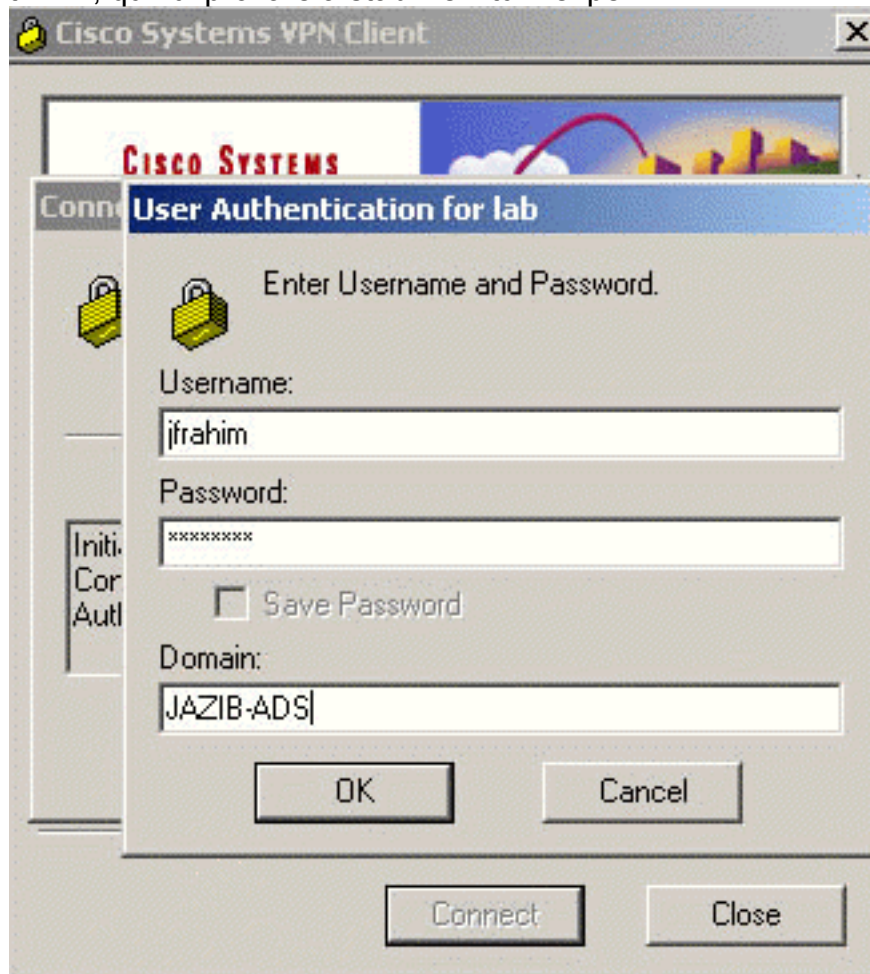
riuscita". Se si riceve un messaggio diverso da quello mostrato sopra, si è verificato un problema di configurazione o connessione. Ripetere i passaggi di configurazione e test descritti in questo documento per verificare che tutte le impostazioni siano state eseguite correttamente. Verificare inoltre la connettività IP tra i dispositivi.

[Autenticazione del dominio NT effettiva tramite proxy RADIUS per verificare la funzionalità di scadenza password](#)

1. Se l'utente è già definito nel server di dominio, modificare le proprietà in modo che all'utente venga richiesto di modificare la password al successivo accesso. Nella scheda Account della finestra di dialogo delle proprietà dell'utente, selezionare l'opzione **Cambiamento obbligatorio password all'accesso successivo**, quindi fare clic su **OK**.



2. Avviare il client VPN, quindi provare a stabilire il tunnel per il



concentratore.

3. Durante l'autenticazione utente, verrà richiesto di modificare la



password.

[Informazioni correlate](#)

- [Cisco VPN serie 3000 Concentrator](#)
- [IPSec](#)
- [Cisco Secure Access Control Server per Windows](#)
- [RAGGIO](#)
- [RFC \(Requests for Comments\)](#)