Configure the Cisco VPN 3000 Series Concentrators to Support the NT Password Expiration Feature with the RADIUS Server

Document ID: 12086

Contents

Introduction

This document includes step−by−step instructions on how to configure the Cisco VPN 3000 Series Concentrators to support the NT Password Expiration feature using the RADIUS server.

Refer to VPN 3000 RADIUS with Expiry Feature Using Microsoft Internet Authentication Server in order to learn more about the same scenerio with the Internet Authentication Server (IAS).

Prerequisites

Requirements

- If your RADIUS server and NT Domain Authentication server are on two separate machines, make sure that you have established IP connectivity between the two machines.
- Make sure that you have established IP connectivity from the concentrator to the RADIUS server. If the RADIUS server is towards the public interface, don't forget to open up the RADIUS port on the Public Filter.
- Ensure that you can connect to the concentrator from the VPN client using the Internal User Database. If this is not configured, please refer to Configuring IPSec − Cisco 3000 VPN Client to VPN 3000 Concentrator.

Note: The Password expiration feature cannot be used with Web VPN or SSL VPN clients.

Components Used

This configuration was developed and tested using the software and hardware versions below.

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

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.

Network Diagram

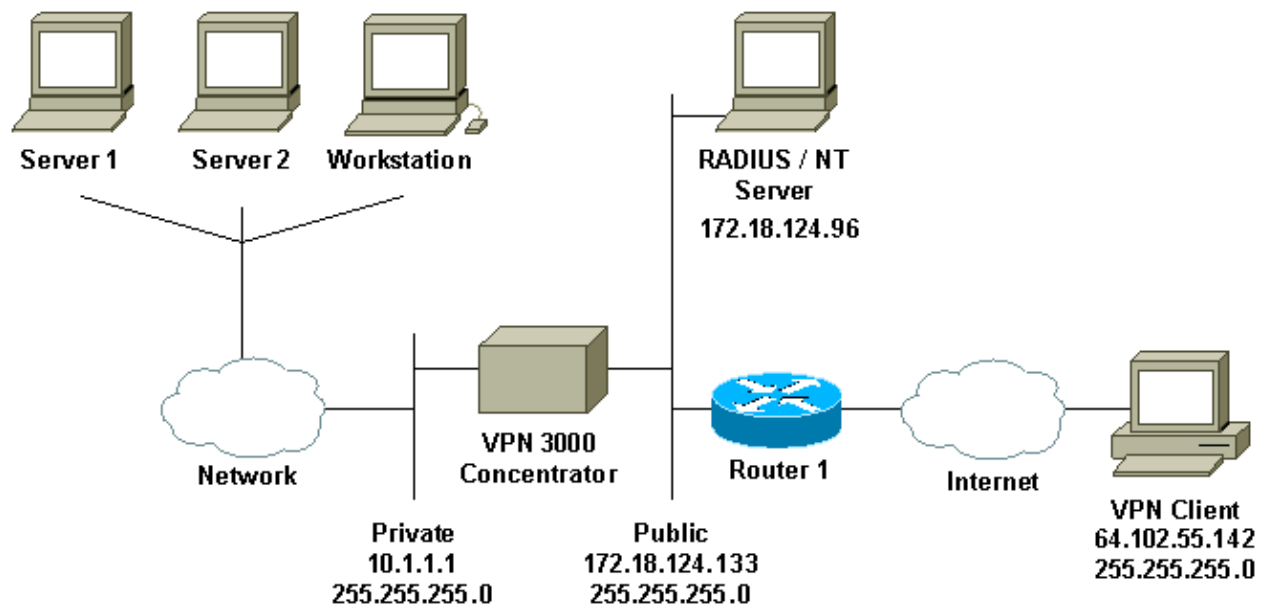This document uses this network setup:

Diagram Notes

1. The RADIUS server in this configuration is on the public interface. If this is the case with your specific setup, please create two rules in your public filter to allow RADIUS traffic to enter and leave the concentrator.
2. This configuration shows CSNT software and NT Domain Authentication Services running on the same machine. These elements can be run on two separate machines if required by your configuration.

Configuring the VPN 3000 Concentrator

Group Configuration

1. To configure the group to accept the NT Password Expiration Parameters from the RADIUS Server, go to **Configuration** > **User Management** > **Groups**, select your group from the list, and click **Modify Group**. The example below shows how to modify a group named "ipsecgroup."

This section lets you configure groups. A group is a collection of users treated as a single entity.

Click the **Add Group** button to add a group, or select a group and click **Delete Group** or **Modify Group**. To modify other group parameters, click **Modify Auth. Servers, Modify Acct. Servers Modify Address Pools** or **Modify Client Update**.

Current Groups	Actions
ipsecgroup (Internally Configured)	Add Group
	Modify Group
	Modify Auth. Servers
	Modify Acct. Servers
	Modify Address Pools
	Modify Client Update
	Delete Group

2. Go to the **IPSec** tab, make sure that **RADIUS with Expiry** is selected for the **Authentication** attribute.

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

IPSec Parameters

Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5	☑	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	☑	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	☑	☑	Check to enable the use of IKE keepalives for members of this group.
Reauthentication on Rekey	☐	☑	Check to reauthenticate the user on an IKE (Phase-1) rekey.
Tunnel Type	Remote Access	☑	Select the type of tunnel for this group. Update the Remote Access parameters below as needed
Remote Access Parameters			
Group Lock	☐	☑	Lock users into this group.
Authentication	RADIUS with Expiry	☐	Select the authentication method for members of this group. This parameter does not apply to **Individual User Authentication**.
IPComp	None / RADIUS / RADIUS with Expiry / NT Domain / SDI / Internal	☑	Select the method of IP Compression for members of this group.
Mode Configuration		☑	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.

Apply   Cancel

3. If you want this feature to be enabled on the VPN 3002 Hardware Clients, go to the **HW Client** tab, make sure that **Require Interactive Hardware Client Authentication** is enabled, then click **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	☑	☐	Check to require the hardware client to be interactively authenticated at each connection attempt.
Require Individual User Authentication	☐	☑	Check to require users behind a hardware client to be authenticated.
User Idle Timeout	30	☑	Enter the session idle timeout in minutes. Use 0 for no timeout.
Cisco IP Phone Bypass	☐	☑	Check to allow Cisco IP Phones to bypass Individual User Authentication behind a hardware client.

Apply   Cancel

RADIUS Configuration

1. To configure the RADIUS server settings on the concentrator, go to **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)

- Add
- Modify
- Delete
- Move Up
- Move Down
- Test

2. On the **Add** screen, type in the values that correspond to the RADIUS server and click **Add**.

The example below uses the following values.

```
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
```

Configure and add a user authentication server.

Server Type	RADIUS	Selecting *Internal Server* will let you add users to the internal user database.
Authentication Server	172.18.124.96	Enter IP address or hostname.
Server Port	0	Enter 0 for default port (1645).
Timeout	4	Enter the timeout for this server (seconds).
Retries	2	Enter the number of retries for this server.
Server Secret	********	Enter the RADIUS server secret.
Verify	********	Re-enter the secret.

Add   Cancel

Configuring the Cisco Secure NT RADIUS Server

Configuring an Entry for the VPN 3000 Concentrator

1. Log into CSNT and click **Network Configuration** in the left panel. Under "AAA Clients," click **Add Entry**.

On the "Add AAA Client" screen, type in the appropriate values to add the concentrator as the RADIUS Client, then click **Submit** + **Restart**.

The example below uses the following values.

```
AAA Client Hostname = 133_3000_conc

AAA Client IP Address = 172.18.124.133

Key = cisco123

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

An entry for your 3000 concentrator will appear under the "**AAA Clients**" section.

Configuring the Unknown User Policy for NT Domain Authentication

1. To configure User Authentication on the RADIUS server as a part of the Unknown User Policy, click **External User Database** in the left panel, then click the link for **Database Configuration**.

2. Under "External User Database Configuration," click **Windows NT/2000**.
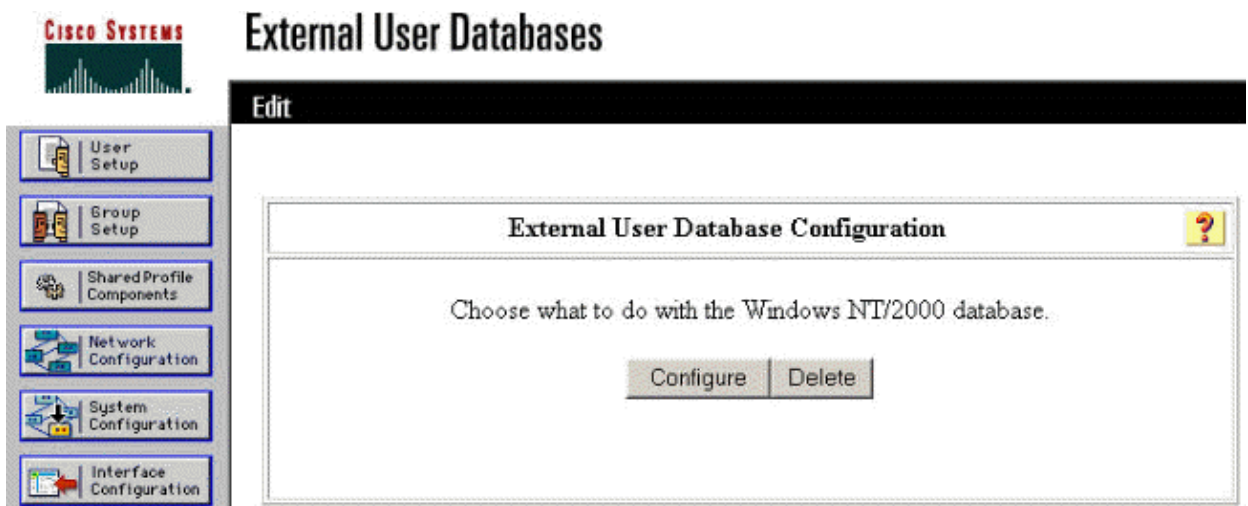

3. On the "Database Configuration Creation" screen, click **Create New Configuration**.
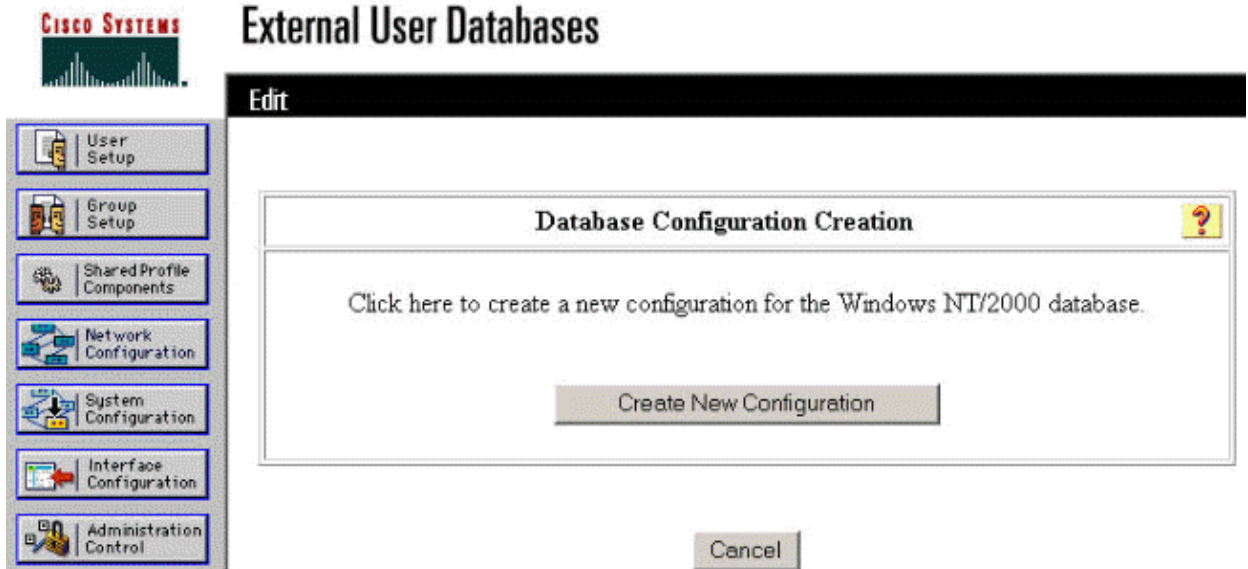
4. When prompted, type a name for the NT/2000 Authentication and click **Submit**. The example below shows the name "Radius/NT Password Expiration."
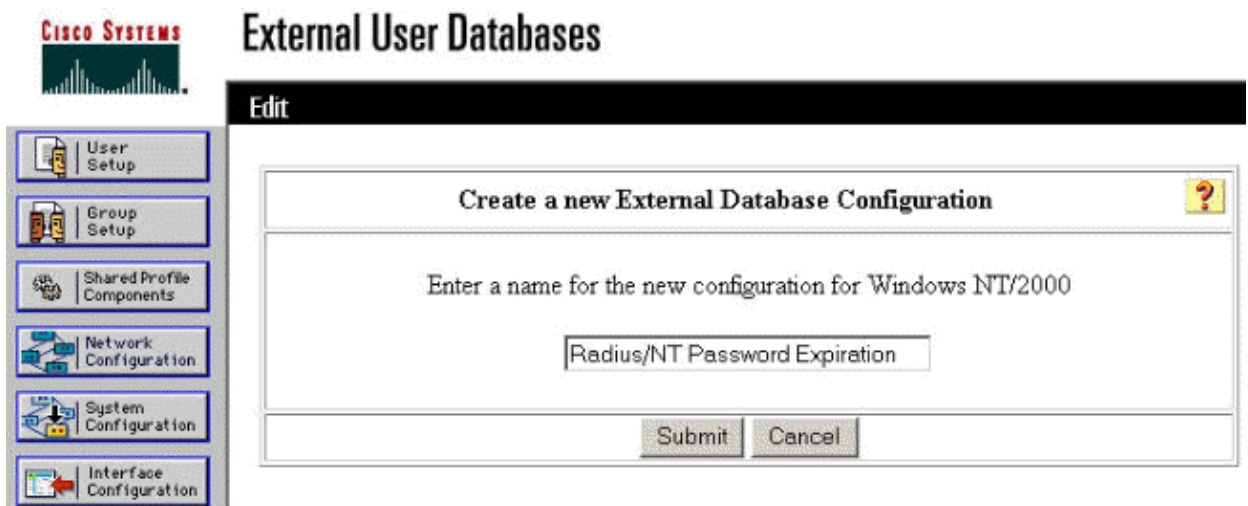
5. Click **Configure** to configure the Domain Name for User Authentication.

6. Select your NT domain from the "Available Domains," then click the right−arrow button to add it to the "Domain List." Under "MS−CHAP Settings," ensure that the options for **Permit password changes using MS−CHAP version 1** and **version 2** are selected. Click **Submit** when you are done.

CISCO SYSTEMS

External User Databases

Configure Domain List

Available Domains   Domain List
                                           JAZIB-ADS

[->]
[<-]

[Up] [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. Click **External User Database** in the left panel, then click the link for **Database Group Mappings** (as seen in this example). You should see an entry for your previously configured external database. The example below shows an entry for "Radius/NT Password Expiration," the database that we just configured.

CISCO SYSTEMS

External User Databases

Select

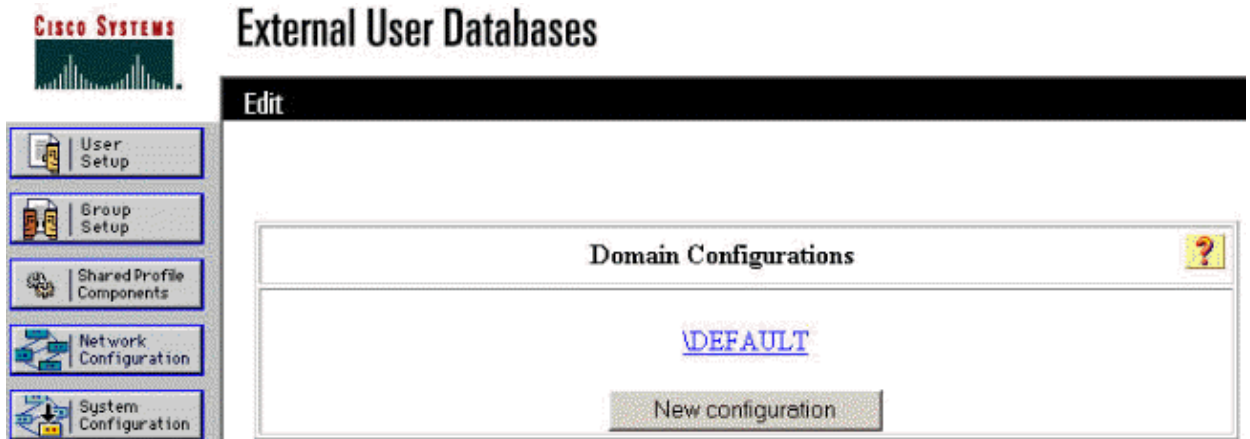**Unknown User Group Mappings**

Choose the External User Database for which you want to configure the group mappings.
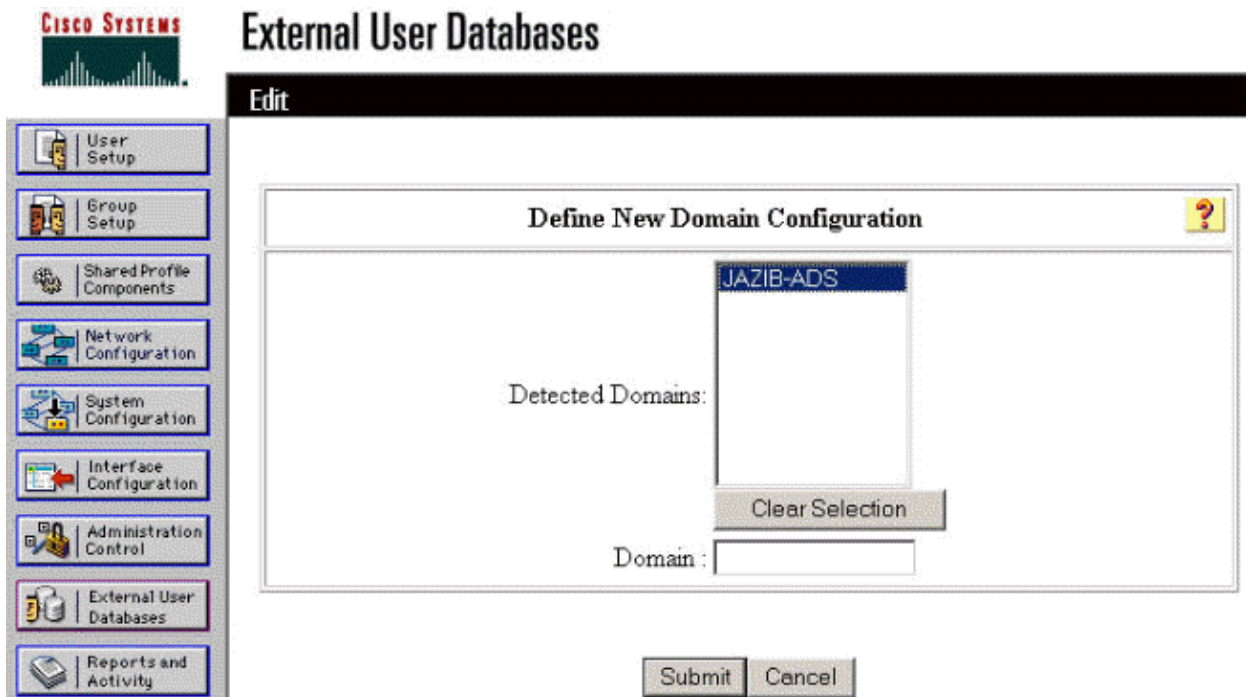
Name	Type
Radius/NT Password Expiration	Windows NT/2000

[Cancel]

8. On the "Domain Configurations" screen, click **New configuration** to add the domain configurations.

9. Select your domain from the list of "Detected Domains" and click **Submit**. The example below shows a domain named "JAZIB−ADS."

10. Click on your domain name to configure the group mappings. This example shows the domain "JAZIB−ADS."

CISCO SYSTEMS — External User Databases

Edit

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration

Domain Configurations [?]

JAZIB-ADS
\DEFAULT

New configuration

11. Click **Add mapping** to define the group mappings.

CISCO SYSTEMS — External User Databases

Edit

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

Group Mappings for Domain : JAZIB-ADS [?]

NT groups   CiscoSecure group
- no mappings defined -

Add mapping

Delete Configuration

12. On the "Create new group mapping" screen, map the group on the NT domain to a group on the CSNT RADIUS server, then click **Submit**.. The example below maps the NT group "Users" to the RADIUS group "Group 1."

CISCO SYSTEMS

External User Databases

Edit

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Reports and Activity
- Online Documentation
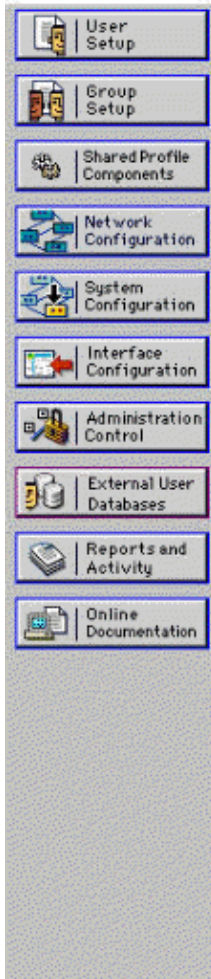
Create new group mapping for Domain : JAZIB-ADS

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. Click **External User Database** in the left panel, then click the link for **Unknown User Policy** (as seen in this example). Make sure that the option for **Check the following external user databases** is selected. Click the right–arrow button to move the previously configured external database from the list of "External Databases" to the list of "Selected Databases."

Testing the NT/RADIUS Password Expiration Feature

The concentrator offers a function to test RADIUS authentication. To test this feature properly, make sure that you follow these steps carefully.

Testing RADIUS Authentication

1. Go to **Configuration** > **System** > **Servers** > **Authentication**. Select your RADIUS server and click **Test**.

2. When prompted, type your NT domain user name and password, and then click **OK**. The example below shows user name "jfrahim" configured on the NT domain server with "cisco123" as the password.

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

User Name |jfrahim|

Password |**********|

OK   Cancel

3. If your authentication is set up properly, you should get a message stating "Authentication Successful."

Success

(i) Authentication Successful

Continue

If you receive any message other than the one shown above, there is some configuration or connection problem. Please repeat the configuration and testing steps outlined in this document to ensure that all settings were made properly. Also check the IP connectivity between your devices.

Actual NT Domain Authentication Using RADIUS Proxy to Test the Password Expiration Feature

1. If the user is already defined on the domain server, modify the properties so that the user will be prompted to change the password at the next logon. Go to the "Account" tab of the user's properties dialog box, select the option for **User must change password at next logon**, then click **OK**.
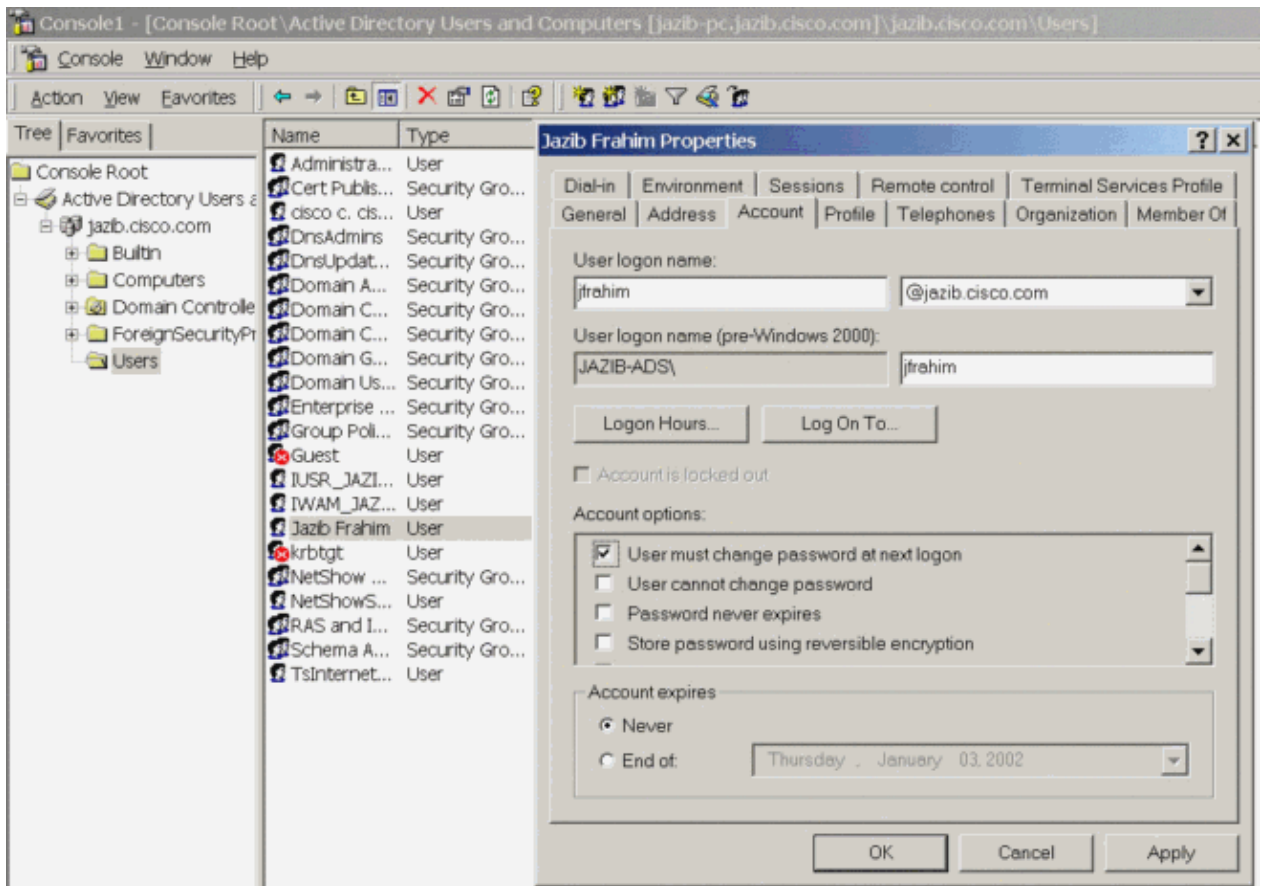
2. Launch the VPN client, then try to establish the tunnel to the concentrator.

3. During User Authentication, you should be prompted to change the password.
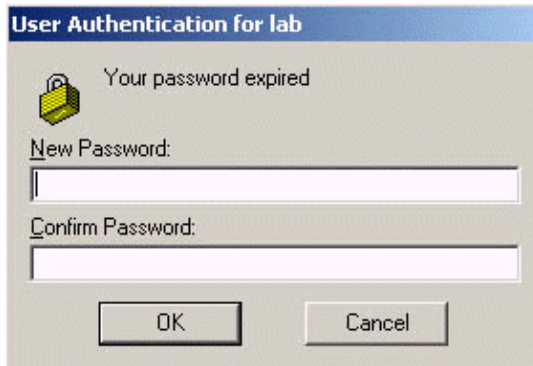
Related Information

- **Cisco VPN 3000 Series Concentrator**
- **IPSec**
- **Cisco Secure Access Control Server for Windows**
- **RADIUS**
- **Requests for Comments (RFCs)**

Updated: Jan 19, 2006   Document ID: 12086