

# RADIUS 서버에서 NT 비밀번호 만료 기능을 지원하도록 Cisco VPN 3000 Series Concentrator 구성

## 목차

### [소개](#)

### [사전 요구 사항](#)

### [요구 사항](#)

### [사용되는 구성 요소](#)

### [네트워크 다이어그램](#)

### [VPN 3000 Concentrator 구성](#)

### [그룹 구성](#)

### [RADIUS 컨피그레이션](#)

### [Cisco Secure NT RADIUS 서버 구성](#)

### [VPN 3000 Concentrator 항목 구성](#)

### [NT 도메인 인증을 위한 알 수 없는 사용자 정책 구성](#)

### [NT/RADIUS 비밀번호 만료 기능 테스트](#)

### [RADIUS 인증 테스트](#)

### [RADIUS 프록시를 사용하여 비밀번호 만료 기능을 테스트하는 실제 NT 도메인 인증](#)

### [관련 정보](#)

## [소개](#)

이 문서에는 RADIUS 서버를 사용하여 NT 비밀번호 만료 기능을 지원하도록 Cisco VPN 3000 Series Concentrator를 구성하는 방법에 대한 단계별 지침이 포함되어 있습니다.

IAS(Internet Authentication Server)와 동일한 [범위에](#) 대한 자세한 내용은 [Microsoft 인터넷 인증 서버를 사용하여 만료](#) 기능이 있는 VPN 3000 RADIUS를 참조하십시오.

## [사전 요구 사항](#)

### [요구 사항](#)

- RADIUS 서버와 NT 도메인 인증 서버가 서로 다른 두 시스템에 있는 경우 두 시스템 간에 IP 연결을 설정했는지 확인합니다.
- Concentrator에서 RADIUS 서버로의 IP 연결을 설정했는지 확인합니다. RADIUS 서버가 공용 인터페이스를 향하는 경우 Public Filter에서 RADIUS 포트를 여는 것을 잊지 마십시오.
- 내부 사용자 데이터베이스를 사용하여 VPN 클라이언트에서 Concentrator에 연결할 수 있는지 확인합니다. 구성되지 않은 경우 IPsec 구성 - [Cisco 3000 VPN Client to VPN 3000](#)

[Concentrator](#)를 참조하십시오.

**참고:** 비밀번호 만료 기능은 웹 VPN 또는 SSL VPN 클라이언트와 함께 사용할 수 없습니다.

## 사용되는 구성 요소

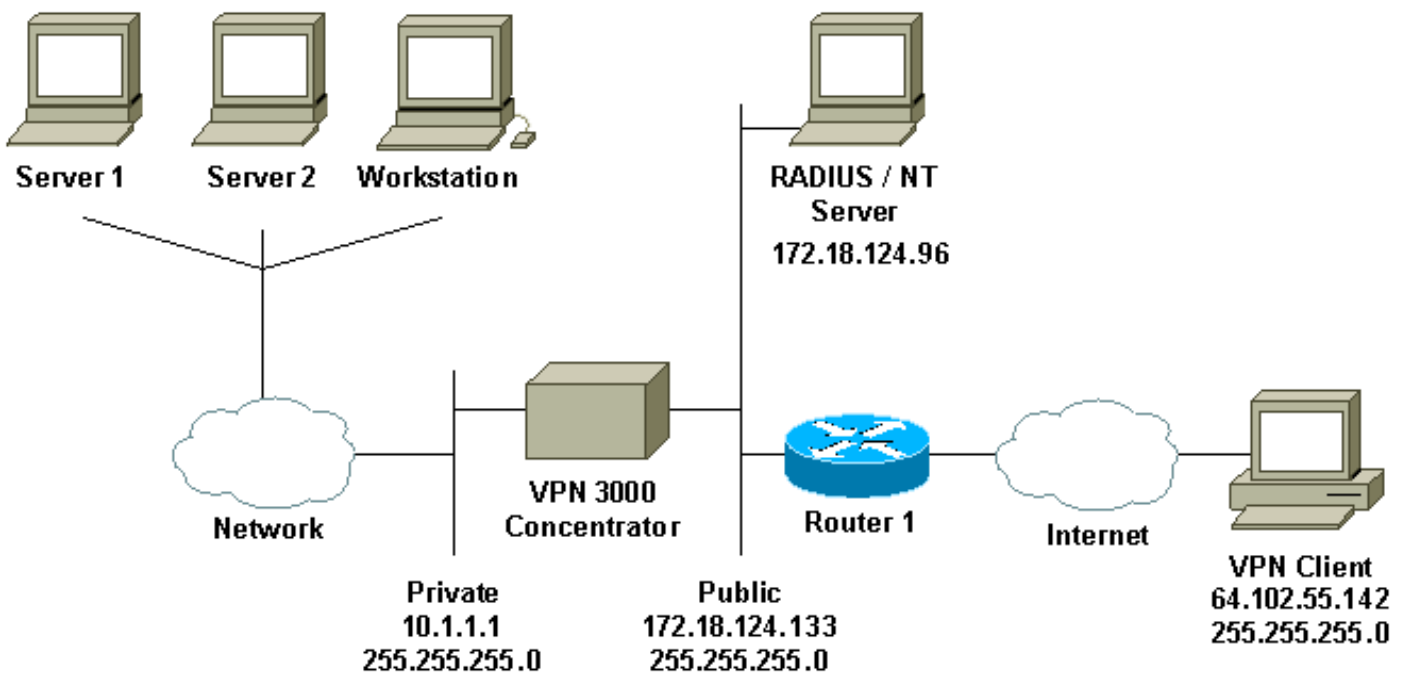
이 구성은 아래의 소프트웨어 및 하드웨어 버전을 사용하여 개발 및 테스트되었습니다.

- VPN 3000 Concentrator Software 버전 4.7
- VPN 클라이언트 릴리스 3.5
- 사용자 인증을 위한 Cisco Secure for NT(CSNT) 버전 3.0 Microsoft Windows 2000 Active Directory Server

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



### 다이어그램 메모

1. 이 컨피그레이션의 RADIUS 서버는 공용 인터페이스에 있습니다. 특정 설정 시 RADIUS 트래픽이 Concentrator로 들어오고 나가도록 허용하려면 공용 필터에 두 개의 규칙을 생성하십시오.
2. 이 구성은 동일한 시스템에서 실행 중인 CSNT 소프트웨어 및 NT 도메인 인증 서비스를 보여줍니다. 이러한 요소는 구성에 필요한 경우 두 개의 개별 시스템에서 실행할 수 있습니다.

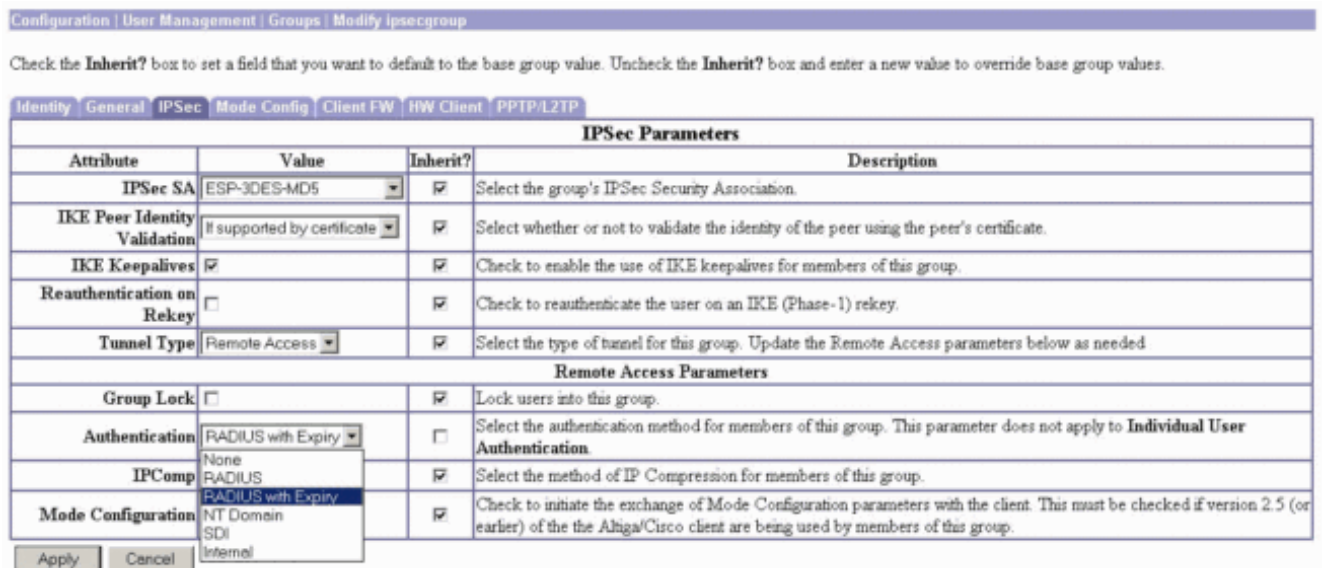
## VPN 3000 Concentrator 구성

### 그룹 구성

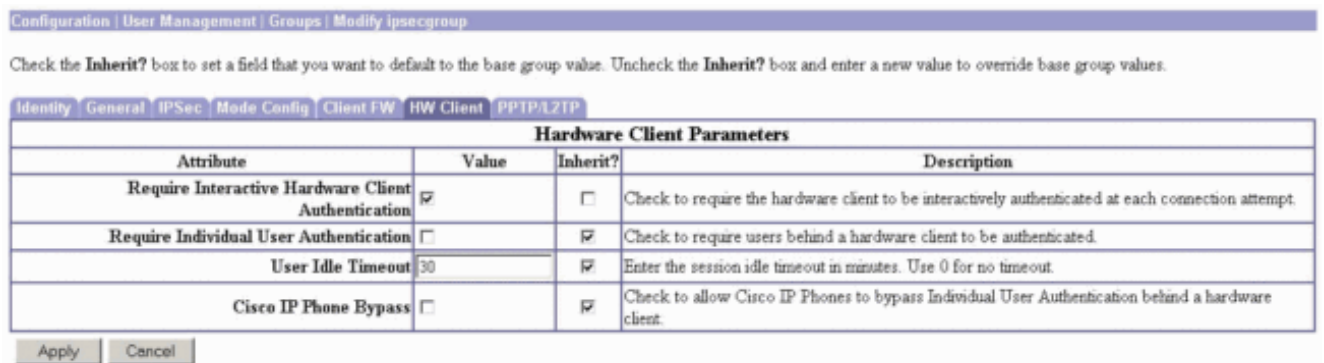
1. RADIUS 서버에서 NT Password Expiration Parameters(NT 비밀번호 만료 매개변수)를 허용하도록 그룹을 구성하려면 Configuration(구성) > User Management(사용자 관리) > Groups(그룹)로 이동하여 목록에서 그룹을 선택하고 **Modify Group(그룹 수정)**을 클릭합니다. 아래 예는 "ipsecgroup"이라는 그룹을 수정하는 방법을 보여줍니다



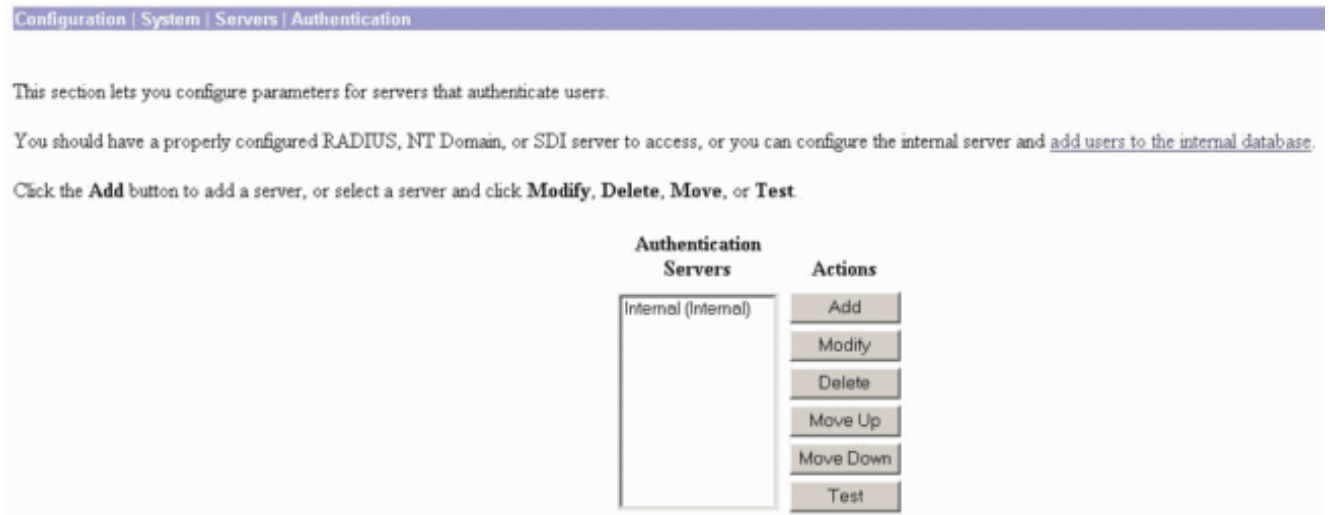
2. IPSec 탭으로 이동하여 **Authentication** 특성에 대해 **Expiry**가 있는 RADIUS가 선택되었는지 확인합니다



3. VPN 3002 Hardware Clients에서 이 기능을 활성화하려면 **HW Client(하드웨어 클라이언트)** 탭으로 이동하여 **Require Interactive Hardware Client Authentication(대화형 하드웨어 클라이언트 인증 필요)**이 활성화되었는지 확인한 다음 **Apply(적용)**를 클릭합니다



1. Concentrator에서 RADIUS 서버 설정을 구성하려면 Configuration(컨피그레이션) > System(시스템) > Servers(서버) > Authentication(인증) > Add(추가)로 이동합니다



2. Add(추가) 화면에서 RADIUS 서버에 해당하는 값을 입력하고 Add(추가)를 클릭합니다.아래 예에서는 다음 값을 사용합니다.

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**

The screenshot shows the 'Add' configuration page for a user authentication server. At the top, there is a breadcrumb trail: Configuration | System | Servers | Authentication | Add. Below this, a text block says 'Configure and add a user authentication server.' The main part of the page is a form with several fields and a description on the right. The fields are: 'Server Type' (a dropdown menu with 'RADIUS' selected), 'Authentication Server' (a text box with '172.18.124.96'), 'Server Port' (a text box with '0'), 'Timeout' (a text box with '4'), 'Retries' (a text box with '2'), 'Server Secret' (a text box with masked characters), and 'Verify' (a text box with masked characters). The description on the right explains the purpose of each field. At the bottom left, there are two buttons: 'Add' and 'Cancel'.

# Cisco Secure NT RADIUS 서버 구성

## VPN 3000 Concentrator 항목 구성

1. CSNT에 로그인하고 왼쪽 패널에서 Network Configuration(네트워크 컨피그레이션)을 클릭합니다. "AAA Clients(AAA 클라이언트)"에서 Add Entry(항목 추가)를 클릭합니다

The screenshot shows the Cisco Secure Network Configuration interface. On the left is a navigation pane with icons for User Setup, Group Setup, Shared Profile Components, Network Configuration (highlighted), System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main area is titled "Network Configuration" and contains three sections:

- AAA Clients:** A table with columns "AAA Client Hostname", "AAA Client IP Address", and "Authenticate Using". One entry is shown with hostname "nsite", IP "172.18.141.40", and authentication "RADIUS (Cisco IOS/PIX)". An "Add Entry" button is below.
- AAA Servers:** A table with columns "AAA Server Name", "AAA Server IP Address", and "AAA Server Type". One entry is shown with name "jazib-pc", IP "172.18.124.96", and type "CiscoSecure ACS for Windows 2000/NT". An "Add Entry" button is below.
- Proxy Distribution Table:** A table with columns "Character String", "AAA Servers", "Strip", and "Account". One entry is shown with character string "(Default)", AAA Servers "jazib-pc", Strip "No", and Account "Local". "Add Entry" and "Sort Entries" buttons are below.

A red warning message is displayed: "The current configuration has been changed. Restart ACS in 'System Configuration:Service Control' to adopt the new settings."


2. "Add AAA Client(AAA 클라이언트 추가)" 화면에서 적절한 값을 입력하여 Concentrator를 RADIUS Client(RADIUS 클라이언트)로 추가한 다음 **Submit + Restart(제출 + 재시작)**를 클릭합니다.아래 예에서는 다음 값을 사용합니다.

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:

AAA Client IP Address:

Key:


Authenticate Using: RADIUS (Cisco VPN 3000)

Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

3000 Concentrator에 대한 항목이 "AAA Clients" 섹션 아래에 표시됩니다



## Network Configuration

Select

### AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
<a href="#">133_3000_conc</a>	172.18.124.133	RADIUS (Cisco VPN 3000)
<a href="#">nsite</a>	172.18.141.40	RADIUS (Cisco IOS/PIX)

### NT 도메인 인증을 위한 알 수 없는 사용자 정책 구성

1. RADIUS 서버에서 User Authentication(사용자 인증)을 Unknown User Policy(알 수 없는 사용자 정책)의 일부로 구성하려면 왼쪽 패널에서 External User Database(외부 사용자 데이터베이스)를 클릭한 다음 Database Configuration(데이터베이스 컨피그레이션) 링크를 클릭합니다



# 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

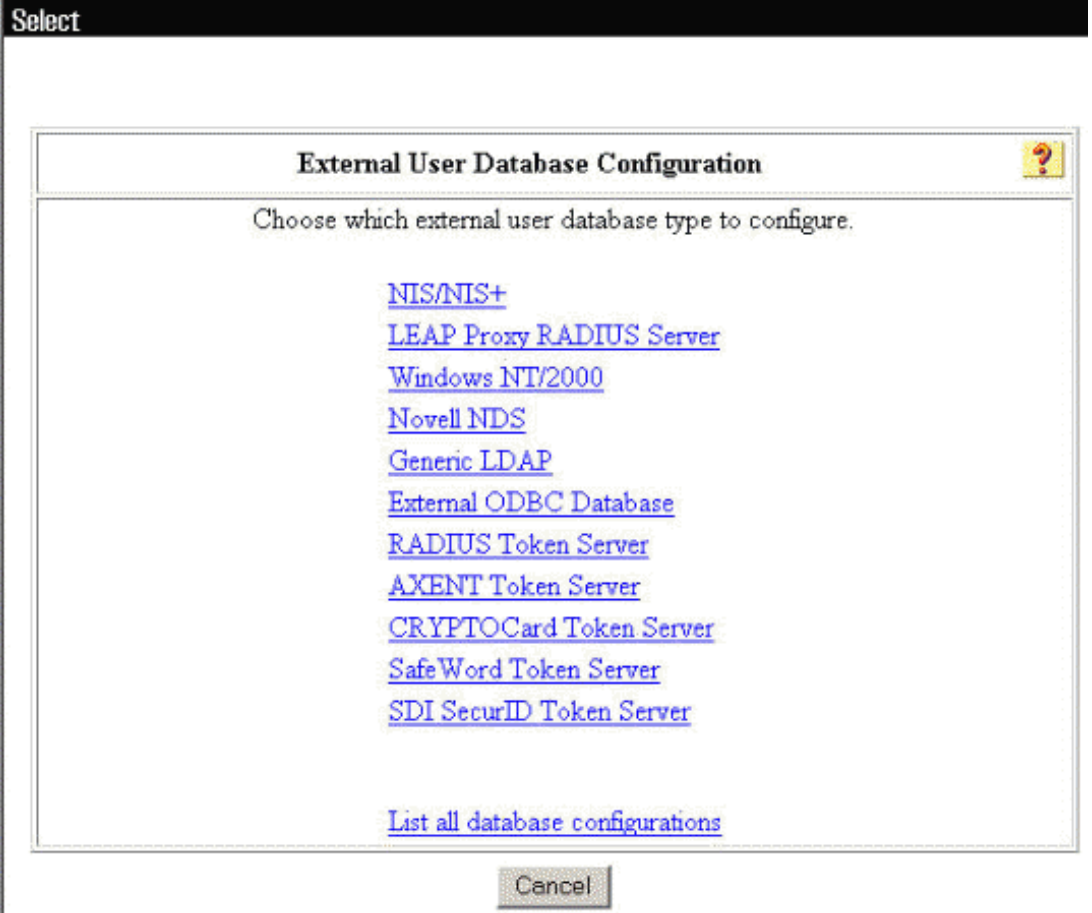
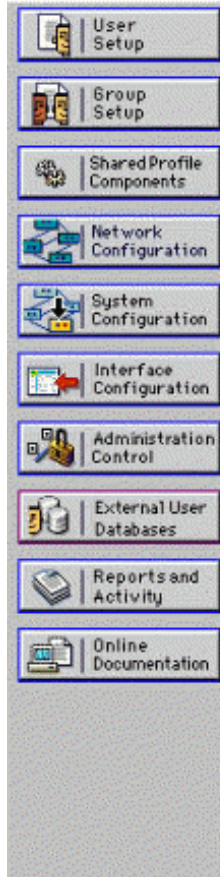
- [Unknown User Policy](#)
- [Database Group Mappings](#)
- [Database Configuration](#)

Back to Help

2. "외부 사용자 데이터베이스 구성"에서 **Windows NT/2000**을 클릭합니다



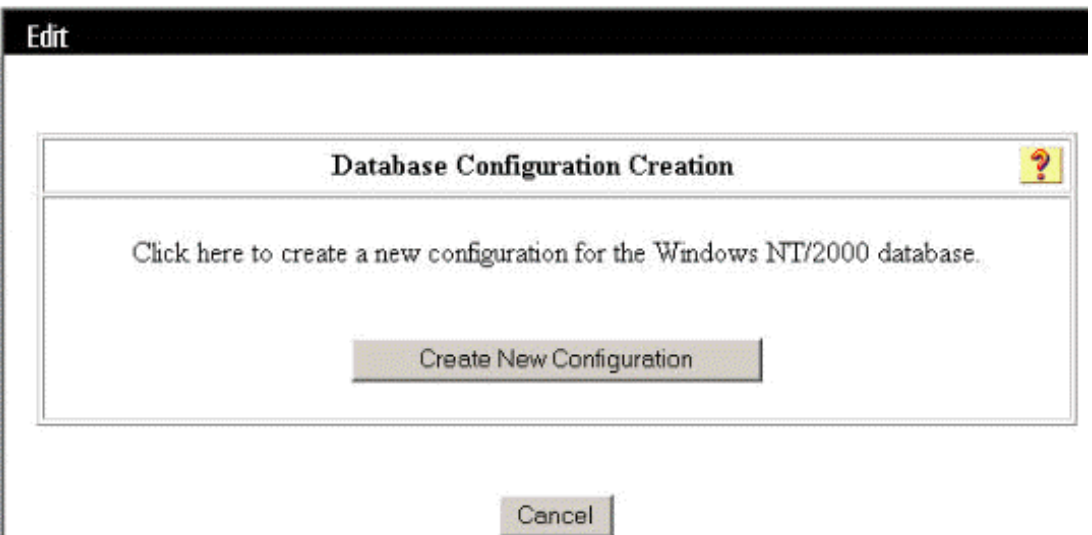
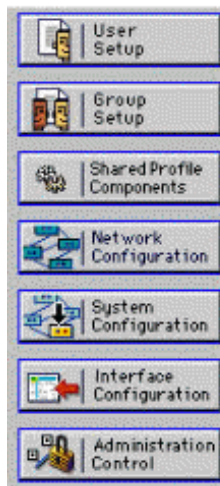
## External User Databases



3. "Database Configuration Creation(데이터베이스 컨피그레이션 생성)" 화면에서 **Create New Configuration(새 컨피그레이션 생성)**을 클릭합니다



## External User Databases



4. 프롬프트가 표시되면 NT/2000 Authentication의 이름을 입력하고 **Submit(제출)**을 클릭합니다. 아래 예는 "Radius/NT Password Expiration"이라는 이름을 보여줍니다





## External User Databases



**Edit**

**Create a new External Database Configuration** ?

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

5. Configure를 클릭하여 사용자 인증을 위한 도메인 이름을 구성합니다



## External User Databases




**Edit**

**External User Database Configuration** ?

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

6. "Available Domains(사용 가능한 도메인)"에서 NT 도메인을 선택한 다음 오른쪽 화살표 단추를 클릭하여 "Domain List(도메인 목록)"에 추가합니다. "MS-CHAP 설정"에서 MS-CHAP 버전 1 및 버전 2를 사용하여 암호 변경 허용 옵션을 선택했는지 확인합니다. 완료되면 Submit(제출)을 클릭합니다



## 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. 왼쪽 패널에서 외부 사용자 데이터베이스를 클릭한 다음 데이터베이스 그룹 매핑 링크(이 [예](#)에 [표시됨](#))를 클릭합니다. 이전에 구성한 외부 데이터베이스에 대한 항목이 표시되어야 합니다. 아래 예는 방금 구성한 데이터베이스인 "Radius/NT Password Expiration"에 대한 항목을 보여줍니다



## External User Databases

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

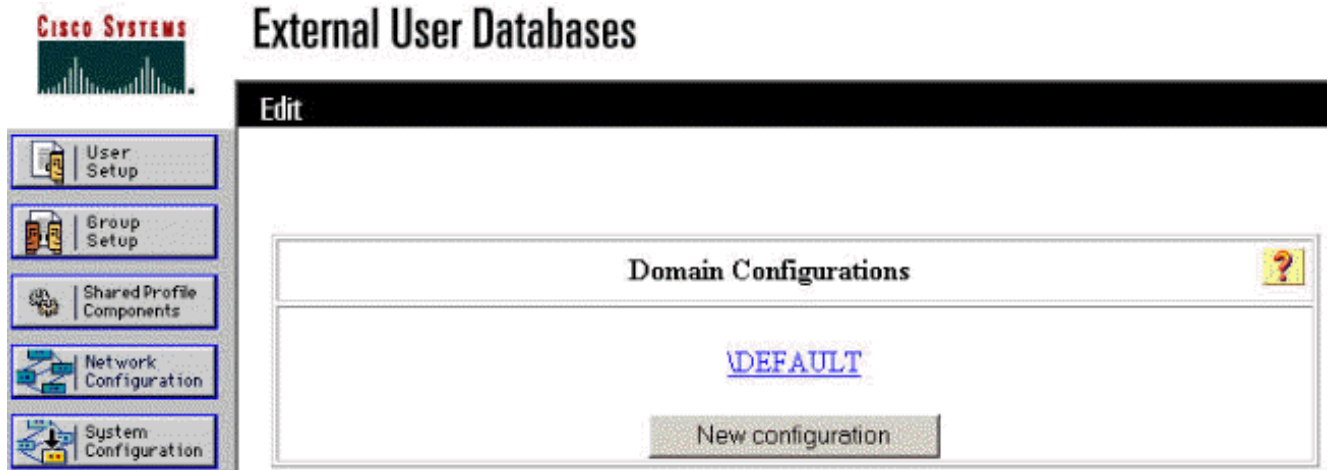
Select

### Unknown User Group Mappings ?

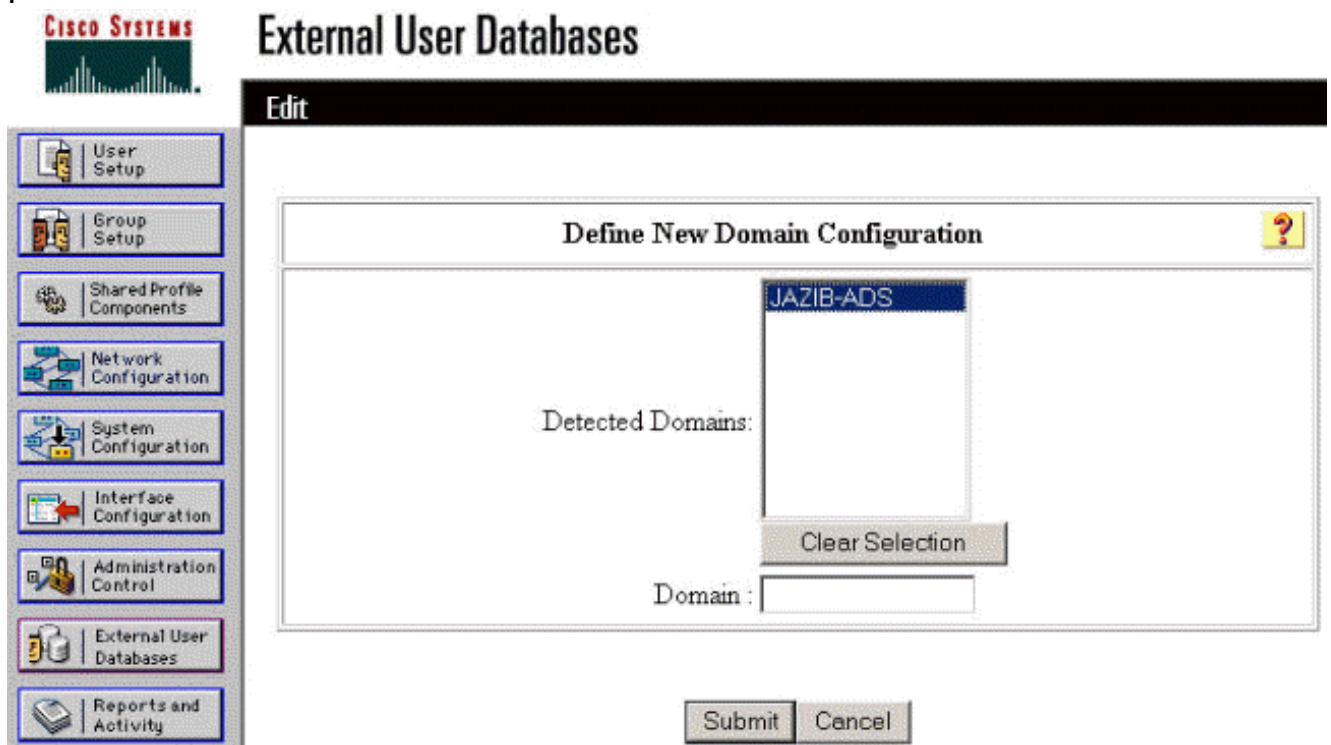
Choose the External User Database for which you want to configure the group mappings.

Name	Type
<a href="#">Radius/NT Password Expiration</a>	Windows NT/2000

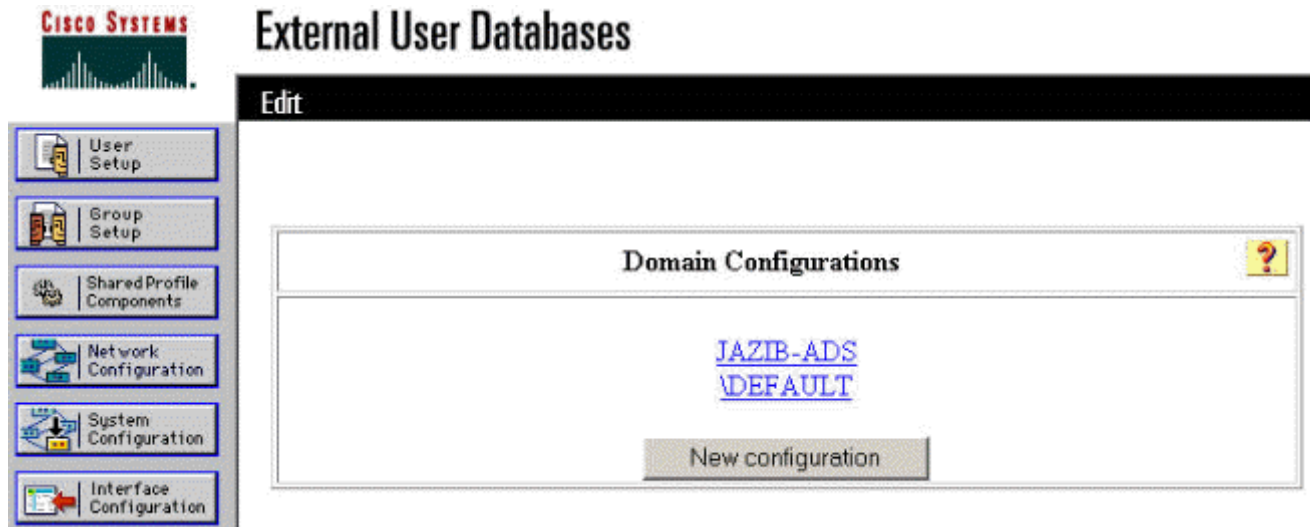
8. "Domain Configurations(도메인 컨피그레이션)" 화면에서 **New configuration(새 컨피그레이션)**을 클릭하여 도메인 컨피그레이션을 추가합니다



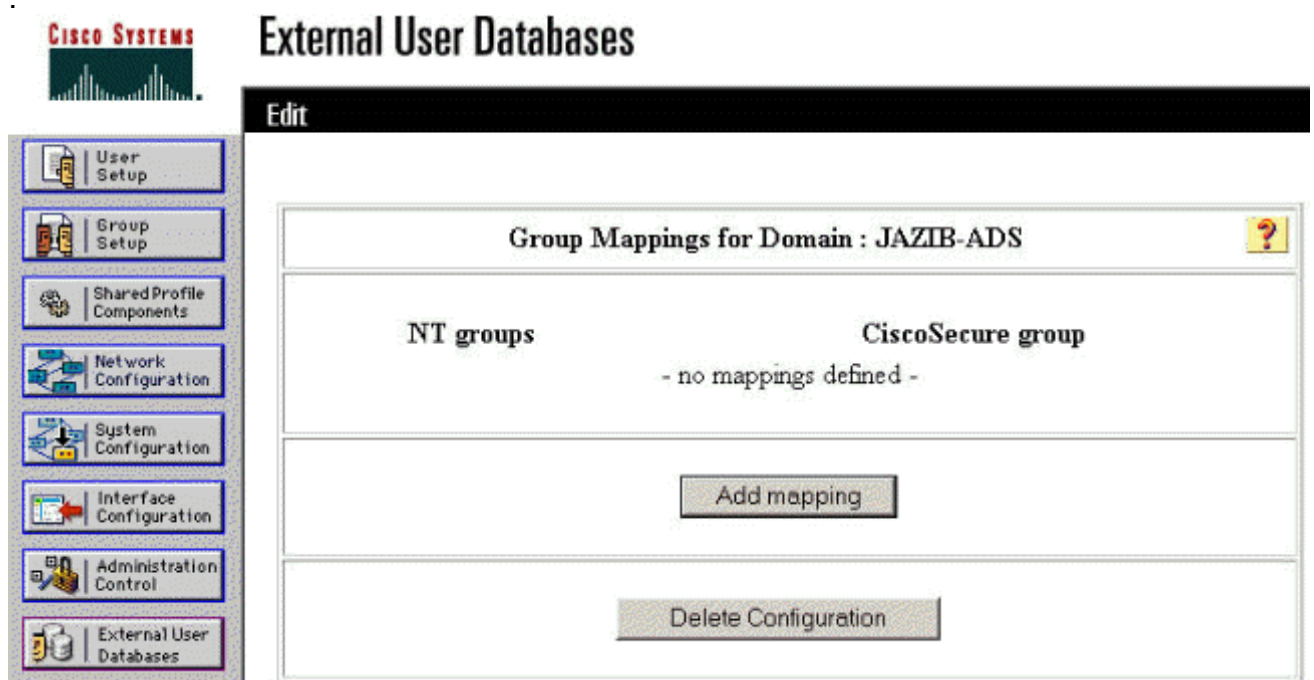
9. "Detected Domains(탐지된 도메인)" 목록에서 도메인을 선택하고 **Submit(제출)**을 클릭합니다  
아래 예는 "JAZIB-ADS"라는 도메인을 보여줍니다



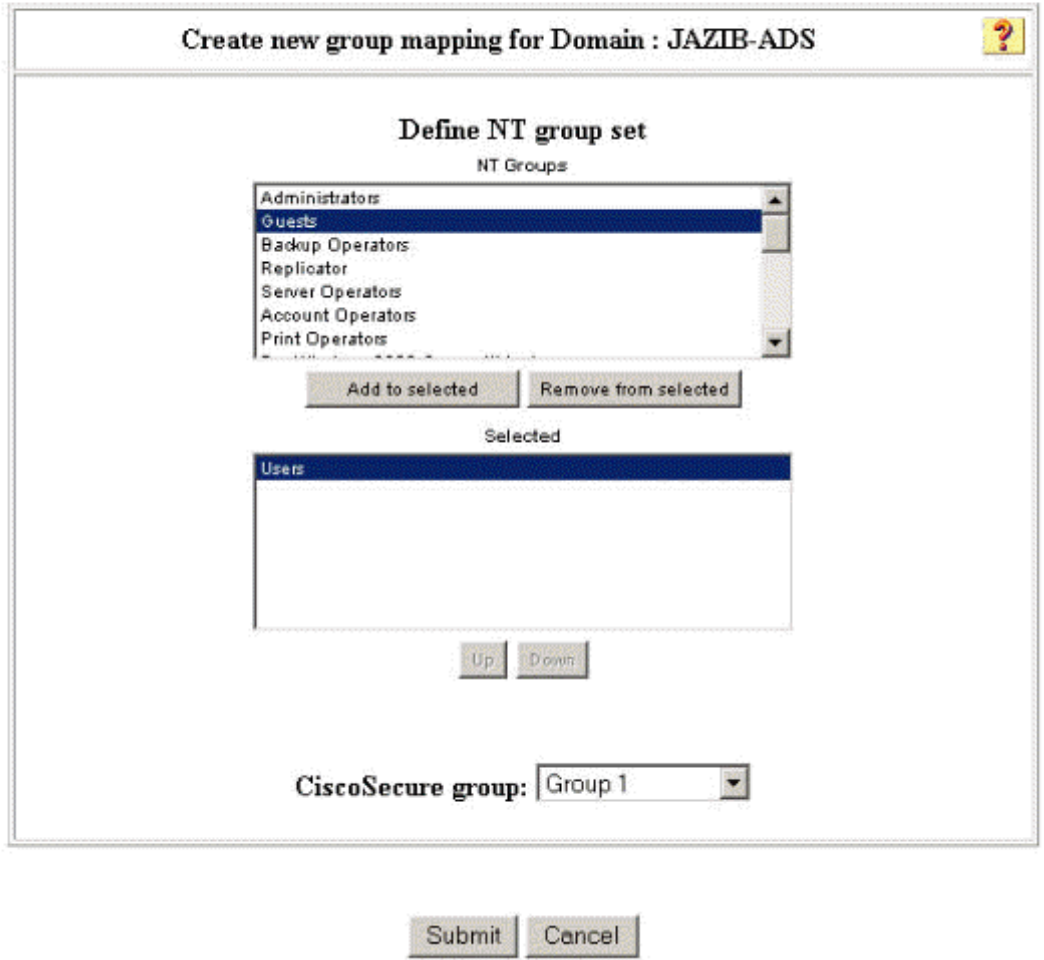
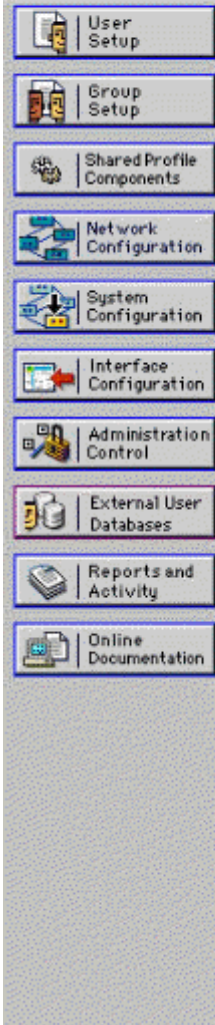
10. 그룹 매핑을 구성하려면 도메인 이름을 클릭합니다. 이 예에서는 도메인 "JAZIB-ADS"를 보여 줍니다



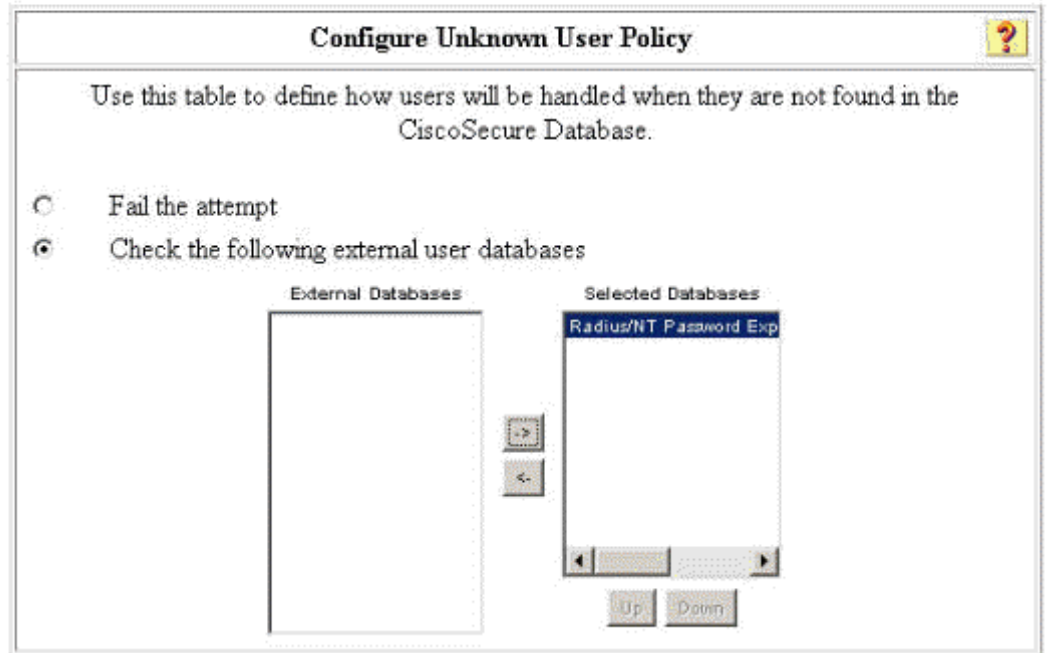
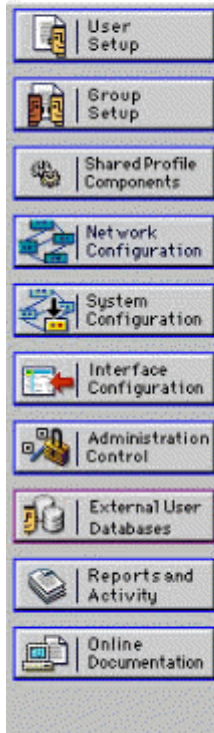
11. Add mapping(매핑 추가)을 클릭하여 그룹 매핑을 정의합니다



12. "Create new group mapping(새 그룹 매핑 생성)" 화면에서 NT 도메인의 그룹을 CSNT RADIUS 서버의 그룹에 매핑한 다음 Submit(제출)을 클릭합니다. 아래 예는 NT 그룹 "Users"를 RADIUS 그룹 "Group 1"에 매핑합니다



13. 왼쪽 패널에서 External User Database(외부 사용자 데이터베이스)를 클릭한 다음 Unknown User Policy(알 수 없는 사용자 정책)에 대한 링크를 클릭합니다(이 예에 표시됨). 다음 외부 사용자 데이터베이스 확인 옵션이 선택되었는지 확인합니다. 오른쪽 화살표 단추를 눌러 이전에 구성된 외부 데이터베이스를 "외부 데이터베이스" 목록에서 "선택한 데이터베이스" 목록으로 이동합니다

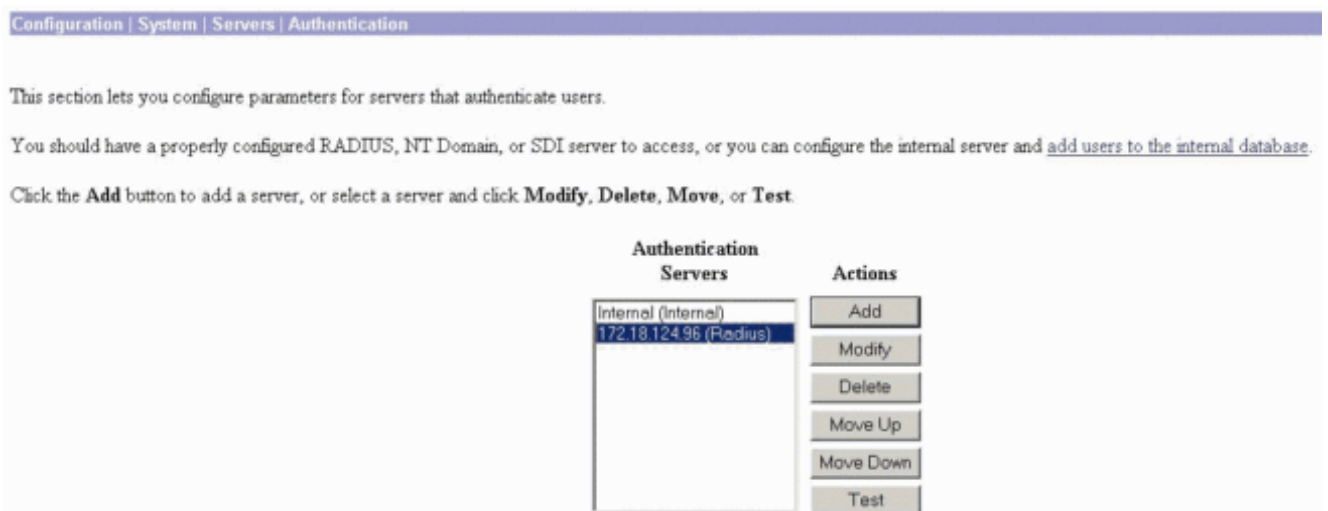


## NT/RADIUS 비밀번호 만료 기능 테스트

Concentrator는 RADIUS 인증을 테스트하는 기능을 제공합니다. 이 기능을 제대로 테스트하려면 다음 단계를 주의 깊게 따라야 합니다.

### RADIUS 인증 테스트

1. Configuration(컨피그레이션) > System(시스템) > Servers(서버) > Authentication(인증)으로 이동합니다. RADIUS 서버를 선택하고 Test(테스트)를 클릭합니다



2. 메시지가 표시되면 NT 도메인 사용자 이름과 암호를 입력한 다음 **확인**을 클릭합니다. 아래 예는 비밀번호로 "cisco123"을 사용하여 NT 도메인 서버에 구성된 사용자 이름 "jbrahim"을 보여 줍니다

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

User Name

Password

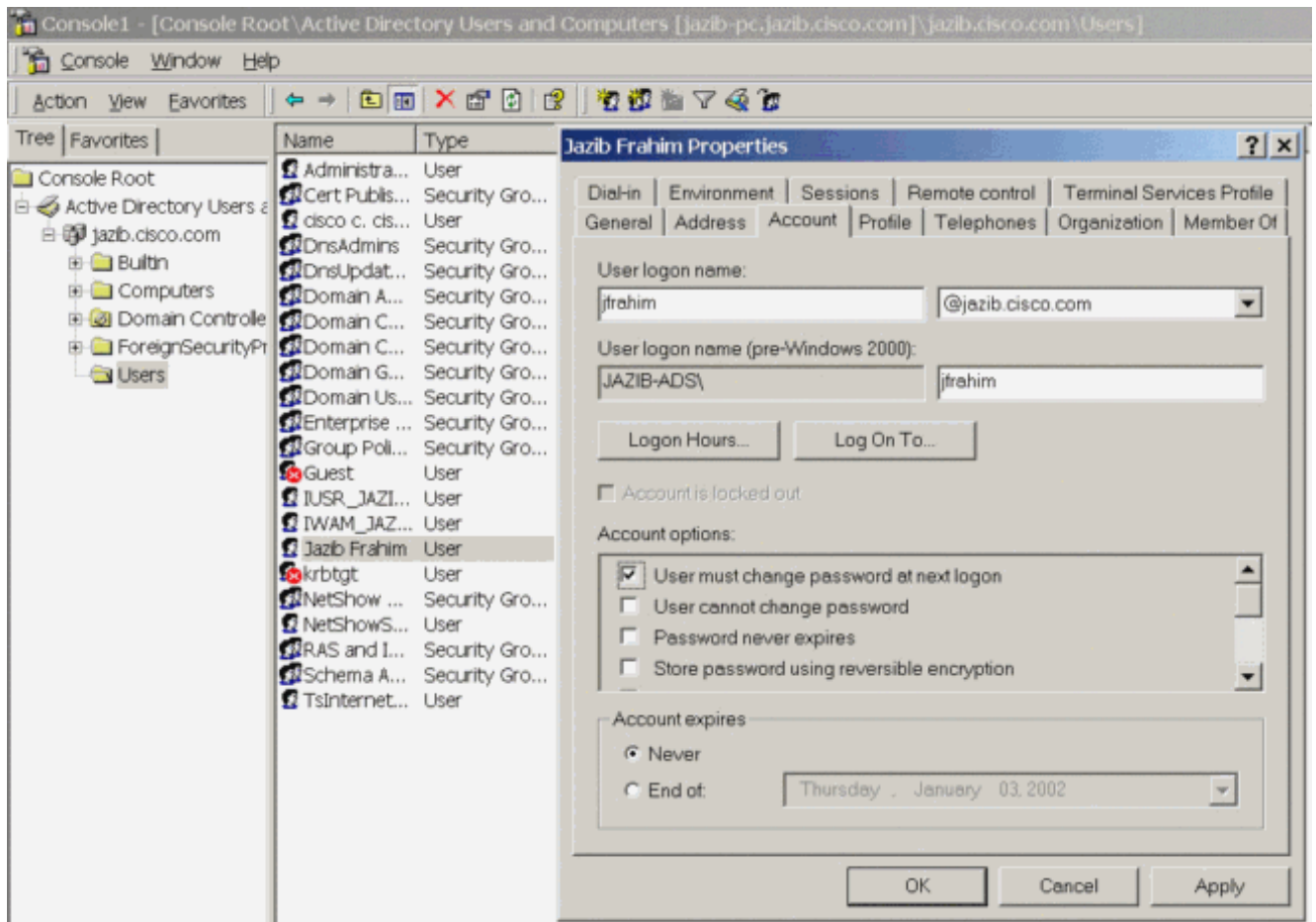
- 인증이 올바르게 설정된 경우 "Authentication Successful(인증 성공)"이라는 메시지를 받아야



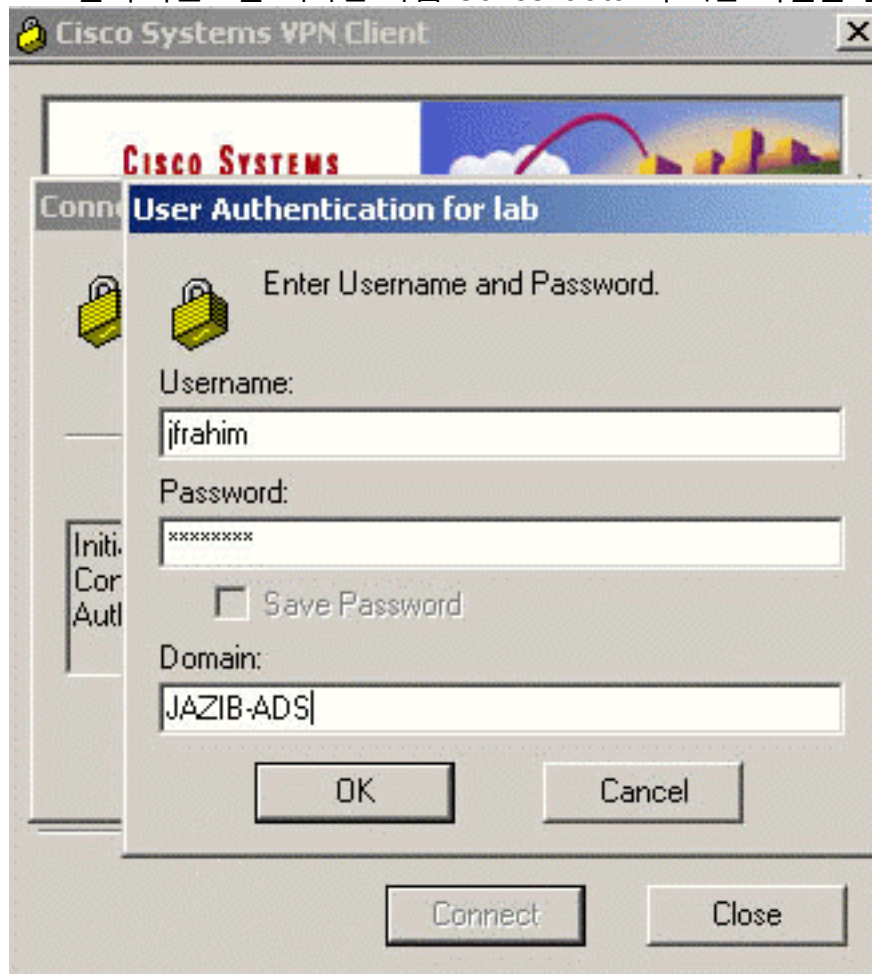
합니다. 위에 표시된 메시지 이외의 메시지가 수신되면 컨피그레이션 또는 연결 문제가 발생합니다. 모든 설정이 올바르게 이루어졌는지 확인하려면 이 문서에 설명된 구성 및 테스트 단계를 반복하십시오. 디바이스 간의 IP 연결도 확인합니다.

## [RADIUS 프록시를 사용하여 비밀번호 만료 기능을 테스트하는 실제 NT 도메인 인증](#)

- 사용자가 도메인 서버에 이미 정의되어 있는 경우 다음 로그인 시 암호를 변경하라는 메시지가 표시되도록 속성을 수정합니다. 사용자 속성 대화 상자의 "계정" 탭으로 이동하여 다음 로그인 시 사용자가 암호를 변경해야 함 옵션을 선택한 다음 확인을 클릭합니다



2. VPN 클라이언트를 시작한 다음 Concentrator에 대한 터널을 설정합니다



3. 사용자 인증 중에 비밀번호를 변경하라는 메시지가 표시됩니다





## [관련 정보](#)

- [Cisco VPN 3000 Series Concentrator](#)
- [IPSec](#)
- [Windows용 Cisco Secure Access Control Server](#)
- [RADIUS](#)
- [RFC\(Request for Comments\)](#)