# RADIUS 서버에서 NT 비밀번호 만료 기능을 지원 하도록 Cisco VPN 3000 Series Concentrator 구 성

# 목차

<u>소개</u> <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>네트워크 다이어그램</u> 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 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

# <u>소개</u>

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)<u>와</u> 동일한<u>범위에</u> 대한 자세한 내용은 <u>Microsoft 인터넷 인증 서</u> <u>버를 사용하여 만료</u> 기능이 있는 VPN 3000 RADIUS를 참조하십시오.

# <u>사전 요구 사항</u>

### <u>요구 사항</u>

- RADIUS 서버와 NT 도메인 인증 서버가 서로 다른 두 시스템에 있는 경우 두 시스템 간에 IP 연 결을 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 <u>- Cisco 3000 VPN Client to VPN 3000</u>

<u>Concentrator를</u> 참조하십시오.

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

### <u>사용되는 구성 요소</u>

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 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

#### <u>네트워크 다이어그램</u>

이 문서에서는 다음 네트워크 설정을 사용합니다.



#### 다이어그램 메모

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

## VPN 3000 Concentrator 구성

### <u>그룹 구성</u>

1. RADIUS 서버에서 NT Password Expiration Parameters(NT 비밀번호 만료 매개변수)를 허용 하도록 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

-	
Configuration   User Management   Groups	
	Save Needed

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 Act. Servers Modify Address Pools or Modify Client Update.



2. IPSec 탭으로 이동하여 Authentication 특성에 대해 Expiry가 있는 RADIUS가 선택되었는지 확인합니다

Configuration	User Mana	agement   Gr	oups   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	R	Select the group's IPSec Security Association.
IKE Peer Identity Validation	It supported by certificate 💌	R	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	R	R	Check to enable the use of IKE keepalives for members of this group.
Reauthentication on Rekey		R	Check to reauthenticate the user on an IKE (Phase-1) rekey.
Tunnel Type	Remote Access 💌	R	Select the type of tunnel for this group. Update the Remote Access parameters below as needed
			Remote Access Parameters
Group Lock	<b>D</b>	. P	Lock users into this group.
Authentication	RADIUS with Expiry	Ę.	Select the authentication method for members of this group. This parameter does not apply to <b>Individual User</b> Authentication.
IPComp	RADIUS	R	Select the method of IP Compression for members of this group.
Mode Configuration	RADIUS with Expiry NT Domein SDI	R	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	Internal		

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

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.

ntity General IPSec Mode Config Client FW HW Client PPTP/LZTP Hardware Client Parameters Attribute Value Inherit? Description **Require Interactive Hardware Client** 5 Check to require the hardware client to be interactively authenticated at each connection attempt Authentication Check to require users behind a hardware client to be authenticated. Require Individual User Authentication User Idle Timeout 30 Enter the session idle timeout in minutes. Use 0 for no timeout. Check to allow Cisco IP Phones to bypass Individual User Authentication behind a hardware Cisco IP Phone Bypass 🗆 되 client. Apply Cancel

RADIUS 컨피그레이션

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

Configuration | System | Servers | Authentication

This section lets you configure parameters for servers that authenticate users.

You should have a property 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.



 Add(추가) 화면에서 RADIUS 서버에 해당하는 값을 입력하고 Add(추가)를 클릭합니다. 에에서는 다음 값을 사용합니다.

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

#### Configuration | System | Servers | Authentication | Add

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 Annuality	Re-enter the secret.
Add Cancel	

# <u>Cisco Secure NT RADIUS 서버 구성</u>

#### VPN 3000 Concentrator 항목 구성

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

	introli			
Select				
<b>%</b>		AAA Clien	ts	2
AAA Client Host	name 🛛 AAA Client II	Address	Authenti	icate Using
nsite	172.18.141.40		RADIUS (C	lisco IOS/PIX)
(	Add E	ntry		
The commont could			1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	110
Configuration:Se	iguration has been ci ervice Control'' to ad	opt the ne	estart ACS in w settings.	a ~System
Configuration:So	iguration has been ci ervice Control'' to ad	opt the ne	estart ACS in w settings.	n ~System
Configuration:So	AAA Server IP Addres	AAA Server	estart ACS in w settings. rs AAA Server	n "System ? Type
AAA Server Name	AAA Server IP Addres	AAA Server	estart ACS in w settings. rs AAA Server ire ACS for Wi	n "System ? Type indows 2000/NT
AAA Server Name	AAA Server IP Addres	AAA Server CiscoSect	estart ACS in w settings. rs AAA Server ire ACS for We	Type
Configuration:So AAA Server Name jazib-pc	AAA Server IP Addres 172.18.124.96 Add E Proxy Distribut	AAA Server CiscoSect ntry	estart ACS in w settings. rs AAA Server ire ACS for Wi	n "System ? Type indows 2000/NT
AAA Server Name	AAA Server IP Addres Add E Proxy Distribut String AAA	AAA Server CiscoSect ntry	estart ACS in w settings. rs AAA Server ire ACS for Wi	Type indows 2000/NT

2. "Add AAA Client(AAA 클라이언트 추가)" 화면에서 적절한 값을 입력하여 Concentrator를 RADIUS Client(RADIUS 클라이언트)로 추가한 다음 Submit + Restart(제출 + 재시작)를 클릭 합니다.아래 예에서는 다음 값을 사용합니다. AAA Client Hostname = 133\_3000\_conc

AAA Client IP Address = 172.18.124.133

Key = cisco123

CISCO SYSTEMS	Network Configuration				
	Edit				
User Setup					
Group Setup		Add AAA Client			
Shared Profile Components	AAA Client Hostname	133_3000_conc			
Network Configuration	AAA Client TP Address	172.18.124.133			
System Configuration		<b>X</b>			
Configuration	Key	cisco123			
Administration Control	Authenticate Using	RADIUS (Cisco VPN 3000) 📃			
External User Databases	Single Connect TACACS+ A	LAA Client (Record stop in accounting on failure).			
Reports and Activity	Log Update/Watchdog Pack	ets from this AAA Client			
Online Documentation	Log KADIOS Tulliellig Facs	Cets II offi tills AAA Ciletii			
	Submi	it Submit + Restart Cancel			
3000 Concentra	_ ator에 대한 항목이 "AAA Cli	ents" 섹션 아래에 표시됩니다			

CISCO SYSTEMS	Network Configuration	n	
	Select		
User Setup	<b>%</b>	AAA Clie	ents 🤰
an I Shared Drofile	AAA Client Hostname	AAA Client IP Address	Authenticate Using
Components	133 3000 conc	172.18.124.133	RADIUS (Cisco VPN 3000)
Network Configuration	nsite	172.18.141.40	RADIUS (Cisco IOS/PIX)
System Configuration		Add Entry	

## <u>NT 도메인 인증을 위한 알 수 없는 사용자 정책 구성</u>

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



CISCO SYSTEMS E)	kternal User Databases	
User Setup	ect	
Group Setup	External User Database Configuration	?
Shared Profile Components	Choose which external user database type to configure.	
Network Configuration	NIS/NIS+	
System	LEAP Proxy RADIUS Server	
Con i con i gar actor	Windows NT/2000	
Configuration	Novell NDS	
Administration	Generic LDAP	
Control	External ODBC Database	
Databases	RADIUS Token Server	
Reports and	AXENT Token Server	
Activity	CRYPTOCard Token Server	
Online Documentation	Sate Word Token Server	
	SDI Securiti Token Server	
	List all database configurations	
	Cancel	

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

CISCO SYSTEMS	External User Databases
IllinIllin	Edit
User Setup	
Group Setup	Database Configuration Creation
Shared Profile Components	Click here to create a new configuration for the Windows NT/2000 database.
Network Configuration	Create New Configuration
Interface Configuration	
Administration Control	Cancel

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

.



5. Configure를 클릭하여 사용자 인증을 위한 도메인 이름을 구성합니다

CISCO SYSTEMS	External User Databases	
	Edit	
Setup	External User Database Configuration	91
Shared Profile Components	Characterial User Database Configuration	
Network Configuration	Configure Delete	
System Configuration		
Configuration		

6. "Available Domains(사용 가능한 도메인)"에서 NT 도메인을 선택한 다음 오른쪽 화살표 단추 를 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



7. 왼쪽 패널에서 **외부 사용자 데이터베이스**를 클릭한 다음 **데이터베이스 그룹 매핑** 링크(이 <u>예</u> 에<u>표시됨</u>)를 클릭합니다. 이전에 구성한 외부 데이터베이스에 대한 항목이 표시되어야 합니 다. 아래 예는 방금 구성한 데이터베이스인 "Radius/NT Password Expiration"에 대한 항목을 보여줍니다

Cisco Systems	External User Databases	
	Select	
User Setup		
Group Setup	Unknown User G	roup Mappings ?
Shared Profile Components	Choose the External User Database for wh	ich you want to configure the group mappings.
Network Configuration	Name	Туре
System Configuration	Radius/NT Password Expiration	Windows NT/2000
Interface Configuration		
Administration Control	Ca	ancel
Databases		

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

CISCO SYSTEMS	External User Databases	
Illin	Edit	
User Setup		
Group Setup		<b>a</b> 1
Shared Profile Components	Domain Configurations	
Network Configuration	DEFAULT	
System Configuration	New configuration	

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

Cisco Systems	External User Databases
- and the and the area of the second se	Edit
User Setup	
Group Setup	Define New Domain Configuration
Shared Profile Components	JAZIB-ADS
Network Configuration	
System Configuration	Detected Domains:
Configuration	
Administration Control	Domain :
Databases	
Reports and Activity	Submit Cancel

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

.

CISCO SYSTEMS	External User Databases	
يسال التسسيل التس	Edit	
User Setup		
Group Setup		
Shared Profile Components	Domain Configurations	?
Net work	JAZIB-ADS	
Sustem	<u>\DEFAULT</u>	
Configuration	New configuration	
Configuration		

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

.

CISCO SYSTEMS	External User Databases
antiliturantilitura.	Edit
Setup	
Group Setup	Group Mappings for Domain : JAZIB-ADS
Shared Profile Components	NT groups CiscoSecure group
Network Configuration	- no mappings defined -
System Configuration	
Configuration	Add mapping
Administration Control	Delus Castanation
External User Databases	Delete Configuration

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

CISCO SYSTEMS	External User Databases
IllinIllin	Edit
User Setup	
Group Setup	Create new group mapping for Domain : JAZIB-ADS
Shared Profile Components	Define NT group set
Network Configuration	NT Groups
- I consideration	Administrators
System Configuration	Backup Operators
	Replicator Server Operators
Configuration	Account Operators
Administration	
Control	Add to selected Remove from selected
External User	Selected
	Users
Activity	
man   Online	
Documentation	
	Up Down
	CiscoSecure group: Group 1
	Submit Cancel

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 <u>예에 표시됨</u>). 다음 외부 사용자 데이터베이스 확인 옵션이 선택되었는지 확인합니다. 오른쪽 화살표 단추를 눌러 이 전에 구성된 외부 데이터베이스를 "외부 데이터베이스" 목록에서 "선택한 데이터베이스" 목 록으로 이동합니다



# NT/RADIUS 비밀번호 만료 기능 테스트

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

#### <u>RADIUS 인증 테스트</u>

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

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.



2. 메시지가 표시되면 NT 도메인 사용자 이름과 암호를 입력한 다음 **확인**을 클릭합니다. 아래 예 는 비밀번호로 "cisco123"을 사용하여 NT 도메인 서버에 구성된 사용자 이름 "jfrahim"을 보여 줍니다 Enter a username and password with which to test. Please wait for the operation to complete or timeout.



합니다.

위에 표시된 메시 지 이외의 메시지가 수신되면 컨피그레이션 또는 연결 문제가 발생합니다. 모든 설정이 올바 르게 이루어졌는지 확인하려면 이 문서에 설명된 구성 및 테스트 단계를 반복하십시오. 디바 이스 간의 IP 연결도 확인합니다.

#### RADIUS 프록시를 사용하여 비밀번호 만료 기능을 테스트하는 실제 NT 도메인 인증

1. 사용자가 도메인 서버에 이미 정의되어 있는 경우 다음 로그온 시 암호를 변경하라는 메시지 가 표시되도록 속성을 수정합니다. 사용자 속성 대화 상자의 "계정" 탭으로 이동하여 다음 로 **그온** 시 **사용자가 암호를 변경해야 함** 옵션을 선택한 다음 확인을 클릭합니다

Console Window Hel	p	tory osers and t	soulbrides Dayo belayorscorrout Jayorascorrout (asis)
Action View Eavorites	⇔ ⇒ €	× 🗗 🙆 😫	2000 10 7 40 10
Tree Favorites	Name	Туре	Jazib Frahim Properties
Console Root	Administra Cert Publis disco c. cis DinsUpdat Domain S Domain C Domain C Domain C Domain C Domain Us Domain Us Enterprise Group Poli Group Poli.	User Security Gro Security Gro Security Gro Security Gro Security Gro Security Gro Security Gro Security Gro User User User User User User Security Gro User Security Gro User Security Gro User Security Gro User	Dial-in       Environment       Sessions       Remote control       Terminal Services Profile         General       Address       Account       Profile       Telephones       Organization       Member Of         User logon name:       [frahim       @jazib cisco.com       •         User logon name (pre-Windows 2000):       [JAZIB-ADS\       •       •         JAZIB-ADS\       [frahim       •       •         Logon Hours       Log On To       •       •         Account lis locked out       •       •       •         Account options:       •       •       •       •         User cannot change password at next logon       •       •       •         •       Vser cannot change password       •       •       •         •       Store password using reversible encryption       •       •       •         •       Never       •       •       •       •       •         •       Never       •       •       •       •       •       •         •       OK       Cancel       Apply       •       •       •       •       •       •       •       •       •       •       • <td< th=""></td<>

2. VPN 클라이언트를 시작한 다음 Concentrator에 대한 터널을 설정합니다

Ind	Jser Authentication for lab
9	Enter Username and Password.
	Username:
	ifrahim
	Password:
niti	******
Cor	🗖 Save Password
	Domain:
	JAZIB-ADS
	OK Cancel

3. 사용자 인증 중에 비밀번호를 변경하라는 메시지가 표시됩니다

User Au	Ithentication for lab
٩	Your password expired
New P	'assword:
Confirm	n Password:
	OK Cancel

# <u>관련 정보</u>

- <u>Cisco VPN 3000 Series Concentrator</u>
- IPSec
- Windows & Cisco Secure Access Control Server
- <u>RADIUS</u>
- RFC(Request for Comments)