

Microsoft RADIUS를 사용하여 Cisco VPN 3000 Concentrator 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[Windows 2000 및 Windows 2003에서 RADIUS 서버 설치 및 구성](#)

[RADIUS 서버 설치](#)

[IAS를 사용하여 Microsoft Windows 2000 서버 구성](#)

[IAS를 사용하여 Microsoft Windows 2003 Server 구성](#)

[RADIUS 인증을 위한 Cisco VPN 3000 Concentrator 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[WebVPN 인증 실패](#)

[Active Directory에 대한 사용자 인증 실패](#)

[관련 정보](#)

소개

현재 Microsoft IAS(Internet Authentication Server) 및 Microsoft Commercial Internet System(MCIS 2.0)을 사용할 수 있습니다. Microsoft RADIUS 서버는 주 도메인 컨트롤러의 Active Directory를 사용자 데이터베이스에 사용하기 때문에 편리합니다. 더 이상 별도의 데이터베이스를 유지 관리할 필요가 없습니다. 또한 PPTP(Point-to-Point Tunneling Protocol) VPN 연결을 위한 40비트 및 128비트 암호화를 지원합니다. [Microsoft 체크리스트](#)를 참조하십시오. [자세한 내용은 전화 접속 및 VPN 액세스 설명서를 위한 IAS를 구성합니다.](#)

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 규칙](#)을 참조하십시오.

[Windows 2000 및 Windows 2003에서 RADIUS 서버 설치 및 구성](#)

[RADIUS 서버 설치](#)

RADIUS 서버(IAS)가 설치되어 있지 않은 경우 설치하려면 다음 단계를 수행하십시오. RADIUS 서버가 이미 설치되어 있는 경우 [구성 단계](#)를 계속 진행합니다.

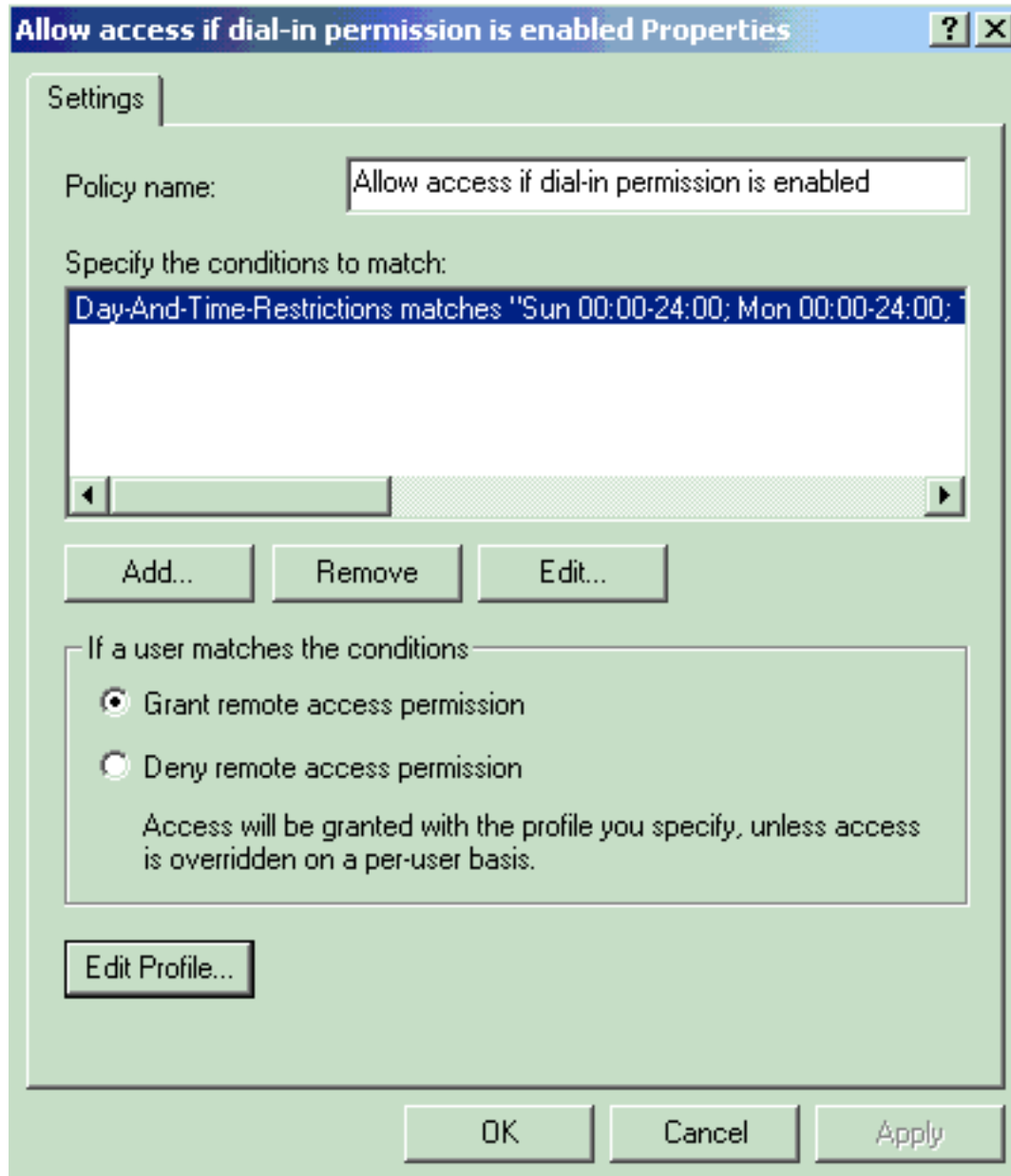
1. Windows Server Compact 디스크를 넣고 설치 프로그램을 시작합니다.
2. Install Add-On Components(추가 기능 구성 요소 설치)를 클릭한 다음 Windows 구성 요소 추가/제거를 클릭합니다.
3. 구성 요소에서 네트워크 서비스(확인란을 선택하거나 선택 취소하지 않음)를 클릭한 다음 세부 정보를 클릭합니다.
4. 인터넷 인증 서비스를 확인하고 확인을 클릭합니다.
5. Next(다음)를 클릭합니다.

[IAS를 사용하여 Microsoft Windows 2000 서버 구성](#)

RADIUS 서버(IAS)를 구성하고 VPN Concentrator에서 사용자를 인증하기 위해 서비스를 시작하려면 다음 단계를 완료하십시오.

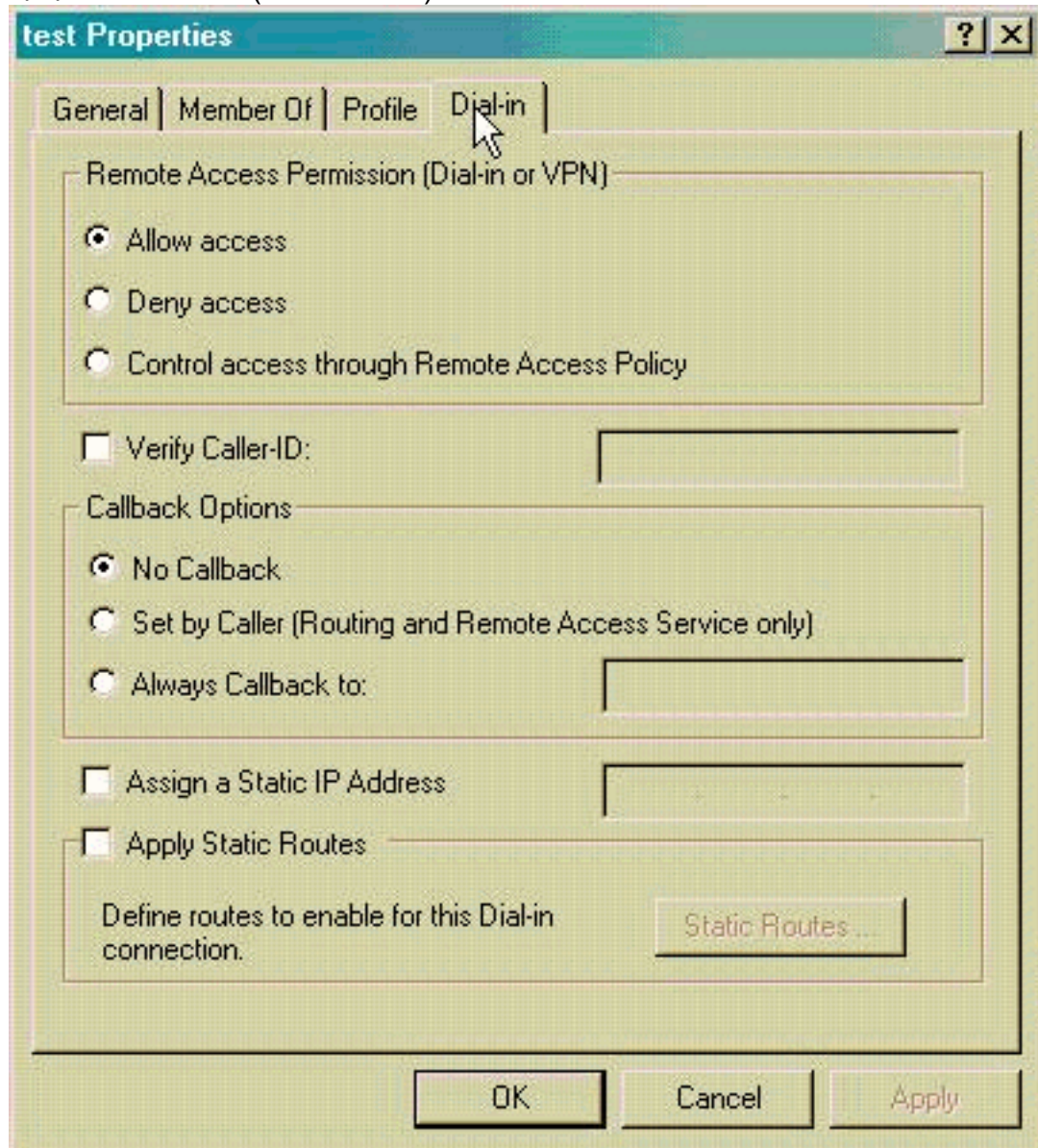
1. 시작 > 프로그램 > 관리 도구 > 인터넷 인증 서비스를 선택합니다.
2. 인터넷 인증 서비스를 마우스 오른쪽 단추로 클릭하고 나타나는 하위 메뉴에서 속성을 클릭합니다.
3. 포트의 설정을 검사하려면 RADIUS 탭으로 이동합니다. RADIUS 인증 및 RADIUS 어카운팅 UDP(User Datagram Protocol) 포트가 Authentication and Accounting에 제공된 기본값(인증의 경우 1812 및 1645, 어카운팅의 경우 1813 및 1646)과 다른 경우 포트 설정을 입력합니다. 완료되면 OK(확인)를 클릭합니다. **참고:** 기본 포트는 변경하지 마십시오. 인증 또는 어카운팅 요청에 여러 포트 설정을 사용하려면 심표로 포트를 구분합니다.
4. VPN Concentrator를 RADIUS 서버(IAS)에 인증, 권한 부여 및 계정 관리(AAA) 클라이언트로 추가하려면 Clients(클라이언트)를 마우스 오른쪽 버튼으로 클릭하고 **New Client(새 클라이언트)**를 선택합니다. **참고:** 두 Cisco VPN 3000 Concentrator 간에 이중화가 구성된 경우 백업 Cisco VPN 3000 Concentrator도 RADIUS 클라이언트로 RADIUS 서버에 추가해야 합니다.
5. 이름을 입력하고 Protocol **Radius**로 선택합니다.
6. 다음 창에서 IP 주소 또는 DNS 이름으로 VPN Concentrator를 정의합니다.
7. Client-Vendor 스크롤 막대에서 Cisco를 선택합니다.
8. 공유 암호를 입력합니다. **참고:** 사용하는 정확한 비밀을 기억해야 합니다. VPN Concentrator를 구성하려면 이 정보가 필요합니다.
9. 마침을 클릭합니다.
10. **Remote Access Policies(원격 액세스 정책)**를 두 번 클릭하고 창 오른쪽에 나타나는 정책을 두 번 클릭합니다. **참고:** IAS를 설치한 후 원격 액세스 정책이 이미 존재해야 합니다. Windows 2000에서는 사용자 계정 및 원격 액세스 정책의 다이얼 인 속성을 기반으로 권한 부여가 부여됩니다. 원격 액세스 정책은 네트워크 관리자가 연결 시도를 보다 유연하게 승인할 수 있도록 하는 조건 및 연결 설정 집합입니다. Windows 2000 라우팅 및 원격 액세스 서비스와 Windows 2000 IAS는 모두 원격 액세스 정책을 사용하여 연결 시도를 허용할지 거부할지를 결정합니다. 두 경우 모두 원격 액세스 정책이 로컬에 저장됩니다. 연결 시도가 처리되는 방

법에 대한 자세한 내용은 Windows 2000 IAS 설명서를 참조하십시오



11. 전화 접속 접속 속성을 구성하려면 원격 액세스 권한 부여를 선택하고 프로파일 편집을 클릭합니다.
12. Authentication(인증) 탭에서 인증에 사용할 프로토콜을 선택합니다. Microsoft **Encrypted Authentication version 2**를 선택하고 다른 모든 인증 프로토콜을 선택 취소합니다.참고: 이 다이얼인 프로파일의 설정은 VPN 3000 Concentrator 컨피그레이션 및 다이얼인 클라이언트의 설정과 일치해야 합니다. 이 예에서는 PPTP 암호화 없는 MS-CHAPv2 인증이 사용됩니다.
13. Encryption(암호화) 탭에서 **No Encryption only**(암호화만 없음)를 선택합니다.
14. 확인을 클릭하여 전화 접속 프로필을 담은 다음 확인을 클릭하여 원격 액세스 정책 창을 닫습니다.
15. 인터넷 인증 서비스를 마우스 오른쪽 단추로 클릭하고 콘솔 트리에서 서비스 시작을 클릭합니다.참고: 이 기능을 사용하여 서비스를 중지할 수도 있습니다.
16. 연결을 허용하도록 사용자를 수정하려면 다음 단계를 완료하십시오.[콘솔] > [스냅인 추가/제거]를 선택합니다.Add(추가)를 클릭하고 Local Users and Groups(로컬 사용자 및 그룹) 스냅인을 선택합니다.Add(추가)를 클릭합니다.로컬 컴퓨터를 선택해야 합니다.Finish(마침)를 클릭하고 OK(확인)를 클릭합니다.
17. Local User and Groups(로컬 사용자 및 그룹)를 확장하고 왼쪽 창에서 Users(사용자) 폴더를 클릭합니다. 오른쪽 창에서 액세스를 허용할 사용자(VPN 사용자)를 두 번 클릭합니다.

18. Dial-in 탭으로 이동하여 Allow Access **Access**(원격 액세스 권한)(전화 접속 또는 VPN) 아래에서 Allow Access(액세스 허용)를 선택합니다



19. 적용 및 **확인**을 클릭하여 작업을 완료합니다. 필요한 경우 콘솔 관리 창을 닫고 세션을 저장할 수 있습니다. 수정한 사용자가 이제 VPN 클라이언트를 사용하여 VPN Concentrator에 액세스할 수 있습니다. IAS 서버는 사용자 정보만 인증합니다. VPN Concentrator는 여전히 그룹 인증을 수행합니다.

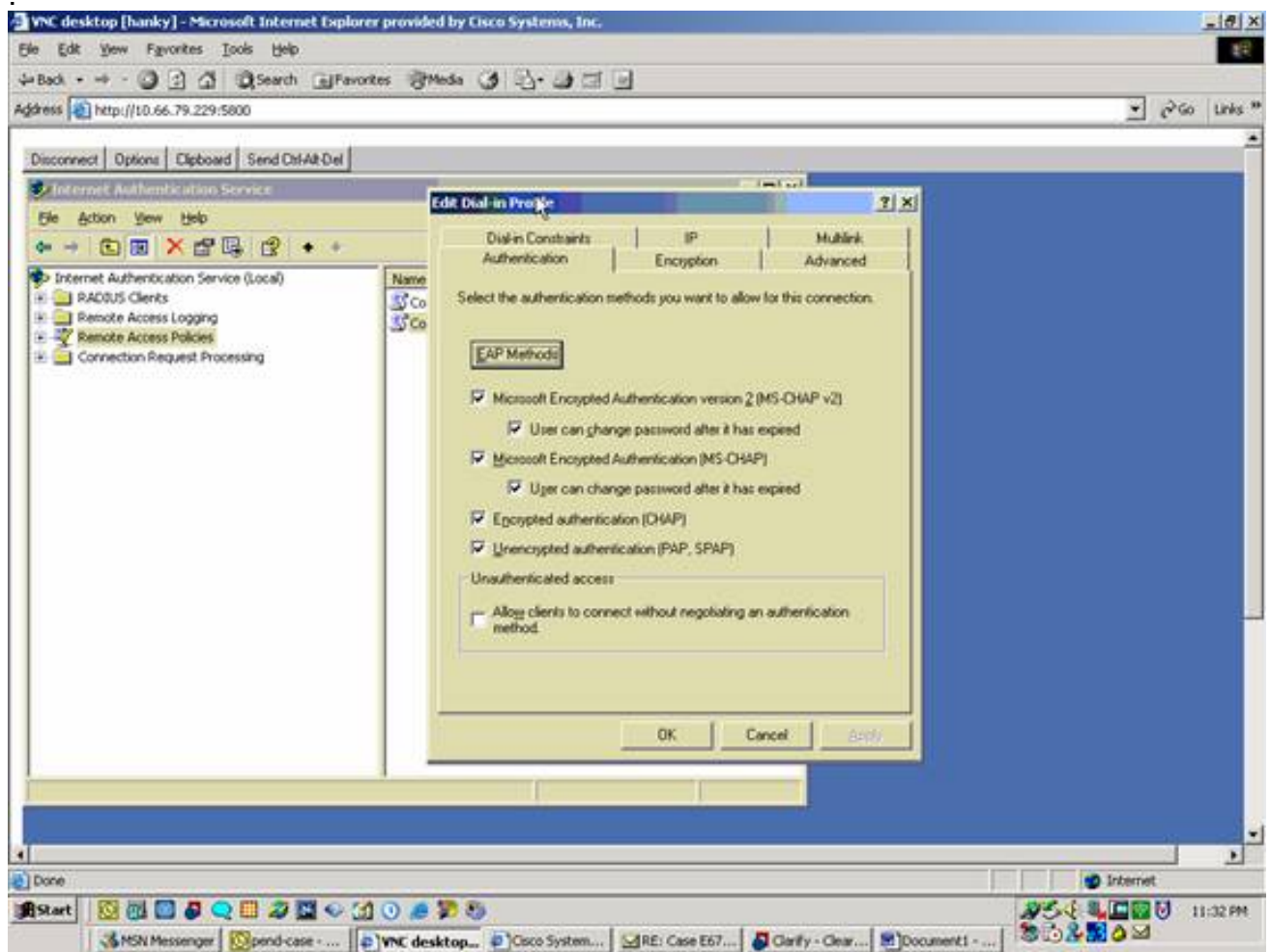
[IAS를 사용하여 Microsoft Windows 2003 Server 구성](#)

Microsoft Windows 2003 서버를 IAS로 구성하려면 다음 단계를 완료하십시오.

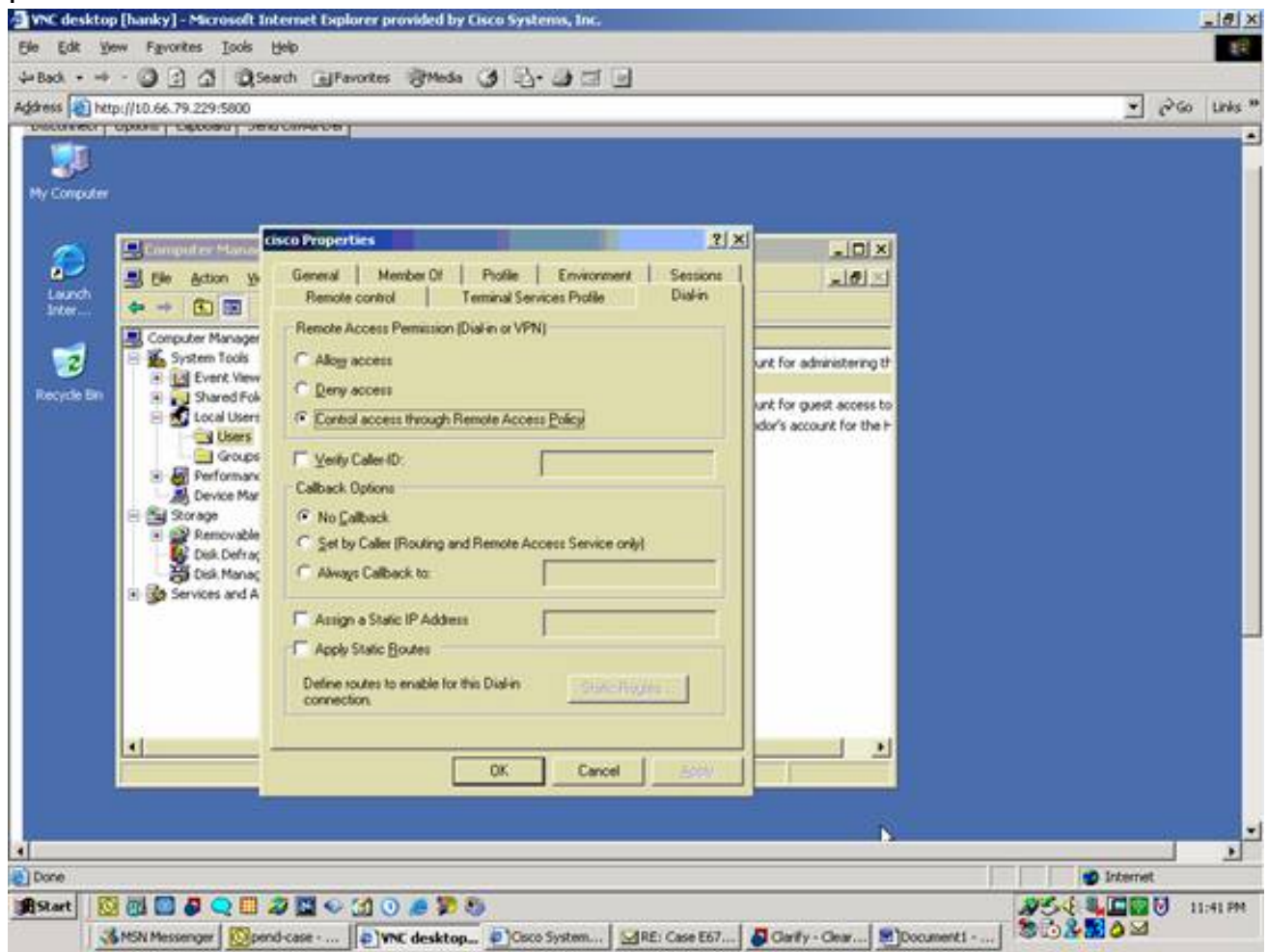
참고: 이 단계에서는 IAS가 로컬 시스템에 이미 설치되어 있다고 가정합니다. 그렇지 않은 경우 제어판 > 프로그램 추가/제거를 통해 추가합니다.

1. Administrative Tools(관리 툴) > Internet Authentication Service(인터넷 인증 서비스)를 선택하고 마우스 오른쪽 버튼으로 RADIUS Client(RADIUS 클라이언트)를 클릭하여 새 RADIUS 클라이언트를 추가합니다. 클라이언트 정보를 입력한 후 OK를 클릭합니다.
2. 이름을 입력합니다.
3. 다음 창에서 IP 주소 또는 DNS 이름으로 VPN Concentrator를 정의합니다.
4. Client-Vendor 스크롤 막대에서 Cisco를 선택합니다.

5. 공유 암호를 입력합니다.**참고:** 사용하는 정확한 비밀을 기억해야 합니다. VPN Concentrator를 구성하려면 이 정보가 필요합니다.
6. OK(확인)를 클릭하여 완료합니다.
7. Remote Access Policies(원격 액세스 정책)로 이동하여 Connections to Other Access Servers(다른 액세스 서버에 대한 연결)를 마우스 오른쪽 버튼으로 클릭하고 Properties(속성)를 선택합니다.
8. 전화 접속 접속 속성을 구성하려면 원격 액세스 권한 부여를 선택하고 프로파일 편집을 클릭합니다.
9. Authentication(인증) 탭에서 인증에 사용할 프로토콜을 선택합니다. Microsoft Encrypted Authentication version 2를 선택하고 다른 모든 인증 프로토콜을 선택 취소합니다.**참고:** 이 다이얼인 프로파일의 설정은 VPN 3000 Concentrator 컨피그레이션 및 다이얼인 클라이언트의 설정과 일치해야 합니다. 이 예에서는 PPTP 암호화 없는 MS-CHAPv2 인증이 사용됩니다.
10. Encryption(암호화) 탭에서 No Encryption only(암호화만 없음)를 선택합니다.
11. 완료되면 OK(확인)를 클릭합니다



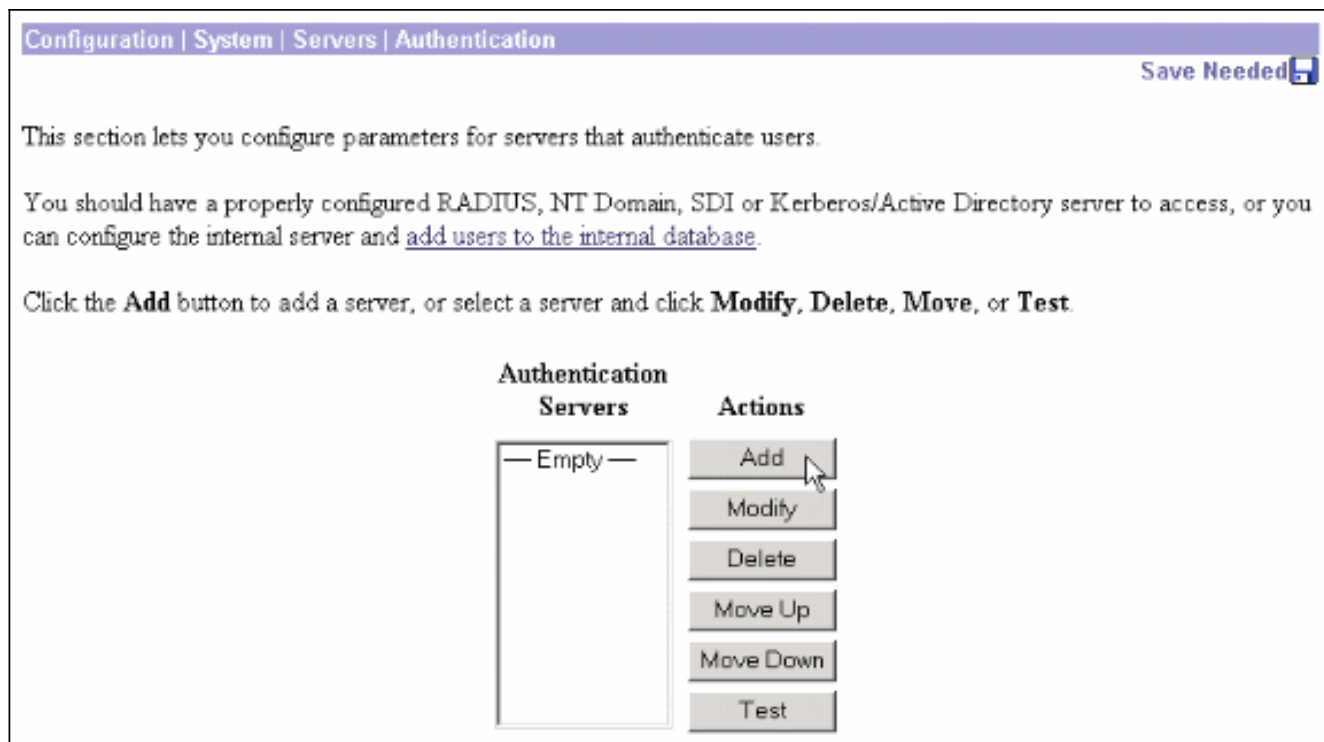
12. 인터넷 인증 서비스를 마우스 오른쪽 단추로 클릭하고 콘솔 트리에서 서비스 시작을 클릭합니다.**참고:** 이 기능을 사용하여 서비스를 중지할 수도 있습니다.
13. 관리 도구 > 컴퓨터 관리 > 시스템 도구 > 로컬 사용자 및 그룹을 선택하고 사용자를 마우스 오른쪽 단추로 클릭한 다음 새 사용자를 선택하여 로컬 컴퓨터 계정에 사용자를 추가합니다.
14. Cisco 비밀번호 "vpnpassword"가 있는 사용자를 추가하고 이 프로파일 정보를 확인합니다. General(일반) 탭에서 User Must Change Password(사용자가 비밀번호를 변경해야 함) 옵션 대신 Password Never Expired(비밀번호 만료되지 않음) 옵션이 선택되어 있는지 확인합니다. Dial-in 탭에서 Allow access(액세스 허용) 옵션을 선택하거나 Control access access through Remote Access Policy(원격 액세스 정책을 통한 제어 액세스)의 기본 설정을 그대로 둡니다. 완료되면 OK(확인)를 클릭합니다



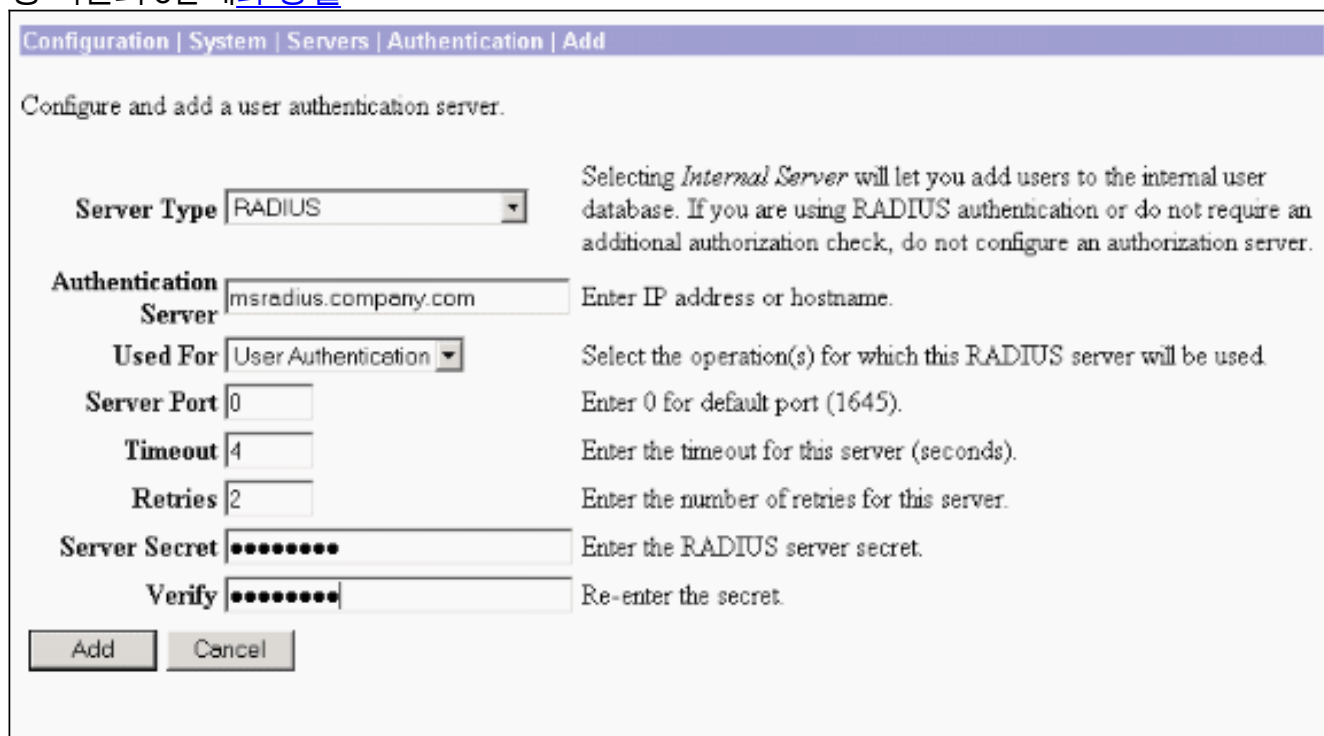
RADIUS 인증을 위한 Cisco VPN 3000 Concentrator 구성

RADIUS 인증을 위해 Cisco VPN 3000 Concentrator를 구성하려면 다음 단계를 완료합니다.

1. 웹 브라우저를 사용하여 VPN Concentrator에 연결하고 왼쪽 프레임 메뉴에서 **Configuration > System > Servers > Authentication**을 선택합니다



2. Add(추가)를 클릭하고 이 설정을 구성합니다. 서버 유형 = RADIUS인증 서버 = RADIUS 서버 (IAS)의 IP 주소 또는 호스트 이름 서버 포트 = 0(0=default=1645)서버 암호 = RADIUS 서버 구성 섹션의 8단계와 동일



3. 실행 중인 컨피그레이션에 변경 사항을 추가하려면 **Add**를 클릭합니다.
4. Add(추가)를 클릭하고 **Internal Server** for Server Type(서버 유형에 대한 내부 서버)을 선택한 다음 Apply(적용)를 클릭합니다.IPsec 그룹을 구성하려면 나중에 필요합니다(Server Type = Internal Server만 필요).

Configuration | System | Servers | Authentication | Add

Configure and add a user authentication server.

Server Type Selecting *Internal Server* will let you add users to the internal user database.


5. PPTP 사용자 또는 VPN 클라이언트 사용자를 위한 VPN Concentrator를 구성합니다 .PPTPPPTP 사용자를 위해 구성하려면 다음 단계를 완료합니다.Configuration > **User Management > Base Group**을 선택하고 PPTP/L2TP 탭을 클릭합니다.MSCHAPv2를 선택하고 PPTP Authentication Protocols 섹션에서 다른 인증 프로토콜을 선택 취소합니다

Configuration | User Management | Base Group

General | IPsec | Client Config | Client FW | HW Client | **PPTP/L2TP** | WebVPN | NAC

PPTP/L2TP Parameters		
Attribute	Value	Description
Use Client Address	<input type="checkbox"/>	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MSCHAPv1 <input checked="" type="checkbox"/> MSCHAPv2 <input type="checkbox"/> EAP Proxy	Check the authentication protocols allowed. Refer to the online help for authentication protocol dependencies. Unchecking all options means that no authentication is required.
PPTP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	Select the allowed encryption methods for PPTP connections for this group.
PPTP Compression	<input type="checkbox"/>	Check to enable MPPC compression for PPTP connections for this group.
L2TP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2 <input type="checkbox"/> EAP Proxy	Check the authentication protocols allowed. Refer to the online help for authentication protocol dependencies. Unchecking all options means that no authentication is required.
L2TP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	Select the allowed encryption methods for L2TP connections for this group.
L2TP Compression	<input type="checkbox"/>	Check to enable MPPC compression for L2TP connections for this group.

실행 중인 컨피그레이션에 변경 사항을 추가하려면 페이지 하단의 **Apply**를 클릭합니다.이제 PPTP 사용자가 연결되면 RADIUS 서버(IAS)에서 인증됩니다.VPN 클라이언트VPN 클라이언트 사용자에게 대해 구성하려면 다음 단계를 완료합니다.Configuration > **User Management > Groups**를 선택하고 **Add**를 클릭하여 새 그룹을 추가합니다

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, select a group and click the appropriate button.

Actions

Add Group

Modify Group

Delete Group

Current Groups

— Empty —

Modify

Authentication Servers

Authorization Servers

Accounting Servers

Address Pools

Client Update

Bandwidth Assignment

WebVPN Servers and URLs

WebVPN Port Forwarding

그룹 이름(예: IPsecUsers) 및 비밀번호를 입력합니다

Configuration | User Management | Groups | Add

This section lets you add a group. 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 | Client Config | Client FW | HW Client | PPTP/L2TP | WebVPN | NAC

Identity Parameters

Attribute	Value	Description
Group Name	IPSecUsers	Enter a unique name for the group.
Password	●●●●●●●●	Enter the password for the group.
Verify	●●●●●●●●	Verify the group's password.
Type	Internal ▾	<i>External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database.</i>

Add Cancel

이 비밀번호는 터널 협상을 위한 사전 공유 키로 사용됩니다. IPsec 탭으로 이동하여 Authentication(인증)을 RADIUS로 설정합니다

Configuration Administration Monitoring			
			below as needed.
Remote Access Parameters			
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Lock users into this group.
Authentication	RADIUS	<input type="checkbox"/>	Select the authentication method for members of this group. This parameter does not apply to Individual User Authentication .
Authorization Type	None	<input checked="" type="checkbox"/>	If members of this group need authorization in addition to authentication, select an authorization method. If you configure this field, you must also configure an Authorization Server.
Authorization Required	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to require successful authorization.
DN Field	CN otherwise OU	<input checked="" type="checkbox"/>	For certificate-based users, select the subject Distinguished Name (DN) field that is used as the username. This field is used for user Authorization.
IPComp	None	<input checked="" type="checkbox"/>	Select the method of IP Compression for members of this group.
Reauthentication on Rekey	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to reauthenticate the user on an IKE (Phase-1) rekey.
			Permit or deny VPN Clients according to

이렇게 하면 RADIUS 인증 서버를 통해 IPsec 클라이언트를 인증할 수 있습니다. 실행 중인 컨피그레이션에 변경 사항을 추가하려면 페이지 하단의 **Add**를 클릭합니다. 이제 IPsec 클라이언트가 연결하고 구성한 그룹을 사용할 때 RADIUS 서버에서 인증됩니다.

다음을 확인합니다.

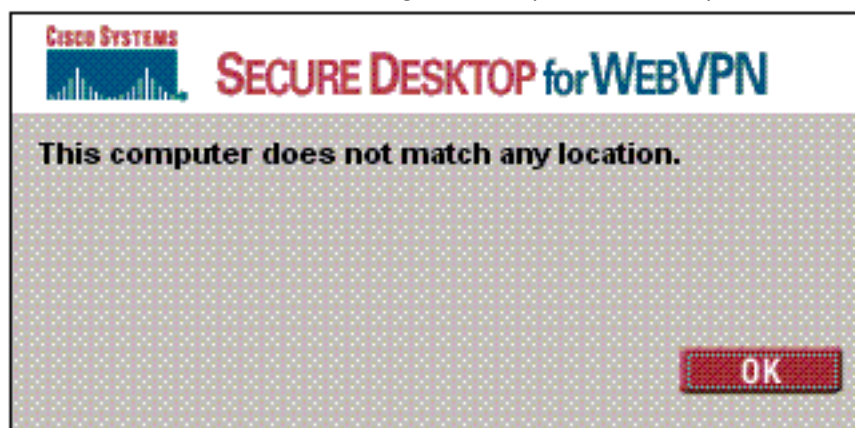
현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

WebVPN 인증 실패

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

- **문제/장애:** WebVPN 사용자는 RADIUS 서버에 대해 인증할 수 없지만 VPN Concentrator의 로컬 데이터베이스를 사용하여 인증할 수 있습니다. "Login failed(로그인 실패)" 및 이 메시지와



같은 오류가 표시됩니다.

원인: 이러한 문제는 Concentrator의 내부 데이터베이스 이외의 데이터베이스를 사용할 때 종종 발생합

니다. WebVPN 사용자는 처음 Concentrator에 연결할 때 Base Group을 누르고 기본 인증 방법을 사용해야 합니다. 대개 이 방법은 Concentrator의 내부 데이터베이스로 설정되며 구성된 RADIUS 또는 다른 서버가 아닙니다. **해결책:** WebVPN 사용자가 인증하면 Concentrator는 Configuration(컨피그레이션) > System(시스템) > Servers(서버) > **Authentication(인증)**에서 정의된 서버 목록을 확인하고 상위 서버를 사용합니다. WebVPN 사용자가 인증할 서버를 이 목록의 맨 위로 이동해야 합니다. 예를 들어 RADIUS가 인증 방법이어야 하는 경우 RADIUS 서버를 목록의 맨 위로 이동하여 인증을 푸시해야 합니다. **참고:** WebVPN 사용자가 처음 Base Group에 도달했다고 해서 Base Group에 국한되는 것은 아닙니다. Concentrator에서 추가 WebVPN 그룹을 구성할 수 있으며, 사용자는 RADIUS 서버에서 **OU=groupname**의 특성 25를 사용하여 할당할 수 있습니다. 자세한 내용은 [내용은 RADIUS 서버를 사용하여 VPN 3000 Concentrator 그룹에 사용자](#) 잠금을 참조하십시오.

[Active Directory에 대한 사용자 인증 실패](#)

Active Directory 서버의 User Properties(사용자 속성)의 Account(계정) 탭에서 다음 확인란을 볼 수 있습니다.

사전 인증 필요 없음

이 확인란을 선택하지 않은 경우 **선택한** 후 이 사용자로 다시 인증해 보십시오.

[관련 정보](#)

- [Cisco VPN 3000 Series Concentrator](#)
- [Cisco VPN 3002 하드웨어 클라이언트](#)
- [IPSec 협상/IKE 프로토콜](#)
- [RADIUS\(Remote Authentication Dial-In User Service\) 지원 페이지](#)
- [원격 인증 전화 접속 사용자 서비스\(RADIUS\)](#)
- [기술 지원 및 문서 - Cisco Systems](#)