

De Cisco VPN 3000 Concentrator met Microsoft RADIUS configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[De RADIUS-server op Windows 2000 en Windows 2003 installeren en configureren](#)

[Installeer de RADIUS-server](#)

[De Microsoft Windows 2000 Server configureren met IAS](#)

[De Microsoft Windows 2003-server configureren met IAS](#)

[Configuratie van Cisco VPN 3000 Concentrator voor RADIUS-verificatie](#)

[Verifiëren](#)

[Problemen oplossen](#)

[WebVPN-verificatiemislukkingen](#)

[Gebruikersverificatie faalt tegen de actieve map](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Microsoft Internet Authentication Server (IAS) en Microsoft Commercial Internet System (MCIS 2.0) zijn momenteel beschikbaar. De Microsoft RADIUS-server is handig omdat deze de actieve map op de primaire controller van het domein gebruikt voor de gebruikersdatabase. U hoeft geen aparte database meer te onderhouden. Het ondersteunt ook 40-bits en 128-bits codering voor Point-to-Point Tunneling Protocol (PPTP) VPN-verbindingen. Raadpleeg de [Microsoft-controlelijst: Het configureren van IAS voor inbeldocumentatie en](#) documentatie over [VPN-toegang](#) voor meer informatie.

[Voorwaarden](#)

[Vereisten](#)

Er zijn geen specifieke vereisten van toepassing op dit document.

[Gebruikte componenten](#)

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

Raadpleeg de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

De RADIUS-server op Windows 2000 en Windows 2003 installeren en configureren

Installeer de RADIUS-server

Als de RADIUS-server (IAS) niet al is geïnstalleerd, voert u deze stappen uit om te installeren. Als de RADIUS-server al geïnstalleerd is, volg de [configuratiestappen](#).

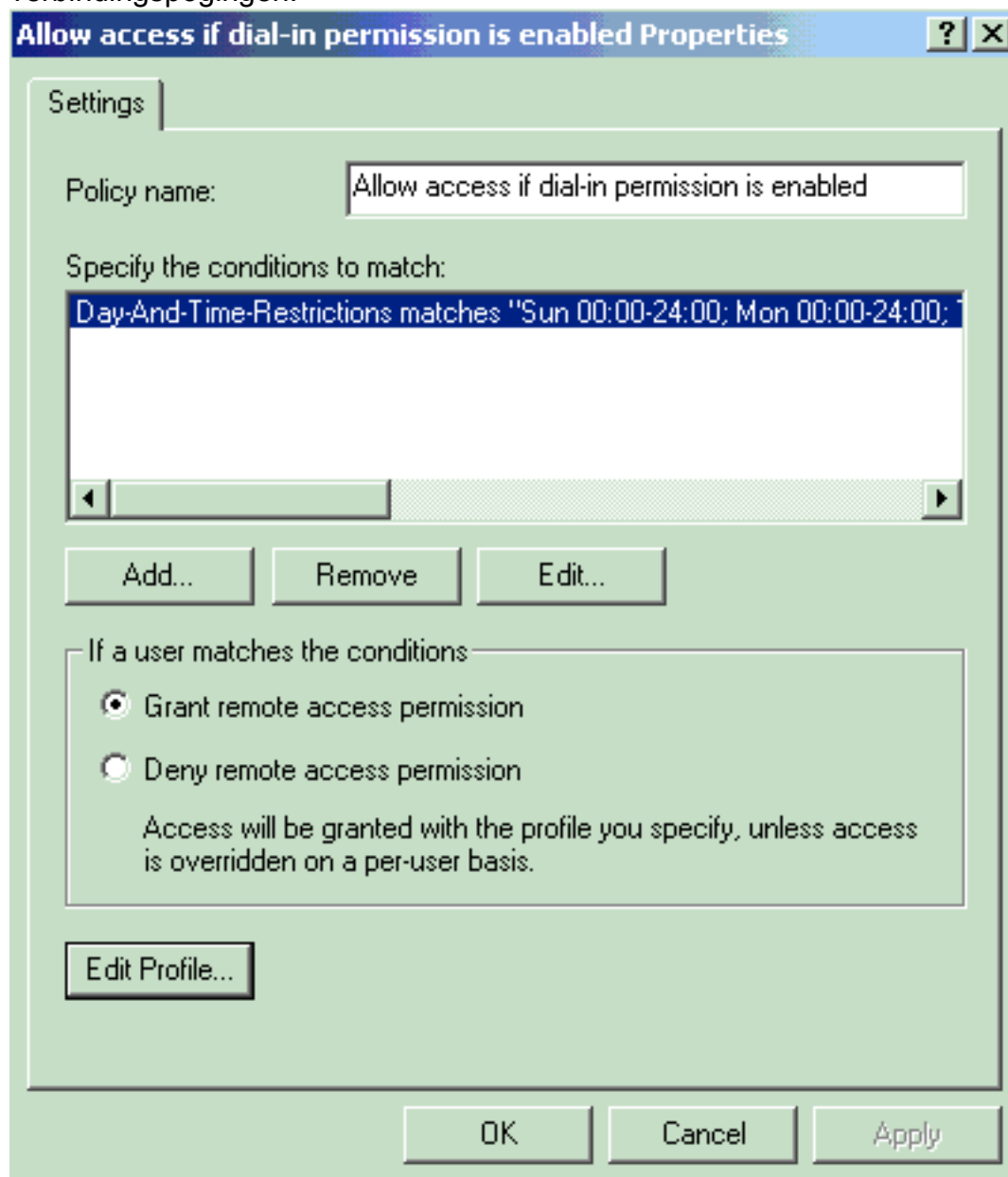
1. Plaats de compacte schijf van Windows Server en start het setup-programma.
2. Klik op **Add-on Componenten installeren** en vervolgens op **Add/Remove Windows Componenten**.
3. In Componenten klikt u op **Netwerkservices** (maar selecteert of deselecteert u het aankruisvakje niet) en vervolgens klikt u op **Details**.
4. Controleer **Internet Verificatieservice** en klik op **OK**.
5. Klik op **Volgende**.

De Microsoft Windows 2000 Server configureren met IAS

Voltooi deze stappen om de RADIUS-server (IAS) te configureren en de service te starten om deze beschikbaar te maken voor authenticatie van gebruikers in de VPN-centrator.

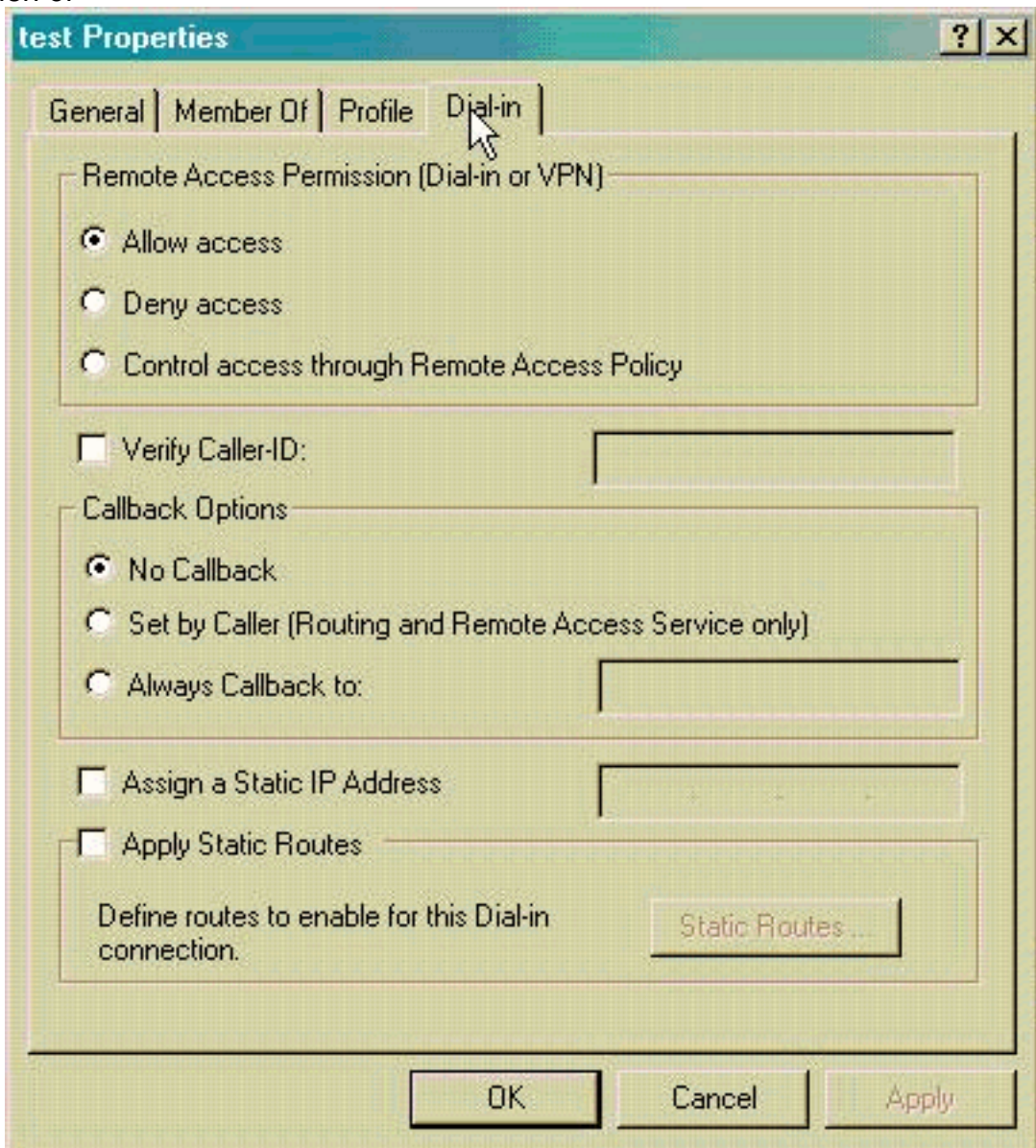
1. Kies **Start > Programma's > Administratieve hulpmiddelen > Internet-verificatieservice**.
2. Klik met de rechtermuisknop op **Internet Verificatieservice** en klik op **Eigenschappen** in het submenu dat verschijnt.
3. Ga naar het tabblad RADIUS om de instellingen voor poorten te onderzoeken. Als uw RADIUS-verificatie en RADIUS-accounting User Datagram Protocol (UDP)-poorten verschillen van de standaardwaarden die zijn opgegeven (1812 en 1645 voor verificatie, 1813 en 1646 voor accounting) in verificatie en accounting, typt u uw poortinstellingen. Klik op **OK** wanneer u klaar bent. **Opmerking:** wijzig de standaardpoorten niet. Scheid de havens door komma's te gebruiken om meerdere haveninstellingen voor authenticatie of boekhoudingsverzoeken te gebruiken.
4. Klik met de rechtermuisknop op **Clients** en kies **Nieuwe client** om de VPN-Concentrator toe te voegen als een verificatie-, autorisatie- en accounting-client (AAA) aan de RADIUS-server (IAS). **Opmerking:** Als redundantie is ingesteld tussen twee Cisco VPN 3000 Concentrators, moet de reservekopie Cisco VPN 3000 Concentrator ook aan de RADIUS-server als een RADIUS-client worden toegevoegd.
5. Voer een vriendelijke naam in en selecteer deze als **protocolstraal**.
6. Defineert de VPN-centrator met een IP-adres of een DNS-naam in het volgende venster.
7. Kies **Cisco** in de schuifbalk tussen client en verkoper.
8. Voer een gedeeld geheim in. **Opmerking:** Je moet het *exacte* geheim onthouden dat je gebruikt. U hebt deze informatie nodig om de VPN-centrator te configureren.
9. Klik op **Voltoeien**.
10. Dubbelklik op **Afstandstoegangsbeleid** en dubbelklik op het beleid dat in de rechterkant van

het venster verschijnt. **Opmerking:** Nadat u IAS hebt geïnstalleerd, dient er al een toegangsbeleid op afstand te bestaan. In Windows 2000 wordt de vergunning verleend op basis van de inbelegenschappen van een gebruikersaccount en het beleid voor externe toegang. Afstandstoegangsbeleid is een reeks voorwaarden en verbindinginstellingen die netwerkbeheerders meer flexibiliteit geven bij het autoriseren van verbindingsoogingen. De Windows 2000 Routing- en Remote Access-service en de Windows 2000-IAS gebruiken allebei toegangsbeleid op afstand om te bepalen of u pogingen tot een verbinding accepteert of afwijst. In beide gevallen wordt het toegangsbeleid op afstand lokaal opgeslagen. Raadpleeg de Windows 2000 IAS-documentatie voor meer informatie over de verwerking van verbindingsoogingen.



11. Kies de toegangstoestemming op afstand verlenen en klik op **Profiel bewerken** om de inbelegenschappen te configureren.
12. Selecteer het protocol dat moet worden gebruikt voor verificatie op het tabblad Verificatie. Controleer **Microsoft Encrypted Authentication versie 2** en controleer alle andere verificatieprotocollen. **Opmerking:** Instellingen in dit inbelprofiel moeten overeenkomen met de instellingen in de VPN 3000 Concentrator-configuratie en inbelclient. In dit voorbeeld wordt MS-CHAPv2-verificatie zonder PPTP-encryptie gebruikt.

13. Controleer alleen op het tabblad Encryptie **geen encryptie**.
14. Klik op **OK** om het inbelprofiel te sluiten en vervolgens op **OK** te klikken om het venster voor toegang op afstand te sluiten.
15. Klik met de rechtermuisknop op **de Internet Verificatieservice** en klik op **Start Service** in de console-boom.**N.B.:** U kunt deze functie ook gebruiken om de service te stoppen.
16. Voltooi deze stappen om de gebruikers te wijzigen, zodat ze een verbinding kunnen maken.Kies **console > Magnetisch-in toevoegen/verwijderen**.Klik op **Toevoegen** en kies **Lokale gebruikers en groepen die willen inschakelen**.Klik op **Add (Toevoegen)**.Zorg ervoor dat u **lokale computer** selecteertKlik op **Voltoeien** en **OK**.
17. **Local User en Group** uitvouwen en klik op de map **Gebruikers** in het linker deelvenster. Dubbelklik in het rechter venster op de gebruiker (VPN-gebruiker) die u toegang wilt verlenen.
18. Ga naar het tabblad Inbellen en kies **Toegang** toestaan onder vergunning op afstand (inbellen of



VPN).

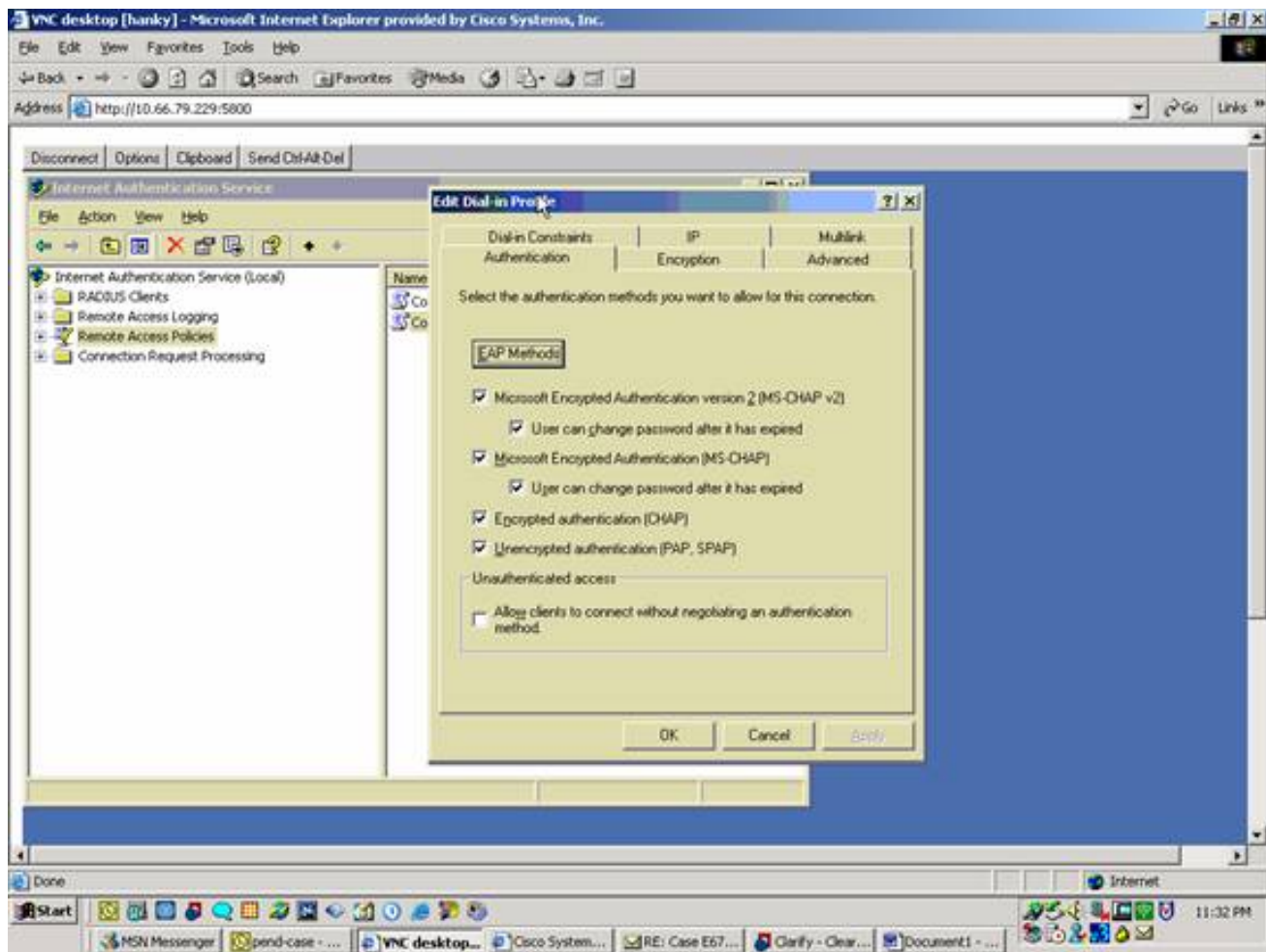
19. Klik op **Toepassen** en **OK** om de actie te voltooien. U kunt het Console Management-venster sluiten en de sessie indien gewenst opslaan.De gebruikers die u hebt aangepast kunnen nu de VPN-centrator met de VPN-client benaderen. Houd in gedachten dat de IAS-server alleen de gebruikersinformatie echt maakt. De VPN Concentrator doet nog steeds de groepsverificatie.

De Microsoft Windows 2003-server configureren met IAS

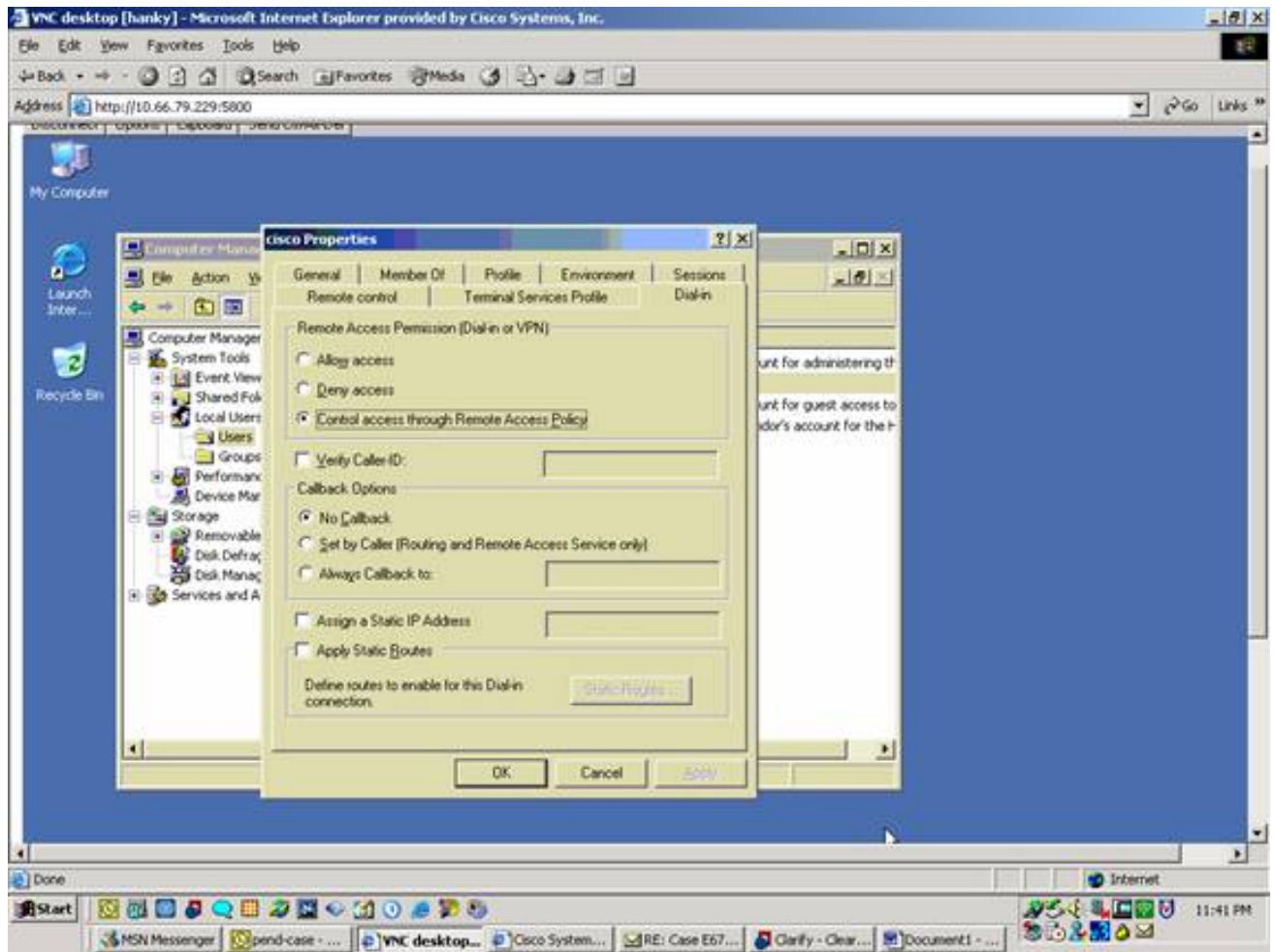
Voltooi deze stappen om de Microsoft Windows 2003-server te configureren met IAS.

Toelichting: In deze stappen wordt ervan uitgegaan dat de IAS reeds op de lokale machine is geïnstalleerd. Als dit niet het geval is, kunt u dit toevoegen via **Configuratiescherm > Software**.

1. Kies **Administratieve Gereedschappen > Internet-verificatieservice** en klik met de rechtermuisknop op **RADIUS-client** om een nieuwe RADIUS-client toe te voegen. Klik nadat u de clientinformatie hebt getypt op **OK**.
2. Voer een vriendelijke naam in.
3. Definieert de VPN-centrator met een IP-adres of een DNS-naam in het volgende venster.
4. Kies **Cisco** in de schuifbalk tussen client en verkoper.
5. Voer een gedeeld geheim in. **Opmerking:** Je moet het *exacte* geheim onthouden dat je gebruikt. U hebt deze informatie nodig om de VPN-centrator te configureren.
6. Klik op **OK** om dit te voltooien.
7. Ga naar **beleid voor externe toegang**, klik met de rechtermuisknop op **Aansluitingen met andere toegangsservers** en kies **Eigenschappen**.
8. Kies **de toegangstoestemming op afstand geven** en klik op **Profiel bewerken** om de inbelegenschappen te configureren.
9. Selecteer het protocol dat moet worden gebruikt voor verificatie op het tabblad Verificatie. Controleer **Microsoft Encrypted Authentication versie 2** en controleer alle andere verificatieprotocollen. **Opmerking:** Instellingen in dit inbelprofiel moeten overeenkomen met de instellingen in de VPN 3000 Concentrator-configuratie en inbelclient. In dit voorbeeld wordt MS-CHAPv2-verificatie zonder PPTP-encryptie gebruikt.
10. Controleer alleen op het tabblad Encryptie **geen encryptie**.
11. Klik op **OK** wanneer u klaar bent.



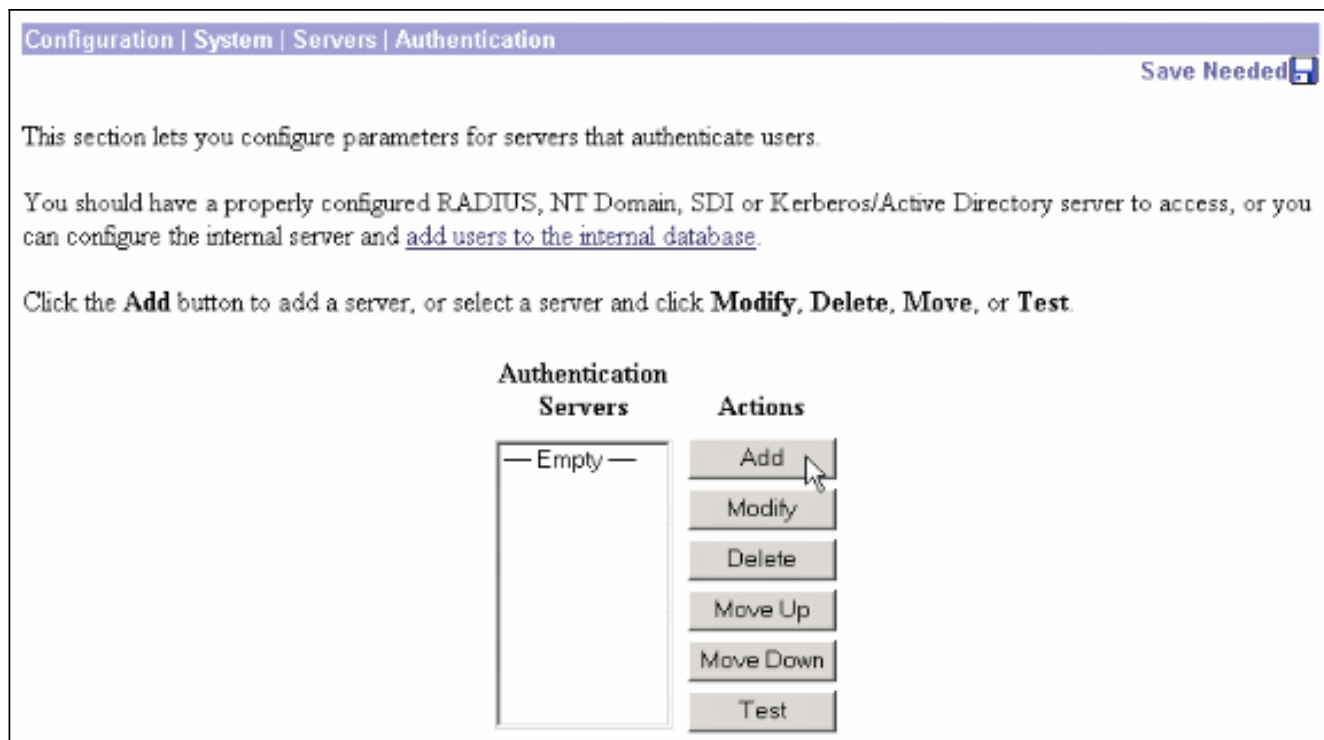
12. Klik met de rechtermuisknop op de **Internet Verificatieservice** en klik op **Start Service** in de console-boom. **N.B.:** U kunt deze functie ook gebruiken om de service te stoppen.
13. Kies **Administratieve tools > Computerbeheer > Systeemtools > Lokale gebruikers en groepen**, klik met de rechtermuisknop op **gebruikers** en kies **Nieuwe gebruikers** om een gebruiker aan de lokale computeraccount toe te voegen.
14. Voeg gebruiker toe met het Cisco-wachtwoord "Wachtwoord" en controleer deze profielinformatie. Zorg er in het tabblad **Algemeen** voor dat de optie voor **Wachtwoord dat nooit is verlopen** is geselecteerd in plaats van de optie voor **Gebruiker moet Wachtwoord wijzigen**. Kies in het tabblad **Inbellen** de optie voor **Toegang toestaan** (of laat standaardinstelling van **Control-toegang via het Afstandsbeleid** toestaan). Klik op **OK** wanneer u klaar bent.



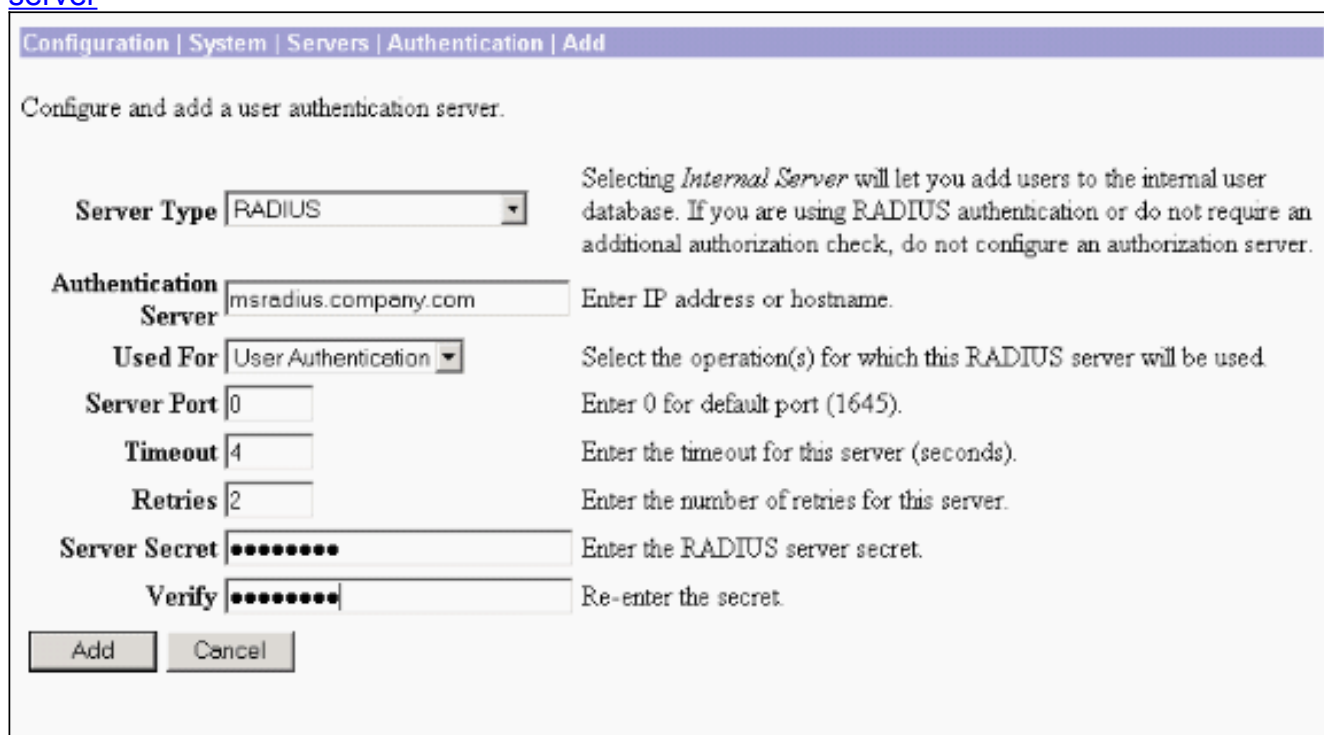
Configuratie van Cisco VPN 3000 Concentrator voor RADIUS-verificatie

Voltooi deze stappen om Cisco VPN 3000 Concentrator voor RADIUS-verificatie te configureren.

1. Sluit aan op de VPN-centrator met uw Web-browser en kies **Configuration > System > Server > Verificatie** in het menu linker frame.



2. Klik op **Add** en stel deze instellingen in. `servertype = RADIUS` Verificatieserver = IP-adres of hostnaam van uw RADIUS-server (IAS) Server poort = 0 (0=standaard=1645) Servergeheim = hetzelfde als in stap 8 in het gedeelte over [het configureren van de RADIUS-server](#)



3. Klik op **Add** om de wijzigingen in de actieve configuratie toe te voegen.
4. Klik op **Add**, kies **Interne Server** voor servertype en klik op **Toepassen**. U hebt dit later nodig om een IPsec Group te kunnen configureren (u hebt alleen servertype = interne server nodig).

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. Configureer de VPN-Concentrator voor PPTP-gebruikers of voor VPN-clientgebruikers. **PPTP**Voltooi deze stappen om ze te configureren voor PPTP-gebruikers. Kies **Configuration > User Management > Base Group** en klik op het tabblad **PPTP/L2TP**. Kies **MSCHAPv2** en verwijder andere authenticatieprotocollen in het gedeelte PPTP-verificatieprotocollen.

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.

Klik op **Toepassen** onder in de pagina om de wijzigingen aan de actieve configuratie toe te voegen. Wanneer PPTP-gebruikers verbinding maken, worden ze geauthentiseerd door de RADIUS-server (IAS). **VPN-client**Voltooi deze stappen om de client te configureren voor VPN-gebruikers. Kies **Configuratie > Gebruikersbeheer > Groepen** en klik op **Toevoegen** om een nieuwe groep toe te voegen.

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	Current Groups	Modify
<input type="button" value="Add Group"/> <input type="button" value="Modify Group"/> <input type="button" value="Delete Group"/>	<div style="border: 1px solid gray; padding: 5px; min-height: 100px;"> — Empty — </div>	<input type="button" value="Authentication Servers"/> <input type="button" value="Authorization Servers"/> <input type="button" value="Accounting Servers"/> <input type="button" value="Address Pools"/> <input type="button" value="Client Update"/> <input type="button" value="Bandwidth Assignment"/> <input type="button" value="WebVPN Servers and URLs"/> <input type="button" value="WebVPN Port Forwarding"/>

Typ een groepsnaam (bijvoorbeeld IPsec-gebruikers) en een wachtwoord.

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	<input type="text" value="IPSecUsers"/>	Enter a unique name for the group.
Password	<input type="password" value="••••••••"/>	Enter the password for the group.
Verify	<input type="password" value="••••••••"/>	Verify the group's password.
Type	<input type="text" value="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>

Dit wachtwoord wordt gebruikt als de vooraf gedeelde sleutel voor de tunnelonderhandeling. Ga naar het tabblad IPsec en stel verificatie in op **RADIUS**.

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

Hiermee kunnen IPsec-clients worden geauthentificeerd via de RADIUS-verificatieserver. Klik op **Add** onder in de pagina om de wijzigingen in de actieve configuratie toe te voegen. Wanneer IPsec-clients worden aangesloten en gebruikt de groep die u hebt ingesteld, worden ze geauthentiseerd door de RADIUS-server.

[Verifiëren](#)

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

[Problemen oplossen](#)

[WebVPN-verificatiemislukkingen](#)

Deze secties geven informatie die u kunt gebruiken om uw configuratie problemen op te lossen.

- **Probleem:** De gebruikers van WebVPN kunnen niet tegen de server van de RADIUS authentiek verklaren maar kunnen met succes met de lokale databank van de VPN Concentrator authenticeren. Ze ontvangen fouten zoals "Aanmelden mislukt" en dit



bericht.

Oorzaak: Dit soort

problemen gebeuren vaak wanneer er een andere database dan de interne database van de Concentrator wordt gebruikt. WebVPN gebruikers slaan op Base Group wanneer ze voor het eerst verbinding maken met de Concentrator, en moeten de standaardverificatiemethode gebruiken. Vaak wordt deze methode ingesteld op de interne database van de Concentrator en is deze niet ingesteld op een RADIUS of een andere server. **Oplossing:** Wanneer een WebVPN-gebruiker verificatie uitvoert, controleert de Concentrator de lijst met servers die zijn gedefinieerd door **Configuration > System > Server > Verificatie** en gebruikt hij de bovenste **servers**. Verplaats de server waarvan u wilt dat de WebVPN-gebruikers ten hoogste in deze lijst authentiek verklaren. Als RADIUS bijvoorbeeld de authenticatiemethode zou moeten zijn, moet u de RADIUS-server bovenin de lijst verplaatsen om de verificatie naar deze server te sturen. **Opmerking:** Alleen omdat WebVPN gebruikers in eerste instantie op de Base Group klikken, betekent dit niet dat ze beperkt blijven tot de Base Group. Aanvullende WebVPN-groepen kunnen op de Concentrator worden ingesteld en gebruikers kunnen aan hen worden toegewezen door de RADIUS-server met de populatie van eigenschap 25 met **OU=groepsnaam**. Zie [Gebruikers vergrendelen in een VPN 3000 Concentrator-groep met een RADIUS-server](#) voor een gedetailleerdere uitleg.

[Gebruikersverificatie faalt tegen de actieve map](#)

In de Active Directory server op het tabblad Account van de Gebruiker Eigenschappen van de falende gebruiker kunt u dit aankruisvakje zien:

Er is geen pre-verificatie nodig

Als dit aankruisvakje niet is ingeschakeld, **controleert u dit** en probeert u het opnieuw te controleren bij deze gebruiker.

[Gerelateerde informatie](#)

- [Cisco VPN 3000 Series Concentrators](#)
- [Cisco VPN 3002 hardwareclients](#)
- [IPsec-onderhandeling/IKE-protocollen](#)
- [Ondersteuningspagina voor RADIUS \(afstandsverificatie, inbel-gebruikersservice\)](#)
- [Inbelservice voor externe verificatie \(RADIUS\)](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)