

# Configurar el Cisco VPN 3000 Concentrator con el Microsoft RADIUS

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Instale y configure al servidor de RADIUS en el Windows 2000 y Windows 2003](#)

[Instale al servidor de RADIUS](#)

[Configure Microsoft Windows 2000 Server con IAS](#)

[Configure el servidor de Microsoft Windows 2003 con IAS](#)

[Configure el Cisco VPN 3000 Concentrator para la autenticación de RADIUS](#)

[Verificación](#)

[Troubleshooting](#)

[La autenticación del WebVPN falla](#)

[La autenticación de usuario falla contra el Active Directory](#)

[Información Relacionada](#)

## [Introducción](#)

El Servidor de autenticación de Internet (IAS) de Microsoft y Microsoft Commercial Internet System (MCI 2.0) están disponibles actualmente. El servidor del Microsoft RADIUS es conveniente porque utiliza el Active Directory en el Primary Domain Controller para su base de datos de usuarios. Ya no necesita mantener una base de datos aparte. También soporta encriptación de 40 y de 128 bits para las conexiones VPN del Point-to-Point Tunneling Protocol (PPTP). Refiera a la [lista de verificación de Microsoft: Configurar IAS para la terminal de marcado manual y la Documentación de acceso VPN](#) para más información.

## [prerrequisitos](#)

### [Requisitos](#)

No hay requisitos específicos para este documento.

### [Componentes Utilizados](#)

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

## Convenciones

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

## Instale y configure al servidor de RADIUS en el Windows 2000 y Windows 2003

### Instale al servidor de RADIUS

Si usted no tiene el servidor de RADIUS (IAS) instalado ya, realice estos pasos para instalar. Si usted tiene ya el servidor de RADIUS instalado, continúe a los [pasos para la configuración](#).

1. Inserte el disco compacto del Servidor Windows y encienda el programa de configuración.
2. El tecleo **instala los componentes adicionales**, y después hace clic **agrega/quita a los componentes de Windows**.
3. En los componentes, los **servicios de red del tecleo** (pero no seleccione ni borre la casilla de verificación), y entonces hacen clic los **detalles**.
4. Marque el **Internet Authentication Service** y haga clic la **AUTORIZACIÓN**.
5. Haga clic en Next (Siguiente).

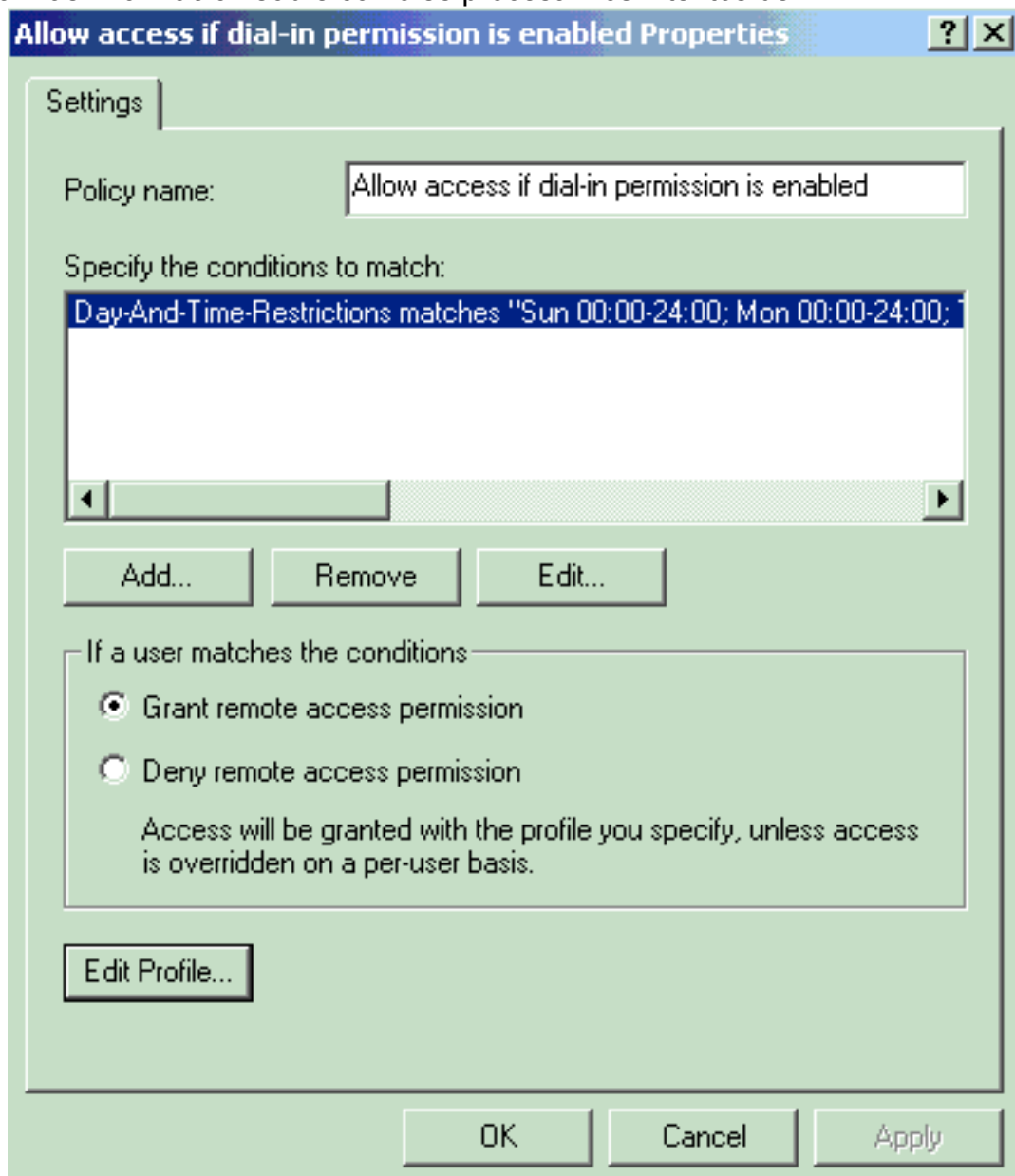
### Configure Microsoft Windows 2000 Server con IAS

Complete estos pasos para configurar al servidor de RADIUS (IAS) y comenzar el servicio para hacerlo disponible para autenticar a los usuarios en el concentrador VPN.

1. Elija el **Start (Inicio) > Programs (Programas) > Administrative Tools (Herramientas administrativas) > el Internet Authentication Service**.
2. Haga clic con el botón derecho del ratón el **Internet Authentication Service**, y haga clic las **propiedades del submenú** que aparece.
3. Vaya a la lengüeta RADIUS para examinar las configuraciones para los puertos. Si su autenticación de RADIUS y puertos del User Datagram Protocol (UDP) de las estadísticas RADIUS diferencian de los valores predeterminados proporcionados (1812 y 1645 para la autenticación, 1813 y 1646 para considerar) en la autenticación y las estadísticas, teclee sus configuraciones de puerto. Haga Click en OK cuando le acaban. **Note:** No cambie los puertos predeterminados. Separe los puertos usando las comas para utilizar las configuraciones del puerto múltiple para las peticiones de la autenticación o de las estadísticas.
4. Haga clic con el botón derecho del ratón a los **clientes** y elija al **nuevo cliente** para agregar el concentrador VPN como cliente del Authentication, Authorization, and Accounting (AAA) al servidor de RADIUS (IAS). **Note:** Si la Redundancia se configura entre dos concentradores del Cisco VPN 3000, el Cisco VPN 3000 Concentrator de reserva se debe también agregar al servidor de RADIUS como cliente RADIUS.
5. Ingrese un nombre cómodo y selecciónelo como **protocolo Radius**.
6. Defina el concentrador VPN con una dirección IP o un nombre DNS en la próxima ventana.
7. Elija **Cisco de Client Vendedor scrollbar**.
8. Ingrese un secreto compartido. **Note:** Usted debe recordar el secreto *exacto* que usted utiliza. Usted necesita esta información para configurar el concentrador VPN.

9. Haga clic en Finish (Finalizar).

10. Haga doble clic las **políticas de acceso remoto** y haga doble clic la directiva que aparece en el lado derecho de la ventana. **Note:** Después de que usted instale IAS, una política de acceso remoto debe existir ya. En el Windows 2000, la autorización se concede sobre la base de las propiedades del dial-in de una cuenta de usuario y de las políticas de acceso remoto. Las políticas de acceso remoto son un conjunto de condiciones y las configuraciones de la conexión que dan a administradores de la red más flexibilidad en los intentos de conexión que autorizan. La encaminamiento y Remote Access Service y el Windows 2000 IAS del Windows 2000 ambas políticas de acceso remoto del uso a determinar si validar o rechazar los intentos de conexión. En ambos casos, las políticas de acceso remoto se salvan localmente. Refiera a la documentación del IAS del Windows 2000 para más información sobre cómo se procesan los intentos de



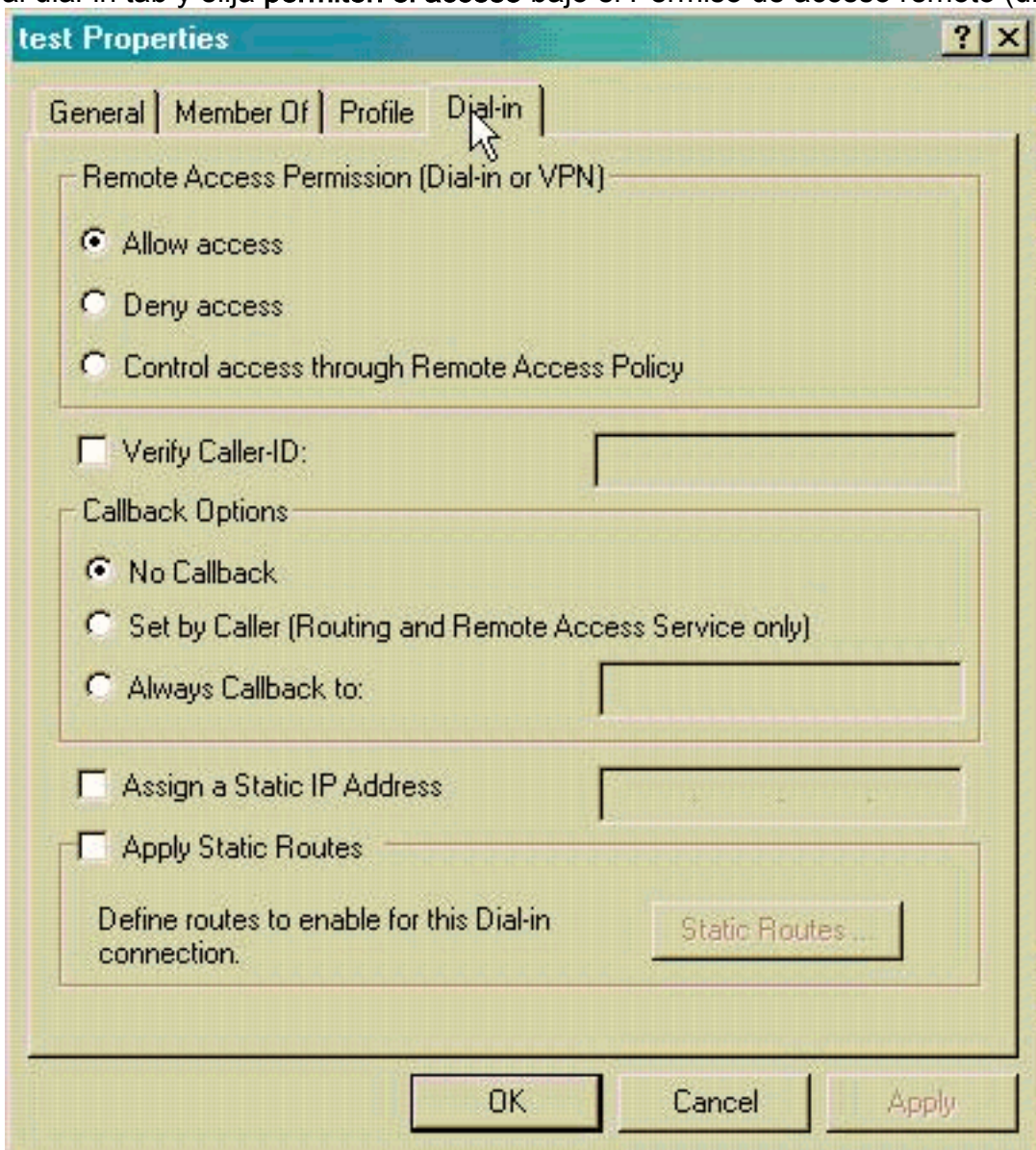
conexión.

11. Elija el **Permiso de acceso remoto de Grant** y el tecleo **edita el perfil** para configurar las propiedades del dial-in.

12. Seleccione el protocolo para utilizar para la autenticación en la lengüeta de la autenticación. Marque la **versión 2 de la autenticación encriptada de Microsoft** y desmarque el resto de los Protocolos de autenticación. **Note:** Las configuraciones en este perfil del dial-in deben hacer juego las configuraciones en la configuración y el cliente dial in

concentradores VPN 3000. En este ejemplo MS-CHAPv2 la autenticación sin la encriptación PPTP se utiliza.

13. En el **no encryption** del control de la lengüeta del cifrado solamente.
14. El Haga Click en OK para cerrar el perfil del dial-in, entonces hace clic la **AUTORIZACIÓN** para cerrar la ventana de la política de acceso remoto.
15. Haga clic con el botón derecho del ratón el **Internet Authentication Service** y haga clic el **servicio del comienzo** en el árbol de la consola. **Note:** Usted puede también utilizar esta función para parar el servicio.
16. Complete estos pasos para modificar a los usuarios para permitir la conexión. Elija el **Console (Consola) > Add/Remove Snap-in (Agregar/Remover complemento)**. El tecleo **agrega** y elige los **usuarios locales y a los grupos broche-en**. Haga clic en **Add (Agregar)**. Asegurese seleccionar la **computadora local** Clic en **Finalizar y AUTORIZACIÓN**.
17. Amplíe el **usuario local y a los grupos** y haga clic la **carpeta del usuario** en el panel izquierdo. En el panel derecho, haga doble clic al usuario (usuario de VPN) que usted quiere permitir el acceso.
18. Vaya al dial-in tab y elija **permiten el acceso** bajo el Permiso de acceso remoto (dial-in o



VPN).

19. El tecleo **se aplica y APRUEBA** para completar la acción. Usted puede cerrar la ventana de administración de la consola y salvar la sesión, si está deseado. Los usuarios que usted modificó pueden ahora acceder el concentrador VPN con el cliente VPN. Tenga presente

que el servidor IAS autentica solamente la información del usuario. El concentrador VPN todavía hace la autenticación del grupo.

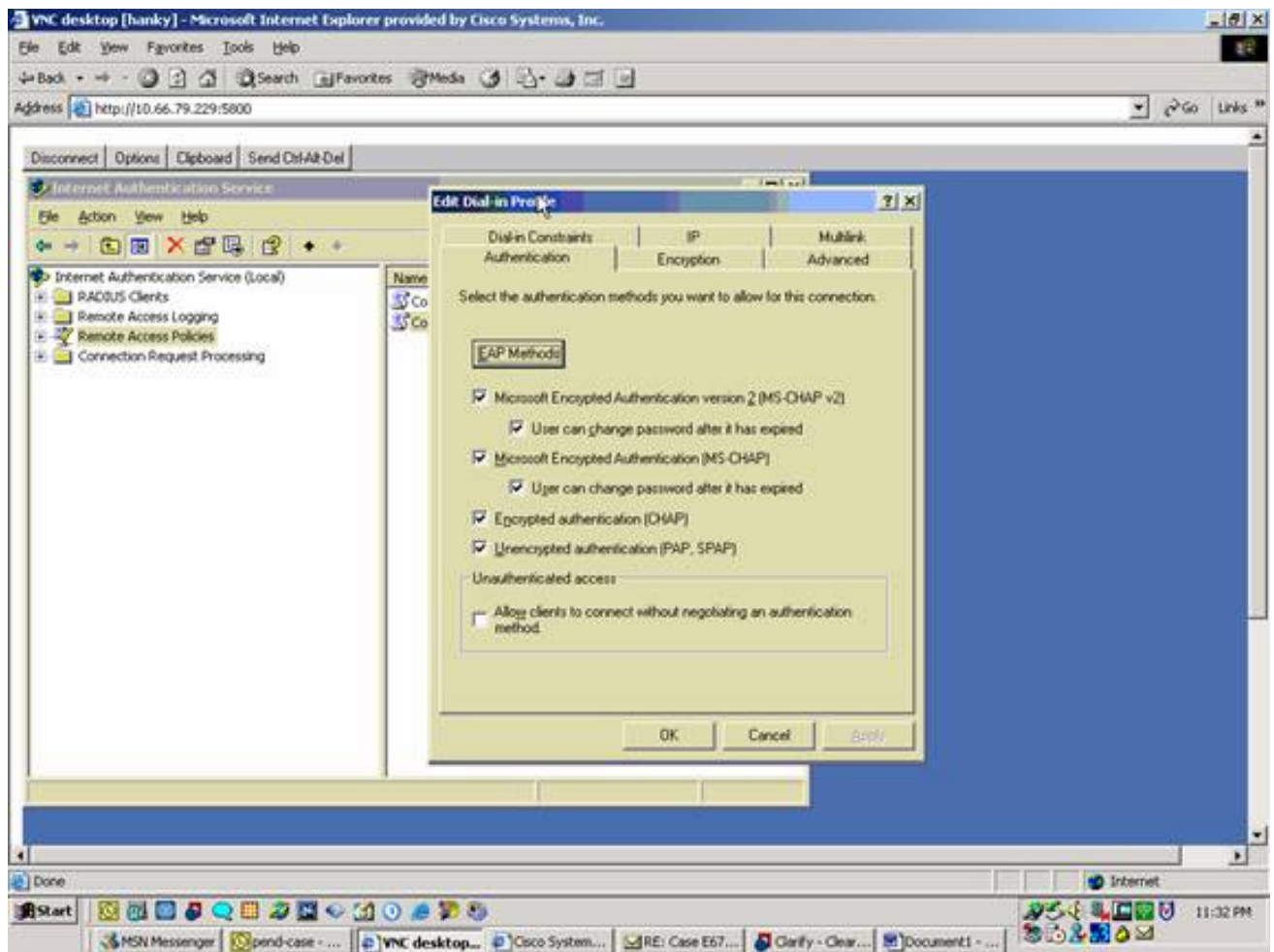
## [Configure el servidor de Microsoft Windows 2003 con IAS](#)

Complete estos pasos para configurar el servidor de Microsoft Windows 2003 con IAS.

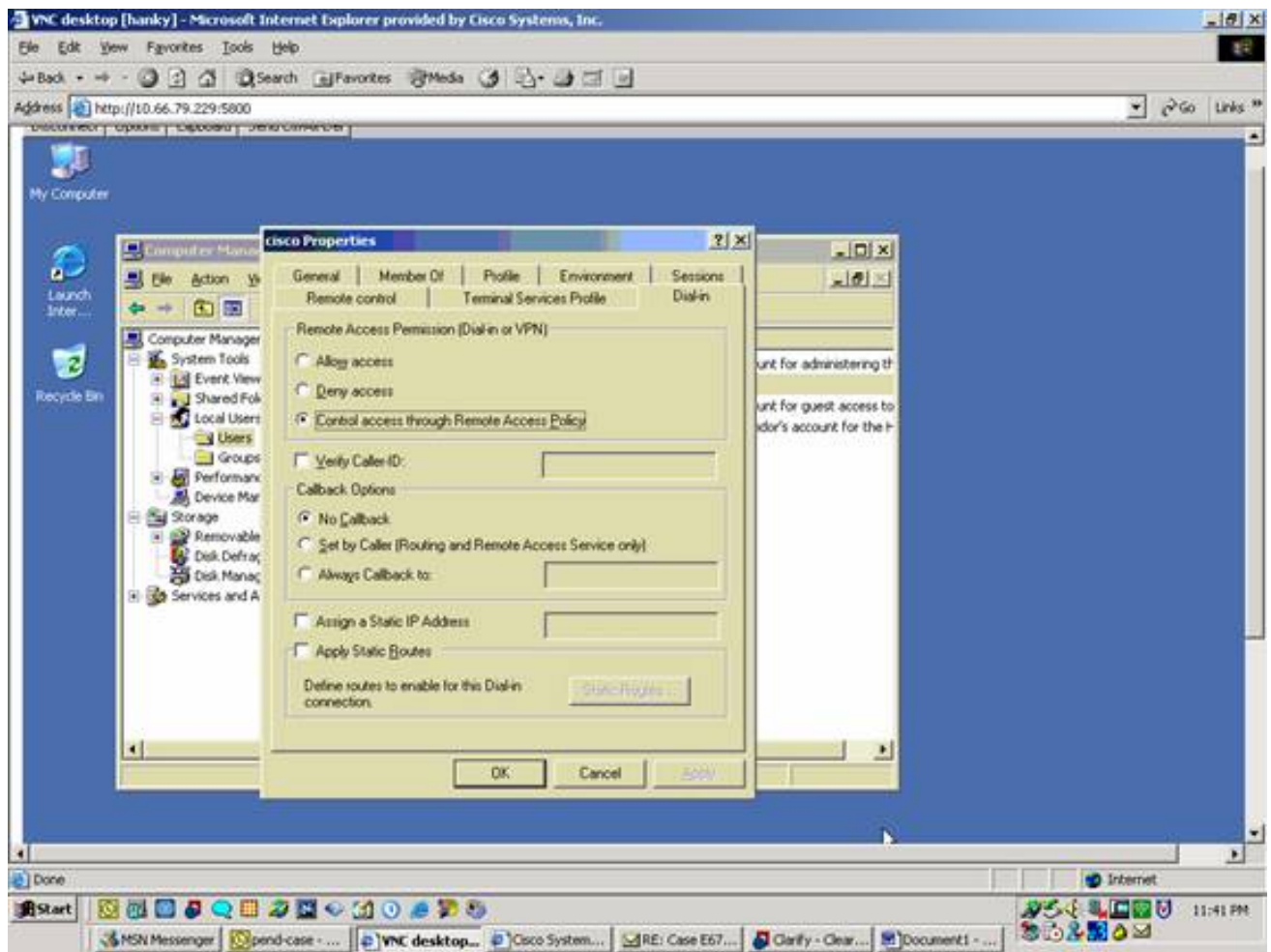
**Note:** Estos pasos asumen que el IAS ya está instalado en el equipo local. De lo contrario, agregue el IAS a través del **Control Panel > Add/Remove Programs**.

1. Elija **Administrative Tools > Internet Authentication Service** y haga clic con el botón derecho en **RADIUS Client** para agregar un nuevo cliente RADIUS. Luego de escribir la información del cliente, haga clic en **OK**.
2. Ingrese un nombre cómodo.
3. Defina el concentrador VPN con una dirección IP o un nombre DNS en la próxima ventana.
4. Elija **Cisco de Client Vendedor** scrollbar.
5. Ingrese un secreto compartido. **Note:** Usted debe recordar el secreto *exacto* que usted utiliza. Usted necesita esta información para configurar el concentrador VPN.
6. Haga Click en OK a completar.
7. Vaya a las **políticas de acceso remoto**, haga clic con el botón derecho del ratón en las **conexiones al otro Access Servers**, y elija las **propiedades**.
8. Elija el **Permiso de acceso remoto de Grant** y el tecleo **edita el perfil** para configurar las propiedades del dial-in.
9. Seleccione el protocolo para utilizar para la autenticación en la lengüeta de la autenticación. Marque la **versión 2 de la autenticación encriptada de Microsoft** y desmarque el resto de los Protocolos de autenticación. **Note:** Las configuraciones en este perfil del dial-in deben hacer juego las configuraciones en la configuración y el cliente dial in concentradores VPN 3000. En este ejemplo MS-CHAPv2 la autenticación sin la encriptación PPTP se utiliza.
10. En el **no encryption del** control de la lengüeta del cifrado solamente.
11. Haga Click en OK cuando le acaban.





12. **Internet Authentication Service** del click derecho y **servicio del comienzo del teclado** en el árbol de la consola. **Note:** Usted puede también utilizar esta función para parar el servicio.
13. Elija el **Administrative Tools (Herramientas administrativas) > Computer Management (Administración de la computadora) > System Tools (Herramientas del sistema) > Local Users and Groups (Usuarios y grupos locales)**, haga clic con el botón derecho del ratón en los **usuarios** y elija a los **usuarios nuevos** para agregar a un usuario en la cuenta de la computadora local.
14. Agregue al usuario con la clave de Cisco "vpnpasword" y marque esta información del perfil. En la pestaña **General**, asegúrese de que esté seleccionada la opción **Password Never Expired** en vez de la opción **User Must Change Password**. En el **dial-in** tab, elija la opción para el **acceso Allow** (o deje la configuración predeterminada del acceso del control con la política de acceso remoto). Haga Click en **OK** cuando le acaban.



## [Configure el Cisco VPN 3000 Concentrator para la autenticación de RADIUS](#)

Complete estos pasos para configurar el Cisco VPN 3000 Concentrator para la autenticación de RADIUS.

1. Conecte con el concentrador VPN con su buscador Web, y elija el **Configuration (Configuración) > Sytem (Sistema) > Servers (Servidores) > Authentication (Autenticación)** del menú del marco izquierdo.

Configuration | System | Servers | Authentication Save Needed

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

You should have a properly configured RADIUS, NT Domain, SDI or Kerberos/Active Directory 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
— Empty —	<input type="button" value="Add"/>
	<input type="button" value="Modify"/>
	<input type="button" value="Delete"/>
	<input type="button" value="Move Up"/>
	<input type="button" value="Move Down"/>
	<input type="button" value="Test"/>

- El tecleo **agrega** y configura estas configuraciones. Tipo de servidor = RADIUS Servidor de autenticación = dirección IP o nombre de host de su servidor de RADIUS (IAS) Puerto de servidor = 0 (0=default=1645) El Secreto de servidor = lo mismo que en el paso 8 en la sección encendido [configura al servidor de RADIUS](#)

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. If you are using RADIUS authentication or do not require an additional authorization check, do not configure an authorization server.

**Authentication Server**  Enter IP address or hostname.

**Used For**  Select the operation(s) for which this RADIUS server will be used.

**Server Port**  Enter 0 for default port (1645).

**Timeout**  Enter the timeout for this server (seconds).

**Retries**  Enter the number of retries for this server.

**Server Secret**  Enter the RADIUS server secret.

**Verify**  Re-enter the secret.

- El tecleo **agrega** para agregar los cambios a la configuración corriente.
- El tecleo **agrega**, elige al **servidor interno** para el tipo de servidor, y el tecleo **se aplica**. Usted necesita esto más adelante para configurar a un grupo IPsec (usted necesita solamente el tipo de servidor = al servidor interno).



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. Configure el concentrador VPN para los Usuarios usuarios PPTP o para los usuarios de cliente VPN. **PPTP (Protocolo de arquitectura de túneles punto a punto)** Complete estos pasos para configurar para los Usuarios usuarios PPTP. Elija el **Configuration (Configuración) > User Management (Administración del usuario) > Base Group (Grupo base)**, y haga clic la lengüeta **PPTP/L2TP**. Elija el **MSCHAPv2** y desmarque otros Protocolos de autenticación en la sección de los protocolos de autenticación PPTP.

Configuration | User Management | Base Group

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

PPTP/L2TP Parameters		
Attribute	Value	Description
<b>Use Client Address</b>	<input type="checkbox"/>	Check to accept and use an IP address received from the client.
<b>PPTP Authentication Protocols</b>	<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. <b>Unchecking all options means that no authentication is required.</b>
<b>PPTP Encryption</b>	<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.
<b>PPTP Compression</b>	<input type="checkbox"/>	Check to enable MPPC compression for PPTP connections for this group.
<b>L2TP Authentication Protocols</b>	<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. <b>Unchecking all options means that no authentication is required.</b>
<b>L2TP Encryption</b>	<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.
<b>L2TP Compression</b>	<input type="checkbox"/>	Check to enable MPPC compression for L2TP connections for this group.

El tecleo **se aplica** en la parte inferior de la página para agregar los cambios a la configuración corriente. Ahora en que los Usuarios usuarios PPTP conectan, al servidor de RADIUS (IAS) los autentican. **Cliente VPN** Complete estos pasos para configurar para los usuarios de cliente VPN. Elija el **Configuration (Configuración) > User Management (Administración del usuario) > Groups (Grupos)** y el tecleo **agrega** para agregar a un nuevo grupo.

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

Teclée un nombre del grupo (por ejemplo, IPsecUsers) y una contraseña.

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

Esta contraseña se utiliza como la clave previamente compartida para la negociación de túnel. Vaya a la lengüeta del IPsec y fije la autenticación al **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 <b>Individual User Authentication</b> .
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

Esto permite que autentiquen a los clientes IPsec vía el servidor de autenticación de RADIUS. El tecléo **agrega** en la parte inferior de la página para agregar los cambios a la configuración corriente. Ahora en que los clientes IPsec conectan y utilizan al grupo que usted configuró, al servidor de RADIUS los autentican.

## [Verificación](#)

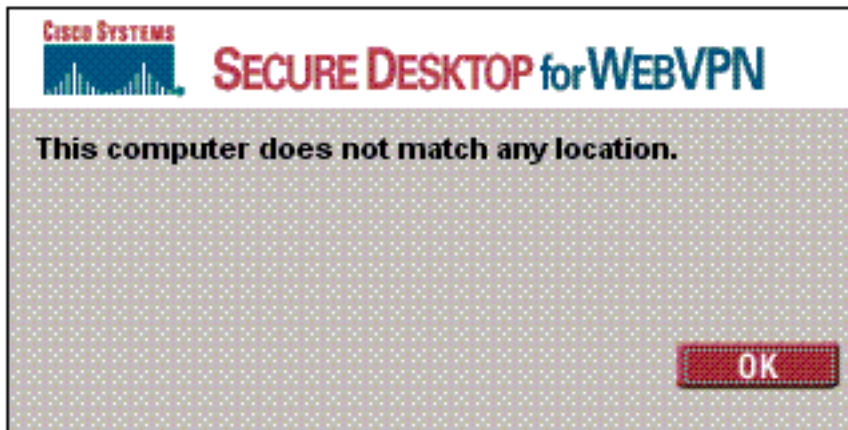
Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

## [Troubleshooting](#)

### [La autenticación del WebVPN falla](#)

Estas secciones proporcionan la información que usted puede utilizar para resolver problemas su configuración.

- Problema: Los usuarios de WebVPN no pueden autenticar contra el servidor de RADIUS sino pueden autenticar con éxito con la base de datos local del concentrador VPN. Reciben los errores tales como "login fallado" y este



mensaje. Causa: Estas clases de problemas suceden a menudo cuando cualquier base de datos con excepción de la base de datos interna del concentrador se utiliza. Los usuarios de WebVPN golpean al grupo base cuando primero conectan con el concentrador y deben utilizar el método de autenticación predeterminada. Este método se fija a la base de datos interna del concentrador y no es a menudo el RADIUS configurado o el otro servidor. Solución: Cuando un usuario de WebVPN autentica, el concentrador marca la lista de servidores definida en el **Configuration (Configuración) > Sytem (Sistema) > Servers (Servidores) > Authentication (Autenticación)** y utiliza el superior. Asegúrese mover el servidor que usted quisiera que los usuarios de WebVPN autenticaran con al top de esta lista. Por ejemplo, si el RADIUS es el método de autenticación, usted necesita mover al servidor de RADIUS al top de la lista para avanzar la autenticación a ella. **Note:** Apenas porque los usuarios de WebVPN golpean inicialmente el grupo base no significa que los confinan al grupo base. Los grupos adicionales del WebVPN pueden ser configurados en el concentrador, y los usuarios pueden ser asignados por el servidor de RADIUS con la población del atributo 25 con **OU=groupname**. Refiera a [bloquear a los usuarios en un VPN 3000 concentrator group usando un servidor de RADIUS](#) para una más explicación detallada.

## [La autenticación de usuario falla contra el Active Directory](#)

En el servidor Active Directory, en la lengüeta de la cuenta de las propiedades del usuario del usuario que falla, usted puede ver esta casilla de verificación:

El  no requiere la PRE-autenticación

Si se desmarca esta casilla de verificación, **marquela**, e intente autenticar otra vez con este usuario.

## [Información Relacionada](#)

- [Cisco VPN 3000 Series Concentrators](#)
- [Cisco VPN 3002 Hardware Clients](#)
- [Negociación IPSec/Protocolos IKE](#)
- [Página de soporte del RADIUS \(Servicio de usuario de acceso telefónico de autenticación remota\)](#)
- [Remote Authentication Dial-In User Service \(RADIUS\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)