

Configuración del concentrador Cisco VPN 3000 con Microsoft RADIUS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Instalación y configuración del servidor RADIUS en Windows 2000 y Windows 2003](#)

[Instalación del servidor RADIUS](#)

[Configuración de Microsoft Windows 2000 Server con IAS](#)

[Configuración de Microsoft Windows 2003 Server con IAS](#)

[Configuración del concentrador VPN 3000 de Cisco para la autenticación RADIUS](#)

[Verificación](#)

[Troubleshoot](#)

[Falla la autenticación WebVPN](#)

[La autenticación de usuario falla en 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 RADIUS de Microsoft es conveniente porque utiliza Active Directory en el controlador de dominio principal 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). Consulte la [lista de comprobación de Microsoft: Configuración de IAS para la documentación de acceso VPN y marcado manual](#) para obtener más información.

[Prerequisites](#)

[Requirements](#)

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.

Instalación y configuración del servidor RADIUS en Windows 2000 y Windows 2003

Instalación del servidor RADIUS

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

1. Inserte el disco compacto de Windows Server e inicie el programa de instalación.
2. Haga clic en **Install Add-On Components** y, a continuación, haga clic en **Add/Remove Windows Components**.
3. En Components, haga clic en **Networking Services** (pero no active o desactive la casilla de verificación) y, a continuación, haga clic en **Details**.
4. Verifique **Internet Authentication Service** y haga clic en **OK**.
5. Haga clic en Next (Siguiente).

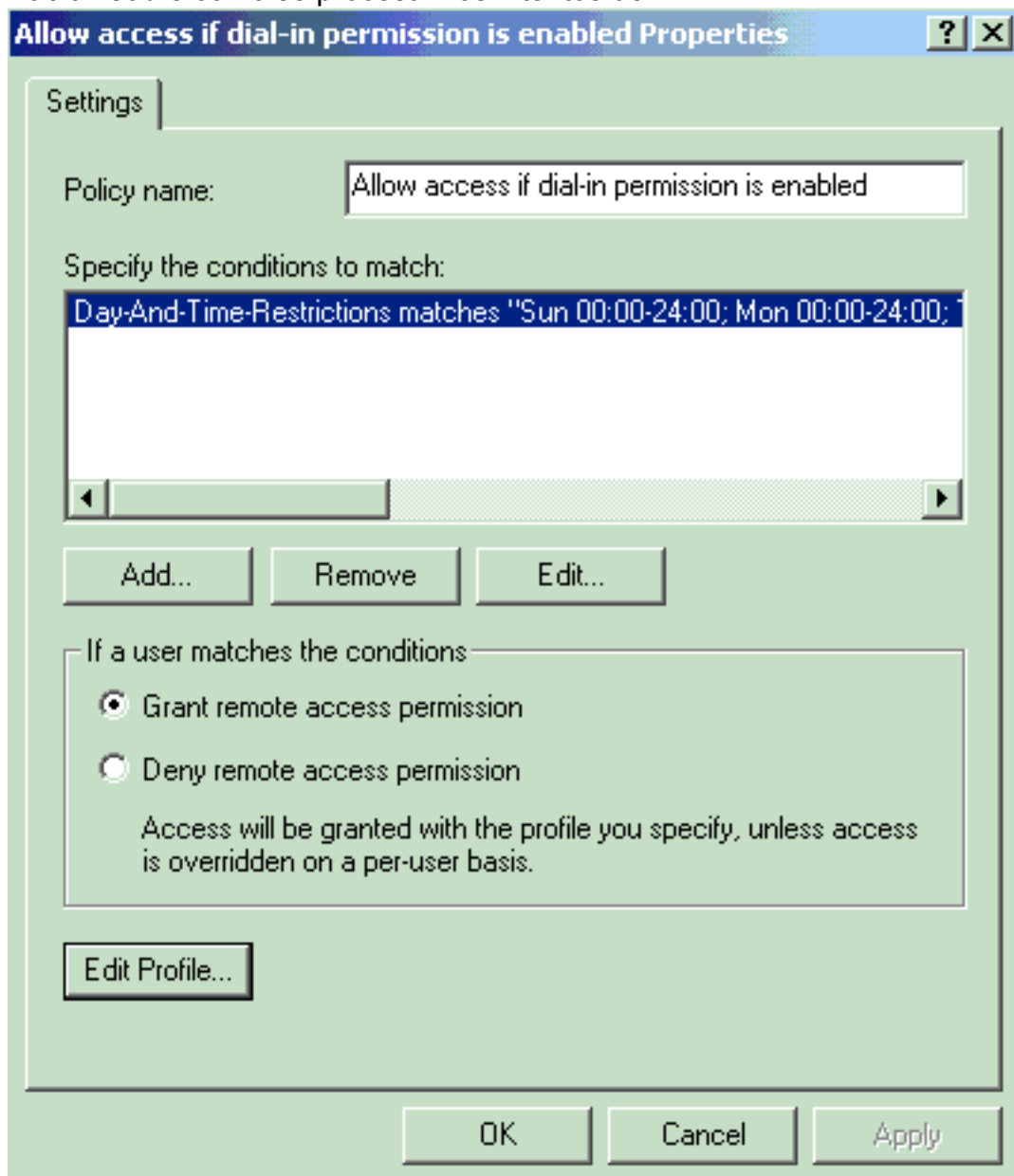
Configuración de Microsoft Windows 2000 Server con IAS

Complete estos pasos para configurar el servidor RADIUS (IAS) e iniciar el servicio para que esté disponible para autenticar a los usuarios en el concentrador VPN.

1. Elija **Inicio > Programas > Herramientas administrativas > Servicio de autenticación de Internet**.
2. Haga clic con el botón derecho del ratón en **Internet Authentication Service** y haga clic en **Properties** en el submenú que aparece.
3. Vaya a la ficha RADIUS para examinar la configuración de los puertos. Si la autenticación RADIUS y los puertos del protocolo de datagramas de usuario (UDP) de la contabilidad RADIUS difieren de los valores predeterminados proporcionados (1812 y 1645 para la autenticación, 1813 y 1646 para la contabilización) en Autenticación y Contabilización, escriba la configuración del puerto. Haga clic en **Aceptar** cuando haya terminado. **Nota:** No cambie los puertos predeterminados. Separe los puertos utilizando comas para utilizar la configuración de varios puertos para las solicitudes de autenticación o contabilización.
4. Haga clic con el botón derecho del mouse en **Clientes** y elija **Nuevo Cliente** para agregar el concentrador VPN como cliente de autenticación, autorización y contabilidad (AAA) al servidor RADIUS (IAS). **Nota:** Si la redundancia se configura entre dos Cisco VPN 3000 Concentrators, el Cisco VPN 3000 Concentrator de respaldo también se debe agregar al servidor RADIUS como un cliente RADIUS.
5. Introduzca un nombre descriptivo y selecciónelo como **RADIUS de protocolo**.
6. Defina el concentrador VPN con una dirección IP o un nombre DNS en la siguiente ventana.
7. Elija **Cisco** en la barra de desplazamiento Cliente-Proveedor.
8. Introduzca un secreto compartido. **Nota:** Debe recordar el secreto *exacto* que utiliza. Necesita esta información para configurar el VPN Concentrator.

9. Haga clic en Finish (Finalizar).

10. Haga doble clic en **Políticas de acceso remoto** y haga doble clic en la política que aparece en el lado derecho de la ventana. **Nota:** Después de instalar IAS, ya debería existir una política de acceso remoto. En Windows 2000, la autorización se concede en función de las propiedades de acceso telefónico de una cuenta de usuario y de las políticas de acceso remoto. Las políticas de acceso remoto son un conjunto de condiciones y configuraciones de conexión que proporcionan a los administradores de red más flexibilidad a la hora de autorizar los intentos de conexión. El servicio de acceso remoto y ruteo de Windows 2000 y el IAS de Windows 2000 utilizan políticas de acceso remoto para determinar si se aceptan o rechazan los intentos de conexión. En ambos casos, las políticas de acceso remoto se almacenan localmente. Consulte la documentación de Windows 2000 IAS para obtener más información sobre cómo se procesan los intentos de



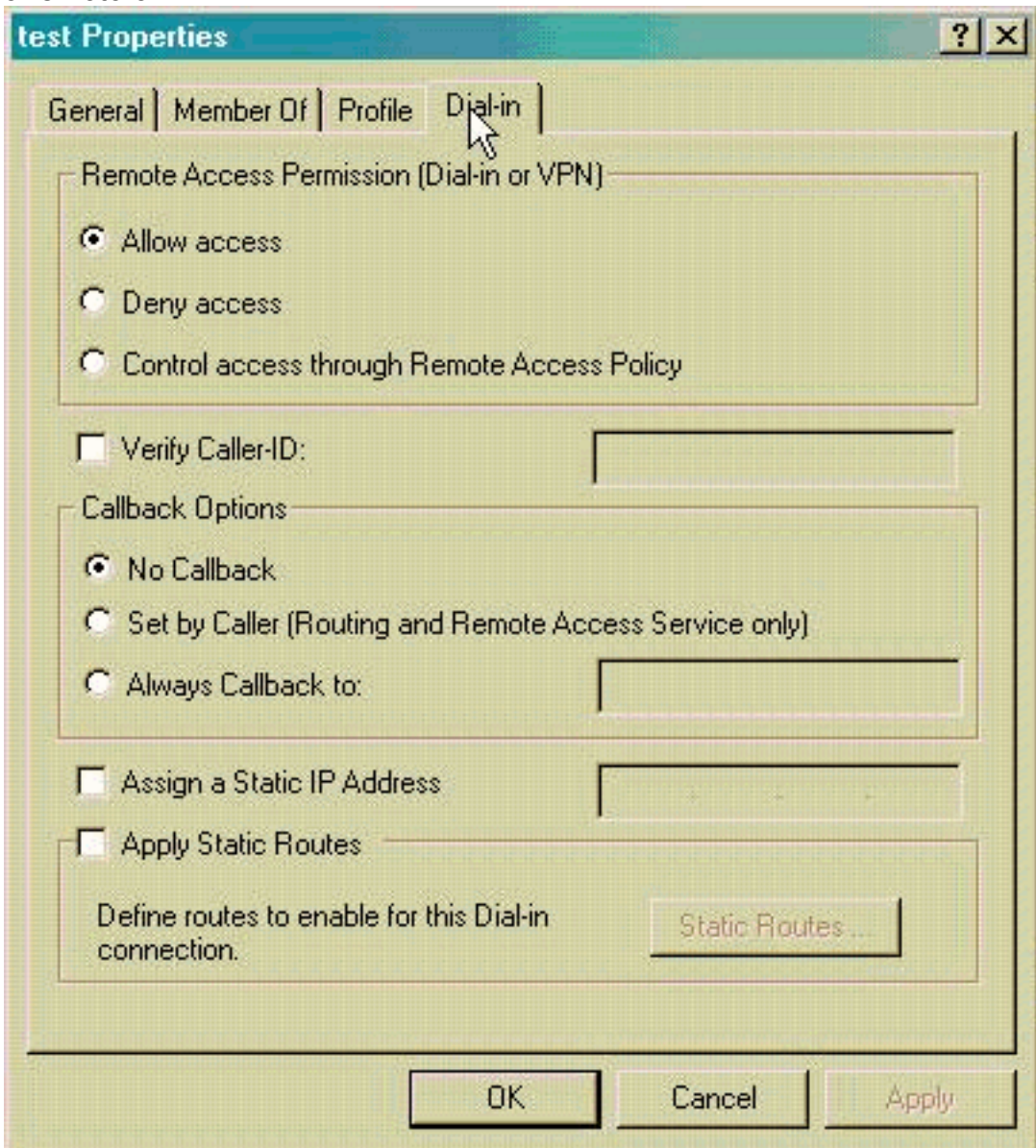
conexión.

11. Elija **Conceder permiso de acceso remoto** y haga clic en **Editar perfil** para configurar las propiedades de marcado.

12. Seleccione el protocolo que se utilizará para la autenticación en la ficha Authentication (Autenticación). Verifique **Microsoft Encrypted Authentication versión 2** y desmarque todos los demás protocolos de autenticación. **Nota:** La configuración de este perfil de marcado debe coincidir con la configuración del concentrador VPN 3000 y del cliente de marcado de

entrada. En este ejemplo se utiliza la autenticación MS-CHAPv2 sin el cifrado PPTP.

13. En la ficha Cifrado, marque **No Encryption only** (No cifrado solamente).
14. Haga clic en **Aceptar** para cerrar el perfil de acceso telefónico y luego haga clic en **Aceptar** para cerrar la ventana de política de acceso remoto.
15. Haga clic con el botón derecho del ratón en **Internet Authentication Service** y haga clic en **Start Service** en el árbol de la consola. **Nota:** También puede utilizar esta función para detener el servicio.
16. Complete estos pasos para modificar los usuarios para permitir la conexión. Elija **Console > Add/Remove Snap-in**. Haga clic en **Agregar** y elija **complemento Usuarios y grupos locales**. Haga clic en **Add** (Agregar). Asegúrese de seleccionar **Equipo local**. Haga clic en **Finalizar** y **Aceptar**.
17. Expanda **Usuario y grupos locales** y haga clic en la carpeta **Usuarios** en el panel izquierdo. En el panel derecho, haga doble clic en el usuario (usuario VPN) al que desea permitir el acceso.
18. Vaya a la ficha Dial-in y elija **Allow Access** en Remote Access Permission (Permiso de acceso remoto o



VPN).

19. Haga clic en **Aplicar** y **Aceptar** para completar la acción. Si lo desea, puede cerrar la ventana Administración de la consola y guardar la sesión. Los usuarios que modificó ahora pueden acceder al concentrador VPN con el cliente VPN. Tenga en cuenta que el servidor

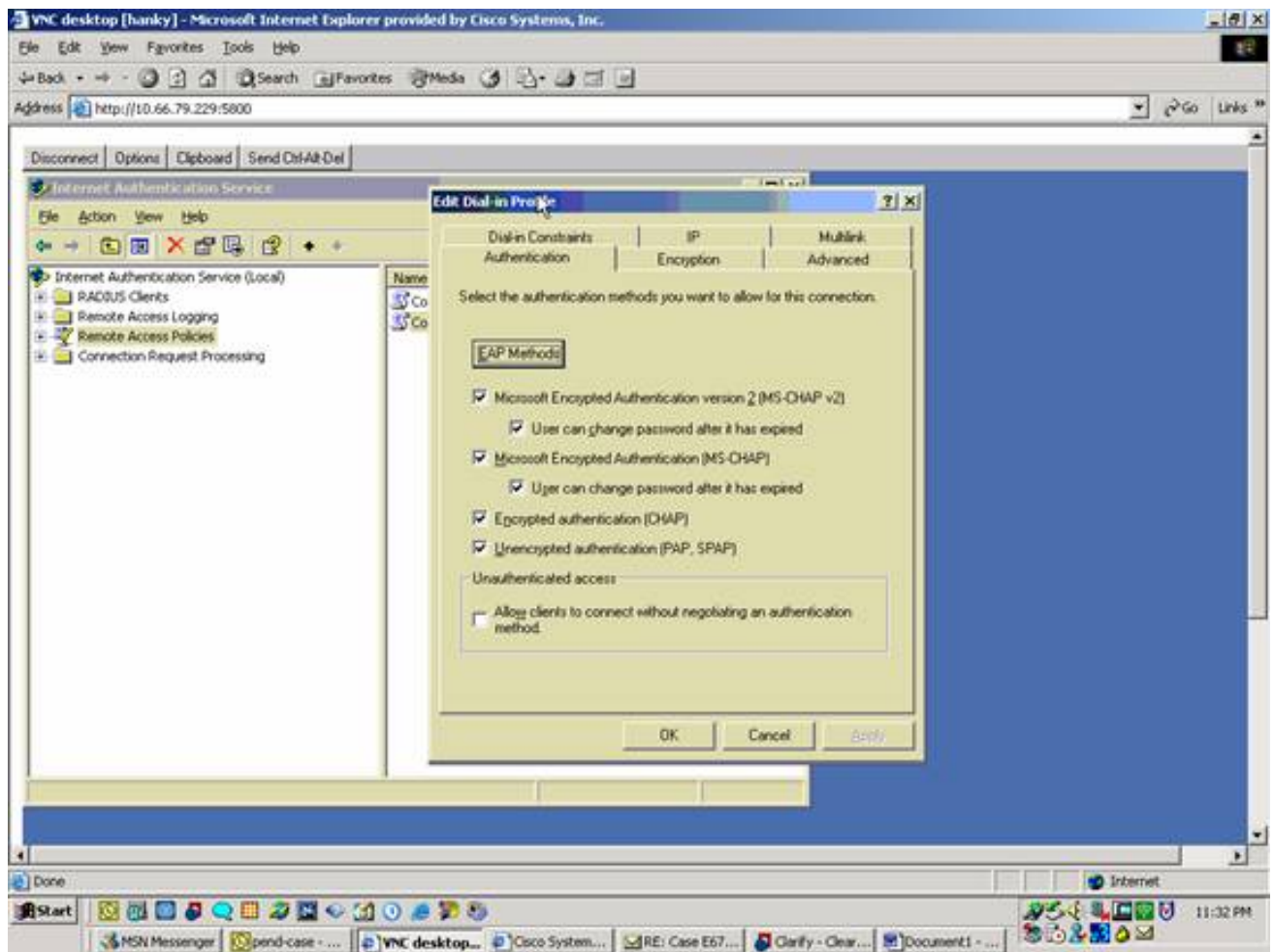
IAS sólo autentica la información del usuario. El concentrador VPN aún realiza la autenticación de grupo.

[Configuración de Microsoft Windows 2003 Server con IAS](#)

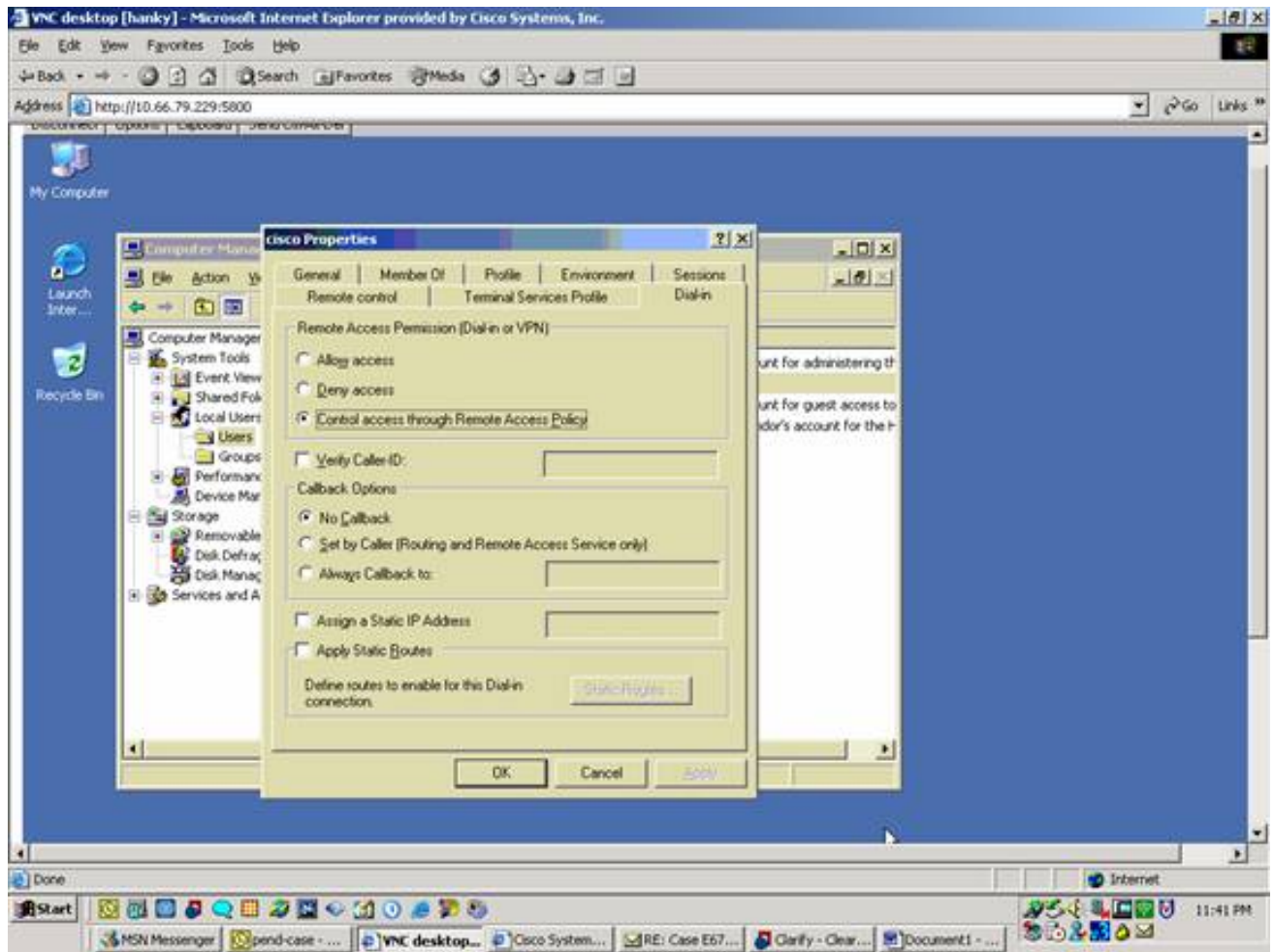
Complete estos pasos para configurar el servidor de Microsoft Windows 2003 con IAS.

Nota: Estos pasos suponen que IAS ya está instalada en la máquina 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. Introduzca un nombre descriptivo.
3. Defina el concentrador VPN con una dirección IP o un nombre DNS en la siguiente ventana.
4. Elija **Cisco** en la barra de desplazamiento Cliente-Proveedor.
5. Introduzca un secreto compartido. **Nota:** Debe recordar el secreto *exacto* que utiliza. Necesita esta información para configurar el VPN Concentrator.
6. Haga clic en **Aceptar** para completarlo.
7. Vaya a **Políticas de acceso remoto**, haga clic con el botón derecho en **Conexiones a otros servidores de acceso** y elija **Propiedades**.
8. Elija **Grant remote access permit** y haga clic en **Edit Profile** para configurar las propiedades Dial-In.
9. Seleccione el protocolo que se utilizará para la autenticación en la ficha Authentication (Autenticación). Verifique **Microsoft Encrypted Authentication versión 2** y desmarque todos los demás protocolos de autenticación. **Nota:** La configuración de este perfil de marcado debe coincidir con la configuración del concentrador VPN 3000 y del cliente de marcado de entrada. En este ejemplo se utiliza la autenticación MS-CHAPv2 sin el cifrado PPTP.
10. En la ficha Cifrado, marque **No Encryption only** (No cifrado solamente).
11. Haga clic en **Aceptar** cuando haya terminado.




12. Haga clic con el botón derecho del ratón en **Internet Authentication Service** y haga clic en **Start Service** en el árbol de la consola. **Nota:** También puede utilizar esta función para detener el servicio.
13. Elija **Administrative Tools > Computer Management > System Tools > Local Users and Groups**, haga clic con el botón derecho en **Users** y elija **New Users** para agregar un usuario a la cuenta de equipo local.
14. Agregue el usuario con la contraseña de Cisco "vpnpasword" y verifique esta información de 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 la ficha Marcar, elija la opción **Permitir acceso** (o deje la configuración predeterminada Control access a través de Remote Access Policy). Haga clic en **Aceptar** cuando haya terminado.



Configuración del concentrador VPN 3000 de Cisco para la autenticación RADIUS

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

1. Conéctese al concentrador VPN con su navegador web y elija **Configuration > System > Servers > Authentication** en el menú de 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"/>

- Haga clic en **Agregar** y configure estos parámetros. Tipo de servidor = RADIUS
 Servidor de autenticación = dirección IP o nombre de host del servidor RADIUS (IAS)
 Puerto del servidor = 0 (0=default=1645)
 Secreto de servidor = igual que en el paso 8 de la sección [Configuración del servidor RADIUS](#)

Configuration | System | Servers | Authentication | Add

Configure and add a user authentication server.

Server Type <input type="text" value="RADIUS"/>	Selecting <i>Internal Server</i> 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 <input type="text" value="msradius.company.com"/>	Enter IP address or hostname.
Used For <input type="text" value="User Authentication"/>	Select the operation(s) for which this RADIUS server will be used.
Server Port <input type="text" value="0"/>	Enter 0 for default port (1645).
Timeout <input type="text" value="4"/>	Enter the timeout for this server (seconds).
Retries <input type="text" value="2"/>	Enter the number of retries for this server.
Server Secret <input type="password" value="••••••••"/>	Enter the RADIUS server secret.
Verify <input type="password" value="••••••••"/>	Re-enter the secret.

- Haga clic en **Agregar** para agregar los cambios a la configuración en ejecución.
- Haga clic en **Add**, elija **Internal Server** para Server Type y haga clic en **Apply**. Necesita esto más adelante para configurar un grupo IPsec (sólo necesita el tipo de servidor = 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 PPTP o para los usuarios de VPN Client. **PPTP (Protocolo de arquitectura de túneles punto a punto)** Complete estos pasos para configurar para los usuarios PPTP. Elija **Configuration > User Management > Base Group** y haga clic en la pestaña **PPTP/L2TP**. Elija **MSCHAPv2** y desmarque otros protocolos de autenticación en la sección PPTP Authentication Protocols

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.

Haga clic en **Aplicar** en la parte inferior de la página para agregar los cambios a la configuración en ejecución. Ahora, cuando los usuarios PPTP se conectan, el servidor RADIUS (IAS) los autentica. **Cliente VPN** Complete estos pasos para configurar para los usuarios de VPN Client. Elija **Configuration > User Management > Groups** y haga clic en **Add** para agregar 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	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"/>

Escriba un nombre de 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	<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>

Esta contraseña se utiliza como clave previamente compartida para la negociación del túnel. Vaya a la ficha IPsec y establezca Authentication en 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

Esto permite que los clientes IPsec sean autenticados a través del servidor de autenticación RADIUS. Haga clic en **Agregar** en la parte inferior de la página para agregar los cambios a la configuración en ejecución. Ahora, cuando los clientes IPsec se conectan y utilizan el grupo que configuré, el servidor RADIUS los autentica.

Verificación

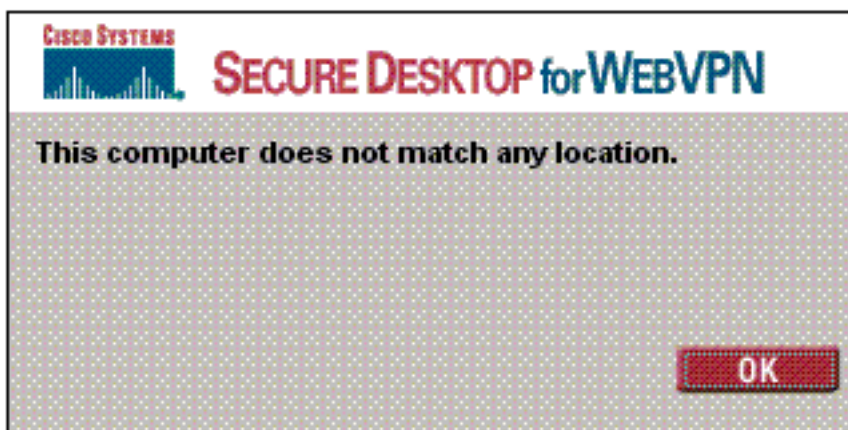
Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Falla la autenticación WebVPN

Estas secciones proporcionan información que puede utilizar para resolver problemas de configuración.

- **Problema:** Los usuarios de WebVPN no pueden autenticarse contra el servidor RADIUS pero pueden autenticarse correctamente con la base de datos local del concentrador VPN. Reciben errores como "Error de inicio de sesión" y este



mensaje.

Causa: Este tipo de problemas a menudo ocurren cuando se utiliza cualquier base de datos que no sea la base de datos interna del concentrador. Los usuarios de WebVPN golpean el grupo base cuando se conectan por primera vez al concentrador y deben utilizar el método de autenticación predeterminado. A menudo, este método se establece en la base de datos interna del concentrador y no es un RADIUS u otro servidor configurado. **Solución:** Cuando un usuario de WebVPN se autentica, el concentrador verifica la lista de servidores definida en **Configuration > System > Servers > Authentication** y utiliza el superior. Asegúrese de mover el servidor con el que desea que los usuarios de WebVPN se autenticuen a la parte superior de esta lista. Por ejemplo, si RADIUS debe ser el método de autenticación, debe mover el servidor RADIUS a la parte superior de la lista para enviarle la autenticación. **Nota:** Sólo porque los usuarios de WebVPN inicien el grupo base no significa que se limiten al grupo base. Los grupos WebVPN adicionales se pueden configurar en el concentrador, y los usuarios pueden ser asignados por el servidor RADIUS con la población del atributo 25 con **OU=groupname**. Refiérase a [Bloqueo de Usuarios en un Grupo de Concentradores VPN 3000 Usando un Servidor RADIUS](#) para obtener una explicación más detallada.

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

En el servidor de Active Directory, en la ficha Cuenta de las propiedades de usuario del usuario que ha fallado, puede ver esta casilla de verificación:

No requiere autenticación previa

Si esta casilla de verificación no está marcada, **márquela** e intente autenticarse de nuevo con este usuario.

[Información Relacionada](#)

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