Configuring the Cisco VPN 3000 Concentrator with MS RADIUS

Document ID: 20585

Contents

Introduction

Microsoft Internet Authentication Server (IAS) and Microsoft Commercial Internet System (MCIS 2.0) are currently available. The Microsoft RADIUS server is convenient because it uses the Active Directory on the Primary Domain Controller for its user database. You no longer need to maintain a separate database. It also supports 40−bit and 128−bit encryption for Point−to−Point Tunneling Protocol (PPTP) VPN connections. Refer to the Microsoft Checklist: Configuring IAS for dial−up and VPN access ↗ documentation for more information.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Install and Configure the RADIUS Server on Windows 2000 and Windows 2003

Install the RADIUS Server

If you do not have the RADIUS server (IAS) already installed, perform these steps in order to install. If you already have the RADIUS server installed, continue to the configuration steps.

1. Insert the Windows Server compact disc and start the setup program.
2. Click **Install Add−On Components**, and then click **Add/Remove Windows Components**.
3. In Components, click **Networking Services** (but do not select or clear the check box), and then click **Details**.
4. Check **Internet Authentication Service** and click **OK**.
5. Click **Next**.

Configure the Microsoft Windows 2000 Server with IAS

Complete these steps in order to configure the RADIUS server (IAS) and to start the service in order to make it available to authenticate users on the VPN Concentrator.

1. Choose **Start > Programs > Administrative Tools > Internet Authentication Service**.
2. Right−click **Internet Authentication Service**, and click **Properties** from the submenu that appears.
3. Go to the RADIUS tab in order to examine the settings for ports.

   If your RADIUS authentication and RADIUS accounting User Datagram Protocol (UDP) ports differ from the default values provided (1812 and 1645 for authentication, 1813 and 1646 for accounting) in Authentication and Accounting, type your port settings. Click **OK** when you are finished.

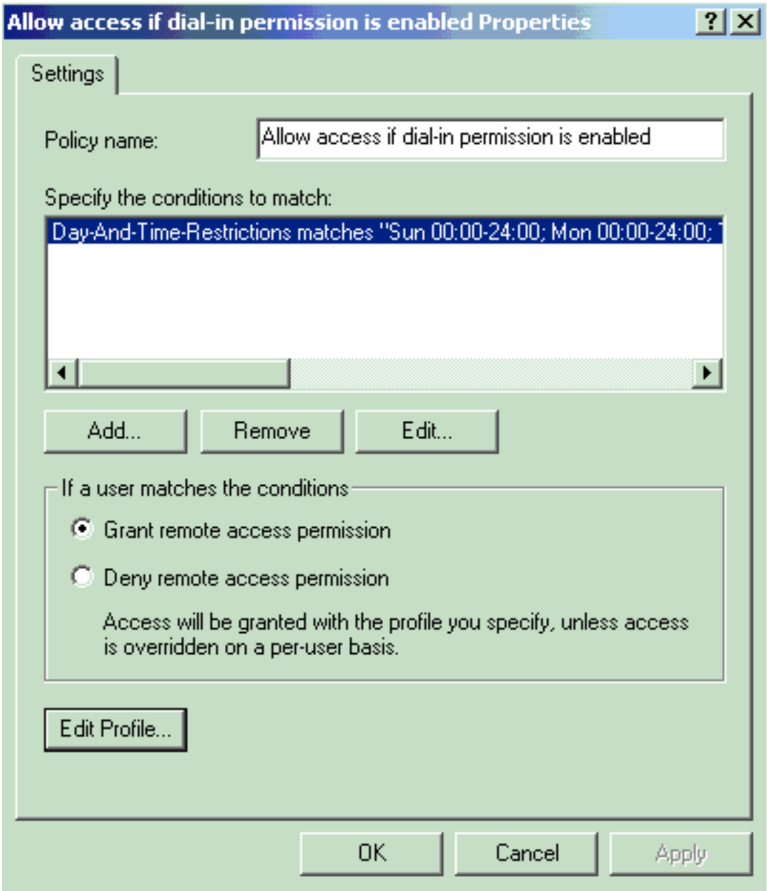
   Note: Do not change the default ports. Separate the ports by using commas to use multiple port settings for authentication or accounting requests.
4. Right−click **Clients** and choose **New Client** in order to add the VPN Concentrator as an authentication, authorization, and accounting (AAA) client to the RADIUS server (IAS).

   Note: If redundancy is configured between two Cisco VPN 3000 Concentrators, the backup Cisco VPN 3000 Concentrator must also be added to the RADIUS server as a RADIUS client.
5. Enter a friendly name and select as **Protocol Radius**.
6. Define the VPN Concentrator with an IP address or DNS name on the next window.
7. Choose **Cisco** from the Client−Vendor scrollbar.
8. Enter a shared secret.

   Note: You must remember the *exact* secret that you use. You need this information in order to configure the VPN Concentrator.
9. Click **Finish**.
10. Double−click **Remote Access Policies** and double−click the policy that appears in the right side of the window.

    Note: After you install IAS, a remote access policy should already exist.

    In Windows 2000, authorization is granted based on the dial−in properties of a user account and remote access policies. Remote access policies are a set of conditions and connection settings that give network administrators more flexibility in authorizing connection attempts. The Windows 2000 Routing and Remote Access service and the Windows 2000 IAS both use remote access policies to determine whether to accept or reject connection attempts. In both cases, the remote access policies are stored locally. Refer to the Windows 2000 IAS documentation for more information about how connection attempts are processed.



Allow access if dial-in permission is enabled Properties

Policy name: Allow access if dial-in permission is enabled

Specify the conditions to match:

Day-And-Time-Restrictions matches "Sun 00:00-24:00; Mon 00:00-24:00;

If a user matches the conditions

● Grant remote access permission

○ Deny remote access permission

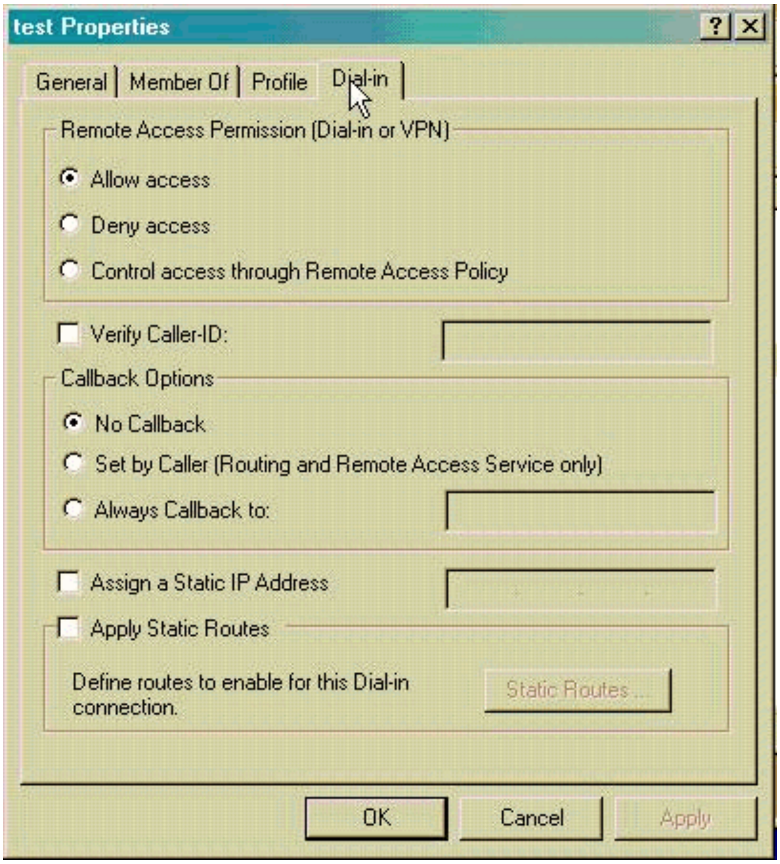
Access will be granted with the profile you specify, unless access is overridden on a per-user basis.

11. Choose **Grant remote access permission** and click **Edit Profile** in order to configure dial−in properties.
12. Select the protocol to use for authentication on the Authentication tab. Check **Microsoft Encrypted Authentication version 2** and uncheck all other authentication protocols.

    Note: Settings in this Dial−In Profile must match the settings in the VPN 3000 Concentrator configuration and Dial−In client. In this example MS−CHAPv2 authentication without PPTP encryption is used.
13. On the Encryption tab check **No Encryption** only.
14. Click **OK** in order to close the Dial−In profile, then click **OK** in order to close the remote access policy window.
15. Right−click **Internet Authentication Service** and click **Start Service** in the console tree.

    Note: You can also use this function to stop the service.
16. Complete these steps in order to modify the users to allow the connection.

    a. Choose **Console** > **Add/Remove Snap−in**.
    b. Click **Add** and choose **Local Users and Groups snap−in**.
    c. Click **Add**.
    d. Make sure to select **Local Computer**
    e. Click **Finish** and **OK**.
17. Expand **Local User and Groups** and click the **Users** folder in the left pane. In the right pane, double−click the user (VPN User) you want to allow access.
18. Go to the Dial−in tab and choose **Allow Access** under Remote Access Permission (Dial−in or VPN).



Remote Access Permission (Dial-in or VPN)

- ● Allow access
- ○ Deny access
- ○ Control access through Remote Access Policy

□ Verify Caller-ID:

Callback Options

- ● No Callback
- ○ Set by Caller (Routing and Remote Access Service only)
- ○ Always Callback to:

□ Assign a Static IP Address

□ Apply Static Routes

Define routes to enable for this Dial-in connection.

19. Click **Apply** and **OK** in order to complete the action. You can close the Console Management window and save the session, if desired.

    The users that you modified are now able to access the VPN Concentrator with the VPN Client. Keep in mind that the IAS server only authenticates the user information. The VPN Concentrator still does the group authentication.

Configure the Microsoft Windows 2003 Server with IAS

Complete these steps in order to configure the Microsoft Windows 2003 server with IAS.

Note: These steps assume that IAS is already installed on the local machine. If not, add this through **Control Panel > Add/Remove Programs**.

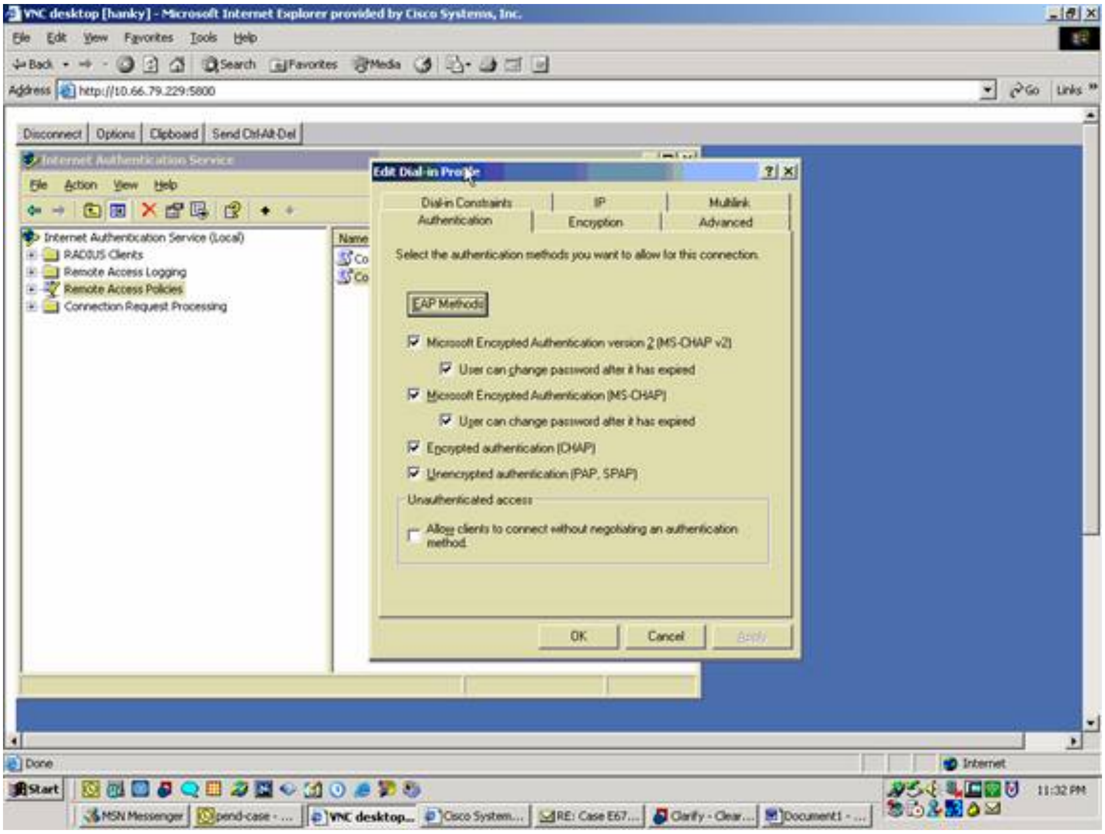
1. Choose **Administrative Tools > Internet Authentication Service** and right−click on **RADIUS Client** in order to add a new RADIUS client. After you type the client information, click **OK**.
2. Enter a friendly name.
3. Define the VPN Concentrator with an IP address or DNS name on the next window.
4. Choose **Cisco** from the Client−Vendor scrollbar.
5. Enter a shared secret.

   Note: You must remember the *exact* secret that you use. You need this information in order to configure the VPN Concentrator.
6. Click **OK** to complete.
7. Go to **Remote Access Policies**, right−click on **Connections to Other Access Servers**, and choose **Properties**.
8. Choose **Grant remote access permission** and click **Edit Profile** in order to configure Dial−In properties.
9. Select the protocol to use for authentication on the Authentication tab. Check **Microsoft Encrypted**

Authentication version 2 and uncheck all other authentication protocols.

Note: Settings in this Dial−In Profile must match the settings in the VPN 3000 Concentrator configuration and Dial−In client. In this example MS−CHAPv2 authentication without PPTP encryption is used.

10. On the Encryption tab check **No Encryption** only.
11. Click **OK** when you are finished.


VNC desktop [hanky] - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.66.79.229:5800
Go Links
Disconnect Options Clipboard Send Ctrl-Alt-Del
Internet Authentication Service
File Action View Help
Internet Authentication Service (Local)
RADIUS Clients
Remote Access Logging
Remote Access Policies
Connection Request Processing
Name
Edit Dial-in Profile
Dial-in Constraints
IP
Multilink
Authentication
Encryption
Advanced
EAP Methods
OK
Cancel
Apply
Done
Internet
Start
11:32 PM

Select the authentication methods you want to allow for this connection.

☑ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

☑ User can change password after it has expired

☑ Microsoft Encrypted Authentication (MS-CHAP)

☑ User can change password after it has expired

☑ Encrypted authentication (CHAP)

☑ Unencrypted authentication (PAP, SPAP)

Unauthenticated access

□ Allow clients to connect without negotiating an authentication method.

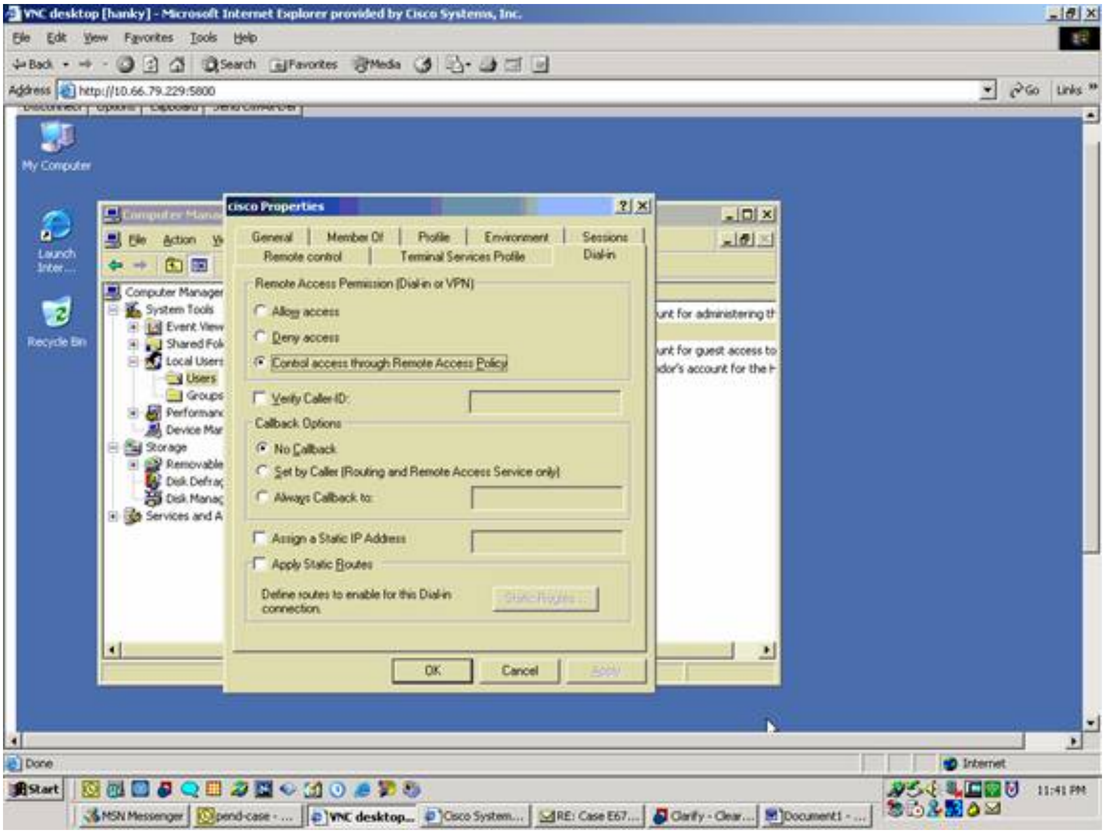
12. Right−click **Internet Authentication Service** and click **Start Service** in the console tree.

Note: You can also use this function in order to stop the service.

13. Choose **Administrative Tools > Computer Management > System Tools > Local Users and Groups**, right−click on **Users** and choose **New Users** in order to add a user into the local computer account.
14. Add user with Cisco password "vpnpassword" and check this profile information.

    - On the General tab, ensure that the option for **Password Never Expired** is selected instead of the option for User Must Change Password.
    - On the Dial−in tab, choose the option for **Allow access** (or leave default setting of Control access through Remote Access Policy).

    Click **OK** when you are finished.



cisco Properties

Remote Access Permission (Dial-in or VPN)

○ Allow access

○ Deny access

● Control access through Remote Access Policy

□ Verify Caller-ID:

Callback Options

● No Callback

○ Set by Caller (Routing and Remote Access Service only)

○ Always Callback to:

□ Assign a Static IP Address

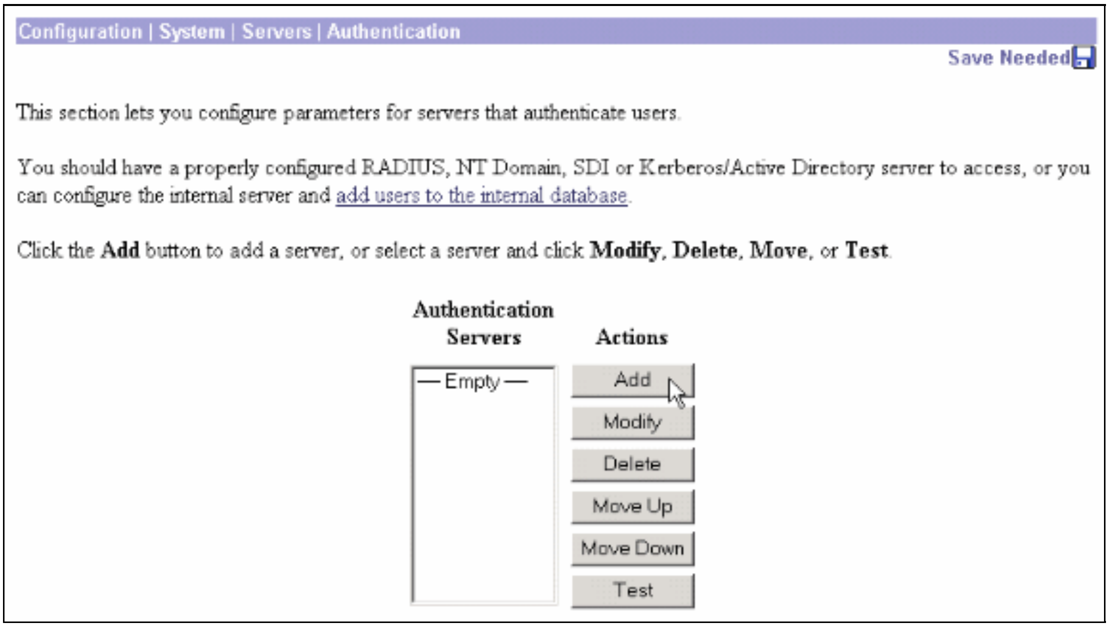
□ Apply Static Routes

Define routes to enable for this Dial-in connection.

Configure the Cisco VPN 3000 Concentrator for RADIUS Authentication

Complete these steps in order to configure the Cisco VPN 3000 Concentrator for RADIUS authentication.

1. Connect to the VPN Concentrator with your Web Browser, and choose **Configuration > System > Servers > Authentication** from the left frame menu.



Configuration | System | Servers | Authentication

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.

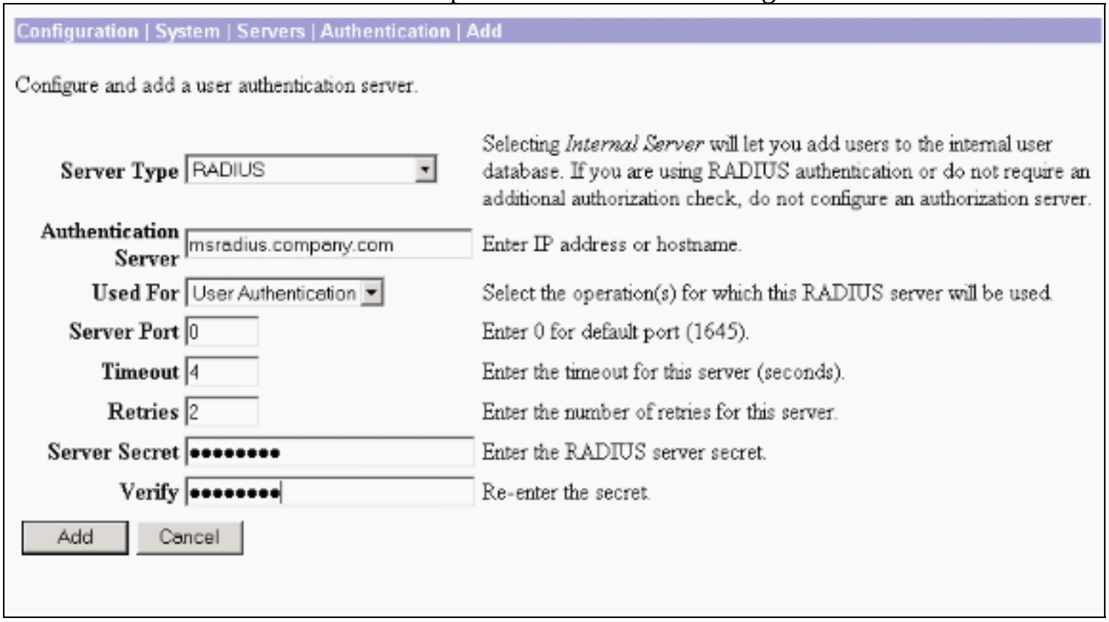
Click the **Add** button to add a server, or select a server and click **Modify**, **Delete**, **Move**, or **Test**.

Authentication Servers	Actions
— Empty —	Add

2. Click **Add** and configure these settings.

    - Server Type = RADIUS

- Authentication Server = IP Address or Hostname of your RADIUS server (IAS)
- Server Port = 0 (0=default=1645)
- Server Secret = same as in step 8 in the section on Configure the RADIUS Server



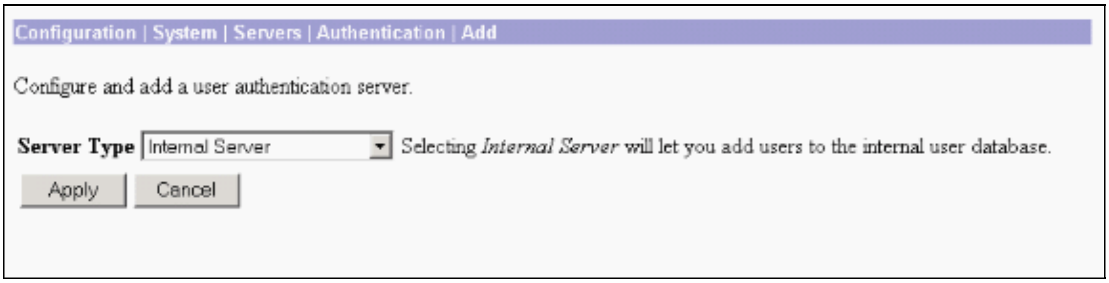
Configuration | System | Servers | Authentication | Add

Configure and add a user authentication server.

Server Type	RADIUS	Selecting *Internal Server* will let you add users to the internal user database. If you are using RADIUS authentication or do not require an additional authorization check, do not configure an authorization server.
Authentication Server	msradius.company.com	Enter IP address or hostname.
Used For	User Authentication	Select the operation(s) for which this RADIUS server will be used.
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	●●●●●●●●●	Re-enter the secret.

3. Click **Add** in order to add the changes to the running configuration.
4. Click **Add**, choose **Internal Server** for Server Type, and click **Apply**.

   You need this later in order to configure an IPsec Group (You need only Server Type = Internal Server).



Configuration | System | Servers | Authentication | Add

Configure and add a user authentication server.

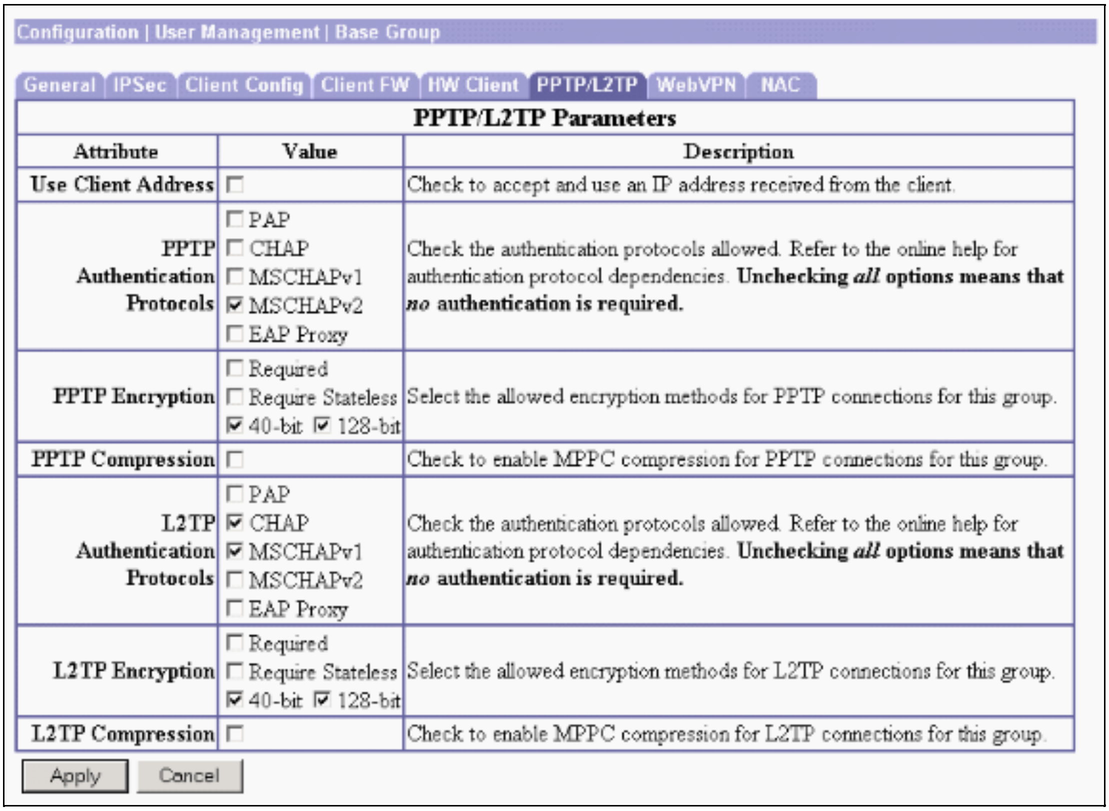
Server Type: Internal Server — Selecting *Internal Server* will let you add users to the internal user database.

5. Configure the VPN Concentrator for PPTP users or for VPN Client users.

   PPTP

   Complete these steps in order to configure for PPTP users.

   a. Choose **Configuration > User Management > Base Group**, and click the **PPTP/L2TP** tab.
   b. Choose **MSCHAPv2** and uncheck other authentication protocols in the PPTP Authentication Protocols section.



PPTP/L2TP Parameters

Attribute	Value	Description
Use Client Address	□	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	□ PAP □ CHAP □ MSCHAPv1 ☑ MSCHAPv2 □ 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	□ Required □ Require Stateless ☑ 40-bit ☑ 128-bit	Select the allowed encryption methods for PPTP connections for this group.
PPTP Compression	□	Check to enable MPPC compression for PPTP connections for this group.
L2TP Authentication Protocols	□ PAP ☑ CHAP ☑ MSCHAPv1 □ MSCHAPv2 □ 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	□ Required □ Require Stateless ☑ 40-bit ☑ 128-bit	Select the allowed encryption methods for L2TP connections for this group.
L2TP Compression	□	Check to enable MPPC compression for L2TP connections for this group.

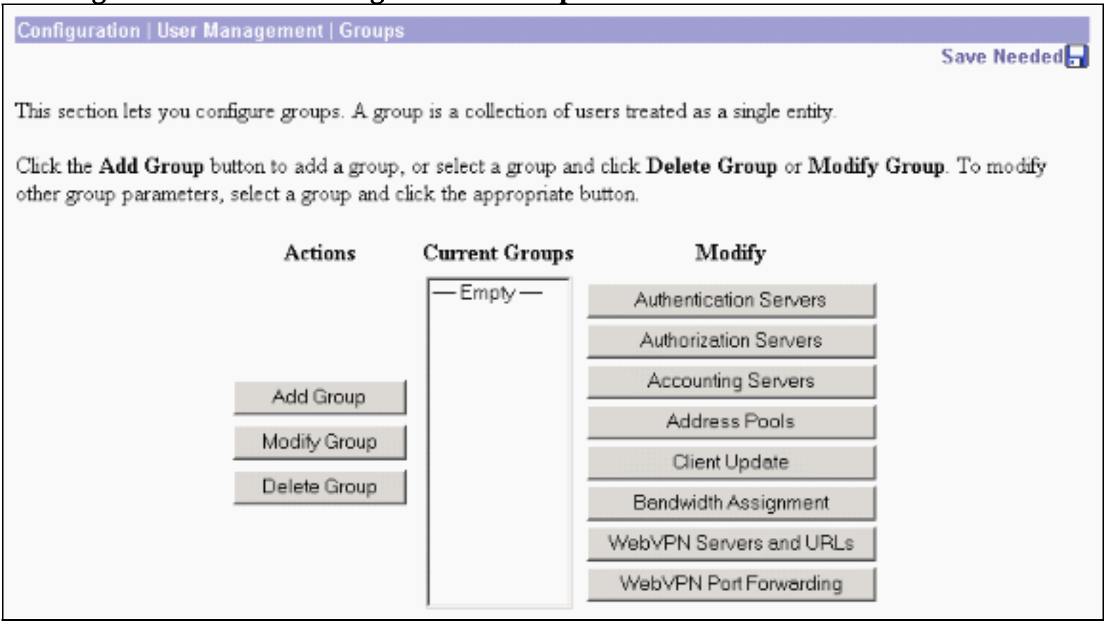
c. Click **Apply** at the bottom of the page in order to add the changes to the running configuration.

Now when PPTP users connect, they are authenticated by the RADIUS server (IAS).

VPN Client

Complete these steps in order to configure for VPN Client users.

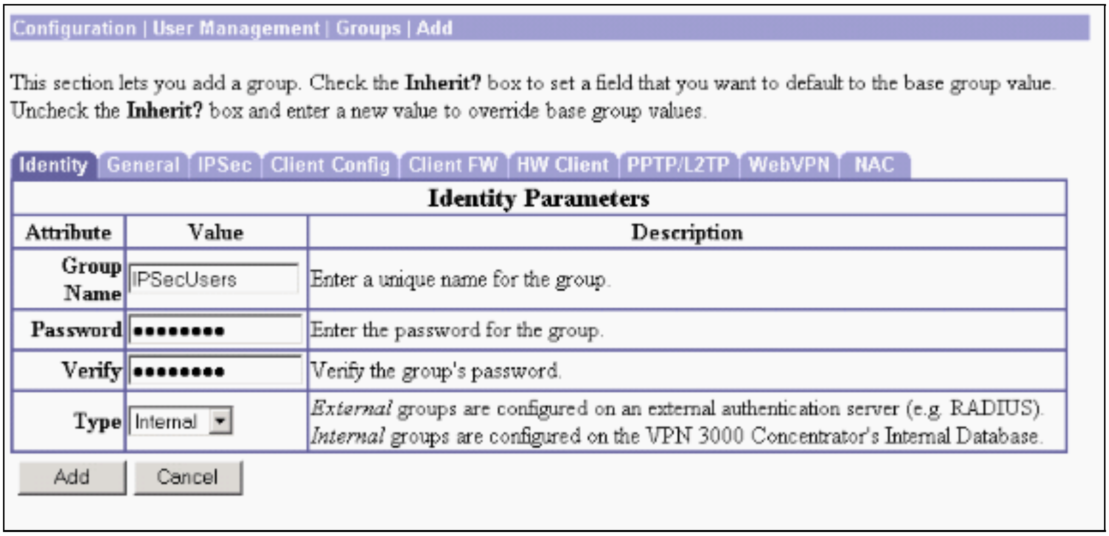
a. Choose **Configuration > User Management > Groups** and click **Add** in order to add a new group.



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.

b. Type a group name (for example, IPsecUsers) and a password.

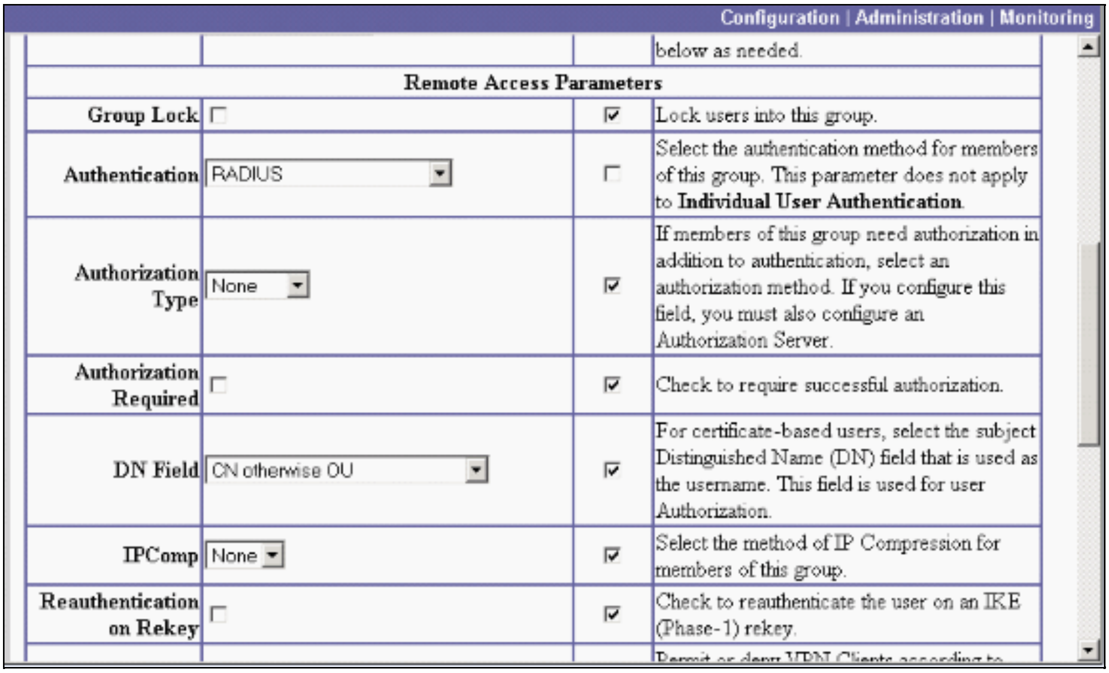


This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity 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	*External* groups are configured on an external authentication server (e.g. RADIUS). *Internal* groups are configured on the VPN 3000 Concentrator's Internal Database.

This password is used as the pre−shared key for the tunnel negotiation.

c. Go to the IPSec tab and set Authentication to **RADIUS**.



			below as needed.
Remote Access Parameters			
Group Lock	□	☑	Lock users into this group.
Authentication	RADIUS	□	Select the authentication method for members of this group. This parameter does not apply to **Individual User Authentication**.
Authorization Type	None	☑	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	□	☑	Check to require successful authorization.
DN Field	CN otherwise OU	☑	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	☑	Select the method of IP Compression for members of this group.
Reauthentication on Rekey	□	☑	Check to reauthenticate the user on an IKE (Phase-1) rekey.
			Permit or deny VPN Clients according to

This allows IPsec clients to be authenticated via the RADIUS Authentication server.

d. Click **Add** at the bottom of the page in order to add the changes to the running configuration.

Now when IPsec clients connect and use the group you configured, they are authenticated by the RADIUS server.

Verify

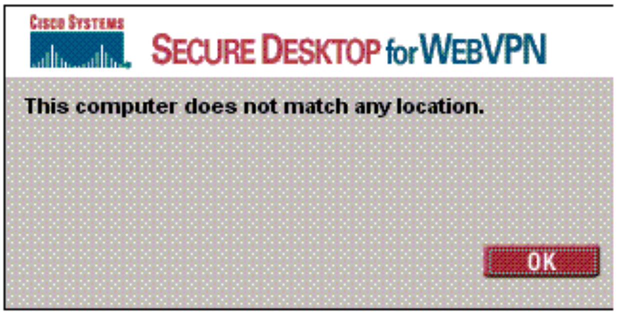
There is currently no verification procedure available for this configuration.

Troubleshoot

WebVPN Authentication Fails

These sections provide information you can use to troubleshoot your configuration.

- **Problem**: The WebVPN users are not able to authenticate against the RADIUS server but can authenticate successfully with the local database of the VPN Concentrator. They receive errors such as "Login failed" and this message.



This computer does not match any location.

Cause: These kinds of problems often happen when any database other than the internal database of the Concentrator is used. WebVPN users hit the Base Group when they first connect to the Concentrator and must use the default authentication method. Often this method is set to the internal database of the Concentrator and is not a configured RADIUS or other server.

Solution: When a WebVPN user authenticates, the Concentrator checks the list of servers defined at **Configuration > System > Servers > Authentication** and uses the top one. Make sure to move the server that you want WebVPN users to authenticate with to the top of this list. For example, if RADIUS should be the authentication method, you need to move the RADIUS server to the top of the list to push the authentication to it.

Note: Just because WebVPN users initially hit the Base Group does not mean that they are confined to the Base Group. Additional WebVPN groups can be configured on the Concentrator, and users can be assigned to them by the RADIUS server with the population of attribute 25 with **OU=*groupname*** . Refer to Locking Users into a VPN 3000 Concentrator Group Using a RADIUS Server for a more detailed explanation.

User Authentication Fails Against the Active Directory

In the Active Directory server, on the Account tab of the User Properties of the failing user, you can see this check box:

[x] Do not require pre−authentication

If this check box is unchecked, **check it**, and try to authenticate again with this user.

Related Information

- **Cisco VPN 3000 Series Concentrators**
- **Cisco VPN 3002 Hardware Clients**
- **IPsec Negotiation/IKE Protocols**
- **RADIUS (Remote Authentication Dial−In User Service) Support Page**
- **Remote Authentication Dial−In User Service (RADIUS)**
- **Technical Support & Documentation − Cisco Systems**

Updated: Mar 24, 2008 Document ID: 20585