

使用Microsoft RADIUS配置Cisco VPN 3000集中器

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[在Windows 2000和Windows 2003上安装和配置RADIUS服务器](#)

[安装RADIUS服务器](#)

[使用IAS配置Microsoft Windows 2000 Server](#)

[使用IAS配置Microsoft Windows 2003 Server](#)

[配置Cisco VPN 3000集中器以进行RADIUS身份验证](#)

[验证](#)

[故障排除](#)

[WebVPN身份验证失败](#)

[针对Active Directory的用户身份验证失败](#)

[相关信息](#)

简介

Microsoft Internet Authentication Server(IAS)和Microsoft Commercial Internet System(MCIS 2.0)目前可用。Microsoft RADIUS服务器非常方便，因为它使用主域控制器上的Active Directory作为其用户数据库。您不再需要维护单独的数据库。它还支持点对点隧道协议(PPTP)VPN连接的40位和128位加密。请参阅Microsoft[核对表：配置IAS以用于拨号和VPN访问文档](#)，以了解详细信息。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档约定的更多信息，请参考 [Cisco 技术提示约定](#)。

在Windows 2000和Windows 2003上安装和配置RADIUS服务器

安装RADIUS服务器

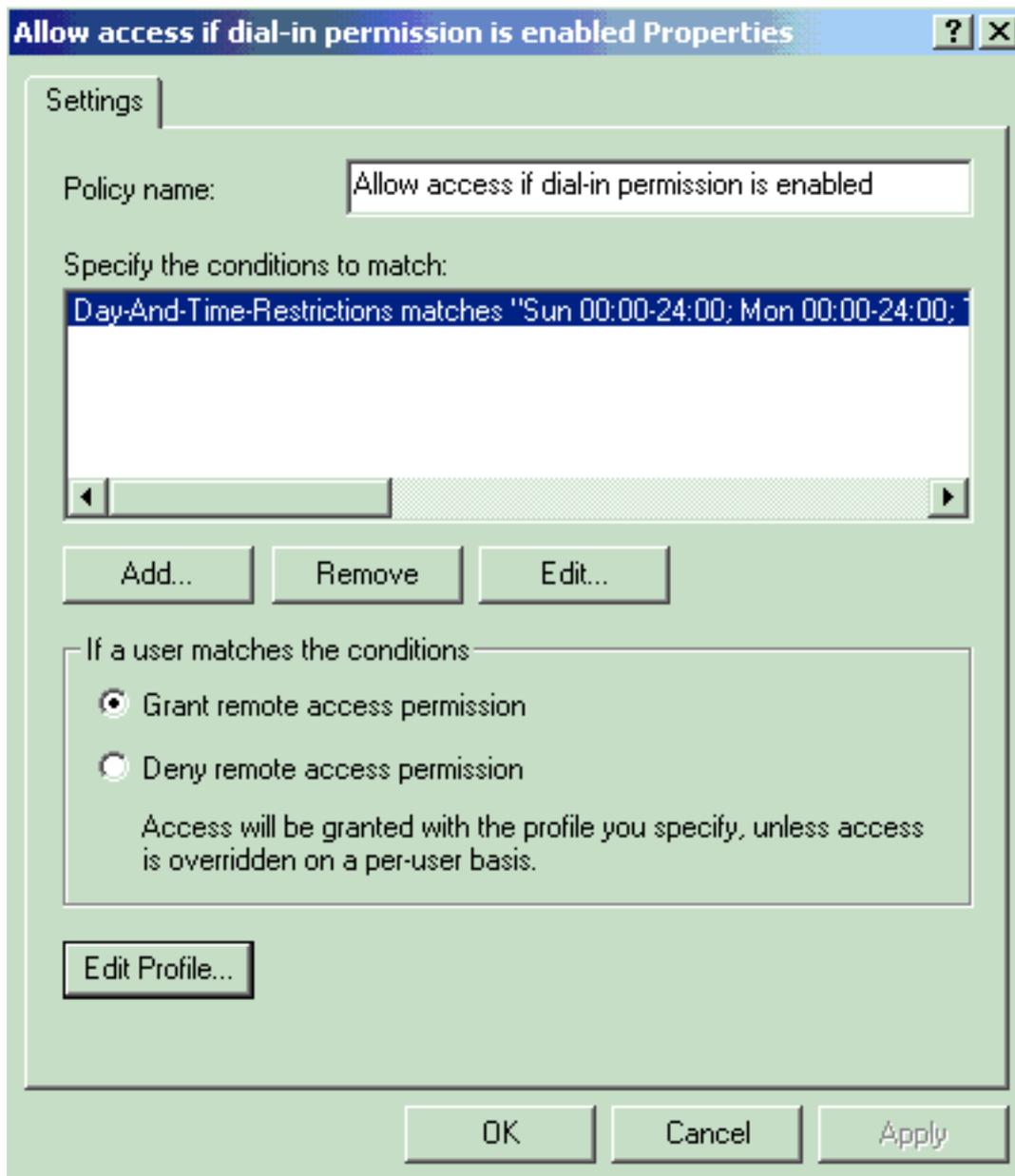
如果尚未安装RADIUS服务器(IAS)，请执行以下步骤以进行安装。如果已经安装了RADIUS服务器，请继续执行[配置步骤](#)。

1. 插入Windows Server光盘并启动安装程序。
2. 单击“Install Add-On Components (安装附加组件)”，然后单击“Add/Remove Windows Components (添加/删除Windows组件)”。
3. 在“组件”中，单击“网络服务”（但不选中或清除复选框），然后单击“详细信息”。
4. 选中“Internet Authentication Service(Internet身份验证服务)”并单击“OK(确定)”。
5. 单击 Next。

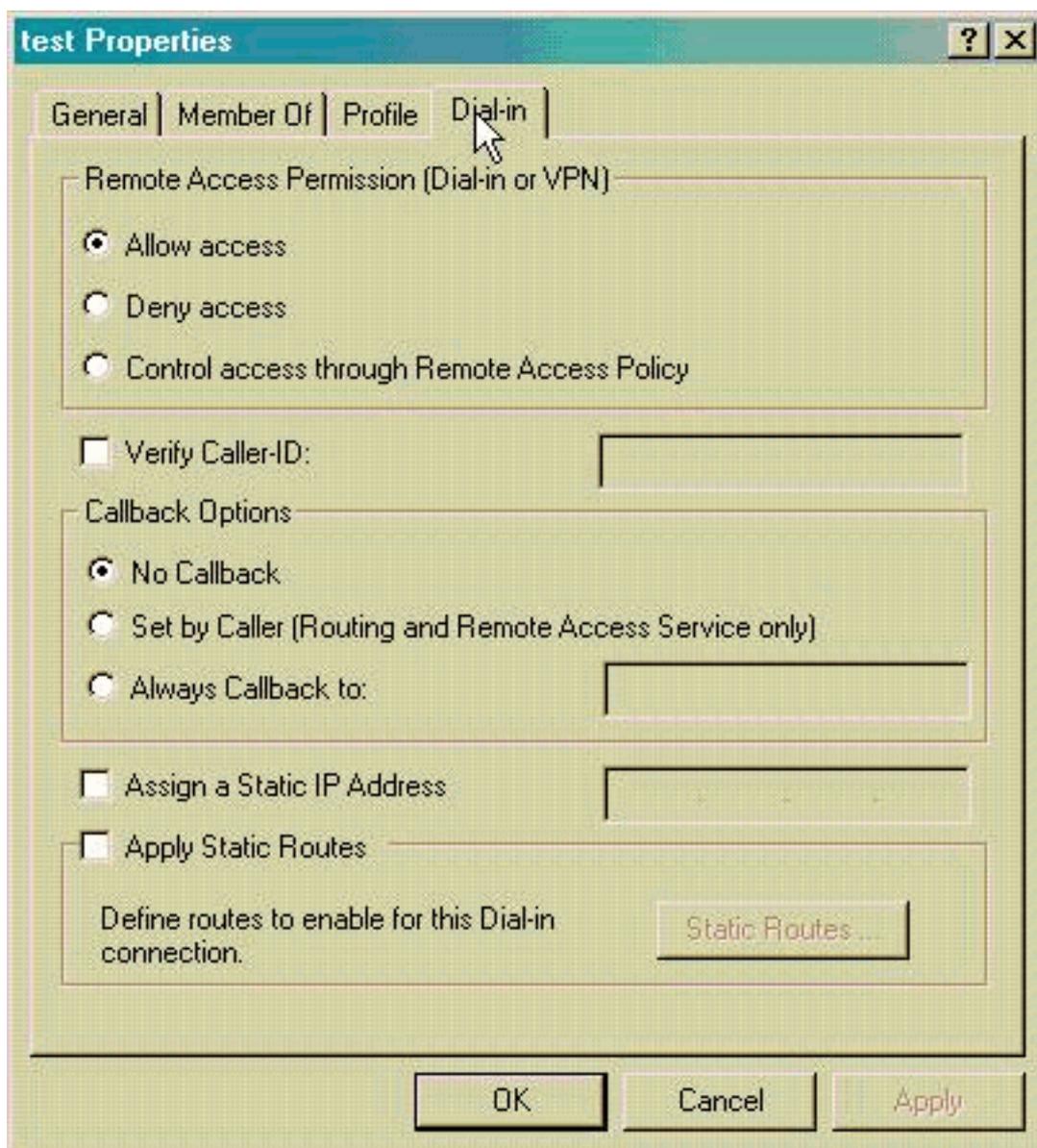
使用IAS配置Microsoft Windows 2000 Server

完成以下步骤以配置RADIUS服务器(IAS)并启动服务，使其可用于对VPN集中器上的用户进行身份验证。

1. 选择开始>程序>管理工具> Internet身份验证服务。
2. 右键单击“Internet Authentication Service(Internet身份验证服务)”，然后从显示的子菜单中单击“Properties (属性)”。
3. 转到RADIUS选项卡以检查端口设置。如果RADIUS身份验证和RADIUS记帐用户数据报协议(UDP)端口与身份验证和记帐中提供的默认值（1812和1645用于身份验证，1813和1646用于记帐）不同，请键入端口设置。完成后，单击**确定**。**注意**：请勿更改默认端口。使用逗号分隔端口，以对身份验证或记帐请求使用多个端口设置。
4. 右键单击Clients并选择**New Client**，以将VPN集中器作为身份验证、授权和记帐(AAA)客户端添加到RADIUS服务器(IAS)。**注**：如果在两个Cisco VPN 3000集中器之间配置了冗余，则备份的Cisco VPN 3000集中器还必须作为RADIUS客户端添加到RADIUS服务器。
5. 输入友好名称并选择为“协议半径”。
6. 在下一个窗口中使用IP地址或DNS名称定义VPN集中器。
7. 从Client-Vendor滚动条中选择**Cisco**。
8. 输入共享密钥。**注意**：您必须记住使用的确切密码。您需要此信息才能配置VPN集中器。
9. 单击 **完成**。
10. 双击**Remote Access Policies**，然后双击窗口右侧显示的策略。**注**：安装IAS后，远程访问策略应已存在。在Windows 2000中，授权基于用户帐户的拨入属性和远程访问策略授予。远程访问策略是一组条件和连接设置，使网络管理员在授权连接尝试时更加灵活。Windows 2000路由和远程访问服务和Windows 2000 IAS都使用远程访问策略来确定是接受还是拒绝连接尝试。在这两种情况下，远程访问策略都存储在本机。有关如何处理连接尝试的详细信息，请参阅Windows 2000 IAS文档。



11. 选择**Grant remote access permission**并单击**Edit Profile**以配置拨入属性。
12. 在Authentication选项卡上选择要用于身份验证的协议。选中**Microsoft Encrypted Authentication version 2**并取消选中所有其他身份验证协议。**注意**：此拨入配置文件中的设置必须与VPN 3000集中器配置和拨入客户端中的设置匹配。在本示例中，使用MS-CHAPv2身份验证而不使用PPTP加密。
13. 在“加密”选项卡上，选中“不加密”。
14. 单击**OK**以关闭拨入配置文件，然后单击**OK**以关闭远程访问策略窗口。
15. 右键单击“**Internet Authentication Service**”，然后单击**控制台树**中的“Start Service”。**注意**：您还可以使用此功能停止服务。
16. 完成以下步骤以修改用户以允许连接。选择**控制台>添加/删除管理单元**。单击**Add**，然后选择**Local Users and Groups**管理单元。单击**Add**。确保选择“**Local Computer(本地计算机)**”单击**完成和确定**。
17. 展开 **Local User and Groups**，然后单击左窗格中的“**Users**”文件夹。在右窗格中，双击要允许访问的用户（VPN用户）。
18. 转到“拨入”选项卡，在“远程访问权限”（“拨入”或“VPN”）下选择“允许访问”。



19. 单击**Apply**和**OK**以完成操作。如果需要，可以关闭控制台管理窗口并保存会话。您修改的用户现在可以使用VPN客户端访问VPN集中器。请记住，IAS服务器仅对用户信息进行身份验证。VPN集中器仍执行组身份验证。

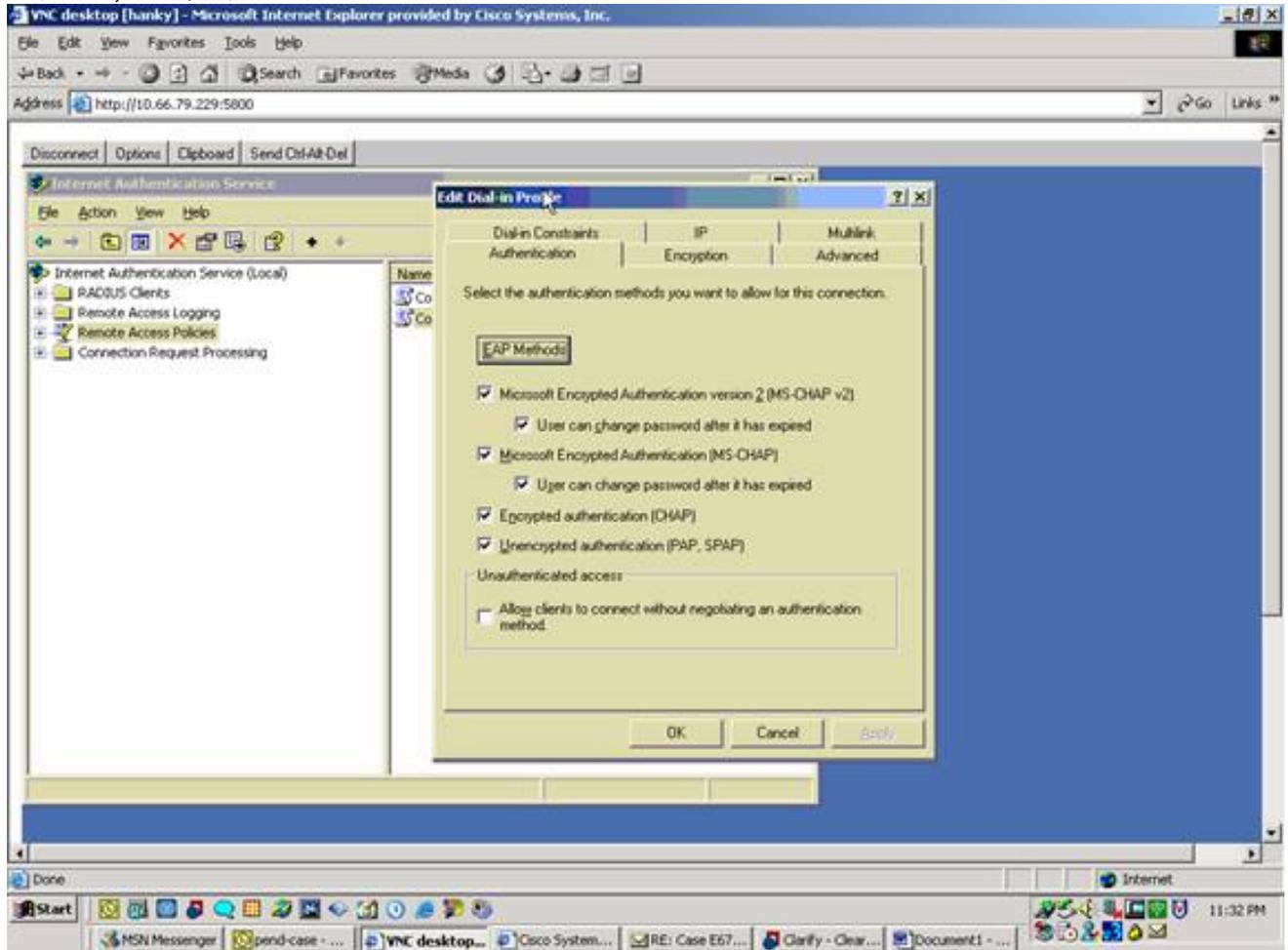
[使用IAS配置Microsoft Windows 2003 Server](#)

完成以下步骤以配置具有IAS的Microsoft Windows 2003 Server。

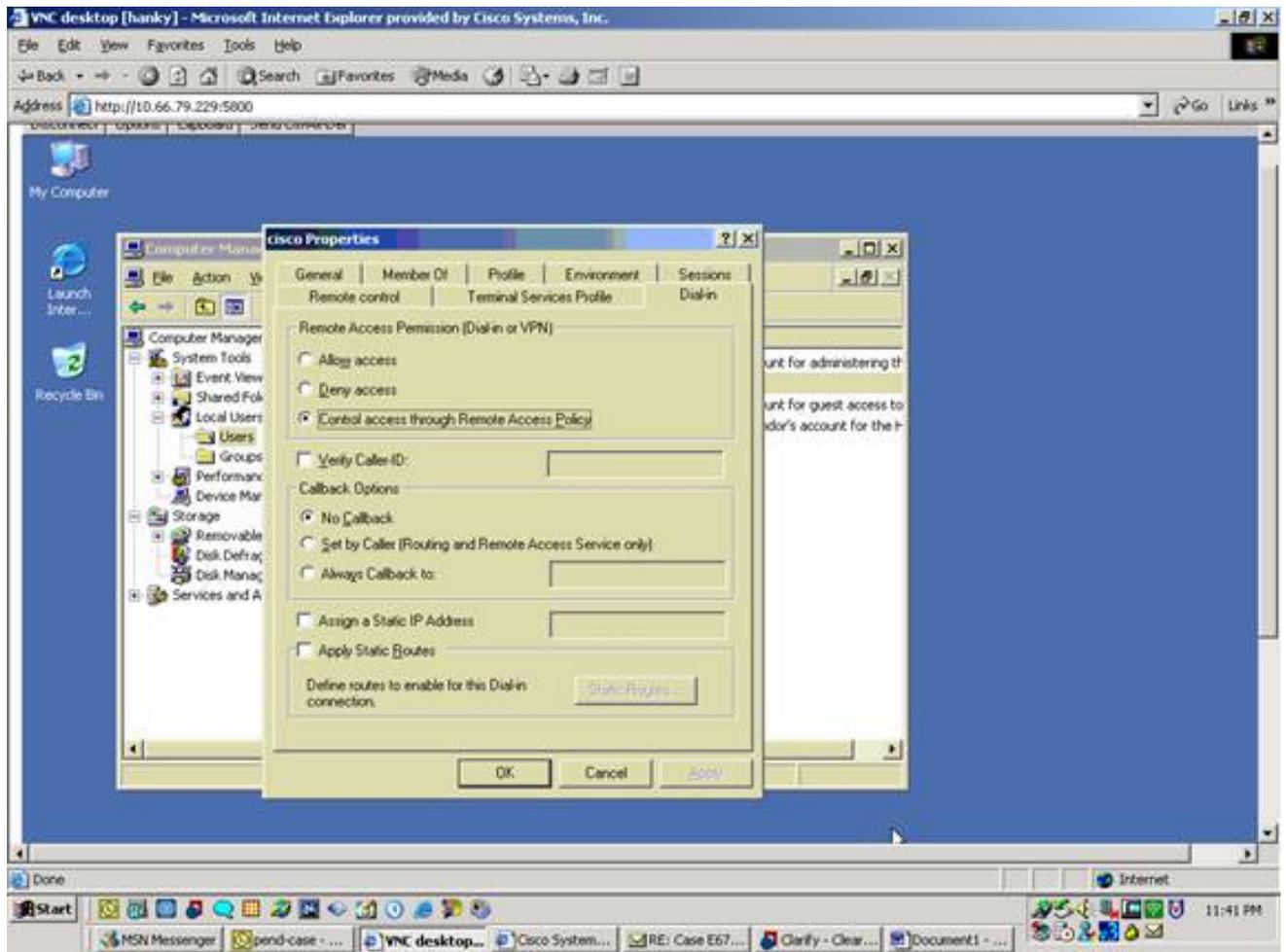
注意：这些步骤假设IAS已安装在本地计算机上。如果未安装，请通过**控制面板 > 添加/删除程序**进行添加。

1. 选择**管理工具 > Internet 验证服务**并右键单击 **RADIUS 客户端**，以添加新的 **RADIUS 客户端**。键入客户端信息后，单击**确定**。
2. 输入友好名称。
3. 在下一个窗口中使用IP地址或DNS名称定义VPN集中器。
4. 从Client-Vendor滚动条中选择**Cisco**。
5. 输入共享密钥。**注意：**您必须记住使用的确切密码。您需要此信息才能配置VPN集中器。
6. 单击 **OK** 完成操作。
7. 转到**Remote Access Policies**，右键单击**Connections to Other Access Servers**，然后选择**Properties**。

8. 选择**Grant remote access permission**并单击**Edit Profile**以配置拨入属性。
9. 在Authentication选项卡上选择要用于身份验证的协议。选中**Microsoft Encrypted Authentication version 2**并取消选中所有其他身份验证协议。**注意**：此拨入配置文件中的设置必须与VPN 3000集中器配置和拨入客户端中的设置匹配。在本示例中，使用MS-CHAPv2身份验证而不使用PPTP加密。
10. 在“加密”选项卡上，选中“不加密”。
11. 完成后，单击**确定**。



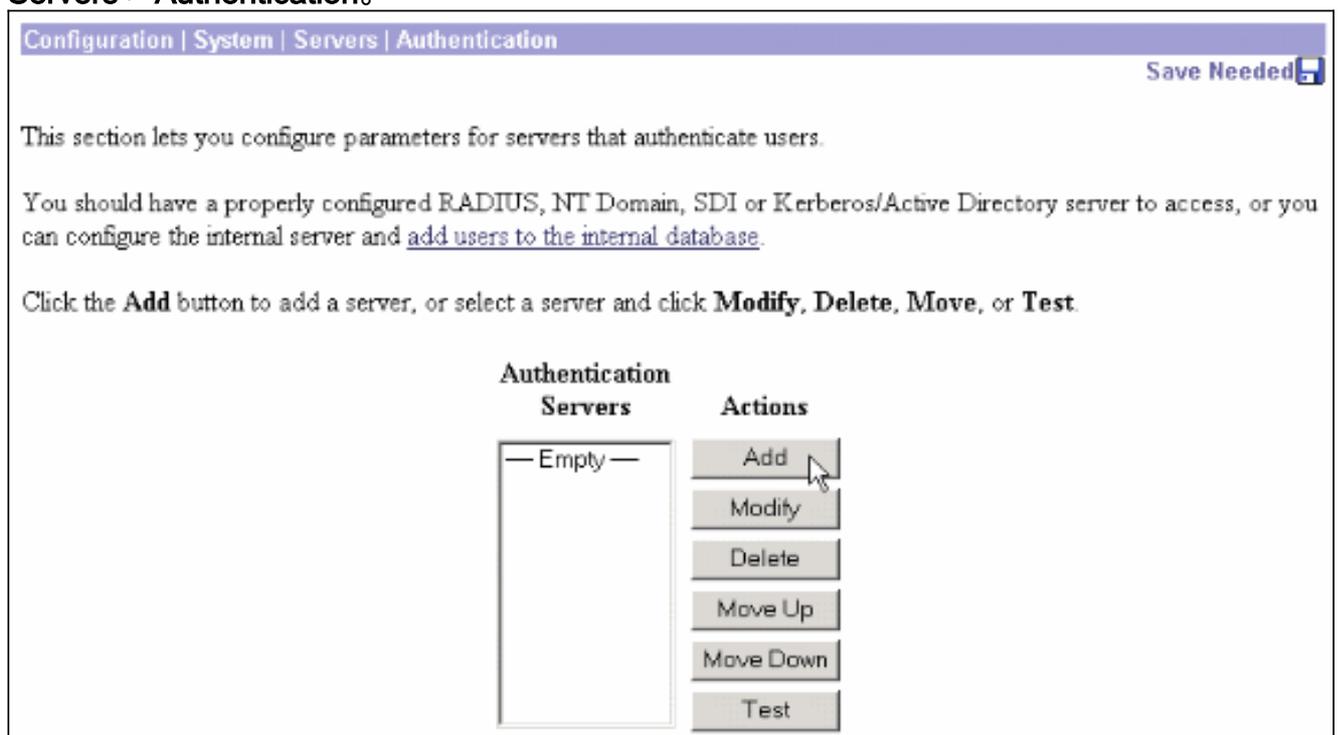
12. 右键单击“**Internet Authentication Service**”，然后单击控制台树中的“**Start Service**”。**注意**：您还可以使用此功能停止服务。
13. 选择**Administrative Tools > Computer Management > System Tools > Local Users and Groups**，右键单击**Users**，然后选择**New Users**，以便将用户添加到本地计算机帐户中。
14. 添加使用思科密码“vpnpassword”的用户并检查此配置文件信息。在“常规”选项卡上，确保选中**口令永不过期**选项而不是“**用户必须更改口令**”选项。在“拨入”选项卡上，选择“**允许访问**”选项（或保留“**通过远程访问策略控制访问**”的默认设置）。完成后，单击**确定**。



配置Cisco VPN 3000集中器以进行RADIUS身份验证

要配置Cisco VPN 3000集中器进行RADIUS身份验证，请完成以下步骤。

1. 使用Web浏览器连接到VPN集中器，然后从左框架菜单中选择**Configuration > System > Servers > Authentication**。



- 单击**Add**并配置这些设置。服务器类型= RADIUS身份验证服务器= RADIUS服务器(IAS)的IP地址或主机名服务器端口= 0(0=default=1645)服务器密钥=与配置RADIUS服务器部分的步骤8中的相同

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.

- 单击**Add**以将更改添加到运行配置。
- 单击**Add**，选择**Internal Server for Server Type**，然后单击**Apply**。您稍后需要此配置才能配置IPsec组（您只需要服务器类型=内部服务器）。

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.

- 为PPTP用户或VPN客户端用户配置VPN集中器。PPTP要为PPTP用户配置，请完成以下步骤。选择**Configuration > User Management > Base Group**，然后单击**PPTP/L2TP**选项卡。选择**MSCHAPv2**，并取消选中PPTP Authentication Protocols部分中的其他身份验证协议。

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 <i>all</i> options means that <i>no</i> 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 <i>all</i> options means that <i>no</i> 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.

Apply Cancel

单击页面底部的**Apply**，将更改添加到运行配置。现在，当PPTP用户连接时，他们由RADIUS服务器(IAS)进行身份验证。**VPN 客户**要为VPN客户端用户配置，请完成以下步骤。选择**Configuration > User Management > Groups**，然后单击**Add**以添加新组。

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"/>

键入组名（例如IPsecUsers）和密码。

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</i> groups are configured on an external authentication server (e.g. RADIUS). <i>Internal</i> groups are configured on the VPN 3000 Concentrator's Internal Database.

Add Cancel

此密码用作隧道协商的预共享密钥。转到IPsec选项卡，将Authentication设置为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

这允许通过RADIUS身份验证服务器对IPsec客户端进行身份验证。单击页面底部的Add，将更改添加到运行配置。现在，当IPsec客户端连接并使用您配置的组时，它们将通过RADIUS服务器进行身份验证。

验证

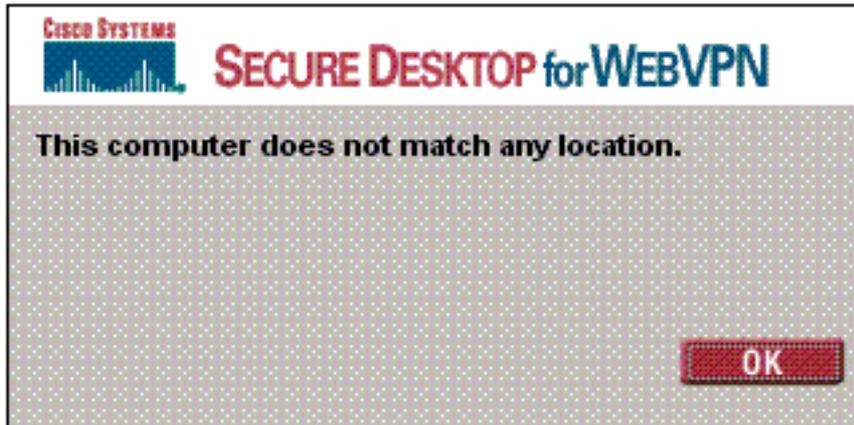
当前没有可用于此配置的验证过程。

故障排除

WebVPN身份验证失败

您可以使用这些部分提供的信息对您的配置进行故障排除。

- **问题：** WebVPN用户无法根据RADIUS服务器进行身份验证，但可以通过VPN集中器的本地数据库成功进行身份验证。他们收到错误，如“登录失败”和此消息。



原因： 当使用集中器的内部数据库以外的任何数据库时，通常会出现这类问题。当WebVPN用户首次连接到集中器时，他们必须使用默认身份验证方法，即会命中基本组。通常，此方法会设置为集中器的内部数据库，而不是已配置的RADIUS或其他服务器。**解决方案：** 当WebVPN用户进行身份验证时，集中器将检查在**Configuration > System > Servers > Authentication**中定义的服务器列表，并使用顶部服务器。确保将希望WebVPN用户进行身份验证的服务器移到此列表的顶部。例如，如果RADIUS应是身份验证方法，则需要将RADIUS服务器移到列表顶部以将身份验证推送到列表顶部。**注意：** 仅仅因为WebVPN用户最初到达了基本组，并不意味着他们仅限于基本组。可以在集中器上配置其他WebVPN组，并且用户可以由RADIUS服务器分配给他们，其属性为25,OU=groupname。有关更[详细的说明，请参阅使用RADIUS服务器将用户锁定到VPN 3000集中器组。](#)

[针对Active Directory的用户身份验证失败](#)

在Active Directory服务器中，在故障用户的用户属性的帐户选项卡上，您可以看到此复选框：

不需要预身份验证

如果未选中此复选框，**请选中**此复选框，然后尝试再次向此用户进行身份验证。

[相关信息](#)

- [Cisco VPN 3000 系列集中器](#)
- [Cisco VPN 3002 硬件客户端](#)
- [IPsec 协商/IKE 协议](#)
- [RADIUS \(远程身份验证拨入用户服务 \) 支持页](#)
- [远程用户拨入认证系统\(RADIUS\)](#)
- [技术支持和文档 - Cisco Systems](#)