



*** Resolution ***

1. The first step is to install IIS on the Windows Server 2003 computer that will act as the Certificate Authority. If IIS is already installed then skip to step 2.

- a. From Control Panel, select Add/Remove Programs.
- b. From Add/Remove Programs, select Add/Remove Windows Components.
- c. Select Application Server and then click on the Details button.
- d. Enable Internet Information Server and then click OK.
- e. Click on Next and then Finish to complete the installation of IIS.

2. The next step is to install Certificate Services on the Windows Server 2003 computer that will act as the Certificate Authority. It's important to note that for best reliability and consistency be sure and install IIS before installing Certificate Services. This will ensure that the proper suppo

rt is installed for web based certificate requests.

- a. From Control Panel, select Add/Remove Programs.
- b. From Add/Remove Programs, select Add/Remove Windows Components.
- c. Select Certificate Services. You will then be presented with a dialog box notifying you that if you continue, you will be unable to change the machine name or the domain membership due to the binding of the machine name to the CA information stored in Active Directory. To continue select Yes and

then Next.

d. Select the type of Certificate Authority you want to create, Stand-alone root CA or Enterprise root CA and the click Next.

e. Enter a common name for the CA – any name is fine, then select Next.

f. At the next prompt select Next to store the certificate database in the default location.

g. At this point you will be prompted to stop IIS. Select Yes and Windows will complete the installation of Certificate Services. Click Finish to exit the installation wizard.

h. To ensure that certificates are automatically issued whenever a request is made we must configure the Policy Module properties. From Administrative Tools, select Certificate Authority to start the Certificate Authority management console.

i. Select the Policy module tab and then select the Properties button.

j. Select the radio button that corresponds to "automatically issue the certificate" and then click OK. You will be prompted to restart the Certificate service so do so now.

3. Now that IIS and Certificate Services are installed, we need to configure Routing and Remote Access on the Windows Server 2003 computer that will host

inbound L2TP connections.

- a. Under Administrative Tools select Routing and Remote Access.
- b. In the Routing and Remote Access management console, right click on the name of the server and select Configure and Enable Routing and Remote Access to start the Routing and Remote Access server Setup Wizard.
- c. Click Next to begin, then select Remote Access (dial-up or VPN) and click Next.
- d. In the next dialog, select the VPN checkbox and click Next.
- e. Select the interface used to connect the RRAS to the Internet and click Next.
- f. Next select the network on which you want the remote clients connected and click Next.
- g. Next specify how IP address assignments will be handled and click Next.
- h. In this example RADIUS will not be used, but if it is then configure that in the next dialog and click Next and then Finish to start the RemoteAccess service.

4. At this point it is best to configure a client and verify that base level PPTP or VPN connections will complete successfully. In this example the client is Windows XP SP1.

- a. From Networks Connections on the client, select Create a New Connection to start the New Connection Wizard, then click Next.
- b. Select Connect to the network at my workplace, then click Next.
- c. Select Virtual Private Network connection and click Next.
- d. Type in a name for the connection and click Next.
- e. If the VPN connection requires an initial connection configure that now.
- f. Type in the host name or IP address of the Windows Server 2003 RRAS and click Next, Next and then Finish.
- g. To test the connection enter the username and password of a user that has permissions to dial in to the network. If the connection succeeds then go on to step 5. If the connection fails then troubleshoot and resolve the issue before proceeding.

5. Now that PPTP/VPN connections work we will want to configure the client and RRAS to use certificates and L2TP. A client authentication certificate must be installed on both the RRAS and the client. Note that you do not need to install a server authentication certificate on the RRAS.

- a. To request and install a client authentication certificate on the client, browse to <[Re: L2TP/IPSec from XP client to Windows 2003 Server](http://> or IP address of the CA>\certsrv.</u>b. Select Request a certificate, then select advanced certificate request.c. Select Create and submit a request to this CA.d. Enter a name and email address in the corresponding fields – any name is and address is fine.e. Under 'Type of Certificate Needed' select 'Client Authentication Certificate'.</div><div data-bbox=)

f. Under 'Key Options' select 'Store certificate in the local computer certificate store', then click the Submit button.

g. Click the Yes button to submit the request, then select 'Install this certificate'.

h. It's a good idea to verify the installation of the certificate at this point. To do so we need to run MMC and add the Certificates snap-in. Click on Start -> Run and run MMC.

i. Select File -> Add/Remove Snap-in.

j. Click the Add button, then select Certificates and Add.

k. Select Computer Account then Next, then select Local Computer and Finish.

l. Close the Add Standalone Snap-ins dialog and then OK on the Add/Remove Snap-in dialog box.

m. In the MMC, go to Console Root -> Certificates (local computer) -> Personal -> Certificates. You should see the certificate you just installed listed here. The name should be whatever name was given in the request screen and the intended purpose should be Client Authentication.

n. Verify that the certificate is valid by double clicking it to bring up the properties. At this point you may see an error with the certificate indicating that the certificate cannot be verified up to a trusted certificate authority. To fix this, within the MMC go to Console Root -> Intermediate

Certification Authorities -> Certificates and find the name of the CA you created in step 2. Using the right mouse button, copy your certificate authority up to Trusted Root Certification Authorities. Once this is done the certificate you requested and installed should appear to be valid.

o. Next install a client authentication certificate on the RRAS by following the exact same steps above.

p. To finalize the installation of the certificate the PolicyAgent service must be restarted. If this is not done the L2TP connection will fail until the client and RRAS are both restarted. To restart the PolicyAgent service on the client type 'Net Stop policyagent' and then 'Net start policyag

ent' from a CMD prompt.

q. Restart the PolicyAgent service on the RRAS, but keep in mind that whenever the PolicyAgent service is restarted the RemoteAccess service must be restarted as well or connections will fail. To restart the RemoteAccess service on the RRAS type 'Net Stop RemoteAccess' and then 'Net Start RemoteAcc

ess' from a CMD prompt.

6. At this point we are ready to test our L2TP connection.

a. From Network Connections, bring up the properties for the PPTP/VPN connection used in step 4 above.

b. On the Networking tab under 'Type of VPN' select L2TP IPSec VPN and then

OK.

c. Initiate the connection from the client and verify that the connection succeeds. If the L2TP connection fails, it's likely that you will receive a 733 error. If you do, you may need to disable and re-enable TCP/IP for the connection on the client to fix this.

d. To verify that L2TP is indeed working bring up the properties of the connection. The Device Name should read 'WAN Miniport (L2TP)' and IPSEC Encryption should read 'IPSec, ESP 3DES'.

e. Now that we know that L2TP connections are working, all that you need to do is specify a RAS policy on the RRAS to determine how inbound connections are established (e.g. only accept L2TP connections) and you're done.

Regards

"Paul" <anonymous@discussions.microsoft.com> wrote in message news:45360620-4BFC-4E1F-BB20-823761CC9AD2@microsoft.com...

> *Why were the last two responses removed from the list?*

> *Are you guys giving up on me?*