

DIS VPN Service Client Documentation

Background-----	1
Downloading the Client-----	1
Installing the Client Software-----	2
Getting Connected-----	4
First Time Users: -----	5
Returning Users:-----	5
Connection Notes-----	6
IP Address Assignment -----	6
'Tunnel Everything' Mode -----	6
Enabling the Client Software to start before the Windows Logon-----	7
VPN Client Statistics-----	7
Troubleshooting -----	8
Logging-----	8
Transport Method-----	9
Common Problems-----	11
Support-----	11

Background

What is VPN?

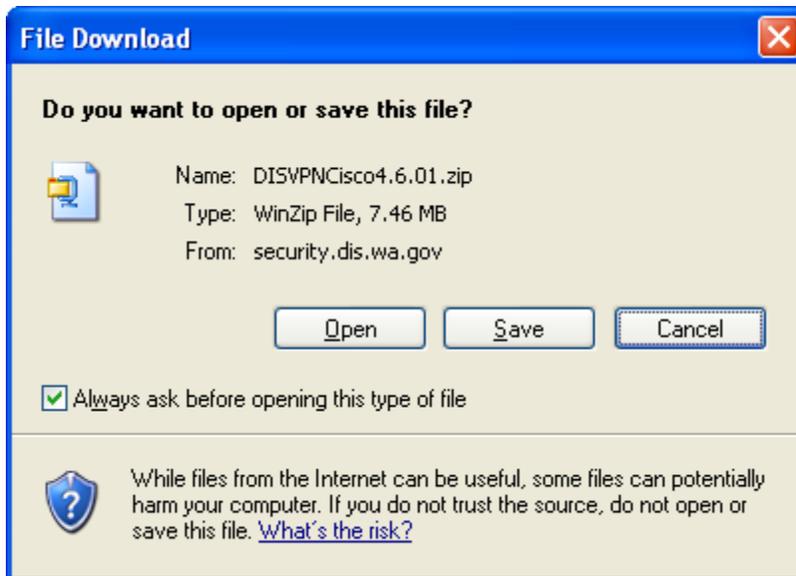
Virtual Private Networks (VPN) use advanced encryption and tunneling to establish secure end-to-end private network connections over third-party networks such as the Internet.

The DIS VPN Service enables traveling employees, telecommuters and branch offices to connect to customer agency networks (Intranets, Extranets) whenever and wherever they require. The DIS VPN Service provides security, affordability, connectivity, reliability, and productivity.

Downloading the Client

The Cisco VPN Client software available from the DIS Enterprise Security Services web site has been preconfigured for the DIS VPN Service offering. This software is available for download as a zip file at <http://security.dis.wa.gov/vpn>. This web site is only available for access from the State Governmental Network (SGN) and the Intergovernmental Network (IGN).

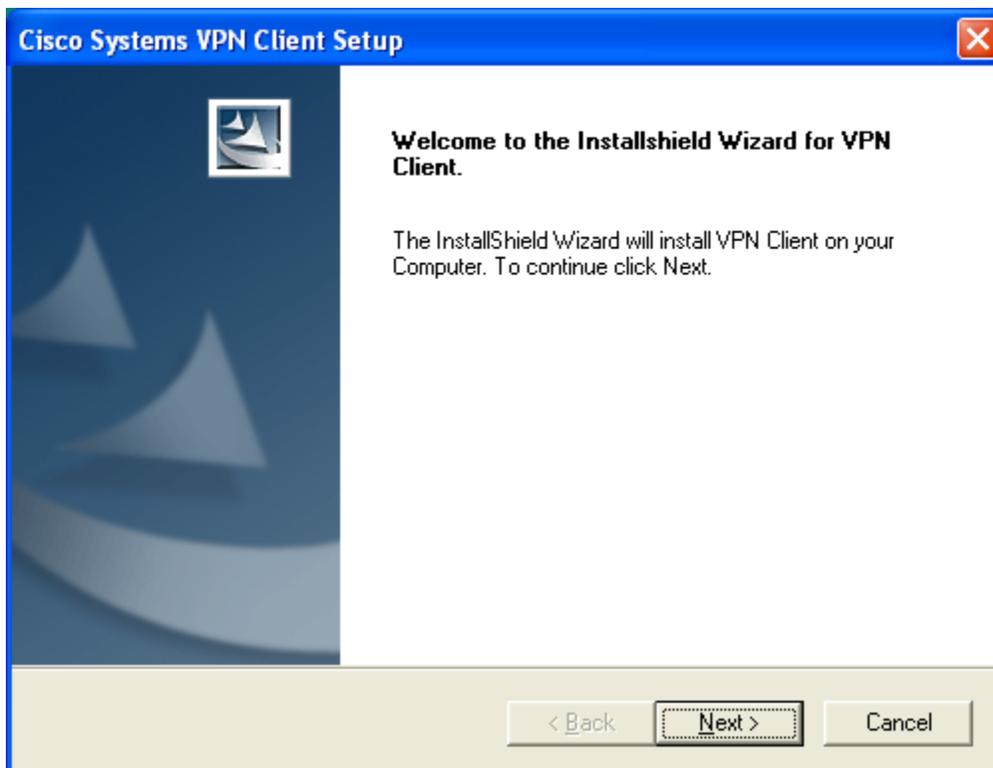
After the file is downloaded, extract the software either to a permanent file location, or allow the compression utility software to choose a temporary location.



Installing the Client Software

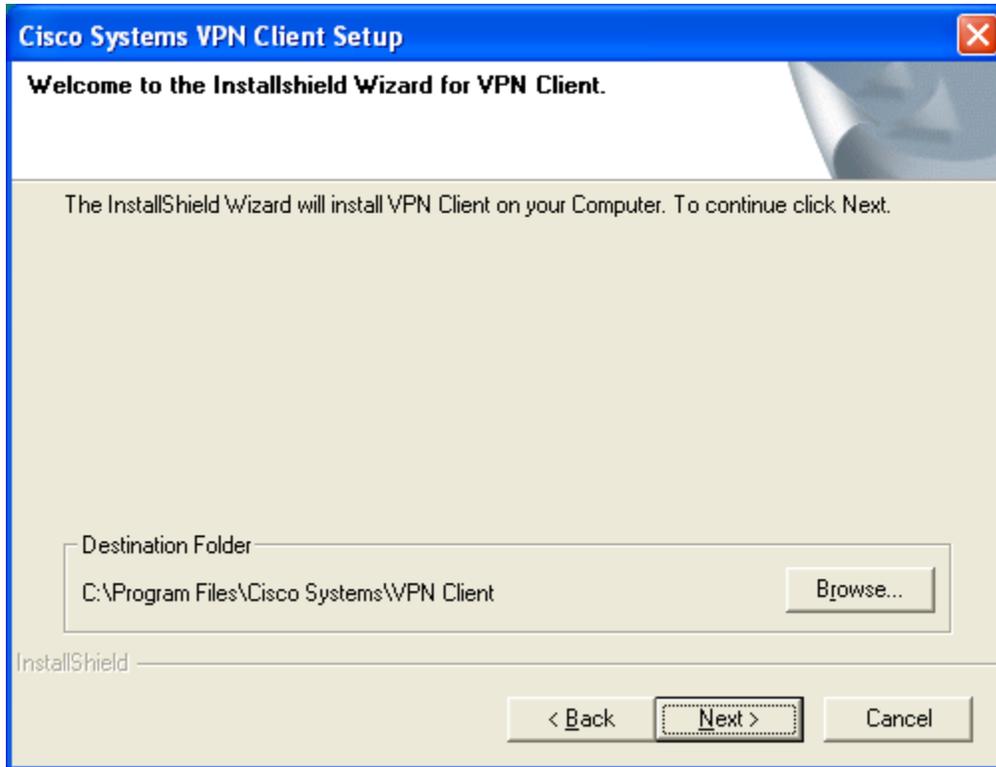
Please note that the workstation will require a reboot after installation of the Cisco VPN software is complete.

After extracting the contents of the zip file, run the Setup.exe program, the following window will appear:



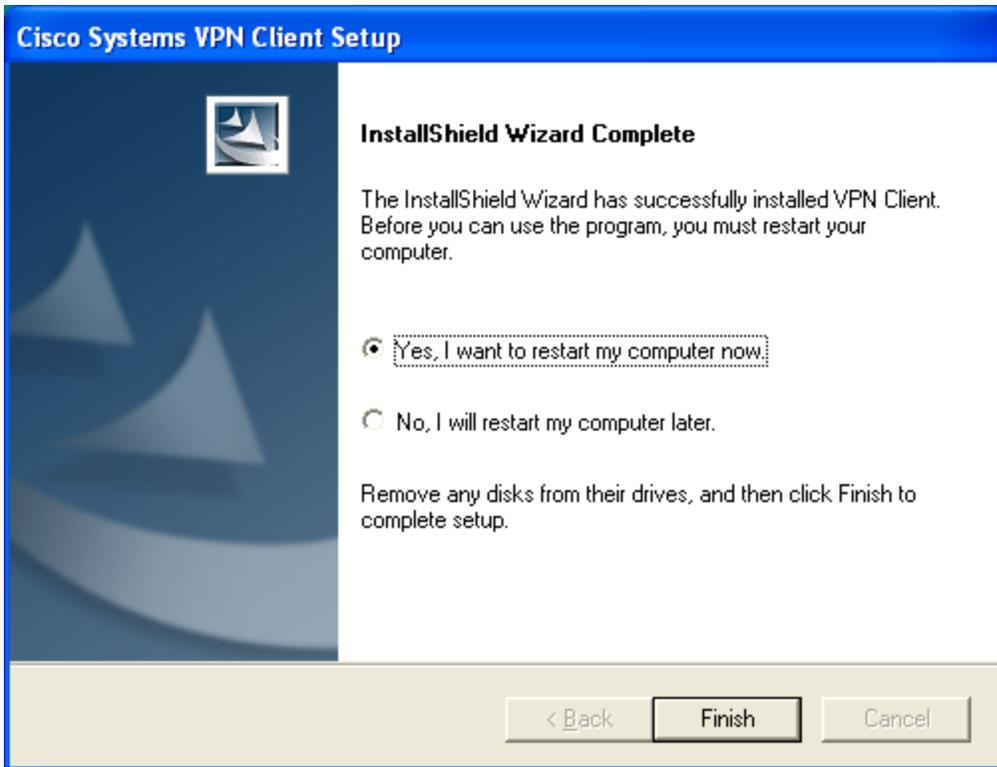
1. Click "Next" to begin installation of the client software.
2. Click "Yes" to accept the license agreement

You will then be presented with the following screen:



3. Click "Next" to accept the default installation directory.

Once the program is successfully installed, the following screen will appear:

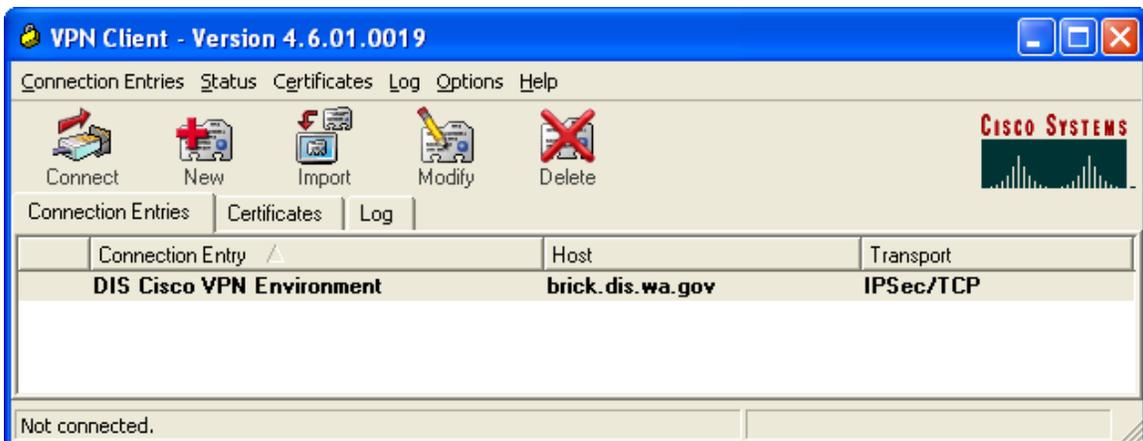


4. Click "Finish" and wait for reboot to complete.

Getting Connected

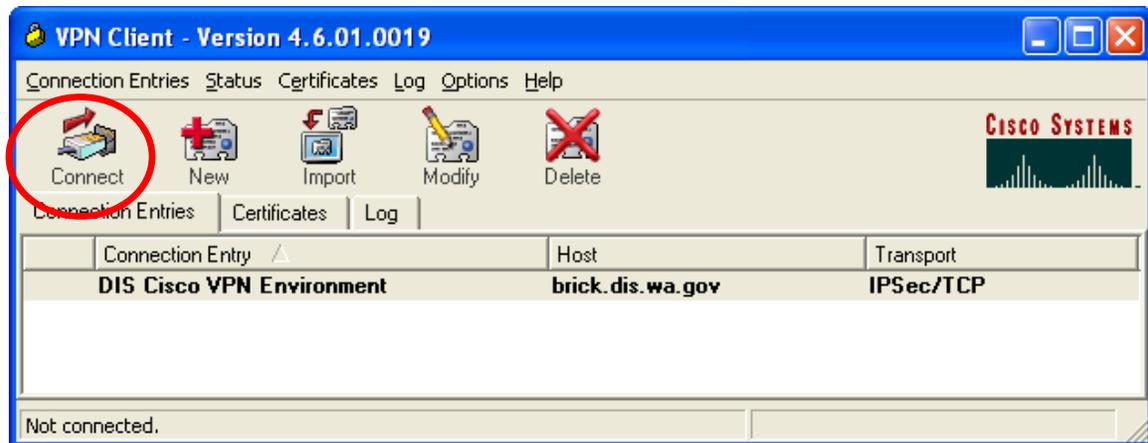
To launch the VPN Client, select **Start > All Programs > Cisco Systems VPN Client > VPN Client**.

The VPN Client Software application will present the following screen. If no connection entries are listed under the connection entries tab, contact the agency VPN technical contact to learn how to enter this information manually.



Please note that by default the transport type is IPSec/TCP, also known as “transparent tunneling.”

1. Click the connect icon in the upper left to initiate the connection.



The 'VPN Client | User Authentication for ...' window appears.



First Time Users:

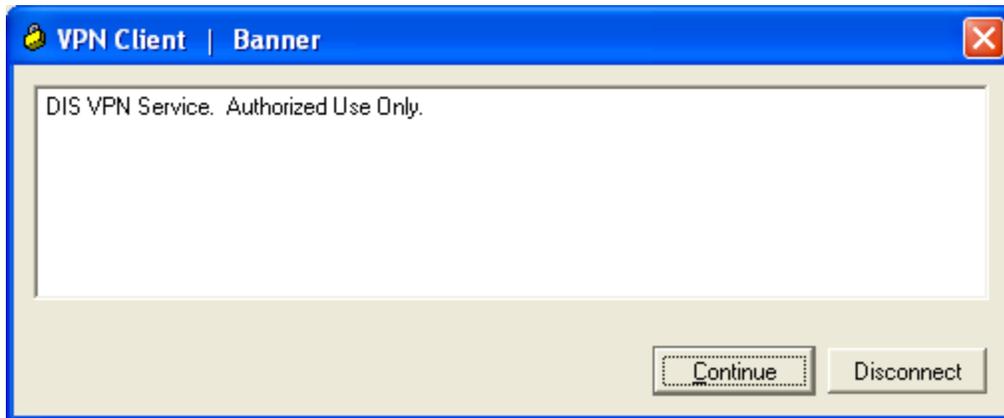
- Enter your UserID, e.g. smith155 in the **Username** field
- Enter the 6-digit token code currently displaying on your RSA SecurID token in the **Password** field
- Enter a 4-digit PIN when prompted
- Re-enter the 4-digit PIN when prompted for confirmation
- After seeing the successful authentication banner, all future connection attempts will require the use of a One-Time Password, which is the PIN followed by the 6-digit token code.

Returning Users:

- Enter your UserID, e.g. smith155 in the **Username** field
- Enter your **One-Time Password (OTP)**, made up of your PIN and the 6-digit token code currently displaying on your RSA SecurID token, in the **Password** field.

2. Click the “OK” button to authenticate.

After successfully authenticating, a banner window will appear with a similar message.



3. Click the “Continue” button. The windows will disappear and a closed yellow padlock will be displayed in the system tray (near the clock) symbolizing that a secure VPN connection is active.



Connection Notes

Now that a VPN connection has been successfully made, verify that routing is occurring properly by accessing an application or intranet site that is only available from within State network.

IP Address Assignment

After establishing a connection to the DIS VPN Service, the remote workstation is assigned an IP address based upon the group to which the User ID has been assigned. This IP address is taken from an address pool which the customer agency has granted permission to access their network resources.

The IP address assigned to a remote computer may differ with each individual connection based upon the number of addresses available and the VPN device to which the connection is made.

‘Tunnel Everything’ Mode

By default, all traffic from the remote workstation is encrypted and routed through the VPN tunnel when connected. This means that when accessing a site such as www.google.com, traffic is being sent through a DIS managed firewall and then being routed to the Internet.

Enabling the Client Software to start before the Windows Logon

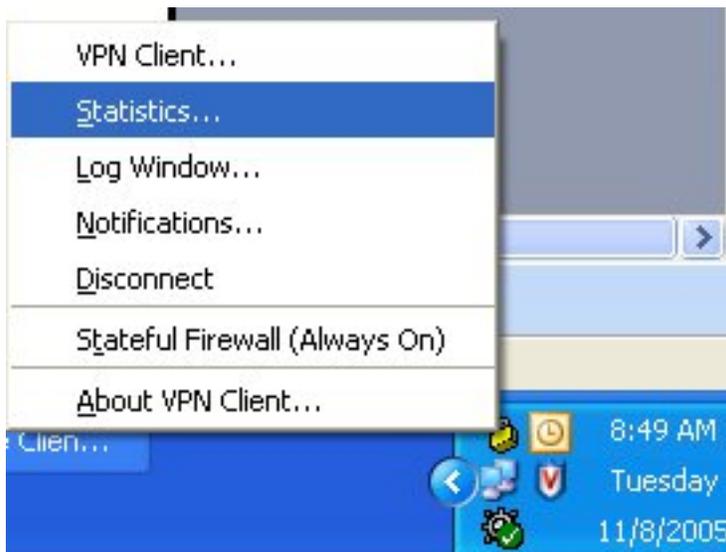
In many instances, a user may want the VPN Client Software to launch prior to logging into their Windows Domain. To enable this feature:

1. Open the VPN Client Software
2. Click Options, 'Windows Logon Properties...'
3. Check the 'Enable start before login' checkbox and click 'OK'

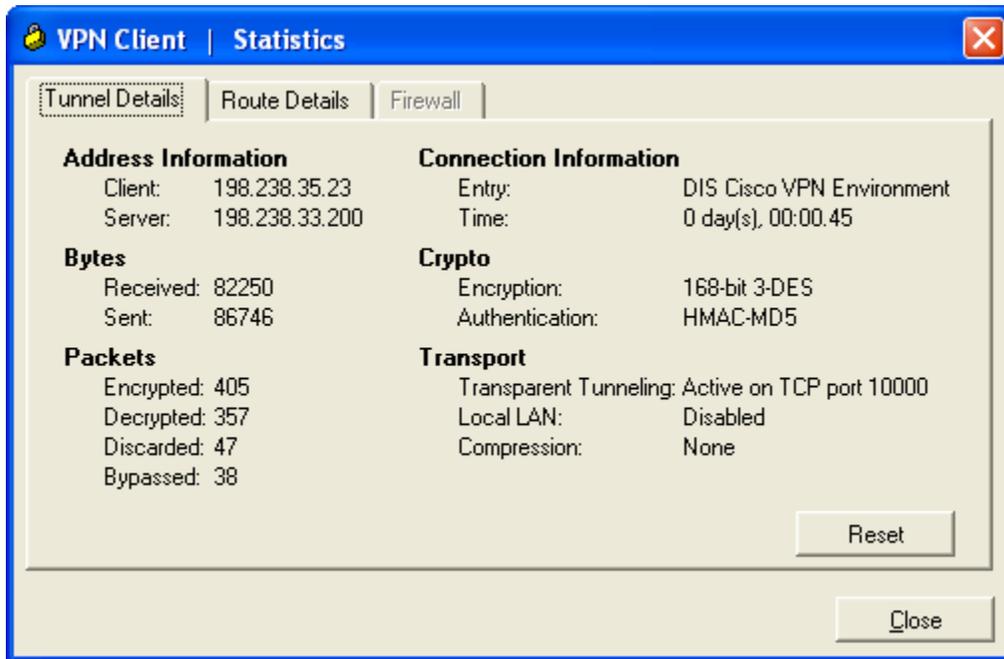


VPN Client Statistics

To view a window displaying statistical information on the current connection, right-click on the yellow padlock in the status bar.



Choose the “Statistics...” option, and the following window will be displayed.



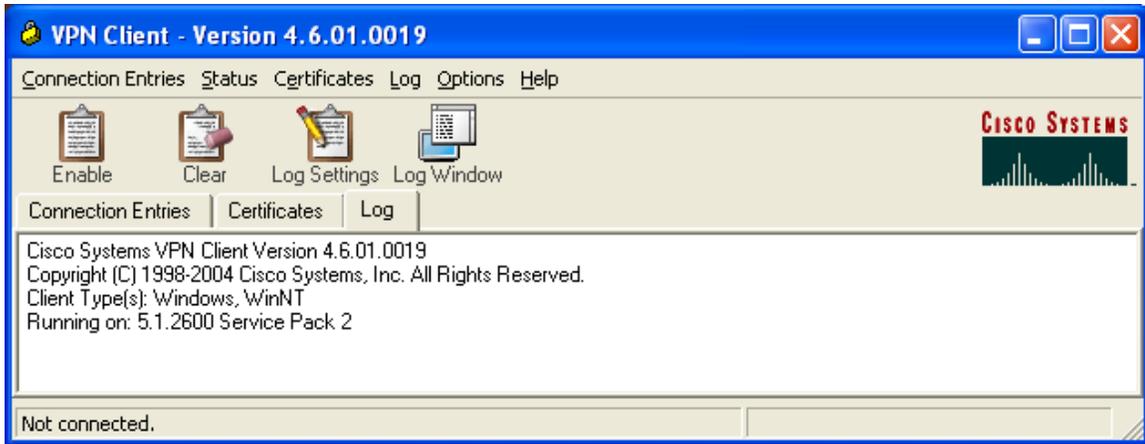
Troubleshooting

If there is need for further information on the client software, the Cisco VPN Client Software documentation can be found on the DIS VPN Service site at <http://security.dis.wa.gov/VPN/Documents.asp>.

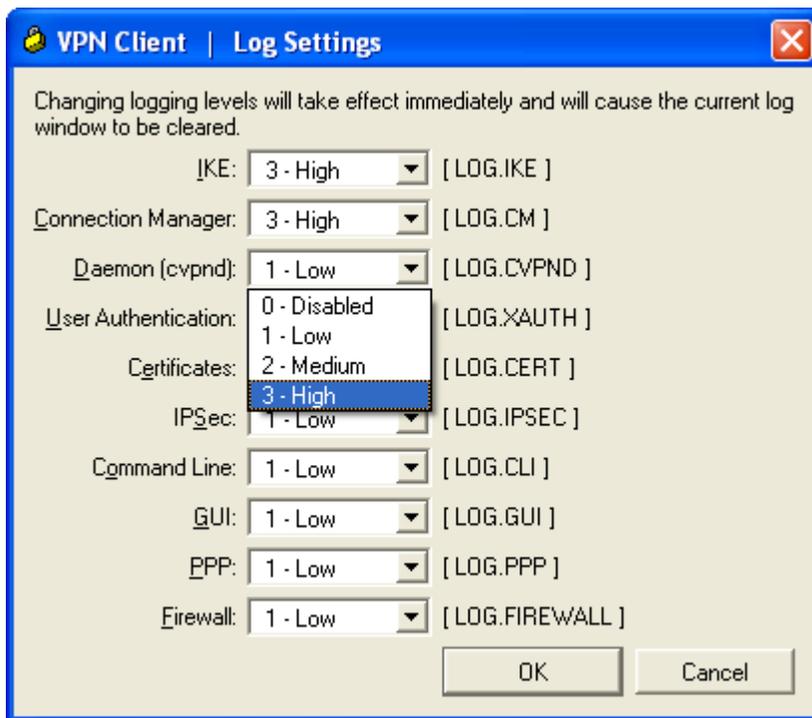
Logging

To troubleshoot problems with a VPN connection, logging may need to be enabled to determine the source of the problem.

1. Start the VPN Client Software, once the Main Window appears, click the Log tab.



2. Click the Log Settings icon. Change all of the drop-down menus on this window to “3-High.” Click “OK” when finished.



3. Click the “Enable” icon to have the client software maintain a log of all items involved with the VPN connection.

Note: The Enable icon will toggle between Enable and Disable, if logging is currently off, the icon will be Enable.

Transport Method

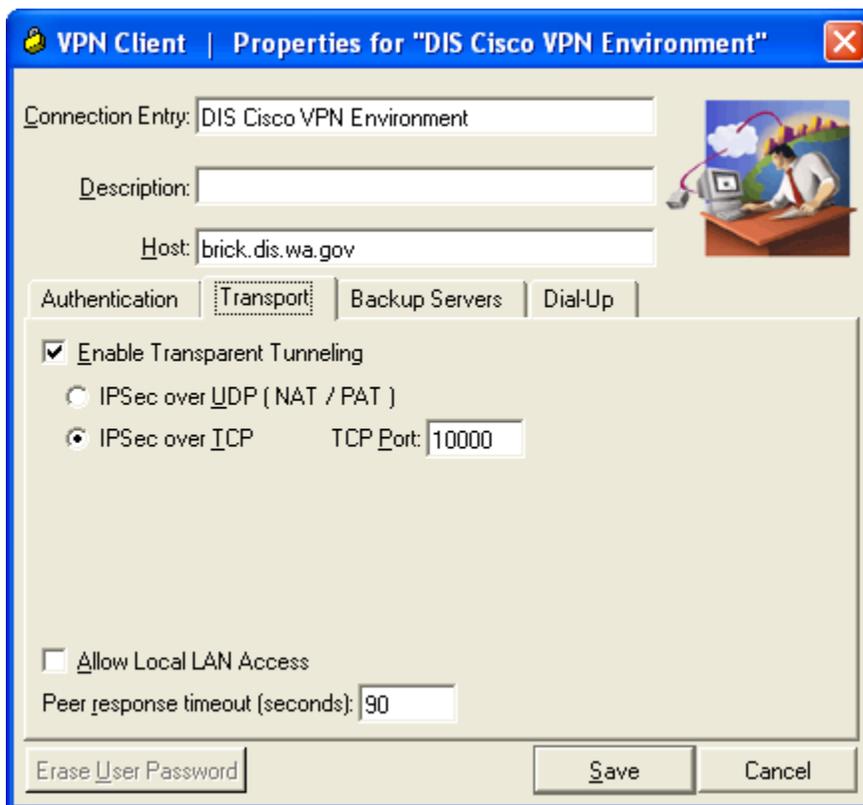
By default, the transport method of the VPN client software is to use IPsec/TCP over port 10000. When troubleshooting a routing issue, this may be disabled.

To disable transparent tunneling:

1. Start the VPN Client Software
2. Highlight the connection entry for the DIS Cisco VPN Environment
3. Click the 'Modify' icon



The following screen will be displayed.



4. Uncheck the 'Enable Transparent Tunneling' box, and click 'Save.'

Common Problems

Error	Possible Remedy
VPN Client Software responds with: Error 403, unable to contact the security gateway	Verify Internet connectivity by attempting to connect to a web page which is not already browser cached. http://www.ipchicken.com will give information about your current IP address to see if NAT is present.
VPN Client Software prompts multiple times for the User ID and Password after entering this information	Verify that the correct Password of PIN followed by 6-digit tokencode is being entered. The PIN code can be reset by the DIS Help Desk.
VPN Client Software prompts for User ID and Password, but then does not connect.	Verify that there is not a software firewall in place on the workstation that is restricting the VPN connection
VPN Client Software connects successfully, but no routing occurs.	Verify that no routing occurs by trying to establish a connection with both an internal Intranet Site and an external Internet site. Toggle the transport method as per the earlier description and attempt to reconnect.
VPN Client Software connects successfully, can reach some Internal hosts but not others.	Verify that there is not an ACL in place restricting access to certain IP's.

If an error code is received and is not represented in the table above, consult [Cisco's VPN 3000 Client GUI Error Dictionary](#).

Support

VPN users should first contact their agency VPN Technical Contact for help with VPN.

For agency VPN Technical Contacts, installation support is available from 9:00am to 5:00pm, Monday through Friday. The DES Solutions Center phone # is: **(360) 407-9100**

If you suspect a problem with the DIS VPN Service, the above Solutions Center number is available 24 hours a day/seven days a week.