

Duke Office of Information Technology

Remote Access Options

Connecting from off-campus

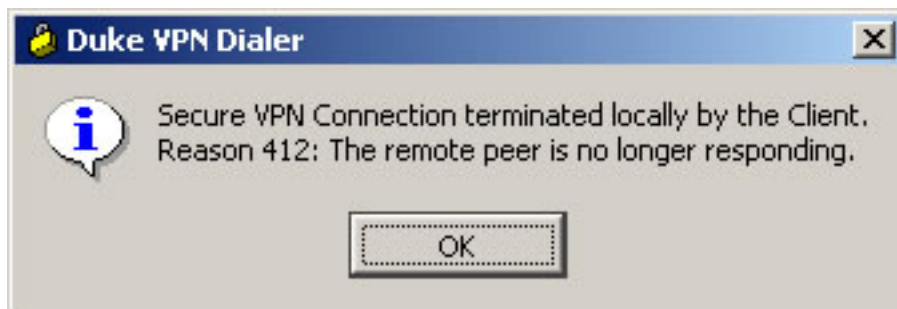
Troubleshooting VPN connection issues

When attempting to connect to Duke's Campus via the VPN Dialer, there are many considerations that have to be accounted for which can cause difficulties that prevent the VPN from establishing a connection. Following are various things to check through which may have effects on any VPN connection.

1) Uninstall/Re-install: As with many other applications, if you ever experience any difficulties with functionality, it is always a good idea to uninstall and re-install the application. The Duke VPN dialer is preconfigured by Network Services, therefore, there are no configuration changes or tweaking needed to get the VPN to work. For this reason, the Helpdesk often recommends users uninstall the VPN and consider the other options in this document as possible culprits, then re-install the VPN software. In many instances, a simple uninstall/re-install may be sufficient; however, to be on the safe side it is better to uninstall, follow the suggestions from the other problem areas in this document, and finally re-install after checking all the other possibilities.

NOTE: The VPN software can be removed from Windows systems by accessing Add/Remove Programs from the Control Panel and Macintosh users can simply drag the application to the Trash

2) Firewall: Do you have a personal firewall installed on the machine in which the VPN Dialer is attempting to make a connection? Often, a firewall will be configured to allow outgoing traffic, but block any incoming traffic. If this is the case the VPN will not connect and return error:

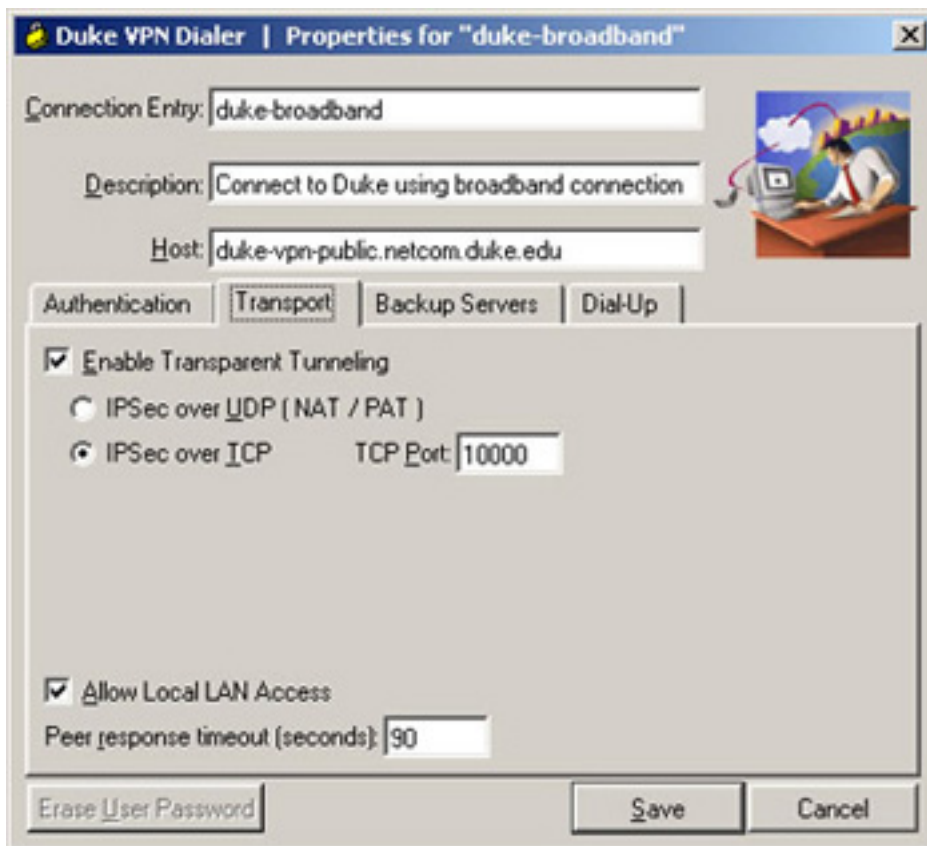


This error is will be displayed before you ever see a login screen allowing you to enter your NetID and password. If you see the error above and have a personal firewall, you will need to configure the firewall to allow the incoming VPN traffic. One option is to ensure your firewall asks whether or not you choose to permit or deny traffic. The Helpdesk does not recommend disabling the firewall; however, for testing purposes you may consider disabling the firewall long enough to establish a connection. If the firewall

is disabled and you successfully connect, this is often a good indication the firewall needs to be reconfigured.

3) Router: Many people now have personal routers in their homes creating personal networks in home to allow multiple computers the ability to connect to the internet. Depending on the features of the router, there may be settings that prevent VPN connections. One setting is called Stateful Packet Inspection (SPI). If SPI is enabled on your router, chances are the VPN connection will not establish. Another option when using a personal router is to ensure the router allows traffic to transmit across port 10000. To ensure your router is configured so that port 10000 is open, you may need to contact the manufacturer of the router.

4) Businesses: Many business networks prevent traffic not deemed appropriate by the company. If you are at another place of business when trying to connect via the Duke VPN Dialer, you will need to ensure first that VPN traffic is allowed, and secondly that any firewalls on the network permit traffic via port 10000. You may need to contact IT support for the business to determine what is allowed. Once you confirm port 10000 is allowed, you will need to make a slight configuration change to your VPN client. NOTE: These changes should only be made if you are connecting from another business. First, ensure you have the appropriate connection selected (most likely duke-broadband) and click the "Modify" button. This will open the properties page for the connection. Next click the "Transport" tab. As shown below, change the transport method to IPSec over TCP and ensure the port is set to 10000.



5) Virus/Spyware Infections: Just as with other applications, virus and spyware problems can cause issues with the VPN. The Helpdesk recommends you update your anti-virus applications and scan for any infections whenever you experience difficulties connecting. Hand-in-hand with virus infections, are spyware/malware problems.

Currently the Helpdesk recommends users combat spyware/malware with tools such as Ad-Aware, Spybot Search & Destroy, and Spywareblaster (all of which are for Microsoft Windows users only). These tools along with other adequate applications can be downloaded for free from <http://www.download.com>

6) Winsock Fix (for Microsoft Windows only): The VPN establishes a network connection to Duke's campus. Within Microsoft Operating Systems, there is a file, winsock.dll, that if corrupted can cause issues amongst various network connections such as the VPN. For additional information on the winsock file, please visit information from [Microsoft](#). If this file is corrupted, there is a tool called the Winsock Fix Tool which will repair the winsock.dll file, force a reboot of the system, and often correct any issues after the system is restarted. The Helpdesk generally recommends running this application after you have uninstalled the VPN software. To download the Winsock Fix Tool, please [click here](#).

If you have issues with the VPN and the information above does not seem to remedy the problem, please contact the helpdesk at 919-684-2200.

[Back to top](#)

Duke Office of Information Technology - www.oit.duke.edu - (919) 684-2200 - help@oit.duke.edu