

## AFTER ENROLLING – USING THE CLIENTLESS VPN

Accessing the Clientless VPN is the next step when:

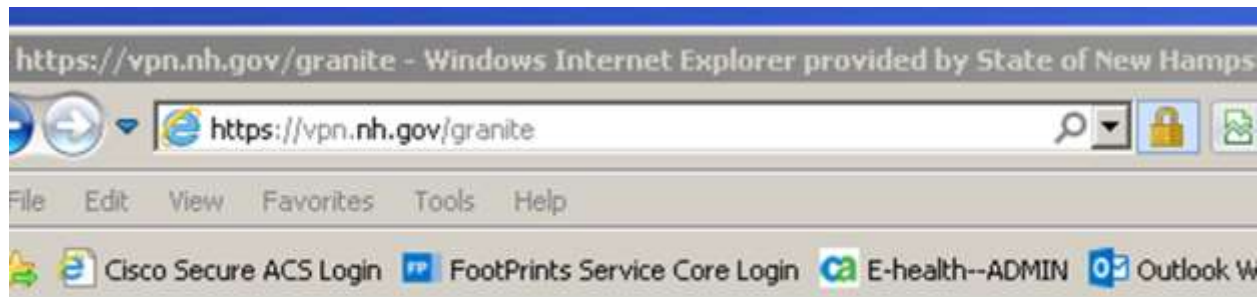
- you need to download AnyConnect (if authorized to use it)
- you need to update your version of AnyConnect or get a different profile for a different domain
- you are a clientless VPN user, to include using a smart-tunnel

Step 1: open Internet Explorer again and go to the same address you used to enroll:

<https://vpn.nh.gov/<domainname>> -- You MUST put in the domain name.

**NOTE:** Behind the scenes the VPN process re-directs people to the appropriate VPN user section based on the domain they list in the address. If you save the address as a Favorite or Bookmark in your browser, make sure that the address for the link is the correct <https://vpn.nh.gov/<domainname>> that you typed in, and NOT the redirect address.

Notice in the screen below, the domain name is granite, and a window popped up to confirm the certificate to use for the VPN. If more than one certificate existed there is the link to “click here to view certificate properties” to help you choose the right one. The certificate validity dates are also displayed.



Once you click on the certificate and select OK, you are taken to the next screen. Note that this time your username is already pre-filled in. If it is not pre-filled there is an error in the process, check the frequently asked questions or the Help Desk to resolve.

Assuming your name is prefilled, just type in your password and click Login.



The screenshot shows a Windows Internet Explorer browser window titled "SSL VPN Service - Windows Internet Explorer provided by S McAfee". The address bar displays "https://vpn.nh....". The browser's menu bar includes File, Edit, View, Favorites, Tools, and Help. The toolbar shows icons for home, back, forward, and search, along with a search bar. Below the toolbar, there are links for "Cisco Secure ACS Login" and "FootPrints Service Core Login". The main content area has a yellow header with the New Hampshire state seal on the left and the text "New Hampshire Granite Domain" in large red font, with "Secure Remote Access" in smaller red font below it. In the center of the page is a "Login" dialog box with a key icon in the top-left corner. The dialog box contains the text "Please enter your Granite Domain username and password." and two input fields: "USERNAME:" with the value "jeffrey.d.pomeroy" and "PASSWORD:" which is empty. A "Login" button is at the bottom of the dialog box.

The next screen will display a warning notification that the VPN is for official use only and that your activity is subject to the same monitoring and restrictions that you have when you are at work on your office PC. After reading the statement, click Continue.



# New Hampshire VPN - NetOps

Secure Remote Access

**\*\*WARNING\*\*** This is a State of NH secure access system and is provided only for authorized use. Users have no implicit or explicit expectation of privacy. State and federal statutes make it a crime to attempt and/or gain unauthorized access. Unauthorized use may be subject to criminal, civil and/or administrative action. !!!

Cancel

Continue

Congratulations, you are now logged into the clientless VPN. The exact screen and options available will depend on what options and resources a person is authorized to use. If you are authorized to only use the clientless VPN, then the AnyConnect button shown below will not appear on that screen. The same with the SSH/Telnet button if you are not authorized for that.



## New Hampshire VPN - NetOps

Secure Remote Access

Home

Web Applications

Browse Networks

AnyConnect

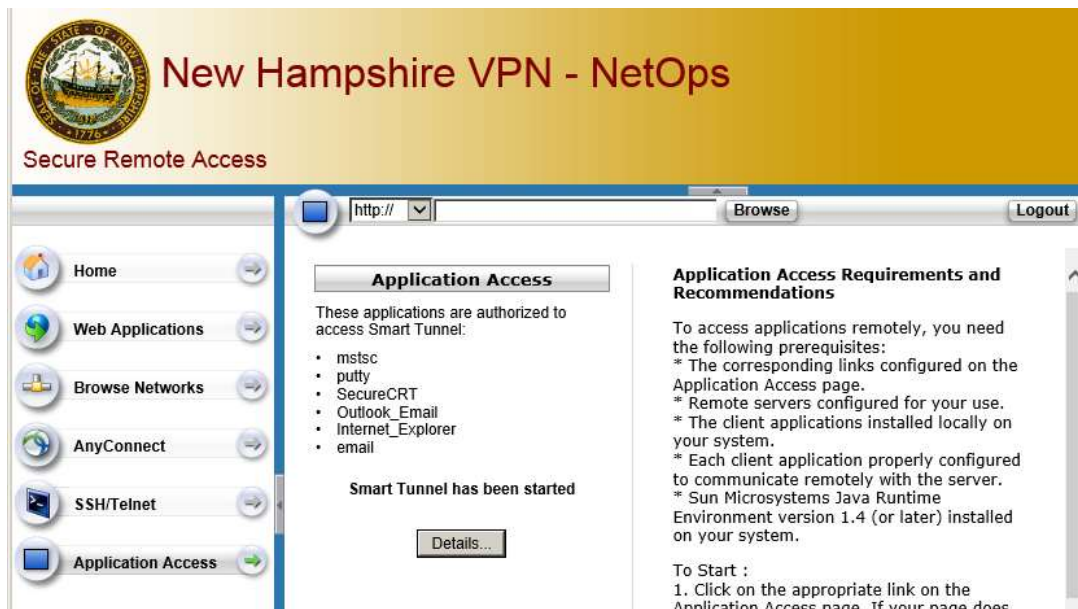
SSH/Telnet

Application Access

Web Bookmarks

- [NetOps Home Page](#)
- [ACS 5.1 Primary](#)
- [ACS 5.1 Secondary](#)
- [Sunspot Employee Directory](#)
- [Sunspot](#)
- [CUCM](#)
- [CallManager Administrative Access](#)
- [CUC](#)
- [Unity Connection Voice Mail](#)
- [CUCCX](#)
- [Contact Center Express \(Help Desk call routing\)](#)
- [OWA New](#)
- [Bookmarks](#)

If authorized, users can start a “Smart Tunnel” by going to the “Application Access” tab on the left. In most cases, especially for vendors, the smart tunnel will have already automatically started. A smart tunnel sends specific application traffic over the internet VPN tunnel to specific VPN network resources such as servers and remote desktops. Network traffic that does not need to go over the tunnel, for example, printing to a person or company’s local printer or looking up something on a search engine like Google, is not sent over the tunnel and instead is sent to the local device.



To continue accessing resources over the smart tunnel or using the clientless VPN portal in general, the VPN portal website must remain open. The page can be minimized, but it must remain open to maintain the connection. When it is time to logout, use the “Logout” button on the upper right-hand side.

