

Cisco Anyconnect Secure Mobility Client

This document contains screen captures of the VPN Client. VPN connections to the State of Missouri's network requires' four pieces of information:

1. VPN Group Name
2. Username
3. Passcode
4. Password

The VPN Group generally is as follows:

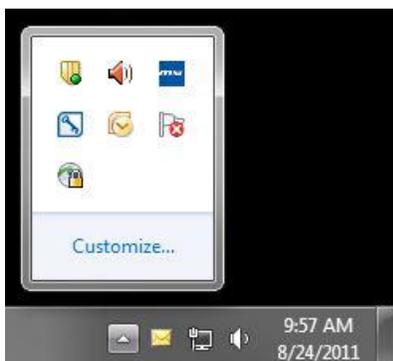
- ITSD2F for Office of Administration's Information Technology Services Division personnel
- Staff2F for other State of Missouri Executive Agency personnel (this is what SHS staff will use)
- Vendor2F for all other business/vendor partners
- There are other exceptions that do not fall into those groups listed above, if unsure contact the ITSD Help Desk.

The Username will be the username that you use to log into your machine.

The Passcode is provided by the RSA token that must be in your possession before you can login to VPN.

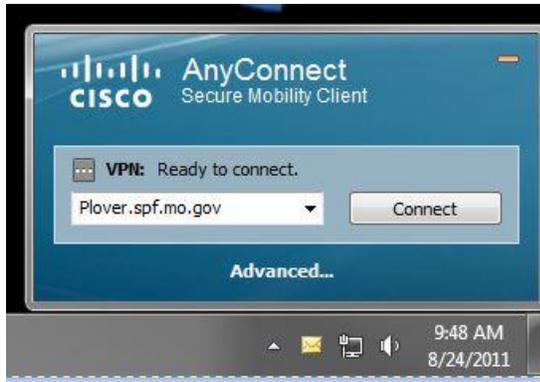
The Password will be the password that you use to log into your machine.

In the image below, it is the lower left icon (the lock is visible as the VPN connection was active when this image was captured).

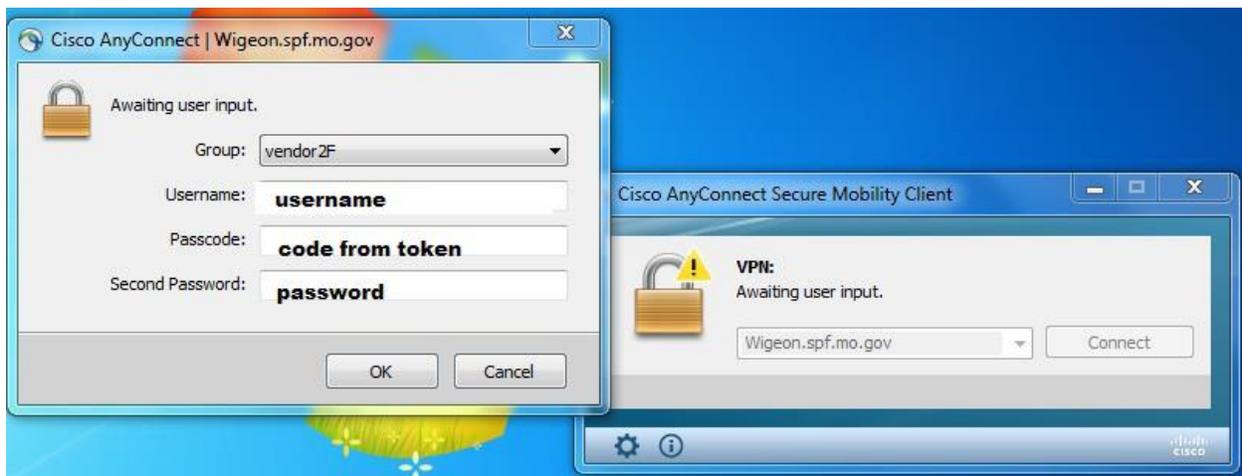


Clicking on the toolbar icon for the Cisco Anyconnect Secure Mobility Client will bring this dialog box up in the lower left corner of the screen.

Cisco Anyconnect Secure Mobility Client



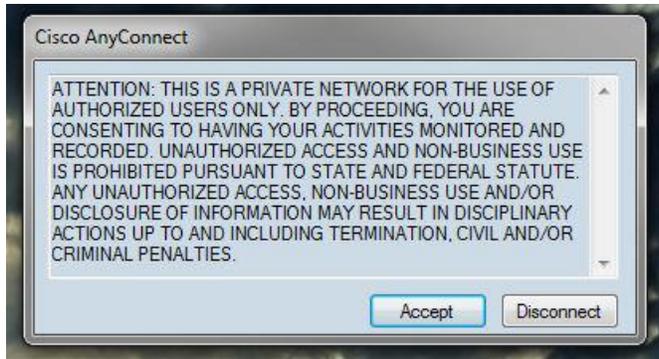
You can select the VPN gateway in the drop-down listbox. Clicking on the Connect button will bring up the following dialog box.



1. Select the appropriate group in the Group drop-down listbox. (Check this each time because after a client upgrade the selection may not be your previously used group.)
2. Enter your VPN username in the text box labeled Username. (Note: for two factor authentication the Active Directory UserPrincipalName [username@domain.state.mo.us] is NOT used as your VPN username. Please enter just the username and no domain information in this text box.)
3. Enter the code from the token in the text box labeled Passcode.
4. Enter your VPN password in the text box labeled Second Password.
5. Click on the OK button to initiate the connection (Note: OK must be clicked before the RSA token passcode changes. The horizontal bars at left of token are an indicator of the displayed passcode's time to live – they decrease until a new passcode is generated.)

Upon successful authentication the following dialog box will be displayed.

Cisco Anyconnect Secure Mobility Client



Click Accept to continue establishing your VPN connection. The status will change in the initial dialog box once connected.



When you are ready to disconnect your VPN session, open the dialog by clicking on the toolbar's VPN client icon.



Now you can click the Disconnect button to gracefully shutdown the VPN session.

Additional Information

- While connected to State of Missouri's network through VPN:
 - You will be restricted access to only required resources.
 - You will not be able to access locally connected resources in your location such as printer, file shares, email, etc. Split-tunneling is not allowed.
 - Some VPN groups are not allowed access to the internet.
 - Your VPN session/access are subject to termination if your connected device shows signs of malware, virus, Trojan, etc.