State of Nebraska - Cisco VPN Instructions
Updated 6/1/21

An MFA (Multifactor Authentication) cloud account will be required to access the State's network remotely. If you have not set up an account, please see this user guide:

Setup Cloud MFA user guide **(here)**

After successfully registering for MFA, you will need to install the Cisco AnyConnect software to connect to the VPN. The following link contains instructions for installing the VPN client:

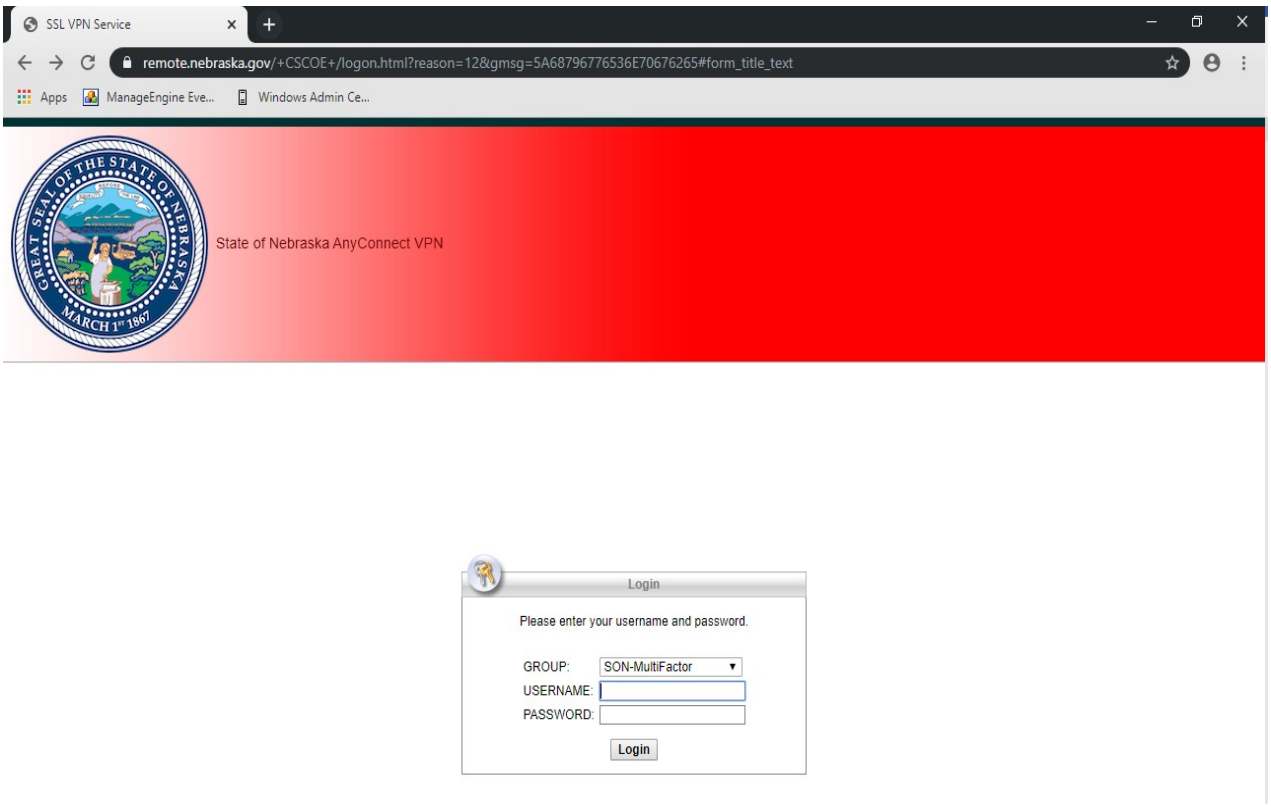
State of Nebraska Cisco VPN Instructions Connection instructions are at the end of the document.

If you are using a managed State computer, you should be able to install Cisco AnyConnect using the Software Center instead of downloading and installing it from the website.
(Press the Windows key and begin typing Software Center)

If you are not using a managed State computer, the Cisco VPN client "AnyConnect" can be installed by going to the following URL at the State of Nebraska:

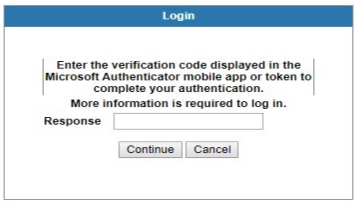
https://remote.nebraska.gov

Regular VPN Login for Multifactor



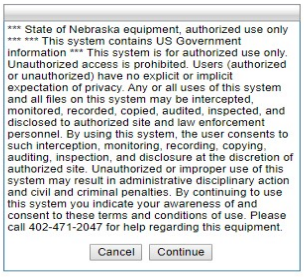
Be sure to select “SON-MultiFactor” as the group.

After your credentials are validated you will need to validate your MFA account. For MFA with a hard token, you will need to enter your verification code

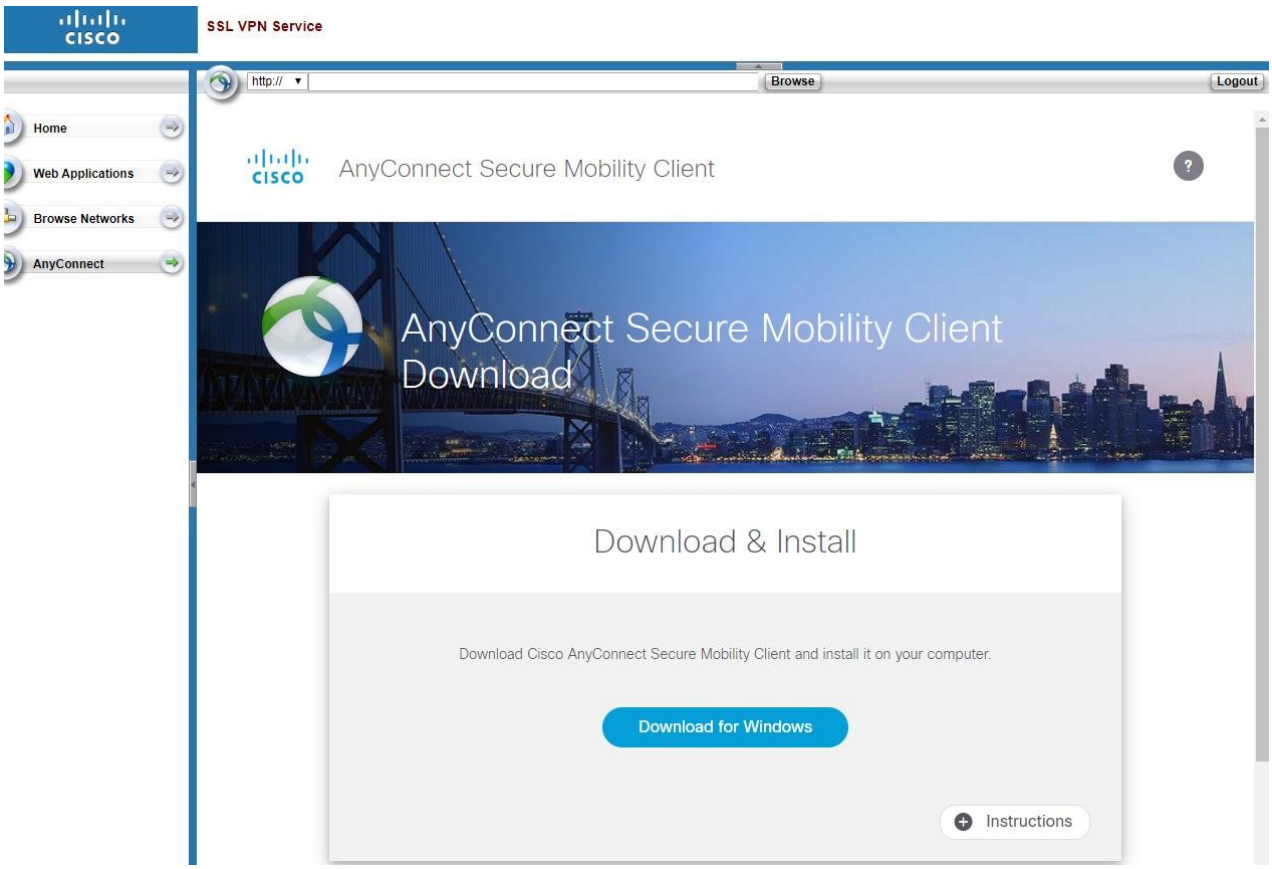


If you are using the Authenticator app (soft token), you will get a pop up on your mobile phone asking that you to approve or deny the verification request.

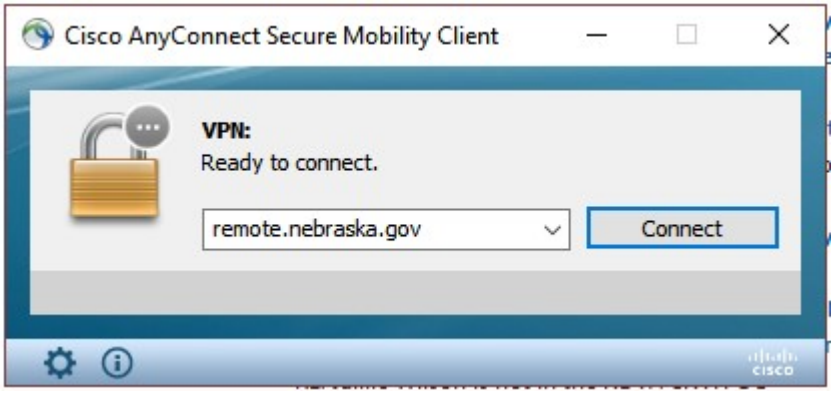
You will be asked to accept the terms and conditions of access to the State of Nebraska's network.



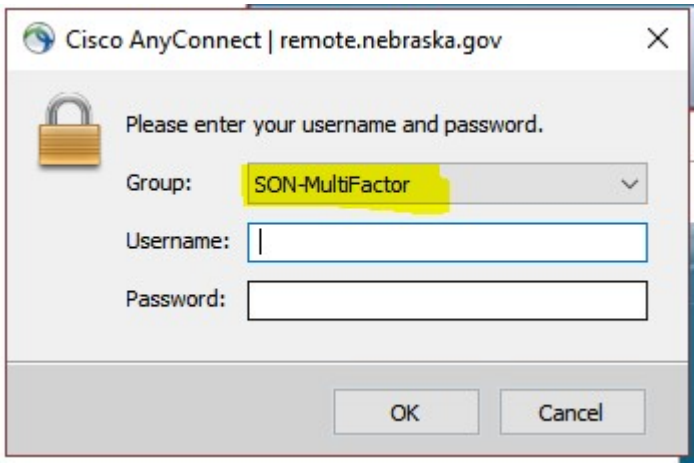
Once authentication is successful, you can download and install the VPN client provided the user has sufficient administrative rights. If not, please contact your IT department for installation assistance.



Once the client is installed, a connection can be established. The user will need to launch the Cisco AnyConnect Secure Mobility client and enter the server name: remote.nebraska.gov



Be sure to select “SON – Multifactor” for the Group



The multifactor verification will function the same as in the initial logon to install the VPN client software.

Once the connection is established, the client will automatically minimize. If the client fails to authenticate, please contact the OCIO help desk for further assistance.

The small “gear” icon at the lower left is for settings and may be adjusted based on agency policy.

The small “graph” icon next to the “gear” icon is for statistics and status. This information may be helpful in troubleshooting and will indicate, for example, if the client is using “FIPS Mode”.

Access to state resources using the VPN is controlled both at the VPN level and at the agency level. If you find your access is not what is expected, please submit a ticket through the IT Help Desk. Troubleshooting will begin with the VPN and then be escalated to your agency’s IT department.