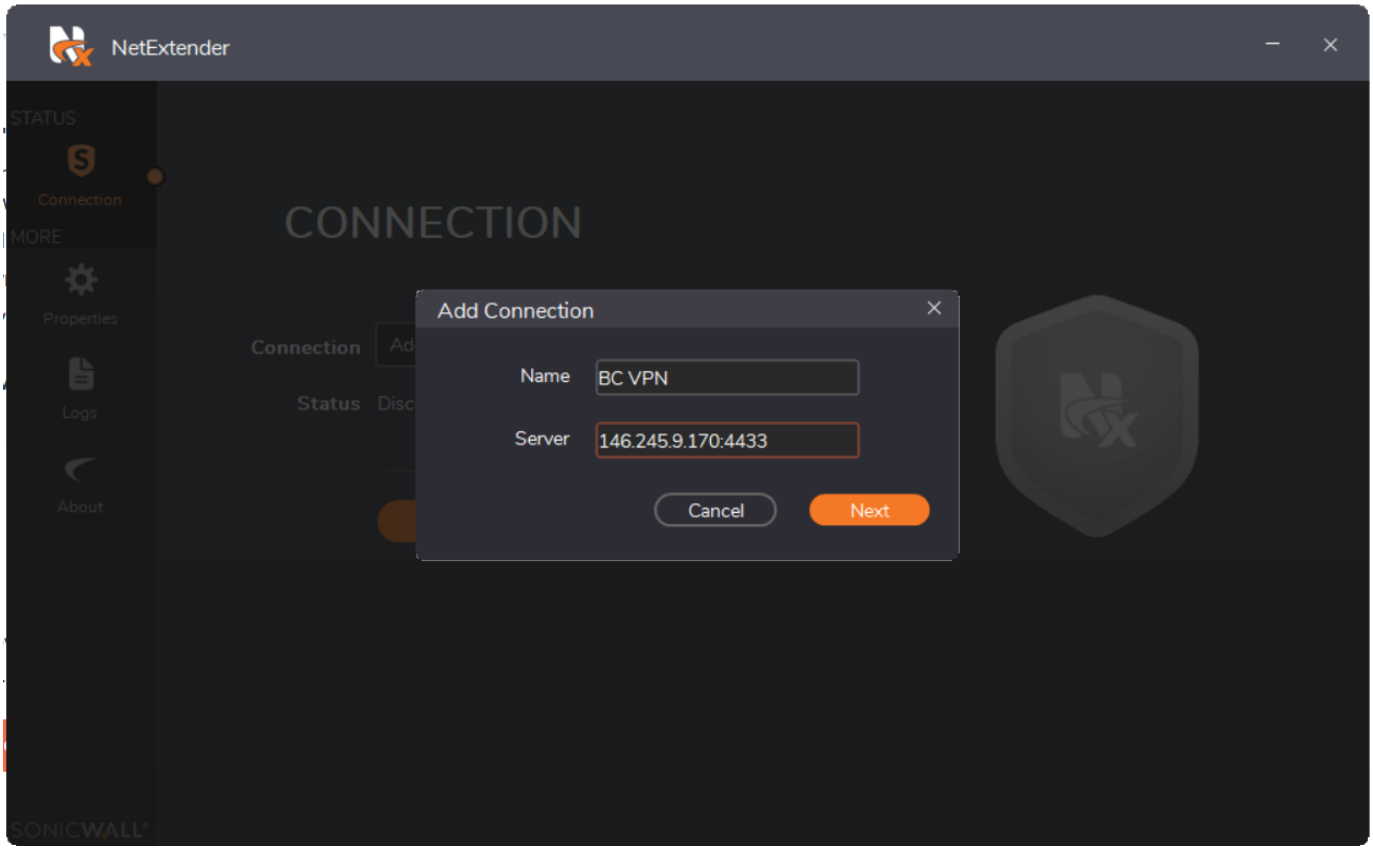
Setting up SonicWall's NetExtender VPN Client for Windows

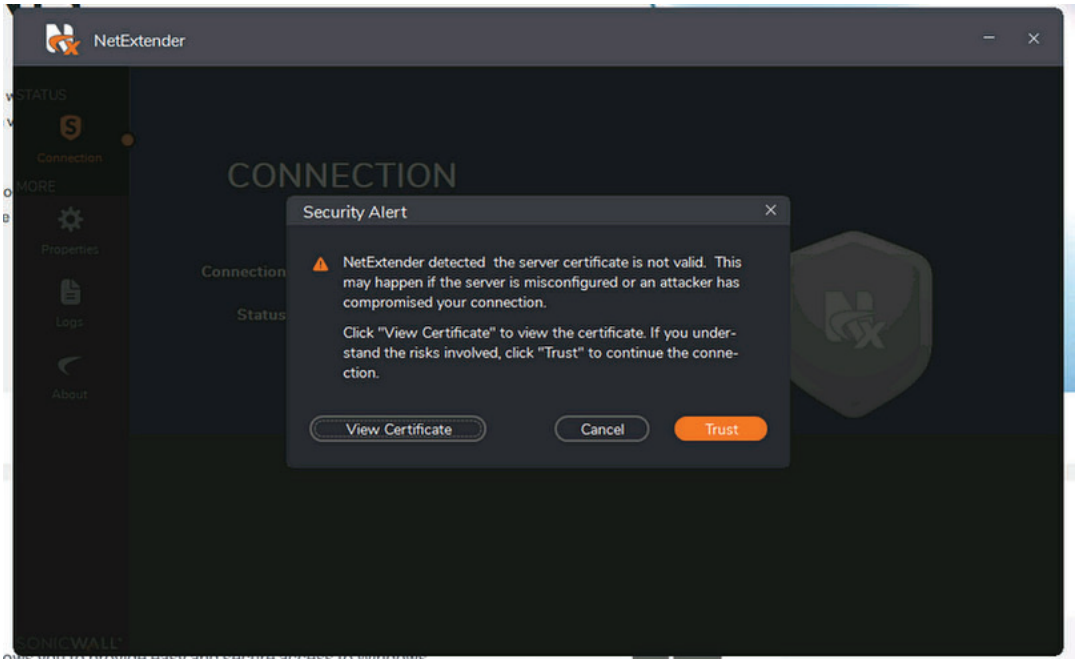
The first step is to download and install the SonicWall's SSL VPN NetExtender. This may have already been provided to you, but if not it can be downloaded directly from SonicWall and selecting Get NetExtender for Windows.

Once installed, launch the software and click the + in the toolbar to Add Connection...

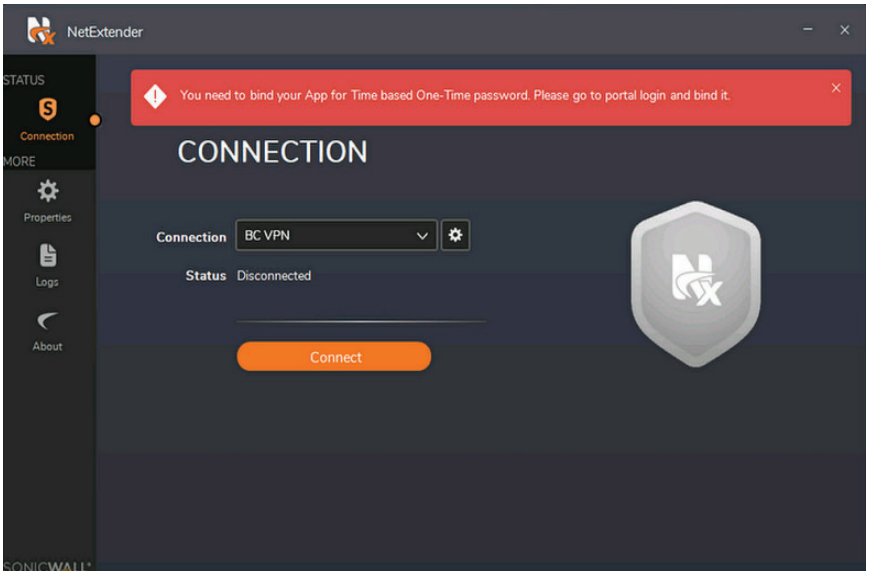
You may specify a connection name in the Name field. Enter **146.245.9.170:4433** in the IP address field.



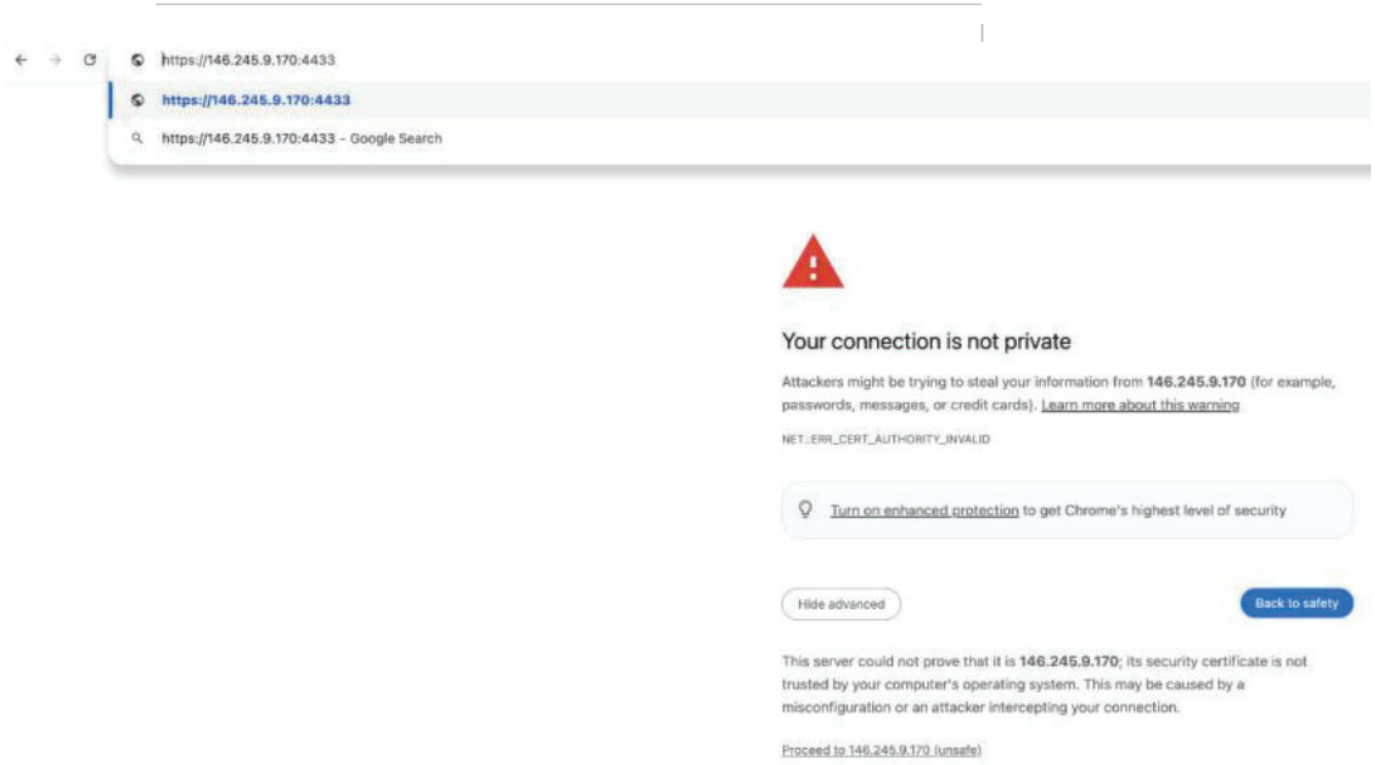
Press Trust to allow the connection.



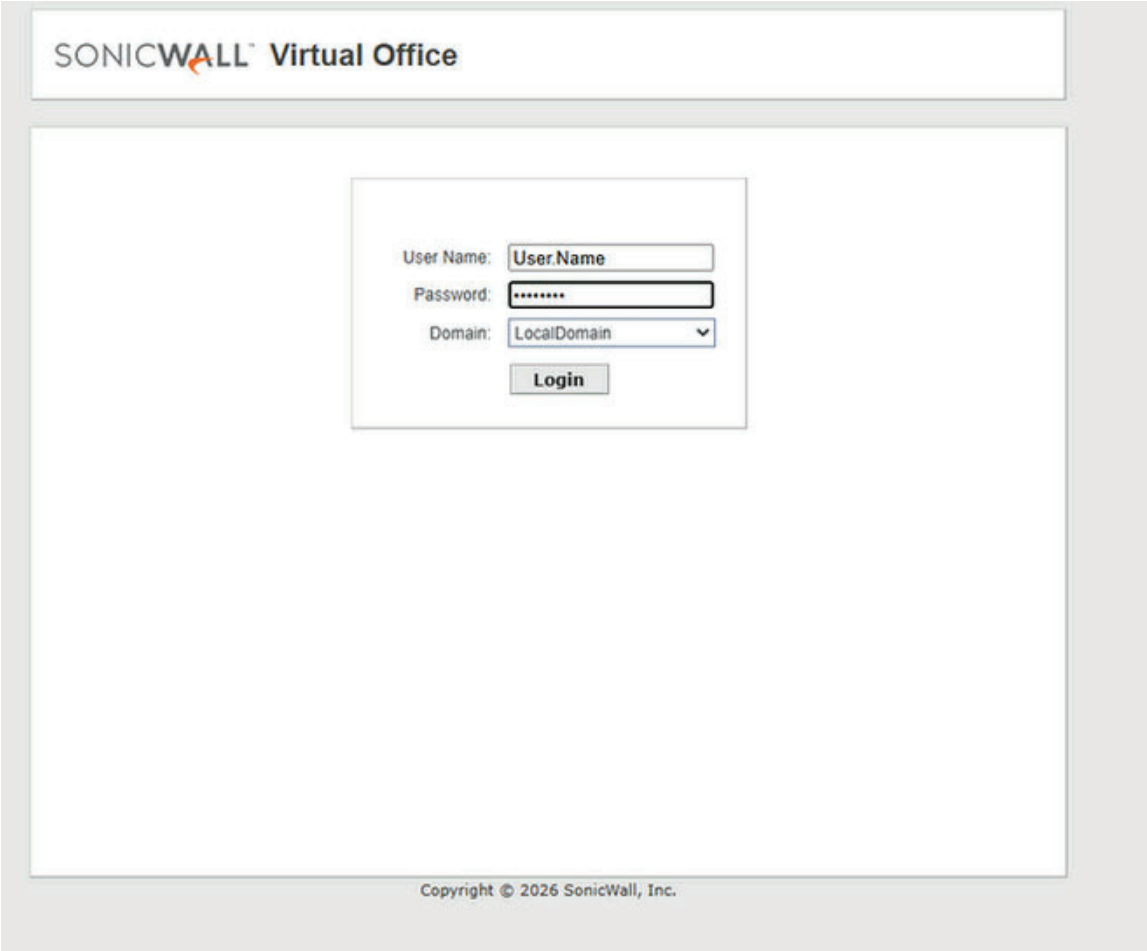
You will be prompted to enter your credentials. These must be provided to you prior to connecting- they are likely unique and not related to any of your existing accounts. **NOTE: THE USERNAME FIELD IS CASE-SENSITIVE!** If you do not have Multi-Factor Authentication (MFA) set up, you may see a Login Failed message.



Open a web browser and enter the URL: https://146.245.9.170:4433. If you see a message stating "Your connection is not private," select Advanced or More Info. Choose the option to proceed unsafely to the server's address.



- Log in using the user's assigned **username** and **password**.



Read the emergency scratch code prompt at the bottom of the page. Set up an Authenticator App on a device. Note: Users can utilize any MFA app that can scan a QR code. After installation, have the user scan the QR code provided and proceed to generate a multi-factor code.

Once you have successfully set up the MFA, sign in to the VPN again. This time, the VPN will prompt for their Bind app code, which will be displayed in the installed MFA app.