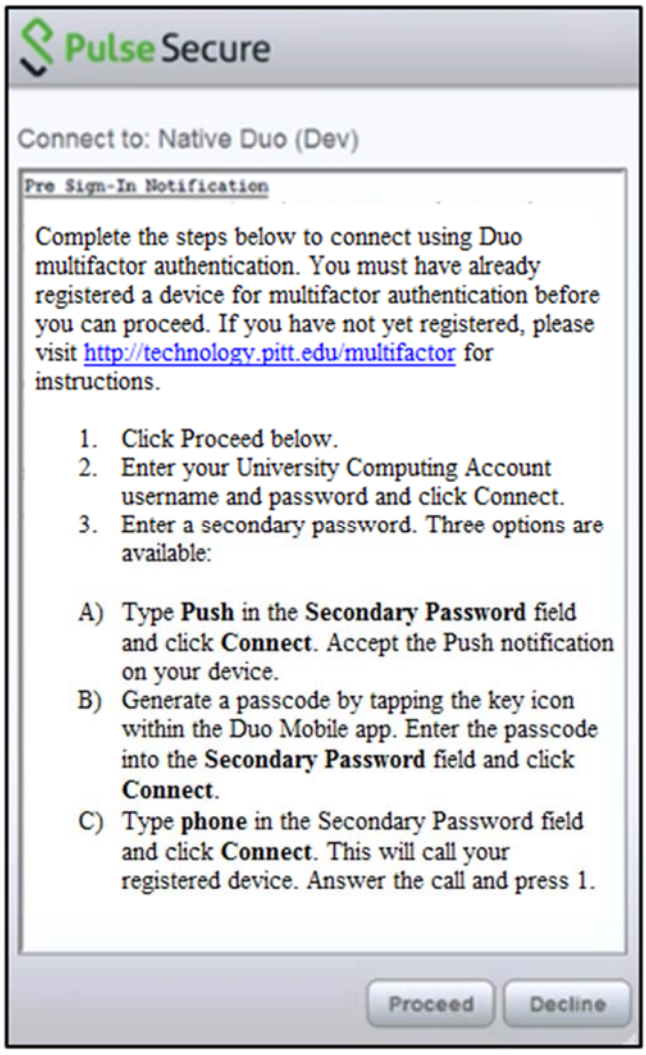
Using MFA with the Pulse Client

1. Launch the Pulse client and open your preferred connection.

2. A new pre-sign in notification will display similar to the one shown below. This page explains your options for using multifactor authentication. Click **Proceed**.

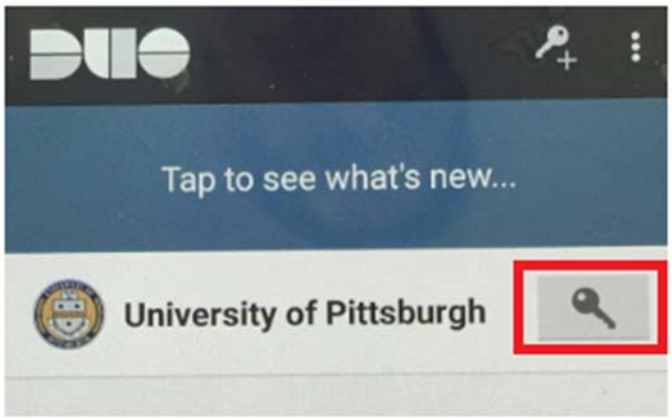


3. Enter your username and password as you normally would and click **Connect**.

4. A new screen will display with a Secondary Password field for multifactor authentication.

You have three options on this screen:

- A. Type **Push** in the **Secondary Password** field and click **Connect**. This will send a Push notification to your registered device. Accept the Push notification to connect.
- B. Generate a passcode by tapping the key icon within the Duo Mobile app. Enter the passcode into the **Secondary Password** field and click **Connect**. (Note: You can also type SMS into the Secondary Password field. This will send a text message to your device that you can enter in the Secondary Password field.)



- C. Type **phone** in the Secondary Password field and click **Connect**. This will call your registered device. Answer the call and press 1.

5. Your connection will be established.

Using MFA with the IPSec Client

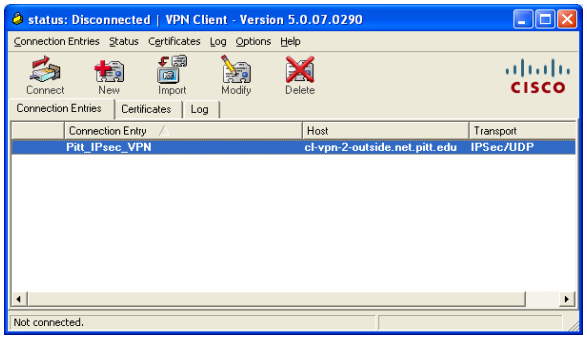
These instructions assume you are already using the IPSec client on your computer. If you need assistance installing or configuring the IPSec client, refer to our instructions for Windows, Mac, or Linux before completing the steps below.

Windows

1. Double click the **Cisco IPSec Client** 

on your desktop, then select the **VPN configuration** from the **Connection Entry** list. The VPN connection entry list window will display.

2. Click the IPSec connection that you use under the **Connection Entry** column.



3. Click the **Connect** button 

.

4. Enter your University Computing Account username in the Username field.

5. In the password field, you have several options to authenticate with multifactor authentication:

- Type your password only. This will use the default multifactor authentication method you selected when registering your device. For example, if you chose to always receive a Push notification, then typing your password will automatically send a Duo Push notification to your registered device. Accept the Push notification to complete the authentication process.
- If you want to use the "Call Me" option for multifactor authentication, type your password followed by the word phone in this format: password,phone. This will automatically call your registered device. Press 1 on your dialpad to authenticate.
- If you want to authenticate with a passcode, generate a passcode within the Duo mobile app, then type your password followed by Duo passcode in this format: password,token. For example, if the passcode you generated was 123456, you would type password,123456 in the Password field.
- If you want to be sent a passcode via text message (SMS), then type your password followed by sms in this format: password,sms. Your login attempt will fail and you will receive a six-digit passcode via text message. Retype your password followed by the passcode that you received in this format: password,123456.

6. Click the **OK** button.

7. A VPN icon will display in your menu bar once the connection has been established.

8. Start the application that requires a secure connection, such as a database client or Web application.

Mac

1. Click the **VPN** icon in the menu bar. Select **Connect *PittNet VPN*,** where *PittNet VPN* is the name of the IPSec connection that you use.

2. Enter your University Computing Account username.

3. In the password field, you have several options to authenticate with multifactor authentication:

- Type your password only. This will use the default multifactor authentication method you selected when registering your device. For example, if you chose to always receive a Push notification, then typing your password will automatically send a Duo Push notification to your registered device. Accept the Push notification to complete the authentication process.
- If you want to use the "Call Me" option for multifactor authentication, type your password followed by the word phone in this format: password,phone. This will automatically call your registered device. Press 1 on your dialpad to authenticate.
- If you want to authenticate with a passcode, generate a passcode within the Duo mobile app, then type your password followed by Duo passcode in this format: password,token. For example, if the passcode you generated was 123456, you would type password,123456 in the Password field.
- If you want to be sent a passcode via text message (SMS), then type your password followed by sms in this format: password,sms. Your login attempt will fail and you will receive a six-digit passcode via text message. Retype your password followed by the passcode that you received in this format: password,123456.

4. Click the **OK** button.

5. A VPN icon will display in your menu bar once the connection has been established.

6. Start the application that requires a secure connection, such as a database client or Web application.

Linux

Configure the Virtual Private Network Connection

1. Use Yum or Aptitude-get to install “vpnc” by typing: `$ sudo apt-get install vpnc`
2. Edit the configuration file by typing: `$ sudo nano /etc/vpnc/pittvpn.conf`
3. Enter the following configuration settings:
   `IPSec gateway vpn.pitt.edu`
   `IPSec ID` <your *department’s group name*>
   `IPSec secret` <*your department’s pre-shared text key*>
   `Xauth username` <*your University Computing Account username*>

Establish a Secure Connection

1. Type the following command: `$ sudo vpnc pittvpn`

Enter Your Password with Duo Multifactor Authentication

You will be presented with a password prompt. You have several options to authenticate with multifactor authentication:

- Type your password only. This will use the default multifactor authentication method you selected when registering your device. For example, if you chose to always receive a Push notification, then typing your password will automatically send a Duo Push notification to your registered device. Accept the Push notification to complete the authentication process.
- If you want to use the "Call Me" option for multifactor authentication, type your password followed by the word phone in this format: password,phone. This will automatically call your registered device. Press 1 on your dialpad to authenticate.
- If you want to authenticate with a passcode, generate a passcode within the Duo mobile app, then type your password followed by Duo passcode in this format: password,token. For example, if the passcode you generated was 123456, you would type password,123456 in the Password field.
- If you want to be sent a passcode via text message (SMS), then type your password followed by sms in this format: password,sms. Your login attempt will fail and you will receive a six-digit passcode via text message. Retype your password followed by the passcode that you received in this format: password,123456.