



Pulse Secure VPN for Macs

Starting with macOS 10.13.1 'High Sierra', Apple introduced a new feature requiring users to approve installs of client kernel extensions used by the Pulse Secure VPN.

For additional information [click here](#).

Installing the VPN

Step 1

Make sure your computer has macOS 10.11 'El Capitan' or newer before proceeding.

If you need to upgrade your computer to the latest macOS, please read the [macOS upgrade overview](#).



Step 2

Ensure you have...

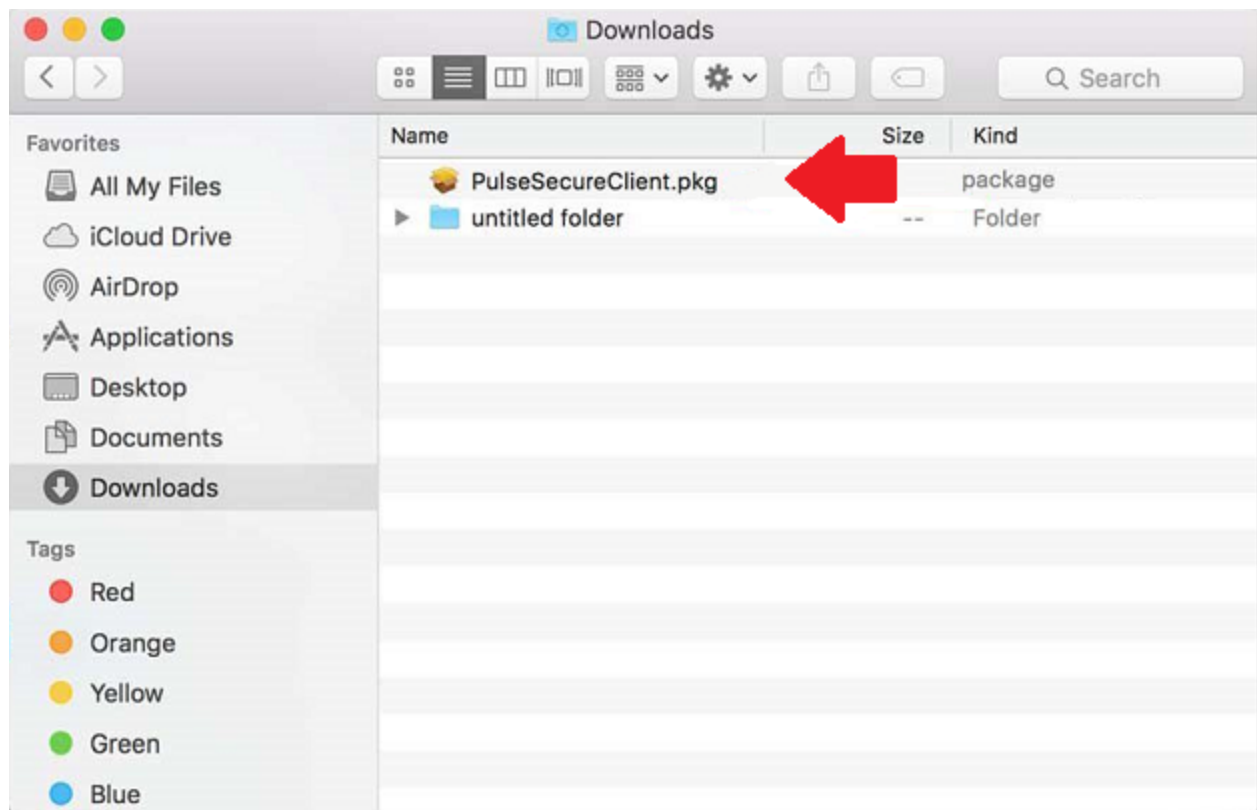
[Enrolled in Azure MFA](#)

[Requested VPN access](#), if applicable

[Downloaded the Pulse Secure VPN client](#)

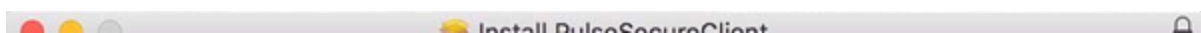
Step 3

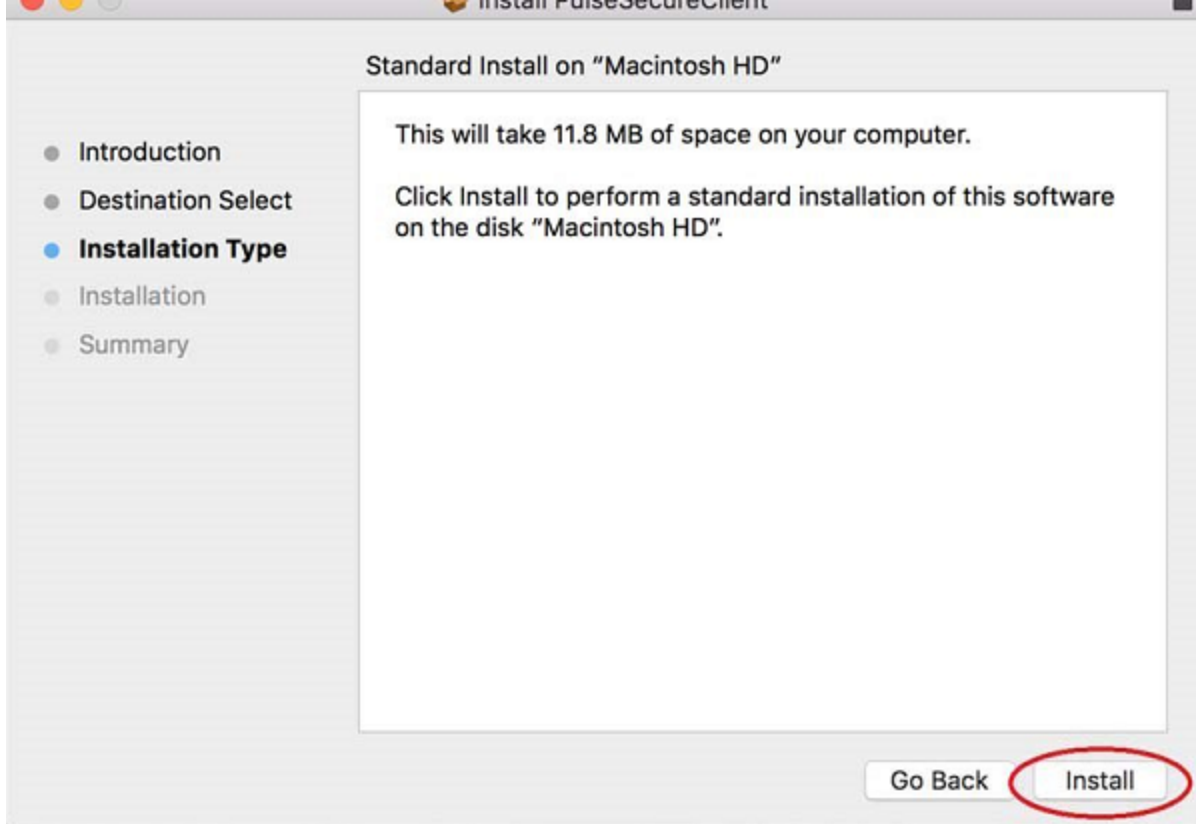
Once the Pulse Secure VPN client has downloaded, run the setup file found in your *Downloads* folder.



Step 4

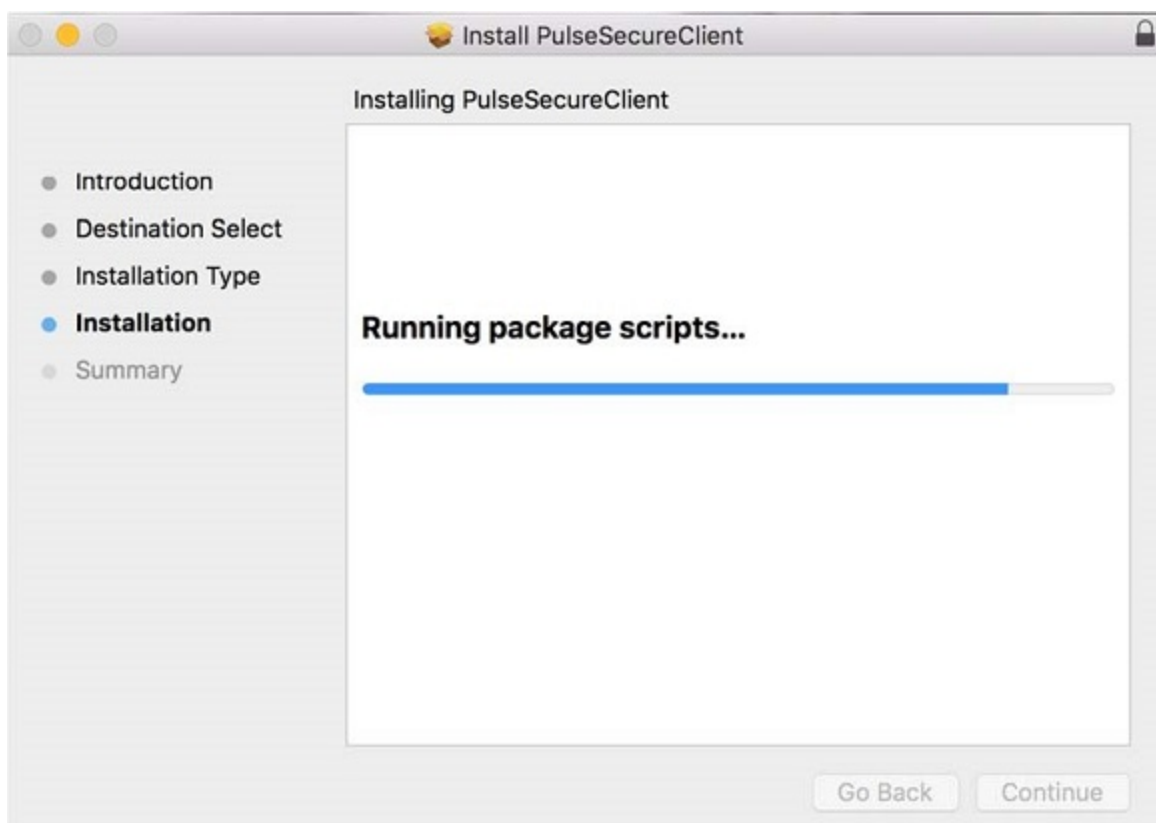
Click *Continue* and *Install* to begin the installation of the VPN client.





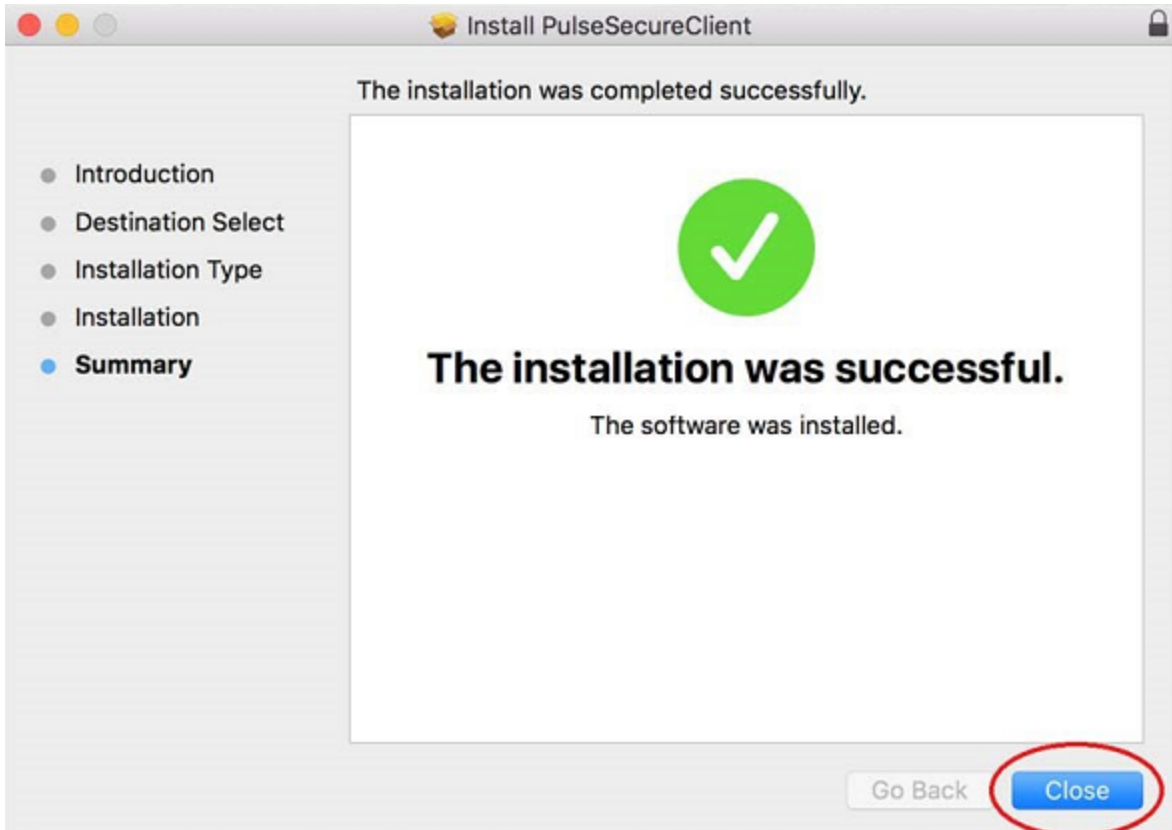
Step 5

You will see a progress bar throughout the installation of the VPN.



Step 6

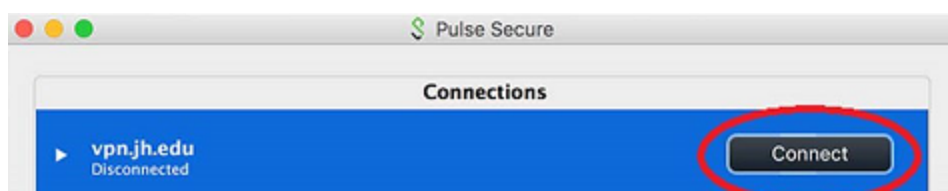
You should see a notification indicating the VPN was successfully installed. Click *Close* to exit the installer.

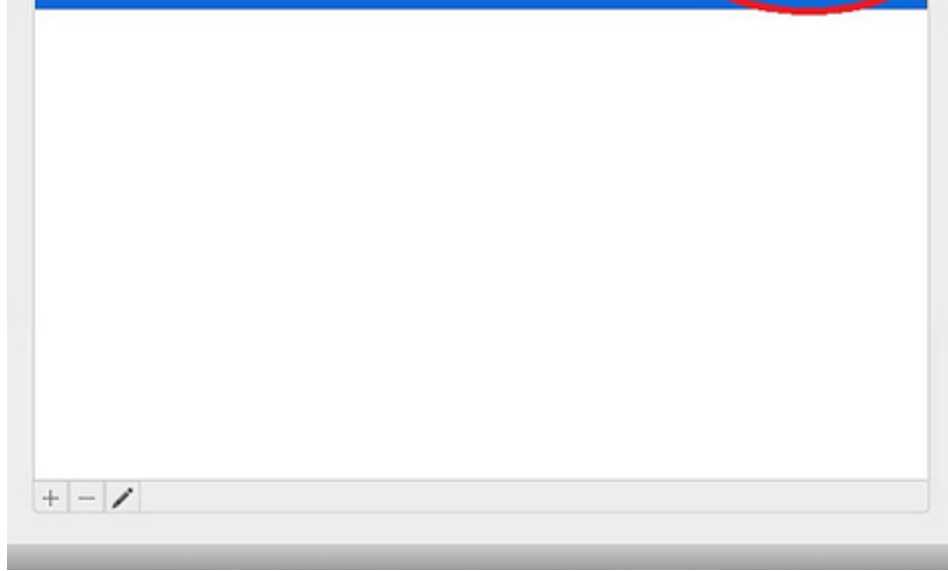


Connecting to the VPN

Step 7

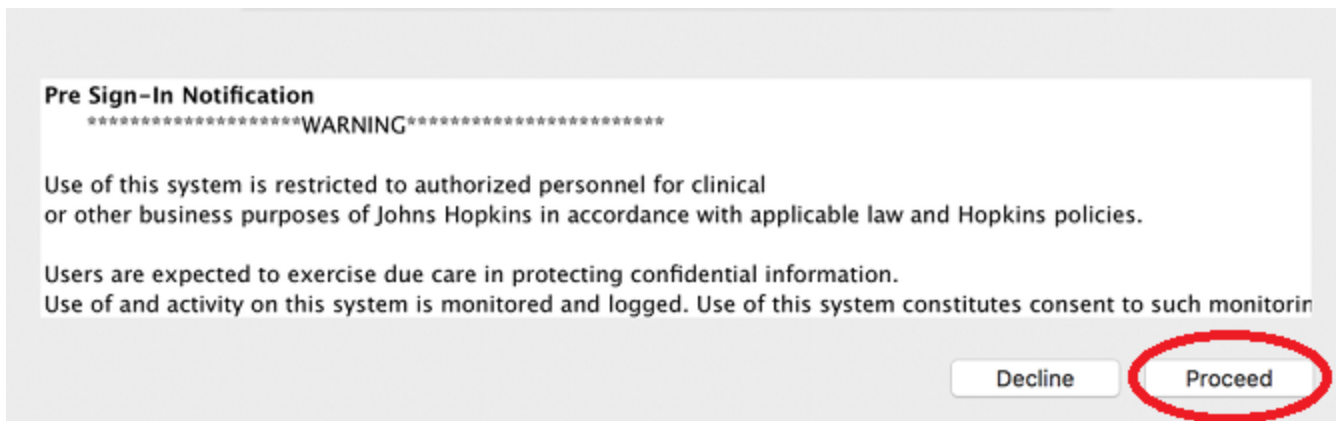
Open the Pulse Secure Client from the Menu bar and click *Connect*.





Step 8

Read the terms of the sign-in notification and click *Proceed*.



Step 9

If you are logged in to a Hopkins-managed computer, you may not be prompted for login information. If prompted, proceed with entering your *JHEDID@jh.edu* username and click *Next*.

Sign in

jhedid@jh.edu

[Can't access your account?](#)

Sign-in options

Back

Next

[First Time JHED Users Click Here](#)

If you are prompted to enter the code displayed on your authenticator app from your device, and have not yet enrolled in Azure MFA, we have migrated your existing JH MyIT Login Code settings for you. Please use the code you were using from that application

The purpose of Johns Hopkins Enterprise Authentication is to provide a single sign-on functionality for our customers to access many applications with just one login.

[Terms of use](#) [Privacy & cookies](#) ...

Cancel

Step 10

Enter the password to your JHED account and click *Sign in*.

 Pulse Secure

Connect to: vpn.jh.edu (vpn.jh.edu)

JOHNS HOPKINS
UNIVERSITY & MEDICINE

Enter password

Because you're accessing sensitive info, you need to verify your password.

Password

[Forgot my password](#)

Sign in

[First Time JHED Users Click Here](#)

If you are prompted to enter the code displayed on your authenticator app from your device, and have not yet enrolled in Azure MFA, we have migrated your existing JH MyIT Login Code settings for you. Please use the code you were using from that application

The purpose of Johns Hopkins Enterprise Authentication is to provide a single sign-on functionality for our customers to access many applications with just one login.

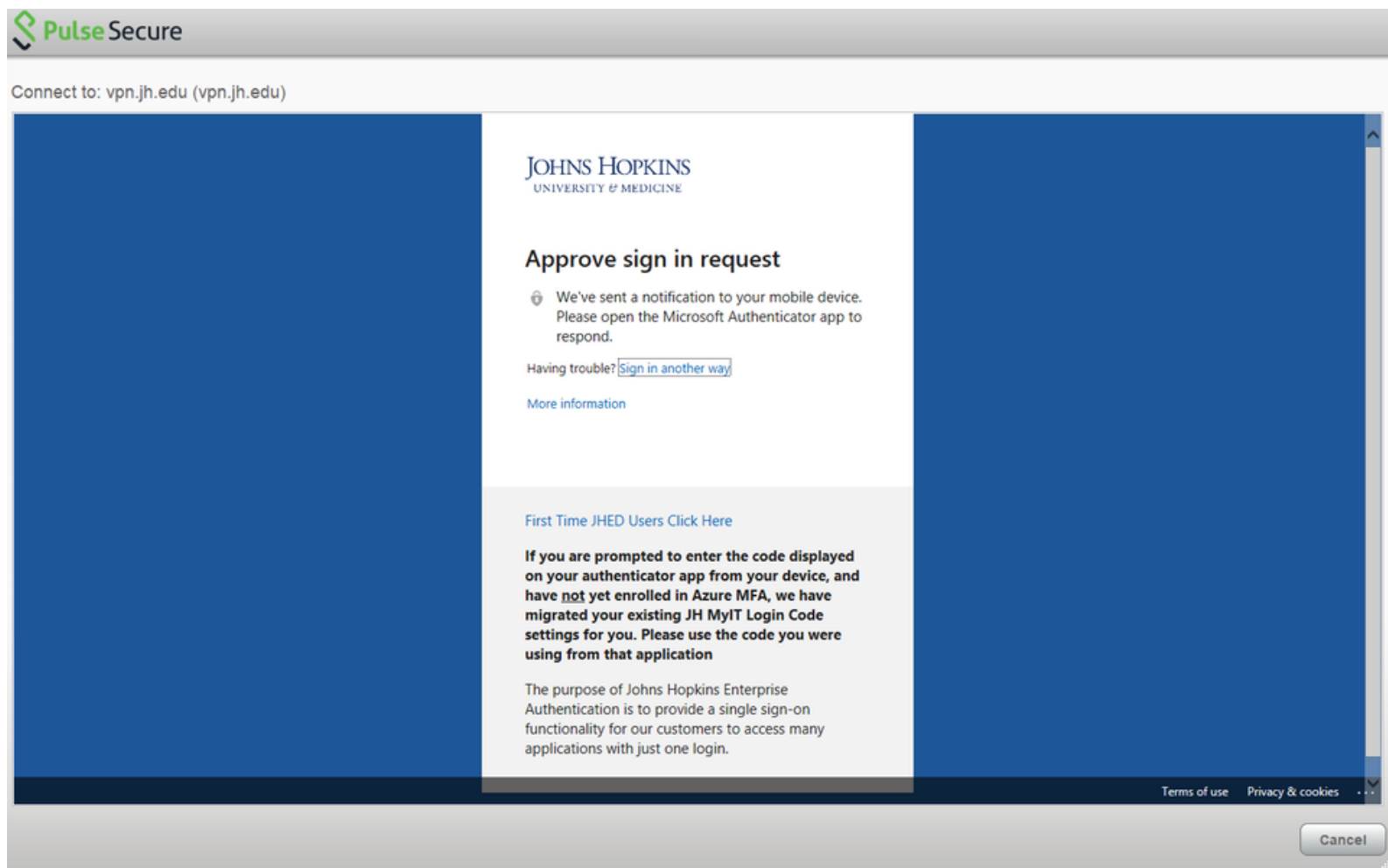
[Terms of use](#) [Privacy & cookies](#) ...

Step 11

Since you are enrolled in Azure MFA, you will need to approve the authentication request. Depending on your default MFA method, this could mean approving a push notification on your smartphone, answering a phone call, or entering a 6-digit code.

Note: If you do not receive your MFA prompt, you may want to click the option *Sign in another way*.

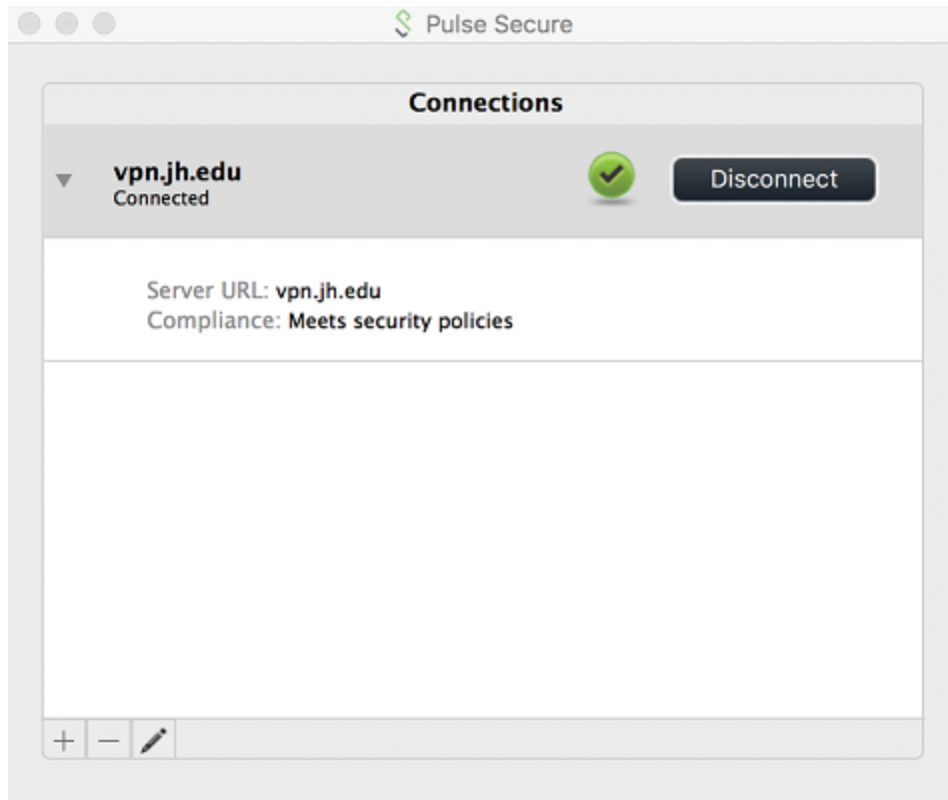
For information about Azure MFA, please visit the [Azure MFA Resource Center](#).



Step 12

If successfully connected to the VPN, you will see the Pulse Secure icon now includes a green check mark.

When you are finished using the VPN, make sure you disconnect your session.



For assistance with the VPN, please submit a Service Now ticket