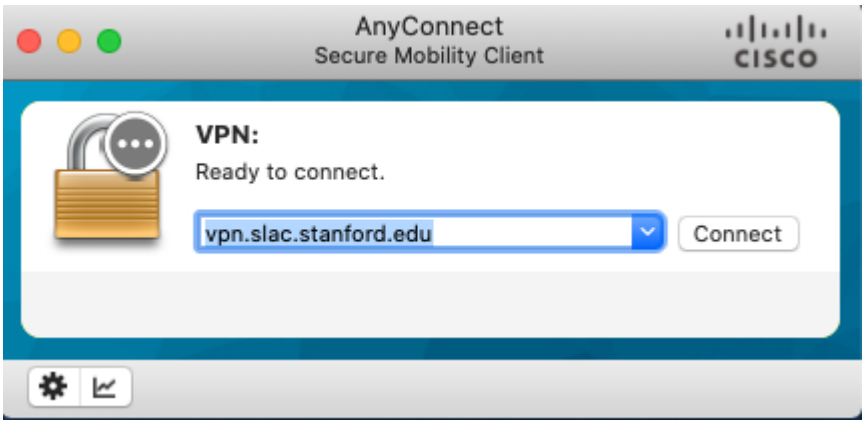
# How to Connect to SLAC VPN

## Quick instruction guide

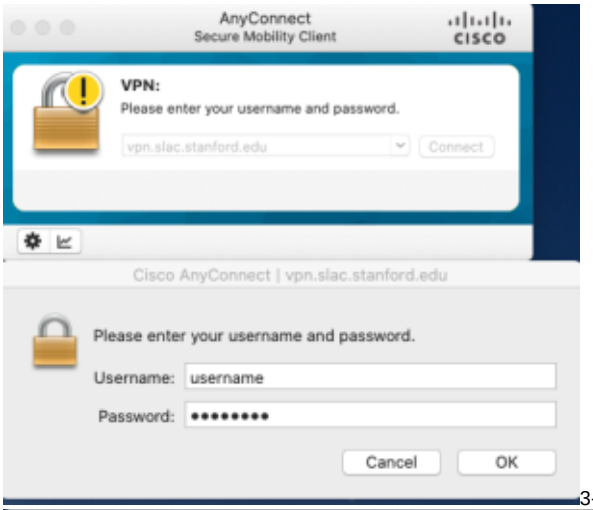
On a SLAC built windows device the vpn client is pre-installed, so you can just go on start menu -> launch Cisco Anyconnect Secure mobility client. Then ensure the connection string is "vpn.slac.stanford.edu" and click on connect. Enter your SLAC's windows credentials, enter the DUO prompt, then accept the banner and you are connected as indicated in the taskbar.

On personal computers, MACs or linux you will need to install the vpn client available at https://vpn.slac.stanford.edu/ . If you are using a mobile device the client to look for in the app store is "Cisco Anyconnect Secure Mobility Client".

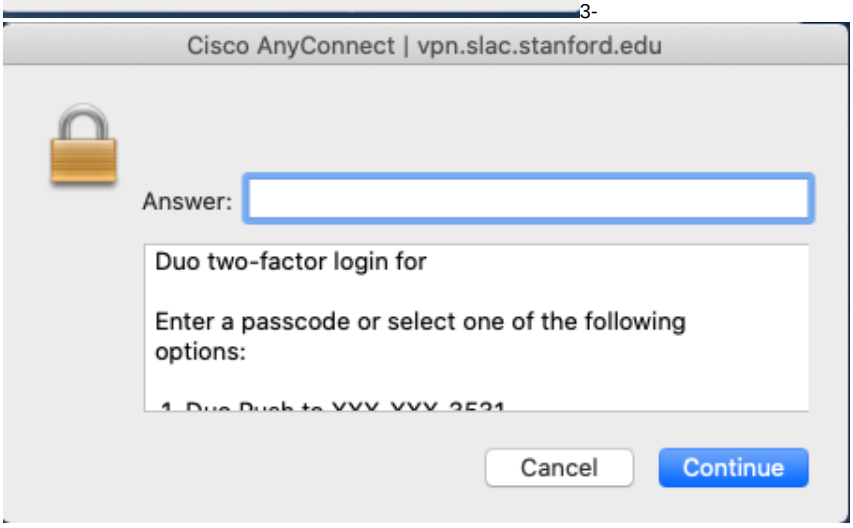
1-

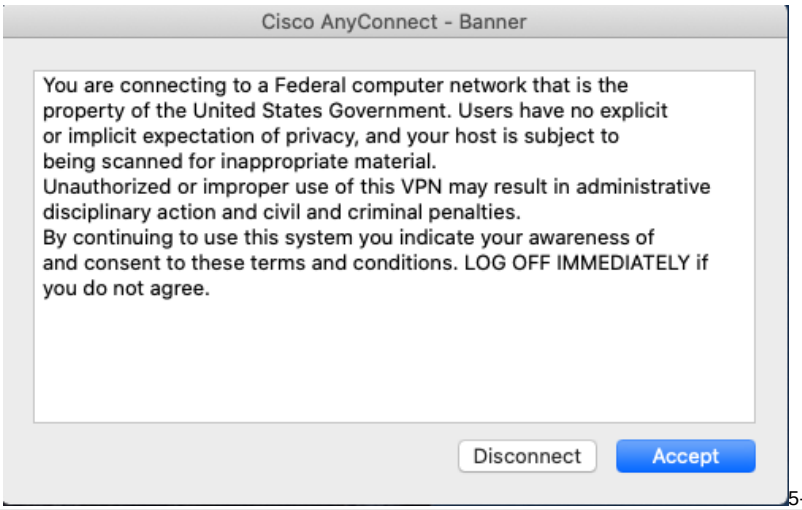



2-



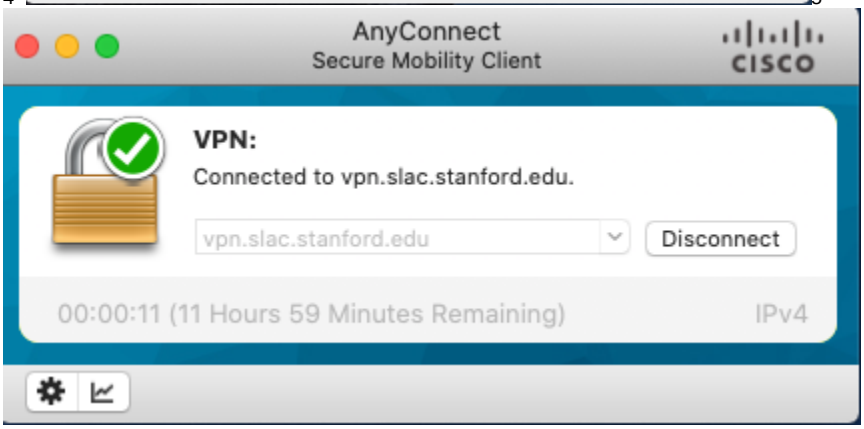

3-






4-

5-




## Table of Contents



## Introduction

This page documents the use of the SLAC VPN service.

Virtual Private Network (VPN) provides a secure connection between your computer and the resources available at your home institution. In the case of SLAC, we offer a VPN service that permits authorized users to gain visibility of SLAC network resources from outside of SLAC. This includes the SLAC Visitor Wireless network.

Assistance with installation and usage of this system is available. Contact our IT helpdesk via the details below.

## Requirements

1. You must have a valid SLAC Windows account
2. Your account must be given SLAC VPN account access, and you must agree to the usage policies outlined.
3. You must be enrolled in two-factor authentication (visit https://www-internal.slac.stanford.edu/twostep/ from a computer on the SLAC network).
4. You must have SLAC supported operating system to get successful connection on SLAC Network. Please refer to the following KB articles:
    a. Windows: https://slacprod.servicenowservices.com/kb_view.do?sysparm_article=KB0010017
    b. Mac OS: https://slacprod.servicenowservices.com/kb_view.do?sysparm_article=KB0010018a
    c. Linux: https://slacprod.servicenowservices.com/kb_view.do?sysparm_article=KB0010019

We officially support Windows, Mac OS and Linux but VPN is available on several other platforms (android, ipads etc.).

# Posture Assessment of Systems Entering SLAC VPN

- **What is changing and why?**

  As an open laboratory, SLAC makes every effort to enable access to tools and systems needed for research purposes without compromising the security and integrity of our other information and systems. The security of the SLAC network, however, must be protected from the risk posed by the number and variety of devices that use it. Consequently, effective March 19, 2018, devices being used to log into the SLAC virtual private network (VPN) will be checked to ensure they do not pose a security risk to SLAC.

- **What's the impact?**

  If you use a SLAC-owned, centrally managed device to connect to VPN, you will most likely be granted access with no issues. If your SLAC-owned device is denied access, contact the IT Service Desk (see contact info below) for assistance.

  If you use a personally owned device, and that device meets the minimum requirements for using the VPN, then you will be allowed in. If, however, your device does not meet the requirements for OS version, virus control, and other security measures, you will be denied access to the VPN. You are responsible for updating your personally owned device.

  If you use a device provided by an institution other than SLAC or Stanford, contact that institution for assistance.

  If you are denied access, the following options are available:

  a. Update the device software so that it is compliant (see Minimum System Requirements below).
  b. Use Citrix as an alternative method for gaining access to the SLAC systems you need. To request Citrix access, in Service Now, go to the Service Catalog, then select Accounts & Access > Citrix Account Request.
  c. If you are using a personal or other non-SLAC-owned device, use a SLAC-owned, centrally managed device instead.
  d. If the device is SLAC-owned, contact the IT Service Desk (see contact info below).

- **Minimum System Requirements**

  The minimum requirements are:

  - Antivirus with current signatures (<15 days old)
  - A current OS version, such as:
    - Windows 10
    - macOS 10.11 and up
    - Android 10 and up
    - iOS 13 and up
    - Specific Linux versions are being confirmed and will be updated here when available.

- **Resources**

  If you are a SLAC employee and need antivirus software for your home computer, free software provided by SLAC can be downloaded from the Cyber Security Resources page.

- **IT Service Desk Contact Information**

  Phone: (650) 926-4357; Extension: x4357 (xHELP)

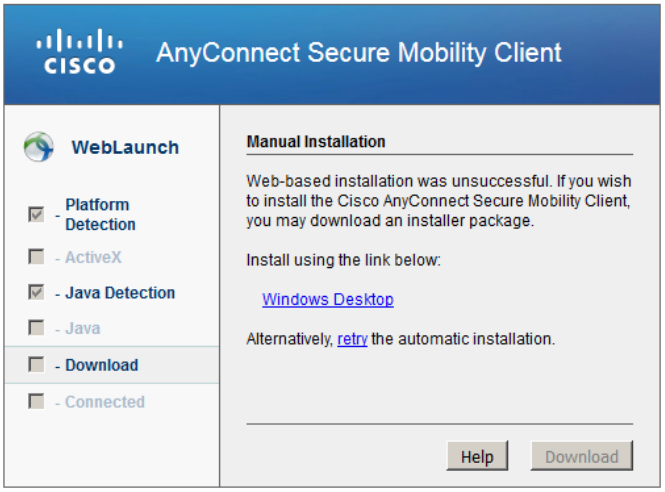
  Service Now: Submit a help request

# Security

The SLAC VPN connects you directly to the SLAC network. All of your network traffic is sent across an encrypted link, including Internet traffic. You should adhere to the same SLAC computing policies that you do when using computers on-site. Remember to disconnect from the VPN before leaving any computer unattended.

# Detailed steps to download the VPN client

The vpn clients is available upon authentication at the webpage https://vpn.slac.stanford.edu/ . Log in and the system will detect which version is suitable for your systems.


The Java installation usually fails, but then it defaults to the manual installation. Download the VPN client by clicking on the link provided. Install it as administrator:

- On linux you need to execute the file that you downloaded as root with the command "sh vpnsetup.sh" (you can also use sudo from your regular account with the command "sudo sh vpnsetup.sh".
- On windows you need to do a right click and "Run as administrator"
- On mac you will need "to allow access" when running it

**The first time you connect, you will have to manually enter the connection hostname, please set it as vpn.slac.stanford.edu**

## What to Do if You Have Problems

Please have a look to the FAQ SLAC VPN Frequently Asked Questions (FAQ) and SLAC ServiceNow KB Article for Posture Assessment.

If necessary, manual download of the client install packages can be done via links here: Cisco AnyConnect Installation Packages

For further help, please contact our IT helpdesk.

## Other Notes

4/5/2016: Two-factor authentication is now deployed on SLAC VPN gateways, if you are already enrolled you will be asked for 2nd factor (push, token, etc.)

1/11/2018: Posture assessment is deployed on SLAC VPN gateways, for FAQs please visit: https://slacprod.servicenowservices.com/kb_view.do?sysparm_article=KB0010903