Install and Use Cisco AnyConnect SSLVPN

When installing and using the Cisco AnyConnect SSLVPN (Secure Sockets Layer Virtual Private Network) client problems may occur. This document will help diagnose and solve some potential issues that may be encountered. Use the links below to jump to a topic or scroll down to read all of the topics.

Installing the SSLVPN Client

AnyConnect is a straightforward installation. To install the client, go to https://sslvpn.asu.edu/2fa (https://sslvpn.asu.edu/2fa) and log in with your ASURITE credentials.

After you have provided your credentials, the installation will start immediately. On Windows machines, the web installation will first attempt to install the AnyConnect client through ActiveX. If you are using Google Chrome or Mozilla Firefox, this will fail, and prompt you to download the client for your operating system:
(For Mac OS X users, the link will display as Mac OS instead of Windows Desktop)

For some permitted users, specifically faculty or staff members, Cisco AnyConnect can be downloaded through My Apps in My ASU. Click on the My Apps icon on the left-hand side-bar, search in the search bar "Cisco AnyConnect," select Download App Now and download the installation file respective to your operating system. To see if your operating is supported, view the Supported Operating Systems list for details.

Once you have finished downloading the manual installation, you are now ready to install. After completing the installation, you can now start the Cisco AnyConnect Secure Mobility Client.

**Launching the SSLVPN Client**

If the web installation completes without failing the automatic session, you will be connected to the VPN. After shutting down your computer, you can always reconnect through the automatic process by going to [https://sslvpn.asu.edu/2fa](https://sslvpn.asu.edu/2fa)

If you completed the manual installation of the VPN client, you will need to start the VPN from where you installed it on your computer.

The name of it on your computer (and icon) should be:

Once you launch the Cisco AnyConnect Secure Mobility Client, you will be prompted with the following window:
NOTE: Access to the ASU VPN (virtual private network) for faculty and staff is now two-factor enabled for both the Cisco AnyConnect VPN client and the VPN website. [See this KB Article for more information](https://kb_view.do?sysparm_article=KB0015179).

To connect via the VPN website, the new site address is: `https://sslvpn.asu.edu/2fa`. If you connect via the Cisco AnyConnect VPN client, you will need to type the new “sslvpn.asu.edu/2fa” address into the field, like below, before clicking on “Connect”.

To use SSLVPN to have a dedicated tunnel for all traffic from you laptop back through the ASU SSLVPN, for example in the special case you are traveling in China, use: “sslvpn.asu.edu/tunnel.”

Students and student resources such as the Library can continue to use the current site address: sslvpn.asu.edu

You will be prompted for your login credentials:

- **Username** - Enter your ASURITE
- **Password** - Enter your ASURITE PASSWORD
- **Enter the name of an Authentication Factor** - Enter name of desired (DUO 2FA code) authentication method, see below for details.

**Authentication Factor Options:**
The third box is used to enter a second authentication factor.

- Type **push** into the box to receive a Duo push notification from the Duo app on your smartphone, then click "OK". After you confirm the Duo push notification on your smartphone, you will be logged into the ASU 2FA VPN.

- Type **phone** into the box to receive a Duo phone call notification, then click "OK". When you receive the phone call, just follow the automated instructions and you will be logged into the ASU 2FA VPN.

- Type **sms** into the box to receive a code via text message, then click "OK". If you enter sms, a code will be sent to you and the Cisco AnyConnect authentication box will appear again. Re-enter your ASURITE ID, password, and in the third box enter the passcode you received from the Duo sms message to log into the ASU 2FA VPN.

- Enter a **Duo Passcode**. You can obtain a Duo passcode by starting the Duo app on your smartphone, clicking on the "key" button associated with your Arizona State University Duo account and then typing in the displayed code into the authentication factor field. This option does not require a cell or internet connection. The Duo app generates the code when you push the "key" button in the Duo app (red box in the image below). The second image below shows where you type this Duo passcode into the authentication factor dialog box.

Note that for security reasons, you will see dots when typing in both your ASURITE **Password** and **authentication factor** selection (push, phone, sms or Duo passcode) and the actual push, phone, sms or Duo passcode you use to authenticate with.

**Duo Generated Passcode Example:**

![Duo Passcode Example](image)

**AnyConnect Sign in screen showing where to type in Duo generated passcode:**

![AnyConnect Sign in Screen](image)

**NOTE:** Please be sure your Cisco AnyConnect VPN client is at least version 4.1 so that you have the best possible connectivity available. Two-factor authentication will not work with older client versions.
Disconnecting from the Cisco AnyConnect Secure Mobility Client

To disconnect to the VPN, find the icon on the lower right hand corner of your Windows Desktop:

Right click the icon, and choose either VPN Disconnect or Quit.

You are now disconnected from the VPN. To reconnect, please follow the steps above listed under "Launching the SSLVPN Client"

Other information and troubleshooting

Remote Connections to either workstations or servers on the ASU Network requires SSLVPN for connections. For security, Windows XP workstations are not able to make a second SSL VPN secure connection to another system. Examples are Sybase, Advantage, etc. Workstations running Windows Vista or Windows 7 are able to manage this without a problem.

Firewall Exceptions

AnyConnect assigns an ASU IP address within the 172.31 range. This means that firewall rules outside of this range will block incoming connections from a remote user connected through AnyConnect. This can be fixed by adding the IP range 172.31.16.10 – 172.31.31.254 the firewall exception scope.

Authentication Failures

If you cannot authenticate in order to use the SSLVPN client, they may not have subscribed to the Border VPN access service. This can be verified at http://asu.edu/selfsub (http://asu.edu/selfsub)

If you receive the error "IP Forwarding error" while attempting to connect, then two different steps can be taken to resolve the issue.
• This is most often caused by a conflict with an optional driver installed by some Adobe products. Uninstall the Bonjour application using Add/Remove Programs, or disable to Bonjour service.
• Upgrade the version of Cisco AnyConnect to version 2.2 or higher. A version that works with Bonjour is available at [https://sslvpn.asu.edu/2fa](https://sslvpn.asu.edu/2fa)

**VPN Client Agent Error**

If you receive the error "The VPN client agent was unable to create the interprocess communication depot", perform the following steps:

**Note:** This solution is for Windows 7 OS computers.

1. Click the Windows **Start** button.
2. Click **Control Panel**.
3. Click Network and **Sharing Center**.

   If View by is set to Category, click on **View network status and tasks** under Network and Internet.

4. Click on **Change Adapter Settings**.
5. Right-click **Shared** in the Status column and click **Properties**.
6. Click the **Sharing** tab.
7. Clear the **Allow other network users to connect through this computer's internet connect** check-box.
8. Click OK.
9. Reinstall Cisco AnyConnect.

**Note:** This solution is for Windows 8/10 OS computers.

1. Press Win + R
2. Type: services.msc and press Enter
3. Find Internet Connection Sharing (ICS)
4. Stop the service
5. Right-click and open the service's Properties
6. Change the Startup type: to Disabled
7. Reboot the computer
8. Install Cisco AnyConnect VPN

**Certificate Errors**

Some users may receive an untrusted certification dialog box when connecting to SSLVPN.asu.edu with the AnyConnect client. This dialog box can appear both before and after entering credentials to connect to SSLVPN. It looks similar to the image below.

This is caused by a configuration issue with the AnyConnect profile. To fix this issue, first close AnyConnect. Then delete the files named ASUPProfile.xml and ASUPProfile2.xml located in the following directory:

• **Windows XP:** `C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\Profile`
• **Windows Vista:** `C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\Profile`
Command Line Interface (CLI)

Alternatively, Cisco AnyConnect has a command-line interface (CLI) which can be useful for scripting automatic VPN connections. After AnyConnect is installed, the method to access the CLI is by launching the file vpncli.exe located in C:\Program Files\Cisco\Cisco AnyConnect VPN Client.

The syntax for connecting is the following:

```
vpncli.exe connect sslvpn.asu.edu
```

To disconnect AnyConnect, use the following command:

```
vpncli.exe disconnect
```

The username will default to the currently logged on user. However the user must enter their password as it is never stored in the client's machine. This method of connecting can be used in a startup script for users who prefer to have uninterrupted access to resources required by the VPN.

Afterwards, go to https://sslvpn.asu.edu/2fa (https://sslvpn.asu.edu/2fa) and log in. Once you are automatically connected, the ASUProfile.xml file will be recreated with the correct settings.

For any additional questions about DUO, contact your department's desk side support staff, visit our Knowledge Article (/kb_view_customer.do?sysparm_article=KB0011028) or call the ASU Help Center at 1-855-278-5080.

Related Articles

- SSL VPN Connection Issues on Windows 8 (/kb_view_customer.do?sysparm_article=KB0010516)