Virtual Private Network (VPN) Set-Up

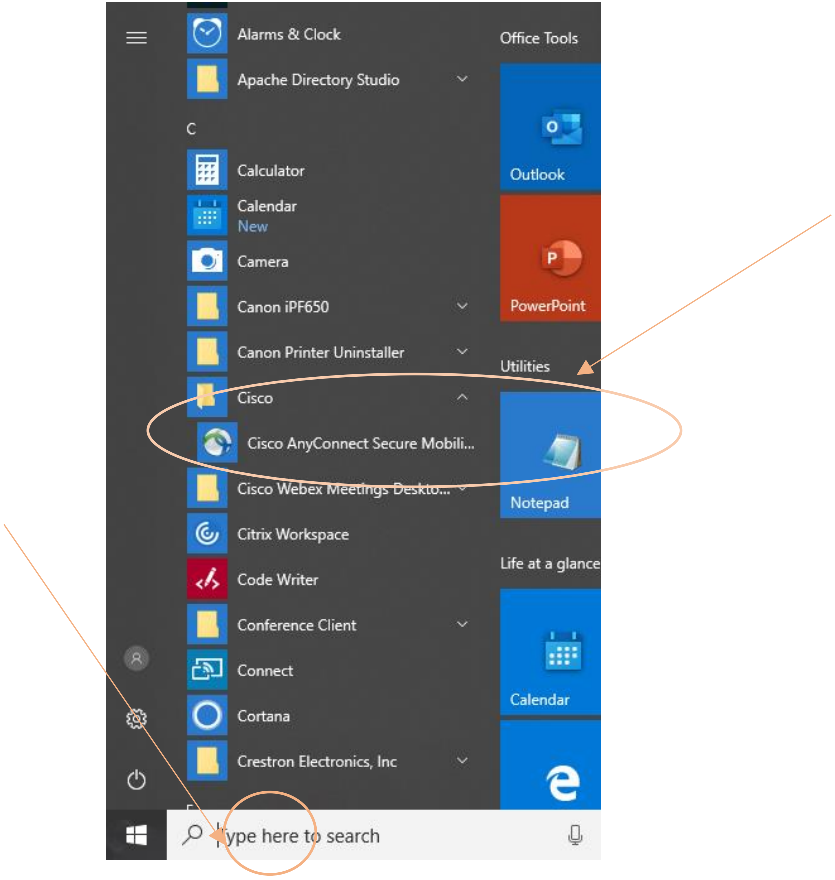
I. You will receive an email which will contain the following information:

  a. Your userid – This is your VPN userid and is not connected to your normal login credentials
  b. Your VPN Profile – This profile will need to be entered to create your VPN connection
  c. Your Initial Password – This password will be needed the first time you log into the Self-Service Console
  d. Link to download the Cisco AnyConnect VPN Client (See Step II-b-i)
  e. Link to download the "On-Demand Authentication VPN Guide". This link will not be used for your install.

Contact your agency IT department or VPN liaison if you have not received this information.

II. Download the Cisco AnyConnect VPN Client – This will install software on your laptop, which will allow you to create a safe and secure connection.

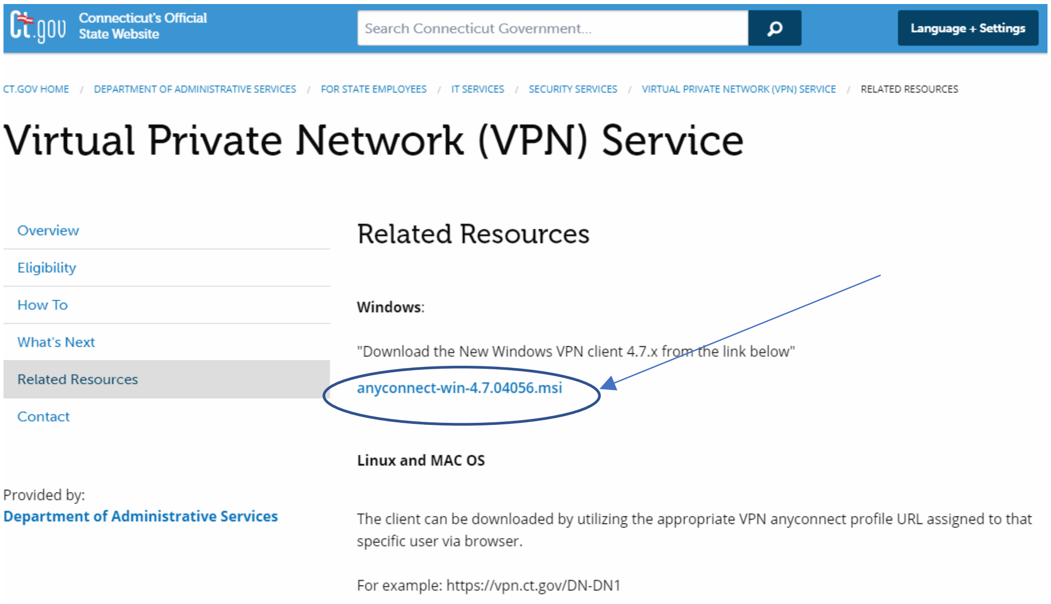
  a. Some users may already have the Cisco AnyConnect Client installed on their device, so check first to see if you have is. To see if it has been installed, go to your Startup Menu (the Windows icon in the bottom left corner of your screen) and there should be a Cisco folder. In that folder should be Cisco AnyConnect Secure Mobility Client



b. If you do not find it there, you will need to download it. If you do not have the permissions required to download and install the client contact your IT department.

   i. Open your web browser and go to http://portal.ct.gov/DAS/BEST/Security-Services/Virtual-Private-Network-VPN-Service/Related-Resources

   ii. On the resulting page, select anyconnect-win-4.7.04056.msi to download the setup file.



Ct.gov
Connecticut's Official State Website
Search Connecticut Government...
Language + Settings

CT.GOV HOME / DEPARTMENT OF ADMINISTRATIVE SERVICES / FOR STATE EMPLOYEES / IT SERVICES / SECURITY SERVICES / VIRTUAL PRIVATE NETWORK (VPN) SERVICE / RELATED RESOURCES

Virtual Private Network (VPN) Service

Provided by:
Department of Administrative Services

Related Resources

Windows:

"Download the New Windows VPN client 4.7.x from the link below"

anyconnect-win-4.7.04056.msi

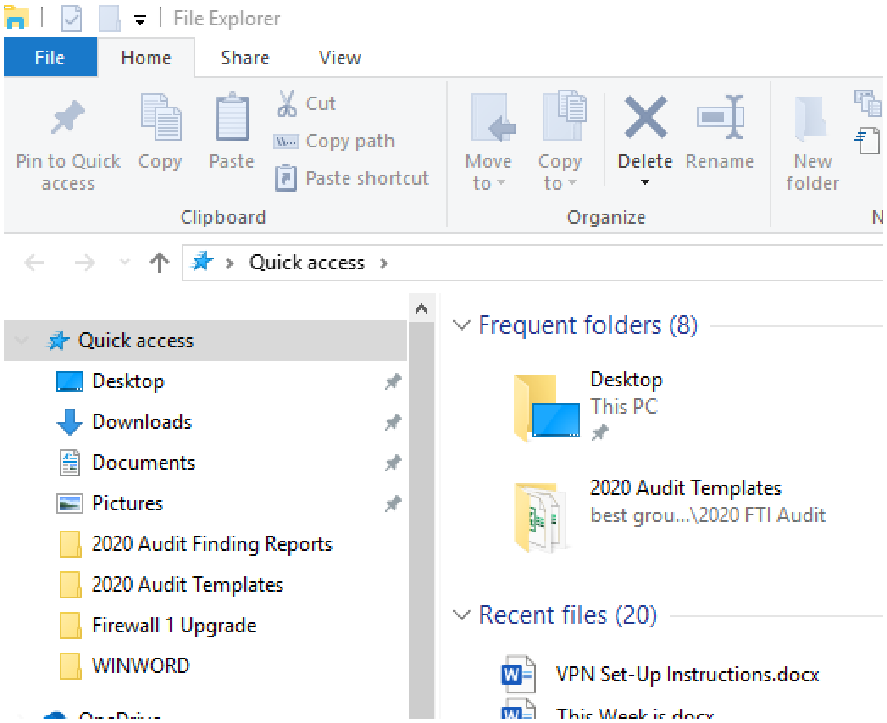
Linux and MAC OS

The client can be downloaded by utilizing the appropriate VPN anyconnect profile URL assigned to that specific user via browser.

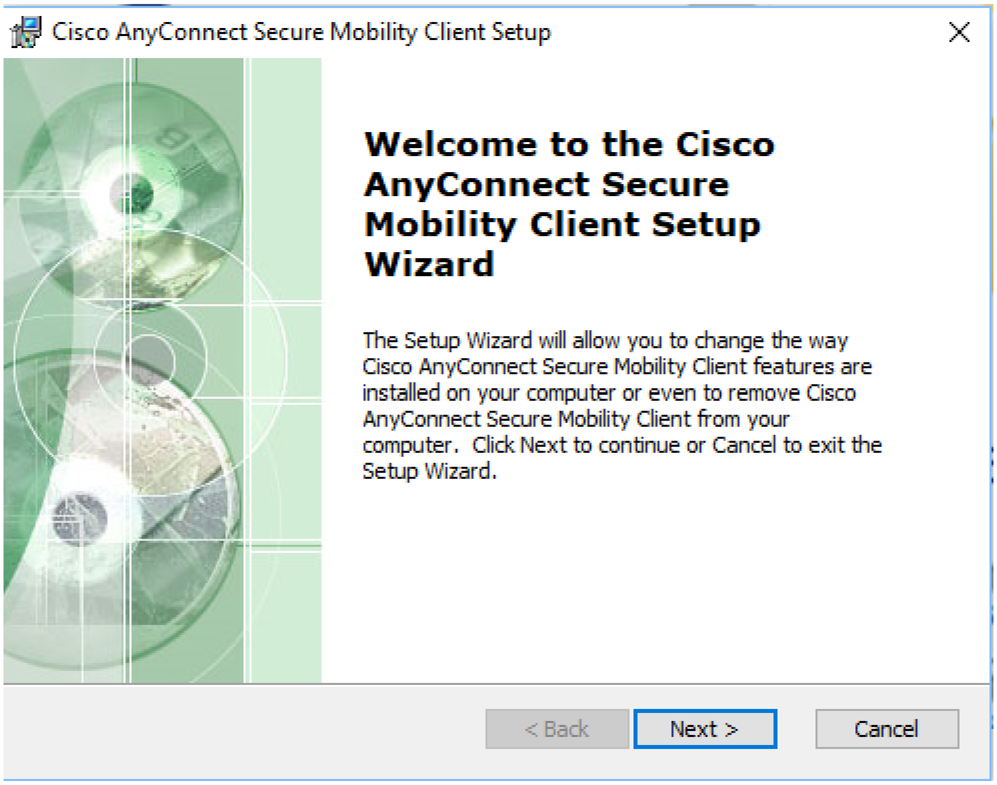
For example: https://vpn.ct.gov/DN-DN1

   iii. The setup file needs to be opened and run. A pop-up may appear asking you to run the file or you may need to open the file and run it from your Downloads folder.

      1. If the pop-up appears, select the Run button.
      2. If you need to run it from your Downloads folder, the Downloads folder can be found in Windows Explorer



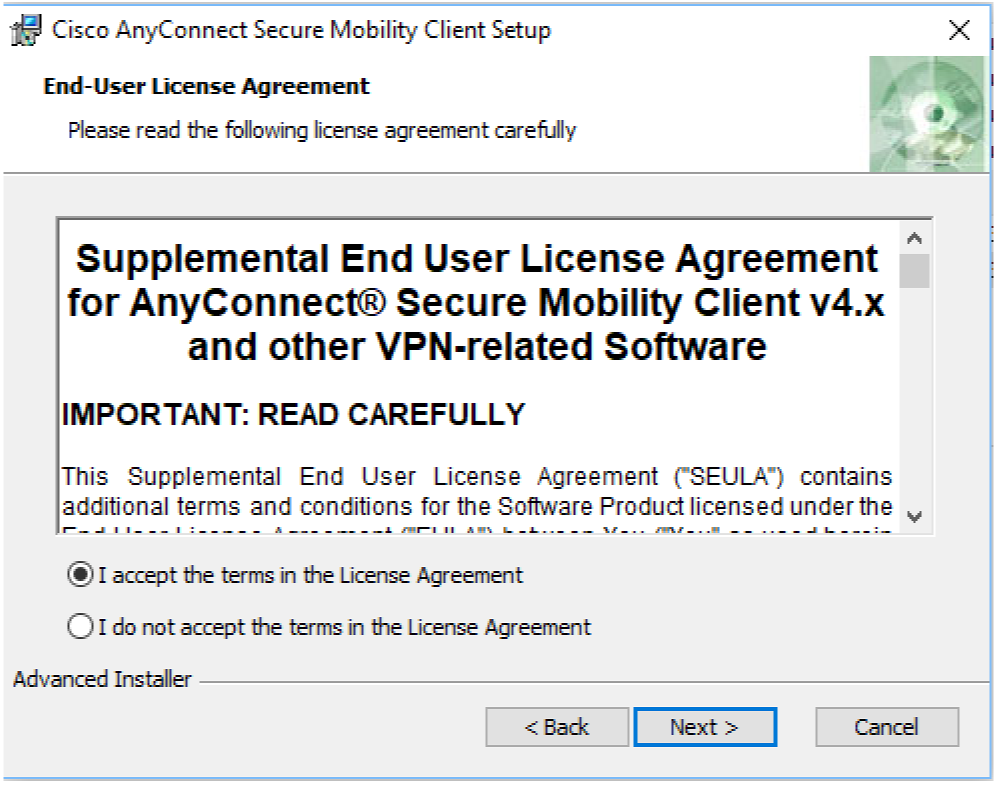
iv. Once run, the following screen will appear:



Welcome to the Cisco AnyConnect Secure Mobility Client Setup Wizard

The Setup Wizard will allow you to change the way Cisco AnyConnect Secure Mobility Client features are installed on your computer or even to remove Cisco AnyConnect Secure Mobility Client from your computer. Click Next to continue or Cancel to exit the Setup Wizard.

c. Select Next



End-User License Agreement

Please read the following license agreement carefully

Supplemental End User License Agreement for AnyConnect® Secure Mobility Client v4.x and other VPN-related Software

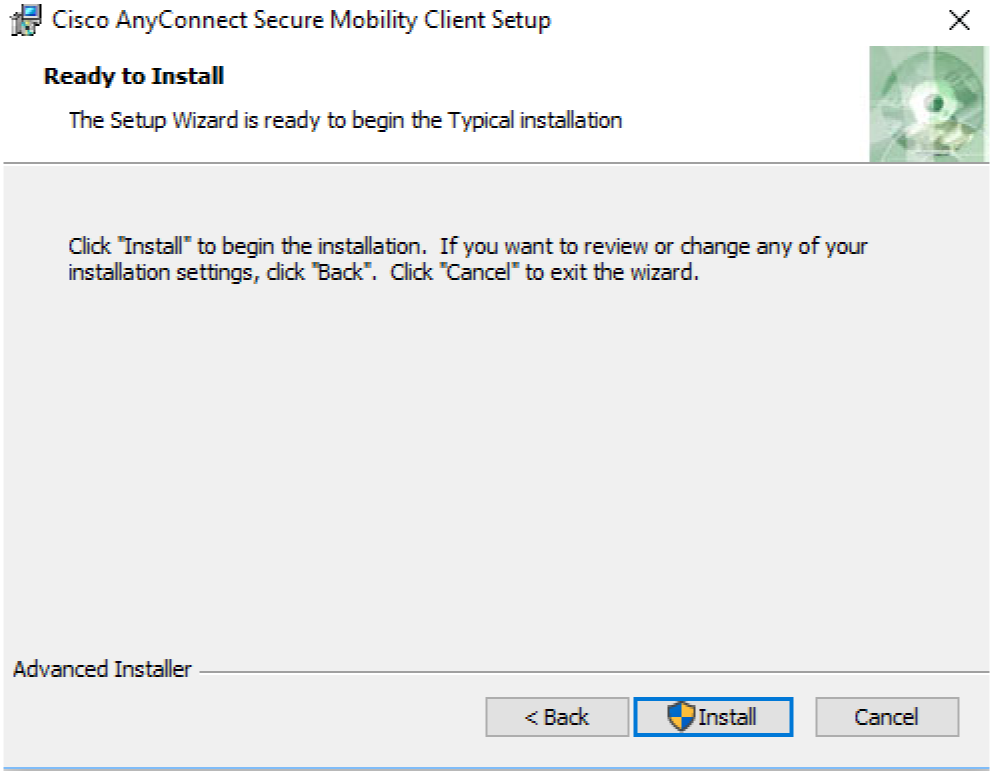
IMPORTANT: READ CAREFULLY

This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software Product licensed under the

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

i. Accept the License Agreement and select Next

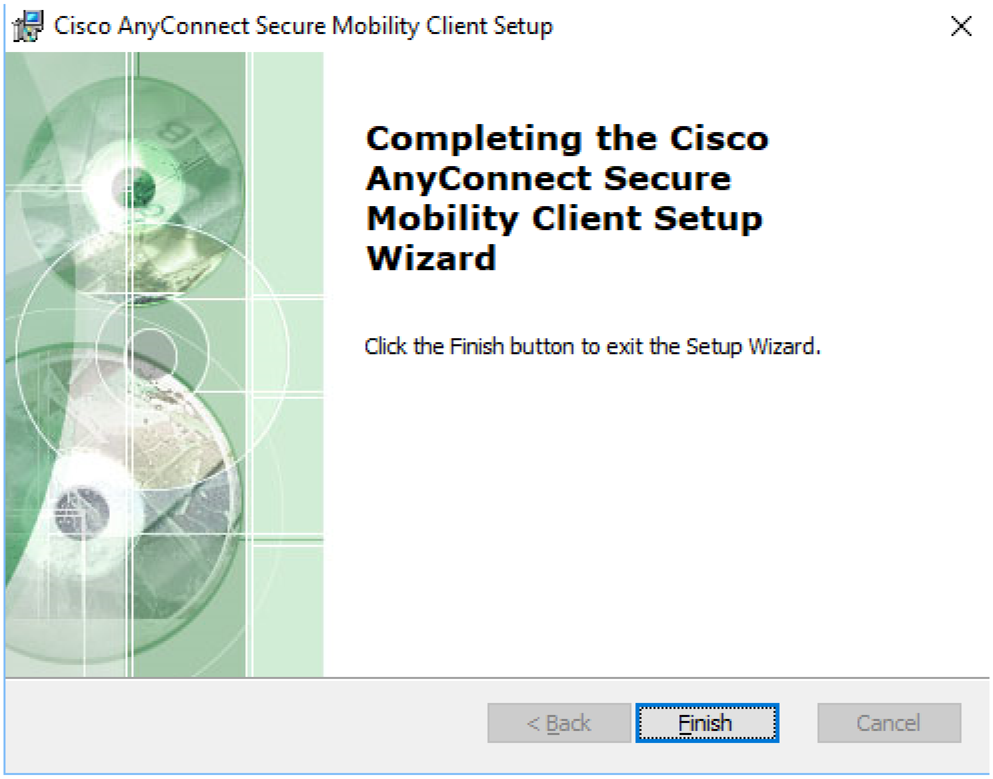


Ready to Install

The Setup Wizard is ready to begin the Typical installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

ii. Select Install



Cisco AnyConnect Secure Mobility Client Setup

Completing the Cisco AnyConnect Secure Mobility Client Setup Wizard

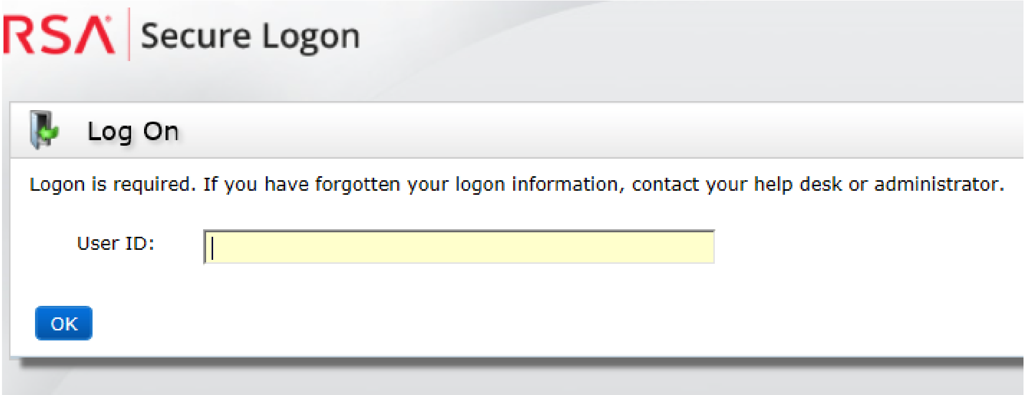
Click the Finish button to exit the Setup Wizard.

iii. Select Finish. The Cisco AnyConnect Client has been installed.To confirm it has been installed, follow Step 2-a above.

III. Set up your Multifactor Authentication – To establish a secure VPN tunnel, we require that you authenticate in 2 separate ways each time that tunnel is created. This adds an extra layer of security to the tunnel and protects your connection.

- a. Obtain an RSA account from your agency VPN Liaison. This account will include the following:
  - i. Userid
  - ii. Password
    1. NOTE: The password is only good for 10 days, so you MUST complete these steps within 10 days of receiving this account information.
- b. Go to https://rast.ct.gov

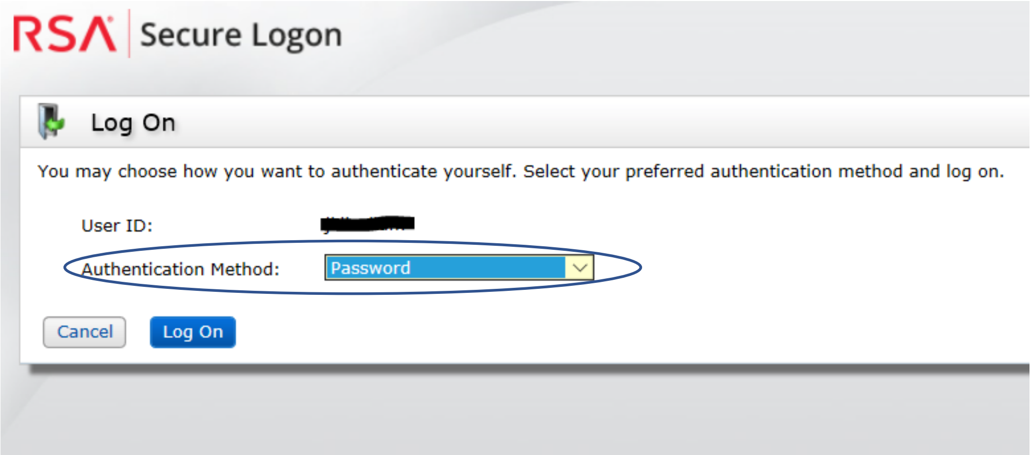
c. From that screen, in the Log On section, enter the RSA Userid (in Step III-i above) in the User ID field. Select OK



Logon is required. If you have forgotten your logon information, contact your help desk or administrator.

User ID:

d. On this screen, make sure the Authentication Method is set to Password. Select Log On

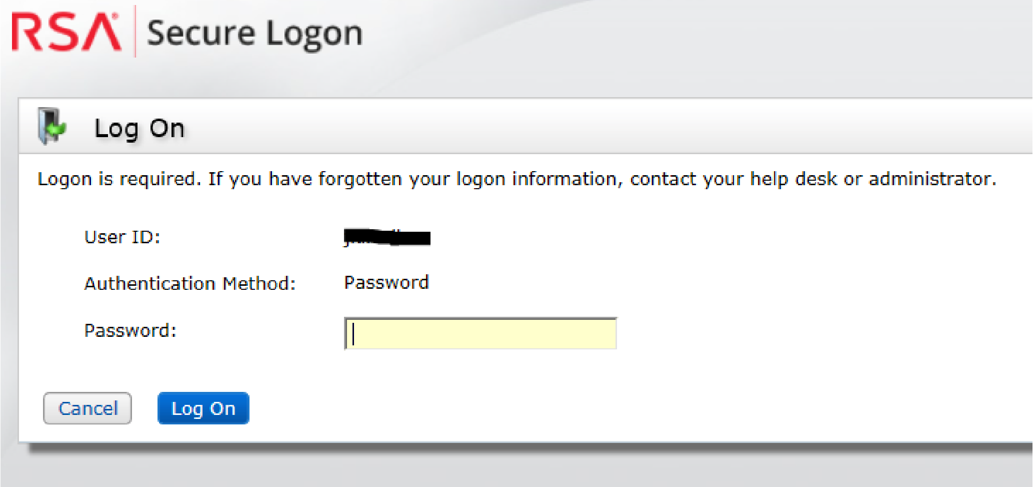


You may choose how you want to authenticate yourself. Select your preferred authentication method and log on.

User ID: [redacted]

Authentication Method: Password

e. Type in the RSA Password (from Step XXXX above). Select Log On



Logon is required. If you have forgotten your logon information, contact your help desk or administrator.

User ID: [redacted]

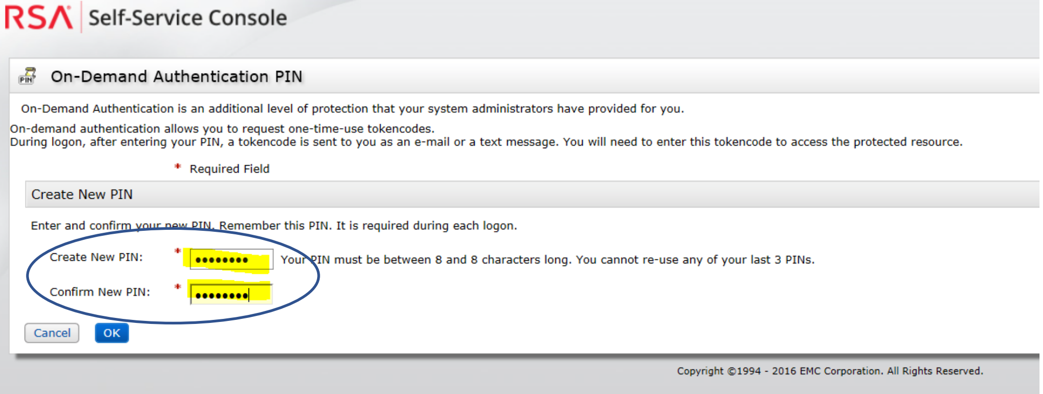
Authentication Method: Password

Password:

f. On this screen, you will be required to create a PIN. The PIN must follow these rules:

   i. 8 characters long (no more, no less)

ii. Letters and numbers only (no special characters or symbols)



RSA Self-Service Console

On-Demand Authentication PIN

On-Demand Authentication is an additional level of protection that your system administrators have provided for you.

On-demand authentication allows you to request one-time-use tokencodes.
During logon, after entering your PIN, a tokencode is sent to you as an e-mail or a text message. You will need to enter this tokencode to access the protected resource.

* Required Field

Create New PIN

Enter and confirm your new PIN. Remember this PIN. It is required during each logon.

Create New PIN: * •••••••• Your PIN must be between 8 and 8 characters long. You cannot re-use any of your last 3 PINs.

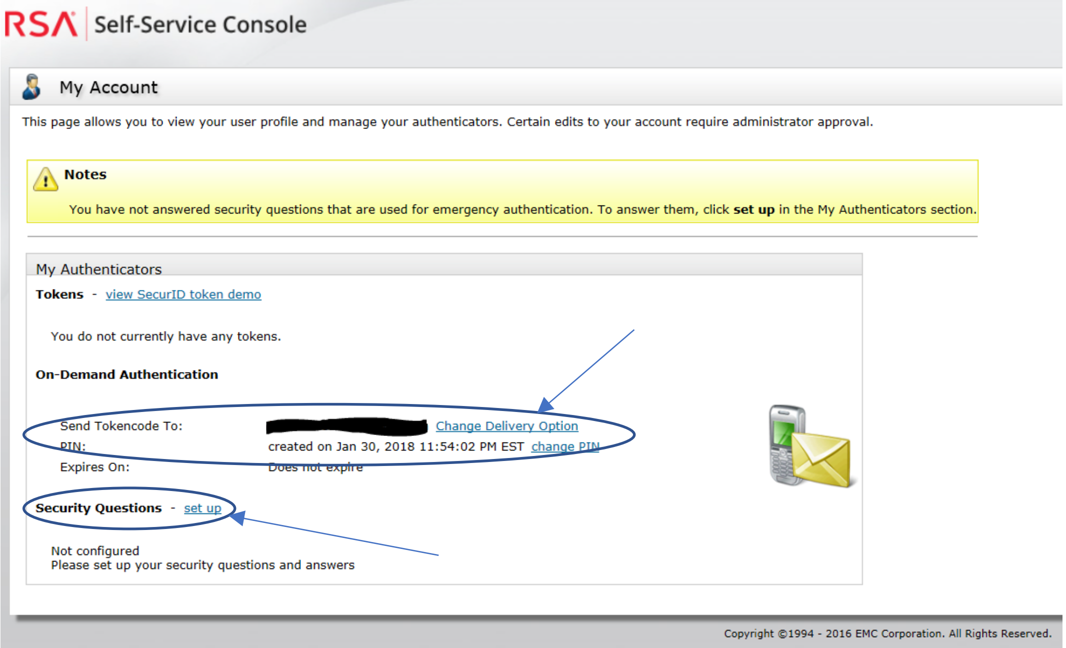
Confirm New PIN: * ••••••••

Cancel OK

Copyright ©1994 - 2016 EMC Corporation. All Rights Reserved.

g. Select OK

h. The next screen is the Console. From this screen, you can change your email and PIN and add Security Questions



RSA Self-Service Console

My Account

This page allows you to view your user profile and manage your authenticators. Certain edits to your account require administrator approval.

Notes

You have not answered security questions that are used for emergency authentication. To answer them, click **set up** in the My Authenticators section.

My Authenticators

Tokens - view SecurID token demo

You do not currently have any tokens.

On-Demand Authentication

Send Tokencode To: [redacted] Change Delivery Option

PIN: created on Jan 30, 2018 11:54:02 PM EST change PIN

Expires On: Does not expire

Security Questions - set up

Not configured
Please set up your security questions and answers

Copyright ©1994 - 2016 EMC Corporation. All Rights Reserved.

i. In the On-Demand Authentication section,

   i. Confirm the email address listed in the “Send Tokencode To:” field is valid and available to you from home

      1. For example, if you used your work email address, but you can only access your work email from your desk, then you should change it

      2. The emails that you will be sent will come from rsa.best@ct.gov. Please make sure that these are not blocked from that Inbox

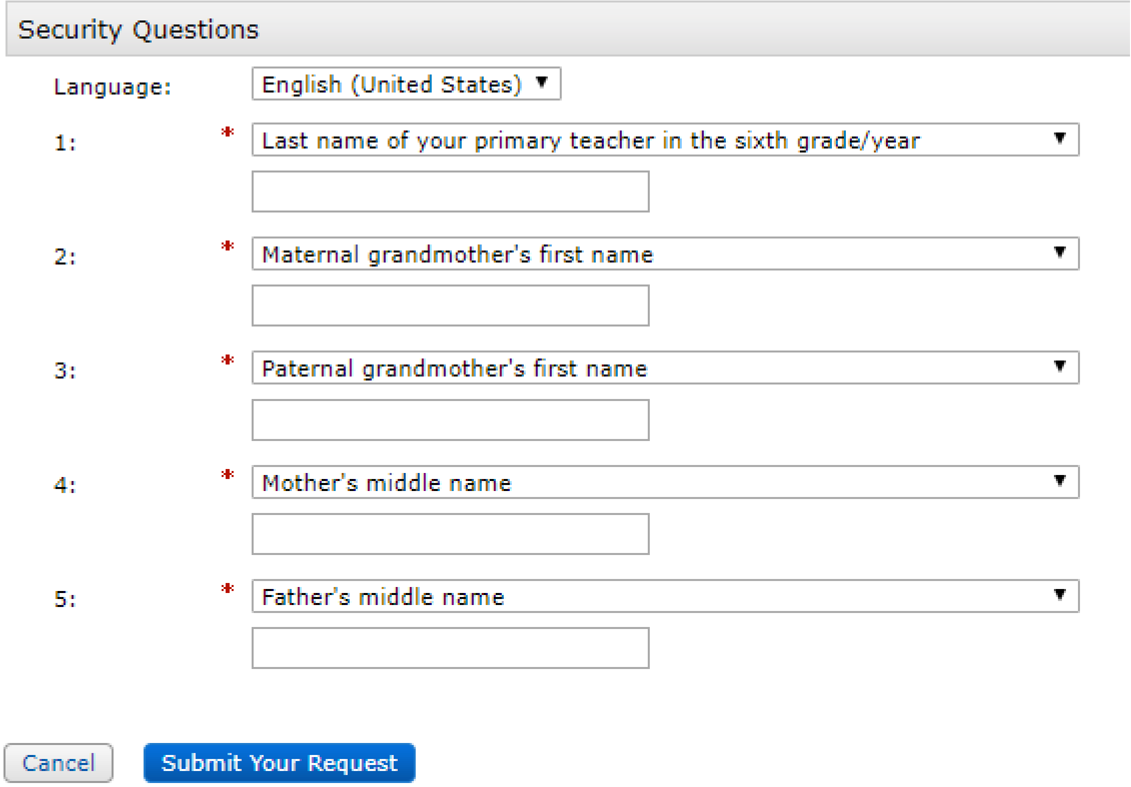
         a. Check with your email provider for instructions on how to confirm that. (It varies by email provider)

   ii. To change the email address, select Change Delivery Option

   iii. If you want to change your PIN, select change PIN

j. Set Up your Security Questions – These questions will be used to occasionally verify your identity when you try to log into VPN

k. Select the set up link next to Security Questions



Security Questions

Language: English (United States) ▼

1: * Last name of your primary teacher in the sixth grade/year ▼

2: * Maternal grandmother's first name ▼

3: * Paternal grandmother's first name ▼

4: * Mother's middle name ▼

5: * Father's middle name ▼

l. In each of the numbered lines, select a question from the dropdown list

   i. In the field below each question, provide your answer to that question

      1. Note: The answers are not case sensitive

   ii. When all five are completed, select Submit Your Request

IV. Test your VPN Access – Once you have the Cisco AnyConnect Client installed and you have created a PIN, you should test the connection

   a. You must not be on the State Network to test, however, you must have internet access

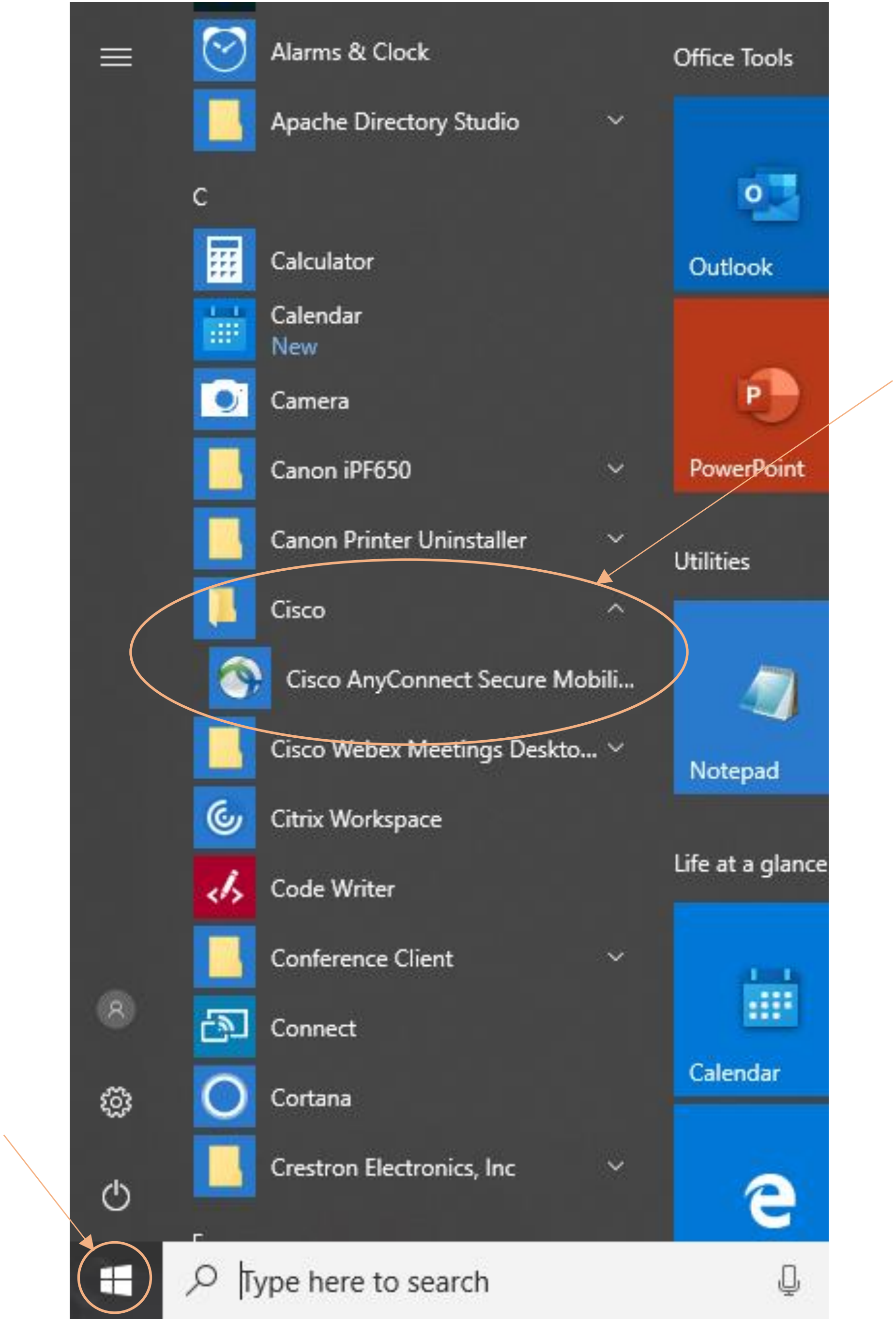
      i. Check with your IT Department to show you how to disconnect from the State Network while at work

      ii. Alternatively, when at home with your device, connect to your internet and test

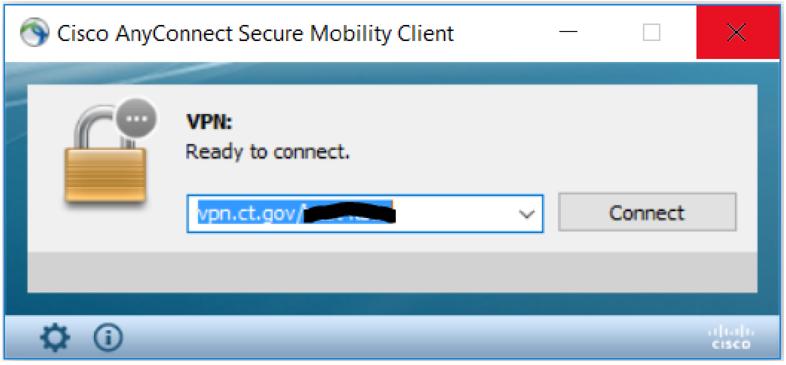
   b. Launch the Cisco AnyConnect Client

      i. Go to your Startup Menu (the Windows icon in the bottom left corner of your screen) and select the Cisco folder. In that folder should be Cisco

AnyConnect Secure Mobility Client. Select that



ii. When the client opens, confirm your VPN Profile is correct



VPN:
Ready to connect.

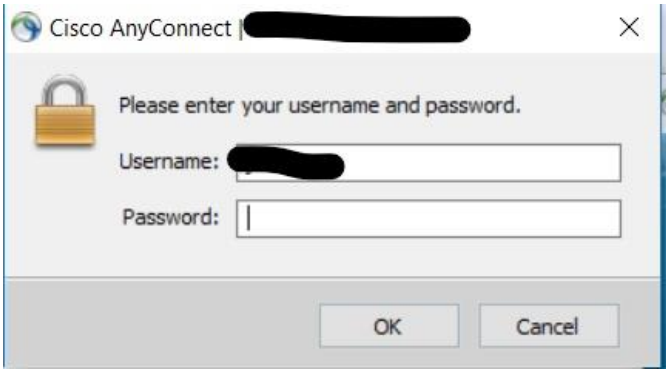
vpn.ct.gov/[redacted]

iii.

1. If it is not, enter the VPN Profile information exactly as presented above

iv. Once the VPN Profile information is correct, select Connect

v. At the next screen, enter the following information and Select OK:



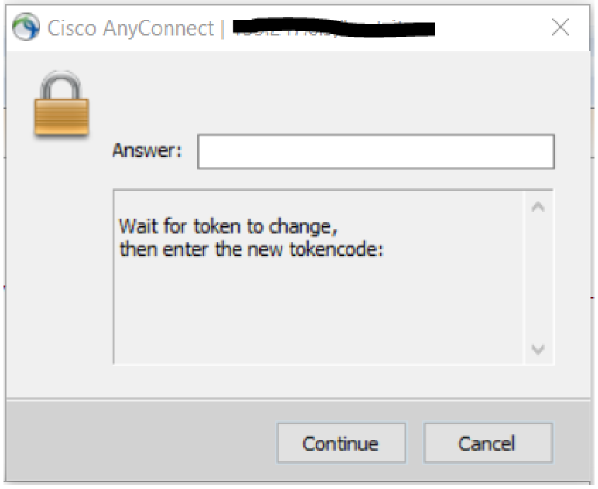
Please enter your username and password.

Username: [redacted]

Password:

1. Enter your Userid (from Step III-i) in the Username field
2. Enter your PIN (from Step III-ii) in the Password field

vi. On the next screen, you will be asked for an Answer



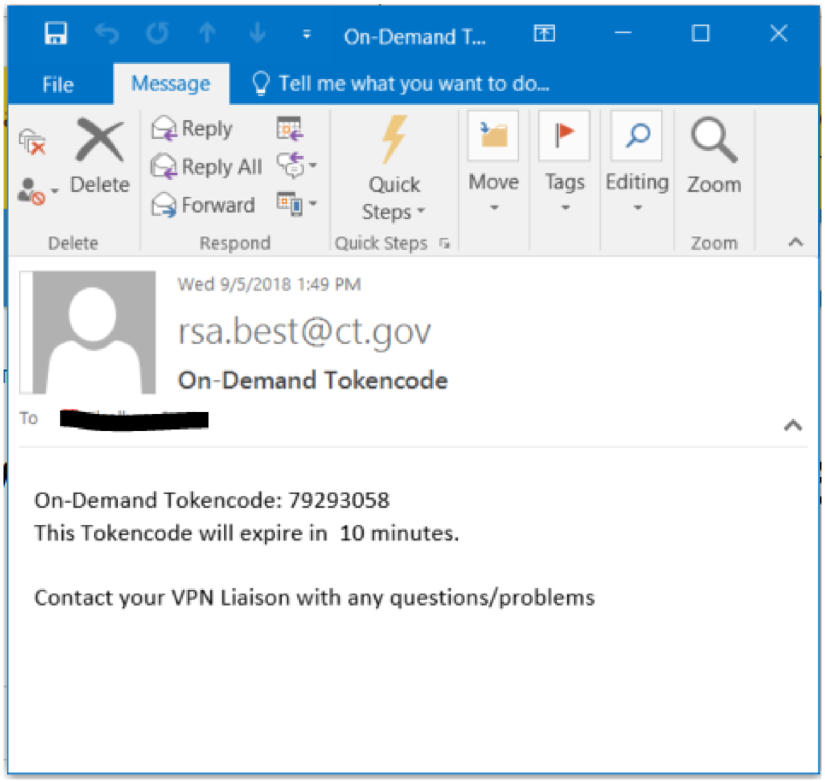
Answer:

Wait for token to change,
then enter the new tokencode:

1. NOTE: The message will say "Wait for the token to change…" This means that an email is being generated and sent to the email

address you provided. Go to that Inbox and wait for the email from rsa.best@ct.gov, using a title On-Demand Tokencode

2. When that email arrives, enter the 8-digit number listed next to On-Demand Tokencode into the Answer field



Wed 9/5/2018 1:49 PM

rsa.best@ct.gov

On-Demand Tokencode

To [redacted]

On-Demand Tokencode: 79293058

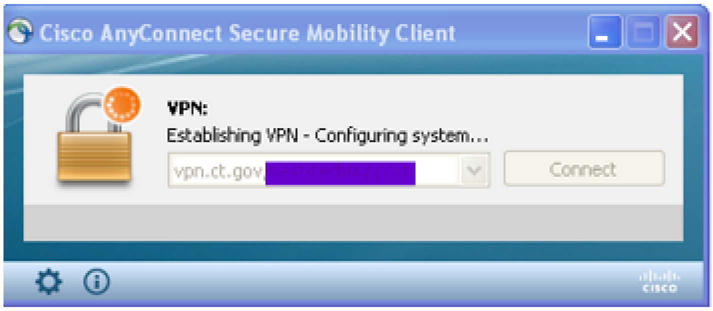
This Tokencode will expire in 10 minutes.

Contact your VPN Liaison with any questions/problems

   a. You can copy from the email and paste into the Answer field
   b. The token will expire after 10 minutes. If that happens, start the test over

3. Select Continue on the Answer screen

vii. After the Answer has been entered, you will see the Cisco AnyConnect Client make the connection to the VPN



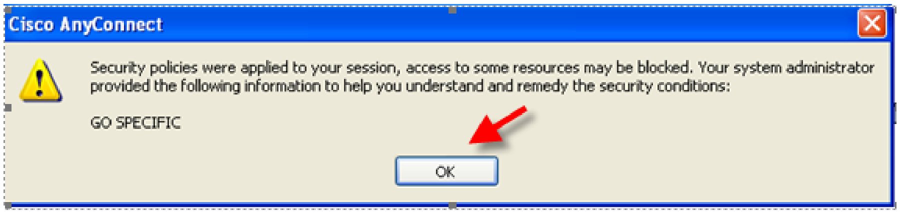
VPN:

Establishing VPN - Configuring system...

vpn.ct.gov [redacted]

   1. Note that this may take a minute to complete

viii. A warning will appear explaining that you are entering the State of Connecticut network. Select OK to complete the connection to your VPN



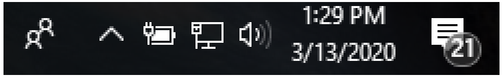
Cisco AnyConnect

Security policies were applied to your session, access to some resources may be blocked. Your system administrator provided the following information to help you understand and remedy the security conditions:

GO SPECIFIC

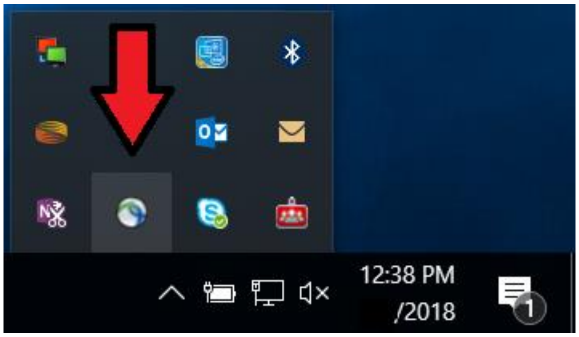
1. NOTE: The wording of the warning varies from VPN Profile to VPN Profile. It may not be the same wording as shown above

ix. When the connection is complete, you may see a message in the lower right corner that reads "Cisco AnyConnect VPN: Connected", but it goes away after a few seconds. To confirm you are connected:
   1. Find the Cisco AnyConnect icon in your system tray
      a. Your system tray can be found in the bottom right corner of your screen near the date and time



         i. NOTE: The icon in that area vary from device to device

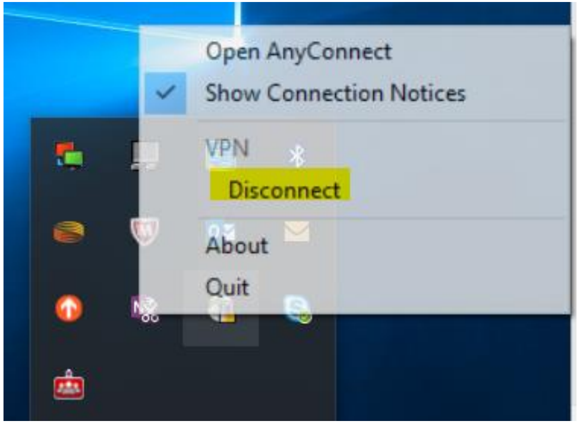
      b. The Cisco AnyConnect icon may show on your screen already, but if not, select the up arrow in your system tray to display all icons



   2. Hover over the Cisco AnyConnect icon with your cursor and the message "Cisco AnyConnect VPN: Connected" will appear if you are connected
      a. If you are not connected, the message "Cisco AnyConnect VPN: Disconnected" will appear

V. To disconnect from the VPN
   a. Find the Cisco AnyConnect icon in your system tray (see above)
   b. Right click on the Cisco AnyConnect icon

c. From the menu that appears, select Disconnect



d. You are now disconnected from VPN