## **Soft & Hard Token Install and setup**

The directions below will show you how to either install the RSA Application for your Soft Token, or build the Hard Token for use, and then to connect to the VPN using the Cisco AnyConnect Client (Download located at this location if needed: <http://portal.ct.gov/DAS/BEST/Security-Services/Virtual-Private-Network-VPN-Service/Related-Resources> )

## **Soft Token Install and setup**

1. For PC/Laptop:
	1. You will have received the following information from your VPN Liaison
		1. Username (aka User ID)
		2. Soft Token Serial Number
		3. URL
		4. Activation Code
		5. VPN Profile
	2. Now go to the below URL to download and install either the 32 or 64 bit package, depending on your Operating System needs
		1. <https://community.rsa.com/docs/DOC-73395>
	3. Once downloaded, extract the files and run the msi (DO NOT run the one with “Auto” in the name)
	4. Accept all defaults and install
	5. Once the RSA App is installed, open the email with the information from your VPN Liaison and then open the RSA App to import your Token
	6. With RSA open, click on “Options” and then “Import Token”
		1. 
	7. Click on the “Import from Web” Hyperlink
		1. 
	8. From the information give to you, copy the URL (DO NOT CLICK IT) and past it to the field “Enter URL:”, then do the same for “Enter Activation Code:”
		1. 
	9. Once completed your RSA SecurID App will show 8 numbers (Tokencode), and rotate every 60 seconds
		1. 
	10. Once the App is functioning, you should be able to connect to the VPN using the remainder of the information from your VPN Liaison (See [BELOW](#_To_Connect_to_1) for instructions to Connect to the VPN)
2. For Mobile Phones
	1. You will have received the following information from your VPN Liaison
		1. Username (aka User ID)
		2. Soft Token Serial Number
		3. URL W/ Activation Code
		4. VPN Profile
	2. Download and install the RSA SecurID App from your app store
		1. Android: Google Play
		2. Apple: iTunes
	3. Once downloaded, open the email and click on the “URL W/ Activation Code”
		1. This should automatically install the seed and begin generating Tokencodes right away
	4. Once the App is functioning, you should be able to connect to the VPN using the remainder of the information from your VPN Liaison (See [BELOW](#_To_Connect_to_1) for instructions to Connect to the VPN)

## **Hard Token Setup**

1. You will have received the following information from your VPN Liaison
	1. Username (aka User ID)
	2. Hard Token Serial Number
	3. VPN Profile
2. Once you have this information you should be able to connect to the VPN (See [BELOW](#_To_Connect_to_1) for instructions to Connect to the VPN)

## **On-Demand Authentication Setup (ODA)**

1. Please refer to the “On-Demand Authentication VPN Guide” located here: <http://portal.ct.gov/DAS/BEST/Security-Services/MultiFactor-Authentication/Documents>

#

# **To Connect to the VPN**

1. Click on Start > Type “AnyConnect”, and then select the “Cisco AnyConnect Client”
	1. 
2. The Cisco Any Connect Secure Mobility Client login will be launched. Enter your VPN Profile in the given format with the group name obtained from your instructions, then click “Connect”.
	1. VPN Profile: **vpn.ct.gov/ “group name” (MUST BE lower case and DO NOT use http or https in front)**

 

*Note: If by chance you enter the Connection Profile incorrectly (ie. wrong case or use of protocol in front FQDN, etc.) the first time, you will need to restart your machine to clear the cache.*

1. Once the “Username” and “Password” pop up comes up, you will need to enter you information based on the style of RSA Authentication you are using (go to [Step a](#Soft_Token). for Soft Token, and [Step b.](#Hard_Token) for Hard Token)
	1. **Soft Token** (PC/Laptop and Mobile Phone):
		1. Enter your “User ID” in the “Username” field, then enter the 8 digits from your RSA Application installed your device in the “Password” field, then click “OK”
			1. 
		2. The following pop up will ask you to create a new PIN, which has to be exactly 8 characters long, and consist of numbers and letters only (NO special characters), then click “Continue”
			1. 
		3. Repeat your chosen PIN in the following pop up to confirm it, then click “Continue”
			1. 
		4. After that you will be asked to “Wait for the token to change, then enter the new tokencode”, in which case you will need to wait for the numbers to rotate on your RSA App, then enter your new PIN+Token number and click “Continue”

*Example: if my newly created PIN was bEsT (which cannot be used because it is only 4 characters), and my Soft Token had on the screen 4416-9741, then I would enter “bEsT44169741”, without the “ ”*

* + - 1. 
		1. You should now be connected to the VPN if you have completed all these steps successfully. Please note; You will only need to enter the Tokencode (PIN+Token Number) from now on when logging in
		2. You will then see the AnyConnect Client making the connection
			1. 
		3. And finally you will get a warning stating that you are entering a State Network, which may vary from Profile to Profile, just click “OK”
			1. 
	1. **Hard Token**
		1. Enter your “User ID” in the “Username” field, then enter the 6 digits from your RSA Hard Token in the “Password” field, then click “OK”
			1. 
		2. The following pop up will ask you to create a new PIN, which has to be exactly 8 characters long, and consist of numbers and letters only (NO special characters), then click “Continue”
			1. 
		3. Repeat your chosen PIN in the following pop up to confirm it, then click “Continue”
			1. 
		4. After that you will be asked to “Wait for the token to change, then enter the new Tokencode”, in which case you will need to wait for the numbers to rotate on your RSA Hard Token, then enter your new PIN+Token number and click “Continue”

*Example: if my newly created PIN was bEsT (which cannot be used because it is only 4 characters), and my Hard Token had on the screen 449 741, then I would enter “bEsT449741”, without the “ ”*

* + - 1. 
		1. You should now be connected to the VPN if you have completed all these steps successfully. Please note; You will only need to enter the Tokencode (PIN+Token Number) from now on when logging in
		2. You will then see the AnyConnect Client making the connection
			1. 
		3. And finally you will get a warning stating that you are entering a State Network, which may vary from Profile to Profile
			1. 
	1. **On-Demand Authentication (ODA)**
		1. Please see the following Guide which will walk you through the setup: <http://portal.ct.gov/DAS/BEST/Security-Services/MultiFactor-Authentication/Documents>

**To Disconnect from the VPN**

1. Find the Cisco AnyConnect icon in your System Tray in the lower right of your screen
	1. 
2. Right Click on it, then select “Disconnect”
	1. 
3. All done.

*For any questions or concerns please contact your VPN Liaison, or reach out to* *best.mfaHelpDesk@ct.gov* *and they will direct you to where you need to go.*