

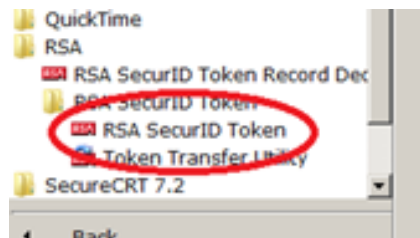
RSA SecurID soft tokens provide security to Commonwealth of Virginia (COV) employees by allowing a secure virtual private network (VPN) connection for personal computers (PC) that are not directly connected to the COV domain. This document explains how to import the RSA software token and set up a PIN for the Cisco AnyConnect VPN client.

If you have any questions regarding the setup or log in process for your VPN services, please contact the VITA Customer Care Center at (866) 637-8482.

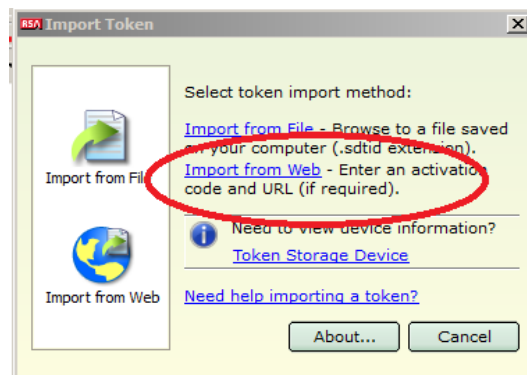
How to Activate and Retrieve Your Software Token



1. Click the Windows **Start** button
2. Select **All Programs**.
3. Select **RSA**.
4. **Select RSA SecurID Token.**
5. Select the **RSA SecurID Token** logo.



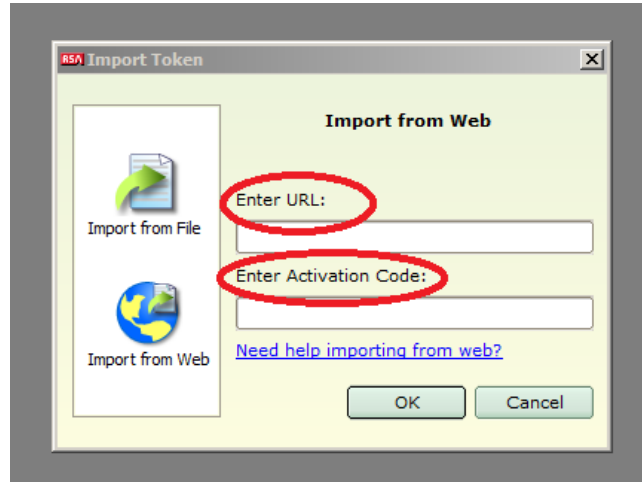
6. When the program opens, select **Import From Web**.



Note: Dialog boxes may be hidden behind open windows.

7. Enter the **URL** and **Activation Code** provided to you in the email.

*Note: Your **Activation Code** is unique; check your documentation for yours.*



RSA Soft Token Import
URL:

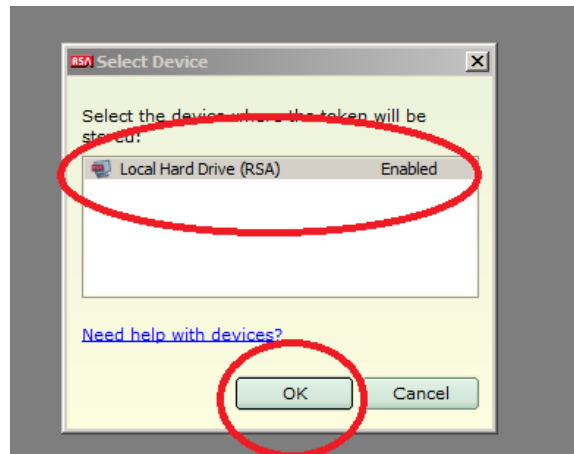
<https://selfsrv.vita.virginia.gov:443/ctkip/services/CtkipService>

Note: The URL is case sensitive.

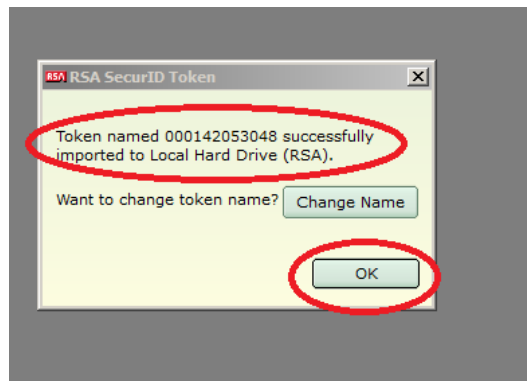
Note: The URL cannot be clicked on, typed in or copied to the address bar.

8. Click **OK**.

9. If you are prompted by a pop-up window to **Select Device**, click once on **Local Hard Drive (RSA)** then select **OK**. (This dialog box may not appear.)



10. Your token will be imported from the Internet server and will display this screen when completed:



Click **OK**.

Note: Do NOT change the name or serial number of the token.

11. Your token now is ready to use. It will display in a format similar to this; the number will be different each time you access it:



Note: Do not enter spaces that may appear between the numbers on the secure token.

For purposes of these instructions only, leave this box open. You will need the number in the next step below. (Numbers are randomly generated and will change about every minute.)

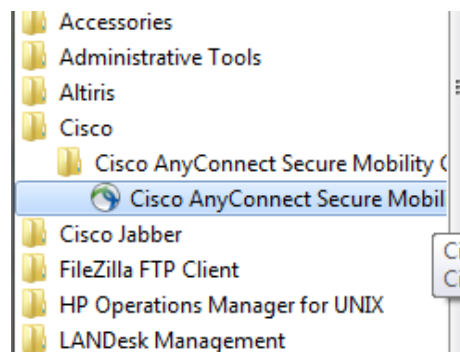
12. Each time you log in to VPN, access your new SecurID token by following steps 1 through 5 above.



**For first time set-up, please proceed to the next section:
How to Create a PIN on the CISCO AnyConnect Client**

How to Create a PIN on the Cisco AnyConnect Client

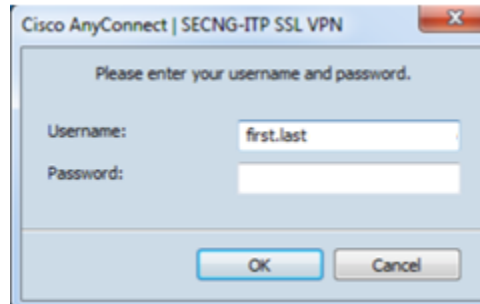
1. If you are connected to VPN, log off.
2. Launch your Cisco AnyConnect VPN client. (If you do not know how to launch the client, follow steps 2 through 6. If you do know how to launch, skip to step 7.)
3. Select **All Programs**.
4. Select **Cisco** folder.
5. Select **Cisco AnyConnect Secure Mobility Client** folder.
6. Select **Cisco AnyConnect Secure Mobility Client** software.



7. Once the application loads, select **Connect**.



- The username field may be populated with your email address. You will need to change this to the soft token username as it appears in the email sent to you.



Cisco AnyConnect | SECNG-ITP SSL VPN

Please enter your username and password.

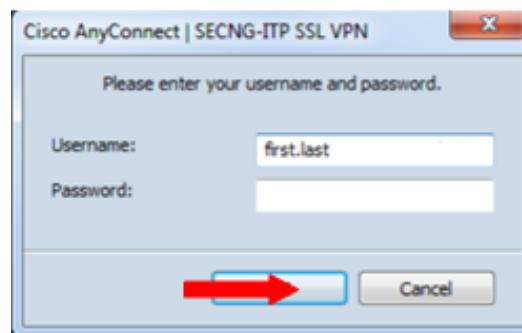
Username: first.last

Password:

OK Cancel

Note: Your username is usually *firstname.lastname* (e.g. *John.Smith*). Please check your documentation to be sure of your credentials.

- Enter the secure code from software token display you activated above as the password **for this setup only**. Remember: do not enter spaces that may appear between the numbers on the secure token.



Cisco AnyConnect | SECNG-ITP SSL VPN

Please enter your username and password.

Username: first.last

Password:

OK Cancel

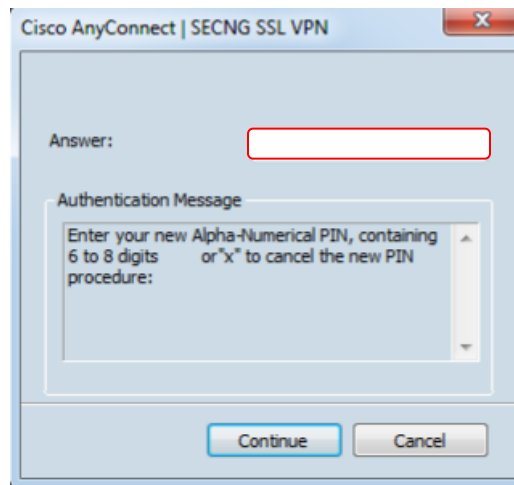
Click **OK**.

10. You will be prompted to enter a PIN. Input only the characters that you wish to use as your PIN. Do **NOT** input the token code here.

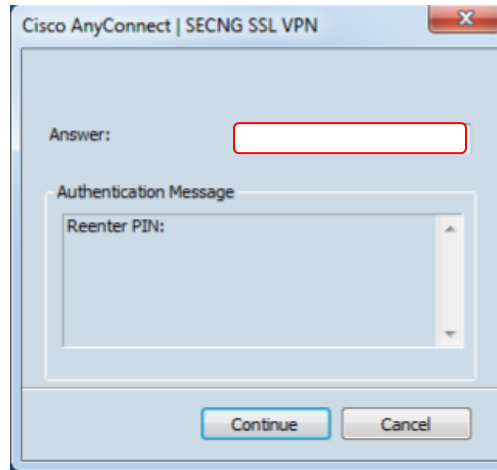
Each PIN must:

- Contain **no fewer than six and no more than eight** characters.
- Contain an **alphabetic character** (e.g. abc).
- Contain a **numeric character** (e.g. 123).
- Contain **NO special characters** (e.g. !@#).
- Contain **only lowercase letters** and use no capitalization.

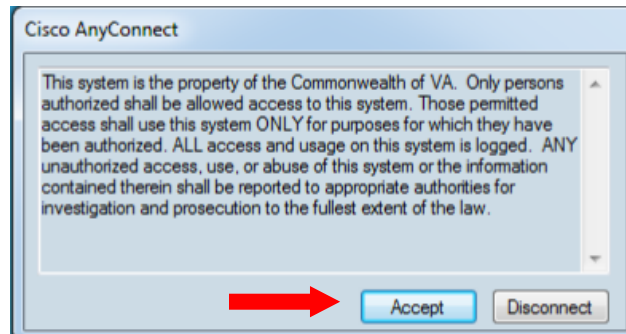
***Example:** A valid PIN might look like: abc123*



You will be prompted a second time to input your PIN. This is to confirm you did not mistype the PIN the first time. Type the same PIN you did from the previous step.



11. Once successful, click **Accept** on the following acceptance box:



12. This completes the setup for your PIN for the Cisco AnyConnect VPN client.

13. Each time you log in to VPN, you will enter your soft token username (usually firstname.lastname) and a passcode as your credentials. **Your passcode is comprised of your PIN and the soft token code.**

Passcode: PIN and soft token code (for example: abc12321778043)

14. You will not need to change your PIN; the soft token code, however, will be different each time.

If you have any questions or forget your PIN, please contact the VITA Customer Care Center at (866) 637-8482.

**You are now ready to sign on to VPN using two-factor authentication.
To learn how to log in to VPN, please proceed to the next section.**



How to Log in to VPN Using Two-Factor Authentication

After activating your soft token and creating your PIN, you must do the following **each time** you log in to VPN:

1. Retrieve your soft token (See steps 1 through 5 in “How to Activate and Retrieve Your Software Token”).
2. Launch the Cisco AnyConnect VPN client.
3. Enter your soft token username (usually firstname.lastname).
4. Enter your passcode
 - a. Your passcode is comprised of the PIN you created and the soft token you retrieved in step 1. (for example: abc12321778043)
5. Once you have logged on to VPN, close the soft token code dialog box.

