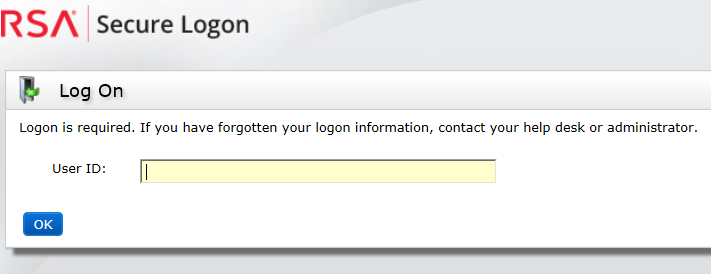
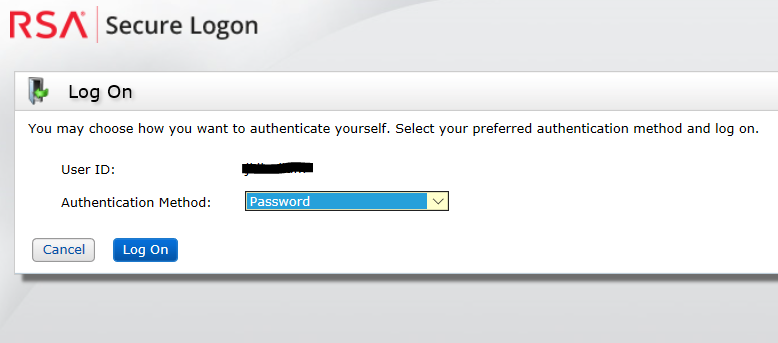
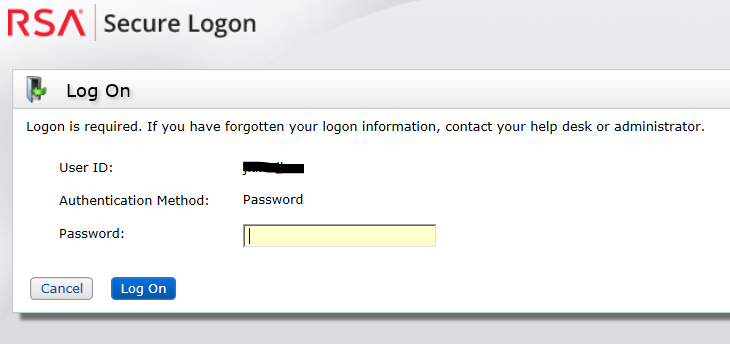
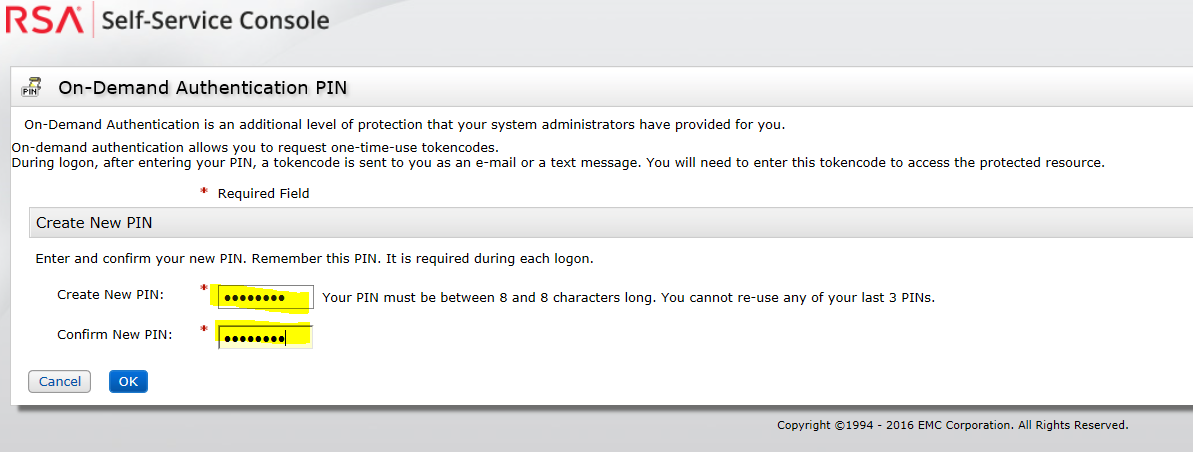
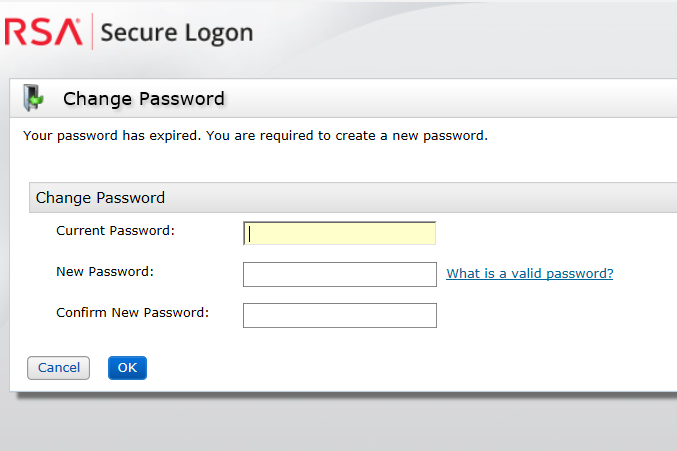
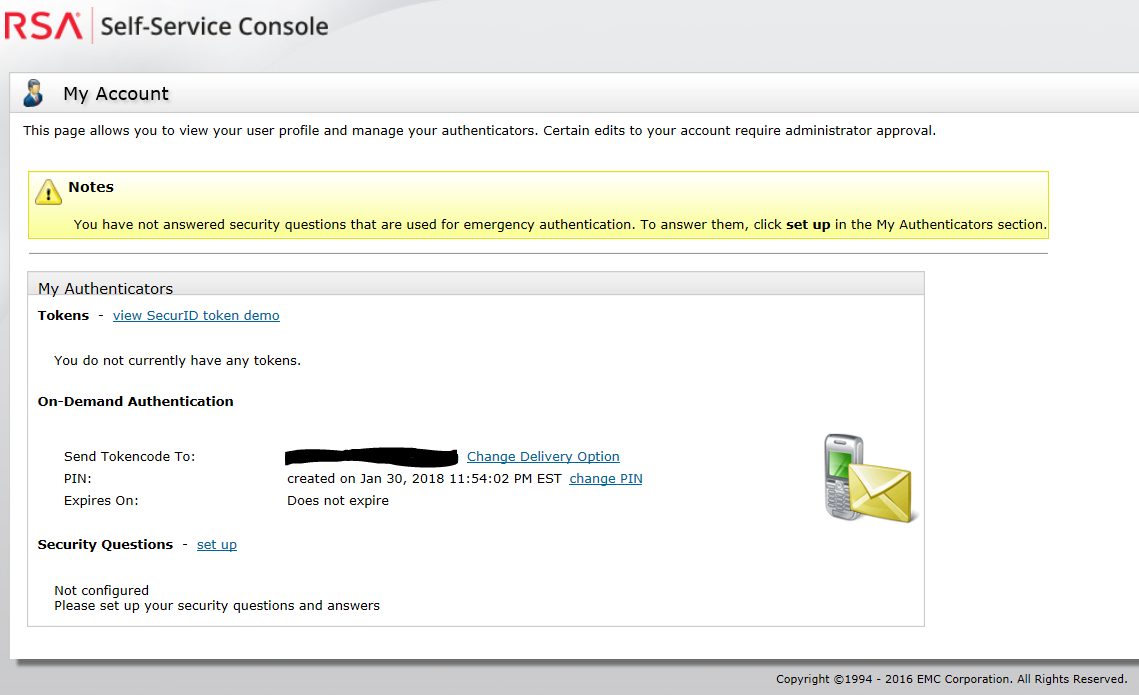
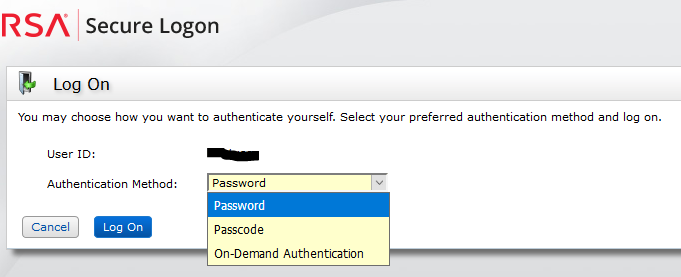
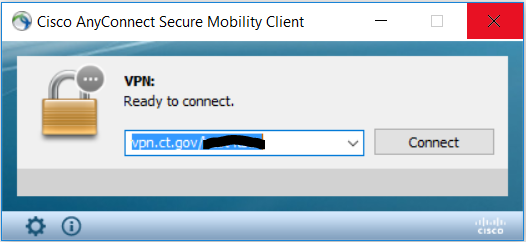
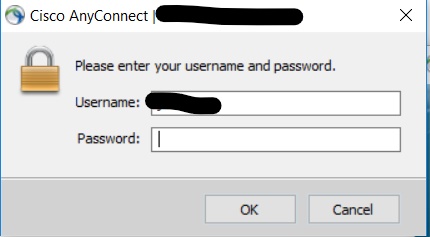
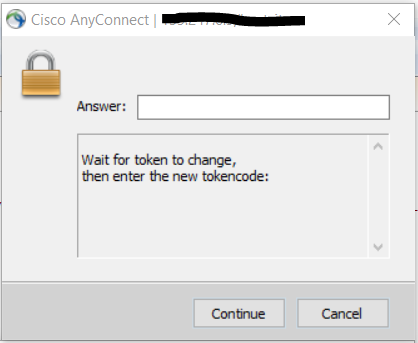
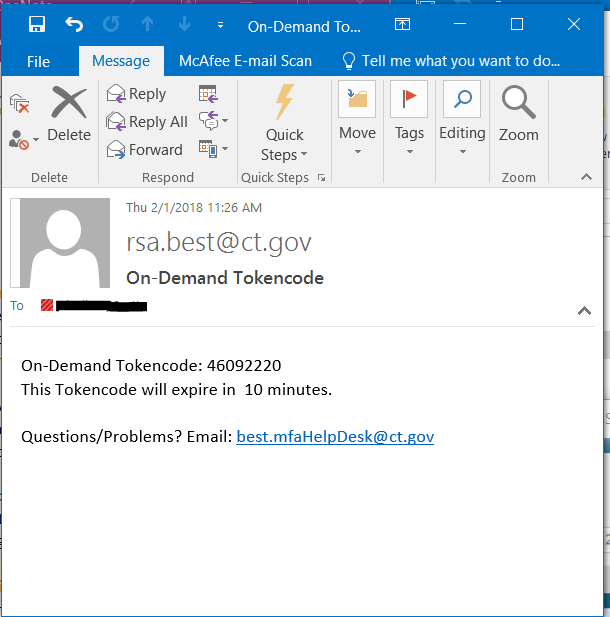
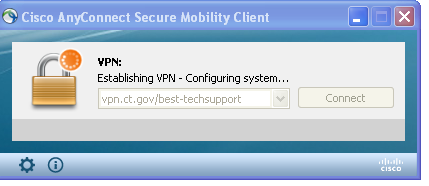
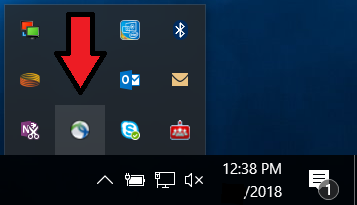
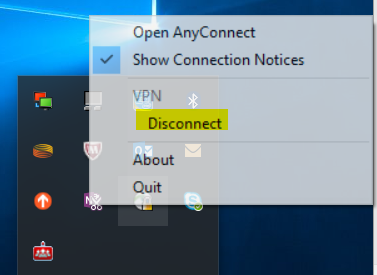
# **On-Demand Authentication (ODA) VPN/RSA User Guide**

Follow these instructions to activate your ODA PIN, set yourself up in the RSA Self-Console, and connect to VPN utilizing the ODA method (Cisco AnyConnect VPN Clients can be found here: <http://portal.ct.gov/DAS/BEST/Security-Services/Virtual-Private-Network-VPN-Service/Related-Resources> )

1. Obtain an RSA account from your VPN Liaison
   1. If you do not know who your Liaison is please email the Multi Factor Authentication Help Desk at [best.mfaHelpDesk@ct.gov](file:///\\exec\dfs\best%20users\kilcollumju\SOP\Active%20HD%20SOP's\In%20Progress\best.mfaHelpDesk@ct.gov) or your IT Department for further instructions
2. Once you have an account, you will need to go to <https://rast.ct.gov> and use the login information given, which should be
   1. User ID: Typically it will be first initial then last name
      1. Ie: Jane Doe would be jdoe
   2. Password: This will be issues to you by your Liaison or Help Desk Associate and will only be active for 10 days
3. Once at the website, please enter your “User ID”, then click “OK”
   1. 
4. Once on the next screen, leave the dropdown menu on “Password”, then enter said Password, and click “Log On”
   1. 
5. On the following screen, type in your Password and click on “Log On” once more
   1. NOTE – The “Authentication Method” should say “Password”, if it does not just click on Cancel, it will return you to Step 3, and be sure the drop down menu says “Password” in Step 4
   2. 
6. Once you have entered the Password you will be brought to a screen to create your PIN. The PIN should be 8 characters (alpha and/or numeric, no symbols or special characters)
   1. 
   2. If the below screen shot shows up then the Password was changed more than 10 days ago and needs to be changed as well (but will expire again in 10 days as well)
      1. 
7. Once in the console all of the users’ Soft/Hard Tokens will be available to change or update the PIN’s.
   1. It is HIGHLY advisable that at this point you need to create or update your Security Questions to stop any delays of getting you your On-Demand Authentication Code when logging in to VPN
   2. We also HIGHLY suggest that you check all other information on this page, confirming especially that the email entered here is available on and off network
   3. 
8. On subsequent logins to the Self-Service Console you will have the option for your method of authentication
   1. PASSWORD – This authentication was sent to you originally to log in for the first time. It expires after 10 days, and is the least likely method to be used beyond the initial logon
   2. PASSCODE – This is the join of your created PIN and the Tokencode from either a Hard or Soft Token. It is a common logon method
   3. ON-DEMAND AUTHENTICATION – This is used by entering your PIN you created in the Self-Service Console, then on the next screen entering the Tokencode which has been sent to you via email/SMS
   4. 
9. Once your “Security Questions” have been created, you can test the ODA PIN on VPN by opening the Cisco AnyConnect Client and confirm the information in it is correct, then click “Connect”
   1. 
10. Once you hit connect you will be prompted for your “Username” and “Password”, please enter your User ID and PIN which you just setup through the RSA Self-Console, then click “OK”
    1. 
11. The next pop up will show up (see sub note a.) will ask you to “Wait for token to change” which means it is generating a Tokencode for you to enter and being sent to you via email (see sub note b.), and once received needs to be entered in the “Answer” Field and press “Continue”
    1. 
    2. 
12. Once you enter in the Tokencode you will see the AnyConnect Client make the connection to the VPN
    1. 
13. And finally you will get a warning that you are entering a State Network which may vary from Profile to Profile, just click “OK”
    1. 

**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*](mailto:best.mfaHelpDesk@ct.gov) *and they will direct you to where you need to go.*