

VPN Remote Access - On-Demand Authentication (ODA) User Guide

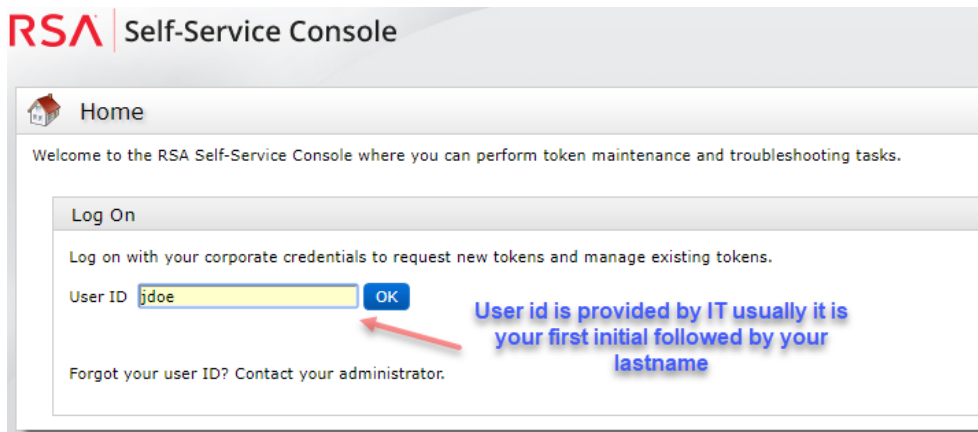
Steps:

A. RSA Self-Console	1
B. Install and setup the software	4
C. VPN Connect	5
D. Remote Desktop Logon	7
E. Remote Desktop Logoff	8
F. VPN disconnect	9

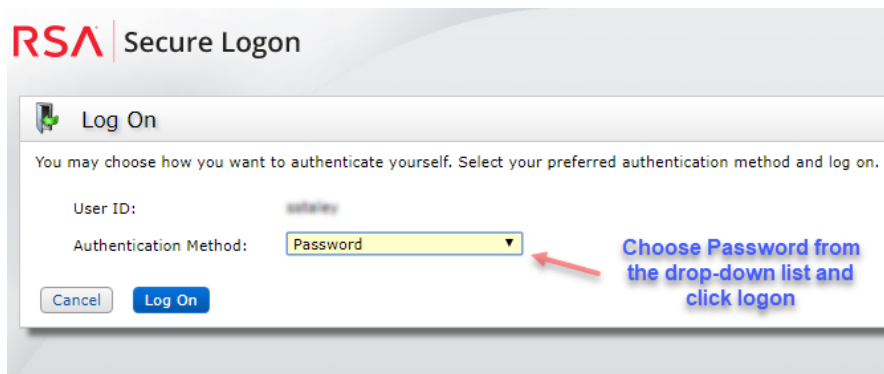
A. RSA Self-Console

Follow these instructions to activate your ODA PIN, set yourself up in the RSA Self-Console, and connect to VPN utilizing the ODA method. This registration procedure must be done as soon as possible.

- 1- Go to the website <https://rast.ct.gov> and enter the User ID sent to you by IT, usually it is your first initial followed by your last name, i.e.: Jane Doe would be jdoe



- 2- On the next screen, select Password from the Authentication Method drop down list and click logon.



- 3- Enter your password provided by IT (this password expires after 10 days)



- 4- 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).

Memorize this PIN, you will need it when you use Cisco AnyConnect (see step C)



- 5- Once you successfully log in, you will see your account information. Click the [Change Delivery Options](#) (refer to image below step 1) and enter your personal email address. This email address will be used to deliver your token code. It is HIGHLY advisable that at this point you need to create or update your Security Questions (refer to image below step 2) to stop any delays of getting you your On-Demand Authentication Code when logging in to VPN

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

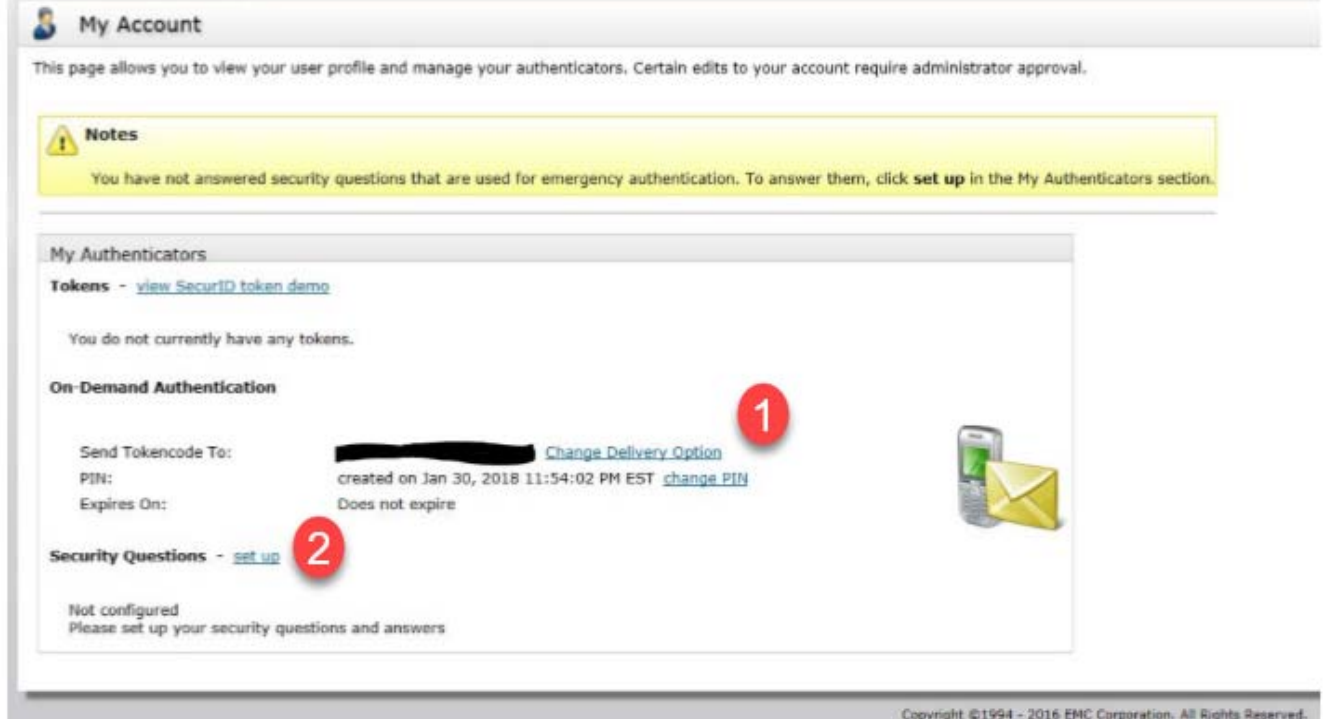
Send Tokencode To: [redacted] [Change Delivery Option](#) **1**

PIN: created on Jan 30, 2018 11:54:02 PM EST [change PIN](#)

Expires On: Does not expire

Security Questions - [set up](#) **2**

Not configured
Please set up your security questions and answers



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

On subsequent logins to the Self-Service Console – Only use when you need to change your email address.

Go to the website <https://rast.ct.gov> **VERIFY THIS STEP**

Use the 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.

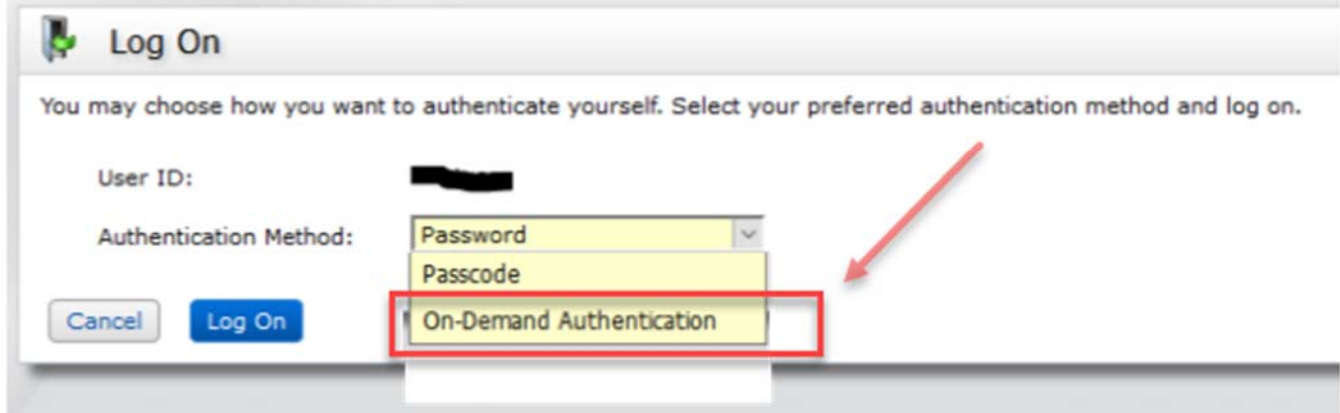
Log On

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

User ID: [redacted]

Authentication Method: Password, Passcode, **On-Demand Authentication**

[Cancel](#) [Log On](#)



B. Install and setup the software:

You need two pieces of software to be able to connect to the work PC/server via VPN.

- 1- Cisco AnyConnect
- 2- Microsoft Remote Desktop

Download and install the software:

Go the AG website <https://portal.ct.gov/ag/it/support/> and download and install the software by following the install wizard.

For windows users:

Download and install the Cisco AnyConnect only. The Microsoft Remote Desktop is already preinstalled with windows.



[Cisco AnyConnect](#)



Microsoft Remote Desktop (included with OS)

For Mac OS X users:



[Cisco AnyConnect](#)



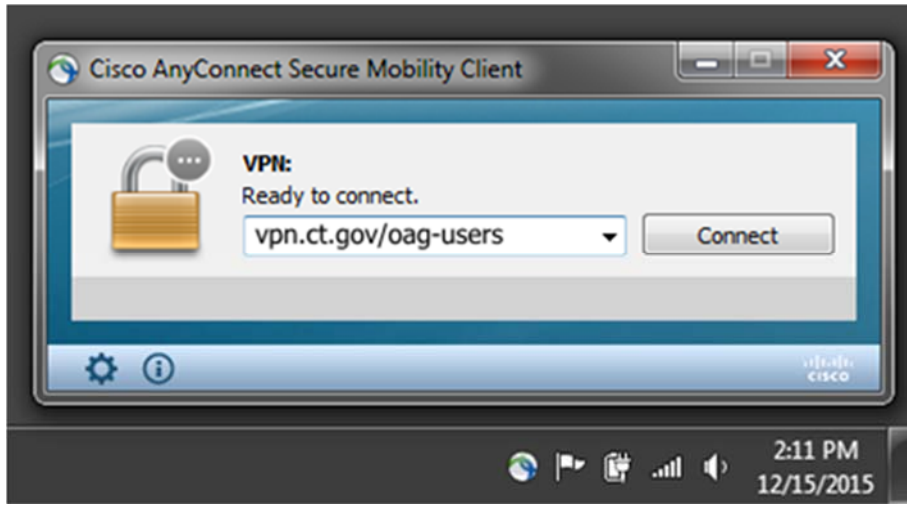
[Microsoft Remote Desktop](#)

C. VPN Connect

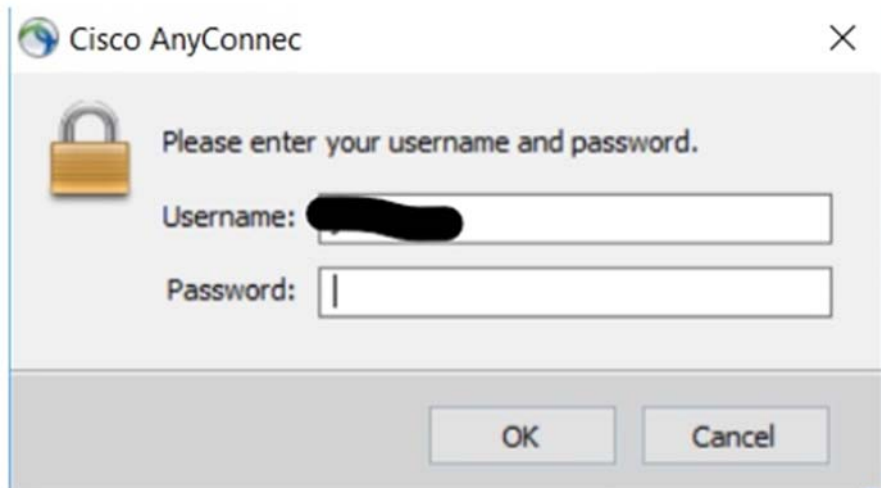
After the installation is complete:

Start the Cisco AnyConnect program and follow the instructions below to login to work.

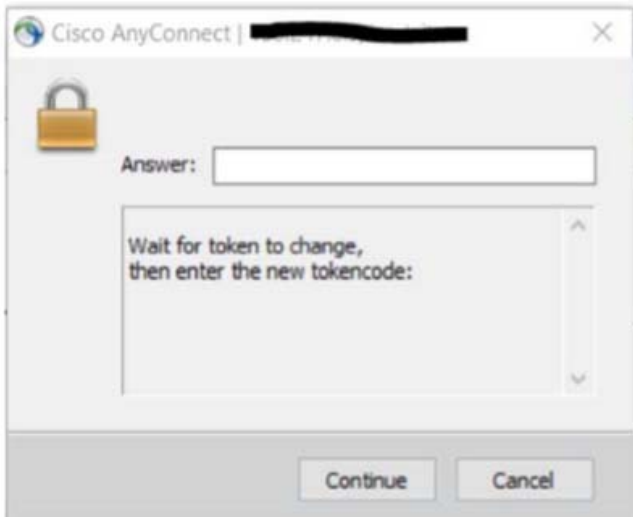
Enter the address `vpn.ct.gov/oag-users` in the text field “Ready to connect” (see below)



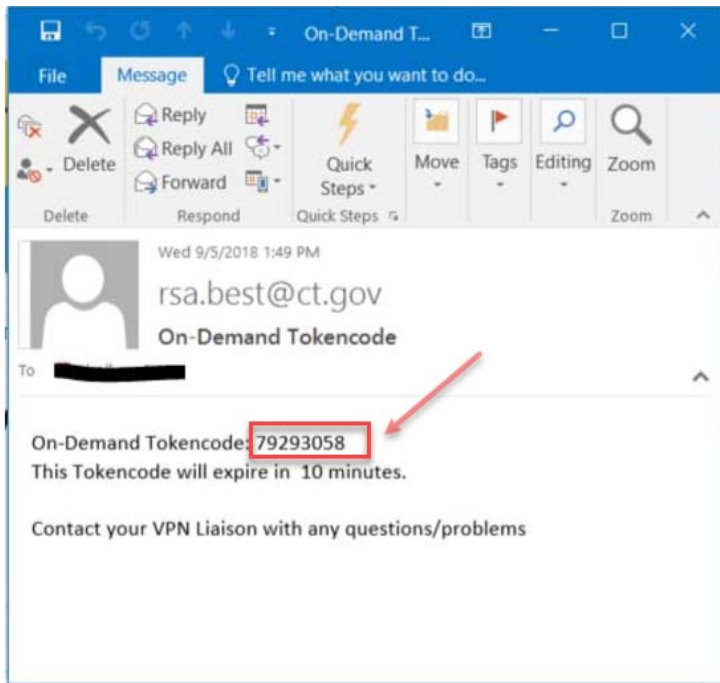
Once you hit connect you will be prompted for your “Username” and “Password”, please enter your User ID (sent to you by IT) and the PIN which you just setup through the RSA Self-Console (From step A-4 above), then click “OK”



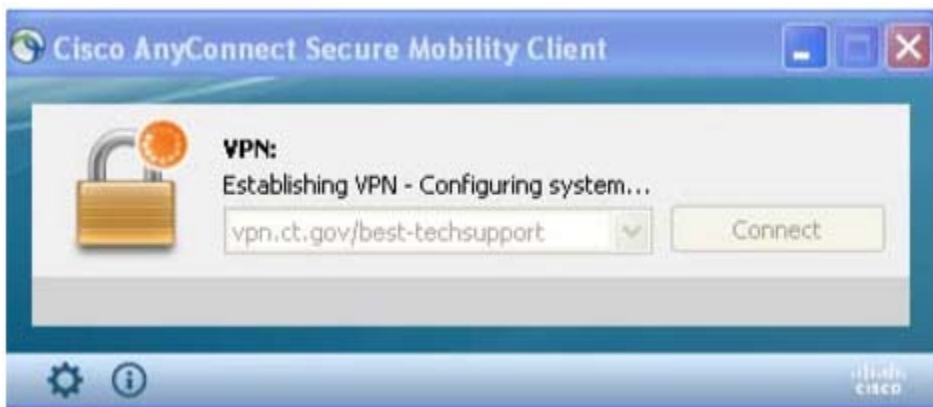
The next pop up will show up (refer to image below) will ask you to “Wait for token to change” which means it is generating a Tokencode for you to enter and being sent to you via email, and once received needs to be entered in the “Answer” Field and press “Continue”.



Email below show the On-Demand Tokencode sent to you by email (personal email used when you setup RSA Self-Console).



Once you enter in the Tokencode you will see the AnyConnect Client make the connection to the VPN



And finally, you will get a warning that you are entering a State Network which may vary from Profile to Profile, just click "OK"



D. Remote Desktop Logon

We will use Windows for this example.

Start » All Programs » Accessories » Remote Desktop Connection. Specify the AG's server: agrds.ct.gov



Click Connect.

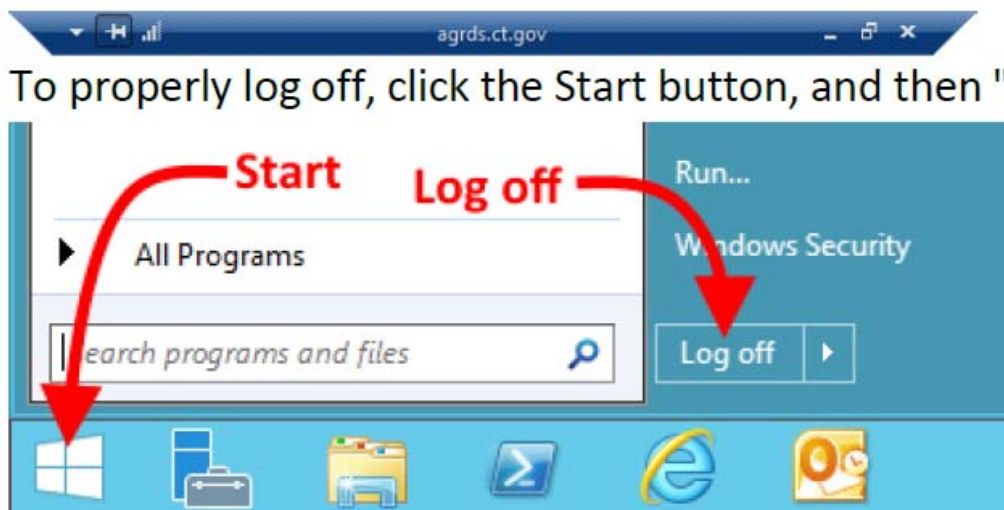
You will be prompted for credentials. Use your regular username and password, but prefix your username with "EXEC\". (For example, john.smith would become EXEC\john.smith)



You are now presented with a desktop similar to the one you see at your workstation. You have access to LawBase, WorkSite, the U drive, L drive, etc.

E. Remote Desktop Logoff

You will see a blue title bar at the top of your screen like the one shown below. If you click the "x" you will be disconnected from your Remote Desktop session but remain logged in. However, after a certain period of time your session will expire and you will be logged off automatically, losing any unsaved work.



To properly log off, click the Start button, and then "Log off."

F. VPN disconnect

Notice that the Cisco AnyConnect icon on the notification area has a "lock" symbol indicating that you're securely connected to the state network. You'll want to disconnect when you are finished with your tasks. Right-click the AnyConnect notification icon, and then select "VPN Disconnect."

