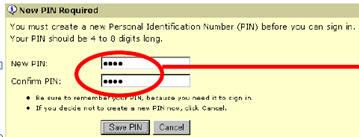
**Remote Access Service ~ what you need to connect to VPN**

* A hard token (ACE SecureID) is required to allow you to connect to

remote access services such as F5 VPN.

* + To request a hard token complete this form:  [http://sc.ge.com/\*requestvpntoken](http://sc.ge.com/*requestvpntoken)
  + Please keep your token in a place you will not forget or lose it, it is needed to connect to VPN for full access to network resources.
* Log in to F5 VPN and create your 4 digit PIN
  + Open your Internet browser and go to <https://remoteoffice.ge.com/>
  + Username = Your SSO Number
  + Password = Type the 6 numbers displayed on your hard token
  + Click Sign In
  + After clicking on “Sign In”, if you receive the message “invalid user name or password, re-enter your SSO Number and wait for the Tokencode to change and enter the new 6 numbers – DO NOT USE THE SAME TOKENCODE TWICE.
  + The next screen will ask you to create a new PIN.
  + Create a PIN using 4-8 numbers (PIN cannot start with a zero)
  + Click on Save PIN.
  + You will see a message after clicking on “Save PIN” stating “Your new PIN has been saved” Be sure to remember your PIN, you will need it each time you sign in.
  + You have successfully set up your PIN!
  + PLEASE WAIT 5 MINUTES BEFORE TRYING TO CONNECT TO THE VPN CLIENT
  + If you are currently in a GE office, you will need to wait until you are OUTSIDE the GE network prior to attempting to connect to VPN.
* Know your other remote access service: **MyApps Anywhere**
  + If you only need to access Outlook, Colab, Folders & Libraries, MyGE, and most GE http web apps (web sites that begin with http:// and end in ge.com/ or select GE https web apps that begin with https:// and end in ge.com/) then MyApps is for you!
  + Sign up for MyApps at <http://ge.com/reg>
  + If you are traveling without your token-you can connect to limited network resources using MyApps Anywhere.
  + For frequently asked questions and information: [http://sl.ge/\*MyApps-FAQ](http://sl.ge/*MyApps-FAQ)

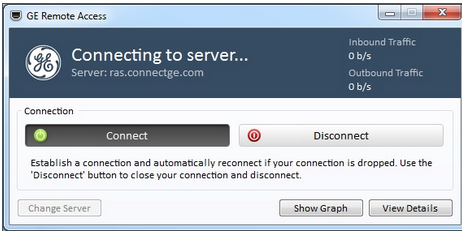
You can find more Remote Access information at <https://ge.service-now.com/ras/>

Can’t connect or create a PIN? Please contact the Helpdesk for assistance at <http://heldesk.ge.com>

**Using F5 VPN**

1. Double click the F5 icon titled **GE Remote Access** on your desktop

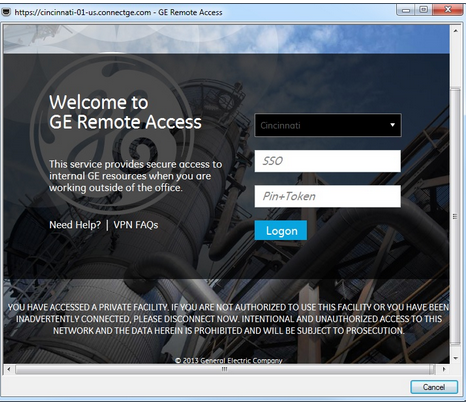
(this program can be found on your start menu)

2. At the GE Remote Access window click **Connect**

**Note** - during first use, the client may auto download & install the latest updates

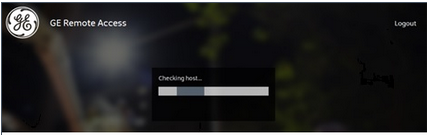
1. At the login screen enter **SSO**, and enter **Passcode** (Pin+Token Code)

* **PIN** is the 4-8 digit password you created when setting up your Remote Access Account
* **Token Code** are the digits displayed on your SecurID token
* **Enter Pin+Token Code with no spaces between them**

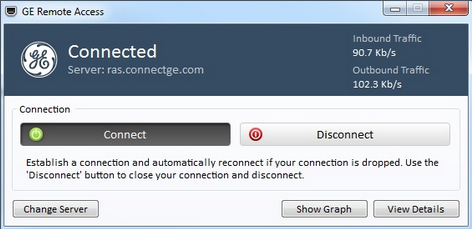


1. Select logon. The client will automatically pre-populate your gateway with your nearest available site.

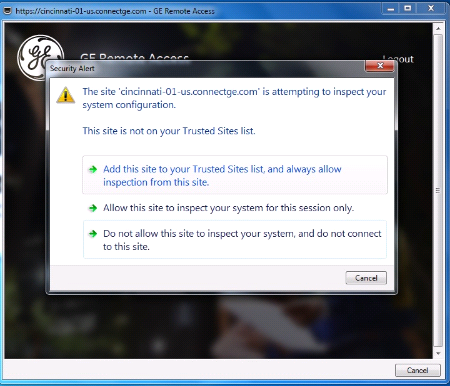
**Note**:  If you are logging via VPN for the first time, enter only the Token Code.   Select Logon and you will be prompted to create a NEW PIN number

5. Click **Logon** to authenticate & initiate the connection process. 

6. Once the host check process has completed, the F5 client will establish the VPN connection and show **Connected**. You are now connected to GE VPN.



*You may receive a warning message; select “Add this site to your Trusted Sites list”.*



## Once the login is successful, the VPN session will be started and the login window will close. You will see the F5 icon in your system tray.



To disconnect from the VPN, you will need to double click on the icon in the tray and click disconnect.

* **ATTENTION:**

**Need access to OLC profiles in Cisco VPN client?** Please submit OLC VPN request via [http://supportcentral.ge.com/\*olcvpnaccess](http://supportcentral.ge.com/*olcvpnaccess) . If you are already have an approved OLC VPN request. You can visit below folder to get OLC VPN instructions and OLC PCF profiles. <http://supportcentral.ge.com/products/sup_products.asp?prod_id=115686>

**Need access to HTS (i.e. UHC or ASP) profiles in Cisco VPN client?** Please visit HTS community site at <http://supportcentral.ge.com/products/sup_products.asp?prod_id=166329>

**Need VPN Support?**

In a GE Office or have VPN access: Please visit the GEHC VPN Support Central site at <http://supportcentral.ge.com/@gehcvpn> for tips, instructions, user guides and helpful information.

If you have access to the Internet, you can find helpful information on the helpdesk portal at <http://helpdesk.ge.com>.

If you are unable to access the Internet, you may call the helpdesk (English language) phone numbers by region:

America’s: 1 855 694 8457 EMEA: +44 203 684-1425 Asia: 1 800 868 4513

# *Self-Service VPN Token Management*

Handle your token administration needs at[**https://OneIDM.ge.com**](https://OneIDM.ge.com)Go to Network/VPN & Personal Security Tools section and SecureID Token / VPN - Corporate and see what you can do!

* Enable/Disable your VPN token
  + Enable Token

By default, an assigned token is enabled unless it has been disabled by an Administrator or a system has disabled it. If your token becomes disabled; use this option to enable.

* + Disable Token

A disabled token can be assigned to you but cannot be used to authenticate (get access to the network). A token becomes disabled if an administrator disables it or after a set number of incorrect PINs or token codes have been entered.

* Clear your current PIN and Set a New Pin
  + Use this option when you would like to create a new PIN. When you use this option, your current PIN will be cleared and you will be required to enter a new 4-8 numeric PIN
* Set your Pin to the Next Token code
  + If you believe your PIN has been compromised; use this option. Your new PIN will be the next code displayed on your token. In addition, you should use this option when you are unable to create a PIN through the normal process [clear PIN / Set New PIN]
* Resynchronize your token
  + Use this option to resync your token. Why? At times, token get out of sync with the system clock - use this option if you are having issues connecting.
* Next Code:  Authenticating when your token is in Next Token Code mode
  + Every once in a while, even after you correctly enter your passcode, you are prompted for the next code displayed on your token. Why? We need to confirm the token is in your possession. When this happens, enter in the next code that displays on your token and then proceed with proceed with the Resynchronize Token operation [above].

**Here are a few key terms you will need to know:**

VPN: **V**irtual **P**rivate **N**etwork. Used to provide a secure remote connection to GE’s network. In order to access VPN, you must have a VPN account with a token assigned to you.

PIN: **P**ersonal **I**dentification **N**umber. The PIN is a secret code created by you that you use to securely logon to GE’s VPN. NEVER share your PIN or record it anywhere on your GE laptop.

Tokencode: The number currently displayed on the token. This number changes every sixty (60) seconds.

Passcode: Combination of PIN number and Tokencode used to connect to VPN.

Remote Office: Remoteoffice.ge.com is a web-based tool that allows users limited access to the GE network when they do not have their GE computer to use the VPN Client, i.e. access to email, Support Central, GE Libraries, etc. We also use this tool to create the PIN for your SecurID token.

VPN Client: The application used to connect to the GE network. GE currently uses the F5 VPN for GE issues laptops. For non-issued GE PCs and identified remote teams, the Cisco VPN Client is used.