

VPN

Frequently Asked Questions (FAQs)

What is a VPN (Virtual Private Network)?

A VPN allows you to access the VITA Network and your applications from anywhere on earth via the internet.

What types of user VPNs does VITA offer?

VITA offers two types of VPN:

- IPsec Dual Factor – You will need A VITA supplied machine, a Key Fob, and your network ID and Password you normally use.
- IPsec Single Factor – You will need a VITA supplied machine and your logon ID and password you normally use.

Which VPN solution will I use?

This will be determined by your agency's security officer and is based on the type of data you access. Generally speaking, you will want to use two-factor access for sensitive data warranting a higher level of protection. Data associated with HIPPA compliance, state contract, and budget data should use dual factor VPN. Single factor VPN may be used to protect such things as site plans, personnel directories, and similar information.

What is a key fob?

A Key Fob is a small device you carry on your key chain or, available as a future capability, software that is installed on your VITA supplied machine. Initially, only the hardware token will be available. In the future, the decision about whether you get a hardware device or the software version will be determined by your agency's security officer.

How does a key fob work?

The key fob is actually a random number generator. When you receive your Key Fob, you will notice a six-digit number in the window. This number will change every 30 seconds. The first time you log in you will be asked to supply a PIN (Personal Identification Number). This number is similar to the PIN you use with your debit or ATM card. You can even use that number if you wish, since when you enter the PIN, it is stored on a server but no one can EVER read it. If you forget the PIN, it must be reset by calling the VCCC. When you log into the VPN you enter your username, but instead of entering your network password, you enter your PIN followed by the six-digit number. The authentication is accomplished via a PIN and the numbers on the token.

Will additional software be installed on my VITA supplied PC to allow me to use the VPN services?

Yes! As part of the initial install process, if you are designated by your agency as a VPN user, the CISCO VPN client will be installed on your machine. This applies whether you need dual factor or single factor VPN.

How do I use the Cisco Client software?

As part of the startup process, you will receive step-by-step instructions for using the VPN solution your agency has chosen. If you have questions, please call or e-mail the VCCC at 1-866-637-8482 or vccc@vita.virginia.gov to help guide you through the process.

Can I access everything from my home PC that I access from work?

It depends on the VPN solution that you are using. If you are using the single factor VPN solution, only very limited services, as identified below, are available:

- http
- https
- e-mail
- file shares
- Active Directory authentication

If you are using the dual factor VPN solution, you can expect the same access you currently enjoy at work. As always, access is based on security policy and roles/ permissions.

Why can I not access everything from my home PC?

There are several reasons, some simple, and some complex. The first is network integrity. We take great pains to insure that no viruses or malware get into our network. We put firewalls and virus protection on VITA owned machines. We do not demand that from you. There are also legal reasons. Much of the data you work with is confidential and should only be saved on VITA-owned assets.

Will having access to a VPN service allow me to work at home sometimes?

That depends on several things:

- The nature of your job
- Your Manager's /Agency's Work At Home policy
- The type of VPN service your agency chooses to implement

Is there an additional cost for the token and/or dual factor VPN service?

Yes. If your agency chooses the dual factor VPN solution, there will be a one-time charge, which includes the cost of the token.

What should I do if I lose my token?

Call or e-mail the VCCC at 1-866-637-8482 or vccc@vita.virginia.gov.

Will there be a charge to replace my token?

Yes, your agency will be charged a replacement fee; they may choose to pass that cost on to you.

Is there a shelf life to the token? If so, will renewal happen automatically or do I need to initiate the process?

Yes. There is a shelf life, which begins when the tokens are ordered from the vendor, in this case, RSA. The exact length of time is variable.

How do I request/order VPN service?

For dual factor IPsec VPN service, you will order service through EVEA.
For single factor access, you will order through the VCCC.



How will I receive my token? How do I activate my token?

Depending on your location, you will receive your token either by FedEx or interoffice mail. Step-by-step instructions are included that explain how to log on and activate your token. If you are having trouble, you can call or e-mail the VCCC at 1-866-637-8482 or vccc@vita.virginia.gov.

Who do I call if I am having problems using my VPN service?

Call or e-mail the VCCC at 1-866-637-8482 or vccc@vita.virginia.gov.

What type of hard tokens are supported under the 2-factor solution?

Initially, only RSA SecureID hard tokens will be supported.

If I already have a RSA token, can I use it with the VITA-provided solution? If so, what is the process?

In theory, yes! It will depend on the age of your token. If it is near its end of life, it will be replaced. The final decision will be made by your agency security officer.

How do I ensure the VPN services/access I have today will exist under the new service?

We will work with your agency and your Information security officer to insure that you have the same capabilities.

VPN FAQ

