VPN Compliance Requirements

When you first establish a VPN connection with UVA Health System you will be prompted to install the ForeScout SecureConnector. The connector will evaluate your machine for compliance. In order to connect to the UVA Health System VPN, you must meet the following requirements:

- Up-to-date security patches
- Up-to-date, approved antivirus software
- Encryption

This document is divided into sections to help you quickly access your specific needs.

Establishing a VPN Connection

In order to connect, you will first need to be approved to access the VPN. If you have not been granted access, please visit the Online Access Request Application. Return to these instructions once you have been granted access.

Install the BIG-IP Edge Client:

- Windows: https://download.hscs.virginia.edu/BIGIPEdgeClient.exe
  - If you need help installing and using the BIG-IP Edge Client please review the documentation here
- MacOS: https://download.hscs.virginia.edu/BIGIPMacEdgeClient.zip
  - If you need help installing and using the BIG-IP Edge Client please review the documentation here
- iOS/Android: These are not subject to NAC due to other access controls.

ForeScout SecureConnector

The SecureConnector application scans your machine and makes sure it is secure enough to join the Health System network.

Normally, the SecureConnector icon appears in your system tray. If it turns red, then your computer has a security problem that should be addressed. To view the details, right click your mouse on SecureConnector icon located on your system tray and then click the “View Compliance Center” from the menu list. The icon looks like this:

Installing for Windows

Determine 64-bit or 32-bit

First, to know which SecureConnector app to download, determine whether you have a 32- or 64-bit Windows Operating system. If you do not know, we will use the System application to check. After opening the application, look for the *System Type* field. It will say either *64-bit Operating System* or *32-bit Operating System*.

For **Windows 7**, right click on the *My Computer* desktop icon and choose *Properties*:

For **Windows 10**, right click on the *Start Menu* and choose *System*

Installing

After determining 64- or 32-bit, it's time to install SecureConnector. Click http://10.6.235.203/sc.jsp to direct your web browser to the correct download page, then use the settings illustrated below.

Select the version of windows you are running, then click download.

If you are using Internet Explorer, there will be a prompt at the bottom of the browser window. Click *Save*. After the download has completed, click on *Run* to launch the Security Compliance Software installation. You will know you were successful if you see the Security Compliance Software icon in your System Tray in the lower right corner of your screen.

Installing for MacOS

Check to see that you have the current macOS version and security updates. This information can be found here:

https://support.apple.com/en-us/HT201222

Now download the Security Compliance Component. Use a web browser to open the following link or navigate to http://10.6.235.203/sc.jsp Select the required information as indicated then click Submit.

Click Download as highlighted.

After the download is complete, navigate to downloads, as indicated by the arrow then click on the file you just downloaded.

After you've opened the downloaded application, you will be presented with the Security Compliance Component installer. Double click on the highlighted area to launch the installer. There will be a security warning pop up; click Open as highlighted.

The software installer will need administrator level access to install the Security Compliance Component. Enter your mac user name and mac administrator password into the highlighted fields then click *OK*.

You will know the installation is complete by seeing the Security Compliance Component in the tray.

 You may now close the installer folder.

Minimum System Security Standards

If you are using a Health System owned device, please call the Help Desk at 434.924.5334 for assistance with compliance.

Operating Systems

To meet compliance standards, personal machines must run one of the following operating systems. At this time, individuals are responsible for any costs associated with operating system upgrades.

Windows 7
Windows 8.1
Windows 10
MacOS 10.12 Sierra
MacOS 10.13 High Sierra
MacOS 10.14 Mojave

Patching

Windows

Follow the instructions to ensure your PC is compliant with *3.1.5 Windows Patch Compliance*.

MacOS

To make sure your Mac has current updates, follow the instructions provided by Apple here.

Antivirus

On personal devices you must run an antivirus program from one of the following vendors listed below. Each vendor name below has a hyperlink to the vendor site for more information. Most offer antivirus versions for Mac and Windows. Some vendors offer free versions of their software, while others require subscriptions that individuals must purchase. The Health System VPN standard requires that the installed antivirus package be actively running and have current virus definitions. For help with specific antivirus packages, please consult the support offered by the antivirus vendor.

[Avast](https://www.avast.com/en-us/index)
[AVG](https://www.avg.com/en-us/homepage)
[BitDefender](https://www.bitdefender.com/)
[eScan](https://www.escanav.com/en/index.asp)
[ESET NOD32](https://www.eset.com/us/home/smart-security-premium/)
[F-Secure](https://www.f-secure.com/en_US/f-secure)
[K7](https://www.k7computing.com/)
[Kaspersky](https://usa.kaspersky.com/)
[McAfee](https://www.mcafee.com/us/index.html)
[Microsoft Security Essentials](https://www.microsoft.com/en-us/download/details.aspx?id=5201)
[Sophos](https://www.sophos.com/en-us.aspx)
[Norton by Symantec](https://us.norton.com/products#pc_mac)
[Trend Micro](https://www.trendmicro.com/en_us/forHome.html)
[Windows Defender](https://www.microsoft.com/en-us/safety/pc-security/windows-defender.aspx)

Encryption

Systems that connect to the Health System must be encrypted so that if they are lost or stolen, any data saved on the device cannot be accessed by unauthorized persons. Unfortunately, only Macs and newer Windows PCs can support no-hassle encryption. It is recommended that you work directly with the Health System IT Help Desk to implement hard drive encryption. The following instructions for BitLocker and Dell Data Protection are provided for your information.

Very Important Note

Before you begin, note that activating hard drive encryption makes your computer's hard drive permanently inaccessible without a password that only you know. The only failsafe is a backup key that you create during the initial encryption process and which you must save to external storage (such as a flash thumb drive) or a network drive (such as the F:) for later use, if necessary. Therefore, it is **very important** that you **do not forget** the primary password you use to access your computer and that you **do not lose** the backup recovery key. If you lose both, and you do not have an unencrypted backup, there is no way to regain access to your hard drive, and all your data will be lost.

MacOS

MacOS provides a built in encryption solution. Please review the following documentation provided by Apple: How to Enable FileVault on MAC

Windows

There are two options available to encrypt your Windows PC: BitLocker and Dell Data Protection. Older PCs or those with Basic or Home editions of Windows should skip down to the instructions for installing Dell Data Protection.

BitLocker

BitLocker is a Microsoft product available for premium versions of Windows on computers that also feature a Trusted Platform Module (TPM). TPM is a chip in your computer that helps make encrypting your hard drive much easier. Most desktop and laptop computers sold since 2010 have a TPM chip, although not all computers that have a TPM chip are set up to use them.

HIT recommends using BitLocker only if your computer has a activated TPM and only if you have one of the following versions of Windows:

Windows 7 Ultimate

- Windows 7 Enterprise
- Windows 8 and 8.1 Pro
- Windows 8 and 8.1 Enterprise
- Windows 10 Pro
- Windows 10 Enterprise
- Windows 10 Education

If you have an edition of Windows not listed above (such as the Home or Basic editions), you must use Dell Data Protection to encrypt your machine.

To find out what edition of Windows your computer is running:

Windows 10

Go to Start , Settings , System , About .

Windows 8 and 8.1

1. Swipe in from the right edge of the screen, tap **Settings**, and then tap **Change PC settings**.
2. (If you're using a mouse, point to the lower-right corner of the screen, move the mouse pointer up, click **Settings**, and then click **Change PC settings**.)

Tap or click **PC** and devices, and then tap or click PC info.

Look under **Windows** for the version and edition of Windows that your PC is running.

Windows 7

1. Click the **Start** button , enter **Computer** in the search box, right-click **Computer**, and then click **Properties**.
2. Look under **Windows edition** for the version and edition of Windows that your PC is running.

These instructions from Stanford University's IT department help explain how to activate BitLocker.

However, when enabling BitLocker, if you receive an error that TPM needs to be activated or that TPM is missing, HIT recommends that you use Dell Data Protection instead of BitLocker.

https://uit.stanford.edu/service/encryption/wholedisk/bitlocker

Dell Data Protection

For machines running Home or Basic editions of Windows 7, 8, 8.1, or 10, and for machines that do not have an active TPM installed, HIT recommends using Dell Data Protection (DDP), a free application provided by the Medical Center. Below are the instructions for installing DDP on your machine.

Help Files

After the DDP application is installed, the following help files may come in handy:

- For help encrypting your PC's hard drive, see C:\Program Files\Dell\Dell Data Protection\Encryption\Help\DellEncrypt.chm
- For all other issues, see http://www.dell.com/DDPESupport

Installing DDP

The Medical Center has created an installation script that should load the correct files necessary to make DDP work. In order to use the script and to install this software on the machine, **you will need:**

- [x] **administrative rights to the PC**
- [x] **an external USB flash drive**
- [x] **VPN connection to download the installation files**

- To begin the DDP install, plug the USB drive into your computer and begin a VPN session. Once the VPN connection is active, press Start on your computer and start typing (or copy and paste):

\\HscInstall\Source$\CliApps\DDPE-Personal Edition

- Press enter.

Your computer will ask you for login credentials to access the files. Use HSCDOM\ before your computing ID as your username (ex., HSCDOM\ABC4AD) and your normal Health System password for the password.

- Highlight all of the files and folders at this location, and copy them to the USB flash drive.
- Open the USB drive in Windows and click the .bat file called "Install DDPE-Personal".

  The installation will begin. Be patient... much of the installation is large.

Note: You may receive a Windows Installer message, if so just click OK.

After installation, please reboot. When you login to the PC with administrative permissions, the Policy Configurator will auto-launch:

- Click Next.

- Select the policy template called "Basic Protection for System Drive Only"
- Click Next.

Note: To launch the above at some later time to change the template, you can find "DellEncrypt.exe" under c:\Program Files\Dell\Dell Data Protection\Encryption\Local console.

- If your PC already requires a login password, you'll simply need to read and acknowledge the Windows password warning.
- If your PC doesn't yet have a password, you'll need to click *Cancel* so you can use Control Panel – Users to create a Windows password, and then return to this Policy Configurator.

(To re-launch, you can find "DellEncrypt.exe"under c:\Program Files\Dell\Dell Data Protection\Encryption\Local console)

This section pertains to securing this Policy Configurator with an "Encryption Administrator Password".

- Create an 8-127 character Encryption Administrator Password and confirm. The password should contain alphabetic, numeric, and special characters.
- **Record and save this password in a safe place.**
- Click Next.

In this section, you create the backup recovery key. Choose a safe, stable place to store the key so that you can recover your data in the event of certain computer failures or if you forget the primary password. **Do not lose this backup key.**

- Click *Browse* to choose a removable storage to back up your encryption keys. The keys are stored in a file named LSARecovery_[*computername*].exe.
    - You can save the backup key to the USB drive you used to download the installer.
- Once you've saved your backup key to a safe place that you will not lose, click Next.

Note: Future policy changes sometimes require that your encryption keys get backed up again. If the network drive or removable storage is available, backing up of your encryption keys is done in the background. However, if the location is not available (such as the original removable storage device not being inserted into the computer), policy changes will not take effect until the encryption keys are manually backed up.

To learn how to manually back up encryption keys, click "? >Help" in the upper right corner of the Local Management Console or click Start > Dell > Encryption Help.

On the Confirm Encryption Settings screen, a list of Encryption Settings display.

- Click Confirm. A progress bar will appear as encryption is configured.

- Click Finish to complete the configuration.

A reboot is required once the computer is configured for encryption. Click Reboot Now or you can postpone the reboot.

Once the computer is rebooted, open the Local Management Console from the Start menu to see the status of encryption.

The encryption process may take many hours (even 24+), depending on how much data is on the computer. The good news is you can use your computer while this is happening. When it is finished, the computer will need to be rebooted once more to finalize the process. Once encryption has been completed and the final reboot has been performed the status should show “In Compliance.”

For the latest information on UVA Health System VPN compliance, please call the Helpdesk at 434-924-5334 or see our website at http://HIT.Healthsystem.virginia.edu