

eToken and Remote Access

I: Requirements for Remote Access Using eToken

- The desired applications (e.g. FIS, ROSI) must be loaded and functioning correctly on the University desktop and the necessary user names and passwords must be up-to-date.
- The university desktop must be already configured and authorized to accept remote access from a user with your windows login. (if you don't already have this, see Section IV)
- The remote device is running on a Windows operating system. Therefore it must be a PC or a Mac running Windows.
- SafeNet Authentication Client (SAC) software is installed on the remote device. (see Section II)
- **The eToken is plugged in to the remote device.**

II. Installing the SafeNet Authentication Client on the Remote Device

- To download the correct version of the SafeNet Authentication Client (SAC) software go to <https://utmed.sharefile.com/download.aspx?id=80aa6e0db1f6408a>
- Select either the 32 bit version or the 64 bit version of the SafeNet Authentication Client (SAC) for download. This choice will depend on which version (system type) of the Windows operating system the remote device is running. **DO NOT DOWNLOAD BOTH.**

To determine what version of Windows (the system type) your remote device is running, follow these instructions:

For devices running Windows Vista or Windows 7

- Find the System Type by clicking the Start button, right-clicking Computer, and then clicking Properties.
- Under System, you can view the system type.

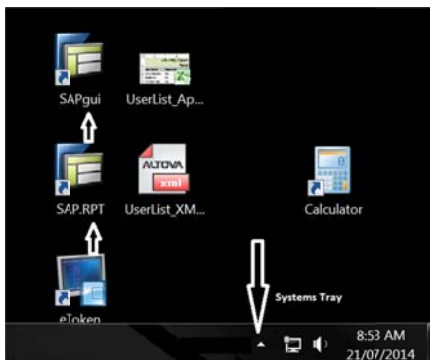
For devices running Windows XP

- Click Start.
- Right-click My Computer, and then click Properties.
 - Under System, if you don't see "x64 Edition" listed, then you're running the 32-bit version of Windows XP. This is the most likely configuration.
 - If "x64 Edition" is listed under System, you're running the 64-bit version of Windows XP.

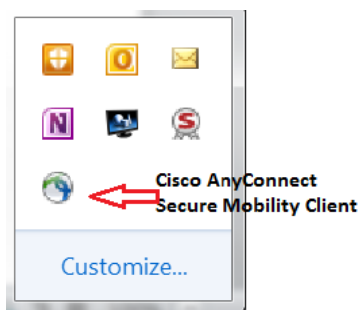
- Make a note of where (to what folder) you have downloaded the file.
- Find the file again and double-click it to run the installation wizard. Follow the instructions in the wizard.

III. Using eToken on the Remote Device

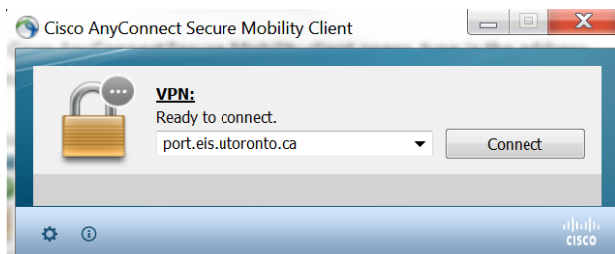
- Plug the eToken in to the remote device (this assumes the SafeNet Authentication Client is installed). **Do not try and login to the eToken from here.**
- If asked about installing a certificate from a certification authority, select Yes.
- Using the Remote Desktop program as you normally would with this remote device, remote in to your University desktop.
- When you see your University desktop, open the systems tray on the University desktop, click on the Cisco AnyConnect Secure Mobility Client and click Connect.



on the University desktop



on the University desktop



on the University desktop

- Once you have established the Virtual Private Network (VPN), use the icons on your University desktop to access the systems with which you want to work.

This is what is happening: The Remote Desktop program on the remote device, working with the SafeNet Authentication Client (SAC) on the remote device, is forwarding the security certificate on the eToken (plugged in to the remote device) to the Cisco AnyConnect Secure Mobility Client on the University desktop.

IV. If You don't Already Have Remote Access to your University Desktop

Getting Set-up and Authorized for Remote Access

For security reasons, users must be authorized to remote in to a University desktop, prior to any attempt to do so with an eToken. This authorization is managed by the Discovery Commons. The university computer must be configured to accept remote access and this configuration is also managed by the Discovery Commons.

To have your University computer set-up to allow for remote access

- Go to <http://dc.med.utoronto.ca/content/documents>
- Download the **Request for Remote Desktop Access Form**
- Fill out the form and get it signed
- Scan the form and attach it to an email to discovery.common@utoronto.ca
Subject = Request for Remote Access

The Discovery Commons will send a technician to configure your University desktop and make the necessary authorizations. Then you may proceed with installing the SafeNet client on the remote device (Section II) and using eToken to remote in (Section III).