

## COTC Remote Access – VPN

1. Open your internet browser and enter in the following address: <https://vpn1.cotc.edu:444/cotc>. Also, you can find a link to the service on the ITS website listed as Remote Access –VPN. Additionally, it is recommended that you save the link in your Favorites/Bookmarks.
2. A Security Alert may come up stating about exchanging information with others. Select **OK** to continue.



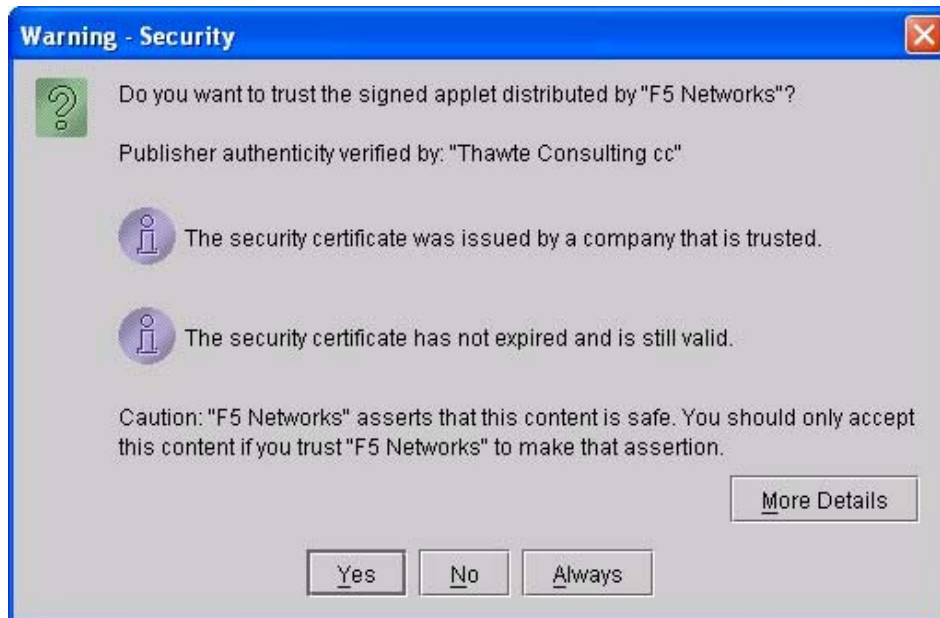
3. A second Security Alert will display asking to accept the certificate from F5 Networks. Select **Yes** to continue.



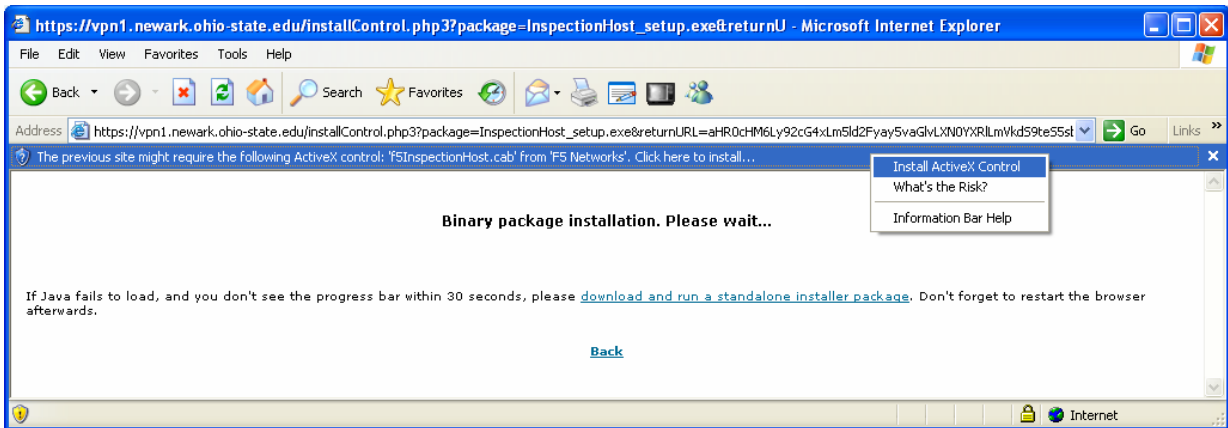
4. A Warning – Security box may pop up asking do you accept the security certificate provided by “vpn1.newark.ohio-state.edu.” Select **Yes** to continue.



5. A warning may display asking to trust the signed applet from F5 Networks. Select **Yes** to continue.



- An ActiveX Control box may pop-up at the top of the page asking if you want to install “f5InspectionHost.cab” from “F5 Networks.” Click the box and select **Install ActiveX Control**.



- An Internet Explorer – Security Warning may come up asking “Do you want to install this software?” Select **Install** to continue.



8. Web controls will automatically be installed, followed by a check for a virus scanner. Once the check is done, it will then scan the active processes for viruses. Once the scan is complete, a login page will display asking for a username and password. The account will be the same as the network login for an office computer. Click **Logon** after entering the credentials.

9. After logging in, an attention page may display stating that the browser is configured to block pop-ups. Follow the directions given and use the address from step 1 to add to the exceptions list. Once the exception is added to the list, the information will not be requested for future sessions.

**ATTENTION**

Your browser is configured to block pop-ups. This interferes with the FirePass controller's ability to launch its browser cache cleanup control pop-up window.

You should add the FirePass controller web site to your list of sites allowing pop-ups.

For Internet Explorer users on Windows XP Service Pack 2, you can manually add the FirePass controller's web site to your list of sites allowing pop-ups. To do this:

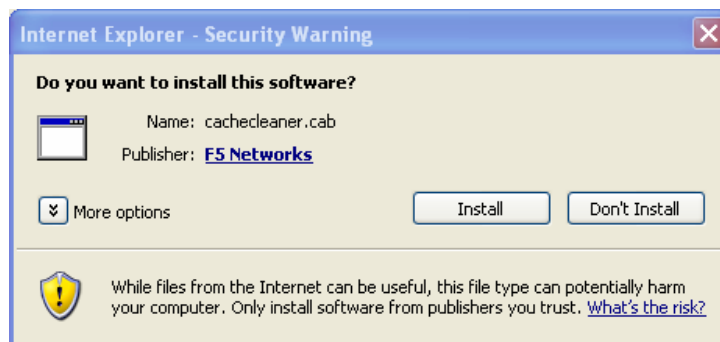
- Navigate to Tools->Internet Options->Privacy.
- Click the Settings button under the Pop-up Blocker section.
- Type the name of the FirePass controller's web site and click the Add button.
- After adding the site to the list, click Close and then Ok to apply the new settings.

For other browser and third-party pop-up blockers, please refer to their documentation on how to enable pop-ups for particular sites.

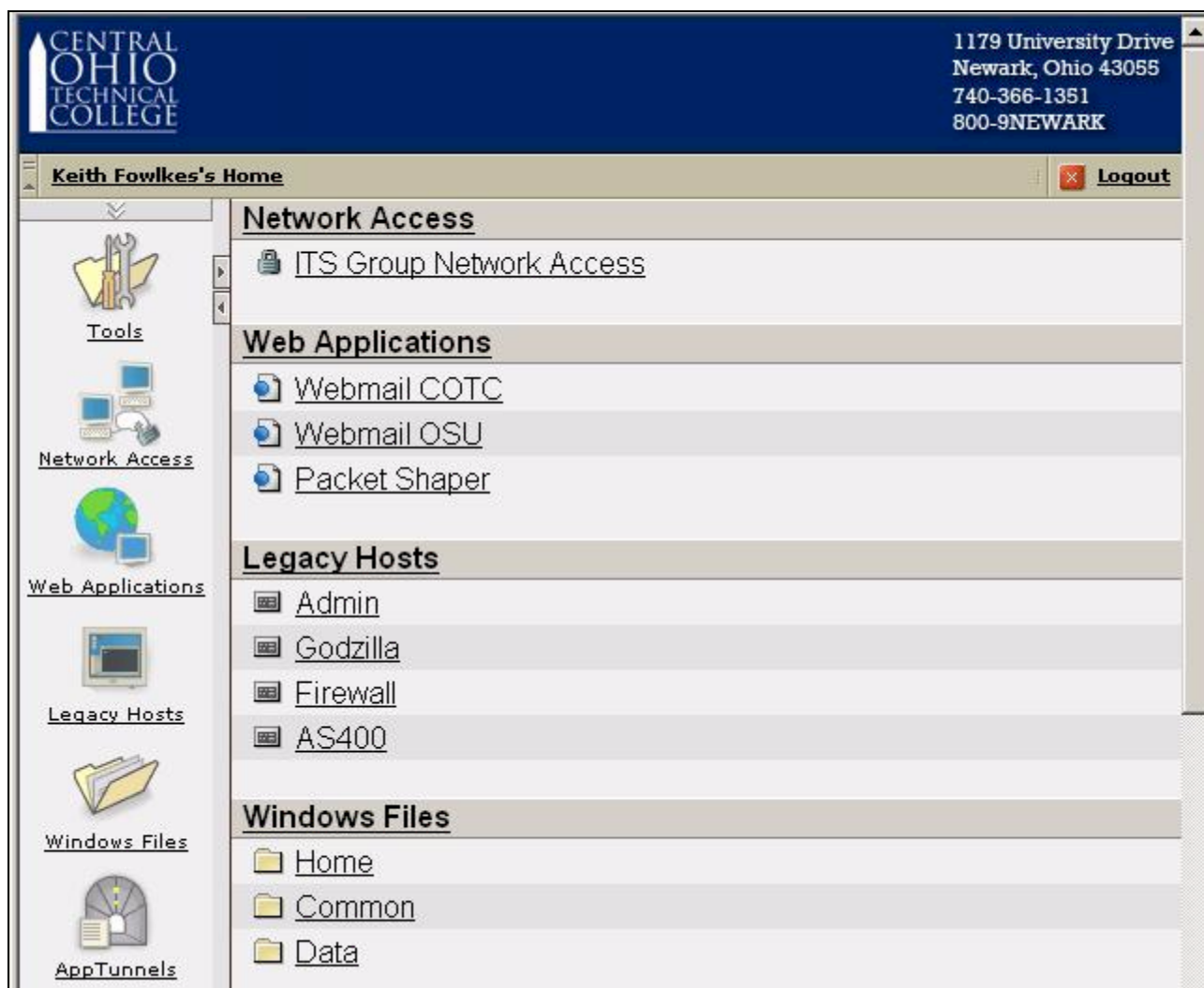
[Then click here, to restart pop-up window >>](#)

10. Click the link, ***Then click here, to restart pop-up window***, to restart the browser window.

11. If prompted to install cachecleaner.cab, select **Install**.



12. The browser should open the portal to Remote Access – VPN displaying options for access to Web mail and network drives. Please note the name of the link under Network Access will vary depending on your work area. The other category lists may vary in content links too.



13. Select **Logout** in the top right-hand corner to exit Remote Access – VPN.

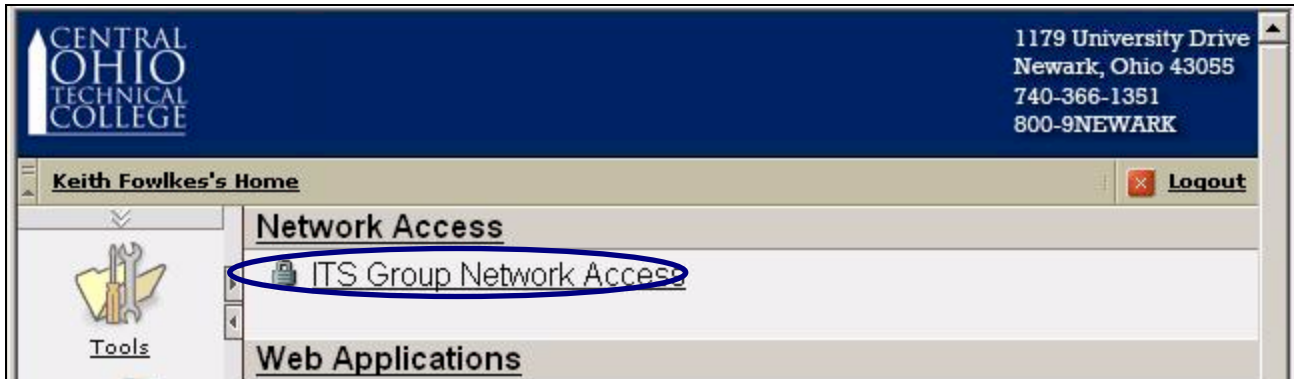


## Methods to access network drives via Remote Access - VPN

There are two ways to access network drives in Remote Access – VPN. One is to map the drives to the local computer using Network Access. The other is to open the network drives within the Remote Access – VPN web portal using Windows Files. If the Internet connection is slower (i.e Dial-up), the preferred method would be Windows Files.

### A. Network Access

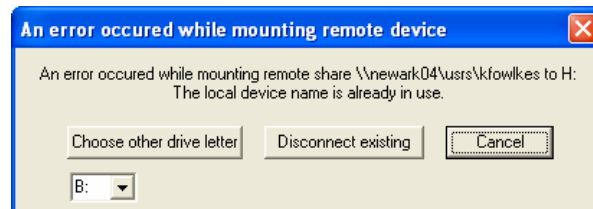
1. After logging into Remote Access – VPN, select the link under Network Access.



2. If prompted to install urxshost.cab, select **Install**.
3. After the install, a small window will pop up and will display the status of the connecting of network drives. A security alert will then pop up asking to accept the certificate, select **Yes**.

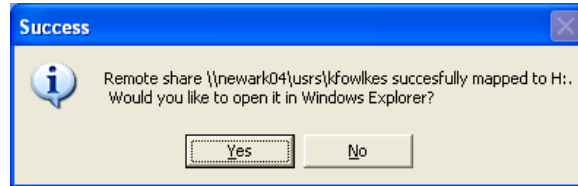


4. If you have a drive designated on your computer as one of the letters used by OSUN – H, K, or L – you will get a box asking to both disconnect your drive and replace it with the network drive from OSUN or designate an alternative letter for the network drive from OSUN.



Select **Choose other drive letter**. You will need to remember the letter you specified to know the proper OSUN network drive is located.

5. If you had to select an alternative letter you will get a Success box giving you the option to open the new network drive now. Select **No** to continue.



6. Once the network drives are connected, a yellow status box will appear at the bottom of the window. Close the status box.
7. Minimize all browser windows. **DO NOT CLOSE THE BROWSER WINDOWS!** Closing them may abruptly close access to the network files.
8. Open My Computer to access the network drives.

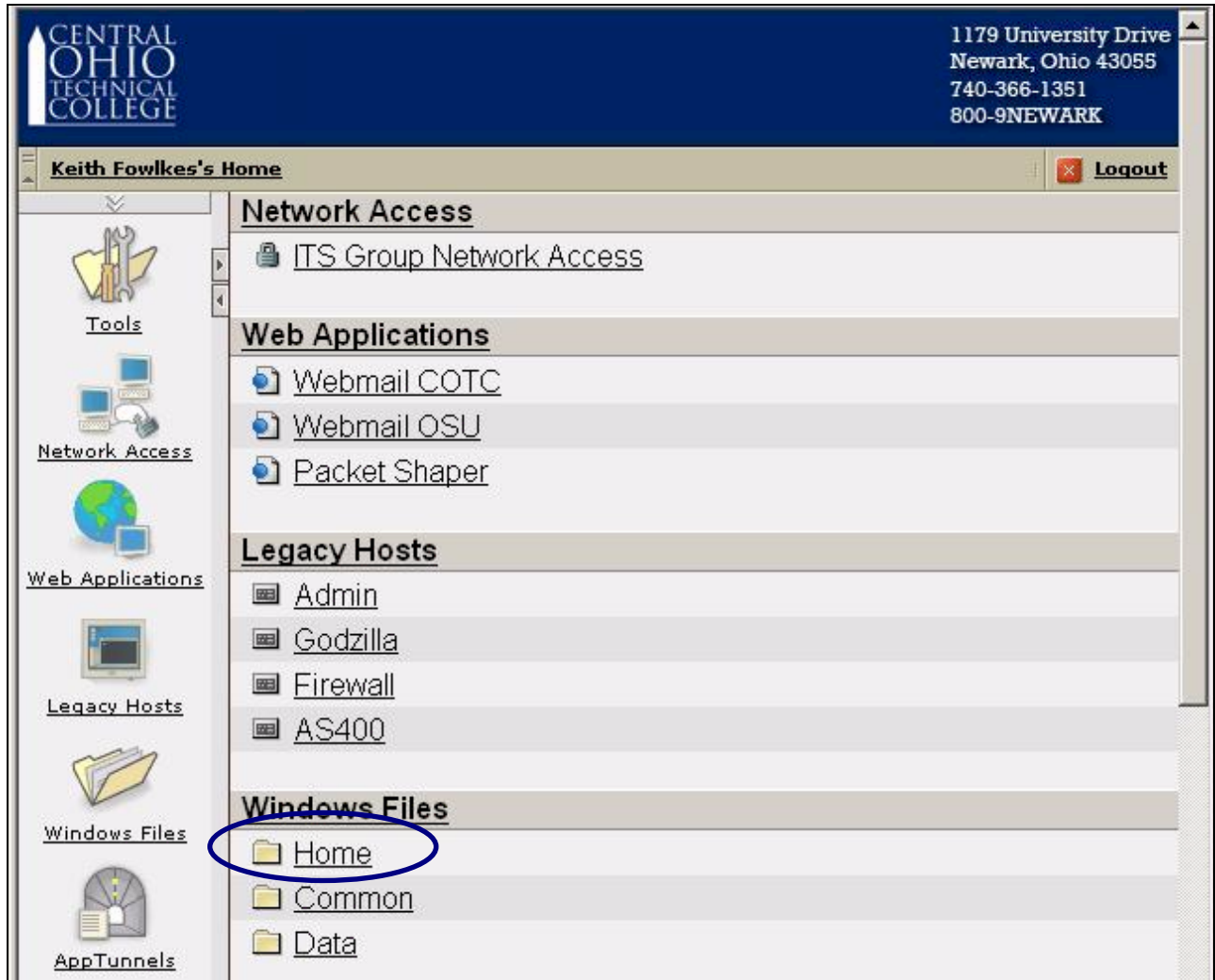


9. You will now see the network drives listed as you would at work.

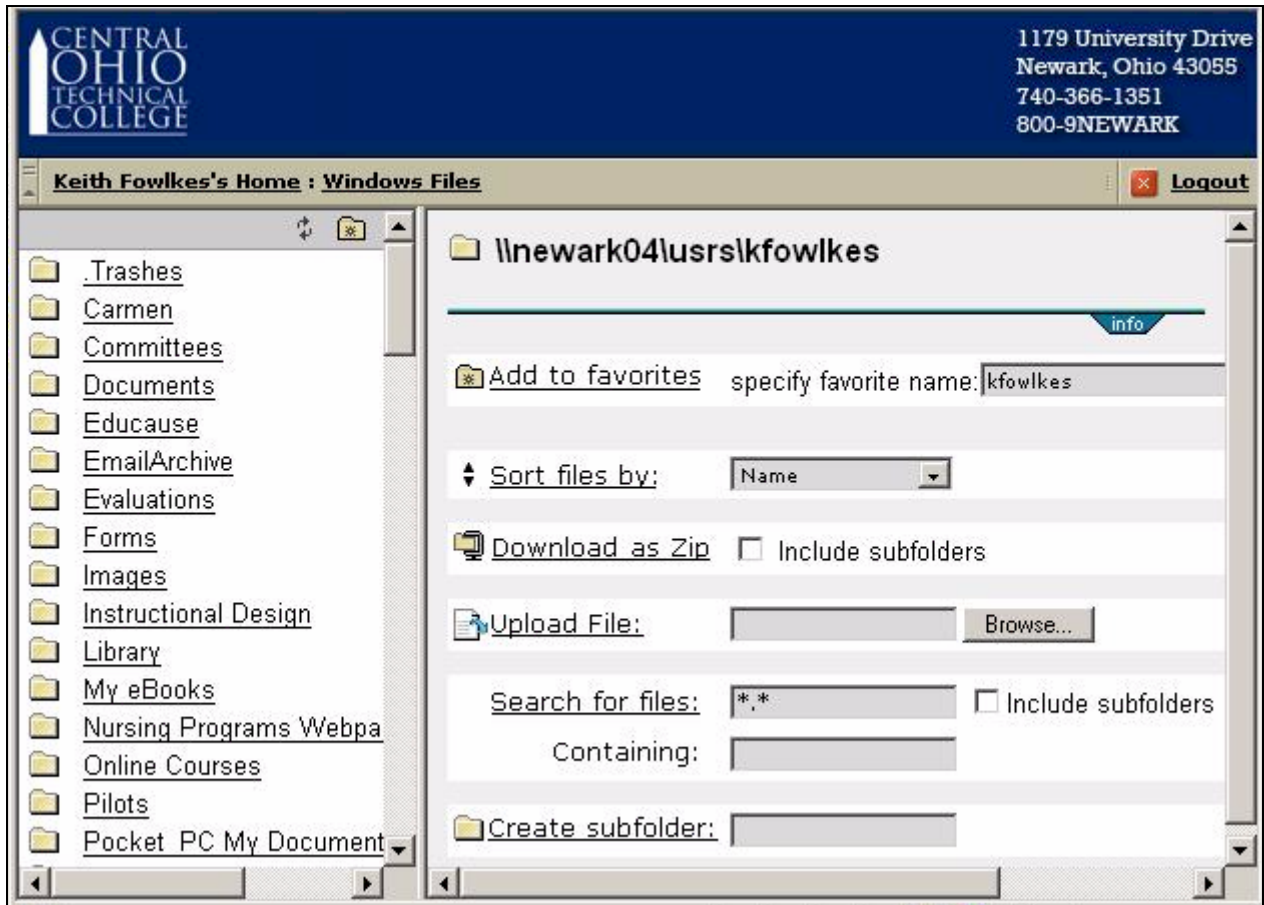
10. When done, open the browser window and select ***Logout*** to exit Remote Access – VPN.

## B. Windows Files

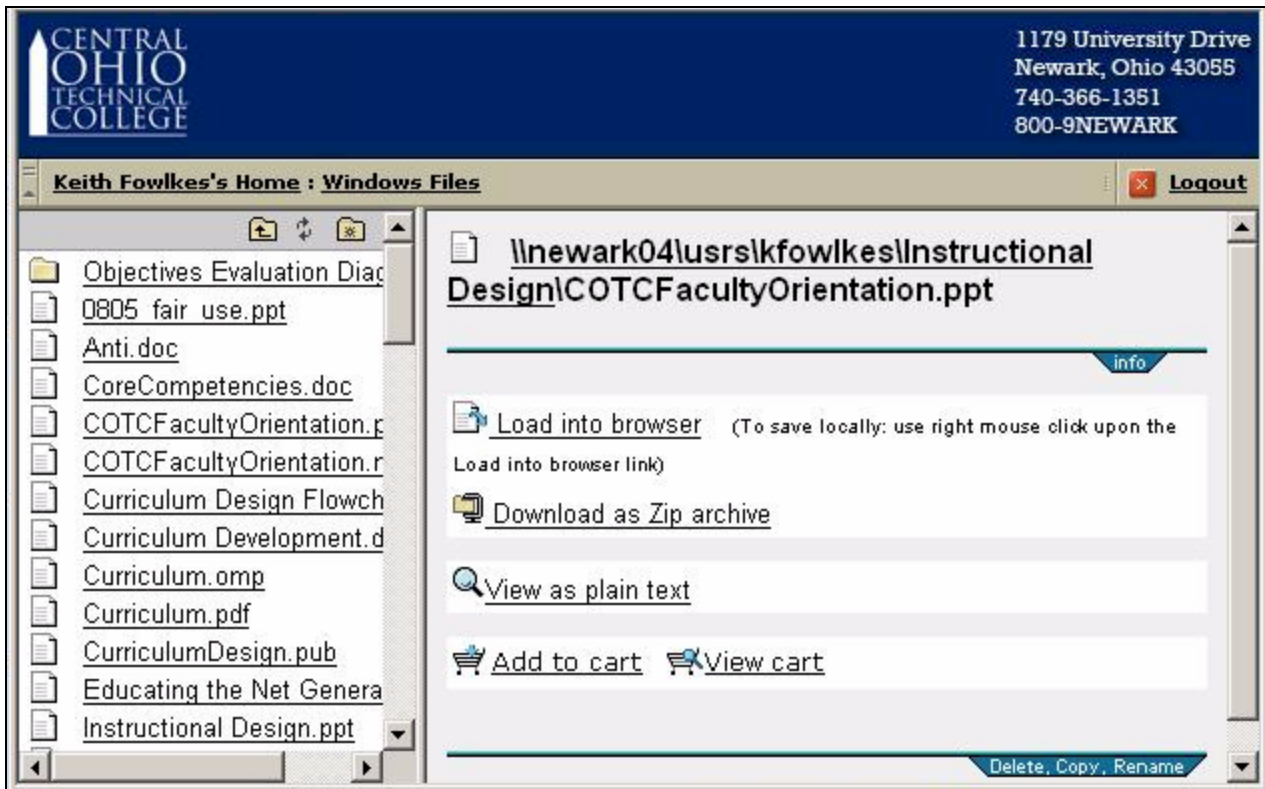
1. After logging into Remote Access – VPN, select the network drive to access under Windows Files. Home is equivalent to the H: on your office computer meant for personal network files, Common is equivalent to the K: on your office computer meant for common network space which all faculty/staff have access to, and Data is equivalent to the L: on your office computer meant for files shared within our department. (see below image)



2. Once a drive link is selected, a two-pane window will open. The left pane displaying the contents of the drive. The right pane displays several options including uploading/downloading files and creating new folders.



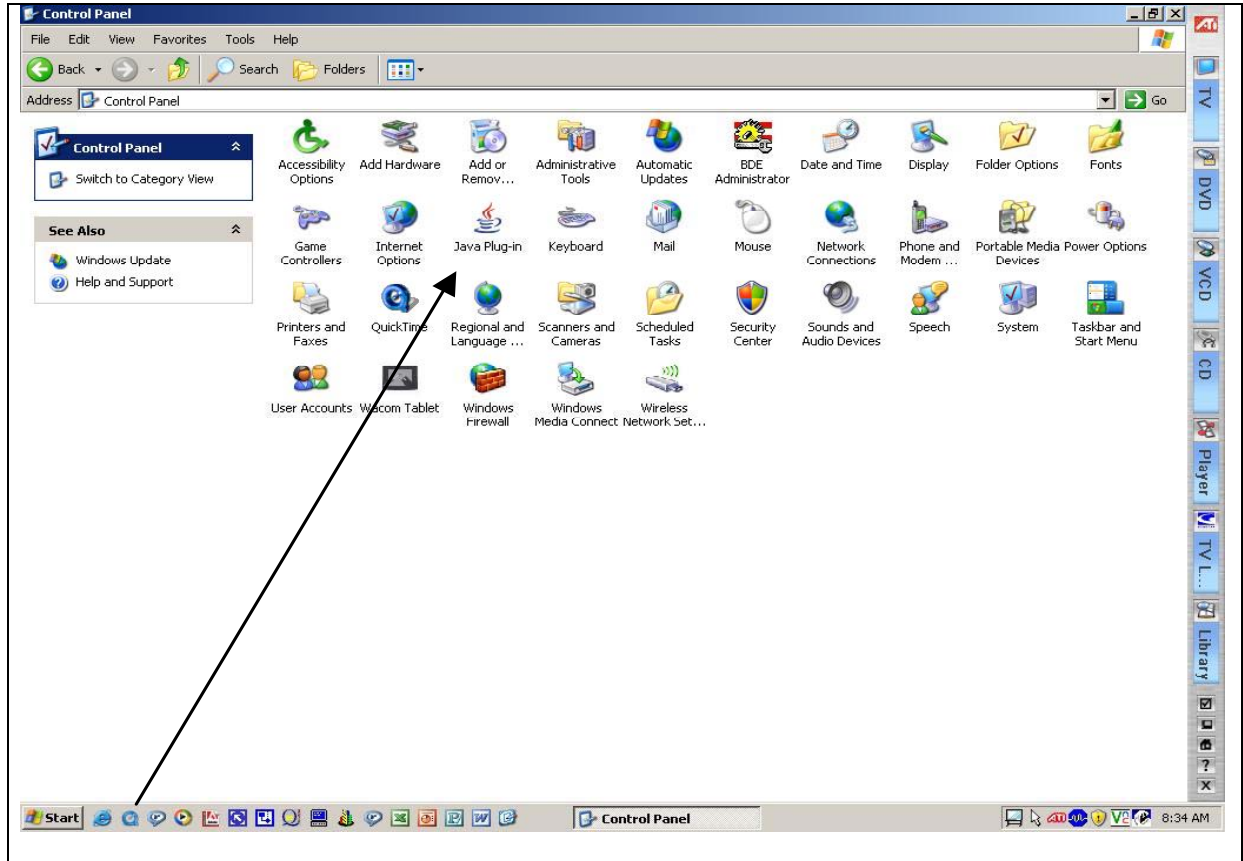
3. To open a file, click the file name. A new pane will display on the right, giving several options including loading file in browser and saving to local computer. Left-click on the “Load into browser” link to open the file. To save the file, right-click the “Load into browser” link and select “Save Target As”.



4. To return to the main page, select *Username's home* in the top left-hand corner where *username* is your username.
5. To logout, select **Logout** in the top right-hand corner.

## Accessing Admin (POISE) from Firepass (COTC only)

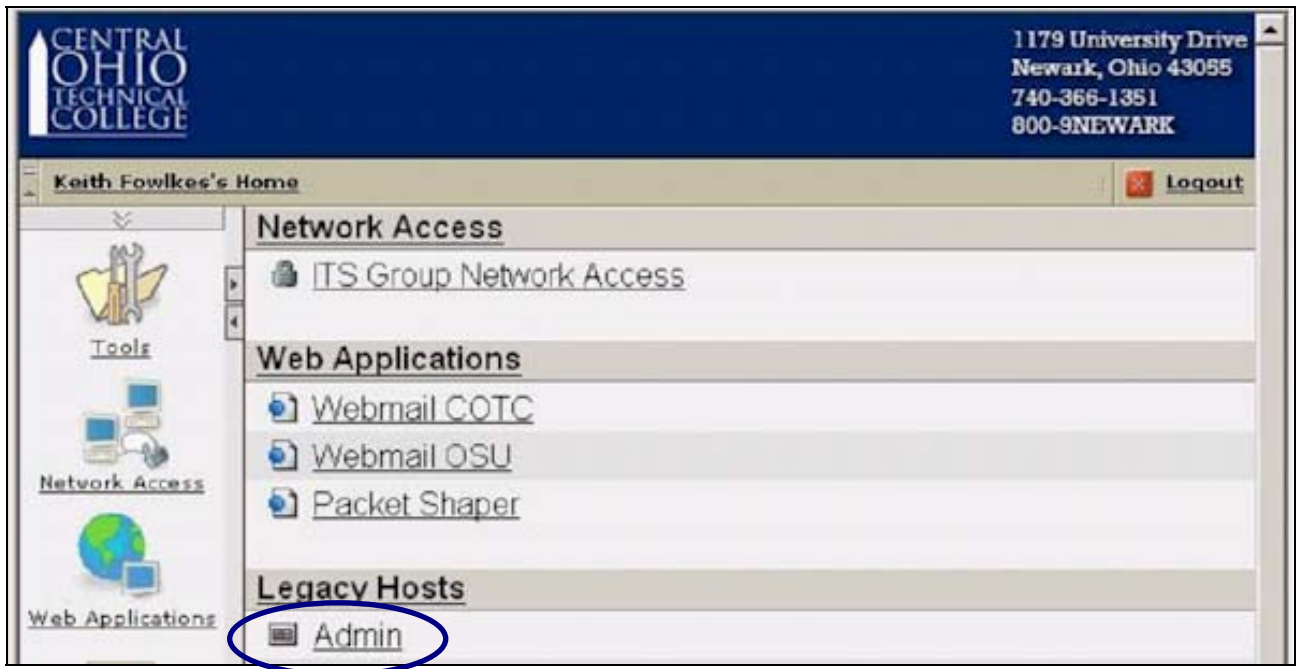
Note: before accessing Admin, make sure that Java is installed on your computer. To verify if java is loaded, open My Computer and open link to Control Panels. Look thru list of control panels. If one is listed with the name of “Java” or “Java Plug-in”, no install is needed.



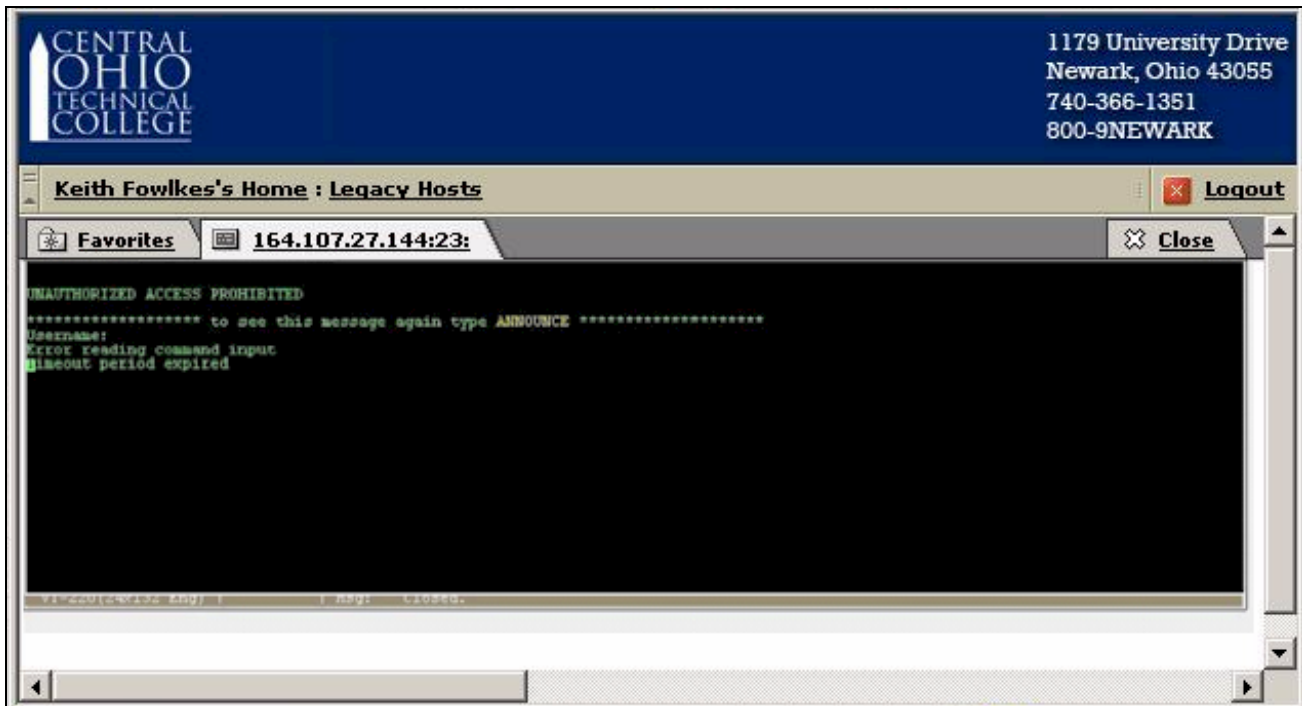
If no java control panel exists, open a web browser and go to <http://java.sun.com>. Select the link on the top right-hand corner “Download Java Software for Your Computer” Follow all subsequent links to download and install the software.



1. Select Admin link under Legacy Hosts.



2. A new window will open and load session to admin



3. Select the Close button in the top right corner to close Admin session.