



Installation and Troubleshooting
Guide for SSL-VPN
CONNECTIONS Access

Version 1
Revised 11/29/2007

Table of Contents

Java Installation:	4
Browser Configuration:	4
Citrix Client Installation:	8
Attempting to Access Connections:	10
Troubleshooting/Additional Configuration:	15
Temporary Internet Files and Cookies Issue:	15
SSL-VPN Access for HSEN ID:	17
Pop-up Blocking:	17
Windows Issues:	19
Proxy Server Issues:	19
Address Resolution Issues:	21
Software Firewall Issues	23
Adding Shortcuts to Connections:	23
Further Assistance:	24



Preface:

SSL-VPN is used for computers that have high-speed Internet access and that are not connected to the New York State network through other means. SSL-VPN allows limited access to the New York State computer network to enable use of the CONNECTIONS application. SSL-VPN stands for “**Secure Sockets Layer-Virtual Private Network.**” The intention of the guide is to be useable by any person attempting to install SSL-VPN to access CONNECTIONS. The guide is intended for users who have a medium level of technical expertise, but should be useable as a “paint by numbers” walkthrough even for those readers who are not as familiar with computers.

*These instructions assume that a PC with Windows 2000 or XP is being used with the Internet Explorer web browser.

If at any point a message is displayed indicating “**You do not have permission to log in. Please contact your administrator,**” please refer to the Temporary Internet Files/Cookies and SSL-VPN Access for HSEN ID sections in the Troubleshooting/Configuration section appearing later in this document.

Java Installation

The first step in setting up your SSL-VPN connection is to ensure that the latest Java software is installed on your PC. Java is a software platform that allows certain types of programs to run. Java may be obtained by accessing the following website: <http://java.sun.com>. Follow the links to obtain the latest Java client. If presented with several options, the latest JRE (Java runtime environment) for the appropriate system platform should be downloaded and installed. In order to properly install Java an administrator account for the PC is usually required.

Browser Configuration

After installing Java, open a web browser and input the following address: <https://rc1.oft.state.ny.us/ocfs>. The following screen should display:

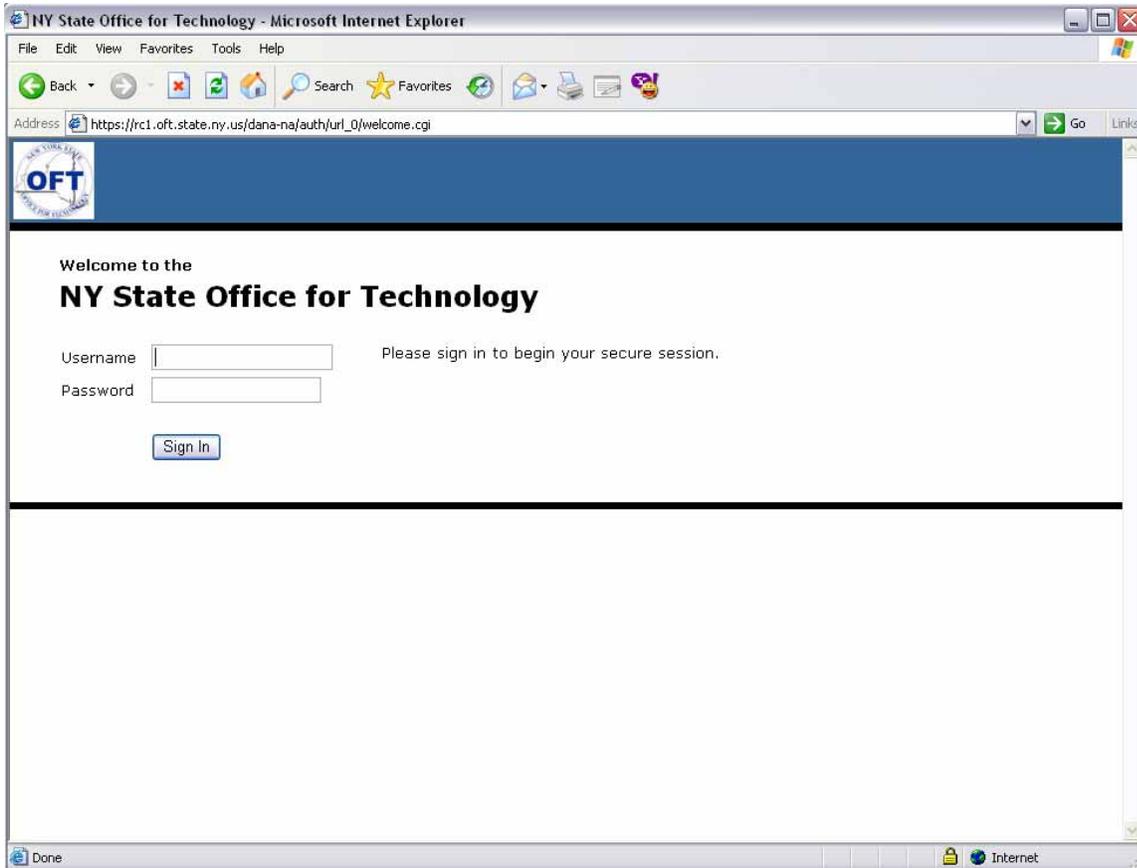


Figure 1: The SSL-VPN Login Screen

If this screen does not appear, the following screen, or one similar to it may display:

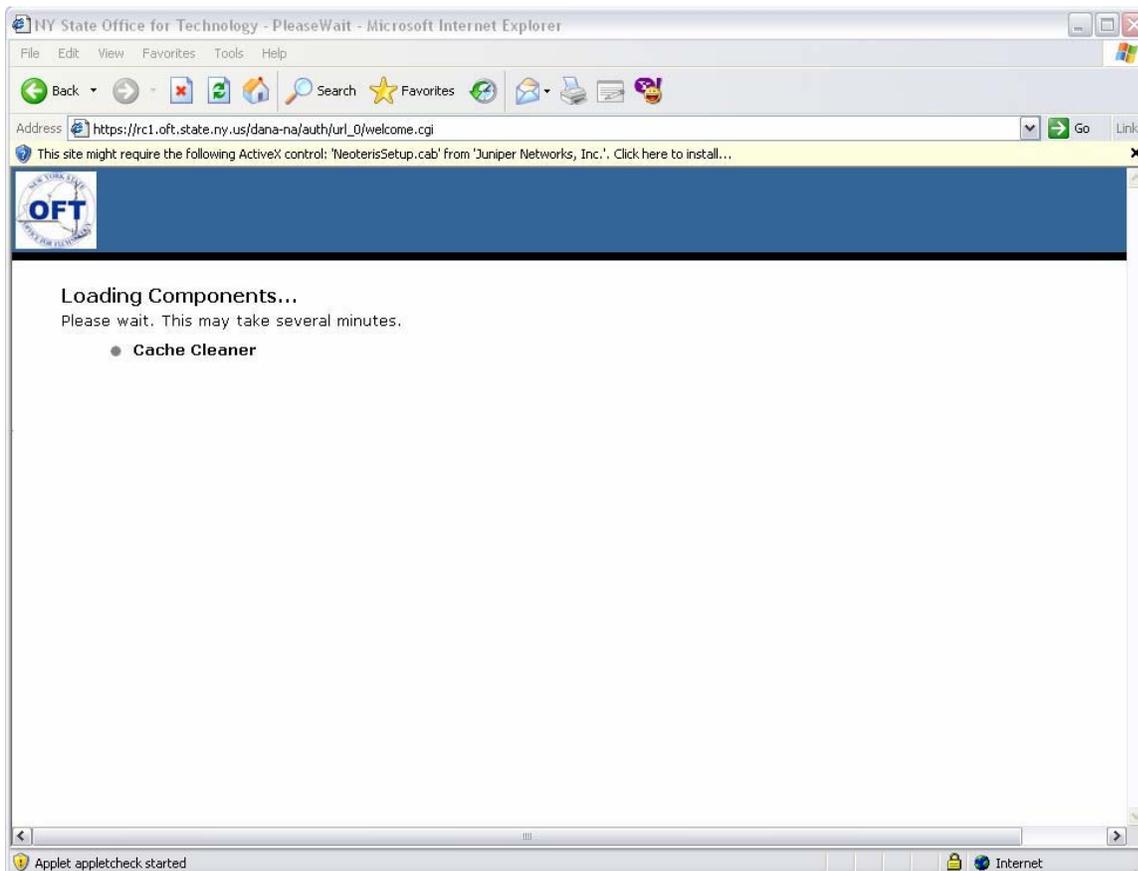


Figure 2: ActiveX Control Prompt

The message at the top of the browser pane is indicating that the ActiveX control, an internet browser based piece of code, that launches the Cache Cleaner, a component of SSL-VPN that clears temporary files in your browser to maintain security, was prevented from automatically running. This is due to restrictions established by the security settings in the browsing software.

The following permission dialog may also appear

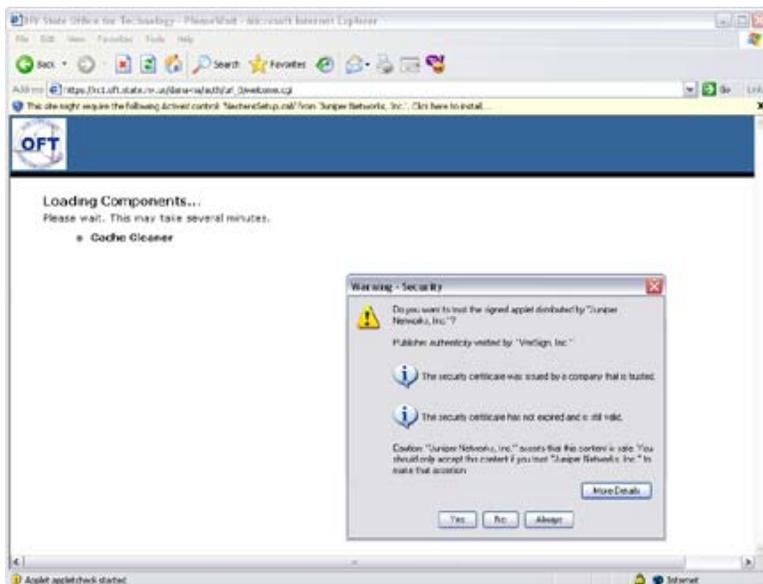


Figure 3: Cache Cleaner Permission Prompt

Click on the *Always* button to allow your browser to install the Juniper Networks Cache Cleaner, a required component for SSL-VPN access.

The gray circle in front of the words *Cache Cleaner* shown above may also display as a red circle. Additionally, an error message may display stating “You do not have permission to login. Please contact your administrator” **without** displaying the Username and Password boxes (if these boxes are present and you see this error message, the problem is possibly related to the HSEN UserID and will be discussed later). This may happen due to an outdated version of Java being installed (although completing the step regarding Java installation would rule this out) or because Java is not being allowed to run properly as a result of restrictive browser security settings.

In Internet Explorer, the easiest way to set up the browser to allow Java and ActiveX for SSL-VPN access is by taking the following steps:

From within Internet Explorer, go to *Tools -> Internet Options -> Security*. The following screen should display:

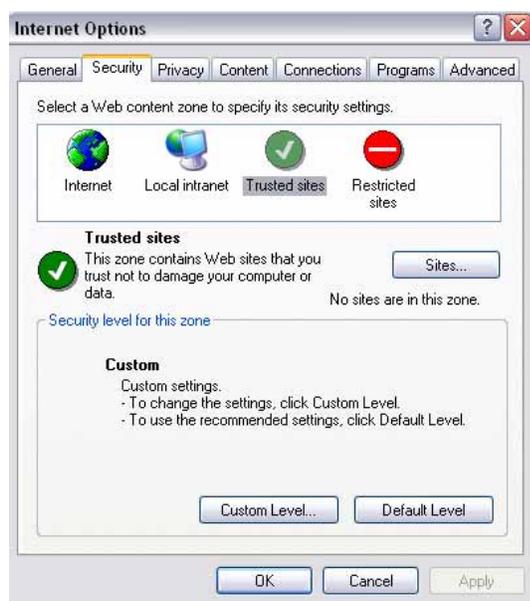


Figure 4: The Security Tab

First, click on the green circle with the white checkmark in it above the words *Trusted sites*. Then click on the *Sites* button, and type https://*.state.ny.us into the box where it says *Add this Web site to the zone*. Click the *Add* button after this is accomplished, and the screen should now look like the following:



Figure 5: The Trusted Sites Window

Click the *OK* button (which will close the above window), and then click on the *Custom Level* button on the next screen. The following screen will display:

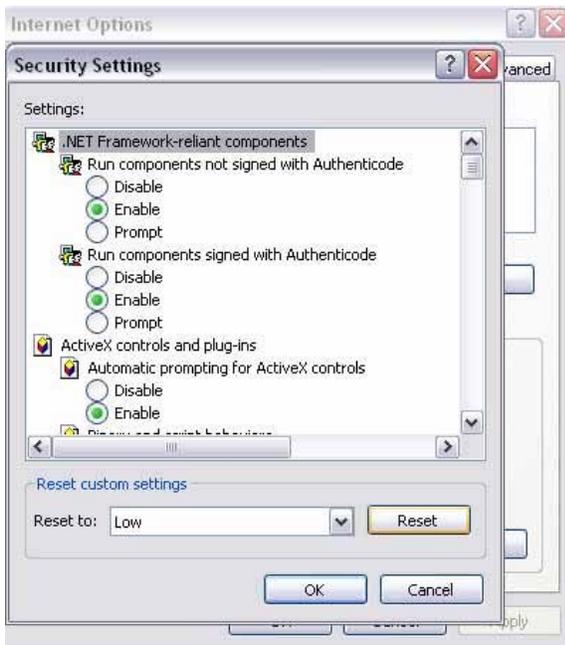


Figure 6: The Security Settings Window

Ensure that the *Low* option is selected in the *Reset to* drop down list, and then press the *Reset* button. A confirmation dialog will now appear. Press *Yes* on this confirmation screen (which will close the confirmation dialog) and then the *OK* button again on the Security Settings screen pictured above.

The browser should now permit Java and ActiveX for all websites belonging to the secure *state.ny.us* domain, including the Connections SSL-VPN access site.

Close out all open browser windows, then re-open the browser, and input the <https://rc1.ofc.state.ny.us/ocfs> address and the Username and Password entry boxes should display.

Citrix Client Installation

The Citrix Presentation Agent (PN Agent) must be downloaded and installed in order to reach the Connections application. This can be downloaded from within the SSL-VPN interface, after successfully logging in to <https://rc1.oft.state.ny.us/ocfs>. After a valid HSEN login and password which has been granted permission to access SSL-VPN has been entered, the following screen appears:

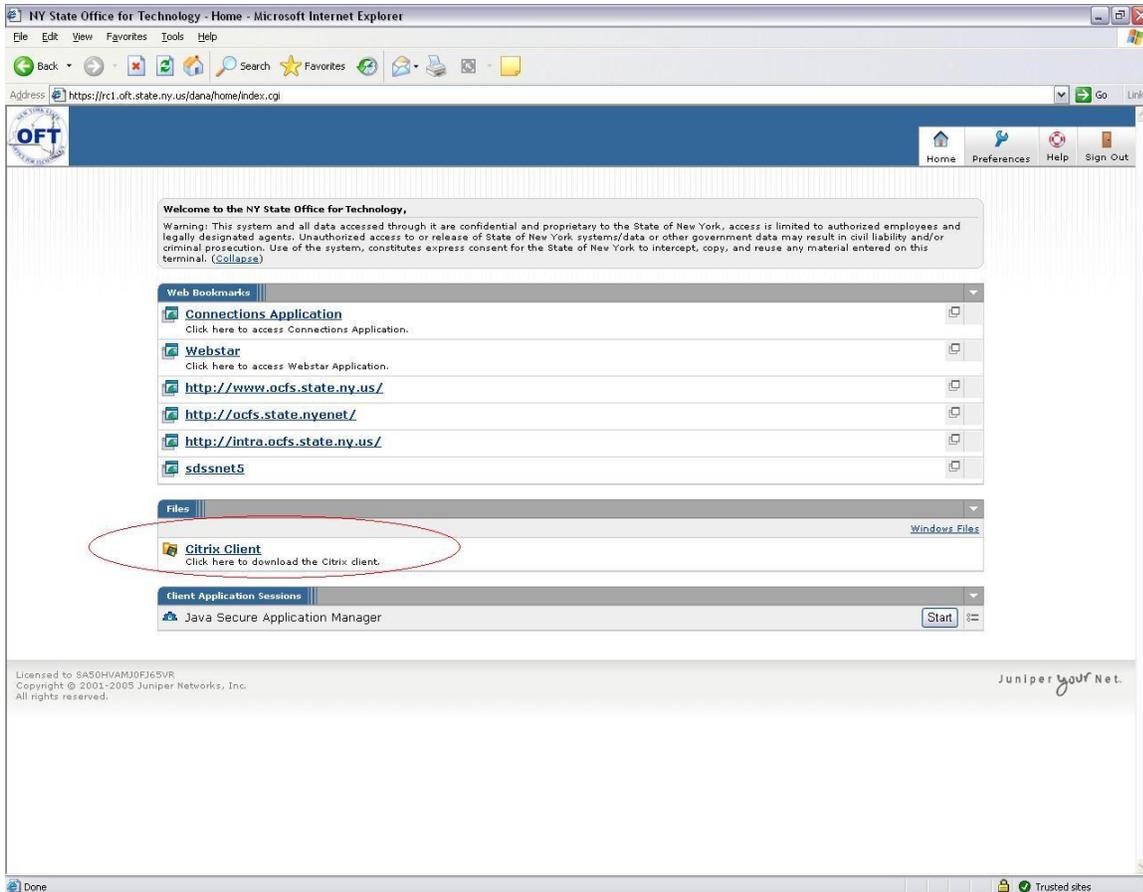


Figure 7: The Web Bookmarks Screen - Citrix Client Download

Scrolling to the bottom of that page displays a section entitled "Files". In the files section, click on the "Citrix Client" link. A page will now display with two files available for download, Citrix.exe and Citrix.zip.

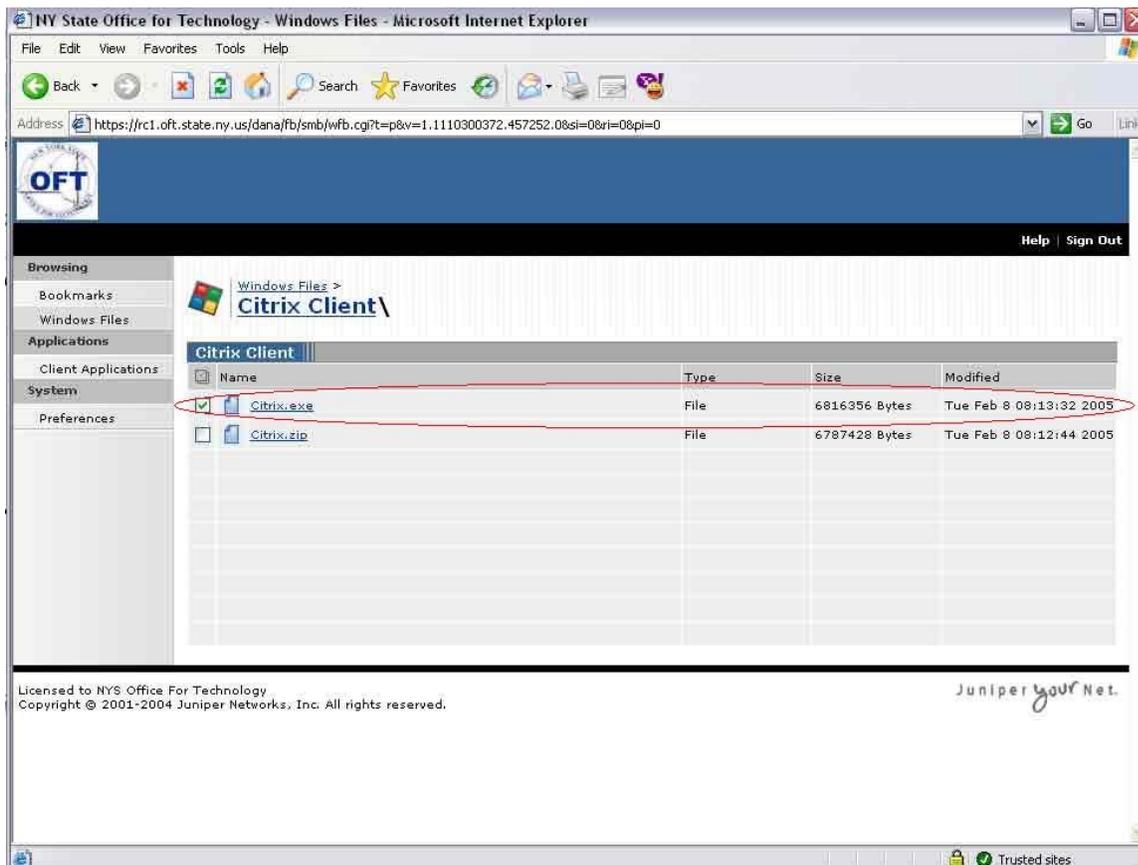


Figure 8: The Citrix.exe download link

Click on the *Citrix.exe* link. A prompt should now appear with the choices of Run, Save, or Cancel. Select Save and download the file to a convenient location, such as the Windows Desktop or My Documents folder.

The Citrix.exe file will now be downloaded and stored to that location. The download may take several minutes to complete. Once the download has finished, navigate to the Citrix.exe file that was just downloaded.

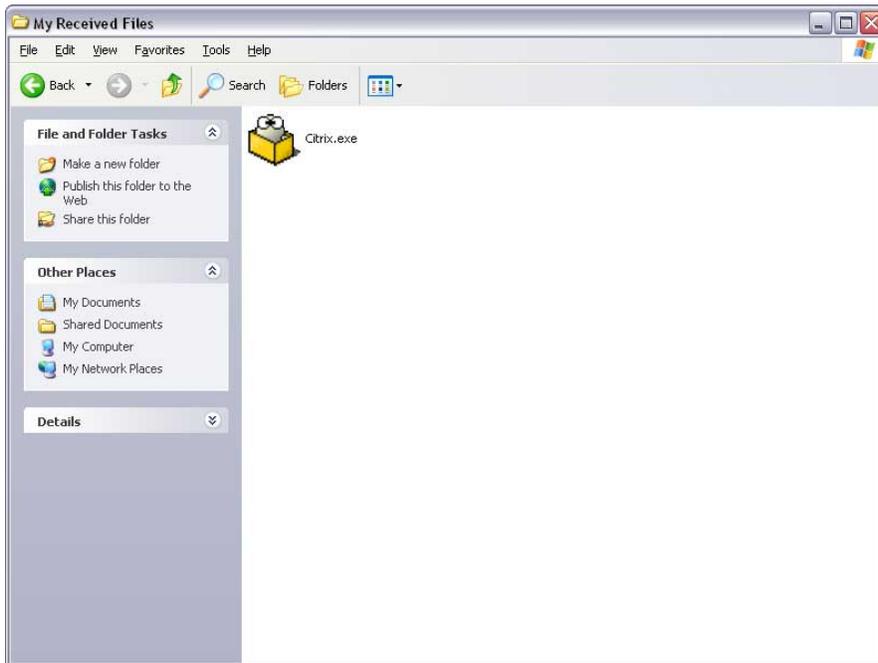


Figure 9: The downloaded Citrix.exe file

Double click on the *Citrix.exe* file, which should appear as above. Several windows will pop up and disappear on their own, and after they complete, the PN Agent should be installed successfully, completing this step. Note that it may be necessary to be logged in with administrative credentials to successfully install the PN Agent.

Attempting to Access Connections

Once the above setup steps have been taken, the computer should now be properly configured for accessing Connections.

Open Internet Explorer, and again go to <https://rc1.oft.state.ny.us/ocfs>, where the login screen will appear.

[Note: If a message is displayed indicating, “You do not have permission to log in. Please contact your administrator”, refer to the Temporary Internet Files/Cookies and SSL-VPN Access for HSEN ID sections in the Troubleshooting/Configuration section appearing later in this document.]

The SSL-VPN login screen should now appear, and the next step will be to enter a valid HSEN UserID and password and press the *Enter* key, or click the *Sign In* button. The following page will then load:

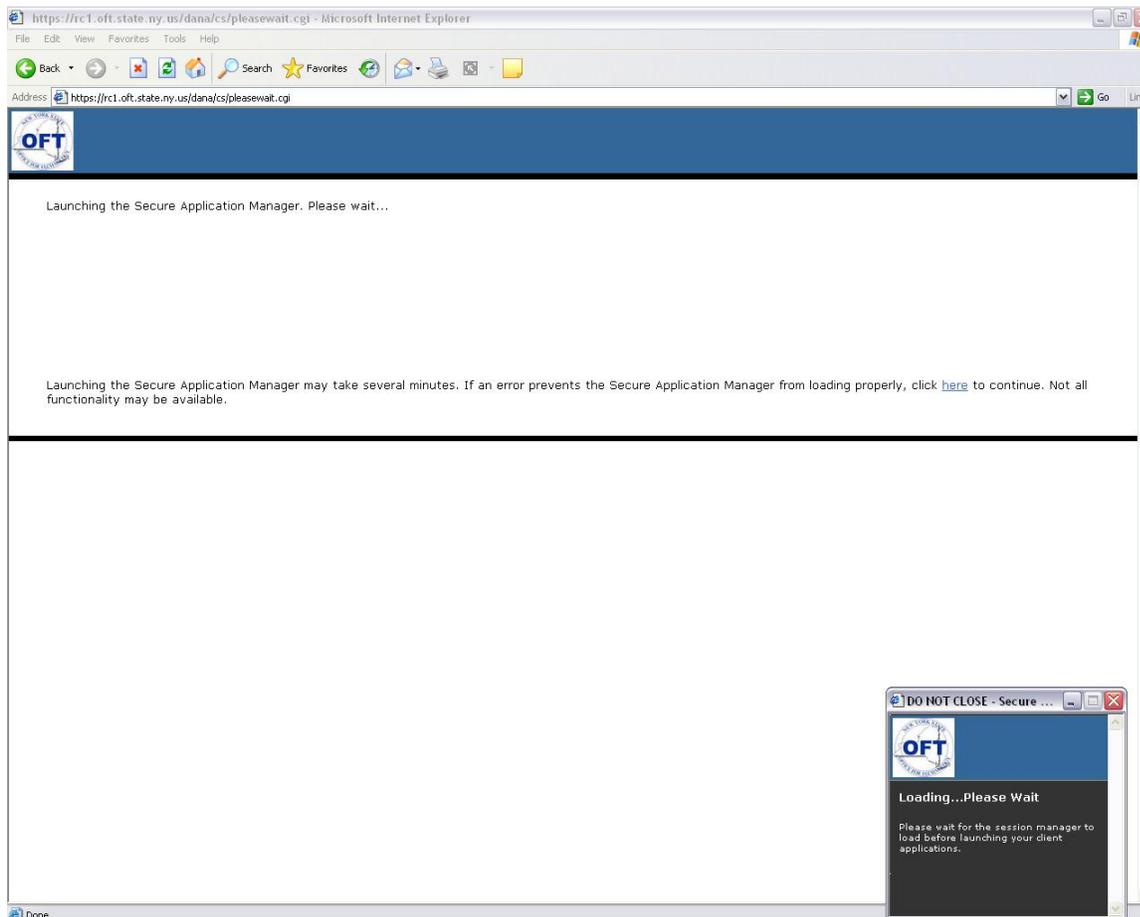


Figure 10: Launching the Secure Session Manager

This page will load the Secure Session Manager, which is necessary for maintaining a secure connection to the state network. The Secure Session Manager will appear in the lower right corner of the screen, as shown in the above picture.

Do not click on the “click here to continue” link unless there has been an extremely long delay (over two minutes) without the Secure Session Manager appearing or signs of activity. Also **do not close the Secure Session Manager window** when it appears.

[Note: If the Secure Session Manager window fails to appear, or a message is received indicating that a Pop-up was blocked, refer to the Pop-up Blocking section in the Troubleshooting/Configuration section appearing later in this document.]

After the Secure Session Manager loads, the Web Bookmarks page should be displayed. To get to Connections, click on the *Connections Application* link, as shown below:

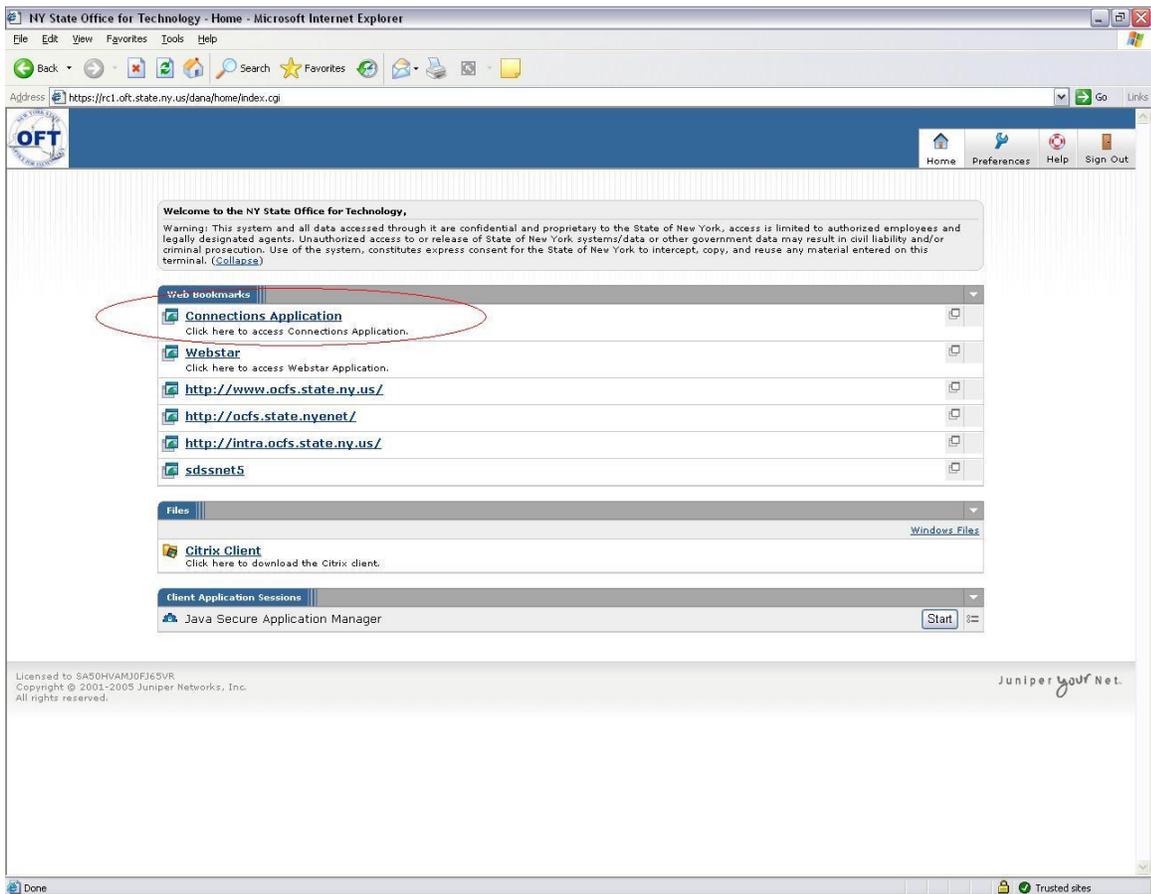


Figure 11 - Selecting the Connections Application Link from the Web Bookmarks Page

A new window should be open, displaying another login screen and entitled Web Interface for MetaFrame Presentation Server, as shown below:

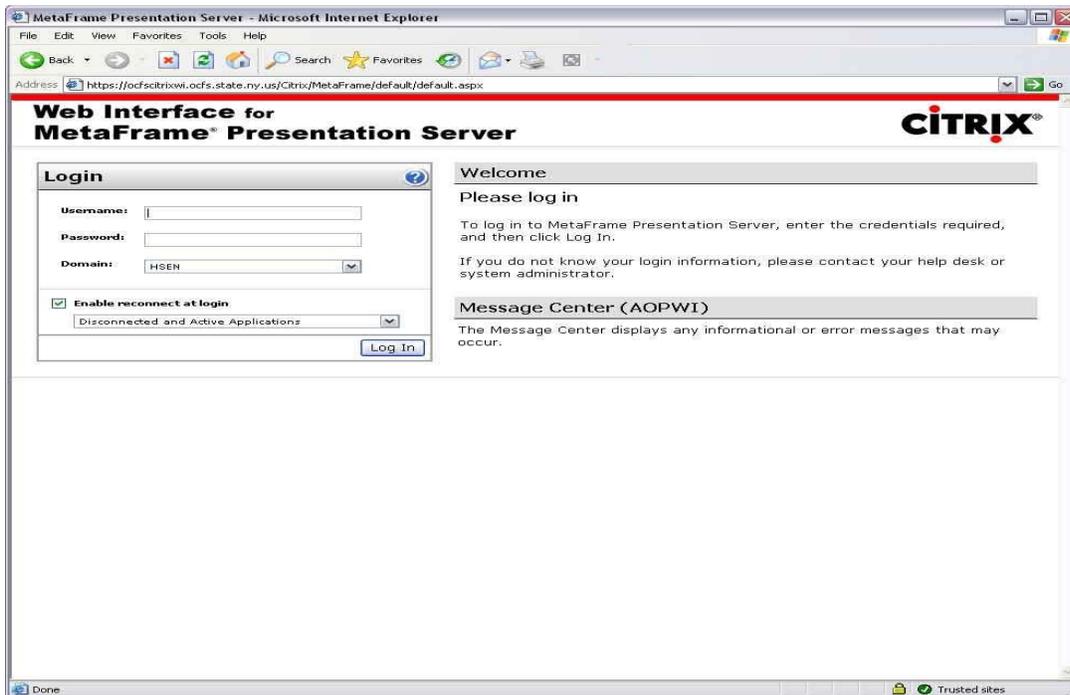


Figure 12: The Web Interface for MetaFrame Presentation Server login screen

[Note: If the Web Interface for MetaFrame Presentation Server window does not appear, and instead there is a window with an error message stating “The page cannot be displayed” or “Action cancelled” please refer to the Proxy Server Issues, Windows Issues, and Address Resolution Issues sections of the Troubleshooting/Configuration section appearing later in this document.]

Enter the HSEN UserID and password of the person whose Connections session is to be accessed, and then press the *Enter* key or click the *Log In* button.

A screen displaying several icons will appear, as shown below. The message stating “Your applications have not been reconnected. Your farms do not support workspace control or do not trust the server” appears, but may be ignored since it does not impact the ability to access Connections. [As a side note, the term “farm” refers to a collection of servers.]

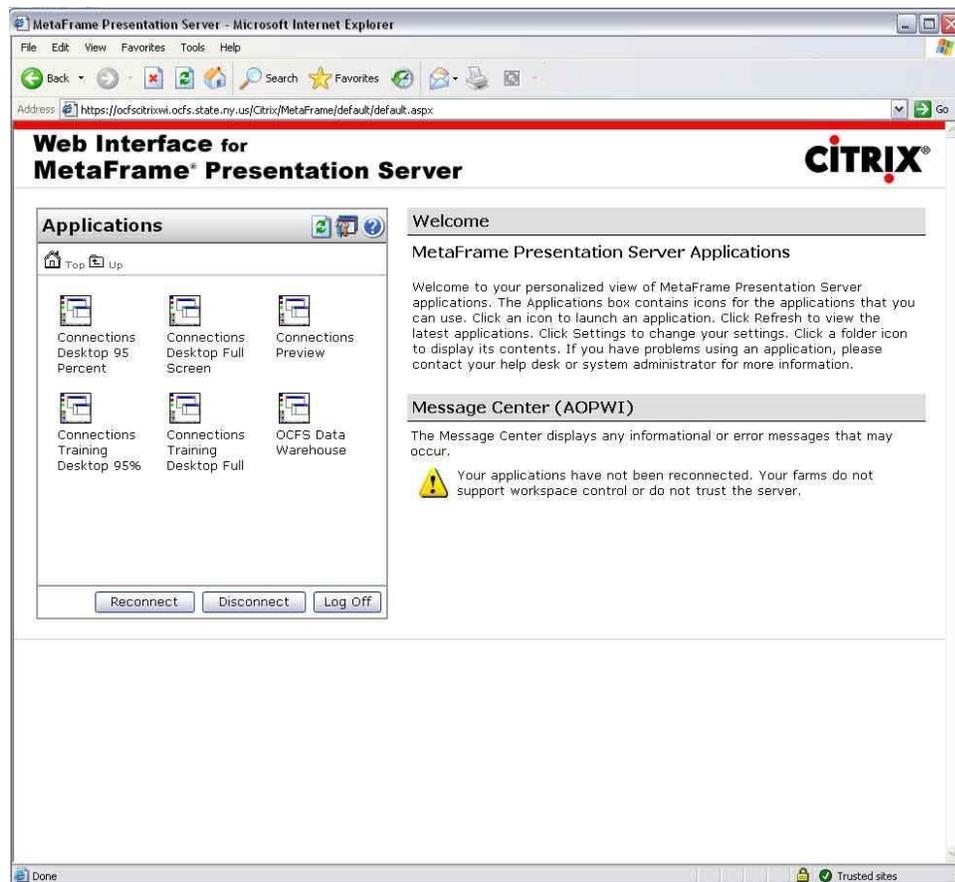


Figure 13: The Connections Application Icons screen

Select either the *Connections Desktop 95 Percent* or the *Connections Desktop Full Screen* icon. Both icons will launch the Connections application, but in different resolution modes. The 95 Percent icon will cause the Connections session to occupy 95% of the desktop, leaving the Windows toolbar and Start Menu visible. In full screen mode, Connections will occupy the entire screen. Which display mode to use is a matter of personal preference, however, if the desktop resolution is set a size less than 1024 by 768, it may be necessary to use the full screen mode in order to view all buttons within Connections.

Upon clicking either of the icons, a progress indicator window will appear, as shown below.

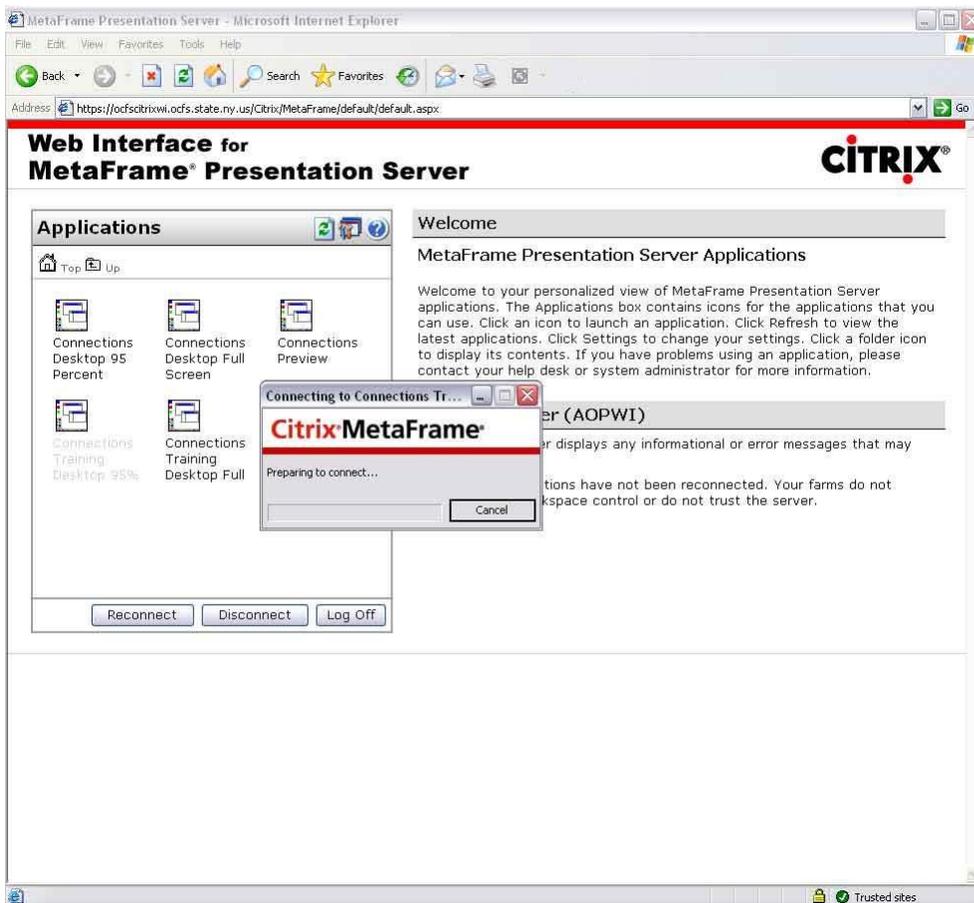


Figure 14: Indicator of Connections application launch progress

After the progress bar is filled, the Citrix session containing the Connections application will appear. After clicking the *OK* button on the confidentiality notice that appears, the Connections desktop will appear, as shown below.

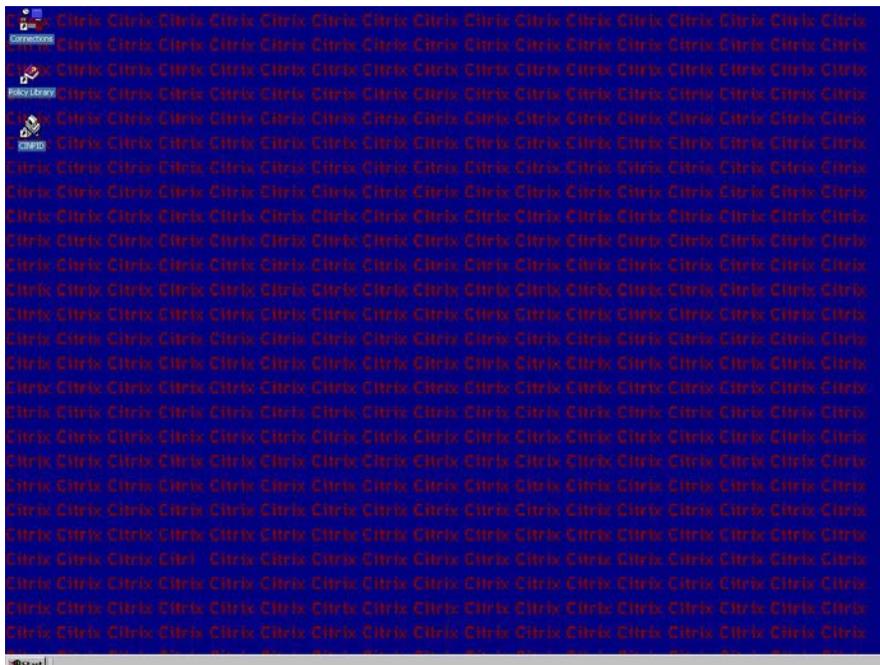


Figure 15: The Connections desktop

Clicking on the *Connections* icon will open the Connections toolbar, and the application is available for use.

Troubleshooting/Additional Configuration

Temporary Internet Files and Cookies Issue

When attempting to login to the SSL-VPN login screen, an error message indicating, “You do not have permission to login. Please contact your administrator” may appear before the login box is presented, as shown below:

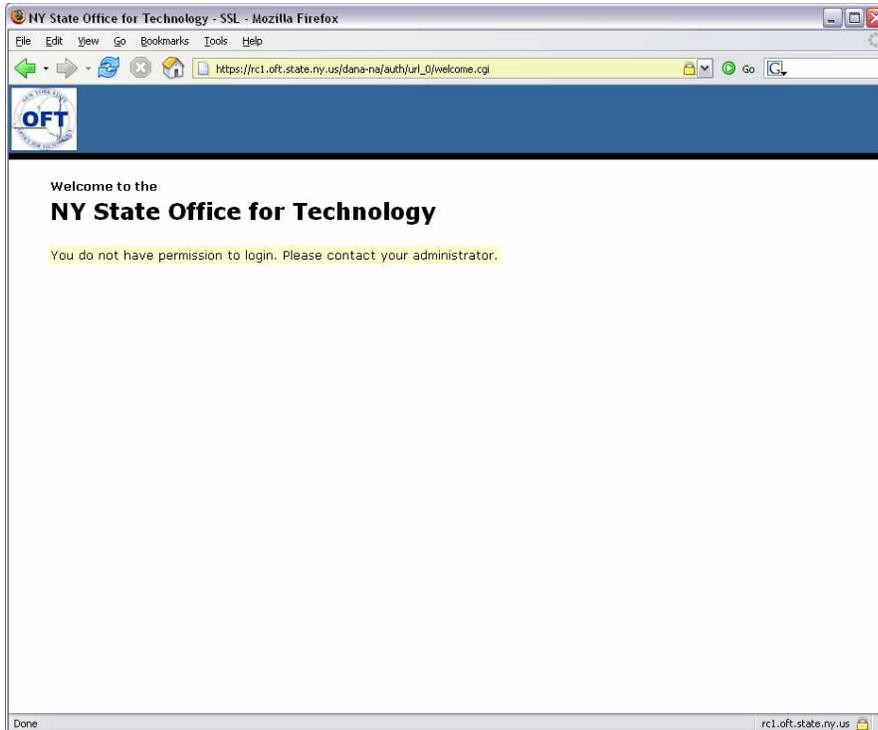


Figure 16: The Lack of Permission error message

This is caused by “congestion” in the temporary files stored by Internet Explorer. In order to remedy this, go to *Tools -> Internet Options*. This will display the General settings tab. Press the *Delete Cookies* button. A box will appear asking permission to delete all cookies, as shown below.

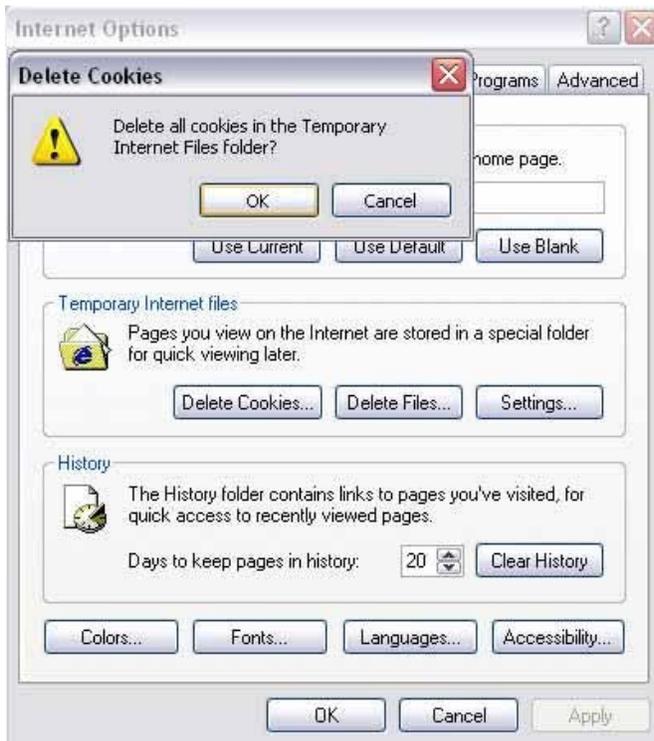


Figure 17: The Delete Cookies button and permission dialog

Press the *OK* button. This will close the dialog and return to the General settings tab.

Next press the *Delete Files* button. A dialog will appear asking permission to delete temporary files, as shown below.



Figure 18: The Delete Files Button and Delete Offline Content dialog

Check the check box for *Delete all offline content*, and then click the *OK* button. An hourglass may appear and there may be a delay of several minutes while the temporary internet files are cleared. Wait until the hourglass goes away.

Click on the *OK* button, which will close the Internet Options screen and return to the browser window. Press the F5 key on the keyboard to refresh the screen, and the SSL-VPN login screen should appear. If it does not, close all open browser windows and re-open Internet Explorer and go to <https://rc1.oft.state.ny.us/ocfs> again. If this does not successfully display the login screen, repeat the above steps and try once more.

Using the *Sign Out* button on the Web Bookmarks screen (shown below) when finished with Connections will greatly reduce the occurrence of temporary internet file and cookie problems.

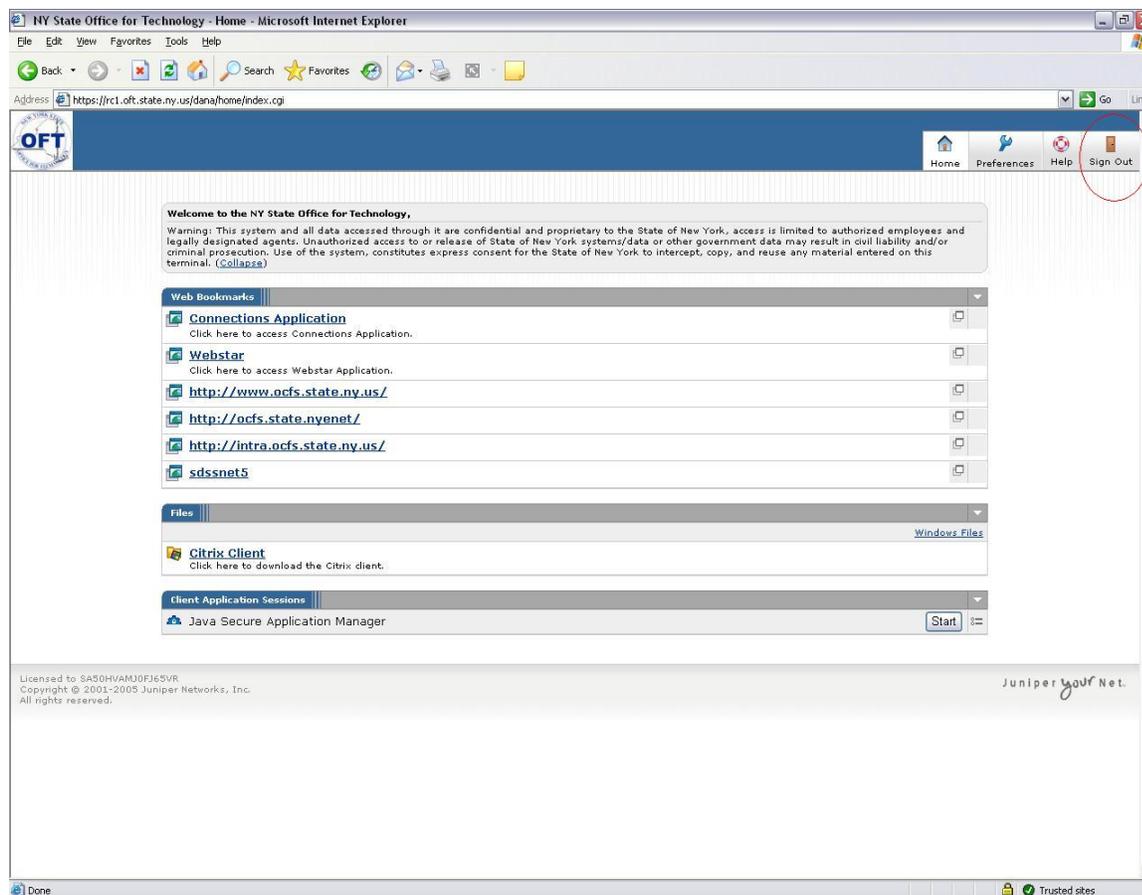


Figure 19: The Sign Out button should be used when finished with Connections (see top right)

SSL-VPN Access for HSEN ID

If a user attempts to login to the SSL-VPN login window and receives the “You do not have permission to login. Contact your administrator” error message, it indicates that the HSEN UserID for that user has not been granted SSL-VPN access. Access can be granted by obtaining the application for SSL-VPN access from <http://ocfs.state.ny.us/main/vpn/sslvpn>. The application form and instructions for completing it are available at that link. The Security Coordinator, Local Security Administrator, or other authorized requestor must submit the form.

Pop-up Blocking

Many pop-up blocking utilities will prevent the Secure Session Manager from opening. These pop-up blockers can include the native Pop-Up Blocker contained in Internet Explorer, the Yahoo Toolbar, the SSL VPN Troubleshooting Guide

Google Toolbar, or other third-party spam/pop-up/adware blocking software. These pop-up blockers must either be disabled, or configured to allow the Secure Session Manager.

Most third-party toolbars have a setting to permit pop-ups for certain sites, but if that cannot be located, the toolbar will need to be uninstalled or removed. This can usually be done by going to *Start Menu -> Settings -> Control Panel -> Add or Remove Programs* and then selecting the offending toolbar and choosing *Remove*. If the offending toolbar cannot be located in this listing, it may be necessary to contact computer support personnel or the toolbar's vendor (e.g. Google, Yahoo, AOL).

Internet Explorer's built in Pop-Up Blocker can be configured to allow the Secure Session Manager to load from within Internet Explorer. Go to *Tools -> Internet Options -> Privacy*, which will display the following screen if the version of Internet Explorer installed on this PC has built-in pop-up blocking.

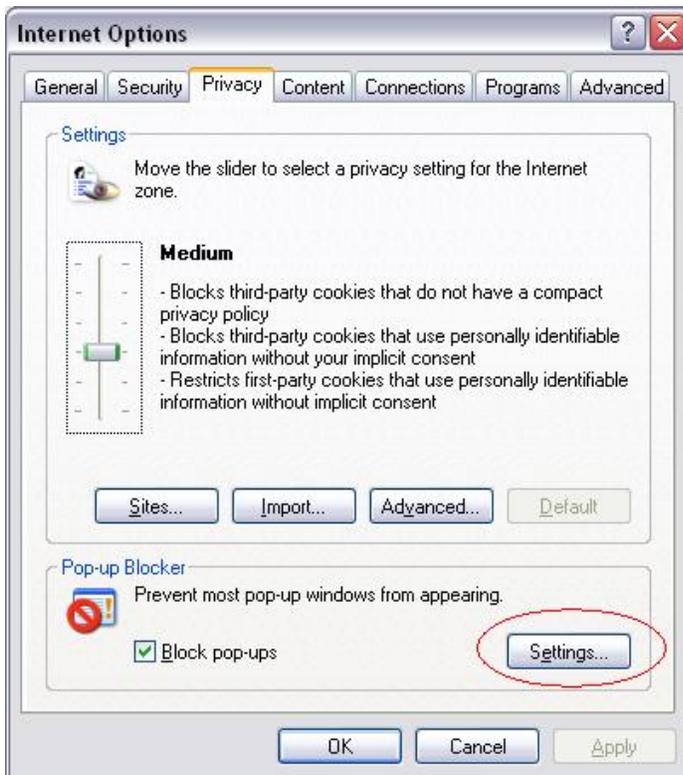


Figure 20: The Privacy Tab and Pop-Up Blocker Settings Button

Click on the *Settings* button, which will display the screen below.



Figure 21: The Pop-Up Blocker Settings window

Enter *.state.ny.us into the Address of Web site to allow box and then click on the *Add* button. Next, click on the *Close* button, followed by the *OK* button on the next screen.

Internet Explorer should no longer prevent the Secure Session Manager window from opening. If something is still preventing the window from opening, continue to look for third-party software that may be blocking pop-ups.

Windows Issues

If after clicking the *Connections Application* link on the Web Bookmarks page, a window appears and states “The page cannot be displayed” or “Action cancelled”, it could possibly be the result of Windows needing to be updated.

Windows can be updated by going to *Start -> Windows Update* and selecting *Custom*, followed by the downloading and installation of all High Priority Updates and any Windows XP Updates listed under Software, Optional. In order to run Windows Update, an administrative account for the local PC is usually required. If the current account does not have administrative privileges, the LAN administrator or computer support staff at the site may be able to perform the necessary steps or grant administrative rights, if appropriate.

Proxy Server Issues

If the “Page cannot be displayed” or “Action cancelled” message is still appearing after clicking the *Connections Application* link on the Web Bookmarks page, there may be an issue with the proxy server, a tool used to filter out certain types of undesired internet traffic, at the site blocking access to Connections.

To set up Internet Explorer’s proxy setting to allow Connections access, go to *Tools -> Internet Options -> Connections*. The following window will appear:



Figure 22: The LAN Settings button on the Connections tab in Internet Explorer

Click on the *LAN Settings* button, and the following window will appear:

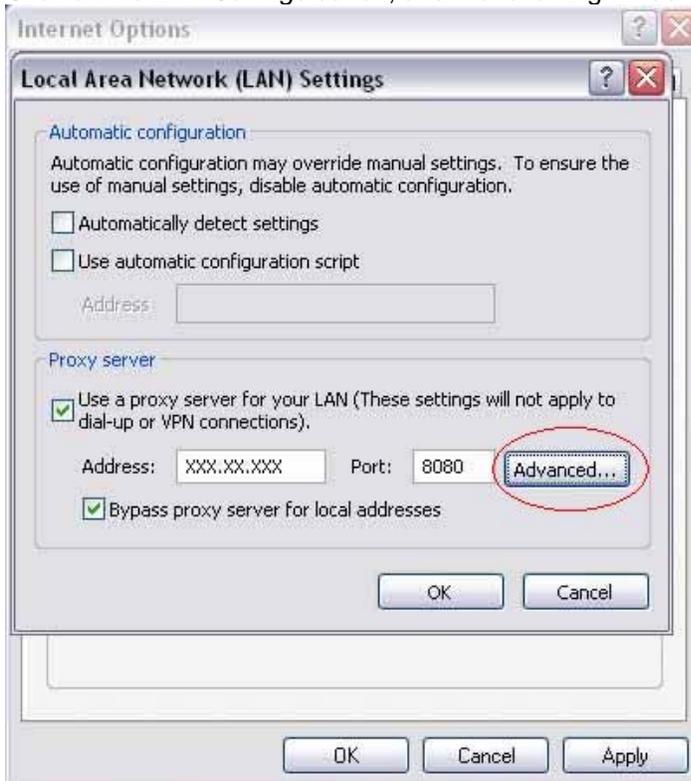


Figure 23: The LAN Settings Window with Proxy Server enabled

If the “Use a proxy server for your LAN” box is not checked, there is no locally configurable proxy server option that will resolve this issue. Do not check this box if it was not already checked, as it may disrupt the network connectivity of the PC.

If the “Use a proxy server for your LAN” is checked, click on the *Advanced* button, and the window pictured below will appear.

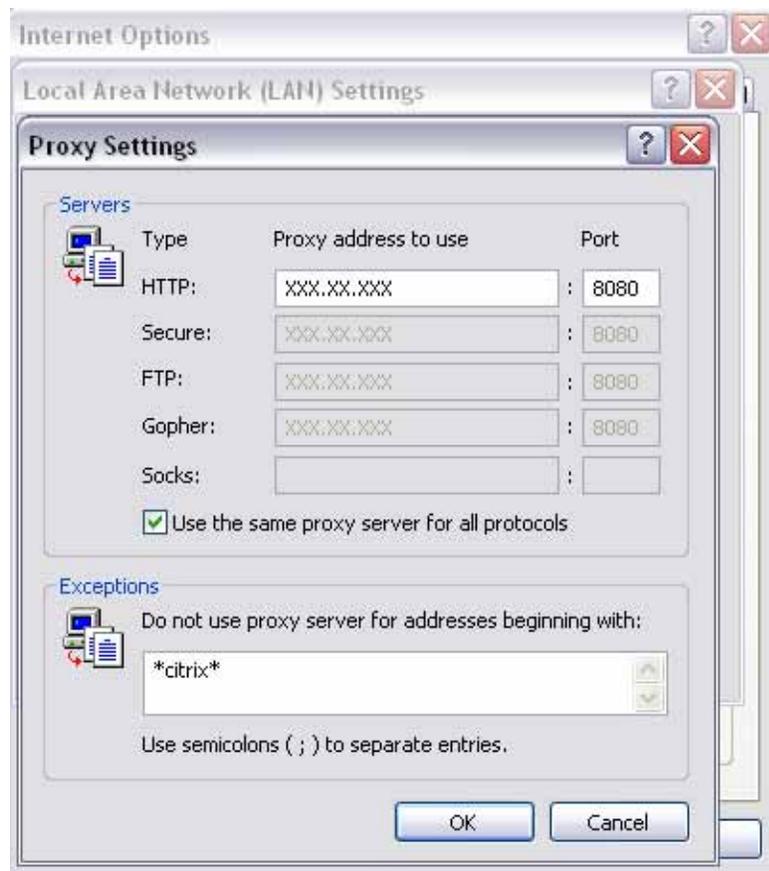


Figure 24: The Proxy Settings Window with *citrix* as an added exception

In the “Do not use proxy server for addresses beginning with:” box, type *citrix*. This will permit Connections to bypass the proxy server and be able to be opened.

[Note: Do not make any other changes to the proxy server settings other than the one listed above. This could affect internet connectivity on this PC.]

Finish this step by clicking the *OK* button on this screen followed by clicking the *OK* button on the next screen. It may be necessary to close all open browser windows and re-open Internet Explorer after this step.

Address Resolution Issues

If the “Page cannot be displayed” or “Action cancelled” message is still appearing after clicking the *Connections Application* link on the Web Bookmarks page, there may be an issue with the network configuration at the site blocking access to Connections.

A modification to the hosts file in Windows can sometimes fix this. Administrative access to the PC is usually necessary to attempt this fix. Additionally, care must be taken when modifying the Hosts file, as it can disable access to network resources if not configured properly.

Open My Computer and navigate to C:\Windows\System32\Drivers\Etc. This will display the folder shown below:

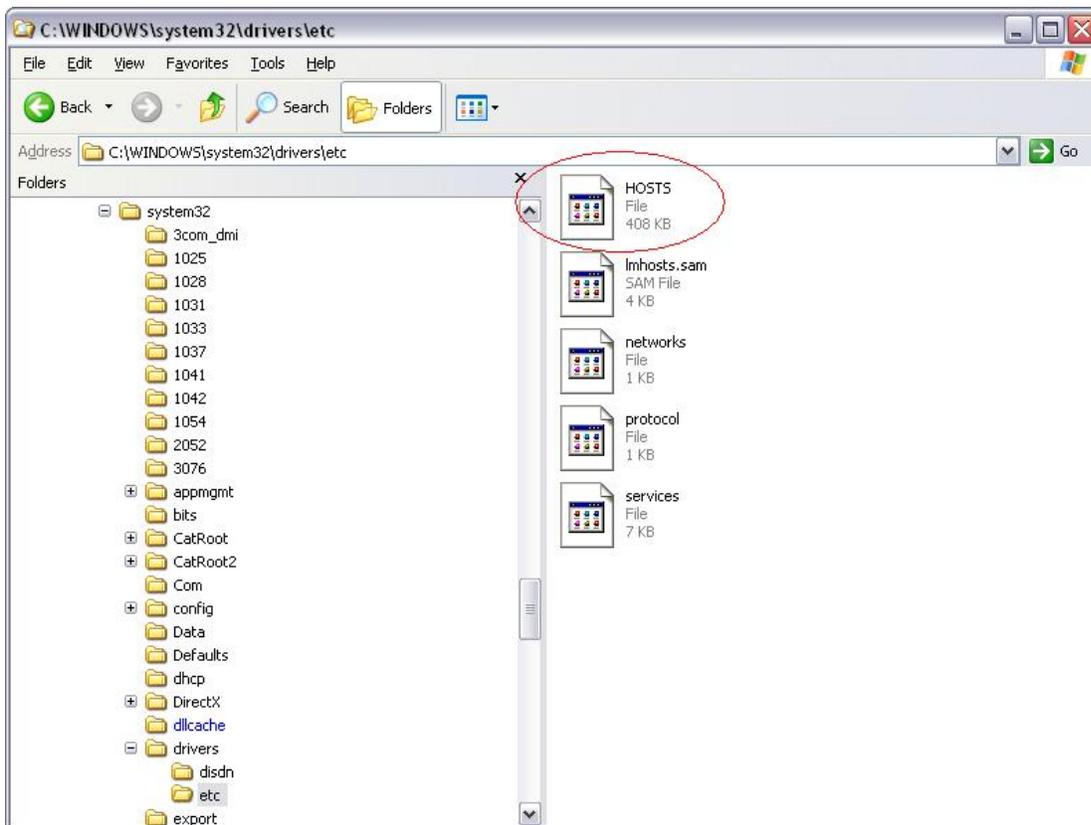


Figure 25: The C:\Windows\System32\Drivers\Etc folder with Hosts file

Double-click on the file named Hosts. If prompted to choose what application is to be used to open this file, select Notepad.

This will open the Hosts file, which will most likely appear as shown below:

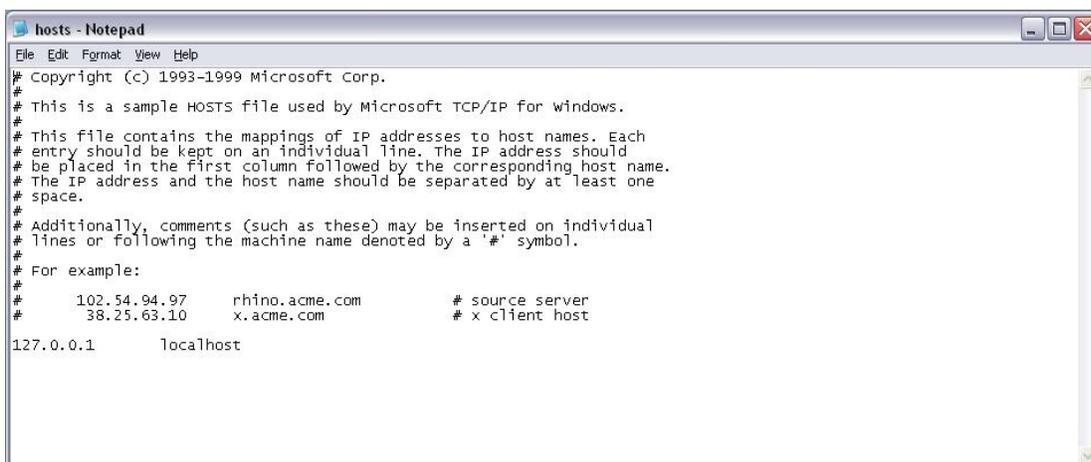
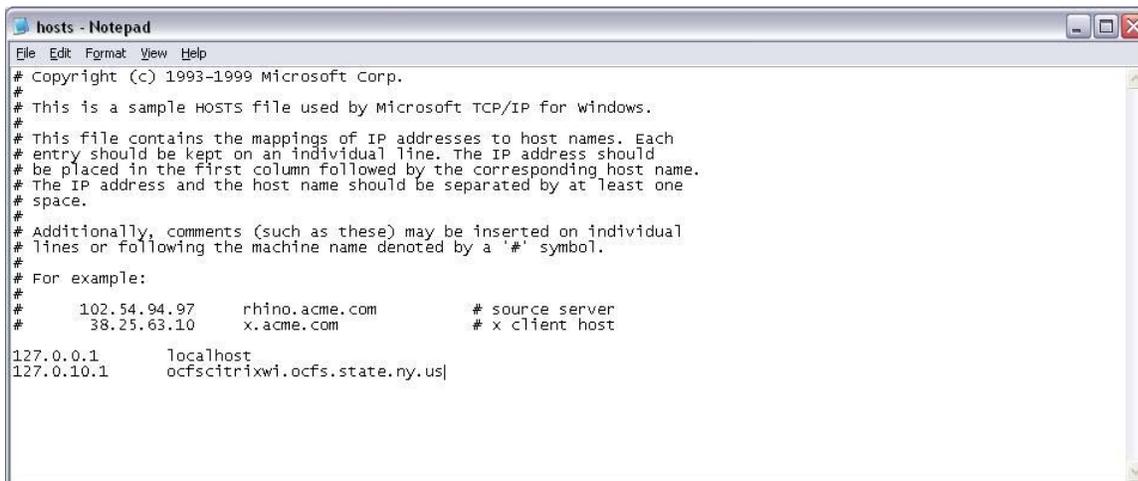


Figure 26: The Unmodified Hosts file

Place the cursor below the last line in the Hosts file, which is the 127.0.0.1 line in this case. Next, type the following without quotation marks "127.0.10.1 [Press the Tab key on the keyboard] ocfsctrixwi.ocfs.state.ny.us". The Hosts file should now appear as below:



```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-1999 Microsoft Corp.
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10      x.acme.com               # x client host
127.0.0.1       localhost
127.0.10.1      ocfscitrixwi.ocfs.state.ny.us|
```

Figure 27: The Modified Hosts file

[Note: **Do not modify or remove** any lines already in the Hosts file. If there are more entries in the Hosts file than the ones pictured above, that is fine. Incorrect changes to the Hosts file can cause network resources to become unavailable.]

Go to *File -> Save*. Close all open browser windows, re-open Internet Explorer, and attempt accessing Connections again. If this does not work, reboot the PC and try again.

If the same “Page cannot be displayed” or “Action cancelled” screen continues to appear, then the problem lies somewhere in the connection between this site and the state network. The network administrator for this site will need to be contacted, as it may be necessary to add permissions for access to the ocfscitrixwi.ocfs.state.ny.us link to the firewall, routing tables, or proxy server of the agency network.

Software Firewall Issues

For PCs with software firewalls installed (such as Zonealarm or Norton Internet Security), it may be necessary to permit access to the internet for the Jupiter Networks Cache Cleaner component.

Typically, if a software firewall is uncertain how to process a request by the Cache Cleaner component to access the internet, a prompt will be displayed asking whether to allow or deny access. There is usually a check box to indicate that the software firewall should remember the decision. If this prompt appears and there is an option to store the setting, select that option and choose to allow access.

If that option is not presented, please refer to the documentation for the software firewall being used to determine the steps necessary to permit access of a specified component to the internet.

Adding Shortcuts to Connections

If Connections will be used frequently on this computer, it may be useful to create a shortcut to this address on the Windows desktop or to save this address to the list of Favorites. This is not a required step, but it may make getting to Connections easier for the person using this computer.

To save this address to the Favorites list, go to *Favorites-> Add to Favorites*. A prompt will appear indicating that this address will be added to the list of Favorites under the name “New York State Office for Technology”. This name can be renamed to anything that will make it easier to determine what this link is to by replacing the “New York State Office for Technology” text with anything else, such as “Connections” or “SSL-VPN Login”.

To place a shortcut to the SSL-VPN login screen on the Windows desktop, go to *File -> Send -> Shortcut to Desktop*. An icon entitled “New York State Office for Technology” will now appear on the desktop. If desired, right clicking on the icon and choosing *Rename* will enable the icon name to be changed.

Further Assistance

If you are still encountering problems using or configuring SSL-VPN, please contact the New York State Enterprise Help Desk at (800) 697-1323. This resource is provided as a free service by New York State and will not incur any costs to the agency or site.