



# **SSL VPN User's Guide**

**v1.0.0**

**August 1st, 2006**

**Office of Academic and Administrative  
Information Systems**

**<http://its.ucsf.edu>**

## Table of Contents

<b>OVERVIEW OF THE SSL VPN@UCSF SERVICE.....</b>	<b>4</b>
WHAT IS THE SSL VPN@UCSF SERVICE? .....	4
WHAT CAN YOU ACCESS THROUGH THE SSL VPN@UCSF SERVICE? .....	4
HOW TO LOGIN TO THE SSL VPN@UCSF SERVICE .....	4
THE SSL VPN@UCSF HOME PAGE EXPLAINED .....	5
<i>Home Page Sections</i> .....	6
<i>Home Page Icons</i> .....	6
HOME PAGE PREFERENCES .....	7
<i>User Home</i> .....	7
<i>General</i> .....	8
<i>Applications</i> .....	8
<i>Advanced</i> .....	8
<b>VPN FEATURES .....</b>	<b>10</b>
CREATING BOOKMARKS .....	10
<i>Creating Web Page Bookmarks</i> .....	10
<i>Creating Files Links</i> .....	11
<i>Creating Secure Shell (SSH) Terminal Sessions</i> .....	12
<i>Creating Telnet Terminal Sessions</i> .....	13
<i>Creating Window Remote Desktop Terminal Sessions</i> .....	15
<i>Creating Citrix Metaframe Terminal Sessions</i> .....	17
USING BOOKMARKS, LINKS AND SESSIONS .....	19
<i>How to use Web Bookmarks</i> .....	19
<i>How to use Files Links</i> .....	19
<i>How to use Terminal Sessions</i> .....	19
MANAGING BOOKMARKS, LINKS AND SESSIONS .....	20
<i>How to Edit a Web Bookmarks, File Links and Terminal Sessions</i> .....	20
<i>How to Change the Order of and Delete Web Bookmarks, File Links and Terminal Sessions</i> .....	20
<b>TRADITIONAL VPN SERVICE WITH NETWORK CONNECT .....</b>	<b>22</b>
WHAT IS NETWORK CONNECT? .....	22
STARTING NETWORK CONNECT .....	22
<b>APPENDIX I – SUPPORTED PLATFORMS .....</b>	<b>24</b>

UCSF SUPPORTED PLATFORMS .....	24
SSL VPN@UCSF SYSTEM SUPPORTED PLATFORMS .....	25
<i>Defining Included Terms</i> .....	25
<i>Multiple Language Support</i> .....	25
<i>Note on Java</i> .....	25
<i>Supported Platforms Matrix</i> .....	25
<i>Notes for JSAM and Platform Support</i> .....	26
<i>Notes for Mobile Devices</i> .....	26
GETTING SUPPORT .....	26
<b>APPENDIX II – INFORMATION ABOUT JAVA ON WINDOWS .....</b>	<b>28</b>
WHAT VERSION OF JAVA AM I RUNNING? .....	28
<i>Web Java Test</i> .....	28
<i>Microsoft Java Virtual Machine (JVM)</i> .....	28
<i>Sun Java Virtual Machine (JVM)</i> .....	28
HOW TO INSTALL THE SUN JVM.....	29
HOW TO SET THE DEFAULT JVM FOR YOUR BROWSER.....	29
<i>Windows XP and 2003 Server</i> .....	30
<i>Windows 98, 98SE, ME and NT (Server and Workstation)</i> .....	30
<b>APPENDIX III – INFORMATION ABOUT JAVA ON MACOS X.....</b>	<b>31</b>
WHAT VERSION OF JAVA AM I RUNNING? .....	31
<i>Web Java Test</i> .....	31
<i>Sun Java Virtual Machine (JVM)</i> .....	31
INSTALLING OR UPGRADING JAVA ON MACOS X v10.4 .....	31
INSTALLING OR UPGRADING JAVA ON MACOS X v10.2 .....	31
INSTALLING OR UPGRADING JAVA ON MACOS X v10.3 .....	32
<b>APPENDIX IV – INFORMATION ABOUT JAVA ON LINUX.....</b>	<b>33</b>
WHAT VERSION OF JAVA AM I RUNNING? .....	33
<i>Web Java Test</i> .....	33
<i>Sun Java Virtual Machine (JVM)</i> .....	33
INSTALLING OR UPGRADING JAVA ON LINUX .....	33

## **Overview of the SSL vpn@UCSF Service**

UCSF is proud to offer two distinct VPN systems to campus community; a traditional thick client VPN and a web based SSL vpn@UCSF. This document outlines the capabilities of the SSL vpn@UCSF service as well as how to use it.

### *What is the SSL vpn@UCSF Service?*

SSL vpn@UCSF, also called Clientless VPN, is a VPN system that utilizes on-demand software through web pages to access protected resources. This means that instead of having to install a VPN client on your computer, as you do with the UCSF Traditional VPN service, the software needed for you to communicate is automatically installed in to your web browser only during the time you need to use it.

The SSL vpn@UCSF system in use at UCSF uses Java to create connections from the user's computer to the UCSF computing network. This allows the user to act like he or she is physically connected in one of the UCSF buildings. This also means that it is not as efficient as a traditional, thick client VPN system. More information on the differences between the two VPN systems can be found at <http://its.ucsf.edu/information/network/vpn/>.

### *What Can You Access Through the SSL vpn@UCSF Service?*

Users can access websites anywhere on the Internet as if they were connected directly to the UCSF computing network. All other services, with the exception of Network Connect, are restricted to communications to the UCSF computing networks only.

What does this mean? You can use the SSL vpn@UCSF system to access Library Resources on the Internet and file servers on the UCSF computing network, but you can not use the SSL vpn@UCSF system to connect to VoIP services like Skype or to play online games.

### *How to Login to the SSL vpn@UCSF Service*

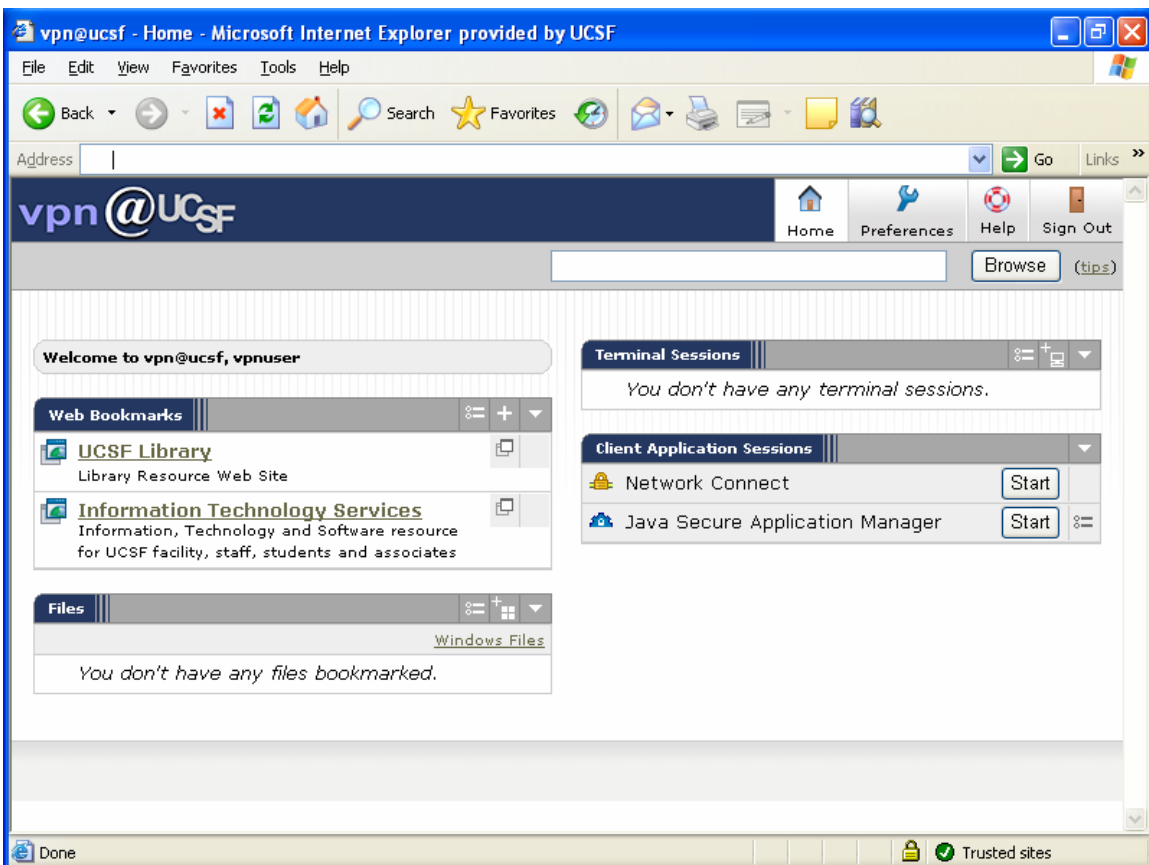
Point your web browser at <https://vpn.ucsf.edu> access the SSL vpn@UCSF system. Once the page has loaded you will be greeted by the vpn@UCSF SSL login page.



Enter your VPN username and password into this page and then click on the Sign In button to access to the SSL vpn@UCSF system.

If you do not have a VPN ID or do not remember your password, please visit <http://its.ucsf.edu/information/network/vpn/get/>.

## *The SSL vpn@UCSF Home Page Explained*



## Home Page Sections

### Browse Services

As discussed in the Quick Start Mini-Guide, the browse field and button act like the URL window of your web browser through which you can access web resources, SSH, and Telnet servers as well as Windows terminal servers.

### Web Bookmarks

Bookmarks allow you to easily navigate to Web pages and other resources using links. Once created, the links are available in the Web Bookmarks panel of the SSL vpn@UCSF home page. You can also use the Telnet and SSH protocols in the Browse field of the SSL vpn@UCSF home page to browse to UNIX servers, networking devices, and other legacy applications that utilize terminal services.

### Terminal Sessions

Terminal services enable you to use Windows-based or Citrix applications that are running directly on your department's terminal server. When you run an application on the terminal server, most actions are performed on the server itself rather than your workstation. The terminal server only transmits keyboard, mouse, and display information over the network. Also, a terminal session provides Telnet and SSH access to UNIX servers.

### Files

File server bookmarks allow you to quickly browse to Window hosted file systems (also MacOS X file systems shared with Windows compatibility and UNIX/Linux file systems shared with Samba). Links stored here provide you with a web browser interface to the remote file system allowing you to view, upload and download files.

### Client Applications Sessions








JSAM, the Java Secure Application Manager provides, support for static TCP port client/server applications, including enhanced support for Microsoft MAPI, Lotus Notes, and Citrix NFuse. JSAM also provides NetBIOS support, which enables users to map drives to specified protected resources.

JSAM works well in many network configurations but does not support dynamic port TCP-based client/server applications, server-initiated connections, or UDP traffic.

Network Connect is a traditional VPN client for the SSL vpn@UCSF system. Where as all of the other features of the SSL vpn@UCSF system only direct specific traffic to the UCSF network, the Network Connect client connects you to the UCSF computing network in the same manner as a traditional thick client VPN.

### Home Page Icons

Many of the functions on the home page are accessed by clicking on an icon. Hovering your mouse over each one (with most browsers) will make a small help window appear with a description of what the icon does.

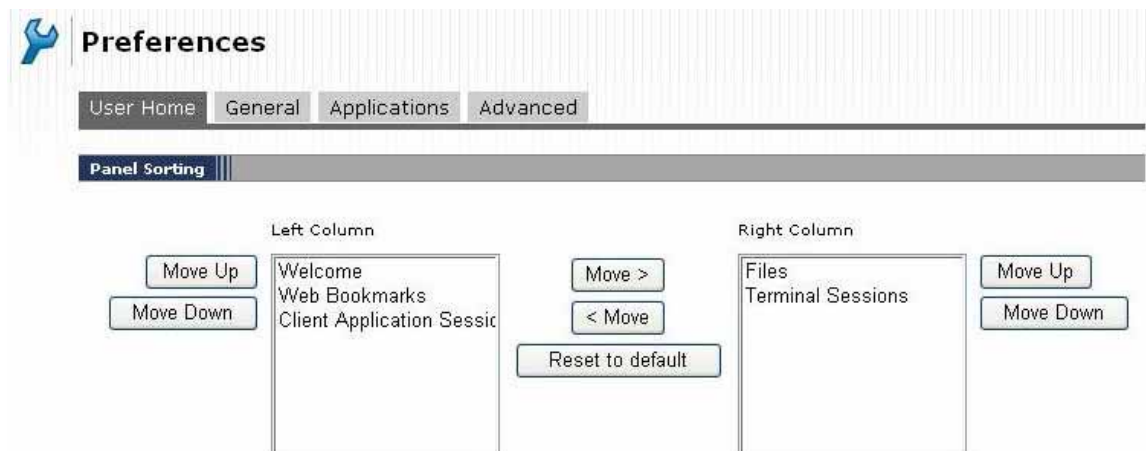
Icon	Meaning
	Return to the Home page
	View the main preferences page
	Opens a separate window with the built in SSL help and VPN documentation
	Logs off of the SSL vpn@UCSF system
	View the preferences page for the item to its left
	Minimizes the current window within the page to save space if you are not using the information inside of it.
	These icons are used to create new bookmarks

## Home Page Preferences

The options on the **Preferences** pages enable you to alter the look of your home page, uninstall client components and delete cookies

To access the preferences click the **Preferences** button at the top of the SSL vpn@UCSF home page. You will be presented with the User Home preferences as well as tabs to access the other preferences screens.

## User Home



The User Home preferences control the look of the SSL vpn@UCSF home page. To rearrange the panels on your secure gateway home page:

- On the **User Home** tab of the **Preferences** page, select the name of a panel in the **Left Column** or **Right Column** list.
- To position the panel above or below the other panels on the secure gateway home page, click **Move Up** or **Move Down**.
- To move the panel to the other side of the secure gateway home page, click **Move>** or **< Move**.
- To rearrange the panels as your system administrator originally specified, click **Reset to default**

Once you have reorganized the home page to suite your needs you can click the **Save Changes** button to make your changes permanent. Clicking on the **Home** icon without clicking on **Save Changes** will cause your changes to be lost.

## General

There are no user configurable features in this tab.

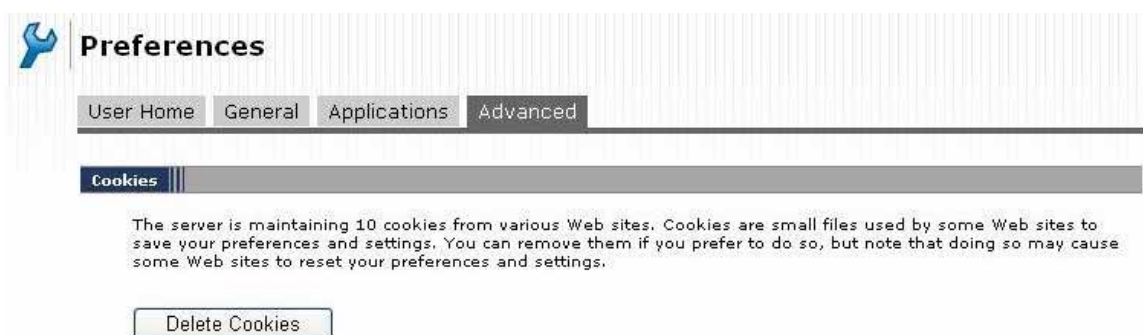
## Applications



The screenshot shows the 'Preferences' window with the 'Applications' tab selected. Under the 'Client Components' section, there are two items: 'Java Secure Application Manager' with a description 'This component secures selected client/server applications' and an '[Uninstall]' link, and 'Network Connect' with a description 'This component provides a secure network connection.' and an '[Uninstall]' link.

The Applications preferences screen is used to uninstall the JSAM and Network Connect software from the host computer. This operation is safe and the software will automatically reinstall the next time the functionality is used.

## Advanced



The screenshot shows the 'Preferences' window with the 'Advanced' tab selected. Under the 'Cookies' section, there is a text block: 'The server is maintaining 10 cookies from various Web sites. Cookies are small files used by some Web sites to save your preferences and settings. You can remove them if you prefer to do so, but note that doing so may cause some Web sites to reset your preferences and settings.' Below this text is a 'Delete Cookies' button.

Use this tab to delete cookies containing preferences and settings from visited Web sites. Clicking the **Delete Cookies** button will remove web cookies associated with your VPN account from the SSL vpn@UCSF system. This will not affect cookies on your computer.

# VPN Features

## Creating Bookmarks

### Creating Web Page Bookmarks



1. On the SSL vpn@UCSF home page, click the **Add a Bookmark**  icon in the title bar for the **Web Bookmarks** panel.

**Add Web Bookmark**

**Details**

Bookmark Name:

Description:

\* URL:  example: <http://www.example.com>

2. Enter the name you would like to use to identify the bookmark in the **Bookmark Name** field.
3. If you would like to display more information about the bookmark, you can fill out the optional **Description** field.
4. Enter the URL of the Web page in the **URL** field.

**Display options**

Open bookmark in a new window

Do not display the Web browser's URL address bar

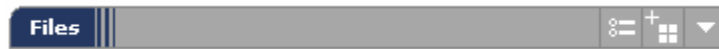
Do not display the Web browser's menu and the toolbar

Display as a favorite

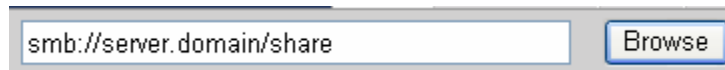
5. By default web bookmarks will open in the current web browser window replacing the vpn@UCSF home page. The **Display Options** section allows you to override this behavior.
  - o If you would like the link to open in a new window, select the **Open bookmark in a new window** option. It is recommended that you select this option so that the vpn@UCSF home page will be available to you to access other sites without leaving the current site. This is the behavior of all pre-defined web bookmarks.

- If you would like the URL input field in the web browser to be turned off select the **Do not display the URL address bar** option. It is recommended that you select this option so that you will not accidentally exit the vpn@UCSF system by typing a URL directly in to this window. This is the behavior of all pre-defined web bookmarks.
  - If you would like the menu and toolbars of the web browser to be turned off select the **Do not display the menu and the toolbar** option. This option is not utilized for the pre-defined web bookmarks, but is useful for the same reasons as the previous option.
  - You can make this link appear on the SSL vpn@UCSF mini-bar during web browsing sessions by selecting **Display as favorite**.
6. Click **Add Bookmark** to save the bookmark. The specified URL appears on the vpn@UCSF home page in the **Web Bookmarks** panel.

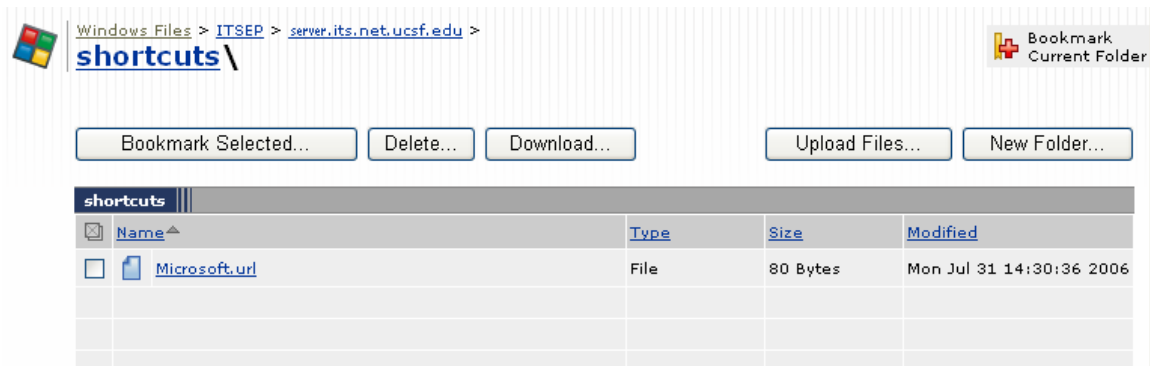
## Creating Files Links



1. On the SSL vpn@UCSF home page, enter the host name you wish to access in the browse service window and click **Browse**.



2. If prompted, enter your username and password to login to the server and click **Continue**.



3. Browse to the location on the remote file server you want to bookmark.
4. Click on the **Bookmark Current Folder** link in to top right hand view of the remote file system



## Add Windows Bookmark

[\server.its.net.ucsf.edu\shortcuts\](http://server.its.net.ucsf.edu/shortcuts/)

Bookmark Name:

Description:

Shared Folder:

5. If you would like the bookmark name to be something other than the URI to the resource enter it in the **Bookmark Name** field.
6. If you would like to display more information about the bookmark, you can fill out the optional **Description** field.
7. Do not change the information in the **Shared Folder** field.
8. Click on the **Add Bookmark** button.

## Creating Secure Shell (SSH) Terminal Sessions



1. On the SSL vpn@UCSF home page, click the **Add a Terminal Session**  icon on the title bar for the **Terminal Sessions** panel.



### Add Terminal Services Session

Session Type:

Bookmark Name:

Description:

2. Select **SSH Secure Shell** from the **Session Type** list.
3. Enter the name you would like to use to identify the bookmark in the **Bookmark Name** field
4. If you would like to display more information about the bookmark, you can fill out the optional **Description** field.

**Settings**

\* Host:  Name or IP address of remote host

\* Port:

\* Screen Size:  Size in characters and rows

\* Screen Buffer:  Number of rows retained for scrolling

\* Font Size:  Fixed Size of  pixels (Note that resizing requires Internet Explorer.)  
 Resize to fit window

5. In the **Settings** section:

- Specify the hostname or IP address of the terminal server in the **Host** field.
- The system will automatically populate the **Port** field with 22. If you need to connect to a non-standard port replace the existing value.
- From the **Screen Size** list, specify how large you want to make the SSH Secure Shell session window on your workstation.
- For **Screen Buffer**, specify the number of lines in the session you want to be able to scroll back through.
- For **Font Size**, select the size of the font you want to display in the SSH Secure Shell session window. You may have to test multiple text sizes to find the best size for your display and vision.

**Session**

**Authentication:**

Username:  Username or <USER> for IVE session username

6. In the **Session** section:

- a. If you will always use the same account name when connecting to this service you can enter that name in the **Username** field of the **Authentication** section, Leaving this field blank will cause the system to prompt you for a username at each launch of the SSH session.

7. Click Add

## Creating Telnet Terminal Sessions

**Terminal Sessions**

1. On the SSL vpn@UCSF home page, click the **Add a Terminal Session** icon on the title bar for the **Terminal Sessions** panel.



## Add Terminal Services Session

Session Type:

Bookmark Name:

Description:

2. Select **Telnet** from the **Session Type** list.
3. Enter a name and optionally a description for the session bookmark.

**Settings**

\* Host:  Name or IP address of remote host

\* Port:

\* Screen Size:  Size in characters and rows

\* Screen Buffer:  Number of rows retained for scrolling

\* Font Size:  Fixed Size of  pixels (Note that resizing requires Internet Explorer.)  
 Resize to fit window

4. In the **Settings** section:
  - a. Specify the hostname or IP address of the terminal server in the **Host** field.
  - b. The system will automatically populate the **Port** field with 23. If you need to connect to a non-standard port replace the existing value.
  - c. From the **Screen Size** list, specify how large you want to make the Telnet session window on your workstation.
  - d. For **Screen Buffer**, specify the number of rows in the session you want to be able to scroll.
  - e. For **Font Size**, select the size of the font you want to display in the SSH Secure Shell session window. You may have to test multiple text sizes to find the best size for your display and vision.

**Session**

**Authentication:**

Username:  Username or <USER> for IVE session username

5. In the **Session** section:
  - a. If you will always use the same account name when connecting to this service you can enter that name in the **Username** field of the **Authentication** section. Leaving this field blank will cause the system to prompt you for a username at each launch of the Telnet session.
6. Click Add

## Creating Window Remote Desktop Terminal Sessions

Terminal Services feature allows terminal emulation session on a Windows server. A *session* defines various information, including the server to which the user can connect, the terminal session's window parameters, and the username and password that the SSL vpn@UCSF system sends to the Windows server.

If a Remote Desktop Protocol (RDP) client is not already present on the user's system, the SSL vpn@UCSF system downloads one directly from the SSL vpn@UCSF system server. An *RDP client* is a Windows component that enables a connection between a Windows server and a user's machine, enabling the user to run an application on the Windows server while only transmitting keyboard, mouse, and display information over the network.



1. On the SSL vpn@UCSF home page, click the **Add a Terminal Session**  icon on the title bar for the **Terminal Sessions** panel.

A screenshot of the 'Add Terminal Services Session' form. The form has a title bar with a terminal icon and the text 'Add Terminal Services Session'. Below the title bar, there are three fields: 'Session Type' with a dropdown menu showing 'Windows Terminal Services', 'Bookmark Name' with a text input field containing 'Sample Terminal Session', and 'Description' with a large text area and a vertical scrollbar.

2. From the new screen, select “Windows Terminal Services” session from the **Session Type** pull down.
3. If you would like to display more information about the session, you can fill out the optional **Description** field

A screenshot of the 'Settings' form. The form has a title bar with the text 'Settings'. Below the title bar, there are five fields: '\* Host' with a text input field containing 'computername.domainname' and a tooltip 'Name or IP address of remote host'; 'Client Port' with an empty text input field and a tooltip 'If a client port is specified and the Juniper terminal services client is unable to bind to this port then the terminal services client will fail. However, if left blank, the Juniper terminal services client will dynamically select an available port.'; 'Server Port' with an empty text input field; 'Screen Size' with a dropdown menu showing 'Full Screen' and a tooltip 'Size in characters and rows'; and 'Color Depth' with a dropdown menu showing '16-bit'.

4. In the **Settings** section:
  - a. Specify the hostname or IP address of the terminal server in the **Host** field.
  - b. Leave the **Client Port** field blank.

- c. Leave the **Server Port** field blank for standard Windows Remote Desktop and Windows Terminal Server systems. If you are using a non-standard port enter that instead.
- d. Use the **Screen Size** pull down list to specify the size of the window you would like to open for the connection to the remote server (the smaller the screen the faster the connection, the larger the screen the more space you have to work in).
- e. Use the **Color Depth** pull down to specify what level of colors you want supported in the connection (the lower the number the faster the connection, but the higher the number the better the quality of the screen).

#### Session

##### Authentication:

Username:  Username or <USER> for IVE session username  
 Password:

##### Start Application:

Path to application:   
 Working directory:

##### Connect Devices:

Connect local drives

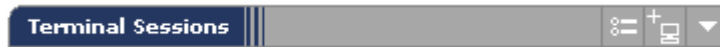
5. In the Session section:
- a. If you will always use the same account name when connecting to this service you can enter that name in the **Username** field of the **Authentication** section and the SSL vpn@UCSF system will fill out the username field in the login window automatically,
  - b. If you have specified a username in the **Username** section you can optionally enter the password for that username in the **Password** section, this will allow you to connect to the remote system and be automatically logged in. We recommend that you *do not* save your password in this screen.
  - c. If you want an application to be started automatically when you login to the remote system you can enter full path to the application in the **Path to application** field (e.g. C:\WINDOWS\EXPLORER.EXE).
  - d. If you have configured an application to start automatically after login by filling out the **Path to application** field you can also provide that application its current working directory by filling out the **Working directory** field (e.g. C:\My Documents).
  - e. If you would like to connect your local disks to the remote system you can select the **Connect local drives** option. This option should be used with caution as viruses on the remote system can use this to infect your local computer.


6. Click “add” on the bottom of page to return to the home page.

## Creating Citrix Metaframe Terminal Sessions

Citrix Services feature allows terminal emulation sessions on a Citrix Metaframe server. A *session* defines various information, including the server to which the user can connect, the terminal session’s window parameters, and the username and password that the SSL vpn@UCSF system sends to the Metaframe server.

If a Remote Desktop Protocol (RDP) client is not already present on the user’s system, the SSL vpn@UCSF system downloads one directly from the SSL vpn@UCSF system server. An *RDP client* is a Windows component that enables a connection between a Windows server and a user’s machine, enabling the user to run an application on the Windows server while only transmitting keyboard, mouse, and display information over the network.



1. On the SSL vpn@UCSF home page, click the **Add a Terminal Session**  icon on the title bar for the **Terminal Sessions** panel.

A screenshot of a web form titled "Add Terminal Services Session". The form has a light blue header with a computer icon and the title. Below the title are three input fields: "Session Type" with a dropdown menu showing "Citrix", "Bookmark Name" with a text box containing "Sample Citrix Session", and "Description" with a large empty text area and a vertical scrollbar.

2. From the new screen, select “Citrix” session from the **Session Type** pull down.
3. If you would like to display more information about the session, you can fill out the optional **Description** field

A screenshot of a web form titled "Settings". The form has a dark grey header with the text "Settings" in white. Below the header are several input fields and a text area: "\* Host:" with a text box containing "computername.domainname" and a tooltip "Name or IP address of remote host"; "Client Port:" with an empty text box and a tooltip "If a client port is specified and the Juniper terminal services client is unable to bind to this port then the terminal services client will fail. However, if left blank, the Juniper terminal services client will dynamically select an available port."; "Server Port:" with an empty text box; "Screen Size:" with a dropdown menu showing "Full Screen" and a tooltip "Size in characters and rows"; and "Color Depth:" with a dropdown menu showing "16-bit".

4. In the **Settings** section:
  - a. Specify the hostname or IP address of the terminal server in the **Host** field.

- b. Leave the **Client Port** field blank.
- c. Leave the **Server Port** field blank for standard Citrix Metaframe systems. If you are using a non-standard port enter that port number.
- d. Use the **Screen Size** pull down list to specify the size of the window you would like to open for the connection to the remote server (the smaller the screen the faster the connection, the larger the screen the more space you have to work in).
- e. Use the **Color Depth** pull down to specify what level of colors you want supported in the connection (the lower the number the faster the connection, but the higher the number the better the quality of the screen).

Session

**Authentication:**

Username:  Username or <USER> for IVE session username

Password:

**Start Application:**

Path to application

Working directory:

**Connect Devices:**

Connect local drives


5. In the Session section:
- a. If you will always use the same account name when connecting to this service you can enter that name in the **Username** field of the **Authentication** section and the SSL vpn@UCSF system will fill out the username field in the login window automatically,
  - b. If you have specified a username in the **Username** section you can optionally enter the password for that username in the **Password** section, this will allow you to connect to the remote system and be automatically logged in. We recommend that you *do not* save your password in this screen.
  - c. If you want an application to be started automatically when you login to the remote system you can enter full path to the application in the **Path to application** field (e.g. C:\WINDOWS\EXPLORER.EXE).
  - d. If you have configured an application to start automatically after login by filling out the **Path to application** field you can also provide that application its current working directory by filling out the **Working directory** field (e.g. C:\My Documents).
  - e. If you would like to connect your local disks to the remote system you can select the **Connect local drives** option. This option should be used with caution as viruses on the remote system can use this to infect your local computer.

6. Click “add” on the bottom of page to return to the home page.

## *Using Bookmarks, Links and Sessions*

### **How to use Web Bookmarks**

Web pages can be accessed through two different methods different :

- Clicking on the name of the bookmark will open the web page as it is configured to do in the preferences.
- Click the **Open in a New Window**  icon that appears to the right of the bookmark’s name to open the resource in a new browser window even if the preferences are set to open that site in the existing window.

### **How to use Files Links**

To view a remote shared file systems:

1. In the **Files** panel on the SSL vpn@UCSF home page, click the link for the network file system you access.
2. If prompted, enter the username and password you use to access the file system.
3. The file system will appear in your web browser window.

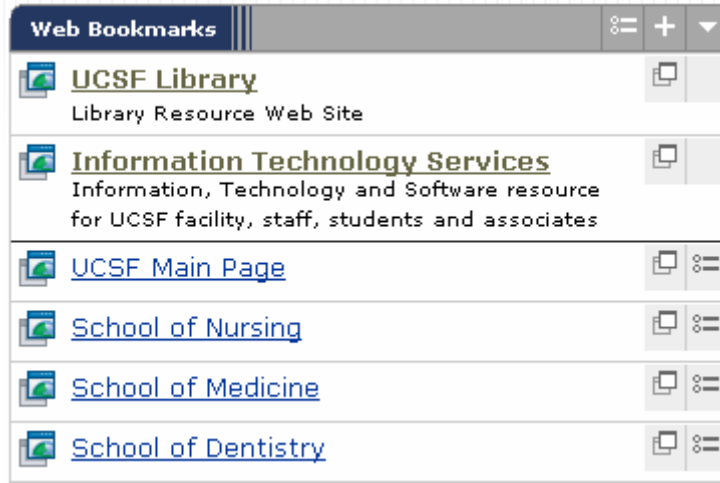
### **How to use Terminal Sessions**


All **Terminal Sessions** bookmarks are accessed the same way, whether they are SSH, Telnet, Windows RDP or Citrix. To start a terminal session:

1. In the **Terminal Sessions** panel on the SSL vpn@UCSF home page, click the link for the terminal session you want to start. A separate window will open and connect to the remote resource.
2. If prompted, login to the remote resource using the username and password you use to access that resource.

## Managing Bookmarks, Links and Sessions

### How to Edit a Web Bookmarks, File Links and Terminal Sessions



1. Click the **Item Properties**  icon next to the bookmark you want to modify

**Note:** Global items such as “UCSF Library” can not be edited.

2. Change the configuration as needed (see the Creating section for more information in the individual fields).
3. Click **Save Changes** to make your changes permanent.

### How to Change the Order of and Delete Web Bookmarks, File Links and Terminal Sessions



1. In the SSL vpn@UCSF home page, on the title bar of the section you would like to reorganize, click on the “Panel Preferences” button.

**Panel Preferences: Web Bookmarks**

Save Changes Cancel

**Bookmark Management**

Your Bookmarks

Move Up  
Move Down  
Sort by name  
Delete

UCSF Main Page  
School of Nursing  
School of Medicine  
School of Dentistry

**Options**

Display my web bookmarks before the permanent web bookmarks.

2. In the new screen, you will see a list of all the Bookmarks that you have defined.
3. To change the order of the bookmarks you have three options:
  - o Select a bookmark and move it up in the list by clicking on the **Move Up** button.
  - o Select a bookmark and move it down in the list by clicking on the **Move Down** button.
  - o Automatically sort the bookmarks by name by selecting the **Sort by name** button.
4. To permanently remove a bookmark you can select it and click on the **Delete** button.

5. If you would prefer that your bookmarks appear above the global bookmarks you can select the **Display my web bookmarks before the permanent web bookmarks** option.

# Traditional VPN Service with Network Connect

## What is Network Connect?

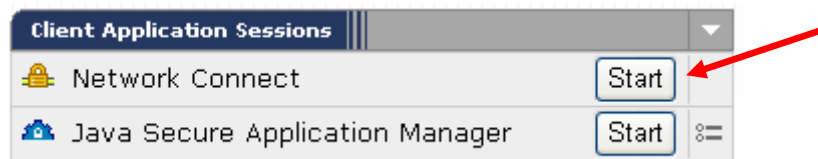
The Network Connect (NC) access option provides a Traditional VPN user experience to users of the SSL vpn@UCSF system. This feature supports all Internet-access modes, including dial-up, broadband, and LAN scenarios, from the client machine and works through client side proxies and firewalls that allow SSL traffic.

When Network Connect runs, the client's machine effectively becomes a node on the UCSF Computing Network; the SSL vpn@UCSF system appliance serves as the Domain Name Service (DNS) gateway for the client and knows nothing about the user's local LAN.

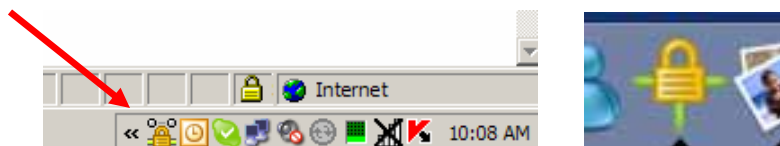
**Note:** NC cannot be used simultaneously with JSAM client. In many cases, NC cannot coexist with IPsec VPN clients that were previously installed on the system.

## Starting Network Connect

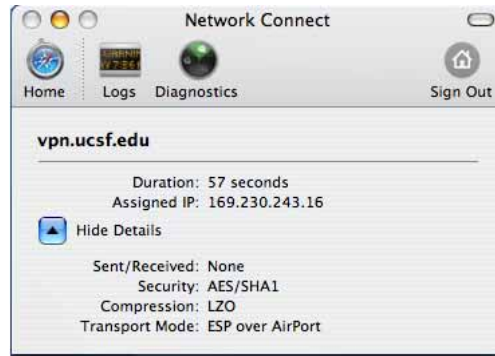
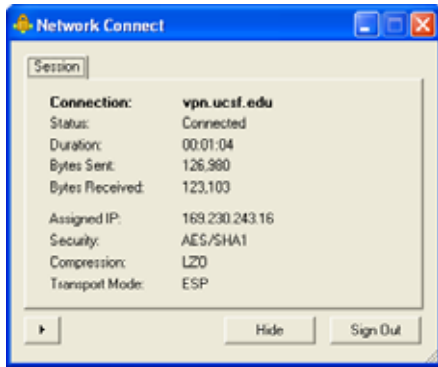
Network connect can be launched from the SSL vpn@UCSF home page or it can be launched directly from your computer from your Start menu (Windows) or Applications folder (MacOS X). The first time the application is used it must be launched from the home page.



1. Under "Client application Sessions" find Network Connect and click on "Start" to run the client. If this is the first time you are using the Network Connect client, it will take about 60 seconds for it to install. Respond to any pop ups displayed by your system.
2. Once Network Connect has been installed, it will show a brief status window that will show "connecting..."
3. When Network Connect has successfully established a VPN tunnel to the gateway, it will display the lock icon pictured below.



4. Once the Network Connect VPN is established, a user can open a browser and/or application client and access the internal resource(s) as if they were connected locally on the UCSF network.



5. You can locate more information on the current open connection by double clicking on the Network Connect icon in your Windows toolbar or MacOS X dock.
6. To close the connection you can right click on the icon and choose **Sign Out** or click on the **Sign Out** button on the information screen.

## Appendix I – Supported Platforms

This appendix includes two lists, the first list are the platforms which the UCSF Office of Academic and Administrative Information Systems group provides support, the second list has been provided by Juniper Networks and iterates the platforms for which they have tested the SSL vpn@UCSF system.

***Please note:** This appendix specifically references specific versions of software, for example Firefox 1.0. When this is the case, newer versions of the software may not be compatible with the SSL vpn@UCSF system and are not supported.*

### *UCSF Supported Platforms*

The UCSF OAAIS customer support team supports the use of SSL vpn@UCSF system with the following platforms

- MacOS X 10.2.8<sup>1</sup>
  - Safari 1.0 with Sun JVM v1.4.1\_01
- MacOS X 10.3.7
  - Safari 1.1 and above with Sun JVM v1.4.2\_04
- MacOS X 10.4
  - Safari 2.0 with Sun JVM v1.4.2\_07
- Windows 2000
  - Firefox 1.0 Sun JVM v1.5.0\_03
  - Internet Explorer 6.0 Sun JVM v1.4.2\_04
- Windows 98SE / ME
  - Internet Explorer 6.0 with Sun JVM v1.4.2\_04
- Windows XP SP2
  - Firefox 1.0 Sun JVM v1.5.0\_03
  - Internet Explorer 6.0 with Sun JVM v1.4.2\_04

---

<sup>1</sup> Please note that some functionality is not supported on the Macintosh platform; this functionality is clearly labeled “Windows clients only” in the documentation.

# SSL vpn@UCSF System Supported Platforms

## Defining Included Terms

### What does “Supported” mean?

A supported platform is one on which a functionality has been tested in depth and verified as functioning correctly. Supported platforms are listed as **S** in the Supported Platforms Matrix.

### What does “Compatible” mean?

A compatible platform is one on which the base feature set of a functionality has been tested and verified as functioning correctly. Compatible platforms are listed as **C** in the Supported Platforms Matrix.

## Multiple Language Support

All the end-user functionality is supported in German, French, Japanese, Traditional Chinese, Simplified Chinese, Spanish, and Korean.

Note: OAAIS documentation is only available in English.

## Note on Java

The minimum version of Java supported by the SSL vpn@UCSF system is Sun JVM v1.4.2\_04, newer versions may be required depending on the application, web browser and platform.

Use of some newer open source web browsers requires a minimum Sun JVM of v1.5.0\_03.

## Supported Platforms Matrix

Platform	Web and Files	Remote Desktop	Citrix Terminal	SSH	Telnet	JSAM	Network Connect
<b>Windows 2000</b>							
Firefox 1.0	<b>S</b>	<b>S</b>	<b>S</b>	<b>S</b>	<b>S</b>	<b>S</b>	<b>S</b>
IE 6.0	<b>S</b>	<b>S</b>	<b>S</b>	<b>S</b>	<b>S</b>	<b>S</b>	<b>S</b>
Netscape 7.1	<b>C</b>			<b>S</b>	<b>S</b>	<b>S</b>	
Netscape 8.0	<b>C</b>			<b>C</b>	<b>C</b>	<b>C</b>	
<b>Windows 98SE</b>							
IE 6.0	<b>S</b>	<b>S</b>		<b>C</b>	<b>C</b>		<b>S</b>
Netscape 4.79	<b>S</b>						
<b>Windows XP SP2</b>							
AOL 8.0	<b>C</b>						
Firefox 1.0	<b>S</b>	<b>S</b>	<b>S</b>	<b>S</b>	<b>S</b>	<b>S</b>	<b>S</b>
IE 6.0	<b>S</b>	<b>S</b>	<b>S</b>	<b>S</b>	<b>S</b>	<b>S</b>	<b>S</b>
<b>MacOS X 10.4 PPC</b>							
Safari 2.0	<b>S</b>			<b>S</b>	<b>S</b>	<b>S</b>	<b>S</b>

<b>MacOS X 10.4 Intel</b>							
Safari 2.0	<b>S</b>						
<b>MacOS X 10.3.7</b>							
Safari 1.1 +	<b>S</b>			<b>S</b>	<b>S</b>	<b>S</b>	<b>S</b>
<b>MacOS X 10.2.8</b>							
Safari 1.0	<b>S</b>			<b>S</b>	<b>S</b>	<b>S</b>	<b>S</b>
Safari 1.1	<b>C</b>			<b>C</b>	<b>C</b>	<b>C</b>	<b>S</b>
<b>MacOS 9.2</b>							
IE 5.1.5	<b>C</b>						
Netscape 4.7.9	<b>C</b>						
<b>RedHat Linux 9.0</b>							
Firefox 1.0	<b>C</b>			<b>C</b>	<b>C</b>	<b>C</b>	<b>S</b>
Mozilla 1.6	<b>S</b>			<b>S</b>	<b>S</b>	<b>S</b>	
Netscape 7.1	<b>C</b>			<b>C</b>	<b>C</b>	<b>C</b>	
<b>Suse Linux 9.3</b>							
Firefox 1.0	<b>S</b>			<b>S</b>	<b>S</b>	<b>S</b>	<b>S</b>
<b>Solaris 8/9</b>							
Mozilla 1.4	<b>C</b>					<b>C</b>	

## Notes for JSAM and Platform Support

For host name mapping to work, your local system account must have Administrative or root level access or you will have to manually use the local IP address assigned to the connection. For more information on this please review the documentation on using JSAM.

## Notes for Mobile Devices

The following mobile devices are supported for Web browsing functionality.

- Windows Mobile 2003 Based Pocket PCs and Mobile Phones using Pocket IE 2003
- NTT DoCoMo i-mode Phone
- AU/KDDI Phone: Openwave Mobile Browser
- Vodafone Phone: Openwave Mobile Browser

The following mobile devices are compatible for Web Browsing functionality.

- Sony Ericsson P910 with Symbian OS 7.1: Opera Web Browser 6.31
- Treo 600 with Palm OS 5.2.1: Blazer Web Browser 3.0

## Getting Support

The first step in troubleshooting problems accessing or using the SSL vpn@UCSF system is to review the SSL vpn@UCSF Technical FAQ available at <http://its.ucsf.edu/information/network/vpn/ssl/sslfaq.jsp>

If you do not find the solution to the issue you are experiencing you can contact your support professional:

**Students:** Call ITS Customer Support at 514-4100, option 2, or send email to [itscs@its.ucsf.edu](mailto:itscs@its.ucsf.edu).

**Campus Faculty & Staff and Associates:** Contact your Department's Computer Support Coordinator (CSC).

**Vendors and Contractors:** Please direct questions to your Departmental Contact.

## Appendix II – Information about Java on Windows

The SSL vpn@UCSF service works better with the Sun Java software; problems with the Microsoft Java software include certificate errors and browser crashes. If you are running an old version of Sun Java or are running Microsoft Java it is recommended that you upgrade to the latest version of Sun Java.

### *What version of Java am I running?*

#### **Web Java Test**

The OAAIS web site provides a quick test to verify the version of Java currently in use by your web browser, it is recommended that you utilize that service before continuing with this document

<http://its.ucsf.edu/information/network/vpn/test/>

#### **Microsoft Java Virtual Machine (JVM)**

If you are running the Windows 95, 98, ME, or 2000 operating system or have upgraded your machine to Windows® XP from one of those operating systems, your PC already has the Microsoft JVM. If your PC was shipped with the Windows XP operating system, you may not have the MS JVM.

To determine if your PC has the MS JVM:

1. Click on the **Start** menu button
2. Click on the **Run...** menu option
3. Type cmd in the dialog box and click **OK** (if cmd produces an error try command instead)
4. In the window that opens type jview and press enter.

The Microsoft JVM is installed on your computer if you see the jview command's usage text and command options. The Microsoft JVM is not installed on your computer if "jview" is not recognized as a valid command.

If you see an error similar to the following:

```
C:\>jview
'jview' is not recognized as an internal or external command,
operable program or batch file
```

Then the Microsoft JVM is not installed on your computer.

#### **Sun Java Virtual Machine (JVM)**

Many versions of Windows do not include Java as part of the install and it is installed by one of the web browsers when it is needed, other times Java is pre-installed by the computer manufacturer or a support department. Usually when this is the case Sun Java is installed.

To determine if your PC has the Sun JVM:

5. Click on the **Start** menu button
6. Click on the **Run...** menu option
7. Type `cmd` in the dialog box and click **OK** (if `cmd` produces an error try `command` instead)
8. In the window that opens type `java -version` and press enter.

If Java is installed on your system you should see a dialog similar to the following:

```
C:\>java -version
java version "1.5.0_07"
Java(TM) 2 Runtime Environment, Standard Edition (build 1.5.0_07-b03)
Java HotSpot(TM) Client VM (build 1.5.0_07-b03, mixed mode, sharing)
```

If Java is not installed on your system you will see an error similar to the following:

```
C:\>jview
'jview' is not recognized as an internal or external command,
operable program or batch file
```

Then the Java is not installed on your computer.

## *How to Install the Sun JVM*

**To** install the Sun JVM on a Windows PC you must first download the installation application for the Java Runtime Environment (JRE) from <http://java.sun.com/j2se/>. (You do not need to download the Software Development Kit (SDK) or the J2SE which contains the SDK).

Note: You will need Administrator or Power User privileges to install Java.

To install the Sun JVM:

1. Download the JRE application from <http://java.sun.com/j2se/>.
2. Double-click the executable file, which ends with `.exe`, within the download.
3. Follow the on-screen instructions.

## *How to Set the Default JVM for Your Browser*

When Sun's JVM is installed on a Windows PC, it becomes the default JVM for Internet Explorer. This setting occurs even if Microsoft's JVM is already installed. You can control which virtual machine is used by the browser through the Control Panel. If Microsoft Java becomes the default JVM you will need to follow these steps to switch your web browser back to Sun JVM.

## Windows XP and 2003 Server

When using Internet Explorer on the Windows XP and Windows 2003 Server operating systems, ensure that the Sun JVM is enabled on your system before following these steps:

1. Launch an Internet Explorer browser window.
2. Select the **Tools** menu and choose **Internet Options**.
3. Select the **Advanced** tab.
4. Scroll to the **Java (Sun)** section. A check mark in the checkbox next to the **Use Java 2 vx.x.x for <applet>** option denotes that Internet Explorer is using the Sun JVM. If no check mark appears, select the checkbox to enable the Sun JVM.
5. Click the **OK** button to save your changes
6. If you enabled the Sun JVM you need to restart your system before the changes take effect.

## Windows 98, 98SE, ME and NT (Server and Workstation)

1. Close all open web browser windows (logout of the SSL vpn@UCSF service if you are currently connected).
2. From the **Start** menu, choose **Control Panel**.
3. Open the Java Plug-In Control Panel
  - a. If you are using version 1.4.1 of the Sun JVM, from the **Control Panel** window, choose **Other Control Panel Options**. Under **Pick a Control Panel** icon, double-click **Java Plug-in** to launch the **Java Plug-in Control Panel**.
  - b. If you are using version 1.4.2 or newer of the Sun JVM: From the **Control Panel** window, choose **Java Plug-in** to launch the **Java Plug-in Control Panel**. Note that if you do not see the Java Plug-in control panel, then your PC does not have the Sun JVM and you do not need to continue.
4. In the **Java Plug-in Control Panel**, click the **Browser** tab and then:
5. Uncheck **Microsoft Internet Explorer** to stop using the Microsoft JVM as the default for Internet Explorer.
6. Check **Microsoft Internet Explorer** to start using the Sun JVM as the default for Internet Explorer.
7. Click **Apply**, and when the confirmation dialog opens, click **OK**.
8. Re-launch your browser and connect to the SSL vpn@UCSF.

## Appendix III – Information about Java on MacOS X

If you are using a Macintosh computer, the SSL vpn@UCSF is supported by OAAIS for use with MacOS X v10.2 and above with the Safari browser.

### *What version of Java am I running?*

#### **Web Java Test**

The OAAIS web site provides a quick test to verify the version of Java currently in use by your web browser, it is recommended that you utilize that service before continuing with this document

<http://its.ucsf.edu/information/network/vpn/test/>

#### **Sun Java Virtual Machine (JVM)**

To determine if your machine has the Sun JVM:

1. Launch the Safari browser.
2. From the **Help** menu, choose **Installed Plug-ins**.
3. Look for the Java plug-in icon. Note that you may have Java 1.3.1, but make sure that you also have at least Java 1.4.1. If you do not have the plug-in, then you need to install it.

### *Installing or Upgrading Java on MacOS X v10.4*

If you are running the current version of MacOS X from Apple your version of Java should be kept up to date automatically by the Software Update service. If you have not run Software Update recently it is strongly recommended that you do so.

Using MacOS X Software Update

1. From the **Apple** menu, choose **System Preferences**.
2. From the **View** menu, choose **Software Update**.
3. Click **Update Now**.
4. Enter an administrator user name and password.

### *Installing or Upgrading Java on MacOS X v10.2*

MacOS v10.2.x does not automatically update Java past version 1.3, Java version 1.4.1 is required for use with the SSL vpn@UCSF system. To download a newer version of Java from Apple please follow these instructions:

1. Launch Safari and go the following site:

<http://www.apple.com/downloads/macosx/apple/java141updateformacosx.html>

2. Download the Java 1.4.1 update to your computer
3. Run the software installer, the account running the installer must have administrative privileges to the computer.
4. Follow the instructions included in the dialog.
5. A reboot is recommended after installing or upgrading Java
6. Re-launch Safari and connect to the SSL vpn@UCSF.

### *Installing or Upgrading Java on MacOS X v10.3*

MacOS v10.3.x does not automatically update Java past version 1.3, Java version 1.4.1 is required for use with the SSL vpn@UCSF system but to access fully functionality version 1.4.2 is required. To download a newer version of Java from Apple please follow these instructions:

1. Launch Safari and go the following site:  
`http://www.apple.com/downloads/macosx/apple/javaupdate142update1.html`
2. Download the Java 1.4.1 update to your computer
3. Run the software installer, the account running the installer must have administrative privileges to the computer.
4. Follow the instructions included in the dialog.
5. A reboot is recommended after installing or upgrading Java
6. Re-launch Safari and connect to the SSL vpn@UCSF.

## Appendix IV – Information about Java on Linux

If you are running Linux, the SSL vpn@UCSF works with Netscape 7 and Mozilla 0.9.9.

### *What version of Java am I running?*

#### **Web Java Test**

The OAAIS web site provides a quick test to verify the version of Java currently in use by your web browser; it is recommended that you utilize that service before continuing with this document

<http://its.ucsf.edu/information/network/vpn/test/>

#### **Sun Java Virtual Machine (JVM)**

To determine if your machine has the Sun JVM:

1. Launch your browser.
2. From the **Help** menu, select **About Plug-ins**.
3. Look for the Java plug-in icon. If you do not have the plug-in, then you need to install it.

### *Installing or Upgrading Java on Linux*

To install applications on a Linux machine, you need to log in to your machine as root. Note that the SSL vpn@UCSF works with Netscape 7 and Mozilla 0.9.9.

To install the Sun JVM:

1. From the Sun site (<http://java.sun.com/j2se/>) download either the:
  - a. Linux RPM for RedHat or
  - b. GNUZIP/Tar (for other Linux platforms) for the JRE file

Note: Make sure that you download the GNUZIP/Tar script to the directory where you want to install the Java Plug-in, such as: /usr/local

2. Run the downloaded executable or extract the archive per the instructions provided by Sun Microsystems.

Create a symbolic link from the browser's plug-in directory to the installed Java library: libjavaplugin\_oji.so per the included readme.txt document.