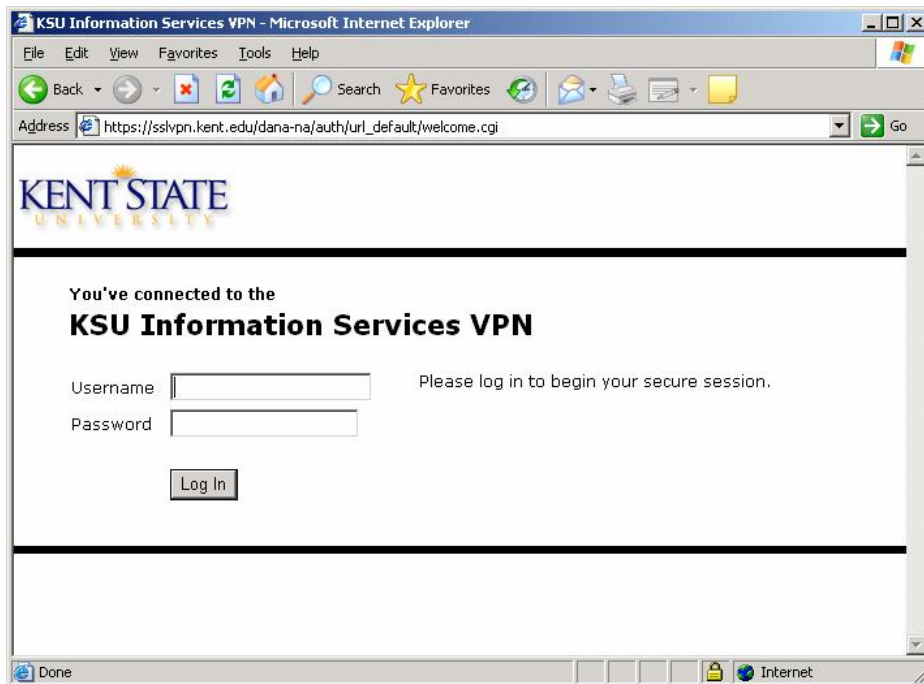


## HOWTO: SSL VPN Encrypted Mainframe TN3270 Sessions

Due to regulations concerning the exposure of sensitive personal data, remote access to mainframe applications through TN3270 sessions must be protected with data encryption. This applies to any session on or off campus that involves data transport over the network.

### Step 1: Log in to the SSLVPN server

- Open a compatible web-browser (Internet Explorer 4.0+, Netscape 6+, Firefox or Safari) on your PC and open the URL <http://sslvpn.kent.edu>.

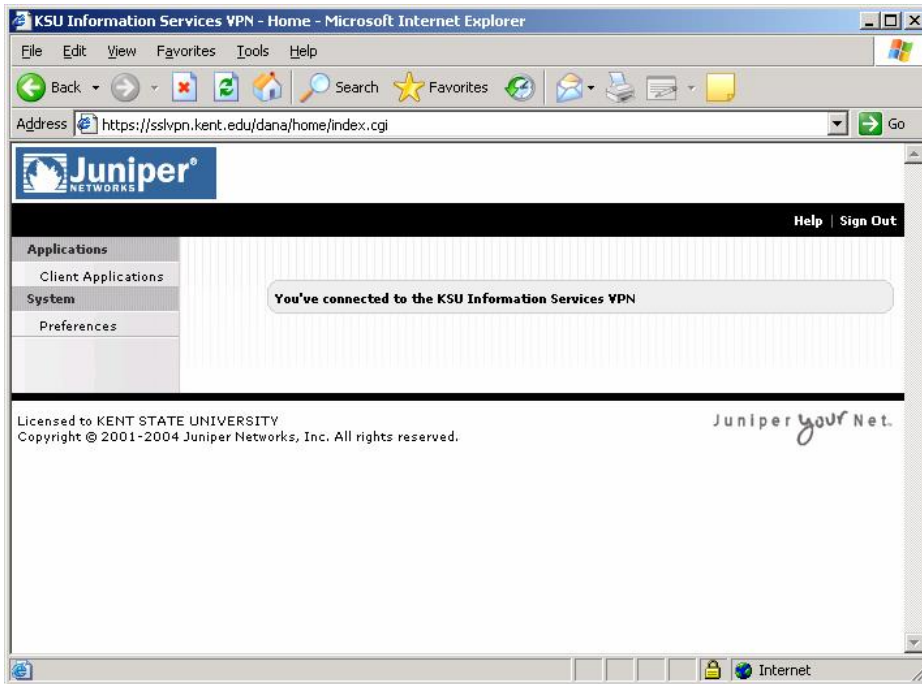


- Enter your Flashline username and password then click on the "Sign In" button.

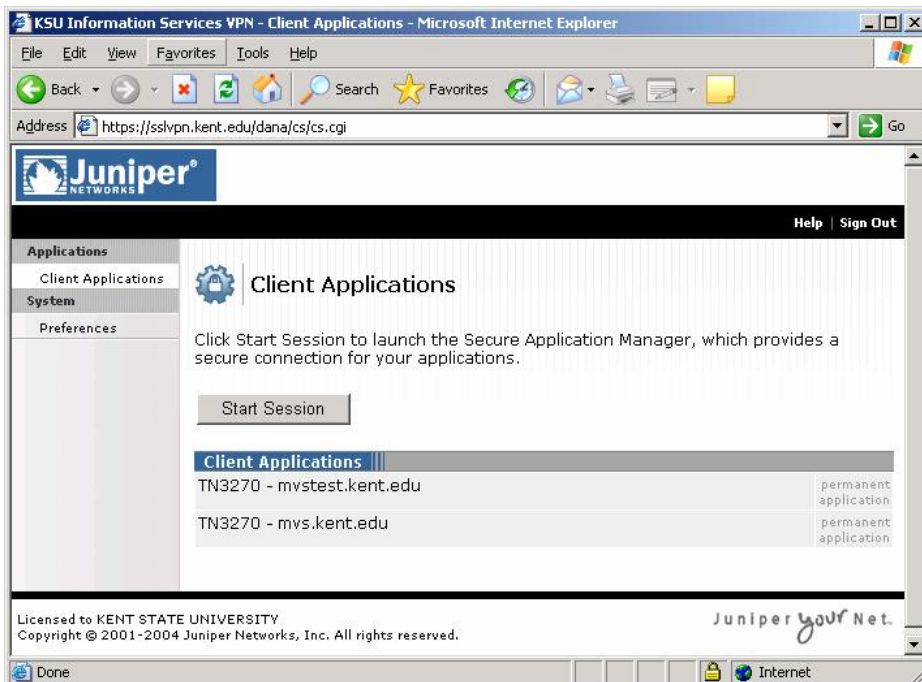
### **Note:**

If you encounter problems logging into the SSLVPN for the first time, your password may not be set properly. Visit <http://flashword.kent.edu> and set a new password with at least 9 characters, then attempt to log in again. If the problem persists, contact the helpdesk (x24357).

## Step 2: Start the SSL VPN client



- In the left hand menu, under Applications, click on the link for Client Applications.



- Click on the Start Session button.

**Note:**

If this is the first time you've used the SSL VPN on your PC, or you've recently installed an upgrade, you may be asked whether you'd like to install software from Juniper Networks. This is the VPN server attempting to install the VPN client software on your PC. You should accept the software download.

- A small window will appear momentarily. It may first say "Loading...Please Wait", but after no more than about 30 seconds, it should be replaced with the status of your VPN connection. Once the VPN client is fully functional, the window will automatically hide itself in your task bar. It will be identified as "DO NOT CLOSE – Secure Application Manager" or "https://sslvpn.kent.edu - DO NOT CLOSE - Secure Application Manager".



**Note:**

If Windows Firewall is enabled on your PC, a Windows Security Alert window **may** pop-up.



Click on the "Unblock" button.

- It is safe to close the "KSU Information Services VPN" browser window at this time. Your VPN session will continue to function as long as the "DO NOT CLOSE – Secure Application Manager" window remains open.

**Step 3: Use your TN3270 application software**

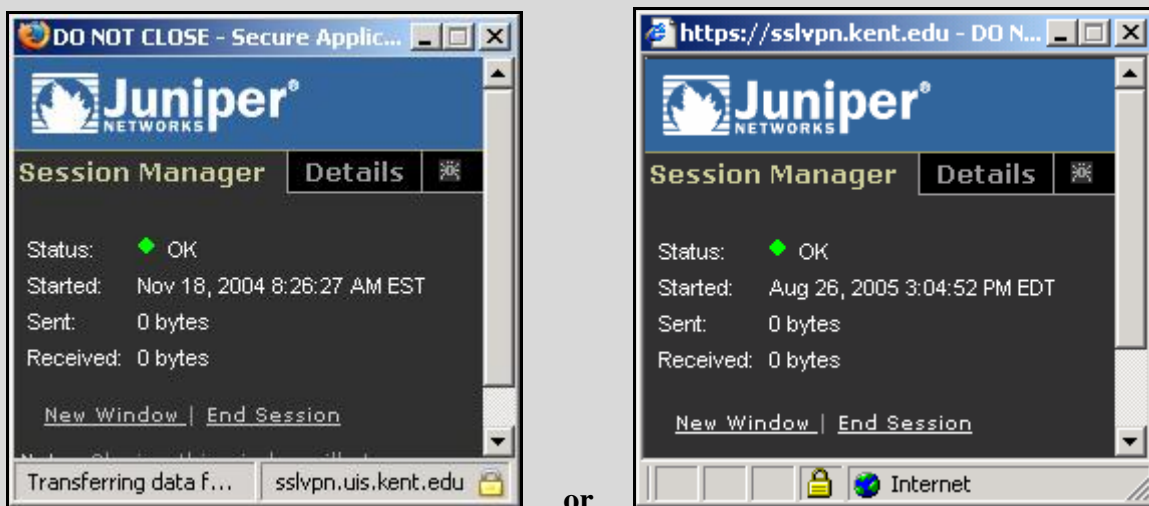
- Start your TN3270 client (QWS or Attachmate), and then log into the mainframe as you normally would.

**Note:**

You can verify the status of the VPN client by clicking on its button in the Windows task manager (*usually* at the bottom of your screen). The button will look similar to this:



The VPN client window looks like this:

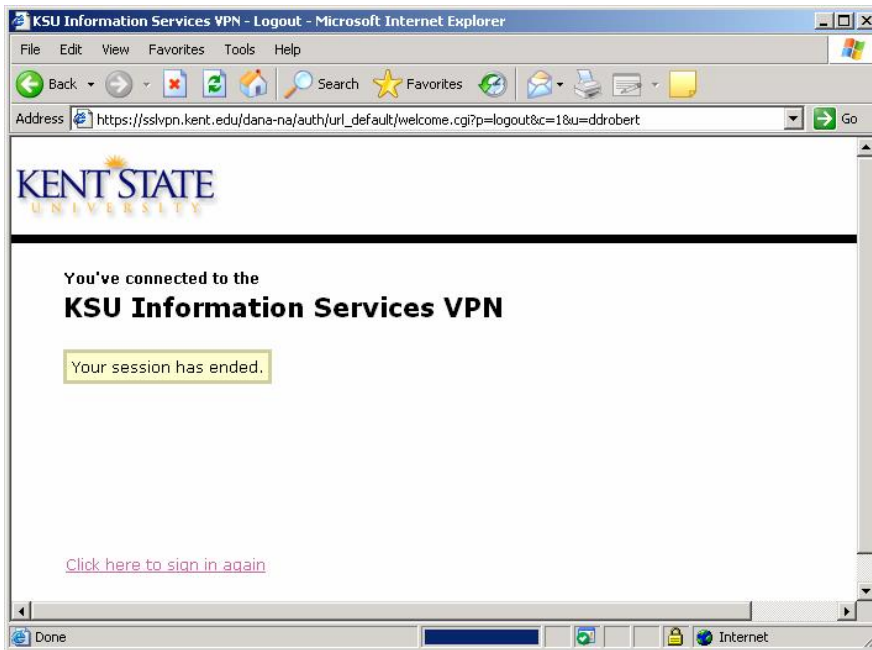


If the "Status:" indicator says "OK", then the VPN client should be functioning properly.

If a message of any kind appears in the space between the "Session Manager" tab and the "Status:" indicator, contact the help desk for assistance.

#### Step 4: Sign out

- When you are finished with your mainframe session, log out of the mainframe and close your TN3270 client as you normally would.
- **If you left your "KSU Information Services VPN" web page open:** Click on the "Sign out" button in the upper right hand corner of the web page.



- **If you no longer have the "KSU Information Services VPN" web page open:** Click on the VPN client's button in the task manager (it's the one that labeled "DO NOT CLOSE – Secure Application Manager"). In the VPN client window, click on "End Session", then click OK on the subsequent warning message window.

