

Feature Article

WebVPN

April 2007

Virtual Private Networks (VPNs) allow for secure communication to internal resources from external locations. Most VPNs require software to be installed on the client machine that is making the connection into the network. This software limits the mobility of the VPN, because you must have administrator rights to install the VPN software on the client machine. WebVPN represents a new technology allowing for secure communication to be established over the Internet through a web browser. Today, most machines have an Internet browser installed by default. The one requirement of WebVPN for basic functionality is that the browser be equipped to handle Secure Socket Layer encryption, SSL. Another benefit is the broad array of platforms and browsers that are compatible with it. Since WebVPN is simply secure web traffic, it is virtually platform and browser independent. There are a couple types of access that can be achieved in WebVPN such as clientless WebVPN and Thin-Client WebVPN.

For clientless WebVPN, simply open any SSL capable browser, surf to the WebVPN IP address, login, and you are ready. With clientless WebVPN, once you login, you are limited to strictly web and secure web traffic. This solution is perfect for secure remote access to internal web servers containing important data. Also, the risk for transmitting viruses from external machines to internal machines is greatly reduced because of the limited types of access.

Thin-Client WebVPN uses a simple Java applet to map local machine TCP ports to remote machine TCP ports. First, the client machine must have Java installed, which is freely available from <http://java.com/en/>. Once installed, simply connect to the WebVPN IP address and a new window will appear which will need to install a Java applet. Once the applet installs, port-forwarding features are now enabled. This option is perfect for securely taking remote control of an internal machine from an external machine. From this internal machine it could be possible to manage the entire internal network. Again, because only certain ports are allowed access through the VPN, and they are mapped to another port on the inside, the risk for spreading malware and viruses is greatly reduced.

There are several great benefits to all types of WebVPN. For example, it allows secure access to internal web servers without having to put those servers directly on the Internet. This prevents many types of attacks simply because the machine is not exposed to the Internet. Also, WebVPN can list only certain internal servers for different users. So it would be possible for financial people to have access to the finance server, for database users to have access to the database, and for everyone to have access to the intranet web server. One of the biggest advantages of WebVPN is that there is no need to install VPN software on either the client or the server machines. This makes it very portable, and easy to use. However, with this increased portability, users will have to be more vigilant about what machines they log in from. If, for instance, a user logs in at a public library and that public machine has been hacked and now records all keystrokes, then that user will unknowingly give away their login and password. The risk for losing a login and password is the same, as it would be, doing online banking from anywhere. Using access to online banking, as a guideline, should keep most WebVPN connected networks safe. Another convenience of WebVPN is the ability to tie into the internal local authentication server, so users can log into WebVPN using the same username and password they use for email. This allows for less user confusion and simpler user setup. These are some of the great advantages of WebVPN.

Clientless WebVPN Example:

Step 1: Open a web browser and go to <http://webvpn.asc.edu>

This will open the page displayed in **Figure 1**.

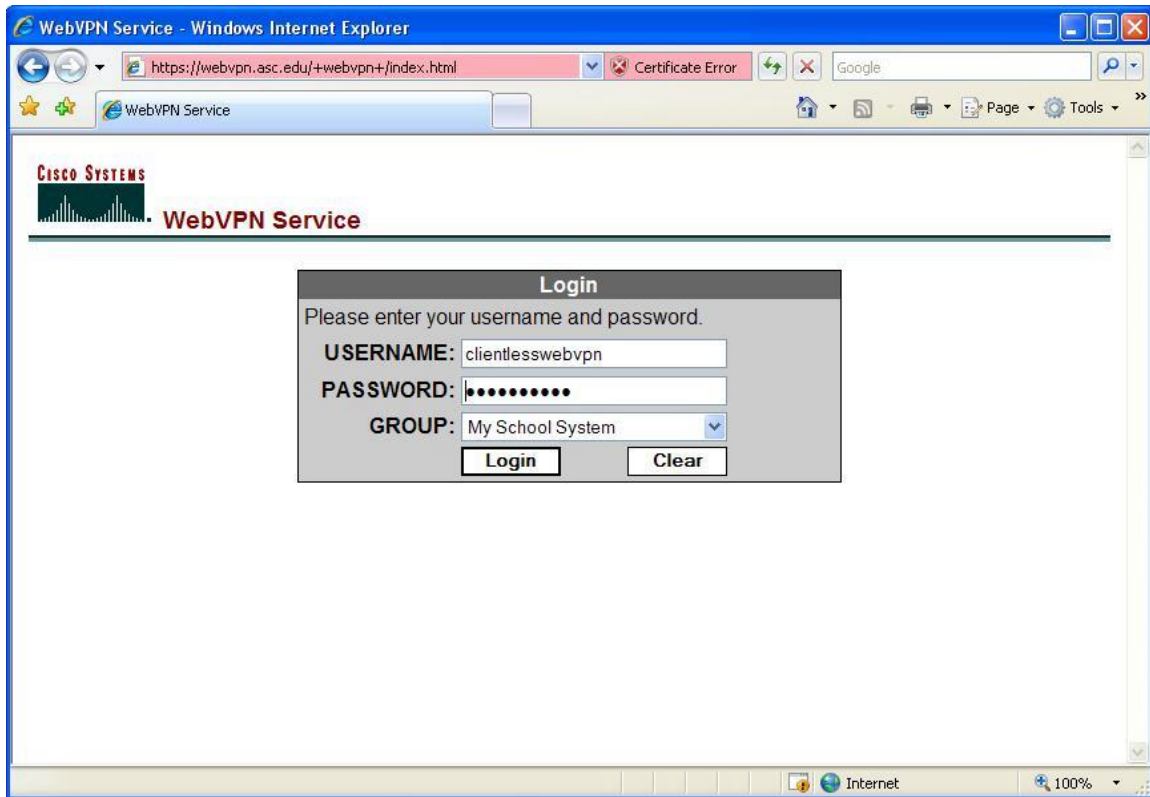


Figure 1: WebVPN Login

Step 2: Enter the username "clientlesswebvpn" and password "webvpntest", choose the group "My School System", and then click the "Login" button.

This takes you to your user's WebVPN homepage, which can be set directly to an internal web server, or can list all available WebVPN resources like the one shown in **Figure 2**.

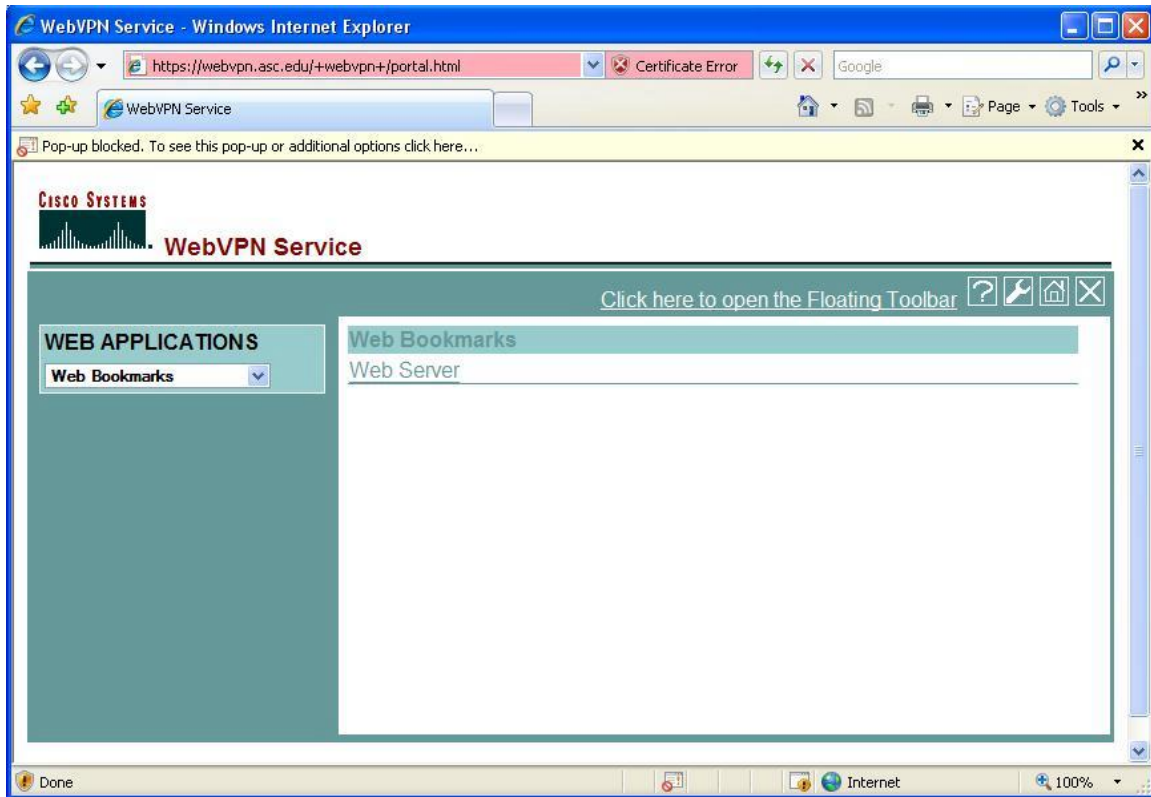


Figure 2: Clientless WebVPN Homepage

The homepage lists all access that can be obtained via this WebVPN account. Notice that the pop-up blocker is enabled. This prevents the toolbar window from appearing. The toolbar window can be accessed by clicking the wrench icon in the top right corner of the homepage. The toolbar is simply a pop-up window containing the information presented on the left-hand navigation bar of the homepage. Here, there is only web access to the device called "Web Server." Clicking either on the link "Web Server" or selecting "Web Server" from the drop-down list under "Web Applications" opens the "Web Server" link. Figure 3 verifies that the connection through WebVPN is successful to the internal web server.

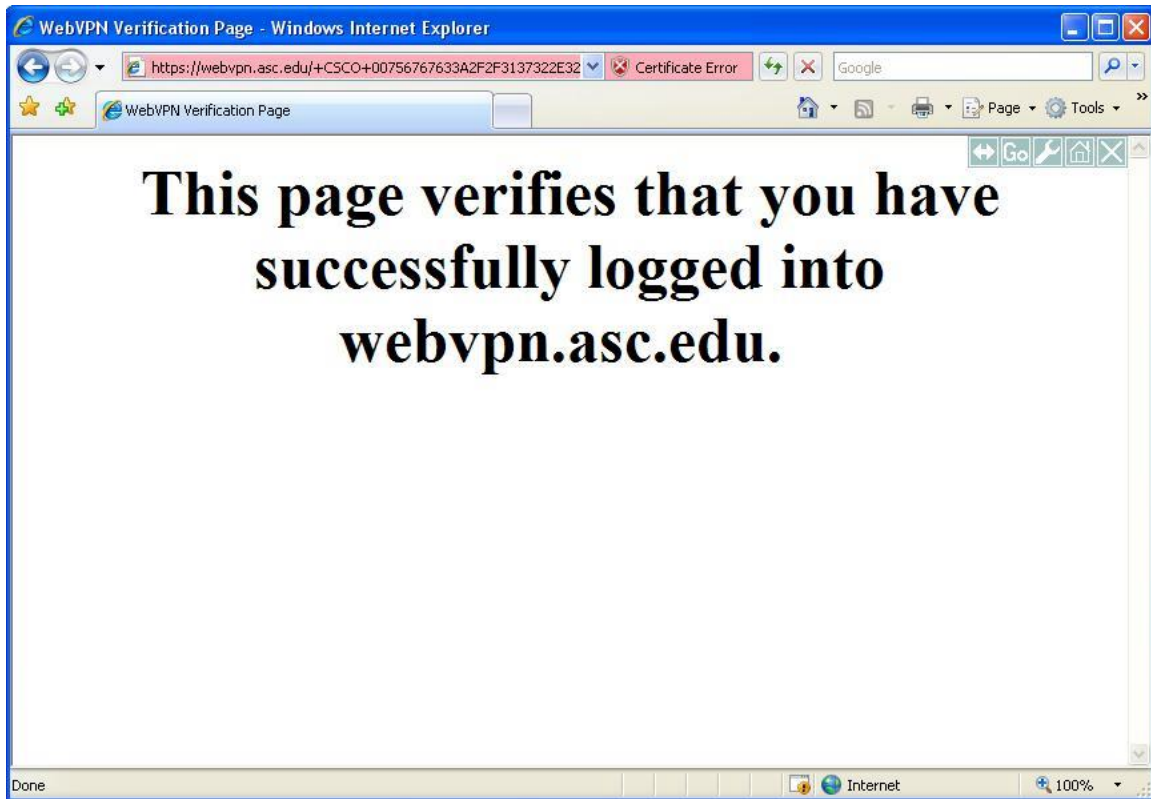


Figure 3: Web Server's Default Web Page

This page is located on the "Web Server" machine and linked from the WebVPN homepage. Notice the toolbar in the top right of the webpage. This is the WebVPN toolbar. Clicking the home icon will return the session to the home page. To exit the WebVPN connection, simply click the "X" icon in the top right of the page. Closing the WebVPN homepage with the browser's close option will cause the WebVPN service to close incorrectly and that session will not complete until after it times out.

Java-enabled WebVPN Example:

Step 1: Open a web browser and go to <http://webvpn.asc.edu>

This will open the page displayed in **Figure 4**.

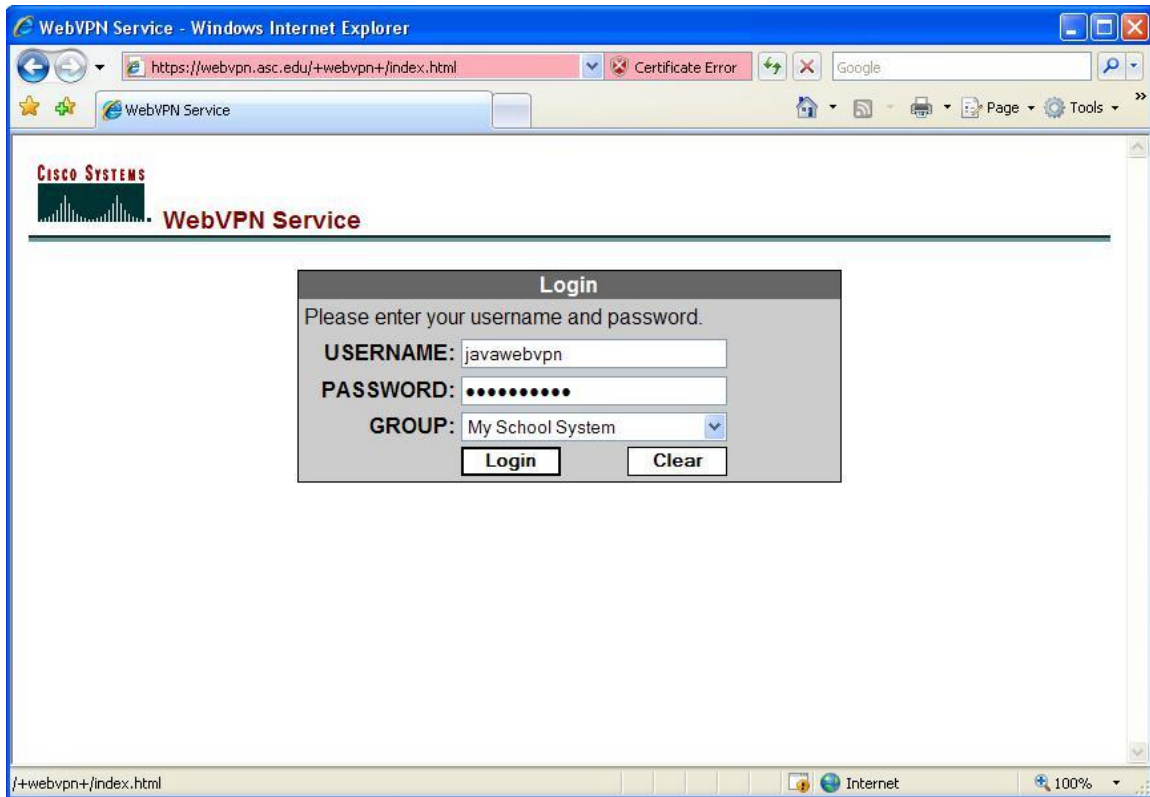


Figure 4: WebVPN Login

Step 2: Enter the username "javawebvpn" and password "webvpntest", choose the group "My School System", and then click the "Login" button.

This takes you to your user's WebVPN homepage, which lists all available WebVPN resources like the one shown in **Figure 5**.

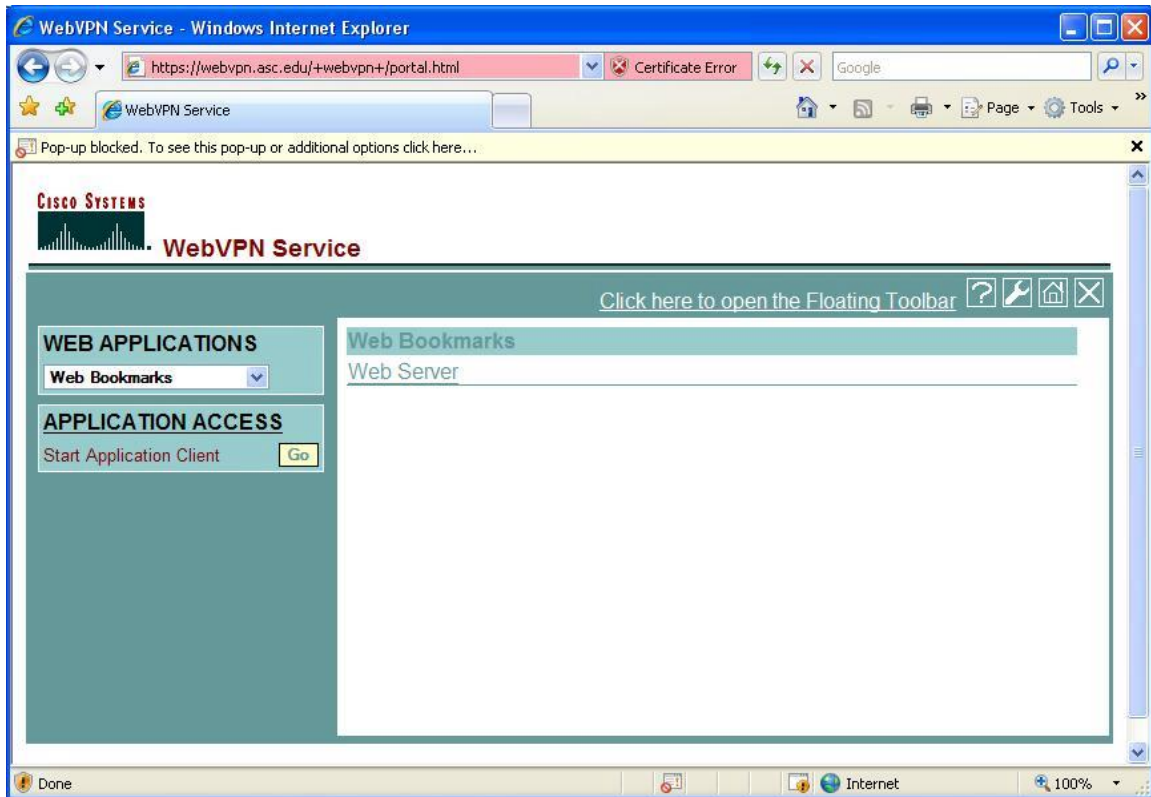


Figure 5: Java-Enabled WebVPN Homepage

The homepage lists all access that can be obtained via this WebVPN account. Notice again that the pop-up blocker is enabled. Also, there is still web access to the device called "Web Server." However, there is also a link to "Application Access." Clicking either on the link "Application Access" or the "Go" button below it will open the Java "Application Access" window seen in **Figure 6**.



Figure 6: Java Application Access Window

If the Java logo does not appear in the white part of the window, that means Java is not installed and must be downloaded and installed from <http://java.com/en/>. If the Java logo appears, as shown above, the Java applet will attempt to download and install automatically. Depending on the security of the machine, a verification window, such as the one featured in **Figure 7** may appear.



Figure 7: Windows Warning

Simply click "Run" and this will install the Java applet. Once installed, the Java "Application Access" windows should now look like **Figure 8**.

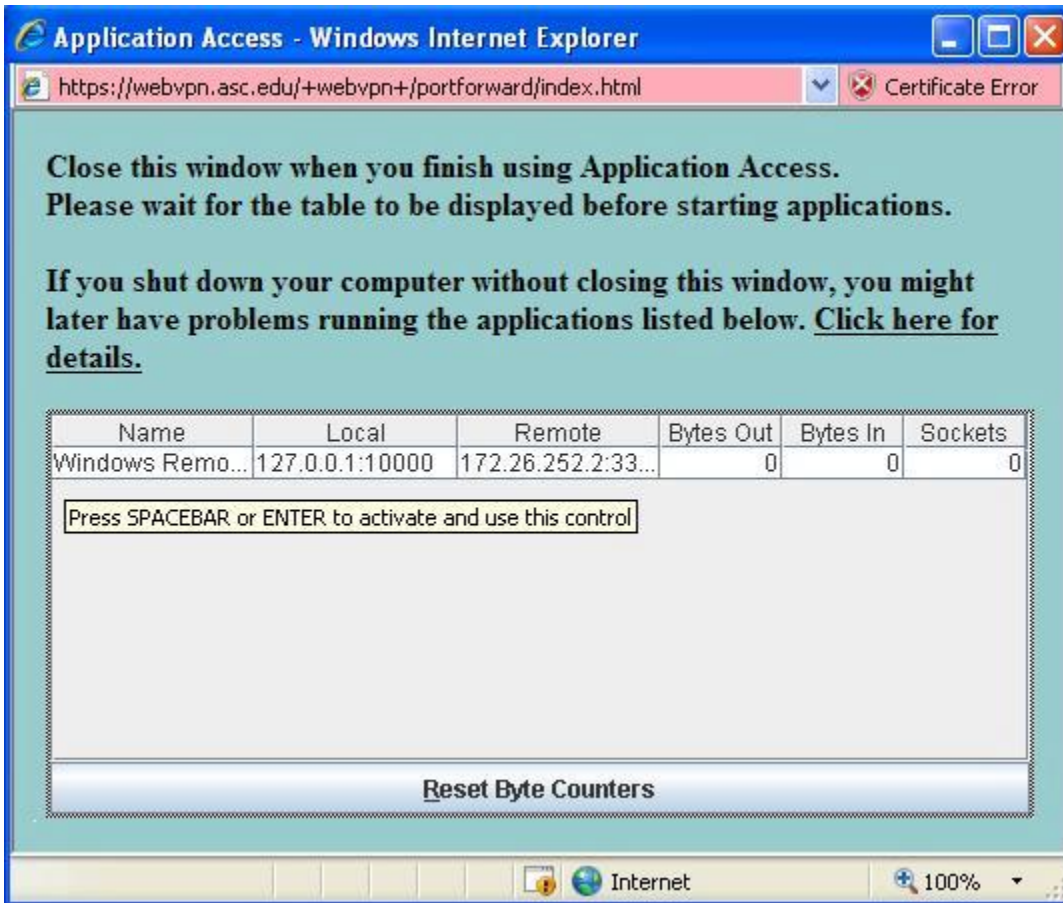


Figure 8: Java Application Access Window After Applet Install

Simply Click on the “Application Access” window and press the space bar or the enter key to activate the port-forwarding access. Notice the “Name”, “Local”, and “Remote” fields in the Java window. “Name” represents the description of the type of access. This can be any text specified by the WebVPN administrator. The “Local” field represents the local IP address and TCP port number needed to access the remote machine. The “Remote” field shows the remote IP address and TCP port number that will be accessed on the remote end for access. In this example, TCP port 10000 on the local machine will be mapped to TCP port 3389 on the remote machine. To verify this functionality, simply open remote desktop and fill in the local information such as in **Figure 9**.

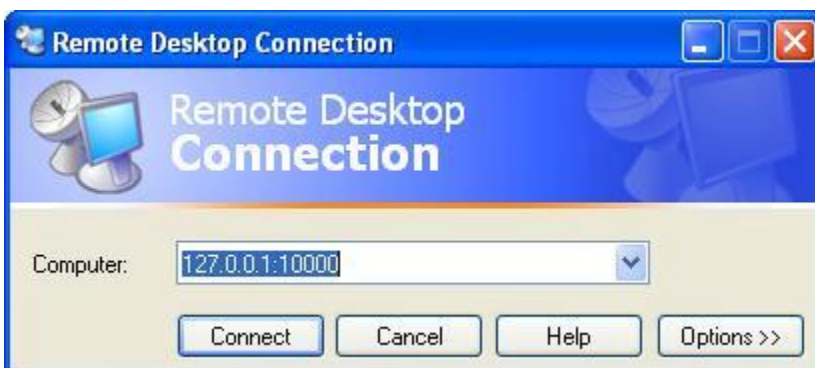


Figure 9: Remote Desktop Access

Notice the “:10000” after the IP address. This tells remote desktop to use TCP port 10000 for the connection to the remote machine. Click “Connect” to complete the connection and a screen similar to **Figure 10** should appear. Optimize the client machine’s remote desktop setting before connecting to ensure a quick connection.

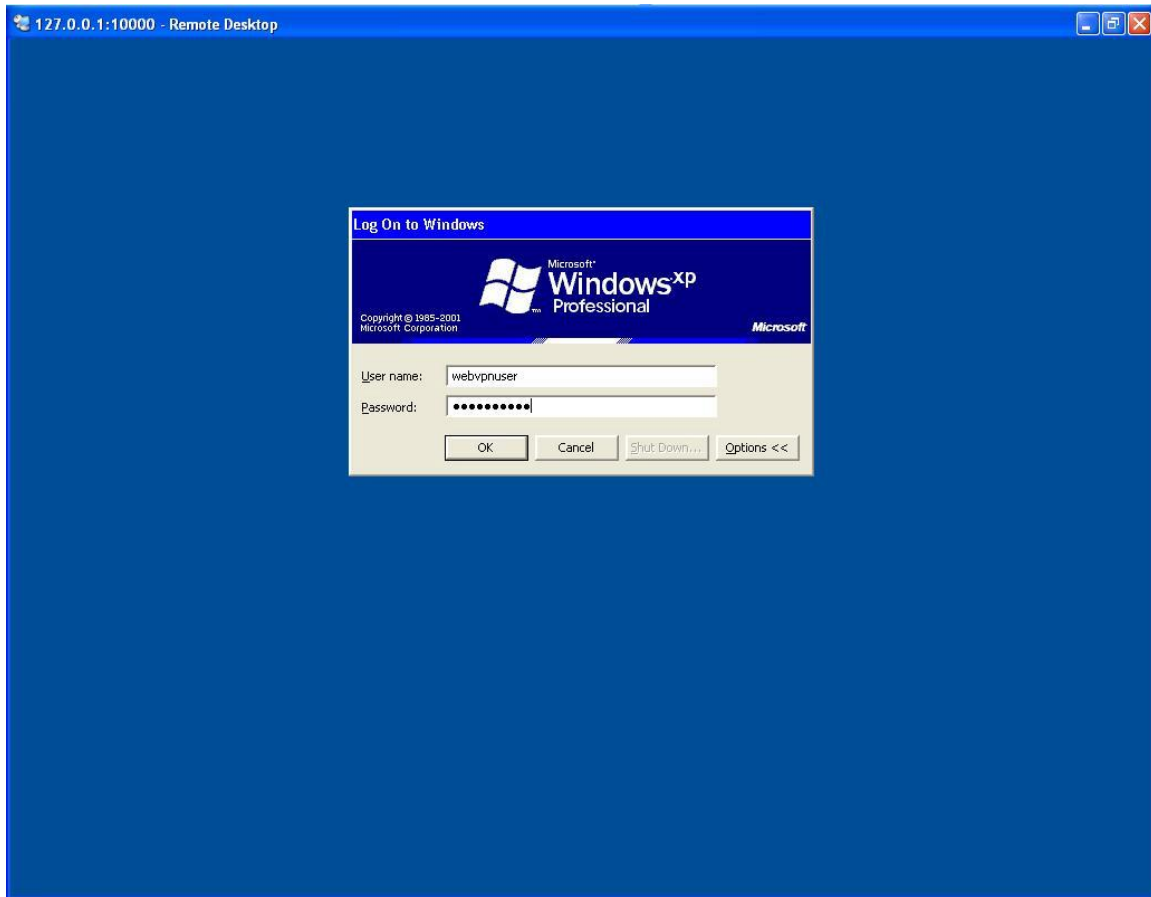


Figure 10: Remote PC Login

To exit the WebVPN connection, simply click the “X” icon in the top right of the WebVPN homepage. Closing the WebVPN homepage with the browser’s close option will cause the WebVPN service to close incorrectly and that session will not complete until after it times out.

Mike Trice, Systems Analyst

Contact

If you have technical questions about WebVPN, you can reach us by calling the help desk at 1-800-338-8320 or by emailing us at helpdesk@asc.edu.