

## SSL VPN Connection

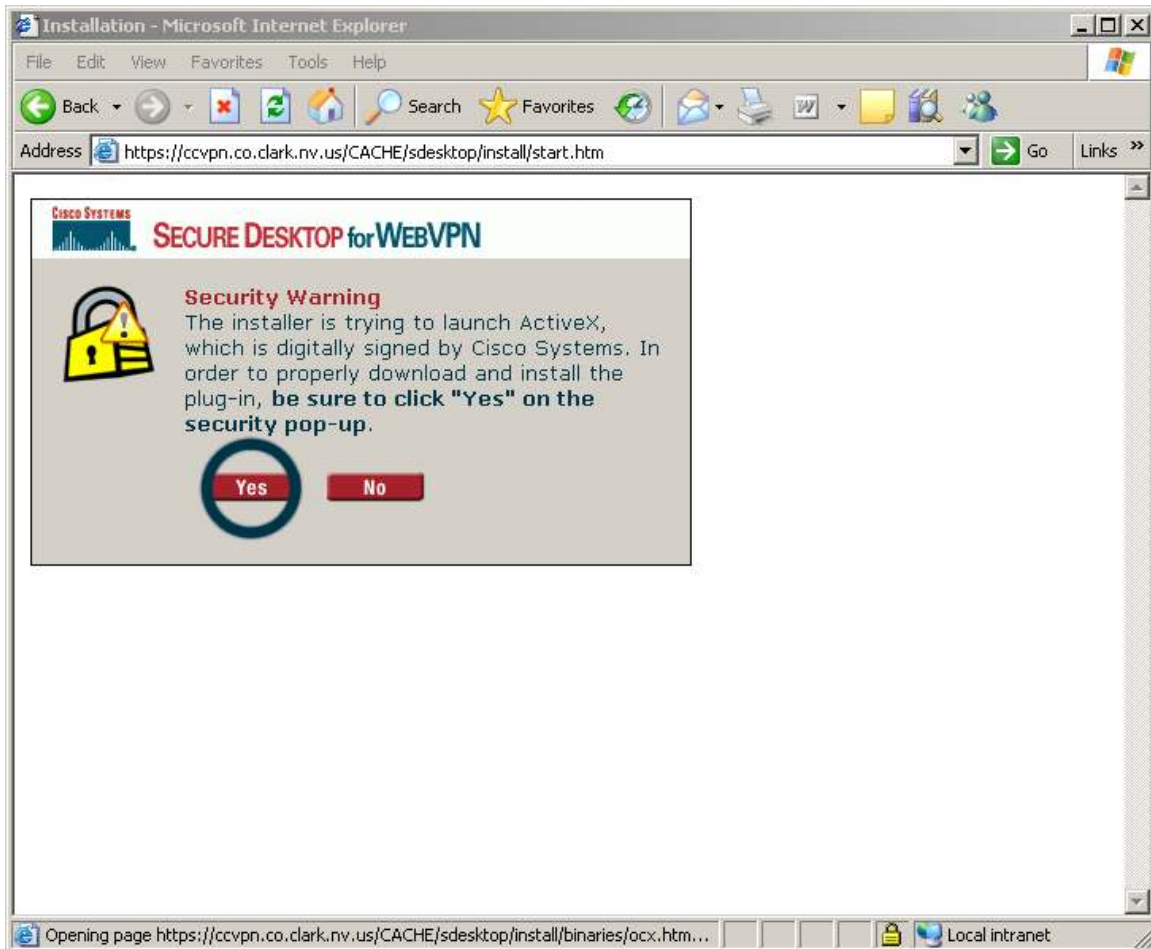
In order to connect to VPN, you are required to run a current antivirus product, and ensure it has current definitions loaded. In order to successfully connect to VPN, you must be running one of the following products, and ensure the virus definitions have been updated within the last 45 days.

- Avast AntiVirus (4.0)
- AVG AntiVirus (7.0-7.5)
- eTrust Antivirus (7.0-2005)
- F-Secure Antivirus (2003-2005)
- McAfee VirusScan (8.0-10.0, Enterprise 7.0-8.0)
- Symantec Antivirus (Corporate 8.0-10.0, Pro 2004-2006)
- Panda Antivirus (Titanium 2004, Platinum 7.0-8.0)
- PC-Cillin (2003-2005)
- Trend Micro OfficeScan Corporate AntiVirus (7.0)

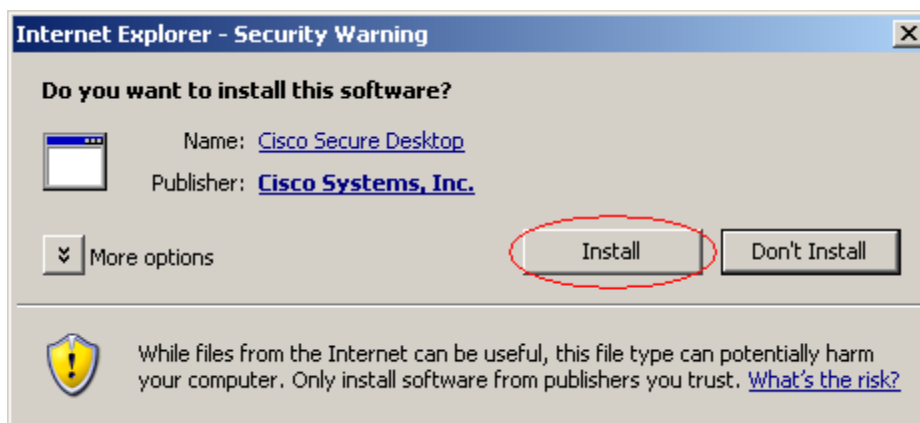
Support for SSL VPN is limited to computers running Windows 2000 or XP. Users needing to connect from a PC running Mac OS, Linux, or Solaris will require a separate client.

To establish a VPN connection, open your web browser and go <http://webvpn.co.clark.nv.us>

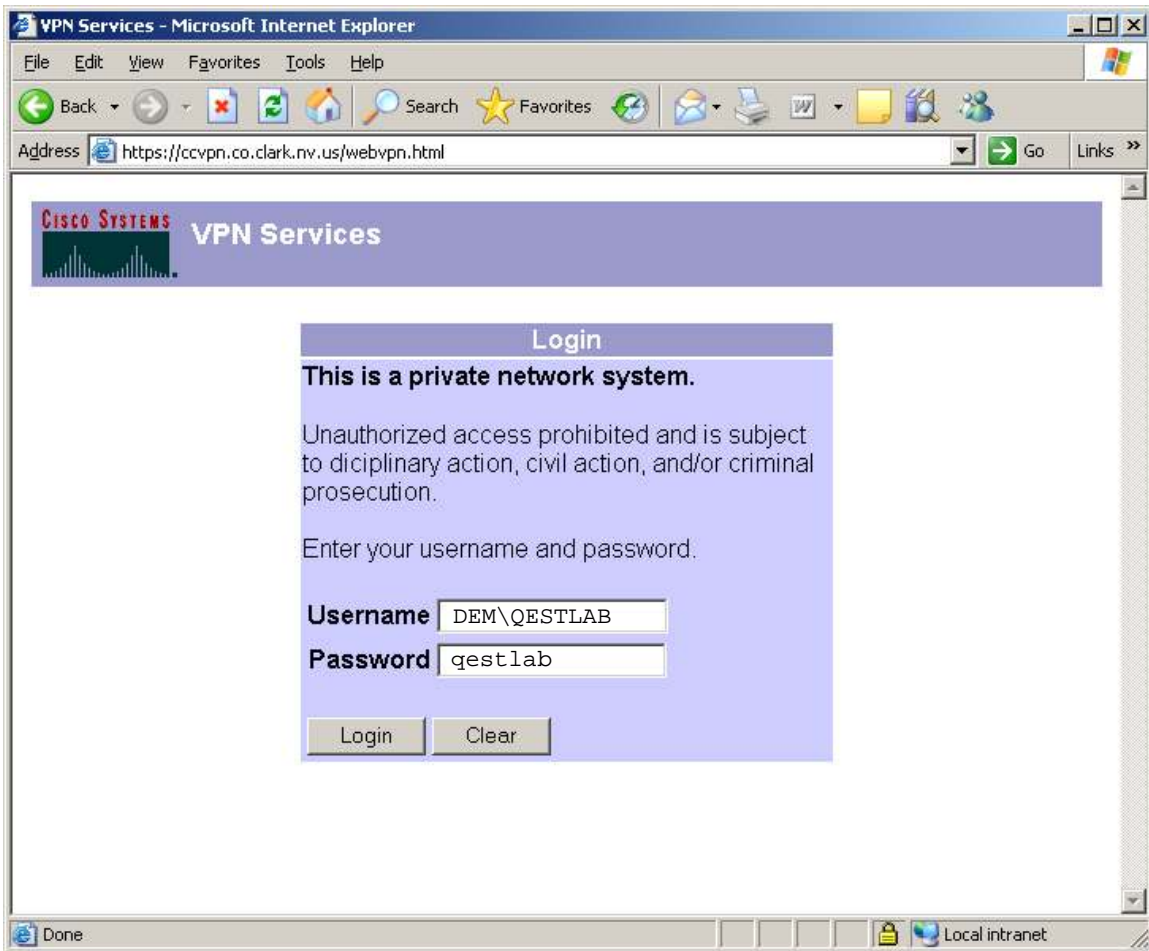
Once you connect, the VPN system will redirect you to the active VPN concentrator, and the URL in the Address bar will change.



Upon connection you will be prompted with a security warning, choose "Install" to proceed.



You should now be presented with a login screen. Enter your VPN login credentials here. Your username and password will be transmitted securely across the connection.



After you login, the Cisco SSL VPN Client should start, you may be presented with a second “Security Warning” dialog box, just click “Install” to continue the installation of the Cisco SSL VPN Client. Once the connection is successfully established, you will see the following:



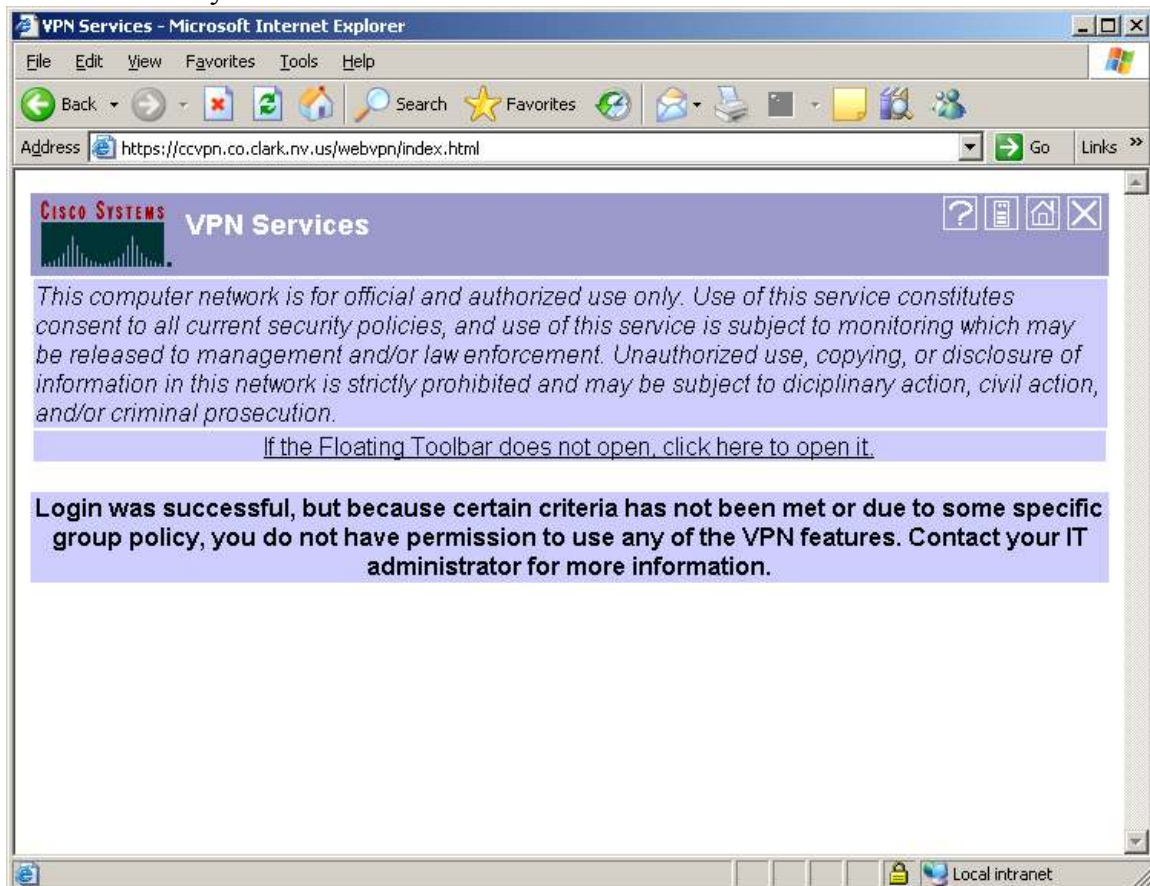
The key icon on your taskbar by your system clock is used to control the VPN connection. When you are ready to disconnect, right-click on the key icon, and select disconnect.



## Troubleshooting

### Problem 1 “certain criteria has not been met”:

I cannot establish a VPN connection, and I get a page with the message “Login was successful, but because certain criteria has not been met or due to some specific group policy, you do not have permission to use any of the VPN features. Contact your IT administrator for more information.”

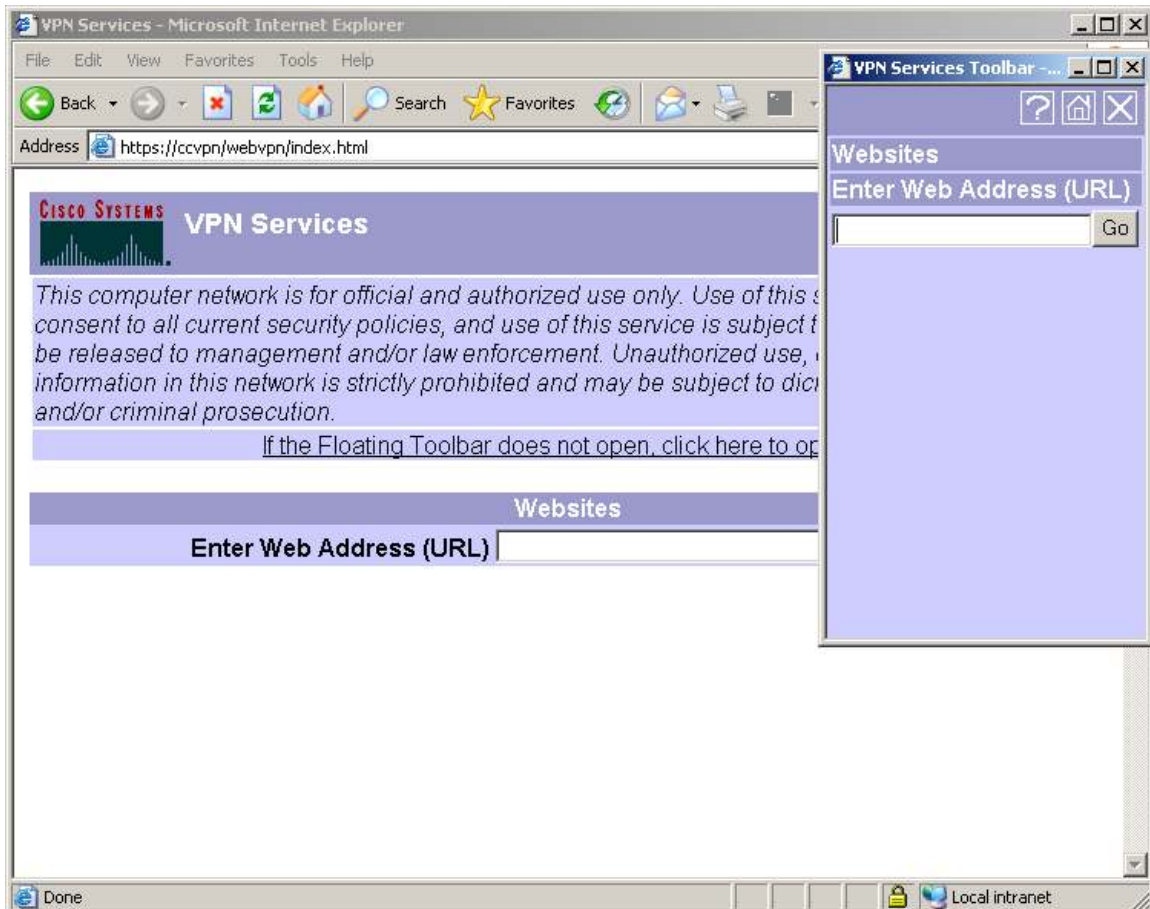


### Resolution 1:

This is most commonly caused by an out-of-date or unsupported antivirus program, or the absence of an antivirus program. Update your antivirus program and try again. This may also be due to your account not being authorized for VPN.

### Problem 2 “Floating Toolbar instead of SSL VPN key”:

After I login I do not get the “The SSL VPN connection has been established” and instead get the floating toolbar as shown below:



## Resolution 2:

This is the WebVPN proxy connection which will allow you to access predetermined systems within the Clark County network. You may see this instead of the screen in the first problem if your machine does not pass the antivirus check. You may also see this if you have an account specifically configured to give you this type of access.

## Problem 3 “Failed client installation”:

When I try to login I get an error message saying the Secure Desktop or SSL VPN Client cannot be installed.

## Resolution 3:

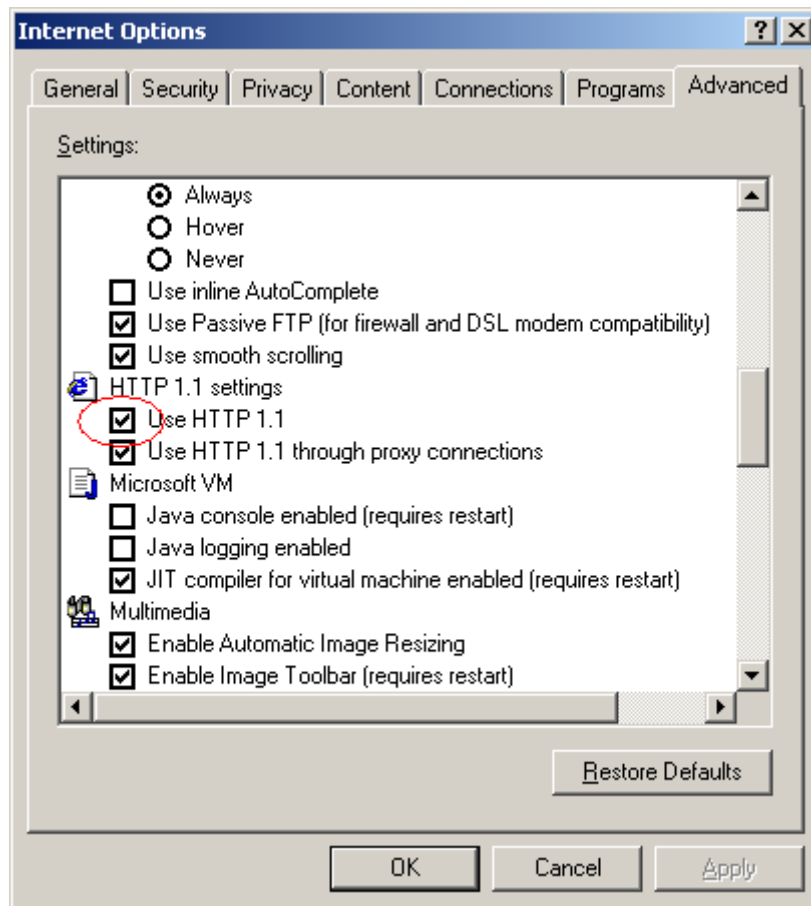
In order for the SSL VPN client to function properly your machine must support either ActiveX or Java. If you are using Internet Explorer, ensure your browser is set to enable HTTP 1.1, or ensure you are running the latest Java plug-in for your browser. If you are using another browser, such as Firefox, ensure the latest Java plug-in is enabled. You can download the latest Java plug-in at <http://www.java.com>

To ensure your Internet Explorer browser is configured to use HTTP 1.1. Open

Internet Explorer, select Tools->Internet Options



Then click on the “Advanced” tab and scroll down to find the “Enable HTTP 1.1” option and ensure it is checked.



#### **Problem 4 Certificate Security Alert when logging in:**

When I am attempting to connect, I get an error message saying the certificate is expired or not yet valid, the certificate is not from a trusted certifying authority, or the name on the certificate is invalid or does not match the name of the site.

**Resolution 4:**

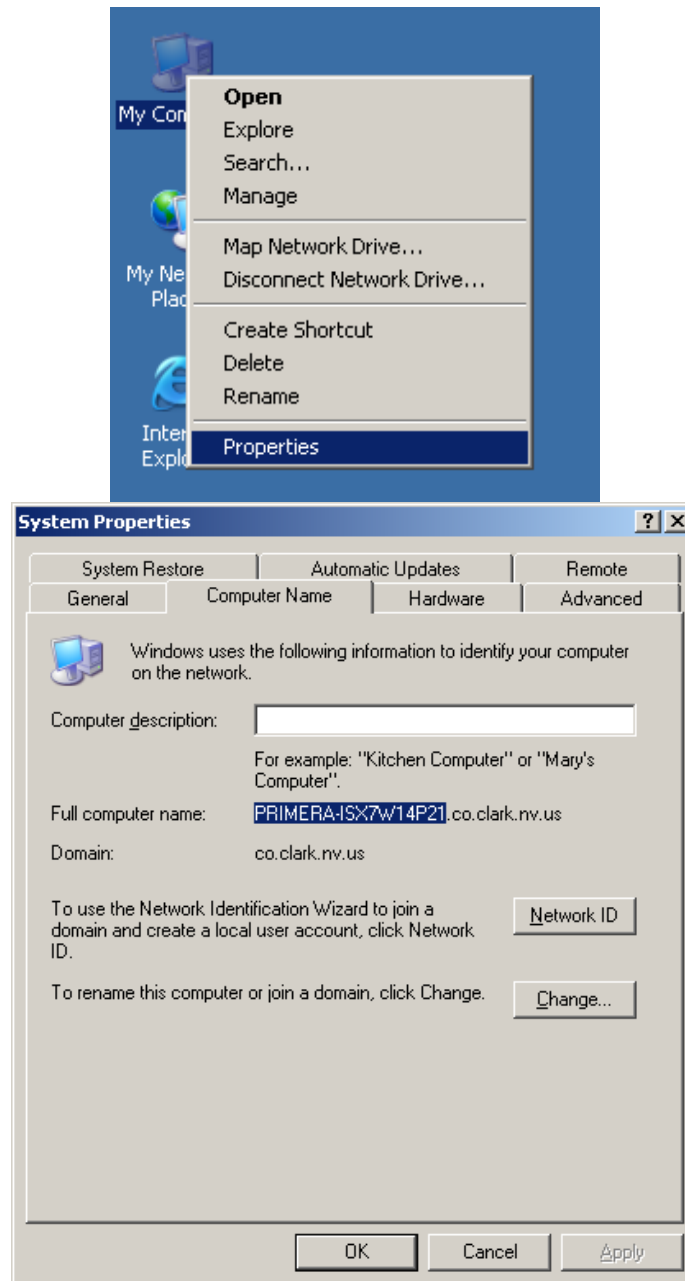
This may be caused if you try to go to <https://webvpn.co.clark.nv.us> instead of <http://webvpn.co.clark.nv.us> (note the difference—s—between the 2 URL's). Use <http://webvpn.co.clark.nv.us> to access the system, you will be redirected to the active concentrator and the session will start to use SSL encryption.

This may also be caused by an expired Verisign certificate that is distributed in versions of Windows XP and 2000. All Clark County systems use Verisign's Professional SSL certificates, however, the Intermediate Certificate distributed with Windows expired in 2004. To resolve this, go to <https://getca.verisign.com/update.html> and follow the update instructions.

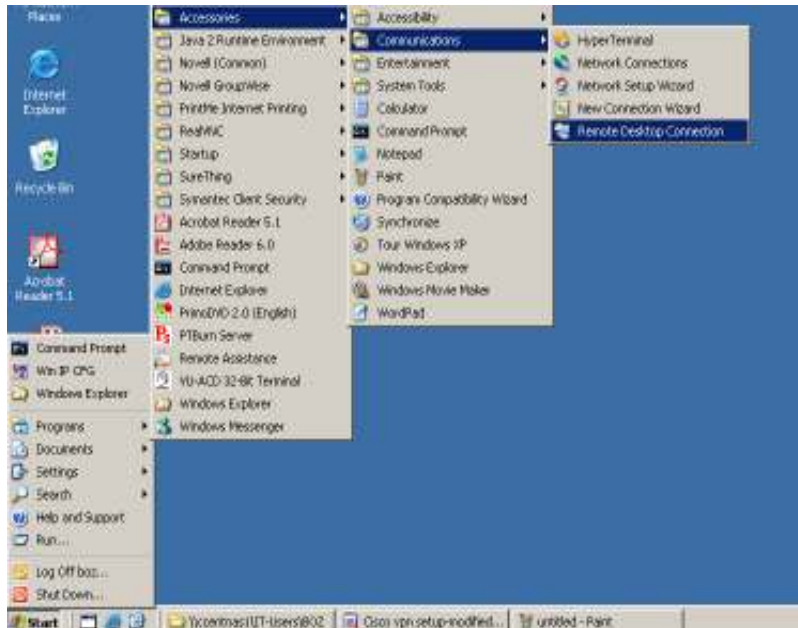
## Remote Desktop Instructions

For current employees, the recommended way to access county resources is by using Remote Desktop. This will allow you to connect to your PC at work, and will create the same exact environment that you would have sitting at your desk at the workplace.

Your first step will be to obtain your workstation name for the computer you use at work. You can find this by right-clicking on “My Computer”, and choosing “Properties”. On the “Computer Name” tab, write down the first part of the Full computer name (That would be PRIMERA-ISX7W14P21 in the example below, yours will be different):



At home, after connecting using the Cisco VPN connection that you setup, you will go to Remote Desktop as shown below:



For Computer, put in your work's workstation name, then click "Connect".



You can then login to the network and use your applications just like you do from the workplace. PLEASE NOTE: YOUR COMPUTER AT WORK MUST BE TURNED ON IN ORDER TO REMOTE DESKTOP TO IT! You do not have to be logged in, just need to have your computer on.