Secure Remote Desktop

Juniper SSL VPN and Windows Remote Desktop
For Windows Vista and Windows 7

Dynamic
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>CLIENT COMPUTER</td>
<td>1</td>
</tr>
<tr>
<td>VPN CONNECTION &amp; PERMITTING REMOTE DESKTOP CONNECTIONS</td>
<td>1</td>
</tr>
<tr>
<td>VPN</td>
<td>1</td>
</tr>
<tr>
<td>RUNNING WINDOWS REMOTE DESKTOP</td>
<td>11</td>
</tr>
<tr>
<td>HOST COMPUTER</td>
<td>16</td>
</tr>
<tr>
<td>INFORMATION AND CONFIGURATION</td>
<td>16</td>
</tr>
<tr>
<td>ENABLE REMOTE CONNECTIONS</td>
<td>16</td>
</tr>
<tr>
<td>CONFIGURE WINDOWS FIREWAL</td>
<td>20</td>
</tr>
<tr>
<td>IP ADDRESS/HOST NAME</td>
<td>26</td>
</tr>
</tbody>
</table>
INTRODUCTION

Remote Desktop is an application that is built-into Windows operating systems providing a means to connect to one computer (call the host) from another computer (called the client) that is located at a physically different place. It will give you the sense of actually sitting at the host computer such as at your office. At UMass Boston, it is mandatory that you also have a VPN account. This is because Remote Desktop by itself is not secure. In addition, you will need to obtain some information about and perform some preliminary configuration on the host computer. The information provided here pertains to the Windows Vista and Windows 7 Operating systems.

CLIENT COMPUTER
VPN CONNECTION & PERMITTING REMOTE DESKTOP CONNECTIONS

In order to connect securely to your office computer using Windows Remote Desktop, it is essential that you have a VPN account. A request form for a new VPN account must be submitted to the IT Service Desk in order to obtain one. You must also know how to use the information about the host computer to use secure Remote Desktop to connect your office computer.

VPN

To use VPN, you must have a VPN account. Once you have received notification that a VPN account has been created for you, you may begin to use it. A copy of the form may be obtained at the URL: http://umb.edu/uploads/File/it/services/security/vpn_form-1(1).pdf. Please be sure to provide all of the information requested on the form. Otherwise the application might be rejected and considered incomplete. The form should be sent to the IT Service Desk, Healey, 3rd floor, room 007. If the application is approved, you will receive an email notification from IT-Security@umb.edu. Your username and password will be your UMB email username and UMB email password.

The other information will instruct you on how to configure Windows Firewall and how to establish a VPN session. Windows Firewall and connecting to VPN are also contained in this document. Connecting to VPN involves two stages: the initial connection and all subsequent connections. This will also be explained in this document.
Initial logon to VPN

After receiving your username, password and domain from IT, go to https://tunnel.umb.edu/VPN. Enter your UMB email username UMB email password. Select UMB-VPN-Dynamic as the domain. Click Sign In.

You might get a notification like that show below. It might say there is an add-on called “JuniperSetupClient.cab”. Click on the information bar where it says to “Click here to install...”.

![Image of SSL VPN Tunnel login page]

![Image of notification for JuniperSetupClient.cab add-on]

- The previous site might require the following add-on: JuniperSetupClient.cab from Juniper Networks, Inc. Click here to install...
Click on “Install this Add-on” from the popup menu.

You may or may not get the User Account Control popup asking, “Do you want to allow the following program to make changes to this computer?” The program might be JuniperSetupClient.cab. Click on Yes.

Once your credentials have been accepted, you will see the screen shown below. Click on Start. Click only once. Please wait. This can take some time.
You might see the following pop-ups briefly on the screen. Just wait.

![Setup window](image)

Launching application, please wait...

and

![Please Wait window](image)

Installing application, please wait...

Once these go away, you may or may not get the **User Account Control** popup asking, "Do you want to allow the following program to make changes to this computer?" The program might be `neoNCSetu.exe`. Click on **Yes**.

During the installation, you might also see the screen below where the connection is being negotiated. Be patient and wait.
Once a connection is established this will go away and you will be back to the screen shown below.

You’re done and you have successfully established a VPN connection. To verify that a connection exists, look down in the lower right-hand corner of your task bar and look for the arrowhead like the icon shown below that is pointing upwards. It will allow you show hidden icons.
Click on the arrow and you will see hidden icons.

If you see an icon similar the one show below, that tells you that you have established secession.

By hovering the mouse pointer over the icon, a popup might say *Connected.*
Another way to determine if you are connected it to use the **Resource Monitor**. Click **Start** and then type in **cmd** and press **Enter**. Some versions of Windows may not have this.

You will then see a screen similar to but not exactly like the one shown below.
Type in `resmon` and press **Enter**.

When the screen below appears, click on the **Network tab**. You will see a line that reads `dsNetworkConnect.exe`. You should also see some numbers under the **Send** and **Receive** columns indicating that there is some communication occurring.

You are done.
Subsequent logons to VPN

For all subsequent logons to VPN, you can go to the Juniper Networks folder and click on the Network Connect icon shown below. Just go to Start and All Programs and look for Juniper Networks. Just click in the Network Connect icon shown below.
After you click on **Network Connect** you will see the logon shown below just as before. Just enter your username, password, and select **UMB-VPN-Static** and click **Sign In**.

You can determine if you have entered a session as described above.
RUNNING WINDOWS REMOTE DESKTOP

Now that you have established a VPN session, you can run Windows Remote Desktop. Click **Start**. Click **All Programs**.

Click **Accessories**.
You should see a screen similar to the one below. Click on **Remote Desktop Connection**.

You will next see a logon prompt as shown below. This is the place where you will enter either the IP address or the host name of the remote computer to which you would like to connect.
Type in the IP address or host name of the host computer. In this example, I typed in 158.121.200.169. Click Connect.

You might see the screen below. Click on Yes.
The screen should now change and you should get the screen to logon to the host computer to which you are trying to connect. In this case, I am connecting to a Windows XP computer. Enter your username and password like you would do usually and this should allow you to logon to your office computer.

If you are trying to connect to a Window Vista or Windows 7 computer, just type in the IP address of the host computer. In this case I am using 158.121.200.554. Click on Connect.
The logon to the host computer will look similar to the one below. Just enter the logon credentials and click **Ok**.

![Windows Security dialog box](image)

You might get a warning message like the one show below. Click on **Yes**.

![Remote Desktop Connection warning](image)

You should now be connected to the remote computer.
Information about the configuration of the host computer is summarized below.

- Enable remote connections on the host
- Configure Windows Firewall on host
- Obtain either or both the IP address and/or host name of the host computer

**ENABLE REMOTE CONNECTIONS**

Go to **Control Panel**. The default view for Window Vista/7 is **Category** view. This is shown below.

Change the view to **Small icons**. To do so, click on the arrow that is pointing downward to the right of **Category**. Click on **Small icons**.
This will change the view to the one shown below.

Look for the icon that says System and click on it. It looks like the one below.

Look for a section that reads “Computer name, domain, and workgroup settings”. Look to the far right of that section and click on Change settings.
Click on the **Remote** tab.
Remove the check in the box at “Allow Remote Assistance connections to this computer”. Place a check in the box at “Allow connections from computers running any version of Remote Desktop (less secure)”. 

Click Ok.
**CONFIGURE WINDOWS FIREWAL**

Go to **Control Panel**. Click on the icon that reads **Windows Firewall**.

![Windows Firewall icon](image)

Look to the column on the left. Click on **Advanced Settings**.

![Control Panel Home](image)

Control Panel Home
- Allow a program or feature through Windows Firewall
- Change notification settings
- Turn Windows Firewall on or off
- Restore defaults
- Advanced settings
- Troubleshoot my network

Select **Inbound Rules** under the left column.
Scroll down to and select **Remote Desktop (TCP-In)** in the middle column.

<table>
<thead>
<tr>
<th>Name</th>
<th>Group</th>
<th>Profile</th>
<th>Enabled</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Assistance (PNRP-In)</td>
<td>Remote Assistance</td>
<td>Public</td>
<td>No</td>
<td>Allow</td>
</tr>
<tr>
<td>Remote Assistance (RA Server TCP-In)</td>
<td>Remote Assistance</td>
<td>Domain</td>
<td>Yes</td>
<td>Allow</td>
</tr>
<tr>
<td>Remote Assistance (SSDP TCP-In)</td>
<td>Remote Assistance</td>
<td>Domain</td>
<td>Yes</td>
<td>Allow</td>
</tr>
<tr>
<td>Remote Assistance (SSDP UDP-In)</td>
<td>Remote Assistance</td>
<td>Domain</td>
<td>Yes</td>
<td>Allow</td>
</tr>
<tr>
<td>Remote Assistance (TCP-In)</td>
<td>Remote Assistance</td>
<td>Domain</td>
<td>Yes</td>
<td>Allow</td>
</tr>
<tr>
<td>Remote Event Log Management (NP-In)</td>
<td>Remote Event Log Management</td>
<td>Private</td>
<td>No</td>
<td>Allow</td>
</tr>
<tr>
<td>Remote Event Log Management (NP-In)</td>
<td>Remote Event Log Management</td>
<td>Domain</td>
<td>No</td>
<td>Allow</td>
</tr>
<tr>
<td>Remote Event Log Management (RPC)</td>
<td>Remote Event Log Management</td>
<td>Private</td>
<td>No</td>
<td>Allow</td>
</tr>
<tr>
<td>Remote Event Log Management (RPC)</td>
<td>Remote Event Log Management</td>
<td>Domain</td>
<td>No</td>
<td>Allow</td>
</tr>
</tbody>
</table>

There is a column on the right under **Remote Desktop (TCP-In)**. Select **Enable Rule**. If the rule is already enabled, go to the next step. Then select **Properties** in the same column.
Select the **Scope** tab. Look under the section that reads “**Remote IP address**” and select **These IP addresses**: and click the **Add** button.
Look under **This IP address or subnet**.

Select **This IP address or subnet**: Enter **158.121.12.0/255.255.255.0**.

Click **OK**.

Click **OK**.
Close Windows Firewall with Advanced Security.

Close Windows Firewall.

Reboot the computer.
In order to connect to the remote computer, you must obtain either the IP address or the host name of the host computer. In order to do so, you must get this information from the host computer.

**How to get the IP address**

Click **Start** and type in **cmd** and press **Enter**.
You will next see a screen like the one below.

Type in `ipconfig`. You will next see a screen similar to the one below. Press the Enter key.
You should see a screen like the one below. Look under the section titled “Ethernet adapter Local Area Connection:”. You will see a line under that section that says “IPv4 Address. ...............: 158.121.200.110”. The numbers 158.121.200.110 is the IP address of the host computer.

![Image of command prompt with Ethernet adapter and nslookup results]

**How to get the host name**

In order to find the host name, you will need to know the IP address. In some cases using the IP address to connect using Remote Desktop will not work. The host name never changes but it is possible that the IP address will.

If you are still at the same screen shown above you can also get the host name of the host computer. Type in `nslookup 158.121.200.110` and press Enter.

![Image of nslookup output]

Look at the line that reads “Name:  HCK91G1.200dhcp-090.umb.edu". HCK91G1.200dhcp-090.umb.edu is called the host name for the host computer.