

Configuration of Windows XP with SP2 for ASAP Remote

The steps in this document provide a minimal configuration of Microsoft® Windows® XP operating system with Service Pack 2 (SP2) for use with ASAP® Remote from Breault Research Organization, Inc.

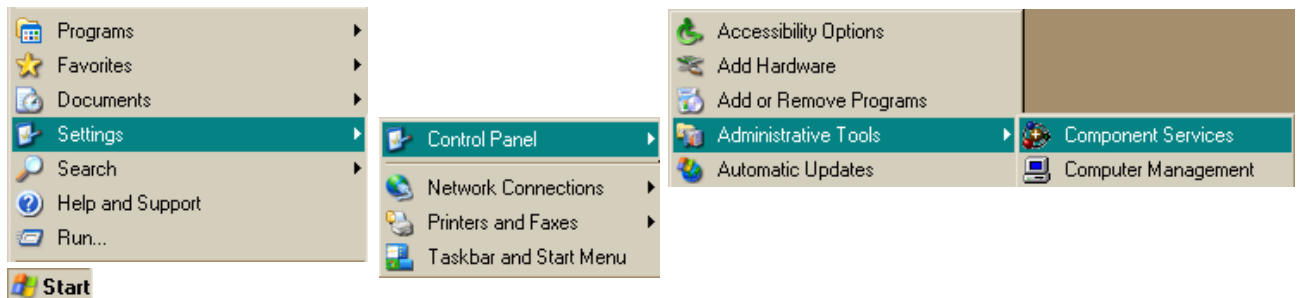
REQUIREMENTS:

- A familiarity with the Windows firewall and DCOM settings is required.
- **The steps must be completed on both the local and remote computer.**
- You must have Administrator permissions on both machines.
- ASAP must be closed.

WARNING: Breault Research Organization, Inc. does not assume risk or damages that may occur by anyone using this procedure to alter the default access configurations of their machine(s) for component or Windows firewall settings. Consult your IT policies before implementing these settings.

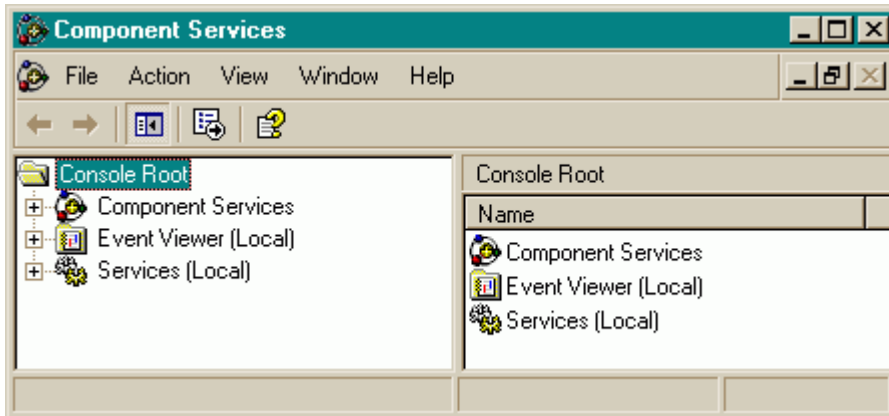
A. Component Services: COM Security

1. From the **Start** menu, select **Settings> Control Panel> Administrative Tools> Component Services**.

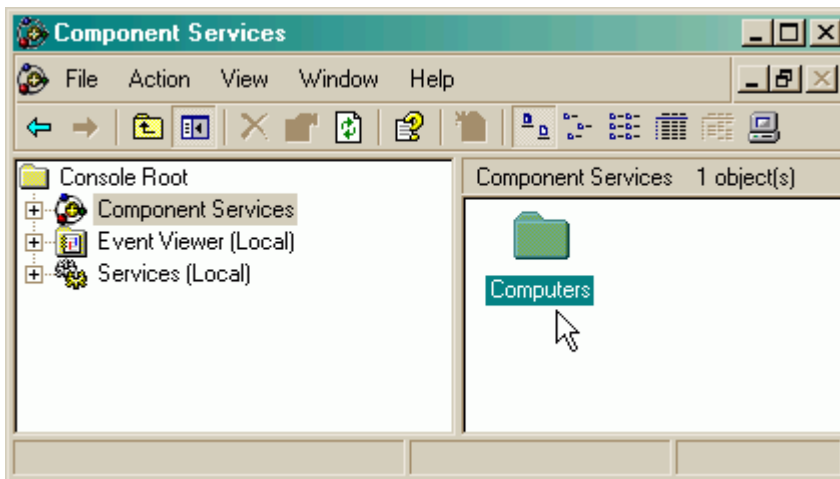


If the Windows Security Alert dialog box is displayed, select **Unblock** to proceed.

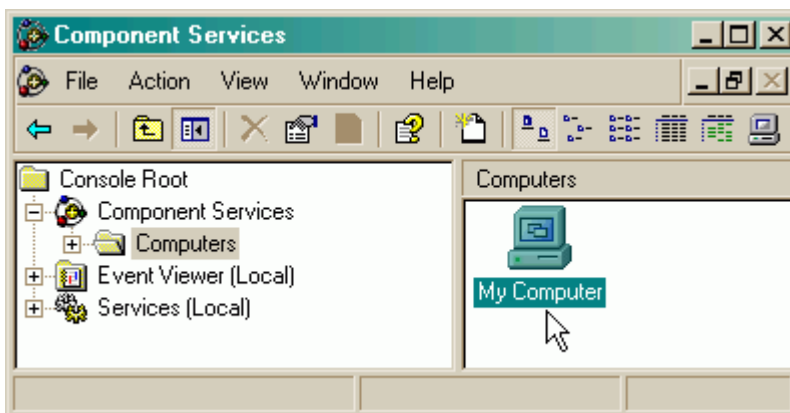
The **Component Services** dialog is displayed next:



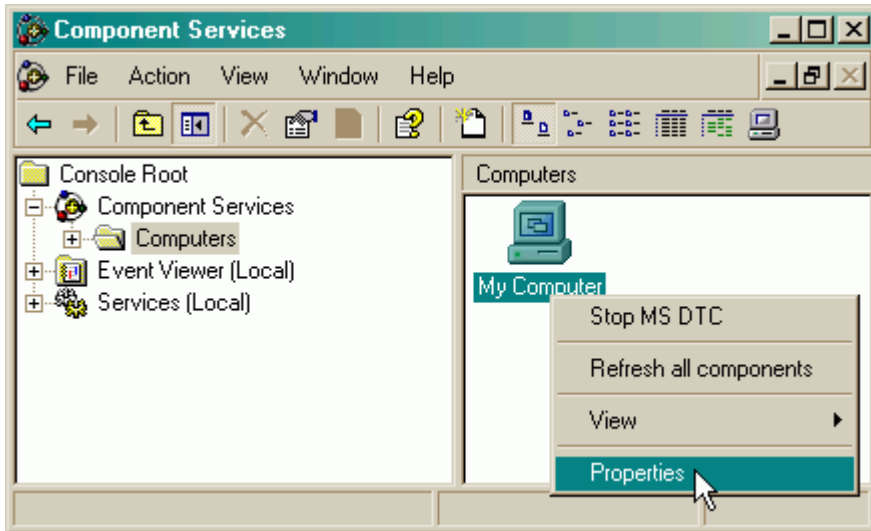
2. Under **Console Root** in the left panel, but do *not* open, select **Component Services**.
3. In the right panel, double-click the **Computers** folder to open it.



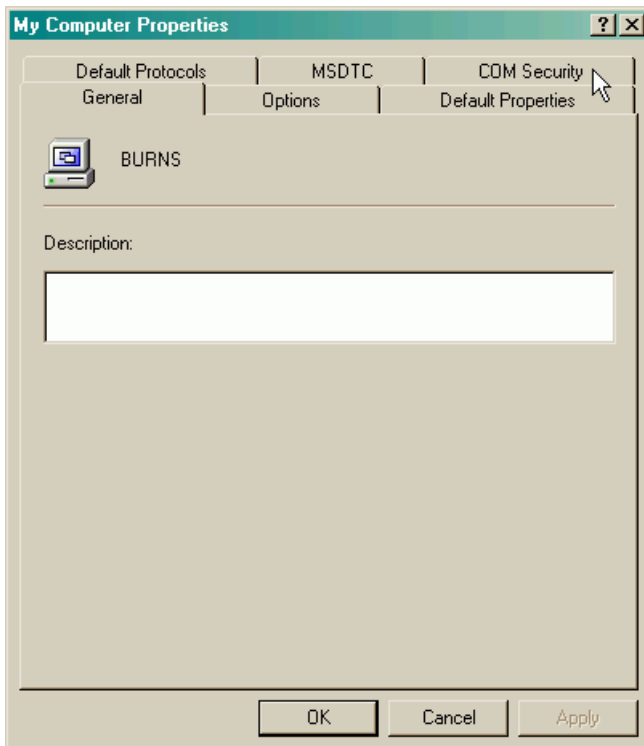
4. Right-click **My Computer**.



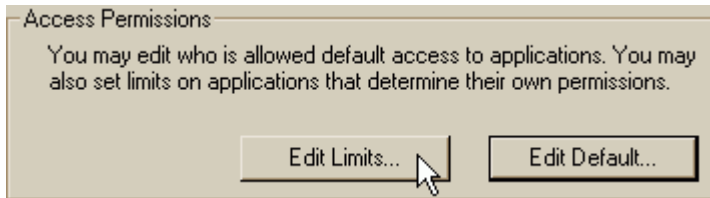
5. Select **Properties** from the pop-up menu.



6. In the **My Computer Properties** dialog box, select **COM Security**.

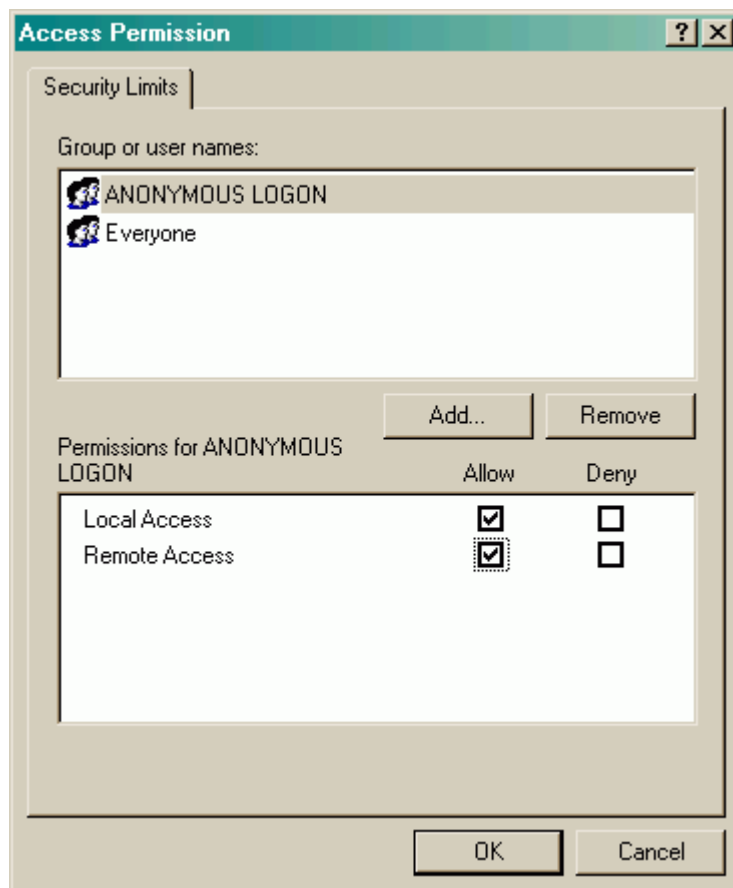


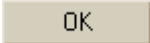
7. In the **Access Permissions** area of the **COM Security** window, click **Edit Limits**.



The **Access Permissions** dialog box is displayed.

NOTE: Under **Group or user names**, the names **ANONYMOUS LOGON** and **Everyone** must be present in this dialog to continue. If they are not present, click **Add** to add them.

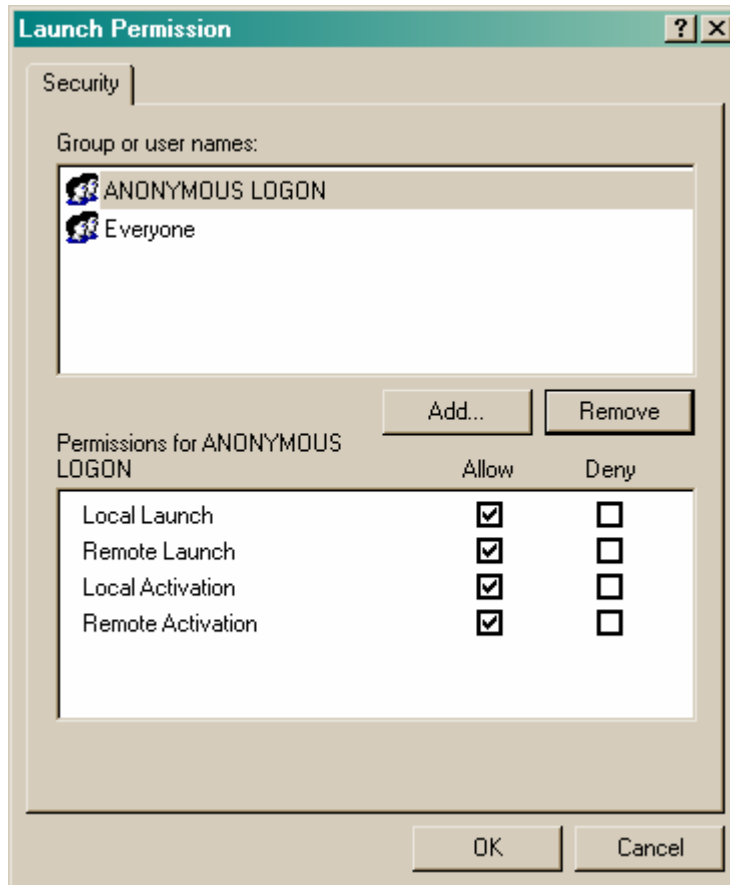


8. Under **Group or user names**, select **ANONYMOUS LOGON**.
9. Under **Permissions for ANONYMOUS LOGON**, select (check) **Allow** for both **Local Access** and **Remote Access**.
10. Repeat these steps for **Everyone**: Under **Group or user names**, select **Everyone**.
11. Under **Permissions for Everyone**, select (check) **Allow** for both **Local Access** and **Remote Access**.
12. Click  on the **Access Permissions** dialog box.
13. Select the **COM Security** tab on the **My Computer Properties** dialog box.

14. In the **Launch and Activation Permissions** area, click **Edit Limits**.

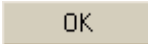
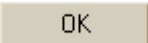



The **Launch Permissions** dialog box is displayed.



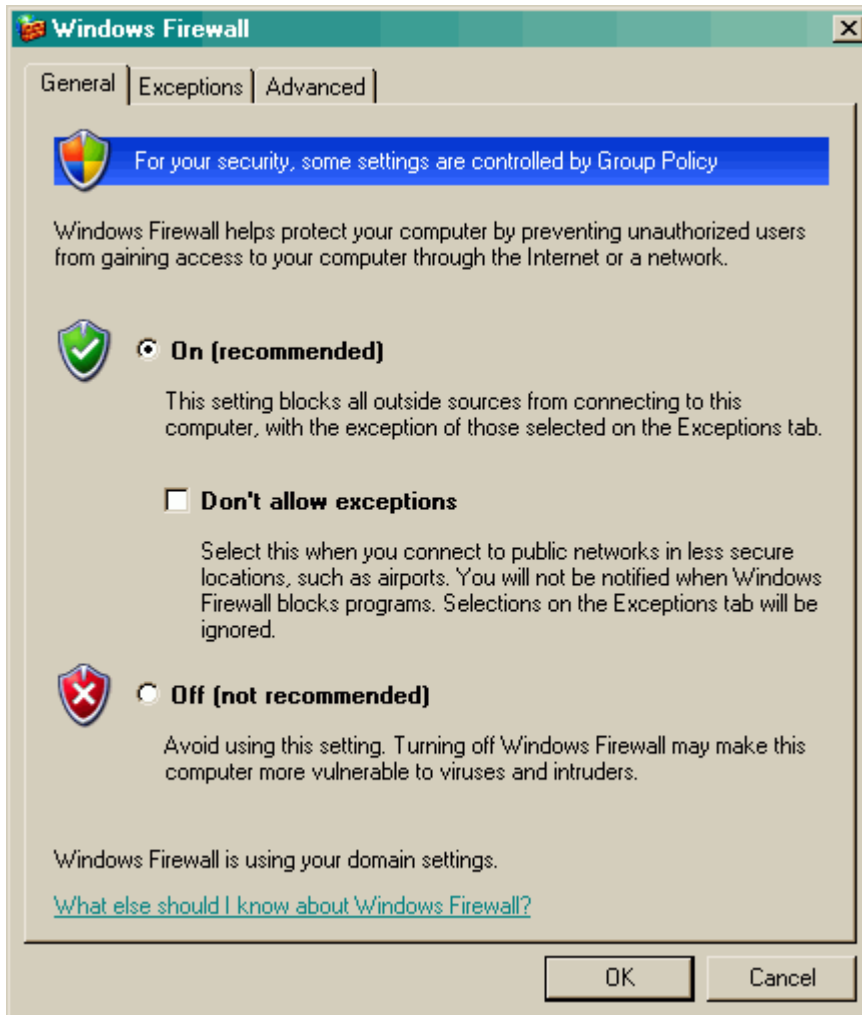
NOTE: Under **Group or user names**, the names **ANONYMOUS LOGON** and **Everyone** must be present.

15. Under **Group and user names**, select **ANONYMOUS LOGON**.
16. Under **Permissions for ANONYMOUS LOGON**, select (check) **Allow** for **Local Launch**, **Remote Launch**, **Local Activation** and **Remote Activation**.
17. Repeat these steps for **Everyone**: Under **Group or user names**, select **Everyone**.
18. Under **Permissions for Everyone**, select (check) **Allow** for **Local Launch**, **Remote Launch**, **Local Activation** and **Remote Activation**.

19. Click  to return to the **COM Security** window.
20. Click  again in the **My Computer Properties** dialog to apply the settings.
21. Close the **Component Services** dialog box by clicking .
22. Proceed to section B, Windows Firewall Settings – General.

B. Windows Firewall Settings—General


1. From the **Start** menu, select **Settings> Control Panel> Windows Firewall**. This opens the **Windows Firewall** dialog box. Adjust the settings, if necessary, to allow exceptions for ASAP REMOTE.
2. On the **General** tab of Windows Firewall dialog box, select **On (recommended)** to enable ASAP Remote.
3. Confirm that **Don't allow exceptions** is NOT checked.

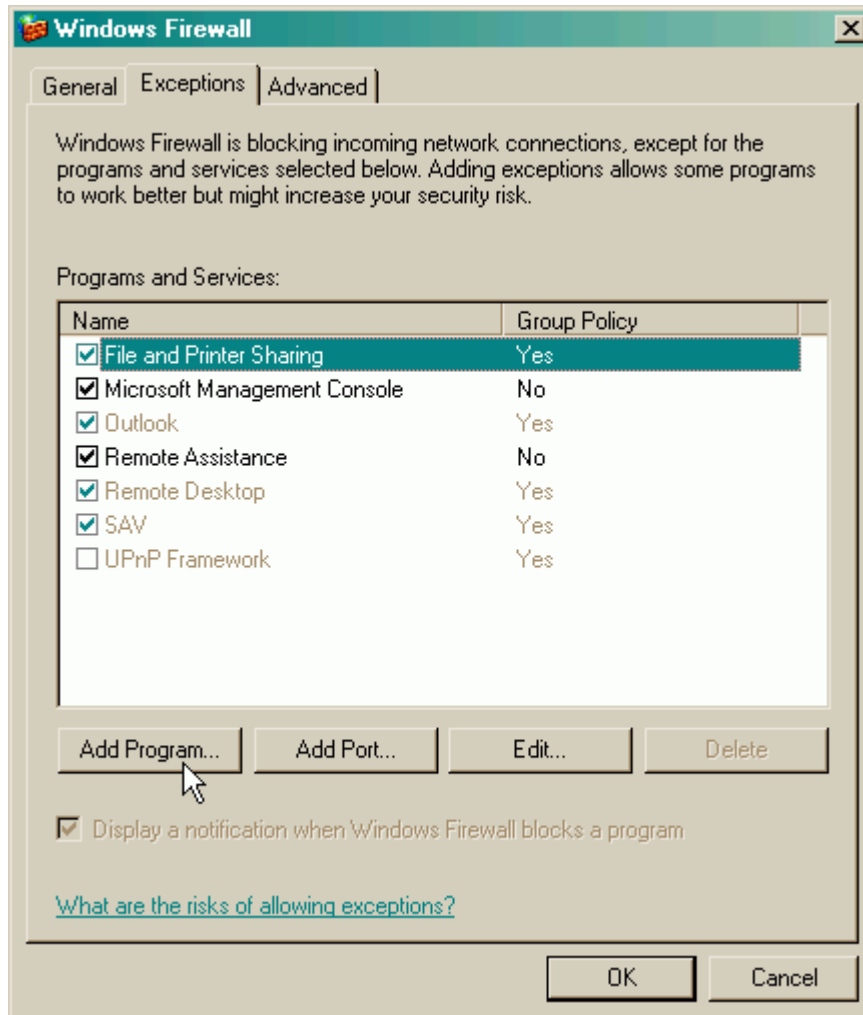


Proceed to section C, Windows Firewall Settings – Add Exceptions for ASAP.exe.

C. Windows Firewall Settings— Add Exceptions for ASAP.exe

Now we need to add an exception for ASAP.

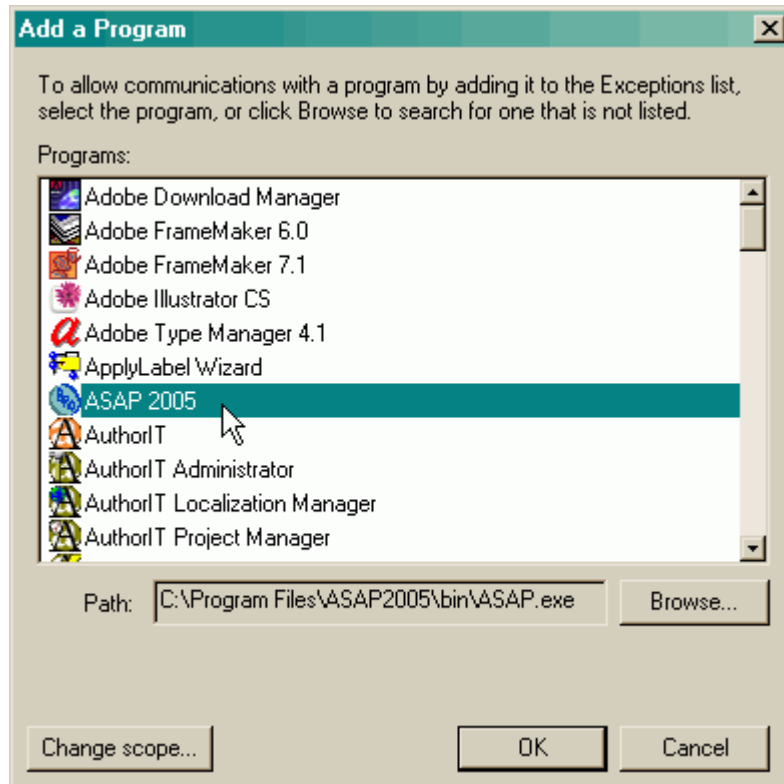
1. If you are not already in the Windows Firewall dialog box, from the **Start** menu, select **Settings> Control Panel> Windows Firewall**.
2. Select the **Exceptions** tab. The names of programs and services may differ from those listed in the figure below.
3. Click  on the **Exceptions** page.



4. Click **Browse...** and locate the ASAP.exe file residing on your machine. It resides in the ASAP 20XX VXXRX\bin folder.

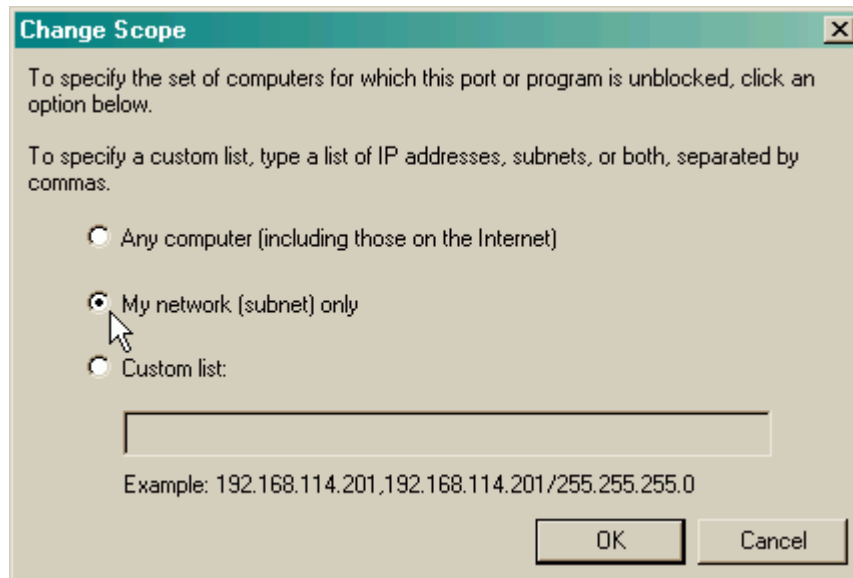
5. In the **Programs** list box, select **ASAP 20XX VXXRX**, and click **Change scope...**.

NOTE: The programs on the **Programs** list box on your machine will differ from those shown below, except the ASAP program.



6. In the **Change Scope** dialog box, select the desired scope for remote machines that are used with ASAP Remote. Typically, the selection is **My Network (subnet only)**.

NOTE: If you prefer, you can limit the scope to machine IP by selecting **Custom list** and entering the IP address.



8. Click **OK** in the **Change Scope** dialog box, and then click **OK** again in the **Add a Program** dialog to apply changes.
9. Proceed to section D. Windows Firewall Settings – Add Exceptions for KernelServ.exe.

D. Windows Firewall Settings—Add Exceptions for KernelServ.exe

This section uses the same steps as in Section B, except we are now adding KernelServ. If you are currently at the **Exceptions** tab, go to step 3.

1. From the **Start** menu, select **Settings> Control Panel> Windows Firewall**.
2. Select the **Exceptions** tab.
3. Click on the **Exceptions** page.
4. Click and locate the Kernel.exe file. It resides on your machine in the ASAP 20XX VXXR\bin folder.
5. In the **Programs** list box, select **KernelServ**, and click .
6. In the **Change Scope** dialog box, select the desired scope for remote machines that are used with ASAP Remote. Typically, the selection is **My Network (subnet only)**.

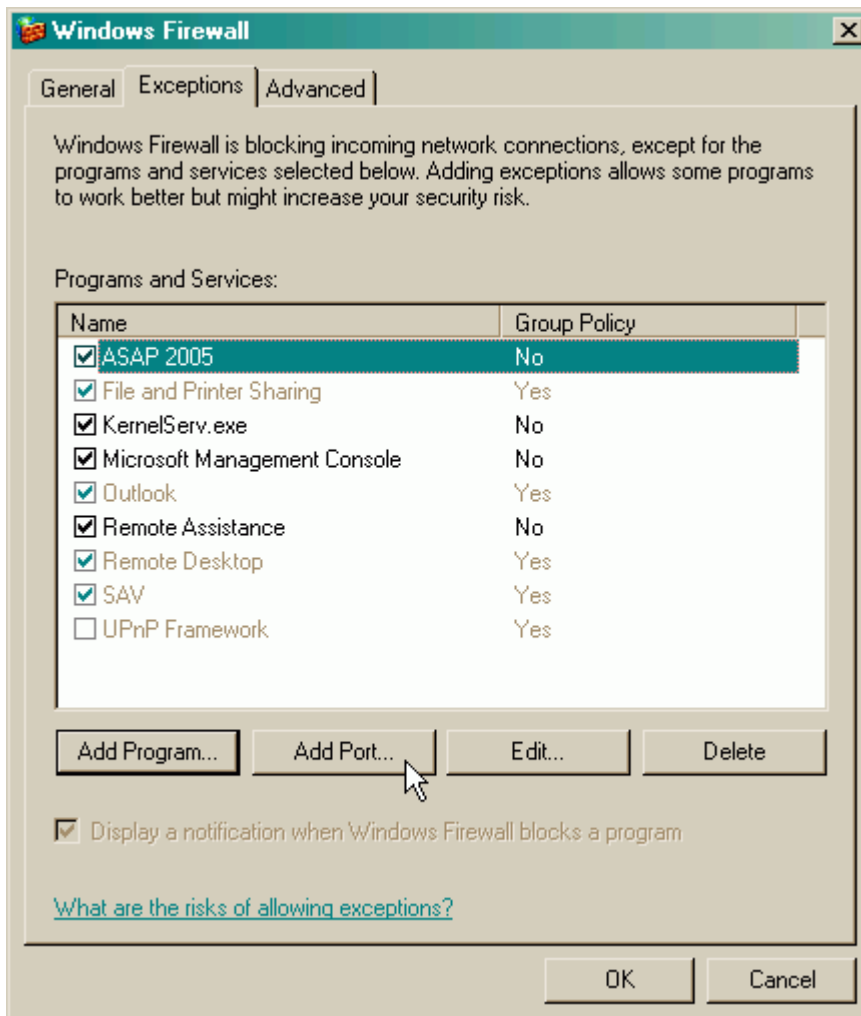
NOTE: If you prefer, you can limit the scope to machine IP by selecting **Custom list** and entering the IP address.

7. Click in the **Change Scope** dialog box, and then click again in the **Add a Program** dialog to apply changes.
8. Proceed to section E, Windows Firewall Settings – Add Exceptions for RPC Port 135.

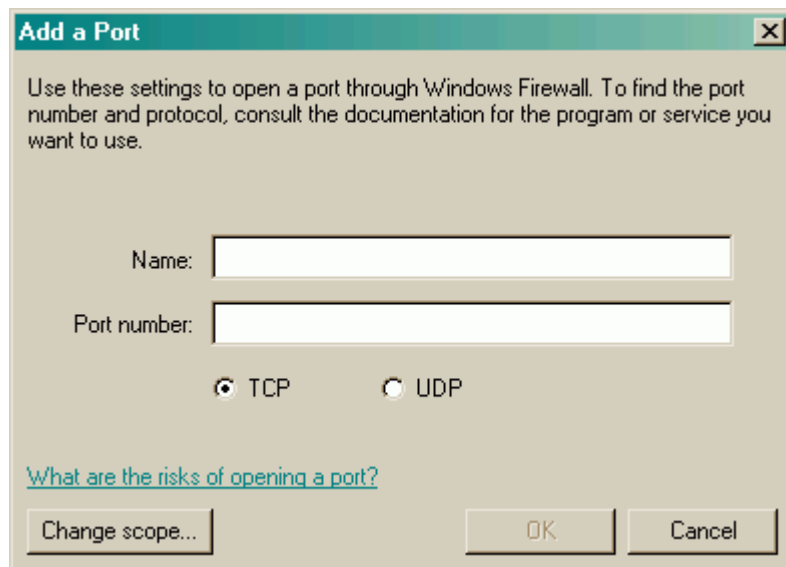
E. Windows Firewall Settings—Add Exceptions for RPC Port 135

In this section, you will set a firewall exception for the port protocol named RPC. If you are in the **Windows Firewall** dialog at the **Exceptions** page, proceed to set 3.

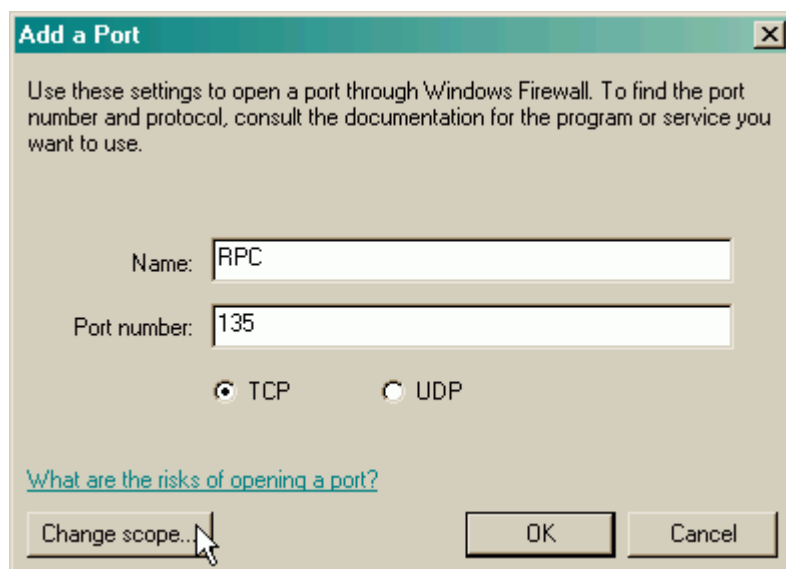
1. From the **Start** menu, select **Settings> Control Panel> Windows Firewall**.
2. Select the **Exceptions** tab.



3. Click **Add Port...** to open the **Add a Port** dialog box.



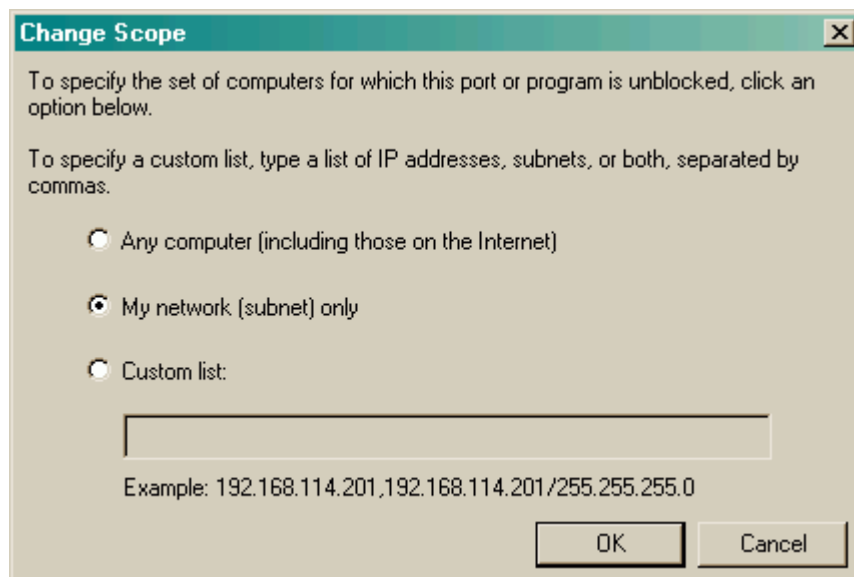
4. In the **Name** field, enter **RPC**.
5. In the **Port number** field, enter **135**.
6. Select **TCP** if it is not already selected.



7. Click **Change scope...** to open the **Change Scope** dialog box.

8. In the **Change Scope** dialog box, select **My network (subnet) only**.

NOTE: If you prefer, you can limit the scope to machine IP by selecting **Custom list** and entering the IP address.



9. Click **OK** on the **Change Scope** dialog box, and then click **OK** again in the **Add a Port** dialog box to apply changes.

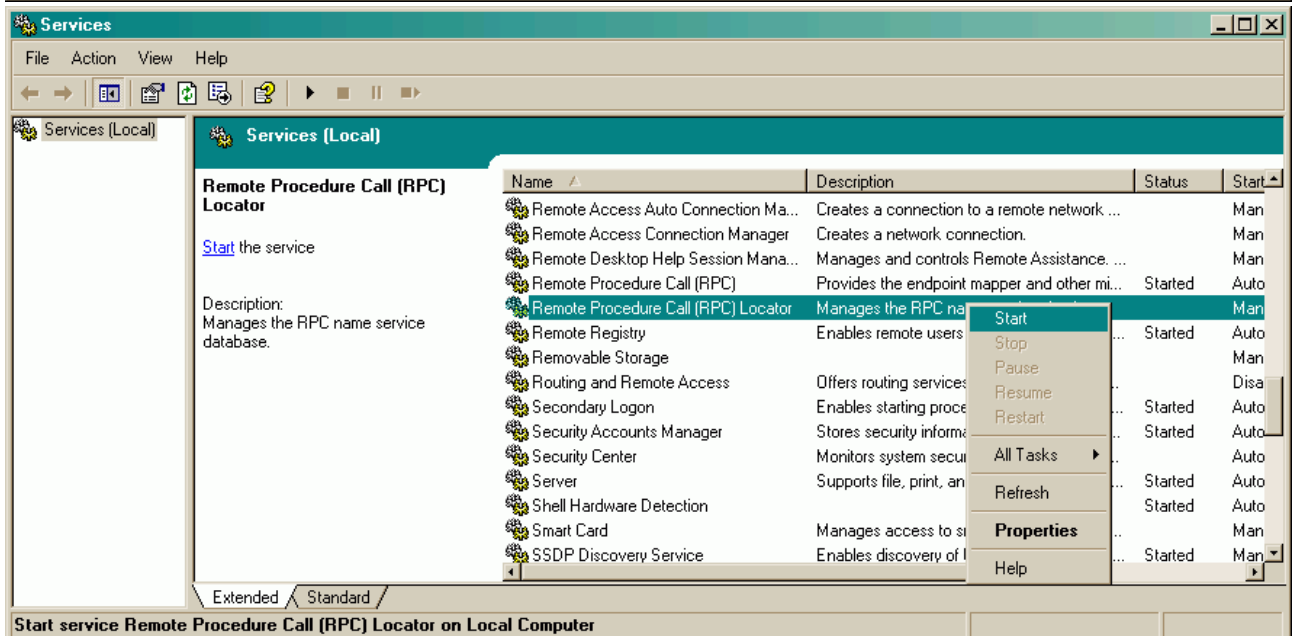
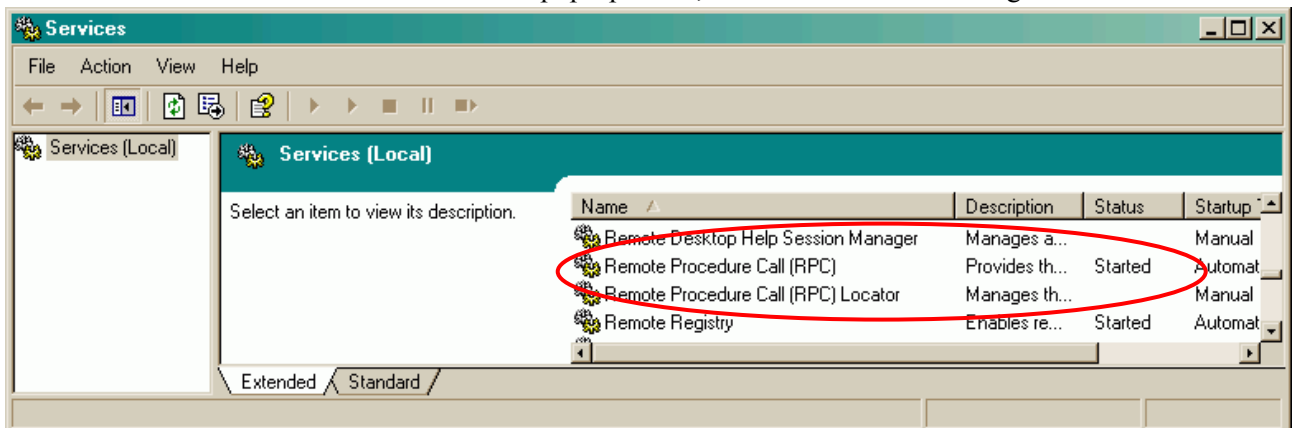
10. Click **OK** on the **Exceptions** dialog box to complete the changes.

11. Proceed to section F, Local Security Settings – Network Access: Sharing and security for local accounts.

F. Services—Remote Procedure Call (RPC) and Remote Procedure Call (RPC) Locator

In this section, you will confirm that local services, Remote Procedure Call (RPC) and Remote Procedure Call (RPC Locator), are set properly for network access.

1. From the **Start** menu, select **Settings> Control Panel> Administrative Tools> Services** to open the **Services** dialog box.
2. In the **Services** dialog box, verify that **Remote Procedure Call (RPC)** shows **Started** in the **Status** column, as shown in the first figure.
 - a) If the **Status** column entry is blank, right-click the service in the **Name** column and select **Start** from the pop-up menu.
3. Verify that **Remote Procedure Call (RPC) Locator** shows **Started** in the **Status** column.
 - a) If the **Status** column entry is blank, as shown below, right-click the service in the **Name** column and select **Start** from the pop-up menu, as shown in the second figure.

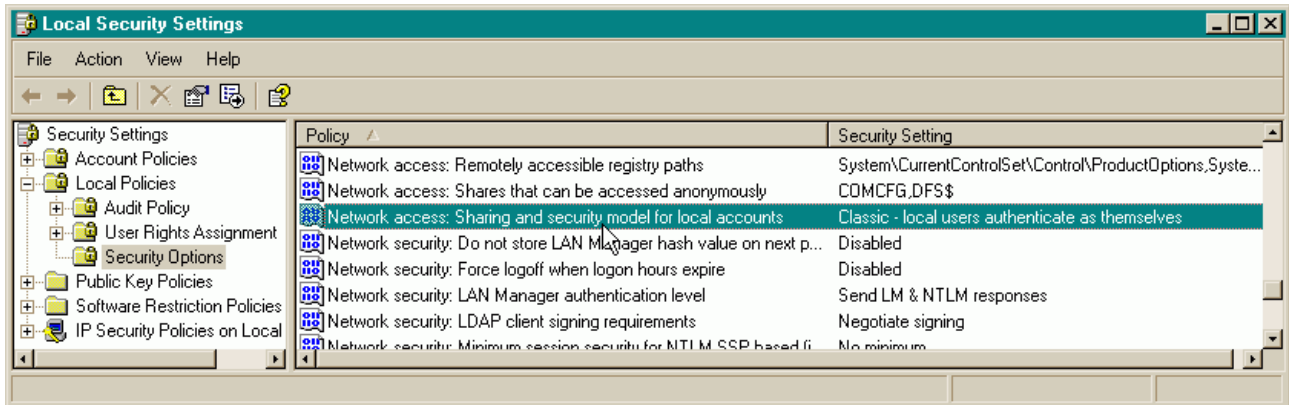


G. Local Security Settings—Network Access: Sharing and security model for local accounts:

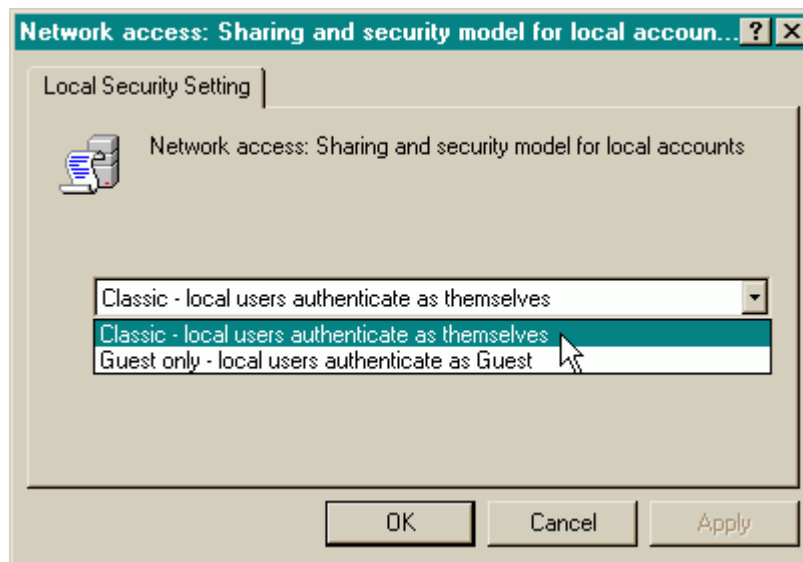
On the **Local Security Setting** page, confirm that **Network Access: Sharing and security model for local accounts** is set to **Classic – local users authenticate as themselves**.

Note: Please consult your network administrator before making a change to your system.

1. From the **Start** menu, select **Settings> Control Panel> Administrative Tools> Local Security Policy** to open the Explorer window for **Local Security Settings**.
2. Under **Security Settings> Local Policies> Security Options**, scroll on the right panel to **Network Access: Sharing and security model for local accounts**. Verify in the **Security Setting** column that the it shows **Classic – local users authenticate as themselves**.



3. If this is not the setting, double-click this **Network access** policy to open the dialog, **Network Access: Sharing and security model for local accounts**. Select **Classic – local users authenticate as themselves** from the drop-down menu. Click **OK**.



This completes the configuration for Windows XP with SP2 for ASAP Remote.

Reference: Technical Publication bro4315, ASAP REMOTE.