# For Windows XP Professional Service Pack 2 Users

***Note:*** *This document is an excerpt from the Secure Perfect® 6.1 Installation Manual.*

If you installed Secure Perfect on a Windows XP Professional operating system with Service Pack 2, the following adjustments must be made to your configuration, in order for Secure Perfect to run successfully. We assume that this is a basic installation of Windows XP Service Pack 2, with no other policies configured other than the base configuration within Windows XP.

## 1. Configuring Windows Firewall

➤ **To configure your Windows Firewall for access to the Database Server from a Secure Perfect client computer:**

1. Log on as a user with administrator permissions.

2. Click **Start**, **Settings**, **Control Panel**, then double-click **Windows Firewall**.

3. When the **Windows Firewall** window opens, select ONE of TWO configurations options:

   - Select **Off**.
   - Select **On** and select the **Exceptions** tab.

4. If you select **Off** (turns off Windows Firewall):

   - Click **OK** to exit this window.
   - Skip Step 5. through Step 26.
   - Continue with "Configuring Launch and Access Permissions" on page 3.

   If you select **On** and the **Exceptions** tab, configure the exceptions:

   - Proceed to Step 5., to configure the ports as indicated.

### Add Programs

5. Click **Add Program.**

6. One at a time, add the following programs to the exceptions list by selecting from the list of programs:

   - Diagnostic Viewer
   - Flashtool
   - Secure Perfect
   - SPLicense

7. Click **OK** to display the selected programs in the **Programs and Services** list.

## Add Ports

8. Click **Add Port**.

   ***Note:*** *To name the ports, type a short name for the port to help you remember for what it is used.*

   - Name the port and enter the SQL Server port number

     (This port number can be obtained from your Server Computer. At the Database Server computer for this client, click **Start**, then **Run** and enter `svrnetcn.exe`. Click **OK**. When the SQL Server Network Utility window displays, select **TCP/IP** and click **Properties**. The port number displays. Note this port number and return to the client computer.)
   - Add Ports 6700 through 6715 for TCP filtering.
   - Add Ports 6700 through 6715 for UDP filtering.
   - Add Port 1024 for TCP DVR filtering.
   - Add Port 135 for RPC filtering.
   - When all entries are complete, click **OK** to exit this window.

## Set Data Sources (ODBC)

***Note:*** *If the Database Server is not Windows XP, skip Step 9. through Step 15.and continue with "Set dcomcnfg Properties" .*

9. In the Control Panel, double-click **Administrative Tools**, then **Data Sources (ODBC)**.

10. On the **ODBC Data Source Administrator** window, select the **System DSN** tab.

11. Select **Secure Perfect SQL**.

12. Click **Configure** and click **Next**.

13. Click **Client Configure**.

14. De-select **Dynamically determine port**.

15. Enter SQL Server Port number, as obtained from the Server computer. (See Step 3. above.)

## Set dcomcnfg Properties

16. Click **Start**, select **Run**, enter `dcomcnfg`, and click **OK**.

    **Result:** The **Component Services** window displays.

17. Click to expand the **Components Services** navigation tree.

    **Result:** If the **Windows Firewall** is **Off**, a window displays the message, **Do you want to keep blocking this program?** Click **Unblock** and the window closes.

18. Again, click to expand the **Components Services** tree to display **My Computer** in the right window pane.

19. Right-click **My Computer** to display a shortcut menu and select **Properties**.

    **Result:** **My Computer Properties** window displays.

20. Click the **Default Protocols** tab.

21. When the **Properties for COM Internet Services** window displays, if not already there, you must add categories to the **DCOM Protocols** window pane. Click **Add**.

22. A **Select DCOM protocol** window displays with a drop-down list of Protocol Sequences from which to choose.

    - Select **Connection-oriented TCP-IP** and click **OK**.
    - Select **Datagram UDP/IP** and click **OK**.

    **Result:** Your selections display in the **DCOM Protocols** window pane.

23. Select **Connection-oriented TCP/IP Filtering** and click **Properties**, then **Add**. Proceed by adding port ranges 6700 through 6715 in the requested format.

24. Select **Datagram UDP/IP** and click **Properties**, then **Add**. Proceed by adding port ranges 6700 through 6715 in the requested format.

25. When all entries are complete, click **OK** to exit this window.

26. Continue with "Configuring Launch and Access Permissions" .

## 2. Configuring Launch and Access Permissions

In this section, you will be configuring two permissions:

- Launch Permission
- Access Permission

In this section, you will be configuring services:

- Secure Perfect System Manager
- Secure Perfect Manager
- Secure Perfect Diagnostics

➤ **To configure the Access and Launch permissions for 'Secure Perfect System Manager' service:**

1. Log on as a user with administrator permissions.

2. Click **Start**, **Settings**, **Control Panel**, **Administrative Tools**, then double-click **Component Services**.

3. In the right windowpane, expand the Component Services navigation tree to display **Computers**, **My Computer**, then **DCOM Config**.

4. Select **Secure Perfect System Manager** and right-click to display the shortcut menu.

5. Select **Properties** to display the properties window.

## Launch and Activation Permissions

6. Select the **Security** tab, and in the **Launch and Activation Permissions** grouping, select **Customize** and click **Edit**.

7. When the **Launch Permission** window displays, select the **Security** tab and click **Add**.

8. When the **Select Users, Computers, or Groups** window displays, click **Advanced**.

9. If you are asked to log on to the Domain, enter your login ID and password and click **OK**.

10. When you are returned to the **Select Users, Computers, or Groups** window, click **Find Now**.

11. When the **Name(RDN)** list displays in the lower windowpane, select **ANONYMOUS LOGON** and click **OK**, then **OK** in the window that follows.

12. Verify that all permission for **ANONYMOUS LOGON** are set to **Allow**. Click **OK**.

## Access Permissions

13. You are returned to the **Security** tab, and in the **Access Permissions** group, select **Customize** and click **Edit**.

14. When the **Launch Permission** window displays, select the **Security** tab and double-click **Add**.

15. When the **Select Users, Computers, or Groups** window displays, click **Advanced**.

16. If you are asked to log on to the Domain, enter your login ID and password and click **OK**.

17. When you are returned to the **Select Users, Computers, or Groups** window, click **Find Now**.

18. When the **Name(RDN)** list displays in the lower windowpane, select **ANONYMOUS LOGON** and click **OK**, then **OK** in the window that follows.

19. Verify that all permission for **ANONYMOUS LOGON** are set to **Allow**. Click **OK**.

***Note:** Ignore the **Configuration Permissions** grouping of the Security tab.*

➤ **To configure the Access and Launch permissions for ‘Secure Perfect Manager’ service and Secure Perfect Diagnostics:**

Repeat the steps as listed, beginning with “To configure the Access and Launch permissions for ‘Secure Perfect System Manager’ service:” on page 3; however, you will select ‘Secure Perfect Manager’ OR ‘Secure Perfect Diagnostics’ in the **DCOM Config** navigation tree, Step 4.

## 3. Configuring Local Security Settings

➤ **To configure the local security settings at each client computer:**

1. Log on as a user with administrator permissions.
2. Click **Start**, **Settings**, **Control Panel**, then **Administrative Tools**.
3. Double-click **Local Security Policy** in the right windowpane.
4. Expand the navigation tree to display Local Policies and select Security Options to display a list box of 'Policies' and 'Security Settings.'
5. Double-click **DCOM Machine Launch Restrictions. . .**
6. Click **Edit Security** and then click **Add**.
7. Click **Advanced**.
8. If you are asked to log on to the Domain, enter your login ID and password and click **OK**.
9. Click **Find Now**.
10. When the **Name(RDN)** list displays in the lower windowpane, select **ANONYMOUS LOGON** and click **OK**, then **OK** in the window that follows.
11. Verify that all permission for **ANONYMOUS LOGON** are set to **Allow**. Click **OK**.
12. Double-click **DCOM Machine Access Restrictions. . .**
13. Click **Edit Security** and then click **Add**.
14. Click **Advanced**.
15. If you are asked to log on to the Domain, enter your login ID and password and click **OK**.
16. Click **Find Now**.
17. When the **Name(RDN)** list displays in the lower windowpane, select **ANONYMOUS LOGON** and click **OK**, then **OK** in the window that follows.
18. Verify that all permission for **ANONYMOUS LOGON** are set to **Allow**. Click **OK**.
19. Exit the **Local Security Setting** window.
20. Continue with "Creating a New Registry Key" .

## 4. Creating a New Registry Key

➤ **To create a new system registry key and set a value that causes the system to bypass RPC interface restrictions:**

1. Click **Start**, then **Run**, and enter `regedit`.

2. Expand the navigation tree in the left windowpane to display HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\ Windows NT.

3. Right-click Windows NT to display a shortcut menu and select **New**, then **Key**.

4. Enter `RPC` as the title of the new key, and then click **Enter**.

5. Right-click RPC to display a shortcut menu, select **New**, and then select **DWORD Value**.

6. Enter the DWORD Value as `RestrictRemoteClients` and click **Enter**.

7. Right-click **RestrictRemoteClients** and select **Modify**.

8. When the **Edit DWORD Value** window displays, verify that the value equals `0`.

9. Click **OK**.

10. Exit the Registry Editor.

## 5. Restart Computers

1. Any computers (Server computers or client computers) that had adjustments to the configuration because Windows XP Professional Service Pack 2 is being used in your Secure Perfect system, must be restarted at this time.

2. Continue with "Licensing Your Secure Perfect System" on page 4.19 of your *Secure Perfect 6.1 Installation Manual*.