

# Using ManageSoft with Windows XP SP2 or Windows 2003 Server SP1

*ManageSoft knowledge base article 100611*

Windows XP Service Pack 2 (SP2) and Windows Server 2003 SP1 include a number of functionality changes, some of which affect the operation of ManageSoft.

The most significant feature that affects ManageSoft is the introduction of Windows Firewall (known in earlier releases of Windows XP as Internet Connection Firewall (ICF)), which is enabled by default. Some configuration of Windows Firewall is required to enable ManageSoft to function.

Windows XP SP2 and Windows 2003 Server SP1 also use Windows Installer 3.0, which does not support FTP. See *ManageSoft and Windows Installer 3.0* on page 10 for details about the possible effects of this on your ManageSoft infrastructure.

MBSA 1.2.1 is required to use ManageSoft Security Patch Management on devices that have Windows XP SP2 or Windows Server 2003 SP1 installed. If you will use ManageSoft Security Patch Management with these managed devices, use one of the following releases:

- ▶ ManageSoft Security Patch Management 7.1.2
- ▶ ManageSoft Security Patch Management 7.2.1 and later releases.

## Configuring Windows Firewall

Some configuration of Windows Firewall is required to enable ManageSoft to function if:

- ▶ The File protocol is to be used to distribute packages from or upload status data to Windows XP SP2 or Windows 2003 Server SP1 computers
- ▶ Any of the HTTP, HTTPS, or FTP protocols are to be used for distributing packages from or uploading status data to Windows XP SP2 or Windows 2003 Server SP1 computers
- ▶ Windows XP SP2 or Windows 2003 Server SP1 computers are to be discovered and adopted under management, or execute remote execution tasks.

You can choose either to:

- ▶ Completely disable Windows Firewall (not recommended unless other firewall software is operating)

- ▶ Selectively configure Windows Firewall to permit ManageSoft to function.

If you choose to configure Windows Firewall, you will need to configure it on any Windows XP SP2 or Windows Server 2003 SP1 computers:

- ▶ Operating as distribution servers or warehouse servers
- ▶ Operating as managed devices
- ▶ That are not currently running ManageSoft, but on which you want to perform a zero-touch inventory, or that will be targeted for adoption into management.

Further details about the configuration required on each of these classes of computer are provided below.

You can configure Windows Firewall:

- ▶ As part of the initial rollout of Windows XP SP2 or Windows Server 2003 SP1, using a `Netfw.inf` file
- ▶ On distribution servers, during installation of, or upgrade to, ManageSoft 7.2
- ▶ Using Group Policy (recommended if you have Active Directory deployed throughout your enterprise)
- ▶ Using ADM templates or logon scripts (recommended if you have NT domains)
- ▶ By deploying a ManageSoft package containing a script to execute (useful if all Windows XP SP2 and Windows Server 2003 SP1 computers in your enterprise are already under ManageSoft management)
- ▶ Locally on each computer (not recommended in a managed environment, for obvious reasons).

Further details about the recommended methods of configuring Windows Firewall are provided below.

## Required Windows Firewall settings

As mentioned previously, Windows Firewall requires different configuration depending on the role (distribution server, warehouse server, managed device, computer not yet under management) of the computer being configured.

### Distribution servers

When you are installing or upgrading ManageSoft on distribution servers, the installation/upgrade script provides the option to configure the Windows Firewall

exceptions necessary to allow ManageSoft to function. Refer to the *ManageSoft Implementation Guide* and/or the *ManageSoft Upgrade Guide* for details.

Follow the instructions below if you chose not to configure Windows Firewall automatically during ManageSoft installation. Alternatively, develop your own script to configure Windows Firewall according to your requirements. You can download a sample script, `netfw.vbs`, that you can customize for your requirements. See *Configuring Windows Firewall using a ManageSoft package* on page 9 for more details.

### Job server

ManageSoft Corporation recommends that distribution servers be configured to poll for jobs from parent distribution servers rather than listen for jobs. Distribution servers that use the listening agent require additional configuration to allow inbound TCP connections on port 7010. Set one of the following exceptions:

- ▶ For **Define program exceptions**, type this definition string:  
`%ProgramFiles%\ManageSoft\Replicator\ndlisten.exe:*:enabled:ManageSoft Connection Agent`
- ▶ For **Define port exceptions**, type this definition string:  
`7010:TCP:*:Enabled:ManageSoft Connection Agent`

In both these examples, `*` is specified as the subnet, meaning that incoming TCP connections on this port are accepted from computers anywhere on the network. Consult *Deploying Windows Firewall Settings for Microsoft® Windows® XP with Service Pack 2* for allowable subnet values. ManageSoft Corporation recommends the use of `localsubnet` when appropriate.

### Connections from child distribution servers and managed devices

Distribution servers receive inbound connection requests from child distribution servers and managed devices on ports 139 and 445. Enable the **Allow file and print sharing exception** to allow these connections.

Distribution servers also receive ICMP echo “ping” requests if managed devices are configured to ping before attempting to establish a connection. (This behavior is governed by the **NetworkSense** ManageSoft preference.) Enabling the **Allow file and print sharing exception** permits these (as does enabling **Allow remote administration exception** or the **Allow ICMP exceptions** with **Allow inbound echo request** selected).

In their capacity as Web/FTP servers, distribution servers receive inbound connection attempts on ports 21 and 80. Configure IIS to allow communication on these ports. (Consult the IIS documentation for instructions.)

## Warehouse servers

If you are running a warehouse core server on a Windows XP SP2 or Windows Server 2003 SP1 computer, the Windows Firewall configuration required is the same as that required for distribution servers, with the exception that the listening agent is not used on the warehouse. That is, you must configure IIS to allow inbound connections on ports 21, 80, and 443. Consult the IIS documentation for instructions.

If you are running a warehouse web server on a Windows XP SP2 or Windows Server 2003 SP1 computer, you must configure IIS to allow inbound connections on port 80.

If you are running a warehouse data server on a separate physical server from your warehouse core and/or web servers, you will need to configure Windows Firewall exceptions to allow SQL Server to listen to the network and receive TCP/IP connections. Refer to the Microsoft website (in particular, <http://support.microsoft.com/default.aspx?scid=kb;en-us;841249>) for details about configuring Windows Firewall for use with SQL Server.

## Other Windows XP SP2 or Windows Server 2003 SP1 computers

The following sections outline the Windows Firewall configuration required on computers other than distribution servers.

### Discovery, adoption, remote execution, and zero-touch inventory

In order to successfully use ManageSoft discovery (including determining remote execution credentials), adoption, remote execution, and zero-touch inventory functionality, you must configure Windows Firewall to accept inbound connections from the relevant distribution server on port 445. You can achieve this in any of these ways:

- ▶ By enabling the **Allow file and print sharing exception**
- ▶ By enabling the **Allow remote administration exception** (recommended)
- ▶ By configuring **Define port exceptions** with port 445 and transport TCP.

## Remote control of managed devices

If you use ManageSoft in conjunction with remote control software such as TightVNC, you must perform some additional configuration of Windows Firewall on managed devices running Windows XP SP2 or Windows Server 2003 SP1.

If your remote control application uses any fixed ports, use the Windows Firewall **Define port exceptions** setting to selectively open the ports used by the remote control application.

If your remote control application uses dynamically-assigned ports for incoming connections, use the Windows Firewall **Define program exceptions** setting to specify the filename of the remote control application.

**Be aware:** Use this same process to configure Windows Firewall to operate with other software, such as Symantec Ghost, if required.

## Configuring Windows Firewall during initial Windows XP SP2 rollout

*If computers in your enterprise already have Windows XP SP2 installed, this section is not relevant.*

You can configure Windows Firewall during installation of Windows XP SP2 or Windows Server 2003 SP1.

If you have not already done so, download *Using the Windows Firewall INF File in Microsoft Windows XP Service Pack 2* from the Microsoft website (<http://www.microsoft.com/downloads/details.aspx?familyid=cb307a1d-2f97-4e63-a581-bf25685b4c43>), and familiarize yourself with its contents.

You can download a sample `Netfw.inf` file from the ManageSoft knowledge base. You can replace the default `Netfw.inf` file with this sample file, or copy and paste the relevant lines from the sample file to the `Netfw.inf` file you will use with your Windows XP SP2 or Windows Server 2003 SP1 rollout.

To edit or replace the default `Netfw.inf` file with this sample file:

- 1 If you are using a CD image of Windows, copy it to a local filesystem so that you can edit `Netfw.inf`. (If your Windows image is already on a filesystem, proceed to the next step.)

- 2 Use `expand.exe` to uncompress a copy of `Netfw.in_` from the `ic` or `ip` directory (the copies of the file are the same).

**Be aware:** *Using the Windows Firewall INF File in Microsoft Windows XP Service Pack 2* incorrectly lists the location of `Netfw.in_` as `Cd_drive:\I386\Netfw.in_`.

The expanded `Netfw.in_` file is renamed `Netfw.inf`.

- 3 Replace `Netfw.inf` with the sample file from the ManageSoft knowledge base, or edit this file to suit your environment.

If you are using the sample file, you need to uncomment the appropriate lines to perform the configuration in your environment, according to whether or not the computers being configured are connected to an Active Directory domain.

Uncomment lines by removing their leading semicolons (;).

[...]

```
; Uncomment these two lines to enable Remote Administration when
; connected to the domain
;HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\Fir
ewallPolicy\DomainProfile\RemoteAdminSettings","Enabled",0x00010001,
1
;HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\Fir
ewallPolicy\DomainProfile\RemoteAdminSettings","RemoteAddresses",0x0
0000000,""
```

[...]

```
; Uncomment these two lines to enable Remote Administration when not
; connected to the domain
;HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\Fir
ewallPolicy\StandardProfile\RemoteAdminSettings","Enabled",0x0001000
1,1
;HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\Fir
ewallPolicy\StandardProfile\RemoteAdminSettings","RemoteAddresses",0
x00000000,""
```

- 4 Use `makecab.exe` to recompress `Netfw.inf` and rename it to `Netfw.in_`.
- 5 Replace the copies of `Netfw.in_` in both the `ip` and `ic` directories of your Windows image with your updated version.

---

## Configuring Windows Firewall using Group Policy

If you have Active Directory deployed throughout your enterprise, you can configure Windows Firewall using Group Policy.

If you have not already done so, download the document *Deploying Windows Firewall Settings for Microsoft® Windows® XP with Service Pack 2* from the Microsoft website (<http://www.microsoft.com/downloads/details.aspx?FamilyID=4454e0e1-61fa-447a-bdcd-499f73a637d1&DisplayLang=en>).

Follow the instructions in *Deploying Windows Firewall Settings for Microsoft® Windows® XP with Service Pack 2* to update your Group Policy objects with the new Windows Firewall settings, making suitable adjustments if you are using Windows Server 2003 SP1.

Then, for each of the Windows Firewall settings discussed above that is relevant to your enterprise, follow the instructions in *Deploying Windows Firewall Settings for Microsoft® Windows® XP with Service Pack 2* to specify the Windows Firewall settings for appropriate Group Policy objects. Again, make appropriate adjustments if you are using Windows Server 2003 SP1.

There are two profiles that use the Windows Firewall Group Policy settings:

- ▶ The **domain** profile is used when a Windows XP SP2 or Windows Server 2003 SP1 computer connects to the network that contains the organization's domain controllers
- ▶ The **standard** profile is used in other cases (for example when a computer connects to the Internet using a public ISP rather than through enterprise networks).

ManageSoft Corporation recommends that the firewall exceptions be configured under the domain profile only, since the ManageSoft functions allowed by these exceptions are typically only required when the computer is operating in the enterprise network environment.

## Configuring Windows Firewall using ADM templates

If you do not have Active Directory implemented across your enterprise, you cannot configure Windows Firewall through Group Policy. An alternative in NT domains is to use ADM templates (administrative templates), which allow configuration of both the User (HKEY\_CURRENT\_USER) and Local Machine (HKEY\_LOCAL\_MACHINE)

sections of the registry database. (You could also use logon scripts, but they only work for users with administrative privileges.)

You can download a sample ADM template file, `winxp.adm`, from the ManageSoft knowledge base. This file defines and describes Windows Firewall properties that are not known to Windows NT by default.

You can use this file with the System Policy Editor (`poledit.exe`) to create one or more policy (`.POL`) files. These policy files are stored on each domain controller to which Windows XP SP2 or Windows Server 2003 SP1 computers may connect.

To use the `winxp.adm` file to create a policy file, complete the following steps:

- 1 Save the downloaded `winxp.adm` file to `\WINNT\Inf` on the machine on which you will create the policy file.
- 2 Start the System Policy Editor (**Start > Run > poledit.exe**).
- 3 From the **Options** menu, select **Policy Template...**  
The **Policy Template Options** dialog is displayed.
- 4 Click **Add...**  
The **Open Template File** dialog is displayed.
- 5 In the **File name** field, enter (or browse to) `\WINNT\Inf\winxp.adm`.
- 6 Click **Open**.  
The **Open Template File** dialog closes.
- 7 Click **OK** to close the **Policy Template Options** dialog.
- 8 Open an existing policy (`.POL`) file or create a new one, and edit the Windows Firewall properties of the Default Computer or the computers to which this policy file will apply, according to the recommended settings outlined in *Required Windows Firewall settings* on page 2.
- 9 Save your policy file and copy it to `\NETLOGON\ntconfig.pol` on each domain controller to which Windows XP SP2 or Windows Server 2003 SP1 computers in your enterprise may connect.

The settings from `ntconfig.pol` are picked up by relevant computers at their next reboot. After the settings have been applied on a computer, they appear in `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall` and `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy`.



## Configuring Windows Firewall using a ManageSoft package

If all Windows XP SP2 and Windows Server 2003 SP1 computers in your enterprise are already under ManageSoft management, you can create one or more packages containing scripts to configure Windows Firewall.

You can download a sample VBScript, `netfw.vbs`, from the ManageSoft knowledge base. It configures the necessary Windows Firewall exceptions to allow ManageSoft to run. You can customize this script to suit your own environment if required.

Alternatively, if you plan to write your own script to deploy to managed devices, you can extract the appropriate `netsh` commands from `netfw.vbs` to use in your own script.

You might choose to create two packages:

- ▶ One containing a script to configure Windows Firewall on distribution servers and warehouse servers
- ▶ One containing a script to configure Windows Firewall on managed devices.

In each case, make sure that the script runs as `SYSTEM`, not the user currently logged in.

Consult your ManageSoft support representative for help if necessary.

### The sample `netfw.vbs` script

The following lines from the `netfw.vbs` script map a port number (in this case, 7010, used by the ManageSoft listening agent) so that you can enable Windows Firewall exceptions on it:

```
set objPort = objShareCfg.AddPortMapping( _  
    "ManageSoft Connection Agent", _  
    6, 7010, 7010, _  
    0, "127.0.0.1", 1)
```

The following lines enable the Windows Firewall exceptions on ports 21, 80, 443, and 7010:

```
Set objPorts = objShareCfg.EnumPortMappings(0)  
If (IsObject(objPorts) = TRUE) Then  
    For Each objPort in objPorts  
        Dim objPortProps  
        Set objPortProps = objPort.Properties
```

```
        Select Case objPortProps.InternalPort
            Case 21    objPort.Enable
            Case 80    objPort.Enable
            Case 443   objPort.Enable
            Case 7010  objPort.Enable
        End Select
    Next
End If
```

Consult the Microsoft documentation for details about other `netsh` commands you might need. For example:

- ▶ `netsh firewall set service FILEANDPRINT ENABLE CUSTOM * ALL` enables file and print sharing exceptions
- ▶ `netsh firewall set service REMOTEADMIN ENABLE CUSTOM * ALL` will allow ManageSoft remote execution and adoption to function successfully.

## ManageSoft and Windows Installer 3.0

Microsoft Windows XP SP2 and Windows Server 2003 SP1 use Windows Installer 3.0, which does not support FTP.

Change the properties of any distribution servers or locations that host Windows Installer files for installation directly from that location. Refer to *To change a distribution location's properties* in the *ManageSoft Operations Guide* and warehouse online help for details about changing the properties of a distribution location.