Security Settings for Wonderware® Products

Created: August 2005
Updated: May 2007

Introduction

Wonderware has released an OS Configuration Utility to support our products on Windows XP SP2 and Windows Server 2003 SP1. If you have not tried using the utility, please go to **Wonderware Technical Support** and download the OS Configurator Utility. If you have already run the utility and are still having problems running Wonderware software, you may need to configure some security settings manually.

There are several reasons that the OS Configurator Utility does not allow Wonderware software to function properly on a Windows XP SP2 or Windows Server 2003 SP1 node. The most likely reason is that the system is part of a Windows 2000 or Windows 2003 Active Directory Domain. If the Active Directory Domain locks down security at the domain level, the utility is not successful in changing the security settings. In this case, the security settings must be changed manually by the network administrator. Alternatively, the network administrator can set it up so that the user is allowed to change security settings on Windows nodes. This allows the utility to set security settings without being overwritten by the domain policies.

If you are having problems running Wonderware software on Windows XP SP2 or Windows Server 2003 SP1, the first thing that Wonderware recommends doing is shutting off the built-in Windows firewall. This software firewall is only useful if you do not have a hardware or corporate firewall protecting your systems from the outside world. If the firewall is not your problem, and you have run the OS Configurator Utility, you must set the following settings manually.

Assumptions

This document simply states what the settings that need to be changed. It does not describe the way to change these settings. If you do not know how to change security settings in Windows or on the Active Directory Domain, you should not be doing it. Please see your network administrator or refer to your Windows Documentation.

This document classifies the necessary settings by Wonderware Software Components. You must know the full path to the files listed below, and you must have administrative rights to the system in order to make these changes.

Application Versions

This document applies to all Wonderware products that are supported on Windows XP SP2 and Windows Server 2003 SP1.

DCOM Global Settings

These settings are used by multiple Wonderware components including IAS and DA Servers:

- Security settings (in Component services)
- Component Services Com Security
- **Launch** and **Activation** Permissions
- **Everyone** and **Remote Activation**
- Access Permission
- Add **Local Access** and **Remote Access** permissions for the **ANONYMOUS** user.

Archestra LogViewer

Used by all FactorySuite A² components including InTouch, IAS, InSQL, DA Servers.

Make the following entry into the registry:

```
HKLM\Software\Policies\Microsoft\WindowsNT\RPC\RestrictRemoteClients = 0
```

SuiteLink

Used by all Wonderware products.

Add the following to the firewall settings exception list:

- `slssvc.exe`

InTouch

Requires SuiteLink common component modification.

Add following programs in exception list:

- `wm.exe`

InSQL

Requires SuiteLink common component modification.

The following processes need to be added to the firewall exclusion list:

- `InSQLData.exe`
- `InSQLConfig.exe`
- `InSQLSCM.exe`
- `InSQLRet.exe`

- SQLServr.exe

Add the following ports to the Firewall exception list:

File and printer sharing	445/tcp
SQL Server Browser	1434/udp
SQL TCP	1433/tcp
DCOM	135/tcp

Industrial Application Server

Requires SuiteLink common component modification.

Add Application list to be excluded in firewall blocking list:

- aaIDE.exe
- aaLogger.exe
- Slssvc.exe
- aaPim.exe
- BootStrap.exe
- aaDcomTransport.exe
- SQLServr.exe
- NmxSvc.exe

Add the following ports to the Firewall exception list:

DCOM	135/tcp
File and printer sharing	445/tcp
SQL TCP	1433/tcp
SQL Server Browser	1434/udp

DA Servers

Requires SuiteLink common component modification.

Add the following ports to the Firewall exception list:

DAS SI Direct	102
DAS MBTCP	502
DAS ABTCP	2221
DAS ABTCP	2222
DAS ABTCP	2223
S/L DA Servers	5413
DAS ABCIP	44818

The following files need to be excluded in the firewall. They are common to all DA Servers:

- aaEngine.exe
- NmxSvc.exe
- OPCEnum.exe
- Dllhost.exe
- DASAgent.exe

The following files need to be excluded in the firewall. They are specific to each DA Server:

- DASABCIP.exe
- DASMBTCP.exe
- DASABTCP.exe
- DASSIDirect.exe
- FSGateway.exe
- DASS7.exe
- S7ConSvr.exe
- DASMBSerial.exe
- DASMBPlus.exe
- DASAlarm2U.exe

If you are using Industrial Application Server and are planning on deploying DI Objects you will need to manually exclude the following files in the firewall. You will need to create dummy files with these names as they are not on the system until a deploy occurs. Windows XP SP2 firewall will not exclude files unless they already exist on the system. These files are deployed to the **\Program Files\Archestra\Framework\Bin** directory.

- DASABCIP.exe
- DASMBTCP.exe
- DASABTCP.exe
- DASSIDirect.exe
- DASS7.exe
- DASMBSerial.exe

- DASMBPlus.exe
- DASAlarm2U.exe
- aaEngine.exe
- NmxSvc.exe
- DASAgent.exe

The following file is deployed to the \Windows\System32 sub-directory:

OPCEnum.exe

IO Servers

Requires SuiteLink common component modification.

InBatch

1. Add ports (9001 - 9016) list to be excluded in firewall blocking list for communication:

Vista	9001/tcp
EnvMngr	9002/tcp
MsgMngr	9003/tcp
SecMngr	9004/tcp
RedMngr	9006/tcp
UnilinkMngr	9007/tcp
BatchMngr	9008/tcp
LogMngr	9011/tcp
InfoMngr	9012/tcp
RedMngrX	9013/udp
RedMngrX2	9014/udp
HistQMngr	9015/tcp
HistQReader	9016/tcp

2. Enable **File and Printer Sharing**:

File and printer sharing	445/tcp

3. Add the InBatch Server to the Local Intranet Zone in Internet Explorer as a trusted site. If the InBatch Server site is not a secured site, you may need to change the Local Intranet Zone to allow unsecured sites.

InControl

Requires SuiteLink common component modification.

Add following programs to the exception list:

- ICDev.exe

- RTEngine.exe
- ICOPCServer.exe

Modifications must be made to the firewall registry settings if you frequently switch between Domain and Workgroup logons. If you do, set both the Domain and Standard profiles so that all Wonderware products are configured in *both* profiles. These profiles are located in the registry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FIrewallPolicy

There is one key per firewall policy. The profile in effect when the machine is connected to the domain is under the key **DomainProfile**. The profile in effect when the machine is not connected to the domain is under the key **StandardProfile**.

The list of application exceptions for each profile is stored as a set of string values under the profile subkey of AuthorizesApplications\List. The list of port exceptions for each profile is stored as a set of string values under the profile subkey of GloballyOpenPorts\List.

So, to see in the registry what application exceptions are in force for the domain firewall profile, look at the values under the following key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\SharedAccess\Parameters\FirewallPolicy\DomainProfile\AuthorizedApplications\List

To see in the registry what port exceptions are in force for the domain firewall profile, look at the values under the following key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\SharedAccess\Parameters\FirewallPolicy\DomainProfile\GloballyOpenPorts\List

To see the exceptions in force for the workgroup policy, please look in the following locations:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List

R. Ekstein

Click the following icon to view this file in .pdf format:

Tech Notes are published occasionally by Wonderware Technical Support. Publisher: Invensys Systems, Inc., 26561 Rancho Parkway South, Lake Forest, CA 92630. There is also technical information on our software products at **Wonderware Technical Support**

back to top