Tech Note 461
Troubleshooting Industrial Application Server Bootstrap Communications

All Tech Notes and KBCD documents and software are provided "as is" without warranty of any kind. See the **Terms of Use** for more information.

Topic#: 002178
Created: January 2007
Updated October 2009

Introduction

This *Tech Note* outlines general troubleshooting steps to address communication issues between a remote node and an Industrial Application Server Galaxy.

Application Versions

- Industrial Application Server version 2.1 and older. Please check the compatability matrix at the Wonderware Tech Support site for supported operating systems.
- Windows® 2000 Server and Server 2003 with all Service Packs and Releases

Note: If you are having trouble opening the SMC logger from a client node or the Server node, please see Tech Note 437: **Unable to Open Logger Under Windows XP SP2 and Windows 2003 SP1**.

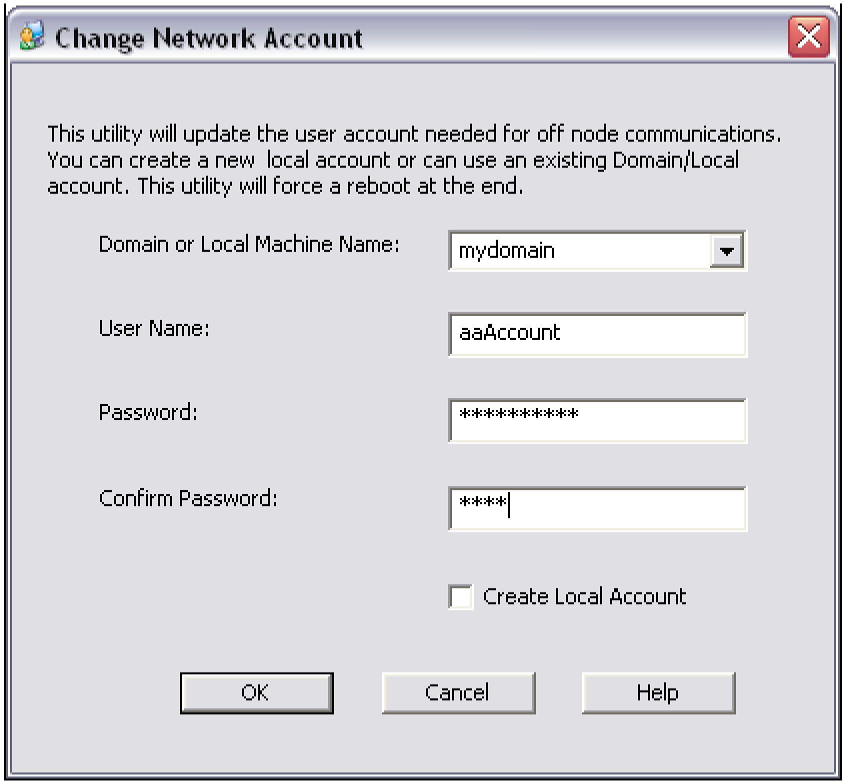
Wonderware Configuration Tools

Use the following Wonderware Configuration tools when troubleshooting the application.

Wonderware Change Network Account Utility

To ensure that the ArchestrA Network Admin Account is the same on all machines that are part of the Galaxy (or wish to interact with nodes on the Galaxy)

1. Launch the **Change Network Account** utility from **Start/All Programs/Wonderware/Common/Change Network Account**.



This utility will update the user account needed for off node communications. You can create a new local account or can use an existing Domain/Local account. This utility will force a reboot at the end.

Domain or Local Machine Name: mydomain

User Name: aaAccount

Password: **********

Confirm Password: ****

□ Create Local Account

Figure 1: Change Network Account Utility Interface

2. Ensure that the local machine name does not have any unusual characters such as a tilde (~) or underscore. These characters can cause communication errors.

Wonderware O/S Configuration Utility

To run the Wonderware O/S Configuration Utility for WinXP SP2 and Windows 2003 SP1

1. Click **Start/All Programs/Wonderware/Common/OSConfiguration Utility**.

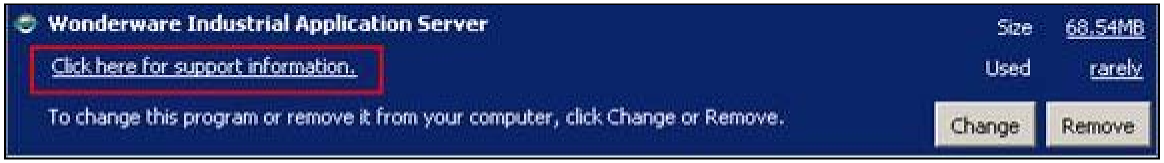
   You can also download the utility from: **www.Wonderware.com/support/mmi**.

   For a complete list of what the utility does, please refer to the Tech Article **Security Settings for Wonderware Products**.

2. Reboot the machine after running the O/S Configuration Utility.

Wonderware Application Versions

1. Ensure that the version of Industrial Application Server installed on the remote node is the same as the version of Industrial Application Server Galaxy.
2. Verify the version by going to Add/Remove Programs and clicking **Click here for support information** on the Wonderware Industrial Application Server program. Verify the versions on both the Galaxy Repository (GR) Node and on the remote node.



Wonderware Industrial Application Server

Click here for support information.

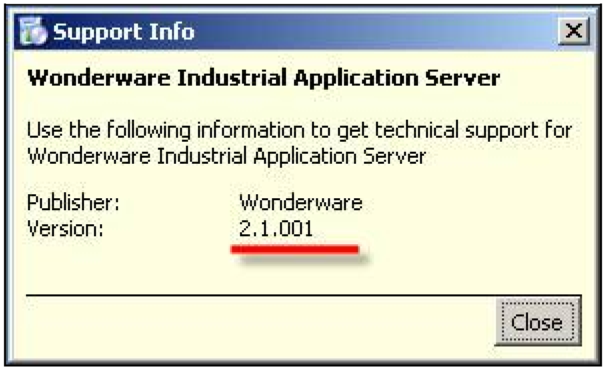
To change this program or remove it from your computer, click Change or Remove.

Size 68.54MB

Used rarely

Figure 2: Add/Remove Programs Version Check

In the example shown below, the version of Industrial Application Server is 2.1 Patch 01.



Support Info

Wonderware Industrial Application Server

Use the following information to get technical support for Wonderware Industrial Application Server

Publisher: Wonderware
Version: 2.1.001

Figure 3: Support Info Dialog Box

Checking Windows DCOM Configuration

The DCOM Ports used by the Bootstrap are:

- Port 135
- Port 139
- Port 445
- Ports 1024 to 65535

For additional info see:

- http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndcom/html/msdn_dcomfirewall.asp
- http://support.microsoft.com/kb/832017
- http://www.linklogger.com/TCP135.htm
- http://www.linklogger.com/TCP139.htm
- http://www.linklogger.com/TCP445.htm

Do the following tasks to ensure DCOM settings are correct.

DCOM – Checking Wonderware Compatible Security Settings

1. Run dcomcnfg.exe from the Start menu, Run command.

   This is the area where you make local DCOM changes that control DCOM security levels on the computer.

2. Expand the branches as follows:

   Component Services/Computers/MyComputer.

3. Right-click **My Computer** and select **Properties**.

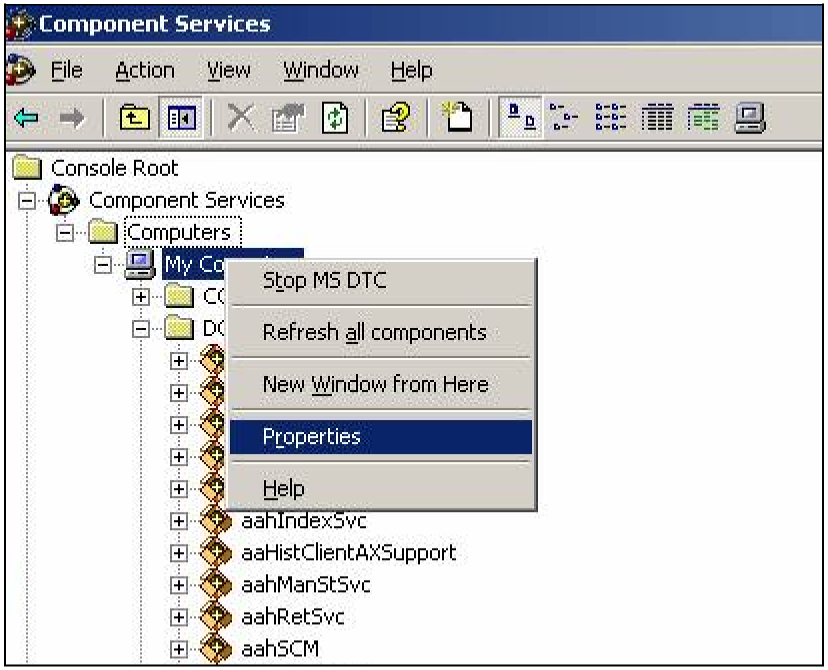
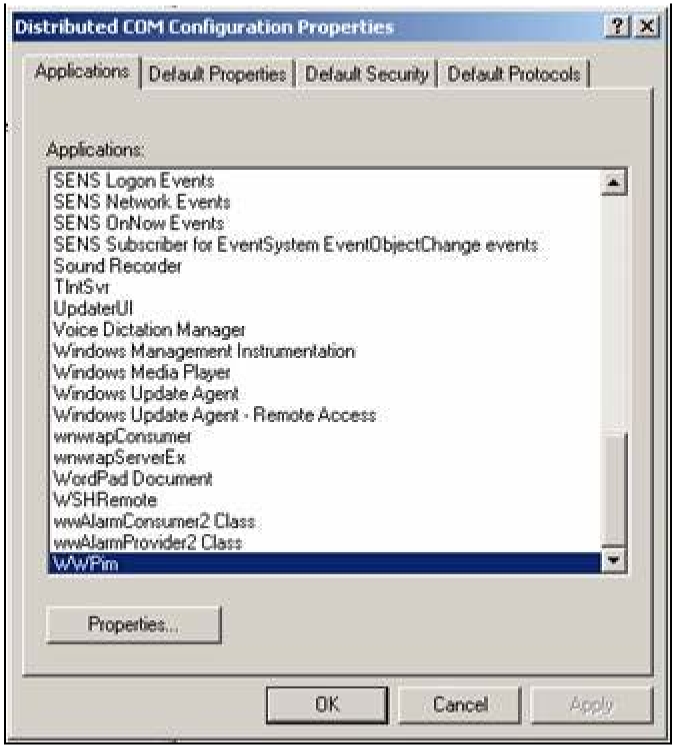


Figure 4: Access DCOM Properties

4. Check the following packages.

- The first package is WWPIM (aka Wonderware Platform Information Manager)
- In Windows 2000, click the **Properties** button, or in Windows 2003 or XP, right click **WWPIM** and select **Properties**.

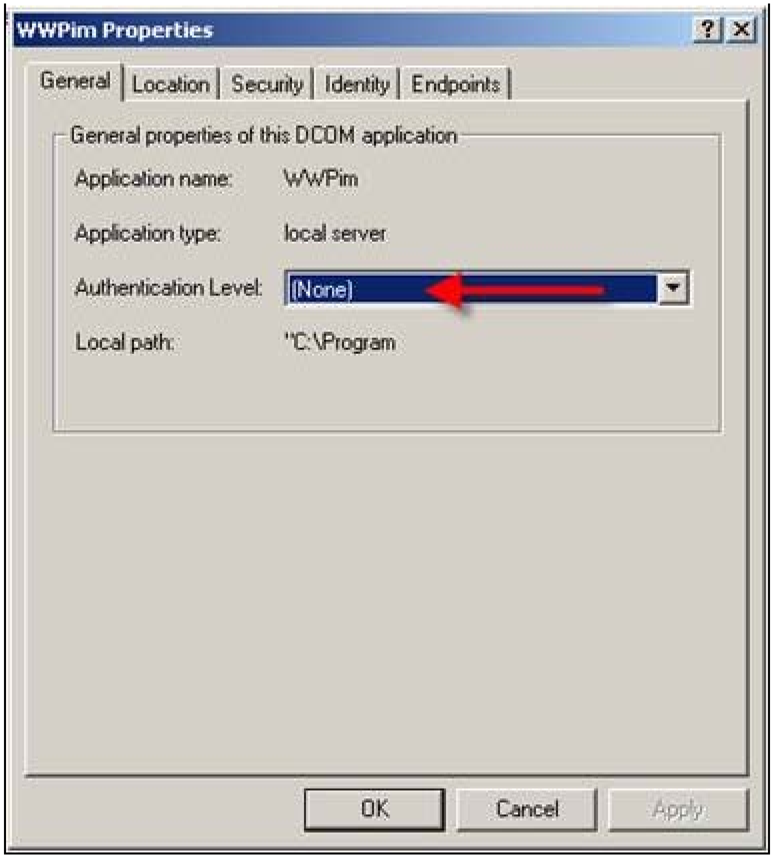


Applications:

SENS Logon Events
SENS Network Events
SENS OnNow Events
SENS Subscriber for EventSystem EventObjectChange events
Sound Recorder
TlntSvr
UpdaterUI
Voice Dictation Manager
Windows Management Instrumentation
Windows Media Player
Windows Update Agent
Windows Update Agent - Remote Access
wnwrapConsumer
wnwrapServerEx
WordPad Document
WSHRemote
wwAlarmConsumer2 Class
wwAlarmProvider2 Class
WWPim

FIGURE 5: WWPIM DCOM SERVICE PROPERTIES DIALOG BOX

- In the **Genera**l tab panel, ensure the **Authentication Level** is **None**.



General properties of this DCOM application

Application name: WWPim

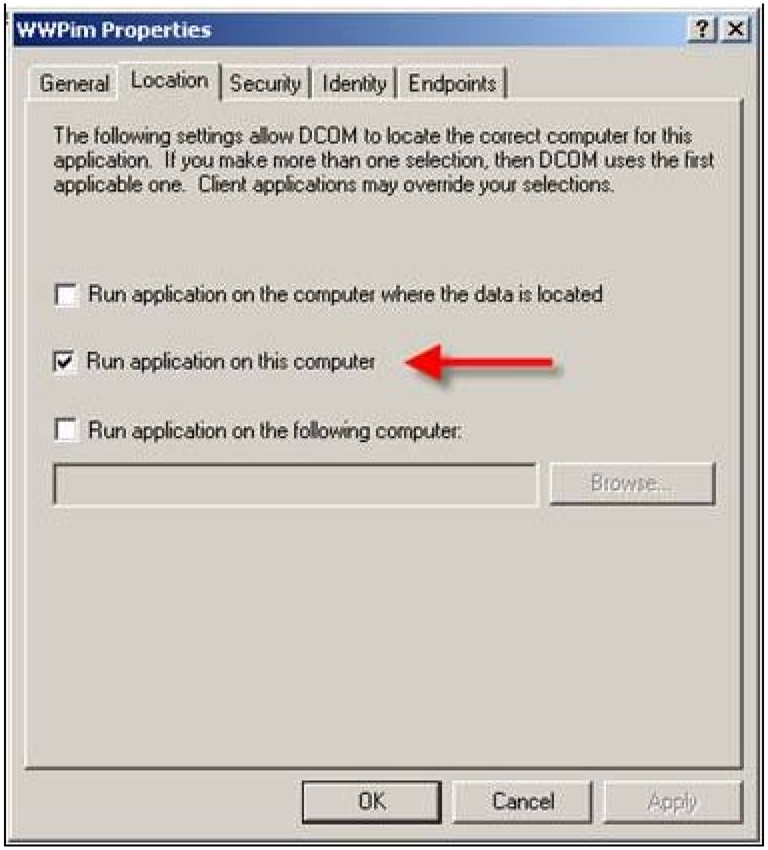
Application type: local server

Authentication Level: (None)

Local path: "C:\Program

FIGURE 6: WWPIM AUTHENTICATION LEVEL

- Click the **Location** tab and ensure the **Run application on this computer** box is checked.



The following settings allow DCOM to locate the correct computer for this application. If you make more than one selection, then DCOM uses the first applicable one. Client applications may override your selections.

□ Run application on the computer where the data is located

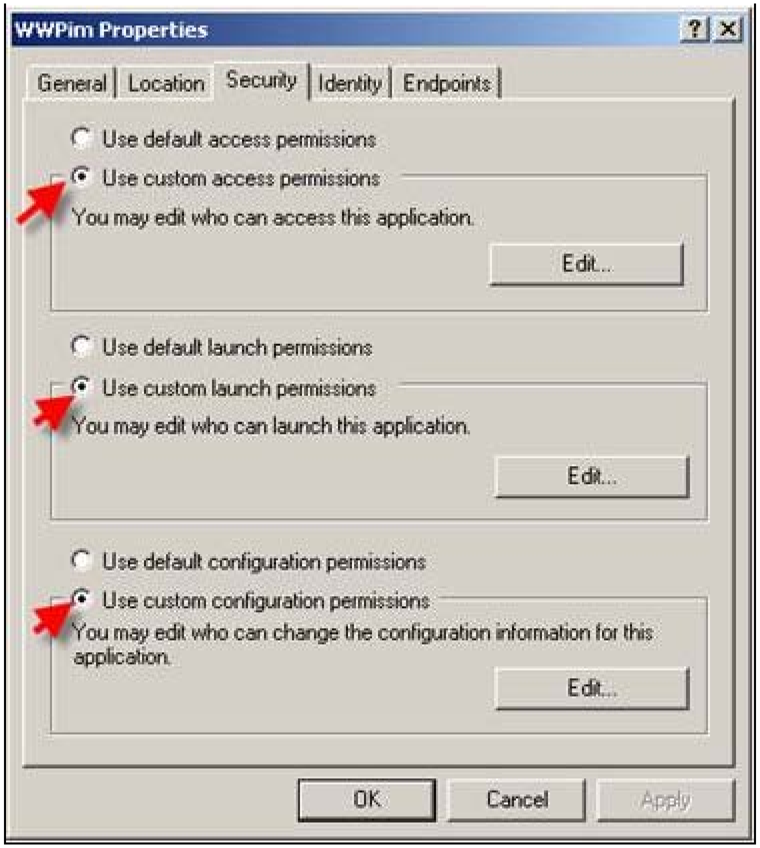
☑ Run application on this computer

□ Run application on the following computer:

Figure 7: Run Application on this Computer

- Click the **Security** tab.

  Under each Security grouping, ensure that the security settings are set similar to those shown in the following graphics. These are the minimum settings needed.



○ Use default access permissions

● Use custom access permissions

You may edit who can access this application.

○ Use default launch permissions

● Use custom launch permissions

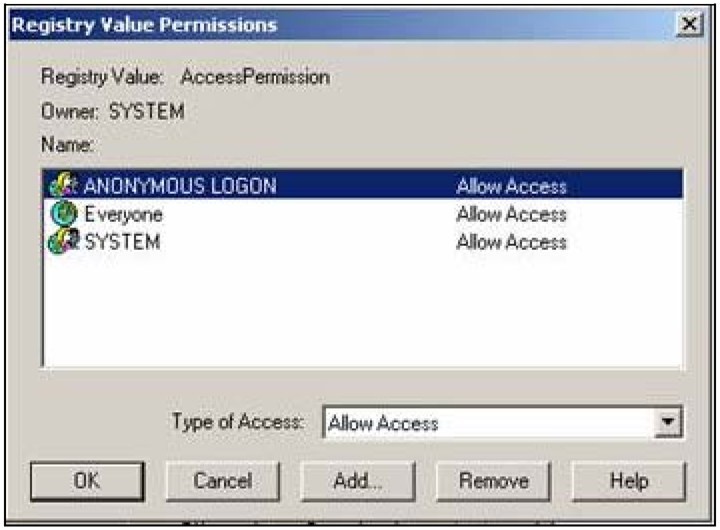
You may edit who can launch this application.

○ Use default configuration permissions

● Use custom configuration permissions

You may edit who can change the configuration information for this application.

Figure 8: Security Properties Tab Panel



Registry Value: AccessPermission

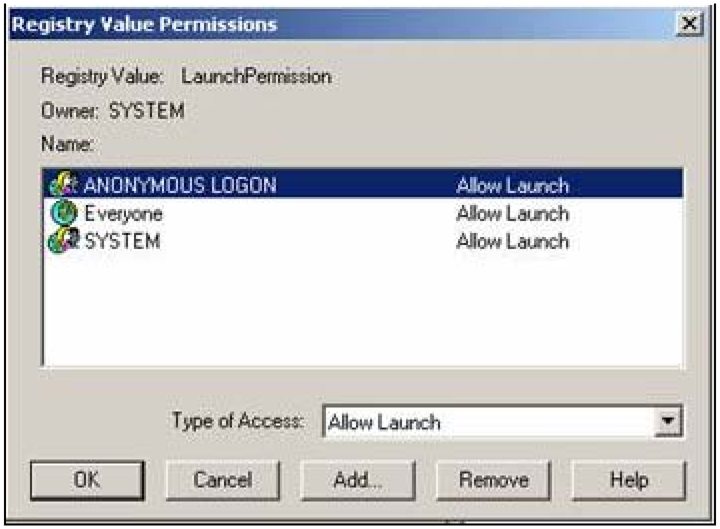
Owner: SYSTEM

Name:

ANONYMOUS LOGON	Allow Access
Everyone	Allow Access
SYSTEM	Allow Access

Type of Access: Allow Access

Figure 9: Security Settings for Access Permissions



Registry Value: LaunchPermission

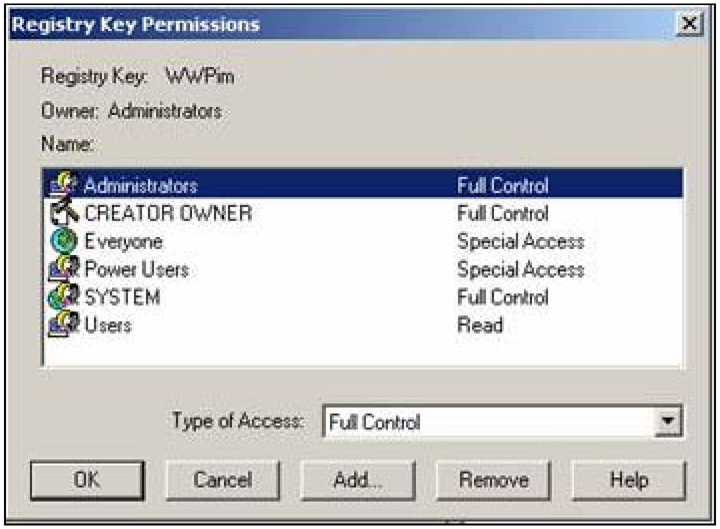
Owner: SYSTEM

Name:

ANONYMOUS LOGON	Allow Launch
Everyone	Allow Launch
SYSTEM	Allow Launch

Type of Access: Allow Launch

Figure 10: Security Settings for Lauch Permissions



Registry Key: WWPim

Owner: Administrators

Name:

Administrators	Full Control
CREATOR OWNER	Full Control
Everyone	Special Access
Power Users	Special Access
SYSTEM	Full Control
Users	Read

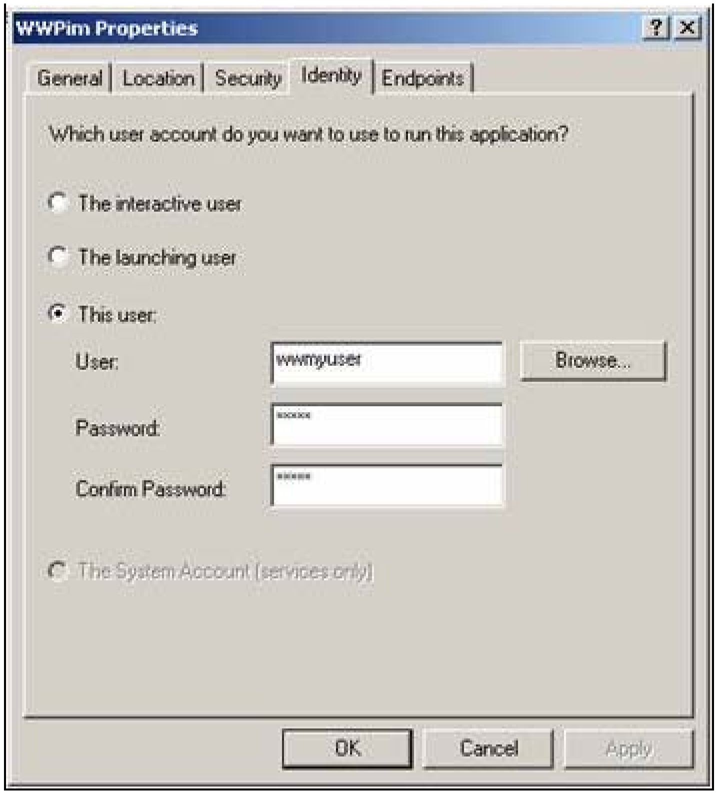
Type of Access: Full Control

Figure 11: Security settings for Custom Configuration Permissions

- Click the **Identity** tab.

The **This user** option shown below should be the ArchestrA Network Admin account defined using the **Wonderware Change Network Account Utility**.

Note: The following graphic shows a different user than Figure 1 and is used here only to illustrate account configuration.



Which user account do you want to use to run this application?

○ The interactive user

○ The launching user

● This user:

User: wwmyuser

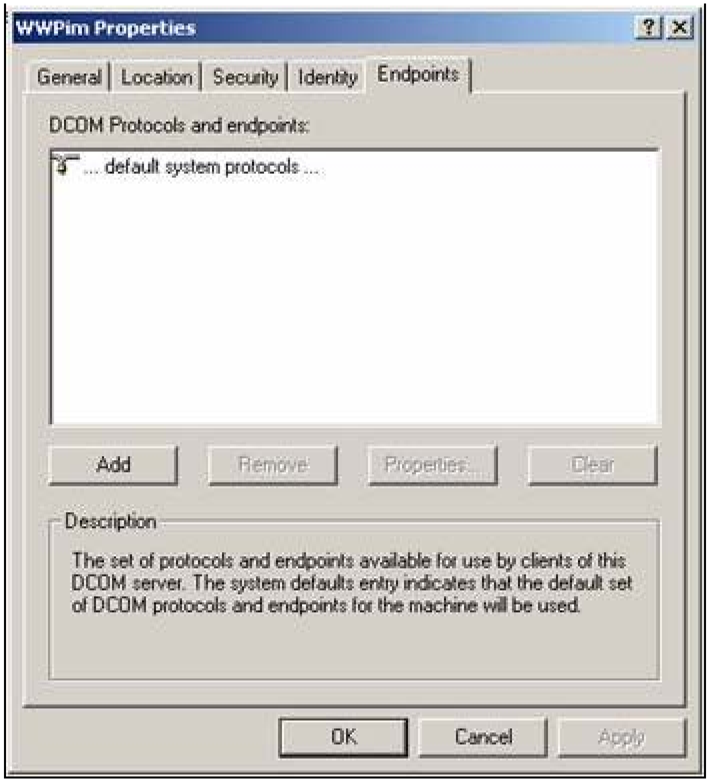
Password: *****

Confirm Password: *****

○ The System Account (services only)

Figure 12: This User Identity Option

The **Endpoints** tab panel should look similar to the following graphic (Figure 13 below).



DCOM Protocols and endpoints:

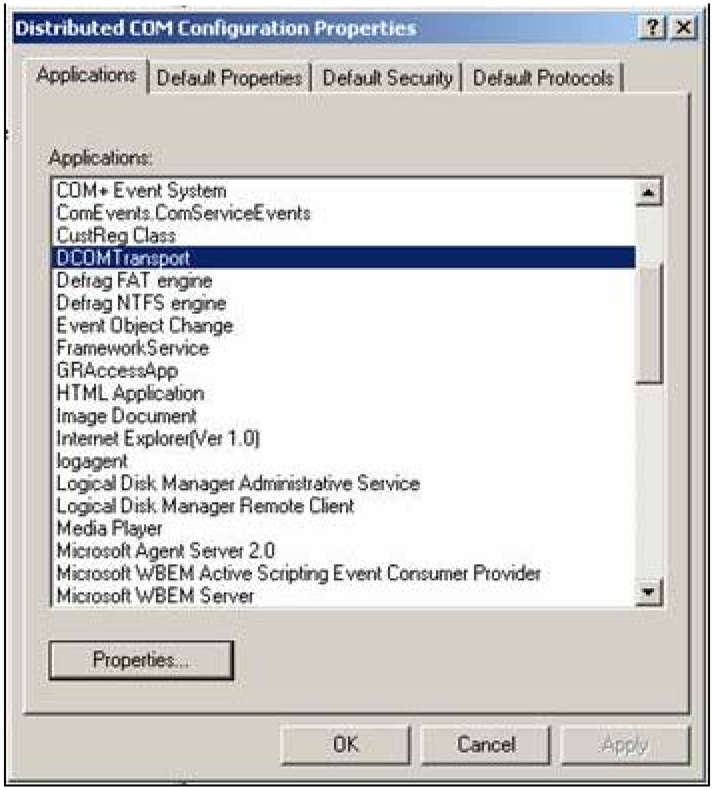
... default system protocols ...

Description

The set of protocols and endpoints available for use by clients of this DCOM server. The system defaults entry indicates that the default set of DCOM protocols and endpoints for the machine will be used.

FIGURE 13: DCOM DEFAULT SYSTEM CLIENT PROTOCOLS

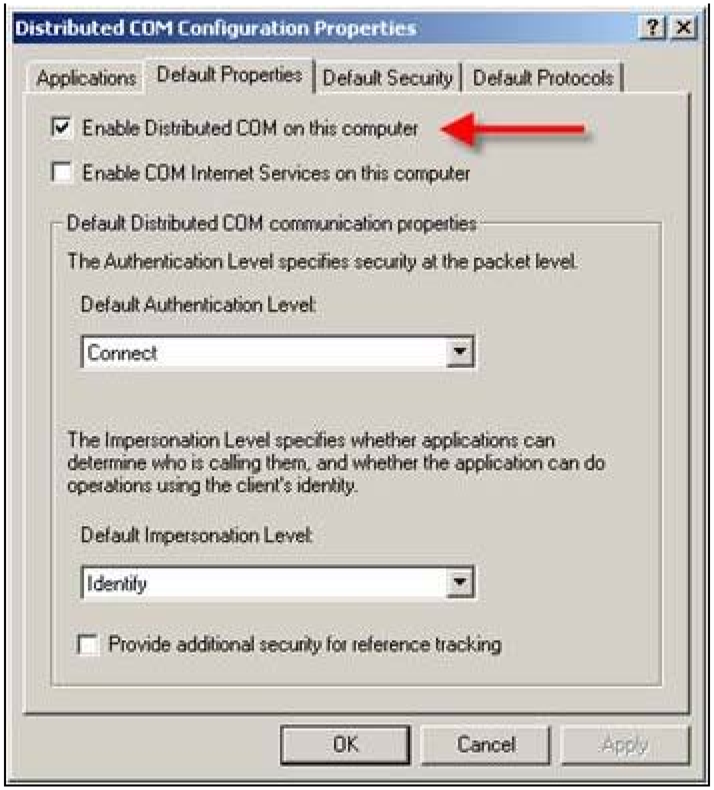
- Click **OK** and select the **DCOM Transport** configuration item from the **Properties** dialog box.



COM+ Event System
ComEvents.ComServiceEvents
CustReg Class
DCOMTransport
Defrag FAT engine
Defrag NTFS engine
Event Object Change
FrameworkService
GRAccessApp
HTML Application
Image Document
Internet Explorer(Ver 1.0)
logagent
Logical Disk Manager Administrative Service
Logical Disk Manager Remote Client
Media Player
Microsoft Agent Server 2.0
Microsoft WBEM Active Scripting Event Consumer Provider
Microsoft WBEM Server

Figure 14: DCOMTransport Configuration

- Ensure the **Enable Distributed COM on this computer** option is checked (Figure 15 below).



☑ Enable Distributed COM on this computer

□ Enable COM Internet Services on this computer

Default Distributed COM communication properties

The Authentication Level specifies security at the packet level.

Default Authentication Level: Connect

The Impersonation Level specifies whether applications can determine who is calling them, and whether the application can do operations using the client's identity.

Default Impersonation Level: Identify

□ Provide additional security for reference tracking

Figure 15: Default Properties Configuration

- Ensure that all the same settings used for **WWPIM** are applied for the DCOM Transport configuration.

Windows Configuration – Checking Local Security Settings

Note: These settings may be overridden by an enforced Group Policy Object from an MS Active Directory setup if the machine is part of a domain.

Configure local security settings from the Control Panel.

1. Click **Administrative Tools/Local Security Policy** (Figure 16 below):

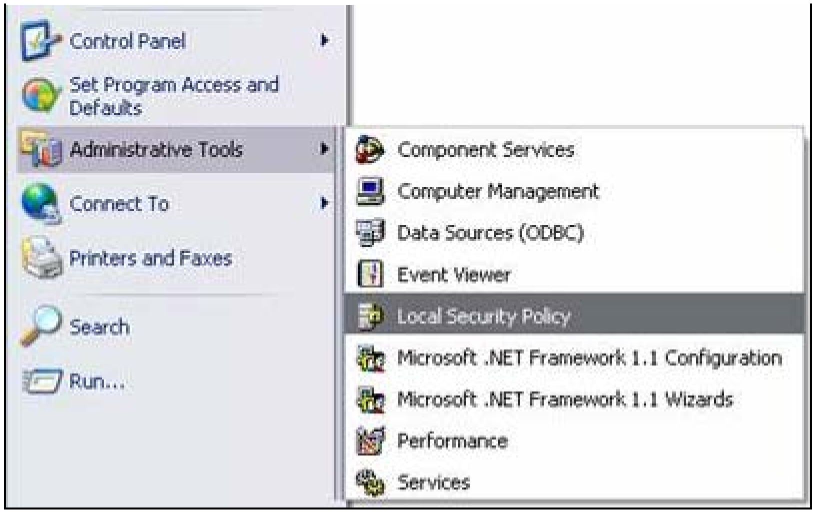
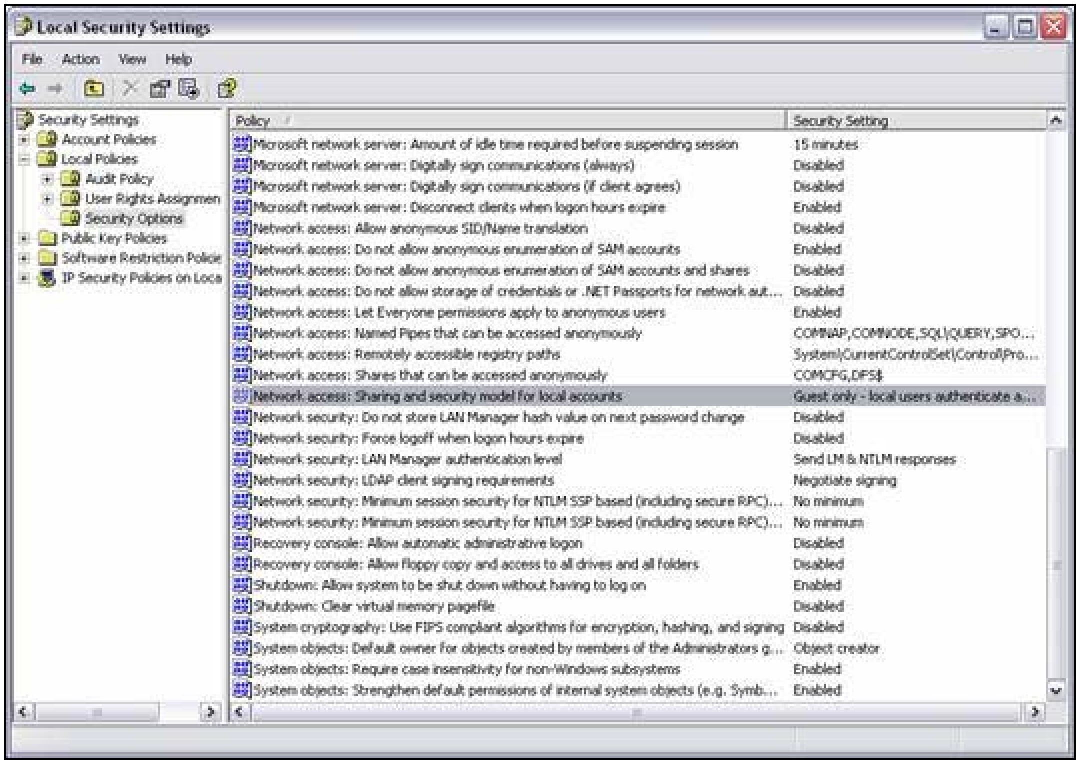


FIGURE 16: LOCAL SECURITY POLICY

2. Expand the **Local Policies** folder , then click **Security Options**.

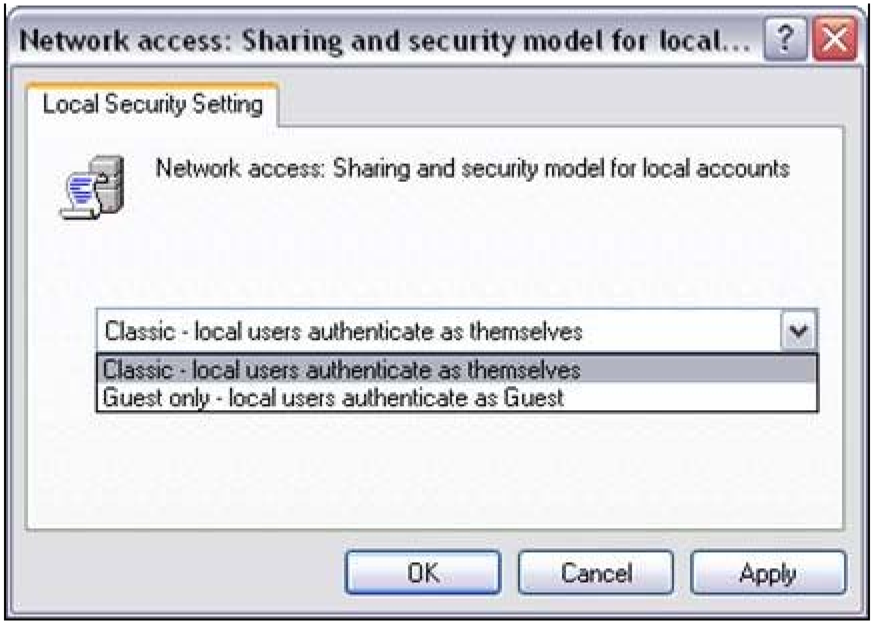
3. Double-click **Network access: Sharing and security model for local accounts**.



Policy	Security Setting
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Digitally sign communications (always)	Disabled
Microsoft network server: Digitally sign communications (if client agrees)	Disabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled
Network access: Do not allow storage of credentials or .NET Passports for network aut...	Disabled
Network access: Let Everyone permissions apply to anonymous users	Enabled
Network access: Named Pipes that can be accessed anonymously	COMNAP,COMNODE,SQL\QUERY,SPO...
Network access: Remotely accessible registry paths	System\CurrentControlSet\Control\Pro...
Network access: Shares that can be accessed anonymously	COMCFG,DFS$
Network access: Sharing and security model for local accounts	Guest only - local users authenticate a...
Network security: Do not store LAN Manager hash value on next password change	Disabled
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Send LM & NTLM responses
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC)...	No minimum
Network security: Minimum session security for NTLM SSP based (including secure RPC)...	No minimum
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled
Shutdown: Allow system to be shut down without having to log on	Enabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Disabled
System objects: Default owner for objects created by members of the Administrators g...	Object creator
System objects: Require case insensitivity for non-Windows subsystems	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symb...	Enabled

FIGURE 17: NETWORK ACCESS: SHARING AND SECURITY MODEL FOR LOCAL ACCOUNTS

4. Ensure that the selected option is **Classic** and not Guest Only.



Network access: Sharing and security model for local...

Network access: Sharing and security model for local accounts

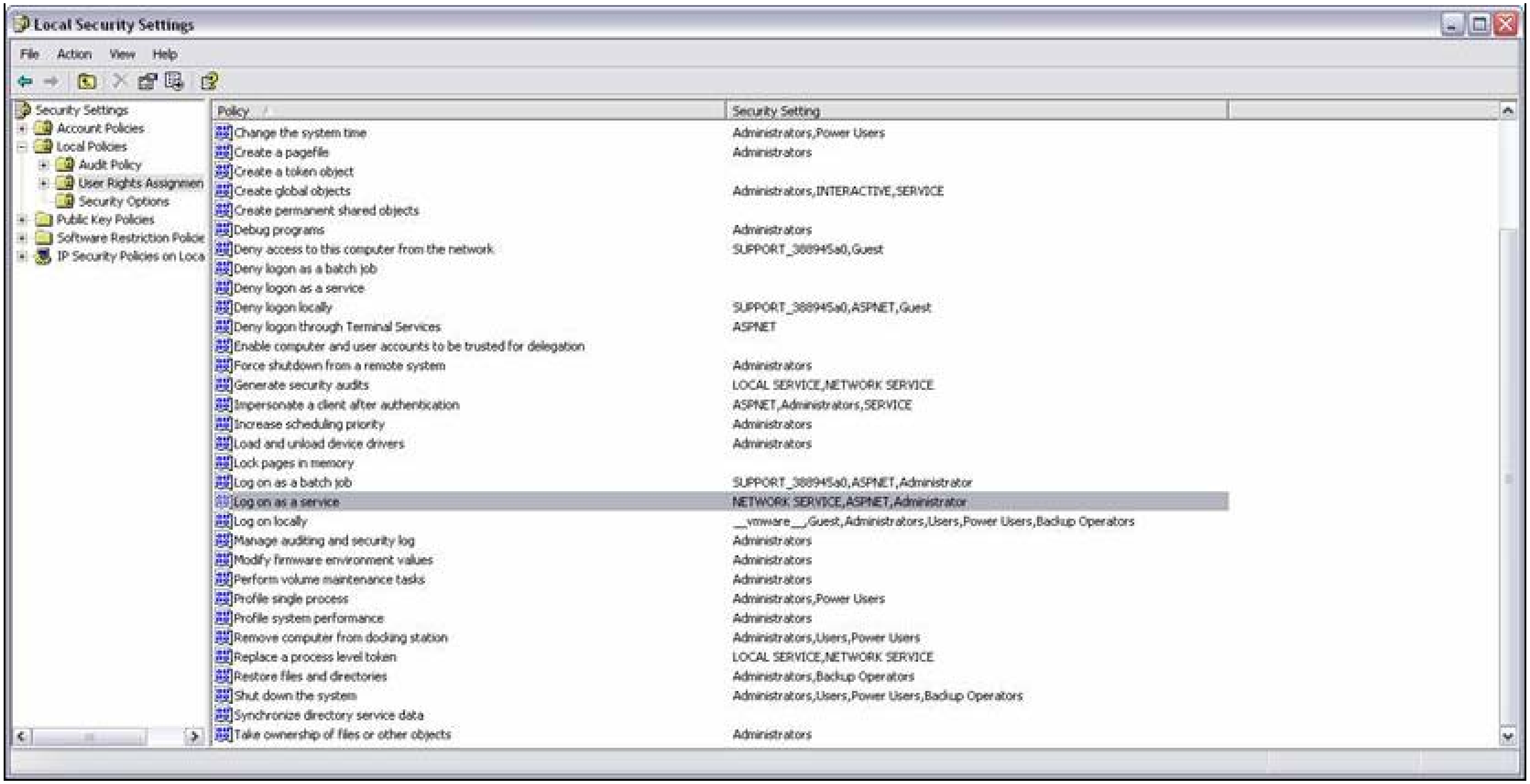
Classic - local users authenticate as themselves

Classic - local users authenticate as themselves
Guest only - local users authenticate as Guest

FIGURE 18: CLASSIC SECURITY SETTING

5. Click **OK** to save the setting.

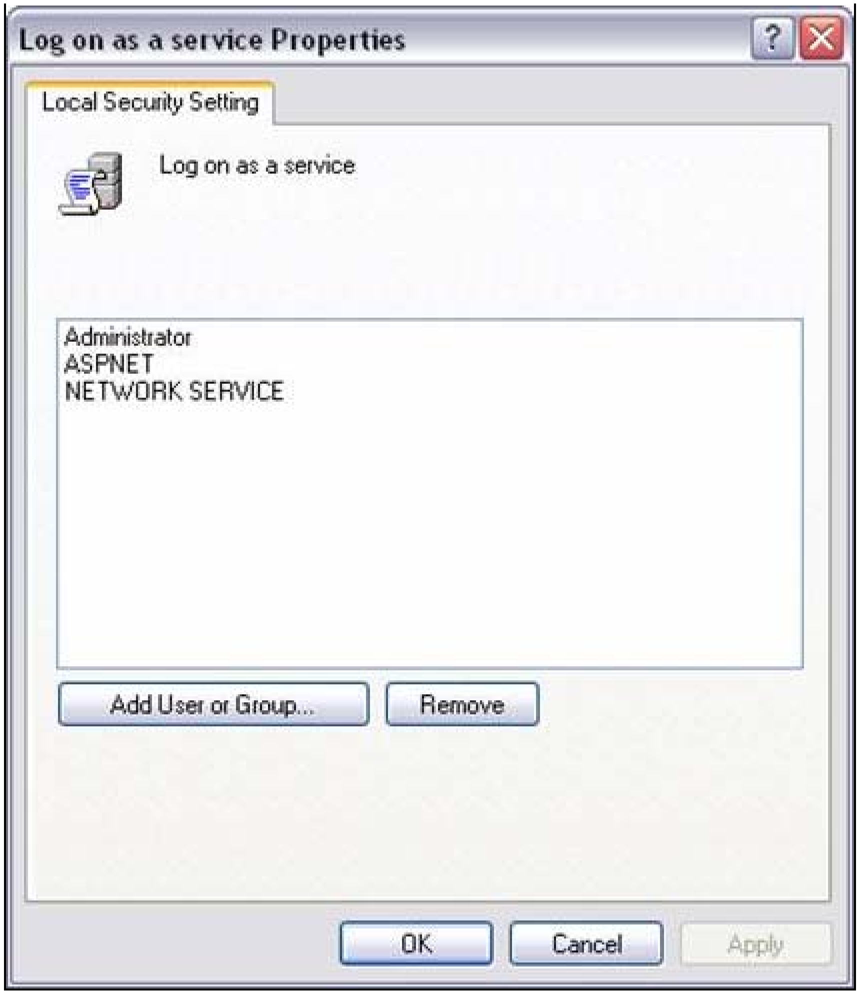
6. Double-click **Log on as a service**.



Policy	Security Setting
Change the system time	Administrators,Power Users
Create a pagefile	Administrators
Create a token object	
Create global objects	Administrators,INTERACTIVE,SERVICE
Create permanent shared objects	
Debug programs	Administrators
Deny access to this computer from the network	SUPPORT_388945a0,Guest
Deny logon as a batch job	
Deny logon as a service	
Deny logon locally	SUPPORT_388945a0,ASPNET,Guest
Deny logon through Terminal Services	ASPNET
Enable computer and user accounts to be trusted for delegation	
Force shutdown from a remote system	Administrators
Generate security audits	LOCAL SERVICE,NETWORK SERVICE
Impersonate a client after authentication	ASPNET,Administrators,SERVICE
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as a batch job	SUPPORT_388945a0,ASPNET,Administrator
Log on as a service	NETWORK SERVICE,ASPNET,Administrator
Log on locally	__vmware__,Guest,Administrators,Users,Power Users,Backup Operators
Manage auditing and security log	Administrators
Modify firmware environment values	Administrators
Perform volume maintenance tasks	Administrators
Profile single process	Administrators,Power Users
Profile system performance	Administrators
Remove computer from docking station	Administrators,Users,Power Users
Replace a process level token	LOCAL SERVICE,NETWORK SERVICE
Restore files and directories	Administrators,Backup Operators
Shut down the system	Administrators,Users,Power Users,Backup Operators
Synchronize directory service data	
Take ownership of files or other objects	Administrators

FIGURE 19: LOG ON AS A SERVICE SETTING

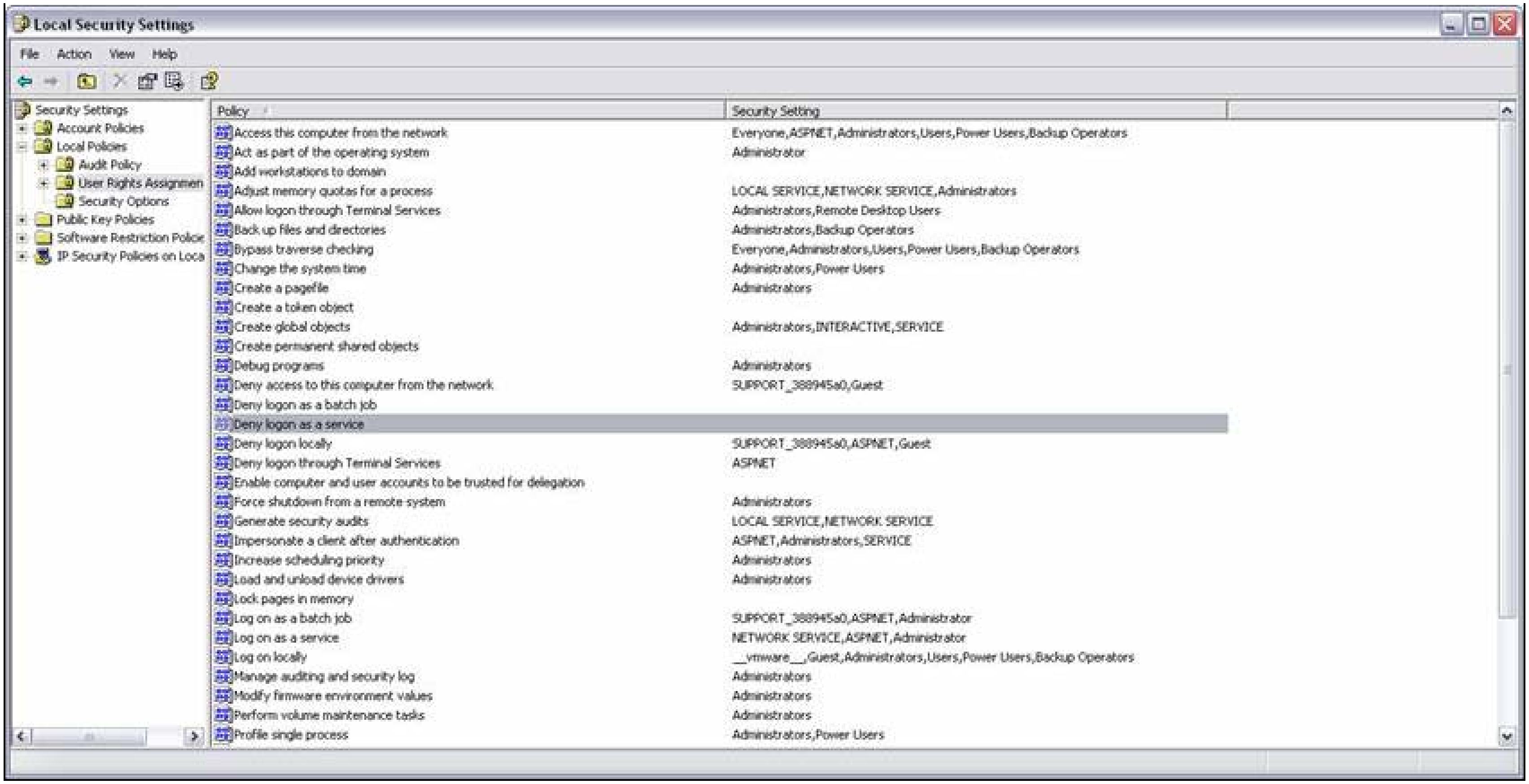
7. Ensure that the **ArchestrA Network Admin** account is listed here.



Administrator
ASPNET
NETWORK SERVICE

FIGURE 20: LOGON AS A SERVICE SECURITY PROPERTY

8. Click **OK**, then double-click **Deny logon as a service**.



Policy	Security Setting
Access this computer from the network	Everyone,ASPNET,Administrators,Users,Power Users,Backup Operators
Act as part of the operating system	Administrator
Add workstations to domain	
Adjust memory quotas for a process	LOCAL SERVICE,NETWORK SERVICE,Administrators
Allow logon through Terminal Services	Administrators,Remote Desktop Users
Back up files and directories	Administrators,Backup Operators
Bypass traverse checking	Everyone,Administrators,Users,Power Users,Backup Operators
Change the system time	Administrators,Power Users
Create a pagefile	Administrators
Create a token object	
Create global objects	Administrators,INTERACTIVE,SERVICE
Create permanent shared objects	
Debug programs	Administrators
Deny access to this computer from the network	SUPPORT_388945a0,Guest
Deny logon as a batch job	
Deny logon as a service	
Deny logon locally	SUPPORT_388945a0,ASPNET,Guest
Deny logon through Terminal Services	ASPNET
Enable computer and user accounts to be trusted for delegation	
Force shutdown from a remote system	Administrators
Generate security audits	LOCAL SERVICE,NETWORK SERVICE
Impersonate a client after authentication	ASPNET,Administrators,SERVICE
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as a batch job	SUPPORT_388945a0,ASPNET,Administrator
Log on as a service	NETWORK SERVICE,ASPNET,Administrator
Log on locally	__vmware__,Guest,Administrators,Users,Power Users,Backup Operators
Manage auditing and security log	Administrators
Modify firmware environment values	Administrators
Perform volume maintenance tasks	Administrators
Profile single process	Administrators,Power Users

Figure 21: Deny Logon as a Service

9. Ensure that the ArchestrA Network Admin account is *not* listed here (Figure 22 below).

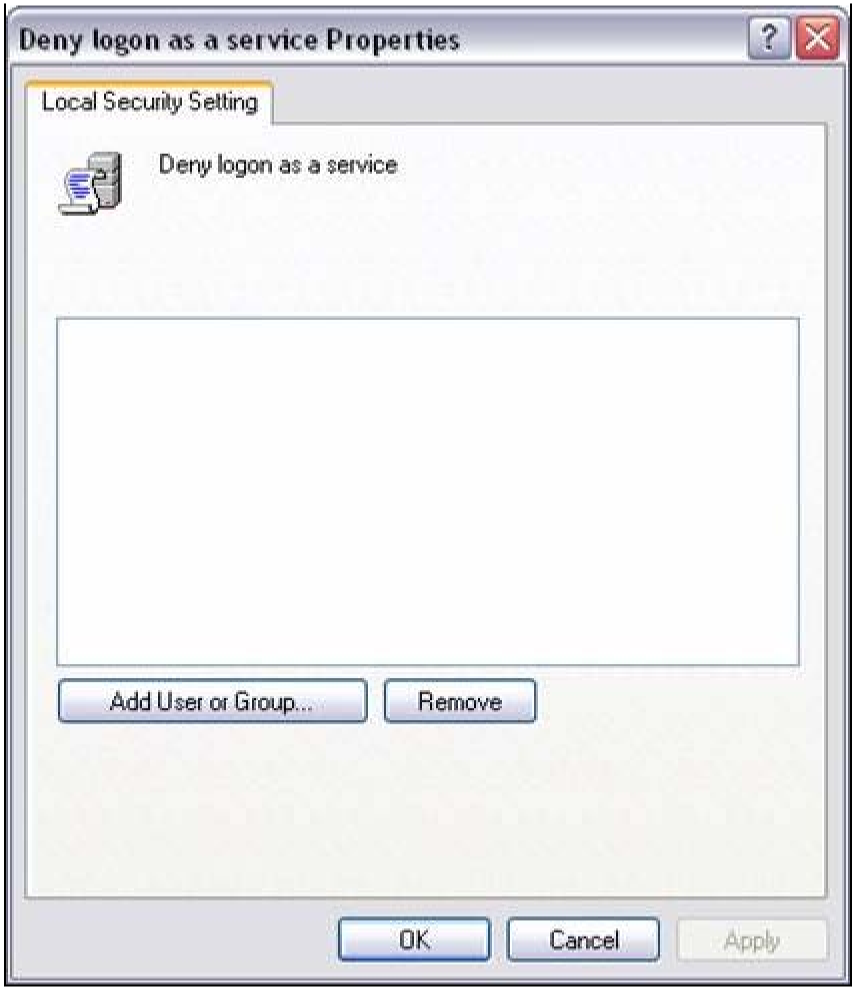
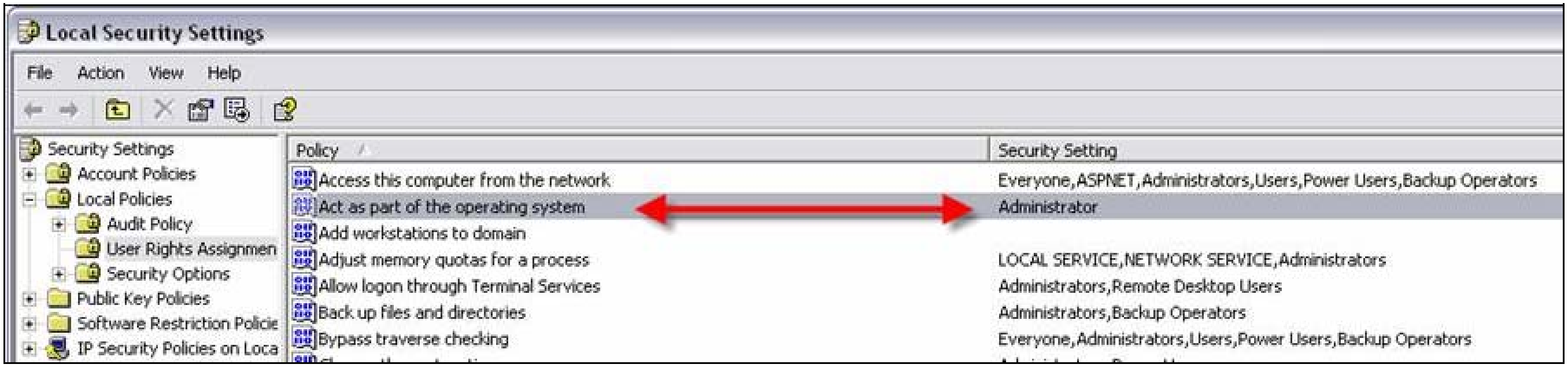


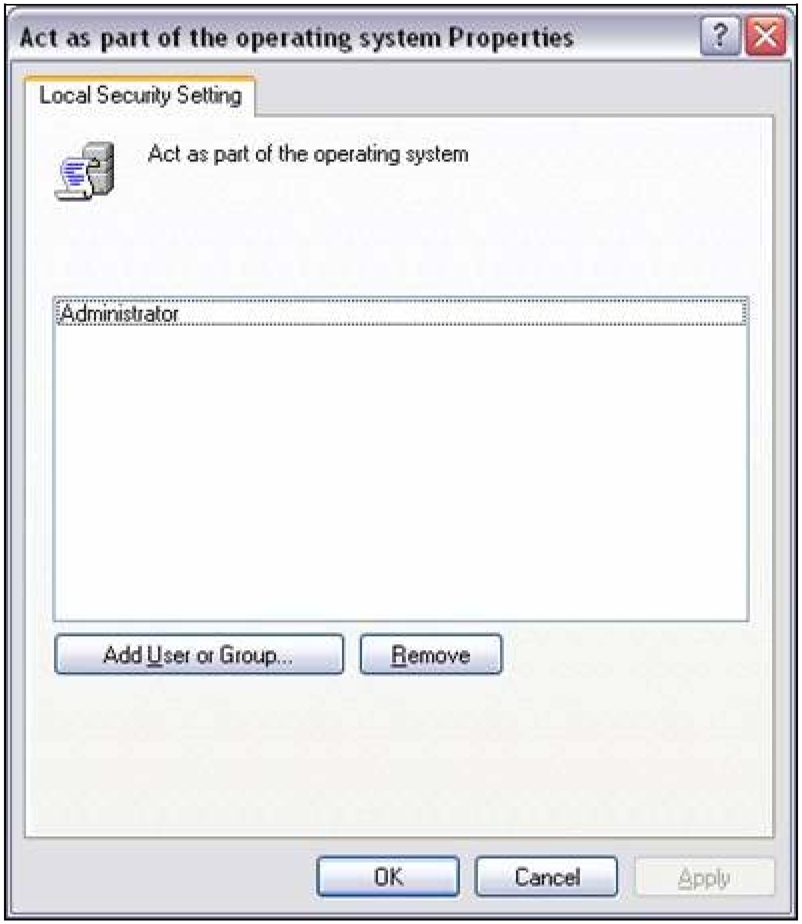
FIGURE 22: DENY LOGON AS A SERVICE SECURITY PROPERTY

10. Click OK.
11. Ensure that the Administrator account is a member of the policy **Act as part of the operating system**.



Policy	Security Setting
Access this computer from the network	Everyone,ASPNET,Administrators,Users,Power Users,Backup Operators
Act as part of the operating system	Administrator
Add workstations to domain	
Adjust memory quotas for a process	LOCAL SERVICE,NETWORK SERVICE,Administrators
Allow logon through Terminal Services	Administrators,Remote Desktop Users
Back up files and directories	Administrators,Backup Operators
Bypass traverse checking	Everyone,Administrators,Users,Power Users,Backup Operators

Figure 23: Administrator Permissions for the Operating System Security Setting



Act as part of the operating system

Administrator

Figure 24: Confirm Administrator Setting

While it is not generally required, in some specific cases – adding the ArchestrA Network admin account to this policy may resolve communication issues.

- Click the following link for information on **Act as part of the operating system** property.

Windows Configuration – Checking Computer Management

The following items must be checked as a part of troubleshooting Bootstrap communication.

Local Users and Groups

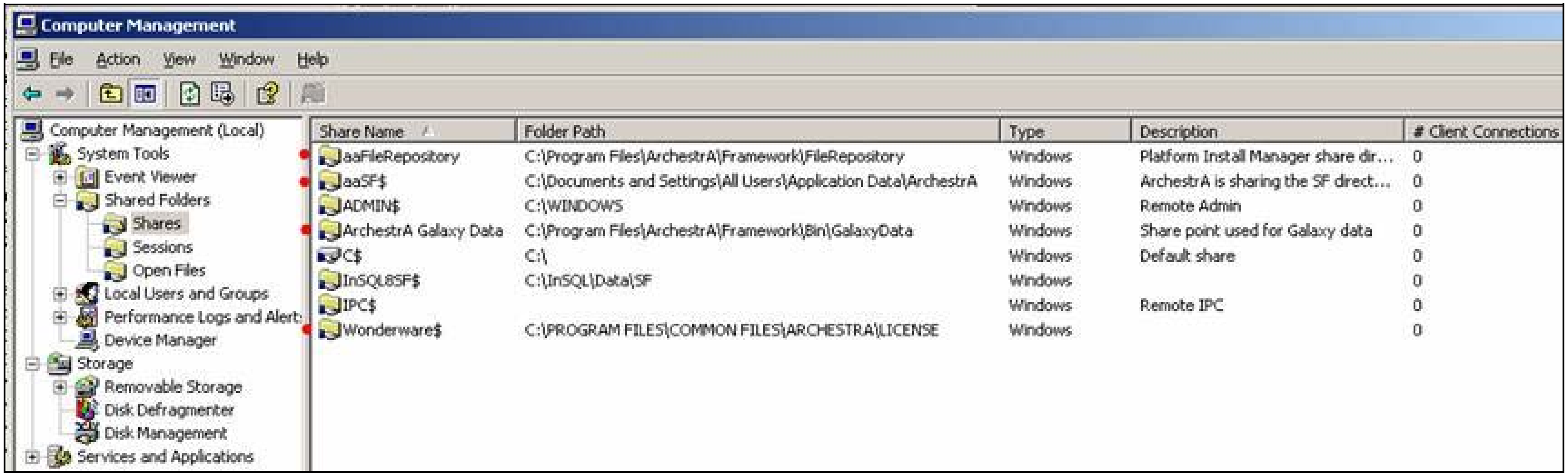
Make sure the ArchestrA Network Admin account is a member of the Administrators group on the local machine, regardless if it is a local or domain account.

Note: The user logged on to the desktop of the remote machine that is trying to launch an IDE for remote GR access must be an Administrator of the remote machine. Administrator permissions are necessary to allow proper DCOM and similar communication.

Shared Folders – Shares

Make sure the following folders are shared on the local machine and that the ArchestrA Network Admin account has permissions to read and write to the folders.

- aaFileRepository
- aaSF$
- ArchestrA Galaxy Data
- Wonderware$



Share Name	Folder Path	Type	Description	# Client Connections
aaFileRepository	C:\Program Files\ArchestrA\Framework\FileRepository	Windows	Platform Install Manager share dir...	0
aaSF$	C:\Documents and Settings\All Users\Application Data\ArchestrA	Windows	ArchestrA is sharing the SF direct...	0
ADMIN$	C:\WINDOWS	Windows	Remote Admin	0
ArchestrA Galaxy Data	C:\Program Files\ArchestrA\Framework\Bin\GalaxyData	Windows	Share point used for Galaxy data	0
C$	C:\	Windows	Default share	0
InSQL8SF$	C:\InSQL\Data\SF	Windows		0
IPC$		Windows	Remote IPC	0
Wonderware$	C:\PROGRAM FILES\COMMON FILES\ARCHESTRA\LICENSE	Windows		0

Figure 25: Shared System Folders

Windows Configuration – Folder Options

1. In Microsoft Windows Explorer's main menu, click **Tools/Folder options**.

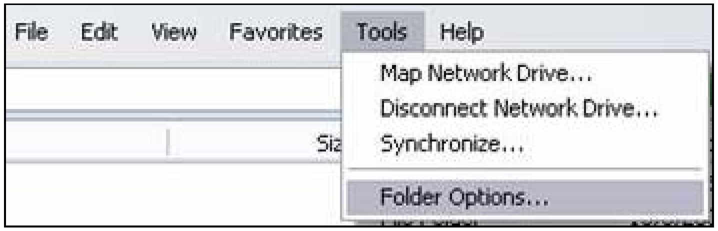
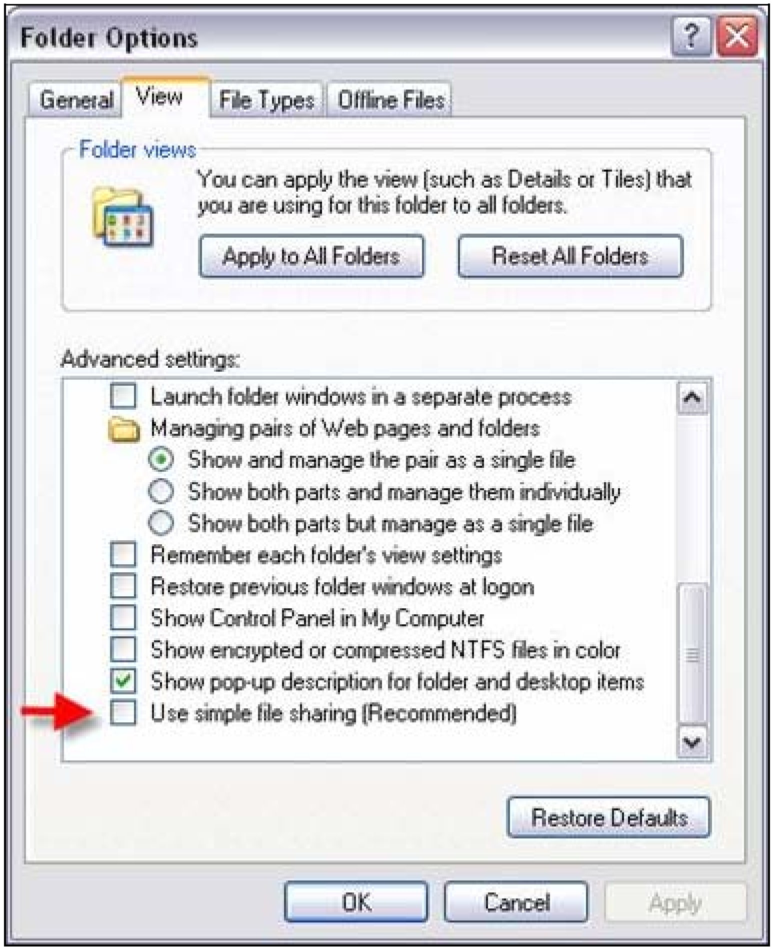


Figure 26: Windows Explorer Folder Options

2. Uncheck the **Use simple file sharing (Recommended)** option.



Folder views

You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.

Advanced settings:

- □ Launch folder windows in a separate process
- Managing pairs of Web pages and folders
  - ● Show and manage the pair as a single file
  - ○ Show both parts and manage them individually
  - ○ Show both parts but manage as a single file
- □ Remember each folder's view settings
- □ Restore previous folder windows at logon
- □ Show Control Panel in My Computer
- □ Show encrypted or compressed NTFS files in color
- ☑ Show pop-up description for folder and desktop items
- □ Use simple file sharing (Recommended)

Figure 27: Disable Simple File Sharing

Note: For more information on File Sharing, click here.

Windows Configuration – Regional Settings

Ensure that the regional settings of the remote and GR nodes are set to **English (United States)**.

Verify the settings using the **Regional and Language Options** dialogue box from the **Control Panel/Regional and Language Options**.

S. Kermani, B. Hunter

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 **www.wonderware.com/support/mmi**

For technical support questions, send an e-mail to **support@wonderware.com**.

back to top