Doc Type	Tech Notes
Doc Id	TN482
Last Modified Date	01/14/2020

Troubleshooting Wonderware Application Server Bootstrap Communications

LEGACY TECH NOTE

876

SUMMARY

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

This *Tech Note* augments TN 461 Troubleshooting Industrial Application Server Bootstrap Communications.

SITUATION

Warning:

After Application Server is installed, the **OsConfigurationUtility** is called, which sets the global DCOM setting on the machine. When the utility was introduced, Microsoft used just one bit to enable COM permissions for account (**Old style ACLs**).

Running the OsConfigurationUtility in prior versions (WSP 2017 / WSP 2014 R3) uses the old style ACL.

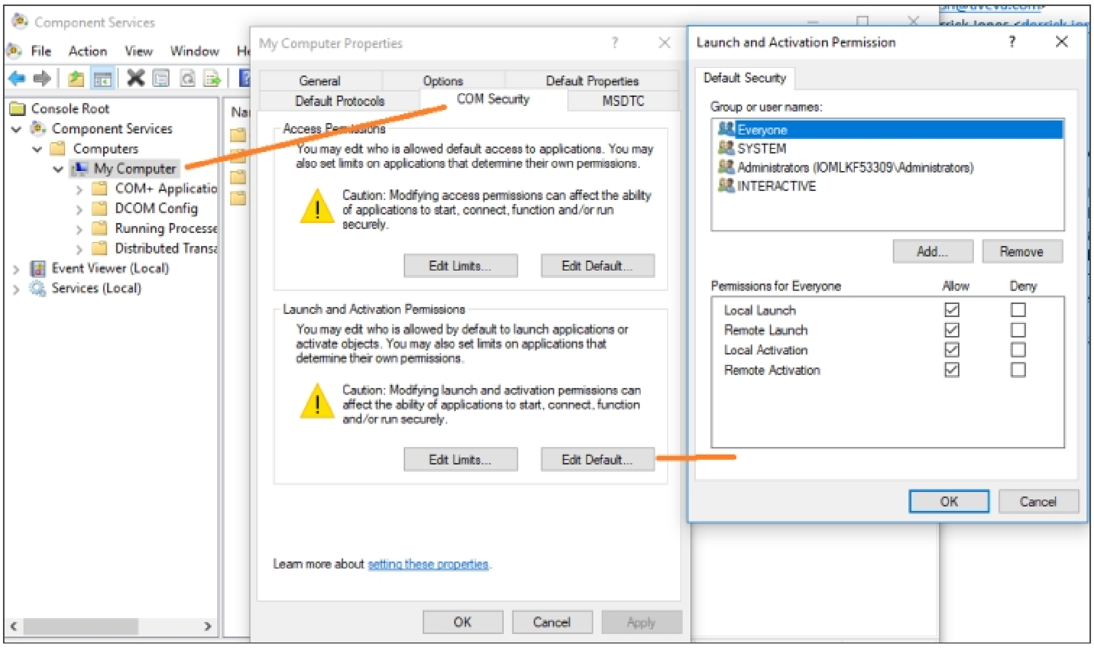
Microsoft has introduced more granular permissions that use multiple bits (**New style ACLs**).

- Run **DcomCnfg** and change **Launch and Activation Permission** (at global level or for a single component) for one user account like **Everyone** and save the changes:

The **Everyone** account will use the new style ACLs. The other user accounts that were configured programmatically are still configured with the "old style" ACL.

At runtime, when a client application tries to CoCreate the server, the call fails because of this old/new style mismatch. The message is: **HRESULT=0x 80040153 - REGDB_E_INVALIDVALUE - Invalid value for registry.** In the configuration editor all settings will look just fine and it is not clear which one is configured with old- or new style permission.

On versions prior to WSP 2017, if you suspect incorrect DCOM settings, follow these recommendations:



My Computer Properties

Access Permissions

You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.

Caution: Modifying access permissions can affect the ability of applications to start, connect, function and/or run securely.

Launch and Activation Permissions

You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions.

Caution: Modifying launch and activation permissions can affect the ability of applications to start, connect, function and/or run securely.

Learn more about setting these properties.

Launch and Activation Permission

Default Security

Group or user names:

Everyone
SYSTEM
Administrators (IOMLKF53309\Administrators)
INTERACTIVE

Permissions for Everyone	Allow	Deny
Local Launch	☑	☐
Remote Launch	☑	☐
Local Activation	☑	☐
Remote Activation	☑	☐

Figure 1: Create 'Everyone' account

Re-Run the **OsConfigurationUtility** and check that the issue is resolved.

If the issue is not resolved, delete all user names from the list below. Add them again with appropriate permissions. This will guarantee there is no old style / new style mismatch Application Versions

- Wonderware Application Server 3.5 (2012). Please check the compatability matrix at the AVEVA Knowledge & Support site for supported operating systems.
- This *Tech Note* uses Windows Server 2008 for the examples.

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.

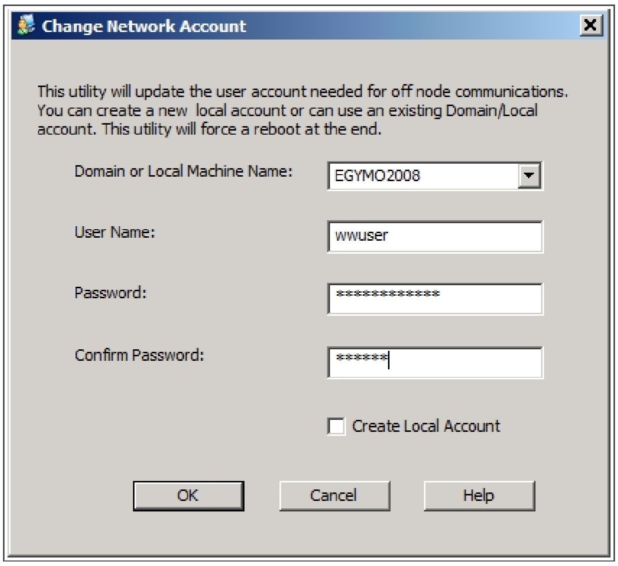
Wonderware Configuration Tools

Use the following Wonderware Configuration tools when troubleshooting the application.

Wonderware Change Network Account Utility

Ensure that the ArchestrA Network Admin Account is the same on all machines in the Galaxy (or wish to interact with nodes in the Galaxy).

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



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: EGYMO2008

User Name: wwuser

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

Use the OS Configuration Utility to add TCP/UDP ports and application authorization to the Windows Firewall exclusion list, in order to allow Wonderware products to operate as designed on Windows XP SP2 , Windows 2003 SP1 or greater, Windows Vista, Windows 2008, and Windows 7.

The OS Configuration utility is delivered with ASP 3.5 (2012).

You can also download the utility from the support site.

To run the Wonderware OS Configuration Utility

1. Navigate to **<RootDrive>\Program Files\Common Files\ArchestrA**.
2. Run the application named **OSConfigurationUtility.exe**.

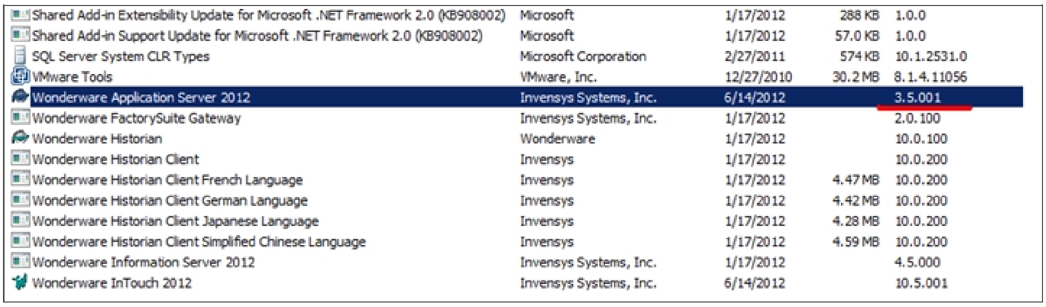
   For a list of what the utility does, please refer to the Tech Article Security Settings for Wonderware Products.
3. Reboot the machine after running the O/S Configuration Utility.

Verify Wonderware Application Versions

Ensure that the version of Wonderware Application Server installed on the remote node is the same as the version of the Wonderware Application Server Galaxy.

1. Verify the version by going to **Control Panel / Programs / Programs and Features**. Verify the Wonderware Application Server 2012 version on the Galaxy Repository (GR) Node and on the remote nodes.

   Note: If the **Version** column is not visible, right click on a column name then click **More**. You can then see the **Version** column.



Shared Add-in Extensibility Update for Microsoft .NET Framework 2.0 (KB908002)	Microsoft	1/17/2012	288 KB	1.0.0
Shared Add-in Support Update for Microsoft .NET Framework 2.0 (KB908002)	Microsoft	1/17/2012	57.0 KB	1.0.0
SQL Server System CLR Types	Microsoft Corporation	2/27/2011	574 KB	10.1.2531.0
VMware Tools	VMware, Inc.	12/27/2010	30.2 MB	8.1.4.11056
Wonderware Application Server 2012	Invensys Systems, Inc.	6/14/2012		3.5.001
Wonderware FactorySuite Gateway	Invensys Systems, Inc.	1/17/2012		2.0.100
Wonderware Historian	Wonderware	1/17/2012		10.0.100
Wonderware Historian Client	Invensys	1/17/2012		10.0.200
Wonderware Historian Client French Language	Invensys	1/17/2012	4.47 MB	10.0.200
Wonderware Historian Client German Language	Invensys	1/17/2012	4.42 MB	10.0.200
Wonderware Historian Client Japanese Language	Invensys	1/17/2012	4.28 MB	10.0.200
Wonderware Historian Client Simplified Chinese Language	Invensys	1/17/2012	4.59 MB	10.0.200
Wonderware Information Server 2012	Invensys Systems, Inc.	1/17/2012		4.5.000
Wonderware InTouch 2012	Invensys Systems, Inc.	6/14/2012		10.5.001

Figure 2: Verify Program Version

Figure 2 (above) shows Wonderware Application Server 2012 -- **3.5 Patch 01**.

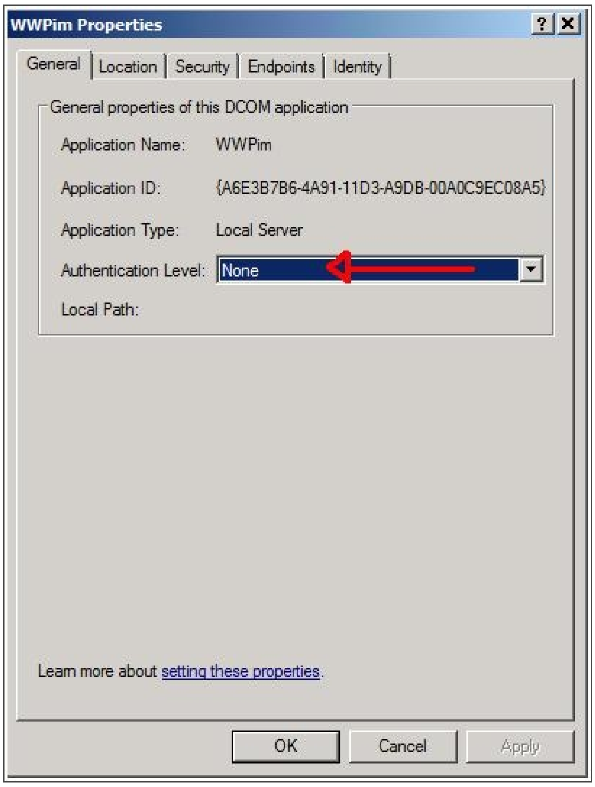
Checking Windows DCOM Configuration

The DCOM Ports used by the Bootstrap are:

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

For additional info see: http://support.microsoft.com/kb/832017

1. In the **General** tab panel, make sure the **Authentication Level** is **None** (Figure 4 below).



General properties of this DCOM application

Application Name: WWPim

Application ID: {A6E3B7B6-4A91-11D3-A9DB-00A0C9EC08A5}

Application Type: Local Server

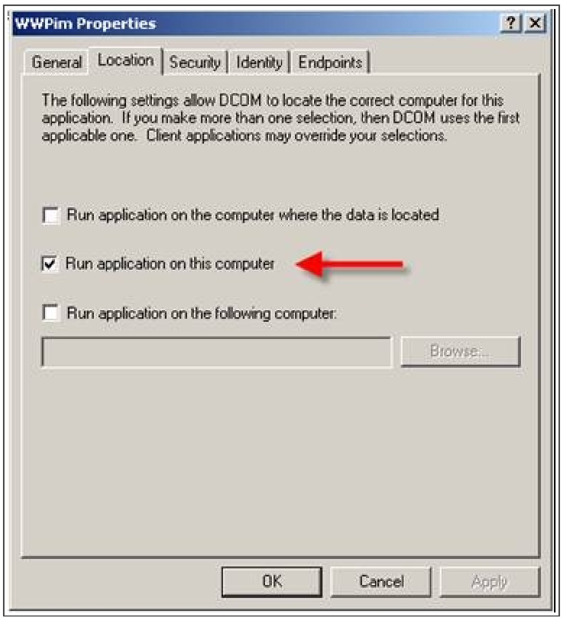
Authentication Level: None

Local Path:

Learn more about setting these properties.

Figure 4: WWPim Authentication Level

Note: On x64 operating systems this option may be grayed out/disabled. The workaround is to use the 32-bit version of DCOMCNFG by using the following command line: **C:\WINDOWS\SysWOW64>mmc comexp.msc /32**.



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

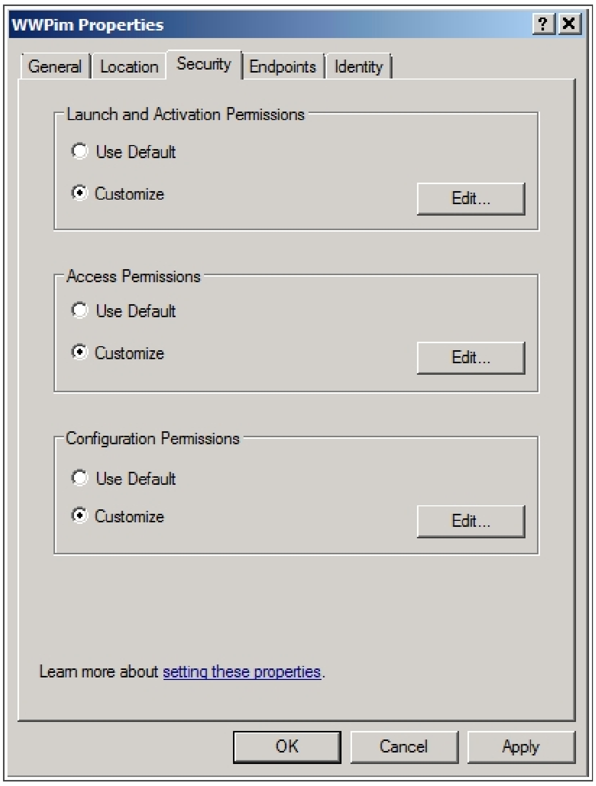
☑ Run application on this computer

☐ Run application on the following computer:

Figure 5: Run Application on this Computer

2. 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.



Launch and Activation Permissions

○ Use Default

● Customize

Access Permissions

○ Use Default

● Customize

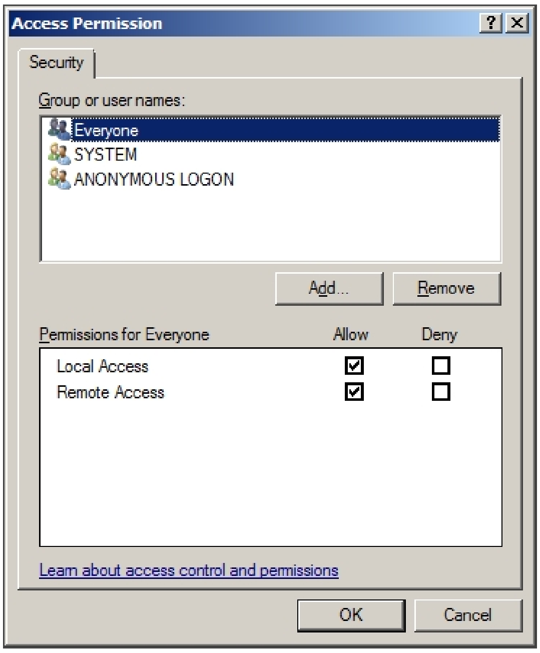
Configuration Permissions

○ Use Default

● Customize

Learn more about setting these properties.

Figure 6: Security Properties Tab Panel



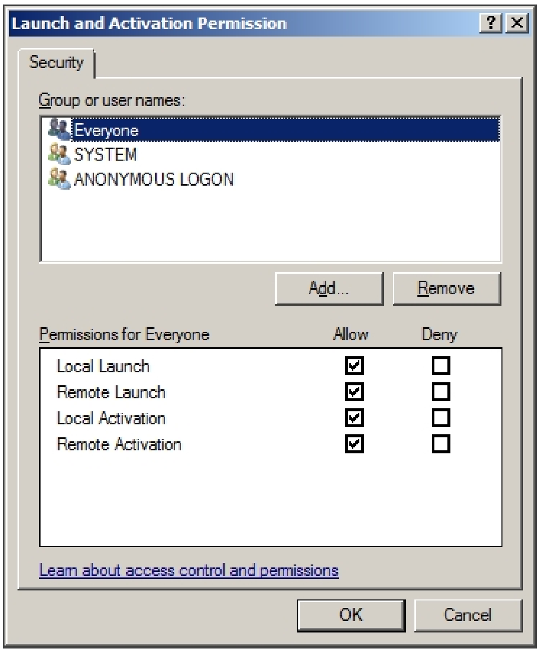
Group or user names:

- Everyone
- SYSTEM
- ANONYMOUS LOGON

Permissions for Everyone	Allow	Deny
Local Access	☑	□
Remote Access	☑	□

Learn about access control and permissions

Figure 7: Security Settings for Access Permissions



Launch and Activation Permission

Security

Group or user names:

- Everyone
- SYSTEM
- ANONYMOUS LOGON

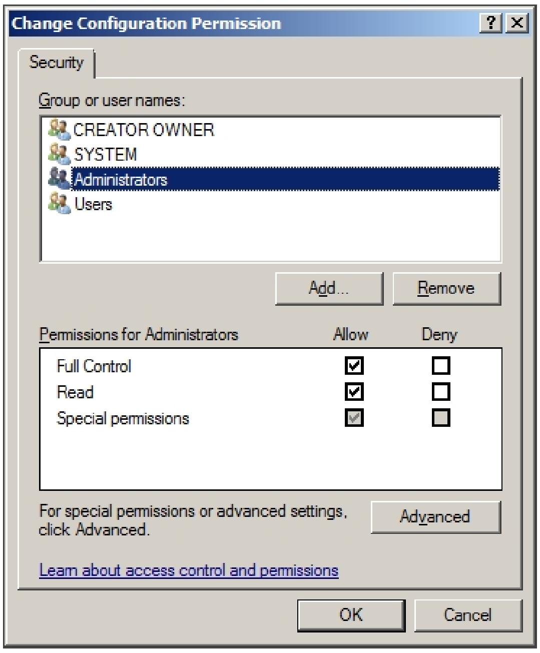
Add... Remove

Permissions for Everyone	Allow	Deny
Local Launch	☑	□
Remote Launch	☑	□
Local Activation	☑	□
Remote Activation	☑	□

Learn about access control and permissions

OK Cancel

Figure 8: Security Settings for Launch and Activation Permissions



Change Configuration Permission

Security

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators
- Users

Add... Remove

Permissions for Administrators	Allow	Deny
Full Control	☑	□
Read	☑	□
Special permissions	☑	□

For special permissions or advanced settings, click Advanced. Advanced

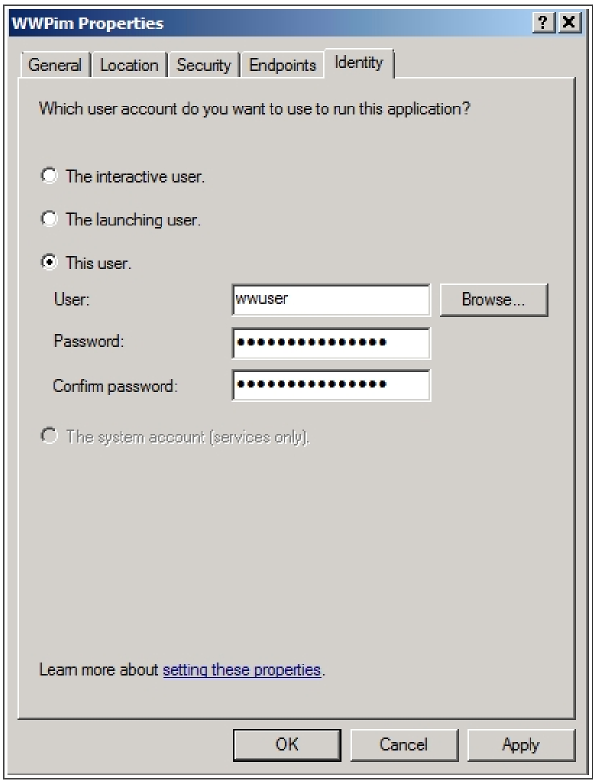
Learn about access control and permissions

OK Cancel

Figure 9: Security settings for Configuration Permissions

3. 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.



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

○ The interactive user.

○ The launching user.

● This user.

User: wwuser

Password: ••••••••••••••••

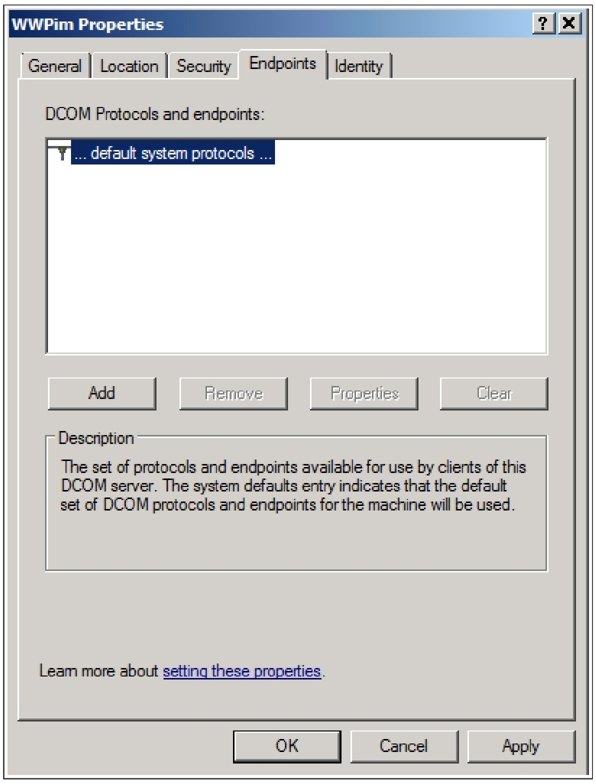
Confirm password: ••••••••••••••••

○ The system account (services only).

Learn more about setting these properties.

Figure 10: This User Identity Option

The **Endpoints** tab panel should look similar to the following graphic (Figure 11 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.

Learn more about setting these properties.

Figure 11: DCOM Default System Client Protocols

4. Click **OK**.
5. Ensure that all the same settings used for **WWPim** are applied for the **DCOMTransport**.
6. From the **Component Services** window, right-click **My Computer** then click **Properties**.

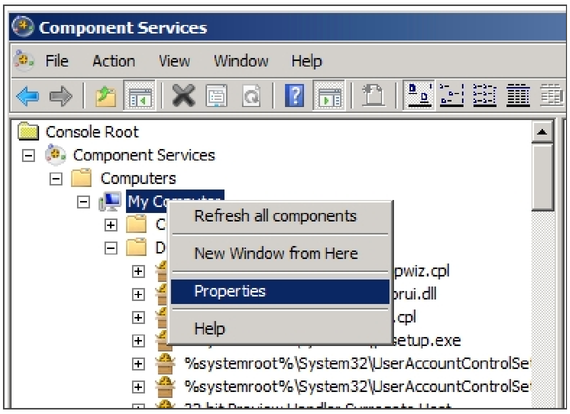
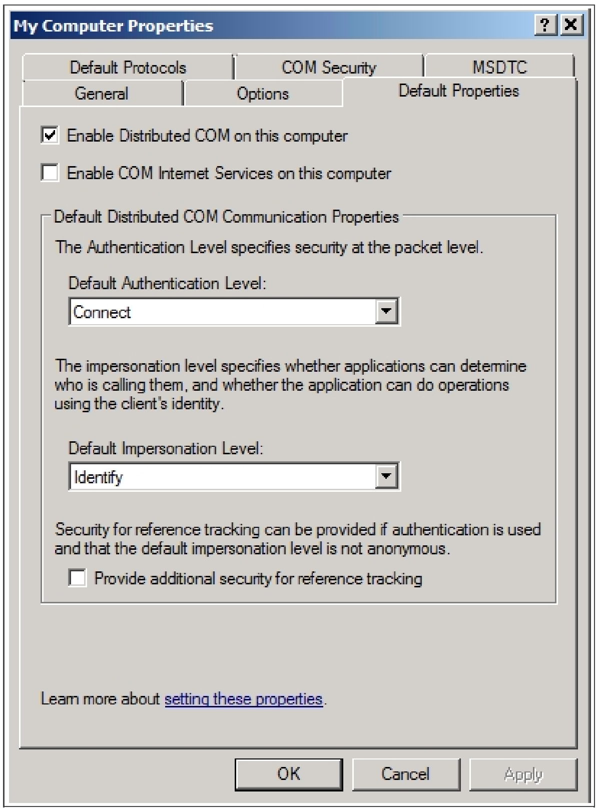


Figure 12: My Computer / Properties

7. Ensure the **Enable Distributed COM on this computer** option is checked (Figure 13 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

Security for reference tracking can be provided if authentication is used and that the default impersonation level is not anonymous.

□ Provide additional security for reference tracking

Learn more about setting these properties.

Figure 13: Default Properties 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 14 below):

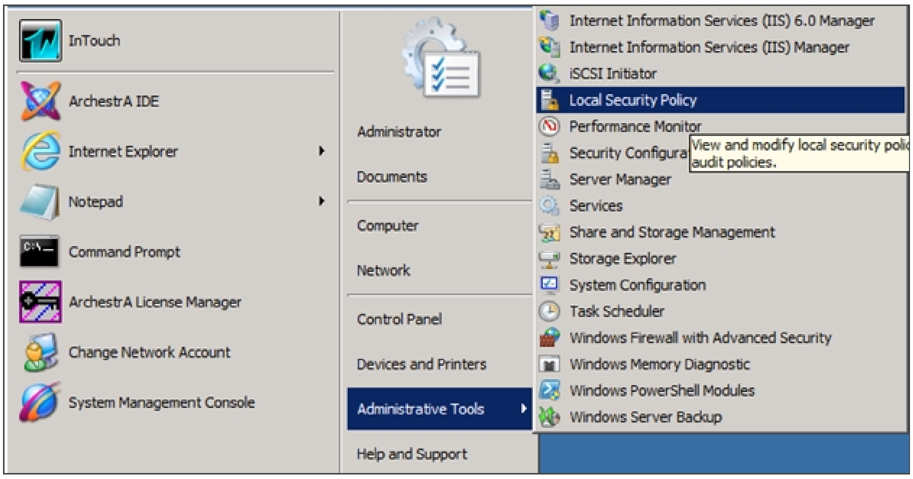
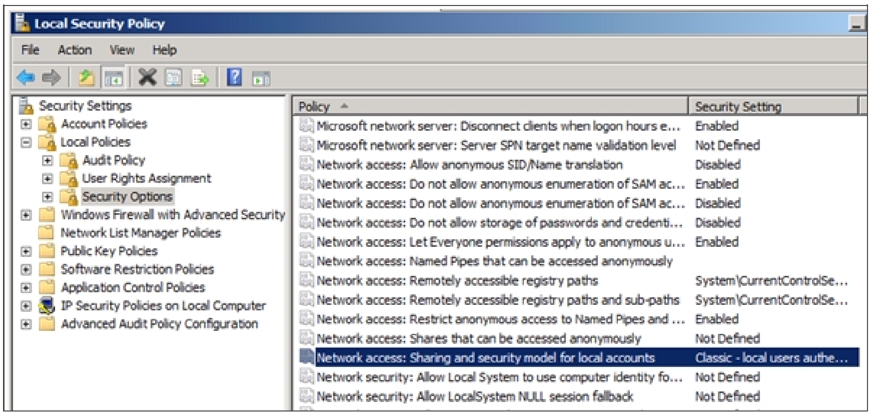


Figure 14: Local Security Policy

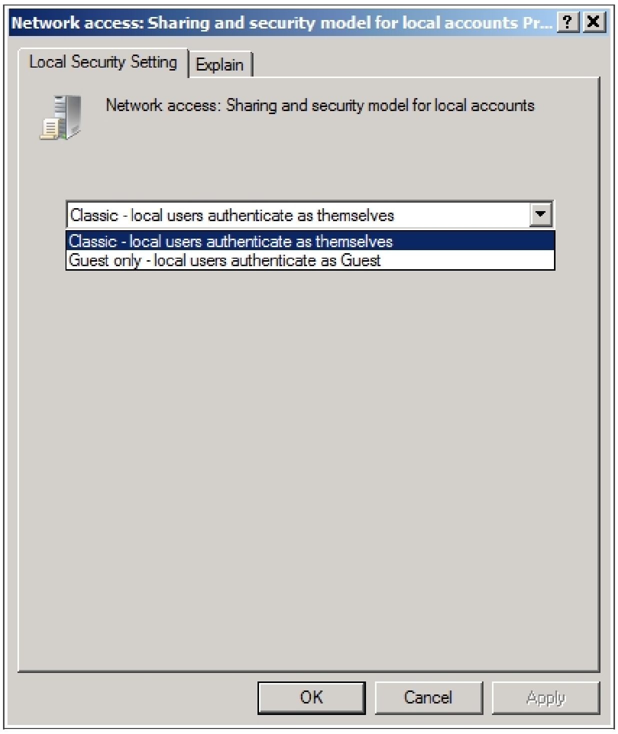
2. Expand the **Local Policies** folder , then click **Security Options**.
3. Double-click **Network access: Sharing and security model for local accounts**.


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration

Policy	Security Setting
Microsoft network server: Disconnect clients when logon hours e...	Enabled
Microsoft network server: Server SPN target name validation level	Not Defined
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM ac...	Enabled
Network access: Do not allow anonymous enumeration of SAM ac...	Disabled
Network access: Do not allow storage of passwords and credenti...	Disabled
Network access: Let Everyone permissions apply to anonymous u...	Enabled
Network access: Named Pipes that can be accessed anonymously	
Network access: Remotely accessible registry paths	System\CurrentControlSe...
Network access: Remotely accessible registry paths and sub-paths	System\CurrentControlSe...
Network access: Restrict anonymous access to Named Pipes and ...	Enabled
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accounts	Classic - local users authe...
Network security: Allow Local System to use computer identity fo...	Not Defined
Network security: Allow LocalSystem NULL session fallback	Not Defined

Figure 15: 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 accounts Pr...
?
Local Security Setting
Explain
OK
Cancel
Apply

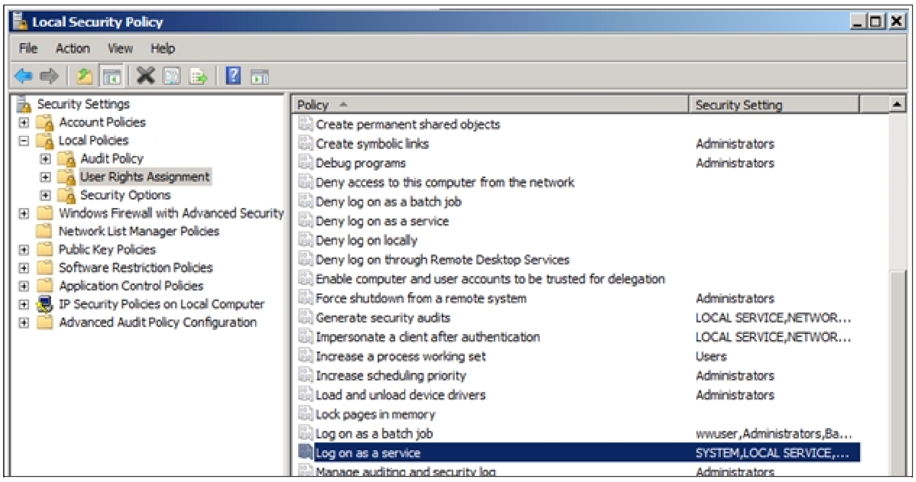
Network access: Sharing and security model for local accounts

Classic - local users authenticate as themselves

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

Figure 16: Classic Security Setting

5. Click **OK** to save the setting.
6. Select **User Rights Assignment** under **Local Policies** then double-click **Log on as a service**.

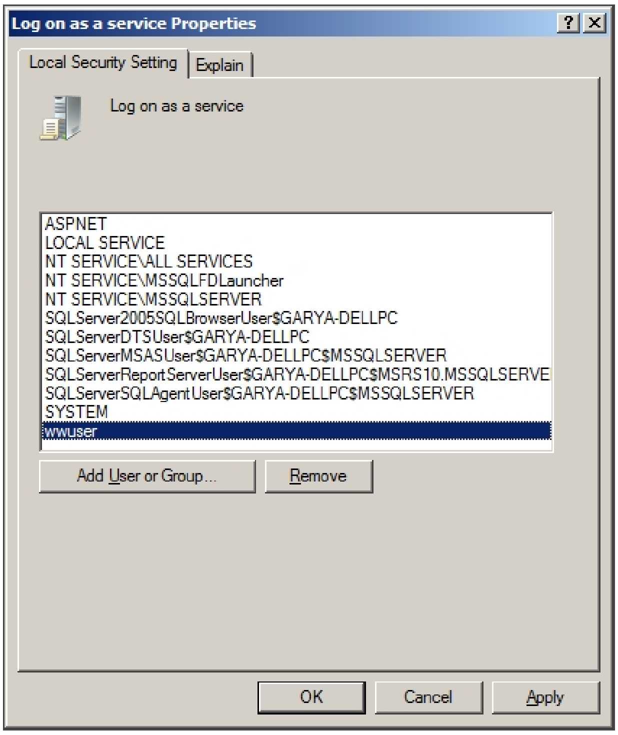


- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Firewall with Advanced Security
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Computer
  - Advanced Audit Policy Configuration

Policy	Security Setting
Create permanent shared objects	
Create symbolic links	Administrators
Debug programs	Administrators
Deny access to this computer from the network	
Deny log on as a batch job	
Deny log on as a service	
Deny log on locally	
Deny log on through Remote Desktop Services	
Enable computer and user accounts to be trusted for delegation	
Force shutdown from a remote system	Administrators
Generate security audits	LOCAL SERVICE,NETWOR...
Impersonate a client after authentication	LOCAL SERVICE,NETWOR...
Increase a process working set	Users
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as a batch job	wwuser,Administrators,Ba...
Log on as a service	SYSTEM,LOCAL SERVICE,...
Manage auditing and security log	Administrators

Figure 17: Log on as a Service Setting

7. Ensure that the ArchestrA Network Admin account is listed here. In Figure 18 (below), it is **wwuser**.

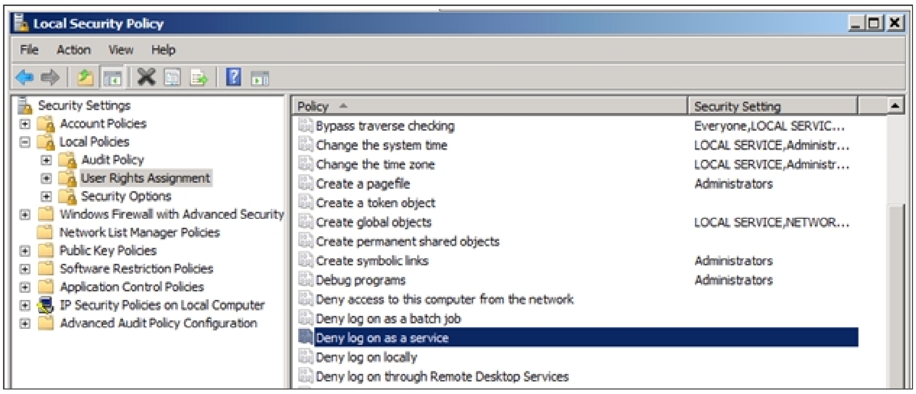


Log on as a service

ASPNET
LOCAL SERVICE
NT SERVICE\ALL SERVICES
NT SERVICE\MSSQLFDLauncher
NT SERVICE\MSSQLSERVER
SQLServer2005SQLBrowserUser$GARYA-DELLPC
SQLServerDTSUser$GARYA-DELLPC
SQLServerMSASUser$GARYA-DELLPC$MSSQLSERVER
SQLServerReportServerUser$GARYA-DELLPC$MSRS10.MSSQLSERVE
SQLServerSQLAgentUser$GARYA-DELLPC$MSSQLSERVER
SYSTEM
wwuser

Figure 18: Logon as a Service Security Property

8. Similarly check if the Archestra Network Admin Account is added in the following policies:
   - Log on as a batch job
   - Deny log on locally
   - Deny log on through Remote Desktop Services
   - Act as part of the operating system. (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.)
9. Double-click **Deny logon as a service**.

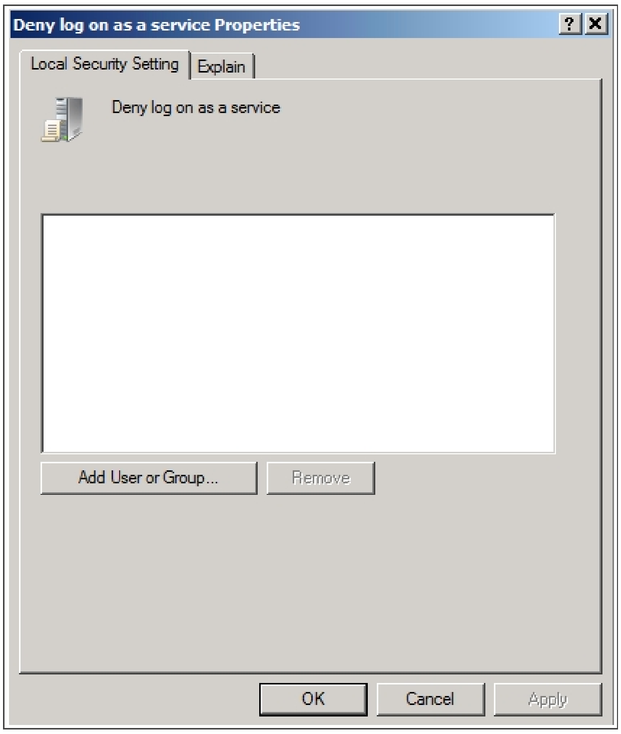


- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Firewall with Advanced Security
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Computer
  - Advanced Audit Policy Configuration

Policy	Security Setting
Bypass traverse checking	Everyone,LOCAL SERVIC...
Change the system time	LOCAL SERVICE,Administr...
Change the time zone	LOCAL SERVICE,Administr...
Create a pagefile	Administrators
Create a token object	
Create global objects	LOCAL SERVICE,NETWOR...
Create permanent shared objects	
Create symbolic links	Administrators
Debug programs	Administrators
Deny access to this computer from the network	
Deny log on as a batch job	
Deny log on as a service	
Deny log on locally	
Deny log on through Remote Desktop Services	

Figure 19: Deny Logon as a Service

10. Ensure that the ArchestrA Network Admin account (referenced above) is *not* listed here (Figure 20 below).



Deny log on as a service

Figure 20: Deny Logon as a Service Security Property

11. Click **OK**.

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.

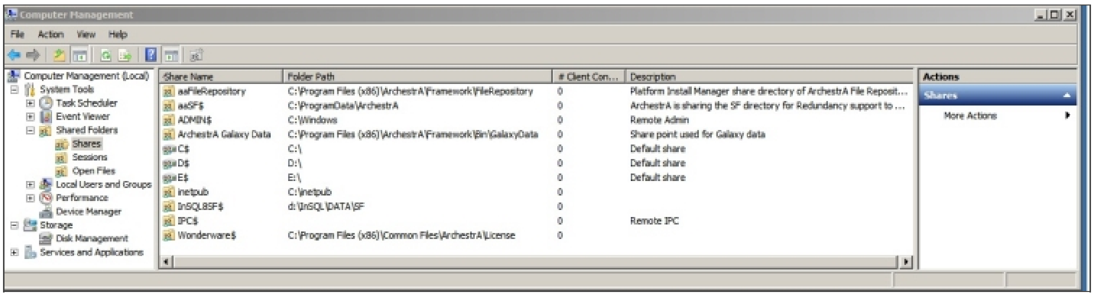
Note: The user logged on to the desktop of the remote machine that is trying to launch an IDE for remote GR access must be an Administrator of the remote machine. Administrator permissions are necessary to allow proper DCOM and similar communication.

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	# Client Con...	Description
aaFileRepository	C:\Program Files (x86)\ArchestrA\Framework\FileRepository	0	Platform Install Manager share directory of ArchestrA File Reposit...
aaSF$	C:\ProgramData\ArchestrA	0	ArchestrA is sharing the SF directory for Redundancy support to ...
ADMIN$	C:\Windows	0	Remote Admin
ArchestrA Galaxy Data	C:\Program Files (x86)\ArchestrA\Framework\Bin\GalaxyData	0	Share point used for Galaxy data
C$	C:\	0	Default share
D$	D:\	0	Default share
E$	E:\	0	Default share
inetpub	C:\inetpub	0	
InSQL8SF$	d:\InSQL\DATA\SF	0	
IPC$		0	Remote IPC
Wonderware$	C:\Program Files (x86)\Common Files\ArchestrA\License	0	

Figure 23: Shared System Folders

Windows Configuration – Folder Options

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

   Note: If the **Tools** menu is not visible, press **F10** to see the menu.

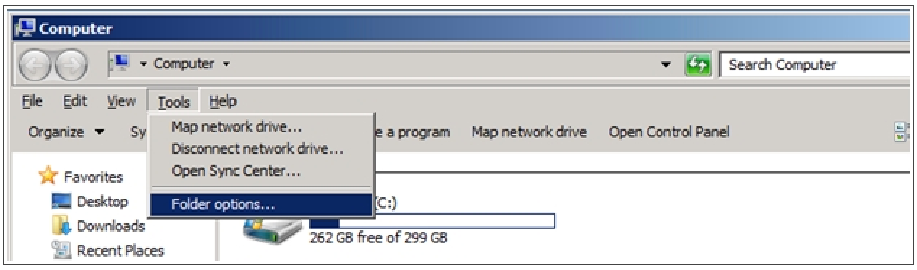
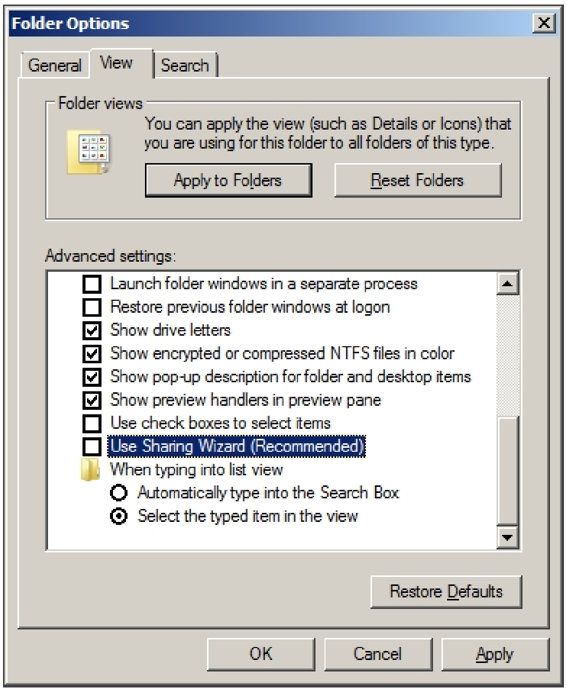


Figure 24: Windows Explorer Folder Options

2. Uncheck the **Use Sharing Wizard (Recommended)** option.



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

Advanced settings:

- □ Launch folder windows in a separate process
- □ Restore previous folder windows at logon
- ☑ Show drive letters
- ☑ Show encrypted or compressed NTFS files in color
- ☑ Show pop-up description for folder and desktop items
- ☑ Show preview handlers in preview pane
- □ Use check boxes to select items
- □ Use Sharing Wizard (Recommended)
- When typing into list view
  - ○ Automatically type into the Search Box
  - ● Select the typed item in the view

Figure 25: Disable Simple File Sharing

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/Clock, Language, and Region/Region and Language**.