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

Application Versions

- Wonderware Application Server 3.5 (2012). Please check the compatability matrix at the Wonderware Tech 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**.
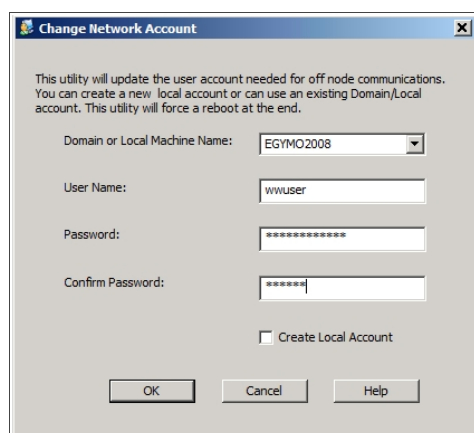

Figure 1: Change Network Account Utility Interface

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 GCS 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.

Terms of Use| Privacy Policy

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).
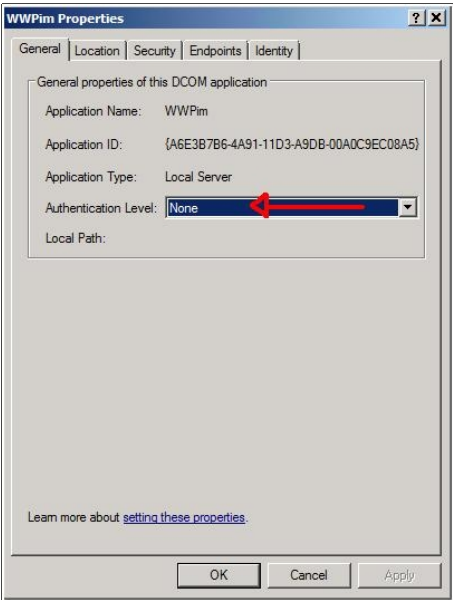

Figure 4: WWPim Authentication Level

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**.
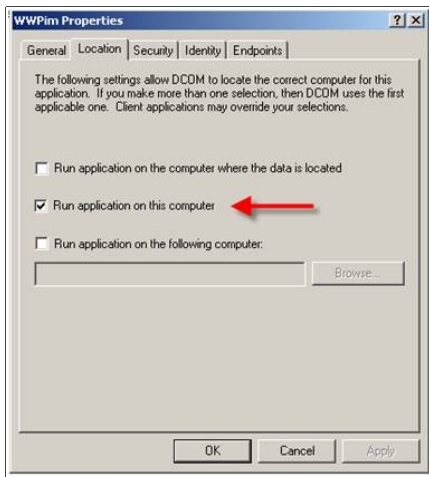
Terms of Use| Privacy Policy

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.
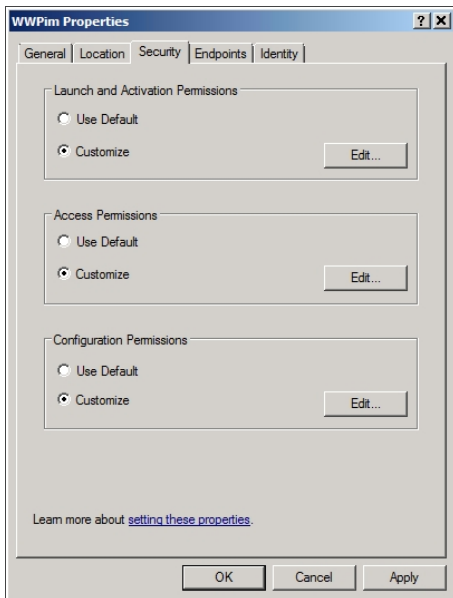

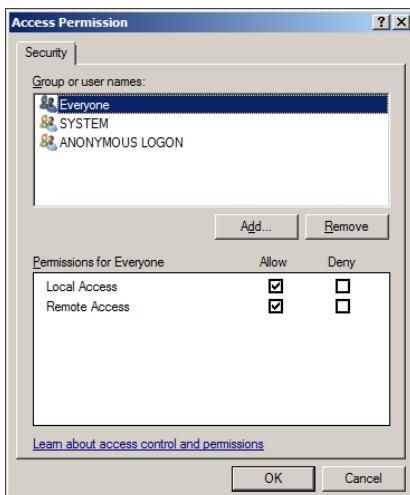Figure 6: Security Properties Tab Panel
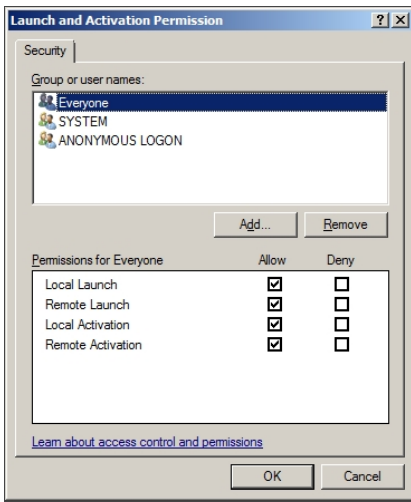

Figure 7: Security Settings for Access Permissions

AVEVA

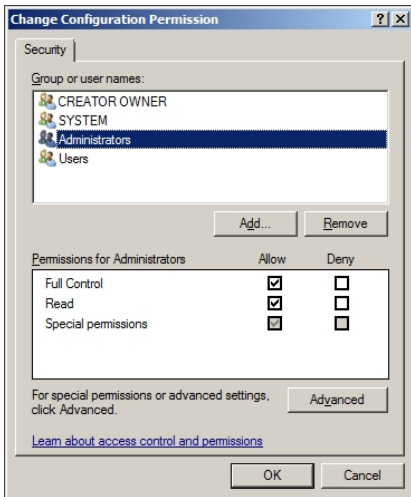Figure 8: Security Settings for Launch and Activation Permissions

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.
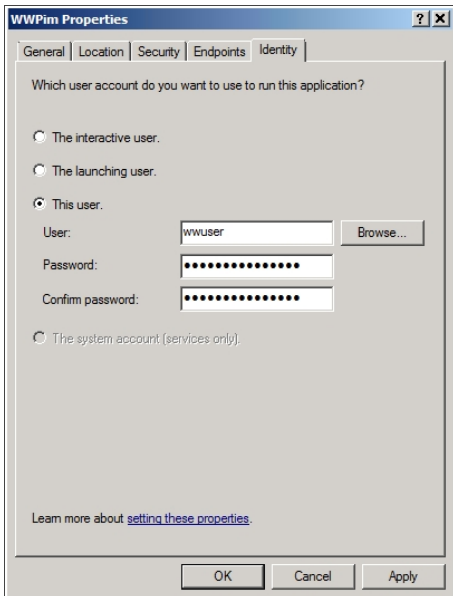
Figure 10: This User Identity Option

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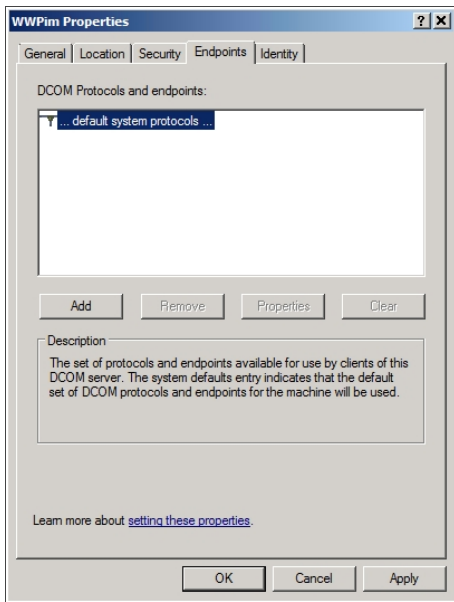
AVEVA

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**.
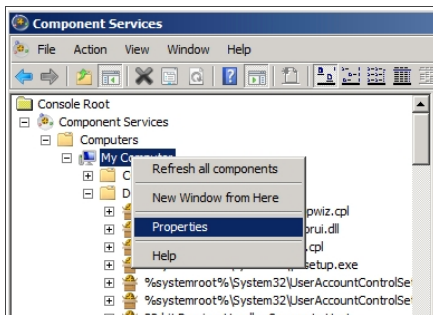6. From the **Component Services** window, right-click **My Computer** then click **Properties**.

Figure 12: My Computer / Properties

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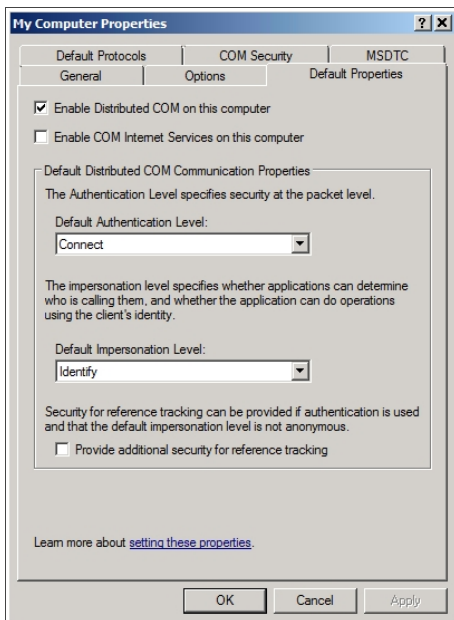

Figure 13: Default Properties Configuration

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.

AVEVA

Configure local security settings from the Control Panel.

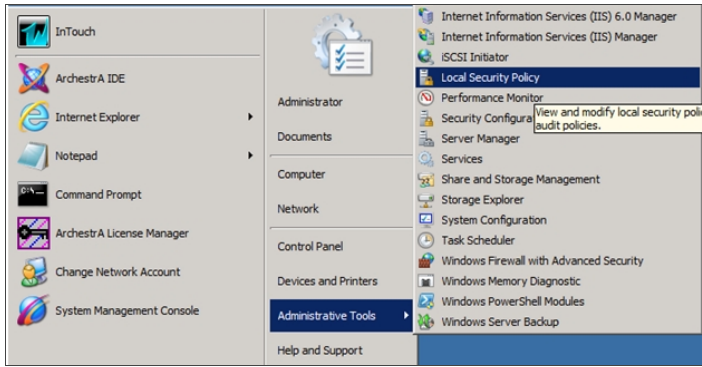1. Click **Administrative Tools/Local Security Policy** (Figure 14 below):

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**.
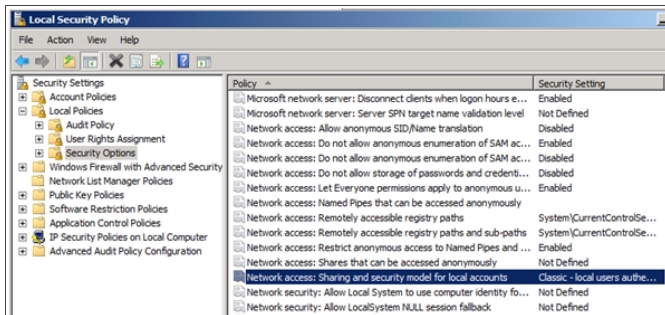

Figure 15: Network Access: Sharing and security model for local accounts

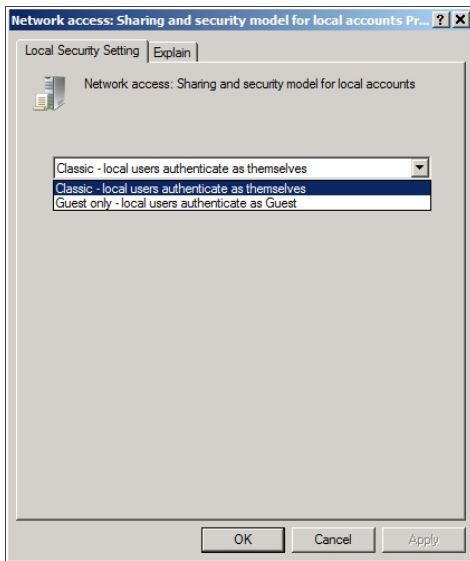4. Ensure that the selected option is **Classic** and not **Guest only**.

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**.
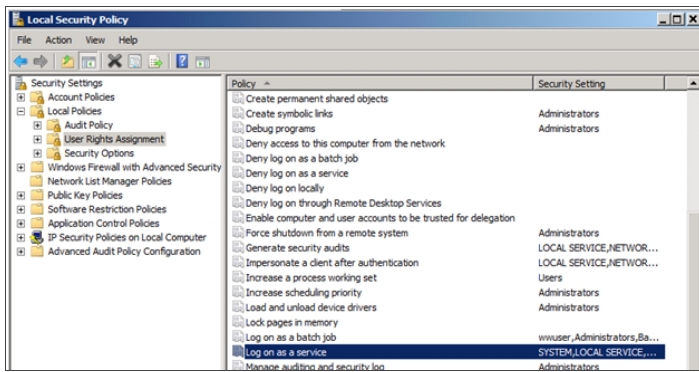
Figure 17: Log on as a Service Setting

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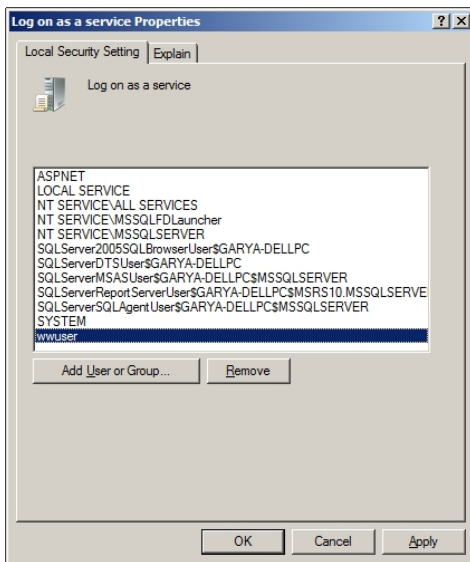

Figure 18: Logon as a Service Security Property

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.)
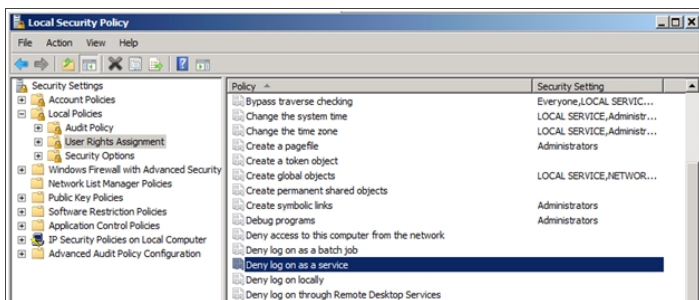9. Double-click **Deny logon as a service**.

Figure 19: Deny Logon as a Service

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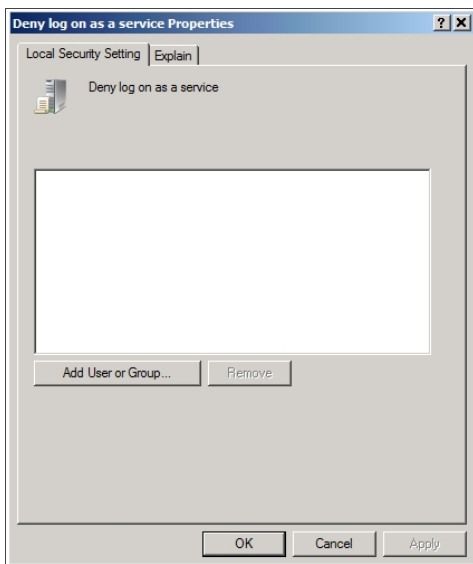
AVEVA

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$**
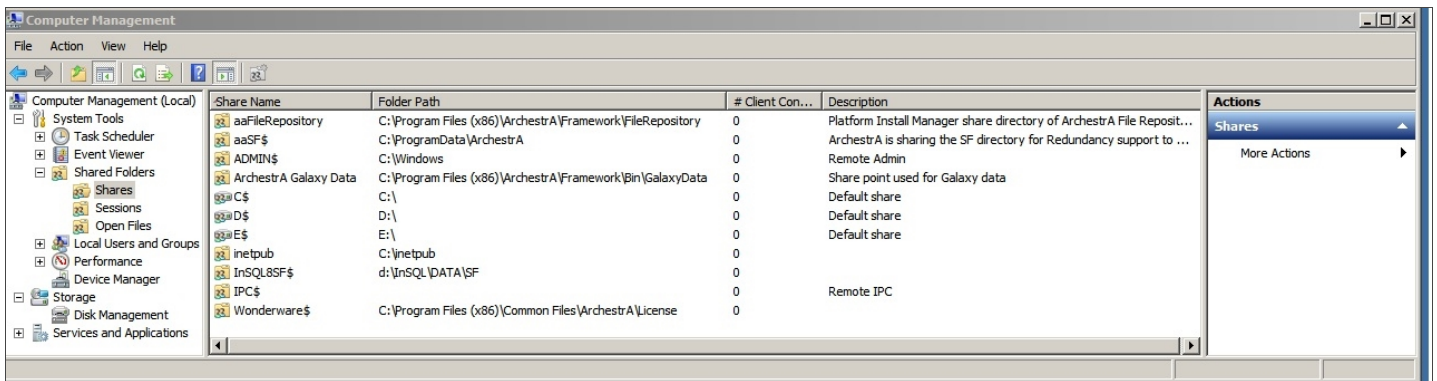- **ArchestrA Galaxy Data**
- **Wonderware$**

Figure 23: Shared System Folders

Windows Configuration – Folder Options

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

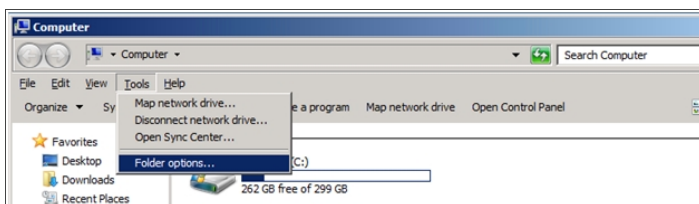   **Note:** If the **Tools** menu is not visible, press **F10** to see the menu.

Figure 24: Windows Explorer Folder Options

2. Uncheck the **Use Sharing Wizard (Recommended)** option.
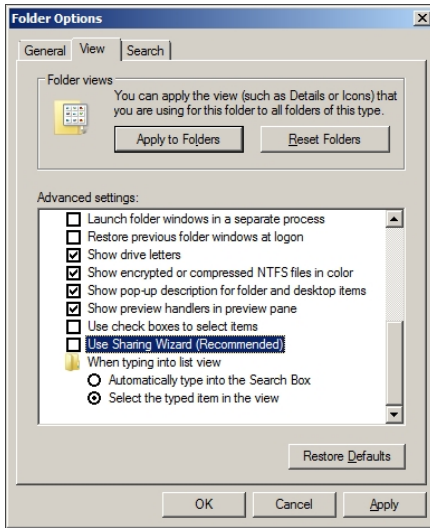
Figure 25: Disable Simple File Sharing

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**.