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#: 002677 Created: August 2012

#### Introduction

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.

#### **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.

Change Network Account		×
This utility will update the user account of You can create a new local account or of account. This utility will force a reboot a	can use an existing Domain/Local	
Domain or Local Machine Name:	EGYMO2008	
User Name:	wwuser	
Password:	******	
Confirm Password:	*****	
	Create Local Account	
ОК	Cancel Help	

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 WDN.

#### To run the Wonderware O/S 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
(D) 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
Rev 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
- http://www.linklogger.com/TCP135.htm

- http://www.linklogger.com/TCP139.htm
- http://www.linklogger.com/TCP445.htm

Complete the following tasks to ensure DCOM settings are correct.

# DCOM – Checking Wonderware-Compatible Security Settings

1. Run dcomcnfg.exe from Start/Run.

This is the editor you use to make local DCOM changes to DCOM security levels on the computer.

2. Expand the branches as follows:

#### Component Services/Computers/MyComputer/DCOM Config.

- 3. Check the following packages.
- The first package is WWPim (aka Wonderware Platform Information Manager)
- Right click WWPim, then click Properties (Figure 3 below).

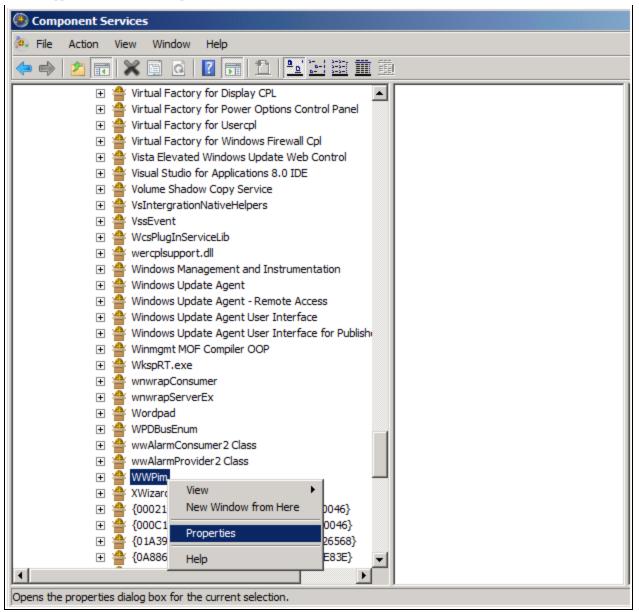


FIGURE 3: WWPIM DCOM SERVICE PROPERTIES

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

WPim Properties		2
General   Location   Secu	urity Endpoints Identity	
General properties of th	nis DCOM application	-12
Application Name:	WWPim	
Application ID:	{A6E3B7B6-4A91-11D3-A9DB-00A0C9EC08A5	}
Application Type:	Local Server	
Authentication Level:	None	
Local Path:		2
Leam more about <u>setting</u>	1 these properties.	
		8
	OK Cancel Apply	j.

FIGURE 4: WWPIM AUTHENTICATION LEVEL

• Click the Location tab and make sure the Run application on this computer box is checked.

**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.

WPim Properties		<u>? ×</u>
General Location	Security   Identity   Endpoints	
application. If you m	s allow DCDM to locate the correct ake more than one selection, ther at applications may override your s	DCOM uses the first
Run application	on the computer where the data is	located
Run application	on this computer	-
Run application	on the following computer:	
		Browse
	OK Can	cel Apply

FIGURE 5: 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.

WWPim Properties		? X
General Location Security Endpoints Identity		
Launch and Activation Permissions		
O Use Default		
Customize	E	dit
Access Permissions		
C Use Default		
Customize	E	dit
Configuration Permissions		
C Use Default		
Customize	E	dit
Learn more about <u>setting these properties</u> .		
OK Can	cel	Apply

FIGURE 6: SECURITY PROPERTIES TAB PANEL

Access Permission		?	×
Security			
Group or user names:			
Everyone SYSTEM			
& ANONYMOUS LOGON			
	A <u>d</u> d	<u>R</u> emove	
Permissions for Everyone	Allow	Deny	
Local Access			
Remote Access	$\mathbf{\nabla}$		
Leam about access control and p	emissione		
			-
	OK	Cancel	

FIGURE 7: SECURITY SETTINGS FOR ACCESS PERMISSIONS

Security Group or user names:	
Everyone	
Sector Se	
SYSTEM ANONYMOUS LOGON	
-	
A <u>d</u> d <u>R</u> emove	
Permissions for Everyone Allow Deny	
Local Launch	
Remote Launch	
Local Activation	
Remote Activation	
Leam about access control and permissions	
OK Cancel	

FIGURE 8: SECURITY SETTINGS FOR LAUNCH AND ACTIVATION PERMISSIONS

Change Configuration Permission		[	<u>? ×</u>
Security			
Group or user names:			_
CREATOR OWNER			
Administrators			
Sers Users			
	A <u>d</u> d	<u>R</u> emove	
Permissions for Administrators	Allow	Deny	
Full Control	$\checkmark$		
Read	$\checkmark$		
Special permissions	$\checkmark$		
			-
For special permissions or advanced click Advanced.	l settings,	Ad <u>v</u> anced	
Leam about access control and per	missions		
	ОК	Cance	el

FIGURE 9: SECURITY SETTINGS FOR 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**.

WWPim Properties
General Location Security Endpoints Identity
Which user account do you want to use to run this application?
O The interactive user.
O The launching user.
This user.
User: www.ser Browse
Password:
Confirm password:
C The system account (services only).
Leam more about <u>setting these properties</u> .
OK Cancel Apply

FIGURE 10: THIS USER IDENTITY OPTION

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

WWPim Properties	? X
General Location Security Endpoints Identity	
DCOM Protocols and endpoints:	
▼ default system protocols	
Add         Remove         Properties         Clear           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.	
Leam more about <u>setting these properties</u> .	
OK Cancel App	ly

FIGURE 11: DCOM DEFAULT SYSTEM CLIENT PROTOCOLS

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

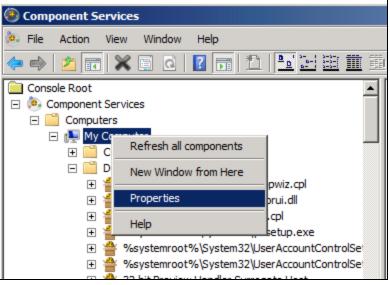


FIGURE 12: MY COMPUTER / PROPERTIES

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

Computer Propertie	es	?)
Default Protocols	COM Security	MSDTC
General	Options	Default Properties
	et Services on this computer	
	OM Communication Propertie	
	evel specifies security at the	packet level.
Default Authenticat	tion Level:	-
Connect	<b>_</b>	
	vel specifies whether applica and whether the application o atity.	
who is calling them, a using the client's iden Default Impersonati	and whether the application of t	
who is calling them, a using the client's iden	and whether the application of t	
who is calling them, a using the client's iden Default Impersonati Identify Security for reference	and whether the application of t	an do operations
who is calling them, a using the client's iden Default Impersonati Identify Security for reference and that the default in	and whether the application of ntity. ion Level:	authentication is used nymous.
who is calling them, a using the client's iden Default Impersonati Identify Security for reference and that the default in	and whether the application of ntity. ion Level: tracking can be provided if mpersonation level is not ano	an do operations
who is calling them, a using the client's iden Default Impersonati Identify Security for reference and that the default in	and whether the application of ntity. ion Level: tracking can be provided if mpersonation level is not ano	an do operations
who is calling them, a using the client's iden Default Impersonati Identify Security for reference and that the default in	and whether the application of ntity. ion Level: tracking can be provided if mpersonation level is not ano	authentication is used nymous.
who is calling them, a using the client's iden Default Impersonati Identify Security for reference and that the default in	and whether the application of ntity. ion Level: tracking can be provided if mpersonation level is not ano nal security for reference trac	an do operations
who is calling them, a using the client's iden Default Impersonati Identify Security for reference and that the default in Provide addition	and whether the application of ntity. ion Level: tracking can be provided if mpersonation level is not ano nal security for reference trac	authentication is used nymous.
who is calling them, a using the client's iden Default Impersonati Identify Security for reference and that the default in Provide addition	and whether the application of ntity. ion Level: tracking can be provided if mpersonation level is not ano hal security for reference trac	authentication is used nymous.

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):

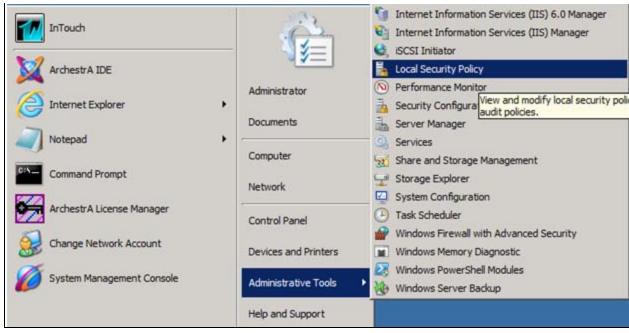


FIGURE 14: LOCAL SECURITY POLICY

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

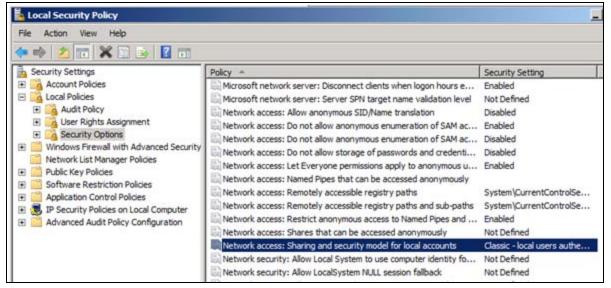


FIGURE 15: NETWORK ACCESS: SHARING AND SECURITY MODEL FOR LOCAL ACCOUNTS

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

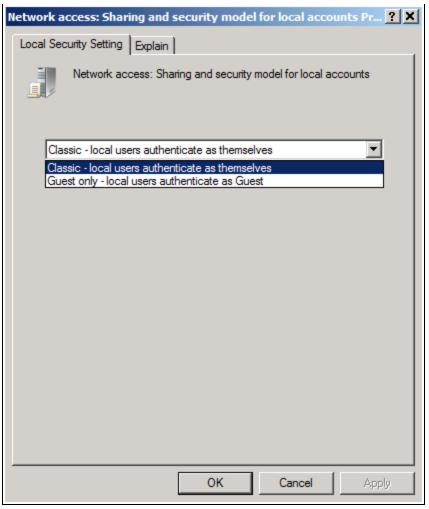


FIGURE 16: CLASSIC SECURITY SETTING

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

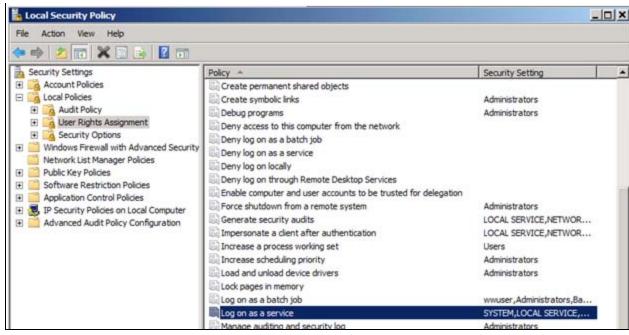


FIGURE 17: LOG ON AS A SERVICE SETTING

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

Log on as a service Properties	? ×
Local Security Setting Explain	
Log on as a service	
ASPNET LOCAL SERVICE NT SERVICEVALL SERVICES NT SERVICEVMSSQLFDLauncher NT SERVICEVMSSQLSERVER SQLServer2005SQLBrowserUser\$GARYA-DELLPC SQLServerDTSUser\$GARYA-DELLPC SQLServerMSASUser\$GARYA-DELLPC\$MSSQLSERVER SQLServerReportServerUser\$GARYA-DELLPC\$MSSQLSERVER SQLServerSQLAgentUser\$GARYA-DELLPC\$MSSQLSERVER SYSTEM	
Add <u>U</u> ser or Group <u>R</u> emove	
OK Cancel Ap	ply

FIGURE 18: LOGON AS A SERVICE SECURITY PROPERTY

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

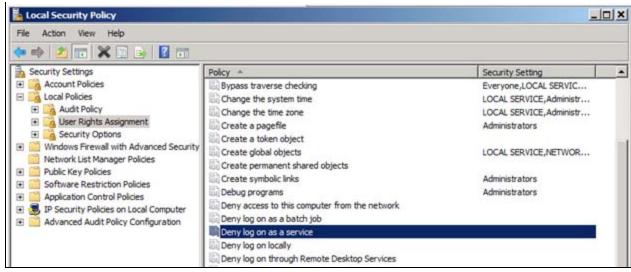


FIGURE 19: DENY LOGON AS A SERVICE

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

Deny log on as a service Properties	×
Local Security Setting Explain	
Deny log on as a service	
Add User or Group Remove	
OK Cancel Apply	

FIGURE 20: 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.

le Action View Help		
Security Settings	Policy *	Security Setting
Account Policies	Access Credential Manager as a trusted caller	Security Security
Local Policies	Access this computer from the network	Everyone, Administrators,
Audit Policy	Act as part of the operating system	www.ser
User Rights Assignment     Security Options     Windows Firewall with Advanced Security     Network List Manager Policies	Add workstations to domain	wwwser
	Adjust memory guotas for a process	LOCAL SERVICE, NETWOR
	Allow log on locally	Administrators,Users,Back
	Allow log on through Remote Desktop Services	Administrators, Remote De
Public Key Policies	Back up files and directories	Administrators, Backup Op
Software Restriction Policies     Application Control Policies     Joint Control Policies     Application Control Policies on Local Computer     Advanced Audit Policy Configuration	Bypass traverse checking	Everyone,LOCAL SERVIC
	Change the system time	LOCAL SERVICE.Administr
	Change the system time	LOCAL SERVICE, Administr
	Create a pagefie	Administrators
	Create a pagene	Administrators
	Create global objects	LOCAL SERVICE NETWOR
		LOCAL SERVICE, NETWOR
	Create permanent shared objects	A designation of the second
	Create symbolic links	Administrators 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

FIGURE 21: ADMINISTRATOR PERMISSIONS FOR THE OPERATING SYSTEM SECURITY SETTING

Act as part of the operating system Properties	? ×
Local Security Setting Explain	
Act as part of the operating system	
	_
wwuser	
Add User or Group Remove	
OK Cancel A	pply

FIGURE 22: 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\$

🚇 Computer Management					
File Action View Help					
🗢 🔿 🞽 🖬 🛛 😫 👔	<b>B</b>				
	-Share Name	Folder Path	# Client Con	Description	Actions
🖻 👔 System Tools	aaFileRepository	C:\Program Files (x86)\ArchestrA\Framework\FileRepository	0	Platform Install Manager share directory of ArchestrA File Reposit	Shares 🔺
🕀 🕒 Task Scheduler	🐹 aaSF\$	C:\ProgramData\ArchestrA	0	ArchestrA is sharing the SF directory for Redundancy support to	
🛨 🛃 Event Viewer	ADMIN\$	C:\Windows	0	Remote Admin	More Actions
Shared Folders	🔞 ArchestrA Galaxy Data	C:\Program Files (x86)\ArchestrA\Framework\Bin\GalaxyData	0	Share point used for Galaxy data	
3 Shares	1 C\$	C:\	0	Default share	
3 Sessions	338 D\$	D:\	0	Default share	
👸 Open Files	1000 E\$	E:\	0	Default share	
	🐹 inetpub	C: \inetpub	0		
Device Manager	1 InSQL8SF\$	d:\InSQL\DATA\SF	0		
E Storage	2 IPC\$		0	Remote IPC	
🔤 Disk Management	🕺 Wonderware\$	C:\Program Files (x86)\Common Files\ArchestrA\License	0		
E Services and Applications	•			•	
	,,				,

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.

COO - Computer -			👻 த Search Computer			
Eile Edit View	Tools Help					
Organize 🔻 Sy	Map network drive Disconnect network drive	e a program	Map network drive	Open Control Pane		
🔆 Favorites	Open Sync Center					
E Desktop	Folder options	(C:)				

FIGURE 24: WINDOWS EXPLORER FOLDER OPTIONS

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

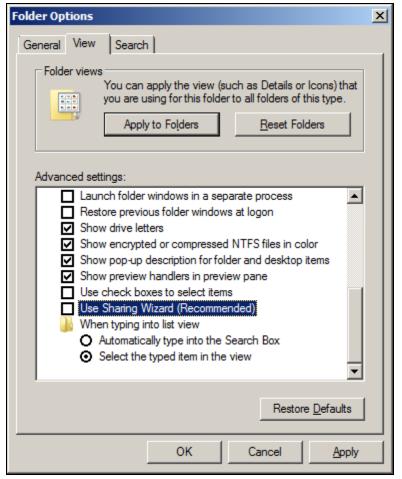


FIGURE 25: DISABLE SIMPLE FILE SHARING

# 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**.

N. Nhadikar, P. Karthekian, G. Alldredge

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

©2012 Invensys Systems, Inc. All rights reserved. No part of the material protected by this copyright may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording, broadcasting, or by anyinformation storage and retrieval system, without permission in writing from Invensys Systems, Inc. Terms of Use.