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

Topic#: 002809 Created: October 2013

### Introduction

Wonderware Historian Client (HistClient) allows you to publish reports using Microsoft Excel, Word, and Trend to the ActiveFactory Reporting Website (AFRWS). If you experience any problem in publishing HistClient reports to the AFRWS, you can use the recommendations in this *Tech Note* to trouble-shoot and to resolve the problem.

Since you can use the Wonderware Information Server (WIS) to view the published reports, AFRWS and WIS are used interchangeably in this *Tech Note*.

Because any of these suggestions can resolve the issue, you should go back to check if it helps resolving the issue after applying each of the tips.

### **Application Versions**

- Wonderware Historian Client 2012 R2 (version 10.1) or above
- Wonderware Information Server (WIS) 2012 R2 (version 5.0) or above
- Wonderware Historian 11.0 P01 or above
- Microsoft Office Excel 2007 SP2 (or later), or 2010 (32-bit)
- Microsoft Office Word 2007 SP2 (or later), or 2010 (32-bit)
- Microsoft SQL Server 2008 SP3 or SQL Server 2012

#### Acronyms

- HC: Historian Client Desktop version (Trend, Excel Workbook, Word Report)
- HCRWS: HistClient Reporting Website (used interchangeably with AFRWS)
- **AFRWS**: ActiveFactory Reporting Website (used interchangeably with HCRWS)
- WIS 5.0: Wonderware Information Server 5.0 (used interchangeably with InfoServer)
- AF Web Client: Machine using Internet browser to view published reports

• Historian: Wonderware Historian version 11.0 or above

# Assumptions

This Tech Note assumes that you are familiar with the following products:

- Historian 11.0 or later
- Historian Client 10.1 or later
- Wonderware Information Server (WIS) 5.0 or later
- MS SQL Server 2008 or later
- MS Windows Operating Systems (2008 or Windows 7)

## Overview

The following components are used during AF report publishing to the AFRWS:

# Historian's Runtime Database Tables

The following tables are added to the Runtime database when AFRWS is first installed.

- **aaHistClientReport**: Contains one row for each report that is published.
- **aaHistClientReportsFolder:** Contains one row for each report folder that appears under the main Published Reports navigation node.
- aaHistClientReportSite: Contains basic configuration information for the AFRWS such as the URL.



FIGURE 1: RUNTIME DB TABLES USED BY AFRWS

### Report Folders Located on the Web Server

These folders contain the published reports. Each report type (Static, On Demand, and Scheduled) has its own folder. By default, they are configured under the AFWeb output folder at C:\Inetpub\wwwroot\AFWeb\Output.

Each of these folders contains two subfolders: **Source** and **Target**. When a report is published, the Report Service copies the published report file to the Source folder. The Target folder is used during the actual generation of the report by the website user. For scheduled reports, there is a subfolder for each time period.

**Important:** These tables and stored procedures are for internal use only. Do not modify them.

### XML Files

The XML files control the configuration and parameters for published reports. They are created during the installation of AFRWS Server in the AFWeb folder at C:\Inetpub\wwwroot\AFWeb\Output. The following XML files are used by the Reporting Website:

- **ReportParameters.xml**: This file stores information related to the reports. There is a section for each report group (Pre-Defined, System Status, Summary Reports, and so on), as well as sections for each type of report in the report groups. For published reports, additional sections are included to contain information regarding the report name, file names and paths, the report type, and so on.
- **Configuration.config**: This file stores basic information for the website, such as schedules and archival rules for reports and the folders for scheduled, static, and on-demand reports.
- **ReportsDefinition.xml**: This file stores all of the query definitions for the pre-configured reports, as well as information regarding the style sheet files for these types of reports.

### aaHistClientReportingService

This service performs all the report publishing tasks.

### **Report Publishing Sequence**

- When a report is published to the AFRWS, information about the report is added to the Historian's Runtime database.
- The report file is then copied to the proper report folder on the computer running AFRWS by the aaHistClientReportingService service. The service checks the Runtime database periodically to see if there is a new report to be published to the AFRWS.
- For a **Static** report, the results are saved as an HTML file. When accessing the report, client users see the saved static data.
- For an **On-demand** report, only the report definition is saved, but no data. Current data is retrieved from the database whenever a client user accesses the report.

# Troubleshooting Tips

- 1. Be sure to install MS Office 2007 (SP2 or later) or 2010 (32-bit version only) on the AFRWS/WIS Server node. This is a base-line requirement and will allow you to generate and view the published report.
- 2. Run the O/S Configuration utility if applicable.
- Click the Enable Distributed COM (DCOM) option for the computers running AF desktop components and AFRWS (or WIS). To check this, navigate to My Computer Properties by clicking through Windows Start -> All Programs -> Administrative Tools -> Component Services -> Computer -> My Computer -> Default Properties tab.

General       Options       Default Properties         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	General       Options       Default Properties         Enable Distributed COM on this computer       Enable COM Internet Services on this computer         Default Distributed COM Communication Properties       Image: Communication Properties         The Authentication Level specifies security at the packet level.       Default Authentication Level:         Connect       Image: Communication can determine the applications can determine the specifies whether applications can determine the specifies identity.         Default Impersonation Level:       Image: Communication Level:         Identify       Image: Communication Level:         Default Impersonation Level:       Image: Communication Level:         Identify       Image: Communication Level:         Image: Communication Level:       Image: Communication Level:         Image: Communication Level:       Image: Communication Level:         Image: Communication Level:       Image: Communication Level:         Image: Com	Default Protocols	MSDTC	COM Security
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	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 Gecurity for reference tracking can be provided if authentication is us and that the default impersonation level is not anonymous.	General	Options	Default Properties
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	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 asing the client's identity. Default Impersonation Level: Identify Decurity for reference tracking can be provided if authentication is us and that the default impersonation level is not anonymous. Provide additional security for reference tracking	Enable Distributed C	OM 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	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 the is calling them, and whether the application can do operations using the client's identity. Default Impersonation Level: Identify Cecurity for reference tracking can be provided if authentication is us and that the default impersonation level is not anonymous. Provide additional security for reference tracking	Enable COM Internet	t Services on this comp	uter
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	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 using that the default impersonation level is not anonymous.  Provide additional security for reference tracking	Default Distributed CO	M Communication Prop	artias
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	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 us and that the default impersonation level is not anonymous.  Provide additional security for reference tracking	The Authentication Le	vel specifies security at	the nacket 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	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		ver specifies security at	the packet level.
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	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 us and that the default impersonation level is not anonymous. Provide additional security for reference tracking	Default Authenticatio	on Level:	
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:	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 us and that the default impersonation level is not anonymous.			ROAD A
	Security for reference tracking can be provided if authentication is us and that the default impersonation level is not anonymous.	The impersonation level who is calling them, and	el specifies whether ap id whether the applicat	Dications can determine
	Provide additional security for reference tracking	The impersonation leve who is calling them, an using the client's identi Default Impersonatio Identify	el specifies whether ap nd whether the applicati ity. n Level:	Interpretations can determine on can do operations
Security for reference tracking can be provided if authentication is use and that the default impersonation level is not anonymous.		The impersonation leve who is calling them, an using the client's identi Default Impersonatio Identify Security for reference to and that the default im	el specifies whether ap id whether the applicati ity. in Level: tracking can be provide personation level is not	<ul> <li>Indications can determine on can do operations</li> <li>Indication is use anonymous.</li> </ul>
Security for reference tracking can be provided if authentication is use and that the default impersonation level is not anonymous. Provide additional security for reference tracking		The impersonation leve who is calling them, an using the client's identi Default Impersonatio Identify Security for reference to and that the default im	el specifies whether ap id whether the applicati ity. in Level: tracking can be provide personation level is not al security for reference	<ul> <li>Image: Second state of the second</li></ul>
Security for reference tracking can be provided if authentication is use and that the default impersonation level is not anonymous. Provide additional security for reference tracking		The impersonation level who is calling them, and using the client's identi Default Impersonatio Identify Security for reference to and that the default im Provide additional	el specifies whether ap id whether the applicati ity. in Level: tracking can be provide personation level is not al security for reference	<ul> <li>Image: Second state of the second</li></ul>

FIGURE 2: ENABLING DCOM

# Configure DCOM for Excel to Use The Launching User

- 1. Click Start/All Programs/Administrative Tools.
- 2. Click Component Services/Computers/My Computer/DCOM Config.
- 3. Right-click Microsoft Excel Application (see Note below).
- 4. Click the Identity tab, then click the The launching user option.

• The interactive User: The application will run using the security context of the user currently logged onto the computer. If this option is selected and the user is not logged on, the application will not start.

• The launching User: The application will run using the security context of the user who started the application. The launching user and the interactive user can be the same.

• This user: You can specify the user whose security context will be used to run the application.

🛞 Component Services	
ie Action View Window Help	Microsoft Excel Application Properties
	General Location Security Endpoints Identity
🕀 🚔 IASDataStoreComServer	Which user account do you want to use to run this application?
🗉 🕀 🟯 IASExtensionHost	
🗉 \Xi IEWindows	
🗉 \Xi IIS Admin Service	C The interactive user.
🗉 \Xi 🗄 IIS W3 Control	
🗉 音 IIS WAMREG admin Service	The launching user.
🗉 🕀 iisctl	0.71
🗉 🕀 🚰 IMAPI2	O This user.
🕀 🚔 Internet Explorer Add-on Installer	User: Browse
🗉 🕀 音 IOSrvCfgPersist	
🕀 🕀 IPBusEnum	Password:
🕀 🛨 logagent	
🕀 音 MAPISendMailServer	Confirm password:
🕀 🕀 MAPISendMailServer	
🕀 音 MediaCatalogMergedDB Provider	O The system account (services only).
🕀 🕀 mfeotlkaddin	
🕀 音 Microsoft Access Application	
🕀 🚔 Microsoft Audio Device Graph Server	
🕀 🚔 Microsoft Equation 3.0	
Microsoft Excel Application	
🕀 🍟 Microsoft Graph Application	
🕀 🍟 Microsoft IMAPI	
🕀 🍟 Microsoft Management Console	
Microsoft OneNote Privilege Elevation	
🕀 🍟 Microsoft Outlook Command Button Co	Learn more about setting these properties.
🕀 🎬 Microsoft PowerPoint Slide	
🛨 🚢 Microsoft Publisher Application	
	OK Cancel Apply

FIGURE 3: CONFIGURE MICROSOFT TO USE THE LAUNCHING USER

**Note:** The Component Services list can display the GUID {00020812-0000-0000-0000-0000000046} instead of the application name for MS Office Excel (Figure 3 above).

### Enable Anonymous Access for AFWeb

1. Open the Internet Information Services (IIS) Manager (Run inetmgr).

- 2. Browse to Web Site/Default Web Site.
- 3. Highlight AFWeb and scroll down to the IIS section. Then double-click on the Authentication icon.



FIGURE 4: ENABLING ANONYMOUS ACCESS FOR AFWEB

4. In the Authentication dialog box, enable the Anonymous Authentication option.

Authentication		
Group by: No Grouping		
Name 🔺	Status	Re
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Forms Authentication	Disabled	HT
Windows Authentication	Enabled	HT
Features View 🚰 Content View		

FIGURE 5: ENABLE ANONYMOUS AUTHENTICATION

• Anonymous access allows users to establish an anonymous connection. The user logs on to IIS with an anonymous or guest account.

# Verify aaHistClienReportService Configuration

- 1. Open Control Panel/Administrative Tools/Services.
- 2. Check that the aaHistClientReportService is configured for Automatic and Local System.
- 3. Restart this service after a report has been published.



#### FIGURE 6: AAHISTCLIENTREPORTSERVICE

### Check Event Logs

Check the **Windows Application**, **System**, and **Security Event Viewer** logs for any related messages. If the report failed to be published to the AFWeb site, you will see messages about the failure. These messages can be very useful and you can use the message text to research solutions.

### Verify the Report Exists

Check if the report exists in the aaHistClientReport table (Figure 6 below).

- 1. On the Historian Server, open SQL Server Management Studio.
- 2. Expand Databases/Runtime/Tables.
- 3. Right-click **dbo.aaHistClientReport** and click **Open table**. If the report's name does not appear in the **FileName** column, make sure the aaHistClientReportService is started and DCOM has been configured correctly as shown in the previous steps. Also, check the Windows EventViewer Application log for any related message.
- 4. Check the value of the **Published** column for the **aaHistClientReport** table to see if the value is **1**. This indicates that the report

has been published successfully (Figure 6 below).

K Microsoft SQL Server Managemen	it Stud	io						- N
Eile Edit View Project Query De	esigner	<u>T</u> ools <u>₩</u> in	dow <u>C</u> ommunity	<u>H</u> elp				
🔛 New Query 📄 📸 📸 🚺	3   🖆	; eş eş 🖬		Þ 🖟 😤 .				
😨 🏢 🕺 🐻 Change Type 🔹 📍	500	(= 1 📩 🚈	-					
Object Explorer 🗸 🕈 🗙	CO	NFIG14358V	.tClientReport	Object Explo	rer Details			- ×
Connect 🕶 🛃 🔳 🝸	ĺ.	ReportT	FileName	Description	ApplicationT	LastRun	ReportData	Published
🕀 🧰 System Tables	•	1	Minute1.xls	NULL	2	11/12/2009 11:	<binary da<="" td=""><td>1</td></binary>	1
🛨 🛄 dbo.aaAreaData		2	test2.aaTrend	NULL	1	2/25/2010 2:21	<binary da<="" td=""><td>1</td></binary>	1
+ dbo.aaAreaXML		2	AFDynaRepo	NULL	2	3/5/2010 1:16:	<binary da<="" td=""><td>1</td></binary>	1
T dbo.aaAttributeDataPendi	*	NULL	NULL	NULL	NULL	NULL	NULL	NULL
🕀 🛄 dbo.aaHistClientReport								
dbo.aaHistClientReportsFc     dbo.aaHistClientReportSite								
🕀 🧾 dbo.aaObjectDataPending								
dbo.ActionType								
dbo.AnalogHistory_OLEDB								
dbo.AnalogSpapshot							-	
F dbo.AnalogTag	8							-
	19 3	1	or 3 P P P	Cell	is Read Only.			), i
Ready								1

#### FIGURE 7: AAHISTCLIENTREPORT

5. If the value of the Published column for the report is **0**, verify that the Historian data source from WIS is configured correctly.

# Verify WIS Configuration

- 1. Start up the Wonderware Information Server.
- 2. From the Launch Pad panel, expand Administrator and click Data Source Manager.
- 3. Click the Historian's Data Source name which has data source type of Historian to go to the Modified Shared Data Source dialog box as shown in the following figure.

# **Wonderware Information Server**

	<b>i</b>	ø	<b>a</b>		?
Data Source Manager					
Use this page to modify the selected shared data source. Enter the values in the t save the details.	text boxe:	s and i	click o	n "Sa	ve'
Modify Shared data sources					
Data Source Type : Historian					
ServerName : MYSERVER2					
Database : Runtime					
Integrated Security :					
User Name : sa					
Password :					
Default for this Data Source Type :					
Connection Timeout(in Sec) : 0					
Query Timeout(in Sec) : 0					
Provider : SQLNCLI11					
Has HTTP Mode :					
URL Connection :					
			٦.		
Save Cancel Test Co	onnectio	on i	J		Ţ
	Data Source Manager         Use this page to modify the selected shared data source. Enter the values in the save the details.         Modify Shared data sources         Data Source Type :         Data Source Name :         Data Source Name :         Data Source Name :         Description :         ServerName :         Database :         Integrated Security :         User Name :         Password :         Default for this Data Source Type :         Query Timeout(in Sec) :         Query Timeout(in Sec) :         Provider :         Nurther is the selected shared data source is satisfiered in the selected in the selected source is satisfiered in the selected sou	Data Source Manager         Use this page to modify the selected shared data source. Enter the values in the text boxe save the details.         Modify Shared data sources         Data Source Type :         Data Source Name :         Data Source Name :         Description :         ServerName :         Database :         Integrated Security :         User Name :         Password :         Default for this Data Source Type :         Query Timeout(in Sec) :         Query Timeout(in Sec) :         Provider :         Has HTTP Mode :         URL Connection :	Data Source Manager         Use this page to modify the selected shared data source. Enter the values in the text boxes and save the details.         Modify Shared data sources         Data Source Type :         Data Source Name :         Data Source Name :         Database :         Integrated Security :         User Name :         Password :         Default for this Data Source Type :         Query Timeout(in Sec) :         Query Timeout(in Sec) :         Provider :         URL Connection :         Save         Cancel	Data Source Manager         Use this page to modify the selected shared data source. Enter the values in the text boxes and click o save the details.         Modify Shared data sources         Data Source Type :         Data Source Name :         Data Source Name :         Description :         ServerName :         Database :         Integrated Security :         User Name :         Password :         Default for this Data Source Type :         Query Timeout(in Sec) :         Query Timeout(in Sec) :         Query Timeout(in Sec) :         Query Timeout(in Sec) :         URL Connection :         Save         Cancel	Content Manager         Use this page to modify the selected shared data source. Enter the values in the text boxes and click on "Seave the details.         Modify Shared data sources         Data Source Type :         Data Source Name :         Description :         ServerName :         Database :         Integrated Security :         User Name :         Default for this Data Source Type :         Parsword :         Default for this Data Source Type :         Query Timeout(in Sec) :         Provider :         NuRL Connection :         Save         Cancel

#### FIGURE 8: HISTORIAN DATA SOURCE MANAGER

4. Click the **Test Connection** button at the bottom of the panel to check if everything is configured correctly, and that the Information Server can connect to the Historian Server.

# Match SITEID and ReportSiteKey Values

The SITEID value is found in Configuration.config and it must match the ReportSitekey value in the aaHistClientReportSite table.

1. Use Notepad to open Configuration.config. The location is C:\inetpub\wwwroot\AFWeb\.

2. Search (Ctrl + F) for SITEID. In this example, the SITEID is value 1, and is the same as the ReportSiteKey value of (Figure 8 below):

<SITEID Description="The ID of this site in the Runtime database's aaHistClientReportSite table. This should be set automatically by the installation.">1</SITEID>

3. Confirm the SiteURL value in the aaHistClientReportSite table is correct.

🕵 SQLQuery3.sql - MYSERVER2.Runtime (MAGELLANDEV2000\www.ser (105))* - Microsoft SQL Server Management Studio (Administrator)	<u> </u>
File Edit View Query Project Debug Tools Window Help	
🛅 = 🕮 = 📂 🛃 🎒 🔔 New Query 📑 📸 📸 🐇 💺 隆 🥙 - 🔍 - 💭 - 🖳 🖓 🕨 -	- 🖄 🗒
💷 🔐   Runtime 💿   📍 Execute 🕨 Debug 💻 🧹 🎲 🖻 🔚 📅 🖷   🍘 雛 🏐   🚍 😩   🚎 🚎   🖏 🖕	
Object Explorer 🔹 🖣 🗙 SQLQuery3.sql - MYSV2000\wwuser (105))* 🗙 SQLQuery2.sql - MYSEV2000\wwuser (67))*	<del>.</del>
Connect Image: Connect   Image: Connect Image: Conne	÷ • •
Beportsterkey SiteURL SitePath Description SiteVersion	Wonderware
Image: State and a state of a state o	
Query executed successfully.     MYSERVER2 (11.0 RTM) MAGELLANDEV2000\www.ser Runtime 00	0:00:00 1 rows
Ready Ln 5 Col 3 Ch 3	INS 🌈

#### FIGURE 9: AAHISTCLIENTREPORTSITE

4. Verify that the **ReportSiteKey** in the **aaHistClientReportSite** table matches with that in the **aaHistClientReport** table for the report in question.

# Verify the Output Source Folder Contains the Matching Excel File

- For **OnDemand** reports, go to **C:\inetpub\wwwroot\AfWeb\OnDemand\Source**.
- For Scheduled reports, go to C:\inetpub\wwwroot\AfWeb\Scheduled\Source.
- For Static reports, go to C:\inetpub\wwwroot\AfWeb\Static\Source.

C:\Inetpub\wwwroot\AFWeb\Output	4		
<u>File Edit View Favorites Tools He</u>	lp		<b>1</b>
🔇 Back 🔹 🕥 👻 🍠 🔎 Search 🌔 Fo	olders	🕼 🕑 🗙 🍤 🛄-	
Address C:\Inetpub\wwwroot\AFWeb\Ou	tput		💌 🔁 Go
Folders	×	Name A	
Graphics  Graphics  Graphics  Graphics  Ja  Language  Gutput  Gutput		Scheduled Static Temp	
i zh-CHS E i aspnet_client	-	•	•

FIGURE 9: AFWEB OUTPUT FOLDERS

• Double-click the report in the **Source** folder to open the file there. Any issue or any popup message preventing the file from opening should be resolved before the report can be published to the web site.

**Note:** Multiple instances of Excel.exe processes can be started on the computer running the ActiveFactory Workbook report. If this is the case, close the Workbook and end all Excel.exe processes from the Windows Task Manager, then run the test again.

# Verify the Target Folders Contain Reports

- Verify that the corresponding Target folder contains the HTML file generated by the Reporting Service (aaHistClientReportService) before publishing the report. If the HTML file is not there in the folder, make sure that the aaHistClientReportService is started and DCOM has been enabled for Excel (above).
- For a Scheduled report, go to C:\inetpub\wwwroot\AfWeb\Output\Scheduled\Target.
- For a Static report, go to C:\inetpub\wwwroot\AfWeb\Output\Static\Target.

• For the **OnDemand** report, the report is generated only after the user clicks on the report in the WIS Published Reports/OnDemand Reports tree. The Reporting Service converts the Excel file in the Source folder into an HTML file, names it as tmpXX.html, where XX is a number the aaHistClientReportService assigns to the temporary file. The Service then puts the file into the C:\inetpub\wwwroot\AfWeb\Output\Temp location.

# Verify the Report Name Exists

The **Reportparameters.xml** file is in **C:\inetpub\wwwroot\AfWeb**. If the report is not there, make sure the following folders are configured for **Everyone** with **Full Control**.

- C:\inetpub\wwwroot\AfWeb\Language
- C:\inetpub\wwwroot\AfWeb\Language\en
- C:\inetpub\wwwroot\AfWeb\Language\en-us
- B. Nguyen

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.

For technical support questions, send an e-mail to wwsupport@invensys.com.

# Back to top

©2013 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 any information storage and retrieval system, without permission in writing from Invensys Systems, Inc. Terms of Use.