TIBCO Spotfire® Automation Services 5.5

Installation and Deployment Manual

TIBCO provides the two-second advantage™

Important Information

SOME TIBCO SOFTWARE EMBEDS OR BUNDLES OTHER TIBCO SOFTWARE. USE OF SUCH EMBEDDED OR BUNDLED TIBCO SOFTWARE IS SOLELY TO ENABLE THE FUNCTIONALITY (OR PROVIDE LIMITED ADD-ON FUNCTIONALITY) OF THE LICENSED TIBCO SOFTWARE. THE EMBEDDED OR BUNDLED SOFTWARE IS NOT LICENSED TO BE USED OR ACCESSED BY ANY OTHER TIBCO SOFTWARE OR FOR ANY OTHER PURPOSE.

USE OF TIBCO SOFTWARE AND THIS DOCUMENT IS SUBJECT TO THE TERMS AND CONDITIONS OF A LICENSE AGREEMENT FOUND IN EITHER A SEPARATELY EXECUTED SOFTWARE LICENSE AGREEMENT, OR, IF THERE IS NO SUCH SEPARATE AGREEMENT, THE CLICKWRAP END USER LICENSE AGREEMENT WHICH IS DISPLAYED DURING DOWNLOAD OR INSTALLATION OF THE SOFTWARE (AND WHICH IS DUPLICATED IN LICENSE_TIBCOSPOTFIREAUTOMATIONSERVICES.PDF) OR IF THERE IS NO SUCH SOFTWARE LICENSE AGREEMENT OR CLICKWRAP END USER LICENSE AGREEMENT, THE LICENSE(S) LOCATED IN THE "LICENSE" FILE(S) OF THE SOFTWARE. USE OF THIS DOCUMENT IS SUBJECT TO THOSE TERMS AND CONDITIONS, AND YOUR USE HEREOF SHALL CONSTITUTE ACCEPTANCE OF AND AN AGREEMENT TO BE BOUND BY THE SAME.

This document contains confidential information that is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of TIBCO Software Inc.

TIBCO and Spotfire are either registered trademarks or trademarks of TIBCO Software Inc. and/or subsidiaries of TIBCO Software Inc. in the United States and/or other countries. All other product and company names and marks mentioned in this document are the property of their respective owners and are mentioned for identification purposes only. This software may be available on multiple operating systems. However, not all operating system platforms for a specific software version are released at the same time. Please see the readme.txt file for the availability of this software version on a specific operating system platform.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENT. TIBCO SOFTWARE INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENT AT ANY TIME.

Copyright © 1996 - 2013 TIBCO Software Inc. ALL RIGHTS RESERVED.

THE CONTENTS OF THIS DOCUMENT MAY BE MODIFIED AND/OR QUALIFIED, DIRECTLY OR INDIRECTLY, BY OTHER DOCUMENTATION WHICH ACCOMPANIES THIS SOFTWARE, INCLUDING BUT NOT LIMITED TO ANY RELEASE NOTES AND "READ ME" FILES.

TIBCO Spotfire is covered by U.S. Patent No. 6,014,661 and U.S. Patent No. 7, 216,116. Other patent(s) pending.

TIBCO Software Inc. Confidential Information

Contents

1 Installing Automation Services

1.1 Overview

Installing Automation Services requires knowledge in how to install and administer Internet Information Services and its add-ons. This manual does not specify in detail how to install and administer these programs. For more information on how to do this, please refer to the documentation of the respective programs, or Microsoft support.

1.2 Prerequisites

The version of the Automation Services package that you deploy to your environment must match the version of the TIBCO Spotfire Server and client that users will use to access the server.

Before you install the Automation Services web service, the following software must be installed on your server:

- Windows Server 2008, 2008 R2, or 2012.

- On Windows Server 2012, you must enable Microsoft .NET Framework 3.5.

- Microsoft .NET Framework version 4.0 or 4.5.
  Note: Make sure to upgrade to the latest version of Microsoft .NET Framework.

- Internet Information Services version 7.0 or 8.0.

Make sure that **ASP.NET 4.030319** is **Allowed** in **Internet Information Services**:

▶ **To allow ASP.NET 4.030319 in Internet Information Services**

1 In the **Internet Information Services Manager**, select the server level in the left hand list and select **ISAPI and CGI Restrictions**.
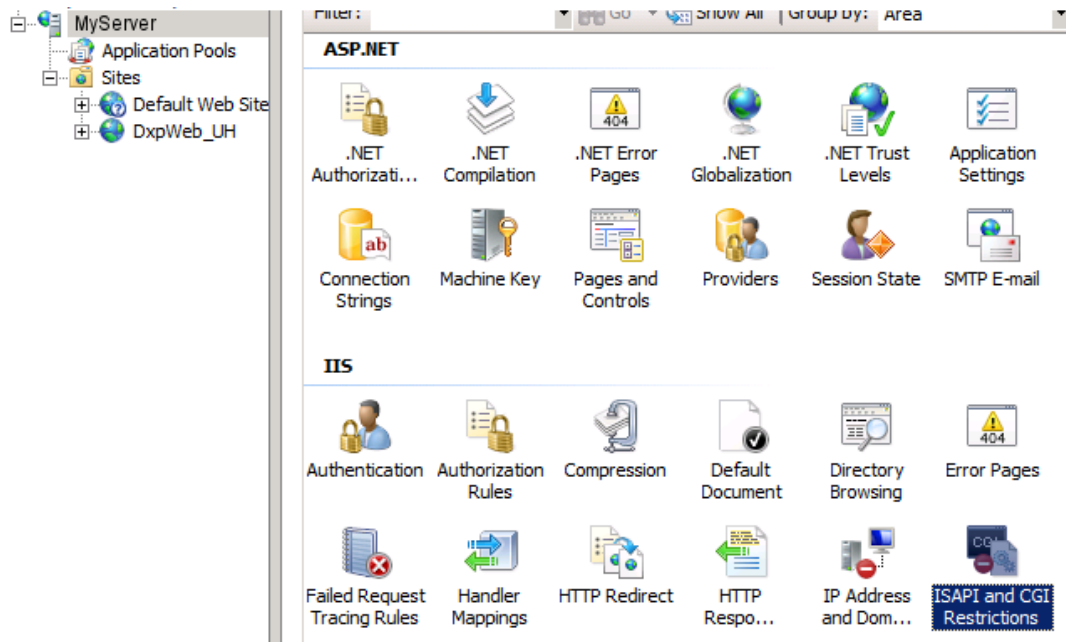
2 Make sure that **ASP.NET 4.0.30319** is present in the list and set it to **Allowed**.

Note: If **ASP.NET 4.0.30319** is not present on Windows Server 2008 or 2008 R2, open the command line and run the following command:

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe /i
```

and return to step 1.

Note: Make sure to use the correct versions of each application. Newer versions, if available, will not necessarily work.

For comprehensive system requirements, refer to the web page http://support.spotfire.com/sr.asp. You should always check here for updated information before you install.

▶ **To enable Microsoft .NET Framework 3.5 on Windows Server 2012**

1 Navigate to the Administrative Tools options on your Microsoft Windows 2012 Server and select **Server Manager**.

2 Select **Dashboard** in the left hand list, and click **Add Roles and Features**.

3 In the Add Roles and Features Wizard, you may see a "Before you begin" dialog. If this is the case click **Next**.

4 In the Select installation type dialog, select **Role-based or feature-based installation** and click **Next**.

5 In the Select destination server dialog, select the target server and click **Next**.

6   In the Select server roles dialog, click **Next**.

7   In the Select features dialog, check the box next to **.Net Framework 3.5 Features** and click **Next**.

8   In the Confirm installation selections dialog, you are prompted to specify an alternate source path for .NET 3.5.

       Note If the target computer does not have access to Windows Update, specify the path to the \sources\sxs folder on the installation media and then click **OK**. After you specify the alternate source, or if the target computer does have access to Windows Update, close the warning.

       For more information about deploying .NET 3.5, see Microsoft .NET Framework 3.5 Deployment Considerations at http://msdn.microsoft.com/library/windows/hardware/hh975396.

9   Click **Install**.

10   When the installation completes, click **Close**.

1.3   Running the Automation Services Web Service Installer

▶   **To Install the Automation Services Web Service:**

1   Copy all files in the installer kit to the server where you will install Automation Services.

1   Run the installer **setup.exe**.

2   The *Welcome* dialog is displayed. Click **Next**.

3   The *License Agreement* dialog is displayed. Read the license agreement and select the appropriate radio button. Click **Next**.

4   The *Destination Folder* dialog is displayed. Specify where you want to install. Click **Next**.

5   The *IIS Web Application Settings* dialog is displayed. Specify a name for the Automation Services Application, and on which port Microsoft IIS listens. Click **Next.**

6   The *Configuration for TIBCO Spotfire Server* dialog is displayed. Specify the URL to your Spotfire Server and the username and password needed to log into it. If you are using Windows Integrated Login, leave username and password blank.

7   The *Configuration for mail* dialog is displayed. Specify a valid SMTP host that can be used to send automatic emails, and a From address to be used in these emails. Click **Next.**

Comment: These settings are necessary for the Send Mail task to function. If you need to change them after installation, they can be set in the configuration file `Spotfire.Dxp.Automation.Launcher.exe.config` located in the `<installation directory>\webroot\bin` folder.

8   The *Ready to Install the Program* dialog is displayed. Click **Install.**

Response: The installation starts.

9   The *Install Complete* dialog is displayed. If you wish, you may select to open the installer log file. Click **Finish**.

Comment: If something went wrong during installation, you may wish to review the installer log file for information. Typically, an installation will fail if the system requirements are not met. This will be reflected in the log file.

1.4   Deploy Extensions

Created extensions must be deployed to the TIBCO Spotfire Automation Services to be able to run.

▸   **To deploy extensions**

1   Copy all files needed to run the extension except **modules.xml** from the **TIBCO Spotfire Client modules** folder.

2   Paste the files into the **Automation Services bin** folder.

3   Open **modules.xml** from the **TIBCO Spotfire Client modules** folder.

4   Copy the *extensions* section.

5   Open **AddIns.xml** from the **webroot/bin** folder.

6   Paste the *extensions* section from **modules.xml** into the *AddInRegistry* section in **AddIn.xml**.

Comment: There are some differences in letter cases between **modules.xml** and **AddIns.xml**. Make sure to replace all occurrences of "*addIn fullTypeName*" with "*AddIn FullTypeName*".

7   Save changes in **AddIn.xml**.

1.5   Enabling Active Scripting

For the Automation Services export tasks to work properly with Text Areas, you need to enable Active Scripting on the computer running Automation Services.

▸   **To Enable Active Scripting**

---

1   Open the Local Group Policy Editor, for example by typing **gpedit.msc** in the Start search box and pressing enter.

2   Select **Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Internet Zone**.

3   Right-click on **Allow active scripting** and select **Properties**.

4   Select **Enabled**.

    Note: If this is done after setting up the IIS you need to restart the IIS for the changes to take effect.

1.6   Deploying the Automation Services Job Builder

In order for users to be able to use Automation Services Job Builder, you must deploy it to the Spotfire Server.

▸   **To deploy the job builder package to the server:**

1   Open the Administration Console located at `http://spotserver/spotfire/ administration` (where spotserver is the name of one of your spotfire servers) in a web browser.

2   Log in as a Spotfire Administrator.

3   Select the tab **Deployment**.

4   Select a **Deployment Area** that contains a valid Spotfire deployment from the View drop-down list.

    Comment: You must select a **Deployment Area** that contains **Spotfire Dxp.sdn.**

5   Click the **Add** button.

    Response: An **Add to Deployment** dialog appears.

6   Click the **Browse** button.

    Response: A **File Upload** dialog appears.

7   Browse to the package file **AutomationServices.spk**.

8   Click **OK** in the **Add to Deployment** dialog to upload and add the file to the distribution.

    Response: The list of packages is updated with the contents of the file.

9 Click the **Validate** button in the lower left corner to make sure the deployment is not damaged or corrupted in any way.

10 Click the **Save** button in the lower left corner to save and publish the deployment.

  <u>Response:</u> The **Save Deployment dialog** appears.

11 Enter a version number and a description for the deployment and click the **OK** button.

  See the online help of the Administration Console.

12 Restart TIBCO Spotfire and log in as usual.

  Response: The new client package will be downloaded to your TIBCO Spotfire client.

▶ **To verify the Job Builder License:**

1 Start TIBCO Spotfire.

2 Log in with an administrator account.

3 If prompted, download all updates from the server.

4 Once the update has been downloaded and installed, and TIBCO Spotfire opens, select **Tools > Administration Manager...** from the menu.

5 Select the **Groups and Licenses** tab.

6 Select a group from the **Available groups** list.

7 In the right-hand pane, click on the **Licenses** tab.

  Response: The "Licenses" interface is displayed.

8 Click on the + sign to expand the **"TIBCO Spotfire Extensions"** license to find the **"Automation Services Job Builder Tool"** license.

9 Make sure that both **Access to Extensions** and the **Automation Services Job Builder Tool** are marked with green checkmarks, as seen in the image below.

TIBCO Spotfire Extensions	✔	Everyone
Access to Extensions	✔	Everyone
Automation Services Job Builder Tool	✔	Everyone

10 If not, click the **Edit** button.

  Response: The "Licenses for group" dialog is displayed.

11 Click on the + sign to expand the **"TIBCO Spotfire Extensions"** license.

12 Select the check boxes for both **Access to Extensions** and the **Automation Services Job Builder Tool**.

13   Click **OK**.

14   Repeat steps 6 through 13 for every group of users permitted to use Automation Services.

15   When you have verified the licenses for all the groups, close the Administration Manager.

For more information on using the Groups and Licenses tab, please refer to TIBCO Spotfire – Deployment and Administration Manual. You can also read more about how to use the Administration Manager in its online help.

1.7 Making the User's Manual Available to Users

In order for the end users to get access to the **Automation Services User's Manual** when they select **Help > PDF Manuals** from the TIBCO Spotfire client, you must copy it to the Spotfire Server and rename it.

▸   **To copy the Automation Services Manual:**

1   From the folder where the PDF manuals are located, copy **TIB_AutomationServices_5.5_UserManual.pdf**

2   Paste it into the following folder on the TIBCO Spotfire Server computer: <installation directory>/tomcat/webapps/spotfire/support/manuals

3   Rename the file by changing the prefix to "TIB_SpotClient_". The PDF manual should have the name: **TIB_SpotClient_AutomationServices_5.5_UserManual.pdf**

Note: In a cluster of more than one Spotfire Server, the PDF manual must be deployed to all Spotfire Servers.

1.8 Client Job Sender

Automation Services includes the Client Job Sender. The tool is made up of the executable, `Spotfire.Dxp.Automation.ClientJobSender.exe`, and a configuration file `Spotfire.Dxp.Automation.ClientJobSender.exe.config`. This tool is used to automate jobs created by the job builder. It can be installed on any computer that has HTTP (or if configured, HTTPS) to the Automation Services web server. The executable file and the configuration file must reside in the same directory.

The Automation Services Client Job Sender returns different codes depending on if a job succeeded or failed, and if it failed the return code also states how it failed. The return values are stored in the ERRORLEVEL environment variable and the valid return codes are shown below.

Return codes:

- `0 = Success`
  Job succeeded.

- `1 = CommandLineParameterError`
  Incorrect command line parameter was supplied.

- `2 = ServerExecutionError`
  The job failed on the server.

- `3 = ClientExecutionError`
  The client failed to send the job to the server.

For information about how to use the Client Job Sender, see the **TIBCO Spotfire Automation Services - User's Manual**.

1.9 Antivirus and malware scanning software

You should disable on-access scanning of files in the Automation Services webroot folder and all sub-folders. When certain antivirus and malware scanning software packages perform an on-access scan, they modify the scanned files or the attributes of the scanned file and that results in IIS triggering a restart of the web application. When the web application restarts, clients can no longer receive the status of the jobs executing and will report them as failed or not loaded.

Also, for performance reasons, we recommend that you disable the on-access scanning for these types of software packages for folders that are used by Automation Services.

You should exclude the following folders from any on-access scans.

- **<Program Files>\TIBCO\Automation Services**
- **C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files**

1.10 Install Hotfixes

Before you continue, please check if any hotfixes have been released for this version of the server. If hotfixes are available, use the following procedure to install the hotfixes.

▶ **To install hotfixes**

1 Open the TIBCO Spotfire Product Hotfixes web site at http://support.spotfire.com/patches.asp. Download the hotfixes that are available and follow the installation instructions included with each hotfix package.

2 Always make sure you have installed the latest hotfixes before troubleshooting or reporting any problems.

When you have installed the hotfixes, the next step is to configure the installation. See "Configuring Automation Services" on page 12.

---

2 Configuring Automation Services

2.1 Overview

To improve security, and to access a Spotfire Server with certain authentication set up, there are some settings you may want or need to tweak.

2.2 Securing the Automation Services Web Service

Encrypting Traffic between Clients and Automation Services

By default, the Automation Services Web Service is set up to use the non-encrypted HTTP protocol for communication between clients (web browsers) and the Web Service. If you wish to encryption traffic between clients and Automation Services, you can enable an SSL binding on the IIS **Web Site** that the Automation Services Web Service is configured in. If you do this, however, you must ensure that the SSL certificate used to encrypt the traffic, or its certification authority, is trusted by the clients.

Important: If the SSL certificate is not trusted by the clients, the Automation Services Web Service will not function.

For more information about how to enable SSL in Internet Information Services and how to make clients trust SSL certificates, refer to the documentation for Internet Information Services.

Setting Up Authentication

By default, any user accessing the Automation Services Web Service with a web browser is able to run the web service. For security reasons, however, you may want to allow for only a limited number of users to access Automation Services.

This is done in two steps. First, you must disable Anonymous Authentication and enable Windows Authentication to the Automation Services Web Service using Internet Information Services Manager.

▶ **To Set Up Web Service Authentication**

1 Open the Internet Information Services Manager and find the Authentication settings

Select the **SpotfireAutomation** *Application* and double click the Authentication icon.

2 Disable **Anonymous Authentication** and enable **Windows Authentication**.

Next, you must configure Automation Services to grant access to certain users.

▸ **To grant access to certain users**

1   Open the Automation Services web configuration file

```
<installation dir>\webroot\Web.config.
```

2   Add the following text within the `<system.web>` element:

```
<identity impersonate="false"/>
      <authentication mode="Windows" />
      <authorization>
            <allow users="domain\user1" />
            <allow users="domain\user2" />
            <deny users="*"/>
      </authorization>
```

Replace **domain\user1** etc., with the domain and users applicable in your organization. You can add however many users you would like.

Example with one user in the domain **serenity** allowed:

```
<identity impersonate="false"/>
      <authentication mode="Windows" />
      <authorization>
            <allow users="serenity\malcolm" />
            <deny users="*"/>
      </authorization>
```

Encrypt Sections of the Spotfire.Dxp.Automation.Launcher.exe.config File

If you have added authentication information to the Spotfire.Dxp.Automation.Launcher.exe.config file, ether to the Spotfire Server or to an SMTP server, you may want to encrypt this section of the file. This can be done by executing the tool `Spotfire.Dxp.Automation.Launcher.exe` tool located in `<installation folder>\webroot\bin` with the `/encryptSection` argument followed by the name of the section.

Examples:

(This will encrypt the section containing the login information used to authenticate with the Spotfire Server)

```
Spotfire.Dxp.Automation.Launcher.exe /encryptSection:"Spotfire.Dxp.Automation/
authentication"
```

(This will encrypt the section containing login information for an SMTP server)

```
Spotfire.Dxp.Automation.Launcher.exe /encryptSection:"spotfire.dxp.automation.tasks/
smtp"
```

To decrypt an encrypted section, use the same tool with the /decryptSection argument followed by the name of the section.

Examples:

```
Spotfire.Dxp.Automation.Launcher.exe /decryptSection:"Spotfire.Dxp.Automation/
authentication"
```

```
Spotfire.Dxp.Automation.Launcher.exe /decryptSection:"spotfire.dxp.automation.tasks/
smtp"
```

2.3 Authenticating to Spotfire Server using Windows Integrated Login

If your Spotfire Server is set up to use Windows Integrated Login, you must configure the Automation Services Web Service to run as a user with login and library permissions to the Spotfire Server.

▶ **To set the user who will run the Automation Services Web Service:**

1 In the **Internet Information Services Manager**, locate and select Application Pools in the tree in the leftmost pane.

2 In the Application Pools pane, right-click the *TIBCO Spotfire Automation Services Application Pool*.

   Select **Advanced Settings** and edit the field **Identity**.

3 Change the identity to a domain user that has login and library permissions to the Spotfire Server.

   Now that the Automation Services Web Service is running as a non-standard user, you must also grant this user Full Control over files in the Automation Services installation folder.

▶ **To set correct file permissions to the Automation Services installation folder:**

1 In the Internet Information Services Manager, locate the Automation Services Web Application in the tree in the left most pane. Expand its contents by clicking the plus symbol next to it.

2 Right-click on the subfolder bin and select *Edit Permissions.*

3 On the Security tab, click Edit.

4 Add the user who was designated to run the Automation Services Application pool, if it is not present.

5 Make sure that the this user has the permissions Full control.

   If you entered a username and password when you installed Automation Services, you must also remove these from the configuration file.

▶ **To remove username and password from Automation Services configuration**

1 Open the file

```
<installation dir>\webroot\bin\Spotfire.Dxp.Automation.Launcher.exe.config
```

in a text editor. Find the section authentication serverUrl and remove the username and password specifications. When you are done, the line should look like this:

```
<authentication serverUrl="http://spotfireserver/" username="" password="">
```

2.4 Authenticating to Spotfire Server Using Client Certificates

If your Spotfire Server is set up to use Client Certificates, you must install the certificate used for authentication on the Automation Services server and configure Automation Services to use it when authenticating to the Spotfire Server. Refer to the **TIBCO Spotfire Server Installation and Configuration Manual** for more information about Client Certificates.

▶ **To install a client certificate**

1 Open Microsoft Management Console (MMC) and add the **Certificates** snap-in. Select to manage certificates for Local Computer.

2 Install the certificate in the **Personal** container.

3 Change the access rights to the certificate so that the *NETWORK SERVICE* account can access it:

In the Microsoft Management Console, right click the installed certificate and select **All Tasks\Manage Private Keys**. Grant the user *NETWORK SERVICE* access rights to the certificate.

▶ **To configure Automation Services to use a client certificate**

1 Open the configuration file

```
<installation dir>\webroot\bin\Spotfire.Dxp.Automation.Launcher.exe.config
```

in a text editor. Find the certificate section. If it is commented out, remove the comment markers around it.

2 Set useCertificates to "true", and storeName, storeLocation, and serial number to match the installed certificate.

Example:

```
<Spotfire.Dxp.Automation>
    <authentication serverUrl="https://spotfireserver.yourorganization.com">
        <!-- <proxy username="" password="" /> -->
```

```
      <certificates useCertificates="true" storeName="MyStore"
storeLocation="LocalMachine" serialNumber="00AABB11CCDD2233DD" />
    </authentication>
  </Spotfire.Dxp.Automation>
```

2.5   TIBCO ActiveSpaces Data Source

You can configure TIBCO ActiveSpaces 2.0.2 as a Spotfire Data Source but to complete the integration you must install ActiveSpaces on the Spotfire Automation Services server.

To configure this integration you can install either TIBCO ActiveSpaces Enterprise Edition or TIBCO ActiveSpaces Remote Client. For more information about installing ActiveSpaces, see https://docs.tibco.com/products/tibco-activespaces-2-0-2.

After the ActiveSpaces installation completes, you must manually copy several *.dll files from the ActiveSpaces installation folder to the Spotfire Automation Services virtual directory.

▶ **Copying ActiveSpaces files to Spotfire folder**

1   Navigate to the ActiveSpaces installation folder, open the **lib** folder, and select the following files:

- as-common.dll

- as-core.dll

- as-tibpgm.dll

- as-tibrv.dll

- TIBCO.ActiveSpaces.Common.dll

2   Copy these files to the Spotfire Automation Services virtual directory.

3   Create an environment variable, %AS_HOME%, and map it to the lib folder under the ActiveSpaces installation folder. For example:

```
Set %AS_HOME%=C:\TIBCO\AS\2.x\LIB\
```

4   Place the ActiveSpaces common DLL in the Global Assembly Cache (GAC) using the following command from the command-line utility:

```
gacutil.exe /i TIBCO.Activespaces.Common.dll
```

Note: If you do not have the GAC utility.exe already installed with Windows, you can download it from internet.

You can verify that the ActiveSpaces DLL is available on the Spotfire Automation Services server by interrogating the GAC using the following command with the Microsoft Global Assembly Cache Tool (gacutil.exe). For example:

```
gacutil.exe /L as-common.dll
```

2.6 Modifying Data Function-Based Data Sources Embedding Behavior

When using Automation Services jobs to save analyses containing data function-based data sources (for example, all on-demand data tables) that are configured to "Load automatically", these data sources are not loaded automatically by default, but have to be refreshed manually. Use the settings below to control that behavior.

▶ **To modify the force update behavior for embedded data**

1 Use a text or xml editor to open the configuration file:

```
<installation dir>\webroot\bin\Spotfire.Dxp.Automation.Launcher.exe.config
```

2 Locate the following line and toggle the force update behavior between true and false:

```
<saveAnalysis forceUpdateBehaviorManualWhenEmbeddingData="false"/>
```

3 Save the changes in **Spotfire.Dxp.Automation.Launcher.exe.config** and restart the Automation Services application pool for the changes to take effect.

▶ **To modify the force update setting on a specific TIBCO Spotfire Professional installation:**

If you want to test Jobs by executing them locally you can modify this setting on your own TIBCO Spotfire Professional computer using the steps below.

1 On the computer where TIBCO Spotfire Professional is installed, locate **Spotfire.Dxp.Main.dll.config** in the Spotfire Forms Modules folder (example path: C:\Program Files (x86)\TIBCO\Spotfire\4.0.0\Modules\Spotfire DXP Forms_9.14.5830.4061).

2 Add the following to the `<configuration><configSections>`:

```
<sectionGroup name="spotfire.dxp.automation.tasks">
 <section name="saveAnalysis" type="Spotfire.Dxp.Automation.Tasks.SaveAnalysisSettings,
Spotfire.Dxp.Automation.Tasks, Version=3.0.2736.26364, Culture=neutral,
PublicKeyToken=789861576bd64dc5" requirePermission="false" />
</sectionGroup>
```

3 Then, anywhere inside the topmost `<configuration>` tag, add:

```
<spotfire.dxp.automation.tasks>
<saveAnalysis forceUpdateBehaviorManualWhenEmbeddingData="false"/>
</spotfire.dxp.automation.tasks>
```

4 Restart TIBCO Spotfire Professional to use the new settings.

3 Upgrading to Automation Services 5.5

This section describes what you need to do in order to upgrade from Automation Services 3.1, 3.2, 3.3, 4.0, 4.5, or 5.0 to Automation Services 5.5. If you are running Automation Services 2.2, you will no longer be able to connect to an Analytics Server 10.1 or older after the upgrade.

▶ **To Upgrade the Web Service:**

1 Navigate to the folder <installation directory>\webroot\bin.

2 Make a copy of the **Spotfire.Dxp.Automation.Launcher.exe.config** file.

   Note: By making a copy of this file you can use it as a reference in step 7 when configuring the new version of the config file.

   Note: If you have any custom extensions deployed, make a copy of these and the **AddIns.xml** file as well.

3 Uninstall the old Automation Services web service.

4 Install the Automation Services 5.5 web service by running **setup.exe** on the computer that hosts the web server and follow the instructions in the installation wizard.

5 Make sure that you have the latest hotfix by going to http://support.spotfire.com/patches.asp. Each hotfix package includes installation instructions. For more information, see "Install Hotfixes" on page 11.

6 Follow the instructions in the section "Securing the Automation Services Web Service" on page 12.

   Tip: Open the old **Spotfire.Dxp.Automation.Launcher.exe.config** next to the new version. This way you can copy the necessary settings from the old file and paste them into the new one.

▶ **To Upgrade the Job Builder:**

The old job builder package will automatically be replaced by the new one when upgrading Automation Services.

▶ **To Upgrade the Command-Line Client:**

The Automation Services 5.5 command-line client should be used instead of the old version.

4   Troubleshooting

If Automation Services is not set up correctly, the users will not be able to run jobs on the server. An error message will appear asking the user to contact the Spotfire Administrator.

To find out what went wrong, you need to review the `Spotfire.Dxp.Automation.log` file, located in the folder <installation directory>\LogFiles.

The file `Spotfire.Dxp.Automation.Launcher.exe.config` located in the folder `<installation directory>\webroot\bin` directory holds all configuration. If you need to change the URL to the Spotfire Server, for instance, or the hostname of your SMTP server, you can do this by opening the file in a text editor.

Configuration File Extract

```
<!--
    If username and password are empty or doesn't exist, then we login using
    the current Windows account (using Windows Authentication).

    serverUrl (Required): The url to the Spotfire Analytics Server "http[s]://
<server>[:port]/"
    username: The spotfire user to authenticate with.
    password: The password to authenticate with.

    proxy (you need to set the system.net/defaultProxy/proxy: proxyaddress to use it if
you run under a system account (from web sites etc.)):
        username: Proxy username for communication between web server and Spotfire
Analytics Server.
        password: Proxy password for communication between web server and Spotfire
Analytics Server.

    certificates (Certificates to use when authenticating with Analytics Server):
        useCertificates (false): Should we use certificates
        storeName (TrustedPeople): The store name to get the certificates from.

[AddressBook|AuthRoot|CertificateAuthority|Disallowed|My|Root|TrustedPeople|TrustedPubl
isher]
        storeLocation (LocalMachine): [CurrentUser|LocalMachine] The location to take
the certificates from.
        serialNumber: The serial number of the certificate to use.
    -->
<authentication serverUrl="http://spotserver/" username="" password="">
```

5 Removing Automation Services

To uninstall Automation Services, use the Program and Features feature found in the Control Panel of your Server. Locate TIBCO Spotfire Automation Services and launch it. Automation Services will be removed from the server and the added Internet Information Services configuration will be removed.

Note: Some files may remain in the installation folder after uninstall. You can remove them by simply deleting the installation folder.