TIBCO Spotfire® Web Player 6.0

Installation and Configuration Manual

TIBCO provides the two-second advantage™

Revision date: 12 November 2013

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_TIBCOSPOTFIREWEBPLAYER.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 Pre-Installation Planning

1.1 Introduction

The TIBCO Spotfire™ Web Player must be installed on a Microsoft Internet Information Services (IIS) server. The Spotfire Web Player renders the Spotfire visualizations and graphics that are delivered to users.

When a user launches a Web browser on a local computer and types the URL to an analysis on the Spotfire Web Player, the Spotfire Web Player opens a connection to the TIBCO™ Spotfire Server. In turn, the Spotfire Server manages the data and delivers the required information to the Spotfire Web Player, the Spotfire Web player then renders the view to be presented in the web browser on the local computer.

Note For new or changed features, functionality changes, and information about issues, see the "TIBCO Spotfire Web Player - Release Notes" at http://docs.tibco.com.

1.2 Architectural Overview

In the most basic Spotfire installation, the Spotfire Web Player and Spotfire clients communicate with a single Spotfire Server, as illustrated below.

In a Spotfire system with more than one Spotfire Server, the Spotfire Web Player communicates with a cluster of Spotfire Servers behind a load balancer.
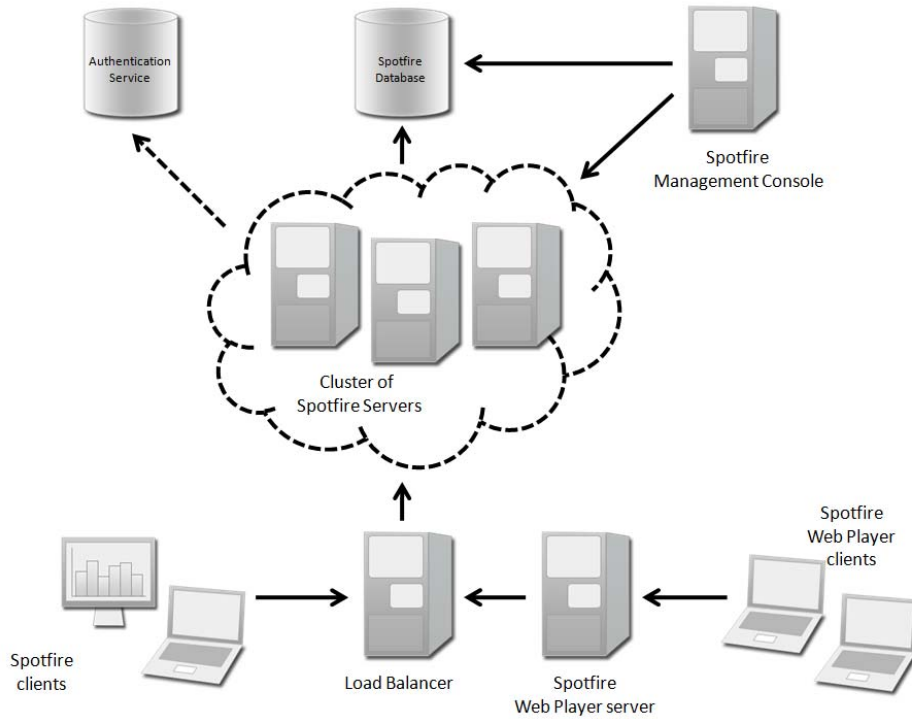
Regardless of whether one or several Spotfire Servers exist in the Spotfire installation, the Spotfire Web Player is installed and configured in the same way.

You can also configure a group of Spotfire Web Player servers as a cluster.
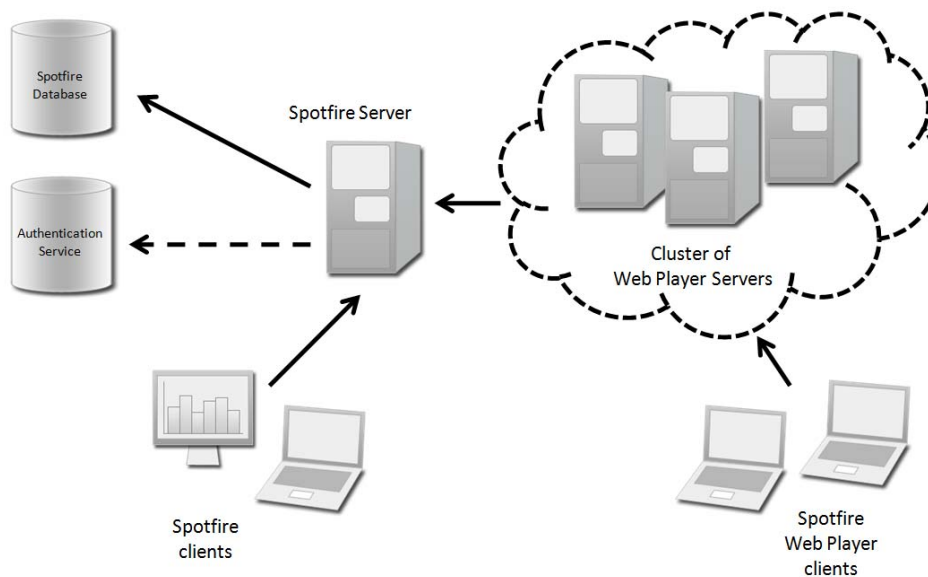
You can configure a Spotfire installation as a combination of Spotfire Server clusters and Spotfire Web Player clusters.

Spotfire Server and Spotfire Web Player on a Single Computer

We recommend that you install Spotfire Web Player on one or more separate computers or dedicated IIS servers. However, it is possible to install Spotfire Web Player on the same computer where you installed Spotfire Server. Since this has an adverse impact on performance for both products, and leads to communication complications because, by default, both Spotfire Server and the Spotfire Web Player are configured to listed on port 80.

Kerberos authentication is not supported in the scenario where Spotfire Server and Spotfire Web player are installed on the same computer.

1.3   Software Overview

Technology

Spotfire Web Player is implemented as an Internet Information Services ASP.NET AJAX web application. For specific system requirements, see

```
http://support.spotfire.com/sr.asp
```

Installation and File Locations

The Spotfire Web Player installation wizard installs and configures Spotfire Web Player on a Windows server. The wizard copies all of the files contained in the distribution to a directory that you specify during the installation process, the default directory is:

```
C:\Program Files\TIBCO\Spotfire Web Player\6.0
```

Note If you are upgrading the Spotfire Web Player with the Upgrade tool, Spotfire Web Player will use the existing directory, such as 5.5.

Windows Service

The Spotfire Web Player installation creates the **TIBCO Spotfire Web Player Keep Alive Service** service. This service is required for the Scheduled Updates feature to operate correctly. To use Scheduled Updates, you must set the Startup Type for the service to **Automatic**.

Upgrade Tool

If you need to install new modules, such as language packs or third party add-ons, you can use the Upgrade tool. The Upgrade tool (`Spotfire.Dxp.Web.UpgradeTool.exe`) is contained in the `<installation directory>\webroot\bin\Tools` directory. For more information on using the Upgrade tool, see the section "Deploying Extensions and Upgrades" on page 54.

Log Files

The Spotfire Web Player log entries are written to log files in the `<installation directory>\webroot\bin\Logfiles` directory. For more information about the Spotfire Web Player Log, see the section "Web Server Log" on page 100.

1.4 Authentication Alternatives

The Spotfire Web Player authentication consists of three components: IIS, ASP.NET and Spotfire Server. Each component can be configured in various ways and the combination of configurations define the overall authentication behavior. The combination of how these three components are configured will define the security of the system and the experience for the users.

Before you begin the Spotfire Web Player installation, it is important that you understand the authentication alternatives discussed in this chapter. You can use this information to help you decide which approach to use to meet your security and usability requirements.
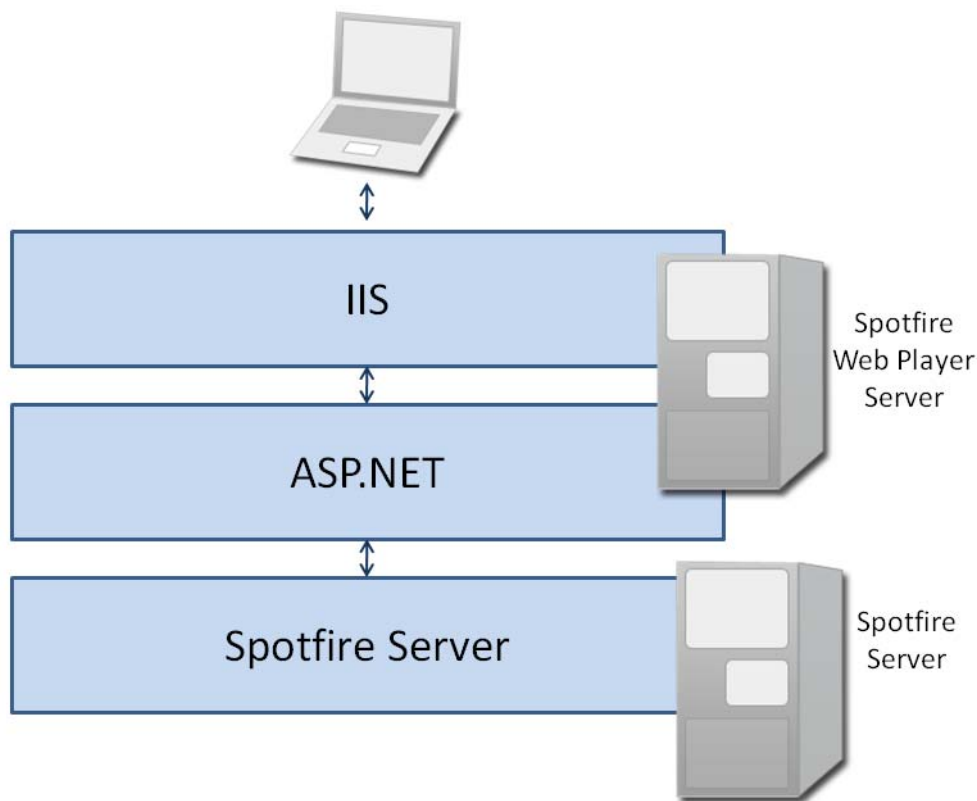
You configure the security on each of these three components in a specific way to determine how the overall Spotfire Web Player authentication works. The most common alternatives are:

- Username & Password – users who connect to the Spotfire Web Player are prompted to enter a username and password. Their credentials are verified against the Spotfire Server, which can be configured in various ways (for example, LDAP, Database, or Windows NT Domain). This is the default

authentication alternative for Spotfire Web Player. If you select this alternative, no post-installation authentication configuration is required.

Component	Setting
IIS	Anonymous and Forms
ASP.NET	Forms Authentication
Spotfire Server	Basic Authentication

- **Anonymous Access** – users who connect to the Spotfire Web Player are logged in automatically using preconfigured credentials that you specify when you configure the ASP.NET component. These credentials are used for all users to access the Spotfire Server.

Component	Setting
IIS	Anonymous
ASP.NET	None (Preset User/Password)
Spotfire Server	Basic Authentication

- **Single Sign-On** – users who connect to the Spotfire Web Player are automatically authenticated using their Windows credentials. As long as the users connect to the Spotfire Web Player from the appropriate Windows Domain and the Spotfire Server is already be configured with the same authentication type, users will not have to supply their credentials again.

  Note In this alternative, when you configure the Spotfire Web Player authentication method to use one of the impersonation authentication methods, you can configure the Spotfire Server to use any authentication method. If you are not using impersonation, the only single sign-on method that can work for both the Spotfire Server and the Spotfire Web Player is delegated Kerberos.

Component	Setting
IIS	Integrated Windows Authentication
ASP.NET	Windows
Spotfire Server	NTLM, Kerberos, or Basic

- **Client Certificate** – users who connect to the Spotfire Web Player are authenticated using client certificates.
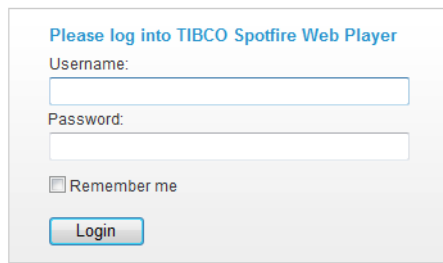
Component	Setting
IIS	Anonymous
ASP.NET	None
Spotfire Server	Client Certificate

These authentication alternatives are described in more detail below, and the procedures required to configure the alternatives are described in the chapter "Install Spotfire Web Player" on page 24.

1.4.1 Username and Password

This is the default authentication configured during the Spotfire Web Player installation. If you select this alternative, no post-installation authentication configuration is required.

In this configuration, when users connect to the Spotfire Web Player, the ASP.NET component displays a login form.

If the user selects **Remember me**, their credentials are stored in a cookie. This cookie is used for authentication during subsequent logins and the login form is not displayed. If a user wants to remove the cached login cookie, they should click logout on the Spotfire Web Player or Library web page.

The credentials that the user types into the login form are validated by the Spotfire Server.

Note Because the username and password are sent as clear text, we recommend that you use this authentication alternative (also known as "Forms Authentication") together with HTTPS (SSL) connections, see "Configure SSL" on page 37.

1.4.2 Anonymous (Preconfigured) Access

With this option, users who access the Spotfire Web Player services are automatically logged in as the user that you specify in the `web.config` file. This means all users who log in to Spotfire Server will appear to be the same Spotfire user. In this scenario, you must create this user, grant the licenses for the library, and configure the user for impersonation on the Spotfire Server.

1.4.3 Single Sign-On

You should use this authentication method to configure a "single sign-on" experience for the Spotfire Web Player users. In this scenario, after a user supplies their Windows credentials to log on to the network the Spotfire Web Player automatically uses the Windows credentials of the user to access the Spotfire Web Player.

There are four ways to achieve a "single sign-on" experience and they are more complex than the **Anonymous** or **Username and Password** methods. this is because each approach requires additional configuration on the Windows Domain Controller or the Spotfire Server, or both. If you choose these alternatives, you should be knowledgeable about Domain Controllers.
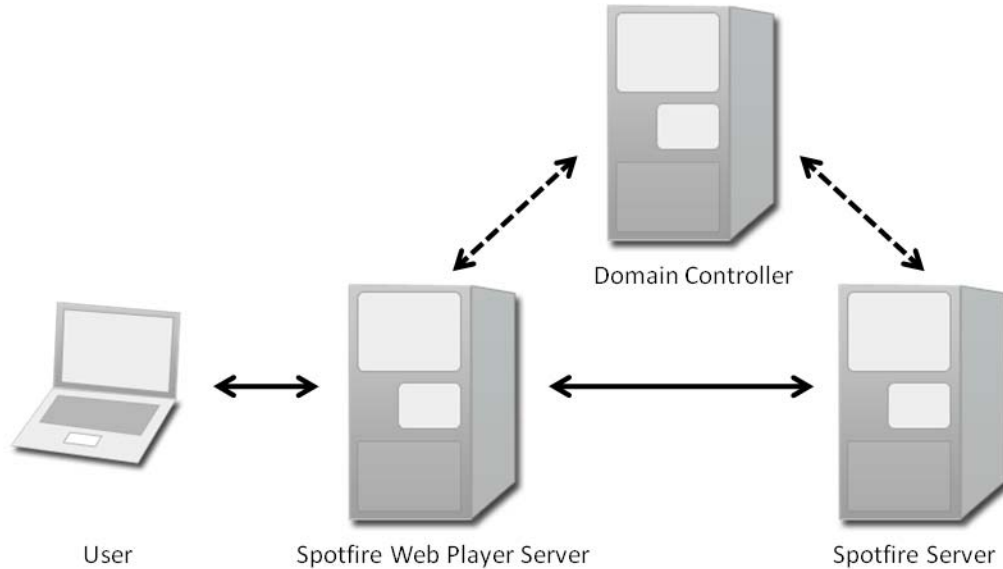
The alternative approaches are to enable Single Sign-On using:

- Impersonation with NTLM Login

- Impersonation with Basic Login

- Impersonation with Kerberos Login

- Delegation with Kerberos Login

Impersonation with NTLM Login

This alternative, to use NTLM with Impersonation, is the recommended single sign-on method for Spotfire Server and is the preferred option for Spotfire Web Player.

In this approach, when a user connects to the Spotfire Web Player from a browser, the Windows credentials are used to automatically log in the user. The Spotfire Web Player then contacts the Spotfire Server, which prompts the Spotfire Web Player to authenticate the user. The Spotfire Web Player automatically logs into the Spotfire Server using a predefined *impersonation account*.

You must add the *impersonation account* to the Spotfire Server **Impersonator** group. Accounts in this group have the **run services as another named user** user right. This user right means that, by stating a valid username, the system can run services as that user without requiring the password for that account.

To reduce the risk of security issues, you can specify the Spotfire Web Player computer name or IP address as the only logon location that the impersonation account can use to access the Spotfire Server.

The requirements for this alternative are:

- An impersonation account for the Spotfire Web Player must be created on the Domain Controller.

- The Spotfire Server must be configured to use NTLM Login System.

- You must enable ASP.NET Impersonation on IIS.

This alternative does not require that you to configure Delegation on the Domain Controller. Instead you configure a trusted account on the Spotfire Web Player that the Spotfire Server allows to run requests as another user. This is referred to as Impersonation.

Impersonation with Basic Login

If you cannot use NTLM, you can use this alternative.

In this approach, when a user connects to the Spotfire Web Player from a browser, the Windows credentials are used to automatically log in the user. The Spotfire Web Player then contacts the Spotfire Server, which prompts the Spotfire Web Player to authenticate the user. The Spotfire Web Player automatically logs into the Spotfire Server using a predefined *impersonation account*.

You must add the *impersonation account* to the Spotfire Server **Impersonator** group. Accounts in this group have the **run services as another named user** user right. This user right means that, by stating a valid username, the system can run services as that user without requiring the password for that account.

Since the Spotfire Server is using a Basic login (**LDAP** or **Database**) system, the list of valid usernames is stored on either an LDAP server or in the Spotfire Server database itself. This is the main difference between this alternative and **Impersonation with NTLM Login System**.

To reduce the risk of security issues, you can specify the Spotfire Web Player computer name or IP address as the only logon location that the impersonation account can use to access the Spotfire Server.

The requirements for this alternative are:

- The Spotfire Server must use either **LDAP** or **Database Login System**.

- You must create an **impersonation account** for the Spotfire Web Player on the LDAP Server or the Spotfire Server (depending on whether the Spotfire Server has been configured to use LDAP or Database login system).

This alternative does not require that you to configure Delegation on the Domain Controller. Instead you configure a trusted account on the Spotfire Web Player that the Spotfire Server allows to run requests as another user. This is referred to as Impersonation.

Impersonation with Kerberos Login

With the Kerberos Login System you can configure single sign-on to use Delegation or Impersonation. If you can not configure Delegation on the Domain Controller you can use this alternative.

In this approach, when a user connects to the Spotfire Web Player from a browser, the Windows credentials are used to automatically log in the user. The Spotfire Web Player then contacts the Spotfire Server, which prompts the Spotfire Web Player to authenticate the user. The Spotfire Web Player automatically logs into the Spotfire Server using a predefined *impersonation account*.

You must add the *impersonation account* to the Spotfire Server **Impersonator** group. Accounts in this group have the **run services as another named user** user right. This user right means that, by stating a valid username, the system can run services as that user without requiring the password for that account.

To reduce the risk of security issues, you can specify the Spotfire Web Player computer name or IP address as the only logon location that the impersonation account can use to access the Spotfire Server.

The requirements for this alternative are:

- You must create an **impersonation account** for the Spotfire Web Player on the Domain Controller.

- The Spotfire Server must use **Kerberos Login System**.

- A member of the **Account Operators** or **Administrators** domain groups must use the **Windows Support Tools**, typically installed on one of the domain controllers, to configure:

  - The **Service Principal Names** (SPNs) for the Spotfire Server.

  - A **keytab** file for the Spotfire Server.

- You must enable ASP.NET Impersonation on IIS.

This alternative does not require that you to configure Delegation on the Domain Controller. Instead you configure a trusted account on the Spotfire Web Player that the Spotfire Server allows to run requests as another user. This is referred to as Impersonation.

More information about **keytab** files and Kerberos on the Spotfire Server refer to the "**TIBCO Spotfire Server — Installation and Configuration Manual**".

If it is not possible to complete these requirements, you can use either *Impersonation with NTLM Login* or *Impersonation with Basic Login* to achieve single sign-on.

Delegation with Kerberos Login

In this approach, when a user connects to the Spotfire Web Player from a browser, the Windows credentials are used to automatically log in the user. The Spotfire Web Player then contacts the Spotfire Server, which prompts the Spotfire Web Player to authenticate the user. The Spotfire Web Player automatically logs into the Spotfire Server as the end user.

Delegation makes it possible for the Spotfire Web Player to log into the Spotfire Server as the end user, and not the account that is actually running the Spotfire Web Player.

The requirements for this alternative are:

- On the Domain Controller, you must configure **Delegation** for the computer account or dedicated user account that is used to run the application pool in IIS on the Spotfire Web Player. An administrator on the Domain Controller must complete this requirement.

- The Spotfire Server must use **Kerberos Login System**.

- A member of the **Account Operators** or **Administrators** domain groups must use the **Windows Support Tools**, typically installed on one of the domain controllers, to configure:

  - The **Service Principal Names** (SPNs) for the Spotfire Server.

  - A **keytab** file for the Spotfire Server.

Note You could create a potential security issue when you enable Unconstrained Delegation for the Spotfire Web Player account, either computer account or dedicated user account, because the change has an impact on all of the services running on the Spotfire Web Player computer or under that dedicated user account. An alternative, if it is supported by the Domain Controller, is to use the more secure Constrained Delegation.

If it is not possible to complete the requirements in this section, you should use one of the Impersonation alternatives instead. More information about **keytab** files and Kerberos on the Spotfire Server refer to the "**TIBCO Spotfire Server — Installation and Configuration Manual**".

1.4.4 Client Certificate

With this option, users who access to the Spotfire Web Player are authenticated using client certificates. The Spotfire Web Player then contacts the Spotfire Server, which prompts the Spotfire Web Player to authenticate the user. The Spotfire Web Player automatically logs into the Spotfire Server using a predefined **impersonation client certificate** and submits the user client certificate to the Spotfire Server to authenticate the user.

Therefore, this authentication alternative requires that the Spotfire Server is set to use client certificates, and that Impersonation is enabled on the Spotfire Server.

Note This manual does not cover how to install and configure the client certificates, or how to configure SSL; only how to configure the Spotfire Web Player to be able to use already installed client certificates for authentication.

1.5 Conceptual Outline of Installation Process

Performing the tasks in **"Prerequisite Installation" on page 17** and **"Install Spotfire Web Player" on page 24** will guide you through a full installation of Spotfire Web Player 6.0 with detailed explanations.

The conceptual overview or process of the installation and configuration procedures:

1   Read the **"Pre-Installation Checklist" on page 15** and record the required information.

2   Spotfire Web Player requires either **Microsoft Windows 2008 Server** or **Microsoft Windows 2012 Server**.

3   You must install Microsoft Internet Information Services (IIS) and configure it with ASP.NET.

4   Copy the Spotfire Web Player installation files to the computer.

5   Run the Spotfire Web Player installer.

6   If required, configure the ASP.NET authentication in the `web.config` file.

   <u>Comment:</u> It is important that you decide which authentication method to use before you install. For more information on the authentication alternatives, see "Authentication Alternatives" on page 8.

7   If required, configure IIS authentication.

8   Review the `web.config` file to verify that no unwanted changes have been made during installation.

9   Complete the configuration of the authentication method you selected for your environment.

10   Configure the licenses and library rights for the Spotfire Web Player users.

11   Configure the URL preference.

1.6   Pre-Installation Checklist

Before you begin the Spotfire Web Player 6.0 installation, there are several things you must determine. This section contains checklists that you must complete.

Compatibility

There are some things that you must take into consideration regarding compatibility and different versions of the software. In order to install Spotfire Web Player 6.0 you must have Spotfire Server 6.0. Also, Spotfire Web Player 6.0 does not support side-by-side installations of different versions of the Spotfire Web Player on the same computer. If you have an earlier version of Spotfire Web Player on the computer, the earlier version will not run.

Authentication

There are seven different authentication alternatives for Spotfire Web Player. Each of these is described in the chapter "Authentication Alternatives" on page 8. You must decide which alternative to use before installing the Spotfire Web Player.

Which of the authentication alternatives will you use for Spotfire Web Player?	

Ports

Before installing Spotfire Web Player, verify that IIS is running and is configured to use the port that the Spotfire Web Player will listen on. The default port is port 80.

What port will you use for Spotfire Web Player?	

Installer Options

When you run the Spotfire Web Player installation wizard, you must answer the following questions.

Name of the Virtual Directory that will be part of the URL of the Spotfire Web Player? We recommend *SpotfireWeb*.	
The URL to the Spotfire Server for communication from the Spotfire Web Player?	
E-mail address of the local Spotfire Administrator?	

SSL

We recommend that you use SSL (https) for the authentication alternatives that send passwords in plain text.

Will you use SSL?	

2 Prerequisite Installation

2.1 Operating System

At this point, for the computer where you intend to install Spotfire Web Player, you should already have installed and configured either **Microsoft Windows 2008 Server** or **Microsoft Windows 2012 Server**. For system requirements, see http://support.spotfire.com/sr.asp

Note If you have an earlier version of Spotfire Web Player installed on the target computer, that version will not work after you install Spotfire Web Player 6.0.

2.1.1 Internet Access

Some of the Spotfire Web Player features require Internet access. Features such as collaboration and for any images in a table that are linked from a Web site on the Internet. Other third party features may also be affected by lack of Internet access.

2.1.2 Active Scripting

If you need to export text areas from the Spotfire Web Player you must enable Active Scripting on the Spotfire Web Player computer.

▸ **Enabling Active Scripting**

1 Start the Local Group Policy Editor (`gpedit.msc`).

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

3 Right-click **Allow active scripting** and select **Properties**. If you are on Windows Server 2008 R2 or Windows Server 2012, select **Edit**.

4 On the "Allow active scripting" page, select **Enabled**.

5 In the **Options** area, make sure that the **Allow active scripting** list is set to **Enabled**, and then click **OK**.

Note If you complete this procedure after you install and configure IIS, you must restart IIS for the changes to take effect.

2.1.3 Antivirus and Malware Scanning Software

You should disable on-access scanning of files in the Spotfire Web Player `webroot` directory and all sub-directories. 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, this results in IIS triggering a restart of the web application. When the web application restarts, users are logged out and the analyses is closed.

For performance reasons, we also recommend that you disable the on-access scanning for these types of software packages for directories that are used by the Spotfire Web Player.

You should exclude the following directories from on-access scans.

```
<Program Files>\TIBCO\Spotfire Web Player\
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET
Files
```

2.2   Internet Information Server and ASP.NET

Install Microsoft Internet Information Services (IIS) on this computer and then set up ASP.NET on IIS.

2.2.1   Install on Microsoft Windows 2008 Server

This section explains how to install IIS and ASP.NET on your Microsoft Windows 2008 Server and how to make sure that IIS has all the necessary components to run Spotfire Web Player. If you have already installed IIS with an earlier version of ASP.NET, you must install Microsoft .NET Framework 4.0.

▶   **Installing on Microsoft Windows 2008 Server**

1   Install **Microsoft .NET Framework 4.0** on the server, if it is not already present. You can download Microsoft .NET Framework 4.0 from
http://download.microsoft.com
Note Make sure that you upgrade to the latest Microsoft .NET Framework 4.0 version.

2   On your Microsoft Windows 2008 Server, navigate to the Administrative Tools options, and then select **Server Manager**.

3   In the navigation pane, select **Roles**, and then click **Add Roles**.
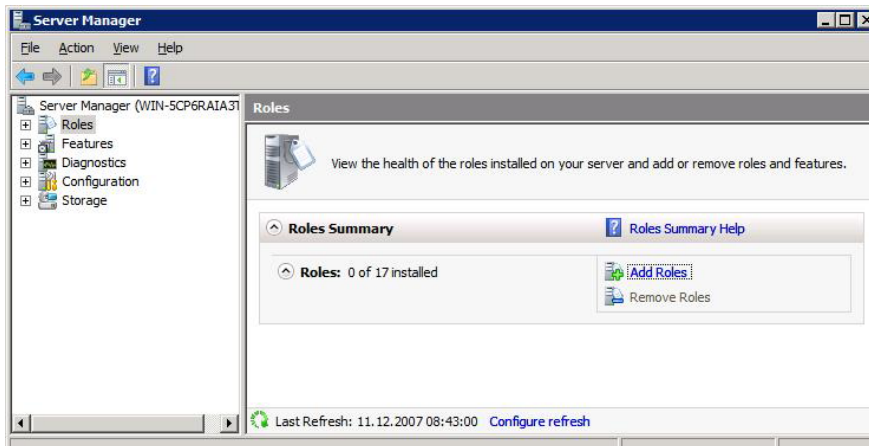
4   If the "Before you begin" page appears, click **Next**.

5   In the "Select Server Roles" page, select **Web Server (IIS)**, and then click **Next**.
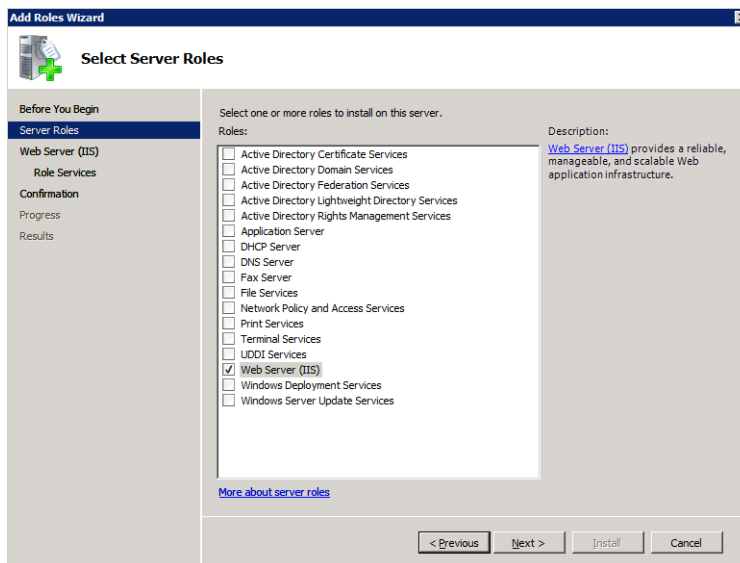
Comment: If a prompt for **Add features required for Web Server (IIS)?** appears, click **Add Required Features**, and then click **Next**.

6   In the "Web Server (IIS)" page, click **Next**.
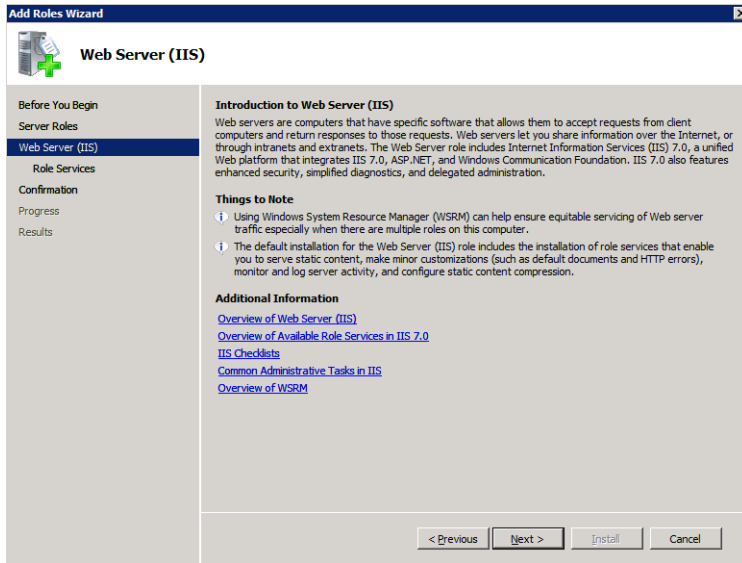
7   In the "Select Role Services" page, you must select, at a minimum, the settings listed for each group in the following table. You may need to select more options for your environment.

Comment: In the Security group, make sure to select the authentication types required in your environment.

Group	Setting
Common HTTP Features	Static Content Default Document Directory Browsing HTTP Errors
Application Development	ASP.NET .NET Extensibility ISAPI Extensions ISAPI Filters
Health and Diagnostics	HTTP Logging Request Monitor
Security	Basic Authentication Windows Authentication Request Filtering
Performance	Static Content Compression

Group	Setting
Management Tools	IIS Management Console IIS Management Scripts and Tools
IIS 6 Management Compatibility	IIS 6 Metabase Compatibility IIS 6 WMI Compatibility IIS 6 Scripting Tools

Comment: If a prompt for **Add role services and features required for ASP.NET?** appears, select **Add Required Role Services**.

8   When you have selected the appropriate settings, click **Next** and then in the "Confirmation" page, click **Install**.

9   When the installation completes, the "Installation Results" page appears, click **Close**.
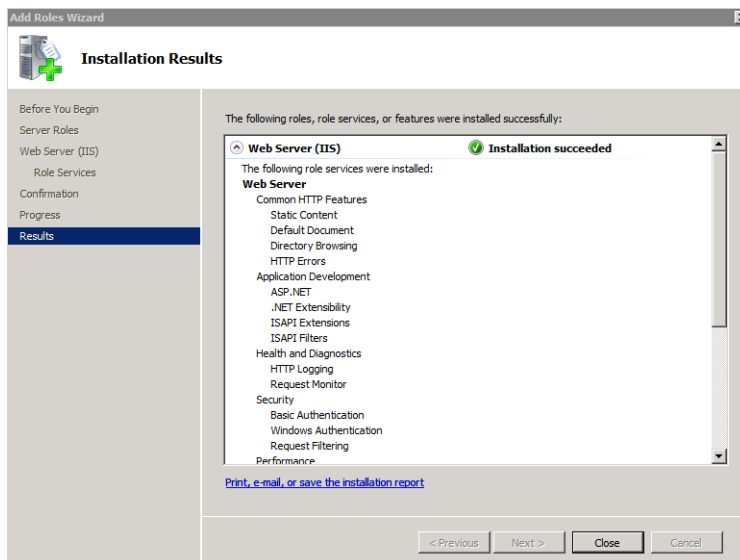
10   Start the IIS Manager.

11 In the navigation pane, select the server (top) node and then select **ISAPI and CGI Restrictions**.
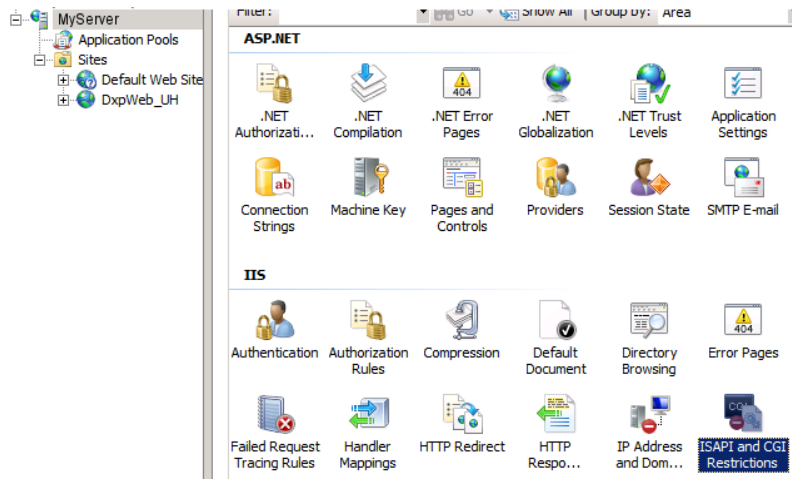
12 Make sure that **ASP.NET 4.0.30319** is present in the list and set it to **Allowed**.

13 If ASP.NET 4.0.30319 is not present, you must open the command console and run the following command. When the command completes, repeat Step 11 and Step 12.

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

2.2.2 Install on Microsoft Windows 2012 Server

This section explains how to install IIS and ASP.NET on your Microsoft Windows 2012 Server and how to make sure that IIS has all the necessary components to run Spotfire Web Player.

▶ **Installing on Microsoft Windows 2012 Server**

1 Make sure to upgrade to the latest version of Microsoft .NET Framework.

2 On your Microsoft Windows 2012 Server, navigate to the Administrative Tools options, and then select **Server Manager**.

3 In the navigation pane, select **Dashboard**, and then click **Add Roles and Features**.

4 If the "Before you begin" page appears, click **Next**.

5 Select the applicable option in the "Installation Type" page, and then click **Next**.

6 Select the server in the "Server Selection" page and click **Next**.

7 On the "Select Server Roles" page, select **Web Server (IIS)**, and then click **Next**.

   Comment: If a prompt for **Add features required for Web Server (IIS)?** appears, click **Add Required Features**, and then click **Next**.

8 On the "Web Server (IIS)" page, click **Next**.

9   On the "Select Role Services" page, you must select, at a minimum, the settings listed for each group in the following table. You may need to select more options for your environment. After you select the correct options, click **Next**.

Comment: In the Security group, you must make sure to select the required authentication types.

Group	Setting
Common HTTP Features	Static Content Default Document Directory Browsing HTTP Errors
Application Development	ASP.NET 4.5 .NET Extensibility 4.5 ISAPI Extensions ISAPI Filters
Health and Diagnostics	HTTP Logging Request Monitor
Security	Basic Authentication Windows Authentication Request Filtering
Performance	Static Content Compression
Management Tools	IIS Management Console IIS Management Scripts and Tools
IIS 6 Management Compatibility	IIS 6 Metabase Compatibility IIS 6 WMI Compatibility IIS 6 Scripting Tools

Comment: If a prompt for **Add role services and features required for ASP.NET?** appears, select **Add Required Role Services**.

10   On the "Features" page, select .NET Framework 4.5, and then click **Next**.

11   When you have selected the appropriate settings, click **Next** and then on the "Confirmation" page, click **Install**.

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

13   Start the IIS Manager.

14   In the navigation pane, select the server (top) node and then select **ISAPI and CGI Restrictions**.

15   Make sure that **ASP.NET 4.0.30319** is present in the list and set it to **Allowed**.

3 Install Spotfire Web Player

This section explains how to install and configure Spotfire Web Player.

3.1 Copy the Installation Files

The Spotfire Web Player installation media contains a **TIBCO Spotfire Web Player Installer** directory. Copy this source directory to a local disk on the target computer.

Note If you have an earlier version of Spotfire Web Player installed on the target computer, that version will be removed when you install Spotfire Web Player 6.0. Before you start the installation process, we recommend that you create a back up the `web.config` file. You can use this file for reference as you configure the new installation.

3.2 Run the Installer

In order to install Spotfire Web Player, you must log in to the target computer with credentials that have Administrator user rights.

Before you install Spotfire Web Player, make sure that the target computer is running IIS.

▶ **Running the Installer**

1 From the directory you copied to the local disk, start the installation wizard by double-clicking `setup.exe`.

   Comment: Installation from a network drive is not supported

2 On the "Welcome" page, Click **Next**.

3 On the "TIBCO Spotfire License Agreement" read the License Agreement. To proceed you must agree to the License Agreement, and then click **Next**.

4 Specify the directory where you want to install Spotfire Web Player, and then click **Next**.

   Comment: If the server has more than one disk, we recommend that you install on the fastest disk. This will decrease the Spotfire Web Player load time and also optimize any swapping.

5 Type the name of the Virtual Directory to create in IIS. The name you type here will be part of the Spotfire Web Player URL. We recommend that you accept the default, `SpotfireWeb`.

   Spotfire Web Player URL pattern: `http[s]://<servername>/SpotfireWeb/`

6 Type a port number for the Spotfire Web Player, and then click **Next**.

Comment: The port number that you type in this step must match the IIS port number.

7 Specify the TIBCO Spotfire Server URL, and then click **Next**.

Note You can modify the URL later by editing the `web.config` file.

8 Type the e-mail address to the Spotfire administrator, and then click **Next**.

Note You can modify the e-mail address later by editing the `web.config` file.

9 Click **Install** to start the installation and when the wizard completes, click **Finish**.

3.3 Configure ASP.NET Authentication

To configure the authentication used by the ASP.NET layer, you must edit the Spotfire Web Player configuration file. The exception is if you are using Username and Password authentication, in this case you do not need to edit the configuration file.

The Spotfire Web Player configuration file, `web.config`, is in the `webroot` directory, for example:

```
C:\Program Files\Tibco\Spotfire Web Player\6.0\webroot\Web.config
```

Note We recommend that you use an XML editor when you modify XML files. An XML editor has features to provide a clear view of the XML code and some text editors corrupt configuration files.

You can modify the configuration file so that the ASP.NET layer uses one of the following authentication alternatives. Each option is described in "Authentication Alternatives" on page 8, and you should decide on which authentication alternative to use before proceeding.

- "Username and Password" on page 25.
- "Anonymous (Preconfigured) Access" on page 28
- "Single Sign-On Using Delegation with Kerberos Login System" on page 29
- "Single Sign-On Using Impersonation with Kerberos Login System" on page 30
- "Single Sign-On Using Impersonation with NTLM Login System" on page 31
- "Single Sign-On Using Impersonation with Basic Login System" on page 33
- "Client Certificate" on page 34

In addition, **Proxy Handling** is explained in this chapter.

3.3.1 Username and Password

The installation wizard configures the ASP.NET Authentication method, however, if you need to change to Username and Password authentication any time after installation, you must edit the following settings.

You must modify the `web.config` file to set `<authentication mode>` to `Forms` (including sub-section).

Also, `<authorization>` should be set to:

```
<deny users="?" />
<allow users="*" />
```

These settings technically mean that the system will deny un-authenticated users and allow any user that has not been denied.

You can also specify whether you want to allow users to save entered username and password. If you do allow user to save this information, it is saved in an encrypted cookie on the client.

Modify the relevant values, indicated by bold text, in the following code.

```
...
...
  <spotfire.dxp.web>
    <setup>
        <impersonation enabled="false" />
      </authentication>
    </setup>
...

...
  <applicationSettings>
    ...
    <Spotfire.Dxp.Web.Properties.Settings>
      ...
      <!--Impersonation:
      This is the username and password used for impersonation.-->
      <setting name="ImpersonationUsername" serializeAs="String">
        <value>impersonator</value>
      </setting>
      <setting name="ImpersonationPassword" serializeAs="String">
        <value>password</value>
      </setting>
      ...
    </Spotfire.Dxp.Web.Properties.Settings>
  </applicationSettings>
...

...
  <system.web>
    <authentication mode="Forms" >
      <forms
        loginUrl="Login.aspx"
        cookieless="UseCookies"
        defaultUrl="Default.aspx"
        slidingExpiration="true"
        timeout="525600" />
    </authentication>
    <authorization>
      <deny users="?" />
      <allow users="*" />
    </authorization>
...
...
```

When you have completed the changes, save the file.

Important To be safe, you should create a backup copy of `web.config` and store it in a reliable location. You might need the information later!

If your environment requires a proxy service, proceed to "Configure Proxy Handling" on page 36.

Otherwise proceed to "Configure IIS Authentication" on page 36.

3.3.1.1 URL Authentication

To simplify integration with other systems, you can allow users to log in via URL or standard basic authentication if Username and Password authentication is configured.

Note This can only be used on the Spotfire Web Player `Login.aspx` Web page.

Add the following attribute to the `<authentication>` element to allow URL authentication:

```
<forms enableUrlLogin="true"/>
```

It is now possible for users to log in using the address:

```
<mywebplayer>/Login.aspx?username=MyUsername&password=MyPassword&
AspxAutoDetectCookieSupport=0
```

Add the following attribute to allow basic login using authorization headers:

```
<forms enableHeaderLogin="true"/>
```

Add the following attribute to allow base64 encoded UTF8 username and password in the header:

```
<forms useUtf8EncodingForBasicHeader="true"/>
```

Example If you add all three attributes to the existing `<forms>` element, the `<authentication>` element will look like the following:

```
<authentication
  serverUrl="http://spotserver/"
  enableAutocomplete="false">
    .
    .
    .
  <forms
    ...
    enableUrlLogin="true"
    enableHeaderLogin="true"
    useUtf8EncodingForBasicHeader="true"
  />
</authentication>
```

3.3.2 Anonymous (Preconfigured) Access

In the `web.config` file, you must enable impersonation by changing the setting to `true`.

You must also specify the username and password to use when authenticating to the Spotfire Server. You enter this information in the `<value>` tags for `ImpersonationUsername` and `ImpersonationPassword`.

Note This user must also be created, given the licenses for the library, and configured for **impersonation on the Spotfire Server**. For more information and procedures, see the "TIBCO Spotfire Server - Installation and Configuration Manual."

Set the `<authentication mode>` to `none`. This also requires authorization to be set to allow all users: `<allow users="*"/>`. Now, remove the `<deny users="?" />` line.

Modify the relevant values, indicated by bold text, in the following code.

```
...
...
  <spotfire.dxp.web>
    <setup>
        <!--
              ImpersonationUsername, and ImpersonationPassword
              must also be set to enable impersonation
        -->
        <impersonation enabled="true" />
      </authentication>
    </setup>
...

...
  <applicationSettings>
    ...
    <Spotfire.Dxp.Web.Properties.Settings>
      ...
      <!--Impersonation:
          This is the username and password used for impersonation.
      -->
      <setting name="ImpersonationUsername" serializeAs="String">
        <value>impersonator</value>
      </setting>
      <setting name="ImpersonationPassword" serializeAs="String">
        <value>password</value>
      </setting>
      ...
    </Spotfire.Dxp.Web.Properties.Settings>
  </applicationSettings>
...

...
  <system.web>
    <authentication mode="None">
    </authentication>
    <authorization>
      <allow users="*"/>
    </authorization>
...
...
```

When you have completed the changes, save the file.

Important To be safe, you should create a backup copy of `web.config` and store it in a reliable location. You might need the information later!

If your environment requires a proxy service, proceed to "Configure Proxy Handling" on page 36.

Otherwise proceed to "Configure IIS Authentication" on page 36.

3.3.3 Single Sign-On Using Delegation with Kerberos Login System

You must modify the `web.config` file to specify `<authentication mode>` as `Windows` and `<identity impersonate>` to `true`.

Note For this configuration you should leave the `<impersonation enabled>` value as `false`.

Modify the relevant values, indicated by bold text, in the following code.

```
...
...
  <spotfire.dxp.web>
    <setup>
        <impersonation enabled="false" />
      </authentication>
    </setup>
...
...
  <system.web>
    <identity impersonate="true"/>
    <authentication mode="Windows">
    </authentication>
    <authorization>
      <deny users="?" />
      <allow users="*" />
    </authorization>
...
...
```

When you have completed the changes, save the file.

Note If **ASP.NET Impersonation** was enabled for the Spotfire Web Player in the IIS management console there may be a `<identity impersonate="true"/>` element in `web.config`. This setting may prevent Spotfire Web Player from working.

Important To be safe, you should create a backup copy of `web.config` and store it in a reliable location. You might need the information later!

If your environment requires a proxy service, proceed to "Configure Proxy Handling" on page 36.

Otherwise proceed to "Configure IIS Authentication" on page 36.

3.3.4 Single Sign-On Using Impersonation with Kerberos Login System

You must modify the `web.config` file to set `<impersonation enabled>` value to `true`, specify `<authentication mode>` as `Windows` and `<identity impersonate>` to `true`.

In order to authenticate to the Spotfire Server you must specify a username and password. You enter this information farther down in the `web.config` file in the `<value>` tags for `ImpersonationUsername` and `ImpersonationPassword`. The account you specify here is the impersonation account you created on the Domain Controller and configured on the Spotfire Server for the Spotfire Web Player to use in connecting to the Spotfire Server.

Important You must include the domain name when you specify the username in the `web.config` file. For example:

```
<setting name="ImpersonationUsername" serializeAs="String">
  <value>MYDOMAIN\user</value>
</setting>
<setting name="ImpersonationPassword" serializeAs="String">
  <value>pa55w0rd</value>
```

Modify the relevant values, indicated by bold text, in the following code.

```
...
...
  <spotfire.dxp.web>
    <setup>
        <!--
            ImpersonationUsername, and ImpersonationPassword
            must also be set to enable impersonation
        -->
        <impersonation enabled="true" />
      </authentication>
    </setup>
...

...
  <system.web>
    <identity impersonate="true"/>
    <authentication mode="Windows">
    </authentication>
    <authorization>
      <deny users="?" />
      <allow users="*" />
    </authorization>
...

...
  <applicationSettings>
    ...
    <Spotfire.Dxp.Web.Properties.Settings>
      ...
      <!--Impersonation:
          This is the username and password used for impersonation.
      -->
      <setting name="ImpersonationUsername" serializeAs="String">
        <value>MYDOMAIN\user</value>
```

```
        </setting>
        <setting name="ImpersonationPassword" serializeAs="String">
          <value>pa55w0rd</value>
        </setting>
        ...
      </Spotfire.Dxp.Web.Properties.Settings>
    </applicationSettings>
...
...
```

When you have completed the changes, save the file.

Note If **ASP.NET Impersonation** was enabled for the Spotfire Web Player in the IIS management console there may be a duplicate `<identity impersonate="true"/>` element in `web.config`. This duplicate setting may prevent Spotfire Web Player from working.

Important To be safe, you should create a backup copy of `web.config` and store it in a reliable location. You might need the information later!

If your environment requires a proxy service, proceed to "Configure Proxy Handling" on page 36.

Otherwise proceed to "Configure IIS Authentication" on page 36.

3.3.5 Single Sign-On Using Impersonation with NTLM Login System

You must modify the `web.config` file to set `<impersonation enabled>` value to `true`, specify `<authentication mode>` as `Windows` and `<identity impersonate>` to `true`.

In order to authenticate to the Spotfire Server you must specify a username and password. You enter this information farther down in the `web.config` file in the `<value>` tags for `ImpersonationUsername` and `ImpersonationPassword`. The account you specify here is the impersonation account you created on the Domain Controller and configured on the Spotfire Server for the Spotfire Web Player to use in connecting to the Spotfire Server.

Important You must include the Domain name when you specify the username in the `web.config` file. For example:

```
<setting name="ImpersonationUsername" serializeAs="String">
  <value>MYDOMAIN\user</value>
</setting>
<setting name="ImpersonationPassword" serializeAs="String">
  <value>pa55w0rd</value>
```

Modify the relevant values, indicated by bold text, in the following code.

```
...
...
  <spotfire.dxp.web>
    <setup>
        <!--
```

```
            ImpersonationUsername, and ImpersonationPassword
            must also be set to enable impersonation
        -->
        <impersonation enabled="true" />
      </authentication>
    </setup>
...

...
  <system.web>
    <identity impersonate="true"/>
    <authentication mode="Windows">
    </authentication>
    <authorization>
      <deny users="?" />
      <allow users="*" />
    </authorization>
...

...
  <applicationSettings>
    ...
    <Spotfire.Dxp.Web.Properties.Settings>
      ...
      <!--Impersonation:
          This is the username and password used for impersonation.
      -->
      <setting name="ImpersonationUsername" serializeAs="String">
        <value>MYDOMAIN\user</value>
      </setting>
      <setting name="ImpersonationPassword" serializeAs="String">
        <value>pa55w0rd</value>
      </setting>
      ...
    </Spotfire.Dxp.Web.Properties.Settings>
  </applicationSettings>
...
...
```

When you have completed the changes, save the file.

Note If **ASP.NET Impersonation** was enabled for the Spotfire Web Player in the IIS management console there may be a duplicate `<identity impersonate="true"/>` element in `web.config`. This duplicate setting may prevent Spotfire Web Player from working.

Important To be safe, you should create a backup copy of `web.config` and store it in a reliable location. You might need the information later!

If your environment requires a proxy service, proceed to "Configure Proxy Handling" on page 36.

Otherwise proceed to "Configure IIS Authentication" on page 36.

3.3.6 Single Sign-On Using Impersonation with Basic Login System

You must modify the `web.config` file to set `<impersonation enabled>` value to `true`, specify `<authentication mode>` as `Windows`, and set `<identity impersonate>` to `true`.

In order to authenticate to the Spotfire Server you must specify a username and password. You enter this information farther down in the `web.config` file in the `<value>` tags for `ImpersonationUsername` and `ImpersonationPassword`. The account you specify here is the impersonation account you created on the Domain Controller and configured on the Spotfire Server for the Spotfire Web Player to use in connecting to the Spotfire Server.

Example:

```
<setting name="ImpersonationUsername" serializeAs="String">
  <value>user</value>
</setting>
<setting name="ImpersonationPassword" serializeAs="String">
  <value>pa55w0rd</value>
```

Modify the relevant values, indicated by bold text, in the following code.

```
...
  <spotfire.dxp.web>
    <setup>
      ...
        <!--
             ImpersonationUsername, and ImpersonationPassword
             must also be set to enable impersonation
        -->
        <impersonation enabled="true" />
      </authentication>
    </setup>
...
...
  <system.web>
    <identity impersonate="true"/>
    <authentication mode="Windows">
    </authentication>
    <authorization>
      <deny users="?" />
      <allow users="*" />
    </authorization>
...
...
  <applicationSettings>
    ...
    <Spotfire.Dxp.Web.Properties.Settings>
      ...
      <!--Impersonation:
          This is the username and password used for impersonation.
      -->
      <setting name="ImpersonationUsername" serializeAs="String">
        <value>user</value>
      </setting>
      <setting name="ImpersonationPassword" serializeAs="String">
        <value>pa55w0rd</value>
```

```
        </setting>
        ...
      </Spotfire.Dxp.Web.Properties.Settings>
    </applicationSettings>
...
```

When you have completed the changes, save the file.

Note If **ASP.NET Impersonation** was enabled for the Spotfire Web Player in the IIS
management console there may be a duplicate `<identity impersonate="true"/>`
element in `web.config`. This duplicate setting may prevent Spotfire Web Player from
working.

Important To be safe, you should create a backup copy of `web.config` and store it in
a reliable location. You might need the information later!

If your environment requires a proxy service, proceed to "Configure Proxy Handling"
on page 36.

Otherwise proceed to "Configure IIS Authentication" on page 36.

3.3.7 Client Certificate

You must modify the `web.config` file to enable `<impersonation enabled>` by
setting it to `true`. In the `<Certificates>` element, set the `useCertificates` value to
`true`, `storeName` to `My`, and `storeLocation` to `LocalMachine`.

Set the `<authentication mode>` to `none`. Since the authentication is handled by the
application, you should set to allow all users: `<allow users="*"/>`. Now, remove the
`<deny users="?" />` line.

You must specify the serial number of the certificate to be used for the impersonation
and, if applicable, for scheduled updates. Enter this information farther down in the
`web.config` file in the `<value>` tags. The serial numbers can be found by double-
clicking on the certificate in the Microsoft Management Console.

Note If you copy the serial number from the certificate dialog you must remove any
spaces.

Note The impersonation certificate and the scheduled update certificate should be
installed in the **Personal** directory in the **Local Computer** certificate store.

Modify the relevant values, indicated by bold text, in the following code.

```
<spotfire.dxp.web>
    ...
    <setup>
      ...
        <!--
            ImpersonationUsername and ImpersonationPassword,
            or ImpersonationCertificateSerialNumber
        -->
        <!--
            must also be set to enable impersonation
        -->
        <impersonation enabled="true" />
```

```
            ...


            <!--
                  ImpersonationCertificateSerialNumber must also be set.
            -->
            <certificates
              useCertificates="true"
              storeName="My"
              storeLocation="LocalMachine"
            />
         </authentication>
...
...
  <system.web>
    <authentication mode="None">
    </authentication>
    <authorization>
      <allow users="*" />
    </authorization>
...
...
  <applicationSettings>
      ...
    <Spotfire.Dxp.Web.Properties.Settings>
        ...
        <!--
              The serial number of the certificate to use.
        -->
        <setting
          name="ImpersonationCertificateSerialNumber"
          serializeAs="String"
        >
          <value>00BDFB57D2A172B66C</value>
        </setting>
        <!--
              The serial number of the certificate to use.
        -->
        <setting
          name="ScheduledUpdatesCertificateSerialNumber"
          serializeAs="String"
        >
          <value>00BDFB57D2A172B66D</value>
        </setting>
        ...
    </Spotfire.Dxp.Web.Properties.Settings>
  </applicationSettings>
...
...
```

When you have completed the changes, save the file.

Important To be safe, you should create a backup copy of web.config and store it in a reliable location. You might need the information later!

If your environment requires a proxy service, proceed to "Configure Proxy Handling" on page 36.

Otherwise proceed to "Configure IIS Authentication" on page 36.

3.3.8 Configure Proxy Handling

Proxy handling from the browser to the Web server is handled by the browser, just as usual. However, if you need to use proxy handling for communication from the Spotfire Web Player server to the Spotfire Server, you must make additional changes to the `web.config` file.

To use proxies, you must configure the settings shown in the example below. If the proxy server is using Basic authentication, you must include the `ProxyUsername` and `ProxyPassword` settings. Enter this information in the `<value>` tags.

The Proxy element of the `web.config` file is a part of the standard .NET Framework. You can find more information about this configuration at the Microsoft Developer Network (MSDN). Use the information at MSDN if you need additional help setting up the attributes and values that are relevant to your specific Proxy server.

```
...
  <system.net>
    <defaultProxy>
      <proxy
        proxyaddress="http://MyProxyServer:3128"
        scriptLocation="MyScriptLocation"
      />
    </defaultProxy>
  </system.net>
...
...
  <applicationSettings>
    <Spotfire.Dxp.Web.Properties.Settings>
      ...
      <!--Proxy
          You need to set the system.net/defaultProxy/proxy:
          proxy address to use this. Proxy username/password
          for communication between web server and Spotfire
          Server.
      -->
      <setting name="ProxyUsername" serializeAs="String">
        <value>user</value>
      </setting>
      <setting name="ProxyPassword" serializeAs="String">
        <value>pa55w0rd</value>
      </setting>
    </Spotfire.Dxp.Web.Properties.Settings>
  </applicationSettings>
...
```

# 3.4 Configure IIS Authentication

If you are using Anonymous (Preconfigured) access, Single Sign-On authentication, or Client Certificate authentication, you must use the IIS Manager to configure IIS Authentication.

For Username and Password authentication, this is configured automatically by the installer, but if you want to confirm that you have the correct settings, use the following procedure.

▶ **Configuring Authentication on IIS 7 and IIS 8**

1 Click **Start > Administrative Tools > Internet Information Services (IIS) Manager**.

2 In the Internet Information Services (IIS) Manager navigation pane, click **Local computer > Sites > Default Web Site**.

3 Expand **SpotfireWeb**, and then double-click **Authentication**.

4 **Enable** or **Disable** authentication methods as required for your environment.
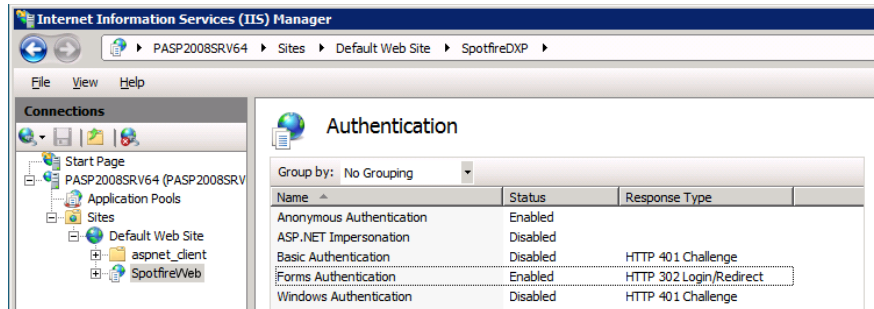
Spotfire Authentication Method	Authentication Setting
Username & Password	`Anonymous Authentication = Enabled` `Forms Authentication = Enabled`
Anonymous Login	`Anonymous Authentication = Enabled`
Single Sign-On	`Windows Authentication = Enabled` `ASP.NET Impersonation = Enabled`
Client Certificate	`Anonymous Authentication = Enabled`

Note If you have set up Single Sign-On (enabled Windows Authentication) then you must also make sure that the **ASP.NET Impersonation** setting is enabled in the `web.config` file by setting the `impersonate` attribute of the `identity` configuration element to `true`.

Regarding Username & Password

Since login validation is granted through a login dialog in the ASP.NET layer, IIS is normally configured to use anonymous access. However, it is possible to set IIS to NTLM. In this case, you can first verify that all users are logged in on your Windows Domain before they attempt to log on to the ASP.NET layer where they are required to log in using their Spotfire credentials.

The Web site in IIS (Directory security) can use Integrated Windows Authentication, Basic authentication, or Anonymous access.

3.4.1 Configure SSL

SSL communication is configured using IIS on the Spotfire Web Player server and then handled automatically by the browser and the web service calls to Spotfire Server.

We recommend that you use SSL when you are using Basic and Forms authentication because these options transmit passwords in plain text.

Note SSL is required for Client Certificate authentication.

You can find more information on configuring SSL at the Microsoft TechNet Web site: http://technet.microsoft.com

3.5   Verify the Configuration File

At this point you should verify the changes you have made to the configuration file.

Note If you enable or disable Forms Authentication in IIS, some unwanted changes may be written to the `web.config` file and you must removed these changes.

▶ **Verifying and Correcting web.config**

1   Use an XML editor to open the `web.config` file from the `webroot` directory, for example:

```
C:\Program Files\Tibco\Spotfire Web Player\6.0\webroot\Web.config
```

Comment: We recommend that you use an XML editor when you modify XML files. An XML editor has features to provide a clear view of the XML code and some text editors corrupt configuration files.

2   Locate the following elements:

```
<authentication mode="...">
  ...
  ...
</authentication>
<authorization>
  ...
  ...
</authorization>
```

3   Verify that these elements match the settings you specified earlier. If they do not match, IIS has modified the file, and you must manually insert the changes you previously made to the file.

4   Save the file.

3.6   Additional Authentication Configuration

The four alternatives for Single Sign-On authentication and Client Certificate authentication require additional configuration. You may need to make changes on either your Windows Domain Controller, the Microsoft Management Console, or the Spotfire Server. Because of this, these alternatives require that you are knowledgeable about how a Domain Controller works. For instructions on the configuration of these alternatives, see the following chapters:

- "Single Sign-On Using Delegation with Kerberos Login System" on page 39.
- "Single Sign-On Using Impersonation with Kerberos Login System" on page 45.
- "Single Sign-On Using Impersonation with NTLM Login System" on page 47
- "Single Sign-On Using Impersonation with Basic Login System" on page 48.
- "Client Certificate" on page 49.

You do not need to complete any additional configuration for Username and Password authentication or for Anonymous (Preconfigured) access, since the configuration for these methods are only in the `web.config` file and on IIS. If you implemented one of these authentication alternatives for your Spotfire environment, you should go directly to "Deploy Web Packages to Spotfire Server" on page 49.

3.6.1 Single Sign-On Using Delegation with Kerberos Login System

Install and Configure Kerberos on the Spotfire Server

To configure Kerberos on the Spotfire Server, follow the instructions in the "TIBCO Spotfire Server — Installation and Configuration Manual".

- Configure the Spotfire Server to support **Kerberos** authentication.
- A member of the **Account Operators** or **Administrators** domain groups must use the **Windows Support Tools**, typically installed on one of the domain controllers, to configure:
  - The **Service Principal Names** (SPNs) for the Spotfire Server.
  - A **keytab** file for the Spotfire Server.

3.6.1.1 Configure the Application Pool Identity on IIS

While it is possible to use Single Sign-On using delegation with Kerberos login system with the application pool running as the pre-defined Network Service account, we recommend that you run the application pool as a dedicated user account when using delegation. To configure this, follow the instructions in this section.

Create a Dedicated User Account

The first step is to create a dedicated user account on the Domain Controller.

▸ **Creating the Dedicated User Account**

1 Select **Start > Administrative Tools > Active Directory Users and Computers**.

2 In the Active Directory Users and Computers area, locate the organizational unit where you want to create the account.

3 Select the organizational unit, right-click, and then select **New > User**.

---

4   Type **Full name** and **User logon** names, and then click **Next**.

> Comment: We recommend that you use the same value for the Full name, the User
> logon name, and the User logon name (pre-Windows 2000) fields.

> Comment: The First name, Initials, and Last name field values are insignificant in this
> scenario.

5   In the following screen, use these settings:

- Clear **User must change password at next logon**.

- Select **Password never expires**.

- Select **User cannot change password**.

- Clear **Account is disabled**.

6   Click **Next** and then click **Finish**.

Configure User Rights for the Dedicated User Account

You must add the dedicated user account to the local **Administrators** group.

▶ **Adding the Dedicated User Account to the Local Groups**

1   On the Spotfire Web Player server, select **Start > Administrative Tools > Computer
Management**.

2   Expand **Local Users and Groups**, and then click **Groups**.

3   Open the **Administrators** group, and add the dedicated user account.

Configure the Application Pool Identity

Finally, you must set the application pool to run as the dedicated user account by
following these steps.

▶ **Configuring the Application Pool Identity**

1   Select **Start > Administrative Tools > Internet Information Services (IIS)
Manager**.

2   In the IIS Manager, select **Local computer > Application Pools**, and then select
TIBCO Spotfire Web Player Pool.

3   Right-click the application pool and select **Advanced Settings**.

4   Select **Identity** and click **...**

5   On the **Application Pool Identity** page, select **Custom account** and click **Set**.

6   Enter the user name and password for the dedicated user account.

7   Click **OK** three times.

8   Locate the web application **SpotfireWeb** and select it.

9   Double-click **Authentication**.

10   Right-click on (the enabled) **Windows Authentication** and select **Advanced Settings**.

11   Clear **Enable Kernel-mode authentication** and click **OK**.

12   Finally, you must restart the web server by entering the following commands in the command prompt:

```
net stop was /y

net start was

net start w3svc
```

3.6.1.2   Register Web Server Principal Names (SPN)

In this section you verify the registration of the Service Principal Names is correct on the IIS computer running Spotfire Web Player.

- If the web application pool hosting Spotfire Web Player is running under a dedicated user account, you must map both SPNs, `HTTP/servername` and `HTTP/servername.domain.tld`, to that dedicated user account.
  Important HTTP SPNs that are already mapped to any other account must be modified to be mapped to the dedicated user account.

- If the Spotfire Web Player is accessible at additional hostnames, for example `www.domain.tld`, then an SPN must be registered for that hostname as well. That is, you must register an SPN for each DNS A record. However, no SPNs should be registered for any DNS CNAME records.

- No action is required if both of the following conditions are met. In this case, default SPNs will apply.

  - IIS is accessible at `http://servername` or `http://servername.domain.tld`, where `tld` = top level domain such as .com or .local.

  - The web application pool hosting the Spotfire Web Player is running under the Network Service account.

▶   **Adding an SPN using SetSPN**

To add a server name mapped to a dedicated user account:

```
setspn -A HTTP/servername[:port] Domain\UserName
setspn -A HTTP/servername.domain.tld[:port] Domain\UserName
```

To add an additional host name mapped to a computer account:

```
setspn -A HTTP/hostname[:port] Domain\ComputerName
setspn -A HTTP/hostname.domain.tld[:port] Domain\ComputerName
```

To add an additional host name mapped to a dedicated user account:

```
setspn -A HTTP/hostname[:port] Domain\UserName
setspn -A HTTP/hostname.domain.tld[:port] Domain\UserName
```

▶ **Removing old SPNs**

If you used a dedicated user account for the application pool and need to change to a pre-defined account, you must modify the existing SPNs. You can do this with the same setspn commands, except you must use the switch to delete (-D) instead of add (-A).

Fully Qualified Name Resolution

When you use Kerberos authentication on the Spotfire Web Player server, all communication must use a fully qualified domain name (FQDN).

▶ **Verifying that IIS can be reached with an FQDN**

1   On the domain controller, open a command prompt.

2   At the command prompt, type ping fqdn. For example:

ping *mywebserver.mydomain.ms.local*

If IIS responds to the ping, the server is configured to respond to FQDN requests.

3.6.1.3 Enabling Delegation

For IIS on the Spotfire Web Player server to be able to pass user tickets to the Spotfire Server, delegation user rights must have been enabled on the Domain Controller for the computer or dedicated user account which the application pool is running under.

▶ **Enabling Unconstrained Delegation for a Computer Account On a Domain Controller in Windows 2000 Mixed or Native Mode**

1   On the Domain Controller, select **Start > Programs > Administrative Tools**.

2   Select **Active Directory Users and Computers**.

3   Locate the computer account.

4   To open the computer properties for the IIS computer, right-click the account name, and then click **Properties**.

5   On the **General** tab, select **Trust computer for delegation**, and then click **Apply**.

▶ **Enabling Unconstrained Delegation for a Dedicated User Account On a Domain Controller in Windows 2000 Mixed or Native Mode**

1   On the Domain Controller, select **Start > Programs > Administrative Tools**.

2   Select **Active Directory Users and Computers**.

3   Locate the dedicated user account.

4   To open the account properties, right-click the account name, and then click
     Properties.

5   Select the **Account** tab, in the **Account Options** list, select **Account is trusted for
     delegation** and then click **Apply**.

▶   **Enabling Unconstrained Delegation for a Computer Account On a
     Domain Controller in Windows Server 2003 Mode**

1   On the Domain Controller, select **Start > Programs > Administrative Tools**.

2   Select **Active Directory Users and Computers**.

3   Locate the computer account.

4   To open the computer properties for the IIS computer, right-click the account name,
     and then click **Properties**.

5   On the **Delegation** tab, select **Trust this computer for delegation to any service
     (Kerberos only)**, and then click **Apply**.

▶   **Enabling Unconstrained Delegation for a Dedicated User Account On a
     Domain Controller in Windows Server 2003 Mode**

1   On the Domain Controller, select **Start > Programs > Administrative Tools**.

2   Select **Active Directory Users and Computers**.

3   Locate the dedicated user account.

4   To open the account properties, right-click the account name, and then click
     Properties.

5   On the **Delegation** tab, select **Trust this user for delegation to any service
     (Kerberos only)**, and then click **Apply**.
     Note The Delegation tab is only visible for accounts that SPNs are mapped to.

▶   **Enabling Constrained Delegation for a Computer Account**

1   On the Domain Controller, select **Start > Programs > Administrative Tools**.

2   Select **Active Directory Users and Computers**.

3   Locate the computer account.

4   To open the computer properties for the IIS computer, right-click the account name,
     and then click **Properties**.

5   On the **Delegation** tab, select **Trust this computer for delegation to specified
     services only**.

6   Select **Use any authentication protocol**.

7   Click **Add…**

---

8   Click **Users or Computers…** and select the account that the Spotfire Server has a
     keytab for and the SPNs are mapped to. (See "Install and Configure Kerberos on the
     Spotfire Server" on page 39.)

9   Select all services that apply, click **OK**, and then click **Apply**.

▶   **Enabling Constrained Delegation for a Dedicated User Account**

1   On the Domain Controller, select **Start > Programs > Administrative Tools**.

2   Select **Active Directory Users and Computers**.

3   Locate the dedicated user account.

4   To open the account properties, right-click the account name, and then click
     Properties.

5   On the **Delegation** tab, select **Trust this user for delegation to specified services
     only**.
     Note The Delegation tab is only visible for accounts that SPNs are mapped to.

6   Select **Use any authentication protocol**.

7   Click **Add…**

8   Click **Users or Computers…** and select the account that the Spotfire Server has a
     keytab for and the SPNs are mapped to. (See "Install and Configure Kerberos on the
     Spotfire Server" on page 39.)

9   Select all services that apply, click **OK**, and then click **Apply**.

Spotfire Web Player Server Requirements

You must configure these settings on the Spotfire Web Player server.

1   Under **Control Panel > Network and Internet > Internet Options > Advanced**
     select **Enable Integrated Windows Authentication (Requires Restart)**.

2   The Spotfire Server you are connecting to must be located in the **Intranet** security
     zone.

Internet Explorer Client Requirements

You must configure these settings on every end-user computer.

1   Under **Tools > Internet Options > Advanced** you must select **Enable Integrated
     Windows Authentication (Requires Restart)**.

2   The Spotfire Web Player server you are connecting to must be located in the **Intranet**
     security zone.

     Note If the website is located in the **Internet** security zone, Internet Explorer will not
     even attempt Kerberos authentication. This is because in most **Internet** scenarios a
     connection with a domain controller can not be established. The simple rule is that any

URL that contains periods, such as an IP address or Fully Qualified Domain Name (FQDN), is in the **Internet** zone. If you are connecting to an IP address or FQDN then you can use the settings in Internet Explorer or Group Policy to add this site to the **Intranet** security zone. For more information on how Internet Explorer evaluates the zone of a resource, see the Microsoft knowledge base article KB 258063.

Google Chrome Client Requirements

You must launch Google Chrome with the following parameters:

- `--auth-server-whitelist`
- `--auth-negotiate-delegate-whitelist`

For example:

```
chrome.exe --auth-server-whitelist=".domain.com" --auth-negotiate-
delegate-whitelist=".domain.com"
```

Where `.domain.com` is the URL to the Spotfire Web Player server. You can enter the URL with a preceding wildcard character '*' to enable Google Chrome to connect to any URL that ends in 'domain.com'.

For more information, see the Chromium Projects developer page at `http://www.chromium.org/developers/design-documents/http-authentication`.

Mozilla Firefox Client Requirements

You must configure these settings on every end-user computer.

1   In the Firefox browser address box, type `about:config`.

2   For the following parameters, set the values to the Spotfire Web Player URL for which you want to activate Negotiate.

- `network.negotiate-auth.delegation-uris`
- `network.negotiate-auth.trusted-uris`

Proceed to "Deploy Web Packages to Spotfire Server" on page 49.

3.6.2   Single Sign-On Using Impersonation with Kerberos Login System

Create an Impersonation Account on the Domain Controller

The dedicated user account you intend to use for Impersonation must be present on the Domain Controller. You should log on to the Domain Controller and create or verify that the dedicated user account you intend to use is available.

Note The account does not need to have Delegation user rights.

Set up Kerberos on the Spotfire Server

Follow the instructions in the "TIBCO Spotfire Server - Installation and Configuration Manual" to set this up.

- The Spotfire Server needs to be configured to support **Kerberos** authentication.

- A member of the **Account Operators** or **Administrators** domain groups must use the **Windows Support Tools**, typically installed on one of the domain controllers, to configure:

  - The **Service Principal Names** (SPNs) for the Spotfire Server.

  - A **keytab** file for the Spotfire Server.

- The Impersonation username specified on the Domain Controller must also be configured for **impersonation on the Spotfire Server**.

Spotfire Web Player Server Requirements

You must configure these settings on the Spotfire Web Player server.

1 Under **Control Panel > Network and Internet > Internet Options > Advanced** you must select **Enable Integrated Windows Authentication (Requires Restart)**.

2 The Spotfire Server you are connecting to must be located in the **Intranet** security zone.

Internet Explorer Client Requirements

You must configure these settings on every end-user computer.

1 Under **Tools > Internet Options > Advanced** you must select **Enable Integrated Windows Authentication (Requires Restart)**.

2 The Spotfire Web Player server you are connecting to must be located in the **Intranet** security zone.

Note If the website is located in the **Internet** security zone, Internet Explorer will not even attempt Kerberos authentication. This is because in most Internet scenarios a connection with a domain controller can not be established. The simple rule is that any URL that contains periods, such as an IP address or Fully Qualified Domain Name (FQDN), is in the Internet zone. If you are connecting to an IP address or FQDN then you can use the settings in Internet Explorer or Group Policy to add this site to the **Intranet** security zone. For more information on how Internet Explorer evaluates the zone of a resource, see the Microsoft knowledge base article KB 258063.

Google Chrome Client Requirements

You must launch Google Chrome with the following parameters:

- `--auth-server-whitelist`
- `--auth-negotiate-delegate-whitelist`

For example:

```
chrome.exe --auth-server-whitelist=".domain.com" --auth-negotiate-
delegate-whitelist=".domain.com"
```

Where `.domain.com` is the URL to the Spotfire Web Player server. You can enter the URL with a preceding wildcard character '*' to enable Google Chrome to connect to any URL that ends in 'domain.com'.

For more information, see the Chromium Projects developer page at `http://www.chromium.org/developers/design-documents/http-authentication`.

Mozilla Firefox Client Requirements

You must configure these settings on every end-user computer.

1   In the Firefox browser address box, type `about:config`.

2   For the following parameters, set the values to the Spotfire Web Player URL for which you want to activate Negotiate.

   - `network.negotiate-auth.delegation-uris`
   - `network.negotiate-auth.trusted-uris`

Proceed to "Deploy Web Packages to Spotfire Server" on page 49.

3.6.3   Single Sign-On Using Impersonation with NTLM Login System

Create an Impersonation Account on the Domain Controller

The dedicated user account you intend to use for Impersonation must be present on the Domain Controller. You should log on to the Domain Controller and create or verify that the dedicated user account you intend to use is available.

If you want to limit the number of computers this impersonation account can log in to, you must give the account the user rights to log in to the service account for the computer running the Spotfire Server.

Note The dedicated user account does not need to have Delegation user rights.

Set up NTLM on the Spotfire Server

Follow the instructions in the "TIBCO Spotfire Server - Installation and Configuration Manual" to set this up.

   - The Spotfire Server needs to be configured to support **NTLM** authentication.
   - The Impersonation username specified on the Domain Controller must also be configured for **impersonation on the Spotfire Server**.

Spotfire Web Player Server Requirements

You must configure these settings on the Spotfire Web Player server.

1   Under **Control Panel > Network and Internet > Internet Options > Advanced**, select **Enable Integrated Windows Authentication (Requires Restart)**.

2   The TIBCO Spotfire Server you are connecting to must be located in the **Intranet** security zone.

Internet Explorer Client Requirements

You must configure these settings on every end-user computer.

1 Under **Tools > Internet Options > Advanced** select **Enable Integrated Windows Authentication (Requires Restart)**.

2 The Spotfire Web Player server you are connecting to must be located in the **Intranet** security zone.

Google Chrome Client Requirements

You must launch Google Chrome with the following parameters:

- `--auth-server-whitelist`
- `--auth-negotiate-delegate-whitelist`

For example:

```
chrome.exe --auth-server-whitelist=".domain.com" --auth-negotiate-
delegate-whitelist=".domain.com"
```

Where `.domain.com` is the URL to the Spotfire Web Player server. You can enter the URL with a preceding wildcard character '*' to enable Google Chrome to connect to any URL that ends in 'domain.com'.

For more information, see the Chromium Projects developer page at `http://www.chromium.org/developers/design-documents/http-authentication`.

Mozilla Firefox Client Requirements

You must configure these settings on every end-user computer.

1 In the Firefox browser address box, type `about:config`.

2 For the following parameters, set the values to the Spotfire Web Player URL for which you want to activate Negotiate.

- `network.automatic-ntlm-auth.trusted-uris`

Proceed to "Deploy Web Packages to Spotfire Server" on page 49.

3.6.4 Single Sign-On Using Impersonation with Basic Login System

Create an Impersonation Account on the Domain Controller

The dedicated user account you intend to use for Impersonation must be present on the Domain Controller. You should log on to the Domain Controller and create or verify that the dedicated user account you intend to use is available.

Note The dedicated user account does not need to have Delegation user rights.

Create an Impersonation Account on the Spotfire Server or LDAP Server

Follow the instructions in the "TIBCO Spotfire Server - Installation and Configuration Manual" to set this up.

- If the Spotfire Server has been configured to use Database login system, the same impersonation username must be present in the Spotfire Server Database.

- If the Spotfire Server has been configured to use LDAP login system, the same impersonation username must be present on the LDAP Server.

- The Impersonation username must also be configured for **impersonation on the Spotfire Server**.

Proceed to "Deploy Web Packages to Spotfire Server" on page 49.

3.6.5   Client Certificate

For the web application to be able to access the impersonation certificate, and, if applicable, the scheduled update certificate, the account running the application pool, for example NETWORK SERVICE, must be given reading permissions for the certificates.

3.6.5.1 Change the Access Rights

Modifying access rights on Windows Server 2008 and Windows Server 2012 is completed using the Microsoft Management Console.

▸   **Changing the Access Rights**

1   Start the Microsoft Management Console.

2   For the **Local Computer,** add the **Certificates** snap-in.

3   Select **Certificates (Local Computer) > Personal > Certificates.**

4   Right-click the installed impersonation user certificate and select **All Tasks > Manage Private Keys...**

5   Click **Add...**

6   Locate and select the account **NETWORK SERVICE**.

7   Grant the **NETWORK SERVICE** account **Read** permissions.

8   Click **OK**.

Proceed to "Deploy Web Packages to Spotfire Server" on page 49.

3.7   Deploy Web Packages to Spotfire Server

Any hotfixes released for Spotfire 6.0 must be deployed first as packages to the Spotfire Server and then pushed to the Spotfire Web Player with the upgrade tool. you

can download hotfixes from the TIBCO Spotfire hotfix download site, `http://support.spotfire.com/patches.asp`.

To deploy any hotfixes, extensions, or upgrades to the Spotfire Web Player, follow the instructions in the chapter "Deploying Extensions and Upgrades" on page 54.

For information on how to deploy packages to the Spotfire Server, please refer to the TIBCO Spotfire - Deployment and Administration Manual.

3.8 Licenses and Library Rights

3.8.1 Licenses

All Spotfire Web Player users must have certain license functions enabled in order to open an analysis. If you are using anonymous/preconfigured authentication, then the preconfigured single user that has been set up must have these license functions.

You can configure licenses from the TIBCO Spotfire Administration Manager found in the TIBCO Spotfire client.

At present, these are the license functions that are relevant for Spotfire Web Player:

TIBCO Spotfire Web Player

- **TIBCO Spotfire Web Player** - select this license for all users of Spotfire Web Player.

TIBCO Spotfire Enterprise Player

- **Open File** - this license function is required to open an analysis from the Spotfire Web Player.

- **Open from Library -** this license function is required to open an analysis saved in the library.

- **Open Linked Data** - this license function is required to open an analysis that has linked data.

- **Save Spotfire Analysis File** - this license function is required for a user to be able to open the current Spotfire Web Player file for additional analysis in either TIBCO Spotfire Professional or Enterprise Player.

For more information on these, and other, licenses, please refer to the "**TIBCO Spotfire - Deployment and Administration Manual**".

▶ **Configuring License Functions**

1 Start TIBCO Spotfire and log in as an administrator.

2 Select **Tools > Administration Manager**.

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

4   Select a group for which you want to configure licenses.

5   Click the **Licenses** tab in the right hand pane.

6   For each group of users that will use the Spotfire Web Player, click the **Edit** button, select the check boxes for the above mentioned license functions and click **OK**.

3.8.2   Spotfire Library User Rights

The analyses shown in the Spotfire Web Player are, in effect, files stored in the Spotfire Library. It is therefore necessary for the various users of Spotfire Web Player to have access to the library sections where a variety of content is stored.

If you configured Spotfire Web Player to use anonymous/preconfigured authentication, then you only need to configure access rights for the single preconfigured user and everyone will automatically use those credentials. If you have configured authentication so that each user will be logged in with their own credentials, you must set up access rights for all users (or groups of users).
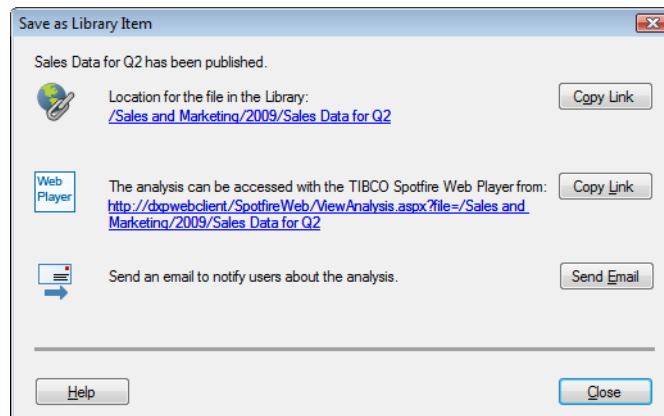
▶   **Configuring Spotfire Library User Rights**

1   Start TIBCO Spotfire and then click **Tools > Library Administration**.

2   For information on how to create library sections and folders, and how to configure access rights to these, see the **Library Administration** section in the TIBCO Spotfire online help, which you can reach by clicking **Help**.

3.9   URL Preference

When a user publishes a new Spotfire analysis file to the Spotfire Library, it is useful to instantly see the URL of that analysis. In order to see this URL, you must perform the following procedure.

When this is configured, users can copy the URL and send it to other people, who can open the analysis in Spotfire Web Player.


In order for this information to appear on the "Save as Library Item" page, you must set a Group Preference containing the Spotfire Web Player URL.

We recommend that you set this preference for the **Everyone** group. That way all Spotfire users will see the URL when publishing files to the Spotfire Library.

▶ **Setting the URL Preference**

1 Start TIBCO Spotfire.

2 Log in as an administrator.

3 Select **Tools > Administration Manager...**.

4 Select the **Preferences** tab.

5 Select the **Everyone** group in the list.

6 Click the **Edit** button.

7 Expand the **Application** node, and select **ApplicationPreferences**.

8 Click in the text field for **DXPLibraryWebURL**, and enter the URL of the Spotfire Web Player.
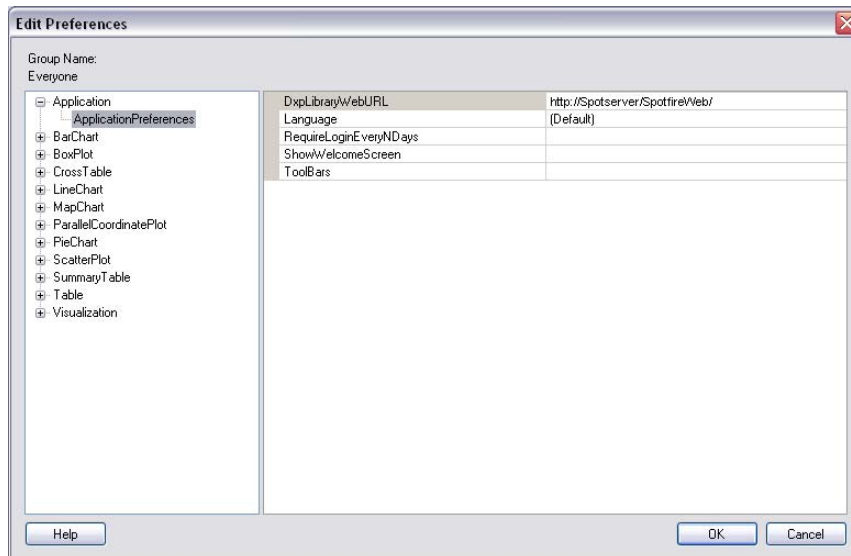
9 Click **OK**.

10 Click **Close**, to exit the Administration Manager.

11 All users should now see the URL of their analysis, when saving to the Spotfire Library.

4   Upgrading

4.1   Upgrading to New Version

Upgrading from TIBCO Spotfire Web Player 5.5 or earlier to TIBCO Spotfire Web Player 6.0 basically consists of uninstalling the previous version and then installing the most recent version.

Performing an upgrade is therefore almost identical to performing a new installation as described in the chapter "Install Spotfire Web Player" on page 24. The new version 6.0 installer will first uninstall the old version of the software, and then install the new version. Therefore, it is important to make backups of files you want to reapply settings from.

However, there are manual steps which you must perform to make sure authentication is configured in the same way as on your previous version. If you have custom extensions to the Spotfire Web Player these will need to be redeployed on the new version as well.

▶   **Upgrading the Spotfire Web Player**

These steps explain the basic workflow you must perform to upgrade the Spotfire Web Player.

However, when performing Step 2 to Step 8 you should read the instructions in the chapter "Install Spotfire Web Player" on page 24.

1   Make a backup of your old installation directory. This is likely to be located in a default directory such as:

```
C:\Program Files\Tibco\Spotfire Web Player\5.5\
```

Note This will contain your `web.config` file and other important files needed for the upgrade.

2   Install **Microsoft .NET Framework 4.0** on the server, if it is not already present. Microsoft .NET Framework 4.0 can be downloaded from http://download.microsoft.com

3   Copy the new Spotfire Web Player 6.0 installer files to a temporary directory on the server.

4   Run the installer.

Note Be sure to specify the same name for the Virtual Directory as for the previous version. If you change it, old links to analyses will not find their targets.

The installer will automatically remove the older Spotfire Web Player and install the new Spotfire Web Player.

5   Edit the new `web.config` in that directory to suit your needs (as described in the Installation chapter). You can review the settings made in the old `web.config` but do not copy entire sections of XML and paste into the new 6.0 `web.config`, since the structure has been changed and needs to be intact.

6   Configure the web site (as described in the Installation chapter).

7   Configure Licenses and Library Rights (as described in the Installation chapter).

8   Set the URL preference (as described in the Installation chapter).

9   Redeploy any custom extensions that were previously deployed on your Spotfire Web Player server.

     If the extensions were not deployed as packages on the old Spotfire Web Player server, you need to build packages of the extensions using the Package Builder located in the Spotfire SDK (`http://stn.spotfire.com/stn/Extend/SDKOverview.aspx`).

     Note The packages must be marked with the intended client "TIBCO Spotfire Any Client" or "TIBCO Spotfire Web Player".

     After you have built the packages, you must upgrade the Spotfire Web Player with the created packages by deploying them to the Spotfire Server and then using a special upgrade tool to make them appear on the Spotfire Web Player server. For more information, see "Deploying Extensions and Upgrades" on page 54.

10   Any changes made to the `ScheduledUpdates.xml` must also be transferred to the new version of this file (see "Upgrade an Existing Schedule" on page 92).

11   If you have customized the Header Banner (see "Customize Web Pages" on page 60), reapply these modifications.

12   Finally, clean up potential remaining files in the old installation directory.

4.2   Deploying Extensions and Upgrades

If you have deployed packages marked with the intended client "TIBCO Spotfire Any Client" or "TIBCO Spotfire Web Player" to a Spotfire Server, it is possible to extend or upgrade Spotfire Web Player with those packages using the upgrade tool. For information on how to deploy packages to the Spotfire Server, please refer to the TIBCO Spotfire – Deployment and Administration Manual.

The upgrade tool is a batch file, named `webupdate.bat`, which is run from the Spotfire Web Player server. It connects to the Spotfire Server specified in the `web.config` file, and you should specify the authorization for the Spotfire Server in the upgrade tool configuration file.

Configure the Upgrade Tool

To use the upgrade tool, you first need to specify certain information in the upgrade tool configuration file. You can find the configuration file,

`Spotfire.Dxp.Web.UpgradeTool.exe.config,` in the `webroot\bin\Tools` directory of the installation.

The available settings in the configuration file are listed below. Enter this information in the `<value>` tags.

```
<applicationSettings>
    <Spotfire.Dxp.Web.UpgradeTool.Properties.Settings>
        <setting name="Credentials_Enabled" serializeAs="String">
            <value>False</value>
        </setting>
        <setting name="Credentials_Username" serializeAs="String">
            <value>CredentialsUsername</value>
        </setting>
        <setting name="Credentials_Password" serializeAs="String">
            <value>CredentialsPassword</value>
        </setting>
        <setting name="WebRootPath" serializeAs="String">
            <value>C:\Program Files\TIBCO\Spotfire Web Player
                \6.0\webroot</value>
        </setting>
        <setting name="ServerArea" serializeAs="String">
            <value>Production</value>
        </setting>
        <setting name="Proxy_Enabled" serializeAs="String">
            <value>False</value>
        </setting>
        <setting name="Proxy_Username" serializeAs="String">
            <value>ProxyUsername</value>
        </setting>
        <setting name="Proxy_Password" serializeAs="String">
            <value>ProxyPassword</value>
        </setting>
        <setting name="Certificate_Enabled" serializeAs="String">
            <value>False</value>
        </setting>
        <setting name="Certificate_StoreName" serializeAs="String">
            <value>My</value>
        </setting>
        <setting name="Certificate_StoreLocation" serializeAs="String">
            <value>CurrentUser</value>
        </setting>
        <setting name="Certificate_SerialNumber" serializeAs="String">
            <value>00BDFB57D2A172B66E</value>
        </setting>
    </Spotfire.Dxp.Web.UpgradeTool.Properties.Settings>
    <Spotfire.Dxp.Internal.Properties.Settings>
        <setting
                name="ManifestDownloadTimeoutMilliseconds"
                serializeAs="String">
         <value>60000</value>
        </setting>
    </Spotfire.Dxp.Internal.Properties.Settings>
</applicationSettings>
```

Key	Description
Credentials_Enabled	Set to true if you use Username/Password authentication. If you use Single Sign-On, set this to false, and make sure that you run the batch file as a user with the proper permissions for the Spotfire Server. **Note** It is possible to encrypt the information in this configuration file. you do this by running the file `Spotfire.Dxp.Web.UpgradeTool.exe`, also located in the `Tools` directory, in the command prompt with the flag `/protectSettings` after you've modified the configuration file. Then, you run the batch file as described below. To remove the encryption, run the `.exe` file with the flag `/unprotectSettings` in the command prompt. Enter this information in the `<value>` tags.
Credentials_Username	Specify the username to log into the Spotfire Server. Enter this information in the `<value>` tags.
Credentials_Password	Specify the password to log into the Spotfire Server. Enter this information in the `<value>` tags.
WebRootPath	The path of the webroot directory of the installation. This is set automatically when installing. Enter this information in the `<value>` tags.
ServerArea	The server area. Default value: Production. Other valid values: Test. Enter this information in the `<value>` tags.
Proxy_Enabled	Set to true if you use proxy handling for communication to the Spotfire Server and need to provide a username and password for the proxy. Enter this information in the `<value>` tags.
Proxy_Username	Specify the username for the proxy server, if needed. Enter this information in the `<value>` tags.
Proxy_Password	Specify the password for the proxy server, if needed. Enter this information in the `<value>` tags.

`Certificate_Enabled`	Set this to true if the Spotfire Server requires Client Certificate authentication. For more information on client certificates, please refer to the **TIBCO Spotfire Server - Installation and Configuration Manual**. Enter this information in the `<value>` tags.
`Certificate_StoreName`	Specify the store name to get the certificate from. Default value: My. Other valid values: AddressBook, AuthRoot, CertificateAuthority, Disallowed, Root, TrustedPeople, TrustedPublisher. Enter this information in the `<value>` tags.
`Certificate_StoreLocation`	Specify the location to get the certificate from. Default value: CurrentUser. Other valid values: LocalMachine. Enter this information in the `<value>` tags.
`Certificate_SerialNumber`	Specify the serial number of the certificate. Enter this information in the `<value>` tags.
`<Spotfire.Dxp.Internal. Properties.Settings>`	
`ManifestDownloadTimeout Milliseconds`	Specify the manifest download time in milliseconds. This is the time the application waits before aborting an operation when the server does not respond. The default value is `60000`.

Use the Upgrade Tool

After configuring the `Spotfire.Dxp.Web.UpgradeTool.exe.config`, run the `webupdate.bat` file, also found in the `webroot\bin\Tools` directory of the installation. You can review the upgrade tool operations in the log file at: `webroot\bin\Tools\Spotfire.Dxp.Web.UpgradeTool.log`.

Make sure that you run the file as a user with the proper permissions for the Spotfire Server if you use Windows integrated authentication. Also make sure that you run the file as a user with the permission to start and stop IIS on the Spotfire Web Player server.

The upgrade tool will check if there are any upgrades available on the Spotfire Server, and if there are, it will automatically stop the application pool, install the upgrades and restart the application pool.

It is also possible to schedule the webupdate.bat file to run at given times using the **Task Scheduler** on the Spotfire Web Player server.

5   Testing the Installation

Perform the following procedures to verify that your installation of Spotfire Web Player works as intended.

▶ **Opening an Analysis in a Web Browser**

1   Open a web browser.

2   Enter the URL to the Spotfire Web Player. For example,

    `http[s]://<servername>/SpotfireWeb/`

3   Log in if necessary.

    <u>Response:</u> You will now see the Spotfire Library which by default contains some folders and a few analysis files.

4   Navigate to a folder and click on an analysis file.

5   Verify that the analysis is displayed in your web browser.

▶ **Publishing an Analysis and Viewing it in a Web Browser**

1   On a computer that has the regular TIBCO Spotfire client installed, start TIBCO Spotfire by selecting **Start > All Programs > TIBCO > TIBCO Spotfire**.

2   Log in.

3   Select **File > Open...** to open some data. For example, use an Excel-file or similar.

4   Click **OK** to accept Import Settings.

    <u>Response:</u> The data is loaded and a visualization appears.

5   Select **File >Save As... > Library Item...**

6   Enter a name and click **Next**.

7   Enter a **Description** and click **Next**.

8   Select **Override these settings and embed all data**, and click **Finish**.

9   On the page that appears, verify that there is a link to the Spotfire Library and also directly to the published file.
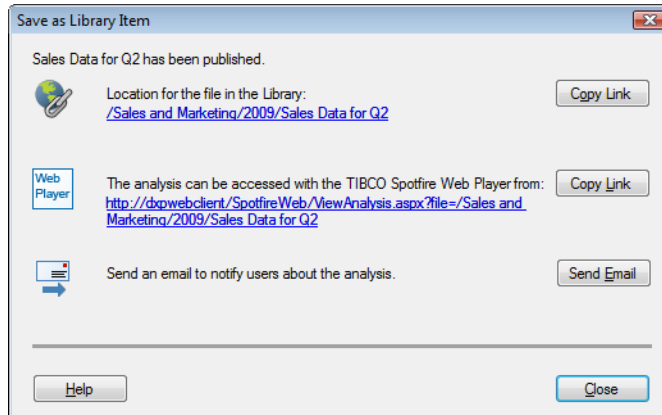
10   Click on the link to the published file.

Response: Your web browser launches.

11   Log in to the Spotfire Library (if necessary).

12   Verify that the analysis is displayed in your web browser.

Testing the Installation from a Web Browser on the Server

If you would like to test the application from a web browser directly on the web server, you need to turn off "Internet Explorer Enhanced Security Configuration". Otherwise you will not be able to use Internet Explorer for more than static web pages.

To turn it off, go to the **Server Manager**, select the **Security Information** section, click **Configure IE ESC** and select **Off**.

A simpler option is to test the installation from another, stand-alone computer.

6 Advanced Procedures and Technical Reference

6.1 Customize Web Pages

This section covers the process to co-brand an analyses file by customizing the header banner and how to modify the error handling to minimize the ability of users to inject malicious code.

6.1.1 Customize the Header Banner

You can co-brand an analyses by displaying your company logo in the top header of the Spotfire Web Player analyses. Perform this modification in the `Header.htm` file in the `App_Data` directory of the installation directory. To enable the display of this co-branding element and modify the height of the display area, you must modify the configuration file.

In `web.config` , update the section `system.web/customErrors` to: `<customErrors mode="On" defaultRedirect="~/ExampleError.html" />`. To enable the header banner and change the height, see Figure 6.2.2, "User Interface Element," on page 66

The `Header.htm` file is a part of an `XHTML` file; it should only contain the `xhtml` of the visible component, NOT the `HTML`, `HEAD`, or `BODY` tags. The `XHTML` is then merged into the top of all the pages (the outlined part in the image below) and displayed to the user.
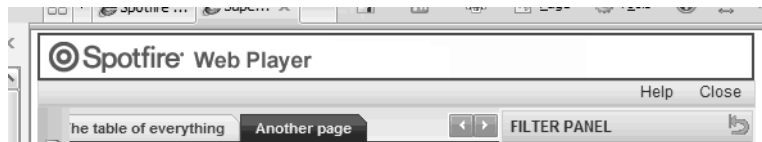
By default, the `XHTML` is:

```
<table cellpadding="0" cellspacing="0" style="white-space:nowrap;">
  <tr>
    <td style="width: 1px; vertical-align: bottom;">
      <img alt="Logo" src="/[%AppPath%]/Images/CompanyLogoWide.png"/>
    </td>
    <td style="white-space: nowrap; vertical-align: bottom;">
      <span class="CustomizationAreaLargeText">
        Spotfire Web Player
      </span>
    </td>
  </tr>
</table>
```

To customize the `XHTML`, edit the `Header.htm` file in the installation directory before installing the product, or edit the file after installation, then located in the `App_Data` directory of the web root.

Note This file is a translatable file that can be loaded in different languages. If you install a language pack, you should modify the file on that installation also. If no translation is needed (the file is language independent) you can just copy the file for the default here. This file is located in
`<web-root>\App_Data\<Language>\Header.htm`
(Example: the German file is located in `<web-root>\App_Data\`**de-DE**`\Header.htm`).

6.1.2 Custom Error Web Page

If your Spotfire Web Player environment is open to external users you can replace the default error messages that are displayed for the Spotfire Web Player to prevent users from injecting user controlled error messages through a URL.

To modify this behavior you must create a new error message file and then modify the configuration file. After you make these changes, any error that occurs in the Spotfire Web Player will be redirected to this static error page.

Note If you make this change, users will not receive any details or information about the error.

▶ **Adding a Custom Error web Page**

1 In `web.config` update the section `system.web/customErrors` to:
   `<customErrors mode="On" defaultRedirect="~/ExampleError.html" />`

2 Create a custom error web page. For example,

```
<!DOCTYPE html>
<html lang="en" xmlns="http://www.w3.org/1999/xhtml">
<head>
  <meta charset="utf-8" />
  <title>Error - TIBCO Spotfire Web Player</title>
</head>
<body>
  <h1>TIBCO Spotfire Web Player</h1>
  <div>An error occurred.</div>
  <div>
    Contact the administrator at (123) 456-7890 or
    <a href="mailto:admin@mycompany.com">admin@mycompany.com</a>.
  </div>
  <div style="margin-top: 10px; font-size: 125%;">
    <a href="Library.aspx">Back to start page</a>
  </div>
</body>
</html>
```

3 Save the web page to `<web-root>\App_Data\` using a name that matches the name in the `<customErrors>` setting, for example, `ExampleError.html`.

6.2 Advanced Web.Config Settings

This section discusses how you can configure advanced settings, such as those for the Spotfire Web Player user interface. The section starts with an example of a

configuration file (`web.config`) followed by a table with an explanation of each setting.

```
<spotfire.dxp.web>
  <!-- **********************************************************
    Web Player settings for non visible items -->
  <setup>
    <!-- Set to true to enable the client Java Script API  -->
    <javaScriptApi enabled="false" />

    <!-- The mailto link on the error page will use the email address below.
    You can also set the maximum length of the email -->
    <errorReporting
      emailAddress="spotfireadmin@yourcompany.com"
      maxMailLength="1000"
      automaticallyShutDownAfterStartupFailureAfterMinutes="5"/>

    <authentication serverUrl="http://spotserver/" enableAutocomplete="false">
      <loginService enabled="true" loginRequireSsl="false" />
    </authentication>
  </setup>

  <!-- **********************************************************
    This section contains settings for the user interface of the Web Player -->
  <userInterface>
    <pages showLogout="true" showAbout="true" showHelp="true" showUserName="true"/>
    <diagnostics errorLogMaxLines="2000" />
    <analysis showToolTip="true"
              showClose="true"
              showToolBar="true"
              showAnalysisInformationTool="true"
              showExportFile="true"
              showExportVisualization="true"
              showUndoRedo="true"
              showDodPanel=""
              showFilterPanel=""
              showPageNavigation="true"
              showStatusBar="true"
              showPrint="true"
              allowRelativeLinks="false" />

    <customHeader enabled="false" fileName="Header.htm" height="40" />
    <closedAnalysis
          showOpenLibrary="true"
          showReopenAnalysis="true"
          redirectToLibrary="true"
    />
    <errorPage showOpenLibrary="true" showReopenAnalysis="true" />
    <serverUnavaliable showOpenLibrary="true" showReopenAnalysis="true" />
  </userInterface>

  <!-- **********************************************************
    This section contains setting for tuning performance.
    Be careful when making changes. -->
  <performance>
    <documentCache purgeInterval="300"
                   itemExpirationTimeout="00:00:00"/>

    <analysis checkClosedInterval="60"
```

Numbered callouts (circled): **1**, **2**, **3**, **4**, **5**, **6**

```
            closedTimeout="120"
            checkInactivityInterval="300"
            inactivityTimeout="Infinite"
            regularPollChangesInterval="500"
            maxPollChangesInterval="3000"
            pollLoadInterval="1000"
            needsRefreshInterval="15"
            toolTipDelay="1000"
            antiAliasEnabled="true"
            useClearType="true"
            documentStateEnabled="true"
            undoRedoEnabled="true"
            userServicesPoolEnabled="true"
            maxRenderTimeMs="60000"
            userPreferencesMaxAge="00:05:00" />

    <hierarchicalClustering maxInteractiveElements="2000"
                            maxElements="30000"
                            maxInteractiveJobs="2"
                            cpuFactorInteractiveJobs="0.8"
                            cpuFactorLargeJobs="0.5"
                            nativeMemory="500" />
  </performance>
</spotfire.dxp.web>

<!-- ****** Settings for the communication with the TIBCO Spotfire Server ******** -->
<Spotfire.Dxp.Services.Settings>
  <!-- Cookies from the TIBCO Spotfire Server that should be sent back on all requests:
-->
  <!-- a ; separated list, example: "ARRAffinity;myCookie;myCookie2" -->
  <cookies autoTransfer="" />
</Spotfire.Dxp.Services.Settings>

<system.web>
  <!--How long before a user is logged out (when no analysis is displayed) -->
  <sessionState timeout="20" cookieless="UseCookies" />
</system.web>

<applicationSettings>
  <Spotfire.Dxp.Internal.Properties.Settings>
    <setting name="ManifestDownloadTimeoutMilliseconds" serializeAs="String">
      <value>60000</value>
    </setting>
    <setting name="LibraryCache_Enabled" serializeAs="String">
      <value>True</value>
    </setting>
    <setting name="LibraryCache_MaxCacheTime" serializeAs="String">
      <value>00:10:00</value>
    </setting>
  </Spotfire.Dxp.Internal.Properties.Settings>

  <Spotfire.Dxp.Data.Properties.Settings>
    <setting name="DataBlockStorageIOSizeKB" serializeAs="String">
      <value>64</value>
    </setting>
    <setting name="DataOnDemand_MaxCacheTime" serializeAs="String">
      <value>01:00:00</value>
    </setting>
    <setting name="AllowedWebRootFiles" serializeAs="String">
```

⑦

⑧

⑨

```
         <value></value>
      </setting>
      <setting name="AllowedFilePaths" serializeAs="Xml">
        <value>
          <ArrayOfString>
            <string/>
          </ArrayOfString>
        </value>
      </setting>

    </Spotfire.Dxp.Data.Properties.Settings>
  </applicationSettings>
```

Use an XML editor to open the `web.config` file from the `webroot` directory, for example:

`C:\Program Files\Tibco\Spotfire Web Player\6.0\webroot\Web.config`

Note We recommend that you use an XML editor when you modify XML files. An XML editor has features to provide a clear view of the XML code and some text editors corrupt configuration files.

Important When you save changes to the `web.config` file, IIS automatically detects that the file has been modified and restarts the Spotfire Web Player application. Users who are logged into the Spotfire Web Player will be disconnected.

6.2.1 Setup Element

The following table contains details about the tags and attributes along with the values that you can modify in the `<setup>` element of the configuration file. This section corresponds to the part of the configuration file labeled "1", "2", and "3" in the previous code sample.

Position	Tag (with default value)	Explanation
1	`<javaScriptApi enabled="false" />`	Enables or disables the Spotfire Web Player Javascript API. Enable this setting to allow users to share and view embedded analysis files using the **Copy Link** or **Embed Code** tools in the Spotfire Web Player.
		You can control the domain of the Spotfire Web Player pages by typing the desired domain name in the `domain` attribute. For example: `<javaScriptApi enabled="true" domain="example.com" />`
		For more information, see the Spotfire Technology Network `http://spotfire.tibco.com/stn`
2	`<errorReporting>`	

	`emailAddress=` `"spotfireadmin@yourcompany.com"`	Specify the e-mail address for the Spotfire Web Player administrator. When a user encounters certain server related errors, a dialog with a **Report error to administrator** `mailto` link is displayed. If the user clicks the link, an e-mail addressed to the administrator and including the error log is created in the default e-mail application.
	`maxMailLength="1000"`	Specify the maximum number of characters in the e-mail that is generated when a user clicks the **Report error to administrator** link. Some e-mail systems, including Lotus Notes, have a 2000 character limit.
	`automaticallyShutDownAfterStartup` `FailureAfterMinutes="5"`	Specify the number of minutes the Spotfire Web Player application will wait before trying to restart if there has been an error during startup. This setting is useful in the case where the Spotfire Server is offline for maintenance. **Note** Do not set this value to a number less than 2 because IIS might disable the Spotfire Web Player application pool if the Spotfire Web Player is restarted several times over a short period.
3	`<authentication>`	
	`serverUrl=` `"http://spotserver/"`	Specify the URL to the Spotfire Server. This is the server to which the Spotfire Web Player will connect. This URL is entered in the installation wizard during the Spotfire Web Player installation but you can modify the URL in this element.
	`enableAutocomplete="false"`	Specify if passwords can be saved in the browser. Set this value to `true` to allow passwords to be saved. This also enables the login dialog to display auto complete suggestions for user names.
	`loginService`	Specify if the login service is enabled. The default setting is `enabled="true"`, which is required for Spotfire on the iPad. **Note** We recommend that you enable the `loginRequireSsl` attribute when `enabled="true"`.

6.2.2 User Interface Element

The following table contains details about the tags and attributes along with the values that you can modify in the `<userInterface>` element of the configuration file. This section corresponds to the part of the configuration file labeled "4" in the previous code sample.

Position	Tag (with default value)	Explanation
4	`<pages showLogout="true" />`	Specify if the **Log out** menu item is displayed. If `true`, the menu item is displayed in the top right menu of the Spotfire Web Player.
	`<pages showAbout="true" />`	Specify if the **About Spotfire Web Player** menu item is displayed. If `true`, the menu item is displayed in the top right menu of the Spotfire Web Player.
	`<pages showHelp="true" />`	Specify if the **Help** menu item is displayed. If `true`, the menu item is displayed in the top right menu of the Spotfire Web Player. When a user clicks **Help**, the Spotfire Web Player online help is launched.
	`<pages showUserName="true" />`	Specify if the Display Name or User Name should appear in the Spotfire Web Player user interface. The default value, `true`, suppresses the display. If you set this value to `false` you can expect the following behavior: • In the Library Browser, the Modified By value will be displayed. If `true`, the entire column is hidden. • In the Analysis Information dialog, the Modified By field will be displayed. • Any place in the user interface where the Display Name or User Name is suppressed by default will be displayed.
	`<diagnostics errorLogMaxLines="2000" />`	Specify the maximum number of lines from the error log files to display on the diagnostics page. Default value is `2000`, range is `1000 - 50000`.
	`<analysis>`	
	`showToolTip="true"`	Specify if highlighting tooltips should be shown in visualizations. Setting this value to `false` will increase performance.

	`showClose="true"`	Specify if the **Close** menu item is displayed. If `true`, the menu item is displayed in the top right menu of the Spotfire Web Player.
	`showToolBar="true"`	Specify if the menu and the **Refresh**, **Collaboration**, **Bookmark**, and **Filter** buttons in the tool bar are displayed. If `true`, the buttons are displayed in the tool bar of the Spotfire Web Player.
		Note If you set this value to `false`, users of the Spotfire Web Player will not be able to use the functionality made available through these controls.
		Note If you set both this value and the value for `showPageNavigation` to `false`, the entire grey, top bar of the Spotfire Web Player will not appear.
	`showAnalysisInformationTool="true"`	Specify if the **Analysis Information** menu item is displayed. If `true`, the menu item is displayed in the top right menu of the Spotfire Web Player.
	`showExportFile="true"`	Specify if the **Open in TIBCO Spotfire** menu item is displayed. If `true`, the menu item is displayed in the top right menu of the Spotfire Web Player.
	`showExportVisualization="true"`	Specify if the **Export Visualization Image** menu item is displayed. If `true`, the menu item is displayed in the top right menu of the Spotfire Web Player. This value also controls the display of the menu item in the **Visualization** menu.
	`showUndoRedo="true"`	Specify if the **Undo** and **Redo** menu items are displayed and if undo is available in the visualization. If `true`, the menu item is displayed in the top right menu of the Spotfire Web Player.
	`showDodPanel=""`	Specify the behavior of the Details-on-Demand (DoD) panel. If the value is: • empty (`""`), the DoD panel is displayed if the author of the analysis file chooses to display the DoD panel. • `false` the DoD panel is always hidden. • `true` the DoD panel is always displayed.

`showFilterPanel=""`	Specify the behavior of the Filter panel. If the value is: ● empty (`""`), the Filter panel is displayed if the author of the analysis file chooses to display the Filter panel. ● `false` the Filter panel is always hidden. ● `true` the Filter panel is always displayed.
`showPageNavigation="true"`	Specify if the Page tabs (or page links) in analyses are displayed. If you set this to `false` only the currently active Page as saved in the analysis will be displayed. **Note** If you set both this value and the value for `showPToolBar` to `false`, the entire grey, top bar of the Spotfire Web Player will not appear.
`showStatusBar="true"`	Specify if the status bar is displayed.
`showPrint="true"`	Specify if the **Print** menu item is displayed. If `true`, the menu item is displayed in the top right menu of the Spotfire Web Player.
`allowRelativeLinks="false"`	Specify if incomplete links in the Spotfire Web Player should be treated as relative to the library root directory. If `false`, incomplete links will be prepended with `http://`.
`<customHeader>`	
`enabled="false"`	Specify if the custom header with logo is displayed. Set this to `true` to enable the custom header file display.
`fileName="Header.htm"`	Specify the name of the file that contains the custom header. For more information about creating or modifying this file, see "Customize the Header Banner" on page 60.
`height="40"`	Specify the pixels for the height of the custom header.
`<closedAnalysis>`	
`showOpenLibrary="true"`	Specify if the **Open Library** link is displayed on the **Closed Analysis** page.
`showReopenAnalysis="true"`	Specify if the **Reopen Analysis** link is displayed on the **Closed Analysis** page.
`redirectToLibrary="true"`	Specify if the **Closed Analysis** page is displayed after an analysis is closed.
`<errorPage>`	

	`showOpenLibrary="true"`	Specify if the **Open Library** link is displayed on an error page.
	`showReopenAnalysis="true"`	Specify if the **Reopen Analysis** link is displayed on an error page.
	`<serverUnavaliable>`	
	`showOpenLibrary="true"`	Specify if the **Open Library** link is displayed on the Server Busy page.
	`showReopenAnalysis="true"`	Specify if the **Reopen Analysis** link is displayed on the Server Busy page.

6.2.3 Performance Element

The following table contains details about the tags and attributes along with the values that you can modify in the `<performance>` element of the configuration file. This section corresponds to the part of the configuration file labeled "5", "6", and "7" in the previous code sample.

Position	Tag (with default value)	Explanation
5	`<documentCache>`	
	`purgeInterval="300"`	Specify the number of seconds between server searches to identify unused, open documents (templates) to be purged. Default value is `300` seconds, range is `60` to `3600`.
	`itemExpirationTimeout="00:00:00"`	Specify the length of time, in the format HH:MM:SS, that a document can remain in the cache when no open analysis is using that document template. Default value is `00:00:00`, maximum value is `23:59:59`.
6	`<analysis>`	
	`checkClosedInterval="60"`	Specify how often, in seconds, the server should check if an analysis has been closed on the client. Default value is `60`, range is `60` to `300`.
	`closedTimeout="120"`	Specify how long, in seconds, an analysis session will stay alive on the server when a ping fails. Default value is `120`, range is `60` to `600`.
	`checkInactivityInterval="300"`	Specify how often, in seconds, the server should check if an analysis session has had no user activity, excluding pings. Default value is `300`, range is `60` to `12*3600`.

	`inactivityTimeout="Infinite"`	Specify the length of time, in the format HH:MM:SS, that an analysis session can be alive on the server when the no user activity has been detected, excluding pings. Default is `Infinite`, range is `00:01:00` to `Infinite`.
	`regularPollChangesInterval="500"`	Specify the base interval, in microseconds, from when a change is made on the client to when the client polls the server for a status update. Default value is `500`, range is `200` to `1000`.
	`maxPollChangesInterval="3000"`	Specify the maximum value, in microseconds, by which the poll interval in `regularPollChangesInterval` is increased for each try until this value is reached. Default value is `3000`, range is `1000` to `10000`.
	`pollLoadInterval="1000"`	Specify the interval, in microseconds, between polls when an analysis file is loading. Default value is `1000`, range is `1000` to `10000`.
	`needsRefreshInterval="15"`	Specify the frequency, in seconds, with which the client should ping or poll the server to keep the analysis alive. Default is `15`, range is `10` to `60`.
	`toolTipDelay="1000"`	Specify the length of time, in microseconds, that the client must wait before requesting a visualization highlighting tooltip from the server. Default value is `1000`, range is `200` to `3000`.
	`antiAliasEnabled="true"`	Specify if anti-aliasing is enabled. The default value is `true` and we recommend that you leave anti-aliasing enabled in order to produce visualizations that are clear and sharp. All graphics in the Spotfire Web Player are rendered with anti-aliasing enabled. However, anti-aliasing does impose a slight performance impact. The performance impact may become noticeable for visualizations that consist of a very large amount of graphical objects. If you encounter this rare situation, you can set this value to `false`.

	`useClearType="true"`	Specify if ClearType is enabled. The default value is `true` and we recommend that you leave ClearType enabled in order to produce clear and sharp text in visualizations. All graphics in the Spotfire Web Player are rendered with ClearType enabled. However, ClearType does impose a slight performance impact. The performance impact may become noticeable for certain visualizations. If your performance is in question, you can disable ClearType by setting this value to `false`.
	`documentStateEnabled="true"`	Specifies that the state of files is maintained between sessions. If this value is set to `true`, when users resume working on a file, the file will be in the state in which that user left the file.
	`undoRedoEnabled="true"`	Specify if the Undo and Redo functionality is enabled.
	`userServicesPoolEnabled="true"`	Specify if the user services pool should be enabled. Enabling the user services pool reduces the number of web service calls to the server because only one set of user services such as preferences and licenses, is created for each user. This is especially useful if the users are logged in to the Spotfire Web Player anonymously, which means that they are all technically logged in as the same user.
	`maxRenderTimeMs="60000"`	Specify the time limit for each request or render job is allowed to create an image on the Spotfire Web Player for a visualization. You can use this setting to prevent long running requests or jobs from making the Spotfire Web Player unresponsive. **Note** If an end user encounters a case where this setting times out they will receive the error, "The max rendering time (`maxRenderTimeMs`) was exceeded." The default value is 60 seconds in milliseconds, `60000`.
	`userPreferencesMaxAge="00:05:00"`	Specify the interval, in the format HH:MM:SS, for the preferences and licenses to be synchronized when additional users log in to the Spotfire Web Player. Default value is `00:05:00`.
7	`<hierarchicalClustering>`	

---

	maxInteractiveElements="2000"	Specify the maximum number of rows or columns of a hierarchical clustering that can be started interactively in the Spotfire Web Player. Default value is 2000.
	maxElements="30000"	Specify the maximum number of rows or columns of a hierarchical clustering that can run on the Spotfire Web Player. Scheduled updates can run hierarchical clustering up to this size. Default value is 30000.
	maxInteractiveJobs="2"	Specify the maximum number of interactive clustering jobs running in parallel. Default value is 2.
	cpuFactorInteractiveJobs="0.8"	Specify an estimate of the number of threads that clustering will use for interactive jobs on a multi-core server running Spotfire Web Player. Default value is 0.8.
	cpuFactorLargeJobs="0.5"	Specify an estimate of the number of threads that clustering will use for scheduled update jobs on a multi-core server running Spotfire Web Player. Default value is 0.5.
	nativeMemory="500" />	Specifies a memory limit, in MBytes, for the clustering algorithm. The default value 500 (MBytes) matches maxElements = 30000.

6.2.4 Spotfire Dxp Services Settings Element

The following table contains details about the tags and attributes along with the values that you can modify in the `<Spotfire.Dxp.Services.Settings>` element of the configuration file. This section corresponds to the part of the configuration file labeled "8" in the previous code sample.

Position	Tag (with default value)	Explanation
8	`<Spotfire.Dxp.Services.Settings>`	
	`<cookies autoTransfer="" />`	For a load balancer or proxy that requires specific cookies to be sent on all requests to the Spotfire Server, you should add the cookies in this value. Separate cookies with a semi-colon (;).

6.2.5 System Web Settings Element

The following table contains details about the tags and attributes along with the values that you can modify in the `<system.web>` element of the configuration file. This

section corresponds to the part of the configuration file labeled "8" in the previous code sample.

Position	Tag (with default value)	Explanation
	```<system.web>```	
	```<sessionState timeout="20" cookieless="UseCookies" />```	Specify the time limit in minutes for a user to be inactive on the Start page or in the Library browser. When the limit is reached, the user is logged out and automatically redirected to the logout page. Default value is 20 minutes.

6.2.6   Application Settings Element

The following table contains details about the tags and attributes along with the values that you can modify in the ```<applicationSettings>``` element of the configuration file. This section corresponds to the part of the configuration file labeled "9" in the previous code sample.

Position	Tag (with default value)	Explanation
9	```<applicationSettings>```	
	```<Spotfire.Dxp.Internal.Properties. Settings>```	
	``` ManifestDownloadTimeout Milliseconds```	Specify the manifest download time in milliseconds. This is the time the application waits before aborting an operation when the server does not respond. The default value is 60000.
	``` LibraryCache_Enabled```	Specify if caching of metadata for items in the library is enabled. Since metadata is retrieved from the cache instead of from the server caching reduces the number of web service calls to the server. The cache is unique for each user. Enabling this is especially useful if the users are logged in anonymously to the Spotfire Web Player as they are all technically logged in as the same user. The default value is true. **Note** If you are using scheduled updates, you should set this value to false.
	``` LibraryCache_MaxCacheTime```	Specify the length of time, in the format HH:MM:SS, for metadata to be cached. Default value is ten minutes, 00:10:00.
	```<Spotfire.Dxp.Data.Properties.Sett ings>```	

	`DataBlockStorageIOSizeKB`	Modify this setting to improve write performance on your Spotfire Web Player server with a RAID enabled storage systems. Set the value of this setting, in KB, to twice the RAID stripe in KB. Default value is `64`. **Note** You must enable the RAID write cache on the server.
	`DataOnDemand_MaxCacheTime`	Specify the length of time, in the format HH:MM:SS, for data on demand to be cached. This setting is only used if you configured data on demand to be cached on the Spotfire Web Player Default value is one hour, `01:00:00`.

	`AllowedWebRootFiles`	Provide the full path to files stored in the Spotfire Web Player installation directory or any of it's subdirectories that you want to access from the Spotfire Web Player. Separate entries with a semi-colon (`;`). All paths are relative to the `webroot` directory. For example `C:\Program Files\Tibco\Spotfire Web Player\6.0\`
		
		 Example:
		 `<value>`
		 `  ..\Logfiles\PerformanceCounter.txt;`
		 `  ..\Logfiles\Spotfire.Dxp.Web.log`
		 `</value>`

	`AllowedFilePaths`	Provide the full path to directories or files on a local disk, other than the Spotfire Web Player installation directory, that you want to access in the Spotfire Web Player.
		
		 Specify each file or directory in a separate `<string>` tag. For example:
		
		 `<value>`
		 `  <ArrayOfString>`
		 `    <string>`
		 `        C:\MyData\`
		 `    </string>`
		 `    <string>`
		 `        C:\Logs\spotfire.txt`
		 `    </string>`
		 `  </ArrayOfString>`
		 `</value>`

6.3   Language Support

This section covers how you can specify a language for the user interface in a browser and information about using Language Packs with Spotfire Web Player.

6.3.1   Specify Language Mappings

You can define a mapping from a language preference configured by users in the browser to one of the languages installed on the Spotfire Web Player server. For example, if your users have `French (Canada) [fr-CA]` as the highest preference language in their web browser, but the Spotfire Web Player uses `French (France) [fr-FR]`, you can specify that `[fr-FR]` should be used even if the end users have not added `[fr-FR]` to their list of supported languages in the browser.

To make this change you must add a new section to the Spotfire Web Player web configuration file.

The highest preference language in the web browser that is either listed among installed languages or listed in the language mappings in the configuration file is picked as the language for the user interface. However, if no browser language matches the languages listed in the language mappings section, the language specified by the IIS setting `<globalization>` is selected as long as this language is one of the installed languages. If a language cannot be mapped from any of these settings, `[en-US]` is selected.

Note Languages listed under `<installedLanguages>` cannot be overridden.

▶ **Specifying Language Mappings**

1   Use an XML editor to open the `web.config` file from the `webroot` directory, for example:

`C:\Program Files\Tibco\Spotfire Web Player\6.0\webroot\Web.config`

Note We recommend that you use an XML editor when you modify XML files. An XML editor has features to provide a clear view of the XML code and some text editors corrupt configuration files.

2   Add a new settings collection named `<languageMappings>`.

3   For each mapping from a browser language that is not directly supported, add a setting in the format:
`<add browserLanguage="en-GB" installedLanguageToUse="en-US"/>`.

4   Save `web.config`.

Important When you save changes to the `web.config` file, IIS automatically detects that the file has been modified and restarts the Spotfire Web Player application. Users who are logged into the Spotfire Web Player will be disconnected.

6.3.2   Language Packs

For information on how to deploy language packs for Spotfire Web Player, please refer to the "TIBCO Spotfire – Deploying and Using a Language Pack" manual.

If you deploy a Japanese or another double-byte language pack, or if you intend to use data containing characters from these languages, you might also need to install

---

Windows files for East Asian Languages from the "Regional and Language Option" on the Spotfire Web Player server.

6.4   Data from External Sources

TIBCO Spotfire can access data directly from the external sources Microsoft® SQL Server®, Microsoft® SQL Server® Analysis Services, Teradata®, and Oracle®. To be able to use analyses with data from these sources in Spotfire Web Player, you must specify the authentication method in the `web.config` file for how users will connect to the external data sources.

Locate the section below and enter information on the authentication method for each data source used.

```
<Spotfire.Dxp.Data.Access.Adapters.Settings>
<!--
    Different authentication modes can be set up for the various
    data sources. Valid modes are:
      WebConfig  To connect with credentials stored in
        Spotfire.Dxp.Web.Properties.Settings/DataAdapterCredentials
        below.
      Kerberos  To connect using Kerberos authentication.
      Prompt  To prompt the user for credentials.
      ServiceAccount  To connect as the account used to run
        the application pool in the IIS.
-->

  <setting name="WebAuthenticationMode" serializeAs="Xml">
    <value>
      <adapters>
        <adapter name="Spotfire.SqlServerAdapter" mode="Prompt"/>
        <adapter name="Spotfire.TeradataAdapter" mode="Prompt"/>
        <adapter name="Spotfire.OracleAdapter" mode="Prompt"/>
        <adapter name="Spotfire.SsasAdapter" mode="Prompt"/>
      </adapters>
    </value>
  </setting>
</Spotfire.Dxp.Data.Access.Adapters.Settings>
```

There are four alternatives for each data source. The authentication methods will differ depending on if the analysis was set up using Windows Authentication or Database Authentication.

Windows Authentication

- WebConfig – select this to force all users that are accessing a specific analysis connect to the external data source using the username and password specified in the DataAdapterCredentials section described later in this chapter.

- Kerberos – select this if your system is configured to authenticate users with Kerberos.

- Prompt – select this to prompt the users for a username and password for the external data source.

- ServiceAccount – select this to make all users connect to the external data source using the computer account or dedicated user account that is used to run the application pool in IIS on the Spotfire Web Player server.

Database Authentication

If an analysis is set up using database authentication, the username and password for the data source can be stored in the analysis file. If it is, the credentials specified in the analysis file will supercede the authentication method specified in the `web.config` file.

If the username and password are not stored in the analysis file, the user will be prompted for a username and password. The exception is if WebConfig is specified and an existing credentials profile is stored in the analysis, then the username and password specified in the DataAdapterCredentials section will be used.

If WebConfig was specified above, you must specify the username and password for a credentials profile in the DataAdapterCredentials section in the `web.config` file, shown below. You can add multiple profiles with different credentials.

```
<!--
Credentials for the data adapters. Each entry within the setting/
value/credentials section should be in this format:

            <entry profile="profile_name">
              <username>user</username>
              <password>password</password>
            </entry>

For integrated security, the username should be in the DOMAIN\user
format.

The profile is an arbitrary string. To use the credentials in an
analysis, enter the same profile in the credentials tab of the data
connection properties dialog in TIBCO Spotfire.
-->

<setting name="DataAdapterCredentials" serializeAs="Xml">
  <value>
    <credentials>
    </credentials>
  </value>
</setting>
```

The credentials profile is used to connect a username and password for an external data source to a specific analysis file, without storing the actual username and password in the analysis. The name of the profile is specified in the `web.config` section above, and in the analysis file. To specify which profile to use for a connection in an analysis, save the profile name in the Data Connection Properties dialog in TIBCO Spotfire.

Example: All users of the Spotfire Web Player should connect to a Teradata connection using the username `terauser` and the password `terapassword`, but it is not appropriate to store these credentials in the analysis file that uses the Teradata connection.

To configure this, you should add a credentials profile in the `web.config` section above with the profile name `teradata`, the username `terauser`, and the password

`teradata`. Then, each analysis file with the Teradata connection is saved with the credentials profile `teradata` that you specified in the **Credentials** tab in the **Data Connection Properties** dialog in TIBCO Spotfire.

6.5   TIBCO Spotfire Statistics Services

If statisticians or analysts in your company use data functions or predictive analytics tools in TIBCO Spotfire as a part of an analysis files and Spotfire Web Player will be used with these analysis files you must configure properties in this section so that TIBCO Spotfire™ Statistics Services can execute the data function or predictive analytic function. Spotfire Web Player does not include any statistical engine such as MATLAB, SAS, S-PLUS, R, or Tibco Enterprise Runtime for R (TERR). Rather, it relies on the engine configured in Spotfire Statistics Services and specified in Spotfire Professional application. For more information, see the "TIBCO Spotfire Statistics Services Installation and Administration Guide" and read the "Configuring TIBCO Spotfire to use TIBCO Spotfire Statistics Services" section.

If Spotfire Statistics Services requires authentication, you must specify these authentication settings in the `web.config` file by entering the Spotfire Statistics Services URL along with the username and password for Spotfire Statistics Services. You can add additional rows to each of the settings to specify URLs, usernames, and passwords for several Spotfire Statistics Services.

Note The URLs must be specified exactly the same for the Spotfire Web Player server and the Spotfire Server. For example, you must use FQDN in both cases or neither case.

Enter information in the places indicated with bold format in the following code:

```
<Spotfire.Dxp.Web.Properties.Settings>
  ...
  <setting
      name="TibcoSpotfireStatisticsServicesURLs"
      serializeAs="Xml">
    <value>
        <ArrayOfString>
          <string></string>
        </ArrayOfString>
    </value>
  </setting>
  <setting
      name="TibcoSpotfireStatisticsServicesUsernames"
      serializeAs="Xml">
    <value>
        <ArrayOfString>
          <string></string>
        </ArrayOfString>
    </value>
  </setting>
  <setting
      name="TibcoSpotfireStatisticsServicesPasswords"
      serializeAs="Xml">
    <value>
        <ArrayOfString>
          <string></string>
        </ArrayOfString>
    </value>
```

```
        </setting>
</Spotfire.Dxp.Web.Properties.Settings>
```

6.6   Scheduled Updates

What are Scheduled Updates?

Scheduled updates are an approach that you can use to reduce the time it takes for a user to open certain analysis files. This is done by preloading analysis files on the Spotfire Web Player server before a user attempts to open them.

Scheduled updates are most effective if you have certain analysis files with linked data (from an information link or any other linkable data source), that are updated regularly with large amounts of new data. Often such updates occur during the night, and the following morning users want to open the corresponding analysis files to view the latest data. If that data has already been preloaded the analysis will open much faster.

The same goes for a large analysis with lots of data, that users might open several times during the day to quickly check for figures or similar. Instead of having to load this into memory every time a user opens the analysis, you can make sure this analysis is always available in memory, ensuring a rapid response for the users.

Scheduled updates let you configure:

- Which analysis files should be pre-loaded.

- When these analysis files should be pre-loaded and kept in memory on the Spotfire Web Player server.

Event-Driven Updates

It is possible for the Spotfire Web Player to update the pre-loaded analysis in two ways. One is to specify that every, for instance 30 minutes, an update is to be made. The other is to use event-driven updates, which means that the update is triggered, not by passed time, but by a message sent from a web service or TIBCO Enterprise Message Service.

To enable event-driven updates, enable scheduled updates. Then apply the appropriate event-driven update settings to the `web.config` file ("Edit the Configuration File" on page 83) and configure and start the keep alive service (See "Configure and Start the Keep Alive Service" on page 89.).

Note For information on TIBCO Enterprise Message Service and details on how to set it up, please refer to the **TIBCO Enterprise Message Service User's Manual**.

Workflow for Scheduled Updates

1   An analyst works with TIBCO Spotfire. She creates an analysis that shows the sales results for the previous day. The data in this analysis comes from an information link which she has created. This information link opens data from a database table, which is updated each midnight with the sales data for the day that has passed. She saves this analysis in the Spotfire Library.

> **Note** The data does not have to come from an information link, but can come from any linkable data source.

2   The administrator of the TIBCO Spotfire Web Player server, receives a call from the analyst asking him to set up a scheduled update for the analysis file she just created. The analyst wants to make sure this analysis is preloaded each morning when the sales department comes to work and starts their day by checking the results from the previous day.

3   The administrator configures the TIBCO Spotfire Web Player. He adds the analysis file to the list of analyses to be scheduled for updates. He sets it to be automatically loaded at 4 am in the morning since he knows the database will be updated at midnight. This should be enough time to get the analysis loaded in memory before people come to work and attempt to open the analysis. He also determines that it should be continually kept in memory for the remainder of the working day; until 8 pm.

     The administrator also needs to specify a "user" that will automatically log into the TIBCO Spotfire Server and access the Spotfire Library in order to preload the analysis. Technically, this user needs access to the file and any other that is scheduled for updates. However, the administrator is careful to pick a user account whose user rights are as limited as possible (see also *Concerning Prompted and Personalized Information Links* below).

4   The administrator tells the analyst that the analysis is now scheduled for updates as requested. The analyst sends an e-mail to the sales department with the URL to the new analysis and tells them that from now on they can check the sales figures from the previous day by clicking the link.

5   At midnight, the company database is updated with the sales figures that were reported during the day. At 4 am, the scheduled update is activated on the TIBCO Spotfire Web Player and the analysis is loaded into memory. It loads the new data from the company database and bases all graphs and results on this.

6   The following morning, the sales people come into the office or turn on their laptops from home. They check their e-mail, read the message from the analyst, and click the link. The web browser launches, and quickly the analysis is displayed on screen, showing the sales results for the previous day. Since the data is already preloaded on the server, there is no waiting time for it to load from the company database.

7   The next midnight the company database will be updated with new numbers. At 4 am the analysis will be preloaded with the new data on the TIBCO Spotfire Web Player server and the sales people can access this the next morning as usual.

If a user should have the analysis open in his web browser overnight, a small icon will appear on the screen after the scheduled update has been performed on the server.
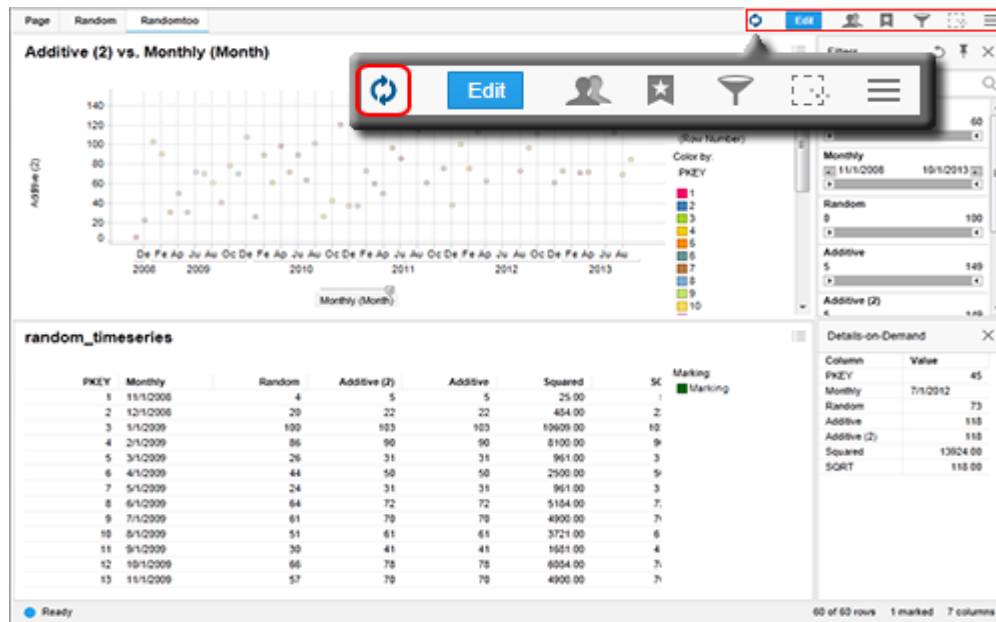
This will tell the user that there is an updated version of the analysis available, and clicking on the icon will refresh the analysis with the latest data.

Concerning Prompted and Personalized Information Links

Scheduled Updates are mainly intended for use with analyses that have been set up using normal information links to load data.

If you set up scheduled updates for an analysis that is based on data from a prompted or personalized information link, there are some issues you should be aware of.

Whenever a user opens an analysis that is based on a prompted information link, the user will select a certain view of the data to be loaded. In the same manner, whenever a user opens an analysis based on a personalized information link, the data loaded will be determined by the user rights of the user who logs in.

However, when a scheduled update of this file occurs, that update will cause the analysis to reload based on the prompted values specified when originally saving the file, and for the user rights of a user that the administrator set up to programmatically run the scheduled update.

This means that users with an analysis already open, will see a different selection of data the next time they update the analysis, since the scheduled update has in fact updated the underlying data on the server.

You need to be especially careful if you are setting up scheduled updates for analyses with personalized information links. If the user you specify for the scheduled updates has access to more data than the intended users of the analyses, then these users might see more data than they have access to (i.e., they will see all the data that the user specified for scheduled updates has access to).

Concerning Sharing Routines for Linked Data

When saving an analysis using linked data you can set up sharing routines. Combining such sharing routines with scheduled updates can provide additional granularity when data should be loaded.

A basic scenario could be that you have an analysis that loads its data from a link to one single data table. When saved to the library the sharing routines for the corresponding data table are set to "always load new data". This means that every time a scheduled update occurs, the analysis will be updated with the latest data from the linked data table. All end users that happen to have the analysis open in their web browsers will see the update icon, and when clicked on, the analysis on their screens will be updated with new data. All end users will share the same data (and RAM) on the server.

However, using sharing routines and multiple linked data tables, you can set up more detailed configurations.

Say you have an analysis that uses two linked data tables. One links to a huge amount of data that is only updated once every midnight. The other data table is smaller, but is updated every ten minutes.

You want to set up a scheduled update that keeps this analysis in memory the entire working day, but continually updates with the latest data. However, it is only the small data table that you must reload and update every ten minutes. Reloading the huge data table every ten minutes would be unnecessary since that will remain unchanged the entire day.

Therefore, when saving the analysis to the library you can set sharing routines for the huge data table to "always share" and sharing routines for the small data table to "always load".

You then set up a scheduled update for the analysis file to load and update every ten minutes, starting at 4 am and ending at 10 pm.

What will happen is that the first time the scheduled update is run (4 am) both the huge data table and the small data table will be loaded as the analysis is opened and kept in memory.

Every ten minutes the analysis file will be updated, but only the small data table will be reloaded since the sharing routines specify that the huge data table will only be loaded **the first time** the analysis is opened. The sharing routine "always share" means that the data table will only be loaded the first time someone opens the analysis (in this case the first scheduled update).

Users opening the analysis in their web browsers during the day will get a quick response from the server since the analysis is already in memory. Every ten minutes the scheduled update will run on the server and the end users will see the icon stating that they can update their analysis by clicking on it. Doing so will update the analysis with the latest data.

The scheduled update will be fast, since it only reloads the small data table and not the huge data table.

6.6.1   Set up Scheduled Updates

There are three steps to setting up scheduled updates. These will be explained in more detail below.

If you want to upgrade an earlier version of an existing schedule, see "Upgrade an Existing Schedule" on page 92.

▶ **Setting up Schedules Updates**

1   Edit `web.config`.

2   Configure the Update Schedule.

3   Configure and Start the Keep Alive service.

6.6.1.1   Edit the Configuration File

The first thing to do is to enable scheduled updates and disable library caching in the configuration file. There are also a few settings you can modify to configure how you want scheduled updates to work in your environment.

Use an XML editor to open the `web.config` file from the `webroot` directory, for example:

```
C:\Program Files\Tibco\Spotfire Web Player\6.0\webroot\Web.config
```

Note We recommend that you use an XML editor when you modify XML files. An XML editor has features to provide a clear view of the XML code and some text editors corrupt configuration files.

Example:

```
<configuration>
  ...
  <spotfire.dxp.web>
    <setup>
     ...
     <scheduledUpdates
       enabled="true"
       useLibrary="true"
       libraryFileName="ScheduledUpdates"
       settingsFile="App_Data\ScheduledUpdates.xml"
       concurrentUpdates="2"
       updateIntervalSeconds="60"
     >
       <forcedUpdate enabled="true" maximumRejectedUpdates="2" />
       <externalUpdate keepAliveMinutes="10">
         <webService enabled="false" />
         <ems
           enabled="false"
           serverUrl=""
           topic=""
           clientId=""
           reconnectAttemptCount="10"
           reconnectAttemptDelayMilliseconds="1000"
           reconnectAttemptTimeoutMilliseconds="1000"
```

```
            />
        </externalUpdate>
      </scheduledUpdates>
    </setup>
   ...
  </spotfire.dxp.web>
  ...
  <applicationSettings>
    ...
    <Spotfire.Dxp.Internal.Properties.Settings>
      ...
      <setting name="LibraryCache_Enabled" serializeAs="String">
        <value>False</value>
      </setting>
      ...
    </Spotfire.Dxp.Internal.Properties.Settings>
    <Spotfire.Dxp.Web.Properties.Settings>
      <setting name="ScheduledUpdatesUsername" serializeAs="String">
        <value>ScheduledUpdatesUsername</value>
      </setting>
      <setting name="ScheduledUpdatesPassword" serializeAs="String">
        <value>ScheduledUpdatesPassword</value>
      </setting>
      <setting name="EmsUpdateUsername" serializeAs="String">
        <value>EmsUpdateUsername</value>
      </setting>
      <setting name="EmsUpdatePassword" serializeAs="String">
        <value>EmsUpdatePassword</value>
      </setting>
    </Spotfire.Dxp.Web.Properties.Settings>
    ...
  </applicationSettings>

  <!--
      EMS Updates:
      spotfire.dxp.web/scheduledUpdates/externalUpdate/ems section
      must be filled in to use this.
      This is the username and password for the user that connects
      to the EMS server.
  -->
```

The following table contains details about the tags and elements that you can modify in the configuration file as listed in the previous code sample

Key	Description
`<scheduledUpdates>`	
`enabled`	To enable Scheduled Updates set this key to `true`.
`useLibrary`	To save the Scheduled Updates settings in the library instead of locally, make sure that this key is set to `true`.
`libraryFileName`	Specifies the name of the file that contains the Scheduled Updates settings in the library.
`settingsFile`	The relative path to the `ScheduledUpdates.xml` file from the `webroot` directory. This key is filled in automatically by default.

`concurrentUpdates`	The maximum number of concurrent updates that can be executed at the same time. This is used to limit resources used by the update mechanism. Default value is `2`, min value is `1` and max value is `10`.
`updateInterval Seconds`	How often the ScheduledUpdates.xml file should be read to check if any updates should be run. This is set in seconds. Default value is `60`, min value `30`, and max value `3600` (=one hour).
`<forcedUpdate>`	
`enabled`	It is possible to force updates upon users even though the analysis is set to notify the users. This is useful if someone has left an analysis open for a long time and you want to avoid numerous versions of the analysis to be kept simultaneously. To enable forced updates set this key to `true`.
`maximumRejected Updates`	Specify the number of times a user can be notified of new updates without accepting them, before the update is forced on the user.
`<externalUpdate>`	
`keepAliveMinutes`	If a schedule has not been set up for when a file is to be pre-loaded, specify the number of minutes the file should be kept alive.
`<webService>`	
`enabled`	To enable updates triggered by a web service, set this key to `true`. **Note** To enable updates triggered by a web service, `scheduledUpdates` must also be enabled and configured.
`<ems>`	**Note** For information on TIBCO Enterprise Message Service and details on the following settings, please refer to the **TIBCO Enterprise Message Service User's Manual**.
`enabled`	To enable updates triggered by a message sent from TIBCO Enterprise Message Service, set this key to `true`. **Note** To enable updates triggered by ems, `scheduledUpdates` must also be enabled and configured.
`serverUrl`	Specify the URL and, if applicable, the port to the EMS server.
`topic`	Specify the topic that the EMS durable subscriber should listen to.

`clientId`	By default, the EMS durable subscriber uses the computer name as the client id. Specify another client id here to be able to use more than one on the same computer.
`reconnectAttempt Count`	Specify the number of reconnect attempts to be made if a connect fails. By default this number is set to `10`.
`reconnectAttempt DelayMilliseconds`	Specify the delay for the reconnect attempts. By default this is set to `1000` milliseconds.
`reconnectAttempt Timeout Milliseconds`	Specify the timeout for the reconnect attempts. By default this is set to `1000` milliseconds.
`<applicationSettin gs>`	
`<Spotfire.Dxp.In ternal.Propertie s.Settings>`	
`LibraryCache_Ena bled`	If caching of metadata for items in the library is enabled metadata is retrieved from the cache instead of from the server. When this is enabled the schedules are not carried out as specified but are delayed until the library cache is updated. Set this value to `false`.
`<Spotfire.Dxp.Web. Properties.Setting s>`	
`ScheduledUpdates Username`	The name of the user that will be used to access the TIBCO Spotfire Server when updating analysis files. This user must have user rights on the Spotfire Server to access the relevant files, and be a member of the **Scheduled Updates Users** group on the server. If you have configured the Spotfire Web Player to use Anonymous (Preconfigured) Access, this user must be the same user you specified for Impersonation (`ImpersonationUsername`). The user name needs to contain the domain, so enter the value on the syntax: domain\username. Enter this information in the `<value>` tags. **Note** If you have configured the Spotfire Web Player to use Client Certificate authentication, this value should be left empty. To specify a scheduled update user with client certificates, see "Client Certificate" on page 34. To encrypt this credential, see "Encrypt Usernames and Passwords" on page 95.

`ScheduledUpdates Password`	The password for the user that will be used to access the TIBCO Spotfire Server when updating analysis files.
	If you have configured the Spotfire Web Player to use Anonymous (Preconfigured) Access, this must be the password for the user you specified for Impersonation (`ImpersonationPassword`).
	Enter this information in the `<value>` tags.
	Note If you have configured the Spotfire Web Player to use Client Certificate authentication, this value should be left empty. To specify a scheduled update user with client certificates, see "Client Certificate" on page 34.
	To encrypt this credential, see "Encrypt Usernames and Passwords" on page 95.
`EmsUpdateUsername`	The name of the user that will be used to access the EMS server.
	Enter this information in the `<value>` tags.
`EmsUpdatePassword`	The password for the user that will be used to access the EMS server.
	Enter this information in the `<value>` tags.

6.6.1.2 Configure the Update Schedule

To set scheduled updates for different analyses, use the Update Schedule dialog in the library.

To be able to configure scheduled updates for different analyses, the user must be a member of the group **Administrator** or the group **Web Player Administrator** on the server. Make sure that the user has the necessary access rights to the appropriate library items.

Note Setting up scheduled updates using the dialog in the library will overwrite locally stored `ScheduledUpdates.xml` files. The only way to upload locally stored scheduled updates is to save the .xml file in a separate location before installing the Spotfire Web Player. Then copy the old `.xml` file to the directory **TIBCO Spotfire Web Player Installer** before enabling scheduled updates the first time. This will upload the existing scheduled updates to the library.

▸ **To Configure the Update Schedule**

1 Go to the library by entering the address of the Spotfire Web Player server in the web browser.

   Note To be able to configure the update schedule, you must be logged in as an administrator or a Spotfire Web Player administrator.

2 Click **Scheduled Updates** in the top right corner.

3   If there are existing files scheduled for updates, click them to edit their update schedule or click **Add analysis file**.

4   Browse to the file to set up an update schedule for and click on it to display the update schedule dialog:

5   Select if the updates are to be done automatically or if the users are to be notified that a new version is available and let them update manually.

6   Select the days and the hours between which you want the analysis file to be pre-loaded on the server.

Note The time is set for the time zone of the web server. If the user configuring the schedule is located in another time zone, the current time of the web server is displayed. This is to help the user calculate the appropriate times for the schedule.

Note If you want different settings for different days or between different hours, click **Add an additional schedule** to add another one.

7   Select how often you want Spotfire Web Player to check if the analysis file or its underlying data has been changed, and if so, update the pre-loaded instance.

Comment: If you set this value too low, Spotfire Web Player will check for updates before the previous update is finished loading. The load time depends on the size of the analysis file and the amount of data it links to.

8   Click **Save**.

Note We recommend that when you set up scheduled updates that you reserve a window of at least one hour each night when no updates are scheduled. As long as no other analyses files are open IIS can recycle itself, clean up resources, and free memory. This recycle process will improve overall performance. If there are open Spotfire Web Player analyses, those connections will keep the server up, because of the values in `NeedsRefresh` and `inactivityTimeout` which are designed to keep the analysis alive. The value in `NeedsRefresh` is, by default, `15` seconds. The default value for `inactivityTimeout` is `infinite`. If you are considering overall performance, you can modify these values to allow IIS to run a recycle process.

6.6.1.3 Configure and Start the Keep Alive Service

The default setting for IIS is to shut down the web application if there has not been a connection to it in the last 20 minutes. This behavior prevents the Scheduled Updates from running their tasks and keeping the specified analysis files instantiated in memory. To avoid this, a windows service will read the configuration file and ping the Spotfire Web Player to make sure that IIS is running during the periods configured in the schedules.

Note IIS needs to periodically restart itself to clear up free memory, so it is recommended to give IIS at least an hour of free time every 24 hours.

When the Spotfire Web Player was installed, a Windows service named `Spotfire.Dxp.Web.KeepAlive.exe` was installed in the `Tools` directory of the Spotfire Web Player server. For example:

```
C:\Program Files\TIBCO\Spotfire Web Player\6.0\webroot\bin\Tools
```

The service is not enabled during the Spotfire Web Player installation and configuration. You must manually enable the service after you have saved your final settings in the configuration file, `Spotfire.Dxp.Web.KeepAlive.exe.config`, which is located in the same directory.

Note We recommend that you use an XML editor because some text editors corrupt configuration files. An XML editor will also provide a more clear view of the XML code.

Example:

```
<configuration>
  ...
    <applicationSettings>
      <Spotfire.Dxp.Web.KeepAlive.Properties.Settings>
       <setting name="SettingsFilePath" serializeAs="String">
         <value>
           C:\Program Files\TIBCO\Spotfire Web Player\6.0\
           webroot\App_Data\ScheduledUpdates.xml
         </value>
       </setting>
       <setting name="PingIntervalMinutes" serializeAs="String">
         <value>10</value>
       </setting>
       <setting name="WindowsUserName" serializeAs="String">
         <value>WindowsUserName</value>
       </setting>
       <setting name="WindowsPassword" serializeAs="String">
         <value>WindowsPassword</value>
       </setting>
       <setting name="WebPlayerUrl" serializeAs="String">
         <value>
           http://localhost:80/SpotfireWeb/KeepAlive.ashx
         </value>
       </setting>
       <setting name="EMS_Enabled" serializeAs="String">
         <value>False</value>
       </setting>
       <setting name="EMS_ServerUrl" serializeAs="String">
         <value>EMSServerUrl</value>
       </setting>
```

```
<setting name="EMS_Topic" serializeAs="String">
  <value>EMSTopic</value>
</setting>
<setting name="EMS_UserName" serializeAs="String">
  <value>EMSUserName</value>
</setting>
<setting name="EMS_Password" serializeAs="String">
  <value>EMSPassword</value>
</setting>
<setting
  name="EMS_ReconnectAttemptCount"
  serializeAs="String"
>
  <value>10</value>
</setting>
<setting
  name="EMS_ReconnectAttemptDelayMilliseconds"
  serializeAs="String"
>
  <value>1000</value>
</setting>
<setting
  name="EMS_ReconnectAttemptTimeoutMilliseconds"
  serializeAs="String"
>
  <value>1000</value>
</setting>

</Spotfire.Dxp.Web.KeepAlive.Properties.Settings>
</applicationSettings>
<!-- Error logging and statistics -->
<log4net>
  <appender
    name="FileAppender"
    type="log4net.Appender.RollingFileAppender"
  >
    <file
      value="C:\Program Files\TIBCO\Spotfire Web Player\6.0\
      Logs\Spotfire.Dxp.Web.KeepAlive.log"
    />
```

Most of the information in this configuration file has already been filled in automatically during installation. However, you should verify that the information is correct and as desired. Enter the information in the `<value>` tags.

Depending on the type of authentication you have configured for your Spotfire Web Player you must also configure the `WindowsUserName` and `WindowsPassword` attributes accordingly (see below).

Key	Description
SettingsFilePath	The path to the `ScheduledUpdates.xml` file. This is by default the `webroot` directory of the Spotfire Web Player server.
PingIntervalMinutes	This setting determines how often the Spotfire Web Player should be pinged. Do not set this to more than half the time of the "IdleTime-out" settings of the Spotfire application pool in IIS. Specify this in minutes.

`WindowsUserName`	If IIS running the Spotfire Web Player, is set to Anonymous login; leave this value empty. The Keep Alive service will then be run using the Local System account.
	If IIS running the Spotfire Web Player is set to Basic Authentication, enter the user name of a user that has the user rights to access IIS in order for the ping to reach the Spotfire Web Player. It must be a valid Windows account that can access the web application.
	The user name needs to contain the domain, so enter the value in the format: `domain\username`
`WindowsPassword`	If IIS running the Spotfire Web Player is set to Anonymous login, leave this value empty.
	If IIS running the Spotfire Web Player is set to Basic Authentication, enter the password for the corresponding user.
`WebPlayerUrl`	The URL to the `KeepAlive.ashx` file on the Spotfire Web Player server that you want to keep alive. Most often this is `localhost`.
`EMS_Enabled`	The value should be `true` if updates triggered by a message sent from TIBCO Enterprise Message Service is enabled.
	Note For information on TIBCO Enterprise Message Service and details on the following settings, please refer to the **TIBCO Enterprise Message Service User's Manual**.
`EMS_ServerUrl`	The URL and, if applicable, the port to the EMS server.
`EMS_Topic`	The topic that the EMS durable subscriber should listen to.
`EMS_UserName`	The name of the user that will be used to access the EMS server.
`EMS_Password`	The password of the user that will be used to access the EMS server.
`EMS_Reconnect AttemptCount`	The number of reconnect attempts to be made if a connect fails. By default this value is `10`.
`EMS_Reconnect AttemptDelay Milliseconds`	The delay for the reconnect attempts. By default this value is `1000` milliseconds.
`EMS_Reconnect AttemptTimeout Milliseconds`	The timeout for the reconnect attempts. By default this value is `1000` milliseconds.
`FileAppender`	The path to the directory where the log file for the keep alive service will be stored.

Now that the `Spotfire.Dxp.Web.KeepAlive.exe.config` file has been configured, you can start the Keep Alive service.

Note If you make any changes to the configuration file later, you must restart the service for them to take effect.

▶ **Starting the Keep Alive Service**

1   Select **Start > Administrative Tools > Services**.

2   Double-click on the service "**TIBCO Spotfire Web Player Keep Alive Service**".

3   Set **Startup Type** to **Automatic**.

4   Start the service.

Comment: The Keep Alive service will create a log at:
              `C:\Program Files\TIBCO\Spotfire Web Player\6.0\Logfiles\Spotfire.Dxp.Web.KeepAlive.log`

5   The Scheduled Updates are now active.

Comment: You can review the `KeepAlive.log` to verify that it is working.

6.6.2 Upgrade an Existing Schedule

We recommend that in order to keep the scheduled updates for Spotfire Web Player 6.0 you should keep them in the library. You can do this by setting the attribute `useLibrary` to `true` in `web.config`. However, if you have an existing schedule that you want to use in the new installation, it is important to follow the instructions below.

▶ **Upgrading an Existing Schedule**

1   Before uninstalling the old version, make a backup of the old `ScheduledUpdates.xml`, located in the `Spotfire Web Player\5.5\webroot\app_data` directory.

2   Copy the `ScheduledUpdates.xml` file to the installation media directory and replace the existing, empty file.

3   Install Spotfire Web Player 6.0.

4   The first time the Spotfire Web Player site starts it will read the installed schedule file, in `Spotfire Web Player\6.0\webroot\app_data` directory, and upload the content to the library.
Note This upload will only be done once for a library, if the file has already been uploaded, the contents in ScheduleUpdates.xml in the `app_data` directory will be overwritten by the content already existing in the library. Therefore, always keep a backup of the file.

Use the Update Schedule dialog in the library to make changes to the scheduled updates.

6.7 Resource Monitoring to Improve Performance

Resource monitoring is a way to ensure good performance to the users of the Spotfire Web Player when the server load gets too high. It allows you to configure threshold values that prevent users from opening new files if these threshold values are exceeded. In effect, it ensures good performance for users already working with analyses on the Spotfire Web Player, while temporarily denying users the ability to open analyses when the server is under heavy load.

To enable resource monitoring you must set `siteLimitations` to `enabled="true"` in the configuration file and add at least one threshold value. If at least one of the threshold values is exceeded, additional users will be prevented from opening analyses.

To modify the configuration file, use an XML editor to open the `web.config` file from the `webroot` directory, for example:

```
C:\Program Files\Tibco\Spotfire Web Player\6.0\webroot\Web.config
```

Note We recommend that you use an XML editor when you modify XML files. An XML editor has features to provide a clear view of the XML code and some text editors corrupt configuration files.

The `web.config` settings have the following default values:

```
<spotfire.dxp.web>
  ...
  ...
   <performance>
    <siteLimitations enabled="false"
                     minimumAvailableMb="Infinite"
                     maximumOpenAnalyses="Infinite" />
```

Key	Description
`enabled`	Enable the server limitation function by setting this to `true`.

`minimumAvailableMb`	This value is the threshold when the Spotfire Web Player server will deny additional users attempting to open an analysis.
	It is specified as "available megabytes of free RAM left for the Spotfire Web Player to use before it starts to swap to disk". This is not the same as the number of Mb available in the computer, since the Spotfire Web Player tries to swap out memory to disk if less than 15% memory is left in the server.
	Recommended value: A good value to try first is `50` Mb. A higher value gives better performance for the users, but fewer people can open files if the limit is reached. Also, a higher value can sometimes affect the .NET framework which will not release its memory if there is too much available on the computer.
	The default value is `Infinite` which means that no resource monitoring will be performed for this attribute.
	Note Specified values should be numeric only. That is, `50` Mb is specified as `50` in the `web.config` file.
`maximumOpenAnalyses`	Users will be prevented from opening analyses if the number of open analyses is above or equal to this setting.
	Recommended value: This is very dependent on the size of the analysis files that are used and if users open the same (sharing) or different analyses. If you are unsure, leave this at the default `Infinite` value and just use the `minimumAvailableMb` setting.
	Note Analyses opened by Scheduled Updates will not be counted towards this limit.

When you have completed modifying the `web.config` file you should save the file. The resource monitoring changes take effect as soon as you save the file.

Logging

To help you determine the threshold values, you can enable the Spotfire Web Player log to state the actual performance values that the settings are compared against. This is done by first enabling `siteLimitations` in the Spotfire Web Player configuration file (`web.config`) and then adding the `<SiteResourceMonitor>` element below to the `log4net.config` file. It is located in the `webroot\App_data` directory of the installation.

```
<logger name="Spotfire.Dxp.Web.SiteResourceMonitor">
  <level value="DEBUG" />
</logger>
```

The Spotfire Web Player log will then add an entry to the log every time a user opens an analysis. This can be viewed by opening the log file or viewing it in the diagnostics page.

Customize the Server Unavailable Page

When a user who attempts to open an analysis is denied the ability to do so, a web page will be displayed stating that the "Server has reached maximum number of open analyses. Please try again later."

You can replace this text with your own custom HTML snippet.

Create a file named `ServerUnavailable.htm`, and place it in the `App_Data` directory:

`webroot\App_Data\ServerUnavailable.htm`

The HTML should not contain any `<Head>` or `<Body>` elements, just the HTML body content.

6.8   Encrypt Usernames and Passwords

All usernames and passwords specified in the `<Spotfire.Dxp.Internal.Properties.Settings>` part of the `web.config` file can be encrypted. These include:

- Username/Password for Impersonation

- Username/Password for Proxy

- Username/Password for Scheduled Updates

To encrypt the credentials specified here, use the standard `aspnet_regis.exe` tool found in ASP.NET.

```
C> aspnet_regiis.exe -pef "applicationSettings/
Spotfire.Dxp.Web.Properties.Settings" "<path_to_web_application>" -
prov "DataProtectionConfigurationProvider"
```

Example:

```
C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -
pef "applicationSettings/Spotfire.Dxp.Web.Properties.Settings"
"C:\Program Files\TIBCO\Spotfire Web Player\6.0\webroot" -prov
"DataProtectionConfigurationProvider"
```

To decrypt the credentials use the following syntax:

```
C> aspnet_regiis.exe -pdf "applicationSettings/
Spotfire.Dxp.Web.Properties.Settings" "<path_to_web_application>"
```

The `web.config` file is encrypted using the machine key of the Spotfire Web Player server the file is residing on. This means that you cannot move the `web.config` to another computer as it will only work on the computer you encrypted it on.

6.9   Configure Maximum Size for File Upload

The default settings for file upload in the configuration file prevent users from working with a data file that exceeds five megabytes (5 MB). To change this behavior you must set both `maxRequestLength` and `maxAllowedContentLength` settings in the configuration file. File upload is limited by both settings but the smaller setting will take precedence.

Users will encounter this limit in the following cases:

- Creating a new analysis from data file.

- Adding or replacing data from a data file to an open analysis.

- Opening an analysis file (.dxp) from disk.

Examples

Default values of 4 Mb and 28.6 Mb (approximately).

```
<!--<location path="Upload.aspx">
  <system.web>
    <httpRuntime maxRequestLength="4096"/>
  </system.web>
  <system.webServer>
    <security>
      <requestFiltering>
        <requestLimits maxAllowedContentLength="30000000" />
      </requestFiltering>
    </security>
  </system.webServer>
</location>-->
```

Settings to allow uploading files that are slightly smaller than 10 Mb.

```
<!--<location path="Upload.aspx">
  <system.web>
    <httpRuntime maxRequestLength="10240"/>
  </system.web>
  <system.webServer>
    <security>
      <requestFiltering>
        <requestLimits maxAllowedContentLength="10485760" />
      </requestFiltering>
    </security>
  </system.webServer>
</location>-->
```

▸ **Configuring maximum size for file upload**

1   Use an XML editor to open the `web.config` file from the `webroot` directory, for example:

```
C:\Program Files\Tibco\Spotfire Web Player\6.0\webroot\Web.config
```

Note We recommend that you use an XML editor when you modify XML files. An XML editor has features to provide a clear view of the XML code and some text editors corrupt configuration files.

2 Find the `<location>` element associated with `maxRequestLength="10240"`, copy the element, and then delete the start and end comment strings, as shown below:

Default	Edited
`<!--<location path="Upload.aspx">`	`<location path="Upload.aspx">`
`</location>-->`	`</location>`

3 Modify the settings for `maxRequestLength` (in KB) and `maxAllowedContentLength` (in bytes) to fit your needs.

4 Save `web.config`.

6.10 Configure the Spotfire Web Player Using FIPS

If you want to run the Spotfire Web Player server on a computer that has FIPS, Federal Information Processing Standard, enabled, an addition must be made to the configuration file.

▶ **Configuring web.config for Use With FIPS**

1 Use an XML editor to open the `web.config` file from the `webroot` directory, for example:

```
C:\Program Files\Tibco\Spotfire Web Player\6.0\webroot\Web.config
```

Note We recommend that you use an XML editor when you modify XML files. An XML editor has features to provide a clear view of the XML code and some text editors corrupt configuration files.

2 Locate the `<system.web>` section.

3 Add the following line in the `<system.web>` section:

```
<machineKey
  validationKey="AutoGenerate,IsolateApps"
  decryptionKey="AutoGenerate,IsolateApps"
  validation="3DES" decryption="3DES"
/>
```

4 Save the `web.config` file.

5 Restart the IIS service.

Note Changing to the 3DES algorithm from the AES algorithm decreases the security level.

6.11 Diagnostics

By entering the following URL in your browser, you will reach the System Information page of Spotfire Web Player:

Example: `http://<servername>/SpotfireWeb/Administration/Diagnostics.aspx`

You can also reach it by clicking **Diagnostics** in the top right corner in the library.

This page consists of several tabs which lists various kinds of system information:
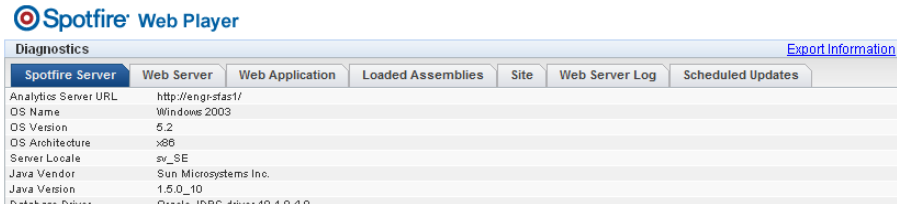
- Spotfire Server
- Web Server
- Web Application
- Loaded Assemblies
- Site
- Web Server Log
- Scheduled Updates (Optional tab)

Access to these tabs is under license control, and can only be accessed by a member of the Spotfire **Administrators** group, the **Web Player Administrator** group, or the **Diagnostics Administrator** group.

6.11.1 Spotfire Server

This tab displays information about the Spotfire Server.
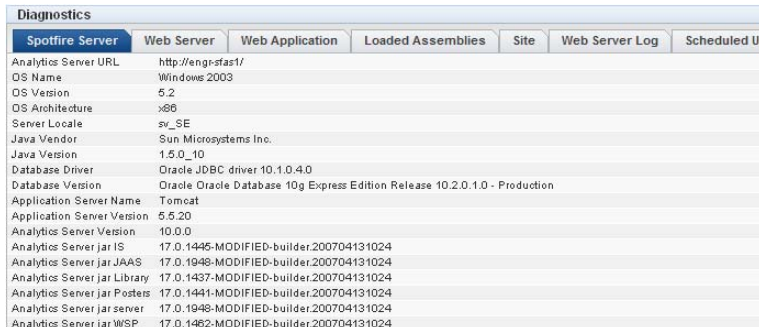
6.11.2 Web Server

This tab displays information about the web server environment.

6.11.3 Web Application

This tab displays information about the Spotfire Web Player web application.

6.11.4 Loaded Assemblies

This tab displays information about the assemblies that are loaded by the web

application.

6.11.5 Site

This tab displays information about the current activity on the web site, such as how long the web application has been running, how many users are logged in at present, etc. Numbers within parentheses indicates the maximum concurrent users/analyses that was measured during this uptime.

The Site tab also shows a list of currently active sessions, a list of which analyses are currently open, and which users are connected.

6.11.6 Web Server Log

This tab displays the log for the web application.

The page shows the log file located at `<Installdir>/Logfiles/ Spotfire.Dxp.Web.log` on the web server. You can customize the severity of events to be logged by changing the following section in the `log4net.config` file, located in the `webroot\App_data` directory of the installation.

```
<appender
  name="FileAppender"
  type="log4net.Appender.RollingFileAppender"
>
  <file value="Logs\Spotfire.Dxp.Web.log" />
  <appendToFile value="true" />
  <rollingStyle value="Size" />
  <maxSizeRollBackups value="10000" />
  <maximumFileSize value="10000kB" />
  <staticLogFileName value="false" />
  <layout type="log4net.Layout.PatternLayout">
    <conversionPattern
      value="%date [%thread] %-5level %logger - %message%newline"
    />
  </layout>
</appender>
<root>
  <level value="INFO" />
```

```
    <appender-ref ref="FileAppender" />
</root>
```

Possible values for log level are: DEBUG, INFO, WARN, ERROR, FATAL. You can specify the minimum level you want to be logged; every event for that level and above will be logged.

Note Be careful of selecting DEBUG since this will log large amounts of events and quickly create huge log files. This level is only to be used when actively trying to find the source of a problem.

Note The tab can only show log information that is logged with the appender type FileAppender.

More information about the log system can be found at http://logging.apache.org/log4net/

6.11.7 Scheduled Updates

This tab displays the log for any Schedules Updates. It contains the path and name of all scheduled files and also information about the time of the last update, the duration of the last update, and the chosen schedule for each file.

6.12 Logging and Monitoring

To track the resource usage for the Spotfire Web Player server, you can enable logging and monitoring of the server by adding and enabling performance counters in the web.config file and by adding the settings for the log files you want to create in the log4net.config file, located in the webroot\App_data directory of the installation.

The following log files can be enabled in the log4net.config file:

- AuditLog.txt: At INFO level, user login and logout, initiate open for analyses, and analysis open and close is logged.
  At DEBUG level, state changes (apply and save) are also logged.

- MonitoringEventsLog.txt: At INFO level, Spotfire Web Player server start up and shut down is logged.
  At DEBUG level, session create and remove, analyses open and close, and cached analyses add and remove are also logged

- DocumentCacheStatisticsLog.txt: The cached analyses sampled regularly.

- OpenFilesStatisticsLog.txt: The open analyses sampled regularly.

- PerformanceCounterLog.txt: Standard and custom performance counters logged regularly.

- `UserSessionStatisticsLog.txt`: The existing sessions sampled regularly.

- `DateTimes.txt`: All time points from the Spotfire Web Player logs collected in one file to simplify joins between tables.

- `MemoryStatisticsLog.txt`: Writes resource usage per document. Logs the amount of memory used by tables and views, the number of internal document nodes, and the execution time. On `INFO` level the total values per document is logged and on `DEBUG` level detailed information per table is recorded.

Note You can log to a database instead of log files. For more information, see "Enable logging in log4net.config" on page 103.

6.12.1 Enable logging in web.config

The following section shows how to configure the collection of user and session statistics, and performance counters in the `web.config` file.

```
<spotfire.dxp.web>
  ...
  <performance>
    ...
    <performanceCounterLogging
      enabled="true"
      logInterval="120"
      counters="
        ...
      "
      debugLogInterval="15"
      debugCounters="
        ...
      "
    />
  ...
  <statistics flushInterval="300" enabled="false" />
```

Key	Description
`performanceCounter Logging`	
`enabled`	Set this to `true` (default) to enable the logging of the specified performance counters. The result of this logging can be found in the `PerformanceCounterLog.txt` file specified in the `log4net.config` file.
`logInterval`	Specify the number of seconds between each performance counter logging at `INFO` level. Default value is `120`.
`counters`	Add performance counters you wish to log, at both `INFO` and `DEBUG` level, separated by a comma "`,`". Each counter consists of three parts: category, counter, and instance, separated by a semi-colon "`;`". Both standard Windows performance counters, as well as a set of internal TIBCO counters, may be included.

`debugLogInterval`	Specify the number of seconds between each performance counter logging at `DEBUG` level. Default value is `15`.
`debugCounters`	Add additional performance counters you wish to log at `DEBUG` level, separated by a comma "`,`".
`statistics`	
`flushInterval`	Specify the number of seconds between each logging. Default value is `300`.
`enabled`	Set this to `true` to enable logging of all the other statistics for the Spotfire Web Player server. The result of this logging can be found in the other log files specified in the `log4net.config` file.

6.12.2 Enable logging in log4net.config

This section shows how you can configure the `log4net.config` file, located in the `webroot\App_data` directory of the installation, to create the log files mentioned earlier. Each section in the configuration file corresponds to a log file. The file paths in each appender have to be set correctly. For example, they should be set to the same directory as the default log file `Spotfire.Dxp.Web.log`, which can be found in the installed `log4net.config`.

There are two levels for logging, `INFO` and `DEBUG`. Select which level to use in this file and specify the performance counters for the levels in the `web.config` file, as described in "Enable logging in web.config" on page 102.

You can log to a database instead of log files. This is done by writing `AdoNetAppenders` instead of the `RollingFileAppenders` in the `log4net.config` file.

Note The logging specified in the `log4.net.config` file can be switched on or off while the Spotfire Web Player server is running. This is done by setting the `level value` to `DEBUG`, `INFO`, or `NONE`.

6.12.2.1 Logging Properties

To extract all information to a log file the default format `%message` is used. However, for most log files it is also possible to specify which properties to write to the log files. This is especially important if you log to a database instead of a log file as this makes it easier to get the properties in separate columns in the database.

AuditLog Properties

Property	Description
`hostName`	The server computer name.
`timeStamp`	The event timestamp.

sessionId	The ASP.NET session ID.
ipAddress	The IP Address of the web client.
userName	The username of the logged on client.
operation	The audit operation, for example "Login".
analysisId	The document id (GUID) of the currently open document.
argument	An argument for the operation, for example the path of the analysis.
status	Failure or Success.

MonitoringEventsLog Properties

Property	Description
hostName	The computer name of the server.
timeStamp	The event timestamp.
eventType	The type of event.
information	Information related to the event.
argument	Arguments related to the event.

DocumentCacheStatisticsLog Properties

Property	Description
hostName	The server computer name.
timeStamp	The event timestamp.
path	The path of the currently open document.
modifiedOn	The modified date of the document.
referenceCount	The count of concurrent open references to the current document.

OpenFilesStatisticsLog Properties

Property	Description
hostName	The server computer name.
timeStamp	The event timestamp.
sessionId	The ASP.NET session ID.

`filePath`	The path of the currently open document.
`modifiedOn`	The modified date of the document.
`fileId`	The file ID.
`elapsedTime`	The time since opened.
`inactiveTime`	The inactivity time.

PerformanceCounterLog Properties

`PerformanceCounterLog` only supports the `%message` format.

UserSessionStatisticsLog Properties

Property	Description
`hostName`	The server computer name.
`timeStamp`	The event timestamp.
`sessionId`	The ASP.NET session ID.
`ipAddress`	The IP Address of the web client.
`userName`	The username of the logged on client.
`browserType`	The name and (major) version number of the browser.
`cookies`	Returns true if cookies are enabled.
`loggedInDuration`	The duration of time the user has been logged in.
`maxOpenFilesCount`	The maximum number of open files.
`openFilesCount`	The number of currently open files.

DateTimesLog Properties

`DateTimesLog` only supports the `%message` format.

MemoryStatisticsLog Properties

Property	Description
`hostName`	The server computer name.
`timeStamp`	The event timestamp.
`sessionId`	The ASP.NET session ID.
`userName`	The username of the logged on client.

analysisId	The unique ID for the analysis.
tableId	The unique ID for the table. This will be empty if the value is a total.
analysisPath	The library path for the analysis.

type	The `type` of information, one of:
	`SharedApproximateTotalTableSize`
	`SharedApproximateTotalViewSize`
	`DocumentNodeCount`
	`SharedDocumentNodeCount`
	`ApproximateExecutionTime`

value	The number of bytes, nodes, or milliseconds depending on `type`.

6.12.2.2 Log to Database Example

This example shows how to log the AuditLog to a database. The `connectionString` should specify a database that contains a table with columns that match the SQL statement specified in `commandText`. For the other logs, replace the relevant properties, names, and settings.

```
<!-- Audit log appender to database -->
<appender
  name="AuditLogAdoNetAppender"
  type="log4net.Appender.AdoNetAppender"
>
<bufferSize value="1" />
<connectionType value="
  System.Data.SqlClient.SqlConnection,
  System.Data,
  Version=1.0.3300.0,
  Culture=neutral,
  PublicKeyToken=b77a5c561934e089"
/>
<connectionString value="
  Data Source=db_server;
  Initial Catalog=spotfire_logging;
  User ID=spotfire;
  Password=spotfire"
/>
<commandText value="
  INSERT INTO AuditLog_Webserver
 ([hostName],[level],[sessionId],[ipAddress],[userName],
[operation],[analysisId],[argument],[status],[timeStamp])
  VALUES (@hostName,@level,@sessionId,@ipAddress,@userName,
@operation,@analysisId,@argument,@status,@timeStamp)"
/>
  <parameter>
    <parameterName value="@level" />
    <dbType value="String" />
    <size value="10" />
    <layout type="log4net.Layout.PatternLayout">
      <conversionPattern value="%level" />
    </layout>
  </parameter>
```

```
<parameter>
  <parameterName value="@timeStamp" />
  <dbType value="String" />
  <size value="50" />
  <layout type="log4net.Layout.PatternLayout">
    <conversionPattern value="%property{timeStamp}" />
  </layout>
</parameter>
<parameter>
  <parameterName value="@hostName" />
  <dbType value="String" />
  <size value="50" />
  <layout type="log4net.Layout.PatternLayout">
    <conversionPattern value="%property{hostName}" />
  </layout>
</parameter>
<parameter>
  <parameterName value="@sessionId" />
  <dbType value="String" />
  <size value="50" />
  <layout type="log4net.Layout.PatternLayout">
    <conversionPattern value="%property{sessionId}" />
  </layout>
</parameter>
<parameter>
  <parameterName value="@ipAddress" />
  <dbType value="String" />
  <size value="50" />
  <layout type="log4net.Layout.PatternLayout">
    <conversionPattern value="%property{ipAddress}" />
  </layout>
</parameter>
<parameter>
  <parameterName value="@userName" />
  <dbType value="String" />
  <size value="50" />
  <layout type="log4net.Layout.PatternLayout">
    <conversionPattern value="%property{userName}" />
  </layout>
</parameter>
<parameter>
  <parameterName value="@operation" />
  <dbType value="String" />
  <size value="50" />
  <layout type="log4net.Layout.PatternLayout">
    <conversionPattern value="%property{operation}" />
  </layout>
</parameter>
<parameter>
  <parameterName value="@analysisId" />
  <dbType value="String" />
  <size value="50" />
  <layout type="log4net.Layout.PatternLayout">
    <conversionPattern value="%property{analysisId}" />
  </layout>
</parameter>
<parameter>
  <parameterName value="@argument" />
  <dbType value="String" />
  <size value="50" />
  <layout type="log4net.Layout.PatternLayout">
    <conversionPattern value="%property{argument}" />
  </layout>
</parameter>
```

```
<parameter>
  <parameterName value="@status" />
  <dbType value="String" />
  <size value="10" />
  <layout type="log4net.Layout.PatternLayout">
    <conversionPattern value="%property{status}" />
  </layout>
</parameter>
</appender>
```

6.12.3 External Monitoring Tool

It is possible to monitor the Spotfire Web Player using an external monitoring tool. There are three sources of information for such a tool.

- General Windows performance counters.

- TIBCO Spotfire Web Player performance counters.

- A dedicated monitoring events log file.

Performance Counters

For a list of the custom performance counters included in the Spotfire Web Player, and a suggested set of general Windows performance counters, see "Enable logging in web.config" on page 102.

Monitoring Log File

For information on the monitoring log file `MonitoringEventsLog.txt`, see the general description in "Logging and Monitoring" on page 101, and for details on the log file, see "Enable logging in log4net.config" on page 103.

6.13 Performance

The system diagnostics page, and the logging and monitoring configuration described earlier are very useful for monitoring the Spotfire Web Player server. As a complement, logging with the **Performance Monitor** tool found in **Microsoft Management Console for Windows Server** can give more information about the server status. The logs can be observed graphically or saved to a file.

Good counters to log for an ASP.NET application is described in "ASP.NET Performance Monitoring, and When to Alert Administrators, MSDN Library, Thomas Marquardt, Microsoft Corporation" http://msdn2.microsoft.com/en-us/library/ms972959.aspx

▶ **Enabling Performance Logging**

1 Select **Start > Administrative Tools > Reliability and Performance Monitor** (**Performance Monitor** on Windows Server 2012).

2 Select **Monitoring Tools > Performance Monitor**.

3 Right-click **Performance Monitor** and select **New > Data Collector Set**.

4   Specify a name for the data collector set and click **Next**.

5   Specify the location to save the log files to and click **Finish**.

6   Select **Data Collector Sets > User Defined > The newly created Data Collector Set**.

7   Right-click **System Monitor Log** in the window to the right and select **Properties**.

8   Add the counters needed.

9   Set various parameters, such as: Sample Interval, Log Format and File Name. The file name is specified as there can be multiple data collectors in the data collector set.

   Comment: Parameters can be found on both the **Performance Counters** tab and the **File** tab.

10   Click **OK**.

11   Right-click **Data Collector Sets > User Defined > The newly created Data Collector Set** and select **Start/Stop** to start or stop collecting the data.

   The logging results will be saved in the specified data collector file.

6.14 Set up a Server Cluster

Spotfire Web Player in a Server Cluster

To obtain better scalability, it is possible to configure a cluster of Spotfire Web Player servers. Many different cluster solutions may be used as long as session affinity is maintained and the same ASP.NET machineKey is set on all Spotfire Web Player servers.

Advantages with a Server Cluster Solution

Setting up a server cluster has some advantages compared to a single server:

● The price for a set of less powerful servers may be lower than for a single high performance server.

● The application will be available as long as at least one server node is up and running, so upgrading will be possible without taking the service down at all.

Setting up a Server Cluster Using Microsoft Network Load Balancing

One alternative is to configure a server cluster making use of the Microsoft Network Load Balancing (NLB) Cluster solution. Setting this up is straight-forward and the NLB solution is included in Windows Server 2008.

You can find, more information about Microsoft NLB on Microsoft TechNet.

Windows Server	Microsoft Technet URL
2008	http://technet.microsoft.com/en-us/library/cc725691(WS.10).aspx
2008 R2	http://technet.microsoft.com/en-us/library/cc725691.aspx
2012	http://technet.microsoft.com/en-us/library/hh831698.aspx

▶ **Setting Up the Server Cluster**

1 Install Microsoft Windows Server 2008 (alternatively Windows Server 2008 R2 or Windows Server 2012) on a set of servers and connect them to the same subnet with fixed IP-addresses.

2 Install Network Load Balancing.

Windows Server	Microsoft Technet URL
2008	http://technet.microsoft.com/en-us/library/cc731695(WS.10).asp
2008 R2	http://technet.microsoft.com/en-us/library/cc731695.aspx
2012	http://technet.microsoft.com/en-us/library/cc731695.aspx

Note Some details of the procedure are different between Windows Server 2008 R2 and Windows Server 2012. For more information, see http://technet.microsoft.com.

3 Install Spotfire Web Player on each server node and:

- Make sure that the local web server is running.
- Verify that you can open a Spotfire analysis in the Spotfire Web Player.

4 Create and configure the cluster, add hosts, and configure them using the Network Load Balancing Manager..

Windows Server	Microsoft Technet URL
2008	http://technet.microsoft.com/en-us/library/cc731499(WS.10).aspx
2008 R2	http://technet.microsoft.com/en-us/library/cc731499.aspx
2012	http://technet.microsoft.com/en-us/library/cc731499.aspx

Note Some details of the procedure are different between Windows Server 2008 R2 and Windows Server 2012. For more information, see http://technet.microsoft.com.

You have now configured a cluster of Spotfire Web Player servers.

Using the Command Prompt, we can see on each of the server nodes that the network settings have been changed:

```
C:\ >ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 192.168.1.6
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   IP Address. . . . . . . . . . . . : 192.168.1.3
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

Connecting to SpotfireWeb on the cluster IP address, in this example `http://192.168.1.6/SpotfireWeb`, will start the Spotfire Web Player against one of the server nodes.

In a clustered Spotfire Web Player environment you should set the `WebPlayerUrl` in the `Spotfire.Dxp.Web.KeepAlive.exe.config` file to a domain name to which all servers in the environment can connect. If some servers cannot reach the server entered in the `WebPlayerUrl` some servers, depending on the load balancer, may not be kept alive by the **keepalive** service. In the situation where some servers cannot reach this URL, we recommend that you use an `IP address` or `localhost` and circumvent the load balancer.

Modify the configuration file:

```
\webroot\bin\Tools\Spotfire.Dxp.Web.KeepAlive.exe.config
```

```
<setting name="WebPlayerUrl" serializeAs="String">
  <value>http://clustername/SpotfireWeb/KeepAlive.ashx</value>
</setting>
```

6.15 Backup and Restore

If Spotfire Web Player needs to be restored, this is done by completing a new installation of the Spotfire Web Player. However, since the Spotfire Web Player does not store any state itself, you must make a backup of important files after configuring the Spotfire Web Player, in order to be able to recover it properly.

Note It is also important to back up the Spotfire Server to be able to recover all settings. Please refer to the TIBCO Spotfire Server – Installation and Configuration Manual for more information on how to back up the Spotfire Server.

Note Do not forget to make a new backup of the Spotfire Web Player after making changes to any of the important files listed below.

Files to Back up

A standard installation is performed in this location.

```
C:\Program Files\TIBCO\Spotfire Web Player\6.0\webroot
```

Back up the following files (paths are relative to the `webroot` directory)

Files	When to include
`web.config`	Always
`app_data\Header.htm`	If the header has been customized. **Note** Include any other files related to the customized header, for example images.
`bin\Tools\Spotfire.Dxp.Web.Keep Alive.exe.config`	If you use scheduled updates and the keep alive service.
`app_data\ScheduledUpdates.xml`	If the scheduled updates are not stored in the library.
`app_data\ServerUnavailable.htm`	If you created a custom page.
`Certificate files`	If you use SSL (https).
`Mashups`	If you have any mashup applications.

▶ **Recovering the Spotfire Web Player**

1 Install Spotfire Web Player as described in this manual and configure it in the same way as the old one.

 Comment: If you are using Kerberos, X.509 certificates, have configured impersonation towards the TIBCO Spotfire Server, or have a server cluster, you should restore to a computer with the same name, the same IP address, and the same port number.

2 Replace the `web.config` file in the `webroot` directory of the new installation with the backup file.

 Comment: If the username and password have been encrypted in `<Spotfire.Dxp.Internal.Properties.Settings>`, they are not readable on a new computer, and the encryption needs to be done again.

3 Replace the other applicable files with the backed up versions.

4 If you have upgraded the Spotfire Web Player with extensions or upgrades, you must upgrade the Spotfire Web Player again.

5 Verify that the new installation works as intended by following the instructions in the chapter "Testing the Installation" on page 58.

7   Uninstall

7.1   Stopping the Application Pool

Before uninstalling TIBCO Spotfire Web Player, it is important to stop the application pool for the Spotfire Web Player in IIS. This is done to make sure that no instances of the Spotfire Web Player are running when you uninstall it.

▶   **To Stop the Application Pool**

1   Select **Start > Administrative Tools > Internet Information Services (IIS) Manager**.

2   Select **Local computer > Application Pools**.

3   Select **TIBCO Spotfire Web Player Pool**.

4   Click **Stop**.

7.2   Spotfire Web Player Software Uninstall

To uninstall TIBCO Spotfire Web Player, go to "Programs and Features" in the Control Panel and uninstall **TIBCO Spotfire Web Player**.

Note   Some temporary files and log files may still exist in the installation directory, by default `C:\Program Files\TIBCO\Spotfire Web Player\6.0.` Simply delete them after uninstalling the Spotfire Web Player.