TIBCO Spotfire® Web Player 5.5

Installation and Configuration Manual

TIBCO provides the two-second advantage™

TIBCO®
The Power of Now®

Revision date: 20 May 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

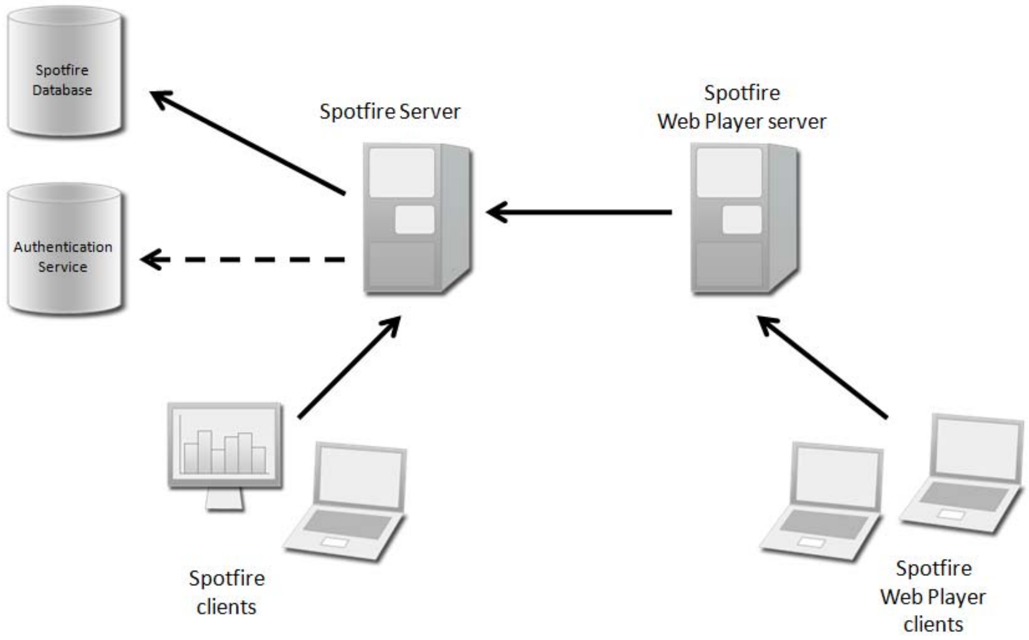
The Spotfire Web Player is installed on a Microsoft IIS web server. This is the software that actually renders the visualizations and graphics for the user.

When a user starts a web browser on his local computer and enters the URL to an analysis on the Spotfire Web Player, the Spotfire Web Player communicates with the Spotfire Server.

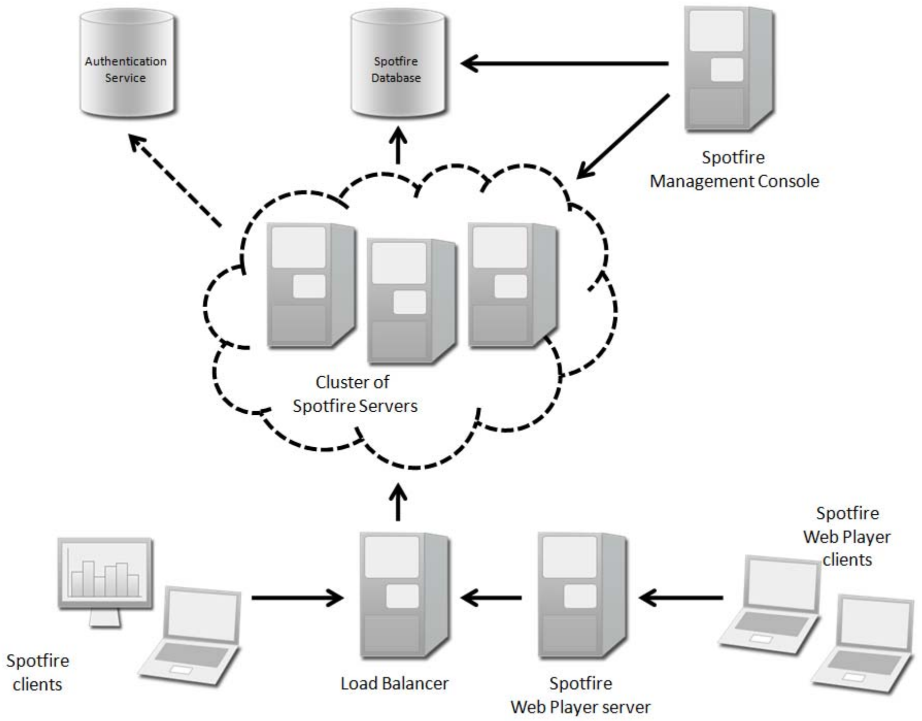
The Spotfire Server manages the data and delivers it to the Spotfire Web Player which then renders the view that is presented in the user’s web browser.

1.2 Architectural Overview

In a simple Spotfire system, the Spotfire Web Player and Spotfire clients communicate with a single Spotfire Server, as illustrated in the following picture.

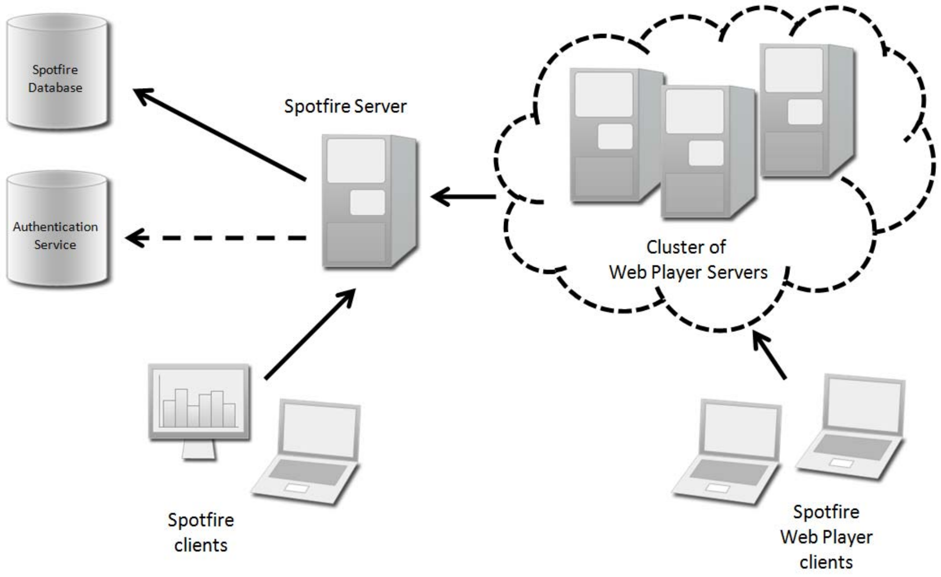


In a Spotfire system with more than one Spotfire Server, the web player communicates with a cluster of Spotfire Servers behind a load balancer.


Authentication Service
Spotfire Database
Spotfire Management Console
Cluster of Spotfire Servers
Spotfire Web Player clients
Spotfire clients
Load Balancer
Spotfire Web Player server

Regardless of whether one or several Spotfire Servers exist in the Spotfire system, the web player is set up in the same way.

It is also possible to set up a cluster of Web Player Servers.



It is of course possible to combine Spotfire Server clusters and Web Player clusters, if required.

Spotfire Server and Spotfire Web Player on the Same Computer

Typically, Spotfire Web Player is installed on one or more separate computers or dedicated web servers. However, it is possible to install it on the same computer as Spotfire Server. This is **not a recommended solution**, as it affects performance for both products, and leads to complications regarding port numbers. Spotfire Server listens to port 80 by default, which is typically the same port the web player listens to. There are also issues regarding Kerberos authentication when the Spotfire Server and the Web Player run on the same computer, so if you want to use Kerberos authentication, **do not** install the Web Player on the same computer as the Spotfire Server.

1.3 Software Overview

Technology

TIBCO Spotfire Web Player is implemented as an Internet Information Services Web Application using ASP.NET and AJAX. For specific system requirements, see `http://support.spotfire.com/sr.asp`.

Installation and File Locations

TIBCO Spotfire Web Player is installed on a Windows server using an InstallShield wizard. All files in the distribution are installed in a directory specified in the installation wizard, by default C:\Program Files\TIBCO\Spotfire Web Player\5.5. If you have upgraded the Web Player using the upgrade tool, the software will still be installed in a folder with the old version’s name, such as 5.0.1.

Windows Service

After installation, you will find a Windows Service called “TIBCO Spotfire Web Player Keep Alive Service” on the Web Player server. This service is important for letting the feature Scheduled Updates operate properly. If you intend to use scheduled updates, Startup Type should be set to “Automatic”.

Upgrade Tool

In the `<installation folder>\webroot\bin\Tools` folder, you will find the executable file called `Spotfire.Dxp.Web.UpgradeTool.exe`. This is the upgrade tool that is used to install new modules, such as language packs or third party add-ons. For more information on how to use this tool, see the section “Deploying Extensions and Upgrades” on page 57.

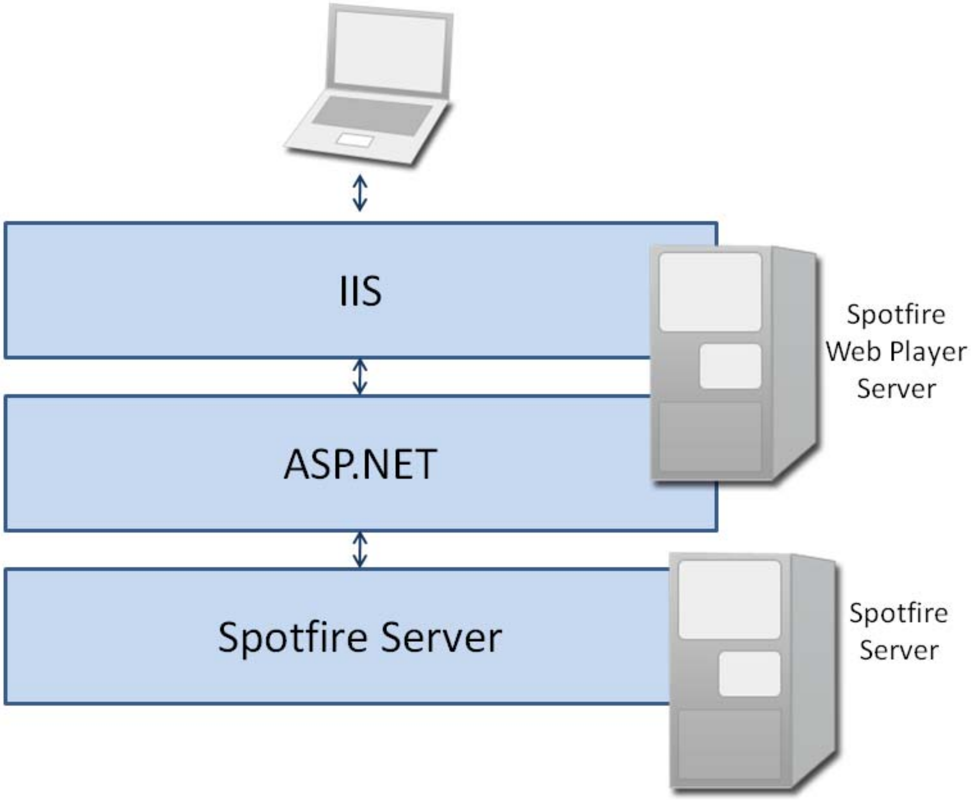
Log Files

In the `<installation folder>\webroot\bin\Logfiles` folder, you will find the Web Player log files. Read more about the Web Player Log in the section “Web Server Log” on page 100.

1.4 Authentication Alternatives

The Spotfire Web Player authentication consists of three layers: IIS, ASP.NET and Spotfire Server. Each of these layers can be configured in various ways to achieve certain authentication behaviors. It is the combination of how these three layers are set up that finally determines the level of security for the system and the experience for the users who connect to it.

The purpose of this chapter is to give you enough information on all authentication alternatives so you can decide which one to use before you begin the installation of Spotfire Web Player.



By configuring these three layers in a certain way, you decide how you want the authentication for Spotfire Web Player to work. The most common alternatives are:

- **Username & Password** – users who connect to the Spotfire Web Player are prompted to enter a username and password. These credentials are verified against the Spotfire Server, which can be set up in various ways (for example, LDAP, Database or Windows NT Domain). This is the default authentication configured during Spotfire Web Player installation and no post-installation authentication configuration is required.

IIS set to:	*Anonymous and Forms*
ASP.NET set to:	*Forms Authentication*
Spotfire Server set to:	*Basic Authentication*

- **Anonymous Access** – all users who connect to the Spotfire Web Player from their web browsers get automatically logged in using a preconfigured username and password. You specify these preconfigured credentials when you configure the ASP.NET layer. These credentials are automatically used for all users to access the Spotfire Server.

IIS set to:	*Anonymous*
ASP.NET set to:	*None (Preset User/Password)*
Spotfire Server set to:	*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 access the Spotfire Web Player from the appropriate Windows Domain, they will not have to enter their credentials.
  Note: In this alternative, when you configure the Web Player authentication method to use one of the impersonation authentication methods, the TIBCO Spotfire Server can 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 Web Player is delegated Kerberos.

IIS set to:	*Integrated Windows Auth.*
ASP.NET set to:	*Windows*
Spotfire Server set to:	*NTLM, Kerberos or Basic*

- **Client Certificate** – users who connect to the Spotfire Web Player are authenticated using client certificates.

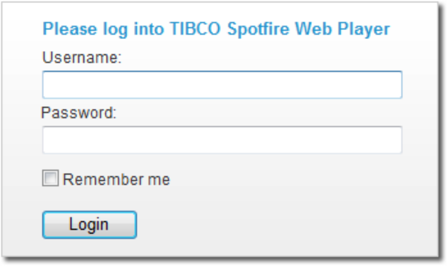
IIS set to:	*Anonymous*
ASP.NET set to:	*None*
Spotfire Server set to:	*Client Certificate*

The authentication alternatives are described in more detail below, and the necessary steps to set up these alternatives are described in the chapter “Installing TIBCO Spotfire Web Player” on page 26.

1.4.1 Username and Password

This is the default authentication configured for Spotfire Web Player and does not require more authentication configuration after the installation completes.

This option presents the user with a login form inside the browser when accessing the Spotfire Web Player site. This login form is displayed by the ASP.NET layer.



The **Remember me** check box in the login form will save the user's login information (username and password) encrypted in a cookie. This cookie will be used for the next login so the dialog will not be shown. To clear the login cookie, press logout in the web player or library browser window.

The credentials that the user enters is validated by the Spotfire Server.

Note: Because the username and password are sent as clear text, we recommend that this authentication alternative (also known as "Forms Authentication") be used together with HTTPS (SSL) connections, see "Configuring SSL" on page 39.

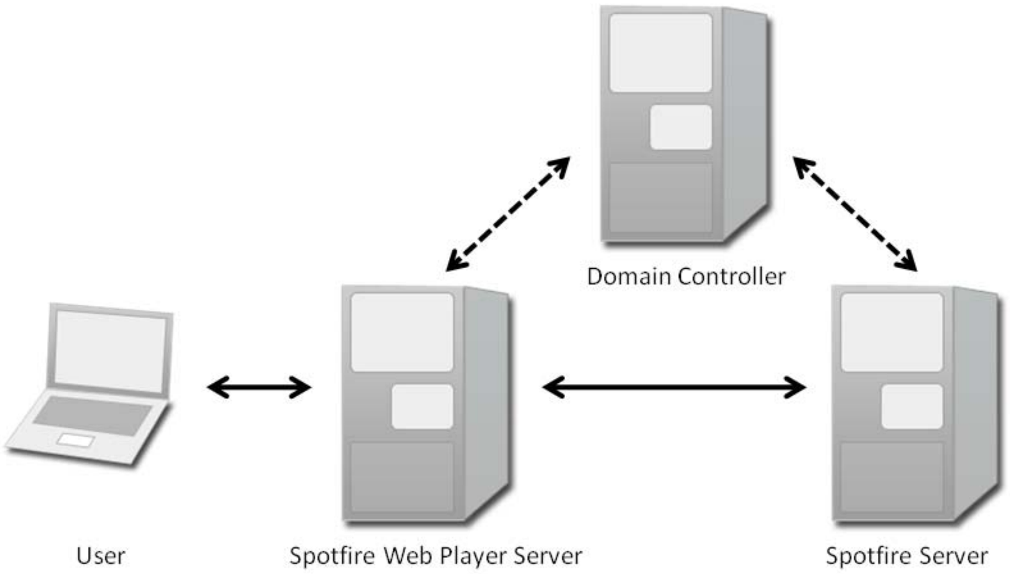
1.4.2 Anonymous (Preconfigured) Access

With this option, users accessing the Spotfire Web Player services will be automatically logged in as a fixed user specified in the **Web.config** file. This means all users will log onto Spotfire Server as the same Spotfire user. This user must also be created, given the licenses for the library and configured for impersonation on the Spotfire Server.

1.4.3 Single Sign-On

This authentication method is used to achieve "single sign-on" for the Spotfire Web Player users. This means that when they have logged into their usual Windows account, they will not be prompted to enter any additional username or password when accessing the Spotfire Web Player. They will be automatically logged in using their Windows credentials.

There are four ways of achieving this. All these are a bit more complex than the "Anonymous" or "Username and Password" methods described earlier, since they require additional configuration on either your Windows Domain Controller and/or the Spotfire Server. These alternatives therefore require that you are somewhat knowledgeable about how a Domain Controller works.



The alternatives, explained below, are:

- Single Sign-On using Impersonation with NTLM Login System
- Single Sign-On using Impersonation with Basic Login System
- Single Sign-On using Impersonation with Kerberos Login System
- Single Sign-On using Delegation with Kerberos Login System

Single Sign-On Using Impersonation with NTLM Login System

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

In this approach, when a user connects to the Spotfire Web Player from his web browser, he is automatically logged in with his standard Windows username.

The Web Player Server then contacts the Spotfire Server, which prompts the Web Player Server to authenticate the user. The Web Player Server automatically logs into the Spotfire Server using a predefined **impersonation account**.

This impersonation account has been added to the **Impersonator** group on the Spotfire Server. This account has the privileges to **run services as another named user**. It does not even need to know the password of the user it impersonates, but can simply run services as another user by stating a valid username.

The system can additionally be set up to require the impersonation account to log on from a specified computer or IP address (that is, the Spotfire Web Player Server) to reduce the risk of security problems.

This alternative requires the following:

- An **impersonation account** for the Spotfire Web Player Server must be created on the Domain Controller.
- The Spotfire Server must use **NTLM Login System**.
- You need to enable ASP.NET Impersonation on the IIS.

This alternative does not require you to set up Delegation on the Domain Controller. Instead you will set up a trusted account on the Web Player Server that the Spotfire Server will allow to run requests as another user. This is called Impersonation.

Single Sign-On Using Impersonation with Basic Login System

If you cannot use NTLM you can use this alternative.

When a user connects to the Spotfire Web Player from his web browser, he gets automatically logged in with his standard Windows username.

The Web Player Server then contacts the Spotfire Server, which prompts the Web Player Server to authenticate the user. The Web Player Server automatically logs into the Spotfire Server using a predefined **impersonation account**.

This impersonation account has been added to the **Impersonator** group on the Spotfire Server. This account has the privileges to **run services as another named user**. It does not even need to know the password of the user it impersonates, but can simply run services as another user by stating a valid username.

Since the Spotfire Server is using a Basic login system (**LDAP** or **Database** login 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 the previous impersonation alternative.

The system can additionally be set up to require the impersonation account to log on from a specified computer or IP address (that is, the Spotfire Web Player Server) to reduce the risk of security problems.

This alternative requires the following:

- The Spotfire Server must use either **LDAP** or **Database Login System**.
- An **impersonation account** for the Spotfire Web Player Server must be created on the LDAP Server or the Spotfire Server (depending on whether the Spotfire Server has been set up to use LDAP or Database login system).

This alternative does not require you to set up Delegation on the Domain Controller. Instead you will set up a trusted account on the Web Player Server that the Spotfire Server will allow to run requests as another user. This is called Impersonation.

Single Sign-On Using Impersonation with Kerberos Login System

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.

When a user connects to the Spotfire Web Player from his web browser, he gets automatically logged in with his standard Windows username.

The Web Player Server then contacts the Spotfire Server, which prompts the Web Player Server to authenticate the user. The Web Player Server automatically logs into the Spotfire Server using a predefined **impersonation account**.

This impersonation account has been added to the **Impersonator** group on the Spotfire Server. This account has the privileges to **run services as another named user**. It does not even need to know the password of the user it impersonates, but can simply run services as another user by stating a valid username.

The system can additionally be set up to require the impersonation account to log on from a specified computer or IP address (that is, the Spotfire Web Player Server) to reduce the risk of security problems.

This alternative requires the following:

- An **impersonation account** for the Spotfire Web Player Server must be created on the Domain Controller.
- The Spotfire Server must use **Kerberos Login System**.
- On a computer with the Windows Support Tools installed (this is typically one of the domain controllers), you must set up the SPNs (**Service Principal Names**) for the Spotfire Server. This must be done by a user which is a member of the **Account Operators** or **Administrators** domain groups.
- On a computer with the Windows Support Tools installed (this is typically one of the domain controllers), you must set up a **keytab file** for the Spotfire Server. This must be done by a user which is a member of the **Account Operators** or **Administrators** domain groups.
- You need to enable ASP.NET Impersonation on the IIS.

This alternative does not require you to set up Delegation on the Domain Controller. Instead you will set up a trusted account on the Web Player Server that the Spotfire Server will allow to run requests as another user. This is called Impersonation.

For more information about Kerberos on the Spotfire Server or keytab files see the “**TIBCO Spotfire Server — Installation and Configuration Manual**”.

Single Sign-On Using Delegation with Kerberos Login System

This alternative lets a user connect to the Spotfire Web Player from his web browser and get automatically logged in using his standard Windows username.

The Web Player Server then contacts the Spotfire Server, which prompts the Web Player Server to authenticate the user. The Web Player Server automatically logs into the Spotfire Server as the end user.

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

This alternative requires the following:

- On the Domain Controller, set up **Delegation** for the computer account or custom user account that is used to run the application pool in the IIS on the Web Player Server.
- The Spotfire Server must use **Kerberos Login System**.
- On a computer with the Windows Support Tools installed (this is typically one of the domain controllers), you must set up the SPNs (**Service Principal Names**) for the Spotfire Server. This must be done by a user which is a member of the **Account Operators** or **Administrators** domain groups.
- On a computer with the Windows Support Tools installed (this is typically one of the domain controllers), you must set up a **keytab file** for the Spotfire Server. This must be done by a user which is a member of the **Account Operators** or **Administrators** domain groups.

This alternative requires you to set up Delegation on the Domain Controller. If you are not the administrator of the Domain Controller, you will need to discuss this with the person who is.

Activating Unconstrained Delegation for the Web Player Server account (computer account or customer user account) will affect all services running on the Web Player Server computer or under that user account, which could be a potential security issue if handled incorrectly. An alternative is to use the more secure Constrained Delegation, if it is supported by the Domain Controller.

If this alternative is not possible in your environment, you should use one of the Impersonation alternatives. More information about keytab files and Kerberos on the Spotfire Server is found in the “**TIBCO Spotfire Server — Installation and Configuration Manual**”.

1.4.4 Client Certificate

Users who connect to the Spotfire Web Player are authenticated using client certificates.

The Web Player Server then contacts the Spotfire Server, which prompts the Web Player Server to authenticate the user. The Web Player Server 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 set up the client certificates, or how to set up SSL; only how to configure the Spotfire Web Player Server to be able to use already installed client certificates for authentication.

1.5 Conceptual Outline of Installation Process

Performing the tasks in **“Installing Prerequisites” on page 17** and **“Installing TIBCO Spotfire Web Player” on page 26** will guide you through a full installation of Spotfire Web Player 5.5 with detailed explanations.

Below is a conceptual overview of the steps involved:

1. Read the **“Pre-Installation Checklist” on page 15** and write down the needed information.

2. Make sure that the computer on which you intend to run Spotfire Web Player has **Microsoft Windows 2008 Server** or **Microsoft Windows 2012 Server** installed.

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

4. Copy the installation files to the computer.

5. Run the installer.

6. If required, configure the ASP.NET authentication in the **Web.config** file.

   Comment: It is important to decide which authentication method to use before starting. For more information on the authentication alternatives, see “Authentication Alternatives” on page 8.

7. If required, configure the IIS authentication.

8. Verify that no unwanted changes have been made to the **Web.config** file during the installation.

9. Complete the configuration of the chosen authentication method.

10. Set up the licenses and library rights for the web player users.

11. Set up the URL preference.

1.6 Pre-Installation Checklist

Before you begin installing Spotfire Web Player 5.5, there are certain things you must determine. Below is a series of checklists that you must provide answers to before starting the installation.

Compatibility

There are some things that you need to take into consideration regarding compatibility and different versions of the software. In order to install Spotfire Web Player 5.5 you also need to have Spotfire Server version 5.5. Also, it is not possible to have side-by-side installations of different versions of the Web Player installed on the same computer. If you have an earlier version of the Web Player on the computer you install Spotfire Web Player 5.5 on, the earlier version will be lost.

Authentication

There are seven different authentication alternatives for Spotfire Web Player. Each of these is described in the chapter “Authentication Alternatives” on page 8. It is important to decide which alternative to use before installing the web player.

Which of the authentication alternatives do you want to use for Spotfire Web Player?	

Ports

Before installing the web player, it is important that the IIS is already running and is configured to use the port the web player will listen to. The default port is port 80.

What port do you intend to use for Spotfire Web Player?	

Installer Options

When running the installer, answers to the following questions must be given.

What name will you use for the Virtual Directory that will be part of the URL to Spotfire Web Player? The recommended name is SpotfireWeb.	
What is the URL to the Spotfire Server with which the Spotfire Web Player will communicate?	
What is the e-mail address to your local Spotfire Administrator?	

SSL

It is highly recommended to use SSL (https) for some of the authentication alternatives, since they send passwords in plain text.

Will you use SSL or not?	

2 Installing Prerequisites

2.1 Setting Up the Computer

In these procedures, we assume that **Microsoft Windows 2008 Server** or **Microsoft Windows 2012 Server** is already installed on the computer where you intend to run Spotfire Web Player. For more detailed information on the system requirements, see http://support.spotfire.com/sr.asp

Note: If you have an earlier version of the Web Player installed on the intended computer, that version will be lost when you install Spotfire Web Player 5.5.

2.1.1 Internet Access

Some features require that the Spotfire Web Player Server has internet access. This applies, for instance, to the collaboration feature and if any images in a table are linked from a web site on the internet. Other third party features may also be affected.

2.1.2 Active Scripting

If you want to be able to export text areas from the web player you need to enable Active Scripting on the Web Player Server.

► **To Enable Active Scripting**

1. Click **Start**.
2. Type **gpedit.msc** in the Start search box and press Enter.
3. Select **Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Internet Zone**.
4. Right-click on **Allow active scripting** and select **Properties** (**Edit** on Windows Server 2008 R2 and Windows Server 2012).
5. Select **Enabled**.
6. Make sure that the **Allow Active Scripting** drop-down list is set to **Enabled**.
7. Click **OK**.

Note: If this is done after setting up the IIS you need to restart the 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 Web Player webroot folder and all sub-folders. When certain antivirus and malware scanning software packages perform an on-access scan, they modify the scanned files or the attributes of the scanned file and that results in IIS triggering a restart of the web application. When the web application restarts, users are logged out and the analyses is closed.

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

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

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

2.2 Setting Up IIS and ASP.NET

The next step is to install Microsoft Internet Information Services (IIS) on this computer and set up ASP.NET on the IIS.

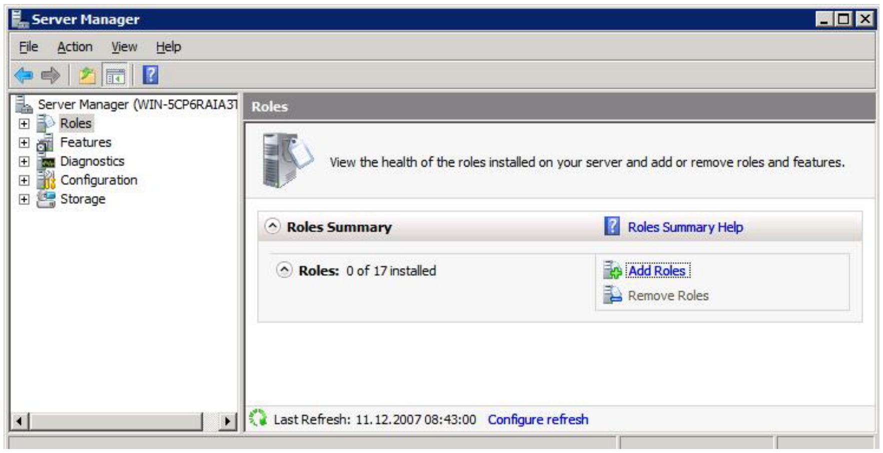
2.2.1 Installing on Microsoft Windows 2008 Server

This section explains how to install IIS and ASP.NET on your Microsoft Windows 2008 Server and how to ensure the IIS has all the necessary components to run TIBCO Spotfire Web Player. If you already have IIS installed, but an earlier version of ASP.NET, you still need to install Microsoft .NET Framework 4.0

1. 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
   Note: Make sure to upgrade to the latest version of Microsoft .NET Framework 4.0.

2. Navigate to the Administrative Tools options on your Microsoft Windows 2008 Server and select **Server Manager**.

3 Select **Roles** in the left hand list, and click **Add Roles**.



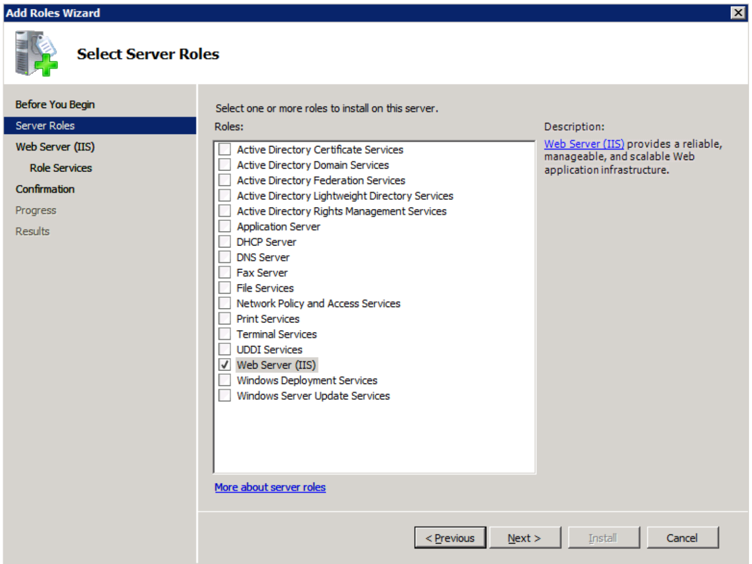
View the health of the roles installed on your server and add or remove roles and features.

Roles: 0 of 17 installed

Last Refresh: 11.12.2007 08:43:00

4 You may see a “Before you begin” dialog. If this is the case click **Next**.

5 In the Select Server Roles dialog, select **Web Server (IIS)**.



Select one or more roles to install on this server.

Roles:

- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- □ File Services
- □ Network Policy and Access Services
- □ Print Services
- □ Terminal Services
- □ UDDI Services
- ☑ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

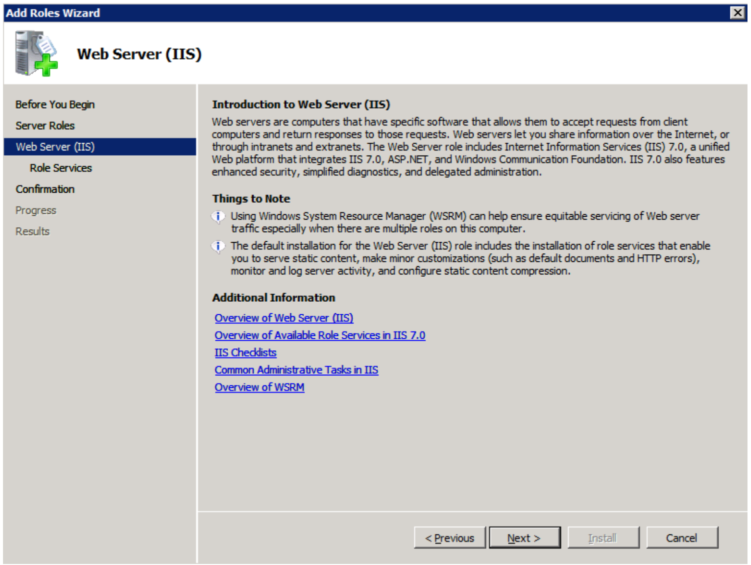
Description:

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

Comment: If you get prompted to “Add features required for Web Server (IIS)?” click **Add Required Features**.

Click **Next**.

6 The Web Server (IIS) dialog appears.



Introduction to Web Server (IIS)

Web servers are computers that have specific software that allows them to accept requests from client computers and return responses to those requests. Web servers let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 7.0, a unified Web platform that integrates IIS 7.0, ASP.NET, and Windows Communication Foundation. IIS 7.0 also features enhanced security, simplified diagnostics, and delegated administration.

Things to Note

- Using Windows System Resource Manager (WSRM) can help ensure equitable servicing of Web server traffic especially when there are multiple roles on this computer.
- The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.

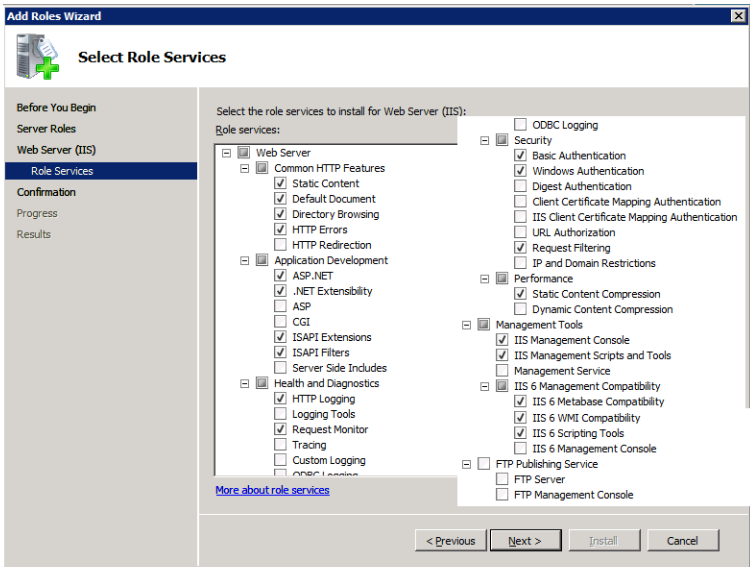
Additional Information

Overview of Web Server (IIS)
Overview of Available Role Services in IIS 7.0
IIS Checklists
Common Administrative Tasks in IIS
Overview of WSRM

Click **Next**.

7 In the Select Role Services dialog, select (at least) the options seen checked below.

Note: Remember to select the required authentication types under the Security section.



Select the role services to install for Web Server (IIS):

Role services:

```
⊟ ▣ Web Server
  ⊟ ▣ Common HTTP Features
      ☑ Static Content
      ☑ Default Document
      ☑ Directory Browsing
      ☑ HTTP Errors
      □ HTTP Redirection
  ⊟ ▣ Application Development
      ☑ ASP.NET
      ☑ .NET Extensibility
      □ ASP
      □ CGI
      ☑ ISAPI Extensions
      ☑ ISAPI Filters
      □ Server Side Includes
  ⊟ ▣ Health and Diagnostics
      ☑ HTTP Logging
      □ Logging Tools
      ☑ Request Monitor
      □ Tracing
      □ Custom Logging
      □ ODBC Logging
  ⊟ ▣ Security
      ☑ Basic Authentication
      ☑ Windows Authentication
      □ Digest Authentication
      □ Client Certificate Mapping Authentication
      □ IIS Client Certificate Mapping Authentication
      □ URL Authorization
      ☑ Request Filtering
      □ IP and Domain Restrictions
  ⊟ ▣ Performance
      ☑ Static Content Compression
      □ Dynamic Content Compression
⊟ ▣ Management Tools
    ☑ IIS Management Console
    ☑ IIS Management Scripts and Tools
    □ Management Service
  ⊟ ▣ IIS 6 Management Compatibility
      ☑ IIS 6 Metabase Compatibility
      ☑ IIS 6 WMI Compatibility
      ☑ IIS 6 Scripting Tools
      □ IIS 6 Management Console
⊟ □ FTP Publishing Service
    □ FTP Server
    □ FTP Management Console
```

Comment: If prompted to “Add role services and features required for ASP.NET?” select **Add Required Role Services**.

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

Management Tools

- IIS Management Console
- IIS Management Scripts and Tools

IIS 6 Management Compatibility

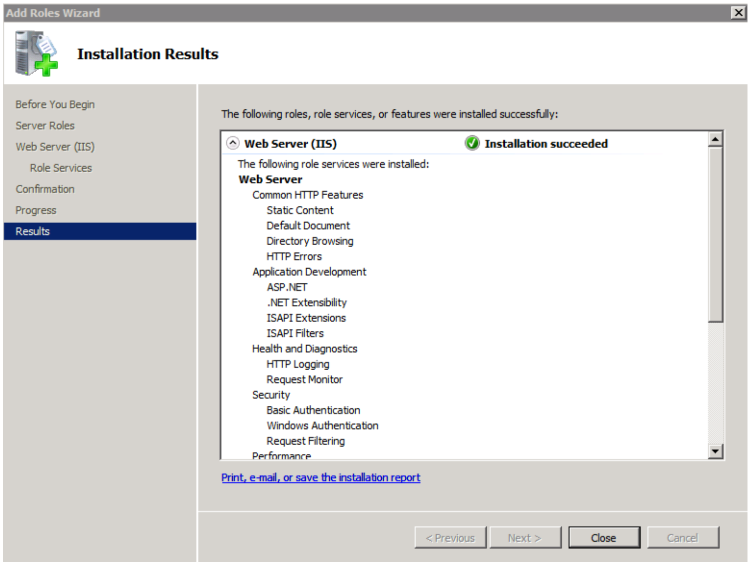
- IIS 6 Metabase Compatibility
- IIS 6 WMI Compatibility
- IIS 6 Scripting Tools

Click **Next**.

8 In the Confirmation dialog, click **Install**.

Response: The installation starts.

9 When the installation is complete, the Installation Results dialog appears.



The following roles, role services, or features were installed successfully:

Web Server (IIS) — Installation succeeded

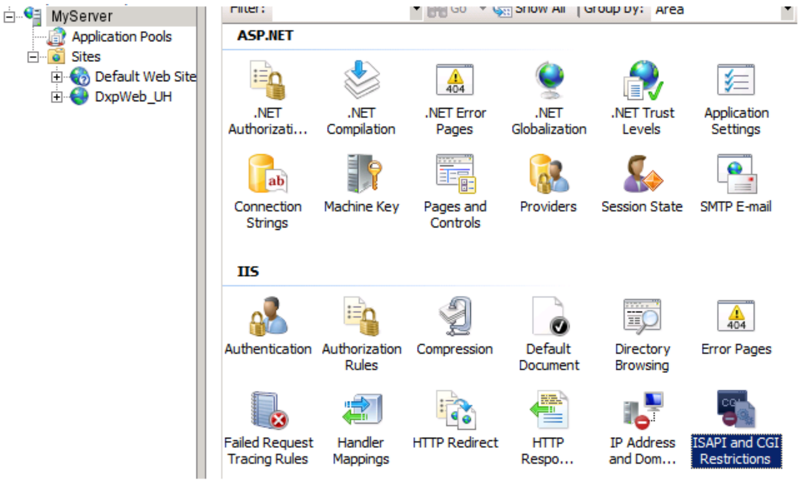
The following role services were installed:

Web Server
  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

Click **Close**.

10 Start the IIS Manager.

11 Select the server level in the left hand list and select **ISAPI and CGI Restrictions**.



12 Make sure that **ASP.NET 4.0.30319** is present in the list and set it to **Allowed**.
Note: If ASP.NET 4.0.30319 is not present open the command console and run the following command:
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe /i
and return to step 11.

13 Done!

2.2.2 Installing on Microsoft Windows 2012 Server

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

1 Upgrade to the latest version of Microsoft .NET Framework.

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

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

4 You may see a “Before you begin” dialog. If this is the case click **Next**.

5 Select the applicable option in the Installation Type dialog and click **Next**.

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

7 In the Select Server Roles dialog, select **Web Server (IIS)**.

Comment: If you get prompted to “Add features required for Web Server (IIS)?” click **Add Required Features**.

Click **Next**.

8 The Web Server (IIS) dialog appears.

Click **Next**.

9 In the Select Role Services dialog, select (at least) the options listed below.

Note: Remember to select the required authentication types under the Security section.

Comment: If prompted to “Add role services and features required for ASP.NET?” select **Add Required Role Services**.

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

Click **Next**.

10 In the Select Features dialog, select the following options.

- .Net Framework 3.5 Features
- .NET Framework 4.5

Click **Next**.

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

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

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

12 Click **Install**.

Response: The installation starts.

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

14 Start the IIS Manager.

15 Select the server level in the left hand list and select **ISAPI and CGI Restrictions**.

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

17 Done!

3 Installing TIBCO Spotfire Web Player

3.1 Copy the Installation Files

On the Spotfire Web Player installation media there is a folder called **TIBCO Spotfire Web Player Installer**. Copy this folder to a local disk on the target computer.

Note: Do not run the installer from a network drive, it will not work.

Note: You must be logged in as an administrator on the target computer to be able to install Spotfire Web Player.

Note: If you have an earlier version of the Web Player installed on the target computer, that version will be removed when you install Spotfire Web Player 5.5. 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

▶ **To Run the Installer:**

1 Double-click on the **setup.exe** you copied to your local disk to start the installer.

Comment: Do not run the installer from a network drive, it will not work.

Response: The installer launches and the first dialog is shown.

2 Click **Next**.

3 Accept the TIBCO Spotfire License Agreement, and click **Next**.

4 Specify the folder where you want to install Spotfire Web Player. Click **Next** to continue.

Comment: If the server has more than one disk, it is recommended to install on the fastest disk. This will decrease the load time of Spotfire Web Player and also optimize any swapping.

5 Specify the name of the Virtual Directory which will be created in IIS. This will be a part of the URL to the server used when pointing out Spotfire Web Player files. It is recommended to leave this as “**SpotfireWeb**”.

The URL will then be: http[s]://<servername>/SpotfireWeb/

6 Specify the port for Spotfire Web Player.

Note: IIS must be running and be configured to use the specified port before installing Spotfire Web Player.

Click **Next** to continue.

7 Specify the URL to the TIBCO Spotfire Server.

Note: If necessary, the URL can be changed afterwards in the **Web.config** file.

Click **Next** to continue.

8 Specify the email address to the Spotfire administrator.

Note: If necessary, the email address can be changed afterwards in the **Web.config** file.

Click **Next** to continue.

9 Click **Install** to start the installation.

10 Click **Finish** to complete the installation.

3.3 Configure ASP.NET Authentication

To configure the authentication used by the ASP.NET layer, you need to edit the configuration file called **Web.config** (if you intend to use Username and Password authentication, this is not necessary). Web.config can be found in the **webroot** folder of the installation. Open this file in an XML editor or text editor of your choice (it is recommended that you use an XML editor, since some text editors can corrupt the Web.config file. An XML editor will also give a clearer view of the XML code).

You can configure this 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 28.
- “Anonymous (Preconfigured) Access” on page 30
- “Single Sign-On Using Delegation with Kerberos Login System” on page 31
- “Single Sign-On Using Impersonation with Kerberos Login System” on page 32
- “Single Sign-On Using Impersonation with NTLM Login System” on page 33
- “Single Sign-On Using Impersonation with Basic Login System” on page 34
- “Client Certificate” on page 36

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

3.3.1 Username and Password

This is done automatically by the installer, but if you need to change to Username and Password authentication after installation, the following settings are required:

The **Web.config** file must be configured to set **Authentication mode** to **Forms** (including sub section).

Also, **Authorization** should be set to:

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

where these settings technically mean to deny users who are not authenticated, and allow any user that has not been denied.

You can also specify if you want to enable users to save their credentials (this information will be saved in an encrypted cookie on the client). You must specify the username and password to use when authenticating to the Spotfire Server. Enter this information in the applicationsettings node in the <value> tags **ImpersonationUsername** and **ImpersonationPassword**.

Enter information in the places seen below.

```
...
...
  <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>
...
...
```

Save the file.

IMPORTANT: Also make a backup copy of Web.config and store this somewhere safe. You may need to refer to it later.

If you wish to set up Proxy proceed to “Configuring Proxy Handling” on page 37.

Otherwise proceed to “Configure IIS Authentication” on page 38.

3.3.1.1 URL Authentication

To simplify integration with other systems, it is possible to allow users to log in via URL or standard basic authentication if Username and Password authentication is set up.

Note: This can only be used on the page **Login.aspx** of the web player.

To allow URL authentication add the following parameter to the authentication section:

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

It is then possible to log in using the following address:

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

To allow basic login using authorization headers add the following parameter:

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

To allow base64 encoded UTF8 username and password in the header add the following parameter:

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

Example when all three parameters have been added to the existing forms section:

```
           <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 set impersonation enabled to “**true**”.

Also, specify the username and password to use when authenticating to the Spotfire Server. 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**. Follow the instructions in the “TIBCO Spotfire Server - Installation and Configuration Manual” to set this up.

Set the **Authentication mode** to **None**. This also requires authorization to be set to **<allow users=“*”/>** which means allow all users. Remove the <deny users="?" /> line.

Enter information in the places seen below.

```
...
...
  <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>
...
...
```

Save the file.

IMPORTANT: Also make a backup copy of Web.config and store this somewhere safe. You might need it later!

If you wish to set up Proxy proceed to “Configuring Proxy Handling” on page 37.

Otherwise proceed to “Configure IIS Authentication” on page 38.

3.3.3 Single Sign-On Using Delegation with Kerberos Login System

The **Web.config** file must be configured to specify **Windows authentication** and set identity impersonate to “**true**”.

Note: Impersonation enabled should still be “false”.

Enter information in the places seen below.

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

Save the file.

IMPORTANT: Also make a backup copy of Web.config and store this somewhere safe. You might need it later!

If you wish to set up Proxy proceed to “Configuring Proxy Handling” on page 37.

Otherwise proceed to “Configure IIS Authentication” on page 38.

3.3.4 Single Sign-On Using Impersonation with Kerberos Login System

The **Web.config** file must be configured. First, set impersonation enabled to “**true**”. Then you must specify **Windows authentication**, and set identity impersonate to “**true**”.

Further down in the Web.config file, you must specify the **ImpersonationUsername** and **ImpersonationPassword.** Enter this information in the <value> tags.

This is the username for the impersonation account you set up on the Domain Controller and on the Spotfire Server, that the Spotfire Web Player Server will use to connect to the Spotfire Server.

Important: You must include the Domain name when specifying the username in the Web.config. For example:

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

Enter information in the places seen below.

```
...
...
  <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>
...
...
```

Save the file.

IMPORTANT: Also make a backup copy of Web.config and store this somewhere safe. You might need it later!

If you wish to set up Proxy proceed to “Configuring Proxy Handling” on page 37.

Otherwise proceed to “Configure IIS Authentication” on page 38.

3.3.5 Single Sign-On Using Impersonation with NTLM Login System

The **Web.config** file must be configured. First, set impersonation enabled to “**true**”. Then you must specify **Windows authentication**, and set identity impersonate to “**true**”.

Further down in the Web.config file, you must specify the **ImpersonationUsername** and **ImpersonationPassword.** Enter this information in the <value> tags.

This is the username for the impersonation account you set up on the Domain Controller and on the Spotfire Server, that the Spotfire Web Player Server will use to connect to the Spotfire Server.

Important: You must include the Domain name when specifying the username in the Web.config. Example:

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

Enter information in the places seen below.

```
...
...
  <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>
...
...
```

Save the file.

IMPORTANT: Also make a backup copy of Web.config and store this somewhere safe. You might need it later!

If you wish to set up Proxy proceed to “Configuring Proxy Handling” on page 37.

Otherwise proceed to “Configure IIS Authentication” on page 38.

3.3.6 Single Sign-On Using Impersonation with Basic Login System

The **Web.config** file must be configured. First, set impersonation enabled to “**true**”. Then you must specify **Windows authentication**, and set identity impersonate to “**true**”.

Further down in the Web.config file, you must specify the **ImpersonationUsername** and **ImpersonationPassword.** Enter this information in the <value> tags.

This is the username for the impersonation account you set up on the Domain Controller and on the Spotfire Server, that the Spotfire Web Player Server will use to connect to the Spotfire Server.

Example:

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

Enter information in the places seen below.

```
...
  <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>
...
```

Save the file.

IMPORTANT: Also make a backup copy of Web.config and store this somewhere safe. You might need it later!

If you wish to set up Proxy proceed to “Configuring Proxy Handling” on page 37.

Otherwise proceed to “Configure IIS Authentication” on page 38.

3.3.7 Client Certificate

In the **Web.config** file, you must set impersonation enabled to “**true**”.

Also, set useCertificates to “**true**”. The default store name, “**My**”, and store location, “**LocalMachine**”, are specified in the same place.

Set the **Authentication mode** to **None**. This also requires authorization to be set to **<allow users=“*”/>** which means allow all users, since the authentication is handled by the application. Remove the <deny users="?" /> line.

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

Note: If you copy the serial number from the certificate dialog, remember to remove the spaces.

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

Enter information in the places seen below.

```
<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>
...
...
```

Save the file.

IMPORTANT: Also make a backup copy of Web.config and store this somewhere safe. You might need it later!

If you wish to set up Proxy proceed to “Configuring Proxy Handling” on page 37.

Otherwise proceed to “Configure IIS Authentication” on page 38.

3.3.8 Configuring Proxy Handling

Proxy handling from the end user’s browser to the web server is handled by the web 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. Proxy username and password are only needed if the proxy server is using Basic authentication. Enter this information in the <value> tags.

The Proxy element of the Web.config file is a part of the standard .NET Framework. More information about this can be found on MSDN. Please see the information there if you need help setting up the parameters that are relevant for 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

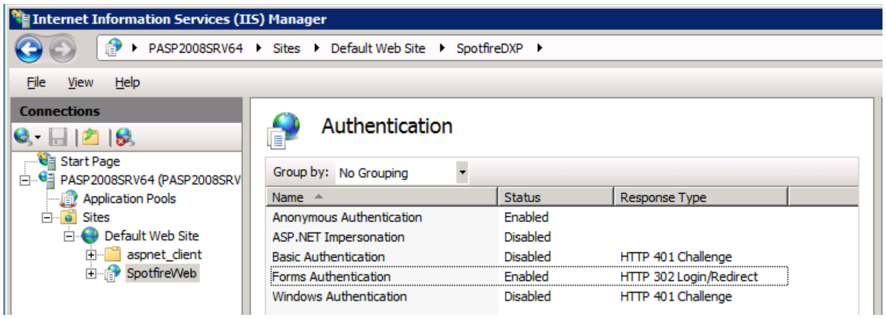
If you are using Anonymous (Preconfigured) access, Single Sign-On authentication, or Client Certificate authentication, you must open the Internet Information Services (IIS) Manager and configure the IIS Authentication.

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

▸ To Configure Authentication on IIS 7 and IIS 8:

1. Select **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. Select **Local computer** > **Sites** > **Default Web Site**.
3. Click on **SpotfireWeb.**
4. Double-click on the **Authentication** icon.

5 **Enable** or **Disable** the appropriate authentication methods.


Internet Information Services (IIS) Manager
PASP2008SRV64 ▸ Sites ▸ Default Web Site ▸ SpotfireDXP ▸
File
View
Help
Connections
Start Page
PASP2008SRV64 (PASP2008SRV
Application Pools
Sites
Default Web Site
aspnet_client
SpotfireWeb
Authentication

Group by: No Grouping

Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Enabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

- **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.

Regarding Username & Password

Since the login validation is made using a login dialog in the ASP.NET layer, the IIS is normally configured to use anonymous access. However, it is of course possible to set the IIS to NTLM to first check that all users are logged into your Windows Domain, and then move on to the ASP.NET layer, where they are required to log in using their Spotfire username/password.

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

3.4.1 Configuring SSL

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

SSL is highly recommended when using Basic and Forms authentication since these options send passwords in plain text.

SSL is required for Client Certificate authentication.

Information on how to set up SSL can be found here: http://technet.microsoft.com

3.5 Verify Web.config

The next thing to do is to once again open the **Web.config** file, placed in the **webroot** folder structure, to verify and potentially correct any unwanted changes.

Whenever Forms Authentication in the IIS is switched between Enabled/Disabled, changes may be made to the Web.config file. Some of these changes are unwanted and, unfortunately, must be corrected afterwards.

▸ Verifying and Correcting Web.config:

1 Open the **Web.config** file in an XML editor or text editor of your choice (it is recommended that you use an XML editor, since some text editors can corrupt the Web.config file. An XML editor will also give a clearer view of the XML code). It is located in the **webroot** folder of the installation, for example:

C:\Program Files\Tibco\Spotfire Web Player\5.5\webroot\Web.config

2 Find the following section of the file:

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

3 Verify that this section matches the settings you have specified. If it doesn’t, the IIS has made changes to it, and you need to change it back to how it was supposed to be.

4 Save the file.

3.6 Additional Authentication Configuration

No further configuration is needed for Username and Password authentication or for Anonymous (Preconfigured) access, since this is set up in the Web.config file and on IIS only. If one of these authentication alternatives is used, proceed to “Deploy Web Packages to Spotfire Server” on page 51.

The four alternatives for Single Sign-On authentication and Client Certificate authentication, require additional configuration on either your Windows Domain Controller, the Microsoft Management Console and/or the Spotfire Server. These alternatives therefore require that you are somewhat 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 41.

- "Single Sign-On Using Impersonation with Kerberos Login System" on page 48.
- "Single Sign-On Using Impersonation with NTLM Login System" on page 49
- "Single Sign-On Using Impersonation with Basic Login System" on page 50.
- "Client Certificate" on page 51.

3.6.1 Single Sign-On Using Delegation with Kerberos Login System

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.
- On a computer with the Windows Support Tools installed (this is typically one of the domain controllers), you must set up the SPNs (**Service Principal Names**) for the Spotfire Server. This must be done by a user which is a member of the **Account Operators** or **Administrators** domain groups.
- On a computer with the Windows Support Tools installed (this is typically one of the domain controllers), you must set up a **keytab file** for the Spotfire Server. This must be done by a user which is a member of the **Account Operators** or **Administrators** domain groups.

3.6.1.1 Configure the Application Pool Identity on the 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, it is highly recommended to run the application pool as a custom user account when using delegation. Follow the instructions in this chapter to set this up.

Create a Custom User Account

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

▸ To Create the Custom User Account:

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

2 Locate the organizational unit where the account should be created.

3 Right-click on the organizational unit and select **New > User**.

4 Enter **Full name** and **User logon** names.

Comment: It is highly recommended to 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.

5 Click **Next**.

6 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**.

7 Click **Next**.

8 Click **Finish**.

Configure Privileges for the Custom User Account

The following steps are done on the Spotfire Web Player Server. You need to add the custom user account to the local **Administrators** group.

▸ To Add the Account to the Local Groups:

1 Select **Start > Administrative Tools > Computer Management**.

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

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

Configure the Application Pool Identity

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

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

2 Select **Local computer > Application Pools**.

3 Select **TIBCO Spotfire Web Player Pool**.

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

5 Select **Identity** and click **...**

6 In the **Application Pool Identity** dialog, select **Custom account** and click **Set...**

7 Enter the custom user account's name and password.

8 Click **OK** three times.

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

10 Double-click **Authentication**.

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

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

13 Finally, you need to 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)

Next you need to make sure that the IIS running Spotfire Web Player has the proper registered Service Principal Names.

- If the IIS is accessible at http://servername or http://servername.domain.tld (tld = Top Level Domain, such .com or .local) and the web application pool is running as Network Service, no action is required since default SPNs will apply.
- If the web application pool hosting the Spotfire Web Player is running under a custom user account, both SPNs –
HTTP/servername and HTTP/servername.domain.tld – need to be mapped to that custom user account.
IMPORTANT: If those HTTP SPNs are already mapped to any other account, they must be removed.
- If the Spotfire Web Player is accessible at additional hostnames
(e.g., www.domain.tld) then an SPN must be registered for that hostname too. That is, you must register an SPN for each DNS A record. However, no SPNs should be registered for any DNS CNAME records.

▸ To add an SPN using SetSPN for:

A servername mapped to a custom user account:

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

An additional hostname mapped to a computer account:

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

An additional hostname mapped to a custom user account:

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

Removing old SPNs

If you have used a custom user account for the application pool and change to a pre-defined account, the old SPNs must be removed. This is done by giving the same setspn commands, but with the option **-D** instead of -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).

To verify that IIS can be reached with an FQDN:

1 On the domain controller, open a command prompt by selecting **Start > Run**.

2 Enter **CMD** and click **OK**.

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

```
ping mywebserver.mydomain.ms.local
```

You will get a response saying whether the operation was successful or not.

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 privileges must have been enabled on the Domain Controller for the computer or custom user account which the application pool is running under.

To Enable 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 Right-click the account name, and then click **Properties** to open the computer properties for the IIS computer.

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

▶ To Enable Unconstrained Delegation for a Custom 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 custom user account.

4 Right-click the account name, and then click **Properties** to open the account properties.

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

6 Click **Apply**.

▶ To Enable 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 Right-click the account name, and then click **Properties** to open the computer properties for the IIS computer.

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

▶ To Enable Unconstrained Delegation for a Custom 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 custom user account.

4 Right-click the account name, and then click **Properties** to open the account 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.

▶ To Enable 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. Right-click the account name, and then click **Properties** to open the computer properties for the IIS computer.
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 TIBCO Spotfire Server has a keytab for and the SPNs are mapped to. (See “Set Up Kerberos on the Spotfire Server” on page 41.)
9. Select all services that apply and click **OK**.
10. Click **Apply**.

▶ To Enable Constrained Delegation for a Custom User Account:

1. On the Domain Controller, select **Start > Programs > Administrative Tools**.
2. Select **Active Directory Users and Computers**.
3. Locate the custom user account.
4. Right-click the account name, and then click **Properties** to open the account 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 TIBCO Spotfire Server has a keytab for and the SPNs are mapped to. (See “Set Up Kerberos on the Spotfire Server” on page 41.)
9. Select all services that apply and click **OK**.

10 Click **Apply**.

11

Spotfire Web Player Server Requirements

These settings need to be configured on the Web Player Server.

1 Under **Control Panel > Network and Internet > Internet Options > Advanced** the option "**Enable Integrated Windows Authentication (Requires Restart)**" must be checked.

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

Internet Explorer Client Requirements

These settings need to be configured on every end-user computer.

1 Under **Tools > Internet Options > Advanced** the option "**Enable Integrated Windows Authentication (Requires Restart)**" must be checked.

2 The Web Player Server you are connecting to must be located in the "**Intranet**" Security zone. If the website is located in the "Internet" zone, IE will not even attempt Kerberos authentication. This is because, in most Internet scenarios, a connection with a domain controller cannot be established. The simple rule is that any website 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 use IE's settings or Group Policy to add this site to the Intranet security zone. (For more information on how IE determines what zone the website is in please see KB 258063.)

Mozilla Firefox Client Requirements

These settings need to be configured on every end-user computer.

1 In Firefox, enter the following in the address field:

```
about:config
```

2 Set the values of the following parameters to the URL of the Web Player Server 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 51.

3.6.2 Single Sign-On Using Impersonation with Kerberos Login System

Create an Impersonation Account on the Domain Controller

The account you intend to use for Impersonation must be present on the Domain Controller. Access the Domain Controller and create or verify that the account you intend to use is available.

Note: It does not need to have Delegation privileges.

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.
- On a computer with the Windows Support Tools installed (this is typically one of the domain controllers), you must set up the SPNs (**Service Principal Names**) for the Spotfire Server. This must be done by a user which is a member of the **Account Operators** or **Administrators** domain groups.
- On a computer with the Windows Support Tools installed (this is typically one of the domain controllers), you must set up a **keytab file** for the Spotfire Server. This must be done by a user which is a member of the **Account Operators** or **Administrators** domain groups.
- The Impersonation username specified on the Domain Controller must also be configured for **impersonation on the Spotfire Server**.

Spotfire Web Player Server Requirements

These settings need to be configured on the Web Player Server.

1 Under **Control Panel > Network and Internet > Internet Options > Advanced** the option "**Enable Integrated Windows Authentication (Requires Restart)**" must be checked.

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

Internet Explorer Client Requirements

These settings need to be configured on every end-user computer.

1 Under **Tools > Internet Options > Advanced** the option "**Enable Integrated Windows Authentication (Requires Restart)**" must be checked.

2 The Web Player Server you are connecting to must be located in the "**Intranet**" Security zone. If the website is located in the "Internet" zone, IE 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 website 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 use IE's settings or Group Policy to add this site to the Intranet security zone. (For more information on how IE determines what zone the website is in please see KB 258063.)

Mozilla Firefox Client Requirements

These settings need to be configured on every end-user computer.

1 In Firefox, enter the following in the address field:

```
about:config
```

2 Set the values of the following parameters to the URL of the Web Player Server that you want to activate Negotiate for.

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

Proceed to “Deploy Web Packages to Spotfire Server” on page 51.

3.6.3 Single Sign-On Using Impersonation with NTLM Login System

Create an Impersonation Account on the Domain Controller

The account you intend to use for Impersonation must be present on the Domain Controller. Access the Domain Controller and create or verify that the account you intend to use is available.

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

Note: It does not need to have Delegation privileges.

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

These settings need to be configured on the Web Player Server.

1 Under **Control Panel > Network and Internet > Internet Options > Advanced** the option "**Enable Integrated Windows Authentication (Requires Restart)**" must be checked.

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

Internet Explorer Client Requirements

These settings need to be configured on every end-user computer.

1 Under **Tools** > **Internet Options** > **Advanced** the option "**Enable Integrated Windows Authentication (Requires Restart)**" must be checked.

2 The Web Player Server you are connecting to must be located in the "**Intranet**" Security zone.

Mozilla Firefox Client Requirements

These settings need to be configured on every end-user computer.

1 In Firefox, enter the following in the address field:

```
about:config
```

2 Set the values of the following parameters to the URL of the Web Player Server that you want to activate Negotiate for.

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

Proceed to “Deploy Web Packages to Spotfire Server” on page 51.

3.6.4 Single Sign-On Using Impersonation with Basic Login System

Create an Impersonation Account on the Domain Controller

The account you intend to use for Impersonation must be present on the Domain Controller. Access the Domain Controller and create or verify that the account you intend to use is available.

Note: It does not need to have Delegation privileges.

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 set up to use Database login system, the same impersonation username must be present in the Spotfire Server Database.
- If the Spotfire Server has been set up 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 51.

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 Changing the Access Rights

Changing the access rights on Windows Server 2008 and Windows Server 2012 is done using the Microsoft Management Console.

To Change the Access Rights:

1 Start the Microsoft Management Console.

2 Add the **Certificates** snap-in for the **Local Computer**.

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 51.

3.7 Deploy Web Packages to Spotfire Server

Any hotfix that is released for Spotfire 5.5 must be deployed as a package to the Spotfire Server. You can download the hotfix from the TIBCO Spotfire hotfix download site, http://support.spotfire.com/patches.asp.

To deploy a hotfix, extension, or upgrade to the Web Player, follow the instructions in the chapter “Deploying Extensions and Upgrades” on page 57.

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

3.8 Set up 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 needed to open an analysis from the Spotfire Web Player.
- **Open from Library -** this license function is needed to open an analysis saved in the library.
- **Open Linked Data** - this license function is needed to open an analysis which has linked data.
- **Save Spotfire Analysis File -** this license function is needed for a user to be able to open the current Web Player file for further 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**".

▶ To Configure 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 you want to configure the licenses for.
5. Click on 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 Privileges

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 have set up Spotfire Web Player to use anonymous/preconfigured authentication, then you will only need to set up access rights for the single preconfigured user that everyone will automatically log in as. If you have set up authentication so that each user will be logged in with her own credentials, you must set up access rights for all users (or groups of users).

▸ To Set Up Spotfire Library Privileges:

1 Start TIBCO Spotfire.

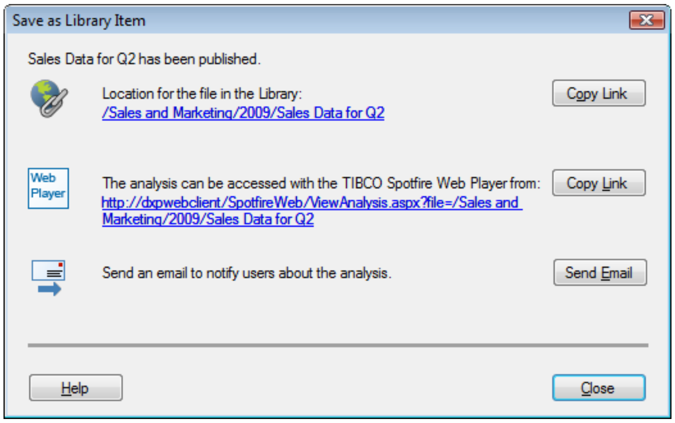
2 Select **Tools > Library Administration**.

3 For information on how to create library sections and folders, and how to set up access rights to these, see the section **Library Administration** in the TIBCO Spotfire online help which is reached by clicking **Help**.

3.9 Set up 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 instructions.

If you set this up correctly, the user can copy the URL and email it to other users, who can open the analysis in Spotfire Web Player.



Save as Library Item

Sales Data for Q2 has been published.

Location for the file in the Library:
/Sales and Marketing/2009/Sales Data for Q2

The analysis can be accessed with the TIBCO Spotfire Web Player from:
http://dxpwebclient/SpotfireWeb/ViewAnalysis.aspx?file=/Sales and Marketing/2009/Sales Data for Q2

Send an email to notify users about the analysis.

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

It is strongly recommended 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...**.

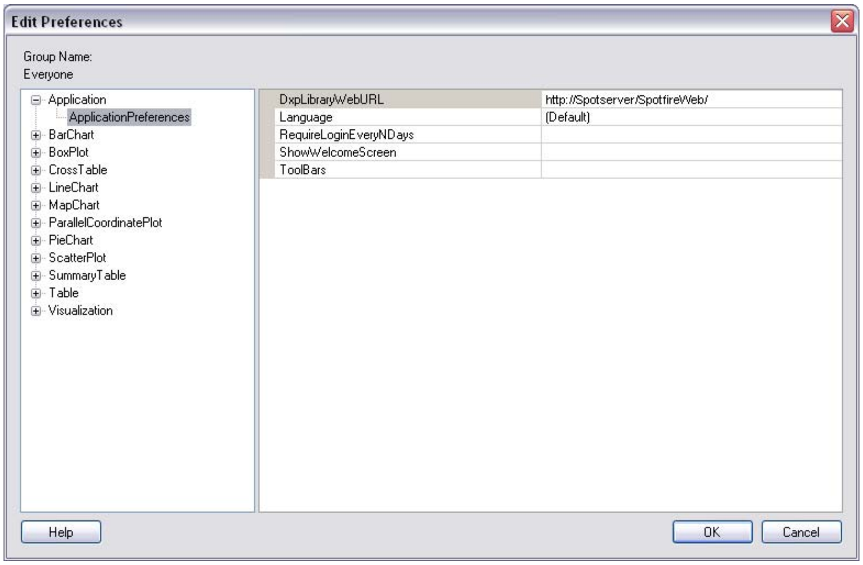
4 Select the **Preferences** tab.

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.



Group Name:
Everyone

DxpLibraryWebURL	http://Spotserver/SpotfireWeb/
Language	(Default)
RequireLoginEveryNDays	
ShowWelcomeScreen	
ToolBars	

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.

3.10 Install Hotfixes

Before you continue, please check if any hotfixes have been released for this version of the server. If hotfixes are available, deploy them to the TIBCO Spotfire Server and then use the upgradetool to deploy them to the Web Player server. Use the following procedure to install the hotfixes.

To install hotfixes

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

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

   When you have installed the hotfixes, the next step is to test the installation. See "Testing the Installation" on page 62.

4 Upgrading

4.1 Upgrading to New Version

Upgrading from TIBCO Spotfire Web Player 5.0.1 or earlier to TIBCO Spotfire Web Player 5.5 basically consists of uninstalling the old version and then installing the latest one.

Performing an upgrade is therefore almost identical to performing a new installation as described in the chapter “Installing TIBCO Spotfire Web Player” on page 26. The new version 5.5 installer will 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 set up 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.

▸ To Upgrade to Spotfire Web Player 5.5:

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 “Installing TIBCO Spotfire Web Player” on page 26.

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\5.0.1\

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 5.5 installer files to a temporary folder 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 old Spotfire Web Player will be automatically uninstalled and the new Spotfire Web Player 5.5 will be installed.

5 Edit the new Web.config in that folder 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 5.5 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 Set up Licenses and Library Rights (as described in the Installation chapter).

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

9 If you have any custom extensions on your old Spotfire Web Player Server, you will need to deploy these again on the newly installed version. However, if the extensions were not deployed as packages on the old 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".
Secondly, 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 Web Player Server (see “Deploying Extensions and Upgrades” on page 57).

10 Any changes made to the ScheduledUpdates.xml must also be transferred to the new version of this file (see “Upgrading an Existing Schedule” on page 93).

11 If you have customized the Header Banner (see “Customizing the Header Banner” on page 64), reapply these modifications.

12 Clean up potential remaining files in the old installation directory.

13 Done!

4.2 Applying Hotfixes

To download the latest hotfix, go to http://support.spotfire.com/patches.asp. Each hotfix package includes installation instructions. For more information, see “Install Hotfixes” on page 54.

4.3 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 .bat file, called **webupdate.bat**, which is run from the Web Player server. It connects to the Spotfire Server specified in the Web.config file, and the authorization for the Spotfire Server is specified in the .config file of the upgrade tool.

Configure the Upgrade Tool

To use the upgrade tool, you first need to specify certain information in the .config file of the upgrade tool.

The file, **Spotfire.Dxp.Web.UpgradeTool.exe.config**, can be found in the **webroot\bin\Tools** folder of the installation. Below are the available settings in the .config file. 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\5.5\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 .bat file as a user with the proper permissions for the Spotfire Server. **Note**: It is possible to encrypt the information in this .config file. This is done by running the file **Spotfire.Dxp.Web.UpgradeTool.exe**, also located in the Tools folder, in the command prompt with the flag **/protectSettings** after you've configured the .config file. Then you run the .bat 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_User name	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 folder 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: Any deployment area to which the value that you specified in the `Credentials_Username` setting can access. 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_Store Name	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_Store Location	Specify the location to get the certificate from. Default value: CurrentUser. Other valid values: LocalMachine. Enter this information in the <value> tags.
Certificate_Serial Number	Specify the serial number of the certificate. Enter this information in the <value> tags.
<Spotfire.Dxp.Internal.Properties.Settings>	
ManifestDownload TimeoutMilliseconds	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.

Run the Upgrade Tool

After configuring the **Spotfire.Dxp.Web.UpgradeTool.exe.config** file, you must run the **webupdate.bat** file, which you can find in the **webroot\bin\Tools** folder.

Run the batch file with a user account that has “Deployment Administrator” or “Administrator” credentials so that the batch file operations have proper permissions for the Spotfire Server. Make sure that this user account has permission to start and stop IIS on the 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 specific times using the **Task Scheduler** on the Web Player server.

If you encounter any problems you can review the log files at C:\Program Files\TIBCO\Spotfire Web Player\5.5.0\webroot\bin\Tools\Spotfire.Dxp.Web.UpgradeTool.log.

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.

Response: 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.

Response: The data is loaded and a visualization appears.

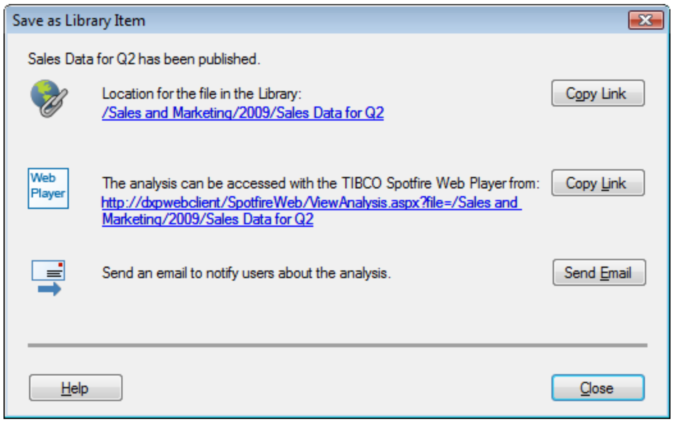
5 Select **File >Save As... > Library Item...**

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 In the dialog that appears, verify that there is a link to the Spotfire Library and also directly to the published file.



Save as Library Item

Sales Data for Q2 has been published.

Location for the file in the Library:
/Sales and Marketing/2009/Sales Data for Q2

The analysis can be accessed with the TIBCO Spotfire Web Player from:
http://dxpwebclient/SpotfireWeb/ViewAnalysis.aspx?file=/Sales and Marketing/2009/Sales Data for Q2

Send an email to notify users about the analysis.

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**.

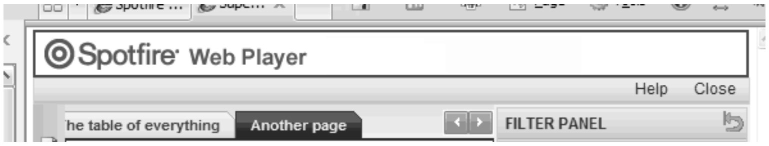
A simpler option is to test the installation from another, stand-alone computer.

6 Advanced Procedures and Technical Reference

6.1 Customizing the Header Banner

The top header of the Spotfire Web Player analyses can be customized to show your company's logotype.

The customization is done through the **Header.htm** file in the **App_Data** folder of the installation directory. This file is a part of an XHTML file; it should only contain the xhtml of the visible part, NOT the HTML, HEAD and BODY tag. The xhtml is then merged into the top of all the pages (the outlined part in the image below) and displayed to the user.



The default xhtml looks like the following:

```
<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 it, change the Header.htm file in the installation folder before installing the product, or modify the file after installation, then located in the App_Data folder of the web root.

To change the height of the header banner, see position 5 under "Advanced Web.Config Settings" on page 65.

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).

6.2 Advanced Web.Config Settings

```
    <spotfire.dxp.web>
      <!-- ************************************************************
        Web Player settings for non visible items -->
      <setup>
①       <!-- 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
②         emailAddress="spotfireadmin@yourcompany.com"
          maxMailLength="1000"
          automaticallyShutDownAfterStartupFailureAfterMinutes="5"/>


③       <authentication serverUrl="http://spotserver/" enableAutocomplete="false">
        </authentication>
      </setup>

      <!-- ************************************************************
        This section contains settings for the user interface of the Web Player -->
      <userInterface>
④       <pages showLogout="true" showAbout="true" showHelp="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" />
        <errorPage showOpenLibrary="true" showReopenAnalysis="true" />
        <serverUnavaliable showOpenLibrary="true" showReopenAnalysis="true" />
      </userInterface>

      <!-- ************************************************************
        This section contains setting for tuning performance.
        Be careful when making changes. -->
      <performance>
⑤       <documentCache purgeInterval="300"
                       itemExpirationTimeout="00:00:00"/>

        <analysis checkClosedInterval="60"
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"
                userPreferencesMaxAge="00:05:00" />

      <hierarchicalClustering maxInteractiveElements="2000"
7                             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>
8  <!-- 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>

  <applicationSettings>
9   <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">
        <value></value>
      </setting>
      <setting name="AllowedFilePaths" serializeAs="Xml">
        <value>
          <ArrayOfString>
            <string/>
          </ArrayOfString>
        </value>
      </setting>
    </Spotfire.Dxp.Data.Properties.Settings>
  </applicationSettings>
```

The above example shows a variety of settings you can add and edit in your **Web.config** file. These settings are explained below.

Open the **Web.config** file in an XML editor or text editor of your choice (it is recommended that you use an XML editor, since some text editors can corrupt the Web.config file. An XML editor will also give a clearer view of the XML code). It is located in the **webroot** folder of the installation, for example:

```
C:\Program Files\Tibco\Spotfire Web Player\5.5\webroot\Web.config
```

Important: When you make changes to the Web.config file and save it, IIS will automatically detect this and restart the Spotfire Web Player application. This means all users logged into the Spotfire Web Player will be disconnected.

Position	Tag (With Default Value)	Explanation
1	`<javaScriptApi enabled="false" />`	Enables or disables the Spotfire Web Player Javascript API. For example, this needs to be enabled to allow users to share and view embedded analyses using the Copy Link or Embed Code tool in the Web Player. The domain of the web player pages can be controlled by setting the domain attribute on the javaScriptApi tag to the desired domain name: <javaScriptApi enabled="true" domain="example.com" /> For more information, please see Spotfire Technology Network (http://spotfire.tibco.com/stn).
2	`<errorReporting>`	
	`emailAddress= "spotfireadmin@yourcompany.com"`	When a user encounters certain server related errors a dialog is shown. This has a mailto link "Report error to administrator" which the affected user can click to send an email to the responsible administrator. This email will automatically include the error log. This email address is specified here.
	`maxMailLength="1000"`	You can limit the maximum number of letters in the email that get sent when a user clicks on the "Report error to administrator" link. This can be useful when emailing to an email address residing on a Lotus Notes system which can have a limit of 2000 letters.

	`automaticallyShutDownAfterStartupFailureAfterMinutes="5"`	Specify the number of minutes the Web Player will wait before trying to restart if there has been an error during startup. This is useful if, for instance, the Spotfire Server is down for maintenance. Do not set this to anything lower than 2, because if the web player is restarted a number of times during a short period of time the IIS might disable the application pool.
3	`<authentication>`	
	`serverUrl= "http://spotserver/"`	This is where you can specify the URL to the Spotfire Server which is to be used with the Spotfire Web Player. It is specified during the installation, but can be changed here.
	`enableAutocomplete="false"`	Set this to true to allow the option to save passwords in the browser and to show auto complete suggestions for usernames in the login dialog.
4	`<pages showLogout="true" />`	Set this to true to enable the Log out menu item in the top right menu of the web player.
	`<pages showAbout="true" />`	Set this to true to enable the About Spotfire Web Player menu item in the top right menu of the web player.
	`<pages showHelp="true" />`	Set this to true to enable the Help menu item in the top right menu of the web player. That menu item launches the help system for the web player.
	`<diagnostics> errorLogMaxLines="2000" />`	Maximum number of lines of the error log files shown in the diagnostics page (1000-50000).
	`<analysis>`	
	`showToolTip="true"`	Show highlighting tooltips in visualizations (disable to increase performance).
	`showClose="true"`	Set this to true to enable the Close menu item in the top right menu of the web player.
	`showToolBar="true"`	Set this to true to show the menu and the Refresh/Reload, Collaboration, Bookmark and Filter buttons in the tool bar of the web player. **Note**: If this is set to false, users of the web player will not be able to use any of the functionality found in these controls. **Note**: If this AND showPageNavigation are set to false, the entire grey top bar of the web player will disappear.

	`showAnalysisInformationTool="true"`	Set this to true to enable the Analysis Information menu item in the top right menu of the web player.
	`showExportFile="true"`	Set this to true to enable the Open in TIBCO Spotfire menu item in the top right menu of the web player.
	`showExportVisualization="true"`	Set this to true to enable the Export Visualization Image menu item in the top right menu of the web player. This also shows/hides the menu item in the visualization menu.
	`showUndoRedo="true"`	Set this to true to enable the Undo/Redo menu items in the top right menu of the web player.This also enables/disables undo in the visualization.
	`showDodPanel=""`	Leaving this setting blank “” will show the DoD if it is saved in the analysis file. Setting it to “false” will hide the DoD on all pages in all analyses. Setting it to “true” will force the DoD to appear on all pages in all analyses.
	`showFilterPanel=""`	Leaving this setting blank “” will show the Filters if it is saved in the analysis file. Setting it to “false” will hide the Filters on all pages in all analyses. Setting it to “true” will force the Filters to appear on all pages in all analyses.
	`showPageNavigation="true"`	Show/Hide the Page tabs (or page links) in analyses. Hiding them will only show the currently active Page as saved in the analysis. **Note**: If this AND showToolBar are set to false, the entire grey top bar of the web player will disappear.
	`showStatusBar="true"`	Show/Hide the status bar.
	`showPrint="true"`	Set this to true to enable the Print menu item in the top right menu of the web player.
	`allowRelativeLinks="false"`	Set this to “true” to treat incomplete links in the web player as relative to the library root folder. False will instead add “http://” to all incomplete links.
	`<customHeader>`	
	`enabled="false"`	Show/Hide the custom header with logo.
	`height="40"`	Set the height of the custom header (in pixels).
	`<closedAnalysis>`	

	showOpenLibrary="true"	Show/Hide the Open Library link on the Closed Analysis page.
	showReopenAnalysis="true"	Show/Hide the Reopen Analysis link on the Closed Analysis page.
	<errorPage>	
	showOpenLibrary="true"	Show/Hide the Open Library link on an error page.
	showReopenAnalysis="true"	Show/Hide the Reopen Analysis link on an error page.
	<serverUnavaliable>	
	showOpenLibrary="true"	Show/Hide the Open Library link on the Server Busy page.
	showReopenAnalysis="true"	Show/Hide the Reopen Analysis link on the Server Busy page.
5	<documentCache>	
	purgeInterval="300"	The frequency with which the server should search for unused open documents (templates) to be purged (seconds, 60 - 3600).
	itemExpirationTimeout="00:00:00"	The length of time a document should remain in the cache when no open analysis uses that document template (HH:MM:SS, 00:00:00 - 23:59:59).
6	<analysis>	
	checkClosedInterval="60"	This setting determines how often the server should check if an analysis has been closed on the client (seconds, 60 - 300).
	closedTimeout="120"	This setting determines how long an analysis session will stay alive on the server when a ping fails (seconds, 60 - 600).
	checkInactivityInterval="300"	This setting determines how often the server should check if an analysis session has had no user activity (pings not counted) (seconds, 60 - 12*3600).
	inactivityTimeout="Infinite"	This setting determines the how long an analysis session should be alive on the server when the no user activity has been detected (pings not counted) (HH:MM:SS, 00:01:00 - Infinite).
	regularPollChangesInterval="500"	This setting determines the base interval from when a change is made on the client to when the client polls the server for a status update (ms, 200 - 1000).

	`maxPollChangesInterval="3000"`	The poll interval in RegularPollChangesInterval, is increased for each try until this value is reached (ms, 1000 - 10000).
	`pollLoadInterval="1000"`	The interval between polls when loading an analysis (ms, 1000 - 10000).
	`needsRefreshInterval="15"`	The frequency with which the client should ping/poll the server to keep the analysis alive (seconds, 10 - 60).
	`toolTipDelay="1000"`	The length of time the client must wait before asking the server for a visualization highlighting tooltip (ms, 200 - 3000).
	`antiAliasEnabled="true"`	By default, all the graphics in the Spotfire Web Player are rendered with anti-aliasing turned on. This produces a nicer and clearer look. However, anti-aliasing imposes a slight performance decrease for visualizations that consist of a large amount of graphical objects. It is therefore possible to turn off anti-aliasing, if this is considered an issue. The recommendation is to leave anti-aliasing enabled.
	`useClearType="true"`	By default, graphics in the Spotfire Web Player are rendered with ClearType turned on. This produces a nicer and clearer look for graphics that contains letters. However, ClearType imposes a slight performance decrease. It is therefore possible to turn off ClearType, if this is considered an issue. The recommendation is to leave ClearType enabled.
	`documentStateEnabled="true"`	Enables the users to resume the state of files they have previously been working on.
	`undoRedoEnabled="true"`	Enable or disable Undo/Redo.
	`userServicesPoolEnabled="true"`	Set this to true to enable the user services pool. This reduces the number of web service calls to the server by only creating one set of user services, such as preferences and licenses, for each user. This is especially useful if the users are logged in anonymously to the web player as they are all technically logged in as the same user.
	`userPreferencesMaxAge="00:05:00"`	Specify how often the preferences and licenses should be synchronized when additional users log in to the web player. (HH:MM:SS)
7	`<hierarchicalClustering>`	

	maxInteractiveElements="2000"	The maximum number of rows or columns of a hierarchical clustering that can be started interactively in the web player.
	maxElements="30000"	The maximum number of rows or columns of a hierarchical clustering that can run on the web player server. Scheduled updates can run hierarchical clustering up to this size.
	maxInteractiveJobs="2"	The maximum number of interactive clustering jobs running in parallel.
	cpuFactorInteractiveJobs="0.8"	On a multi-core web player server computer this is used to estimate the number of threads the clustering will use for interactive jobs.
	cpuFactorLargeJobs="0.5"	On a multi-core web player server computer this is used to estimate the number of threads the clustering will use for scheduled update jobs.
	nativeMemory="500" />	A memory limit for the clustering algorithm. The default value 500 (MBytes) is matching maxElements = 30000.
8	<Spotfire.Dxp.Services.Settings>	
	<cookies autoTransfer="" />	If you use a load balancer or proxy that requires specific cookies to be sent on all requests to the Spotfire Server, add these here. Cookies are separated with **;**.
9	<applicationSettings>	
	<Spotfire.Dxp.Internal.Properties.Settings>	
	ManifestDownloadTimeoutMilliseconds	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	Set this to true to enable caching of metadata about items in the library. This reduces the number of web service calls to the server since metadata is retrieved from the cache instead of from the server. The cache is unique for each user. This is especially useful if the users are logged in anonymously to the web player as they are all technically logged in as the same user. The default value is True.
	LibraryCache_MaxCacheTime	Specify how long the metadata will be cached for. (HH:MM:SS) The default value is ten minutes.

	`<Spotfire.Dxp.Data.Properties.Settings>`	
	`DataBlockStorageIOSizeKB`	If you have a RAID system on your Spotfire Web Player server, you can improve write performance by adjusting this setting. Change the value of this setting to twice the RAID stripe in KB. Also, make sure that the RAID write cache is enabled on your server computer. The default value is 64.
	`DataOnDemand_MaxCacheTime`	If you have set up data on demand to be cached on the web player server, this value determines how long the data will be cached. The default value is one hour.
	`AllowedWebRootFiles`	If you have files located in the web player installation folder, for example `C:\Program Files\Tibco\Spotfire Web Player\5.5\`, or any of it's subfolders you must specify them in the value tags for this setting to be able to access them in the web player. Files are separated with **;**. All paths are relative to the webroot folder. Example: `<value>..\Logfiles\PerformanceCounter.txt;..\Logfiles\Spotfire.Dxp.Web.log</value>`

	`AllowedFilePaths`	If you have files located in any other location than the web player installation folder you must specify these folders or files in the value tags for this setting to be able to access them in the web player. Each file or folder should be specified in a separate string tag.
		Example:
		`<value>`
		`<ArrayOfString>`
		`<string>C:\MyData\</string>`
		`<string>C:\Logs\spotfire.txt</string>`
		`</ArrayOfString>`
		`</value>`

6.3 Setting up Language Support

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

If you deploy a Japanese or another East Asian 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 in the Web Player, you must specify the authentication method for how the users will connect to the external data sources in the **Web.config** file.

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. Depending on if the analysis was set up using Windows Authentication or Database Authentication the authentication methods will differ.

Windows Authentication

- WebConfig – select this to make all users 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 set up 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 custom user account that is used to run the application pool in the IIS on the 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 be used regardless of authentication method chosen 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 chosen 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 selected above, you need to specify the username and password for a credentials profile in the DataAdapterCredentials section in the Web.config file, shown below. Multiple profiles with different credentials can be added.

```
<!-- 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 seen 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 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 set this up, a credentials profile is added 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 specified in the Credentials tab in the Data Connection Properties dialog in TIBCO Spotfire.

6.5 TIBCO ActiveSpaces Data Source

You can configure TIBCO ActiveSpaces 2.0.2 as a Spotfire Data Source but to complete the integration you must install ActiveSpaces on the Spotfire Professional computer or Spotfire Web Player server.

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

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

▶ Copying ActiveSpaces files to Spotfire folder

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

   - as-common.dll
   - as-core.dll
   - as-tibpgm.dll
   - as-tibrv.dll
   - TIBCO.ActiveSpaces.Common.dll

2. Copy these files to the Spotfire Web Player virtual directory.

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

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

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

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

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

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

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

5 Finally, you should run the upgrade tool to apply these upgrades. For more information see, “Deploying Extensions and Upgrades” on page 57.

6.6 TIBCO Spotfire Statistics Services

Web player analysis files can contain data functions executing on TIBCO Spotfire Statistics Services. If Spotfire Statistics Services requires authentication, you need to specify these authentication settings in the **Web.config** file. This is done by entering the Spotfire Statistics Services URL and the username and password for Spotfire Statistics Services.

Note: You can specify URLs, usernames and passwords for several Spotfire Statistics Services, by adding additional rows to each of the settings.

Note: The URLs must be specified exactly the same for the Spotfire Web Player Server and the Spotfire Server. For example, FQDN must be used in both cases, or neither of them.

Enter information in the places seen below:

```
<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>
```

6.7 Scheduled Updates

What are Scheduled Updates?

Scheduled Updates can reduce the time it takes for a user to open certain analysis files because it preloads the 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 is preloaded, the analysis opens much faster.

Scheduled Updates are also useful in the case of a large analysis with a lot of data that users might need to open several times during the day to check for figures or similar information. Instead of having to load this analysis into memory every time a user opens it, you can ensure this analysis is always available in memory, providing a rapid response for the users.

With Scheduled Updates, you can 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.

Additionally, the Spotfire Professional users can specify which data files they want to have updated.

Event-Driven Updates

The Spotfire Web Player can update the pre-loaded analysis in one of two ways:

- Create an update on a schedule (for example, one that occurs every 30 minutes).
- Use event-driven updates.

When an update is event driven, it means that the update is triggered, not by a specific time, but by a message sent from a web service or TIBCO Enterprise Message Service (TIBCO EMS).

To enable event-driven updates, you must enable Scheduled Updates and then apply the appropriate event-driven update settings to the Web.config file (see “Edit Web.config” on page 82) and configure and start the keep alive service. (See “Configure and Start the Keep Alive Service” on page 87.)

To use TIBCO EMS MapMessages notifications, you must install a TIBCO EMS server on the Spotfire Web Player server.

Note: For information on how to install the TIBCO EMS server, refer to the **TIBCO Enterprise Message Service Installation and Configuration** manual.

Note: For details on using TIBCO EMS, see the **TIBCO Enterprise Message Service User’s Manual**.

If TIBCO EMS is not installed or correctly configured, the services *webplayer* and *keepalive* operate normally, but because the TIBCO EMS notifications are not configured, the logging service writes messages to the *webplayer* and *keepalive* logs reporting that TIBCO EMS is missing.

You can verify that the TIBCO EMS client-side DLL is available on the Spotfire Web Player server by interrogating the Global Assembly Cache (GAC) using the following command with the Microsoft Global Assembly Cache Tool (gacutil.exe):

```
gacutil.exe /L TIBCO.EMS.dll
```

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 that she 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 it can come from any linkable data source.

2. The analyst asks the administrator of the TIBCO Spotfire Web Player server to create a Scheduled Update for the analysis file she created because she wants to make sure this analysis is preloaded each morning when the sales department checks the results from the previous day.

3. The administrator configures the TIBCO Spotfire Web Player:

   a He adds the analysis file to the list of analyses to be scheduled for updates.

   b He sets it to be loaded automatically at 4 in the morning because 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.

   c He determines that it should be kept in memory continually for the remainder of the working day, until 8 pm.

   Note: Users can specify in the **Data Table Properties** that the file is refreshed only with data specific to the sales department (in our example case).

   The administrator must also specify a “user” to log into the TIBCO Spotfire Server automatically and access the Spotfire Library to preload the analysis. Technically, this user needs access to any files scheduled for updates. However, the administrator is careful to pick a user account whose privileges are as limited as possible (see also “Concerning Prompted and Personalized Information Links” on page 80).

4. The administrator tells the analyst that the analysis is now scheduled for updates, as requested.

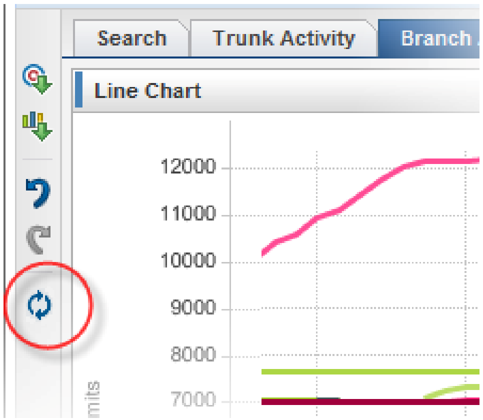
5. The analyst sends an email (containing the URL to the new analysis) to the sales department and tells them that, from now on, they can check the sales figures from the previous day by clicking the link.

6. At midnight, the company database is updated with the sales figures that were reported during the day. At 4 a.m., 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.

7 The following morning, the sales people check their email, read the message from the analyst, and click the link. The web browser launches, and the analysis is displayed immediately on screen, showing the sales results for the previous day. Because the data is preloaded on the server, the sales people do not need to wait for it to load from the company database.

8 The next midnight, the company database is updated with new numbers. At 4 a.m. the analysis is preloaded with the new data on the TIBCO Spotfire Web Player server and the sales people can access it the next morning as usual.

If a user has the analysis open in a web browser overnight, a small icon appears on the screen after the Scheduled Update has occurred on the server.



This icon prompts the user that an updated version of the analysis is available, and clicking the icon refreshes the analysis with the latest data.

Concerning Prompted and Personalized Information Links

Scheduled Updates are intended mainly 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.

When a user opens an analysis that is based on a prompted information link, the user selects 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 is determined by the privileges of the user who logs in.

However, when a Scheduled Update for this analysis occurs, that update causes the analysis to reload based on the prompted values specified when the file was originally saved, and for the privileges of the user that the administrator set up to programmatically run the Scheduled Update.

As a result, a user with an analysis already open sees a different selection of data the next time she updates the analysis, because the Scheduled Update has updated the underlying data on the server.

You must be especially careful if you are creating 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 (in other words, they see all the data that the user specified for Scheduled Updates has access to).

Concerning Updating Analyses Using Data Specified by Role

Your users might have analysis files that contain shared data tables that need reloading only at specified scheduled times, but also data that must be reloaded on a per-user level or per-role level. For example, your sales people might be interested in only the sales data for their individual regions, but they might also want to compare this data with the general customer database. From the Spotfire Professional, an individual user accesses the **Data Table Properties** dialog, and then using the **Scheduled Updates** tab, configures the data source to be reloaded according to her needs.

For these situations, the Scheduled Update is made in two steps:

1. Scheduled Updates loads the file for the first time, and all data sources are loaded as the Scheduled Updates user.
2. When the user opens the file, Scheduled Updates reloads only data from data sources that are marked to be reloaded.

If other data sources depend on a data source that should be reloaded, then these data sources are also be reloaded. For example if the table contains a join (add columns) between two data source and one of those is marked for reloading, then that data source is reloaded and the join is performed again.

This technique is useful for user/role specific data, and it can be used improve performance when a user opens analysis files that contain a combination of unchanging and dynamic data. That is, by using the two-step scheduled updates, you can use Scheduled Updates to fetch stable data from (for example) a data warehouse and combine it with dynamic data, such as stock prices or recent sales data. By marking the dynamic data to be reloaded for all users, you can get up-to-date data while not having to reload the stable data.

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 further granularity when data should be loaded.

For example, consider 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**. As a result, every time a Scheduled Update occurs, the analysis is updated with the latest data from the linked data table. All end users who have the analysis open in their web browsers see the update icon. When they click the update icon, the analysis displayed on their screens is updated with new data. All end users 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. For example, consider that you have an analysis that uses two linked data tables: One data table links to a huge amount of data that is updated only once every midnight. The other data table is smaller, but it 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. You need only the small data table to reload and update every ten minutes, because reloading the huge data table every ten minutes is unnecessary because it remains unchanged the entire day.

When you save 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**.

Next, create a Scheduled Update for the analysis file to load and update every ten minutes, starting at 4 a.m. and ending at 10 p.m.

The first time the scheduled update is run (4 a.m.), both the huge data table and the small data table are loaded as the analysis is opened and kept in memory.

Every ten minutes, the analysis file is updated, but only the small data table is reloaded because the sharing routines specify that the huge data table is loaded only **the first time** the analysis is opened. The sharing routine **always share** indicates that the data table is loaded only the first time a user opens the analysis (in this case, the first Scheduled Update).

Users opening the analysis in their web browsers get a quick response from the server because the analysis is already in memory. Every ten minutes, the Scheduled Update runs on the server, and the end users see the icon stating that they can update the analysis. They click to update the analysis with the latest data. The Scheduled Update is fast, because it reloads only the small data table and not the huge data table.

6.7.1 Setting up Scheduled Updates

Setting up Scheduled Updates is a three-step process. These steps are explained further below.

To upgrade an earlier version of an existing schedule, see “Upgrading an Existing Schedule” on page 93.

▸ To Set up Schedules Updates:

1. Edit Web.config.
2. Configure the Update Schedule.
3. Configure and Start the Keep Alive service.

6.7.1.1 Edit Web.config

First, enable Scheduled Updates in the Web.config file. You can also modify a few settings to configure Scheduled Updates to work in your environment.

In the **webroot** folder of your Spotfire installation, open the file **Web.config** in an XML editor. (We recommend that you use an XML editor, because some text editors can corrupt the Web.config file. An XML editor also provides a clearer view of the XML code.)

Example:

```
C:\Program Files\Tibco\Spotfire Web Player\5.5\webroot\Web.config



<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.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. -->
```

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, 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 folder. This key is supplied by default.
concurrentUpdates	The maximum number of concurrent updates that can be executed simultaneously. 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	Specifies how often the ScheduledUpdates.xml file is read to check for updates to run. Set in seconds. Default value is 60, min value 30, and max value 3600 (=one hour).
<forcedUpdate>	
enabled	It is possible to force updates 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 multiple versions of the analysis to be kept simultaneously. To enable forced updates, set to “true”.
maximumRejected Updates	Specify the number of times a user can be notified of new updates without accepting them, before the update is required.
<externalUpdate>	
keepAliveMinutes	If no schedule has been established for preloading a file, use this key to specify the number of minutes the file should be kept alive.
<webService>	
enabled	To enable updates triggered by a web service, set 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, see the **TIBCO Enterprise Message Service User’s Manual**.
enabled	To enable updates triggered by a message sent from TIBCO Enterprise Message Service, set 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. Use this key to specify another client ID 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, set to 10.
reconnectAttempt DelayMilliseconds	Specify the delay for the reconnect attempts. By default, set to 1000 milliseconds.
reconnectAttempt Timeout Milliseconds	Specify the timeout for the reconnect attempts. By default, set to 1000 milliseconds.
<Spotfire.Dxp.Web. Properties.Settings>	
ScheduledUpdates Username	The username used to access the TIBCO Spotfire Server when updating analysis files. This user must have privileges on the Spotfire Server to access the relevant files, and be a member of the **Scheduled Updates Users** group on the server. If you set up the Spotfire Web Player to use Anonymous (Preconfigured) Access, this user must be the same user you specified for Impersonation (`ImpersonationUsername`) . The user name must contain the domain, so provide the value using the syntax domain\username. Enter this information in the <value> tags. **Note**: If you set up 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 36. To encrypt this credential, see “Encrypting Usernames and Passwords” on page 96.

ScheduledUpdates Password	The user password used to access the TIBCO Spotfire Server when updating analysis files. If you set up 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 set up 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 36. To encrypt this credential, see “Encrypting Usernames and Passwords” on page 96.
EmsUpdateUsername	The username used to access the EMS server. Enter this information in the <value> tags.
EmsUpdatePassword	The user password used to access the EMS server. Enter this information in the <value> tags.

6.7.1.2 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 Scheduled Updates from the dialog in the library overwrites locally-stored **ScheduledUpdates.xml** files.

To upload locally-stored scheduled updates, save the .xml file in a separate location before installing the Spotfire Web Player, and then copy the old .xml file to the folder **TIBCO Spotfire Web Player Installer** before enabling scheduled updates the first time. This uploads the existing scheduled updates to the library.

▸ **To Configure the Update Schedule:**

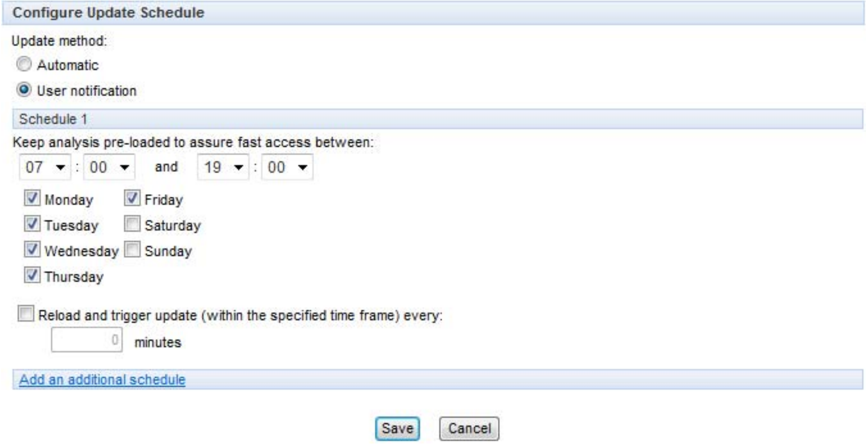
1 In a web browser, enter the address of the web player to access the library.

Note: To be able to configure the update schedule, you must log in either as an administrator or as a web player administrator.

2 In the top right corner, click **Scheduled Updates**.

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

4 Select the file for which to establish a Schedule Update to display the **Configure Update Schedule** dialog:



Configure Update Schedule

Update method:

○ Automatic

● User notification

Schedule 1

Keep analysis pre-loaded to assure fast access between:

07 : 00 and 19 : 00

☑ Monday ☑ Friday

☑ Tuesday ☐ Saturday

☑ Wednesday ☐ Sunday

☑ Thursday

☐ Reload and trigger update (within the specified time frame) every:

0 minutes

Add an additional schedule

5 Specify if the updates are to occur automatically, or if the users can update manually upon notification of a new version.

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 cue helps 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**.

7 Select the frequency for which the Spotfire Web Player should check if the analysis file or its underlying data has changed, and if so, update the pre-loaded instance. Be careful not to set the parameter too low; otherwise, Spotfire Web Player tries to 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 to which it links.

8 Click **Save**.

Note: When setting up your scheduled updates, we recommend that you leave a window of at least an hour each night when nothing is scheduled for updates. This allows the IIS to recycle itself, cleaning up resources and freeing memory, which improves performance.

6.7.1.3 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 Scheduled Updates from running tasks and keeping the specified analysis files instantiated in memory. To avoid this, a Windows service reads the configuration file and pings the Spotfire Web Player to make sure that IIS is running during the periods configured in the schedules.

Note: IIS must periodically restart itself to free memory, so we recommended giving IIS at least an hour of free time every 24 hours.

When the Spotfire Web Player was installed, a Windows Service called **Spotfire.Dxp.Web.KeepAlive.exe** was installed in the Tools folder of the Spotfire Web Player server.

Example**:**

C:\Program Files\TIBCO\Spotfire Web Player\5.5\webroot\bin\Tools

However, it is not activated by default. You must activate it explicitly, after you have set its configuration options in the file **Spotfire.Dxp.Web.KeepAlive.exe.config**, which is located in the same folder.

Open this file in an XML editor or text editor. (W recommend that you use an XML editor, because some text editors can corrupt the Web.config file. An XML editor also provides a clearer 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\5.5\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\5.5\Logs\Spotfire.Dxp.Web.KeepAlive.log"/>
```

Most of the information in this configuration file is prepopulated during installation. However, you should verify that the information is correct. Enter the information in the <value> tags.

Depending on the type of authentication you set up for your Spotfire Web Player, you must also set up the WindowsUserName and WindowsPassword parameters accordingly (see below).

Key	**Description**
SettingsFilePath	The path to the ScheduledUpdates.xml file. By default, the webroot folder of the Spotfire Web Player server.
PingIntervalMinutes	This setting determines how often the Spotfire Web Player is pinged. Do not set this to more than half the time of the “IdleTime-out” settings of the Spotfire application pool in IIS. Specify in minutes.
WindowsUserName	If the IIS running the Spotfire Web Player is set to Anonymous login, leave this value empty. The Keep Alive service is run using the Local System account. If the IIS running the Spotfire Web Player is set to Basic Authentication, enter the user name of a user with privileges to access the IIS 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 must contain the domain, so enter the value using the syntax domain\username
WindowsPassword	If the IIS running the Spotfire Web Player is set to Anonymous login, leave this value empty. If the 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. Usually, this is localhost.
EMS_Enabled	Set to “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, see 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 to access the EMS server.
EMS_Password	The password of the user to access the EMS server.
EMS_Reconnect AttemptCount	The number of reconnect attempts to be made if a connect fails. By default, this number is set to 10.
EMS_Reconnect AttemptDelay Milliseconds	The delay for the reconnect attempts. By default, this is set to 1000 milliseconds.
EMS_Reconnect AttemptTimeout Milliseconds	The timeout for the reconnect attempts. By default, this is set to 1000 milliseconds.
FileAppender	The path to the folder where the log file for the keep alive service is stored.

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

Note: If you change the config file, you must restart the service for any changes to take effect.

▶ To Start 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 creates a log of its activity. This log is located as exemplified below:

C:\Program Files\TIBCO\Spotfire Web Player\5.5\Logfiles\Spotfire.Dxp.Web.KeepAlive.log

5 The Scheduled Updates are now active.

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

6.7.1.4 Use TIBCO EMS for Event Driven Updates

The following code example demonstrates implementing a message publisher for event driven updates of a Spotfire Web Player analysis.

This example uses the TIBCO EMS C# client library.

```
TopicConnectionFactory factory =
new TopicConnectionFactory(emsServerUrl);
TopicConnection connection =
factory.CreateTopicConnection(emsUserName, emsPassword);
TopicSession session =
connection.CreateTopicSession(false, Session.AUTO_ACKNOWLEDGE);
Topic topic = session.CreateTopic(topicName);
// Same topic name as configured in web.config
TopicPublisher publisher =
session.CreatePublisher(topic);
MapMessage message =
session.CreateMapMessage();
message.SetString("Path", "/path/to/analysis");
message.SetString("ClientUpdate", "automatic");
publisher.Publish(message);
```

The following MapMessage objects are used to send sets of name-value pairs that define the update.

Key	Description
path	Used to enable EMS MapMessages. The library path to the analysis to update. This is a required value with a type of “string”. **Note**: This entry must match the settings you configured in the web.config file for the webplayer service.

clientupdate	Used to enable EMS MapMessages. Use the value “automatic” to update all running web browser clients. Use the value “manual” to have normal update where each client should update manually, as in Spotfire 2.2. If the “manual” or “automatic” client update behavior is supplied and is valid, this value is used for the update. If the value is not supplied or if it is invalid, the scheduled behaviour defined for the supplied analysis is used. Otherwise the server uses the “manual” update behavior. This is an optional value with a type of “string”. **Note**: This entry must match the settings you configured in the web.config file for the webplayer service.
KeepAliveMinutes	Used to enable EMS MapMessages. The number of minutes that the web player server should keep an inactive analysis (that is, an analysis not used by any user) before it is recycled. This applies only if no schedule is defined for the analysis. Invalid values, values below “0”, and values above “1440” result in the use of the default value configured in Web.config. The original default value is “10”. This is an optional value with a type of “int”. **Note**: This entry must match the settings you configured in the web.config file for the Web Player service.

6.7.1.5 Web Service Updater Schema

You can use a web service to trigger an update. The web service in the Spotfire Web Player is at the URL [*Web Player Server URL*]/*UpdateService.asmx*. To retrieve the WSDL definition of the web service use /*UpdateService.asmx?wsdl*.

The two requirements to trigger an update are:

- The web service must be enabled in *Web.config*.
- The user calling the web service must have Administrator privileges or the *TIBCO Spotfire Web Player\External updates of analysis in TIBCO Spotfire Web Player* license enabled.

Note: The web service is never enabled when running anonymous sites.

Note: Additional client coding is required to use Forms Authentication.

Web Service Updater Schema

```
<s:schema elementFormDefault="qualified" targetNamespace="http://
schemas.spotfire.tibco.com/webplayer/2009/05/">
  <s:element name="UpdateAnalysis">
    <s:complexType>
      <s:sequence>
        <s:element minOccurs="0" maxOccurs="1" name="path" type="s:string" />
        <s:element minOccurs="0" maxOccurs="1" name="clientUpdate" type="s:string" />
        <s:element minOccurs="1" maxOccurs="1" name="keepAliveMinutes" nillable="true"
type="s:int" />
      </s:sequence>
    </s:complexType>
  </s:element>
  <s:element name="UpdateAnalysisResponse">
    <s:complexType />
  </s:element>
</s:schema>
```

6.7.2 Upgrading an Existing Schedule

The recommended way to keep the scheduled updates for Spotfire Web Player 5.5 is to keep them in the library. This is done 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.

To Upgrade an Existing Schedule:

1. Before uninstalling the old version, make a backup of the old **ScheduledUpdates.xml**, located in the **Spotfire Web Player\5.0.1\webroot\app_data** folder.

2. Copy the **ScheduledUpdates.xml** file to the installation media folder and replace the existing, empty file.

3. Install Spotfire Web Player 5.5.

4. The first time the Web Player site starts it will read the installed schedule file, in **Spotfire Web Player\5.5\webroot\app_data** folder, 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** folder 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.

6.8 Resource Monitoring to Improve Performance

Resource monitoring is a way to ensure good performance to the users of the 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 web player, while temporarily denying users the ability to open analyses when the server is under heavy load.

To enable resource monitoring, you must change the *enabled* attribute to **true** in the **Web.config** 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.

In the **webroot** folder of the installation you will find the **Web.config** file. Open this file in an XML editor or text editor of your choice (it is recommended that you use an XML editor, since some text editors can corrupt the Web.config file. An XML editor will also give a clearer view of the XML code).

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 Web Player server will deny additional users attempting to open an analysis. It is specified as “available megabytes of free RAM left for the 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 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 done for this parameter. **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.

Save the **Web.config** file when you are done configuring it, and the resource monitoring changes will take effect.

Logging

To help you determine the threshold values, you can enable the Web Player log to state the actual performance values that the settings are compared against. This is done by adding the SiteResourceMonitor section below to the **log4net.config** file. It is located in the **webroot\App_data** folder of the installation.

```
<logger name="Spotfire.Dxp.Web.SiteResourceMonitor">
```

```
    <level value="DEBUG" />
  </logger>
```

The 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.

Customizing 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 if you like.

Create a file called ServerUnavailable.htm, and place it in the App_Data folder:

webroot\App_Data\ServerUnavailable.htm

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

6.9 Encrypting 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\5.5\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 machineKey of the 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.

6.10 Configuring the Web Player Using FIPS

If you want to run the web player server on a computer that has FIPS, Federal Information Processing Standard, enabled, an addition must be made to the **Web.config** file.

▸ To Configure Web.config for Use With FIPS:

1 Open the **Web.config** file in an XML editor or text editor of your choice (it is recommended that you use an XML editor, since some text editors can corrupt the Web.config file. An XML editor will also give a clearer view of the XML code). It is located in the **webroot** folder of the installation.

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.

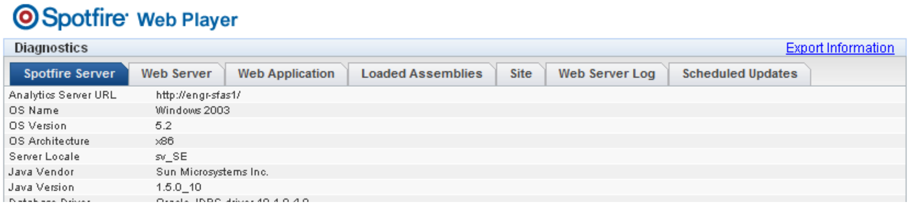
6.11 Diagnostics

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:



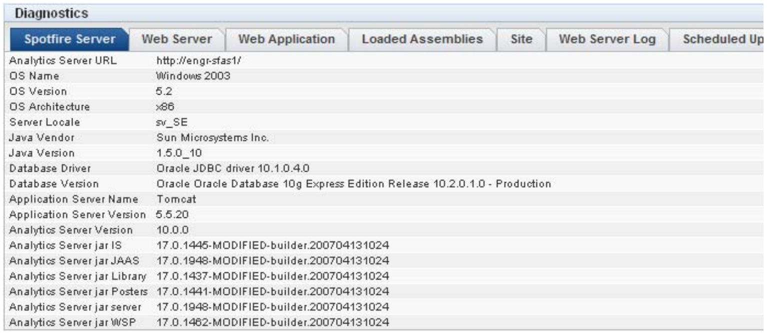
Analytics Server URL	http://engr-sfas1/
OS Name	Windows 2003
OS Version	5.2
OS Architecture	x86
Server Locale	sv_SE
Java Vendor	Sun Microsystems Inc.
Java Version	1.5.0_10
Database Driver	Oracle JDBC driver 10.1.0.4.0

- 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

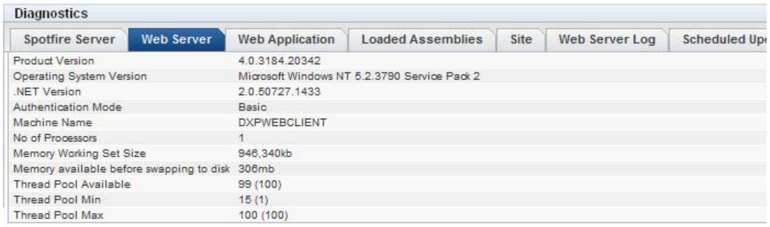
This tab displays information about the Spotfire Server.



Analytics Server URL	http://engr-sfas1/
OS Name	Windows 2003
OS Version	5.2
OS Architecture	x86
Server Locale	sv_SE
Java Vendor	Sun Microsystems Inc.
Java Version	1.5.0_10
Database Driver	Oracle JDBC driver 10.1.0.4.0
Database Version	Oracle Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production
Application Server Name	Tomcat
Application Server Version	5.5.20
Analytics Server Version	10.0.0
Analytics Server jar IS	17.0.1445-MODIFIED-builder.200704131024
Analytics Server jar JAAS	17.0.1948-MODIFIED-builder.200704131024
Analytics Server jar Library	17.0.1437-MODIFIED-builder.200704131024
Analytics Server jar Posters	17.0.1441-MODIFIED-builder.200704131024
Analytics Server jar server	17.0.1948-MODIFIED-builder.200704131024
Analytics Server jar WSP	17.0.1462-MODIFIED-builder.200704131024

6.11.2 Web Server

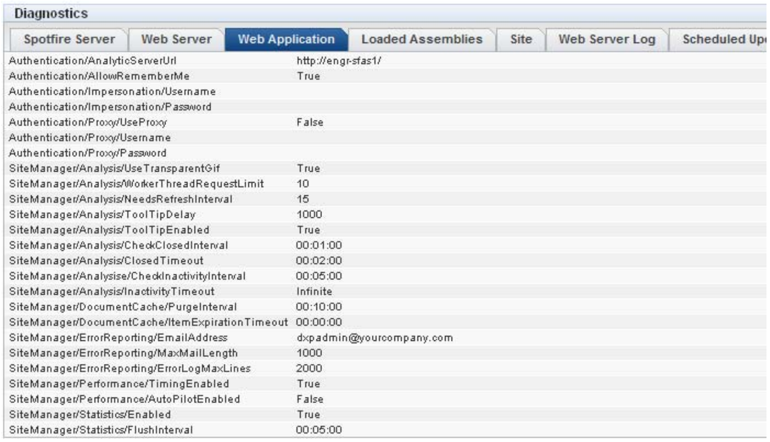
This tab displays information about the web server environment.



Product Version	4.0.3184.20342
Operating System Version	Microsoft Windows NT 5.2.3790 Service Pack 2
.NET Version	2.0.50727.1433
Authentication Mode	Basic
Machine Name	DXPWEBCLIENT
No of Processors	1
Memory Working Set Size	946,340kb
Memory available before swapping to disk	306mb
Thread Pool Available	99 (100)
Thread Pool Min	15 (1)
Thread Pool Max	100 (100)

6.11.3 Web Application

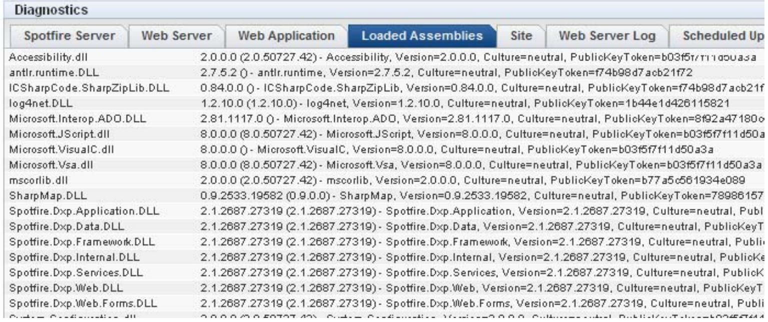
This tab displays information about the Spotfire Web Player web application.



Authentication/AnalyticServerUrl	http://engr-sfas1/
Authentication/AllowRememberMe	True
Authentication/Impersonation/Username	
Authentication/Impersonation/Password	
Authentication/Proxy/UseProxy	False
Authentication/Proxy/Username	
Authentication/Proxy/Password	
SiteManager/Analysis/UseTransparentGif	True
SiteManager/Analysis/WorkerThreadRequestLimit	10
SiteManager/Analysis/NeedsRefreshInterval	15
SiteManager/Analysis/ToolTipDelay	1000
SiteManager/Analysis/ToolTipEnabled	True
SiteManager/Analysis/CheckClosedInterval	00:01:00
SiteManager/Analysis/ClosedTimeout	00:02:00
SiteManager/Analysise/CheckInactivityInterval	00:05:00
SiteManager/Analysis/InactivityTimeout	Infinite
SiteManager/DocumentCache/PurgeInterval	00:10:00
SiteManager/DocumentCache/ItemExpirationTimeout	00:00:00
SiteManager/ErrorReporting/EmailAddress	dxpadmin@yourcompany.com
SiteManager/ErrorReporting/MaxMailLength	1000
SiteManager/ErrorReporting/ErrorLogMaxLines	2000
SiteManager/Performance/TimingEnabled	True
SiteManager/Performance/AutoPilotEnabled	False
SiteManager/Statistics/Enabled	True
SiteManager/Statistics/FlushInterval	00:05:00

6.11.4 Loaded Assemblies

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

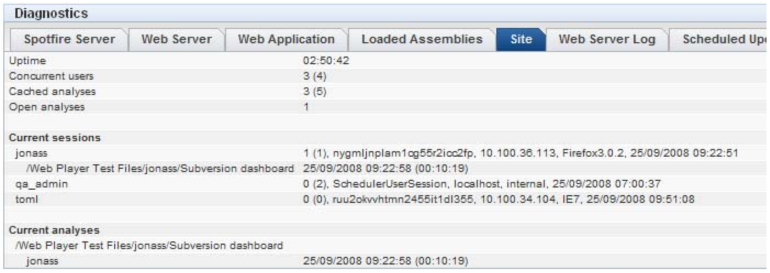


Accessibility.dll	2.0.0.0 (2.0.50727.42) - Accessibility, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a
antlr.runtime.DLL	2.7.5.2 () - antlr.runtime, Version=2.7.5.2, Culture=neutral, PublicKeyToken=f74b98d7acb21f72
ICSharpCode.SharpZipLib.DLL	0.84.0.0 () - ICSharpCode.SharpZipLib, Version=0.84.0.0, Culture=neutral, PublicKeyToken=f74b98d7acb21f
log4net.DLL	1.2.10.0 (1.2.10.0) - log4net, Version=1.2.10.0, Culture=neutral, PublicKeyToken=1b44e1d426115821
Microsoft.Interop.ADO.DLL	2.81.1117.0 () - Microsoft.Interop.ADO, Version=2.81.1117.0, Culture=neutral, PublicKeyToken=8f92a47180c
Microsoft.JScript.dll	8.0.0.0 (8.0.50727.42) - Microsoft.JScript, Version=8.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a
Microsoft.VisualC.dll	8.0.0.0 () - Microsoft.VisualC, Version=8.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a
Microsoft.Vsa.dll	8.0.0.0 (8.0.50727.42) - Microsoft.Vsa, Version=8.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a
mscorlib.dll	2.0.0.0 (2.0.50727.42) - mscorlib, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089
SharpMap.DLL	0.9.2533.19582 (0.9.0.0) - SharpMap, Version=0.9.2533.19582, Culture=neutral, PublicKeyToken=78986157
Spotfire.Dxp.Application.DLL	2.1.2687.27319 (2.1.2687.27319) - Spotfire.Dxp.Application, Version=2.1.2687.27319, Culture=neutral, Publ
Spotfire.Dxp.Data.DLL	2.1.2687.27319 (2.1.2687.27319) - Spotfire.Dxp.Data, Version=2.1.2687.27319, Culture=neutral, PublicKeyT
Spotfire.Dxp.Framework.DLL	2.1.2687.27319 (2.1.2687.27319) - Spotfire.Dxp.Framework, Version=2.1.2687.27319, Culture=neutral, Publi
Spotfire.Dxp.Internal.DLL	2.1.2687.27319 (2.1.2687.27319) - Spotfire.Dxp.Internal, Version=2.1.2687.27319, Culture=neutral, PublicKe
Spotfire.Dxp.Services.DLL	2.1.2687.27319 (2.1.2687.27319) - Spotfire.Dxp.Services, Version=2.1.2687.27319, Culture=neutral, PublicK
Spotfire.Dxp.Web.DLL	2.1.2687.27319 (2.1.2687.27319) - Spotfire.Dxp.Web, Version=2.1.2687.27319, Culture=neutral, PublicKeyT
Spotfire.Dxp.Web.Forms.DLL	2.1.2687.27319 (2.1.2687.27319) - Spotfire.Dxp.Web.Forms, Version=2.1.2687.27319, Culture=neutral, Publi
System.Configuration.dll	2.0.0.0 (2.0.50727.42) - System.Configuration, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11

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.

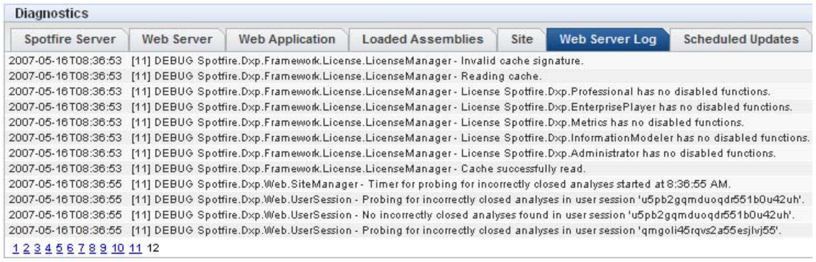
The Site tab also shows a list of currently active sessions, a list of which analyses are currently open, and which users are connected.



Uptime	02:50:42
Concurrent users	3 (4)
Cached analyses	3 (5)
Open analyses	1
Current sessions	
jonass	1 (1), nygmljnplam1og55r2icc2fp, 10.100.36.113, Firefox3.0.2, 25/09/2008 09:22:51
/Web Player Test Files/jonass/Subversion dashboard	25/09/2008 09:22:58 (00:10:19)
qa_admin	0 (2), SchedulerUserSession, localhost, internal, 25/09/2008 07:00:37
toml	0 (0), ruu2okvvhtmn2455it1dl355, 10.100.34.104, IE7, 25/09/2008 09:51:08
Current analyses	
/Web Player Test Files/jonass/Subversion dashboard	
jonass	25/09/2008 09:22:58 (00:10:19)

6.11.6 Web Server Log

This tab displays the log for the web application.



```
2007-05-16T08:36:53  [11] DEBUG Spotfire.Dxp.Framework.License.LicenseManager - Invalid cache signature.
2007-05-16T08:36:53  [11] DEBUG Spotfire.Dxp.Framework.License.LicenseManager - Reading cache.
2007-05-16T08:36:53  [11] DEBUG Spotfire.Dxp.Framework.License.LicenseManager - License Spotfire.Dxp.Professional has no disabled functions.
2007-05-16T08:36:53  [11] DEBUG Spotfire.Dxp.Framework.License.LicenseManager - License Spotfire.Dxp.EnterprisePlayer has no disabled functions.
2007-05-16T08:36:53  [11] DEBUG Spotfire.Dxp.Framework.License.LicenseManager - License Spotfire.Dxp.Metrics has no disabled functions.
2007-05-16T08:36:53  [11] DEBUG Spotfire.Dxp.Framework.License.LicenseManager - License Spotfire.Dxp.InformationModeler has no disabled functions.
2007-05-16T08:36:53  [11] DEBUG Spotfire.Dxp.Framework.License.LicenseManager - License Spotfire.Dxp.Administrator has no disabled functions.
2007-05-16T08:36:53  [11] DEBUG Spotfire.Dxp.Framework.License.LicenseManager - Cache successfully read.
2007-05-16T08:36:55  [11] DEBUG Spotfire.Dxp.Web.SiteManager - Timer for probing for incorrectly closed analyses started at 8:36:55 AM.
2007-05-16T08:36:55  [11] DEBUG Spotfire.Dxp.Web.UserSession - Probing for incorrectly closed analyses in user session 'u5pb2gqmduoqdr551b0u42uh'.
2007-05-16T08:36:55  [11] DEBUG Spotfire.Dxp.Web.UserSession - No incorrectly closed analyses found in user session 'u5pb2gqmduoqdr551b0u42uh'.
2007-05-16T08:36:55  [11] DEBUG Spotfire.Dxp.Web.UserSession - Probing for incorrectly closed analyses in user session 'qmgoli45rqvs2a55esjlvj55'.
```

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** folder 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.

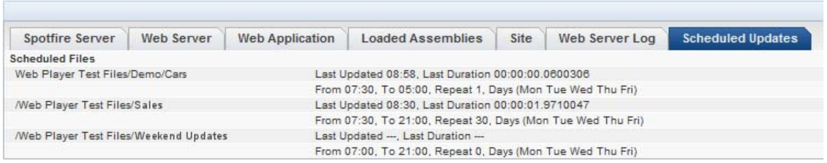
Note: Be careful of selecting DEBUG since this will log large amounts of events and quickly create huge log files. This level is only to be used when actively trying to find the source of a problem.

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.



Scheduled Files

Web Player Test Files/Demo/Cars	Last Updated 08:58, Last Duration 00:00:00.0600306
	From 07:30, To 05:00, Repeat 1, Days (Mon Tue Wed Thu Fri)
/Web Player Test Files/Sales	Last Updated 08:30, Last Duration 00:00:01.9710047
	From 07:30, To 21:00, Repeat 30, Days (Mon Tue Wed Thu Fri)
/Web Player Test Files/Weekend Updates	Last Updated ---, Last Duration ---
	From 07:00, To 21:00, Repeat 0, Days (Mon Tue Wed Thu Fri)

6.12 Logging and Monitoring

To keep track of the resource usage for the Spotfire Web Player server, it is possible to enable logging and monitoring of the server.

This is done by adding and enabling performance counters in the **Web.config** file and by adding the settings for the wanted log files in the **log4net.config** file, located in the **webroot\App_data** folder of the installation.

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

- **AuditLog.txt**: At INFO level, login/logout is logged.
  At DEBUG level, opening/closing analyses, active tabs in analyses and library browsing is also logged.
- **MonitoringEventsLog.txt**: At INFO level, Web Player Server starting/shutting down is logged.
  At DEBUG level, sessions created/removed, analyses opened/closed and cached analyses added/removed is 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.

Note: It is also possible to 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 set up the collection of user and session statistics, and performance counters in the Web.config file.

```
<spotfire.dxp.web>
  ...
  <performance>
    ...
    <performanceCounterLogging
      enabled="false"
      logInterval="120"
      debugLogInterval="15"
      counters="
        TIBCO Spotfire Webplayer;# cached documents;,
        TIBCO Spotfire Webplayer;# open documents;,
        TIBCO Spotfire Threading;thread pool queue age in milliseconds;,
        Process;Private bytes;w3wp,
        Processor;% Processor Time;_Total"
      debugCounters="
        TIBCO Spotfire Webplayer;# concurrent users;,
        TIBCO Spotfire Webplayer;# accumulated cached documents;,
        TIBCO Spotfire Webplayer;# accumulated open documents;,
        TIBCO Spotfire Webplayer;# analyses under scheduled updates control;,
        TIBCO Spotfire Webplayer;Web Player Uptime Seconds;,
        TIBCO Spotfire Webplayer;Web Player MB Working Set Size;,
        TIBCO Spotfire Webplayer;Web Player MB Available Before Swapping To Disk;,
        .NET CLR LocksAndThreads;;w3wp,
        .NET CLR Memory;;w3wp,
        ASP.NET;Application Restarts;,
        ASP.NET;Request Execution Time;,
        ASP.NET;Requests Current;,
        ASP.NET;Requests Queued;,
        Memory;Available Bytes;,
        Network Interface;Bytes Total/sec;,
        PhysicalDisk;Avg. Disk Queue Length;_Total,
       PhysicalDisk;% Disk Time;_Total,
        PhysicalDisk;Current Disk Queue Length;_Total,
        PhysicalDisk;% Disk Read Time;_Total,
        PhysicalDisk;% Disk Write Time;_Total,
        Process;Handle Count;w3wp,
        Processor;% Processor Time;,
        Processor;% Privileged Time;_Total,
        System;;,
        Web Service;Current Connections;_Total,
        Web Service;ISAPI Extension Requests/sec;_Total"
    />
  ...
<statistics enabled="false" flushInterval="60"/>
```

Key	Description
performanceCounter Logging	
enabled	Set this to true 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.
debugLogInterval	Specify the number of seconds between each performance counter logging at DEBUG level.
counters	Add performance counters you wish to log, at both INFO and DEBUG level, separated by “,”. Each counter consists of three parts: category, counter, and instance, separated by “;”. Both standard Windows performance counters, as well as a set of internal TIBCO counters, may be included.
debugCounters	Add additional performance counters you wish to log at DEBUG level, separated by “,”.
statistics	
enabled	Set this to true to enable logging of all the other statistics for the Web Player server. The result of this logging can be found in the other log files specified in the log4net.config file.
flushInterval	Specify the number of seconds between each logging.

6.12.2 Enable logging in log4net.config

The following is an example of how the log4net.config file can be set up to create the log files mentioned earlier. Each section in the config 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 folder 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.

It is also possible to 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 server computer name.
timeStamp	The event timestamp.
eventType	The type of event.
information	Information 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	User name of the logged on client.

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.

6.12.2.2 log4net.config Examples

Logging to Log Files Example

This example shows how to set up all the log files. The logs that support separate properties have been set up that way, the ones that does not have been set up using the “%message” format.

```
<!-- WebLogger logging level (DEBUG, INFO or OFF) -->
    <logger name="WebLogger">
      <level value="DEBUG" />
    </logger>

    <!-- Audit log for successful and failed authentications -->
    <appender name="AuditLog" type="log4net.Appender.RollingFileAppender">
      <file value="Logs\AuditLog.txt"/>
      <appendToFile value="true"/>
      <rollingStyle value="Size" />
      <maxSizeRollBackups value="10" />
      <maximumFileSize value="100MB" />
      <staticLogFileName value="false" />
      <layout type="log4net.Layout.PatternLayout">
        <conversionPattern value="%-
5level;%property{hostName};%property{timeStamp};%property{sessionId};%property{ipAddres
s};%property{userName};%property{operation};%property{analysisId};%property{argument};%
property{status}%newline"/>
      </layout>
    </appender>
    <logger name="WebLogger.WebAuditLog" additivity="false">
      <appender-ref ref="AuditLog"/>
      <appender-ref ref="AuditLogAdoNetAppender"/>
    </logger>

<!-- Event log to be used for monitoring -->
    <appender name="MonitoringEventsLog" type="log4net.Appender.RollingFileAppender">
      <file value="Logs\MonitoringEventsLog.txt"/>
      <appendToFile value="true"/>
      <rollingStyle value="Size" />
      <maxSizeRollBackups value="10" />
      <maximumFileSize value="100MB" />
      <staticLogFileName value="false" />
      <layout type="log4net.Layout.PatternLayout">
        <conversionPattern value="%-
5level;%property{hostName};%property{timeStamp};%property{eventType};%property{informat
ion}%newline"/>
```

```
      </layout>
    </appender>
    <logger name="WebLogger.MonitoringEventsLog" additivity="false">
      <appender-ref ref="MonitoringEventsLog"/>
    </logger>

    <!-- Statistics log for document cache information -->
    <appender name="DocumentCacheStatisticsLog"
type="log4net.Appender.RollingFileAppender">
      <file value="Logs\DocumentCacheStatisticsLog.txt"/>
      <appendToFile value="true"/>
      <rollingStyle value="Size" />
      <maxSizeRollBackups value="10" />
      <maximumFileSize value="100MB" />
      <staticLogFileName value="false" />
      <layout type="log4net.Layout.PatternLayout">
        <conversionPattern value="%-
5level;%property{hostName};%property{timeStamp};%property{path};%property{modifiedOn};%
property{referenceCount}%newline"/>
      </layout>
    </appender>
    <logger name="WebLogger.DocumentCacheStatisticsLog" additivity="false">
      <appender-ref ref="DocumentCacheStatisticsLog"/>
    </logger>

    <!-- Statistics log for open files information -->
    <appender name="OpenFilesStatisticsLog"
type="log4net.Appender.RollingFileAppender">
      <file value="Logs\OpenFilesStatisticsLog.txt"/>
      <appendToFile value="true"/>
      <rollingStyle value="Size" />
      <maxSizeRollBackups value="10" />
      <maximumFileSize value="100MB" />
      <staticLogFileName value="false" />
      <layout type="log4net.Layout.PatternLayout">
        <conversionPattern value="%-
5level;%property{hostName};%property{timeStamp};%property{sessionId};%property{filePath
};%property{modifiedOn};%property{fileId};%property{elapsedTime};%property{inactiveTime
}%newline"/>
      </layout>
    </appender>
    <logger name="WebLogger.OpenFilesStatisticsLog" additivity="false">
      <appender-ref ref="OpenFilesStatisticsLog"/>
    </logger>

    <!-- Performance counter values -->
    <appender name="PerformanceCounterLog" type="log4net.Appender.RollingFileAppender">
      <file value="Logs\PerformanceCounterLog.txt" />
      <appendToFile value="true" />
      <rollingStyle value="Size" />
      <maxSizeRollBackups value="10" />
      <maximumFileSize value="100MB" />
      <staticLogFileName value="false" />
      <layout type="log4net.Layout.PatternLayout">
        <conversionPattern value="%message%newline" />
      </layout>
    </appender>
    <logger name="WebLogger.PerformanceCounterLog" additivity="false">
      <appender-ref ref="PerformanceCounterLog"/>
    </logger>
    <!-- Statistics log for user session information -->
    <appender name="UserSessionStatisticsLog"
type="log4net.Appender.RollingFileAppender">
      <file value="Logs\UserSessionStatisticsLog.txt"/>
      <appendToFile value="true"/>
      <rollingStyle value="Size" />
      <maxSizeRollBackups value="10" />
      <maximumFileSize value="100MB" />
      <staticLogFileName value="false" />
      <layout type="log4net.Layout.PatternLayout">
        <conversionPattern value="%-
5level;%property{hostName};%property{timeStamp};%property{sessionId};%property{ipAddres
s};%property{userName};%property{browserType};%property{cookies};%property{loggedInDura
tion};%property{maxOpenFilesCount};%property{openFilesCount}%newline"/>
      </layout>
    </appender>
    <logger name="WebLogger.UserSessionStatisticsLog" additivity="false">
      <appender-ref ref="UserSessionStatisticsLog"/>
    </logger>

    <!-- A file that contains all DateTimes from the other WebLogger log files.
         Use this file to join the other log files.  -->
    <appender name="DateTimesLog" type="log4net.Appender.RollingFileAppender">
      <file value="Logs\DateTimesLog.txt"/>
      <appendToFile value="true"/>
      <rollingStyle value="Size" />
      <maxSizeRollBackups value="10" />
      <maximumFileSize value="100MB" />
      <staticLogFileName value="false" />
      <layout type="log4net.Layout.PatternLayout">
        <conversionPattern value="%message%newline"/>
      </layout>
    </appender>
    <logger name="WebLogger.DateTimesLog" additivity="false">
      <appender-ref ref="DateTimesLog"/>
    </logger>
```

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

Logging to Database Example

This example shows how to log the AuditLog to a database. The connectionString should point out a database that contains a table with columns matching 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 myAuditLog
([hostName],[level],[sessionId],[ipAddress],[userName],[operation],[analysisId],[status
],[timeStamp]) VALUES
```

```
(@hostName,@level,@sessionId,@ipAddress,@userName,@operation,@analysisId,@status,@timeS
tamp)" />
      <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="@analysisPath" />
        <dbType value="String" />
        <size value="50" />
        <layout type="log4net.Layout.PatternLayout">
          <conversionPattern value="%property{analysisPath}" />
        </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 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 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

▶ To Enable 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 Setting up a Server Cluster

Running Spotfire Web Player in a Server Cluster

To obtain better scalability, it is possible to set up 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 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 one high performing one.
- 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 set up a server cluster making use of Microsoft’s Network Load Balancing (NLB) Cluster solution. Setting this up is pretty straight forward and Microsoft’s NLB solution is included in Windows Server 2008.

More information on Microsoft’s Network Load Balancing solution can be found on Microsoft TechNet.

For Windows Server 2008, see:
http://technet.microsoft.com/en-us/library/cc725691(WS.10).aspx

For Windows Server 2008 R2, see:
http://technet.microsoft.com/en-us/library/cc725691.aspx

For Windows Server 2012, see:
http://technet.microsoft.com/en-us/library/hh831698.aspx

▸ To Set 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.
For Windows Server 2008, see:
http://technet.microsoft.com/en-us/library/cc731695(WS.10).aspx
For Windows Server 2008 R2 and Windows Server 2012, see:
http://technet.microsoft.com/en-us/library/cc731695.aspx
Note: Some task details are changed from 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:

a. Make sure that the local web server is running.

b. Verify that it is possible to open a Spotfire analysis in the Web Player.

4 Create and configure the cluster, add hosts and configure them using the Network Load Balancing Manager.
For Windows Server 2008, see:
http://technet.microsoft.com/en-us/library/cc731499(WS.10).aspx
For Windows Server 2008 R2 and Windows Server 2012, see:
http://technet.microsoft.com/en-us/library/cc731499.aspx
Note: Some task details are changed from Windows Server 2008 R2 and Windows Server 2012. For more information, see http://technet.microsoft.com.

A cluster of Web Player Servers has now been set up.

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 Web Player against one of the server nodes.

6.15 Backup and Restore

If Spotfire Web Player needs to be restored, this is done by completing a new installation of the web player. However, since the web player does not store any state itself, you need to make a backup of important files after configuring the 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 done to the location

C:\Program Files\TIBCO\Spotfire Web Player\5.5\webroot

Back up the following files (paths are relative to the webroot directory):

- **Web.config**
- **app_data\Header.htm**
  If the header has been customized.
  Note: This is also applicable for any other files related to the customized header, for example images.
- **bin\Tools\Spotfire.Dxp.Web.KeepAlive.exe.config**
  If scheduled updates and the keep alive service are used.
- **app_data\ScheduledUpdates.xml**
  If the scheduled updates are not stored in the library.
- **app_data\ServerUnavailable.htm**
  If there is a custom page.
- **Certificate files**
  If you use SSL (https).
- **Mashups**
  If you have any mashup applications these need to be backed up.

To Recover the 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 folder 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 web player with extensions or upgrades, you need to upgrade the web player again.

5 Verify that the new installation works as intended by following the instructions in the chapter “Testing the Installation” on page 62.

7 Uninstall

7.1 Stopping the Application Pool

Before uninstalling TIBCO Spotfire Web Player, it is important to stop the application pool for the web player in the IIS. This is done to make sure that no instances of the 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 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\5.5. Simply delete them after uninstalling the web player.