

TIBCO® Spotfire® Analytics Server 10.1.2

Installation and Configuration Manual

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_TIBCOSPOTFIRESERVER.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 - 2012 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	Introduction	5
1.1	Overview of Server Functionality	5
1.2	Different Server Configurations	8
1.3	Selecting Login & User Directory	10
1.4	Single Sign-on	12
2	Installation	14
2.1	Bundled Oracle 10g XE	14
2.2	Existing Oracle Database	31
2.3	Existing Microsoft SQL Server Database	51
2.4	LDAP Installation	70
2.5	NTLM Installation	76
2.6	X.509 Certificate Installation	78
2.7	Microsoft Windows NT Domain Installation	83
2.8	Completing the Installation	86
2.9	Final Installation Procedures	88
3	Upgrading	91
3.1	Introduction	91
3.2	Stop and Disable the 10.0 Service	93
3.3	Select the Appropriate Installer	94
3.4	Run the Installer	94
3.5	Completing the Upgrade	102
4	Removal Procedures	108
5	Configuration Reference	110
5.1	Important Configuration Files	110
5.1.1	/WEB-INF/web.xml	110
5.1.2	/jdk/jre/lib/security/spotfire.login	114
5.1.3	/WEB-INF/data-sources.xml	118
5.1.4	/WEB-INF/userdirconfig.xml	124
5.1.5	/WEB-INF/im-service.xml	136
5.1.6	/WEB-INF/library-service.xml	142
5.1.7	/WEB-INF/settings.xml	146
5.1.8	/WEB-INF/manifest.xml	147
5.1.9	<server install dir>/server/conf/server.xml	148
5.2	Server Logging	150
6	Configuration Procedures	156
6.1	Changing Login System	156
6.1.1	Preparations	156
6.1.2	Changing to Database Table Login System	156
6.1.3	Changing to Microsoft Windows NT Domain Login System	159
6.1.4	Changing to LDAP Login System	161
6.1.5	Changing to Windows Integrated Authentication (NTLM)	163
6.1.6	Configuring SSL Support	167
6.1.7	HTTPS and Client Certificates with Basic Authentication Login	172
6.1.8	HTTPS and Client Certificates with Automatic Login	174
6.1.9	HTTPS in Visualization Services	175
6.2	Changing User Directory Back-end	179
6.2.1	Preparations	179
6.2.2	Changing to Database Table User Directory Back-end	179
6.2.3	Changing to Microsoft Windows NT Domain User Directory Back-end	180
6.2.4	Changing to LDAP User Directory Back-end	182

6.3	Setting Up Kerberos Authentication	186
6.4	Enabling Impersonation	198
6.5	Enabling External LDAP Group Synchronization	200
6.6	Changing Database Connection Settings	204
6.7	Configuring IS to Access a New Type of JDBC Data Source	207
6.8	Configuring Information Services for Heavy Load	225
6.9	Pivot Column Naming Schemes	226
6.10	Resizing Temporary Tablespace	228
6.11	Changing Administrator Email Address	228
6.12	Modifying the Virtual Memory	229
6.13	Configuring the Server for LDAPS	230
6.14	Resetting Passwords for the Database Table Login System	232
6.15	Enabling RSS Feed in the Login Dialog	232
6.16	Deploying and Configuring a Custom Credential Transform	234
6.17	Changing to a Different JDK	238
7	Appendix: License Information	241

1 Introduction

The TIBCO Spotfire Analytics Server provides basic infrastructure, which is used by the clients: TIBCO Spotfire and TIBCO Spotfire DecisionSite Client.

The Spotfire Analytics Server has functionality for identifying users and assigning privileges, serve as a central storage for program updates, be a central repository for analysis files, and to connect to different external datasources.

1.1 Overview of Server Functionality

1.1.1 Overview User Handling

The Spotfire Analytics Server is fundamentally a web server with additional, built in logic. Even if most users only see the user interface of TIBCO Spotfire DecisionSite Client or TIBCO Spotfire, there is also functionality in web pages and Web Services which can be requested. Some content is available for everyone to see, while some content is protected from unauthorized access. For example, the Spotfire Analytics Server “welcome page” is open for everyone, while the administration pages are available only to administrators. The protected pages require a user to log in.

To describe how the server verifies if a user is allowed to access certain information three distinct parts are of interest:

- the user directory back-end
- the login system
- the login method

The user directory back-end is a repository containing all users which are allowed to use the system. A user must be present in the user directory to log in. The login system checks if a user has entered the correct password. The login method describes how a user is prompted for login information. These three aspects are explained in more detail below.

1.1.2 User Directory Back-end

The User Directory Back-end contains the list of potential users, that is, if a user should be allowed to use the system or not. The user directory back-end can be either an external LDAP server or Windows NT Domain server, or the Spotfire Analytic Server’s internal database. In addition to LDAP, NT Domain and Database it is also possible to write custom code to connect to other systems.

Even if an external system such as LDAP is used, the users are still added to the Spotfire Analytics Server's database where they are assigned internal identifiers. This is necessary to be able to assign users to groups, check licenses and access rights to certain features or information. The Spotfire Analytics Server is eager when it comes to assigning users to the internal database tables, that is, whenever the Spotfire Analytics Server comes across an unknown user it is assigned an internal identifier and stored.

Note: A general recommendation is to avoid issuing requests that will list all users in an external system if only a handful of them are supposed to use the server, e.g. by entering '*' as search criteria in the administration interfaces.

If LDAP is selected, the Spotfire Analytics Server can be configured to use certain group information from the LDAP server. For example, if the Windows domain controller is set as the LDAP server then a mail distribution list can be used as a group by the Spotfire Analytics Server, so that whenever a user is added to the mail distribution list that user will also get appropriate privileges to the Spotfire Analytics Server.

1.1.3 Login System

If the user is prompted for user name and password, then this information is validated by the login system. The login system can be an LDAP server, Windows NT Domain Server, or the Spotfire Analytics Server's database.

The login system is written with a standard Java API called JAAS (Java Authentication and Authorization Service), which makes it possible to write specific functionality to perform custom made checks.

1.1.4 Login Method

There are three different login methods possible for the Spotfire Analytics Server. The most basic one is when the user is prompted for user name and password.

The second method uses Windows Integrated Authentication functionality (also known as NTLM) where the existing login to the domain controller is used as proof that the user is legitimate and the user's Windows login identity is used as user name. No login system is called upon since the Spotfire Analytics Server trusts the domain controller's decision to allow a user to log into the domain. The user will get a single sign-on experience, that is, the user will only log into Windows but will not be prompted to log in when starting his Spotfire client.

The server can be configured to provide HTTPS communication, i.e. an encrypted communication channel is established between the server and its clients to protect from eavesdropping. When the server is set to accept HTTPS it can, optionally, also be configured to only accept connection from a client which has a certificate issued by a certain certificate issuer. If a client does not have a proper certificate it will not be able to connect.

With this configuration one can, optionally, use the fact that a certain certificate is issued to a certain user, and use this certificate to login to the server. The user will get a single sign-on experience. In this case the server trusts that the certificate has been issued to a certain user, and uses the information about to whom the certificate was issued to as username. So just as with the case of Windows Integrated Authorization no use is made of the Login System.

1.1.5 Groups

The Spotfire Analytics Server database contains information about groups. A user can belong to many groups, and groups can in turn belong to other groups. Circular group memberships are not allowed.

To include a group as a member of another group can only be done using the Administration Manager interface in TIBCO Spotfire.

If LDAP is used as a user directory back-end, you can set up the Spotfire Analytics Server to populate certain groups with members of corresponding groups on the LDAP server.

In certain cases when a user is member of many groups or a complex group hierarchy, there are rules that decide how the different memberships should be rated. This can be important when determining preferences for instance. In general, a user is more related to its parent than to its grandparent. When choosing priority between many parents, there is a concept of primary group which is a user's prime membership. This means that if a user is a member of both the groups "Sales Europe" and "Sales Global" you can specify that "Sales Europe" is more important, and the preferences, etc., should be determined by looking at that group first.

1.1.6 TIBCO Spotfire Preferences

The server stores preferences for users of TIBCO Spotfire. If a user does not have a specific preference assigned then the server looks at the groups to whom the users belongs, until a preference is found. The basic rule is that the closest group is the one used for preferences; see "Groups" on page 7.

1.1.7 Licenses

The Spotfire Analytics Server also handles licenses for users of TIBCO Spotfire and TIBCO Spotfire DecisionSite. Licenses determine what features and functionality should be available to each user. TIBCO Spotfire and TIBCO Spotfire DecisionSite use different mechanisms for licenses and each has its own administration tool to handle this.

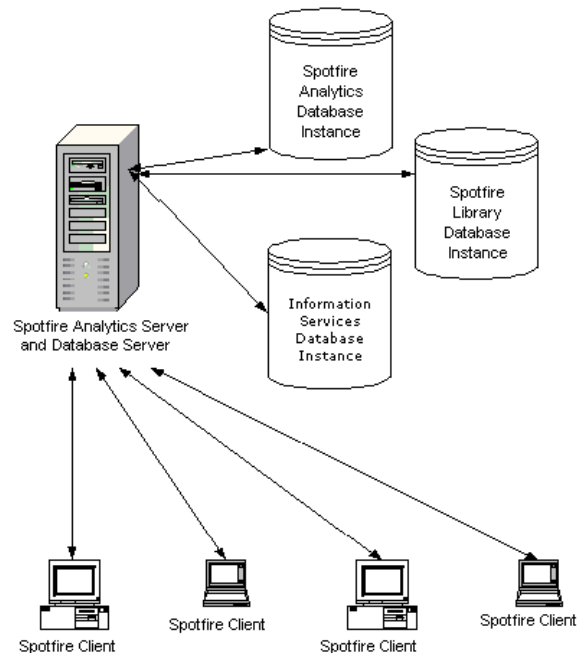
1.2 Different Server Configurations

The Spotfire Analytics Server needs three main components to run: the **Spotfire Analytics Server** itself, which runs on an **Application Server**, and uses a **Database** to store information.

There are two ways you can set up a system to run the Spotfire Analytics Server, the application server and databases needed. The following Installation chapter in this manual is separated into these two configurations.

The bundled database configuration

The Spotfire Analytics Server installer bundles a Tomcat application server and an Oracle XE database. These can be installed on a single machine as seen below.



The downside of this solution is that it is more performance demanding, since both the application server and the database are located on the same machine.

The bundled database has some built in limitations making it unsuitable for heavy usage. Some of these are listed below:

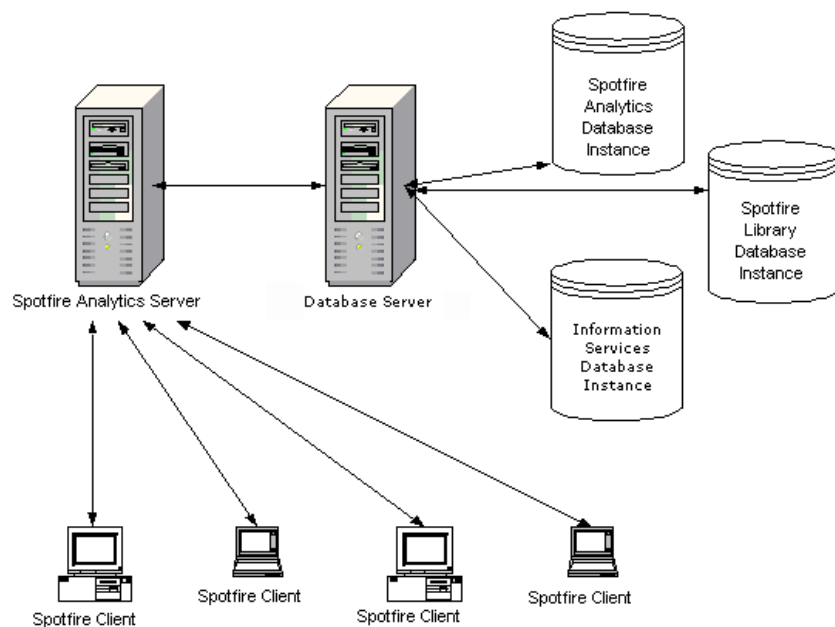
- Will only store max 4GB of user data.
- Will only utilize 1GB of memory.
- Will only utilize 1 CPU regardless of how many is available on the machine.

If your users intend to store many analyses files and data in the Spotfire Library, be aware of the 4GB limitation.

Also, if your users will use Information Services joins between large data sets, the temporary tables caused by this operation will grow large and might also be affected by the 4GB limitation.

The external database configuration

This configuration uses one machine for the Tomcat application server that runs the Spotfire Analytics Server, and another machine for the databases. This configuration is intended for companies that have an existing Oracle or Microsoft SQL Server 2005 database in place, and want to use that for the Spotfire Analytics Server databases too.



This configuration will generally provide better performance, since the work load is distributed over several machines.

1.3 Selecting Login & User Directory

When you install the Spotfire Analytics Server you will need to specify how users will be authenticated when they log in, and which type of user directory will hold the list of all your users.

It is a good idea to determine which type of login and user directory back-end you wish to use before starting the installation.

Login

DecisionSite Client and TIBCO Spotfire users who log into the Spotfire Analytics Server must be authenticated in order to be allowed access to the server.

When installing the Spotfire Analytics Server you can configure it to use one of the five combinations of Login System and Login method described below.

User Directory Back-end

A bit simplified, you could say that the user directory is where the list of all your users is kept. For example, some companies have thousands of users already listed in a Microsoft Active Directory which they want to use, whereas some companies might decide it is sufficient to use the Spotfire Analytics Server database and add their users to that.

What is the Difference?

For a large company the user directory often contains thousands of users. You might not want all of these to have access to the Spotfire Analytics Server. Therefore, you can set up a different login system that only allows a certain number of these to log in.

The possible combinations available from the installer are indicated in the chart below.

Login	User Directory Back-end		
	Database Table	LDAP (For example, Microsoft Active Directory)	Windows NT Domain
Database Table	X		
LDAP (For example, Microsoft Active Directory)	X	X	
NTLM	X	X	X
X.509 Certificates	X	X	X
MS Windows NT Domain	X		X

1. Database Table

When using this login system, usernames and passwords provided by the end users logging in are compared with credentials stored in the Spotfire Analytics Server's database. For security reasons, the passwords are never stored in cleartext. Instead, the Spotfire Analytics Server computes encrypted one-way hashes of the passwords.

Database Table authentication is ideal for small groups of users, but the administration of larger groups can be cumbersome because each user has to be manually added to the Database Table directory using the DecisionSite Administrator tool or the TIBCO Spotfire Administration Manager tool.

2. LDAP (for example, Microsoft Active Directory)

When using this login system, usernames and passwords provided by the end users logging in are validated by an LDAP server. The Spotfire Analytics Server stores a list of usernames in its database, but no passwords.

The Spotfire Analytics Server directly supports Microsoft Active Directory and Sun Java System Directory Server and should work with most other servers as well, though this might require some manual configuration.

3. NTLM (Windows Integrated Authentication)

When the Spotfire Analytics Server is configured for Windows Integrated Authentication (NTLM), DecisionSite Client or TIBCO Spotfire will be logged in automatically if the user has logged in using his or her Windows domain account. Spotfire Analytics Server delegates the authentication itself to a Windows NT domain controller or an Active Directory server in compatibility mode. The Spotfire Analytics Server stores a list of usernames in its database, but no passwords.

4. X.509 Client Certificate

When the Spotfire Analytics Server is configured for X.509 Client Certificate authentication, the DecisionSite Client or TIBCO Spotfire will automatically try to log in by sending an X.509 client certificate to the Spotfire Analytics Server. If the server can validate the certificate, it accepts the identity indicated by the certificate. The Spotfire Analytics Server stores a list of usernames in its database, but no passwords or other security credentials.

5. Microsoft Windows NT Domain

When using this login system, usernames passwords provided by the end users logging in are validated by a Windows NT domain controller. The Spotfire Analytics Server stores a list of usernames in its database, but no passwords.

Please note that if you are using Microsoft Active Directory servers for authentication on your network, then the LDAP login system (see above) should be selected instead of this method.

1.4 Single Sign-on

There are several ways to set up the Spotfire Analytics Server and DecisionSite Client or TIBCO Spotfire, so that the end users will not have to provide a user name and password when they start their clients. By using one of the following configurations they can be logged in automatically using security credentials either from Windows or an X.509 Client Certificate.

- Windows Integrated Authentication (NTLM)
- Windows Integrated Authentication (Kerberos)
- X.509 Client Certificate

1.4.1 Windows Integrated Authentication (NTLM)

Setting up the server to use Windows Integrated Authentication (NTLM) will allow the users to automatically log into the Spotfire Analytics Server using the username of the current login session to the Windows domain server.

Note: If a user tries to log in using a client that is located in a foreign NT Domain, NTLM authentication will still work, but the user will be prompted for a user/password/domain that is valid. The specified account must be part of the domain the user is logging into.

Performance

Windows Integrated Authentication (NTLM) makes use of a built in mechanism in Windows, which requires more frequent reauthentication. For every reauthentication a call is made to the domain controller, which may affect performance negatively.

1.4.2 Windows Integrated Authentication (Kerberos)

Kerberos is a type of authentication implemented by Microsoft as an authentication protocol for use in Active Directory domains on Windows 2000 and later. It is considered a better and more secure alternative than NTLM, but is more demanding to set up.

Also, in some cases NTLM cannot be used to pass along login credentials between systems, which makes Kerberos authentication an alternative. For example, a default installation of Windows Vista on an end-user machine does not support NTLM. In such case, a

solution can be to set up the entire system for Kerberos authentication instead.

Kerberos authentication requires that you can access the Windows Active Directory server and make certain settings or perform certain commands.

If you wish to use Kerberos authentication on the Spotfire Analytics Server, it is recommended that you first install the server using an LDAP Login System and LDAP or Database User Directory Back-End. Once that has been set up and you have verified that things work as intended, make the switch to Kerberos by performing the necessary configuration procedures.

For more information, see “Setting Up Kerberos Authentication” on page 186.

Note: If you have users running Internet Explorer version 6, there is an issue that requires you to install the Spotfire Analytics Server on port 80. More information can be found in the Kerberos chapter of this manual.

1.4.3 X.509 Client Certificate

If the users have been assigned Internet Explorer compatible X.509 client certificates, you can optionally set up the Spotfire Analytics Server and Client to use these for automatic login. The client certificate including the security credentials will then be sent to the Spotfire Analytics Server, thus removing the need for supplying username and password. However it is still possible to not use this information for login, i.e., you can require certificates but still use username and password as login to further increase the security.

This setup requires the Spotfire Analytics Server to be configured with HTTPS and also to be set to require Client Certificates.

Also, the client machines need to set an option in Internet Explorer, “Don’t prompt for client certificate selection when no certificates or only one certificate exists”.

Performance

Using Client Certificates for authentication will affect performance negatively. Creating an encrypted connection requires more CPU cycles than doing an ordinary socket connection. This overhead will reduce the maximum capacity and increase latency in all communication between the client and server.

2 Installation

There are three database alternatives when installing the Spotfire Analytics Server:

- Install a bundled Oracle 10g XE database
- Use an already existing Oracle database
- Use an already existing Microsoft SQL Server database

The first option is bundled in the Spotfire Analytics Server installer. The last two options requires you to already have a working Oracle or Microsoft SQL Server database up and running which can be used by the Spotfire Analytics Server.

Please proceed to the option you want:

- **“Bundled Oracle 10g XE” on page 14.**
- **“Existing Oracle Database” on page 31.**
- **“Existing Microsoft SQL Server Database” on page 51.**

2.1 Bundled Oracle 10g XE

2.1.1 Prerequisites

See <http://tibco.spotfire.com/sr> for details, and make sure all requirements are met before proceeding.

Note: Read about the limitations of the bundled database in “Different Server Configurations” on page 8.

Hardware:

- CPU: Intel Pentium 4, 2 Ghz or higher
- RAM: 1 GB minimum (recommended 2GB or greater)
- Hard disk space:
 - 1 GB of free space to complete installation
 - 500 MB for base server software to execute
 - Recommended 10 GB or greater when Spotfire Analytics Server 10.0 is configured with database on the same machine.

Software:

Spotfire Analytics Server 10.1.2 using Apache Tomcat can be installed on the following Windows platforms:

- Microsoft Windows 2000 Server SP4 or higher
- Microsoft Windows Server 2003 SP1 or higher
- Microsoft Windows Server 2008

Administrative Privileges:

Since you are installing on a Microsoft Windows operating system, you must log in as a member of the administrators group to run the Spotfire Analytics Server installer. Specifically, the administrator should have the following:

- Full access to the file system of the target installation directory
- Full access to Windows system directory
- Permission to install and remove system services
- Full access to HKEY_LOCAL_MACHINE registry key

Folder Privileges for the Local System User:

By default, the Local System user will be used to run the server. You need to make sure that the corresponding user “System” has Full Control permission to the installation target folder and all its subfolders.

Other:

- Make sure you do not already have a database installed on the machine, which could conflict with the bundled database that is about to be installed.
- Make sure that you do not already have a web server installed on the machine, which could conflict with the ports of the Spotfire Analytics Server that is about to be installed.
- If you are installing the Spotfire Analytics Server on a Microsoft Windows Server 2008, be sure to make the appropriate changes to the built in firewall, to allow clients to access the Spotfire Analytics Server.

2.1.2 Checklist

Installing Spotfire Analytics Server requires you to specify various parameters in the installer. Therefore, its a good idea to make sure you have all the information needed before starting the installer. Use the checklist below and write down the settings needed.

Installation

Important: Do not use the same username for the three databases (Analytics Server database, Information Model database, Library database). You must specify a different username for each database.

Important: You must make sure that the port numbers you intend to use for the Spotfire Analytics Server are free, and not already occupied by some other application on the machine.

Parameter:	Fill in value here:
Apache Tomcat Listen Port:	<i>Default: 80</i>
Apache Tomcat Administrator User:	
Apache Tomcat Administrator Password:	
Oracle Server Listen Port	<i>Default: 1521</i>
Oracle MTS Port:	<i>Default: 2030</i>
Oracle HTTP Port:	<i>Default: 8080</i>
Oracle System Password:	
Spotfire Analytics Server Database User:	
Spotfire Analytics Server Database Password:	
Spotfire Information Model Database User:	
Spotfire Information Model Database Password:	
Spotfire Library Database User:	
Spotfire Library Database Password:	

2.1.3 Select the Appropriate Installer

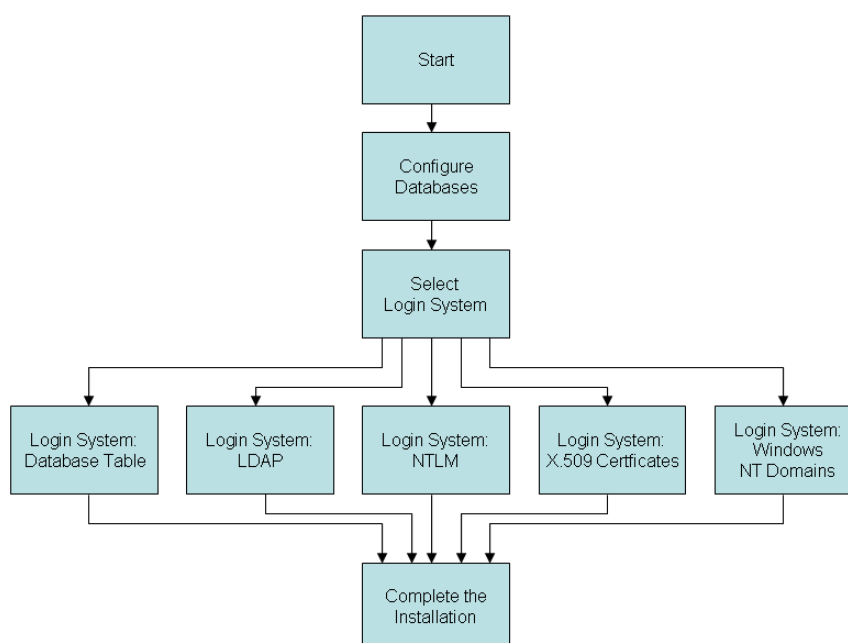
You are now ready to run the Spotfire Analytics Server installer.

Since you have decided to install the bundled Oracle 10g XE database, you must make sure to use the appropriate version of the installation kit:

- **TIB_ASWin_10.1.2_ORXE**

2.1.4 Installation Overview

The following flowchart outlines the basic sections of the installation.

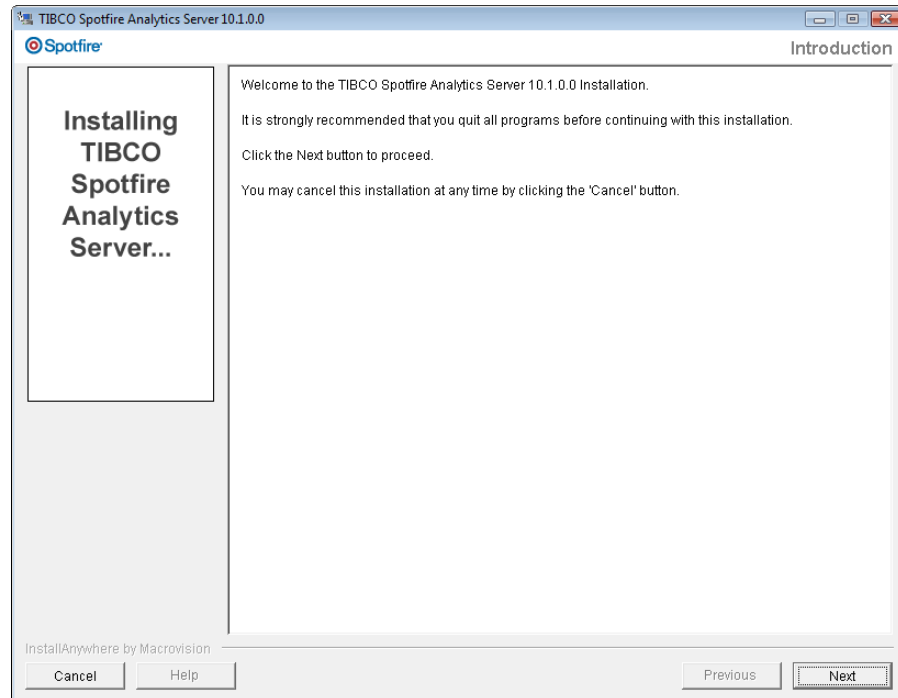


2.1.5 Main Installation

- ▶ **Run the Installer:**
 - 1 Copy the **TIB_ASWin_10.1.2_ORXE** directory to the Spotfire Analytics Server machine. Start the Spotfire Analytics Server installer by running the file **install.exe**.

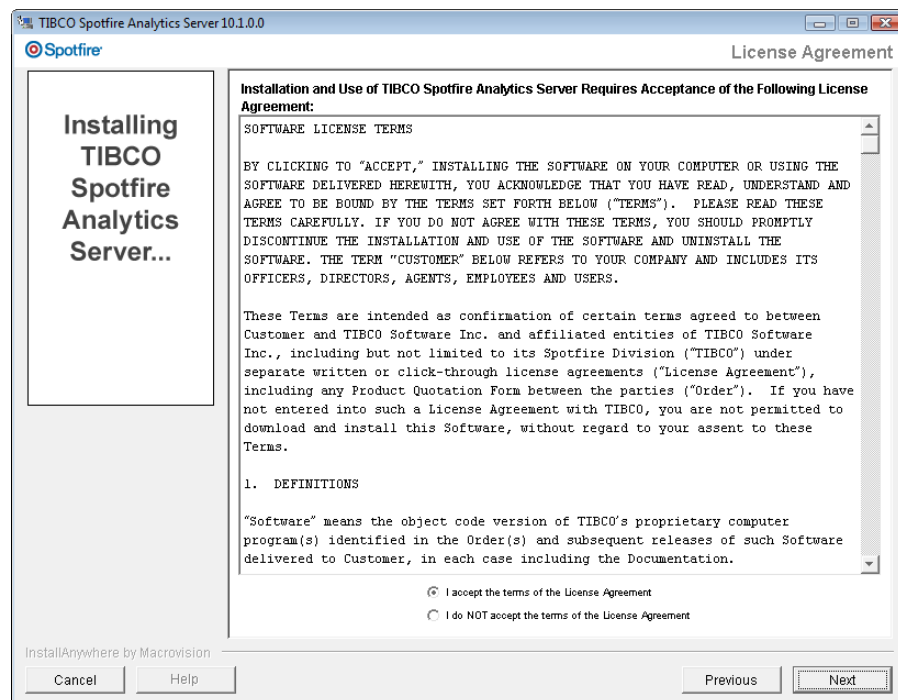
Installation

2



The installer starts. Click **Next** to continue.

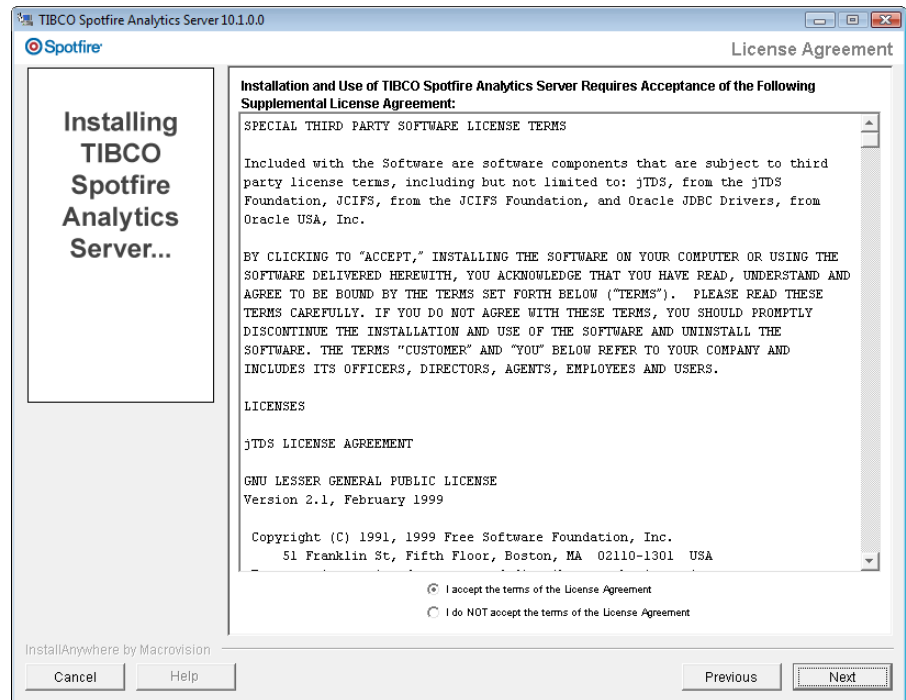
3



Read the license agreement, and select the appropriate radio button.

Click **Next** to continue.

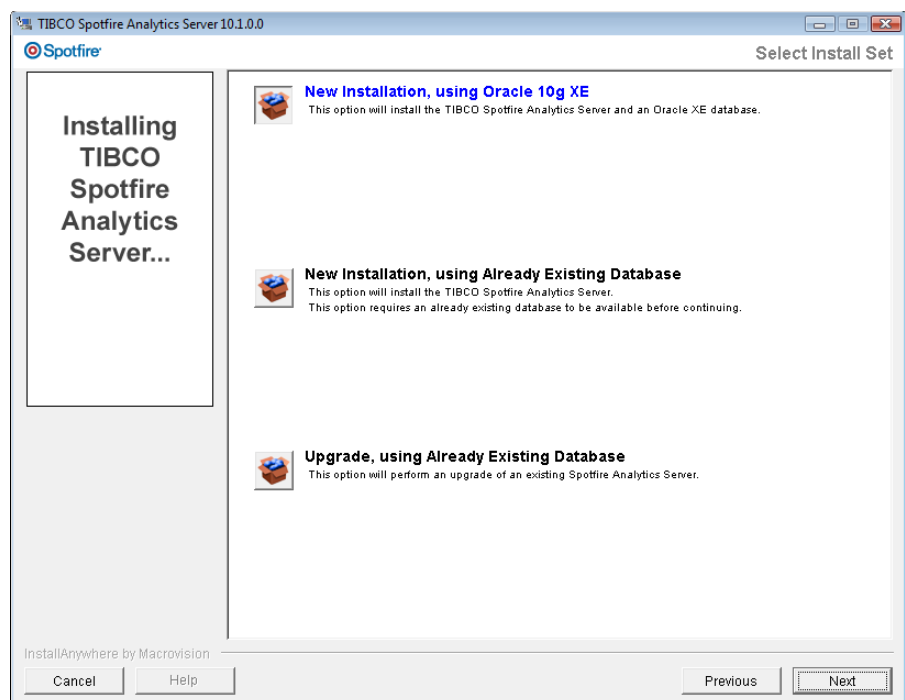
4



Read the supplemental license agreement, and select the appropriate radio button.

Click **Next** to continue.

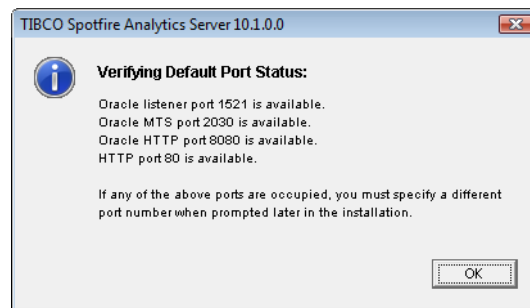
5



Select the topmost option, **New Installation, using Oracle 10g XE**.

Click **Next** to continue.

6



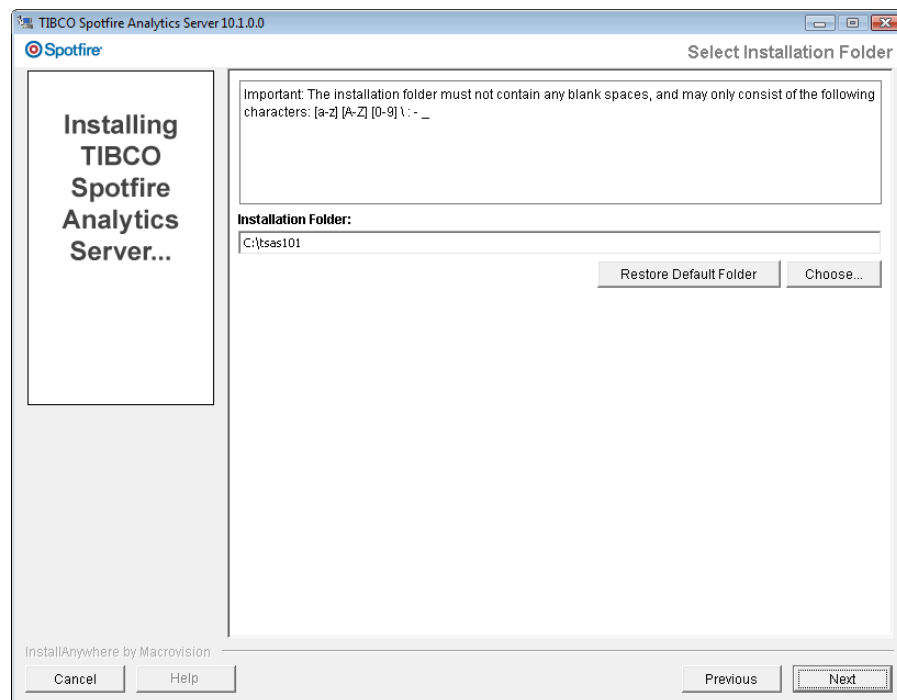
Since the Spotfire Analytics Server installer will install a Tomcat web server and an Oracle XE database, an automatic check is performed to verify if the default ports for these are available.

If all ports are listed as “available” you can choose to install everything on the suggested default ports. However, should any port be listed as “occupied” there is already some software on this machine using that port. This means you must specify a different port number for the corresponding port when prompted later in the installation.

Make a note of any occupied ports and port numbers, so you can avoid accidentally specifying identical port numbers later.

Click **OK** to continue.

7



Select or specify where you would like to install the Spotfire Analytics Server.

Note: Since Windows cannot handle paths with more than 255 characters, it is recommended that the server be installed as close to root level as possible. Also note that since you are not allowed to use certain characters such as blank spaces, you cannot install in the Program Files folder.

Click **Next** to continue.

8

TIBCO Spotfire Analytics Server 10.1.0.0

Apache Tomcat Configuration

Installing TIBCO Spotfire Analytics Server...

Specify the configuration information for the Apache Tomcat Server.
The Administrator User and Password you provide, will be needed when accessing the Apache Tomcat administration console.

Server Listen Port:
80

Administrator User:

Administrator Password:

Confirm Password:

InstallAnywhere by Macrovision

Cancel Help Previous Next

Enter the configuration information you want for the Apache Tomcat application server.

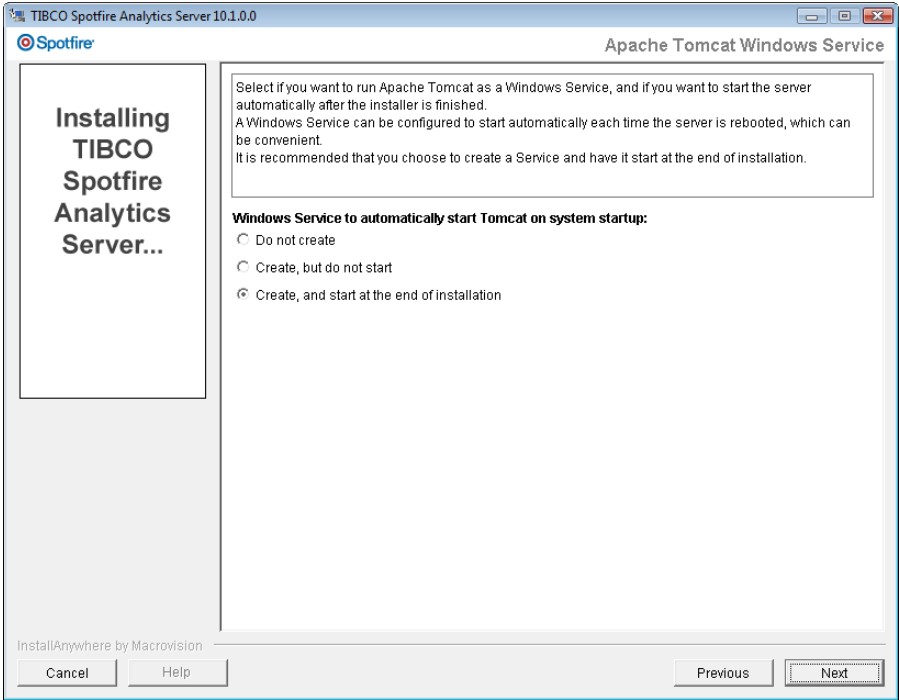
IMPORTANT!

Make a note of the Administrator username and password you specify, since you will need it to access the Apache Tomcat administration console later.

There is no way to retrieve this password if you forget, so make sure you remember it and write it down.

Click **Next** to continue.

9

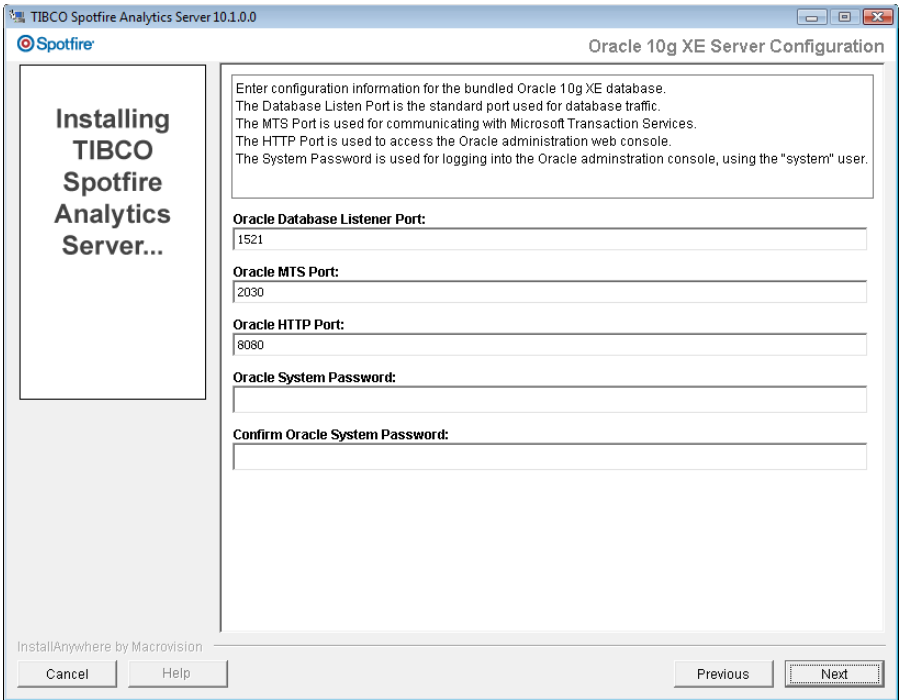


Select whether or not you want to create a Windows Service that will start the Apache Tomcat server each time the system restarts.

The recommended option is to **Create, and start at the end of installation.**

Click **Next** to continue.

10



Specify the configuration information for the bundled Oracle 10g XE database.

- The Database Listen Port is the standard port used for database traffic. Default value is 1521.
- The MTS Port is used for communicating with Microsoft Transaction Services. Default value is 2030.
- The HTTP Port is used to access the Oracle administration web console. Default value is 8080.
- The System Password is used for logging into the Oracle administration console, using the "system" user.

Click **Next** to continue.

11

Enter configuration information for the Spotfire Analytics Server database. This is used for storing information about Spotfire users, groups, their licenses and preferences.

Important: Do not use the same username for the three databases (Analytics Server database, Information Model database, Library database). You must specify a different username for each database.

Click **Next** to continue.

Installing TIBCO Spotfire Analytics Server...

Enter configuration information for the TIBCO Spotfire Information Model database. This is used by the TIBCO Spotfire Information Services component, which lets the end users access data from information links.

User:

Password:

Confirm Password:

Cancel Help Previous Next

InstallAnywhere by Macrovision

Enter configuration information for the Spotfire Information Model database. This is used by the Spotfire Information Services component, which lets the end users access data from information links.

Important: Do not use the same username for the three databases (Analytics Server database, Information Model database, Library database). You must specify a different username for each database.

Click **Next** to continue.

13

TIBCO Spotfire Analytics Server 10.1.0.0

Spotfire

TIBCO Spotfire Library Database

Enter configuration information for the TIBCO Spotfire Library database.
This database contains the TIBCO Spotfire Library which is used by the end users to share their TIBCO Spotfire files.

User:

Password:

Confirm Password:

InstallAnywhere by Macrovision

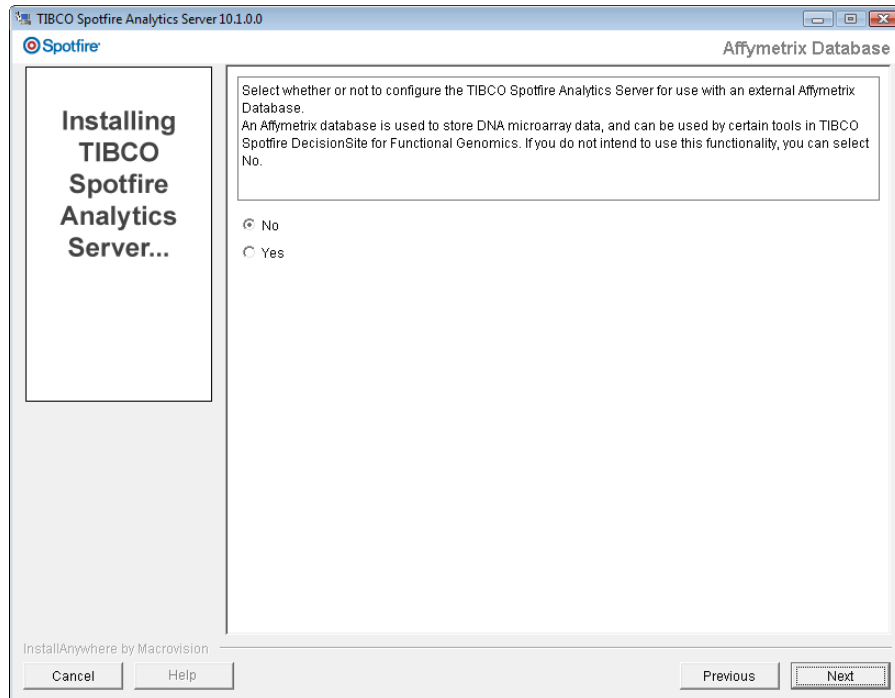
Cancel Help Previous Next

Enter configuration information for the Spotfire Library database. This database contains the Spotfire Library which is used by the end users to share their Spotfire files.

Important: Do not use the same username for the three databases (Analytics Server database, Information Model database, Library database). You must specify a different username for each database.

Click **Next** to continue.

14



Select whether or not to configure the Spotfire Analytics Server for use with an external Affymetrix Database.

An Affymetrix database is used to store DNA microarray data, and can be used by certain tools in TIBCO Spotfire DecisionSite for Functional Genomics. If you do not intend to use this functionality, you can select No.

Click **Next** to continue.

- If you selected **NO**, just skip the next step.

15

Installing TIBCO Spotfire Analytics Server...

Affymetrix Database Configuration

Enter configuration information for the external Affymetrix database that the TIBCO Spotfire Analytics Server should connect to.
An Affymetrix database is used to store DNA microarray data, and can be used by certain tools in TIBCO Spotfire DecisionSite for Functional Genomics.

Oracle Server:

Oracle Server Listen Port:

Oracle Service Name:

Oracle User:

Oracle Password:

Confirm Oracle Password:

If the database owner above is not the owner of the AADM tables, you must enter the correct table owner information below.

Table Owner:

InstallAnywhere by Macrovision

Enter configuration information for the external Affymetrix database that the Spotfire Analytics Server should connect to.

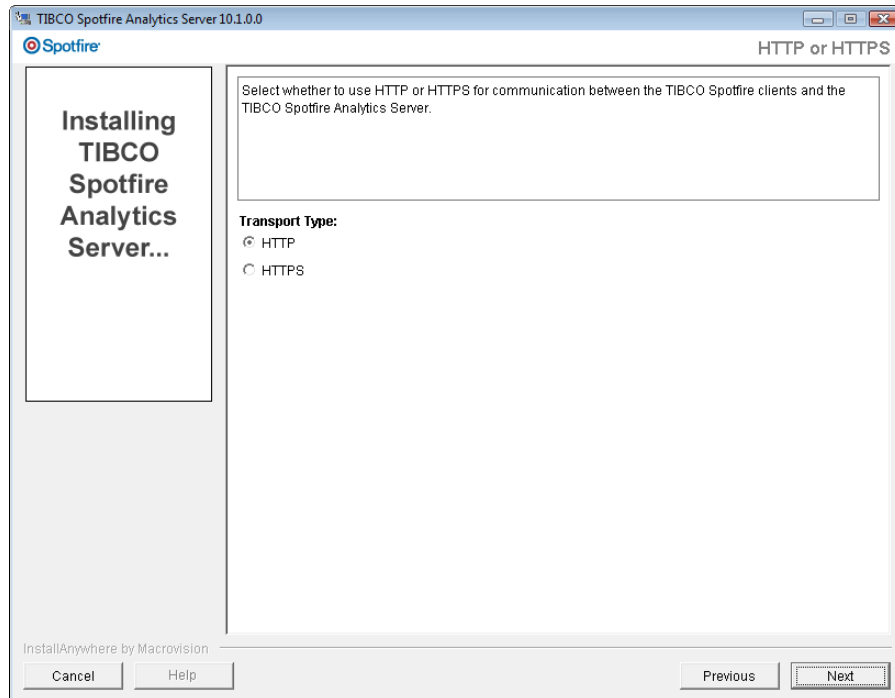
An Affymetrix database is used to store DNA microarray data, and can be used by certain tools in TIBCO Spotfire DecisionSite for Functional Genomics.

The **Oracle Server**, **Oracle Server Listen Port** and **Oracle Service Name** should point to the server which provides the AADM schema. The **Oracle User** and **Oracle Password** should be a user who has access to this database.

If the specified database user is not the owner of the AADM tables, it is also necessary to enter the correct **Table Owner** in the last field.

Click **Next** to continue.

16

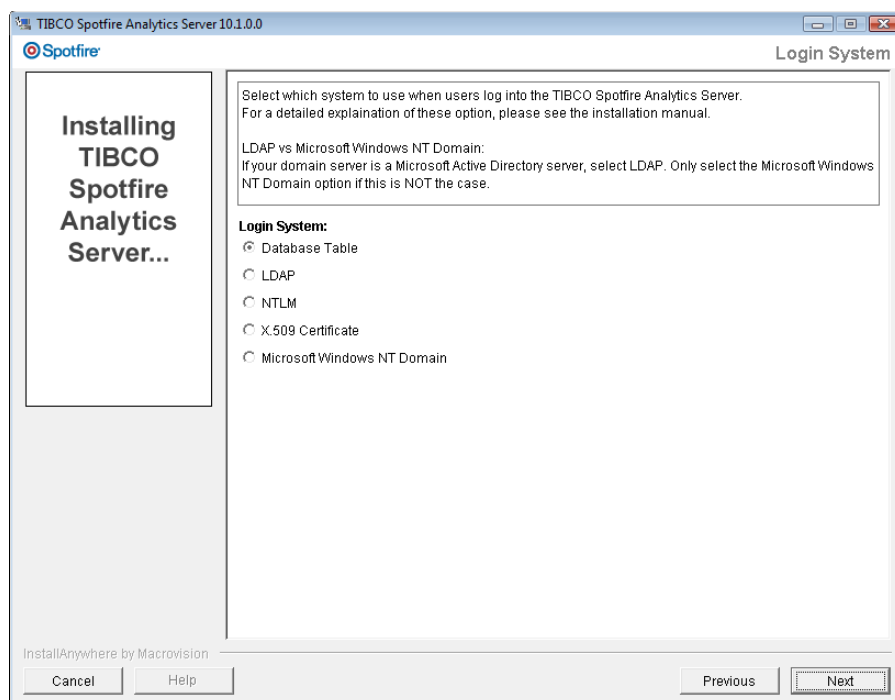


Select whether to use HTTP or HTTPS for communication between the Spotfire clients and the Spotfire Analytics Server.

Note: If you intend to use X.509 Certificates to authenticate users when logging in, you must select HTTPS.

Click **Next** to continue.

17



When you install the Spotfire Analytics Server you will need to specify how users will be authenticated when they log in, and which type of user directory will hold the list of all your users.

Login

DecisionSite Client and TIBCO Spotfire users who log into the Spotfire Analytics Server must to be authenticated in order to be allowed access to the server.

When installing the Spotfire Analytics Server you can configure it to use one of the five combinations of Login System and Login method described below.

User Directory Back-end

A bit simplified, you could say that the user directory is where the list of all your users is kept. For example, some companies have thousands of users already listed in a Microsoft Active Directory which they want to use, whereas some companies might decide it is sufficient to use the Spotfire Analytics Server database and add their users to that.

What is the Difference?

For a large company the user directory often contains thousands of users. You might not want all of these to have access to the Spotfire Analytics Server. Therefore, you can set up a different login system that only allows a certain number of these to log in.

The possible combinations available from the installer are indicated in the chart below.

Login	User Directory Back-end		
	Database Table	LDAP (For example, Microsoft Active Directory)	Windows NT Domain
Database Table	X		
LDAP (For example, Microsoft Active Directory)	X	X	
NTLM	X	X	X
X.509 Certificates	X	X	X
MS Windows NT Domain	X		X

1. Database Table

When using this login system, usernames and passwords provided by the end users logging in are compared with credentials stored in the Spotfire Analytics Server's database. For security reasons, the passwords are never stored in cleartext. Instead, the Spotfire

Analytics Server computes encrypted one-way hashes of the passwords.

Database Table authentication is ideal for small groups of users, but the administration of larger groups can be cumbersome because each user has to be manually added to the Database Table directory using the DecisionSite Administrator tool or the TIBCO Spotfire Administration Manager tool.

2. LDAP (for example, Microsoft Active Directory)

When using this login system, usernames and passwords provided by the end users logging in are validated by an LDAP server. The Spotfire Analytics Server stores a list of usernames in its database, but no passwords.

The Spotfire Analytics Server directly supports Microsoft Active Directory and Sun Java System Directory Server and should work with most other servers as well, though this might require some manual configuration.

3. NTLM (Windows Integrated Authentication)

When the Spotfire Analytics Server is configured for Windows Integrated Authentication (NTLM), DecisionSite Client or TIBCO Spotfire will be logged in automatically if the user has logged in using his or her Windows domain account. Spotfire Analytics Server delegates the authentication itself to a Windows NT domain controller or an Active Directory server in compatibility mode. The Spotfire Analytics Server stores a list of usernames in its database, but no passwords.

4. X.509 Client Certificate

When the Spotfire Analytics Server is configured for X.509 Client Certificate authentication, the DecisionSite Client or TIBCO Spotfire will automatically try to log in by sending an X.509 client certificate to the Spotfire Analytics Server. If the server can validate the certificate, it accepts the identity indicated by the certificate. The Spotfire Analytics Server stores a list of usernames in its database, but no passwords or other security credentials.

5. Microsoft Windows Domain

When using this authentication type, the usernames and passwords provided by the end users when logging in are validated by a Windows NT domain controller. The Spotfire Analytics Server stores a list of usernames in its database, but no passwords.

Please note that if you are using Microsoft Active Directory servers for authentication on your network, then the LDAP authentication method (see below) should be selected instead of this method.

Select which system to use to authenticate users when they log into the Spotfire Analytics Server.

Click **Next** to continue.

- **Database Table** - proceed to “Completing the Installation” on page 86.
- **LDAP** - proceed to “LDAP Installation” on page 70.
- **NTLM** - proceed to “NTLM Installation” on page 76.
- **X.509 Certificate** - proceed to “X.509 Certificate Installation” on page 78.
- **Microsoft Windows NT Domain** - proceed to “Microsoft Windows NT Domain Installation” on page 83.

2.2 Existing Oracle Database

2.2.1 Prerequisites

See <http://tibco.spotfire.com/sr> for details, and make sure all requirements are met before proceeding.

Hardware:

- CPU: Intel Pentium 4, 2 Ghz or higher
- RAM: 1 GB minimum (recommended 2GB or greater)
- Hard disk space:
 - 1 GB of free space to complete installation
 - 500 MB for base server software to execute
 - Recommended 10 GB or greater when Spotfire Analytics Server 10.0 is configured with database on the same machine.

Software:

Spotfire Analytics Server 10.1.2 using Apache Tomcat can be installed on the following Windows platforms:

- Microsoft Windows 2000 Server SP4 or higher
- Microsoft Windows Server 2003 SP1 or higher
- Microsoft Windows Server 2008

In order to use an Oracle Enterprise/Standard database, please note that this is third-party software that must be installed by the customer prior to the Spotfire software installation.

Supported Versions:

- Oracle 11g Release 1 (11.1.0.x)
- Oracle10g Release 2 (10.2.0.x)
- Oracle10g Release 1 (10.1.0.x)
- Oracle9i Release 2 (9.2.0.x)

Administrative Privileges:

Since you are installing on a Microsoft Windows operating system, you must log in as a member of the administrators group to run the Spotfire Analytics Server installer. Specifically, the administrator should have the following:

- Full access to the file system of the target installation directory
- Full access to Windows system directory
- Permission to install and remove system services
- Full access to HKEY_LOCAL_MACHINE registry key

Folder Privileges for the Local System User:

By default, the Local System user will be used to run the server. You need to make sure that the corresponding user “System” has Full Control permission to the installation target folder and all its subfolders.

Other:

- Make sure that you do not already have a web server installed on the machine, which could conflict with the ports of the Spotfire Analytics Server that is about to be installed.

2.2.2 Checklist

Installing Spotfire Analytics Server requires you to specify various parameters in the installer and in database scripts. Therefore, it is a good idea to make sure you have all the information needed before starting the installer. Use the checklist below and write down the settings needed.

- Rows that are shaded grey indicate values that are already set for your system; these you must find out and specify.
- Rows that are not shaded indicate values that you must now specify for the first time.

Important: Do not use the same username for the three databases (Analytics Server database, Information Model database, Library database). You must specify a different username for each database.

Important: You must make sure that the port numbers you intend to use for the Spotfire Analytics Server are free, and not already occupied by some other application on the machine.

Parameter:	Fill in value here:
Apache Tomcat Listen Port:	<i>Default: 80</i>
Apache Tomcat Administrator User:	
Apache Tomcat Administrator Password:	
Oracle Server Name:	
Oracle Instance Name: (also mentioned as CONNECTIDENTIFIER)	<i>Default: spotfire</i>
Oracle Server Listen Port	<i>Default: 1521</i>
Oracle System Password:	
Spotfire Analytics Server Database User:	
Spotfire Analytics Server Database Password:	
Spotfire Information Model Database User:	
Spotfire Information Model Database Password:	
Spotfire Library Database User:	
Spotfire Library Database Password:	

2.2.3 Preinstallation Procedures

2.2.3.1 Select the Appropriate Installer

You are now ready to run the Spotfire Analytics Server installer.

To install on an external already existing Oracle database, use the **TIB_ASWin_10.1.2_NoDB** installer.

2.2.3.2 Copy the Scripts to the Local Disk

Before you can run the Spotfire Analytics Server installer, you must set up the Spotfire Analytics Server Databases. This is done by running a few scripts. However, these must first be opened and modified to suit your preferences. In order to do this, the files must be copied to the local disk of your intended database server.

- 1 Find the directory **\scripts\oracle_install** on the installation media.
- 2 Copy this entire directory to a temporary place on the local disk of your intended database server.

2.2.3.3 Modify the **create_databases.bat** script

The next thing to do is to modify the **create_databases.bat** script. You will find this in the **\scripts** directory you just copied.

Note: If your database server is a Solaris machine, use the **create_databases.sh** script instead.

- 1 Open the file **create_databases.bat** in a text editor.
- 2 Find the rows:


```
set CONNECTIDENTIFIER=<SID>
set ADMINNAME=system
set ADMINPASSWORD=<ORACLEDB_PASSWORD>
set SERVERDB_USER=<SERVERDB_USER>
set SERVERDB_PASSWORD=<SERVERDB_PASSWORD>
set IIMDB_USER=<IIMDB_USER>
set IIMDB_PASSWORD=<IIMDB_PASSWORD>
set LIBRARY_USER=<LIBRARY_USER>
set LIBRARY_PASSWORD=<LIBRARY_PASSWORD>
```
- 3 Set the **CONNECTIDENTIFIER** variable. This is the Oracle TNS name for the database.
- 4 Set the **ADMINNAME** variable.
- 5 Set the **ADMINPASSWORD** variable.
- 6 Specify the User and Password for the three database tables that will be created.

Important: Remember or write these down in the checklist above, since you will need to enter them again during the installation.

Comment: Exchange the <PARAMETER> for a username or password of your choice. Example:
set LIBRARY_PASSWORD=my5ecretpa55w0rd
with no brackets.

- 7 Save the file, and exit the editor.

2.2.3.4 Modify the SQL scripts

The next thing to do is to open and modify three .SQL files:

- create_dss_env.sql
- create_iim_env.sql
- create_library_env.sql

Important: Do not use the same username for the three databases (Analytics Server database, Information Model database, Library database). You must specify a different username for each database.

- 1 Open the above mentioned files in a text editor. The files can be found in the \scripts\oracle_install directory you just copied to disk.
- 2 In the **create_dss_env.sql** file, do a search/replace in the file, and replace <ORACLE_HOME> with a suitable file system path.

The tablespaces will be created under <ORACLE_HOME>, thus it must be a directory that is writable for the Oracle instance, usually <oracle install dir>/oradata/<SID>.

Do a search/replace in the file, and replace <SERVERDB_USER> with the username you specified in the create_databases.bat file.

Do a search/replace in the file, and replace <SERVERDB_PASSWORD> with the password you specified in the create_databases.bat file.

- 3 In the **create_iim_env.sql** file, do a search/replace in the file, and replace <ORACLE_HOME> with a suitable file system path.

The tablespaces will be created under <ORACLE_HOME>, thus it must be a directory that is writable for the Oracle instance, usually <oracle install dir>/oradata/<SID>.

Do a search/replace in the file, and replace <IIMDB_USER> with the username you specified in the create_databases.bat file.

Do a search/replace in the file, and replace <IIMDB_PASSWORD> with the password you specified in the create_databases.bat file.

- 4 In the **create_library_env.sql** file, do a search/replace in the file, and replace **<ORACLE_HOME>** with a suitable file system path.

The tablespaces will be created under **<ORACLE_HOME>**, thus it must be a directory that is writable for the Oracle instance, usually **<oracle install dir>/oradata/<SID>**.

Do a search/replace in the file, and replace **<LIBRARY_USER>** with the username you specified in the **create_databases.bat** file.

Do a search/replace in the file, and replace **<LIBRARY_PASSWORD>** with the password you specified in the **create_databases.bat** file.

- 5 Review the suggested size of the tablespaces. It is strongly recommended that you keep the settings as they are, unless you have a good reason to change them.
- 6 Save the files, and exit the editor.

2.2.3.5 Run the **create_databases.bat** script

Once the scripts have been properly set up, run the **create_databases.bat** script.

Note: If your database server is a Solaris machine, use the **create_databases.sh** script instead.

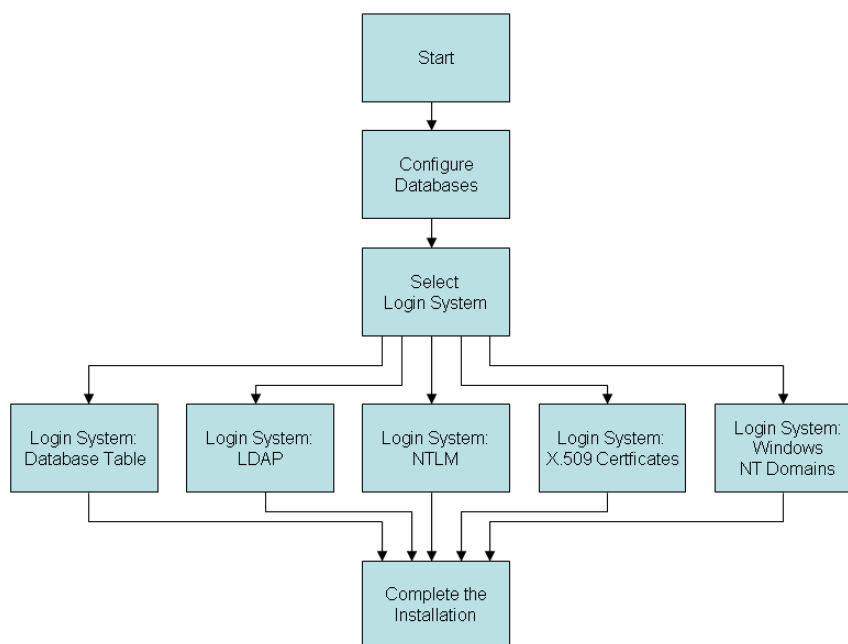
- 1 Open a command prompt window.
- 2 Navigate to the directory where you placed the scripts.
- 3 Type **create_databases.bat** and press **Enter**.

Response: The scripts now set up the databases tables needed to run Spotfire Analytics Server.

A number of log files called **log*.txt** will be created in the same directory as the **create_databases** file. Please examine these files to verify that no errors occurred.

2.2.4 Installation Overview

The following flowchart outlines the basic sections of the installation.

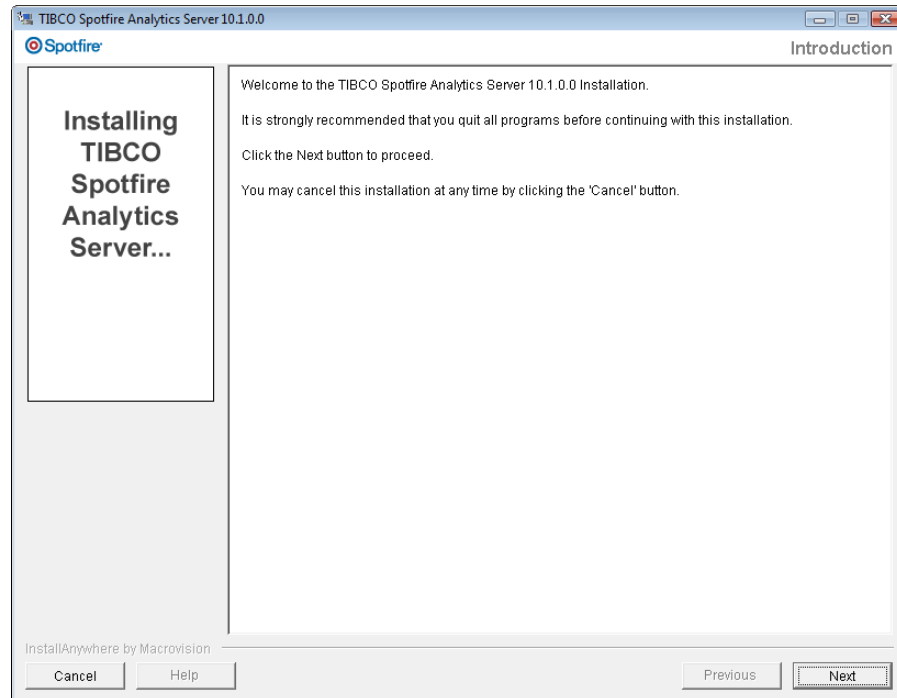


2.2.5 Main Installation

- ▶ **Run the Installer:**
 - 1 Copy the **TIB_ASWin_10.1.2_NoDB** directory to the Spotfire Analytics Server machine. Start the Spotfire Analytics Server installer by running the file **install.exe**.

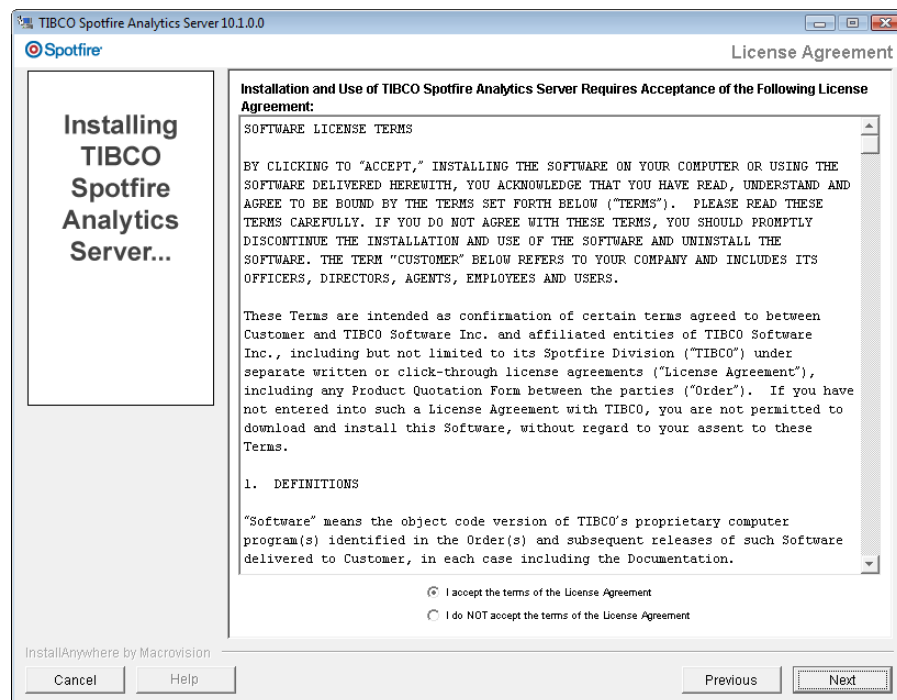
Installation

2



The installer starts. Click **Next** to continue.

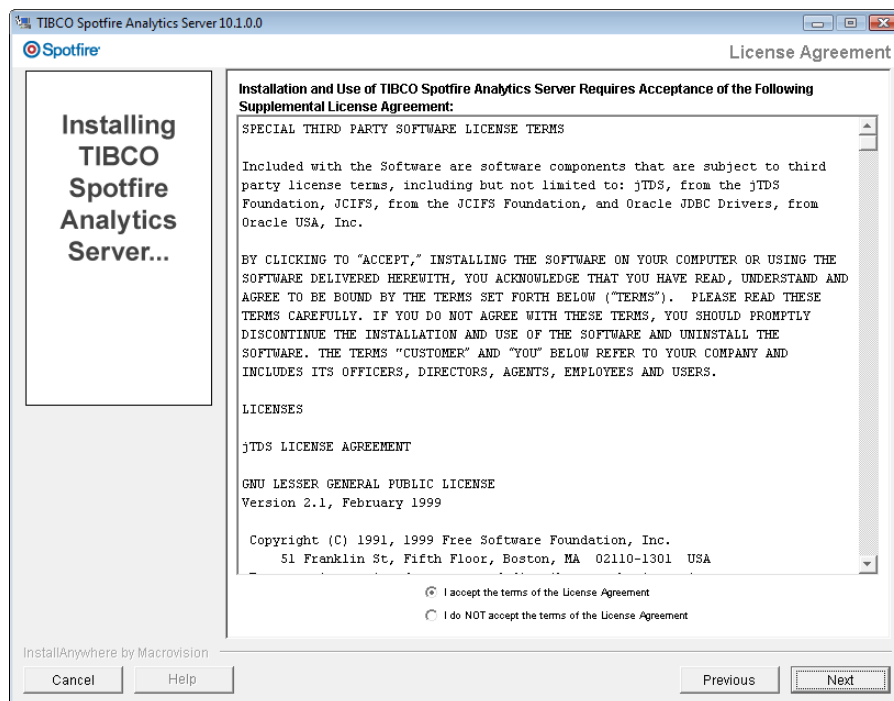
3



Read the license agreement, and select the appropriate radio button.

Click **Next** to continue.

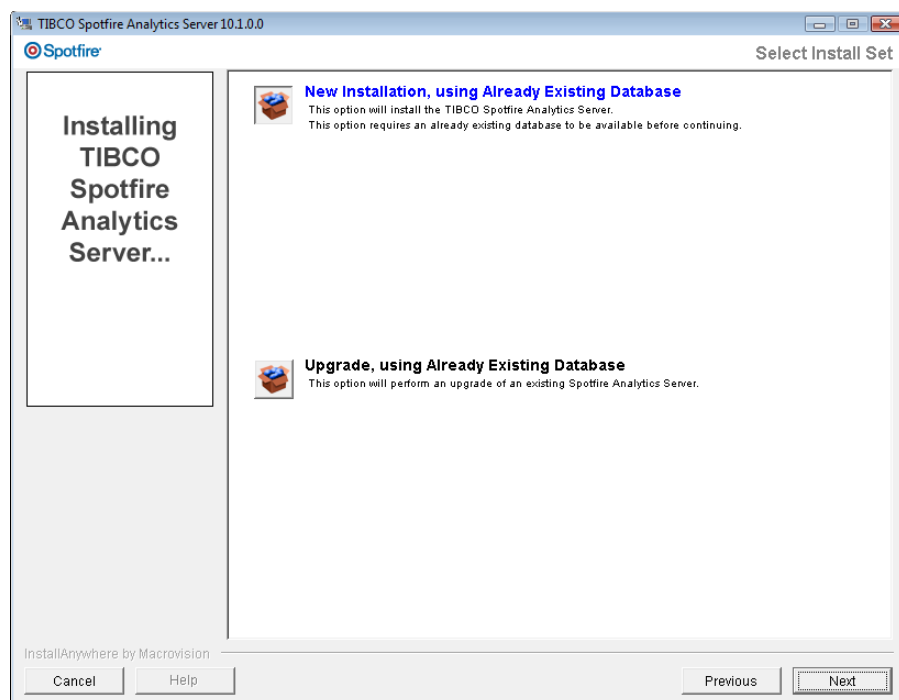
4



Read the supplemental license agreement, and select the appropriate radio button.

Click **Next** to continue.

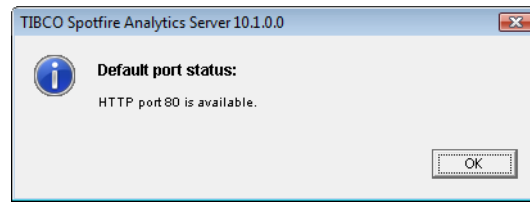
5



Select **New Installation, using Already Existing Database**.

Click **Next** to continue.

6



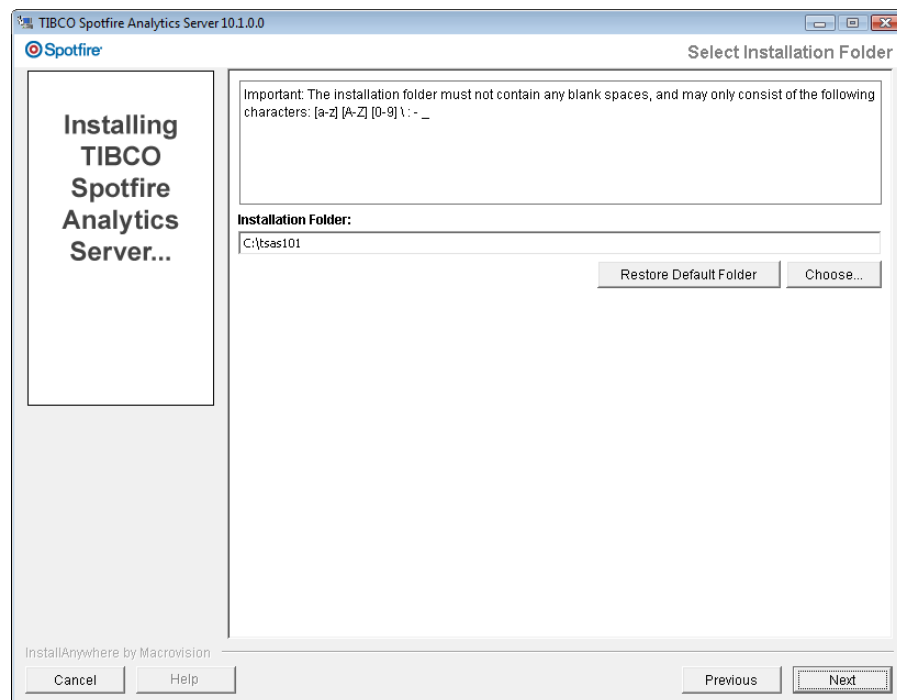
Since the Spotfire Analytics Server installer will install a Tomcat web server, an automatic check is performed to verify if the default ports for this are available.

If all ports are listed as “available” you can choose to install everything on the suggested default ports. However, should any port be listed as “occupied” there is already some software on this machine using that port. This means you must specify a different port number for the corresponding port when prompted later in the installation.

Make a note of any occupied ports and port numbers, so you can avoid accidentally specifying identical port numbers later.

Click **OK** to continue.

7



Select or specify where you would like to install the Spotfire Analytics Server.

Note: Since Windows cannot handle paths with more than 255 characters, it is recommended that the server be installed as close to

root level as possible. Also note that since you are not allowed to use certain characters such as blank spaces, you cannot install in the Program Files folder.

Click **Next** to continue.

8

TIBCO Spotfire Analytics Server 10.1.0.0

Apache Tomcat Configuration

Installing TIBCO Spotfire Analytics Server...

Specify the configuration information for the Apache Tomcat Server.
The Administrator User and Password you provide, will be needed when accessing the Apache Tomcat administration console.

Server Listen Port:
80

Administrator User:

Administrator Password:

Confirm Password:

Cancel Help Previous Next

InstallAnywhere by Macrovision

Enter the configuration information you want for the Apache Tomcat application server.

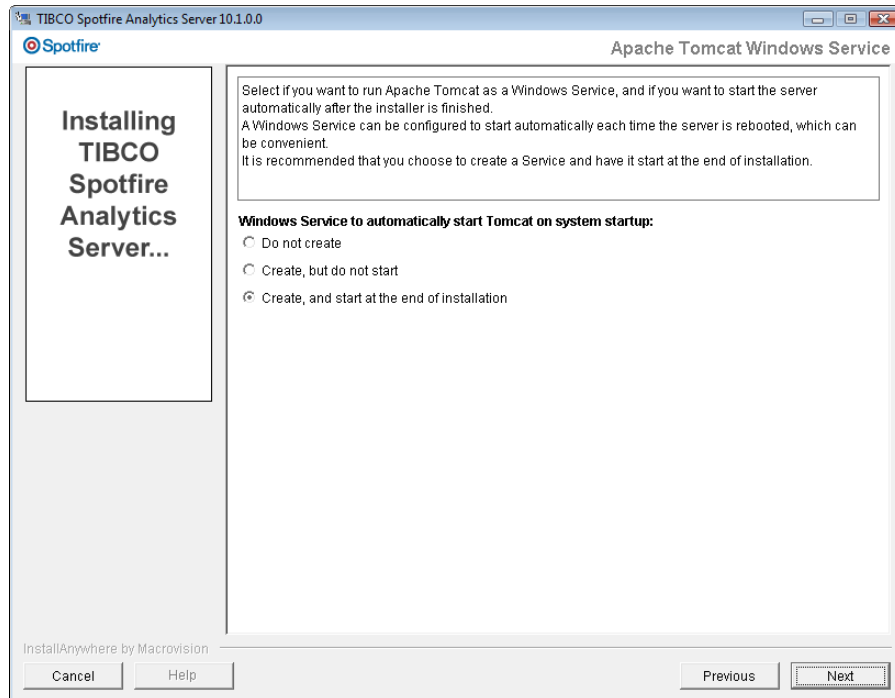
IMPORTANT!

Make a note of the Administrator username and password you specify, since you will need it to access the Apache Tomcat administration console later.

There is no way to retrieve this password if you forget, so make sure you remember it and write it down.

Click **Next** to continue.

9

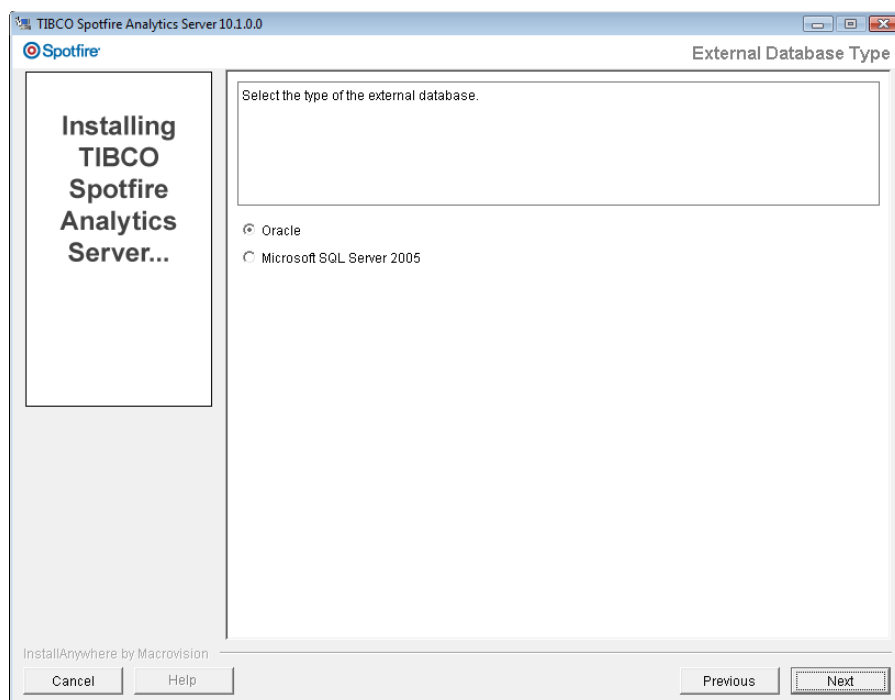


Select whether or not you want to create a Windows Service that will start the Apache Tomcat server each time the system restarts.

The recommended option is to **Create, and start at the end of installation.**

Click **Next** to continue.

10



Select to use an **Oracle** database.

Click **Next** to continue.

11

The screenshot shows the 'TIBCO Spotfire Analytics Server Database' configuration window. On the left, a sidebar reads 'Installing TIBCO Spotfire Analytics Server...'. The main area contains instructions: 'Enter configuration information for the TIBCO Spotfire Analytics Server database. This is used for storing information about TIBCO Spotfire users, their licenses and preferences. For an Oracle database, the default port is 1521.' Below this are input fields for 'Server:', 'Port:' (with '1521' entered), 'Instance Name:' (with 'spotfire' entered), 'User:', 'Password:', and 'Confirm Password:'. At the bottom are 'Cancel', 'Help', 'Previous', and 'Next' buttons. The status bar at the bottom left says 'InstallAnywhere by Macrovision'.

Enter configuration information for the Spotfire Analytics Server database. This is used for storing information about Spotfire users, groups, their licenses and preferences.

Specify the Server name, the Server port (default: **1521**) and the Instance Name (default: spotfire) as well as username and password for the data tables.

Important: Do not use the same username for the three databases (Analytics Server database, Information Model database, Library database). You must specify a different username for each database.

Click **Next** to continue.

Installing TIBCO Spotfire Analytics Server...

Enter configuration information for the TIBCO Spotfire Information Model database. This is used by the TIBCO Spotfire Information Services component, which lets the end users access data from information links. For an Oracle database, the default port is 1521.

Server:

Port: 1521

Instance Name: spotfire

User:

Password:

Confirm Password:

Cancel Help Previous Next

InstallAnywhere by Macrovision

Enter configuration information for the Spotfire Information Model database. This is used by the Spotfire Information Services component, which lets the end users access data from information links.

Specify the Server name, the Server port (default: **1521**) and the Instance Name (default: spotfire) as well as username and password for the data tables.

Important: Do not use the same username for the three databases (Analytics Server database, Information Model database, Library database). You must specify a different username for each database.

Click **Next** to continue.

13

TIBCO Spotfire Analytics Server 10.1.0.0

Installing TIBCO Spotfire Analytics Server...

TIBCO Spotfire Library Database

Enter configuration information for the TIBCO Spotfire Library database.
This database contains the TIBCO Spotfire Library which is used by the end users to share their TIBCO Spotfire files.
For an Oracle database, the default port is 1521.

Server:

Port: 1521

Instance Name: spotfire

User:

Password:

Confirm Password:

InstallAnywhere by Macrovision

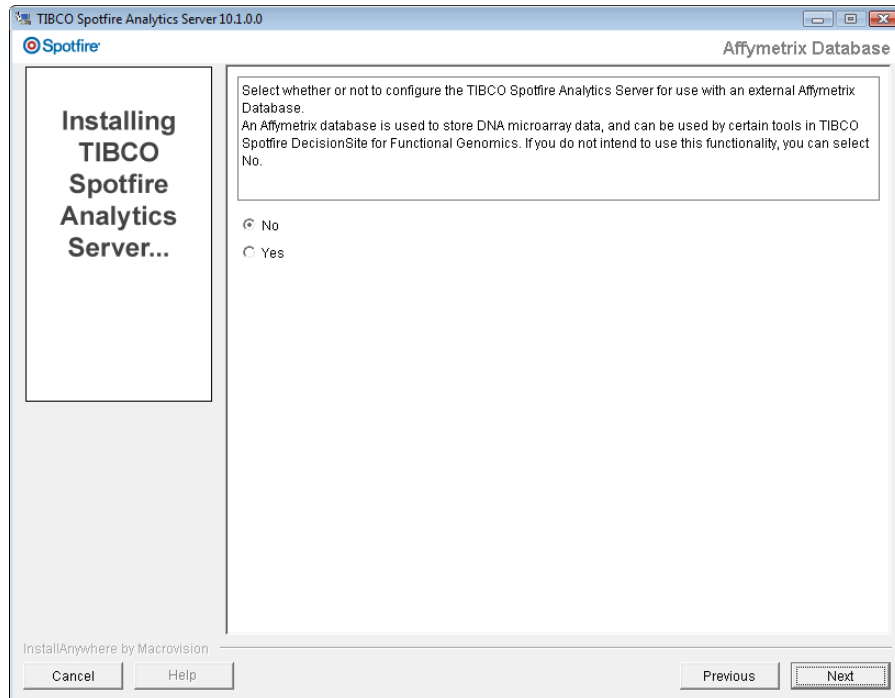
Cancel Help Previous Next

Enter configuration information for the Spotfire Library database. This database contains the Spotfire Library which is used by the end users to share their Spotfire files.

Specify the Server name, the Server port (default: **1521**) and the Instance Name (default: spotfire) as well as username and password for the data tables.

Important: Do not use the same username for the three databases (Analytics Server database, Information Model database, Library database). You must specify a different username for each database.

Click **Next** to continue.



Select whether or not to configure the Spotfire Analytics Server for use with an external Affymetrix Database.

An Affymetrix database is used to store DNA microarray data, and can be used by certain tools in TIBCO Spotfire DecisionSite for Functional Genomics. If you do not intend to use this functionality, you can select No.

Click **Next** to continue.

- If you selected **NO**, just skip the next step.

15

Enter configuration information for the external Affymetrix database that the Spotfire Analytics Server should connect to.

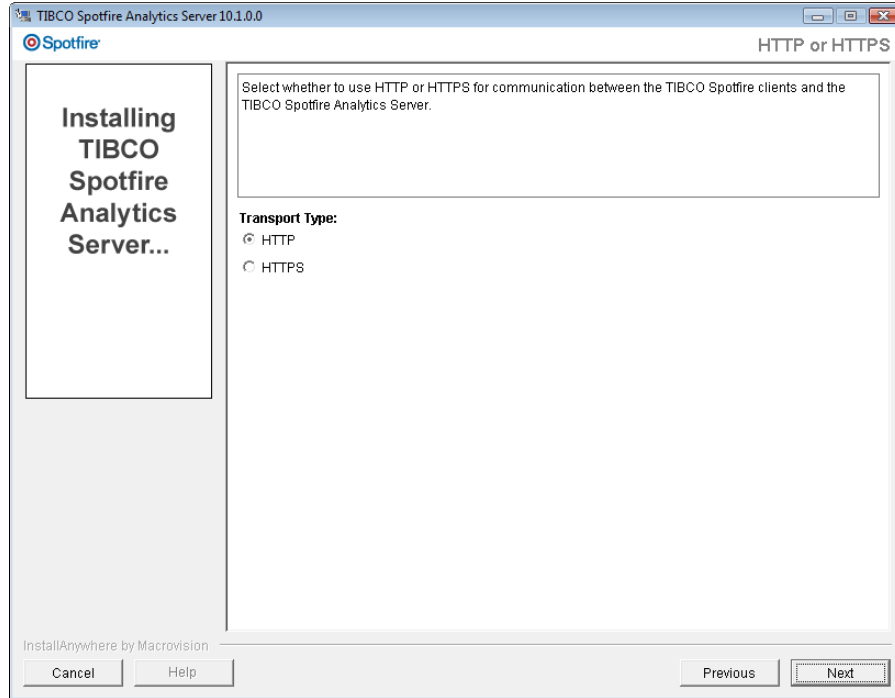
An Affymetrix database is used to store DNA microarray data, and can be used by certain tools in TIBCO Spotfire DecisionSite for Functional Genomics.

The **Oracle Server**, **Oracle Server Listen Port** and **Oracle Service Name** should point to the server which provides the AADM schema. The **Oracle User** and **Oracle Password** should be a user who has access to this database.

If the specified database user is not the owner of the AADM tables, it is also necessary to enter the correct **Table Owner** in the last field.

Click **Next** to continue.

16

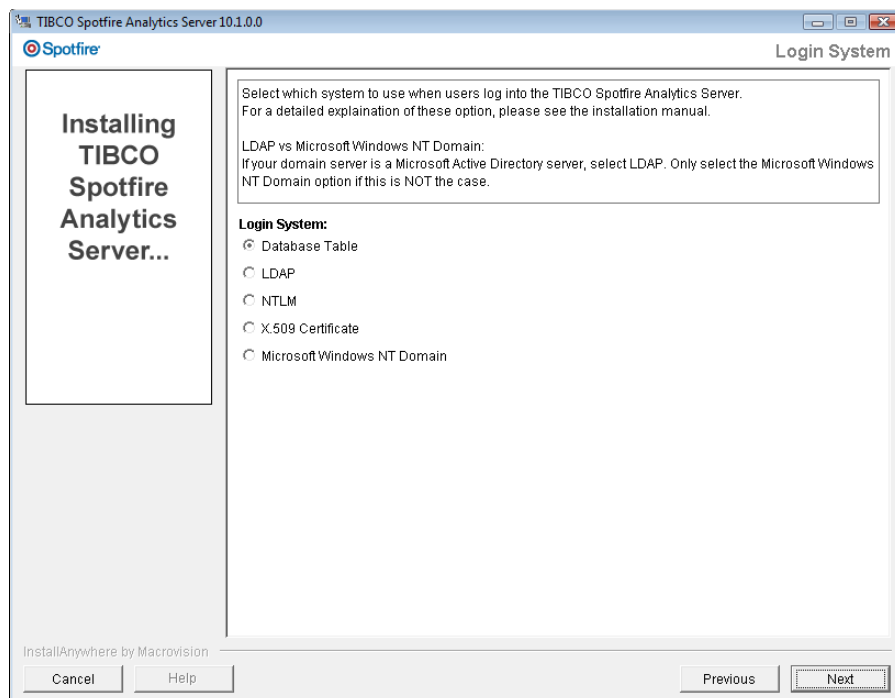


Select whether to use HTTP or HTTPS for communication between the Spotfire clients and the Spotfire Analytics Server.

Note: If you intend to use X.509 Certificates to authenticate users when logging in, you must select HTTPS.

Click **Next** to continue.

17



When you install the Spotfire Analytics Server you will need to specify how users will be authenticated when they log in, and which type of user directory will hold the list of all your users.

Login

DecisionSite Client and TIBCO Spotfire users who log into the Spotfire Analytics Server must to be authenticated in order to be allowed access to the server.

When installing the Spotfire Analytics Server you can configure it to use one of the five combinations of Login System and Login method described below.

User Directory Back-end

A bit simplified, you could say that the user directory is where the list of all your users is kept. For example, some companies have thousands of users already listed in a Microsoft Active Directory which they want to use, whereas some companies might decide it is sufficient to use the Spotfire Analytics Server database and add their users to that.

What is the Difference?

For a large company the user directory often contains thousands of users. You might not want all of these to have access to the Spotfire Analytics Server. Therefore, you can set up a different login system that only allows a certain number of these to log in.

The possible combinations available from the installer are indicated in the chart below.

Login	User Directory Back-end		
	Database Table	LDAP (For example, Microsoft Active Directory)	Windows NT Domain
Database Table	X		
LDAP (For example, Microsoft Active Directory)	X	X	
NTLM	X	X	X
X.509 Certificates	X	X	X
MS Windows NT Domain	X		X

1. Database Table

When using this login system, usernames and passwords provided by the end users logging in are compared with credentials stored in the Spotfire Analytics Server's database. For security reasons, the passwords are never stored in cleartext. Instead, the Spotfire

Analytics Server computes encrypted one-way hashes of the passwords.

Database Table authentication is ideal for small groups of users, but the administration of larger groups can be cumbersome because each user has to be manually added to the Database Table directory using the DecisionSite Administrator tool or the TIBCO Spotfire Administration Manager tool.

2. LDAP (for example, Microsoft Active Directory)

When using this login system, usernames and passwords provided by the end users logging in are validated by an LDAP server. The Spotfire Analytics Server stores a list of usernames in its database, but no passwords.

The Spotfire Analytics Server directly supports Microsoft Active Directory and Sun Java System Directory Server and should work with most other servers as well, though this might require some manual configuration.

3. NTLM (Windows Integrated Authentication)

When the Spotfire Analytics Server is configured for Windows Integrated Authentication (NTLM), DecisionSite Client or TIBCO Spotfire will be logged in automatically if the user has logged in using his or her Windows domain account. Spotfire Analytics Server delegates the authentication itself to a Windows NT domain controller or an Active Directory server in compatibility mode. The Spotfire Analytics Server stores a list of usernames in its database, but no passwords.

4. X.509 Client Certificate

When the Spotfire Analytics Server is configured for X.509 Client Certificate authentication, the DecisionSite Client or TIBCO Spotfire will automatically try to log in by sending an X.509 client certificate to the Spotfire Analytics Server. If the server can validate the certificate, it accepts the identity indicated by the certificate. The Spotfire Analytics Server stores a list of usernames in its database, but no passwords or other security credentials.

5. Microsoft Windows Domain

When using this authentication type, the usernames and passwords provided by the end users when logging in are validated by a Windows NT domain controller. The Spotfire Analytics Server stores a list of usernames in its database, but no passwords.

Please note that if you are using Microsoft Active Directory servers for authentication on your network, then the LDAP authentication method (see below) should be selected instead of this method.

Select which system to use to authenticate users when they log into the Spotfire Analytics Server.

Click **Next** to continue.

- **Database Table** - proceed to “Completing the Installation” on page 86.
- **LDAP** - proceed to “LDAP Installation” on page 70.
- **NTLM** - proceed to “NTLM Installation” on page 76.
- **X.509 Certificate** - proceed to “X.509 Certificate Installation” on page 78.
- **Microsoft Windows NT Domain** - proceed to “Microsoft Windows NT Domain Installation” on page 83.

2.3 Existing Microsoft SQL Server Database

2.3.1 Prerequisites

See <http://tibco.spotfire.com/sr> for details, and make sure all requirements are met before proceeding.

Hardware:

- CPU: Intel Pentium 4, 2 Ghz or higher
- RAM: 1 GB minimum (recommended 2GB or greater)
- Hard disk space:
1 GB of free space to complete installation
500 MB for base server software to execute
Recommended 10 GB or greater when Spotfire Analytics Server 10.0 is configured with database on the same machine.

Software:

Spotfire Analytics Server 10.1.2 using Apache Tomcat can be installed on the following Windows platforms:

- Microsoft Windows 2000 Server SP4 or higher
- Microsoft Windows Server 2003 SP1 or higher
- Microsoft Windows Server 2008

In order to use a Microsoft SQL Server 2005 database, please note that this is third-party software that must be installed by the customer prior to the Spotfire software installation.

Supported Database Versions:

- Microsoft SQL Server 2005 Enterprise SP2
- Microsoft SQL Server 2005 Standard SP2
- Microsoft SQL Server 2005 Workgroup SP2
- Microsoft SQL Server 2005 Express SP2

Administrative Privileges:

Since you are installing on a Microsoft Windows operating system, you must log in as a member of the administrators group to run the Spotfire Analytics Server installer. Specifically, the administrator should have the following:

- Full access to the file system of the target installation directory
- Full access to Windows system directory
- Permission to install and remove system services
- Full access to HKEY_LOCAL_MACHINE registry key

Folder Privileges for the Local System User:

By default, the Local System user will be used to run the server. You need to make sure that the corresponding user “System” has Full Control permission to the installation target folder and all its subfolders.

Other:

- Make sure that you do not already have a web server installed on the machine which could conflict with the ports of the Spotfire Analytics Server that is about to be installed.
- The Microsoft SQL Server 2005 must not be set to “case sensitive” mode. Make sure it is set to “case insensitive”.
- The Microsoft SQL Server 2005 must be set to “mixed mode” for authentication.

2.3.2 Checklist

Installing Spotfire Analytics Server requires you to specify various parameters in the installer and in database scripts. Therefore, it's a good idea to make sure you have all the information needed before starting the installer. Use the checklist below and write down the settings needed.

- Rows that are shaded gray indicate values that are already set for your system; these you must find out and specify.

- Rows that are not shaded indicate values that you must now specify for the first time.

Important: Do not use the same username for the three databases (Analytics Server database, Information Model database, Library database). You must specify a different username for each database.

Important: You must make sure that the port numbers you intend to use for the Spotfire Analytics Server are free, and not already occupied by some other application on the machine.

Parameter:	Fill in value here:
Apache Tomcat Listen Port:	<i>Default: 80</i>
Apache Tomcat Administrator User:	
Apache Tomcat Administrator Password:	
Microsoft SQL Server 2005 Server Name:	
Microsoft SQL Server 2005 Instance Name:	
Microsoft SQL Server 2005 Server Listen Port	<i>Default: 1433</i>
Microsoft SQL Server 2005 System Admin Password:	
Spotfire Analytics Server Database User:	
Spotfire Analytics Server Database Password:	
Spotfire Information Model Database User:	
Spotfire Information Model Database Password:	
Spotfire Library Database User:	
Spotfire Library Database Password:	

2.3.3 Preinstallation Procedures

2.3.3.1 Set Specific TCP Port for Microsoft SQL Server 2005

The Microsoft SQL Server 2005 must be configured to listen on a specific TCP port. The standard port number for a Microsoft SQL Server 2005 is 1433.

Some versions of Microsoft SQL Server 2005 use a dynamic TCP port by default, this must be re-configured. For more information on how to do this, see Microsoft article “How to: Configure a Server to Listen on a Specific TCP Port (SQL Server Configuration Manager)”:

[http://msdn2.microsoft.com/en-us/library/ms177440\(SQL.90\).aspx](http://msdn2.microsoft.com/en-us/library/ms177440(SQL.90).aspx)

Make sure to enable the TCP/IP protocol, and to restart the SQL Server service to make the changes take effect.

2.3.3.2 Select the Appropriate Installer

To install on an external already existing Microsoft SQL Server database, use the **TIB_ASWin_10.1.2_NoDB** installer.

2.3.3.3 Copy the Scripts to the Local Disk

Before you can run the Spotfire Analytics Server installer, you must set up the Spotfire Analytics Server Databases. This is done by running a few scripts. However, these must first be opened and modified to suit your preferences. In order to do this, the files must be copied to the local disk of your intended database server.

- 1 Find the directory **\scripts\mssql_install** on the installation media.
- 2 Copy this entire directory to a temporary place on the local disk of your intended database server.

2.3.3.4 Modify the **create_databases.bat** script

The next thing to do is to modify the **create_databases.bat** script. You will find this in the **\scripts\mssql_install** directory you just copied.

- 1 Open the file **create_databases.bat** in a text editor.
- 2 Find the rows:


```
set CONNECTIDENTIFIER=<SERVER>\<MSSQL_INSTANCENAME>
set ADMINNAME=sa
set ADMINPASSWORD=<MSSQL_SAPASSWD>
```
- 3 Set the **CONNECTIDENTIFIER** variable. This is done by replacing **<SERVER>** with the name of the server running the SQL Server

instance, and replacing <MSSQL_INSTANCENAME> with the name of the SQL Server instance.

- 4 Set the ADMINNAME variable.
- 5 Set the ADMINPASSWORD variable.
- 6 Save the file, and exit the editor.

2.3.3.5 Modify the create_users.sql script

The next thing to do is to modify the **create_users.sql** script. You will find this in the **\scripts\mssql_install** directory you just copied.

Important: Do not use the same username for the three databases (Analytics Server database, Information Model database, Library database). You must specify a different username for each database.

- 1 Open the file **create_users.sql** in a text editor.
- 2 Do a search/replace in the file, and replace <SERVERDB_USER> with a user that you wish to create and use for this database table.
- 3 Do a search/replace in the file, and replace <IIMDB_USER> with a user that you wish to create and use for this database table.
- 4 Do a search/replace in the file, and replace <LIBRARY_USER> with a user that you wish to create and use for this database table.
- 5 Do a search/replace in the file, and replace <SERVERDB_PASSWORD> with the password you specified in the checklist. This must be 8-14 characters long.
- 6 Do a search/replace in the file, and replace <IIMDB_PASSWORD> with the password you specified in the checklist. This must be 8-14 characters long.
- 7 Do a search/replace in the file, and replace <LIBRARY_PASSWORD> with the password you specified in the checklist. This must be 8-14 characters long.
- 8 Save the files, and exit the editor.

2.3.3.6 Run the create_databases.bat script

Once the script has been properly set up, run the create_databases.bat script.

- 1 Open a command prompt window.
- 2 Navigate to the directory where you placed the scripts.

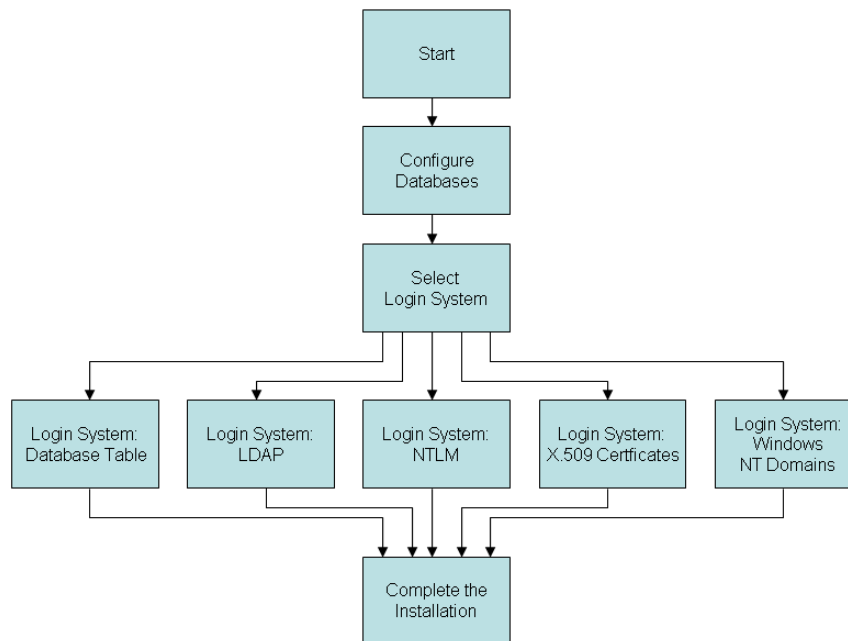
- 3 Type **create_databases.bat** and press **Enter**.

Response: The scripts now set up the databases tables needed to run Spotfire Analytics Server. Note that this may take some time.

A number of log files called log*.txt will be created in the same directory as the create_databases file. Please examine these files to verify that no errors occurred.

2.3.4 Installation Overview

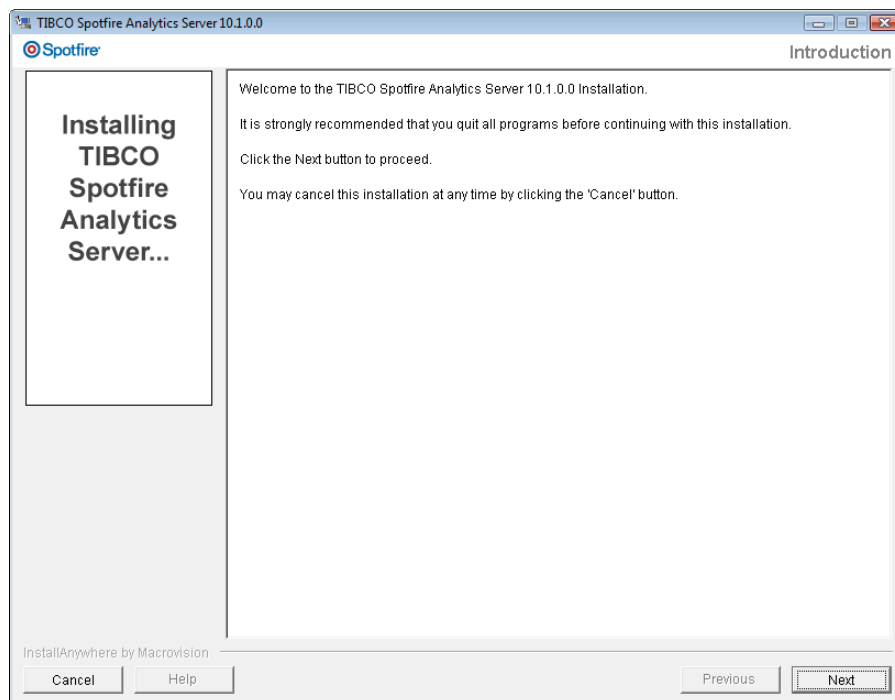
The following flowchart outlines the basic sections of the installation.



2.3.5 Main Installation

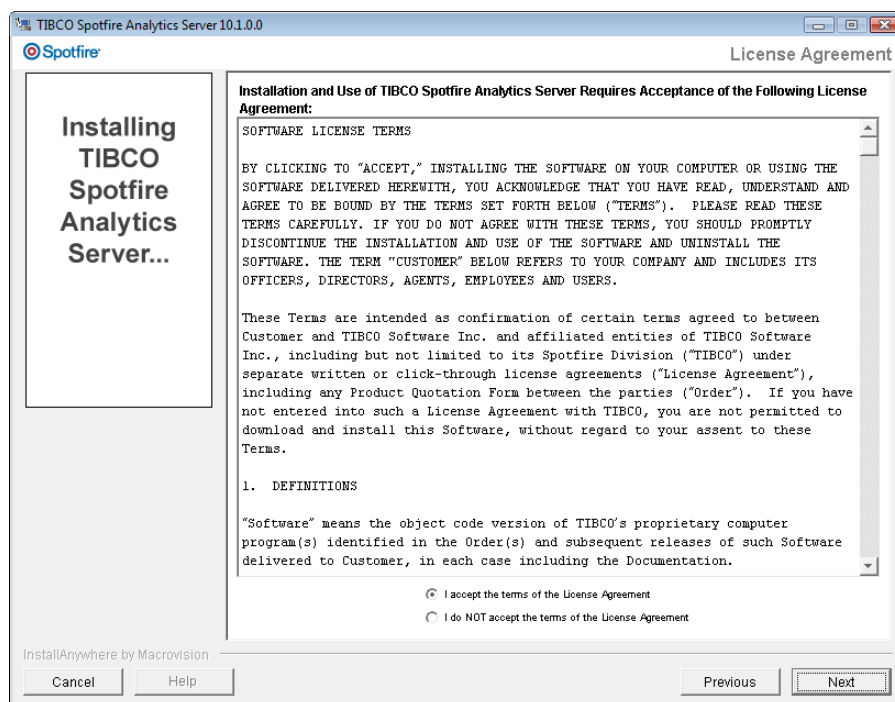
- ▶ **Run the Installer:**
 - 1 Copy the **TIB_ASWin_10.1.2_NoDB** directory to the Spotfire Analytics Server machine. Start the Spotfire Analytics Server installer by running the file **install.exe**.

2



The installer starts. Click **Next** to continue.

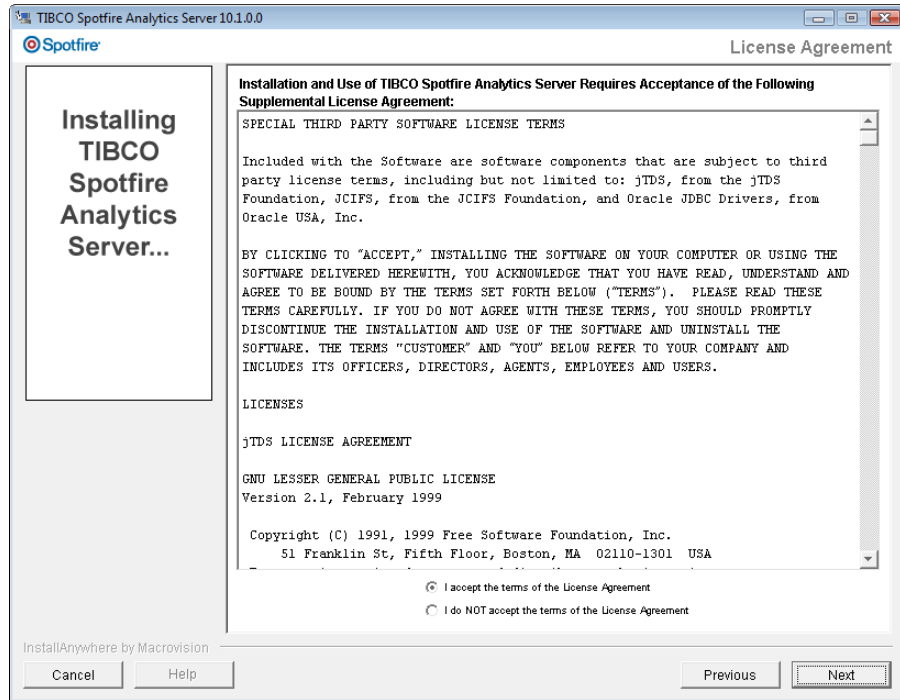
3



Read the license agreement, and select the appropriate radio button.

Click **Next** to continue.

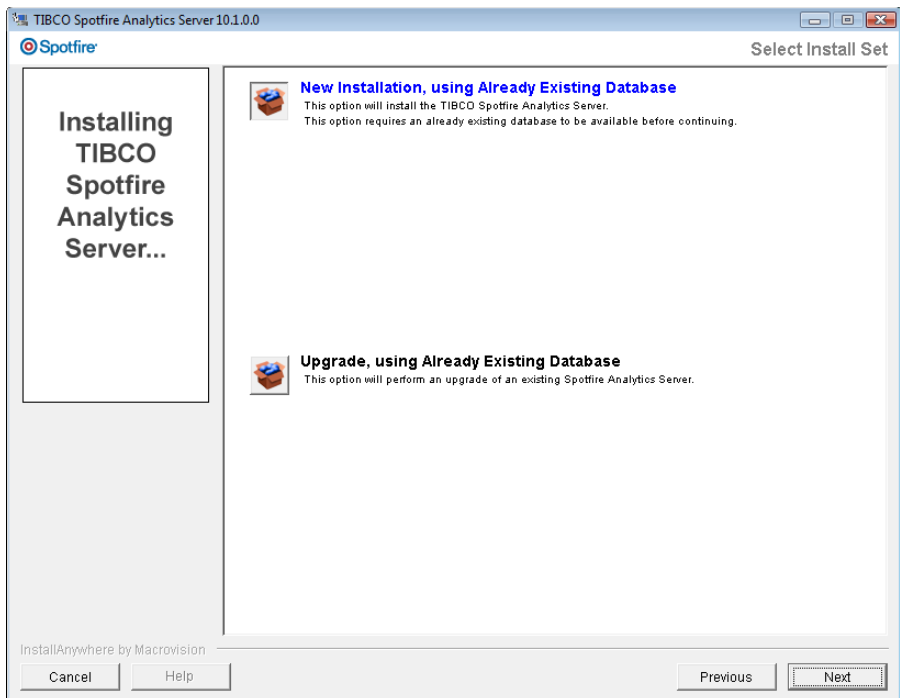
4



Read the supplemental license agreement, and select the appropriate radio button.

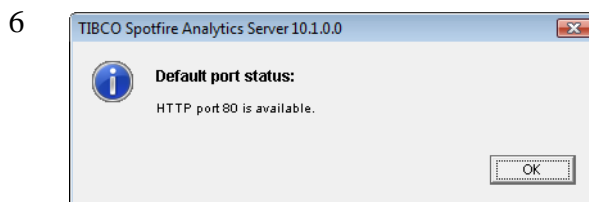
Click **Next** to continue.

5



Select **New Installation, using Already Existing Database**.

Click **Next** to continue.

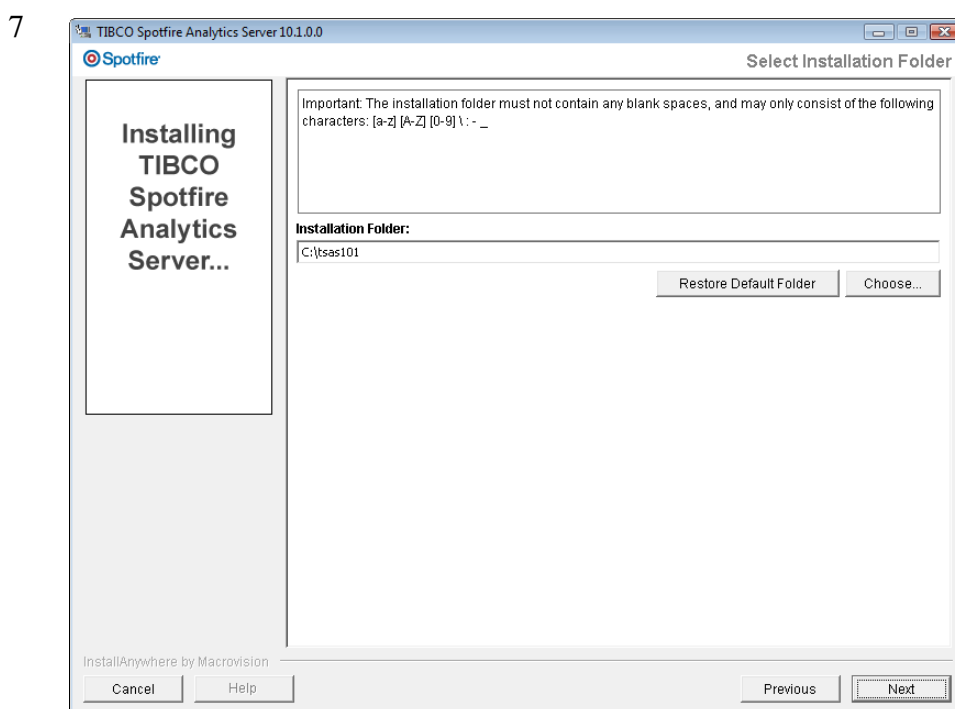


Since the Spotfire Analytics Server installer will install a Tomcat web server, an automatic check is performed to verify if the default ports for this are available.

If all ports are listed as “available” you can choose to install everything on the suggested default ports. However, should any port be listed as “occupied” there is already some software on this machine using that port. This means you must specify a different port number for the corresponding port when prompted later in the installation.

Make a note of any occupied ports and port numbers, so you can avoid accidentally specifying identical port numbers later.

Click **OK** to continue.



Select or specify where you would like to install the Spotfire Analytics Server.

Note: Since Windows cannot handle paths with more than 255 characters, it is recommended that the server be installed as close to

root level as possible. Also note that since you are not allowed to use certain characters such as blank spaces, you cannot install in the Program Files folder.

Click **Next** to continue.

8

Installing TIBCO Spotfire Analytics Server...

Specify the configuration information for the Apache Tomcat Server.
The Administrator User and Password you provide, will be needed when accessing the Apache Tomcat administration console.

Server Listen Port:
80

Administrator User:

Administrator Password:

Confirm Password:

InstallAnywhere by Macrovision

Cancel Help Previous Next

Enter the configuration information you want for the Apache Tomcat application server.

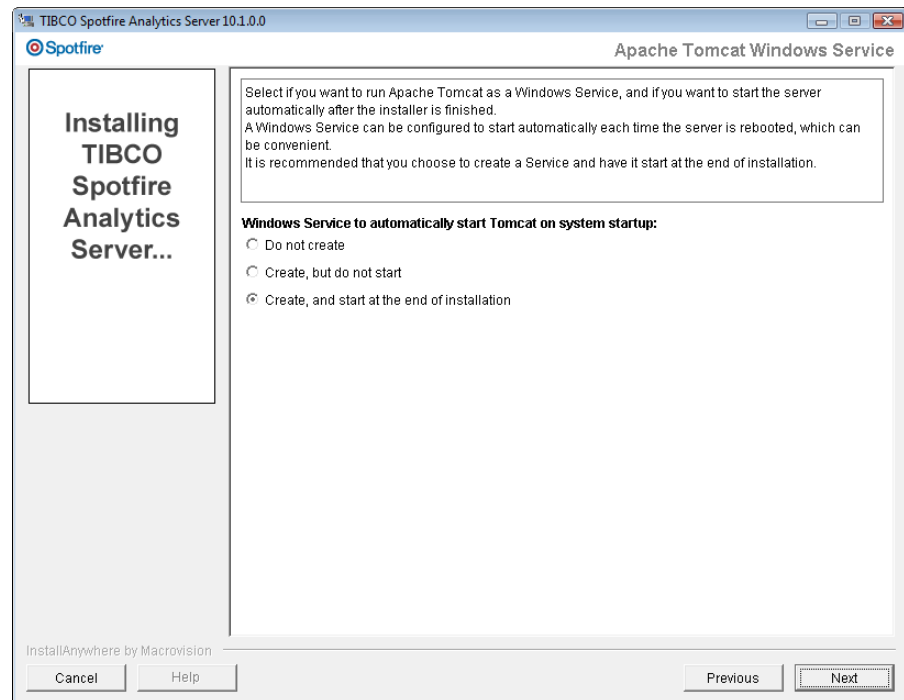
IMPORTANT!

Make a note of the Administrator username and password you specify, since you will need it to access the Apache Tomcat administration console later.

There is no way to retrieve this password if you forget, so make sure you remember it and write it down.

Click **Next** to continue.

9

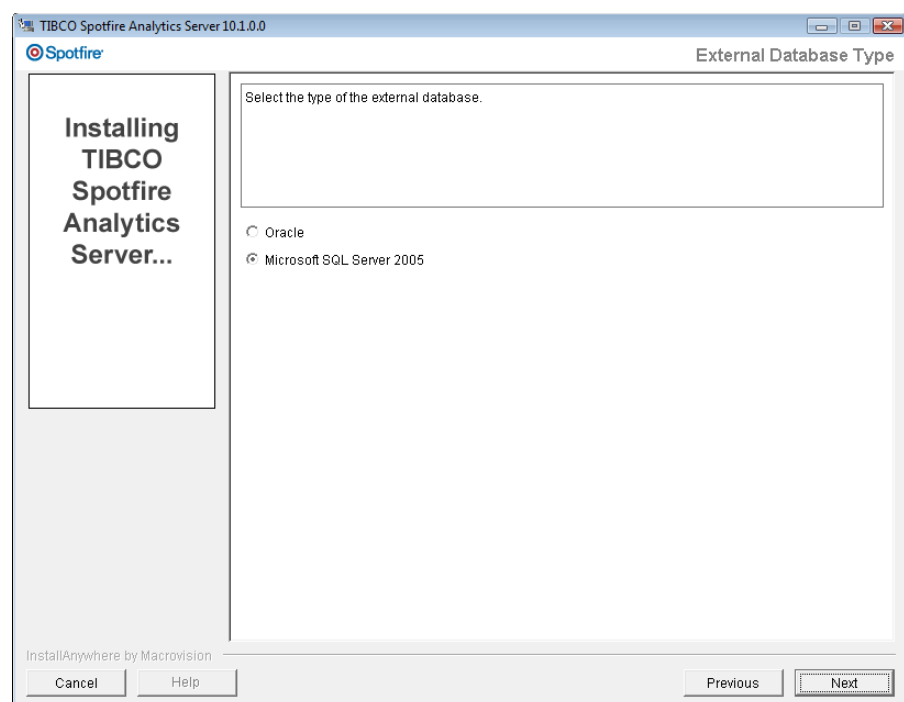


Select whether or not you want to create a Windows Service that will start the Apache Tomcat server each time the system restarts.

The recommended option is to **Create, and start at the end of installation.**

Click **Next** to continue.

10



Select **Microsoft SQL Server 2005**.

Click **Next** to continue.

11

The screenshot shows the 'TIBCO Spotfire Analytics Server Database' configuration window. On the left, a sidebar reads 'Installing TIBCO Spotfire Analytics Server...'. The main area contains instructions: 'Enter configuration information for the TIBCO Spotfire Analytics Server database. This is used for storing information about TIBCO Spotfire users, their licenses and preferences. For a Microsoft SQL Server 2005 database, the default port is 1433.' Below this are input fields for 'Server:', 'Port:' (with '1433' entered), 'User:', 'Password:', and 'Confirm Password:'. At the bottom, there are 'Cancel', 'Help', 'Previous', and 'Next' buttons. The window title bar says 'TIBCO Spotfire Analytics Server 10.1.0.0'.

Enter configuration information for the Spotfire Analytics Server database. This is used for storing information about Spotfire users, groups, their licenses and preferences.

Specify the Server name and the Server port (default: **1433**) as well as username and password for the data tables.

Important: Do not use the same username for the three databases (Analytics Server database, Information Model database, Library database). You must specify a different username for each database.

Click **Next** to continue.

12

Installing TIBCO Spotfire Analytics Server...

TIBCO Spotfire Information Model Database

Enter configuration information for the TIBCO Spotfire Information Model database. This is used by the TIBCO Spotfire Information Services component, which lets the end users access data from information links.

For a Microsoft SQL Server 2005 database, the default port is 1433.

Server:

Port: 1433

User:

Password:

Confirm Password:

InstallAnywhere by Macrovision

Cancel Help Previous Next

Enter configuration information for the Spotfire Information Model database. This is used by the Spotfire Information Services component, which lets the end users access data from information links.

Specify the Server name and the Server port (default: **1433**) as well as username and password for the data tables.

Important: Do not use the same username for the three databases (Analytics Server database, Information Model database, Library database). You must specify a different username for each database.

Click **Next** to continue.

13

Installing TIBCO Spotfire Analytics Server...

TIBCO Spotfire Library Database

Enter configuration information for the TIBCO Spotfire Library database.
This database contains the TIBCO Spotfire Library which is used by the end users to share their TIBCO Spotfire files.
For a Microsoft SQL Server 2005 database, the default port is 1433.

Server:

Port:

User:

Password:

Confirm Password:

InstallAnywhere by Macrovision

Cancel Help Previous Next

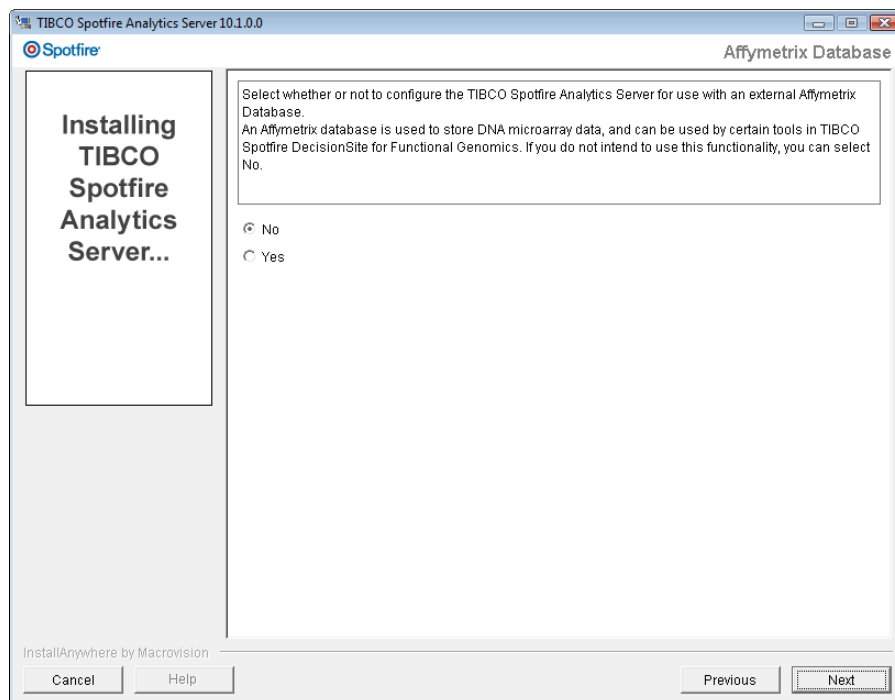
Enter configuration information for the Spotfire Library database. This database contains the Spotfire Library which is used by the end users to share their Spotfire files.

Specify the Server name and the Server port (default: **1433**) as well as username and password for the data tables.

Important: Do not use the same username for the three databases (Analytics Server database, Information Model database, Library database). You must specify a different username for each database.

Click **Next** to continue.

14



Select whether or not to configure the Spotfire Analytics Server for use with an external Affymetrix Database.

An Affymetrix database is used to store DNA microarray data, and can be used by certain tools in TIBCO Spotfire DecisionSite for Functional Genomics. If you do not intend to use this functionality, you can select No.

Click **Next** to continue.

- **If you selected NO, just skip the next step.**

15

Installing TIBCO Spotfire Analytics Server...

Enter configuration information for the external Affymetrix database that the TIBCO Spotfire Analytics Server should connect to.
An Affymetrix database is used to store DNA microarray data, and can be used by certain tools in TIBCO Spotfire DecisionSite for Functional Genomics.

Oracle Server:

Oracle Server Listen Port:

Oracle Service Name:

Oracle User:

Oracle Password:

Confirm Oracle Password:

If the database owner above is not the owner of the AADM tables, you must enter the correct table owner information below.

Table Owner:

InstallAnywhere by Macrovision

Cancel Help Previous Next

Enter configuration information for the external Affymetrix database that the Spotfire Analytics Server should connect to.

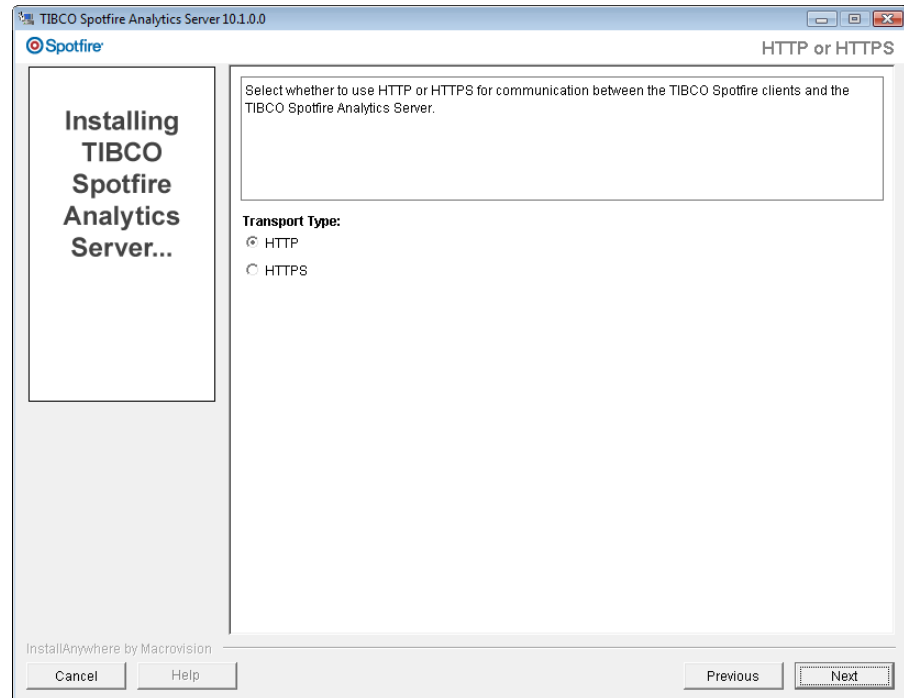
An Affymetrix database is used to store DNA microarray data, and can be used by certain tools in TIBCO Spotfire DecisionSite for Functional Genomics.

The **Oracle Server**, **Oracle Server Listen Port** and **Oracle Service Name** should point to the server which provides the AADM schema. The **Oracle User** and **Oracle Password** should be a user who has access to this database.

If the specified database user is not the owner of the AADM tables, it is also necessary to enter the correct **Table Owner** in the last field.

Click **Next** to continue.

16

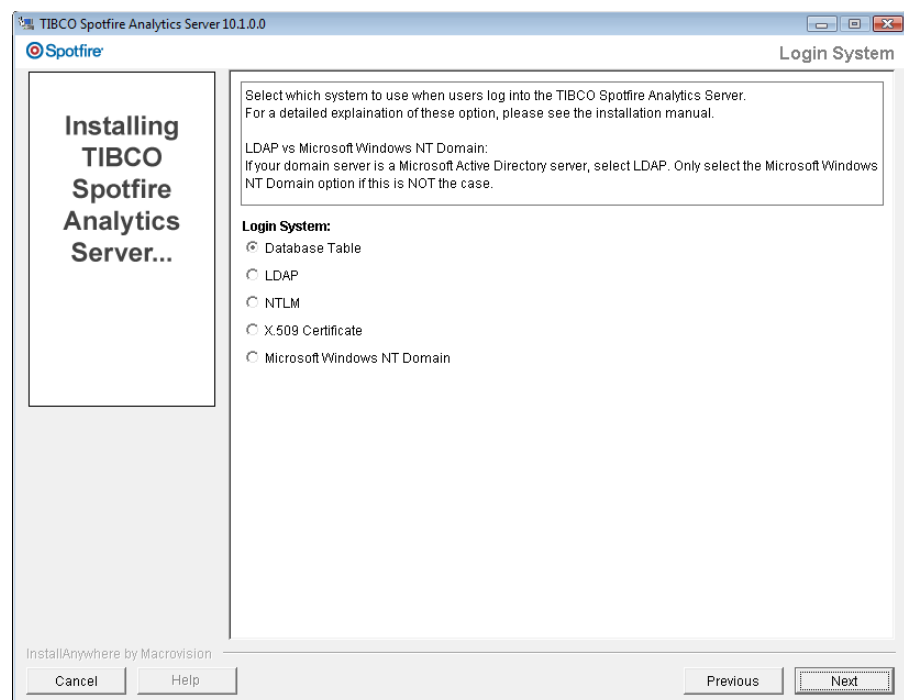


Select whether to use HTTP or HTTPS for communication between the Spotfire clients and the Spotfire Analytics Server.

Note: If you intend to use X.509 Certificates to authenticate users when logging in, you must select HTTPS.

Click **Next** to continue.

17



When you install the Spotfire Analytics Server you will need to specify how users will be authenticated when they log in, and which type of user directory will hold the list of all your users.

Login

DecisionSite Client and TIBCO Spotfire users who log into the Spotfire Analytics Server must be authenticated in order to be allowed access to the server.

When installing the Spotfire Analytics Server you can configure it to use one of the five combinations of Login System and Login method described below.

User Directory Back-end

A bit simplified, you could say that the user directory is where the list of all your users is kept. For example, some companies have thousands of users already listed in a Microsoft Active Directory which they want to use, whereas some companies might decide it is sufficient to use the Spotfire Analytics Server database and add their users to that.

What is the Difference?

For a large company the user directory often contains thousands of users. You might not want all of these to have access to the Spotfire Analytics Server. Therefore, you can set up a different login system that only allows a certain number of these to log in.

The possible combinations available from the installer are indicated in the chart below.

Login	User Directory Back-end		
	Database Table	LDAP (For example, Microsoft Active Directory)	Windows NT Domain
Database Table	X		
LDAP (For example, Microsoft Active Directory)	X	X	
NTLM	X	X	X
X.509 Certificates	X	X	X
MS Windows NT Domain	X		X

1. Database Table

When using this login system, usernames and passwords provided by the end users logging in are compared with credentials stored in the Spotfire Analytics Server's database. For security reasons, the passwords are never stored in cleartext. Instead, the Spotfire

Analytics Server computes encrypted one-way hashes of the passwords.

Database Table authentication is ideal for small groups of users, but the administration of larger groups can be cumbersome because each user has to be manually added to the Database Table directory using the DecisionSite Administrator tool or the TIBCO Spotfire Administration Manager tool.

2. LDAP (for example, Microsoft Active Directory)

When using this login system, usernames and passwords provided by the end users logging in are validated by an LDAP server. The Spotfire Analytics Server stores a list of usernames in its database, but no passwords.

The Spotfire Analytics Server directly supports Microsoft Active Directory and Sun Java System Directory Server and should work with most other servers as well, though this might require some manual configuration.

3. NTLM (Windows Integrated Authentication)

When the Spotfire Analytics Server is configured for Windows Integrated Authentication (NTLM), DecisionSite Client or TIBCO Spotfire will be logged in automatically if the user has logged in using his or her Windows domain account. Spotfire Analytics Server delegates the authentication itself to a Windows NT domain controller or an Active Directory server in compatibility mode. The Spotfire Analytics Server stores a list of usernames in its database, but no passwords.

4. X.509 Client Certificate

When the Spotfire Analytics Server is configured for X.509 Client Certificate authentication, the DecisionSite Client or TIBCO Spotfire will automatically try to log in by sending an X.509 client certificate to the Spotfire Analytics Server. If the server can validate the certificate, it accepts the identity indicated by the certificate. The Spotfire Analytics Server stores a list of usernames in its database, but no passwords or other security credentials.

5. Microsoft Windows Domain

When using this authentication type, the usernames and passwords provided by the end users when logging in are validated by a Windows NT domain controller. The Spotfire Analytics Server stores a list of usernames in its database, but no passwords.

Please note that if you are using Microsoft Active Directory servers for authentication on your network, then the LDAP authentication method (see below) should be selected instead of this method.

Select which system to use to authenticate users when they log into the Spotfire Analytics Server.

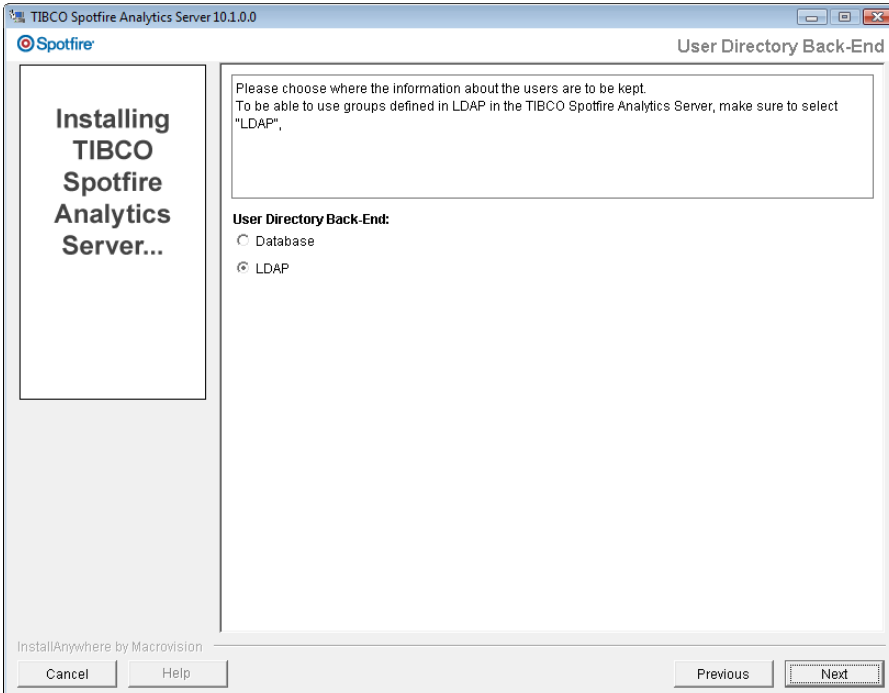
Click **Next** to continue.

- **Database Table** - proceed to “Completing the Installation” on page 86.
- **LDAP** - proceed to “LDAP Installation” on page 70.
- **NTLM** - proceed to “NTLM Installation” on page 76.
- **X.509 Certificate** - proceed to “X.509 Certificate Installation” on page 78.
- **Microsoft Windows NT Domain** - proceed to “Microsoft Windows NT Domain Installation” on page 83.

2.4 LDAP Installation

- 1 This section explains how to set up Spotfire Analytics Server to use LDAP for authentication and/or user directory back-end.

Some dialogs in the procedure below will only appear if you make certain selections along the way. If a certain step does not match the dialog you see before you on screen, just skip the step in the manual and proceed to the next matching step. Of course, be sure to enter information in all dialogs presented to you on screen.

- 2 

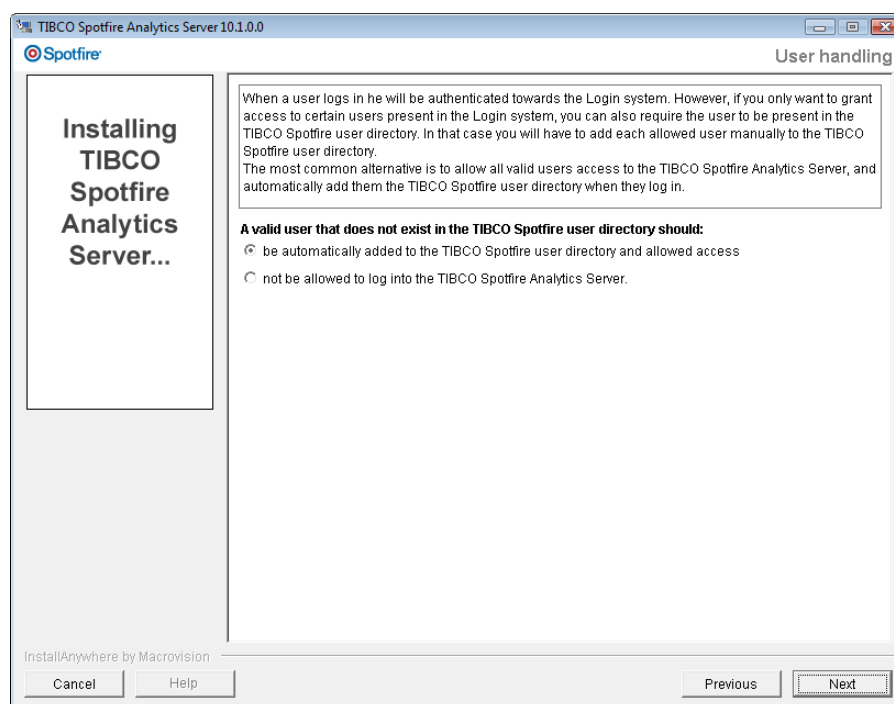
Select which User Directory Back-End you want. This directory is where the list of all Spotfire users is located. When you view the list of users from the Spotfire administration tools, the user directory back-end is what determines which users appear for you to manage.

If you select Database in this dialog, you will only use your LDAP server to authenticate which users are allowed to log into the Spotfire Analytics Server. The Spotfire Analytics Server Database will contain the list of all users (see next step for additional information).

If you select LDAP in this dialog, the specified LDAP server will be used to list all users. This means you can list all the users in your specified LDAP server from the Spotfire environment. Also, if you want to use groups defined on your LDAP server, be sure to select “LDAP” in this dialog to enable this. After the installation, perform the instructions in “Enabling External LDAP Group Synchronization” on page 200 to set up which groups you want to synchronize with the Spotfire Analytics Server.

Click **Next** to continue.

3



If you selected to use a database back-end for the user directory this dialog will be displayed.

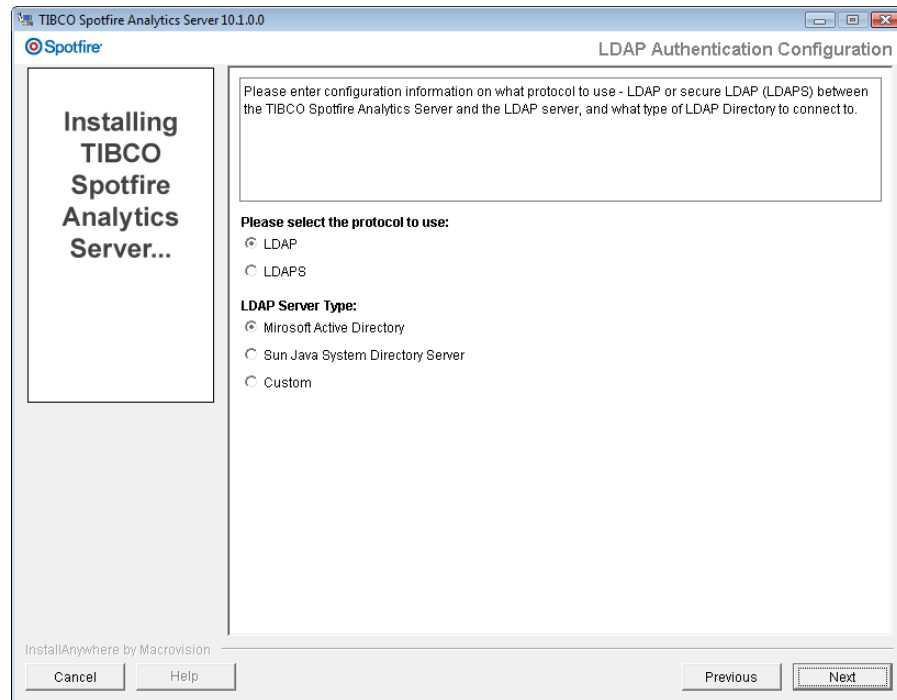
When a user logs in she will be authenticated towards the LDAP server. However, if you only want to grant certain users in the LDAP server access to the Spotfire Analytics Server, you can **also** require the user to be present in the Spotfire user directory. In that case you will have to add each allowed user manually to the Spotfire user directory.

Installation

The most common alternative is to allow all valid LDAP users access to the Spotfire Analytics Server, and automatically add them to the Spotfire user directory when they log in. Listing users from the Spotfire administration tools will only list the users who have logged in at some time, and thus have been added to the Spotfire user directory.

Click **Next** to continue.

4



Select if you want to use a standard LDAP protocol or a secure LDAP (LDAPS) protocol for communication between the Spotfire Analytics Server and the LDAP server.

Select which type of LDAP Server you intend to connect to.

Click **Next** to continue.

5

TIBCO Spotfire Analytics Server 10.1.0.0

LDAP Authentication Configuration

Installing TIBCO Spotfire Analytics Server...

Please enter configuration information on whether to use "Global Catalog" or not.

Use Global Catalog:

☐ Yes

☒ No

Cancel Help Previous Next

If you selected to use a **Microsoft Active Directory** as an LDAP Server, then you must select whether or not to use Global Catalog. For more information on Global Catalogs, please see your Microsoft Active Directory documentation.

Click **Next** to continue.

6

TIBCO Spotfire Analytics Server 10.1.0.0

LDAP Authentication Configuration

Installing TIBCO Spotfire Analytics Server...

Please enter configuration information for connecting to an LDAP server.

Server Name:

Port: 636

User Name:

Password:

Confirm Password:

Contexts:

Ex: CN=users,DC=dom,DC=example,DC=com|CN=users,DN=dom2,DN=com

Cancel Help Previous Next

Enter configuration information for connecting to your LDAP Server.

- Server Name - the name of the LDAP server.
- Port number - the port of the LDAP server.

Note: The default port number for the LDAP protocol is 389. The default port number for the LDAPS protocol is 636.

Note: If you are using multiple Active Directory servers in your network, and have selected to use “Global Catalog”, the default port number is 3268 for the LDAP protocol, or 3269 when using the LDAPS protocol. Using the “Global Catalog” you will be able to find all users in the company.

- User Name - this user needs to have privileges to read the users in all contexts using the name-attribute and user-search-filter.

Note: If your LDAP server allows anonymous binding, you can leave the User Name and Password fields blank.

- Password - the password of the above user.

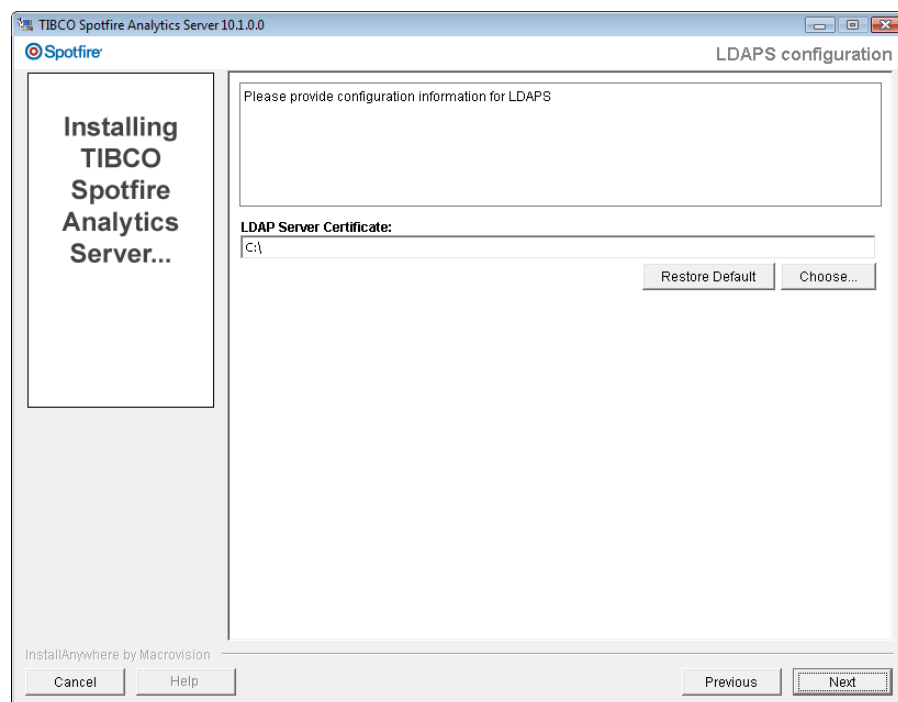
Context - the context path to the LDAP folder which holds the user information. You can enter several paths by separating them with a pipe sign “|”.

Example:

CN=users,DC=userdomain1,DC=company,DC=com|CN=users,DC=userdomain2,DC=company,DC=com

Click **Next** to continue.

7



If you selected **LDAPS** as the communication protocol earlier, you must now provide configuration information for LDAPS.

Note: The LDAP Server Certificate path may only contain these valid characters: [0-9][a-z][A-Z][!#\$%&'()*+,-./:;<=>@^_`~'].

Click **Next** to continue.

8

If you selected to use a **Custom LDAP Server** earlier, you must now provide configuration information for that.

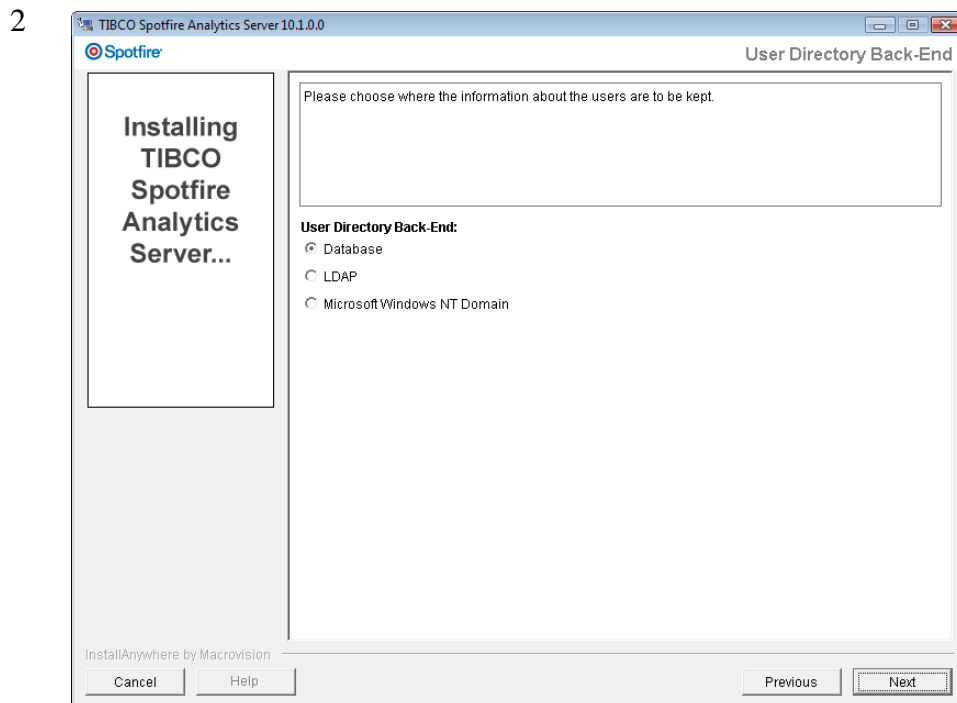
Click **Next** to continue.

- If you have selected **LDAP Login System**, proceed to “Completing the Installation” on page 86.
- If you have selected **NTLM Login System** and LDAP User Directory Back-end, return to “NTLM Installation” on page 76.
- If you have selected **X.509 Certificate Login System** and LDAP User Directory Back-end, return to “X.509 Certificate Installation” on page 78.

2.5 NTLM Installation

- 1 This section explains how to set up Spotfire Analytics Server to use NTLM for authentication.

Some dialogs in the procedure below will only appear if you make certain selections along the way. If a certain step does not match the dialog you see before you on screen, just skip the step in the manual and proceed to the next matching step. Of course, be sure to enter information in all dialogs presented to you on screen.



Select which User Directory Back-End you want. This directory is where the list of all Spotfire users is located. When you view the list of users from the Spotfire administration tools, the user directory back-end is what determines which users appear for you to manage.

If you select Database in this dialog, the Spotfire Analytics Server Database will contain the list of all users. This means you will have to add every user manually to the Spotfire Analytics Server in order to set Spotfire licenses and preferences for them.

If you select LDAP in this dialog, the specified LDAP server will be used to list all users. This means you can list all the users in your specified LDAP server from the Spotfire environment. Also, if you want to use groups defined on your LDAP server, be sure to select “LDAP” in this dialog to enable this. After the installation, perform the instructions in “Enabling External LDAP Group Synchronization” on page 200 to set up which groups you want to synchronize with the Spotfire Analytics Server.

If you select Microsoft Windows NT Domain you can list all the users in your specified NT Domains from the Spotfire environment.

Click **Next** to continue.

- If you select **LDAP**, proceed to “LDAP Installation” on page 70 and perform the instructions concerning LDAP there. Then return here.
- If you select Database or Microsoft Windows NT Domain, proceed below.

3

TIBCO Spotfire Analytics Server 10.1.0.0

Microsoft Windows NT Domain Authentication Configuration

Please enter configuration information for Microsoft Windows NT4 Domain Authentication.

Domains:

Example:
domain1, domain2, domain3

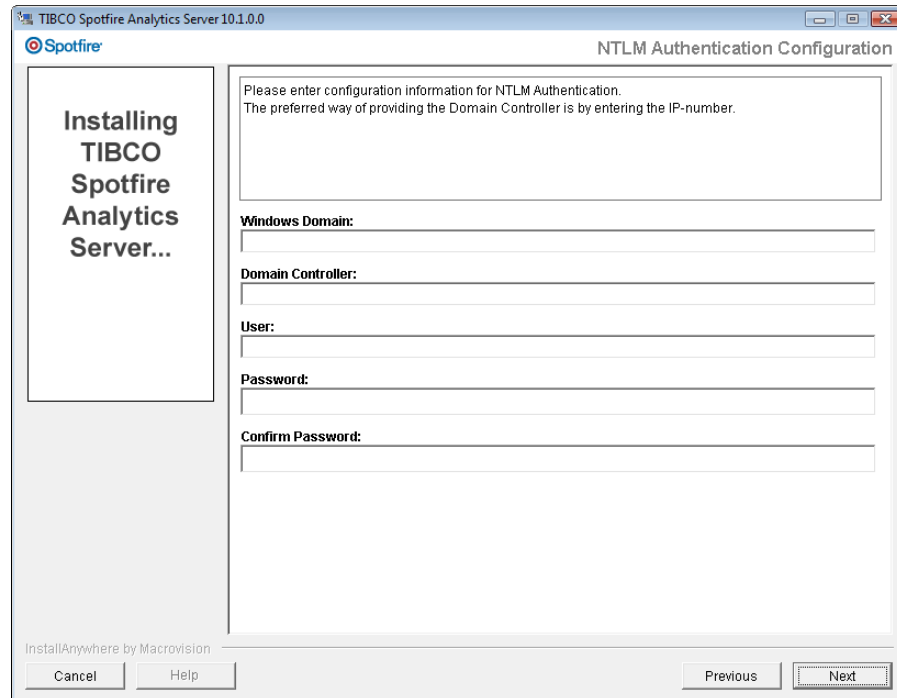
Cancel Help Previous Next

InstallAnywhere by Macrovision

If you selected **Microsoft Windows NT Domain** for user directory back-end, specify the domains you wish to include here.

Click **Next** to continue.

4



Enter configuration information for the NTLM login authentication. The preferred way of specifying the Domain Controller is by entering its IP-number.

Click **Next** to continue.

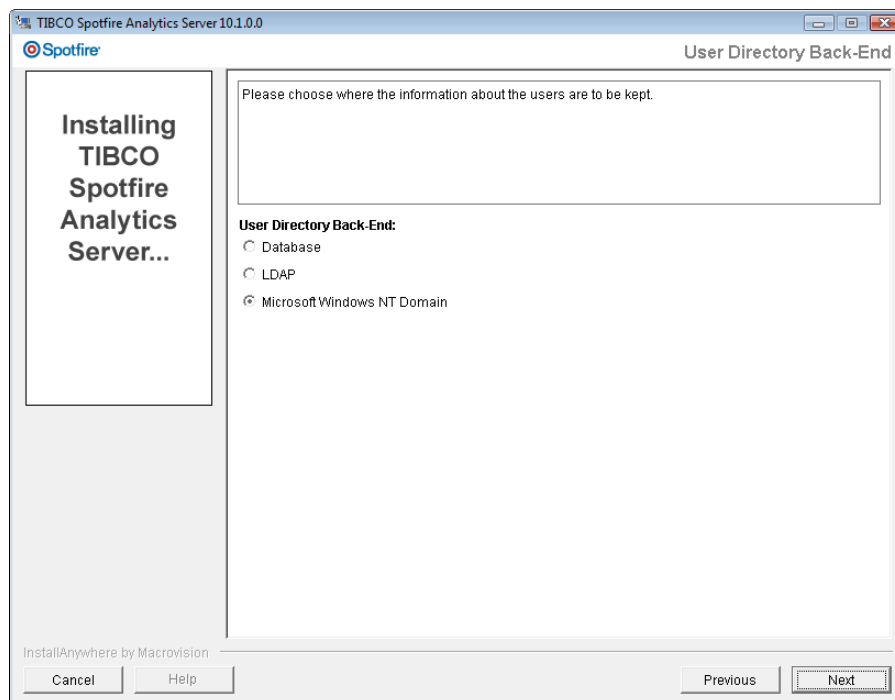
Proceed to “Completing the Installation” on page 86.

2.6 X.509 Certificate Installation

- 1 This section explains how to set up Spotfire Analytics Server to use X.509 Certificates for authentication.

Some dialogs in the procedure below will only appear if you make certain selections along the way. If a certain step does not match the dialog you see before you on screen, just skip the step in the manual and proceed to the next matching step. Of course, be sure to enter information in all dialogs presented to you on screen.

2



Select which User Directory Back-End you want. This directory is where the list of all Spotfire users is located. When you view the list of users from the Spotfire administration tools, the user directory back-end is what determines which users appear for you to manage.

If you select Database in this dialog, the Spotfire Analytics Server Database will contain the list of all users. This means you will have to add every user manually to the Spotfire Analytics Server in order to set Spotfire licenses and preferences for them.

If you select LDAP in this dialog, the specified LDAP server will be used to list all users. This means you can list all the users in your specified LDAP server from the Spotfire environment. Also, if you want to use groups defined on your LDAP server, be sure to select “LDAP” in this dialog to enable this. After the installation, perform the instructions in “Enabling External LDAP Group Synchronization” on page 200 to set up which groups you want to synchronize with the Spotfire Analytics Server.

If you select Microsoft Windows NT Domain you can list all the users in your specified NT Domains from the Spotfire environment.

Click **Next** to continue.

- If you select **LDAP**, proceed to “LDAP Installation” on page 70 and perform the instructions concerning LDAP there. Then return here.
- If you select Database or Microsoft Windows NT Domain, proceed below.

3

The screenshot shows the 'Microsoft Windows NT Domain Authentication Configuration' window. On the left, a vertical panel reads 'Installing TIBCO Spotfire Analytics Server...'. The main area contains the text 'Please enter configuration information for Microsoft Windows NT4 Domain Authentication.' Below this is a text box labeled 'Domains:' with an example 'domain1, domain2, domain3' shown underneath. At the bottom, there are 'Cancel', 'Help', 'Previous', and 'Next' buttons. The title bar indicates 'TIBCO Spotfire Analytics Server 10.1.0.0' and the Spotfire logo is in the top left.

If you selected **Microsoft Windows NT Domain** for user directory back-end, specify the domains you wish to include here.

Click **Next** to continue.

4

The screenshot shows the 'Certificate Support' window. On the left, a vertical panel reads 'Installing TIBCO Spotfire Analytics Server...'. The main area contains the text 'Please select whether your organization has a root certificate to use with the TIBCO Spotfire Analytics Server.' Below this is a section labeled 'Use root certificate:' with two radio buttons: 'Yes' (which is selected) and 'No'. At the bottom, there are 'Cancel', 'Help', 'Previous', and 'Next' buttons. The title bar indicates 'TIBCO Spotfire Analytics Server 10.1.0.0' and the Spotfire logo is in the top left.

Select whether or not your organization has a root certificate to use with the Spotfire Analytics Server.

Click **Next** to continue.

5

TIBCO Spotfire Analytics Server 10.1.0.0

Spotfire

Certificate Support

Please provide configuration information for the X.509 Root Certificate Support.

Keystore Password:

Root Certificate:
C:\

Restore Default Choose...

InstallAnywhere by Macrovision

Cancel Help Previous Next

If you selected to use a Root Certificate, enter configuration information for the X.509 Root Certificate Support here. Otherwise skip this step.

Click **Next** to continue.

6

TIBCO Spotfire Analytics Server 10.1.0.0

Spotfire

Certificate Support

Please provide configuration information for the X.509 Server Certificate Support.

Keystore Password:

Server Certificate:
C:\

Restore Default Choose...

InstallAnywhere by Macrovision

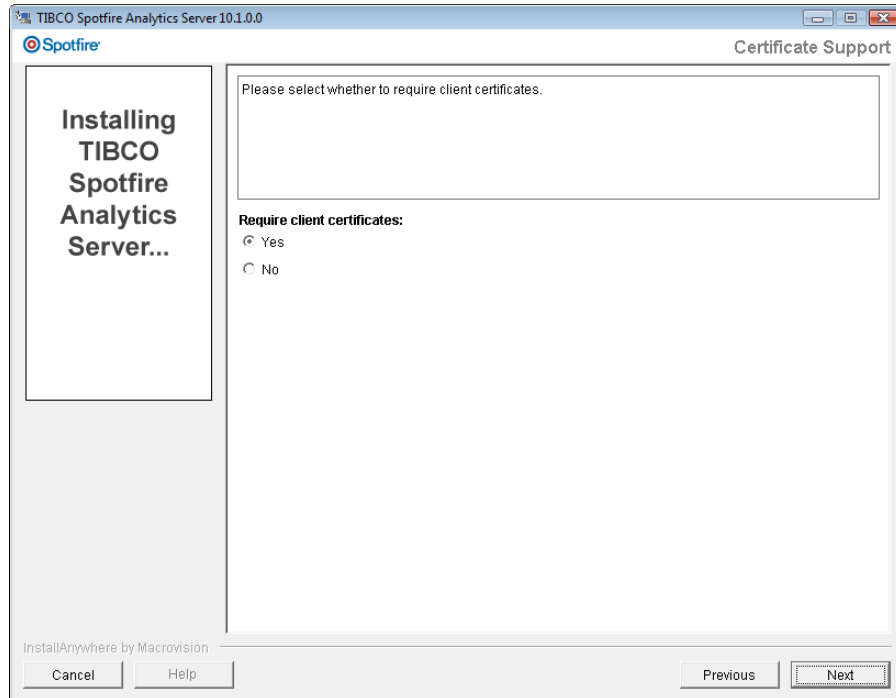
Cancel Help Previous Next

Installation

Enter configuration information for the X.509 Server Certificate Support.

Click **Next** to continue.

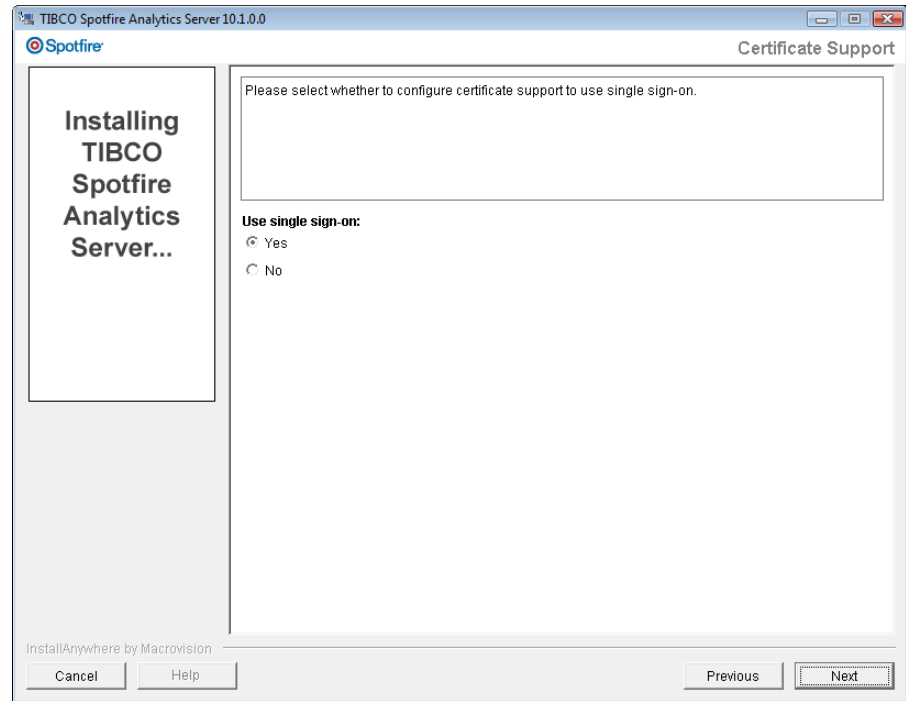
7



Select whether or not you wish to require client certificates for all users attempting to log into the Spotfire Analytics Server.

Click **Next** to continue.

8



Select whether or not to configure certificate support to use single sign-on.

Click **Next** to continue.

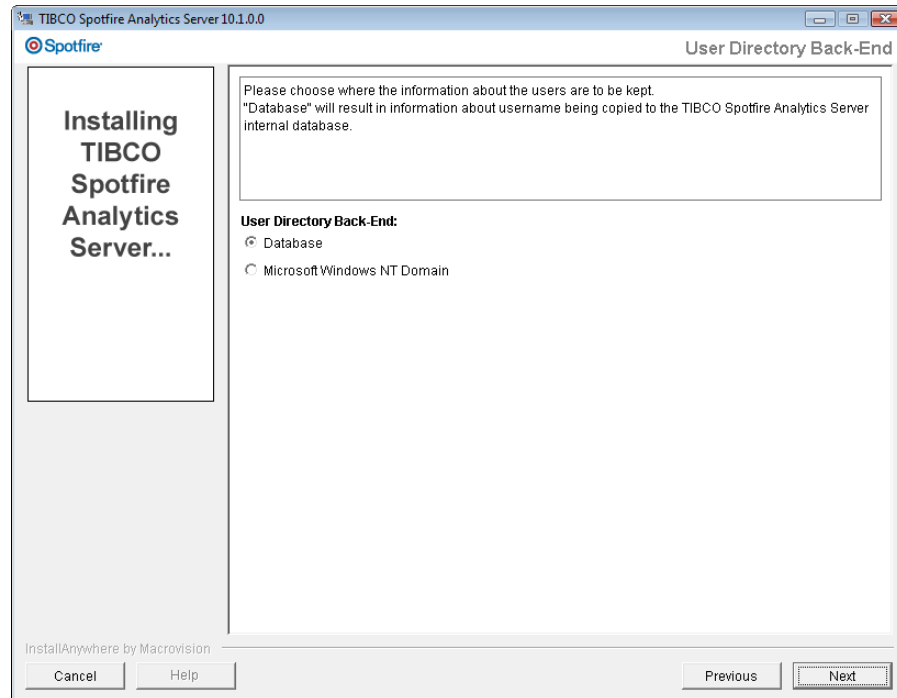
Proceed to “Completing the Installation” on page 86.

2.7 Microsoft Windows NT Domain Installation

- 1 This section explains how to set up the Spotfire Analytics Server to use Microsoft Windows NT Domains for authentication.

Some dialogs in the procedure below will only appear if you make certain selections along the way. If a certain step does not match the dialog you see before you on screen, just skip the step in the manual and proceed to the next matching step. Of course, be sure to enter information in all dialogs presented to you on screen.

2



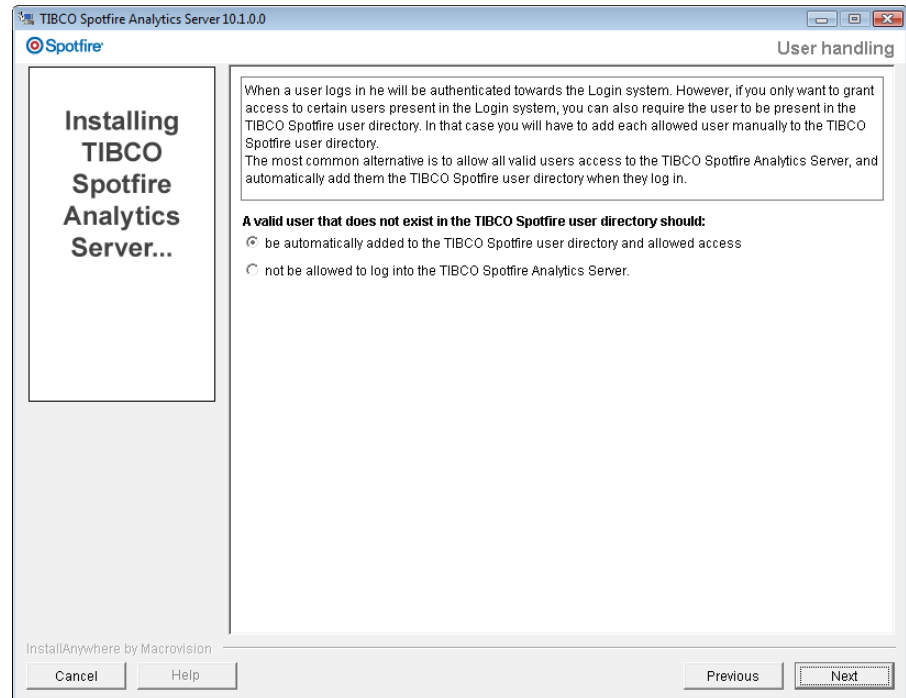
Select which User Directory Back-End you want. This directory is where the list of all Spotfire users is located. When you view the list of users from the Spotfire administration tools, the user directory back-end is what determines which users appear for you to manage.

If you select Database in this dialog, you will only use your Microsoft Windows NT Domain server to authenticate which users are allowed to log in to the Spotfire Analytics Server. The Spotfire Analytics Server Database will contain the list of all users (see next step for additional information).

If you select Microsoft Windows NT Domain you can list all the users in your specified NT Domains from the Spotfire environment.

Click **Next** to continue.

3

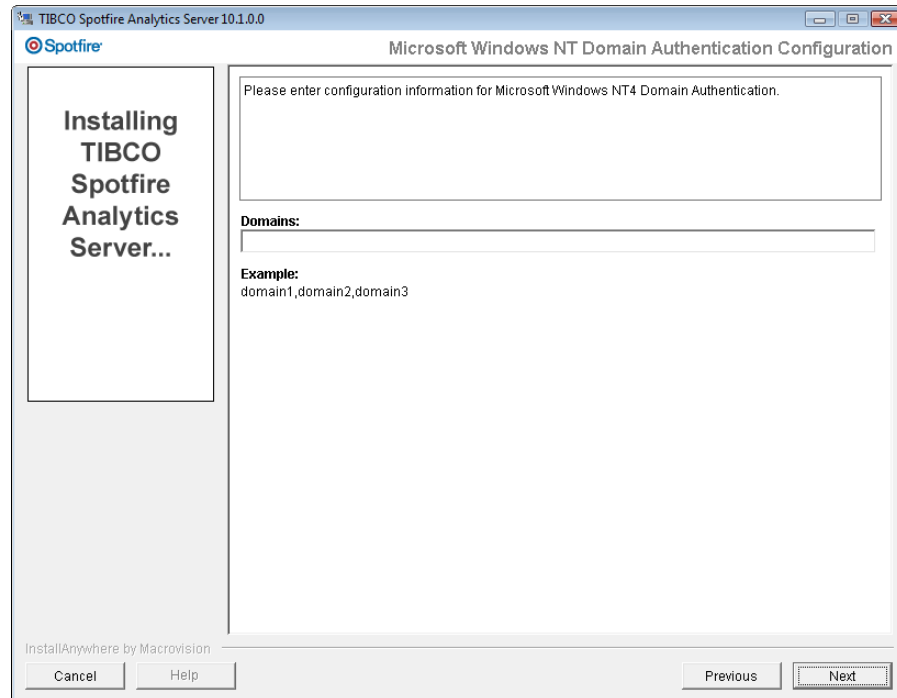


When a user logs in she will be authenticated towards the Microsoft Windows NT Domains. However, if you only want to grant certain users in the domains access to the Spotfire Analytics Server, you can **also** require the user to be present in the Spotfire user directory. In that case you will have to add each allowed user manually to the Spotfire user directory.

The most common alternative is to allow all valid users from the specified Microsoft Windows NT Domains access to the Spotfire Analytics Server, and automatically add them the Spotfire user directory when they log in. Listing users from the Spotfire administration tools will only list the users who have logged in at some time, and thus have been added to the Spotfire user directory.

Click **Next** to continue.

4



Specify the Microsoft Windows NT Domains that include the users you wish to allow to log into Spotfire Analytics Server.

Click **Next** to continue.

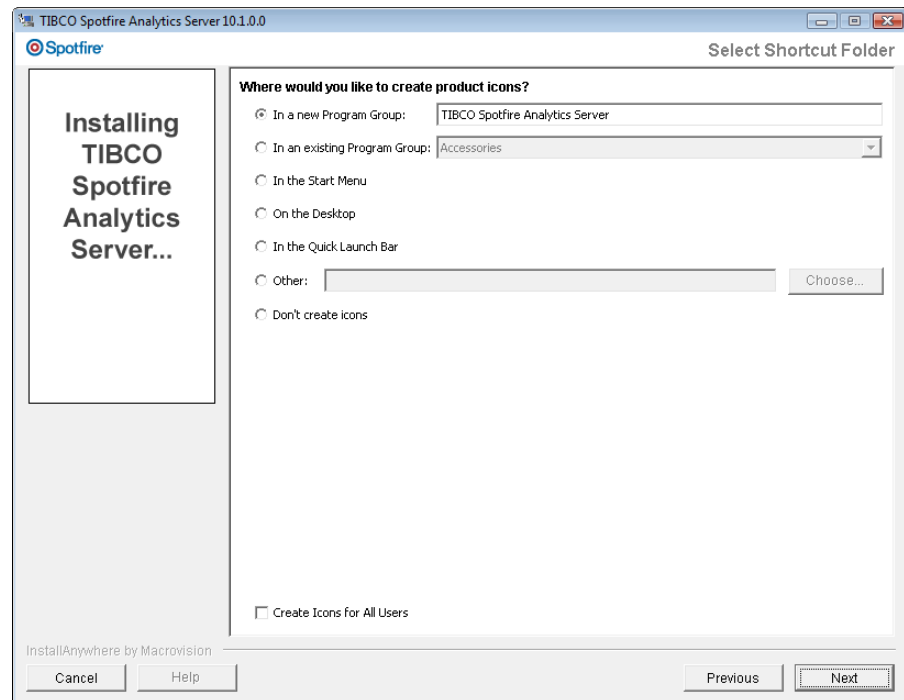
Proceed to “Completing the Installation” on page 86.

2.8 Completing the Installation

- 1 You have now configured everything the installer needs to know about databases, authentication and user directory back-ends.

You are soon ready to install.

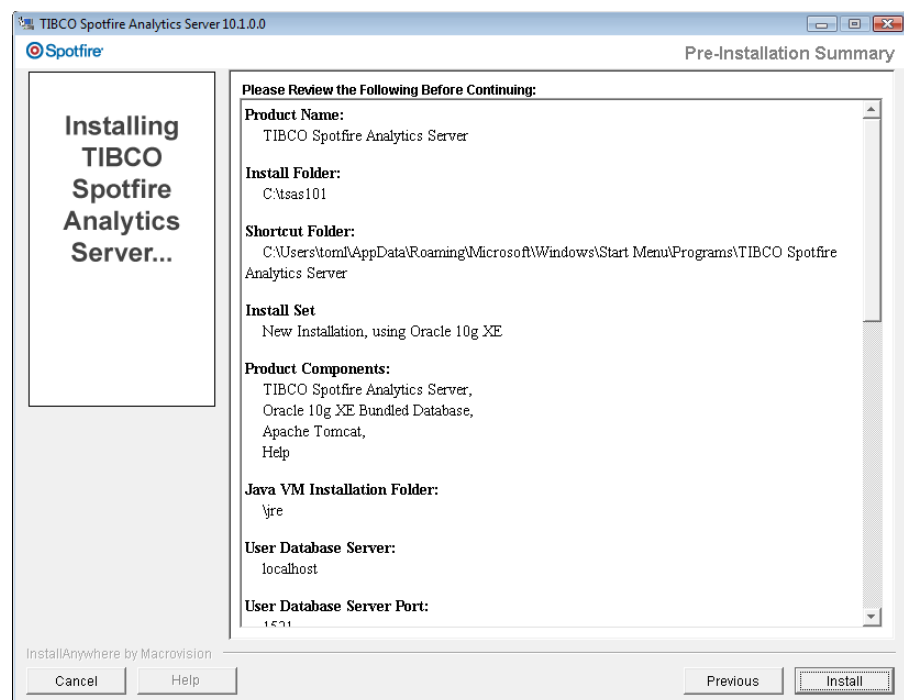
2



Select where you would like to place product icons for the Spotfire Analytics Server.

Click **Next** to continue.

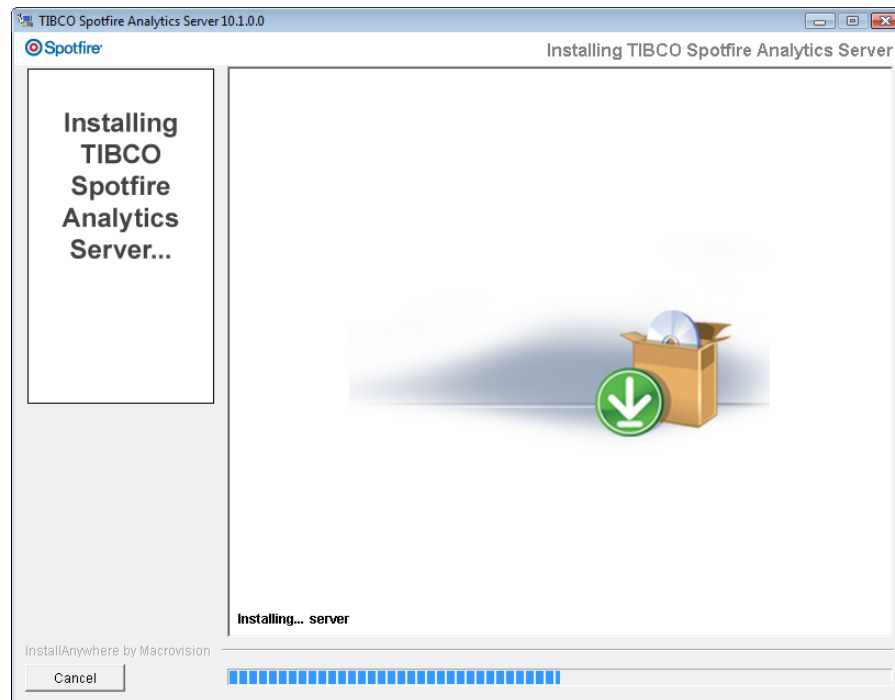
3



The pre-installation summary states the selections you have made.

Click **Install** to start the installation.

Response: The wizard begins to install all the components.



4 Done!

A web browser opens with the Spotfire Analytics Server Registration form. Please fill this in. It will aid customer support, should you have any questions later.

If you selected to run the server as a service and to start this service automatically, the Spotfire Analytics Server will now be running. The name of the service will be “Spotfire Analytics Server 10”.

2.9 Final Installation Procedures

If you selected to run the server as a service and to start this service automatically, the Spotfire Analytics Server will now be running. The name of the service will be “Spotfire Analytics Server 10”.

2.9.1 Windows NT Domain Authentication and No Windows Service for the Server

If for some reason, you are unable to run Spotfire Analytics Server as a Windows Service, and are using Windows NT Domain Authentication, there are some steps you need to take before you can start the Spotfire Analytics Server.

These steps are **only** for Spotfire Analytics Servers using Windows NT Domain Authentication but **not** running Spotfire Analytics Server as a Windows Service. In all other cases, skip this chapter.

- 1 Decide upon the user who should be the one to start the Tomcat server and the Spotfire Analytics Server. In the following steps this user will be referred to as the “**dsadmin**”.
 - 2 In the central Windows Domain controller, assign the **dsadmin** user “**Act as part of the operating system**” privileges. You may have to ask your IT Department to aid you with this.
 - 3 Log into Windows on the Spotfire Analytics Server machine as **Administrator**.
 - 4 Add the **dsadmin** user to the Windows group “**Administrators**”.
 - 5 Select **Control Panel > Administrative Tools > Local Security Policy**.
- Note:** the above path may vary on different kinds of Windows OS.
- 6 Select **Local Policies > User Rights Assignments**.
 - 7 Double-click on the line “**Act as part of the operating system**”.
 - 8 Add the **dsadmin** user to the list.
 - 9 Log out as **Administrator**.
 - 10 Log into Windows on the Spotfire Analytics Server machine as the **dsadmin** user.

2.9.2 Modifying the Virtual Memory

If many simultaneous users intend to perform heavy data pivoting via Information Services or in other ways severely stress the server, you may need to modify the amount of memory available to the virtual machine. See “Modifying the Virtual Memory” on page 229 for information on how to do this.

2.9.3 Starting the Spotfire Analytics Server

Verify that the Spotfire Analytics Server is not already running, before attempting to start it. Select **Start > Settings > Control Panel > [Administrative Tools] > Services** and find the “**Spotfire Analytics Server 10**” service. If its Status = Started then the Spotfire Analytics Server is already running.

► **To start Spotfire Analytics Server as a service:**

Select **Start > Settings > Control Panel > [Administrative Tools] > Services** and start the “**Spotfire Analytics Server 10**” service.

► **To start Spotfire Analytics Server in a console window:**

Start the Spotfire Analytics Server by double-clicking on the product icon (see 2 on page 87). If you chose to place it in the Start menu, instead select:

Start > Programs > Spotfire > Spotfire Analytics Server > Start Spotfire Analytics Server 10.0.

2.9.4 Deploying TIBCO Spotfire or TIBCO Spotfire DecisionSite

The Spotfire Analytics Server is now installed. The next step is to deploy TIBCO Spotfire and/or TIBCO Spotfire DecisionSite on the server in order for your end users to use their clients.

If you want to deploy TIBCO Spotfire, please continue performing the tasks described in the “TIBCO Spotfire - Deployment and Administration Manual”.

If you want to deploy TIBCO Spotfire DecisionSite, please continue performing the tasks described in the “TIBCO Spotfire DecisionSite - Deployment and Administration Manual”.

3 Upgrading

3.1 Introduction

The supported upgrade scenario is as follows:

From:

- Spotfire Analytics Server 10.0 or 10.0.1
- Apache Tomcat
- Existing Oracle or MS SQL Database

To:

- Spotfire Analytics Server 10.1.2
- Apache Tomcat
- Existing Oracle or MS SQL Database

Note: If you have installed a 10.0 server with a “bundled Oracle XE database”, this is considered an “existing Oracle database” when upgrading, and is supported in the following scenario.

3.1.1 Prerequisites

See <http://tibco.spotfire.com/sr> for details, and make sure all requirements are met before proceeding.

Hardware:

- CPU for Windows: Intel Pentium 4, 2 Ghz or higher
- CPU for Sun Solaris: UltraSparc IIIi, 1 Ghz or higher
- RAM: 1 GB minimum (recommended 2GB or greater)
- Hard disk space:
 - 1 GB of free space to complete installation
 - 500 MB for base server software to execute
 - Recommended 10 GB or greater when Spotfire Analytics Server 10.0 is configured with database on the same machine.

Software:

Spotfire Analytics Server 10.1.2 using Apache Tomcat can be installed on the following platforms:

- Microsoft Windows 2000 Server SP4 or higher
- Microsoft Windows Server 2003 SP1 or higher
- Microsoft Windows Server 2008
- Sun Solaris 8 with J2SE Solaris 8 Recommended Patch Cluster
- Sun Solaris 9 with J2SE Solaris 9 Recommended Patch Cluster
- Sun Solaris 10 with J2SE Solaris 10 Recommended Patch Cluster

In order to use an Oracle Enterprise/Standard database please note that this is third-party software that must be installed by the customer prior to the Spotfire software installation.

Supported Versions:

- Oracle 11g Release 1 (11.1.0.x)
- Oracle10g Release 2 (10.2.0.x)
- Oracle10g Release 1 (10.1.0.x)
- Oracle9i Release 2 (9.2.0.x)

Windows - Administrative Privileges:

If you are installing on a Microsoft Windows operating system, you must log in as a member of the administrators group to run the Spotfire Analytics Server installer. Specifically, the administrator should have the following:

- Full access to the file system of the target installation directory
- Full access to Windows system directory
- Permission to install and remove system services
- Full access to HKEY_LOCAL_MACHINE registry key

Solaris - Administrative Privileges:

You must install Spotfire Analytics Server 10.1.2 using the same account as for Spotfire Analytics Server 10.0. If Spotfire Analytics Server 10.0 was installed as root, then you must install 10.1.2 as root as well.

Windows - Folder Privileges for the Local System User:

By default, the Local System user will be used to run the server. You need to make sure that the corresponding user “System” has Full Control permission to the installation target folder and all its subfolders.

3.1.2 Checklist

Installing Spotfire Analytics Server requires you to specify various parameters in the installer. Therefore, it's a good idea to make sure you have all the information needed before starting the installer. Use the checklist below and write down the settings needed.

Important: You must make sure that the port numbers you intend to use for the Spotfire Analytics Server are free, and not already occupied by some other application on the machine.

Parameter:	Fill in value here:
Apache Tomcat Listen Port:	<i>Default: 80</i>
Apache Tomcat Administrator User:	
Apache Tomcat Administrator Password:	

3.2 Stop and Disable the 10.0 Service

Before you begin the upgrade procedure, make sure the Spotfire Analytics Server 10.0 is stopped.

Windows

If you are running the Spotfire Analytics Server 10.0 on Windows, stop the service and set it to “Manual” start. This means that the 10.0 service will not be started automatically when the server is restarted. This is to prevent both the old 10.0 service and the new 10.1.2 service to start and possibly interfere with each other, if they happen to be set up to use the same port numbers.

Solaris

If you are running Spotfire Analytics Server 10.0 on Solaris, make sure the Spotfire Analytics Server 10.0 is stopped. Also, if you have selected to start Spotfire Analytics Server 10.0 automatically after reboot, you need to remove this setting by deleting three files.

- 1 Log in as **root**.
- 2 Close all open files in the Spotfire Analytics Server 10.0 directory.
- 3 Delete the following three files:

- /etc/rc2.d/S98spotfireas
- /etc/rc0.d/K05spotfireas
- /etc/init.d/spotfireas

The autostartup setting is removed.

3.3 Select the Appropriate Installer

You are now ready to run the Spotfire Analytics Server installer in order to upgrade your server.

Depending on the operating system the Spotfire Analytics Server 10.0 is running on, pick the appropriate version of the installation kit:

- Windows: select the **TIB_ASWin_10.1.2_ORXE** or **TIB_ASWin_10.1.2_NoDB** installer, either one will work.
- Solaris: select the **TIB_ASSol_10.1.2_Sol** installer.

3.4 Run the Installer

► Run the Installer:

- 1 Make sure the Spotfire Analytics Server 10.0 is stopped.
- 2 Copy the entire Spotfire Analytics Server 10.1.2 installation kit to the Spotfire Analytics Server machine.

Important note when upgrading on Solaris: You must install Spotfire Analytics Server 10.1.2 using the same account as for Spotfire Analytics Server 10.0. If Spotfire Analytics Server 10.0 was installed as root, then you must install 10.1.2 as root as well.

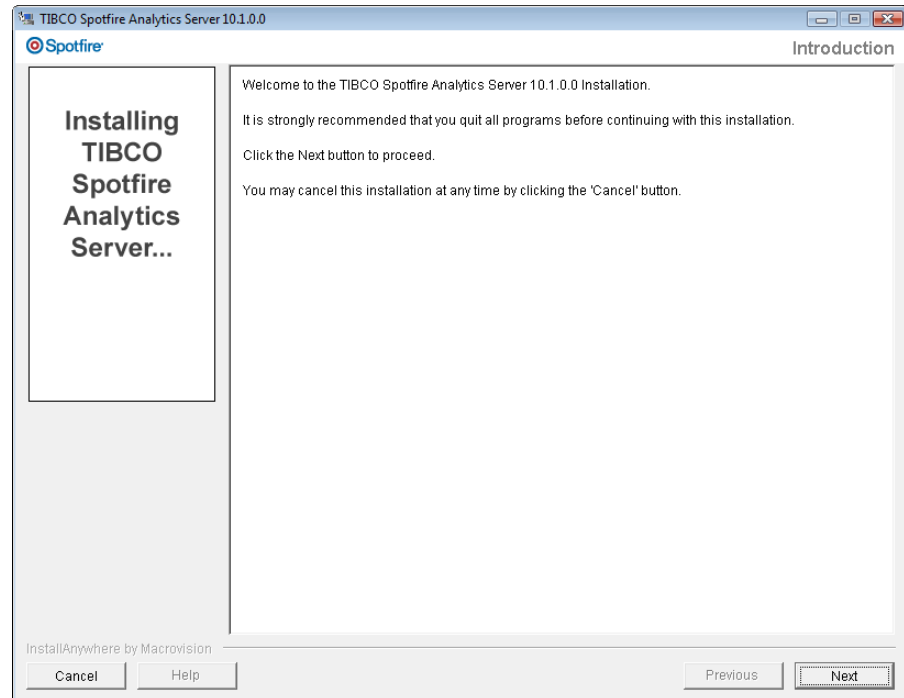
Note: On UNIX systems, only processes that run under a privileged user account (in most cases, root) can bind to ports lower than 1024. However, it is recommended that long-running processes like Tomcat should not run under these privileged accounts.

- 3 If you are running Solaris, you may need to set execute permissions for the installer.

chmod u+x install.bin

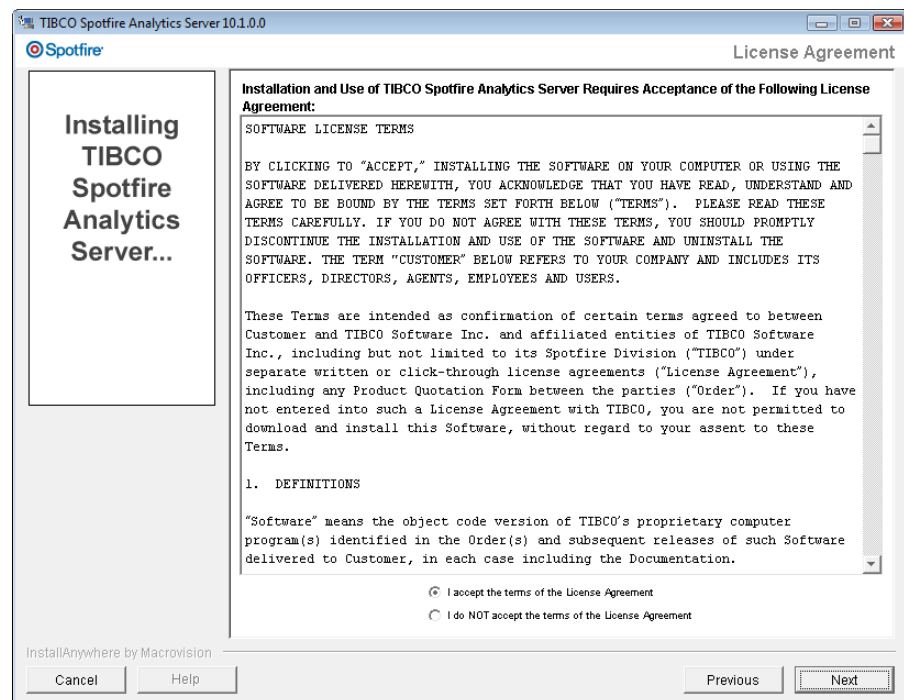
- 4 Start the Spotfire Analytics Server installer by running the file **install.exe** (or **install.bin** for Solaris) provided on the installation media.

5



The installer starts. Click **Next** to continue.

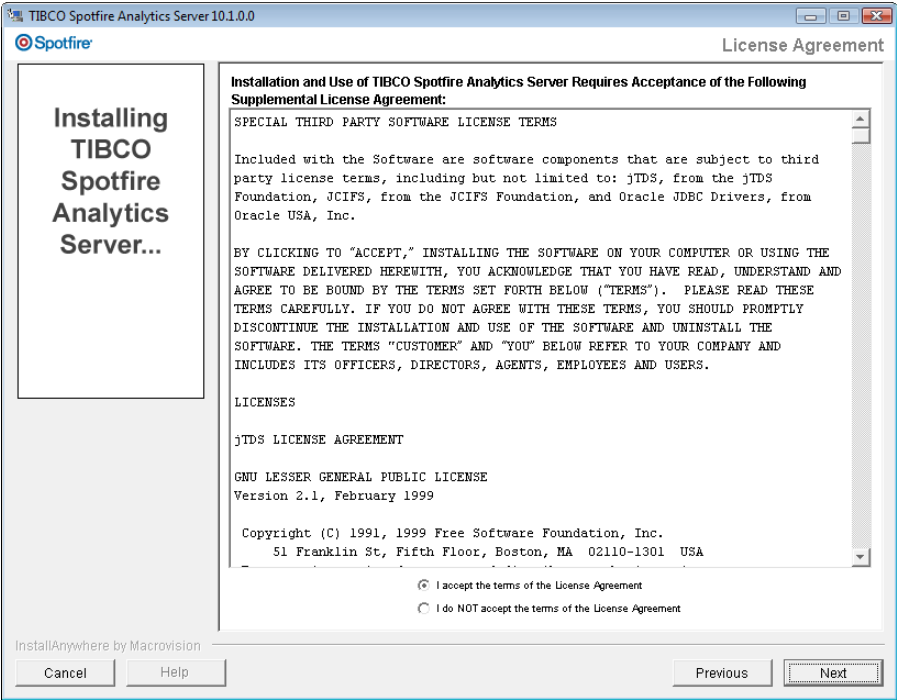
6



Read the license agreement, and select the appropriate radio button.

Click **Next** to continue.

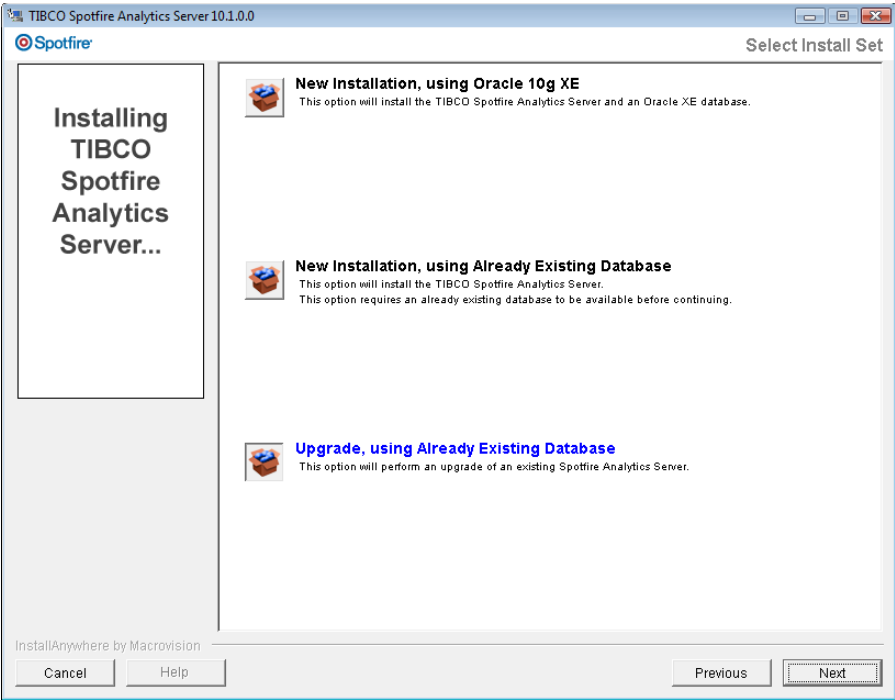
7



Read the supplemental license agreement, and select the appropriate radio button.

Click **Next** to continue.

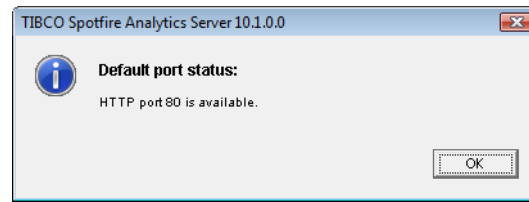
8



Select the type of installation you want to perform, in this case an **Upgrade, using Already Existing Database**.

Click **Next** to continue.

9



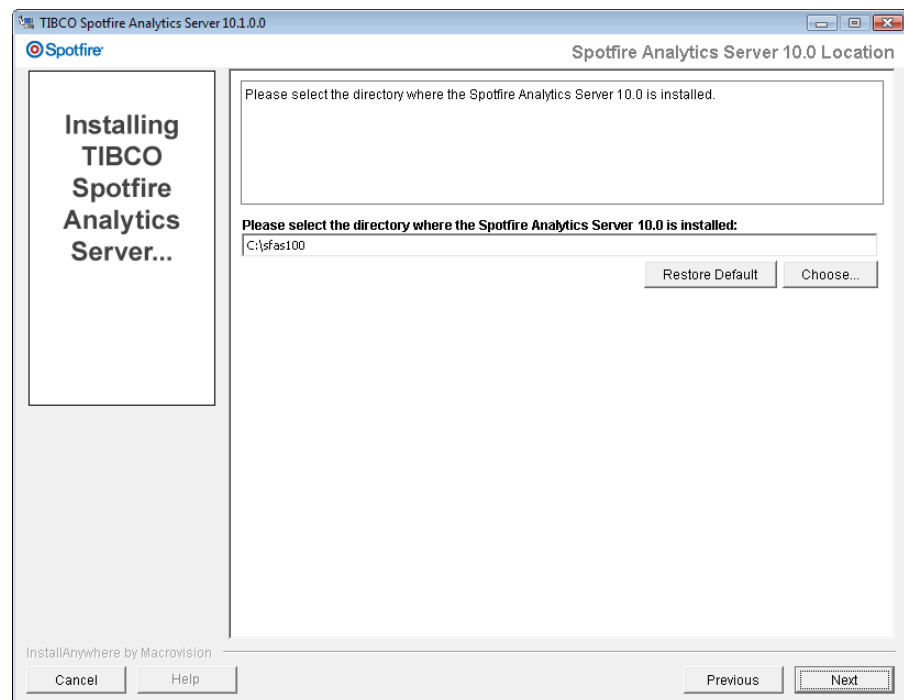
Since the Spotfire Analytics Server installer will install a Tomcat web server, an automatic check is performed to verify if the default ports for this are available.

If all ports are listed as “available” you can choose to install everything on the suggested default ports. However, should any port be listed as “occupied” there is already some software on this machine using that port. This means you must specify a different port number for the corresponding port when prompted later in the installation.

Make a note of any occupied ports and port numbers, so you can avoid accidentally specifying identical port numbers later.

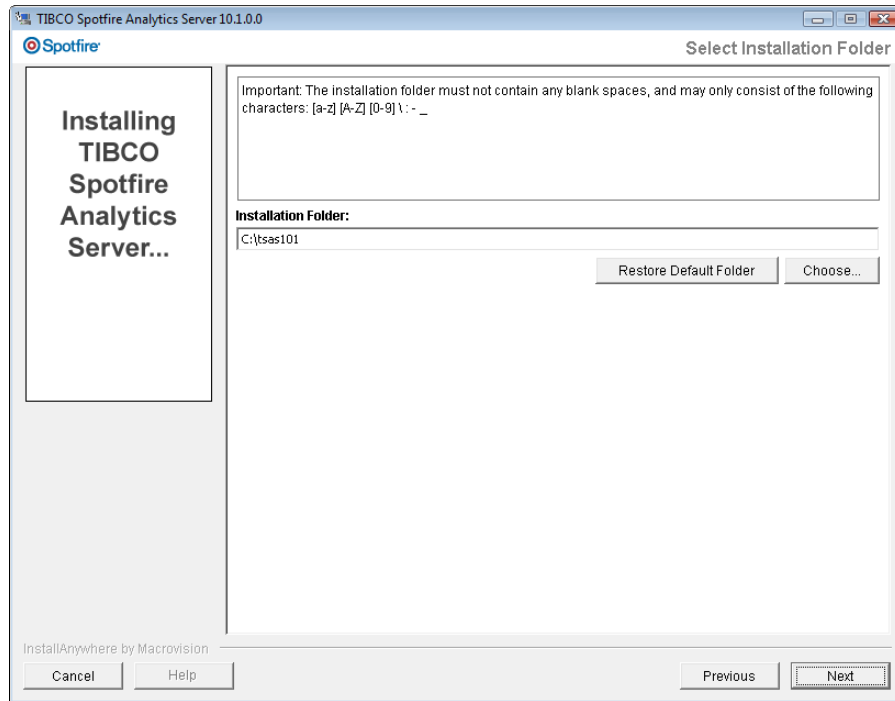
Click **OK** to continue.

10



Select or specify the installation directory of the old Spotfire Analytics Server 10.0 (For example: C:\Spotfire\SpotfireAS100)

Click **Next** to continue.



Select or specify where you would like to install the new Spotfire Analytics Server 10.1.2.

Note that you cannot use certain characters such as blank spaces in the path name.

Important: You **must** specify a different directory for the Spotfire Analytics Server 10.1.2 than the Spotfire Analytics Server 10.0. The 10.1.2 server cannot be installed in the same directory as the old 10.0 server.

Click **Next** to continue.

12

Enter the configuration information you want for the Apache Tomcat application server.

IMPORTANT!

Make a note of the Administrator username and password you specify, since you will need it to access the Apache Tomcat administration console later.

There is no way to retrieve this password if you forget, so make sure you remember it and write it down.

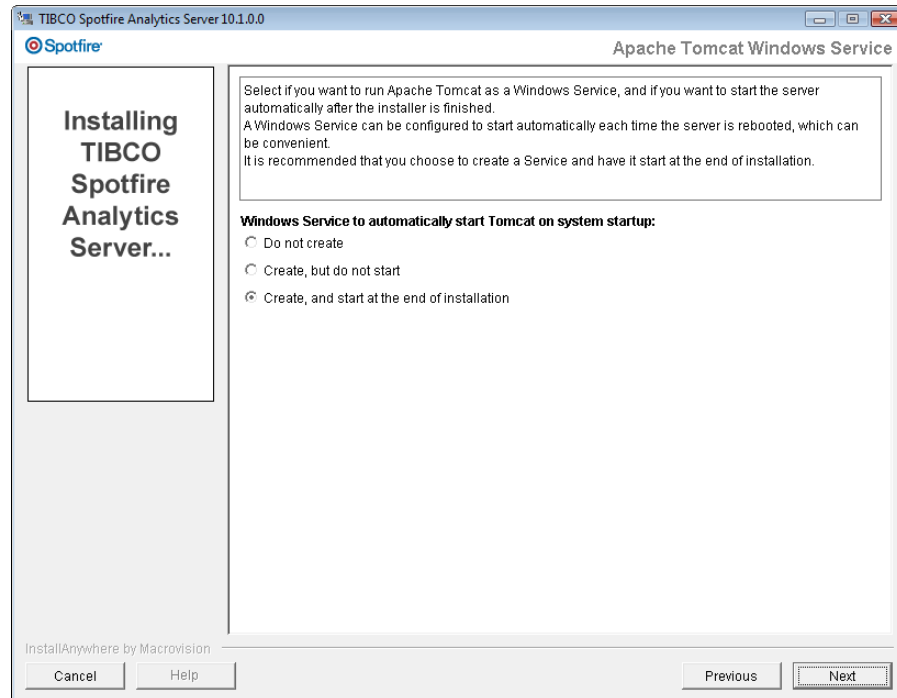
Note: On UNIX systems, only processes that run under a privileged user account (in most cases, root) can bind to ports lower than 1024. However, it is recommended that long-running processes like Tomcat should not run under these privileged accounts.

It is therefore advised that you **do not** install Spotfire Analytics Server as **root**. Instead, create a Solaris user who will be the owner of the Spotfire Analytics Server application. (Note that this means you cannot use port 80 for the Spotfire Analytics Server).

However, when upgrading you **must** use the same user as you did when installing Spotfire Analytics Server 10.0.

Click **Next** to continue.

13



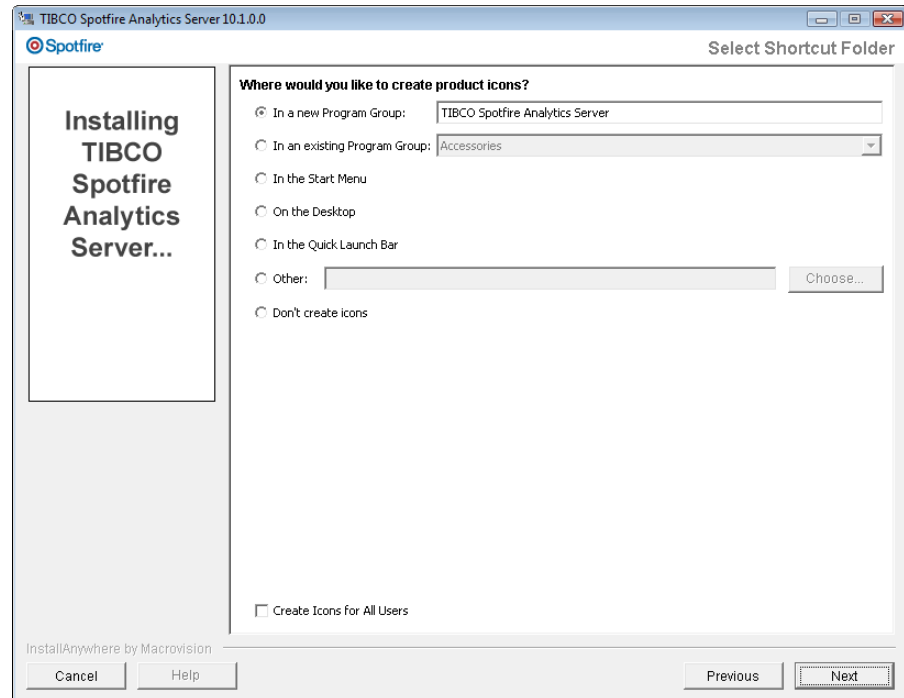
This step is for Windows only.

Select whether or not you want to create a Windows Service that will start the Apache Tomcat server each time the system restarts.

The recommended option is to **Create, and start at the end of installation.**

Click **Next** to continue.

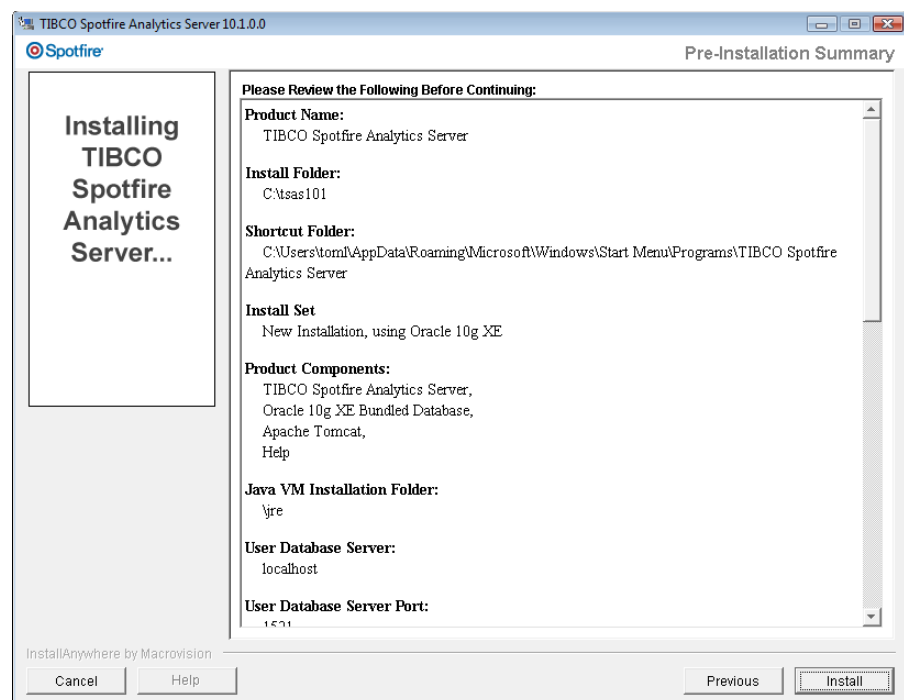
14



Select where you would like to place product icons for the Spotfire Analytics Server 10.1.2 (or place links for Solaris).

Click **Next** to continue.

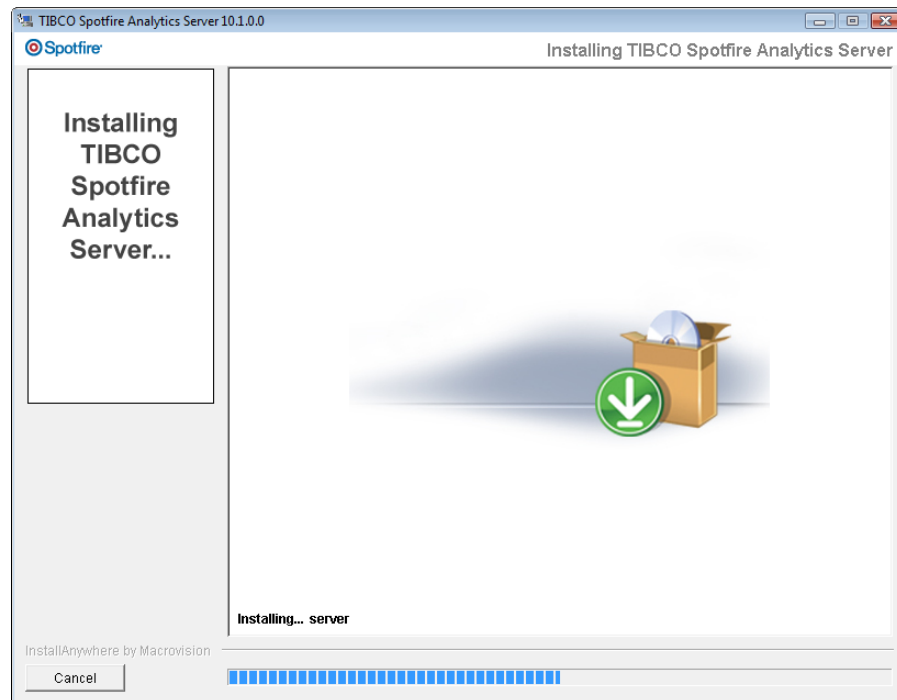
15



The pre-installation summary states the selections you have made.

Click **Install** to start the installation.

Response: The wizard begins to install all the components.



16 Done!

A web browser opens with the Spotfire Analytics Server Registration form. Please fill this in. It will aid customer support, should you have any questions later.

If you selected to run the server as a service and to start this service automatically, the Spotfire Analytics Server will now be running. The name of the service will be “TIBCO Spotfire Analytics Server 10.1.2”.

3.5 Completing the Upgrade

3.5.1 Moving Custom JDBC Data Source Configurations

If you have set up custom JDBC Data Source Configurations on your Spotfire Analytics Server 10.0, you must manually transfer these to the Spotfire Analytics Server 10.1.2.

- 1 Stop the Spotfire Analytics Server 10.1.2, if it is running.

- 2 Locate the file **settings.xml** in the <installation directory>/spotfire/spotfire/WEB-INF directory on the **Spotfire Analytics Server 10.0**.
- 3 Open the file in a text editor.
- 4 Copy your XML Configuration JDBC Data Source from this file.
- 5 Locate the file **settings.xml** in the <installation directory>/server/webapps/spotfire/WEB-INF directory on the **Spotfire Analytics Server 10.1.2**.
- 6 Open the file in a text editor.
- 7 Paste the copied XML Configuration to the corresponding place in this file.
- 8 Save the file.
- 9 Copy the custom driver file(s) from the <installation directory>/spotfire/spotfire/WEB-INF/lib directory of the Spotfire Analytics Server 10.0, to <installation directory>/server/webapps/spotfire/WEB-INF/lib on the Spotfire Analytics Server 10.1.2.

The following .jar files are installed by default on the Spotfire Analytics Server 10.0.

Do NOT copy (and overwrite) these to the 10.1.2 server. Any OTHER files may be custom drivers. If they are drivers they should be copied.

```
activation.jar
antlr.jar
axis.jar
commons-discovery.jar
commons-logging.jar
diagnostics.jar
dsfg.jar
dss-jaas.jar
dss.jar
iis.jar
jakarta-regexp-1-2.jar
jaxen-core.jar
jaxen-jdom.jar
jaxrpc.jar
jcifs-ext.jar
jcifs.jar
jdom.jar
jtds.jar
ldapbp.jar
library.jar
log4j.jar
logging.jar
mail.jar
ojdbc14.jar
posters.jar
saa.jar
saxpath.jar
uc.jar
```

```
wSDL4j.jar
wsp.jar
xalan.jar
xercesImpl.jar
```

For more information, please see “Configuring IS to Access a New Type of JDBC Data Source” on page 207.

3.5.2 Reconfiguring Settings

NTLM

If you have upgraded a Spotfire Analytics Server 10.0 using NTLM login, you need to make certain modifications to the following files:

- catalina.bat (or catalina.sh for a UNIX system)
- service.bat (not used on a UNIX system)

► Copying Settings from 10.0 to 10.1.2:

- 1 On the Spotfire Analytics Server 10.0, open the following file in a text editor:

```
<10.0 installation directory>/server/bin/catalina.bat
```

- 2 Find the row:

```
rem Set Java runtime options
```

- 3 The row below this starts with “**set CATALINA_OPTS=**”. Copy this row and paste it into the corresponding place in the corresponding file on the 10.1.2 server:

```
<10.1.2 installation directory>/server/bin/catalina.bat
```

Only for Windows:

- 4 On the Spotfire Analytics Server 10.0, open the following file in a text editor:

```
<10.0 installation directory>/server/bin/service.bat
```

- 5 Find the row, near the end of the file, that starts with:

```
"%EXECUTABLE%" //US//%SERVICE_NAME%...
```

- 6 Copy this row and paste it into the corresponding place (thus replacing the existing line) in the corresponding file on the 10.1.2 server:

```
<10.1.2 installation directory>/server/bin/service.bat
```


Important: Before you replace the row, check the values for `--JvmMs 512 --JvmMx 512` in the original 10.1.2 version of the file, and make sure that these are kept after you copy the row from the 10.0 version.

Certificates

It is also necessary to reconfigure certificate settings if certificates are used.

For example, if you have set up the Spotfire Analytics Server 10.0 to use LDAPS, you need to perform the appropriate steps in section “Configuring the Server for LDAPS” on page 230.

Logging

If the default logging level has been altered in web.xml this should be rechecked.

3.5.3 Setting up Computation Services and/or Chemistry Services

If you are upgrading from a Spotfire Analytics Server 10.0 that already has Computation Services and/or Chemistry Services set up, all you have to do is copy the contents of the following directory from the 10.0 server:

```
<10.0 installation directory>\server\application-data
```

and paste at the corresponding place on the 10.1.2 server:

```
<10.1.2 installation directory>\server\application-data
```

If you are upgrading from a Spotfire Analytics Server that does not have Computation Services or Chemistry Services set up, and you wish to configure this for the new upgraded server, you will find instructions for this in the manual “TIBCO Spotfire DecisionSite - Deployment Manual”.

3.5.4 Starting the Spotfire Analytics Server

3.5.4.1 Windows

Verify that the Spotfire Analytics Server is not already running, before attempting to start it. Select **Start > Settings > Control Panel > [Administrative Tools] > Services** and find the “**Spotfire Analytics Server 10.1.2**” service. If its Status = Started then the Spotfire Analytics Server is already running.

► **To start Spotfire Analytics Server as a service:**

Select **Start > Settings > Control Panel > [Administrative Tools] > Services** and start the “**Spotfire Analytics Server 10.1.2**” service.

► **To start Spotfire Analytics Server from a console window:**

Go to <server install dir>/server/bin and type

> **catalina.bat start**

3.5.4.2 Solaris

► **To start Spotfire Analytics Server on reboot:**

After the installation, you may want to configure Spotfire Analytics Server to start automatically each time the Solaris machine is rebooted. This can be set up by running a script called `install_startup_script.sh`.

- 1 Log in as **root**.

Comment: In order to have a service automatically start at reboot you must be **root**. No other user can do this.

- 2 Navigate to the <**installation directory**>/server/bin.

- 3 Execute the file **install_startup_script.sh**.

Response: The Spotfire Analytics Server will now start automatically after each machine reboot.

To start the server right now, just run the script
/etc/init.d/spotfireas start

► **To start Spotfire Analytics Server in a console window:**

If you wish to run Spotfire Analytics Server in a console window, then execute the command **catalina.sh run** located in the directory <**installation directory**>/server/bin with the same user as the one who installed the Spotfire Analytics Server.

3.5.5 Deploying TIBCO Spotfire or TIBCO Spotfire DecisionSite

The Spotfire Analytics Server is now upgraded. The next step is to deploy TIBCO Spotfire and/or TIBCO Spotfire DecisionSite on the server in order for your end users to use their clients.

If you want to deploy TIBCO Spotfire, please continue performing the tasks described in the “TIBCO Spotfire - Deployment and Administration Manual”.

If you want to deploy TIBCO Spotfire DecisionSite, please continue performing the tasks described in the “TIBCO Spotfire DecisionSite - Deployment and Administration Manual”.

3.5.6 Removing the Old Spotfire Analytics Server 10.0

It is recommended that you wait, and do not remove the old Spotfire Analytics Server before you have deployed all packages on the new 10.1.2 server and verified that it runs properly.

► Uninstall Spotfire Analytics Server 10.0:

- 1 Close all open files in the Spotfire Analytics Server 10.0 directory.
- 2 Open a command prompt.
- 3 Navigate to the
<**Spotfire Analytics Server 10.0 installation directory**>_uninst directory.
- 4 Run the file **uninstaller.exe** (or **uninstaller.bin** for Solaris).

Response: The system is cleared of all 10.0 configuration parameters and standard files.

- 5 Some files may still be present in the old Spotfire Analytics Server 10.0 installation directory. When you have confirmed that your Spotfire Analytics Server 10.1.2 is running properly, and that all users can access what they should, you can delete the old 10.0 installation directory.

Note: Regardless of whether your Spotfire Analytics Server 10.0 was installed using an existing Oracle database, an existing Microsoft SQL Server database, or with a bundled Oracle XE database—uninstalling the 10.0 server after an upgrade will not remove the database. The database will continue to be used for the 10.1.2 server.

4 Removal Procedures

These instructions are valid for installations of Spotfire Analytics Server 10.1.2 using either a bundled Oracle 10g XE database, or an external database.

If you have installed the bundled Oracle 10g XE database, this will be completely removed along with all database tables.

If you have installed on an already existing database, this will be left untouched. You will have to manually remove the Spotfire Analytics Server database tables after the uninstallation. These database tables are described in “Existing Oracle Database” on page 31 or “Existing Microsoft SQL Server Database” on page 51.

4.1 Windows

► **To Remove Spotfire Analytics Server 10.1.2:**

- 1 Select **Start > Settings > Control Panel**.
- 2 Select **Add or Remove Programs**.
- 3 Select **Spotfire Analytics Server** and click **Change/Remove**.

Response: The Uninstall wizard starts.

- 4 Click **Next**.
- 5 Select **Complete Uninstall** and click **Next**.

Response: The Spotfire Analytics Server is uninstalled.

- 6 When the uninstall wizard is finished, click **Done**.

4.2 Solaris

► **To remove Spotfire Analytics Server from a Solaris Server:**

- 1 Stop the Spotfire Analytics Server 10.1.2.
- 2 Close all open files in the Spotfire Analytics Server 10.1.2 directory.
- 3 Log in as the same user who installed Spotfire Analytics Server.
- 4 Navigate to the **<installation directory>/Uninstall_Spotfire Analytics Server/** directory.

5 Execute the file **Uninstall_Spotfire_Analytics_Server**.

The Spotfire Analytics Server files are deleted. The databases used for the Spotfire Analytics Server are not dropped, but all connections to them are removed.

Note: If you have performed the instructions in Section 3.5.4.2 on page 106, to have the Spotfire Analytics Server start automatically on server reboot, you should remove the service doing this.

5 Configuration Reference

5.1 Important Configuration Files

This chapter provides a technical description of the most important configuration files on the Spotfire Analytics Server. These can be modified to change the configuration of the server. However, be very careful and exact if you attempt this.

For descriptions of some of the common configuration procedures, see “Configuration Procedures” on page 156.

Most of the server’s configuration files can be found in the web application’s /WEB-INF directory. The full path to this directory is <server install dir>/server/webapps/spotfire/WEB-INF.

Use caution when modifying these files:

- Always make back-up copies of a configuration file before modifying it.
- Do not attempt to modify any other files than the ones listed in this chapter.
- Do not attempt to modify any other configuration parameters than the ones described in this chapter.

Note: After you have made a modification, you must restart the server for the changes to take effect (see “Starting the Spotfire Analytics Server” on page 105).

5.1.1 /WEB-INF/web.xml

The web.xml file is the web application’s main configuration file. The parameters described in the following sections are of special interest.

5.1.1.1 Configuring the Logging Framework

The value of the `com.spotfire.logging.config.file` parameter is the name of the configuration file to be used when configuring the logging framework at server startup. The logging configuration can also be changed using the DecisionSite Administrator Logging Workbench, but such modifications will only affect the logging configuration for the running process and will not affect the server after restart. To make a persistent change, edit the value of this parameter instead.

5.1.1.2 Configuring the PostAuthenticationFilter

The PostAuthenticationFilter SPI provides a way to customize the login system. After a successful validation of a client's security credentials, the configured PostAuthenticationFilter gets the opportunity to perform additional processing, that is, block the login attempt if the username cannot be found in the user directory; block the login attempt if the same IP number already has a valid session; or modify the name of the logged in user.

Unlike the legacy Authenticator mechanism, the PostAuthenticationFilter components work with all supported login methods and login systems. However, if a PostAuthenticationFilter is to be used with HTTP Basic authentication, the authenticator.configuration parameter (see “Configuring the Authenticator” on page 112 below) **must** be set to “com.spotfire.server.security.DefaultJAASAuthenticator”. By using any other Authenticator with HTTP Basic authentication, the PostAuthenticationFilter mechanism is effectively bypassed.

The default PostAuthenticationFilter component has two modes: blocking and autocreating. In the blocking mode (which is enabled by default), the filter requires that an authenticated user is to be found in the server's user directory. If the user cannot be found in the user directory, the login attempt fails even though the provided security credentials are valid. In the autocreating mode, an authenticated user which cannot be found in the user directory will get an account automatically created. The autocreating mode must only be used with the Database Table user directory back-end, since account creation is not supported by any other back-end. To enable the autocreating mode, set the authentication.filter.configuration parameter to “autocreate”. For all other configuration values, the blocking mode is enabled.

authentication.filter.class

This parameter specifies the name of the Java class that implements the PostAuthenticationFilter interface. This parameter is by default not present in the WEB-INF/web.xml file. The implicit default filter class is “com.spotfire.server.security.PostAuthenticationFilterImpl”.

authentication.filter.configuration

This parameter specifies an arbitrary configuration string for the configured PostAuthenticationFilter component. The default filter component's configuration controls whether the filter runs in blocking mode or autocreating mode. By setting this configuration parameter to “autocreate”, the autocreating mode is enabled. For all other parameter values, the filter runs in blocking mode (which is also the default behavior). This parameter is by default not present in the WEB-INF/web.xml file.

5.1.1.3 Configuring the Authenticator

The Authenticator SPI is a legacy mechanism to customize the login system. It is now superseded by the PostAuthenticationFilter mechanism, but it is still possible to use custom Authenticator components.

authenticator.class

This parameter affects the behavior of the login system when the server is configured for HTTP Basic authentication. It has no effect when the server is configured for Windows Integrated Authentication (NTLM or Kerberos) or X.509 Client Certificates.

Unless a custom authenticator component is to be deployed, it is recommended that the DefaultJAASAuthenticator is to be used. This component performs the actual username/password validation using the specified JAAS application configuration, but delegates all post authentication processing to the configured PostAuthenticationFilter. The additional functionality provided by the JAASAuthenticator and the JAASRegisteringAuthenticator (see below) is also provided by the blocking and the autocreating modes of the default PostAuthenticationFilter component. To enable the DefaultJAASAuthenticator component, set the authenticator.class parameter to “com.spotfire.server.security.DefaultJAASAuthenticator”.

Note: Whenever a PostAuthenticationFilter component is to be used with HTTP Basic authentication, the DefaultJAASAuthenticator **must** be used. By using any other Authenticator with HTTP Basic authentication, the PostAuthenticationFilter mechanism is effectively bypassed.

In addition to the DefaultJAASAuthenticator, the server also features the JAASAuthenticator and JAASRegisteringAuthenticator components.

The JAASAuthenticator component can be used with any user directory back-end. After a successful username/password validation, the JAASAuthenticator checks if the user is present in the server's user directory. If the user cannot be found, the login attempt fails even though the provided security credentials are valid. To enable this component, set the authenticator.class parameter to “com.spotfire.server.security.JAASAuthenticator”.

The JAASRegisteringAuthenticator component can only be used with the Database Table user directory back-end. After a successful username/password validation, the JAASRegisteringAuthenticator checks if the user is present in the server's user directory. If the user cannot be found, an account for the user is automatically created. As long as the provided security credentials are correct, the login attempt will always succeed and the logged in user will be guaranteed to have an account on the server. To enable this component, set the

`authenticator.class` parameter to
`"com.spotfire.server.security.JAASRegisteringAuthenticator"`.

Example: On a server configured with an LDAP login system and an LDAP user directory back-end, any successfully authenticated user will always be present in the user directory, since the LDAP user directory back-end consults the same LDAP server as the login system. Login attempts will thus always succeed, as long as the username and password is correct.

Example: If the server is configured with an LDAP login system and a Database Table user directory back-end, successfully authenticated users must also be present in the database for the login attempt to succeed. Correct username and password is not sufficient for logging in to the server, an administrator must also have created a user account on the server for the user.

authenticator.configuration

This parameter specifies the login system to be used, unless the server is configured for Windows Integrated Authentication (NTLM or Kerberos) or X.509 Client Certificates, in which case it has no effect. The value of this parameter must refer to a JAAS application configuration in the `spotfire.login` configuration file. Out-of-the-box, possible values are `"SpotfireDBLogin"`, `"SpotfireLDAP"` and `"SpotfireWindows"`. The documentation for the `spotfire.login` file describes these options in more detail.

5.1.1.4 Configuring a Custom Credential Transform

The Credential Transform SPI is a mechanism that enables password encryption and decryption using a custom defined algorithm. By implementing a custom transform and enabling it, it is possible to replace all clear-text passwords in application configuration files with encrypted ones.

credential.transform.class

This parameter specifies the name of the Java class that implements the `CredentialTransform` interface and that contains the encryption and decryption algorithm. This parameter is by default not present in the `WEB-INF/web.xml` file.

credential.transform.configuration

This optional parameter specifies an arbitrary configuration string for the configured Credential Transform implementation. The usage of the value of this parameter is up to the active Credential Transform to decide. The default configuration string is empty.

5.1.2 /jdk/jre/lib/security/spotfire.login

This file is located here:

<server install dir>/jdk/jre/lib/security/spotfire.login

The spotfire.login file contains the server's JAAS application configurations. When editing these configurations, be very careful with the syntax, since the JAAS parser is very exact in its interpretation. E.g., empty parameter values are not allowed.

The authenticator.configuration parameter in the /WEB-INF/web.xml file determines which configuration to use. By default, there are three such configurations present: **SpotfireDBLogin**, **SpotfireLDAP** and **SpotfireWindows**.

5.1.2.1 SpotfireDBLogin

This configuration is used when the server is configured with a Database Table login system.

In older versions of the server, this configuration contained some database connection parameters that now belongs in the /WEB-INF/data-sources.xml file. However, in some upgraded servers, this information can still be present in the spotfire.login file. It is advised that the parameters are removed; the configuration should always have the following content:

```
SpotfireDBLogin
{
    com.spotfire.server.jaas.dblogin.DBLoginModule
        required;
};
```

5.1.2.2 SpotfireWindows

This configuration is used when the server is configured with a Microsoft Windows NT Domain login system.

The **domains** parameter contains a comma-separated list of the names of the Windows NT domains to which the user accounts belong. If the Microsoft Windows NT Domain login system is combined with a Microsoft Windows NT Domain user directory back-end, then you need to make sure that the value of this parameter is synchronized with the value of the <**domains**> parameter in the "Windows" external directory provider configuration in the /WEB-INF/userdirconfig.xml file.

Example: A configuration for two domains called “engineering” and “sales”

```
SpotfireWindows
{
    com.spotfire.server.jaas.win.WinLoginModule
        required
        domains="engineering, sales";
};
```

5.1.2.3 SpotfireLDAP

This configuration is used when the server is configured with an LDAP login system.

If the LDAP login system is combined with an LDAP user directory back-end, make sure that the **serverURL**, **contextNames**, **user**, **password**, **nameAttribute** and **userFilter** parameters are synchronized with the corresponding parameters in the /WEB-INF/userdirconfig.xml configuration file (the **nameAttribute** and **userFilter** parameters map to the **<user-name-attribute>** and **<user-search-filter>** parameters, respectively). For more information, see “/WEB-INF/userdirconfig.xml” on page 124.

The **serverURL** parameter contains the URL to the LDAP server, including an optional port number and an optional protocol name, using the pattern [protocol://]server[:port]. The optional protocol name must, if specified, either be ldap or ldaps. For the LDAP protocol, the port number defaults to 389 and can usually be omitted. For the LDAPS protocol, the port number defaults to 636 and can usually be omitted. However, when accessing the Global Catalog of an Active Directory server, the LDAP port should be set to 3268, and the LDAPS port should be set to 3269.

The **contextNames** parameter contains the full distinguished name (DN) of the LDAP container to which the users belong. Multiple context names can be separated by a pipe character (“|”). If the containers contain a large amount of users, of which only a few should be allowed access to the Spotfire Analytics Server, a user search filter can be specified to include only the designated users (see the **userFilter** parameter below).

The **user** parameter contains the name of an administrator account to be used when searching for users and groups in the LDAP server. This account does not need to have any write permissions, but it needs to have read permissions for all configured contexts.

The **password** parameter contains the password for the administrator user account.

The **nameAttribute** parameter determines the name of the LDAP attribute containing the names of the user accounts. For Microsoft

Active Directory servers, it should be set to “sAMAccountName”. For a Sun Java System Directory Server (or any older Sun ONE Directory Server or iPlanet Directory Server) with a default configuration, it should be set to “uid”.

The **userFilter** parameter contains an LDAP search expression filter to be used when searching for users. For Microsoft Active Directory servers, it should be set to “objectClass=user”. For a Sun Java System Directory Server (or any older Sun ONE Directory Server or iPlanet Directory Server) with a default configuration, it should be set to “objectClass=person”. If only a subset of all the users in the specified LDAP containers should be allowed access to the Spotfire Analytics Server, a more detailed user search filter can be used. E.g., the search expression can be expanded so that it also puts restrictions on which groups the users belong to, or which roles they have.

For Microsoft Active Directory servers, access can be restricted to only those users belonging to a certain group by using a search expression with the pattern “&(objectClass=user)(memberOf=<groupDN>)”, where “<groupDN>” is to be replaced by the real DN of the group to which the users must belong. If the users are divided among multiple groups, use the pattern “&(objectClass=user)((memberOf=<groupOneDN>)(memberOf=<groupTwoDN>))”. Add extra “(memberOf=<groupDN>)” sub-expressions as needed.

For a Sun Java System Directory Server version 6 and later, the same effect can be achieved by using a search expression with the pattern “&(objectClass=person)(isMemberOf=<groupDN>)”. If the users are divided among multiple groups, use the pattern “&(objectClass=person)((isMemberOf=<groupOneDN>)(isMemberOf=<groupTwoDN>))”. Add extra “(isMemberOf=<groupDN>)” sub-expressions as needed.

For Sun ONE Directory Servers (as well as the newer Sun Java System Directory Servers or the older iPlanet Directory Server), access can be restricted to only those users having certain specific roles. The search expression for role filtering must match the pattern “&(objectClass=person)(nsRole=<roleDN>)”. If multiple roles are of interest, use the pattern “&(objectClass=person)((nsRole=<roleOneDN>)(nsRole=<roleTwoDN>))”. Add extra “(nsRole=<roleDN>)” sub-expressions as needed.

The syntax of LDAP search expression filters is specified by the RFC 4515 document available at <http://tools.ietf.org/html/rfc4515>. Please consult this documentation for information about more advanced filters.

Example: All users in the OUs have access to the server

```
SpotfireLDAP
{
    com.spotfire.server.jaas.ldap.LDAPLoginModule
        required
        serverURL="ldap://engr-dc:3268"
        contextNames="ou=engineering,dc=example,dc=com|ou=sales,dc=example,dc=com"
        user="hagbard"
        password="ifkgbg04"
        nameAttribute="sAMAccountName"
        userFilter="objectClass=user";
};
```

Example: Restricting access to members of the AISB group

```
SpotfireLDAP
{
    com.spotfire.server.jaas.ldap.LDAPLoginModule
        required
        serverURL="ldap://engr-dc:3268"
        contextNames="ou=engineering,dc=example,dc=com|ou=sales,dc=example,dc=com"
        user="hagbard"
        password="ifkgbg04"
        nameAttribute="sAMAccountName"
        userFilter="(&(objectClass=user)(memberOf=cn=AISB,dc=example,dc=com))";
};
```

It is also possible to define completely custom LDAP connection parameters, that will be used when creating the LDAP connections. Simply add a new <key>=<value> row in the JAAS application configuration for each such parameter that is requested. The only restriction is that the name of a custom LDAP connection parameter may not conflict with the name of a standard LDAPLoginModule parameter. Also, be careful and make sure to terminate with a semicolon after the last parameter.

Example: Defining a custom LDAP connection parameter

```
SpotfireLDAP
{
    com.spotfire.server.jaas.ldap.LDAPLoginModule
        required
        serverURL="ldap://engr-dc:3268"
        contextNames="ou=engineering,dc=example,dc=com|ou=sales,dc=example,dc=com"
        user="hagbard"
        password="ifkgbg04"
        nameAttribute="sAMAccountName"
        userFilter="objectClass=user"
        dereference="0";
};
```

It is also possible to have more than one LDAP server configuration, in case there are multiple LDAP servers belonging to separate LDAP forrests. Please note that this feature is not designed or suited for adding extra LDAP servers for fail-over or back-up purposes.

Simply add a new `com.spotfire.server.jaas.ldap.LDAPLoginModule` configuration block for each extra LDAP server, and change the “required” keywords to “sufficient”.

If the server is also configured for an LDAP user directory back-end, make sure to add the extra server configurations to the LDAP provider configuration in the `/WEB-INF/userdirconfig.xml` configuration file as well (see “`/WEB-INF/userdirconfig.xml`” on page 124.)

Example: LDAP configuration for two separate LDAP forrests

```
SpotfireLDAP
{
    com.spotfire.server.jaas.ldap.LDAPLoginModule
        sufficient
        serverURL="ldap://engr-dc:3268"
        contextNames="CN=Users,DC=example,DC=com"
        user="hagbard"
        password="ifkgbg04"
        nameAttribute="sAMAccountName"
        userFilter="objectClass=user";

    com.spotfire.server.jaas.ldap.LDAPLoginModule
        sufficient
        serverURL="ldap://engrldap"
        contextNames="OU=engineering,DC=example,DC=net|OU=sales,DC=example,DC=net"
        user="george"
        password="18gold"
        nameAttribute="uid"
        userFilter="objectClass=person";
};
```

5.1.3 /WEB-INF/data-sources.xml

The `data-sources.xml` file contains the configuration for the server platform's database connection pool. The file can contain multiple data sources, but the server currently only uses the default data source. The default data source is specified by the **<default-data-source>** parameter, which contains the name of the default data source.

5.1.3.1 Data Source Properties

Each data source has many parameters, where the following are of general interest:

The **<name>** parameter contains the name of the data source.

The **<driver-class>** parameter contains the JDBC driver class name. It should be set to `oracle.jdbc.OracleDriver` if the database used by the Spotfire Analytics Server is an Oracle database. It should be set to `net.sourceforge.jtds.jdbc.Driver` if the database is a Microsoft SQL Server database.

The **<url>** parameter contains the JDBC connection URL. It should use the syntax `"jdbc:oracle:thin:@[server]:[port]:[sid]"` if the database is an Oracle database, or the syntax `"jdbc:jtds:sqlserver://[server]:[port]/spotfire_dss"` if the database is a Microsoft SQL Server database. The `[server]` part should be replaced by the name of the database server, and the `[port]` part should be replaced by the port number used by the database. The Oracle database server defaults to port 1521, and Microsoft SQL Server database server defaults to port 1433. The `[sid]` part is specific for Oracle database servers, and defaults to `"xe"` for the bundled Oracle 10g Express Edition database server.

The **<username>** parameter contains the name of the database user to connect as.

The **<password>** parameter contains the password for the specified database user.

The **<min-connections>** parameter contains the minimum number of allocated connections.

The **<max-connections>** parameter contains the maximum number of allocated connections. Under high load, the total number of connections created by the server may be higher than the value of this parameter, but all such extra connections will automatically be closed when the load decreases. By setting this parameter to zero or a negative value, connection pooling is effectively disabled and new connections will be continuously created, whenever needed.

The **<pooling-scheme>** parameter defines the connection pooling algorithm to be used. There are four possible algorithms to choose among: `"dynamic_adaptive"`, `"dynamic_conservative"`, `"wait_adaptive"` and `"wait_conservative"`. The `"dynamic_adaptive"` algorithm is default. The pooling algorithms are described in detail in the section below.

5.1.3.2 Connection Pooling Schemes

dynamic_adaptive

When initialized, the data source creates a number of idle database connections equal to the **min-connections** parameter and puts them in the connection pool. When the data source receives a request for a database connection, it checks if the pool contains any idle connections and uses one of those, if available. If there are no idle connections in the pool, the data source automatically creates a new database connection. There is no upper limit for how many connections a data source can have open at the same time. However, as long as the number of open connections exceeds the **max-connections** parameter, any returned connection will be closed and discarded. Also, the idle connections in the pool eventually time out if they aren't used. The **connection-timeout** parameter defines how long time (given in seconds) a connection can stay idle in the connection pool before being closed and discarded.

Example: Configuring the dynamic_adaptive pooling scheme with a connection timeout of 30 minutes for a data source

```
<data-sources>
...
<data-source>
  <name>Server.Default</name>
  ...
  <pooling-scheme>DYNAMIC_ADAPTIVE</pooling-scheme>
  <connection-timeout>1800</connection-timeout>
  <min-connections>5</min-connections>
  <max-connections>20</max-connections>
</data-source>
...
</data-sources>
```

dynamic_conservative

When initialized, the connection pool creates a number of database connections equal to the **min-connections** parameter and puts them in the connection pool. When the data source receives a request for a database connection, it checks if the pool contains any idle connections and uses one of those, if available. If there are no idle connections in the pool, the data source automatically creates a new database connection. There is no upper limit for how many connections a data source can have open at the same time. However, as long as the number of open connections exceeds the **min-connections** parameter, any returned connection will be closed and discarded. Idle connections in the pool never time out, as is the case for the “dynamic_adaptive” and “wait_adaptive” schemes.

Example: Configuring the dynamic_conservative pooling scheme for a data source


```

<data-sources>
...
<data-source>
  <name>Server.Default</name>
  ...
  <pooling-scheme>DYNAMIC_CONSERVATIVE</pooling-scheme>
  <min-connections>5</min-connections>
  <!-- The max-connection parameter value must be a positive number
        equal to or larger than the min-connections parameter value,
        but the actual value is never used for the DYNAMIC_CONSERVATIVE
        pooling scheme -->
  <max-connections>5</max-connections>
</data-source>
...
</data-sources>

```

wait_adaptive

When initialized, the connection pool creates a number of database connections equal to the **min-connections** parameter and puts them in the connection pool. When the data source receives a request for a database connection, it checks if the pool contains any idle connections and uses one of those, if available. If there are no idle connections in the pool and the number of already open connections is less than the **max-connections** parameter, the data source creates a new database connection. If the number of already open connections is equal to the **max-connections** parameter, the data source waits for an active connection to be returned to the pool. If the request cannot be fulfilled within a number of seconds equal to the **login-timeout** parameter, the request times out. Thus, in **wait_adaptive** mode, the data source can never have more open (active or idle) connections than the value of the **max-connections** parameter. Whenever a database connection is returned to the data source, it is put in the pool of idle connections, unless it is used immediately to fulfill an already waiting request. The idle connections in the pool eventually time out if they aren't used. The **connection-timeout** parameter defines how long time (given in seconds) a connection can stay idle in the connection pool before being closed and discarded.

Example: Configuring the wait_adaptive pooling scheme with a login timeout of 30 seconds and a connection timeout of 30 minutes for a data source

```

<data-sources>
...
<data-source>
  <name>Server.Default</name>
  ...
  <pooling-scheme>WAIT_ADAPTIVE</pooling-scheme>
  <login-timeout>30</login-timeout>
  <connection-timeout>1800</connection-timeout>
  <min-connections>5</min-connections>
  <max-connections>20</max-connections>
</data-source>
...
</data-sources>

```

wait_conservative

When initialized, the connection pool creates a number of database connections equal to the **min-connections** parameter and puts them in the connection pool. When the data source receives a request for a database connection, it checks if the pool contains any idle connections and uses one of those, if available. If there are no idle connections in the pool and the number of already open connections is less than the **max-connections** parameter, the data source creates a new database connection. If the number of already open connections is equal to the **max-connections** parameter, the data source waits for an active connection to be returned to the pool. If the request cannot be fulfilled within a number of seconds equal to the **login-timeout** parameter, the request times out. Thus, in **wait_conservative** mode, the data source can never have more open (active or idle) connections than the value of the **max-connections** parameter. Database connections returned to the data source are used to fulfill already waiting requests. If there are no waiting requests and the number of open (active or idle) connections is equal to or exceeds the **min-connections** parameter, the returned connections are closed and discarded. If there are no waiting requests and the number of open (active or idle) connections is less than the **min-connections** parameter, the returned connections are stored in the pool. Idle connections in the pool never time out, as is the case for the “dynamic_adaptive” and “wait_adaptive” schemes.

Example: Configuring the wait_conservative pooling scheme with a login timeout of 30 seconds for a data source

```
<data-sources>
...
<data-source>
  <name>Server.Default</name>
  ...
  <pooling-scheme>WAIT_CONSERVATIVE</pooling-scheme>
  <login-timeout>30</login-timeout>
  <min-connections>5</min-connections>
  <max-connections>20</max-connections>
</data-source>
...
</data-sources>
```

5.1.3.3 JDBC Connection Properties

The data source also supports the configuration of JDBC connection properties parameter to be used when connecting to the database server. A typical use case for this feature is to specify encryption and integrity checksum algorithms for secure database connections. If defined in data-sources.xml, the connection properties should probably also be defined in the /WEB-INF/im-service.xml, /WEB-INF/library-service.xml and /WEB-INF/settings.xml files.

For more information, see “/WEB-INF/im-service.xml” on page 136, “/WEB-INF/library-service.xml” on page 142 and

“/WEB-INF/settings.xml” on page 146.

Each connection property consists of a key-value pair. The syntax for specifying JDBC connection properties is shown in the configuration example below.

Example: Defining connection properties for a data source

```
<data-sources>
...
<data-source>
  <name>Server.Default</name>
  ...
  <connection-properties>

    <connection-property>
      <key>oracle.net.encryption_client</key>
      <value>REQUIRED</value>
    </connection-property>

    <connection-property>
      <key>oracle.net.encryption_types_client</key>
      <value>( 3DES168 )</value>
    </connection-property>

    <connection-property>
      <key>oracle.net.crypto_checksum_client</key>
      <value>REQUIRED</value>
    </connection-property>

    <connection-property>
      <key>oracle.net.crypto_checksum_types_client</key>
      <value>( MD5 )</value>
    </connection-property>

  </connection-properties>
</data-source>
...
</data-sources>
```

5.1.3.4 Database Connections with Kerberos Authentication

When using Kerberos authentication for database connections, the parameter **<kerberos-login-context>** defines the name of the JAAS application configuration to use for retrieving the initial ticket-granting ticket (TGT) that will be used when performing the Kerberos authentication handshake with the database server. The specified JAAS application configuration must enable the retrieval of a TGT for the database client user, usually through a referenced keytab file. Consult Section 6.3.6 on page 198 for more information about how to create such a configuration.

All JDBC connection properties required to configure the JDBC driver for Kerberos authentication must also be added, and all necessary modifications to the JDBC URL must also be made. Please

consult your database server's documentation for more information about configuring the JDBC driver.

When all necessary JDBC connection properties have been added and the JDBC URL has been edited, save the file and restart the server.

Example: Referencing a JAAS application configuration for using Kerberos to authenticate with an Oracle data source

```
<data-sources>
...
<data-source>
  <name>Server.Default</name>
  ...

  <kerberos-login-context>DatabaseKerberos</kerberos-login-context>
  ...

  <connection-properties>
    <connection-property>
      <key>oracle.net.authentication_services</key>
      <value>(KERBEROS5)</value>
    </connection-property>
  </connection-properties>

</data-source>
...
</data-sources>
```

5.1.4 /WEB-INF/userdirconfig.xml

The userdirconfig.xml file contains the configuration for the server's user directory. The configuration consists of three parts: one for the mandatory internal directory provider, one for the optional external directory provider and one for the optional external group synchronization feature.

5.1.4.1 Internal Directory Provider

The **<internal-directory-provider>** element contains the name of the **<internal-directory-provider-configuration>** element to be used when configuring the internal directory provider. Leave this setting untouched.

The **<internal-directory-provider-configuration>** element's **<provider-class>** child element contains the name of the internal directory provider's database adaptor component to be used. When using an Oracle database with the Spotfire Analytics Server, the "com.spotfire.server.userdir.db.DBUserDirectoryInternalProviderOracle" database adaptor component should be used. When using a Microsoft SQL Server database with the Spotfire Analytics Server, the "com.spotfire.server.userdir.db.DBUserDirectoryInternalProviderMS SQL" database adaptor component should be used.

5.1.4.2 External Directory Provider

The **<external-directory-provider>** element contains the name of the **<external-directory-provider-configuration>** element to be used when creating and configuring an external directory provider. An external directory provider is only needed for LDAP or Microsoft Windows NT Domain user directory back-ends.

External Directory Provider for Database Table User Directory Back-end

If a Database Table user directory back-end is to be used, the **<external-directory-provider>** element should be left empty, since no external directory provider is needed for this configuration.

Example: Database Table User Directory Back-end

```
<userdir>

  <external-directory-provider/>

  ...

</userdir>
```

or

```
<userdir>

  <external-directory-provider></external-directory-provider>

  ...

</userdir>
```

The Microsoft Windows NT Domain Provider

The Microsoft Windows NT Domain directory provider is called “Windows”.

The **<domains>** parameter should contain a comma-separated list of the names of the Windows NT domains to which the user accounts belong. If this provider is combined with a Microsoft Windows NT Domains login system, then the value of this parameter must be synchronized with the value of the **domains** parameter in the SpotfireWindows JAAS application configuration in the **<server install dir>/jdk/jre/lib/security/spotfire.login** configuration file.

When the server starts and the Windows external directory provider is created and initialized, the directory provider creates a background thread that manages a user cache containing the names of all users in the specified domains. Whenever the directory provider needs to lookup users, it consults this cache instead of going directly to the

domain controllers. The background thread continuously synchronizes its user cache with the domain controllers. Each time a synchronization has been completed, the thread goes to sleep for a certain period before it performs a new synchronization. The **<refresh-time>** parameter specifies how long the background thread sleeps between each such synchronization. The parameter value should be specified in minutes. Finally, note that if the parameter value is set to 60 minutes, it does not mean that the thread performs a synchronization every hour, but that it sleeps one hour between each synchronization.

Example: Microsoft Windows NT Domain User Directory Back-end

```
<userdir>

  <external-directory-provider>Windows</external-directory-provider>

  ...

  <external-directory-provider-configuration>
    <provider-name>Windows</provider-name>
    <provider-class>com.spotfire.server.userdir.win.WinUserDirectoryProvider</provider-
class>
    <config>
      <connector-class>com.spotfire.server.util.win.WinConnectorImpl</connector-class>
      <domains>engineering, sales</domains>
      <refresh-time>60</refresh-time>
    </config>
  </external-directory-provider-configuration>

  ...

</userdir>
```

The LDAP Directory Provider

The LDAP directory provider is called “LDAP” and can be integrated with Microsoft Active Directory servers or Sun Java System Directory Servers (the latter product is formerly also known as Sun ONE Directory Server, iPlanet Directory Server and Netscape Directory Server). Through the use of the custom configuration capabilities, it might also work with other brands of LDAP servers. The LDAP directory provider’s configuration contains both mandatory and optional parameters. Do not attempt to alter the optional parameters unless you are very comfortable with LDAP configuration.

If the LDAP user directory back-end is combined with an LDAP login system, make sure that the **<server-url>**, **<context-names>**, **<user>**, **<password>**, **<user-name-attribute>** and **<user-search-filter>** parameters are synchronized with the corresponding parameters in the SpotfireLDAP JAAS application configuration in the `jre/lib/security/spotfire.login` configuration file (the **<user-name-**

attribute> and **<user-search-filter>** maps to the **nameAttribute** and **userFilter** parameters, respectively). For more information, see “/jdk/jre/lib/security/spotfire.login” on page 114.

The mandatory **<ldap-server-type>** parameter defines the type of LDAP server that the Spotfire Analytics Server will connect to. The parameter should be set to “activeDirectory” for Microsoft Active Directory servers, “sunOneDirectoryServer” for any version of the Sun Directory Servers, or “custom” for custom configurations. When the “activeDirectory” and “sunOneDirectoryServer” server types are specified, most parameters (except for the deployment-specific **<server-url>**, **<context-names>**, **<user>** and **<password>** parameters) are automatically given appropriate default values, though any default value can be overridden by specifying a new value for this parameter. If a default value is correct, the parameter should simply be left out.

Example:

```
<ldap-server-type>activeDirectory</ldap-server-type>
```

The mandatory **<server-url>** parameter specifies the URL to the LDAP server, including an optional port number and an optional protocol name, using the pattern [protocol://]server[:port]. The optional protocol name must, if specified, either be ldap or ldaps. For the LDAP protocol, the port number defaults to 389 and can usually be omitted. For the LDAPS protocol, the port number defaults to 636 and can usually be omitted. However, when accessing the Global Catalog of an Active Directory server, the LDAP port should be set to 3268, and the LDAPS port should be set to 3269.

Example:

```
<server-url>ldap://dc2:3268</server-url>
```

The mandatory **<context-names>** parameter should contain the full distinguished names (DNs) of the containers (e.g., organizational units, OUs) to which the users belong. Each DN is specified in a **<context-name>** child element. Multiple context names can also be specified as direct text content of the **<context-names>** element, and must then be separated by a pipe character (“|”). However, this older syntax is deprecated and might not work in future versions. If the specified containers contain a large number of users, of which only a few should be allowed access to the Spotfire Analytics Server, a user search filter can be specified to include only the designated users (see the **<user-search-filter>** parameter below).

Example:

```
<context-names>
  <context-name>OU=Engineering,DC=example,DC=com</context-name>
  <context-name>OU=Sales,DC=example,DC=com</context-name>
```

```
</context-names>
```

The mandatory **<user>** parameter should contain the name of an administrator account which is used to search for users and groups in the LDAP server. This account does not need to have any write permissions, but it needs to have read permissions for all configured contexts.

Example:

```
<user>hagbard</user>
```

The mandatory **<password>** parameter specifies the password for the administrator user account.

Example:

```
<password>ifkbg04</password>
```

The **<user-name-attribute>** parameter determines the name of the LDAP attribute containing the names of the user accounts. The parameter is mandatory for all custom configurations. For Microsoft Active Directory servers, the parameter value defaults to “sAMAccountName”. For any version of the Java Directory Servers, it defaults to “uid”.

Example:

```
<user-name-attribute>prid</user-name-attribute>
```

The **<group-name-attribute>** parameter determines the name of the LDAP attribute containing the names of the groups. The parameter is mandatory for any custom configuration with external group synchronization enabled. For Microsoft Active Directory servers, the parameter value defaults to “sAMAccountName”. For any version of the Sun Directory Servers, the parameter value defaults to “cn”.

Example:

```
<group-name-attribute>cn</group-name-attribute>
```

The **<member-attribute>** parameter determines the name of the LDAP attribute containing the names of the group or role members. The parameter is mandatory for any custom configuration with external group synchronization enabled. For Microsoft Active Directory servers, the parameter value defaults to “memberOf”. For any version of the Sun Directory Servers, it defaults to “nsRole”. For Sun Java System Directory Server version 6.0 or later, a custom configuration using groups instead of the role mechanism can have the parameter value set to “isMemberOf”. See “External Group Synchronization” on page 135 for more information about groups and roles.

Example:


```
<member-attribute>isMemberOf</member-attribute>
```

The **<user-search-filter>** parameter should contain an LDAP search expression filter to be used when searching for users. The parameter is mandatory for all custom configurations. For Microsoft Active Directory servers, the parameter value defaults to “objectClass=user”. For any version of the Sun Directory Servers, it defaults to “objectClass=person”. If only a subset of all the users in the specified LDAP containers should be allowed access to the Spotfire Analytics Server, a more detailed user search filter can be used. E.g., the search expression can be expanded so that it also puts restrictions on which groups the users belong to, or which roles they have. See the documentation for the **userFilter** parameter in the SpotfireLDAP JAAS application configuration in the <server install dir>/jdk/jre/lib/security/spotfire.login file, “SpotfireLDAP” on page 115.

Example:

```
<user-search-filter>&(objectClass=person)(isMemberOf=cn=projectX,dc=example,dc=com)</user-search-filter>
```

The **<group-search-filter>** parameter should contain an LDAP search expression filter to be used when searching for groups. The parameter is mandatory for all custom configurations with external group synchronization enabled. For Microsoft Active Directory servers, the parameter value defaults to “objectClass=group”. For any version of the Sun Directory Servers, it defaults to “&((objectclass=nsManagedRoleDefinition)(objectClass=nsNestedRoleDefinition))(objectclass=ldapSubEntry)”. For Sun Java System Directory Server version 6.0 or later, a custom configuration using groups instead of the role mechanism can have the parameter value set to “(objectClass=groupofuniquenames)”. See “External Group Synchronization” on page 135 for more information about groups and roles.

Example:

```
<group-search-filter>(objectClass=groupofuniquenames)</group-search-filter>
```

The **<ignore-member-groups>** parameter has a boolean value indicating whether the external group synchronization mechanism should recursively traverse the synchronized groups’ non-synchronized subgroups and include their members in the search result or not. This parameter is mandatory for any custom configuration with external group synchronization enabled. For Microsoft Active Directory servers, the parameter value defaults to “false”. For any version of the Sun Directory Servers, it defaults to “true”, since the role mechanism in those servers automatically include those members. For Sun Java System Directory Server version 6.0 or later, a custom configuration using groups instead of the role mechanism can have the parameter value set to “false”. See “External Group Synchronization” on page 135 for more information about groups and roles.

Example:

```
<ignore-member-groups>false</ignore-member-groups>
```

The **<external-groups-config>** parameter specifies the name of the configuration file with the names of the external LDAP groups to be synchronized. The parameter is mandatory for any configuration with external group synchronization enabled. The name must either be an absolute path to the configuration file, or a path starting with “/WEB-INF/”, indicating that the configuration file is located within the /WEB-INF directory. The specified configuration file should be in XML format, with an **<external-groups>** root element. The name of each LDAP group to synchronize should be added as a **<group-name>** child element to the root element.

Example:

```
<external-groups-config>/WEB-INF/external-groups-config.xml</external-groups-config>
```

Example: An external group synchronization configuration file

```
<external-groups>
  <group-name>SALESEU</group-name>
  <group-name>SALESUS</group-name>
  <group-name>MANAGEMENT</group-name>
</external-groups>
```

The optional **<request-control>** parameter determines the type of LDAP controls used in requests to the LDAP server. The default behavior is to probe the LDAP server for the best supported request control. The paged results control is always preferred, but the virtual list view control can also be used if the paged results control is not supported. The virtual list view control is always used together with a sort control. Both the paged results control and the virtual list view control supports a configurable page size. It is possible to set just the page size, without affecting the default request control type or to set just the request control type, without affecting the default page size.

The type of request control to be used is specified in the optional **<name>** element, which is a child element to the **<request-control>** element. To explicitly configure the server for probing, set the **<name>** parameter value to “probe”. To configure the server for the paged results control, set the **<name>** parameter value to “PagedResultsControl”. To request the virtual list view control, set the **<name>** parameter value to “VirtualListViewControl”. It is also possible to completely disable request controls by setting the **<name>** parameter value to “none”. If the **<name>** parameter is omitted, the value defaults to “probe”.

Example:

```
<request-control>
  <name>VirtualListViewControl</name>
</request-control>
```

The page size for the paged results control and the virtual list view control is specified in the optional **<page-size>** element, which is a child element to the **<request-control>** element. The page size value defaults to 2000 for both the paged results control and the virtual list view control.

Example:

```
<request-control>
  <name>PagedResultsControl</name>
  <page-size>5000</page-size>
</request-control>
```

The optional **<referral-mode>** parameter determines how the Spotfire Analytics Server should handle LDAP referrals. The default mode is “follow”. Other supported modes are “ignore” and “throw”. In most cases, it is recommended to leave this parameter untouched.

Example:

```
<referral-mode>follow</referral-mode>
```

The optional **<import-limit>** parameter offers the possibility to limit the number of users retrieved from the LDAP server. This feature can be handy at deployment sites where the number of expected Spotfire users are few, but the total number of users in the LDAP servers are tens of thousands or even more. By setting an import limit, the administrator can be sure that the number of users won’t affect the server’s performance. This functionality is probably of most use in test deployments. By default, there is no import limit. To explicitly request unlimited import, set the parameter value to “-1”. All positive numbers are treated as an import limit. In most cases, it is recommended to leave this parameter untouched.

Example:

```
<import-limit>100</import-limit>
```

The optional **<initial-context-factory>** parameter specifies the full class name of the initial JNDI context factory to be used when created LDAP connections. The default value is “com.sun.jndi.ldap.LdapCtxFactory”, and it is recommended to leave this parameter untouched.

Example:

```
<initial-context-factory>com.sun.jndi.ldap.LdapCtxFactory</initial-context-
factory>
```

It is also possible to define completely custom LDAP connection properties, that will be used when creating the LDAP connections. Simply create a new **<custom-properties>** element as a child to the appropriate **<server>** tag in the LDAP provider configuration. Each property is then defined by a **<property><key>parameter name</key><value>parameter value</value></property>** block.

Example: Defining a custom LDAP connection properties

```
<server>
...
<custom-properties>
  <property>
    <key>dereference</key>
    <value>0</value>
  </property>
</custom-properties>
</server>
```

Here follows some complete example configurations for the LDAP user directory back-end:

Example: LDAP User Directory Back-end

```
<userdir>

  <external-directory-provider>LDAP</external-directory-provider>

  ...

  <external-directory-provider-configuration>
    <provider-name>LDAP</provider-name>
    <provider-class>com.spotfire.server.userdir.ldap.LDAPUserDirectoryProvider</
provider-class>
    <config>
      <server>
        <ldap-server-type>activeDirectory</ldap-server-type>
        <server-url>ldap://dc2:3268</server-url>
        <context-names>
          <context-name>CN=Users,DC=example,DC=com</context-name>
        </context-names>
        <user>hagbard</user>
        <password>ifkgbg04</password>
      </server>
    </config>
  </external-directory-provider-configuration>

</userdir>
```

Example: LDAP User Directory Back-end

```
<userdir>
```

```

<external-directory-provider>LDAP</external-directory-provider>

...

<external-directory-provider-configuration>
  <provider-name>LDAP</provider-name>
  <provider-class>com.spotfire.server.userdir.ldap.LDAPUserDirectoryProvider</
provider-class>
  <config>
    <server>
      <ldap-server-type>sunOneDirectoryServer</ldap-server-type>
      <server-url>ldap://engr1ldap</server-url>
      <context-names>
        <context-name>OU=Engineering,DC=example,DC=com</context-name>
        <context-name>OU=Sales,DC=example,DC=com</context-name>
      </context-names>
      <user>hagbard</user>
      <password>ifkgbg04</password>
    </server>
  </config>
</external-directory-provider-configuration>

</userdir>

```

Example: LDAP User Directory Back-end

```

<userdir>

  <external-directory-provider>LDAP</external-directory-provider>

  <external-group-synchronization>
    <enabled>true</enabled>
    <sleep-time>60</sleep-time>
  </external-group-synchronization>

  <external-directory-provider-configuration>
    <provider-name>LDAP</provider-name>
    <provider-class>com.spotfire.server.userdir.ldap.LDAPUserDirectoryProvider</
provider-class>
    <config>
      <server>
        <ldap-server-type>custom</ldap-server-type>
        <server-url>ldaps://ldapsrv:636</server-url>
        <context-names>
          <context-name>OU=Research & Design,DC=example,DC=com</context-name>
        </context-names>
        <user>hagbard</user>
        <password>ifkgbg04</password>
        <user-name-attribute>prid</user-name-attribute>
        <group-name-attribute>cn</group-name-attribute>
        <member-attribute>isMemberOf</member-attribute>
        <user-search-
filter>&(objectClass=person)(isMemberOf=cn=projectX,dc=example,dc=com)</user-search-
filter>
        <group-search-filter>(objectClass=groupofuniqueNames)</group-search-filter>
        <ignore-member-groups>false</ignore-member-groups>
        <request-control>
          <name>VirtualListViewControl</name>
          <page-size>5000</page-size>

```

```
        </request-control>
        <referral-mode>follow</referral-mode>
        <external-groups-config>/WEB-INF/external-groups-config.xml</external-groups-
config>
    </server>
</config>
</external-directory-provider-configuration>

</userdir>
```

5.1.4.3 Accessing Multiple LDAP Servers

It is possible to have more than one LDAP server configuration, in case there are multiple LDAP servers belonging to separate LDAP forests. Please note that this feature is not designed or suited for adding extra LDAP servers for fail-over or back-up purposes.

Simply add a new **<server>** configuration block for each extra LDAP server. These servers do not even need to be of the same brand.

If the server is also configured for an LDAP login system, make sure to add the extra server configurations in the SpotfireLDAP JAAS application configuration in the `jre/lib/security/spotfire.login` configuration file as well (see “`/jdk/jre/lib/security/spotfire.login`” on page 114).

Example: LDAP configuration for two separate LDAP forests

```
<userdir>

    <external-directory-provider>LDAP</external-directory-provider>

    ...

    <external-directory-provider-configuration>
        <provider-name>LDAP</provider-name>
        <provider-class>com.spotfire.server.userdir.ldap.LDAPUserDirectoryProvider</
provider-class>
        <config>
            <server>
                <ldap-server-type>activeDirectory</ldap-server-type>
                <server-url>ldap://dc2:3268</server-url>
                <context-names>
                    <context-name>CN=Users,DC=example,DC=com</context-name>
                </context-names>
                <user>hagbard</user>
                <password>ifkbg04</password>
            </server>
            <server>
                <ldap-server-type>sunOneDirectoryServer</ldap-server-type>
                <server-url>ldap://engrldap</server-url>
                <context-names>
                    <context-name>OU=Engineering,DC=example,DC=net</context-name>
                    <context-name>OU=Sales,DC=example,DC=net</context-name>
                </context-names>
                <user>george</user>
            </server>
        </config>
    </external-directory-provider-configuration>
</userdir>
```

```

    <password>18gold</password>
  </server>
</config>
</external-directory-provider-configuration>

</userdir>

```

5.1.4.4 External Group Synchronization

When using an LDAP user directory back-end, the Spotfire Analytics Server offers the capability to synchronize the group memberships for selected LDAP groups with its own internal groups. This makes it possible for an administrator to assign licenses and privileges to Spotfire groups in the normal fashion, but being relieved of the duty of having to manage the group memberships.

All synchronized LDAP groups will be immutable in the Spotfire administration tools, i.e., you can neither rename or remove such a group, nor alter its member list. However, you can still include such a group as a subgroup of another non-immutable group.

If a synchronized LDAP group contains a subgroup, the members of the subgroup will automatically also be included in the member list for the synchronized parent group, unless the subgroup is also one of the synchronized LDAP groups, in which case the subgroup itself will be included in the parent group's member list. A subgroup that is not synchronized will not be visible in the Spotfire Analytics Server. If the non-synchronized subgroups should simply be ignored instead of automatically traversed, the **<ignore-member-groups>** parameter in the LDAP external directory provider's configuration in /WEB-INF/userdirconfig.xml can be set to "true". If the role-based mechanism is used for the Sun Directory Servers, this parameter should always be set to "false" to avoid inconsistent data, since the recursive memberships are automatically always resolved. For more information see "Enabling External LDAP Group Synchronization" on page 200.

In Microsoft Active Directory servers and in Sun Java System Directory Server 6.0 or later, most types of groups should be possible to synchronize. In Sun ONE Directory Servers (or the older iPlanet Directory Servers), however, it is not possible to use the same group synchronization mechanism as for the other servers. Instead, a role-based synchronization mechanism can be used, where the internal Spotfire groups are synchronized with nested or managed roles (but not filtered roles!) in the Sun ONE Directory Server. This role-based synchronization can of course also be used with the newer Sun Java System Directory Server.

Note: When setting up external group synchronization, make sure not to introduce any cyclic group memberships, where the ancestor of a group is also a descendant of the same group.

The **<enabled>** parameter determines whether the external group synchronization is enabled or not. By default, this parameter is set to “false”. When the synchronization is enabled by modifying the parameter value to “true”, make sure to set the **<external-groups-config>** parameter for the LDAP external directory provider configuration in the /WEB-INF/userdirconfig.xml file, so that the synchronization mechanism knows which groups it should synchronize.

When the server starts and the group synchronization mechanism is initialized, a background thread is created that periodically synchronizes the external LDAP groups with the internal groups in the Spotfire Analytics Server. Each time a synchronization has been completed, the thread goes to sleep for a certain period before it performs a new synchronization. The **<sleep-time>** parameter specifies how long the background thread sleeps between each such synchronization. The parameter value should be specified in minutes. By default, the sleep time is set to 60 minutes. Finally, note that if the parameter value is set to 60 minutes, it does not mean that the thread performs a synchronization every hour, but that it sleeps one hour between each synchronization.

5.1.5 /WEB-INF/im-service.xml

The im-service.xml file contains the configuration for Information Services.

5.1.5.1 Database Adaptors

Some Information Services components use database adaptors to communicate with the database server. The database adaptors are different for each database server brand.

The Element Model Database Adaptor

The database adaptor for the element model component is specified in the **class** attribute of the **<storage>** element, which is a child element to the **<element-model>** element (see the example below). The database adaptor should be set to “com.spotfire.ws.im.element.storage.OracleStorage” for Oracle database servers, or to “com.spotfire.ws.im.element.storage.MSSQLStorage” for Microsoft SQL Server database servers.

The Configuration Model Database Adaptor

The database adaptor for the configuration model component is specified in the **class** attribute of the **<storage>** element, which is a child element to the **<configuration-model>** element (see the

example below). The database adaptor should be set to “com.spotfire.ws.im.config.storage.OracleStorage” for Oracle database servers, or to “com.spotfire.ws.im.config.storage.MSSQLStorage” for Microsoft SQL Server database servers.

Example: A configuration for Oracle database servers

```
<im-service>

...

<!-- Element model -->
<element-model>
  <!-- database storage -->
  <storage class="com.spotfire.ws.im.element.storage.OracleStorage">
    <connection-pool-name>im-connection-pool</connection-pool-name>
  </storage>
</element-model>

...

<!-- Configuration model -->
<configuration-model>
  <!-- database storage -->
  <storage class="com.spotfire.ws.im.config.storage.OracleStorage">
    <connection-pool-name>im-connection-pool</connection-pool-name>
  </storage>
</configuration-model>

...

</im-service>
```

Example: A configuration for Microsoft SQL Server database servers

```
<im-service>

...

<!-- Element model -->
<element-model>
  <!-- database storage -->
  <storage class="com.spotfire.ws.im.element.storage.MSSQLStorage">
    <connection-pool-name>im-connection-pool</connection-pool-name>
  </storage>
</element-model>

...

<!-- Configuration model -->
<configuration-model>
  <!-- database storage -->
  <storage class="com.spotfire.ws.im.config.storage.MSSQLStorage">
    <connection-pool-name>im-connection-pool</connection-pool-name>
  </storage>
</configuration-model>
```

```
...  
</im-service>
```

5.1.5.2 Connection Pool Properties

The **<connection-pool>** element contains the configuration for Information Services' database connection pool. The element must have a **name** attribute with the value "im-connection-pool".

The **<driver-class>** parameter contains the JDBC driver class name. It should be set to "oracle.jdbc.OracleDriver" if the database used by the Spotfire Analytics Server is an Oracle database. It should be set to "net.sourceforge.jtds.jdbc.Driver" if the database is a Microsoft SQL Server database.

The **<connection-url>** parameter contains the JDBC connection URL. It should use the syntax "jdbc:oracle:thin:@[server]:[port]:[sid]" if the database is an Oracle database, or the syntax "jdbc:jtds:sqlserver://[server]:[port]/spotfire_iim" if the database is a Microsoft SQL Server database. The [server] part should be replaced by the name of the database server, and the [port] part should be replaced by the port number used by the database. The Oracle database server defaults to port 1521, and Microsoft SQL Server database server defaults to port 1433. The [sid] part is specific for Oracle database servers, and defaults to "xe" for the bundled Oracle 10g Express Edition database server.

The **<user>** parameter contains the name of the database user to connect as.

The **<password>** parameter contains the password for the specified database user.

The **<min-count>** parameter contains the minimum number of allocated connections.

The **<max-count>** parameter contains the maximum number of allocated connections.

The **<ping-command>** parameter should contain a dummy SQL query that can be used for testing database connection. For Oracle database servers, the typical SQL query is "SELECT 1 FROM DUAL". For Microsoft SQL Server databases, the typical SQL query is "SELECT 1".

Example: Connection pool properties for a Microsoft SQL Server database

```
<im-service>
```

```

...

<!-- JDBC connection pool -->
<connection-pool name="im-connection-pool">
  <driver-class>net.sourceforge.jtds.jdbc.Driver</driver-class>
  <connection-url>jdbc:jtds:sqlserver://localhost:1433/spotfire_iim</connection-url>
  <user>spotuser_iim</user>
  <password>dsfsd324fvgsd</password>
  <!-- Please, do not change the size -->
  <max-count>3</max-count>
  <min-count>3</min-count>
  <ping-command>SELECT 1</ping-command>
</connection-pool>

</im-service>

```

5.1.5.3 JDBC Connection Properties

The optional **<connection-properties>** parameter block can be used to define JDBC connection properties parameters to be used when connecting to the database server. A typical use case for this feature is to specify encryption and integrity checksum algorithms for secure database connections. If JDBC connection properties are defined in im-service.xml, the properties should probably also be defined in the /WEB-INF/data-sources.xml, /WEB-INF/library-service.xml and /WEB-INF/settings.xml files. For more information about those configuration files, see “/WEB-INF/data-sources.xml” on page 118, “/WEB-INF/library-service.xml” on page 142 and “/WEB-INF/settings.xml” on page 146.

Each connection property consists of a key-value pair. The syntax for specifying JDBC connection properties for a **<connection-pool>** is shown in the configuration example below.

Example: Connection pool properties for an Oracle database server with JDBC connection properties

```

<im-service>

...

<!-- JDBC connection pool -->
<connection-pool name="im-connection-pool">
  <driver-class>oracle.jdbc.OracleDriver</driver-class>
  <connection-url>jdbc:oracle:thin:@localhost:1521:xe</connection-url>
  <user>spotuser_iim</user>
  <password>dsfsd324fvgsd</password>
  <!-- Please, do not change the size -->
  <max-count>3</max-count>
  <min-count>3</min-count>
  <ping-command>SELECT 1 FROM DUAL</ping-command>
  <connection-properties>
    <connection-property>
      <key>oracle.net.encryption_client</key>

```

```

    <value>REQUIRED</value>
  </connection-property>
</connection-property>
  <key>oracle.net.encryption_types_client</key>
  <value>( 3DES168 )</value>
</connection-property>
</connection-property>
  <key>oracle.net.crypto_checksum_client</key>
  <value>REQUIRED</value>
</connection-property>
</connection-property>
  <key>oracle.net.crypto_checksum_types_client</key>
  <value>( MD5 )</value>
</connection-property>
</connection-properties>
</connection-pool>

</im-service>

```

5.1.5.4 Advanced Connection Pool Configuration

Starting with Spotfire Analytics Server 10.1 a new type of connection pool is used for Information Services. The new connection pool was introduced for the user directory and other components from version 9.0. Those components retrieve their database configurations from the /WEB-INF/data-sources.xml file, but the Information Services' database configuration still resides in the /WEB-INF/im-service.xml file.

The Information Services do not support all the configuration parameters that appears in the /WEB-INF/data-sources.xml file, but the following special parameters are available:

- **“spotfire.pooling.data.source.scheme”**
(corresponds to the “pooling-scheme” parameter in the /WEB-INF/data-source.xml configuration file, see “/WEB-INF/data-sources.xml” on page 118).
- **“spotfire.pooling.data.source.connection.timeout”**
(corresponds to the “connection-timeout” parameter)
- **“spotfire.pooling.data.source.login.timeout”**
(corresponds to the “login-timeout” parameter).
- **“spotfire.kerberos.login.context”**
(corresponds to the “kerberos-login-context” parameter)

It is also possible to revert to the old type of connection pool by setting the **“spotfire.connection.pool.factory.data.source”** parameter to “init.commands.data.source”. The default value for this parameter is “pooling.data.source”.

All these parameters should be added as JDBC connection properties (see the previous section). However, they will never be used as real

JDBC connection properties and will never be sent to a database server.

Example: Configuring a PoolingDataSource for an Oracle database

```
<im-service>

...

<!-- JDBC connection pool -->
<connection-pool name="im-connection-pool">
  <driver-class>oracle.jdbc.OracleDriver</driver-class>
  <connection-url>jdbc:oracle:thin:@localhost:1521:xe</connection-url>
  <user>spotuser_iim</user>
  <password>dsfsd324fvgsd</password>
  <!-- Please, do not change the size -->
  <max-count>3</max-count>
  <min-count>3</min-count>
  <ping-command>SELECT 1 FROM DUAL</ping-command>
  <connection-properties>
    <connection-property>
      <key>spotfire.pooling.data.source.scheme</key>
      <value>WAIT_ADAPTIVE</value>
    </connection-property>
    <connection-property>
      <key>spotfire.pooling.data.source.connection.timeout</key>
      <value>1800</value>
    </connection-property>
    <connection-property>
      <key>spotfire.pooling.data.source.login.timeout</key>
      <value>30</value>
    </connection-property>
  </connection-properties>
</connection-pool>

</im-service>
```

5.1.5.5 Database Connections with Kerberos Authentication

Kerberos authentication for database connections are configured in a similar way to the data sources in data-sources.xml (see Section 5.1.3.4 on page 123). When configuring this service for Kerberos authentication, dummy username and password parameter values are required for legacy reasons.

Example: Referencing a JAAS application configuration for using Kerberos to authenticate with an Oracle data source

```
<im-service>

...
```

```
<!-- JDBC connection pool -->
<connection-pool name="im-connection-pool">
  <driver-class>oracle.jdbc.OracleDriver</driver-class>
  <connection-url>jdbc:oracle:thin:@localhost:1521:xe</connection-url>
  <user>dummy</user>
  <password>dummy</password>
  <!-- Please, do not change the size -->
  <max-count>3</max-count>
  <min-count>3</min-count>
  <ping-command>SELECT 1 FROM DUAL</ping-command>
  <connection-properties>
    <connection-property>
      <key>spotfire.kerberos.login.context</key>
      <value>DatabaseKerberos</value>
    </connection-property>
    <connection-property>
      <key>oracle.net.authentication_services</key>
      <value>( KERBEROS5 )</value>
    </connection-property>
  </connection-properties>
</connection-pool>

</im-service>
```

5.1.6 /WEB-INF/library-service.xml

The library-service.xml file contains the configuration for the Spotfire Library.

5.1.6.1 Connection Pool Properties

The **<connection-pool-properties>** element contains the configuration for Spotfire Library's database connection pool. The element must have a **name** attribute with the value "library-storage".

The **<driver-class>** parameter contains the JDBC driver class name. It should be set to "oracle.jdbc.OracleDriver" if the database used by the Spotfire Analytics Server is an Oracle database. It should be set to "net.sourceforge.jtds.jdbc.Driver" if the database is a Microsoft SQL Server database.

The **<connection-url>** parameter contains the JDBC connection URL. It should use the syntax "jdbc:oracle:thin:@[server]:[port]:[sid]" if the database is an Oracle database, or the syntax "jdbc:jtds:sqlserver://[server]:[port]/spotfire_lib" if the database is a Microsoft SQL Server database. The [server] part should be replaced by the name of the database server, and the [port] part should be replaced by the port number used by the database. The Oracle database server defaults to port 1521, and Microsoft SQL Server database server defaults to port 1433. The [sid] part is specific for Oracle database servers, and defaults to "xe" for the bundled Oracle 10g Express Edition database server.

The **<user>** parameter contains the name of the database user to connect as.

The **<password>** parameter contains the password for the specified database user.

The **<min-count>** parameter contains the minimum number of allocated connections.

The **<max-count>** parameter contains the maximum number of allocated connections.

The **<ping-command>** parameter should contain a dummy SQL query that can be used for testing database connection. For Oracle database servers, the typical SQL query is “SELECT 1 FROM DUAL“. For Microsoft SQL Server databases, the typical SQL query is “SELECT 1“.

The optional **<init-command>** parameter should contain an SQL command that is used when initializing the database connections. Leave this parameter untouched.

The **<auto-commit>** parameter should always be set to “false”. Leave this parameter untouched.

Example: Connection pool properties for a Microsoft SQL Server database

```
<library>
  <library-service-config xmlns:library="http://schemas.spotfire.com/ws/2004/05/
library.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="library:LibraryServiceConfig">
    <connection-pool-properties name="library-storage">
      <driver-class>net.sourceforge.jtds.jdbc.Driver</driver-class>
      <connection-url>jdbc:jtds:sqlserver://localhost:1433/spotfire_lib</connection-
url>
      <user>spotuser_library</user>
      <password>dsfsd324fvgsd</password>
      <max-count>3</max-count>
      <min-count>3</min-count>
      <auto-commit>false</auto-commit>
      <ping-command>SELECT 1</ping-command>
      <init-command>SELECT 1</ping-command>
    </connection-pool-properties>
  </library-service-config>
</library>
```

5.1.6.2 JDBC Connection Properties

The optional **<connection-properties>** parameter block can be used to define JDBC connection properties parameters to be used when connecting to the database server. A typical use case for this feature is

to specify encryption and integrity checksum algorithms for secure database connections. If JDBC connection properties are defined in library-service.xml, the properties should probably also be defined in the /WEB-INF/data-sources.xml, /WEB-INF/im-service.xml and /WEB-INF/settings.xml files. For more information about those configuration files, see “/WEB-INF/data-sources.xml” on page 118, “/WEB-INF/im-service.xml” on page 136 and “/WEB-INF/settings.xml” on page 146.

Each connection property consists of a key-value pair. The syntax for specifying JDBC connection properties for a **<connection-pool>** is shown in the configuration example below.

Example: Connection pool properties for an Oracle database server with JDBC connection properties

```
<library>
  <library-service-config xmlns:library="http://schemas.spotfire.com/ws/2004/05/
library.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="library:LibraryServiceConfig">
    <connection-pool-properties name="library-storage">
      <driver-class>oracle.jdbc.OracleDriver</driver-class>
      <connection-url>jdbc:oracle:thin:@localhost:1521:xe</connection-url>
      <user>spotuser_library</user>
      <password>dsfsd324fvgsd</password>
      <max-count>3</max-count>
      <min-count>3</min-count>
      <auto-commit>false</auto-commit>
      <ping-command>SELECT 1 FROM DUAL</ping-command>
      <init-command>SELECT 1 FROM DUAL</ping-command>
      <connection-properties>
        <connection-property>
          <key>oracle.net.encryption_client</key>
          <value>REQUIRED</value>
        </connection-property>
        <connection-property>
          <key>oracle.net.encryption_types_client</key>
          <value>( 3DES168 )</value>
        </connection-property>
        <connection-property>
          <key>oracle.net.crypto_checksum_client</key>
          <value>REQUIRED</value>
        </connection-property>
        <connection-property>
          <key>oracle.net.crypto_checksum_types_client</key>
          <value>( MD5 )</value>
        </connection-property>
      </connection-properties>
    </connection-pool-properties>
  </library-service-config>
</library>
```

5.1.6.3 Advanced Connection Pool Configuration

Starting with Spotfire Analytics Server 10.1 a new type of connection pool is used for Spotfire Library. The new connection pool was

introduced for the user directory and other components from version 9.0. Those components retrieve their database configurations from the /WEB-INF/data-sources.xml file, but the Spotfire Library's database configuration still resides in the /WEB-INF/library-service.xml file.

The Spotfire Library does not support all the configuration parameters that appears in the /WEB-INF/data-sources.xml file, but the following special parameters are available:

- **“spotfire.pooling.data.source.scheme”**
(corresponds to the “pooling-scheme” parameter in the /WEB-INF/data-source.xml configuration file, see “/WEB-INF/data-sources.xml” on page 118).
- **“spotfire.pooling.data.source.connection.timeout”**
(corresponds to the “connection-timeout” parameter)
- **“spotfire.pooling.data.source.login.timeout”**
(corresponds to the “login-timeout” parameter).
- **“spotfire.kerberos.login.context”**
(corresponds to the “kerberos-login-context” parameter)

It is also possible to revert to the old type of connection pool by setting the **“spotfire.connection.pool.factory.data.source”** parameter to **“init.commands.data.source”**. The default value for this parameter is **“pooling.data.source”**.

All these parameters are added as JDBC connection properties. However, they will never be used as real JDBC connection properties and will never be sent to a database server.

Example: Configuring a PoolingDataSource for an Oracle database

```
<library>
  <library-service-config xmlns:library="http://schemas.spotfire.com/ws/2004/05/
library.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="library:LibraryServiceConfig">
    <connection-pool-properties name="library-storage">
      <driver-class>oracle.jdbc.OracleDriver</driver-class>
      <connection-url>jdbc:oracle:thin:@localhost:1521:xe</connection-url>
      <user>spotuser_library</user>
      <password>dsfsd324fvgsd</password>
      <max-count>3</max-count>
      <min-count>3</min-count>
      <ping-command>SELECT 1 FROM DUAL</ping-command>
      <init-command>SELECT 1 FROM DUAL</init-command>
      <connection-properties>
        <connection-property>
          <key>spotfire.pooling.data.source.scheme</key>
          <value>WAIT_ADAPTIVE</value>
        </connection-property>
        <connection-property>
          <key>spotfire.pooling.data.source.connection.timeout</key>
          <value>1800</value>
        </connection-property>
      </connection-properties>
    </connection-pool-properties>
  </library-service-config>
</library>
```

```
<connection-property>
  <key>spotfire.pooling.data.source.login.timeout</key>
  <value>30</value>
</connection-property>
</connection-properties>
</connection-pool-properties>
</library-service-config>
</library-service>
```

5.1.6.4 Database Connections with Kerberos Authentication

Kerberos authentication for database connections are configured in a similar way to the data sources in data-sources.xml (see Section 5.1.3.4 on page 123). When configuring this service for Kerberos authentication, dummy username and password parameter values are required for legacy reasons.

Example: Referencing a JAAS application configuration for using Kerberos to authenticate with an Oracle data source

```
<library>
  <library-service-config xmlns:library="http://schemas.spotfire.com/ws/2004/05/library.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:type="library:LibraryServiceConfig">
    <connection-pool-properties name="library-storage">
      <driver-class>oracle.jdbc.OracleDriver</driver-class>
      <connection-url>jdbc:oracle:thin:@localhost:1521:xe</connection-url>
      <user>dummy</user>
      <password>dummy</password>
      <max-count>3</max-count>
      <min-count>3</min-count>
      <auto-commit>false</auto-commit>
      <ping-command>SELECT 1 FROM DUAL</ping-command>
      <init-command>SELECT 1 FROM DUAL</init-command>
      <connection-properties>
        <connection-property>
          <key>spotfire.kerberos.login.context</key>
          <value>DatabaseKerberos</value>
        </connection-property>
        <connection-property>
          <key>oracle.net.authentication_services</key>
          <value>( KERBEROS5 )</value>
        </connection-property>
      </connection-properties>
    </connection-pool-properties>
  </library-service-config>
</library>
```

5.1.7 /WEB-INF/settings.xml

The settings.xml file is described in chapter “Configuring IS to Access a New Type of JDBC Data Source” on page 207.

5.1.8 /WEB-INF/manifest.xml

Example:

```
<client-login>
  <show-login-dialog>standard</show-login-dialog>
  <always-online>false</always-online>
  <allow-save-information>true</allow-save-information>
  <offline-days-permitted>infinite</offline-days-permitted>
  <rss>/spotfire/rss.xml</rss>
</client-login>

<server-info>
  <authentication-modes>
    <username-and-password />
  </authentication-modes>
</server-info>
```

The **<client-login>** node specifies the behavior of the login dialog in Spotfire for the users:

<show-login-dialog>

- **default** - behavior set by the user.
- **always** - always show the login dialog.
- **never** - never show the login dialog.

<always-online>

- **true** - user must always be logged in to the Spotfire Analytics Server to run Spotfire.
- **false** - user can select to work offline.

<allow-save-information>

- **true** - allows the user to select “Remember Me” in the login dialog and store his login information for future automatic login.
- **false** - the user cannot store his login information, and must provide this each time he wants to login.

<offline-days-permitted>

- **infinite** - the users can select to Work Offline and will never be forced to connect to the Spotfire Analytics Server.
- **#** - the users can select to Work Offline but will be prompted and forced to log in after # number of days.

<rss>

- A path or URL to an RSS feed which will be displayed in the login dialog of the end users. For more information see “Enabling

RSS Feed in the Login Dialog” on page 232.

The **<authentication-modes>** property tells DecisionSite Client which login method it should use. Possible values are: **<client-certificate/>**, **<integrated-authentication/>**, and **<username-and-password/>**.

5.1.9 <server install dir>/server/conf/server.xml

This file controls, among other things, which port the server should listen to, if it should use http or https, timeouts, etc.

An important node here is the **connector** node.

The sample below listens to ordinary http on port 80:

```
<Connector
port="80"
maxHttpHeaderSize="8192"
maxThreads="150"
minSpareThreads="25"
maxSpareThreads="75"
enableLookups="false"
redirectPort="8443"
acceptCount="100"
connectionTimeout="30000"
disableUploadTimeout="true" />
```

In this example we are using https and require client certificates:

```
<Connector port="443"
maxHttpHeaderSize="8192"
maxThreads="150"
minSpareThreads="25"
maxSpareThreads="75"
enableLookups="false"
disableUploadTimeout="true"
acceptCount="100"
scheme="https"
secure="true"
clientAuth="true"
sslProtocol="TLS"
keystoreFile="c:/cert.jks"
keystorePass="spotfire"
keystoreType="JKS" />
```

For more information about this file see the standard documentation on Tomcat.

5.1.10 /WEB-INF/security-filter.xml

The /WEB-INF/security-filter.xml file contains the configuration for the server’s security filter, which is responsible for authenticating users and making access controls for requested resources. Most of the

configuration should be left as is, but the following two parameters in the **<login-config>** element can be edited manually: **<auth-method>** and **<realm-name>**.

The **<auth-method>** parameter defines the authentication scheme to be used by the server. Supported values are “BASIC”, “NTLM” and “Negotiate”, where the latter is used for Kerberos v.5 authentication only. NTLM authentication over the Negotiate scheme is not supported.

The **<realm-name>** parameter defines the name of the realm presented in Basic authentication dialog prompts. The realm-name can be set to any custom realm name. Its function is purely cosmetic.

Servers that have been upgraded from older versions may have more than one **<login-config>** entry in the /WEB-INF/security-filter.xml file. In those cases, all those entries must be configured exactly the same.

Example: Configuring the security filter for Basic authentication with a custom realm name

```
<security-filter-config>

  <login-config>
    <auth-method>BASIC</auth-method>
    <realm-name>TIBCO Spotfire Analytics Server</realm-name>
  </login-config>

  ...

</security-filter-config>
```

Example: Configuring the security filter for NTLM authentication

```
<security-filter-config>

  <login-config>
    <auth-method>NTLM</auth-method>
    ...
  </login-config>

  ...

</security-filter-config>
```

Example: Configuring the security filter for Kerberos authentication

```
<security-filter-config>
```

```
<login-config>
  <auth-method>Negotiate</auth-method>
  ...
</login-config>

...

</security-filter-config>
```

Impersonation

The security-filter.xml file can also be used to set up Impersonation on the Spotfire Analytics Server. More information about this can be found in “Enabling Impersonation” on page 198.

5.2 Server Logging

5.2.1 Overview

The main purpose of logging is to aid in the detection, diagnosis and resolution of any problems the server experiences. Therefore, in the normal operation of the server, a very minimal amount of logging is enabled.

5.2.2 Log Configuration Files

You can determine what should be logged in the log files, by selecting a certain Log Configuration File. This configuration file will set the level of detail for the actual log files.

There are six "levels" of logging you can choose between, by selecting different Log Configuration Files:

- **log4j-minimal.properties** - The DecisionSite Log will only log errors, and the SQL Log will be deactivated.
- **log4j.properties** - The default setting. The DecisionSite Log will log warnings, errors and basic information. The SQL Log will log basic SQL information.
- **log4j-debug.properties** - The DecisionSite Log will log detailed debug information as well as warnings, errors and other detailed information. The SQL Log will log more detailed SQL information.
- **log4j-debug-soap.properties** - The DecisionSite Log will log detailed SOAP information in addition to all the debug information from log4j-debug.properties.

- **log4j-trace.properties** - This DecisionSite Log will log extremely low-level debug information including all the debug information from log4j-debug.properties.
- **log4j-trace-soap.properties** - This DecisionSite Log will log extremely low-level SOAP information including all the debug information from log4j-trace.properties.

Warning: Do not use the “Debug”, “Debug with SOAP”, “Trace” or “Trace with SOAP” modes for continuous server use, since it decreases the performance of the server, and also produces very large log files.

If you want to configure the logs in other ways than the above options let you, you can create your own Log Configuration File using standard Log4j syntax

(more info at <http://logging.apache.org/log4j/docs/documentation.html>).

Placing a new log4j configuration file with the name matching the pattern **log4j*.properties** in the <installation directory>/server/webapps/spotfire/WEB-INF/ directory, will cause it to appear in the drop-down list among the other Log Configuration Files and can thus be selected.

Note: When you reboot the server, the Log Configuration File will revert to the default selection. To set the default Log Configuration File to be used, modify the com.spotfire.logging.config.file parameter in the /WEB-INF/web.xml file.

For more information, see “/WEB-INF/web.xml” on page 110.

Console Debugging:

All levels of logging are also available in “Console Debugging” versions:

- **log4j-minimal-with-console.properties**
- **log4j-with-console.properties**
- **log4j-debug-with-console.properties**
- **log4j-debug-soap-with-console.properties**
- **log4j-trace-with-console.properties**
- **log4j-trace-soap-with-console.properties**

These should only be used temporarily when running the server in console mode. This will provide real-time logging in a console window.

Do NOT use these while running the Spotfire Analytics Server as a service, since this may rapidly create huge log files.

5.2.3 Log Files

Spotfire Analytics Server uses rolling logs, which means that when a log file gets too big it splits into several files. These are indexed by a number, (the higher the number, the older the log) and can be selected in the drop-down list in DecisionSite Administrator. When a rolled log file reaches a certain number it is deleted.

The log files are located in the <installation directory>/server/logs directory.

There are several log files that you can configure and view:

DecisionSite Log

Actual file located in <installation directory>/server/logs/**dss.log**.

This file logs all activity on the server except the events recorded in the DecisionSite Access Log and the DecisionSite Client Log. It includes the SQL log and a simplified version of the Access log. You can set the detail level of what this file shall log, by selecting different Log Configuration Files.

DecisionSite Access Log

Actual file located in <installation directory>/server/webapps/spotfire/administrator/**dssaccess.log**.

This file logs all logins and logouts from DecisionSite Clients to the Spotfire Analytics Server. It shows which user logged in/out and when. It is always enabled, and is unaffected by Log Configuration File settings.

In the same directory there is also a file called **dssaccess.sfs** which can be opened in TIBCO Spotfire DecisionSite Client for an easy analysis and overview. If you log in to DecisionSite Client with admin privileges, there is a menu item **Tools > Administration > Server Usage**. By clicking this, the **dssaccess.sfs** file will automatically be opened and displayed.

DecisionSite SQL Log

Actual file located in <installation directory>/server/logs/**sql.log**.

This file logs the SQL that is generated each time a user executes an information link. You can set the detail level of what this file shall log, by selecting different Log Configuration Files (below).

DecisionSite Client Log

Actual file located in <installation directory>/server/logs/**dssclient.log**.

This file logs information each time an unsupported client tries to log on to the Spotfire Analytics Server. The log entry will state the Operating System, Web browser version, etc. It is always enabled, and is unaffected by Log Configuration File settings.

Note: By default, the DecisionSite logs use standard ISO 8601 date format. If you prefer another date format you can edit the log4j-config files. For more information, see

<http://jakarta.apache.org/log4j/docs/index.html>.

DecisionSite Posters Log (posteraccess.log)

Actual file located in <installation directory>/server/logs/**posteraccess.log**.

This file logs an entry every time a user creates or opens a Poster. The format is: Timestamp; User; User IP; Command; GUID.

DecisionSite Visualization Services log

The file **RenderingService.log** is located in the installation directory of Visualization Services, by default C:\Program Files\Spotfire\VisualizationServices. The file logs information about any errors that might occur when Visualization Services renders the images used in DecisionSite Posters.

This file is not visible via DecisionSite Administrator; it can only be viewed via the local file system of the machine running Visualization Services.

DecisionSite Soap (soap.log)

This log stores information about the SOAP communication on the server.

Server Diagnostics

Actual file located in <installation directory>/server/logs/**server-diagnostics.log**

This log is always enabled and contains diagnostics information collected during server startup. It shows whether or not the server could be started successfully and other vital information collected from various parts of the server. This log is always enabled and unaffected by Log Configuration File settings.

Server Access

Actual file located in <installation directory>/server/logs/**access.log**

This log is always enabled and contains all access attempts to the Spotfire Analytics Server. It shows which user has accessed what files on the server, when the access took place, and whether or not the access was granted. In normal mode, this file does not log login ticket refresh requests from TIBCO Spotfire DecisionSite clients. It uses standard "W3C common logfile format".

Server Usage

Actual file located in <installation directory>/server/logs/**usage.log**.

This file is a lighter alternative to the access log described above as it does not contain information regarding the file accessed. Besides that, the two files contain the same information. This log is always enabled and unaffected by Log Configuration File settings.

Server Axis (dss-axis.log)

This file logs the Axis SOAP tool from Apache.

Tomcat StdOut Log

Actual file located in <installation directory>/server/logs/**stdout_YYYYMMdd.log**, where YYYYMMdd is replaced by the log file's creation date.

The Tomcat application server redirects all output to StdOut to this log file. Note: By default, this log file is not rolled.

Tomcat StdErr Log

Actual file located in <installation directory>/server/logs/**stderr_YYYYMMdd.log**, where YYYYMMdd is replaced by the log file's creation date.

The Tomcat application server redirects all output to StdErr to this log file. Note: By default, this log file is not rolled.

Jakarta Service Log

Actual file located in <installation directory>/server/logs/**jakarta_service_YYYYMMdd.log**, where YYYYMMdd is replaced by the log file's creation date.

This log file contains information about when the Tomcat service is started and stopped.

isusage.log Log

Actual file located in <installation directory>/server/logs/**isusage.log**.

This log file contains information about what user accesses which Information Link and when.

library.log Log

Actual file located in
<installation directory>/server/logs/library.log.

This log file logs whenever a user stores, opens or deletes a file from the library.

5.2.4 Installation Log for Packages on the DecisionSite Client

This log is not a server log as such, but is listed here for sake of completeness. It is a log for DecisionSite Client, and is found on each end-user machine.

Packages are installed using Spotfire.PackageManager. The installer engine operates silently in most situations. Generally problems with installation, uninstallation, upgrade or local registration can be diagnosed with this log of events prior to the problem.

If the user has sufficient privileges all information will be stored per machine. Default Locations:

%PROGRAMFILES%\Spotfire\Packages\

%USERPROFILE%\Local Settings\Application Data\

Spotfire\Packages\

The log contains:

- Timestamp (Format: YYYY-MM-DD hh:mm:ss)
- Operation (install, uninstall, upgrade, register, restore, repair)
- Status (ok, failed, retry)
- Package name
- Package version
- Scope (machine, user)
- Path
- User name
- Machine name
- Engine version
- Details

6 Configuration Procedures

6.1 Changing Login System

6.1.1 Preparations

6.1.1.1 Backup Configuration Files

Before changing login system, make sure to backup the following configuration files:

- <server install dir>\server\webapps\spotfire\WEB-INF\web.xml
- <server install dir>\server\webapps\spotfire\WEB-INF\userdirconfig.xml
- <server install dir>\jdk\jre\lib\security\spotfire.login

6.1.1.2 Backup Database

Before changing login system, make sure to perform a backup of the server's database tables.

6.1.2 Changing to Database Table Login System

When changing to a Database Table login system, the following files must be modified:

- <server install dir>\server\webapps\spotfire\WEB-INF\web.xml
- <server install dir>\jdk\jre\lib\security\spotfire.login

Note: The Database Table login system can only be combined with a Database Table user directory back-end.

6.1.2.1 Edit the authenticator.class Parameter in web.xml

Locate the authenticator.class parameter in the <server install dir>\server\webapps\spotfire\WEB-INF\web.xml file and change the value to "com.spotfire.server.security.JAASAuthenticator". The "com.spotfire.server.security.JAASRegisteringAuthenticator" is not supported for use with the Database Table login system.

The configuration should now look like this:

```

<web-app>

...

<context-param>
  <param-name>authenticator.class</param-name>
  <param-value>com.spotfire.server.security.JAASAuthenticator</param-value>
</context-param>

...

</web-app>

```

6.1.2.2 Edit the authenticator.configuration parameter in web.xml

Locate the authenticator.configuration parameter in the <server install dir>\server\webapps\spotfire\WEB-INF\web.xml file and change the value to “SpotfireDBLogin”.

The configuration should now look like this:

```

<web-app>

...

<context-param>
  <param-name>authenticator.configuration</param-name>
  <param-value>SpotfireDBLogin</param-value>
</context-param>

...

</web-app>

```

6.1.2.3 Review the SpotfireDBLogin configuration in spotfire.login

Make sure the file <server install dir>\jdk\jre\lib\security\spotfire.login contains no database connection parameters. If present, remove the **dbDriver**, **dbURL**, **dbUser** and **dbPassword** parameters. Using these parameters in the spotfire.login file is deprecated.

Corrected example:

```

SpotfireDBLogin
{
    com.spotfire.server.jaas.dblogin.DBLoginModule
        required;
};

```

6.1.2.4 Assign Passwords

Since the Database Table login system verifies the passwords provided by the users at login against password hashes stored in the database, all users existing prior to the login system switch must be given new passwords.

If only a few users are affected, this can be done manually by using the Spotfire administration tools. However, this approach requires a new administrator account to be created, since none of the old administrator accounts won't be able to login either.

If a large number of users are affected, they can be given default passwords by running an SQL command in the database.

- 1 Start sqlplus (for an Oracle database), sqlcmd (for a Microsoft SQL Server database) or your preferred database tool and log in to the database. Use the account and database specified in the Server.Default data source in the <server installation>\server\webapps\spotfire\WEB-INF\data-sources.xml file.
- 2 For an Oracle database server, run the following SQL commands:

```
UPDATE USERS SET PASSWORD = CHR(16) || CHR(16) || '8iaByxiChEJ464jHbh7TEgWWCW8='
WHERE PASSWORD IS NULL;
COMMIT;
```

For a Microsoft SQL Server database, run the following SQL commands:

```
UPDATE USERS SET PASSWORD = NCHAR(16) + NCHAR(16) + '8iaByxiChEJ464jHbh7TEgWWCW8='
WHERE PASSWORD IS NULL;
COMMIT;
```

- 3 Disconnect from the database.
- 4 All users that previously had no password will now have the default password "spotfire".

6.1.2.5 Change to Database Table User Directory Back-end

When the login system has been changed, proceed to the instructions for changing to a Database Table user directory back-end in section “Changing to Database Table User Directory Back-end” on page 179. The Database Table login system cannot work with other back-ends.

6.1.2.6 Restart the Server

Finally, restart the Spotfire Analytics Server (see “Starting the Spotfire Analytics Server” on page 105).

6.1.3 Changing to Microsoft Windows NT Domain Login System

When changing to a Microsoft Windows NT Domain login system, the following files must be modified:

- <server install dir>\server\webapps\spotfire\WEB-INF\web.xml
- <server install dir>\jdk\jre\lib\security\spotfire.login

Note: The Microsoft Windows NT Domain login system can only be combined with a Microsoft Windows NT Domain or a Database Table user directory back-end.

Note: The Microsoft Windows NT Domain login system and user directory back-end can only be used on machines running a supported Windows operating system.

6.1.3.1 Edit the authenticator.class parameter in web.xml

Locate the authenticator.class parameter in the <server install dir>\server\webapps\spotfire\WEB-INF\web.xml file and change the value to “com.spotfire.server.security.JAASAuthenticator”. If the Microsoft Windows NT Domain login system is used with a Database Table user directory back-end, the “com.spotfire.server.security.JAASRegisteringAuthenticator” option can also be used. For more information see “/WEB-INF/web.xml” on page 110.

The configuration should now look like this:

```
<web-app>
```

```
...
```

```
<context-param>
```

```
<param-name>authenticator.class</param-name>
```

```
<param-value>com.spotfire.server.security.JAASAuthenticator</param-value>
```

```
</context-param>
```

```
...
```

```
</web-app>
```

or

```
<web-app>
```

```
...
```

```
<context-param>
```

```
<param-name>authenticator.class</param-name>
```

```
<param-value>com.spotfire.server.security.JAASRegisteringAuthenticator</param-value>
```

```
</context-param>
```

```
...  
</web-app>
```

6.1.3.2 Edit the authenticator.configuration parameter in web.xml

Locate the authenticator.configuration parameter in the <server install dir>\server\webapps\spotfire\WEB-INF\web.xml file and change the value to “SpotfireWindows”.

The configuration should now look like this:

```
<web-app>  
  
...  
  
<context-param>  
  <param-name>authenticator.configuration</param-name>  
  <param-value>SpotfireWindows</param-value>  
</context-param>  
  
...  
</web-app>
```

6.1.3.3 Update the SpotfireWindows configuration in spotfire.login

Open the file <server install dir>\jdk\jre\lib\security\spotfire.login and edit the SpotfireWindows configuration. The domains parameter should contain a comma-separated list of the Windows **domains** containing the user accounts. For more detailed information about the parameters see “/jdk/jre/lib/security/spotfire.login” on page 114.

Example:

```
SpotfireWindows  
{  
  
  com.spotfire.server.jaas.win.WinLoginModule  
    required  
    domains="engineering, sales";  
  
};
```

6.1.3.4 Change the User Directory Back-end

The Microsoft Windows NT Domain login system requires either a Microsoft Windows NT Domain or a Database Table user directory

back-end. If necessary, proceed to the instructions for changing to a Microsoft Windows NT Domain user directory back-end in section “Changing to Microsoft Windows NT Domain User Directory Back-end” on page 180, or a Database Table user directory back-end in section “Changing to Database Table User Directory Back-end” on page 179.

6.1.3.5 Restart the Server

Finally, restart the Spotfire Analytics Server (see “Starting the Spotfire Analytics Server” on page 105).

6.1.4 Changing to LDAP Login System

When changing to an LDAP login system, the following files must be modified:

- <server install dir>\server\webapps\spotfire\WEB-INF\web.xml
- <server install dir>\jdk\jre\lib\security\spotfire.login

Note: The LDAP login system can only be combined with an LDAP or a Database Table user directory back-end.

6.1.4.1 Edit the authenticator.class parameter in web.xml

Locate the authenticator.class parameter in the <server install dir>\server\webapps\spotfire\WEB-INF\web.xml file and change the value to “com.spotfire.server.security.JAASAuthenticator”. If the LDAP login system is used with a Database Table user directory back-end, the “com.spotfire.server.security.JAASRegisteringAuthenticator” option can also be used. Consult the reference documentation for the web.xml file for more information. See “/WEB-INF/web.xml” on page 110.

The configuration should now look like this:

```
<web-app>

...

<context-param>
  <param-name>authenticator.class</param-name>
  <param-value>com.spotfire.server.security.JAASAuthenticator</param-value>
</context-param>

...

</web-app>
```

or

```
<web-app>

...

<context-param>
  <param-name>authenticator.class</param-name>
  <param-value>com.spotfire.server.security.JAASRegisteringAuthenticator</param-
value>
</context-param>

...

</web-app>
```

6.1.4.2 Edit the authenticator.configuration parameter in web.xml

Locate the authenticator.configuration parameter in the <server install dir>\server\webapps\spotfire\WEB-INF\web.xml file and change the value to “SpotfireLDAP”.

The configuration should now look like this:

```
<web-app>

...

<context-param>
  <param-name>authenticator.configuration</param-name>
  <param-value>SpotfireLDAP</param-value>
</context-param>

...

</web-app>
```

6.1.4.3 Update the SpotfireLDAP configuration in spotfire.login

Open the file <server install dir>\jdk\jre\lib\security\spotfire.login and edit the SpotfireLDAP configuration. The configuration should contain proper values for the following parameters: **serverURL**, **contextNames**, **user**, **password**, **nameAttribute** and **userFilter**. For more detailed information on these parameters, see “/jdk/jre/lib/security/spotfire.login” on page 114.

Example:

```
SpotfireLDAP
{

    com.spotfire.server.jaas.ldap.LDAPLoginModule
        required
        serverURL="ldap://engr-dc:389"
        contextNames="OU=Engineering,DC=example,DC=com"
```

```

user="hagbard"
password="ifkbg04"
nameAttribute="sAMAccountName"
userFilter="(objectClass=user)";

};

```

6.1.4.4 Change the User Directory Back-end

The LDAP login system requires either an LDAP or a Database Table user directory back-end. If necessary, proceed to the instructions for changing to an LDAP user directory back-end in section “Changing to LDAP User Directory Back-end” on page 182, or a Database Table user directory back-end in section “Changing to Database Table User Directory Back-end” on page 179.

6.1.4.5 Restart the Server

Finally, restart the Spotfire Analytics Server (see “Starting the Spotfire Analytics Server” on page 105).

6.1.5 Changing to Windows Integrated Authentication (NTLM)

6.1.5.1 Client Configuration

Setting up the Spotfire Analytics Server to use Windows Integrated Authentication (NTLM) will allow the users to log into Microsoft Windows using their regular Windows username and password, and when launching DecisionSite Client or Spotfire they will automatically use the same security credentials when connecting to the Spotfire Analytics Server.

The Windows Integrated Authentication (NTLM) mechanism uses the automatic log in of Internet Explorer, which enables automatic reuse of the Windows authentication for the local intranet zone.

On many networks NTLM will not require any further configuration of the clients to work, but in some cases you will need to make the following adjustments.

► **Setting up Internet Explorer options:**

- 1 Open Internet Explorer.
- 2 Select **Tools > Internet Options > Security > Local intranet > Sites > Advanced**.

- 3 Add the machine running the Spotfire Analytics Server here, that is `http://machinename.domain`
- 4 Select **Tools > Internet Options > Security > Local intranet > Custom Level**.
- 5 Under **User Authentication > Logon** select the radio button **"Automatic Logon only in Intranet zone"**.

6.1.5.2 Server Configuration

Setting up the server to use Windows Integrated Authentication (NTLM) will allow the users to log into Microsoft Windows using their regular Windows username and password, and when launching DecisionSite Client or Spotfire they will automatically use the same security credentials when connecting to the Spotfire Analytics Server.

Note: If a user attempts to log in to the Spotfire Analytics Server from another Windows Domain, he or she will be asked to provide a Windows domain, username, and password, since the server is on another domain.

Performance

NTLM makes use of a built in mechanism in Windows, which requires more frequent reauthentication. For every reauthentication a call is made to the domain controller, which will mean some extra performance cost. Spotfire is not as affected by this as DecisionSite Client.

Note: When creating users in DecisionSite Administrator, there will still be a password field. This field can be set to anything, as it is ignored. The password given here will only be used if one later reverts back to basic authentication. If one want to revert back it might be a good idea to reset all passwords to a standard value, see "assign standard password for all users".

Authentication and User Directory

NTLM authentication extracts a username, which is used towards the ordinary Spotfire Analytics Server user directory, that is, Database, LDAP, or Windows user directories. The login alias from the current windows login is extracted and must exist in the user directory if that mechanism is used.

Example: If your name is John Doe and you log in to the Windows client machine as johnd, then johnd is the username that is extracted and expected to exist in the user directory database, in LDAP, or in Windows.

NTLM requires that the Windows domain controller has been configured to support NTLM. Once the domain controller has been configured to support NTLM, there are certain things on the Spotfire Analytics Server that needs to be set up.

The following Java startup parameters must be set:

- **jcifs.smb.client.domain** - The windows domain.
- **jcifs.http.domainController** - The domain controller for the Windows domain, preferably given as an IP number.
- **jcifs.smb.client.username** - A user defined in the domain controller, used by the server to log into the domain controller to check the login identities.
- **jcifs.smb.client.password** - The password for the above user.

► **To Set Up the Start Script (not running as a service):**

Open the file <server install dir>/bin/catalina.bat in a text editor.

Add the following entries to the JAVA_OPTS entry

-Djcifs.smb.client.username=<username>

-Djcifs.smb.client.password=<password>

-Djcifs.smb.client.domain=<mycompany.com>

-Djcifs.http.domainController=<domaincontroller>

► **To Set Up the Service (when running as a service):**

Go to the <server install dir>\bin\

Run service.bat remove

Edit the <server install dir>\bin\service.bat

Look for “JvmOptions”, where this occurs, add the following entries as well

-Djcifs.smb.client.username=<username>

-Djcifs.smb.client.password=<password>

-Djcifs.smb.client.domain=<mycompany>

-Djcifs.http.domainController=<domaincontroller>

Run <server install dir>\bin\service.bat install

► **Alter Configuration Files**

Next you need to alter some files. Make a backup of these before editing them.

Edit the file:

```
<server install dir>\webapps\spotfire\WEB-INF\security-filter.xml
```

For every occurrence of the "auth-method" node alter this to:

```
<auth-method>NTLM</auth-method>
```

To ensure that the client understands that it should use NTLM edit the file:

```
<server install dir>\webapps\spotfire\WEB-INF\manifest.xml
```

Alter the node authentication-modes to read:

```
<manifest>
...
<server-info>
  <authentication-modes>
    <integrated-authentication/>
  </authentication-modes>
</server-info>
</manifest>
```

Debug Hints:

If things don't work as expected here are a couple of hints.

- Give -Djcifs.http.domainController as an IP number.
- To get plenty of debug information add "-Djcifs.util.loglevel=10" to JAVA_OPTS.

This will log to stderr. To view this it is easiest to start the application server from a command line prompt.

- It is possible to still be prompted for user and password, this will allow login as another user. Also, a valid Windows domain login is needed here.

In Internet Explorer select

Tools > Internet options > Security > Custom level > User authentication > Logon to prompt for username and password

Another way to run as a different user, even if NTLM is activated is to start the Internet Explorer or DecisionSite Client.

To run as the user foo in the domain BAR you can start Internet Explorer like this (the exact path may be different):

```
C:\>runas /user:BAR\foo "c:\Program Files\Internet Explorer\iexplore.exe"
```

Likewise for the client (again the exact path might be different):

```
C:\>runas /user:BAR\foo "c:\Program  
Files\Spotfire\DecisionSite\Program\Spotfire.exe"
```

or

```
C:\>runas /user:BAR\foo "c:/Program Files/TIBCO/Spotfire/2.1/  
Spotfire.Dxp.exe"
```

- You might get a different behavior if you connect to <http://machinename> than <http://machinename.foo.com> (the latter might not be recognized as the Local Intranet, if so add the machine with the full domain name, see above).

6.1.6 Configuring SSL Support

6.1.6.1 Introduction

HTTPS (HyperText Transfer Protocol Secure) means that the communication between the client and server is encrypted.

The application server can be configured to use HTTPS. In order to encrypt the communication, the server needs a certificate with a private key, which is used to present the identity of the server to connecting clients.

With a correct certificate on the server side the communication can be encrypted. This is the most common case when surfing on the internet, that is, using server side certificates only. But to increase security certificates can be issued to the clients as well. If certificates are issued to all clients then the server can be configured to reject requests without a valid client certificate. If client certificates are required the server can be configured either to require username and password as usual, or it can be configured to use identity information from the client's certificate as login information, the user will not be prompted for username and password.

The server can be set up to use HTTPS and Certificates in the above mentioned three degrees:

HTTPS with Server Certificate

The server is configured to use HTTPS and a Server Certificate to encrypt the communication. The users will log in to Spotfire Analytics Server with username and password. The connection is encrypted.

HTTPS and Client Certificates with Basic Authentication

Requires the above step. Additionally each client is setup to use an individual client certificate which must be present to log in to the Spotfire Analytics Server. The user will still need to log in to the client using his username and password.

HTTPS and Client Certificates with Automatic Login

Requires the above two steps. Additionally the server is configured to use identity information from the client's certificate as login information, so the user will not be prompted for username and password.

Performance

Creating an encrypted connection requires more CPU cycles than doing an ordinary socket connection. This overhead will reduce the maximum capacity and increase latency.

6.1.6.2 HTTPS with Server Certificate

Obtaining a Server Certificate

The application server must have access to a correctly issued certificate. Such a certificate can be obtained from different vendors, or might be issued within companies. The server needs the certificate on JKS (Java Keystore) format.

Here is an example of the steps necessary to issue a certificate using Microsoft Certificate Server. This is an example only. It is fairly complex, intended for the power user. Try to obtain suitable certificates through the ordinary channels first.

► Example - Getting the Private Certificate Using Microsoft Certificate Services:

- 1 Start Internet Explorer.
- 2 Connect to your Active Directory Certificate Service homepage, for example, **http://<certificate server machine>/certsrv/**
- 3 Select **Request a certificate... > Advanced Request > Submit a certificate request to this CA using a form.**
- 4 Enter **username** and **e-mail**.
Note: As username use the machine name of the server, i.e. what a client will use to connect to: **http://<machine-name>**.
- 5 Mark **Purpose as Server Authentication Certificate**.
- 6 Mark **Key as Exportable** (but do not check Export Key to File).

- 7 Click **Submit** and acknowledge that a certificate is being requested.
- 8 Open the **Certification Authority** application on the machine where the Certificate Server is installed.
- 9 Select **Certification Authority > Test > Pending requests**, where a pending request should be available.
- 10 Mark the request, right-click and select **All tasks > Issue**.

Response: The new certificate should now be visible under "Issued Certificates".

- 11 Close the application.
- 12 Connect to your Active Directory Certificate Service homepage, for example, **http://<certificate server machine>/certsrv/** from the local computer using Internet Explorer.
- 13 Select **Check on a pending certificate > Next**.

Response: A page with the text "Check On a Pending Certificate Request" and "Please Select the Certificate Request You Want to Check" is displayed.

- 14 Select the Certificate and click **Next**.

Response: A page with the text "Certificate Issued / The certificate you requested was issued to you." is displayed.

- 15 Select **Install this certificate > Yes > Yes**.

Response: A page confirming that the certificate is installed is displayed.

- 16 In Internet Explorer, select **Tools > Internet Options**.

- 17 Select the **Content** tab.

- 18 Click the **Certificates** button.

- 19 Mark the certificate that was issued to you.

- 20 Click **Export > Next > Yes, export the private key > Next**.

- 21 Check **Include all certificates**.

Comment: There is no need to select "Enable strong protection".

- 22 Select **Next**.

- 23 Enter **password** for the file.

- 24 Specify where the key should be saved.

25 Select **Next > Finish**.

Comment: It is now ok to delete the certificate from Internet Explorer.

► **Example - Converting the Certificate to a Format Suitable for the Application Server:**

Next the certificate might need to be transformed to JKS format, which can be used by the application server.

If you follow the example above with the Microsoft Certificate Services you will get a certificate on PKCS12 format. This needs to be converted. One way of doing this is to use the PKCS12Import Java utility, for example, which is found in the Jetty web server distribution. To find this search the internet for “Jetty” and “webserver”.

This needs to be downloaded and possibly compiled.

Next the certificate created above should be converted. Enter the file name for the certificate created above (for example in.pfx) and a suitable name for the result file (for example out.jks).

Example:

```
java -cp lib\jetty-6.1.7.jar org.mortbay.jetty.security.PKCS12Import in.pfx out.jks
```

You need to enter the password for the input certificate and for the resulting Java keystore. Make sure to note the alias that is printed when this command is performed, as it will be needed later. (The skilled user can modify the program to get a shorter alias.)

Configuring the Server to use SSL

Edit the <server install dir>/server/conf/server.xml file and replace (or add) a connector node

```
<Connector port="443"
maxHttpHeaderSize="16384"
maxThreads="150"
minSpareThreads="25"
maxSpareThreads="75"
enableLookups="false"
disableUploadTimeout="true"
acceptCount="100"
scheme="https"
secure="true"
SSLEnabled="true"
clientAuth="false"
sslProtocol="TLS"
keystoreFile="<path to server's private certificate>"
keystorePass="spotfire"
keystoreType="JKS" />
```

Restart the server.

Note: Verify that you can connect to the Spotfire Analytics Server using https, that is, `https://<mySpotServer>`. You should get a warning that the certificate is not trusted.

6.1.6.3 Getting and Installing a Trusted Certificate

Even if the server does not require client certificates it is advisable to configure the certificates the server should trust.

► **Example - Retrieving the Trusted Certificate from Microsoft Certificate Services:**

- 1 Connect to your Active Directory Certificate Service homepage, for example, `http://<certificate server machine>/certsrv/`
- 2 Select **Retrieve the CA certificate or certificate revocation list (CRL)**.
- 3 Select **Base64 encoded** and **Download CA certificate**.
- 4 Select **Save** and specify a name for the file.
- 5 The key certificate needs to be imported into the trust keystore.

```
<server install dir>\jdk\bin\keytool.exe -importcert -v
-file <cert_file.cer>
-keystore <server install dir>\jdk\jre\lib\security\cacerts
```

Note: If only one issuer of certificates should be trusted the keystore `<server install dir>\jdk\jre\lib\security\cacerts` needs to be emptied of other certificates. See the documentation for the keytool command.

6.1.6.4 Client Configuration, Making the Server's Certificate Trusted

When a browser is directed to the server, pop-up windows may appear, which asks if this server is to be trusted. To get rid of these prompts the issuer of the server certificate needs to be identified as a Certificate issued by a trusted authority. These instructions need to be performed for all clients.

► **Example - Installing the Trusted Certificate to the Client using Microsoft Certificate Services:**

- 1 Connect to your Active Directory Certificate Service homepage, for example, `http://<certificate server machine>/certsrv/` with Internet Explorer.
- 2 Select **Retrieve the CA certificate or certificate revocation list** > **Next**.

- 3 Click on the link **Install this CA certification path > Yes > Yes**.

Note: Verify that you can connect to the Spotfire Analytics Server using https and that the client and server trusts each other without producing warnings.

6.1.7 HTTPS and Client Certificates with Basic Authentication Login

6.1.7.1 Introduction

It is possible to use client certificates in the Spotfire environment as well. The server can be configured to require these certificates. It can be used as an extra security layer and still require the ordinary login (username and password) once connected. If the client does not have a good certificate the server will simply reject the calls.

Client certificates can also be used to authenticate the user (see next chapter).

A prerequisite for Client Certificates is that the server has been set up with server certificate and trust (see previous chapter). The latter is used to decide if a client certificate should be allowed or rejected.

Example - Configuring the Client Installing a Certificate using Microsoft Certificate Services:

► **Request a Certificate:**

- 1 Connect to your Active Directory Certificate Service homepage, for example, **http://<certificate server machine>/certsrv/** using Internet Explorer.
- 2 Request a certificate of the type “Client Authentication Certificate”.

Comment: If the certificate is used as the only authentication method the username is used as the identity. If the user directory is using windows authentication, then this should be the shorter alias, e.g., not "John Doe", but "johnd".

► **Issue the Certificate:**

- 1 Open the **Certification Authority** application on the machine running the Certificate Services.
- 2 Select **Certification Authority > Test > Pending requests**, where a pending request should be available.
- 3 Mark the request, right-click and select **All tasks > Issue**.

Response: The new certificate should now be visible under Issued Certificates.

- 4 Close the application.

► **Install the Certificate:**

- 1 Connect to your Active Directory Certificate Service homepage, for example, **http://<certificate server machine>/certsrv/** from the client computer.
- 2 Select **Check on a pending certificate > Next**.
- 3 Verify that a Client Authentication certificate is selected.
- 4 Click **Next**.

Response: A page with the text "Certificate Issued/The certificate you requested was issued to you." is displayed.

- 5 Select **Install this certificate**.
- 6 Select **Yes** in the confirmation dialogs.

Response: A page confirming that the certificate is installed is displayed.

► **Optional IE Settings:**

- 1 Internet Explorer might provide you with a selection box which lets you specify which certificate is to be used. To be rid of these certificate selection boxes, **Open Tools > Internet Options** in Internet Explorer.

Note: This works if there is only one matching certificate, thus if there is more than one certificate which can be used by the server, there will still be selection dialogues.

- 2 Select the **Security** tab.
- 3 Select **Local Intranet**.
- 4 Click **Sites > Advanced**.
- 5 Add **https://<server machine name>** to the list of hosts in this zone.
- 6 Click **OK**.
- 7 Select **Custom level** for the Intranet zone security settings.
- 8 Make sure that **Don't prompt for client certificate selection when no certificates or only one certificate exists** is **Enabled**.
- 9 Click **OK** and confirm that the security settings should be changed.

6.1.7.2 Configure the Server

- ▶ **To configure the application server to require client certificates:**

Assuming that Basic Authentication is selected already all that is needed is to alter in the communication layer. Follow the instructions in “Configuring SSL Support” on page 167. Then continue and

- 1 Edit the <server install dir>/server/conf/server.xml file, which was created in section “Configuring the Server to use SSL” on page 170

Edit the node `clientAuth="false"` and set it to
`clientAuth="true"`

- 2 Restart the server (see “Starting the Spotfire Analytics Server” on page 105).

Note: Verify that you can only connect to the Spotfire Analytics Server if the client has a valid certificate installed.

6.1.8 HTTPS and Client Certificates with Automatic Login

Client certificates can also be used to authenticate the user. In this case the common name ("CN") information from the certificate is used as the username. (If it is a certificate chain, then the first certificate in the chain will be used).

A prerequisite is that client certificates are enforced (see previous section, “HTTPS and Client Certificates with Basic Authentication Login” on page 172).

The client certificates can be used both as an extra security layer and as a way to achieve single sign on, that is, the user's identity is retrieved from the certificate, and that certificate is issued by a trusted certificate authority is sufficient proof of identity.

Note: When creating users in DecisionSite Administrator, there will still be a password field. This field can be set to anything, as it is ignored. The password given here will only be used if one later reverts back to basic authentication. If one wants to revert back it might be a good idea to reset all passwords to a standard value, see "assign standard password for all users".

- ▶ **To configure single sign on using certificates:**

- 1 Edit the file <server install dir>/server/webapps/spotfire/WEB-INF/security-filter.xml.

- 2 For every occurrence of the <auth-method> node alter this to:

```
<auth-method>CLIENT-CERT</auth-method>
```

- 3 To ensure that the client understands that it should use certificates, edit the file:

```
<server install dir>/server/webapps/spotfire/WEB-INF/manifest.xml
```

- 4 Find the following node:

```
<server-info>
<authentication-modes>
  <username-and-password/>
</authentication-modes>
</server-info>
```

- 5 Replace the <username-and-password/> tag with <client-certificate/>.

```
<server-info>
<authentication-modes>
<client-certificate/>
</authentication-modes>
</server-info>
```

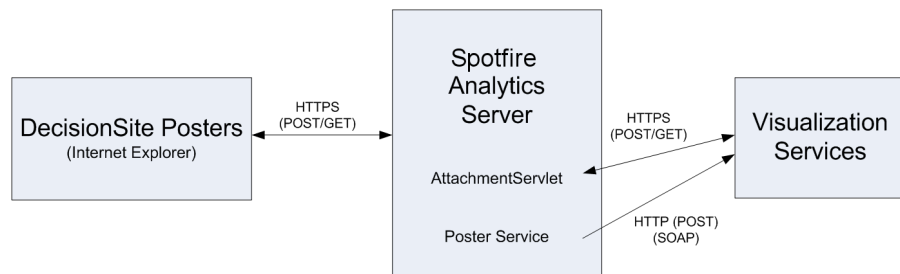
Restart the server (see “Starting the Spotfire Analytics Server” on page 105).

Note: Verify that automatic login to the Spotfire Analytics Server works when launching the client. If you have several certificates installed on the client machine, you should be prompted to choose which certificate to use.

6.1.9 HTTPS in Visualization Services

6.1.9.1 Communication

The basic communication between the DecisionSite Poster (Internet Explorer), the Spotfire Analytics Server and Visualization Services is described in the picture below.



The DecisionSite Poster only communicates with the Spotfire Analytics Server, thus if the Spotfire Analytics Server is set up to use HTTPS, all communication will be via HTTPS.

The Spotfire Analytics Server and Visualization Services communicate via two different channels.

- 1 The Poster Service (part of the Spotfire Analytics Server) calls Visualization Services via HTTP POST (Soap).

Note: This part is communicating via HTTP.

- 2 Visualization Services communicates with the attachment part of the Spotfire Analytics Server using both POST and GET. This part is communicating via HTTPS.

Note that in order to use HTTPS for DecisionSite Posters, the client machine needs to run Internet Explorer 6.0 or later.

6.1.9.2 Recommended Configurations

There are essentially two different configurations:

No Client Certificates Required

No adjustments or additional installation has to be made to Visualization Services.

Client Certificates Required

To run Visualization Services and a Spotfire Analytics Server that requires client certificates, some configurations must be made:

- A valid client certificate must be installed on the machine running Visualization Services.
- Microsoft Web Service Enhancements must be installed on the machine running Visualization Services.
- The Visualization Services configuration file must be edited.
- Visualization Services must run from a user account, not as Local System.

► **To Set up Visualization Services with HTTPS and Client Certificates:**

- 1 Retrieve a valid client certificate and install it on the machine running Visualization Services. To verify that certificate is installed correctly the following page should be accessible from Internet Explorer:

`https://[servername]:[port]/spotfire/ws/servlet/attachmentservlet`

The text "AttachmentServlet up and running" should appear in the resulting page.

- 2 Download Web Services Enhancements (WSE) 2.0 SP2 for Microsoft .NET Redistributable Runtime MSI from <http://www.microsoft.com/downloads/details.aspx?FamilyID=d3c8f18b-7bbf-489d-90e1-e8d4147205b8&DisplayLang=en> and install it on the machine running Visualization Services.

Note: The system requirements for WSE 2.0 states that Microsoft IIS is required for certain parts of the WSE 2.0. However, the parts that Visualization Services use do not require IIS.

- 3 Open the configuration file InstallDir/SpotfireRenderingService.exe.config and uncomment the rows containing:

```
<add key="HttpsUseClientCertificates" value="true" />
```

```
<add key="HttpsStoreLocation" value="CurrentUser" />
```

```
<add key="HttpsStore" value="My" />
```

- 4 Make sure that Visualization Services is running from the same user account as the client certificate was installed for. This is done by editing the properties for Visualization Services:

- Select **Start > Control Panel > Administrative Tools > Services**.

- Select the Spotfire DecisionSite Visualization Services service, right-click on it and select **Properties**.

- Select the **Log On** tab.

- Enter the account that should be used.

- 5 Restart Visualization Services, by clicking the **Stop** button and the **Start** button.

6.1.9.3 Technical Configuration Details

Note that in order to use HTTPS for DecisionSite Posters, the client machine needs to run Internet Explorer 6.0 or later.

Accepting all server certificates

When the server presents its certificate to the user in normal web browsing, a dialog is shown in which the user can select to either accept or decline the certificate. In web services communication no dialog can be shown. Therefore all server certificates are accepted.

Client certificates

If client certificates are required, **all** certificates from a certain certification store and store location (on the local machine) are appended to the request. This means that a valid client certificate must be installed on the machine (either for a user running the windows

service or on the local machine account). For more information see the Configuration Details chapter below.

Configuration

HTTPS configuration is setup via the Visualization Services configuration file (<Installation Directory>/SpotfireRenderingService.exe.config).

Configuration file

The configuration file of the Rendering Service (<Installation Directory>/SpotfireRenderingService.exe.config) controls how HTTPS communication is performed in Visualization Services. The following properties are available to configure:

HttpsUseClientCertificates

Controls whether or not client certificates should be used. Defaults to false.

HttpsStoreLocation

Controls which certificate store location to use Defaults to LocalMachine. Possible values are:

- **LocalMachine**. Certificate store for the local computer (default).
- **CurrentUser**. Certificate store for the currently logged-on user.
- **CurrentService**. Certificate store for the current service.
- **Services**. Certificate store for a specified service account.
- **CurrentUserGroupPolicy**. Certificate store for the currently logged-on group.
- **LocalMachineEnterprise**. The certificate store for the local machine enterprise downloaded from a network setting.
- **LocalMachineGroupPolicy**. The certificate store for the local machine group policy downloaded from a network setting.
- **Unknown**. The location is unknown.
- **Users**. Certificate store for the users group of this computer.

HttpsStore

Controls the store in which certificates will be looked for. Defaults to My (Personal store). Possible values are:

- **My** The personal store (default)
- **CA** Certificate Authorities
- **Root** store (Trusted Root Certificates)

- **Trust** Trusted publishers
- **Disallowed** Untrusted Certificates

6.2 Changing User Directory Back-end

6.2.1 Preparations

6.2.1.1 Backup Configuration Files

Before changing user directory back-end, make sure to backup the following configuration file:

- `<server install dir>\server\webapps\spotfire\WEB-INF\userdirconfig.xml`

6.2.1.2 Backup Database

Before changing user directory back-end, make sure to perform a backup of the server's database tables.

6.2.2 Changing to Database Table User Directory Back-end

The Database Table user directory back-end can be used with any login system on any operating system.

6.2.2.1 Edit the `<external-directory-provider>` parameter in `userdirconfig.xml`

Locate the `<external-directory-provider>` parameter in the `<server install dir>\server\webapps\spotfire\WEB-INF\userdirconfig.xml` file and make sure its empty.

Example:

```
<userdir>
...
<external-directory-provider/>
...
</userdir>
```

or

```
<userdir>
...
<external-directory-provider></external-directory-provider>
...
</userdir>
```

6.2.2.2 Edit the <external-group-synchronization> parameters in userdirconfig.xml

The Database Table user directory back-end does not support synchronization of external groups. Locate the **<external-group-synchronization>** parameter in the <server install dir>\server\webapps\spotfire\WEB-INF\userdirconfig.xml file and set the value of the **<enabled>** child element to “false”.

Example:

```
<userdir>
...
<external-group-synchronization>
  <enabled>false</enabled>
  <sleep-time>60</sleep-time>
</external-group-synchronization>
...
</userdir>
```

6.2.2.3 Restart the Server

Finally, restart the Spotfire Analytics Server (see “Starting the Spotfire Analytics Server” on page 105).

6.2.3 Changing to Microsoft Windows NT Domain User Directory Back-end

The Microsoft Windows NT Domain user directory back-end can be combined with the Microsoft Windows NT Domain, NTLM, Kerberos and X.509 Certificates login systems on any supported Windows operating system. It not supported on Solaris.

6.2.3.1 Edit the <external-directory-provider> parameter in userdirconfig.xml

Locate the **<external-directory-provider>** parameter in the <server install dir>\server\webapps\spotfire\WEB-INF\userdirconfig.xml file and change the value to “Windows”.

Example:

```
<userdir>
...
<external-directory-provider>Windows</external-directory-provider>
...
</userdir>
```

6.2.3.2 Edit the <external-group-synchronization> parameters in userdirconfig.xml

The Microsoft Windows NT Domain user directory back-end does not support synchronization of external groups. Locate the **<external-group-synchronization>** parameter in the <server install dir>\server\webapps\spotfire\WEB-INF\userdirconfig.xml file and set the value of the **<enabled>** child element to “false”.

Example:

```
<userdir>
...
<external-group-synchronization>
  <enabled>false</enabled>
  <sleep-time>60</sleep-time>
</external-group-synchronization>
...
</userdir>
```

6.2.3.3 Edit the <external-directory-provider-configuration> parameters in userdirconfig.xml

Open the file <server install dir>\server\webapps\spotfire\WEB-INF\userdirconfig.xml file and locate the **<external-directory-provider-configuration>** element with the **<provider-name>** child element set to “Windows”. The value of the **<domains>** parameter

must be set to a comma-separated list of the Window NT domains containing the users.

Example:

```
<userdir>

...

<external-directory-provider-configuration>
  <provider-name>Windows</provider-name>
  <provider-class>com.spotfire.server.userdir.win.WinUserDirectoryProvider</provider-
class>
  <config>
    <connector-class>com.spotfire.server.util.win.WinConnectorImpl</connector-class>
    <domains>sales, engineering</domains>
    <refresh-time>60</refresh-time>
  </config>
</external-directory-provider-configuration>

</userdir>
```

6.2.3.4 Restart the Server

Finally, restart the Spotfire Analytics Server (see “Starting the Spotfire Analytics Server” on page 105).

6.2.4 Changing to LDAP User Directory Back-end

The LDAP user directory back-end can be combined with the LDAP, NTLM, Kerberos and X.509 Certificates login systems on any operating system.

6.2.4.1 Edit the <external-directory-provider> parameter in userdirconfig.xml

Locate the <external-directory-provider> parameter in the <server install dir>\server\webapps\spotfire\WEB-INF\userdirconfig.xml file and change the value to “LDAP”.

Example:

```
<userdir>

...

<external-directory-provider>LDAP</external-directory-provider>

...

</userdir>
```

6.2.4.2 Edit the <external-group-synchronization> parameters in userdirconfig.xml

The LDAP user directory back-end supports synchronization of external LDAP groups. If this feature should be enabled, locate the **<external-group-synchronization>** parameter in the <server install dir>\server\webapps\spotfire\WEB-INF\userdirconfig.xml file and set the value of the **<enabled>** child element to “true”. If the feature should be disabled, the parameter should be set to “false”. When enabling this feature, make sure not to forget to specify a configuration file for the external LDAP groups in the next step.

Example:

```
<userdir>

...

<external-group-synchronization>
  <enabled>true</enabled>
  <sleep-time>60</sleep-time>
</external-group-synchronization>

...

</userdir>
```

6.2.4.3 Edit the <external-directory-provider-configuration> parameters in userdirconfig.xml

Open the file <server install dir>\server\webapps\spotfire\WEB-INF\userdirconfig.xml file and locate the **<external-directory-provider-configuration>** element with the **<provider-name>** child element set to “LDAP”. Five mandatory parameters must now be specified: **<ldap-server-type>**, **<server-url>**, **<context-names>**, **<user>** and **<password>**. Custom configurations have extra mandatory parameters, see the reference documentation for the userdirconfig.xml file. If the external LDAP group synchronization was enabled in the previous step, the **<external-groups-config>** parameter must also be defined.

For more information, see “/WEB-INF/userdirconfig.xml” on page 124.

- The **<ldap-server-type>** parameter should be set to “activeDirectory” if the LDAP server is a Microsoft Active Directory server, or to “sunOneDirectoryServer” if the LDAP server is a Sun Java Systems Directory Server (or one of the older ancestors known as Sun ONE Directory Server, iPlanet Directory Server or Netscape Directory Server). If the LDAP server is of another brand, the parameter should be set to “custom”. You will

probably also need to consult the reference documentation for the `userdirconfig.xml` file, since there are extra mandatory parameters for custom configurations.

- The **<server-url>** parameter should be set to the URL used for connecting to the LDAP server. The URL must follow the pattern `[protocol]://server[:port]`. The optional protocol specification defaults to “ldap”, but can also be set to “ldaps”. The port number defaults to 389 for the LDAP protocol and to 636 for the LDAPS protocol. These default values are usually correct, unless you have multiple Active Directory servers in your network and you need to access the “Global Directory”. In this case, the port number must be explicitly set to 3268 (LDAP) or 3269 (LDAPS).
- The **<context-names>** parameter contains the full distinguished names (DNs) of the containers (e.g., organizational units, OUs) to which the users belong. Each DN is specified in a **<context-name>** child element. If the specified containers contain a large number of users, of which only a few should be allowed access to the Spotfire Analytics Server, a user search filter can be specified to include only the designated users. See the reference documentation for the **<user-search-filter>** parameter in section “/WEB-INF/userdirconfig.xml” on page 124.
- The **<user>** parameter should contain the name of the administrator account to be used when searching for users and groups in the LDAP server. This account does not need to have any write permissions, but it needs to have read permissions for all configured contexts. If your LDAP server allows anonymous binding, you can leave this empty.
- The **<password>** parameter should contain the password for the specified administrator user account. If your LDAP server allows anonymous binding, you can leave this empty.
- If the external LDAP group synchronization was enabled in the previous step, the **<external-groups-config>** parameter must also be defined. The parameter value should point to a configuration file containing the names of the LDAP groups to be synchronized using a /WEB-INF relative path. See the example below or the reference documentation for the LDAP directory provider for information about the structure of the referenced configuration file.

Example: Active Directory User Directory Back-end

```
<userdir>

...

<external-directory-provider-configuration>
  <provider-name>LDAP</provider-name>
  <provider-class>com.spotfire.server.userdir.ldap.LDAPUserDirectoryProvider</
provider-class>
  <config>
```



```

<server>
  <ldap-server-type>activeDirectory</ldap-server-type>
  <server-url>ldap://dc2:3268</server-url>
  <context-names>
    <context-name>CN=Engineering,DC=example,DC=com</context-name>
    <context-name>CN=Sales,DC=example,DC=com</context-name>
  </context-names>
  <user>hagbard</user>
  <password>ifkgbg04</password>
  <external-groups-config>/WEB-INF/external-groups-config.xml</external-groups-
config>
</server>
</config>
</external-directory-provider-configuration>

</userdir>

```

Example: An external group synchronization configuration file

```

<external-groups>
  <group-name>ProjectX</group-name>
  <group-name>ProjectY</group-name>
  <group-name>ProjectManagement</group-name>
</external-groups>

```

Example: Sun Directory Server User Directory Back-end

```

<userdir>

...

<external-directory-provider-configuration>
  <provider-name>LDAP</provider-name>
  <provider-class>com.spotfire.server.userdir.ldap.LDAPUserDirectoryProvider</
provider-class>
  <config>
    <server>
      <ldap-server-type>sunOneDirectoryServer</ldap-server-type>
      <server-url>engrldap</server-url>
      <context-names>
        <context-name>OU=Engineering,DC=example,DC=com</context-name>
        <context-name>OU=Sales,DC=example,DC=com</context-name>
      </context-names>
      <user>hagbard</user>
      <password>ifkgbg04</password>
    </server>
  </config>
</external-directory-provider-configuration>

</userdir>

```

6.2.4.4 Restart the Server

Finally, restart the Spotfire Analytics Server (see “Starting the Spotfire Analytics Server” on page 105).

6.3 Setting Up Kerberos Authentication

6.3.1 Introduction

Starting with Windows 2000, Microsoft introduced Kerberos as the new authentication protocol to use with Active Directory domains. It is considered a better and more secure alternative than NTLM, but is more demanding to set up.

Kerberos authentication requires that you can access the Windows Active Directory server and make certain settings or perform certain commands.

If you wish to use Kerberos authentication on the Spotfire Analytics Server, it is recommended that you first install the server using an LDAP Login System and LDAP or Database User Directory Back-End. Once those have been set up and you have verified that things work as intended, make the switch to Kerberos by performing the necessary configuration procedures.

Important!

This chapter assumes that you have a good knowledge of how a Domain Controller works and how to use the administrative tools needed for this.

When performing the instructions below, it is vital that you are meticulous and careful. Misspelling a command or parameter can cause severe problems and may require a significant effort to correct.

Pay close attention to the case of letters in parameters and commands. These are case-sensitive and must be entered exactly as stated in the examples.

It is recommended that you have a basic understanding of how the Kerberos protocol works before attempting to set this up.

6.3.2 Prerequisites

- All computers involved in a Kerberos system must belong to the same Windows domain.
- All computers involved must have synchronized clocks, otherwise the Kerberos protocols will fail to work.
- All users must also belong to the same Windows domain or a trusted domain.
- The Domain Controller must have the Windows Server 2003 (SP1 / R2) Support Tools installed.

- Before setting up Kerberos, The Spotfire Analytics Server should be installed with LDAP Login System and LDAP or Database User Directory Back-end. You should verify that the system works correctly before making the switch to Kerberos.

Concerning Internet Explorer 6 and Port 80

If you have users who will use Internet Explorer version 6 or earlier when accessing the Spotfire Analytics Server, there are some concerns regarding port numbers that you must be aware of. A bug in Internet Explorer 6 prevents specifying a specific port number when using Kerberos. This means that you must install the Spotfire Analytics Server without specifying a port number (thus defaulting to port 80).

Therefore, whenever there is an option to specify a port number in the setspn commands or configuration files mentioned below, you **must NOT specify a port number** at all. This will make all settings use the default port 80 as needed.

More information about the issue with Internet Explorer 6 can be found here: <http://support.microsoft.com/kb/908209/>

6.3.3 Setting Up the Service Account

The following steps must be performed on the Domain Controller.

Note: The following instructions describes how to create a new Service Account to use for Kerberos with the Spotfire Analytics Server. If you already have an existing Service Account that you want to use, some of the instructions below may not apply to you. It is recommended that you create a new Service Account.

6.3.3.1 Create a Service Account

Create a Service Account for the Spotfire Analytics Server. The service account should be a regular domain user account.

Do not enter a First Name, Initial or Last Name for the account.

Enter the same information in the **Full Name** field as in the **User Logon Name** field. This string must not contain any blank spaces. This is the account name you will use later on for the setspn command.

Check/Uncheck the Account Options as stated below:

- User must change password at next logon: **Not** checked
- User cannot change password: **Not** checked
- Password never expires: Checked
- Account is disabled: **Not** checked

After the account is created, there is also an additional option (available in the Accounts tab of the Properties dialog) called: “Account is trusted for delegation”. This is optional and should be checked when the Spotfire Analytics Server should be able to access other services (e.g., databases) on behalf of logged in clients. See the separate instructions for “Setting Up Kerberos Delegation Between the Spotfire Analytics Server and Databases” on page 198. If you intend to set this up later, it is recommended that you check this option now. However, setting up an account as trusted for delegation does incur certain security aspects, so only select this option if you need it.

- Account is trusted for delegation: (checked/not checked)

6.3.3.2 Run the setspn.exe Tool to Set Up the SPNs

This section explains how to create the two Service Principal Names (SPNs) needed for the Kerberos authentication.

To do this you will use the setspn.exe command which is a part of the Windows Server 2003 Support Tools mentioned earlier in the prerequisites. For more information about these tools visit Microsoft’s TechNet documentation.

Note: The setspn.exe command is not always available in the command path by default. You may have to make sure you can run the command by first adding it to the path.

When executing the commands below, replace “myHost”, “mydomain” and “myServiceAccount” with proper values.

Note that it is **VERY IMPORTANT** to use the **correct case** for the parameter values.

Also, always use **Fully Qualified Domain Names (FQDN)** when specifying domains.

- **myHost**: the name of the Spotfire Analytics Server host computer (case-sensitive)
- **mydomain**: the name of the Windows domain to which the host computer belongs (lower case)
- **myServiceAccount**: the name of the service account (case-sensitive)
- **port**: the service's port number (See important note concerning Internet Explorer 6 and Port 80 in Section 6.3.2 on page 186.)

Both the following commands must be executed.

Again, note that it is **VERY IMPORTANT** to use the **correct case** for the parameter values.

Syntax:

```
> setspn -A HTTP/myHost.mydomain[:port] myServiceAccount
> setspn -A HTTP/myHost[:port] myServiceAccount
```

Example:

Setting SPNs for the service account "**spotsvc**" and the computer **spotserver.research.example.com** using the HTTP port **8080**.

```
> setspn -A HTTP/spotserver.research.example.com:8080 spotsvc
> setspn -A HTTP/spotserver:8080 spotsvc
```

This would result in the following two SPNs:

- HTTP/spotserver.research.example.com:8080
- HTTP/spotserver:8080

To verify the result you can enter the following command.

Syntax:

```
> setspn -L myServiceAccount
```

Example:

Verifying SPNs for the service account "**spotsvc**".

```
> setspn -L spotsvc
```

```
Registered ServicePrincipalNames for  
CN=spotsvc,CN=Users,DC=research,DC=example,DC=com:
```

```
HTTP/spotserver:8080
```

```
HTTP/spotserver.research.example.com:8080
```

6.3.3.3 Run the ktpass.exe Tool to Create the keytab File

This section explains how to create the keytab file which then will be used on the Spotfire Analytics Server to set up the Kerberos authentication.

The name of this keytab file must be **spotfire.keytab**.

This requires the ktpass.exe tool which again is included in the Windows Server 2003 Support Tools mentioned earlier in the prerequisites. For more information about these tools, visit Microsoft's TechNet documentation.

Note: The ktpass.exe command is not always available in the command path by default. You may have to make sure you can run the command by first adding it to the path.

When executing the command below, replace "myHost", "mydomain", "MYDOMAIN", and "myServiceAccount" with proper values.

Note that it is **VERY IMPORTANT** to use the **correct case** for the parameter values.

Also, always use **Fully Qualified Domain Names (FQDN)** when specifying domains.

- **myHost**: the name of the Spotfire Analytics Server host computer (case-sensitive), as seen in section 6.3.3.2.
- **mydomain**: the name of the Windows domain to which the host computer belongs, always in lower case, as seen in section 6.3.3.2.
- **MYDOMAIN**: the Kerberos Realm, in Windows always the name of the Windows domain to which the host computer belongs (in upper case).
- **myServiceAccount**: the name of the service account created in section 6.3.3.1 (case-sensitive).
- **port**: the port number (See important note concerning Internet Explorer 6 and Port 80 in Section 6.3.2 on page 186.)
- **Password**: the **password of the Service Account** that was created in section 6.3.3.1 above. You **MUST** enter this case-sensitive.

- All the parameters should be entered on the same row, in the same command.
- The keytab file must be named spotfire.keytab.
- The keytab file will be placed in the current working directory.

Syntax:

```
> ktpass /princ HTTP/myHost.mydomain[:port]@MYDOMAIN
      /mapuser myServiceAccount /ptype krb5_nt_principal /crypto rc4-hmac-nt
      /out spotfire.keytab /pass Password
```

Example:

Generating the keytab file for example.com.

```
> ktpass /princ HTTP/spotserver.research.example.com:8080@RESEARCH.EXAMPLE.COM
      /mapuser spotsvc /ptype krb5_nt_principal /crypto rc4-hmac-nt
      /out spotfire.keytab /pass Pa55w0rd
```

Move the Keytab file to the Spotfire Analytics Server

You will now have the spotfire.keytab file in your working directory on the Domain Controller. This file must now be moved to the following directory on the Spotfire Analytics Server:

```
<installation dir>\jdk\jre\lib\security
```

Important Security Note: This file is extremely sensitive. If it came into the wrong hands it would cause a severe security issue. You should therefore be very mindful of how you handle this file. Copying it over a public network drive is strongly discouraged; rather use encrypted file transfer or a portable media that you can destroy after the file has been placed on the Spotfire Analytics Server. You should also consider limiting the read/write access to the file after it is placed on the Spotfire Analytics Server.

Note: Avoid changing the password of the specified Service Account after you have created the keytab file. If the password changes, Kerberos will stop working and you will have to create a new keytab file and perform the necessary procedures again.

6.3.4 Configuring the TIBCO Spotfire Analytics Server for Kerberos

The following steps must be performed on the Spotfire Analytics Server.

6.3.4.1 Edit the Kerberos Configuration File

Locate the krb5.conf file and open it in a text editor:

<installation dir>\jdk\jre\lib\security\krb5.conf

Replace “mydomain” and “MYDOMAIN” with proper values, corresponding to the setting made in section 6.3.3.3. Replace “mydc” with the name of the domain controller.

- **mydomain**: the name of the Windows domain to which the host computer belongs (lower case), as seen in section 6.3.3.3.
- **MYDOMAIN**: the name of the Kerberos realm, as seen in section 6.3.3.3. Equal to the Windows domain to which the host computer belongs (upper case).
- **mydc**: the name of the domain controller (lower case). (This parameter has not been used in previous commands above.)

Note that it is **VERY IMPORTANT** to use the **correct case** for the parameter values.

Also, always use **Fully Qualified Domain Names (FQDN)** when specifying domains.

Installed Unmodified Template:

```
[libdefaults]
default_realm = MYDOMAIN
default_keytab_name = spotfire.keytab
default_tkt_enctypes = rc4-hmac
default_tgs_enctypes = rc4-hmac

[realms]
MYDOMAIN = {
    kdc = mydc.mydomain
    admin_server = mydc.mydomain
    default_domain = mydomain
}
```



```

}

[domain_realm]
    .mydomain = MYDOMAIN
    mydomain = MYDOMAIN

[appdefaults]
    autologin = true
    forward = true
    forwardable = true
    encrypt = true

```

Example of Modified File:

```

[libdefaults]
    default_realm = RESEARCH.EXAMPLE.COM
    default_keytab_name = spotfire.keytab
    default_tkt_enctypes = rc4-hmac
    default_tgs_enctypes = rc4-hmac

[realms]
    RESEARCH.EXAMPLE.COM = {
        kdc = example-dc.research.example.com
        admin_server = example-dc.research.example.com
        default_domain = research.example.com
    }

[domain_realm]
    .research.example.com = RESEARCH.EXAMPLE.COM
    research.example.com = RESEARCH.EXAMPLE.COM

[appdefaults]
    autologin = true
    forward = true
    forwardable = true
    encrypt = true

```

Save the file.

6.3.4.2 Edit the spotfire.login File

Open the **spotfire.login** file in a text editor and edit the SpotfireKerberos section.

<installation dir>/jdk/jre/lib/security/spotfire.login

Replace “myHost”, “mydomain” and “MYDOMAIN” with the proper values.

Set the **path** to the keytab file. Make sure to use **forward slashes** and not backslashes in the path!

Note that it is **VERY IMPORTANT** to use the **correct case** for the parameter values.

- **myHost**: the name of the Spotfire Analytics Server host computer (case-sensitive), as seen in section 6.3.3.2 and 6.3.3.3.
- **mydomain**: the name of the Windows domain to which the host computer belongs (lower case), as seen in section 6.3.3.2 and 6.3.3.3.
- **MYDOMAIN**: the name of the Kerberos realm, as seen in section 6.3.3.3. Equal to the Windows domain to which the host computer belongs (upper case).
- **Port**: the port number (See important note concerning Internet Explorer 6 and Port 80 in Section 6.3.2 on page 186.)

Installed Unmodified Template:

```
SpotfireKerberos
{
    com.sun.security.auth.module.Krb5LoginModule
        required
        debug=false
        storeKey=true
        useKeyTab=true
        keyTab="<absolute path to spotfire.keytab>"
        principal="HTTP/myHost.mydomain@MYDOMAIN";
};
```

Example of Modified File:

```
SpotfireKerberos
{
    com.sun.security.auth.module.Krb5LoginModule
        required
        debug=false
        storeKey=true
        useKeyTab=true
        keyTab="C:/spotserver/jdk/jre/lib/security/spotfire.keytab"
        principal="HTTP/spotserver.research.example.com:8080@RESEARCH.EXAMPLE.COM";
};
```

6.3.4.3 Verify that the spotfire.keytab File is in Place and Works

Verify that the spotfire.keytab file created earlier has been moved from the Domain Controller and is now placed on the Spotfire Analytics Server in the following directory:

<installation dir>/jdk/jre/lib/security/spotfire.keytab

Optional:

In the folder <installation directory>jdk/jre/bin there are a number of tools that can help you verify and troubleshoot the spotfire.keytab file.

You can verify that the spotfire.keytab file works as intended by entering the following command in a command prompt on the Spotfire Analytics Server:

```
> kinit.exe -k -t spotfire.keytab HTTP/myServer.mydomain[:port]@MYDOMAIN
```

If the spotfire.keytab file is correct, and works as intended, a ticket cache file will be created.

Example for Windows Server 2003:

C:\Documents and Settings\<user>\krb5cc_<user>

Important! As soon as you have verified that the ticket cache was created, you **must** delete the file.

You can also check the contents of the spotfire.keytab file using the following command. It will list the principal name and security credentials.

```
> klist.exe -k -t -K spotfire.keytab
```

6.3.4.4 Edit the security-filter.xml File

Locate the **security-filter.xml** file in the following directory, and open it in a text- or xml editor.

<installation dir>\server\webapps\spotfire\WEB-INF\security-filter.xml

Modify the file so that the <login-config> element looks like the following:

```
<login-config>
  <auth-method>Negotiate</auth-method>
  <realm-name>SpotfireRealm</realm-name>
</login-config>
```

6.3.4.5 Edit the manifest.xml File

Locate the **manifest.xml** file in the following directory, and open it in a text- or xml editor.

```
<installation dir>\server\webapps\spotfire\WEB-INF\manifest.xml
```

Modify the file so that the **<authentication-modes>** element looks like the following:

```
<server-info>
  <authentication-modes>
    <integrated-authentication/>
  </authentication-modes>
</server-info>
```

6.3.4.6 Edit the web.xml File

Locate the **web.xml** file in the following directory, and open it in a text- or xml editor.

```
<installation dir>\server\webapps\spotfire\WEB-INF\web.xml
```

Edit the file, and add the following node next to the already existing **<context-param>** nodes:

```
<context-param>
  <param-name>kerberos.login.context</param-name>
  <param-value>SpotfireKerberos</param-value>
</context-param>
```

6.3.4.7 Restart the Spotfire Analytics Server

Restart the Spotfire Analytics Server. When it comes back online, the Kerberos settings should take effect.

Finished!

6.3.5 Configuring Kerberos Credentials for Database Connections

To configure Kerberos authentication for database connections, a Kerberos account for database server access must be created and given access permissions to the relevant databases. Use the “Active Directory Users and Computers” control panel on the Windows domain controller to create the Kerberos account.

On the Spotfire Analytics Server computer, the Kerberos configuration file **<installation directory>jdk/jre/lib/security/krb5.conf** must be configured properly (if the server is already configured for end-user Kerberos authentication, this file is already configured). Consult Section 6.3.4.1 on page 192 for information about how to do that.

When the Kerberos configuration file is set up, use the ktab.exe tool in the folder **<installation directory>jdk/jre/bin** to create a keytab file for the database user account. The keytab file should be placed in the **<installation directory>jdk/jre/lib/security/** directory. Replace **<dbuser>** and **<dbpassword>** with the name and the password of the database account created above (the name should not be qualified with the domain name) :

```
> ktab.exe -k database.keytab -a <dbuser> <dbpassword>
```

In the folder **<installation directory>jdk/jre/bin** there are a number of additional tools that can help you verify and troubleshoot the database.keytab file.

You can verify that the database.keytab file works as intended by entering the following command in a command prompt:

```
> kinit.exe -k -t database.keytab <dbuser>
```

If the spotfire.keytab file is correct, and works as intended, a ticket cache file will be created.

Example for Windows Server 2003:

```
C:\Documents and Settings\<user>\krb5cc_<user>
```

Important! As soon as you have verified that the ticket cache was created, you **must** delete the file.

You can also check the contents of the database.keytab file using the following command. It will list the principal name and security credentials.

```
> klist.exe -k -t -K database.keytab
```

When the keytab file is created and working as expected, a JAAS application configuration must be created in the **<installation directory>jdk/jre/lib/security/spotfire.login** file. Use the following template and substitute dbuser with the name of the database account (in lower case) and MYDOMAIN with the name of the Kerberos realm (in upper case).

```
DatabaseKerberos
{

    com.sun.security.auth.module.Krb5LoginModule
        required
        debug=true
        storeKey=true
        useKeyTab=true
        keyTab="<absolute path to database.keytab>"
        principal="dbuser@MYDOMAIN";

};
```

6.3.6 Setting Up Kerberos Delegation Between the Spotfire Analytics Server and Databases

An optional further use of Kerberos is to set up Kerberos delegation between the Spotfire Analytics Server and the databases. This means that each user using an Information Link will access the corresponding databases using his or her personal credentials, instead of a predefined user specified in the Information Link.

More information about this can be found in “Configuring JDBC Data Sources for Kerberos Authentication with Delegated Credentials” on page 224.

6.4 Enabling Impersonation

When the Spotfire Analytics Server is used in conjunction with the Spotfire Web Player server which has been configured for certain authentication methods, impersonation should be enabled on the Spotfire Analytics Server for seamless login.

Impersonation means that the Spotfire Web Player is responsible for authenticating users. Calls from the Spotfire Web Player to the Spotfire Analytics Server will be made on behalf of the person authenticated.

For example, consider that the Spotfire Web Player server is configured for certificate authentication. This authentication method is done on the https network level and there is no username or password which can be conveyed to the Spotfire Analytics Server for login. Instead the Spotfire Web Player server is trusted for impersonation. The Spotfire Web Player server is allowed to make calls on behalf of any user without the ordinary authentication mechanism. This means the user will see his/her specific files in the library etc.

Enabling impersonation can pose a potential security issue, which is why this is disabled by default. To strengthen security there are a number of requirements that can be imposed on a call in order for it to be allowed to impersonate. More information about this is described below.

Impersonation is configured in the file:

```
<install dir>/server/webapps/spotfire/WEB-INF/security-filter.xml
```

The impersonation node has the following structure:

```
<impersonation-config>
  <enabled>true</enabled>
  <require-ssl>>false</require-ssl>
  <allowed-user>malcom</allowed-user>
  <allowed-user>kaylee</allowed-user>
  <originating-ip>192.168.1.2</originating-ip>
  <originating-ip>192.168.1.3</originating-ip>
  <originating-name>acme-wps</originating-name>
</impersonation-config>
```

To enable impersonation, the element “enabled” should be set to “true”.

The other possible configuration settings determine which requirements must be met in order to allow impersonation. These requirements are on the impersonate call from the Spotfire Web Player server to the Spotfire Analytics Server. All the requirements you decide to set up must be met for the impersonation call to be allowed.

If you want to require the impersonation call to be made on https, the element “require-ssl” should be set to “true”. If you set it to “false” then both http and https are allowed.

The call from the Spotfire Web Player server to the Spotfire Analytics Server will always require authentication. This is most often done as a certain user which has been specified in the configuration of the Spotfire Web Player server. The Spotfire Analytics Server can be configured to only allow certain users to be able to issue impersonation calls - typically the very user specified in the Spotfire Web Player server configuration.

On the Spotfire Analytics Server this is configured using “allowed-user” nodes. These nodes can be 0, 1 or more. With 0 nodes any authenticated user can issue impersonate calls, otherwise the call must be one of the identities specified. The most common use is to specify the same user as previously configured on the Spotfire Web Player server.

Note: This is a requirement on the originally logged in user and has nothing to do with identities which one impersonates to.

Specific requirements can also be made on the origin of an impersonate call. Typically you would want to configure the Spotfire Analytics Server to only allow impersonation calls originating from the machine running the Spotfire Web Player server.

If one or more are listed in the security-filter.xml file, then only calls originating from these machines are allowed. Allowed machines can be specified on two forms <originating-ip> or <originating-name>. The first should be the IP number of the machine, the second is resolved to one (or more) IP numbers using DNS. Only calls originating from one of the mentioned machines can do impersonation calls. If no such node exists then calls originating from any machine can do impersonation.

Note: When IPv6 is used then the exact form of the IP number should be different than in the example.

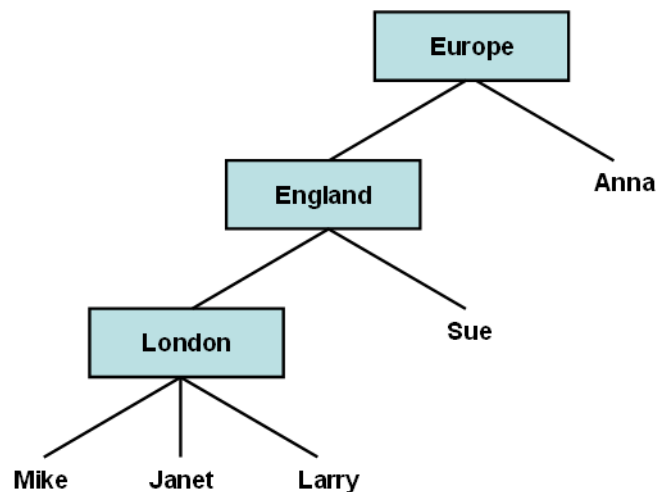
6.5 Enabling External LDAP Group Synchronization

When using an LDAP user directory back-end, the Spotfire Analytics Server offers the capability to synchronize the group memberships for selected LDAP groups with its own internal groups. This makes it possible for an administrator to assign licenses and privileges to Spotfire groups in the normal fashion, but being relieved of the duty of having to manage the group memberships.

All such synchronized groups will be immutable in the Spotfire administration tools, i.e., you can neither rename or remove such a group, nor alter its member list. However, you can still include such a group as a subgroup of another non-immutable group.

In Microsoft Active Directory servers and in Sun Java System Directory Server 6.0 or later, most types of groups should be possible to synchronize. In Sun ONE Directory Servers, however, it is not possible to use the same group synchronization mechanism as for the other servers. Instead, a role-based synchronization mechanism can be used, where the internal Spotfire groups are synchronized with nested or managed roles (but not filtered roles!) in the Sun ONE Directory Server. This role-based synchronization can of course also be used with the newer Sun Java System Directory Server.

Each synchronization task will, by default, be followed by a 60 minutes long sleeping period, before a new synchronization task starts.



Group-based Synchronization

Spotfire Analytics Server supports synchronization with most types of groups in Microsoft Active Directory servers and Sun Java System Directory Servers. In the image above, there are three groups: Europe, England and London. London has three users, and is a member of the group England. The group England has one user as a member and also the group London as a member. The group Europe has one user and also the group England as a member.

Let us assume you decide to only synchronize the group “Europe” in the LDAP server. Listing the members of the group Europe in the Spotfire administration tools will present all the users of the actual LDAP group itself and also any members of its subgroups: Anna, Sue, Mike, Janet and Larry. The subgroups themselves will not be seen, that is, England and London will not appear in the Spotfire administration tools.

Let us instead assume you decide to synchronize all three groups explicitly. Listing the members of the group “Europe” would then present the user Anna and a subgroup: England. Settings made for Europe would be inherited down the group hierarchy as expected.

Note: The DecisionSite Administrator tool only supports users as members of groups. Any subgroups will not be visible.

For more information about the group-based synchronization, see “External Group Synchronization” on page 135.

Role-based Synchronization

Using Sun ONE Directory Servers, you cannot for performance reasons synchronize against what is called “groups”. Instead, the Spotfire Analytics Server offers the capability to synchronize its internal groups with what is called “roles” in the LDAP server. More specifically, “managed roles” and “nested roles” are supported, whereas “filtered roles” are not.

Contrary to the group-based synchronization, the role-based synchronization mechanism will never let you list nested roles (which can be compared with subgroups) from the Spotfire administration tools. Regardless of whether you explicitly synchronize toward only the “Europe” group, or if you also synchronize towards the “England” and “London” groups, listing the members of “Europe” will always present only the resulting users: Anna, Sue, Mike, Janet and Larry.

Note: The DecisionSite Administrator tool only supports users as members of groups. Any subgroups will not be visible.

For more information about the role-based synchronization, see “External Group Synchronization” on page 135.

Prerequisites:

The Spotfire Analytics Server must be set up to use an **LDAP user directory back-end**.

► Setting up LDAP Synchronization:

- 1 Open the file `<installation directory>/server/webapps/spotfire/WEB-INF/userdirconfig.xml` in a text editor.
- 2 Set the `<external-group-synchronization>` `<enabled>` tag to “true”.
- 3 Specify the path and file name of an xml-file that you will soon create, which will hold information about which groups you want to synchronize. It is recommended that you place the file in the WEB-INF catalog, so specify the path according to the example below:

```
<userdir>
...
  <external-group-synchronization>
    <enabled>true</enabled>
    <sleep-time>60</sleep-time>
  </external-group-synchronization>
```

```

...
<external-directory-provider-configuration>
  <provider-name>LDAP</provider-name>
  <provider-class>...</provider-class>
  <config>
    <server>
      <ldap-server-type>...</ldap-server-type>
      <server-url>...</server-url>
      <context-names><context-name>...</context-name></context-names>
      <user>...</user>
      <password>...</password>
      <external-groups-config>/WEB-INF/external-groups.xml</external-groups-config>
    </server>
  </config>
</external-directory-provider-configuration>
...
</userdir>

```

- 4 Save the file.
- 5 Next, create a new XML-file with the file name you specified above.
- 6 Specify the LDAP groups you want to synchronize as shown below:

```

<external-groups>
  <group-name>SALESEU</group-name>
  <group-name>SALESUS</group-name>
  <group-name>MANAGEMENT</group-name>
</external-groups>

```

Note: When specifying the LDAP groups to be synchronized, make sure not to introduce any cyclic group memberships, where the ancestor of a group is also a descendant of the same group.

- 7 Save this file in the
<server install dir>/server/webapps/spotfire/WEB-INF folder.
- 8 Restart the Spotfire Analytics Server for the changes to take effect (see “Starting the Spotfire Analytics Server” on page 105).

Note: You can now edit the synchronization file anytime you want, without restarting the Spotfire Analytics Server. The file will be consulted for each new synchronization task.

► Changing the Synchronization Timer:

- 1 Open the file <installation directory>/spotfire/spotfire/WEB-INF/userdirconfig.xml in a text editor.
- 2 Under the <external-group-synchronization> tag, find a tag called <sleep-time>.

```
<sleep-time>60</sleep-time>
```

- 3 Enter a new time in minutes. This time is how long the system will wait after a synchronization is complete, until it starts the next synchronization task.

It is highly recommended that you not set this to lower than 60 minutes, since a synchronization task may lower the performance of the LDAP server while in progress. Therefore you might not want such a task to be performed too often.

- 4 Save the file.
- 5 Restart the Spotfire Analytics Server for the changes to take effect (see “Starting the Spotfire Analytics Server” on page 105).

► Removing a Synchronized Group:

- 1 Open the synchronization XML file you created in the **<installation directory>/spotfire/spotfire/WEB-INF/** folder.
- 2 Delete the **<external-groups>** tags specifying the groups you no longer want to synchronize.
- 3 Save the file.

Comment: You do not need to restart the Spotfire Analytics Server for the changes to take effect.

- 4 The group in question will still be visible in the Spotfire administration tools, but is now considered a normal Spotfire Analytics Server group. You must now manually delete the group from within the Spotfire administration tool.

6.6 Changing Database Connection Settings

This section describes how the database connection settings can be changed after installation of the Spotfire Analytics Server. It does not describe how to update any data source in Information Services, which instead is described in the Information Designer chapter of the “TIBCO Spotfire - User’s Manual”.

6.6.1 Changing the Spotfire Analytics Server Database Settings

- 1 Before changing the Spotfire Analytics Server database connection settings, make sure to backup the following configuration files:
 - **<server install dir>\jdk\jre\lib\security\spotfire.login**

- <server install dir>\server\webapps\spotfire\WEB-INF\data-sources.xml
- 2 Open the <server install dir>\jdk\jre\lib\security\spotfire.login file and make sure that the SpotfireDBLogin configuration block does not contain any database connection settings. It should look like this:

```
SpotfireDBLogin
{

    com.spotfire.server.jaas.dblogin.DBLoginModule
        required;

};
```

- 3 Open the <server install dir>\server\webapps\spotfire\WEB-INF\data-sources.xml file and edit the necessary parameters. Typically, the <user>, <password>, and <connection-url> are the parameters that need to be updated. All parameters in the data-sources.xml file are described in detail in Section 5.1.3 on page 118.
- 4 Proceed to update the database connection settings for Information Services and Spotfire Library, if necessary.
- 5 Finally, restart the server (see “Starting the Spotfire Analytics Server” on page 105) and make sure everything works as expected.

6.6.2 Changing the Spotfire Information Model Database Settings

- 1 Before changing the database connection settings, make sure to backup the following configuration file:
 - <server install dir>\server\webapps\spotfire\WEB-INF\im-service.xml
- 2 Open the <server install dir>\server\webapps\spotfire\WEB-INF\im-service.xml file and edit the necessary parameters. Typically, the <user>, <password>, and <connection-url> are the parameters that need to be updated. All parameters in the im-service.xml file are described in detail in Section 5.1.5 on page 136.
- 3 Proceed to update the database connection settings for Spotfire Analytics Server and Spotfire Library, if necessary.
- 4 Finally, restart the server (see “Starting the Spotfire Analytics Server” on page 105) and make sure everything works as expected.

6.6.3 Changing the Spotfire Library Database Settings

The database connection settings for the Spotfire Library can be edited in two ways: either by using the Library Administrator Tool or by manually editing the configuration file. When changing the database connection settings for the Spotfire Analytics Server and/or the Spotfire Information Model, edit the file manually. When changing the database connection settings for just the Spotfire Library, use the Library Administrator Tool which does not require the server to be restarted.

Manually Editing the Configuration File

- 1 Before changing the database connection settings, make sure to backup the following configuration file:
 - <server install dir>\server\webapps\spotfire\WEB-INF\library-service.xml
- 2 Open the <server install dir>\server\webapps\spotfire\WEB-INF\library-service.xml file and edit the necessary parameters. Typically, the <user>, <password>, and <connection-url> are the parameters that need to be updated. All parameters in the library-service.xml file are described in detail in Section 5.1.6 on page 142.
- 3 Proceed to update the database connection settings for Spotfire Analytics Server and Spotfire Information Model, if necessary.
- 4 Finally, restart the server (see “Starting the Spotfire Analytics Server” on page 105) and make sure everything works as expected.

Using the Library Administrator Tool

- 1 Before changing the database connection settings, make sure to backup the following configuration file:
 - <server install dir>\server\webapps\spotfire\WEB-INF\library-service.xml
- 2 Open an Internet Explorer browser.
- 3 Browse to the Spotfire Analytics Server start page by entering its address in the Address field. (Example: http://sfas/spotfire)
Response: This opens the Spotfire Analytics Server start page.
- 4 Click on **Library Administrator**.
Response: This launches the Library Administrator tool.
- 5 Stop the Spotfire Library service by clicking on the stop button.

- 6 Edit the necessary parameters. Typically, the **server name**, **user name**, and **password** are the parameters that need to be updated.
- 7 Start the Spotfire Library service by clicking on the start button.

6.7 Configuring IS to Access a New Type of JDBC Data Source

6.7.1 Configure IS to Access a New Type of JDBC Data Source

By default, Information Services supports the following data sources:

- Oracle
- DB2
- MySQL
- SQLServer
- SAS/SHARE
- Sun JDBC ODBC

Oracle is set up by default, but to make Information Services connect to any other of these data sources, you need to make some configurations.

However, it is also possible to configure Information Services to be able to access other types of data sources. To extend Information Services to support a specific type of JDBC data source, an XML configuration must be created. This XML configuration includes a number of settings that customize the way Information Services interacts with the data source.

6.7.2 Settings

The table below shows all settings available. Note that the only mandatory settings needed in the XML-file are the first four:

- type-name
- display-name
- driver
- connection-url-pattern

If left out, all other settings will automatically use their default values.

Setting	Description	Default	Notes
type-name	A unique name for the configuration		
display-name	The name shown in the Information Designer, Data Sources workbench		
driver	The JDBC driver Java class used for creating connections		
connection-url-pattern	A pattern for the connection URL		URL syntax is driver specific
ping-command	A dummy command to test connections	SELECT 1	
connection-properties	JDBC connection properties		
metadata-provider	Java class that provides database metadata	BasicJDBCMetadataProvider	See Spotfire Technical Network for more info.
sql-filter	Java class that generates SQL	BasicSQLFilter	See Spotfire Technical Network for more info.
sql-runtime	Java class that handles SQL execution	BasicSQLRuntime	See Spotfire Technical Network for more info.
fetch-size	A fetch size specifies the amount of data fetched with each database round trip for a query. The fetch size is measured as the number of fields, which is calculated to the number of rows for a particular query.	10000	The specified value is shown as the default value in ID. May be changed at instance level.

batch-size	A batch size specifies the amount of data in each batch update. The batch size is the number of fields, which is calculated to the number of operations for a particular type of operation.	100	The specified value is shown as the default value in ID. May be changed at instance level.
max-column-name-length	The maximum length of a database column name	30	This limit is used when creating temporary tables.
table-types	Specify which table types to retrieve	TABLE, VIEW	
supports-catalogs	Tells if the driver supports catalogs	true	
supports-schemas	Tells if the driver supports schemas	true	
supports-procedures	Tells if the driver supports stored procedures.	false	
supports-distinct	Tells if the driver supports distinct option in SQL queries	true	
supports-order-by	Tells if the driver supports order-by option in SQL queries.	true	
column-name-pattern	Determines how a column name is written in the SQL query.	“\$\$name\$\$”	
table-name-pattern	Determines how a table name is written in the SQL query.	“\$\$name\$\$”	
schema-name-pattern	Determines how a schema name is written in the SQL query.	“\$\$name\$\$”	

Configuration Procedures

catalog-name-pattern	Determines how a catalog name is written in the SQL query.	“\$\$name\$\$”	
procedure-name-pattern	Determines how a procedure name is written in the SQL query.	“\$\$name\$\$”	
column-alias-pattern	Determines how a column alias is written in the SQL query.	“\$\$name\$\$”	
string-literal-quote	The character used as quote for string literals		SQL-92 standard
max-in-clause-size	The maximum size of an SQL IN-clause. Larger lists are split into several clauses that are OR:ed together.	1000	
condition-list-threshold	A temporary table is used when executing an SQL query, where total size of a condition list is larger than this threshold value.	10000	Depends on the maximum SQL query size.
expand-in-clause	If true, an SQL IN-clause will be expanded into OR conditions.	false	
table-expression-pattern	Determines how a table expression is written in the SQL query.	[\$\$catalog\$\$][\$\$schema\$\$]\$\$table\$\$	catalog and schema may be optional (surrounded by brackets)
procedure-expression-pattern	Determines how a procedure expression is written in the SQL query.	[\$\$catalog\$\$][\$\$schema\$\$]\$\$procedure\$\$	

procedure-table-jdbc-type	Integer representing the jdbc type identifying a table returned from a procedure as defined by java.sql.Types.	0	
procedure-table-type-name	Display name for tables from procedure.	null	This is currently not visible to the user in any UI.
date-format-expression	An expression that converts a date field to a string value on the format: "YYYY-MM-DD", e.g., "2002-11-19"	\$\$value\$\$	Used in WHERE and HAVING clauses. The tag \$\$value\$\$ is a placeholder for the date field.
date-literal-format-expression	An expression that converts a date literal on the format "YYYY-MM-DD" to a date field value.	'\$\$value\$\$'	Used in WHERE and HAVING clauses. The tag \$\$value\$\$ is a placeholder for the date literal.
time-format-expression	An expression that converts a time field to a string value on the format: "HH:MM:SS", e.g., "14:59:00"	\$\$value\$\$	Used in WHERE and HAVING clauses. The tag \$\$value\$\$ is a placeholder for the time field.
time-literal-format-expression	An expression that converts a time literal on the format "HH:MM:SS" to a time field value.	'\$\$value\$\$'	Used in WHERE and HAVING clauses. The tag \$\$value\$\$ is a placeholder for the time literal.
date-time-format-expression	An expression that converts a datetime field to string value on the format: "YYYY-MM-DD HH:MM:SS", e.g. "2002-11-19 14:59:00"	\$\$value\$\$	Used in WHERE and HAVING clauses. The tag \$\$value\$\$ is a placeholder for the date-time field.

Configuration Procedures

date-time-literal-format-expression	An expression that converts a date-time literal on the format "YYYY-MM-DD HH:MM:SS" to a date-time field value.	'\$\$value\$\$'	Used in WHERE and HAVING clauses. The tag \$\$value\$\$ is a placeholder for the date-time literal.
java-to-sql-type-conversions: String Integer Long Float Double Date Time DateTime	Type conversions needed when a join data source creates a temporary table for result from a subquery. For String conversion %s will be replaced by the size of the string. A match-length attribute may be specified (see MySQL).	VARCHAR(\$\$value\$\$) VARCHAR(255) INTEGER BIGINT REAL DOUBLE PRECISION DATE TIME TIMESTAMP	Different String types may be needed dependant of the length of the string. Note that there must be a VARCHAR conversion for when the length of the string is unknown (255 in the example here). When several VARCHAR mappings are specified, the mapping that first matches the match-length is used.
temp-table-name-pattern	Determines how to format a temporary table name in an SQL command.	\$\$name\$\$	

create-temp-table-command	SQL commands for creating a temporary table. This is used to store filter values (when more than 'condition-list-threshold') and to store result from subqueries. \$\$name\$\$ is a placeholder for the table name. \$\$column_list\$\$ is a placeholder for a column list on the format "(name type, name type, ...)"	CREATE TEMPORARY TABLE \$\$name\$\$ \$\$column_list\$\$	The syntax may vary between databases.
drop-temp-table-command	SQL commands for deleting a temporary table. \$\$name\$\$ is a placeholder for the table name.	DROP TABLE \$\$name\$\$	The syntax may vary between databases.
data-source-authentication	Default value data source authentication. (boolean).	false	This value can be set (overridden) in the Information Interaction Designer.
lob-threshold	Threshold when LOB values used as parameters in a WHERE clause, must be written in temporary tables	-1	The default (-1) means no limit.

Configuration Procedures

use-ansii-style-outer-join	The default generated SQL uses the Oracle way with “(+)” to indicate joins. If this setting is set to true an attempt is made to rewrite it to standard ANSI format, making it possible to run on non Oracle databases	false	
----------------------------	--	-------	--

Example of XML Syntax with Default Settings

The following example is the XML syntax showing all the default settings. Use this template when you are about to create your own JDBC data source.

```
<!--
<jdbc-type-settings>
  <type-name>[NAME]</type-name>
  <display-name>[DISPLAY NAME]</display-name>
  <driver>[DRIVER CLASS]</driver>
  <connection-url-pattern>
    [CONNECTION URL PATTERN]
  </connection-url-pattern>
  <ping-command>SELECT 1</ping-command>
  <column-name-pattern>"$$name$$"</column-name-pattern>
  <table-name-pattern>"$$name$$"</table-name-pattern>
  <schema-name-pattern>"$$name$$"</schema-name-pattern>
  <catalog-name-pattern>"$$name$$"</catalog-name-pattern>
  <procedure-name-pattern>"$$name$$"</procedure-name-pattern>
  <column-alias-pattern>"$$name$$"</column-alias-pattern>
  <string-literal-quote>'</string-literal-quote>
  <fetch-size>10000</fetch-size>
  <batch-size>100</batch-size>
  <table-types>TABLE, VIEW</table-types>
  <supports-catalogs>true</supports-catalogs>
  <supports-schemas>true</supports-schemas>
  <supports-procedures>false</supports-procedures>
  <max-in-clause-size>1000</max-in-clause-size>
  <condition-list-threshold>10000</condition-list-threshold>
  <expand-in-clause>false</expand-in-clause>
  <max-column-name-length>30</max-column-name-length>
  <table-expression-pattern>
    [$$catalog$$].[ $$schema$$ ]. $$table$$
  </table-expression-pattern>
  <procedure-expression-pattern>
    [ $$catalog$$ ]. [ $$schema$$ ]. $$procedure$$
  </procedure-expression-pattern>
  <date-format-expression>$$value$$</date-format-expression>
  <time-format-expression>$$value$$</time-format-expression>
  <date-time-format-expression>$$value$$</date-time-format-expression>
```

```

<java-to-sql-type-conversions>
  <type-mapping>
    <from max-length="255">String</from>
    <to>VARCHAR($$value$$)</to>
  </type-mapping>
  <type-mapping>
    <from>String</from>
    <to>VARCHAR(255)</to>
  </type-mapping>
  <type-mapping>
    <from>Integer</from>
    <to>INTEGER</to>
  </type-mapping>
  <type-mapping>
    <from>Long</from>
    <to>BIGINT</to>
  </type-mapping>
  <type-mapping>
    <from>Float</from>
    <to>REAL</to>
  </type-mapping>
  <type-mapping>
    <from>Double</from>
    <to>DOUBLE PRECISION</to>
  </type-mapping>
  <type-mapping>
    <from>Date</from>
    <to>DATE</to>
  </type-mapping>
  <type-mapping>
    <from>Time</from>
    <to>TIME</to>
  </type-mapping>
  <type-mapping>
    <from>DateTime</from>
    <to>TIMESTAMP</to>
  </type-mapping>
</java-to-sql-type-conversions>
<temp-table-name-pattern>$$name$$</temp-table-name-pattern>
<create-temp-table-command>
  CREATE TABLE $$name$$ $$column_list$$
</create-temp-table-command>
<drop-temp-table-command>DROP TABLE $$name$$
</drop-temp-table-command>
<sql-filter>com.spotfire.ws.im.ds.BasicSQLFilter</sql-filter>
<metadata-provider>com.spotfire.ws.im.ds.BasicJDBCMetadataProvider
</metadata-provider>
<sql-runtime>com.spotfire.ws.im.ds.sql.BasicSQLRuntime
</sql-runtime>
<use-ansii-style-outer-join>false</use-ansii-style-outer-join>
</jdbc-type-settings>
-->

```

Example of XML Syntax for Oracle Data Source

The following example is the XML syntax for the Oracle data source.

```
<jdbc-type-settings>
<type-name>oracle</type-name>
<display-name>Oracle</display-name>
<driver>oracle.jdbc.driver.OracleDriver</driver>
<connection-url-pattern>jdbc:oracle:thin:@<host>:<port1521>:<sid></connection-url-
pattern>
<ping-command>SELECT 1 FROM DUAL</ping-command>
<metadata-provider>com.spotfire.ws.im.ds.sql.oracle.OracleMetadataProvider</metadata-
provider>
<sql-filter>com.spotfire.ws.im.ds.sql.oracle.OracleSQLFilter</sql-filter>
<sql-runtime>com.spotfire.ws.im.ds.sql.oracle.OracleSQLRuntime</sql-runtime>
<fetch-size>10000</fetch-size>
<batch-size>100</batch-size>
<table-types>TABLE, VIEW</table-types>
<supports-catalogs>true</supports-catalogs>
<supports-schemas>true</supports-schemas>
<max-in-clause-size>1000</max-in-clause-size>
<condition-list-threshold>10000</condition-list-threshold>
<expand-in-clause>false</expand-in-clause>
<table-expression-pattern>[ $$schema$$ . ] $$table$$ [ @ $$catalog$$ ] </table-expression-
pattern>
<date-format-expression>TO_CHAR( $$value$$ , 'YYYY-MM-DD' ) </date-format-expression>
<time-format-expression>TO_CHAR( $$value$$ , 'HH24:MI:SS' ) </time-format-expression>
<date-time-literal-format-expression>TO_DATE( ' $$value$$ ' , 'YYYY-MM-DD HH24:MI:SS' ) </
date-time-literal-format-expression>
<java-to-sql-type-conversions>
<type-mapping>
<from max-length="4000">String</from>
<to>VARCHAR2( $$value$$ ) </to>
</type-mapping>
<type-mapping>
<from>String</from>
<to>VARCHAR2(4000) </to>
</type-mapping>
<type-mapping>
<from>Integer</from>
<to>NUMBER(10) </to>
</type-mapping>
<type-mapping>
<from>Long</from>
<to>NUMBER(38) </to>
</type-mapping>
<type-mapping>
<from>Float</from>
<to>REAL </to>
</type-mapping>
<type-mapping>
<from>Double</from>
<to>FLOAT </to>
</type-mapping>
<type-mapping>
<from>Date</from>
<to>DATE </to>
</type-mapping>
<type-mapping>
```



```

<from>Time</from>
<to>DATE</to>
</type-mapping>
<type-mapping>
<from>DateTime</from>
<to>DATE</to>
</type-mapping>
</java-to-sql-type-conversions>
<create-temp-table-command>CREATE GLOBAL TEMPORARY TABLE $$name$$ $$column_list$$ ON
COMMIT PRESERVE ROWS</create-temp-table-command>
<drop-temp-table-command>TRUNCATE TABLE $$name$$;DROP TABLE $$name$$</drop-temp-
table-command>
<lob-threshold>4000</lob-threshold>
</jdbc-type-settings>

```

6.7.3 Configuring Information Services

Custom JDBC Drivers and Documentation

Before you begin configuring TIBCO Spotfire DecisionSite or TIBCO Spotfire to access a new type of JDBC data source, obtain the custom driver that you wish to use and also the documentation concerning it. The following instructions explain how to set up Information Services to access a new data source, but you may need additional information on how your specific driver works.

► **Configure IS to Access an IBM Information Integrator V8.1 database using the DB2 JDBC driver:**

- 1 Obtain the IBM DB2 Administration Client v8.1 and install it on the machine hosting Spotfire Analytics Server.
- 2 Run the <DB2_Admin_Client_Install_Dir>/sqllib/db2profile file to initialize the DB2 environment.
- 3 Make sure that you can connect to your DB2 database using the IBM DB2 Administration Client.
- 4 Rename the db2java.zip file (found in the java12 or java directory) to db2java.jar, and copy it to:

<installation directory>/server/webapps/spotfire/WEB-INF/lib

- 5 Uncomment the 'db2-ibm' <jdbc-type-settings> section in settings.xml located in:

<installation directory>/server/webapps/spotfire/WEB-INF

Comment: Uncomment means remove the <!-- and --> parts encompassing the section in the XML file.

- 6 Restart the Spotfire Analytics Server (see “Starting the Spotfire Analytics Server” on page 105).

► **Configure IS to Access a Sybase database using the jTDS JDBC driver:**

- 1 The jTDS JDBC driver necessary to connect to a Sybase database is included and preinstalled on the Spotfire Analytics Server.
- 2 Uncomment the 'sybase_jtds' <jdbc-type-settings> section in settings.xml located in:

<installation directory>/server/webapps/spotfire/WEB-INF

Comment: Uncomment means remove the <!-- and --> parts encompassing the section in the xml-file.

- 3 Restart the Spotfire Analytics Server (see “Starting the Spotfire Analytics Server” on page 105).

► **Configure IS to Access a MySQL database using MySQL JDBC driver:**

- 1 Obtain a JDBC driver for MySQL. Spotfire supports the MySQL Connector/J driver from MySQL AB (<http://www.mysql.com/>).

We recommend version 3.0.14 or later (mysql-connector-java-3.0.14-production-bin.jar).

- 2 Copy the driver jar file to

<installation directory>/server/webapps/spotfire/WEB-INF/lib

- 3 Uncomment the 'mysql' <jdbc-type-settings> section in settings.xml located in:

<installation directory>/server/webapps/spotfire/WEB-INF

Comment: Uncomment means remove the <!-- and --> parts encompassing the section in the xml-file.

- 4 Restart the Spotfire Analytics Server (see “Starting the Spotfire Analytics Server” on page 105).

Note: To be able to use the feature of aggregated columns in IS, the underlying database must support nested subqueries. This is only supported in MySQL version 4.0 and above. Hence, if you want to be able to use this feature, make sure that the version of MySQL that IS connects to is 4.0 or higher.

► **Configure IS to Access a SAS/SHARE database using the SAS/SHARE JDBC driver:**

- 1 Obtain the SAS/SHARE JDBC driver included in the SAS/SHARE distribution.
- 2 Copy the connect.jar and netutil.jar files to the

<installation directory>/server/webapps/spotfire/WEB-INF/lib

- 3 Uncomment the 'sas/share' <jdbc-type-settings> section in settings.xml located in:

<installation directory>/server/webapps/spotfire/WEB-INF

Comment: Uncomment means remove the <!-- and --> parts encompassing the section in the xml-file.

- 4 Restart the Spotfire Analytics Server (see “Starting the Spotfire Analytics Server” on page 105).

► **Configure IS to Access an ODBC Data Source using the Sun JDBC ODBC driver:**

The Sun JDBC ODBC driver is a part of the Sun JRE and therefore preinstalled on all Spotfire Analytics Servers.

Note: Unicode data is not supported using this configuration.

- 1 Uncomment the 'ODBC' <jdbc-type-settings> section in settings.xml located in:

<installation directory>/server/webapps/spotfire/WEB-INF

Comment: Uncomment means remove the <!-- and --> parts encompassing the section in the xml-file.

- 2 Restart the Spotfire Analytics Server (see “Starting the Spotfire Analytics Server” on page 105).

► **Configure IS to Access another type of database through a JDBC Data Source:**

Perform the following steps to deploy a new JDBC data source type configuration:

- 1 Copy applicable driver files (one or several jar-files) into:

<installation directory>/server/webapps/spotfire/WEB-INF/lib

- 2 Add your XML configuration to the file:

<installation directory>/server/webapps/spotfire/WEB-INF/settings.xml.

- 3 Add additional java files, if any, to:

<installation directory>/server/webapps/spotfire/WEB-INF/classes.

- 4 Restart Spotfire Analytics Server (see “Starting the Spotfire Analytics Server” on page 105).

6.7.4 Verify the New JDBC Data Source

You can now verify that the new JDBC Data Source can be accessed from Information Services.

► **To verify the JDBC data source from Spotfire DecisionSite:**

- 1 Log into DecisionSite Client as an administrator and start the 'Information Designer' application.
- 2 Choose the 'Data Source' workbench.
- 3 Enter a name for the data source connection.
- 4 Specify the data source type name in the type field.
- 5 Enter the connection URL.
- 6 Enter a username and a password to connect to the database.
- 7 Enter max/min-values for the connection pool.
- 8 Press Save.
- 9 The data source name should appear in the tree to the left, ready for use.

► **To verify the JDBC data source from TIBCO Spotfire:**

- 1 Log into TIBCO Spotfire as an administrator.
- 2 Select Tools > Create Information Link....
- 3 Click on the Setup Data Source link.
- 4 Enter a name for the data source connection.
- 5 Specify the type of data source.
- 6 Enter the connection URL.
- 7 Enter max/min-values for the connection pool.
- 8 Enter a username and a password to connect to the database.
- 9 Press Save.
- 10 Click on the Data sources tab in the left pane.
- 11 The data source name should appear in the tree to the left, ready for use.

6.7.5 Defining JDBC Connection Properties for JDBC Data Sources

The optional **<connection-properties>** parameter block in the **<jdbc-type-settings>** configuration can be used to define JDBC connection properties parameters to be used when connecting to the data sources of the given type. A typical use case for this feature is to specify encryption and integrity checksum algorithms for secure database connections.

Each connection property consists of a key-value pair. The syntax for specifying JDBC connection properties for a **<connection-pool>** is shown in the configuration example below.

When adding JDBC connection properties to a **<jdbc-type-setting>** configuration for an already used data source type, you need to open all data sources of that type for editing and save them again so that they are populated with the JDBC connection properties. It is not sufficient to just update the **<jdbc-type-setting>** configuration in the /WEB-INF/settings.xml file.

If you need different JDBC connection properties for different data sources of the same type, just duplicate the **<jdbc-type-setting>** configuration, rename the configurations for each variant needed and define the proper JDBC connection properties. Make sure to update any already existing data sources so that they are of the correct type.

Example: Defining JDBC Connection Properties for data source of type “oracle”:

```
<jdbc-type-settings>
  <type-name>oracle</type-name>
  <display-name>Oracle</display-name>
  <driver>oracle.jdbc.OracleDriver</driver>
  <connection-url-
pattern>jdbc:oracle:thin:@<host>;:<port>1521<port>;:<sid><sid></connection-url-
pattern>
  <ping-command>SELECT 1 FROM DUAL</ping-command>
  <connection-properties>
    <connection-property>
      <key>oracle.net.encryption_client</key>
      <value>REQUIRED</value>
    </connection-property>
    <connection-property>
      <key>oracle.net.encryption_types_client</key>
      <value>( 3DES168 )</value>
    </connection-property>
    <connection-property>
      <key>oracle.net.crypto_checksum_client</key>
      <value>REQUIRED</value>
    </connection-property>
    <connection-property>
      <key>oracle.net.crypto_checksum_types_client</key>
      <value>( MD5 )</value>
    </connection-property>
```

```

</connection-properties>
...
</jdbc-type-settings>

```

6.7.6 Advanced Connection Pool Configuration

Beginning with Spotfire Analytics Server 10.1 a new type of connection pool is used for the data sources in Information Services. The new connection pool was introduced for the user directory and other components from version 9.0. Those components retrieve their database configurations from the /WEB-INF/data-sources.xml file, but the configuration templates for the data sources in Information Services still resides in the /WEB-INF/settings.xml file.

Not all configuration parameters that appears in the /WEB-INF/data-sources.xml file are supported for data sources in Information Services, but the following special parameters are available:

- **“spotfire.pooling.data.source.scheme”**
(corresponds to the “pooling-scheme” parameter in the /WEB-INF/data-source.xml configuration file, see “/WEB-INF/data-sources.xml” on page 118).
- **“spotfire.pooling.data.source.connection.timeout”**
(corresponds to the “connection-timeout” parameter)
- **“spotfire.pooling.data.source.login.timeout”**
(corresponds to the “login-timeout” parameter).
- **“spotfire.kerberos.login.context”**
(corresponds to the “kerberos-login-context” parameter)

It is also possible to revert to the old type of connection pool by setting the **“spotfire.connection.pool.factory.data.source”** parameter to “init.commands.data.source”. The default value for this parameter is “pooling.data.source”.

All these parameters should be added as JDBC connection properties (see the previous section). However, they will never be used as real JDBC connection properties and will never be sent to a database server.

Example: Configuring a PoolingDataSource for Oracle databases

```

<jdbc-type-settings>
  <type-name>oracle</type-name>
  <display-name>Oracle</display-name>
  <driver>oracle.jdbc.OracleDriver</driver>
  <connection-url-
pattern>jdbc:oracle:thin:@&lt;host>;&lt;port1521>&lt;sid></connection-url-
pattern>
  <ping-command>SELECT 1 FROM DUAL</ping-command>
  <connection-properties>
    <connection-property>
      <key>spotfire.pooling.data.source.scheme</key>

```

```

    <value>WAIT_ADAPTIVE</value>
  </connection-property>
</connection-property>
  <key>spotfire.pooling.data.source.connection.timeout</key>
  <value>1800</value>
</connection-property>
</connection-property>
  <key>spotfire.pooling.data.source.login.timeout</key>
  <value>30</value>
</connection-property>
</connection-properties>
...
</jdbc-type-settings>

```

6.7.7 Using Kerberos Authentication for JDBC Data Sources

Configuration of Kerberos authentication for JDBC data source are performed in a similar way to the data sources in data-sources.xml, see Section 5.1.3.4 on page 123. See also Section 6.3.5 on page 197 for more information about how to create the necessary JAAS application configuration and Kerberos credentials.

Example: Configuring a PoolingDataSource for Oracle databases

```

<jdbc-type-settings>
  <type-name>oracle</type-name>
  <display-name>Oracle</display-name>
  <driver>oracle.jdbc.OracleDriver</driver>
  <connection-url-
pattern>jdbc:oracle:thin:@<host>:<port1521>:<sid></connection-url-
pattern>
  <ping-command>SELECT 1 FROM DUAL</ping-command>
  <connection-properties>
    <connection-property>
      <key>spotfire.kerberos.login.context</key>
      <value>DatabaseKerberos</value>
    </connection-property>
    <connection-property>
      <key>oracle.net.authentication_services</key>
      <value>( KERBEROS5 )</value>
    </connection-property>
  </connection-properties>
  ...
</jdbc-type-settings>

```

6.7.8 Configuring JDBC Data Sources for Kerberos Authentication with Delegated Credentials

Before configuring JDBC Data Sources for Kerberos authentication with delegated credentials, it must be verified that it is possible for clients to connect to the Spotfire Analytics Server using Kerberos authentication. When the server is correctly set up and everything works, it is time to proceed to the next step.

To set up Information Services to use delegated Kerberos credentials when making connections to database servers, the Spotfire Analytics Server's service account used for retrieving the ticket-granting ticket (TGT) must be given the permission to delegate client credentials. In the "Active Directory Users and Computers" control panel on the domain controller, the "Account" tab of the properties dialog for the service account contains an "Account is trusted for delegation" checkbox that can be checked to give the service account that permission.

After setting up the service account's delegation rights, a new JDBC Data Source must be created in the /WEB-INF/settings.xml file. Copy a non-Kerberos definition for the same type of data source and add the special JDBC connection property **"spotfire.connection.pool.factory.data.source"** with the value **"kerberos.data.source"**. All JDBC connection properties required to configure the JDBC driver for Kerberos authentication should also be added. Please consult your database server's documentation for more information about configuring the JDBC driver.

When all necessary JDBC connection properties have been added, save the file and restart the server. It is now possible to create a new data source based on this template.

Example: Setting up Kerberos authentication with delegated credentials for an Oracle database

```
<jdbc-type-settings>
  <type-name>oracle-kerberos</type-name>
  <display-name>Oracle Kerberos</display-name>
  <driver>oracle.jdbc.OracleDriver</driver>
  <connection-url-
pattern>jdbc:oracle:thin:@&lt;host&gt;:&lt;port1521&gt;:&lt;sid&gt;</connection-url-
pattern>
  <ping-command>SELECT 1 FROM DUAL</ping-command>
  <connection-properties>
    <connection-property>
      <key>spotfire.connection.pool.factory.data.source</key>
      <value>kerberos.data.source</value>
    </connection-property>
    <connection-property>
      <key>oracle.net.authentication_services</key>
      <value>(KERBEROS5)</value>
```



```

    </connection-property>
  </connection-properties>
  ...
</jdbc-type-settings>

```

6.8 Configuring Information Services for Heavy Load

The database holding the Information Model (IM) can either be the same instance as for the rest of TIBCO Spotfire DecisionSite, or a completely different database instance.

For heavy use of the Information Services (IS), it is better to place the Information Model on a different instance. Information Services is pre-configured to spawn 10 new Oracle connections. This can be changed in the file:

```
<installation directory>/server/webapps/spotfire/WEB-INF/im-service.xml
```

Edit in the part documented below.

```

<connection-pool name="im-connection-pool">
  <user>[login name]</user>
  <password>[password]</password>
  <driver-class>oracle.jdbc.driver.OracleDriver</driver-class>
  <max-count>10</max-count>
  <min-count>5</min-count>
  <ping-command>SELECT 1 FROM DUAL</ping-command>
  <connection-url>jdbc:oracle:thin:@{server name}:[port nr]:[database SID]</connection-
url>
</connection-pool>

```

Restart the server after these modifications have been made (see “Starting the Spotfire Analytics Server” on page 105).

These connections stay alive for as long as the server hosting Information Services is up and running. In order for Information Services to work properly, the Oracle instance that will be hosting the Information Model database must have the Oracle parameters that control the maximum number of open connections and open cursors set to a minimum value as follows:

processes = 200 (or more)

open_cursors = 200 (or more)

This is done by modifying the file "init.ora" that can be found in the "admin" directory in the Oracle installation directory (for Windows it is usually found in a directory called "pfile" which is, in turn, located in a directory with the same name as the database SID).

6.9 Pivot Column Naming Schemes

When pivoting data sets in Information Builder, the users can select how to name these new columns in the data set. By default there are two choices: **Spotfire Old Style** and **Spotfire New Style**. The individual users can also choose to edit and create a custom naming scheme from the UI.

However, there is also a way to add more naming schemes on the server which will then be available for all users to choose from in the UI.

► Adding a Pivot Column Naming Scheme:

- 1 Find the directory:

<installation directory>/server/webapps/spotfire/WEB-INF

- 2 Open the file **settings.xml** in a text editor.

- 3 Locate the following section:

```
<setting>
<category>spotfire.dat.reshape</category>
<name>column-naming-schemes</name>
<user-editable>true</user-editable>
<value xsi:type="dat:NamingSchemeArray">
<scheme xsi:type="dat:ColumnNamingScheme">
<name>Spotfire Old Style</name>
<default>true</default>
<pattern>%M(%V) for %C</pattern>
<category-string-separator>_</category-string-separator>
</scheme>
<scheme xsi:type="dat:ColumnNamingScheme">
<name>Spotfire New Style</name>
<default>false</default>
<pattern>%C - %M(%V)</pattern>
<category-string-separator>_</category-string-separator>
</scheme>
</value>
<description>Column name generation schemes.</description>
</setting>
```

- 4 Insert a new scheme after the last </scheme> tag, and edit it to suit your needs.

```
<scheme xsi:type="dat:ColumnNamingScheme">
<name>My Own Naming Scheme</name>
<default>true</default>
<pattern>%M(%V) for %C</pattern>
<category-string-separator>_</category-string-separator>
</scheme>
```

- 5 The <name> value is where you enter the name of the Naming scheme as it will appear in the drop-down list box in the Information Builder UI.
- 6 The <default> value can be set to either true or false. True means that it will be selected by default in the Information Builder UI. Make sure only one naming scheme in the settings.xml file is set to true, or the first scheme will be the default one.
- 7 The <pattern> value is where you define your naming scheme. Use the three parameters and any additional text to create the naming scheme you desire.

 %M = Computation Method

 %V = Value Columns

 %C = Category Values
- 8 The <category-string-separator> value is the character or characters used to separate multiple category strings, if such should occur.
- 9 Save the settings.xml file.
- 10 Restart the Spotfire Analytics Server for the changes to take effect (see “Starting the Spotfire Analytics Server” on page 105).

Example:

The following table is transformed by pivoting:

City	Month	Temp
London	February	4
New York	February	6
London	May	16
New York	May	19
London	August	28
New York	August	26
London	November	13
New York	November	11

By using the Expression pattern "[%C] - Aggregation: %M:(%V)" we would get the following table with column names.

City	[February] - Aggregation: avg(Temp)	[May] - Aggregation: avg(Temp)	[August] - Aggregation: avg(Temp)	[November] - Aggregation: avg(Temp)
London	4	16	28	13
New York	6	19	26	11

6.10 Resizing Temporary Tablespace

The tablespaces/database files for Spotfire Analytics Server using Oracle/MSSQL Database uses autoextend/autogrowth by default. If this turns out to be of an inappropriate for your needs alter this settings. It might be desired to alter the amount the files should be altered by with each increment. For Oracle there is a maxsize for each tablespace which should be reviewed. For MSSQL there is an unlimited growth this should also be reviewed. If the bundled database is used, it might be prudent to allocate the maximum total size between the tablespaces according to the typical usage.

6.11 Changing Administrator Email Address

To add an email address of your company's Spotfire Analytics Server administrator, you need to add the email address to the following file:

<installation directory>/server/webapps/spotfire/WEB-INF/web.xml

Find the tag:

<param-name>support.admin_email</param-name>

Change

<param-value/>

to

<param-value>myadministrator@company.com</param-value>

If you do not add any email address here, a contact email address will not display in the 'add software' page.

6.12 Modifying the Virtual Memory

If many simultaneous users intend to perform heavy data pivoting via Information Services or in other ways stress the server, you may need to modify the amount of memory available to the virtual machine. The application server's JVM must have equal settings for the initial and maximum heap sizes, otherwise data pivoting in Information Services will not work properly and there might be a risk that the server will run out of memory.

Note: Do not allocate too much heap memory because every JVM has a specific upper limit for how much memory it can handle. If the memory allocation exceeds this limit, the JVM may not start.

► **To Set Up the Start Script (not running as a service):**

Open the file <server install dir>/bin/catalina.bat in a text editor.

Alter the “256” values in the following entries:

```
-Xms256M -Xmx256M
```

to the amount of memory you desire to allocate.

Restart the server.

► **To Set Up the Service (when running as a service):**

Stop the service

Go to the <server install dir>/bin directory

Run <server install dir>/bin/service.bat remove TsAs101.

Edit the <server install dir>/bin/service.bat

Look for the entries:

```
--JvmMs 256 --JvmMx 256
```

Alter the “256” to suitable memory values (in MBytes).

Run <server install dir>/bin/service.bat install TsAs101

Start the service.

6.13 Configuring the Server for LDAPS

6.13.1 Preparations

6.13.1.1 Backup Configuration Files

Before changing user directory back-end, make sure to backup the following configuration file:

- <server install dir>\server\webapps\spotfire\WEB-INF\userdirconfig.xml
- <server install dir>\jdk\jre\lib\security\spotfire.login
- <server install dir>\jdk\jre\lib\security\cacerts

6.13.1.2 Setting Up for LDAPS

To make the Spotfire Analytics Server trust the LDAP server, the LDAP server's certificate must be added to the Spotfire Analytics Server's list of trusted certificates.

For more information on how to create a certificate for your LDAP server, please see the documentation for your specific LDAP server.

- 1 Open a command prompt and navigate to the <server install dir>\jdk\jre\lib\security directory. Enter the following command to add the LDAP server's certificate to the cacerts keystore (replace <ldapserver.crt> with the name of the file containing the certificate):

```
..\..\bin\keytool -import -file <ldapserver.crt> -
keystore cacerts -alias spotfire_ldaps
```

Enter the password to the cacerts keystore when prompted. The default password is "changeit".

- 2 Verify that the certificate has been successfully added by entering the command below. The certificate should be included in the displayed certificate list.

```
keytool -list -keystore cacerts -alias spotfire_ldaps
```

Enter the password to the cacerts keystore when prompted.

- 3 Open the <server install dir>\jdk\jre\lib\security\spotfire.login file and update the necessary LDAP parameters. Typically, modifying the **serverURL** parameter is sufficient. It should follow the pattern ldaps://ldapserver[:port], where the optional port number defaults to 636. If accessing the Global Catalog of an Active Directory server, the port number should be set to 3269.

Example: Accessing a Sun Directory Server

```
SpotfireLDAP
{
    com.spotfire.server.jaas.ldap.LDAPLoginModule
        required
        serverURL="ldaps://ldapsrv"
        contextNames="OU=Engineering,DC=example,DC=com"
        user="hagbard"
        password="ifkgbg04"
        nameAttribute="uid"
        userFilter="(objectClass=person)";
};
```

Example: Accessing the Active Directory's Global Catalog

```
SpotfireLDAP
{
    com.spotfire.server.jaas.ldap.LDAPLoginModule
        required
        serverURL="ldaps://engr-dc:3269"
        contextNames="OU=Engineering,DC=example,DC=com"
        user="hagbard"
        password="ifkgbg04"
        nameAttribute="sAMAccountName"
        userFilter="(objectClass=user)";
};
```

- 1 Open the <server install dir>\server\webapps\spotfire\WEB-INF\userdirconfig.xml file and edit the same parameters as in the previous step.

```
<userdir>

    <external-directory-provider>LDAP</external-directory-provider>

    ...

    <external-directory-provider-configuration>
        <provider-name>LDAP</provider-name>
        <provider-class>com.spotfire.server.userdir.ldap.LDAPUserDirectoryProvider</
provider-class>
        <config>
            <server>
                <ldap-server-type>activeDirectory</ldap-server-type>
                <server-url>ldaps://engr-dc:3269</server-url>
                <context-names>
                    <context-name>OU=Engineering,DC=example,DC=com</context-name>
                </context-names>
                <user>hagbard</user>
                <password>ifkgbg04</password>
            </server>
        </config>
    </external-directory-provider-configuration>
```

```
</config>  
</external-directory-provider-configuration>  
  
</userdir>
```

- 2 Restart the Spotfire Analytics Server (see “Starting the Spotfire Analytics Server” on page 105).

6.14 Resetting Passwords for the Database Table Login System

To reset the passwords for **all users** in the database, the administrator can run an SQL command in the database.

- 1 Start sqlplus (for an Oracle database), sqlcmd (for a Microsoft SQL Server database) or your preferred database tool and log in to the database. Use the account and database specified in the Server.Default data source in the <server installation>\server\webapps\spotfire\WEB-INF\data-sources.xml file.
- 2 For an Oracle database server, run the following SQL commands:

```
UPDATE USERS SET PASSWORD = CHR(16) || CHR(16) || '8iaByxiChEJ464jHbh7TEgWWCW8=';  
COMMIT;
```

For a Microsoft SQL Server database, run the following SQL commands:

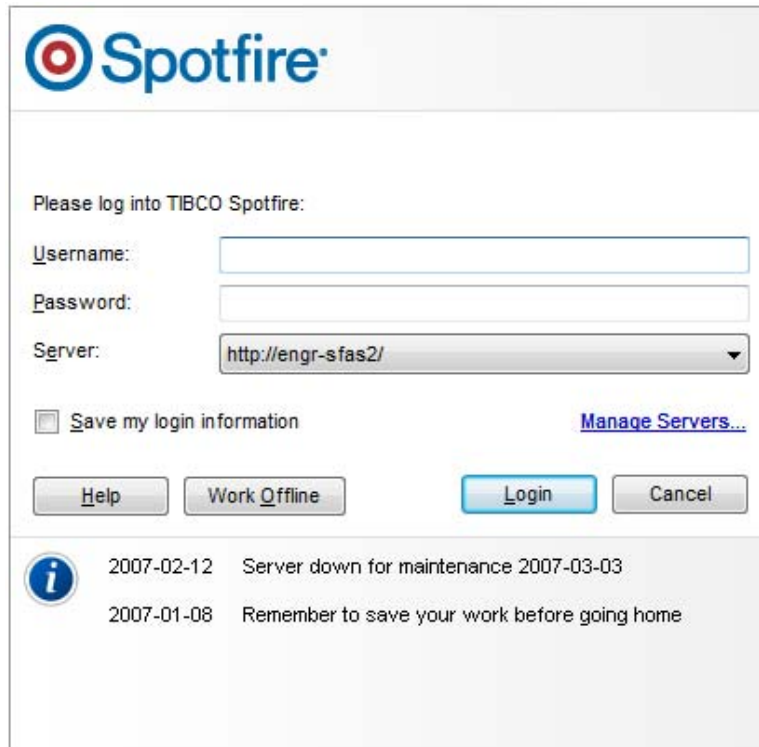
```
UPDATE USERS SET PASSWORD = NCHAR(16) + NCHAR(16) + '8iaByxiChEJ464jHbh7TEgWWCW8=';  
COMMIT;
```

- 3 Disconnect from the database. You do not need to restart the Spotfire Analytics Server.

All users, including any administrator account, will now have the password "spotfire".

6.15 Enabling RSS Feed in the Login Dialog

It is possible to configure the Spotfire Analytics Server to show messages in the login dialog for the end users. For example, news of upcoming scheduled maintenance of the Spotfire Analytics Server could be shown.



The image shows the Spotfire login dialog box. At the top is the Spotfire logo. Below it, the text "Please log into TIBCO Spotfire:" is displayed. There are three input fields: "Username:", "Password:", and "Server:". The "Server:" field has a dropdown menu showing "http://engr-sfas2/". Below the input fields is a checkbox labeled "Save my login information" and a link "Manage Servers...". At the bottom, there are four buttons: "Help", "Work Offline", "Login", and "Cancel". Below the buttons is a section with an information icon and two entries: "2007-02-12 Server down for maintenance 2007-03-03" and "2007-01-08 Remember to save your work before going home".

The login dialog will show a maximum of five or six entries.

To enable the RSS feed in the login dialog, you must edit the manifest file on the Spotfire Analytics Server:

/WEB-INF/manifest.xml

Add an <rss> node as shown below:

```
<client-login>
  <show-login-dialog>always</show-login-dialog>
  <always-online>false</always-online>
  <allow-save-information>true</allow-save-information>
  <offline-days-permitted>infinite</offline-days-permitted>
  <rss>/spotfire/rss.xml</rss>
</client-login>
```

One option is to specify a path to an rss.xml file on the Spotfire Analytics Server itself, which you can update manually with news. Another is to specify the URL to an external rss-feed.

Regardless, you must make sure the specified rss-feed complies with the standard RSS 2.0 specification, and that the source is available to the end users' clients. Note that HTML in the rss feed is not supported.

Note: If you want to make sure all users see the news in the login dialog, you can set the <show-login-dialog> node to "always". This

means the login dialog will be shown to all users regardless if they have opted to save their login credentials for automatic login.

Below is an example of an RSS 2.0 compliant RSS file:

```
<?xml version="1.0"?>
<rss version="2.0">
  <channel>
    <title>Spotfire Analytics Server News</title>
    <link>http://myserver/spotfire/rss</link>
    <description>My description goes here.</description>
    <language>en-us</language>
    <pubDate>Wed, 03 Jan 2007 04:00:00 GMT</pubDate>
    <lastBuildDate>Mon, 12 Feb 2007 09:41:01 GMT</lastBuildDate>
    <docs>http://myserver/spotfire/rss </docs>
    <generator>Weblog Editor 2.0</generator>
    <managingEditor>editor@example.com</managingEditor>
    <webMaster>webmaster@example.com</webMaster>

    <item>
      <title>Server down for maintenance 2008-03-03 </title>
      <link>http://sharepoint/news/item1.aspx</link>
      <description></description>
      <pubDate>Mon, 12 Feb 2007 09:39:21 GMT</pubDate>
      <guid>123456</guid>
    </item>

    <item>
      <title>Remember to save your work before going home</title>
      <link>http://internal/department/test</link>
      <description>Servers will be down this weekend.</description>
      <pubDate>Mon, 08 Jan 2007 11:06:42 GMT</pubDate>
      <guid>123455</guid>
    </item>
  </channel>
</rss>
```

6.16 Deploying and Configuring a Custom Credential Transform

A number of application configuration files contain references to subsystem passwords, which are by default stored in clear-text. If you want to store these passwords encrypted instead, you can use the Credential Transform SPI.

In general, the Credential Transform SPI enables the use of custom encryption and decryption algorithms for passwords. Once such a transform is implemented and enabled in the server, a command-line tool can be used to transform passwords.

Note that the transformed passwords do not automatically replace their clear-text representations in applicable configuration files. This must be manually performed in all applicable files.

Additionally, when Credential Transform is enabled, the passwords entered in the following user interfaces must be the encrypted representations:

- Library database connection password entered in the Library Administration user interface.
- Data source passwords entered in the DecisionSite Information Designer user interface.
- Data source connection passwords entered in the 'Create Information Link' user interface of TIBCO Spotfire Professional.

The Credential Transform SPI comes with one predefined transform: **com.spotfire.server.util.transform.Base64Transform**. This Base64 encoding/decoding transform should not be considered a real cryptographic transform, but it can still be handy to prevent the use of clear text passwords in the configuration files, or as a base for developing custom transforms.

6.16.1 Implementing a Custom Credential Transform

A custom Credential Transform is created by implementing the interface **com.spotfire.server.util.transform.CredentialTransform** as described in the SPI available in Spotfire Technology Network.

Once the transform is created and packaged in a Java archive (JAR) file, it needs to be deployed on the Spotfire Analytics Server by copying the JAR to the folder:
<installation dir>/server/webapps/spotfire/WEB-INF/lib

6.16.2 Editing the WEB-INF/web.xml File

Locate the web.xml file in the following directory, and open it in a text or XML editor.

<installation dir>/server/webapps/spotfire/WEB-INF/web.xml

Add the parameters **<credential.transform.class>** and **<credential.transform.configuration>** (if not already added) and set their respective values as described in Section 5.1.1.4 on page 113.

The following example shows how the built-in Base64Transform is added to the web.xml file:

```
<web-app>
```

```
...
```

```
<context-param>
  <param-name>credential.transform.class</param-name>
  <param-value>com.spotfire.server.util.transform.Base64Transform</param-value>
</context-param>
<context-param>
  <param-name>credential.transform.configuration</param-name>
  <param-value>UTF-8</param-value>
</context-param>

...

</web-app>
```

6.16.3 Running the Credential Transform Application

Run the built-in Credential Transform Application to encrypt your passwords. A list of the relevant passwords can be found in Section 6.16.4 on page 236.

The application requires a command line with a console. The standard Windows command prompt fulfills that requirement.

When executed, the tool accepts two arguments.

- The first is the class name of the custom transform implementation.
- The second argument is optional and contains any arguments that you may wish to pass to the transform.

To execute the transform application, type the following from command-line while having the **<installation dir>/server/webapps/spotfire/WEB-INF/lib** as the current work directory.

In this following example, **mytransform.jar** contains the transform implementation class **com.acme.transform.MyTransform**.

```
> java -cp dss.jar;dss-jaas.jar;logging.jar;log4j.jar;mytransform.jar
com.spotfire.server.util.transform.CredentialTransformApp
com.acme.transform.MyTransform
```

Once the application has started, you will be prompted for the password to encrypt. Enter the password and press Enter for the tool to encrypt your password and output the result on the command line.

6.16.4 Replacing Existing Clear-text Passwords

Once the Credential Transform Application has been used to obtain an encrypted password, all occurrences of clear-text passwords in the server configuration files must be manually replaced with their respective encrypted representations.

data-sources.xml

- Contains the default data source password(s).
<installation dir>\server\webapps\spotfire\WEB-INF

im-service.xml

- Contains the Information model database password.
<installation dir>\server\webapps\spotfire\WEB-INF

library-service.xml

- Contains the Library service database password.
<installation dir>\server\webapps\spotfire\WEB-INF

isis.xml

- Contains the ISIS data source passwords. Only applicable if any ISIS connections have been defined.
<installation dir>\server\webapps\spotfire\WEB-INF

6.16.4.1 LDAP Login System

If your Spotfire Analytics Server is configured to use an LDAP login system you need to replace the following passwords as well:

spotfire.login

- JAAS application configuration file.
 LDAP server connection password.
<installation dir>\jdk\jre\lib\security

userdirconfig.xml

- External directory provider configuration.
 LDAP server connection password.
<installation dir>\server\webapps\spotfire\WEB-INF

6.16.4.2 Windows Integrated NTLM System

If your Spotfire Analytics Server is configured to use an NTLM login system you need to replace the following passwords as well:

catalina.bat

- Web application server start script file.
 Property: jcifs.smb.client.password
<installation dir>\server\bin

service.bat

- Web server service installation script.
 Property: jcifs.smb.client.password
<installation dir>\server\bin

Important: The service needs to be removed and then reinstalled.

6.16.4.3 Upgraded Installations

If your Spotfire Analytics Server has been upgraded from older versions, passwords may also be found in the following files:

spotfire.login

- JAAS application configuration file.
Spotfire Analytics Server database server connection password.
<installation dir>\jdk\jre\lib\security

appmgrconfig.xml

- TIBCO Spotfire DecisionSite Application Manager configuration file.
<installation dir>\server\webapps\spotfire\WEB-INF

6.17 Changing to a Different JDK

This chapter provides information on how to use a different JDK than the one bundled with the Spotfire Analytics Server installer.

One reason for changing to a different JDK could be to run a 64-bit JDK on Windows. The JDK which is bundled with the Spotfire Analytics Server installer for Windows is a 32-bit version. The JDK included in the Spotfire Analytics Server installer for Solaris has both 32- and 64-bit support. However, to activate 64-bit support on Solaris the flag “-d64” should be added, see below.

The Spotfire Analytics Server requires a JDK and not only a JRE, since certain items are compiled in runtime. The bundled JDK is version jdk1.6.0_30, so this version or later should be used.

Note: The Windows NT Domain Login System uses a native 32-bit library. This login system will only work on Windows and 32-bit systems. Do not move the files in
<server install dir>/jdk/jre/lib/ext

If you want to change the JDK on a Spotfire Analytics Server that is already installed and working properly, the following things should be altered.

Changes need to be done to the start script:

On Windows, if you are running with the catalina startscript, alter:

```
<server install dir>/server/bin/catalina.bat
```

On Solaris:

```
<server install dir>/server/bin/catalina.sh
```

In these files, the JAVA_HOME variable needs to be altered to point to the new JDK, for example:

```
JAVA_HOME=/usr/jdk/instances/jdk1.6.0_XX
```

Next you need to make changes to the files and settings in the directory:

```
<installation dir>/jdk/jre/lib/security/
```

- java.security
- spotfire.login
- krb5.conf
- spotfire.keytab
- database.keytab (if present)

The changes can either be to copy these files to the same directory in the new JDK. This is not always desirable, for example if the JDK is installed for many users on Solaris. Instead of copying the files they can be pointed out with Java startup parameters. In the start script items could be added to the JAVA_OPTS.

java.security has a line which point out the spotfire.login file:

```
login.config.url.1=file:${java.home}/lib/security/spotfire.login
```

This line is not needed if you instead point out the file with an entry in JAVA_OPTS

```
-Djava.security.auth.login.config=/home/some_user/spotfire.login
```

The krb5.conf file can also be handled with JAVA_OPTS so it can be placed in another location

```
-Djava.security.krb5.conf=/home/some_user/krb5.conf
```

If the spotfire.keytab file is placed in another location, configuration entries pointing to it will need to change (for example, spotfire.login).

To make use of 64-bit support on Solaris (and Linux) another flag should be added to JAVA_OPTS:

```
-d64
```

It is worth mentioning that the directory where the server has been installed is self contained, that is, it could be copied to another location. If the absolute location is changed then some paths needs to be altered. The Windows service must to be reinstalled. The

deinstallation of the product will not work. But other than that, it should be possible to move an installation if some paths are altered.

An example of how JAVA_OPTS might look like, for a non kerberos setup:

```
JAVA_OPTS="-server -d64 -XX:+DisableExplicitGC -Xms16G -Xmx16G  
-Djava.security.auth.login.config=/home/some_user/  
spotfire.login"
```

If you are using the Windows Service to start the server, the service needs to be reinstalled. First the service needs to be removed:

```
<server install dir>/server/bin/service.bat remove TsAs101
```

The JAVA_HOME variable in service.bat must be altered to point to the new JDK, for example:

```
JAVA_HOME=C:\jdk1.6.0_XX
```

If you have opted to alter JAVA_OPTS above then the same alteration should be done in JvmOptions.

If the JDK is 64-bit, the following files need to be replaced with appropriate binaries for the processor architecture.

```
<server install dir>\server\bin\tomcat6.exe
```

```
<server install dir>\server\bin\tomcat6w.exe
```

These files can be downloaded from <http://tomcat.apache.org>.

Finally, restart the server and then reinstall the service:

```
<server install dir>\server\bin\service.bat install TsAs101
```


7 Appendix: License Information

TIBCO Spotfire Analytics Server - License Agreement

END USER LICENSE AGREEMENT ("AGREEMENT")

PLEASE READ CAREFULLY: IF YOU HAVE ANOTHER VALID, SIGNED AGREEMENT WITH TIBCO WHICH APPLIES TO THE SPECIFIC SOFTWARE, EQUIPMENT, CLOUD OR HOSTED SERVICES YOU WILL BE DOWNLOADING, ACCESSING OR OTHERWISE RECEIVING, (INDIVIDUALLY AND COLLECTIVELY REFERRED TO AS THE "PRODUCTS"), THAT OTHER AGREEMENT APPLIES TO THE PRODUCTS. OTHERWISE, BY USING, DOWNLOADING, INSTALLING, COPYING, OR ACCESSING PRODUCTS, OR BY CLICKING ON "I ACCEPT" ON OR ADJACENT TO THE SCREEN WHERE THIS AGREEMENT MAY BE DISPLAYED, YOU HEREBY AGREE TO BE BOUND BY AND ACCEPT THE TERMS OF THIS AGREEMENT ("ACCEPTANCE"). THIS AGREEMENT SHALL ALSO APPLY TO ANY MAINTENANCE OR CONSULTING SERVICES ("SERVICES") YOU ACQUIRE FROM TIBCO RELATING TO THE PRODUCT.

IF YOU DO NOT AGREE TO THESE TERMS 1) DO NOT DOWNLOAD OR INSTALL THE SOFTWARE, AND OR 2) DO NOT ACCESS OR REGISTER TO ACCESS ANY CLOUD OR HOSTED SERVICES. IF YOU DO NOT AGREE TO THESE TERMS, AND DELIVERY OF THE PRODUCTS IS AFFECTED, DO NOT USE, DOWNLOAD, INSTALL, COPY, OR ACCESS THE PRODUCTS. PROMPTLY RETURN THE PRODUCT WITH PROOF OF PURCHASE TO THE PARTY FROM WHOM YOU ACQUIRED IT AND OBTAIN A REFUND OF THE AMOUNT YOU PAID, IF ANY. IF YOU DOWNLOADED ANY SOFTWARE, CONTACT THE PARTY FROM WHOM YOU ACQUIRED IT.

IF YOU ARE ACCEPTING THIS AGREEMENT ON BEHALF OF ANOTHER PERSON OR PERSONS,, COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND EACH PERSON, COMPANY, OR LEGAL ENTITY TO THIS AGREEMENT. THIS AGREEMENT IS ENTERED INTO BY AND BETWEEN TIBCO SOFTWARE INC. and any entities, regardless of corporate status, controlled by, controlling, or under common control with TIBCO Software Inc. (COLLECTIVELY, "TIBCO", "WE", "US" OR "OUR") AND YOU, YOUR CO-WORKERS, YOUR EMPLOYEES, AGENTS AND CONTRACTORS AND ANY OTHER PERSON OR PERSONS, COMPANY OR OTHER LEGAL ENTITY ON WHOSE BEHALF YOU ARE ACCEPTING THIS AGREEMENT (COLLECTIVELY, "CUSTOMER", "YOU" OR "YOUR").

further, you warrant and agree that You are not (a) a citizen, national or resident of, and are not under the control of, the government of: Cuba, Iran, North Korea, Sudan, Syria, or any other country to which the United States has prohibited export, or (b) listed on the United States TREASURY Department'S lists of Specially Designated Nationals, Specially Designated Terrorists, OR Specially Designated Narcotic Traffickers, or listed on the United States COMMERCE Department'S Table of Denial Orders. You further warrant and agree that You will not (x) download or otherwise export or re-export the Products OR Materials, directly or indirectly, to persons on the abovementioned lists, (y) use the Products or Materials for, and will not allow the Products OR Materials to be used for, any purposes prohibited by United States OR OTHER APPLICABLE law, including, without limitation, for the development, design, manufacture or production of nuclear, chemical or biological weapons of mass destruction, and (z) download or otherwise export or re-export the Products or Materials, directly or indirectly, to the above mentioned countries or to citizens, nationals or residents of those countries.

1. Upon your Acceptance, the following shall govern your use of the Products and Services, except to the extent all or any portion are (a) subject to a separate written, duly executed agreement, or (b) also subject to the terms of an Addendum at the end of this Agreement, in which case the terms of such Addendum shall control over inconsistent terms in this Agreement.

2. Definitions. Capitalized terms used in this Agreement and not otherwise defined, are defined below or at <http://www.tibco.com/software/parametersdefinitions.jsp>. "Order Form" means any purchase order or similar document, written agreement, or a web store or web site order or registration requesting Products or Services. "Purchase Date" means the date the Order Form is accepted by us and in the case of a web store or web site transaction, the date of your download or access a Product. If proprietary source code is included as part of the standard delivery of a Product and is not subject to open source license terms, use of such source code is controlled by the terms of this Agreement. "Updates" means Product bug fixes, enhancements, and updates, if and when made generally available by us as part of Maintenance.

Appendix: License Information

3.Alpha, Beta and Evaluation Licenses. If the Products are provided or accessed for demonstration, alpha or beta testing, or evaluation purposes, then you agree (a) to use the Products solely for such purposes, (b) that the Products will not be used or deployed in a production or development environment, and (c) that such use shall automatically terminate upon the earlier of (i) thirty days from the date you receive the right to install or access the Product, (ii) your receipt of notice of termination from us, or (iii) you no longer have access to the Cloud or the Hosted Services.

4.License Grant. The Products are the property of TIBCO or its licensors and are protected by copyright and other laws. While TIBCO continues to own or have license rights to the Products, we hereby grant you a limited, non-transferable, non-exclusive license to use the Number of Units set forth in the Order Form solely for your internal business use.

5.License Term. The term of each license for a Product shall be either perpetual or limited as designated on an Order Form. If a Product is licensed on a limited term basis, then, unless otherwise set forth in an Order Form, the term shall commence on the Purchase Date and have the following duration:

Alpha, Beta and Evaluation - thirty (30) days.

Hosted Services - one (1) year

Cloud - one (1) year

Software purchases on a term limited basis - three (3) years

If you originally registered to download or access a Product for Alpha, Beta or Evaluation purposes, upon re-registration you may be permitted one (1) additional term. On expiration of a limited term, you must cease using and return or destroy all copies of the Products and related Confidential Information.

6.Delivery. Products are delivered electronically, and delivery deemed complete when duly made available to you.

7.Equipment Lease or Purchase.

A. Lease. The term of each Equipment Lease shall be limited as set forth in an Order Form. However, the first forty-five (45) days from the initial term Purchase Date shall be considered the first month of the term and charged as such. As long as you are not then in breach of any term of this Agreement, you will have the right to renew an Equipment Lease annually, for a one (1) year term, subject to payment of the annual lease renewal fee. We will send you a renewal invoice at least sixty (60) days prior to the term anniversary date. In the event we do not receive payment for the lease renewal thirty (30) days prior to the term anniversary date, the existing lease term will terminate at the end of the lease, in accordance with terms of this Agreement.

B. Purchase. When we accept your order to Purchase the Equipment, we agree to sell you the Equipment described in the Order Form. We transfer all title to the hardware component of the Equipment when we or our agent ships the Equipment. Notwithstanding the foregoing, we reserve, and you consent to our reservation of, a purchase money security interest in the Equipment until we receive the fees set forth in the Order Form. For a feature, conversion, or upgrade involving the removal of parts in connection with the Equipment, which parts become our property, we reserve, and you consent to our reservation of a security interest in the Equipment until we receive payment of all the amounts due and the removed parts. You authorize us to file appropriate documents to permit the perfection of our purchase money security interest.

C. Equipment Insurance. If you are leasing Equipment, You shall procure and continuously maintain and pay for (i) all risk insurance against loss of and damage to the Equipment for not less than the full replacement value of each Unit, naming us as loss payee, and (ii) public liability and property damage insurance insuring against third party personal and property damage in respect of the use and operation of the Equipment in an amount not less than 1,000,000 USD per occurrence, (iii) Each insurance policy shall name us as an additional named insured and a loss payee and provide that there shall be no recourse against us for payment of premiums or other amounts. The insurance shall be in such form and with such company or companies as shall be reasonably acceptable to us. You shall provide to us a certificate evidencing such insurance. You hereby appoint us as your attorney-in-fact to make claim for, receive payment of, and execute and endorse all documents, checks, or drafts received in payment for any loss or damage to the Equipment under any such insurance policy.

D. Equipment Delivery. Title is deemed to transfer upon delivery by (i) our agent to our designated freight carrier, FCA Ontario, Canada (Incoterms 2000), or (ii) by us to our designated freight carrier, FCA TIBCO's premises (Incoterms 2000). All freight, insurance and other shipping expenses shall be paid to the freight carrier by us. You will be invoiced for shipping and handling charges listed on the Order Form. Delivery is subject to the availability of Equipment.

8.Hosted Services. We shall use commercially reasonable efforts to make the Hosted Services you have purchased available 24 hours a day, 7 days a week, except for: (a) planned downtime under our direct control (of which we shall give at least 8 hours notice via the Hosted Services and which we shall schedule to the extent practicable during the weekend hours from 6:00 p.m. Pacific time Friday to 3:00 a.m. Pacific time Monday), (b) to the extent we are notified by third party service providers of planned downtime (of which we shall provide such notice to you via the Hosted services as soon we can reasonably do so), or (c) any unavailability caused by circumstances beyond our reasonable control, including, without limitation, acts of God, acts of government, flood, fire, earthquakes, civil unrest, acts of terror, strikes or other labor problems, internet service or third party hosting provider failures or delays ("Force Majeure"). Hosted Services are provided in accordance with applicable laws and government regulations.

9.Cloud. Provisioning of the Cloud will be confirmed electronically and delivery deemed complete when such confirmation is made available to you. Provisioning of the Cloud requires an account be established for you in TIBCOCommunity. You agree to and accept the Terms of Use for TIBCOCommunity (http://www.tibcommunity.com/themes/tibcotucon/resources/html/terms_of_use.html) if you use the credentials to access the TIBCOCommunity site. Certain Software products provided for installation by you and are provided solely to enable the functionality of the Cloud, and may not be used for any other purpose. You are solely responsible for procuring your own account with the applicable TIBCO approved third party service provider ("Provider") for the Cloud and for the technical operation of the content of your account.

10.Hosted Services and Cloud Restrictions.

A. In connection with your use of Hosted Services or a Cloud, in addition to the Restrictions below, you shall (i) be responsible for your users' compliance with this Agreement (ii) be solely responsible for the accuracy, quality, integrity and lawfulness of and of the means by which you acquire and disclose your data, (iii) not store or transmit infringing, libelous, or otherwise unlawful or tortious material or malicious code, nor store or transmit material in violation of third-party privacy rights, (iv) not sell, resell, rent or lease the Hosted Services or Cloud (v) use commercially reasonable efforts to prevent unauthorized access to or use of the Hosted Services or Cloud, and notify us promptly of any such unauthorized access or use, (vi) not interfere with or disrupt the integrity or performance of any Provider services or third-party data contained there, (vii) not attempt to gain unauthorized access to the Hosted Services, Cloud or their related systems or networks, and (viii) use the Hosted Services or Cloud only in accordance with any applicable Documentation and all applicable laws and government regulations. Hosted Services or the Cloud may be subject to other limitations, such as, for example, limits on disk storage space, on the number of calls or number of users, third party terms of use, etc., specified in the applicable Documentation, web store or web site. You are responsible for handling and processing notices sent to you by any third party claiming that our content in connection with the Hosted Services, Cloud or any Provider services violates such party's rights including, without limitation, notices pursuant to the Digital Millennium Copyright Act.

Appendix: License Information

B. You represent and warrant that you will not use Hosted Services or the Cloud to promote any illegal activities or post any materials in violation of any law. In addition, in using and accessing Hosted Services or the Cloud, you shall not use any third party software in connection with a Provider's or TIBCO service in any manner that requires, pursuant to the license applicable to such software, that any Provider or TIBCO property or services be: (i) disclosed or distributed in source code form; (ii) made available free of charge to recipients; or (c) modifiable without restriction by recipients. You represent and warrant that no software or content provided by you or your users in connection with your use of Hosted Services or the Cloud will contain any malicious or hidden mechanism or code for the purpose of damage or corrupting the Hosted Services, Cloud or the Provider service.

C. You are solely responsible for adequate security, protection and back up of your date/content. We are not responsible for Provider services; any unauthorized access; or the deletion, destruction, damage, loss or failure to store any of your content or other data that you submit or use in Hosted Services or the Cloud.

11.Restrictions. You agree not to (a) make more copies than the Number of Units (except for a reasonable number of copies for archival and disaster recovery purposes) or use any unlicensed versions of the Software; (b) use any Software not listed in an Order Form, even if such unlicensed software is made available to you as part of the general delivery mechanism for the Products; (c) provide access to the Products to anyone other than employees, contractors, or consultants who agree in writing to be bound by terms at least as protective of TIBCO as those in this Agreement; (d) sublicense, transfer, assign, distribute to any third party, pledge, lease, rent, or commercially share the Products or any of your rights under this Agreement (for the purposes of the foregoing a change in control of your company is deemed to be an assignment); (e) use the Products for purposes of providing a service bureau, including, without limitation, providing third-party hosting, or third-party application integration or application service provider-type services, or any similar services; (f) use the Products in connection with ultrahazardous activities, or any activity for which failure of the Products might result in death or serious bodily injury to you or a third party; or (g) directly or indirectly, in whole or in part, modify, translate, reverse engineer, decrypt, decompile, disassemble, make error corrections to, create derivative works based on, or otherwise attempt to discover the source code or underlying ideas or algorithms of the Products. You may engage in such conduct as is necessary to ensure the interoperability of the Software as required by law, provided that prior to commencing any decompilation or reverse engineering of any Software, you agree to observe strict obligations of confidentiality and provide us reasonable advance written notice and the opportunity to assist with and/or conduct such activity on your behalf and at your expense.

Any additional license parameters applicable to Products are set forth at <http://www.tibco.com/software/parametersdefinitions.jsp>.

12.Proprietary Notices. The Products, Documentation and Materials are proprietary to TIBCO and its licensors and protected by applicable U.S. and international patent, copyright, trademark and trade secret laws. TIBCO and its licensors shall retain ownership in the Products, Documentation and Materials; all derivatives thereof (in whole or part); and any intellectual property or other rights embodied therein. All proprietary notices incorporated in or affixed to any Products, Documentation or Materials shall be duplicated by you on all copies of the Products, Documentation, or Material, as applicable, and shall not be altered, removed or obliterated. Lease Equipment is, and shall at all times be and remain Our sole and exclusive property; you have no right, title or interest therein or thereto except as expressly set forth in this Agreement. You shall keep the Lease Equipment free and clear of all levies, liens and encumbrances and shall immediately notify us in writing of any circumstances with respect to the location of the Equipment which will adversely affect it or our security interests therein. You shall not install, attach, mount or otherwise house the Lease Equipment in a manner that would render it a fixture under applicable law within the jurisdiction in which the Lease Equipment is located.

13.Extraordinary Corporate Event. To the extent you or your successors or assigns enter into an Extraordinary Corporate Event after the Purchase Date, this Agreement shall not apply to those additional users, divisions or entities, which were added to your organization as a result of the Extraordinary Corporate Event until those additional users, divisions or entities are added to this Agreement by way of a written amendment signed by duly authorized officers of you and us.

14.Maintenance. Maintenance, if ordered (or if included in Lease, Cloud or Hosted Services), is provided under the policies set forth in the Maintenance Program Guide in effect at the time Maintenance services are provided. The policies set forth in the Maintenance Program Guide, incorporated into this Agreement, are subject to change at our discretion; however the level of Maintenance service provided by us will not be materially reduced if we change the policies during any twelve (12) month period for which Maintenance fees have been paid by you. The current version of the Maintenance Program Guide can be accessed at <http://www.tibco.com/services/support/default.jsp>. Updates provided under Maintenance or for any other reason by us, or our authorized resellers or distributors (if applicable), are subject to the license rights, limitations and restrictions of this Agreement. To receive Maintenance, all Products must be properly licensed and annual Maintenance fees paid. We are not obligated to continue providing Maintenance if annual Maintenance fees have not been paid.

15.Consulting Services.

A. You may procure installation, configuration, training or other consulting or support services ("Consulting Services") either in an Order Form, a purchase order (as set forth in the purchasing guidelines located at http://www.tibco.com/multimedia/purchase-order-guidelines-cons-services_tcm8-5441.pdf) or a work order executed by both parties ("Work Order"). We will use commercially reasonable efforts to perform such Consulting Services. Unless otherwise expressly agreed in a Work Order, all Consulting Services shall be: (i) performed on a time and materials basis ("T&M"), with meals, lodging, travel and other reasonably necessary out-of-pocket expenses ("Expenses") invoiced in addition to T&M fees, (ii) deemed accepted upon delivery, and (iii) incorporate the Work Order Terms defined at <http://www.tibco.com/resources/company/customer-relations/work-order-terms.pdf>.

B. We hereby grant you a nonexclusive license to use the Materials (and a reasonable number of copies thereof) solely for your internal operations in conjunction with your use of the Products. Materials obtained during your attendance at or from your purchase of virtual training courses, unless otherwise agreed in an Order Form, are limited to the one copy received by each attendee and may not be duplicated.

C. In the event you are purchasing a license to specific training course content as set forth in an Order Form, the content of each such training course shall constitute a Product for the purpose of this Agreement. Subject to your payment of fees due, you are granted a limited, non-transferable, non-exclusive, license to use, modify, translate, create derivative works, reproduce and distribute the Product solely for your internal business use, provided that the copyright notice and other legends of ownership are reproduced on each complete or partial copy of such Product. We retain all right, title and interest in the Product, excluding your Confidential Information. All complete or partial copies of the Product in any form shall be subject to the same terms as the original copy. The term of each license and level of annual Maintenance for the Product shall be as set forth in the Order Form.

16.Limited Warranty.

A. If you obtained Software directly from us, we warrant for a period of thirty (30) days from the Purchase Date that (i) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (ii) the Software will substantially conform to its Documentation. This limited warranty extends to you personally and is not transferable. Your sole and exclusive remedy and the entire liability of TIBCO and its licensors under this limited warranty will be, at our option, to repair or replace (with respect to the affected Software product), or refund the Software license fee. In the event of a refund, this Agreement shall terminate with respect to the affected Software product.

B. This warranty does not apply to any Software which (I) is licensed for alpha, beta, evaluation, testing or demonstration purposes for which we did not receive a license fee; (II) has been altered or modified, (Unless by us); (III) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by us; (IV) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident; or (V) is used in violation of any other term of this Agreement. You agree to pay us for any Maintenance or Consulting Services provided by us related to a breach of the foregoing on a T&M and Expense basis. If you have obtained the Software from a reseller or distributor, the terms of any warranty shall be as provided by such reseller or distributor; we provide no warranty to you with respect to such Software.

Appendix: License Information

C. EXCEPT AS SPECIFIED IN THIS LIMITED WARRANTY, THE PRODUCTS AND SERVICES ARE PROVIDED "AS IS". ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW. CERTAIN THIRD PARTY SOFTWARE MAY BE PROVIDED TO CUSTOMER ALONG WITH CERTAIN PRODUCTS AS AN ACCOMMODATION TO CUSTOMER. THIS THIRD PARTY SOFTWARE IS PROVIDED "AS IS", IS SUBJECT TO THE TERMS OF THE THIRD PARTY LICENSE, AND MAY ONLY BE USED WITH THE PRODUCTS. YOU MAY CHOOSE NOT TO USE THIRD PARTY SOFTWARE PROVIDED AS AN ACCOMMODATION. NO WARRANTY IS MADE REGARDING THE RESULTS OF ANY PRODUCTS OR SERVICES; THAT THE PRODUCTS WILL OPERATE WITHOUT ERRORS, PROBLEMS OR INTERRUPTIONS; THAT ERRORS OR BUGS WILL BE CORRECTED, OR THAT THE PRODUCT FUNCTIONALITY OR SERVICES WILL MEET YOUR REQUIREMENTS. NO TIBCO DEALER, DISTRIBUTOR, AGENT OR EMPLOYEE IS AUTHORIZED TO MAKE ANY MODIFICATIONS, EXTENSIONS OR ADDITIONS TO THIS WARRANTY ON TIBCO'S BEHALF.

17. Indemnity. If you obtained the Software from us directly, then we agree at our own expense to defend or, at our option, to settle, any claim or action brought against you to the extent it is based on a claim that the unmodified Software infringes any patent issued by the United States, Canada, Australia, Japan, or any member of the European Union, or any copyright, or any trade secret of a third party. We will indemnify and hold you harmless from and against any damages, costs and fees reasonably incurred (including reasonable attorneys' fees) that are attributable to such claim or action and which are assessed against you in a final judgment; provided that we are promptly notified in writing of such claim, we have the exclusive right to control such defense and/or settlement, and you provide reasonable assistance (at our expense) in the defense thereof. In no event shall you settle any claim, action or proceeding without our prior written approval. In the event of any such claim, litigation or threat thereof, we, at our sole option and expense, shall (a) procure for you the right to continue to use the Software, (b) replace or modify the Software with functionally equivalent software. If such license or modification is not commercially reasonable (in our reasonable opinion), we may cancel this Agreement with respect to the affected Software product upon sixty days prior written notice to you and refund to you the unamortized portion of the associated license fees paid by you to us based on a five-year straight-line depreciation. This Section states our entire liability with respect to the infringement of any intellectual property rights, and you hereby expressly waive any other liabilities or obligations we have with respect thereto. The foregoing indemnity shall not apply to the extent any claim is based on or attributable to (x) modifications made by you to the Software, or portions thereof, (y) such claim would have been avoided by use of the then-current release version of the Software, or (z) your continued allegedly infringing activity after being provided with modifications that would have avoided the alleged infringement.

18. Limitation of Liability.

A. EXCEPT AS PROVIDED UNDER THE INDEMNITY ABOVE; OR IN CONNECTION WITH THE MISAPPROPRIATION OF THE OTHER PARTY'S INTELLECTUAL PROPERTY, INCLUDING, WITHOUT LIMITATION, TRADE SECRETS; DAMAGES FOR BODILY INJURY, DEATH, DAMAGE TO REAL OR TANGIBLE PERSONAL PROPERTY; OR INTENTIONAL OR GROSS NEGLIGENCE (THE "EXCLUDED MATTERS"), IN NO EVENT WILL EITHER PARTY OR TIBCO'S LICENSORS BE LIABLE FOR ANY LOSS OR UNAVAILABILITY OF OR DAMAGE TO DATA, LOST REVENUE, LOST PROFITS, FAILURE TO REALIZE EXPECTED SAVINGS, DAMAGE TO REPUTATION, BUSINESS INTERRUPTION, DOWNTIME COSTS, OR ANY OTHER INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, PUNITIVE, EXEMPLARY OR SIMILAR TYPE OF DAMAGES ARISING OUT OF THIS AGREEMENT, THE USE OR THE INABILITY TO USE THE PRODUCTS, OR THE PROVISION OF ANY MAINTENANCE, CONSULTING SERVICES, EVEN IF A PARTY HAS BEEN ADVISED OR WAS AWARE OR SHOULD HAVE BEEN AWARE OF THE POSSIBILITY OF SUCH COSTS, EXPENSES OR DAMAGES.

B. EXCEPT FOR THE EXCLUDED MATTERS, IN NO EVENT SHALL A PARTY'S LIABILITY TO THE OTHER, WHETHER IN CONTRACT, TORT (INCLUDING ACTIVE OR PASSIVE NEGLIGENCE), BREACH OF WARRANTY, CLAIMS BY THIRD PARTIES OR OTHERWISE, EXCEED THE GREATER OF 50,000 USD OR THE PRICE PAID BY YOU UNDER THE APPLICABLE ORDER FORM.

C. THE FOREGOING LIMITATIONS SHALL APPLY EVEN IF THE ABOVE-STATED REMEDY OR LIMITED WARRANTY FAILS OF ITS ESSENTIAL PURPOSE. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO CUSTOMER. TO THE EXTENT ALLOWED BY LOCAL LAW, THESE LIMITATIONS WILL APPLY REGARDLESS OF THE BASIS OF LIABILITY, INCLUDING NEGLIGENCE, MISREPRESENTATION, BREACH OF ANY KIND, OR ANY OTHER CLAIMS IN CONTRACT, TORT OR OTHERWISE.

19. Confidentiality.

A. "Confidential Information" means any information disclosed by either party, whether or not marked, including, without limitation, the terms of this Agreement; the Products; Materials; individual contact information provided by either party; Product or related performance test results derived by you, including but not limited to benchmark test results; and your Protected Data and Output. Each party agrees to protect Confidential Information in the same manner as it protects its own Confidential Information (but using no less than a reasonable degree of protection) and shall only disclose Confidential Information to those with a need to know that information and who have agreed in writing to be bound by terms at least as protective as those contained in this Agreement. Information will not be deemed Confidential Information if (i) available to the public other than by a breach of a confidentiality obligation, (ii) rightfully received from a third party not in breach of a confidentiality obligation, (iii) independently developed by one party without use of the Confidential Information of the other; (iv) known to the recipient at the time of disclosure (other than under a separate confidentiality obligation); or (v) produced in compliance with applicable law or court order, provided the other party is given reasonable advance notice of the obligation to produce Confidential Information. Each party agrees to indemnify the other for any damages (including reasonable expenses) the other may sustain resulting from the unauthorized use and/or disclosure of the other's Confidential Information and that money damages would not be a sufficient remedy for a breach of confidentiality. The parties shall be entitled to seek injunctive or other equitable relief without the necessity of posting a bond even if otherwise normally required. Such injunctive or equitable relief shall not be the exclusive remedy for any breach of confidentiality, but shall be in addition to all other rights and remedies available at law or in equity.

B. To the extent we are exposed to individual personal data owned or otherwise held by you during the provision of Hosted Services, Cloud, or Services, which is subject to various data protection laws and/or regulations ("Protected Data"), we agree to treat such Protected Data in accordance with the Customer Privacy and Security Statement set forth at http://www.tibco.com/customer_privacy_security_statement.jsp (the "Statement"). The policies and procedures set forth in the Statement as well as those set forth in the Data Protection Policy Statement at http://www.tibco.com/resources/data_protection_statement.pdf are in place to meet our obligations for the protection, integrity and confidentiality of any Protected Data which exceed our standard obligations to safeguard Confidential Information.

C. Confidential Information shall remain the sole property of the disclosing party, and each party acknowledges and agrees that it does not acquire any rights therein. Use by a recipient of Confidential Information for the purposes contemplated under this Agreement, including, but not limited to, any configuration or use by you of Products or Materials shall not affect or diminish the disclosing party's rights, title and interest in and to Confidential Information.

D. We may use any individual contact information provided by you or your users for support, product information and other business to business communications in connection with this Agreement. In the event you or your users wish to "opt-out" you should do so on the web store or web site page where you originally submitted provided your information or at <http://tibco.market2lead.com/go/tibco/unsubscribe?userId=179027619&>.

E. You acknowledge and agree that any feedback, suggestions, comments, improvements, modifications and other information (including any ideas, concepts, "know-how" or techniques contained therein) that you provide to us about our Products or their performance (collectively, "Feedback") shall not be deemed as your Confidential Information and may be used, disclosed, disseminated and/or published by us for any purpose, including developing, manufacturing and marketing products incorporating Feedback, without obligation of any kind to you, and you waive any rights whatsoever in or to all Feedback.

Appendix: License Information

20.Export. Products, Documentation, Materials and related technical data, are subject to U.S. export control laws, including without limitation the U.S. Export Administration Act and its associated regulations and may be subject to export or import regulations of other countries. You agree that you will not nor permit your users to export or re-export the Licenser Software, Documentation and Materials in any form in violation of any applicable export or import laws of any jurisdiction.

21.Government Use. If the Products or Services are being or have been acquired with U.S. Federal Government funds, or you are an agency, department, or other entity of the United States Government ("Government"), the use, duplication, reproduction, release, modification, disclosure or transfer of the Software, Maintenance or Services, or any related documentation of any kind, including technical data, or manuals, is restricted in accordance with Federal Acquisition Regulation 12.212 for civilian agencies and Defense Federal Acquisition Regulation Supplement 227.7202 for military agencies. The Products and Services are COMMERCIAL ITEMS AS DEFINED BY THE FEDERAL ACQUISITION REGULATION. Use by the Government is further restricted according to the terms of this Agreement and any amendment hereto.

22.Entire Agreement. This Agreement, and any terms which are incorporated by written reference (including written reference to information contained in a URL, Documentation or reference policy) constitutes the entire agreement between the parties with respect to the use of the Products and Services, and supersedes all proposals, oral or written, and all other representations, statements, negotiations and undertakings relating to the subject matter hereof. All orders of Products or Services by you to us shall be deemed to occur, with or without reference, under the terms of this Agreement, unless expressly superseded by a signed written agreement between the parties. Except for additional terms you have agreed to in connection with our web stores or web sites, none of the terms of the Order Form (other than the product names, Number of Units, level of Maintenance, description of Consulting Services, and fees due in connection therewith) shall apply for any reason or purpose whatsoever, regardless of any statement on any Order Form to the contrary. Neither the license to use granted in this Agreement nor the obligation to pay license fees are dependent upon the performance by any party of any Consulting Services or the supply of any other software program or product.

23.Termination.

A. This Agreement and all Order Forms shall automatically terminate if: (i) either party files for bankruptcy, or otherwise goes into receivership, becomes insolvent or makes an assignment for the benefit of creditors; or (ii) a writ of attachment or execution is levied on the Equipment (where we are lessor) and is not released or satisfied within ten (10) days thereafter, or (iii) where we are lessor or in a Purchase where payment in full to us has not been made, if a receiver is appointed in any proceeding or action to which you are a party with authority to take possession or control of the Equipment. In all cases, the Equipment shall be promptly returned to us and not be treated as your asset.

B. Maintenance or Consulting Services may be terminated: (i) by either party upon a default of the other, such default remaining uncured for fifteen days from written notice from the non-defaulting party; (ii) upon the filing for bankruptcy or insolvency of the other party, (iii) by either party upon prior written notice at least sixty (60) days prior to the end of any annual Maintenance term; or (iv) by you for Consulting Services, upon ten (10) days prior written notice or (e) by us for Consulting Services upon thirty (30) days prior written notice. Termination of Maintenance or Consulting Services shall not terminate this Agreement.

C. A Cloud will terminate if or when your or our agreement for services with a Provider is terminated or otherwise expires for any reason. In the event of a termination of your Provider services, by Provider, in connection with a Cloud, without cause (where you are not in breach), to the extent you have pre-paid us fees for the Cloud, you may submit written notice requesting a refund, such notice to include evidence of Provider's termination without cause (e.g. a copy of Provider's notice of termination). Following receipt of such written notice, we will refund the pre-paid unearned pro-rata portion, from the date we received your notice, for the remaining Cloud term, or in the case of multiple Cloud purchases, each remaining term. In the event of a termination, for any reason, of TIBCO Provider service accounts upon which we rely to provide Hosted Services or the Cloud, to the extent you have pre-paid us fees for Hosted Services or Cloud to us, we will refund, as of the date of notice of termination from Provider to us, for the unearned pro-rata portion of the prepaid fees.

D. You may terminate this Agreement in its entirety at any time, in regard to Software, by destroying all copies of the Software. We may terminate this Agreement at any time, in regard to Software provided to you for evaluation or alpha/beta purposes. In the case of an evaluation of Equipment, where we exercise our right to terminate the Lease for a reason other than your breach of the Agreement, and you have pre-paid fees for the month in which our termination occurs, we will refund the unearned monthly pro-rated fee to you within thirty (30) days following our receipt of the returned Equipment.

E. If a license, Cloud, Hosted Services or Lease under this Agreement terminates or expires, or upon termination of this Agreement in its entirety for any reason, you shall (i) cease using the Products, Documentation, and related Confidential Information, and (ii) return or notify us in writing within thirty (30) days after termination that you have destroyed any Software (excluding Equipment), Documentation, related Confidential Information, and all copies thereof, whether or not modified or merged into other materials. Equipment shall be returned in good repair, condition and working order (ordinary wear and tear resulting from proper use thereof excepted), by delivering the Equipment to our designated carrier. You are responsible for all costs associated with de-installation of equipment and returning the Equipment in accordance with the Equipment Return Guidelines available at http://www.tibco.com/resources/equipment_return_guidelines.pdf.

F. Termination of this Agreement, any license, Cloud, Hosted Services or Lease, or any Order Form shall not limit either party from pursuing other remedies available to it, including injunctive relief, nor shall such termination relieve you of your obligation to pay all fees that have accrued or are otherwise owed by you under this Agreement. Except as set forth in sections entitled "Termination", "Limited Warranty" or "Indemnity", all fees paid under or in connection with this Agreement are non-refundable and no right of set off exists. The parties' rights and obligations under this section and sections entitled "Limited Warranty", "Indemnity", "Limitation of Liability", "Proprietary Notices", "Confidentiality", "General", "Governing Law" and your warranties in connection with Hosted Services and the Cloud, shall survive the expiration or earlier termination of this Agreement.

24. Open Source Software. If you use any third party software not supplied by us, including any open source software, in conjunction with any Product, you must ensure that such use does not require any of the following, pursuant to the terms of such software: (i) disclosure or distribution of any Product in source code form; or (ii) licensing of any Product for the purpose of making derivative works; or (iii) redistribution of any Product at no charge. For the avoidance of doubt, you may not combine Product with any software licensed under any version of or derivative of the GNU General Public License ("GPL") in any manner that could cause, or could be interpreted or asserted to cause, the Product or any modifications to the Product to become subject to the terms of the GPL.

25. Special Product Provisions. Software products TIBCO BusinessEvents®, TIBCO Collaborative Information Manager™, TIBCO ActiveMatrix® Service Performance Manager, TIBCO® ActiveFulfillment (and each of the foregoing, when included in any Bundle or Embedded/ Bundled Products) are subject to a restricted license and contain third party proprietary code that you can only use in conjunction with the Software and may be subject to additional terms as provided by us.

26. General. All payments of fees due shall be made in U.S. dollars, net 30 from Purchase Date, or, for any other amounts coming due hereafter, net 30 from our invoice. Fees do

Appendix: License Information

not include sales, use, withholding, value-added or similar taxes, and you agree to pay all sales, use, value-added, goods and services, consumption, withholding, excise and any other similar taxes or government charges, exclusive of our income tax. You agree to pay all reasonable costs incurred (including reasonable attorneys' fees) in collecting past due amounts. Except as set forth in the sections entitled "Limited Warranty", "Indemnity" and "Termination" all fees paid under or in connection with this Agreement are non-refundable and no right of set-off exists. A service charge of one and one-half percent per month will be applied to all invoices that are not paid on time. No delay in the performance of any obligation by either party, excepting all obligations to make payment, shall constitute a breach of this Agreement to the extent caused by Force Majeure. You hereby grant us and our independent auditors the right to audit your compliance with this Agreement and report any results to our licensors. You agree to provide reasonable assistance to ensure a complete and accurate audit by us and our independent auditors. If any portion of this Agreement is found to be void or unenforceable, the remaining provisions shall remain in full force and effect. All notices related to this Agreement shall be in writing. Notices will be effective if dispatched by facsimile; or electronic mail; by hand; reliable overnight delivery service or first-class, pre-paid mail if sent to the contract address for the intended recipient set forth in the Order Form. A copy of any notice of default, breach or termination shall also being sent to that party's General Counsel.

27. Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the State of California, United States of America, as if performed wholly within the state and without giving effect to the principles of conflict of law. The United Nations Convention on Contracts for the International Sale of Goods and the Uniform Computer Information Transactions Act are excluded from application hereto.

Addenda:

Version December 2010

Copyright © 1994-2010 TIBCO Software Inc. ALL RIGHTS RESERVED.

Third Party Software Notices and License Agreements

ANTLR 2.7.6

ANTLR 1989-2004 Developed by Terence Parr.

Apache Axis 1.4.0

Apache Commons Discovery 0.2

Apache Commons Logging 1.0.4

Apache Jakarta Regexp 1.2

Apache Log4J 1.2.13

Apache Tomcat 6.0.35

Apache XalanJ 2.5

Apache Xerces-J 2.4.0

IBM WSDL4J 1.5.1

Apache License

Version 2.0, January 2004

<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction,

and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable

Appendix: License Information

copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.
4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:
 - (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
 - (b) You must cause any modified files to carry prominent notices stating that You changed the files; and
 - (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
 - (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with

the conditions stated in this License.

5. **Submission of Contributions.** Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.
6. **Trademarks.** This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.
7. **Disclaimer of Warranty.** Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.
8. **Limitation of Liability.** In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.
9. **Accepting Warranty or Additional Liability.** While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

Jaxen Xpath Engine 1.0

Copyright (C) 2000-2002 bob mcwhirter & James Strachan.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Appendix: License Information

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the disclaimer that follows these conditions in the documentation and/or other materials provided with the distribution.
3. The name "Jaxen" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact license@jaxen.org.
4. Products derived from this software may not be called "Jaxen", nor may "Jaxen" appear in their name, without prior written permission from the Jaxen Project Management (pm@jaxen.org).

This product includes software developed by the Jaxen Project (<http://www.jaxen.org/>).

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE Jaxen AUTHORS OR THE PROJECT CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Jaxen Project and was originally created by bob mcwhirter <bob@werken.com> and James Strachan <jstrachan@apache.org>. For more information on the Jaxen Project, please see <<http://www.jaxen.org/>>.

Java CIFS Client Library (JCIFS) 0.9.5

GNU Lesser General Public License v2.1, February 1999

This product uses Java CIFS Client Library. Java CIFS Client Library is distributed pursuant to the terms of the Lesser General Public License.

The source code for the Java CIFS Client Library may be obtained from <http://jcifs.samba.org>.

For a period of time not to exceed three years from the Purchase Date, TIBCO also offers to provide Customer, upon written request of Customer, a copy of the source code for Java CIFS Client Library."

Java CIFS Client Library Extension Suite (JCIFS-Ext) 0.9.4

GNU Lesser General Public License v2.1, February 1999

This product uses Java CIFS Client Library Extension Suite. Java CIFS Client Library Extension Suite is distributed pursuant to the terms of the Lesser General Public License.

The source code for the Java CIFS Client Library Extension Suite may be obtained from <http://sourceforge.net/projects/jcifs-ext>. For a period of time not to exceed three years from the Purchase Date, TIBCO also offers to provide Customer, upon written request of Customer, a copy of the source code for Java CIFS Client Library Extension Suite.

JDOM 1.0b9

This product includes software developed by the JDOM Project (<http://www.jdom.org/>)

jTDS 1.2.2

GNU Lesser General Public License v2.1, February 1999

This product uses jTDS. jTDS is distributed pursuant to the terms of the Lesser General Public License.

The source code for the jTDS may be obtained from <http://jtds.sourceforge.net>. For a period of time not to exceed three years from the Purchase Date, TIBCO also offers to provide Customer, upon written request of Customer, a copy of the source code for jTDS.

Oracle JDBC Drivers for 11g 11.1.0.6.0

This product includes Oracle Technology Network JDBC Drivers. Oracle is a limited third party beneficiary to the TIBCO EULA, with respect to the Oracle Technology Network JDBC Drivers.

Saxpath 1.0 FCS

Copyright (C) 2000-2002 werken digital.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the disclaimer that follows these conditions in the documentation and/or other materials provided with the distribution.
3. The name "SAXPath" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact license@saxpath.org.
4. Products derived from this software may not be called "SAXPath", nor may "SAXPath" appear in their name, without prior written permission from the SAXPath Project Management (pm@saxpath.org).

This product includes software developed by the

Appendix: License Information

SAXPath Project (<http://www.saxpath.org/>).

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE SAXPath AUTHORS OR THE PROJECT CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the SAXPath Project and was originally created by bob mcwhirter <bob@werken.com> and James Strachan <jstrachan@apache.org>. For more information on the SAXPath Project, please see <<http://www.saxpath.org/>>.

Sun Java Development Kit (JDK) 1.6.0_30

As provided in Java™ SE Development Kit additional copyright notices and license terms may be applicable to portions of the Software and are set forth in the THIRDPARTYLICENSEREADME.txt file.

DO NOT TRANSLATE OR LOCALIZE.

%% The following software may be included in this product: CS CodeViewer v1.0;
Use of any of this software is governed by the terms of the license below:
Copyright 1999 by CoolServlets.com.

Any errors or suggested improvements to this class can be reported as instructed on CoolServlets.com. We hope you enjoy this program... your comments will encourage further development! This software is distributed under the terms of the BSD License. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. Neither name of CoolServlets.com nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY COOLSERVLETS.COM AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT

(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE."

%% The following software may be included in this product: Crimson v1.1.1 ; Use of any of this software is governed by the terms of the license below:

```

/*
 * The Apache Software License, Version 1.1
 *
 *
 * Copyright (c) 1999-2000 The Apache Software Foundation. All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 * notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 * notice, this list of conditions and the following disclaimer in
 * the documentation and/or other materials provided with the
 * distribution.
 *
 * 3. The end-user documentation included with the redistribution,
 * if any, must include the following acknowledgment:
 * "This product includes software developed by the
 * Apache Software Foundation (http://www.apache.org/)."
 * Alternately, this acknowledgment may appear in the software itself,
 * if and wherever such third-party acknowledgments normally appear.
 *
 * 4. The names "Crimson" and "Apache Software Foundation" must
 * not be used to endorse or promote products derived from this
 * software without prior written permission. For written
 * permission, please contact apache@apache.org.
 *
 * 5. Products derived from this software may not be called "Apache",
 * nor may "Apache" appear in their name, without prior written
 * permission of the Apache Software Foundation.
 *
 * THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED
 * WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
 * OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
 * DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
 * LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
 * USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND
 * ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
 * OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT
 * OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * =====*
 * This software consists of voluntary contributions made by many
 * individuals on behalf of the Apache Software Foundation and was
 * originally based on software copyright (c) 1999, International
 * Business Machines, Inc., http://www.ibm.com. For more
 * information on the Apache Software Foundation, please see
 * <http://www.apache.org/>.

```

Appendix: License Information

*/

%% The following software may be included in this product: Xalan J2; Use of any of this software is governed by the terms of the license below:

Apache License
Version 2.0, January 2004
<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. "Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity. "You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies

Appendix: License Information

with the conditions stated in this License.

5. **Submission of Contributions.** Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. **Trademarks.** This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. **Disclaimer of Warranty.** Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. **Limitation of Liability.** In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. **Accepting Warranty or Additional Liability.** While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use

this file except in compliance with the License. You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

%% The following software may be included in this product: NSIS 1.0j; Use of any of this software is governed by the terms of the license below:
Copyright (C) 1999-2000 Nullsoft, Inc.

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.
Justin Frankel justin@nullsoft.com

%% Some Portions licensed from IBM are available at:
<http://www.ibm.com/software/globalization/icu/>

%% Portions Copyright Eastman Kodak Company 1992

%% Lucida is a registered trademark or trademark of Bigelow & Holmes in the U.S. and other countries.

%% Portions licensed from Taligent, Inc.

%% The following software may be included in this product: IAIK PKCS Wrapper; Use of any of this software is governed by the terms of the license below:

Copyright (c) 2002 Graz University of Technology. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment:

Appendix: License Information

"This product includes software developed by IAIK of Graz University of Technology."

Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names "Graz University of Technology" and "IAIK of Graz University of Technology" must not be used to endorse or promote products derived from this software without prior written permission.

5. Products derived from this software may not be called "IAIK PKCS Wrapper", nor may "IAIK" appear in their name, without prior written permission of Graz University of Technology.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE LICENSOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

%% The following software may be included in this product: Document Object Model (DOM) v. Level 3; Use of any of this software is governed by the terms of the license below:

W3C SOFTWARE NOTICE AND LICENSE

<http://www.w3.org/Consortium/Legal/2002/copyright-software-20021231>

This work (and included software, documentation such as READMEs, or other related items) is being provided by the copyright holders under the following license. By obtaining, using and/or copying this work, you (the licensee) agree that you have read, understood, and will comply with the following terms and conditions.

Permission to copy, modify, and distribute this software and its documentation, with or without modification, for any purpose and without fee or royalty is hereby granted, provided that you include the following on ALL copies of the software and documentation or portions thereof, including modifications:

- 1.The full text of this NOTICE in a location viewable to users of the redistributed or derivative work.
- 2.Any pre-existing intellectual property disclaimers, notices, or terms and conditions. If none exist, the W3C Software Short Notice should be included (hypertext is preferred, text is permitted) within the body of any redistributed or derivative code.
- 3.Notice of any changes or modifications to the files, including the date changes were made. (We recommend you provide URIs to the location from which the code is derived.)

THIS SOFTWARE AND DOCUMENTATION IS PROVIDED "AS IS," AND COPYRIGHT HOLDERS MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE OR DOCUMENTATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

COPYRIGHT HOLDERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE SOFTWARE OR DOCUMENTATION. The name and trademarks of copyright holders may NOT be used in advertising or publicity pertaining to the software without specific, written prior permission. Title to copyright in this software and any associated documentation will at all times remain with copyright holders.

This formulation of W3C's notice and license became active on December 31 2002. This version removes the copyright ownership notice such that this license can be used with materials other than those owned by the W3C, reflects that ERCIM is now a host of the W3C, includes references to this specific dated version of the license, and removes the ambiguous grant of "use". Otherwise, this version is the same as the previous version and is written so as to preserve the Free Software Foundation's assessment of GPL compatibility and OSI's certification under the Open Source Definition. Please see our Copyright FAQ for common questions about using materials from our site, including specific terms and conditions for packages like libwww, Amaya, and Jigsaw. Other questions about this notice can be directed to site-policy@w3.org.

%% The following software may be included in this product: Xalan, Xerces; Use of any of this software is governed by the terms of the license below: /*

```
* The Apache Software License, Version 1.1
*
*
* Copyright (c) 1999-2003 The Apache Software Foundation. All rights
* reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. The end-user documentation included with the redistribution,
*    if any, must include the following acknowledgment:
*       "This product includes software developed by the
*        Apache Software Foundation (http://www.apache.org/)."
```

Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

```
*
* 4. The names "Xerces" and "Apache Software Foundation" must
*    not be used to endorse or promote products derived from this
*    software without prior written permission. For written
*    permission, please contact apache@apache.org.
*
* 5. Products derived from this software may not be called "Apache",
*    nor may "Apache" appear in their name, without prior written
*    permission of the Apache Software Foundation.
*
```

Appendix: License Information

```
* THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED
* WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
* OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
* DISCLAIMED.  IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
* LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
* USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND
* ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
* OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT
* OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
* =====
*
* This software consists of voluntary contributions made by many
* individuals on behalf of the Apache Software Foundation and was
* originally based on software copyright (c) 1999, International
* Business Machines, Inc., http://www.ibm.com.  For more
* information on the Apache Software Foundation, please see http://www.apache.org
*
```

%% The following software may be included in this product: W3C XML Conformance Test Suites v. 20020606; Use of any of this software is governed by the terms of the license below:

W3C SOFTWARE NOTICE AND LICENSE

Copyright 1994-2002 World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved.
<http://www.w3.org/Consortium/Legal/>

This W3C work (including software, documents, or other related items) is being provided by the copyright holders under the following license. By obtaining, using and/or copying this work, you (the licensee) agree that you have read, understood, and will comply with the following terms and conditions:

Permission to use, copy, modify, and distribute this software and its documentation, with or without modification, for any purpose and without fee or royalty is hereby granted, provided that you include the following on ALL copies of the software and documentation or portions thereof, including modifications, that you make:

1. The full text of this NOTICE in a location viewable to users of the redistributed or derivative work.
2. Any pre-existing intellectual property disclaimers, notices, or terms and conditions. If none exist, a short notice of the following form (hypertext is preferred, text is permitted) should be used within the body of any redistributed or derivative code: "Copyright [\$date-of-software] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. <http://www.w3.org/Consortium/Legal/>"
3. Notice of any changes or modifications to the W3C files, including the date changes were made. (We recommend you provide URIs to the location from which the code is derived.)

THIS SOFTWARE AND DOCUMENTATION IS PROVIDED "AS IS," AND COPYRIGHT HOLDERS

MAKENO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITEDTO, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THATTHE USE OF THE SOFTWARE OR DOCUMENTATION WILL NOT INFRINGE ANY THIRD PARTYPATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

COPYRIGHT HOLDERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL ORCONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE SOFTWARE OR DOCUMENTATION.

The name and trademarks of copyright holders may NOT be used in advertising or publicity pertaining to the software without specific, written prior permission. Title to copyright in this software and any associated documentation will at all times remain with copyright holders.

This formulation of W3C's notice and license became active on August 14 1998 soas to improve compatibility with GPL. This version ensures that W3C software licensing terms are no more restrictive than GPL and consequently W3C software may be distributed in GPL packages. See the older formulation for the policy prior to this date. Please see our Copyright FAQ for common questions about using materials from our site, including specific terms and conditions for packages like libwww, Amaya, and Jigsaw. Other questions about this notice can be directed to site-policy@w3.org.

%% The following software may be included in this product: W3C XML Schema Test Collection v. 1.16.2; Use of any of this software is governed by the terms of the license below: W3C DOCUMENT NOTICE AND LICENSE

Copyright 1994-2002 World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique,Keio University). All Rights Reserved.
<http://www.w3.org/Consortium/Legal/>

Public documents on the W3C site are provided by the copyright holders under the following license. The software or Document Type Definitions (DTDs) associated with W3C specifications are governed by the Software Notice. By using and/or copying this document, or the W3C document from which this statement is linked,you (the licensee) agree that you have read, understood, and will comply with the following terms and conditions:

Permission to use, copy, and distribute the contents of this document, or theW3C document from which this statement is linked, in any medium for any purpose and without fee or royalty is hereby granted, provided that you include the following on ALL copies of the document, or portions thereof, that you use:

1. A link or URL to the original W3C document.
2. The pre-existing copyright notice of the original author, or if it doesn't exist, a notice of the form: "Copyright [\$date-of-document] World Wide WebConsortium, (Massachusetts Institute of Technology, Institut National deRecherche en Informatique et en Automatique, Keio University). All Rights Reserved. <http://www.w3.org/Consortium/Legal/>" (Hypertext is preferred, but atextual representation is permitted.)
3. If it exists, the STATUS of the W3C document.

When space permits, inclusion of the full text of this NOTICE should be provided. We request that authorship attribution be provided in any software,documents, or other items or products that you create pursuant to the

Appendix: License Information

implementation of the contents of this document, or any portion thereof.

No right to create modifications or derivatives of W3C documents is granted pursuant to this license. However, if additional requirements (documented in the Copyright FAQ) are satisfied, the right to create modifications or derivatives is sometimes granted by the W3C to individuals complying with those requirements. THIS DOCUMENT IS PROVIDED "AS IS," AND COPYRIGHT HOLDERS MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR TITLE; THAT THE CONTENTS OF THE DOCUMENT ARE SUITABLE FOR ANY PURPOSE; NOR THAT THE IMPLEMENTATION OF SUCH CONTENTS WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

COPYRIGHT HOLDERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE DOCUMENT OR THE PERFORMANCE OR IMPLEMENTATION OF THE CONTENTS THEREOF.

The name and trademarks of copyright holders may NOT be used in advertising or publicity pertaining to this document or its contents without specific, written prior permission. Title to copyright in this document will at all times remain with copyright holders.

This formulation of W3C's notice and license became active on April 05 1999 so as to account for the treatment of DTDs, schema's and bindings. See the older formulation for the policy prior to this date. Please see our Copyright FAQ for common questions about using materials from our site, including specific terms and conditions for packages like libwww, Amaya, and Jigsaw. Other questions about this notice can be directed to site-policy@w3.org. webmaster (last updated by reagle on 1999/04/99.)

%% The following software may be included in this product: Mesa 3-D graphics library v. 5; Use of any of this software is governed by the terms of the license below:

core Mesa code	include/GL/gl.h	Brian Paul
Mesa GLX driver	include/GL/glx.h	Brian Paul
Mesa Ext registry	include/GL/glext.h	SGI
SGI Free B	include/GL/glxext.h	

Mesa license:

The Mesa distribution consists of several components. Different copyrights and licenses apply to different components. For example, GLUT is copyrighted by Mark Kilgard, some demo programs are copyrighted by SGI, some of the Mesa device drivers are copyrighted by their authors. See below for a list of Mesa's components and the copyright/license for each.

The core Mesa library is licensed according to the terms of the XFree86 copyright (an MIT-style license). This allows integration with the XFree86/DRId project. Unless otherwise stated, the Mesa source code and documentation is licensed as follows:

Copyright (C) 1999-2003 Brian Paul All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the

Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESSOR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL BRIAN PAUL BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

SGI FREE SOFTWARE LICENSE B (Version 1.1 [02/22/2000])

1. Definitions.

1.1 "Additional Notice Provisions" means such additional provisions as appear in the Notice in Original Code under the heading "Additional Notice Provisions."

1.2 "Covered Code" means the Original Code or Modifications, or any combination thereof.

1.3 "Hardware" means any physical device that accepts input, processes input, stores the results of processing, and/or provides output.

1.4 "Larger Work" means a work that combines Covered Code or portions thereof with code not governed by the terms of this License.

1.5 "Licensable" means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.6 "License" means this document.

1.7 "Licensed Patents" means patent claims Licensable by SGI that are infringed by the use or sale of Original Code or any Modifications provided by SGI, or any combination thereof.

1.8 "Modifications" means any addition to or deletion from the substance or structure of the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is: A. Any addition to the contents of a file containing Original Code and/or addition to or deletion from the contents of a file containing previous Modifications. B. Any new file that contains any part of the Original Code or previous Modifications.

1.9 "Notice" means any notice in Original Code or Covered Code, as required by and in compliance with this License.

1.10 "Original Code" means source code of computer software code that is described in the source code Notice required by Exhibit A as Original Code, and updates and error corrections specifically thereto.

1.11 "Recipient" means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 8. For legal entities, "Recipient" includes any entity that controls, is controlled by, or is under common control with Recipient. For purposes of this definition, "control" of an entity means (a)

Appendix: License Information

the power, direct or indirect, to direct or manage such entity, or (b) ownership of fifty percent (50%) or more of the outstanding shares or beneficial ownership of such entity.

1.12 "Recipient Patents" means patent claims Licensable by a Recipient that are infringed by the use or sale of Original Code or any Modifications provided by SGI, or any combination thereof.

1.13 "SGI" means Silicon Graphics, Inc.

1.14 "SGI Patents" means patent claims Licensable by SGI other than the Licensed Patents.

2. License Grant and Restrictions.

2.1 SGI License Grant. Subject to the terms of this License and any third party intellectual property claims, for the duration of intellectual property protections inherent in the Original Code, SGI hereby grants Recipient a worldwide, royalty-free, non-exclusive license, to do the following: (i) under copyrights Licensable by SGI, to reproduce, distribute, create derivative works from, and, to the extent applicable, display and perform the Original Code and/or any Modifications provided by SGI alone and/or as part of a Larger Work; and (ii) under any Licensable Patents, to make, have made, use, sell, offer for sale, import and/or otherwise transfer the Original Code and/or any Modifications provided by SGI. Recipient accepts the terms and conditions of this License by undertaking any of the aforementioned actions. The patent license shall apply to the Covered Code if, at the time any related Modification is added, such addition of the Modification causes such combination to be covered by the Licensed Patents. The patent license in Section 2.1(ii) shall not apply to any other combinations that include the Modification. No patent license is provided under SGI Patents for infringements of SGI Patents by Modifications not provided by SGI or combinations of Original Code and Modifications not provided by SGI.

2.2 Recipient License Grant. Subject to the terms of this License and any third party intellectual property claims, Recipient hereby grants SGI and any other Recipients a worldwide, royalty-free, non-exclusive license, under any Recipient Patents, to make, have made, use, sell, offer for sale, import and/or otherwise transfer the Original Code and/or any Modifications provided by SGI.

2.3 No License For Hardware Implementations. The licenses granted in Section 2.1 and 2.2 are not applicable to implementation in Hardware of the algorithms embodied in the Original Code or any Modifications provided by SGI.

3. Redistributions.

3.1 Retention of Notice/Copy of License. The Notice set forth in Exhibit A, below, must be conspicuously retained or included in any and all redistributions of Covered Code. For distributions of the Covered Code in source code form, the Notice must appear in every file that can include a text comments field; in executable form, the Notice and a copy of this License must appear in related documentation or collateral where the Recipient's rights relating to Covered Code are described. Any Additional Notice Provisions which actually appears in the Original Code must also be retained or included in any and all redistributions of Covered Code.

3.2 Alternative License. Provided that Recipient is in compliance with the terms of this License, Recipient may, so long as without derogation of any of SGI's rights in and to the Original Code, distribute the source code and/or

executable version(s) of Covered Code under (1) this License; (2) a license identical to this License but for only such changes as are necessary in order to clarify Recipient's role as licensor of Modifications; and/or (3) a license of Recipient's choosing, containing terms different from this License, provided that the license terms include this Section 3 and Sections 4, 6, 7, 10, 12, and 13, which terms may not be modified or superseded by any other terms of such license. If Recipient elects to use any license other than this License, Recipient must make it absolutely clear that any of its terms which differ from this License are offered by Recipient alone, and not by SGI. It is emphasized that this License is a limited license, and, regardless of the license form employed by Recipient in accordance with this Section 3.2, Recipient may relicense only such rights, in Original Code and Modifications by SGI, as it has actually been granted by SGI in this License.

3.3 Indemnity. Recipient hereby agrees to indemnify SGI for any liability incurred by SGI as a result of any such alternative license terms Recipient offers.

4. Termination. This License and the rights granted hereunder will terminate automatically if Recipient breaches any term herein and fails to cure such breach within 30 days thereof. Any sublicense to the Covered Code that is properly granted shall survive any termination of this License, absent termination by the terms of such sublicense. Provisions that, by their nature, must remain in effect beyond the termination of this License, shall survive.

5. No Trademark Or Other Rights. This License does not grant any rights to: (i) any software apart from the Covered Code, nor shall any other rights or licenses not expressly granted hereunder arise by implication, estoppel or otherwise with respect to the Covered Code; (ii) any trade name, trademark or service mark whatsoever, including without limitation any related right for purposes of endorsement or promotion of products derived from the Covered Code, without prior written permission of SGI; or (iii) any title to or ownership of the Original Code, which shall at all times remains with SGI. All rights in the Original Code not expressly granted under this License are reserved.

6. Compliance with Laws; Non-Infringement. There are various worldwide laws, regulations, and executive orders applicable to dispositions of Covered Code, including without limitation export, re-export, and import control laws, regulations, and executive orders, of the U.S. government and other countries, and Recipient is reminded it is obliged to obey such laws, regulations, and executive orders. Recipient may not distribute Covered Code that (i) in any way infringes (directly or contributorily) any intellectual property rights of any kind of any other person or entity or (ii) breaches any representation or warranty, express, implied or statutory, to which, under any applicable law, it might be deemed to have been subject.

7. Claims of Infringement. If Recipient learns of any third party claim that any disposition of Covered Code and/or functionality wholly or partially infringes the third party's intellectual property rights, Recipient will promptly notify SGI of such claim.

8. Versions of the License. SGI may publish revised and/or new versions of the License from time to time, each with a distinguishing version number. Once Covered Code has been published under a particular version of the License, Recipient may, for the duration of the license, continue to use it under the terms of that version, or choose to use such Covered Code under the terms of any subsequent version published by SGI. Subject to the provisions of Sections 3 and 4 of this License, only SGI may modify the terms applicable to Covered Code created under this License.

Appendix: License Information

9. **DISCLAIMER OF WARRANTY.** COVERED CODE IS PROVIDED "AS IS." ALL EXPRESS AND IMPLIED WARRANTIES AND CONDITIONS ARE DISCLAIMED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. SGI ASSUMES NO RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE. SHOULD THE SOFTWARE PROVE DEFECTIVE IN ANY RESPECT, SGI ASSUMES NO COST OR LIABILITY FOR SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY IS AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT SUBJECT TO THIS DISCLAIMER.

10. **LIMITATION OF LIABILITY.** UNDER NO CIRCUMSTANCES NOR LEGAL THEORY, WHETHER TORT (INCLUDING, WITHOUT LIMITATION, NEGLIGENCE OR STRICT LIABILITY), CONTRACT, OR OTHERWISE, SHALL SGI OR ANY SGI LICENSOR BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, LOSS OF DATA, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SGI'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THAT EXCLUSION AND LIMITATION MAY NOT APPLY TO RECIPIENT.

11. **Indemnity.** Recipient shall be solely responsible for damages arising, directly or indirectly, out of its utilization of rights under this License. Recipient will defend, indemnify and hold harmless Silicon Graphics, Inc. from and against any loss, liability, damages, costs or expenses (including the payment of reasonable attorneys fees) arising out of Recipient's use, modification, reproduction and distribution of the Covered Code or out of any representation or warranty made by Recipient.

12. **U.S. Government End Users.** The Covered Code is a "commercial item" consisting of "commercial computer software" as such terms are defined in title 48 of the Code of Federal Regulations and all U.S. Government End Users acquire only the rights set forth in this License and are subject to the terms of this License.

13. **Miscellaneous.** This License represents the complete agreement concerning the its subject matter. If any provision of this License is held to be unenforceable, such provision shall be reformed so as to achieve as nearly as possible the same legal and economic effect as the original provision and the remainder of this License will remain in effect. This License shall be governed by and construed in accordance with the laws of the United States and the State of California as applied to agreements entered into and to be performed entirely within California between California residents. Any litigation relating to this License shall be subject to the exclusive jurisdiction of the Federal Courts of the Northern District of California (or, absent subject matter jurisdiction in such courts, the courts of the State of California), with venue lying exclusively in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys fees and ex penses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation that provides that the language of a contract shall be construed against the drafter shall not apply to this License.

Exhibit A License Applicability. Except to the extent portions of this file are made subject to an alternative license as permitted in the SGI Free Software License B, Version 1.1 (the "License"), the contents of this file are subject

only to the provisions of the License. You may not use this file except in compliance with the License. You may obtain a copy of the License at Silicon Graphics, Inc., attn: Legal Services, 1600 Amphitheatre Parkway, Mountain View, CA 94043-1351, or at: <http://oss.sgi.com/projects/FreeB> Note that, as provided in the License, the Software is distributed on an "AS IS" basis, with ALL EXPRESS AND IMPLIED WARRANTIES AND CONDITIONS DISCLAIMED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. Original Code. The Original Code is: [name of software, version number, and release date], developed by Silicon Graphics, Inc. The Original Code is Copyright (c) [dates of first publication, as appearing in the Notice in the Original Code] Silicon Graphics, Inc. Copyright in any portions created by third parties is as indicated elsewhere herein. All Rights Reserved. Additional Notice Provisions: [such additional provisions, if any, as appear in the Notice in the Original Code under the heading "Additional Notice Provisions"]

%% The following software may be included in this product: Byte Code Engineering Library (BCEL) v. 5; Use of any of this software is governed by the terms of the license below:

Apache Software License

/

=====

The Apache Software License, Version 1.1

Copyright (c) 2001 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).". Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names "Apache" and "Apache Software Foundation" and "Apache BCEL" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this software may not be called "Apache", "Apache BCEL", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT

Appendix: License Information

NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org>. /

%% The following software may be included in this product: Regexp, Regular Expression Package v. 1.2; Use of any of this software is governed by the terms of the license below: The Apache Software License, Version 1.1

Copyright (c) 2001 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).". Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names "Apache" and "Apache Software Foundation" and "Apache Turbine" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this software may not be called "Apache", "Apache Turbine", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache

Software Foundation, please see <http://www.apache.org>.

%% The following software may be included in this product: CUP Parser Generator for Java v. 0.10k; Use of any of this software is governed by the terms of the license below: CUP Parser Generator Copyright Notice, License, and Disclaimer

Copyright 1996-1999 by Scott Hudson, Frank Flannery, C. Scott Ananian

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both the copyright notice and this permission notice and warranty disclaimer appear in supporting documentation, and that the names of the authors or their employers not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

The authors and their employers disclaim all warranties with regard to this software, including all implied warranties of merchantability and fitness. In no event shall the authors or their employers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of this software.

%% The following software may be included in this product: JLex: A Lexical Analyzer Generator for Java v. 1.2.5; Use of any of this software is governed by the terms of the license below: JLEX COPYRIGHT NOTICE, LICENSE AND DISCLAIMER.

Copyright 1996-2003 by Elliot Joel Berk and C. Scott Ananian

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both the copyright notice and this permission notice and warranty disclaimer appear in supporting documentation, and that the name of the authors or their employers not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

The authors and their employers disclaim all warranties with regard to this software, including all implied warranties of merchantability and fitness. In no event shall the authors or their employers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of this software.

Java is a trademark of Oracle Corporation. References to the Java programming language in relation to JLex are not meant to imply that Oracle endorses this product.

%% The following software may be included in this product: SAX v. 2.0.1; Use of any of this software is governed by the terms of the license below: Copyright Status

SAX is free!

In fact, it's not possible to own a license to SAX, since it's been placed in the public domain.

Appendix: License Information

No Warranty

Because SAX is released to the public domain, there is no warranty for the design or for the software implementation, to the extent permitted by applicable law. Except when otherwise stated in writing the copyright holders and/or other parties provide SAX "as is" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The entire risk as to the quality and performance of SAX is with you. Should SAX prove defective, you assume the cost of all necessary servicing, repair or correction.

In no event unless required by applicable law or agreed to in writing will any copyright holder, or any other party who may modify and/or redistribute SAX, be liable to you for damages, including any general, special, incidental or consequential damages arising out of the use or inability to use SAX (including but not limited to loss of data or data being rendered inaccurate or losses sustained by you or third parties or a failure of the SAX to operate with any other programs), even if such holder or other party has been advised of the possibility of such damages.

Copyright Disclaimers

This page includes statements to that effect by David Megginson, who would have been able to claim copyright for the original work.

SAX 1.0

Version 1.0 of the Simple API for XML (SAX), created collectively by the membership of the XML-DEV mailing list, is hereby released into the public domain.

No one owns SAX: you may use it freely in both commercial and non-commercial applications, bundle it with your software distribution, include it on a CD-ROM, list the source code in a book, mirror the documentation at your own web site, or use it in any other way you see fit.

David Megginson, sax@megginson.com
1998-05-11

SAX 2.0

I hereby abandon any property rights to SAX 2.0 (the Simple API for XML), and release all of the SAX 2.0 source code, compiled code, and documentation contained in this distribution into the Public Domain. SAX comes with NO WARRANTY or guarantee of fitness for any purpose.

David Megginson, david@megginson.com
2000-05-05

%% The following software may be included in this product: Cryptix; Use of any of this software is governed by the terms of the license below:

Cryptix General License

Copyright © 1995-2003 The Cryptix Foundation Limited. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1.Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2.Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. THIS SOFTWARE IS PROVIDED BY THE CRYPTIX FOUNDATION LIMITED AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE CRYPTIX FOUNDATION LIMITED OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

%% The following software may be included in this product: W3C XML Schema Test Collection; Use of any of this software is governed by the terms of the license below:

W3C DOCUMENT NOTICE AND LICENSE

Copyright 1994-2002 World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved.

<http://www.w3.org/Consortium/Legal/>

Public documents on the W3C site are provided by the copyright holders under the following license. The software or Document Type Definitions (DTDs) associated with W3C specifications are governed by the Software Notice. By using and/or copying this document, or the W3C document from which this statement is linked, you (the licensee) agree that you have read, understood, and will comply with the following terms and conditions:

Permission to use, copy, and distribute the contents of this document, or the W3C document from which this statement is linked, in any medium for any purpose and without fee or royalty is hereby granted, provided that you include the following on ALL copies of the document, or portions thereof, that you use:

1. A link or URL to the original W3C document.
2. The pre-existing copyright notice of the original author, or if it doesn't exist, a notice of the form: "Copyright [date-of-document] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. <http://www.w3.org/Consortium/Legal/>" (Hypertext is preferred, but a textual representation is permitted.)
3. If it exists, the STATUS of the W3C document.

When space permits, inclusion of the full text of this NOTICE should be provided. We request that authorship attribution be provided in any software, documents, or other items or products that you create pursuant to the implementation of the contents of this document, or any portion thereof.

No right to create modifications or derivatives of W3C documents is granted pursuant to this license. However, if additional requirements (documented in the Copyright FAQ) are satisfied, the right to create modifications or

Appendix: License Information

derivatives is sometimes granted by the W3C to individuals complying with those requirements.

THIS DOCUMENT IS PROVIDED "AS IS," AND COPYRIGHT HOLDERS MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR TITLE; THAT THE CONTENTS OF THE DOCUMENT ARE SUITABLE FOR ANY PURPOSE; NOR THAT THE IMPLEMENTATION OF SUCH CONTENTS WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

COPYRIGHT HOLDERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE DOCUMENT OR THE PERFORMANCE OR IMPLEMENTATION OF THE CONTENTS THEREOF.

The name and trademarks of copyright holders may NOT be used in advertising or publicity pertaining to this document or its contents without specific, written prior permission. Title to copyright in this document will at all times remain with copyright holders.

This formulation of W3C's notice and license became active on April 05 1999 so as to account for the treatment of DTDs, schema's and bindings. See the older formulation for the policy prior to this date. Please see our Copyright FAQ for common questions about using materials from our site, including specific terms and conditions for packages like libwww, Amaya, and Jigsaw. Other questions about this notice can be directed to site-policy@w3.org. webmaster (last updated by reagle on 1999/04/99.)

%% The following software may be included in this product: Stax API; Use of any of this software is governed by the terms of the license below:

Streaming API for XML (JSR-173) Specification
Reference Implementation
License Agreement

READ THE TERMS OF THIS (THE "AGREEMENT") CAREFULLY BEFORE VIEWING OR USING THE SOFTWARE LICENSED HEREUNDER. BY VIEWING OR USING THE SOFTWARE, YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCESSING THE SOFTWARE ELECTRONICALLY, INDICATE YOUR ACCEPTANCE OF THESE TERMS BY SELECTING THE "ACCEPT" BUTTON AT THE END OF THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL THESE TERMS, PROMPTLY RETURN THE UNUSED SOFTWARE TO ORIGINAL CONTRIBUTOR, DEFINED HEREIN.

1.0 DEFINITIONS.

1.1. "BEA" means BEA Systems, Inc., the licensor of the Original Code.

1.2. "Contributor" means BEA and each entity that creates or contributes to the creation of Modifications.

1.3. "Covered Code" means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof and corresponding documentation released with the source code.

1.4. "Executable" means Covered Code in any form other than Source Code.

1.5. "FCS" means first commercial shipment of a product.

1.6. "Modifications" means any addition to or deletion from the substance or

structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

(a) Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

(b) Any new file that contains any part of the Original Code or previous Modifications.

1.7. "Original Code" means Source Code of computer software code Reference Implementation.

1.8. "Patent Claims" means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent for which the grantor has the right to grant a license.

1.9. "Reference Implementation" means the prototype or "proof of concept" implementation of the Specification developed and made available for license by or on behalf of BEA.

1.10. "Source Code" means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated documentation, interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice.

1.11. "Specification" means the written specification for the Streaming API for XML, Java technology developed pursuant to the Java Community Process.

1.12. "Technology Compatibility Kit" or "TCK" means the documentation, testing tools and test suites associated with the Specification as may be revised by BEA from time to time, that is provided so that an implementer of the Specification may determine if its implementation is compliant with the Specification.

1.13. "You" (or "Your") means an individual or a legal entity exercising rights under, and complying with all of the terms of, this Agreement or a future version of this Agreement issued under Section 6.1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2.0 SOURCE CODE LICENSE.

2.1. Copyright Grant. Subject to the terms of this Agreement, each Contributor hereby grants You a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Covered Code of such Contributor, if any, and such derivative works, in Source Code and Executable form.

2.2. Patent Grant. Subject to the terms of this Agreement, each Contributor hereby grants You a non-exclusive, worldwide, royalty-free patent license under the Patent Claims to make, use, sell, offer to sell, import and otherwise transfer the Covered Code prepared and provided by such Contributor, if any, in Source Code and Executable form. This patent license shall apply to the Covered Code if, at the time a Modification is added by the Contributor, such addition of the Modification causes such combination to be covered by the Patent Claims.

Appendix: License Information

The patent license shall not apply to any other combinations which include the Modification.

2.3. Conditions to Grants. You understand that although each Contributor grants the licenses to the Covered Code prepared by it, no assurances are provided by any Contributor that the Covered Code does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to You for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, You hereby assume sole responsibility to secure any other intellectual property rights needed, if any. For example, if a thirdparty patent license is required to allow You to distribute Covered Code, it is Your responsibility to acquire that license before distributing such code.

2.4. Contributors' Representation. Each Contributor represents that to its knowledge it has sufficient copyright rights in the Covered Code it provides , if any, to grant the copyright license set forth in this Agreement.

3.0 DISTRIBUION RESTRICTIONS.

3.1. Application of Agreement.

The Modifications which You create or to which You contribute are governed by the terms of this Agreement, including without limitation Section 2.0. The Source Code version of Covered Code may be distributed only under the terms of this Agreement or a future version of this Agreement released under Section 6.1, and You must include a copy of this Agreement with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this Agreement or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.3.

3.2. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by BEA and including the name of BEA in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

%% The following software may be included in this product: X Window System; Use of any of this software is governed by the terms of the license below:
Copyright The Open Group

Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation.

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESSFOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE OPEN GROUPBE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION

OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of The Open Group shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from The Open Group.

Portions also covered by other licenses as noted in the above URL.

%% The following software may be included in this product: dom4j v. 1.6; Use of any of this software is governed by the terms of the license below:

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain copyright statements and notices. Redistributions must also contain a copy of this document.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "DOM4J" must not be used to endorse or promote products derived from this Software without prior written permission of MetaStuff, Ltd. For written permission, please contact dom4j-info@metastuff.com.
4. Products derived from this Software may not be called "DOM4J" nor may "DOM4J" appear in their names without prior written permission of MetaStuff, Ltd. DOM4J is a registered trademark of MetaStuff, Ltd.
5. Due credit should be given to the DOM4J Project - <http://www.dom4j.org>

THIS SOFTWARE IS PROVIDED BY METASTUFF, LTD. AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL METASTUFF, LTD. OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright 2001-2005 (C) MetaStuff, Ltd. All Rights Reserved.

%% The following software may be included in this product: Retroweaver; Use of any of this software is governed by the terms of the license below:

Copyright (c) February 2004, Toby Reyelts All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. Neither the name of Toby Reyelts nor the names of his

Appendix: License Information

contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

%% The following software may be included in this product: stripper; Use of any of this software is governed by the terms of the license below:

Stripper : debug information stripper Copyright (c) 2003 Kohsuke Kawaguchi All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the copyright holders nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

%% The following software may be included in this product: libpng official PNG reference library; Use of any of this software is governed by the terms of the license below:

This copy of the libpng notices is provided for your convenience. In case of any discrepancy between this copy and the notices in the file png.h that is included in the libpng distribution, the latter shall prevail.

COPYRIGHT NOTICE, DISCLAIMER, and LICENSE:

If you modify libpng you may insert additional notices immediately following this sentence.

libpng version 1.2.6, December 3, 2004, is Copyright (c) 2004 Glenn Randers-Pehrson, and is distributed according to the same disclaimer and license as libpng-1.2.5 with the following individual added to the list of Contributing Authors Cosmin Truta

libpng versions 1.0.7, July 1, 2000, through 1.2.5 - October 3, 2002, are Copyright (c) 2000-2002 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-1.0.6 with the following individuals added to the list of Contributing Authors Simon-Pierre Cadieux Eric S. Raymond Gilles Vollant

and with the following additions to the disclaimer:

There is no warranty against interference with your enjoyment of the library or against infringement. There is no warranty that our efforts or the library will fulfill any of your particular purposes or needs. This library is provided with all faults, and the entire risk of satisfactory quality, performance, accuracy, and effort is with the user.

libpng versions 0.97, January 1998, through 1.0.6, March 20, 2000, are Copyright (c) 1998, 1999 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-0.96, with the following individuals added to the list of Contributing Authors: Tom Lane Glenn Randers-Pehrson Willem van Schaik

libpng versions 0.89, June 1996, through 0.96, May 1997, are Copyright (c) 1996, 1997 Andreas Dilger Distributed according to the same disclaimer and license as libpng-0.88, with the following individuals added to the list of Contributing Authors: John Bowler Kevin Bracey Sam Bushell Magnus Holmgren Greg Roelofs Tom Tanner

libpng versions 0.5, May 1995, through 0.88, January 1996, are Copyright (c) 1995, 1996 Guy Eric Schalnat, Group 42, Inc.

For the purposes of this copyright and license, "Contributing Authors" is defined as the following set of individuals:

Andreas Dilger
Dave Martindale
Guy Eric Schalnat
Paul Schmidt
Tim Wegner

The PNG Reference Library is supplied "AS IS". The Contributing Authors and Group 42, Inc. disclaim all warranties, expressed or implied, including, without limitation, the warranties of merchantability and of fitness for any purpose. The Contributing Authors and Group 42, Inc. assume no liability for direct, indirect, incidental, special, exemplary, or consequential damages, which may result from the use of the PNG Reference Library, even if advised of the possibility of such damage.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, without fee, subject to the following restrictions:

1. The origin of this source code must not be misrepresented.
2. Altered versions must be plainly marked as such and must not be misrepresented as being the original source.

Appendix: License Information

3. This Copyright notice may not be removed or altered from any source or altered source distribution.

The Contributing Authors and Group 42, Inc. specifically permit, without fee, and encourage the use of this source code as a component to supporting the PNG file format in commercial products. If you use this source code in a product, acknowledgment is not required but would be appreciated.

A "png_get_copyright" function is available, for convenient use in "about"boxes and the like:

```
printf("%s",png_get_copyright(NULL));
```

Also, the PNG logo (in PNG format, of course) is supplied in the files "pngbar.png" and "pngbar.jpg (88x31) and "pngnow.png" (98x31).

Libpng is OSI Certified Open Source Software. OSI Certified Open Source is a certification mark of the Open Source Initiative.

Glenn Randers-Pehrson
glennrp at users.sourceforge.net
December 3, 2004

%% The following software may be included in this product: Libungif - An uncompressed GIF library; Use of any of this software is governed by the terms of the license below:

The GIFLIB distribution is Copyright (c) 1997 Eric S.Raymond

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

%% The following software may be included in this product: Ant; Use of any of this software is governed by the terms of the license below: License The Apache Software License Version 2.0

The Apache Software License Version 2.0 applies to all releases of Ant starting with ant 1.6.1

```
/*
 *
 * Apache License
 * Version 2.0, January 2004
```

```

*                                     http://www.apache.org/licenses/
*
* TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION
*
* 1. Definitions.
*
*     "License" shall mean the terms and conditions for use, reproduction,
*     and distribution as defined by Sections 1 through 9 of this document.
*
*     "Licensor" shall mean the copyright owner or entity authorized by
*     the copyright owner that is granting the License.
*
*     "Legal Entity" shall mean the union of the acting entity and all
*     other entities that control, are controlled by, or are under common
*     control with that entity. For the purposes of this definition,
*     "control" means (i) the power, direct or indirect, to cause the
*     direction or management of such entity, whether by contract or
*     otherwise, or (ii) ownership of fifty percent (50%) or more of the
*     outstanding shares, or (iii) beneficial ownership of such entity.
*
*     "You" (or "Your") shall mean an individual or Legal Entity
*     exercising permissions granted by this License.
*
*     "Source" form shall mean the preferred form for making modifications,
*     including but not limited to software source code, documentation
*     source, and configuration files.
*
*     "Object" form shall mean any form resulting from mechanical
*     transformation or translation of a Source form, including but
*     not limited to compiled object code, generated documentation,
*     and conversions to other media types.
*
*     "Work" shall mean the work of authorship, whether in Source or
*     Object form, made available under the License, as indicated by a
*     copyright notice that is included in or attached to the work
*     (an example is provided in the Appendix below).
*
*     "Derivative Works" shall mean any work, whether in Source or Object
*     form, that is based on (or derived from) the Work and for which the
*     editorial revisions, annotations, elaborations, or other modifications
*     represent, as a whole, an original work of authorship. For the purposes
*     of this License, Derivative Works shall not include works that remain
*     separable from, or merely link (or bind by name) to the interfaces of,
*     the Work and Derivative Works thereof.
*
*     "Contribution" shall mean any work of authorship, including
*     the original version of the Work and any modifications or additions
*     to that Work or Derivative Works thereof, that is intentionally
*     submitted to Licensor for inclusion in the Work by the copyright owner
*     or by an individual or Legal Entity authorized to submit on behalf of
*     the copyright owner. For the purposes of this definition, "submitted"
*     means any form of electronic, verbal, or written communication sent
*     to the Licensor or its representatives, including but not limited to
*     communication on electronic mailing lists, source code control systems,
*     and issue tracking systems that are managed by, or on behalf of, the
*     Licensor for the purpose of discussing and improving the Work, but
*     excluding communication that is conspicuously marked or otherwise
*     designated in writing by the copyright owner as "Not a Contribution."
*

```

Appendix: License Information

* "Contributor" shall mean Licensor and any individual or Legal Entity
* on behalf of whom a Contribution has been received by Licensor and
* subsequently incorporated within the Work.
*

* 2. Grant of Copyright License. Subject to the terms and conditions of
* this License, each Contributor hereby grants to You a perpetual,
* worldwide, non-exclusive, no-charge, royalty-free, irrevocable
* copyright license to reproduce, prepare Derivative Works of,
* publicly display, publicly perform, sublicense, and distribute the
* Work and such Derivative Works in Source or Object form.
*

* 3. Grant of Patent License. Subject to the terms and conditions of
* this License, each Contributor hereby grants to You a perpetual,
* worldwide, non-exclusive, no-charge, royalty-free, irrevocable
* (except as stated in this section) patent license to make, have made,
* use, offer to sell, sell, import, and otherwise transfer the Work,
* where such license applies only to those patent claims licensable
* by such Contributor that are necessarily infringed by their
* Contribution(s) alone or by combination of their Contribution(s)
* with the Work to which such Contribution(s) was submitted. If You
* institute patent litigation against any entity (including a
* cross-claim or counterclaim in a lawsuit) alleging that the Work
* or a Contribution incorporated within the Work constitutes direct
* or contributory patent infringement, then any patent licenses
* granted to You under this License for that Work shall terminate
* as of the date such litigation is filed.
*

* 4. Redistribution. You may reproduce and distribute copies of the
* Work or Derivative Works thereof in any medium, with or without
* modifications, and in Source or Object form, provided that You
* meet the following conditions:
*

* (a) You must give any other recipients of the Work or
* Derivative Works a copy of this License; and
*

* (b) You must cause any modified files to carry prominent notices
* stating that You changed the files; and
*

* (c) You must retain, in the Source form of any Derivative Works
* that You distribute, all copyright, patent, trademark, and
* attribution notices from the Source form of the Work,
* excluding those notices that do not pertain to any part of
* the Derivative Works; and
*

* (d) If the Work includes a "NOTICE" text file as part of its
* distribution, then any Derivative Works that You distribute must
* include a readable copy of the attribution notices contained
* within such NOTICE file, excluding those notices that do not
* pertain to any part of the Derivative Works, in at least one
* of the following places: within a NOTICE text file distributed
* as part of the Derivative Works; within the Source form or
* documentation, if provided along with the Derivative Works; or,
* within a display generated by the Derivative Works, if and
* wherever such third-party notices normally appear. The contents
* of the NOTICE file are for informational purposes only and
* do not modify the License. You may add Your own attribution
* notices within Derivative Works that You distribute, alongside
* or as an addendum to the NOTICE text from the Work, provided
* that such additional attribution notices cannot be construed

* as modifying the License.

* You may add Your own copyright statement to Your modifications and

* may provide additional or different license terms and conditions

* for use, reproduction, or distribution of Your modifications, or

* for any such Derivative Works as a whole, provided Your use,

* reproduction, and distribution of the Work otherwise complies with

* the conditions stated in this License.

* 5. Submission of Contributions. Unless You explicitly state otherwise,

* any Contribution intentionally submitted for inclusion in the Work

* by You to the Licensor shall be under the terms and conditions of

* this License, without any additional terms or conditions.

* Notwithstanding the above, nothing herein shall supersede or modify

* the terms of any separate license agreement you may have executed

* with Licensor regarding such Contributions.

* 6. Trademarks. This License does not grant permission to use the trade

* names, trademarks, service marks, or product names of the Licensor,

* except as required for reasonable and customary use in describing the

* origin of the Work and reproducing the content of the NOTICE file.

* 7. Disclaimer of Warranty. Unless required by applicable law or

* agreed to in writing, Licensor provides the Work (and each

* Contributor provides its Contributions) on an "AS IS" BASIS,

* WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or

* implied, including, without limitation, any warranties or conditions

* of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A

* PARTICULAR PURPOSE. You are solely responsible for determining the

* appropriateness of using or redistributing the Work and assume any

* risks associated with Your exercise of permissions under this License.

* 8. Limitation of Liability. In no event and under no legal theory,

* whether in tort (including negligence), contract, or otherwise,

* unless required by applicable law (such as deliberate and grossly

* negligent acts) or agreed to in writing, shall any Contributor be

* liable to You for damages, including any direct, indirect, special,

* incidental, or consequential damages of any character arising as a

* result of this License or out of the use or inability to use the

* Work (including but not limited to damages for loss of goodwill,

* work stoppage, computer failure or malfunction, or any and all

* other commercial damages or losses), even if such Contributor

* has been advised of the possibility of such damages.

* 9. Accepting Warranty or Additional Liability. While redistributing

* the Work or Derivative Works thereof, You may choose to offer,

* and charge a fee for, acceptance of support, warranty, indemnity,

* or other liability obligations and/or rights consistent with this

* License. However, in accepting such obligations, You may act only

* on Your own behalf and on Your sole responsibility, not on behalf

* of any other Contributor, and only if You agree to indemnify,

* defend, and hold each Contributor harmless for any liability

* incurred by, or claims asserted against, such Contributor by reason

* of your accepting any such warranty or additional liability.

* END OF TERMS AND CONDITIONS

* APPENDIX: How to apply the Apache License to your work.

*

Appendix: License Information

```
*      To apply the Apache License to your work, attach the following
*      boilerplate notice, with the fields enclosed by brackets "[]"
*      replaced with your own identifying information. (Don't include
*      the brackets!) The text should be enclosed in the appropriate
*      comment syntax for the file format. We also recommend that a
*      file or class name and description of purpose be included on the
*      same "printed page" as the copyright notice for easier
*      identification within third-party archives.
*
*      Copyright [yyyy] Apache Software Foundation
*
*      Licensed under the Apache License, Version 2.0 (the "License");
*      you may not use this file except in compliance with the License.
*      You may obtain a copy of the License at
*
*          http://www.apache.org/licenses/LICENSE-2.0
*
*      Unless required by applicable law or agreed to in writing, software
*      distributed under the License is distributed on an "AS IS" BASIS,
*      WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
*      See the License for the specific language governing permissions and
*      limitations under the License.
*/
```

You can download the original license file [here](http://www.apache.org/licenses/LICENSE-2.0).

The License is accompanied by a NOTICE

```
=====
== NOTICE file corresponding to the section 4 d of ==
== the Apache License, Version 2.0, ==
== in this case for the Apache Ant distribution. ==
=====
This product includes software developed by
The Apache Software Foundation (http://www.apache.org/).
```

This product includes also software developed by : - the W3C consortium
(<http://www.w3c.org>) , - the SAX project (<http://www.saxproject.org>)

Please read the different LICENSE files present in the root directory of this distribution.

The names "Ant" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

The Apache Software License, Version 1.1

The Apache Software License, Version 1.1, applies to all versions of up to ant1.6.0 included.

```
/*
* =====
*           The Apache Software License, Version 1.1
* =====
*
*      Copyright (C) 2000-2003 The Apache Software Foundation. All
*      rights reserved.
```

```

*
* Redistribution and use in source and binary forms, with or without modifica-
* tion, are permitted provided that the following conditions are met:
*
* 1. Redistributions of source code must retain the above copyright notice,
*    this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright notice,
*    this list of conditions and the following disclaimer in the documentation
*    and/or other materials provided with the distribution.
*
* 3. The end-user documentation included with the redistribution, if any, must
*    include the following acknowledgment: "This product includes software
*    developed by the Apache Software Foundation (http://www.apache.org/)."
*    Alternately, this acknowledgment may appear in the software itself, if
*    and wherever such third-party acknowledgments normally appear.
*
* 4. The names "Ant" and "Apache Software Foundation" must not be used to
*    endorse or promote products derived from this software without prior
*    written permission. For written permission, please contact
*    apache@apache.org.
*
* 5. Products derived from this software may not be called "Apache", nor may
*    "Apache" appear in their name, without prior written permission of the
*    Apache Software Foundation.
*
* THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES,
* INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND
* FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE
* APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT,
* INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLU-
* DING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS
* OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON
* ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
* (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
* THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
*
* This software consists of voluntary contributions made by many individuals
* on behalf of the Apache Software Foundation. For more information on the
* Apache Software Foundation, please see http://www.apache.org/.
*
*/

```

%% The following software may be included in this product: XML Resolver
library; Use of any of this software is governed by the terms of the license
below:

Apache License
Version 2.0, January 2004
<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction,
and distribution as defined by Sections 1 through 9 of this document.

Appendix: License Information

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.
4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:
 - (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
 - (b) You must cause any modified files to carry prominent notices stating that You changed the files; and
 - (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
 - (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.
5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

Appendix: License Information

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.
7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.
8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.
9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

%% The following software may be included in this product: ICU4J; Use of any of this software is governed by the terms of the license below:

ICU License - ICU 1.8.1 and later COPYRIGHT AND PERMISSION NOTICE Copyright (c)

1995-2003 International Business Machines Corporation and others All rights reserved Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE. Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

%% The following software may be included in this product: NekoHTML; Use of any of this software is governed by the terms of the license below: The CyberNeko Software License, Version 1.0

(C) Copyright 2002,2003, Andy Clark. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment:
"This product includes software developed by Andy Clark."
Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names "CyberNeko" and "NekoHTML" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact andy@cyberneko.net.
5. Products derived from this software may not be called "CyberNeko",

Appendix: License Information

nor may "CyberNeko" appear in their name, without prior written permission of the author.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR OTHER CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====
This license is based on the Apache Software License, version 1.1

%% The following software may be included in this product: Jing; Use of any of this software is governed by the terms of the license below: Jing Copying Conditions

Copyright (c) 2001-2003 Thai Open Source Software Center Ltd All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of the Thai Open Source Software Center Ltd nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

%% The following software may be included in this product: RelaxNGCC; Use of any of this software is governed by the terms of the license below:

Copyright (c) 2000-2003 Daisuke Okajima and Kohsuke Kawaguchi.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment:

"This product includes software developed by Daisuke Okajima and Kohsuke Kawaguchi (<http://relaxngcc.sf.net/>)."

Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names of the copyright holders must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact the copyright holders.
5. Products derived from this software may not be called "RELAXNGCC", nor may "RELAXNGCC" appear in their name, without prior written permission of the copyright holders.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

%% The following software may be included in this product: RELAX NG Object Model/Parser; Use of any of this software is governed by the terms of the license below: The MIT License

Copyright (c)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Appendix: License Information

%% The following software may be included in this product: XFree86-VidMode Extension; Use of any of this software is governed by the terms of the license below: Version 1.1 of Project Licence.

Copyright (C) 1994-2004 The Project, Inc. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution, and in the same place and form as other copyright, license and disclaimer information.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by The XFree86 Project, Inc (<http://www.xfree86.org/>) and its contributors", in the same place and form as other third-party acknowledgments. Alternately, this acknowledgment may appear in the software itself, in the same form and location as other such third-party acknowledgments.
4. Except as contained in this notice, the name of The XFree86 Project, Inc shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from The XFree86 Project, Inc.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE XFREE86PROJECT, INC OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

%% The following software may be included in this product: RelaxNGCC; Use of any of this software is governed by the terms of the license below: This is version 2003-May-08 of the Info-ZIP copyright and license. The definitive version of this document should be available at <ftp://ftp.info-zip.org/pub/infozip/license.html> indefinitely.

Copyright (c) 1990-2003 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup

Gailly, Hunter Goatley, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Christian Spieler, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).
4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

%% The following software may be included in this product: XML Security; Use of any of this software is governed by the terms of the license below: The Apache Software License, Version 1.1 PDF

Copyright (C) 2002 The Apache Software Foundation.

All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Appendix: License Information

3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).". Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names "Apache Forrest" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org. 5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation. THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org>.

%% The following software may be included in this product: Regexp, Regular Expression Package v. 1.2; Use of any of this software is governed by the terms of the license below: The Apache Software License, Version 1.1 Copyright (c) 2001 The Apache Software Foundation. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).". Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names "Apache" and "Apache Software Foundation" and "Apache Turbine" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this software may not be called "Apache", "Apache Turbine", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE

SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org>.

=====

%% The following software may be included in this product: zlib; Use of any of this software is governed by the terms of the license below:

zlib.h -- interface of the 'zlib' general purpose compression library
version 1.1.3, July 9th, 1998

Copyright (C) 1995-1998 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly	Mark Adler
jloup@gzip.org	madler@alumni.caltech.edu

The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files <ftp://ds.internic.net/rfc/rfc1950.txt> (zlib format), [rfc1951.txt](ftp://ds.internic.net/rfc/rfc1951.txt) (deflate format) and [rfc1952.txt](ftp://ds.internic.net/rfc/rfc1952.txt) (gzip format)

%% The following software may be included in this product: Mozilla Rhino. Use of any of this software is governed by the terms of the license below:

- * The contents of this file are subject to the Netscape Public
- * License Version 1.1 (the "License"); you may not use this file
- * except in compliance with the License. You may obtain a copy of
- * the License at <http://www.mozilla.org/NPL/>
- *
- * Software distributed under the License is distributed on an "AS
- * IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or

Appendix: License Information

```
* implied. See the License for the specific language governing
* rights and limitations under the License.
*
* The Original Code is Rhino code, released
* May 6, 1999.
*
* The Initial Developer of the Original Code is Netscape
* Communications Corporation. Portions created by Netscape are
* Copyright (C) 1997-2000 Netscape Communications Corporation. All
* Rights Reserved.
*
* Contributor(s):
*
* Kemal Bayram
* Patrick Beard
* Norris Boyd
* Igor Bukanov, igor@mir2.org
* Brendan Eich
* Ethan Hugg
* Roger Lawrence
* Terry Lucas
* Mike McCabe
* Milen Nankov
* Attila Szegedi, szegedia@freemail.hu
* Ian D. Stewart
* Andi Vajda
* Andrew Wason
*/

%% The following software may be included in this product: Apache Derby. Use
of any of this software is governed by the terms of the license below:
```

Apache License
Version 2.0, January 2004
<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications,

including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.
3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct

Appendix: License Information

or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:
 - (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
 - (b) You must cause any modified files to carry prominent notices stating that You changed the files; and
 - (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
 - (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.
6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.
7. Disclaimer of Warranty. Unless required by applicable law or

agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.
9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Appendix: License Information

%%The following software may be included in this product:
UPX

Use of any of this software is governed by the terms of the license below:

-----BEGIN PGP SIGNED MESSAGE-----

```

00000      000 000000000.  0000000 00000
`888'      `8' `888 `Y88.  `8888  d8'
888        8 888 .d88'   Y888..8P
888        8 88800088P'   `8888'
888        8 888          .8PY888.
`88.      .8' 888        d8' `888b
`YbodP'    o888o      o888o o88888o

```

The Ultimate Packer for eXecutables
Copyright (c) 1996-2000 Markus Oberhumer & Laszlo Molnar
<http://wildsau.idv.uni-linz.ac.at/mfx/upx.html>
<http://www.nexus.hu/upx>
<http://upx.tsx.org>

PLEASE CAREFULLY READ THIS LICENSE AGREEMENT, ESPECIALLY IF YOU PLAN
TO MODIFY THE UPX SOURCE CODE OR USE A MODIFIED UPX VERSION.

ABSTRACT
=====

UPX and UCL are copyrighted software distributed under the terms
of the GNU General Public License (hereinafter the "GPL").

The stub which is imbedded in each UPX compressed program is part
of UPX and UCL, and contains code that is under our copyright. The
terms of the GNU General Public License still apply as compressing
a program is a special form of linking with our stub.

As a special exception we grant the free usage of UPX for all
executables, including commercial programs.
See below for details and restrictions.

COPYRIGHT
=====

UPX and UCL are copyrighted software. All rights remain with the authors.

UPX is Copyright (C) 1996-2000 Markus Franz Xavier Johannes Oberhumer
UPX is Copyright (C) 1996-2000 Laszlo Molnar

UCL is Copyright (C) 1996-2000 Markus Franz Xavier Johannes Oberhumer

GNU GENERAL PUBLIC LICENSE

=====

UPX and the UCL library are free software; you can redistribute them and/or modify them under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

UPX and UCL are distributed in the hope that they will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; see the file COPYING.

SPECIAL EXCEPTION FOR COMPRESSED EXECUTABLES

=====

The stub which is imbedded in each UPX compressed program is part of UPX and UCL, and contains code that is under our copyright. The terms of the GNU General Public License still apply as compressing a program is a special form of linking with our stub.

Hereby Markus F.X.J. Oberhumer and Laszlo Molnar grant you special permission to freely use and distribute all UPX compressed programs (including commercial ones), subject to the following restrictions:

1. You must compress your program with a completely unmodified UPX version; either with our precompiled version, or (at your option) with a self compiled version of the unmodified UPX sources as distributed by us.
2. This also implies that the UPX stub must be completely unmodified, i.e. the stub imbedded in your compressed program must be byte-identical to the stub that is produced by the official unmodified UPX version.
3. The decompressor and any other code from the stub must exclusively get used by the unmodified UPX stub for decompressing your program at program startup. No portion of the stub may get read, copied, called or otherwise get used or accessed by your program.

ANNOTATIONS

=====

- You can use a modified UPX version or modified UPX stub only for programs that are compatible with the GNU General Public License.
- We grant you special permission to freely use and distribute all UPX compressed programs. But any modification of the UPX stub (such as, but not limited to, removing our copyright string or making your program non-decompressible) will immediately revoke your right to use and distribute a UPX compressed program.
- UPX is not a software protection tool; by requiring that you use the unmodified UPX version for your proprietary programs we make sure that any user can decompress your program. This protects both you and your users as nobody can hide malicious code - any program that cannot be decompressed is highly suspicious by definition.

Appendix: License Information

- You can integrate all or part of UPX and UCL into projects that are compatible with the GNU GPL, but obviously you cannot grant any special exceptions beyond the GPL for our code in your project.
- We want to actively support manufacturers of virus scanners and similar security software. Please contact us if you would like to incorporate parts of UPX or UCL into such a product.

Markus F.X.J. Oberhumer Laszlo Molnar
markus.oberhumer@jk.uni-linz.ac.at mll1050@cdata.tvnet.hu

Linz, Austria, 25 Feb 2000

Additional License(s)

The UPX license file is at <http://upx.sourceforge.net/upx-license.html>.

%The following software may be included in this product:
LZMA Software Development Kit

Use of any of this software is governed by the terms of the license below:

License

LZMA SDK is available under any of the following licenses:

1. GNU Lesser General Public License (GNU LGPL)
2. Common Public License (CPL)
3. Simplified license for unmodified code (read SPECIAL EXCEPTION)
4. Proprietary license

This means that you can select one of these four options and follow rules of that license.

SPECIAL EXCEPTION: Igor Pavlov, as the author of this code, expressly permit you statically or dynamically to link your code (or bind by name) to the files from LZMA SDK without subjecting your linked code to the terms of the CPL or GNU LGPL. Any modification or addition to any file in the LZMA SDK, however, is subject to the GNU LGPL or CPL terms.

This SPECIAL EXCEPTION allows you to use LZMA SDK in applications with proprietary code, provided you keep the LZMA SDK code unmodified.

SPECIAL EXCEPTION #2: Igor Pavlov, as the author of this code, expressly permits you to use LZMA SDK 4.43 under the same terms and conditions contained in the License Agreement you have for any previous version of LZMA SDK developed by Igor Pavlov.

SPECIAL EXCEPTION #2 allows holders of proprietary licenses to use latest version of LZMA SDK as update for previous versions.

GNU LGPL and CPL are pretty similar and both these licenses are classified as free software licenses at <http://www.gnu.org/> and OSI-approved at <http://www.opensource.org/>.

LZMA SDK also is available under a proprietary license which can include:

1. The right to modify code from the LZMA SDK without subjecting the modified code to the terms of the CPL or GNU LGPL
2. Technical support for LZMA SDK via email

To request such a proprietary license, or for any additional consultations, send an email message, using the 7-Zip support page: Send message to LZMA developer

The source code of 7-Zip is released under the terms of the GNU LGPL. You can download the source code of 7-Zip at 7-Zip's Source Forge Page

Additional License(s)

The license included with the software differs slightly from the version posted on the website. Specifically it includes SPECIAL EXCEPTION #3, which is not present in the license on the website. The license from the software archive follows:

LICENSE

LZMA SDK is available under any of the following licenses:

- 1) GNU Lesser General Public License (GNU LGPL)
- 2) Common Public License (CPL)
- 3) Simplified license for unmodified code (read SPECIAL EXCEPTION)
- 4) Proprietary license

It means that you can select one of these four options and follow rules of that license.

1,2) GNU LGPL and CPL licenses are pretty similar and both these licenses are classified as

- "Free software licenses" at <http://www.gnu.org/>
- "OSI-approved" at <http://www.opensource.org/>

3) SPECIAL EXCEPTION

Igor Pavlov, as the author of this code, expressly permits you to statically or dynamically link your code (or bind by name) to the files from LZMA SDK without subjecting your linked code to the terms of the CPL or GNU LGPL. Any modifications or additions to files from LZMA SDK, however, are subject to the GNU LGPL or CPL terms.

SPECIAL EXCEPTION allows you to use LZMA SDK in applications with closed code, while you keep LZMA SDK code unmodified.

SPECIAL EXCEPTION #2: Igor Pavlov, as the author of this code, expressly permits you to use this code under the same terms and conditions contained in the License Agreement you have for any previous version of LZMA SDK developed by Igor Pavlov.

SPECIAL EXCEPTION #2 allows owners of proprietary licenses to use latest version of LZMA SDK as update for previous versions.

Appendix: License Information

SPECIAL EXCEPTION #3: Igor Pavlov, as the author of this code, expressly permits you to use code of the following files: BranchTypes.h, LzmaTypes.h, LzmaTest.c, LzmaStateTest.c, LzmaAlone.cpp, LzmaAlone.cs, LzmaAlone.java as public domain code.

4) Proprietary license

LZMA SDK also can be available under a proprietary license which can include:

- 1) Right to modify code without subjecting modified code to the terms of the CPL or GNU LGPL
- 2) Technical support for code

To request such proprietary license or any additional consultations, send email message from that page:<http://www.7-zip.org/support.html>

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

You should have received a copy of the Common Public License along with this library.