



TIBCO Spotfire® Server and Environment Installation and Administration

*Software Release 7.11 LTS
Document Updated: February 2020*

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 THE LICENSE FILE) 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.

ANY SOFTWARE ITEM IDENTIFIED AS THIRD PARTY LIBRARY IS AVAILABLE UNDER SEPARATE SOFTWARE LICENSE TERMS AND IS NOT PART OF A TIBCO PRODUCT. AS SUCH, THESE SOFTWARE ITEMS ARE NOT COVERED BY THE TERMS OF YOUR AGREEMENT WITH TIBCO, INCLUDING ANY TERMS CONCERNING SUPPORT, MAINTENANCE, WARRANTIES, AND INDEMNITIES. DOWNLOAD AND USE OF THESE ITEMS IS SOLELY AT YOUR OWN DISCRETION AND SUBJECT TO THE LICENSE TERMS APPLICABLE TO THEM. BY PROCEEDING TO DOWNLOAD, INSTALL OR USE ANY OF THESE ITEMS, YOU ACKNOWLEDGE THE FOREGOING DISTINCTIONS BETWEEN THESE ITEMS AND TIBCO PRODUCTS.

This document 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, the TIBCO logo, the TIBCO O logo, TIBCO Spotfire, TIBCO Spotfire Analyst, TIBCO Spotfire Automation Services, TIBCO Spotfire Server, TIBCO Spotfire Web Player, TIBCO Spotfire Developer, TIBCO Enterprise Message Service, TIBCO Enterprise Runtime for R, TIBCO Enterprise Runtime for R - Server Edition, TERR, TERR Server Edition, TIBCO Hawk, and TIBCO Spotfire Statistics Services are either registered trademarks or trademarks of TIBCO Software Inc. in the United States and/or other countries.

Java and all Java based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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.

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.

This and other products of TIBCO Software Inc. may be covered by registered patents. Please refer to TIBCO's Virtual Patent Marking document (<https://www.tibco.com/patents>) for details.

Copyright © 1994-2020. TIBCO Software Inc. All Rights Reserved.

Contents

TIBCO Spotfire Server Documentation and Support Services	21
Getting started	23
Introduction to the TIBCO Spotfire environment	24
Spotfire Server introduction	24
Spotfire database introduction	25
Nodes and services introduction	25
Spotfire clients introduction	25
Environment communication introduction	25
Authentication and user directory introduction	26
Users and groups introduction	27
Licenses and preferences introduction	28
Deployment introduction	28
Spotfire library introduction	28
Routing introduction	28
Data sources introduction	29
Logging introduction	30
Administration interface introduction	30
Example scenario	31
Upgrading from Spotfire 7.0 or earlier – an introduction	32
Basic installation process for Spotfire	34
Installation and configuration	35
Preparation	35
Downloading required software	35
Collecting required information	36
Setting up the Spotfire database (Oracle)	39
Setting up the Spotfire database (SQL Server)	42
Setting up the Spotfire database (SQL Server with Integrated Windows authentication)	44
Running database preparation scripts manually	47
Installation	48
Installing the Spotfire Server files (interactively on Windows)	48
Installing the Spotfire Server files (silently on Windows)	49
Installing the Spotfire Server files (RPM Linux)	50
Installing the Spotfire Server files (Tarball Linux)	51
Database drivers	51
Installing the Oracle database driver	52
Installing database drivers for Information Designer	52

Applying hotfixes to the server	52
Initial configuration	53
Configuration using the configuration tool	53
Opening the configuration tool	53
Running the configuration tool on a local computer	53
Creating the bootstrap.xml file	54
Setting up the Spotfire Server bootstrap file for Integrated Windows authentication	55
Saving basic configuration data (authentication towards Spotfire database)	56
Creating an administrator user	57
Configuration using the command line	57
Executing commands on the command line	57
Executing commands on a local computer	58
Viewing help on configuration commands	58
Configuration and administration commands by function	58
Action log configuration commands	59
Administration commands	59
Authentication commands	61
Client configuration command	62
Information Services commands	62
JAAS commands	63
LDAP commands	63
Library commands	63
Monitoring commands	64
Server configuration commands	64
Server database commands	65
Services commands	65
Spotfire collective commands	66
User directory commands	67
Miscellaneous configuration commands	67
Manually creating a simple configuration	67
Scripting a configuration	69
Editing and running a basic configuration script	70
Script language	71
Configuration.xml file	72
Manually editing the Spotfire Server configuration file	72
Start or stop Spotfire Server	72
Starting or stopping Spotfire Server (as a Windows service)	73
Starting or stopping Spotfire Server (Windows, no service)	73
Starting or stopping Spotfire Server (Windows, service exists, Integrated Authentication for SQL Server)	74

Starting or stopping Spotfire Server (Windows, no service, Integrated Authentication for SQL Server)	74
Starting or stopping Spotfire Server (Linux)	74
Clustered server deployments	75
Setting up a cluster of Spotfire Servers	75
Using Hazelcast for clustering	77
Using ActiveSpaces for clustering	78
Installing ActiveSpaces	78
Configuring a server cluster with ActiveSpaces (Windows)	79
Configuring a server cluster with ActiveSpaces (Linux)	80
Enabling secure transport for ActiveSpaces	82
Using Apache Ignite for clustering	83
Configuring NTLM for a cluster of Spotfire Servers	83
Enabling health check URL for load balanced servers	84
Kerberos authentication for clustered servers with load balancer	84
X.509 client certificates for clustered servers with load balancer	84
Configuring shared import and export folders for clustered deployments	85
Deploying client packages to Spotfire Server	85
User authentication	85
User name and password authentication methods	86
Authentication towards the Spotfire database	86
Authentication towards LDAP	86
Configuring LDAP	87
Configuring LDAPS	90
SASL authentication for LDAP	90
Configuring Spotfire Server for DIGEST-MD5 authentication of LDAP	90
Configuring Spotfire Server for GSSAPI authentication of LDAP	91
Authentication towards Windows NT Domain (legacy)	92
Combination of LDAP and Spotfire database authentication	92
Disabling adding database users when using LDAP	92
Authentication towards a custom JAAS module	92
Single sign-on authentication methods	93
NTLM authentication	93
Downloading third-party components (JCIFS) for NTLM authentication	94
Creating a computer service account in your Windows domain	94
Creating a computer service account manually	95
Configuring NTLM authentication for a single server	95
Kerberos authentication	97
Setting up Kerberos authentication on Spotfire Server	97
Creating a Kerberos service account	97

Registering Service Principal Names	98
Creating a keytab file for the Kerberos service account	99
Configuring Kerberos for Java	101
Copying the Kerberos service account's keytab file to Spotfire Server	102
Using Kerberos authentication with delegated credentials	102
Enabling constrained delegation	103
Enabling unconstrained delegation on a domain controller in Windows Server 2003 mode	103
Enabling unconstrained delegation for an account on a domain controller in Windows 2000 mixed or native mode	104
Selecting Kerberos as the Spotfire login method	104
Disabling the username and password fields in the Spotfire Analyst login dialog	105
Kerberos authentication for clustered servers with load balancer	105
Setting up Kerberos authentication on nodes	105
Enabling constrained delegation on nodes	106
Enable Kerberos authentication for end-users	106
Enabling Kerberos for Internet Explorer and Spotfire Analyst	107
Enabling delegated Kerberos for Google Chrome	107
Enabling Kerberos for Mozilla Firefox	107
Using Kerberos to log in to the Spotfire database	108
Creating a Windows domain account for the Spotfire database	109
Configuring the Spotfire database account to the Windows domain account	109
Keytab file for the Kerberos service account	110
Creating a keytab file for the Kerberos service account (using the ktpass.exe command from Microsoft Support)	110
Creating a keytab file for the Kerberos service account (using the ktpass.exe command from the bundled JDK)	110
Creating a keytab file for the Kerberos service account (using the ktutil command on Linux)	111
Creating a JAAS application configuration for the Spotfire database connection pool	112
Acquiring a Kerberos ticket by using a keytab file	113
Acquiring a Kerberos ticket by using a username and password	113
Acquiring a Kerberos ticket by using the identity of the account running the Spotfire Server process	113
Registering the JAAS application configuration file with Java	114
Configuring the database connection for Spotfire Server using Kerberos (Oracle)	114
Configuring the database connection for Spotfire Server using Kerberos (SQL Server)	114
Authentication using X.509 client certificates	115
Installing CA certificates	115
Configuring Spotfire Server to require client certificates for HTTPS	115
Configuring Spotfire Server to use X.509 client certificates to authenticate users	116
Configuring anonymous authentication	117

Web authentication	117
Configuring OpenID Connect	117
Advanced OpenID Connect settings	118
Configuring custom web authentication	119
Two-factor authentication	120
Configuring two-factor authentication	120
Configuring two-factor authentication using the command line	120
External authentication	120
Configuring external authentication	121
External directories and domains	123
LDAP synchronizations	125
User synchronization	125
Group synchronization	126
Group-based and role-based synchronization	126
LDAP authentication and user directory settings	129
Post-authentication filter	136
HTTPS	136
Configuring HTTPS	137
Node manager installation	138
Installing a node manager interactively	139
Installing a node manager silently	140
Starting or stopping a node manager (as a Windows service)	142
Trusting a node	143
Automatically trusting new nodes	143
Automatically installing services and instances	144
Login behavior configuration	146
Enabling an RSS feed in the Spotfire login dialog	146
Service installation on a node	147
Preconfiguring Spotfire Web Player services (optional)	147
Installing Spotfire Web Player instances	148
Multiple service instances on one node	149
Preconfiguring Spotfire Automation Services (optional)	149
Installing Spotfire Automation Services instances	149
Automation Services Job Builder and Client Job Sender	150
Sites	151
Creating sites	152
Setting different authentication methods and user directories for sites	152
Moving a server and its nodes to a different site	153
Sites administration	154

Deleting sites	155
Connectors	155
Setting up connectors	156
Configuring connectors for use with web clients and Spotfire Automation Services	156
Authentication modes	157
Connector configuration examples	158
Connector names in configuration file	160
Access to the connectors	161
Installing Oracle Essbase Client on client computers	162
Creating environment variables	162
Configuring the Google Analytics connector	163
Additional configuration	164
Updating a server configuration in the configuration tool	164
Updating a server configuration on the command line	164
Manually editing the Spotfire Server configuration file	165
Manually editing the service configuration files	165
Viewing the name of the active service configuration	166
Service configuration files	167
Spotfire.Dxp.Worker.Automation.config file	167
Spotfire.Dxp.Worker.Core.config file	171
Spotfire.Dxp.Worker.Host.exe.config file	172
Spotfire.Dxp.Worker.Web.config file	179
Customizing the service logging configuration	194
Customize statistics and performance counter logging	195
Service log levels	195
Configuring a specific directory for library import and export	196
Enabling cached and precomputed data for scheduled update files	196
Disabling the attachment manager cache	197
Post-installation steps	198
Enabling demo database use	198
Enabling geocoding tables for map charts	198
Administration	200
Opening Spotfire Server	200
Nodes, services, and resource pools	200
Creating resource pools	200
Adding resources to resource pools	201
Removing resources from resource pools	201
Changing the name of a resource pool	201
Deleting resource pools	201

Updating node managers	202
Rolling back a node manager update	202
Updating services	203
Rolling back a service update	203
Shutting down a service instance	204
Revoking trust of a node	204
User administration	205
Creating new Spotfire users	205
Adding a user to one or more groups	205
Removing a user from one or more groups	206
Changing a user's name, password, or email	206
Disabling a user account	206
Deleting users from the system	207
Group administration	207
Roles and special groups	207
Creating a new group	209
Adding users to a group	209
Adding groups to a group	210
Assigning a primary group to a subgroup	210
Assigning a deployment area to a group	210
Renaming a group	211
Removing members from a group	211
Deleting groups from the system	212
Deployments and deployment areas	212
Creating a new deployment area	213
Adding software packages to a deployment area	213
Copying a distribution to another deployment area	214
Exporting a distribution	214
Changing the default deployment area	214
Renaming a deployment area	215
Removing packages from a deployment area	215
Clearing a deployment area	215
Deleting a deployment area	216
Scheduled updates to analyses	216
Creating a scheduled update by using Spotfire Server	217
Additional settings for scheduled updates	218
Setting the number of Spotfire Web Player instances to make available for a scheduled update	218
Switching the scheduled update method from automatic to manual	219
Disallowing cached and precomputed data in individual scheduled update files	219

Scheduled updates with prompted or personalized information links	220
Editing a scheduled update	220
Creating a reusable schedule	220
Manually updating a file outside of its update schedule	221
Copying routing rules and schedules from one site to another	221
Exporting routing rules and schedules for import in a different Spotfire environment	222
Importing routing rules and schedules from a different Spotfire environment	222
Disabling or deleting scheduled updates and routing rules	223
Deleting schedules	223
Creating a scheduled update by using TIBCO EMS	223
Creating a scheduled update by using a SOAP web service	225
Scheduled updates monitoring	226
Changing the priority of a rule	228
Changing the number of retries for failed scheduled updates	228
Changing how often the scheduled update history is cleared	229
Common analysis loading errors	229
Routing rules	230
The default routing rule	230
Creating a routing rule	230
Monitoring and diagnostics	231
Server and node logging levels	231
Changing server and node logging levels	232
Changing the logging level for a server or node that is not running	233
Switching back to the Standard (default) logging level	233
Accessing Spotfire Server and node logs	234
Spotfire Server logs	234
Location of server logs	235
Changing the default location of server logs	236
Node logs	236
Enabling Kerberos debug logging	237
Accessing services logs	239
Service logs	239
General logging properties	241
Auditlog	241
DateTimesLog	241
DocumentCacheStatisticsLog	242
MemoryStatisticsLog	242
MonitoringEventsLog	242
OpenFilesStatisticsLog	243

PerformanceCounterLog	243
Spotfire.Dxp.Worker.Host and Spotfire.Dxp.Worker.Host.Debug	243
TimingLog	244
UserSessionStatisticsLog	244
Action logs and system monitoring	245
Configure action logging from the command line	246
Enabling action logging and system monitoring from the command line	246
Configuring logging to a Microsoft SQL Server database with the command line	247
Configuring logging to an Oracle database with the command line	248
Configuring the action log web service from the command line	250
Configure action logging using the configuration tool	251
Setting action logging to write to a file from the configuration tool	251
Setting action logging to write to a database from the configuration tool	252
Configuring the action log web service from the configuration tool	252
Importing a library to Spotfire Analyst for analyzing action logs	253
Setting the action log interval	254
Database logging	254
Action log reference	258
Action log data collected	258
Action log generic entries	259
Action log categories	259
admin actions logged on Spotfire Server	261
auth actions logged from Spotfire Server	261
dblogging actions logged from the database	262
ems action logged from Spotfire Server	262
info_link actions logged from Spotfire Server	262
library actions logged from Spotfire Server	263
routing_rules actions logged from Spotfire Server	263
scheduled_updates actions logged from Spotfire Server	264
Automation Services actions logged from the web service	265
Spotfire Analyst actions logged from the web service	266
Web Player actions logged from the web service	268
Action log actions	269
Action log properties	275
Action log entries	282
Sample action log output	295
System monitoring reference	297
System monitoring entries	297
System monitoring properties	297

Update action logs and system monitoring	298
Updating the Oracle database	299
Updating the Microsoft SQL Server database	300
Server monitoring using JMX	300
Spotfire Server instrumentation	301
JMX configuration security features	302
JMX configuration commands	303
JMX levels	303
Enabling the JMX logging appender	304
Setting up JMX monitoring for JConsole	304
Services monitoring	305
Accessing performance data	305
Web Player analyses information - Overview	306
Web Player analysis information - Details	307
Web Player service performance counters	308
Automation Services instance performance counters	312
Performance troubleshooting	315
Examining the statistics of an individual analysis	316
Logging and exporting monitoring diagnostics	316
Viewing node information	317
Viewing service configuration information	318
Monitoring CPU usage by instances	318
Viewing assemblies information	319
Viewing site information	319
Website diagnostics	319
Viewing routing	320
Enabling automatic dump capture from non-responsive Web Players	321
Basic troubleshooting	322
Troubleshooting Spotfire Server	322
Spotfire Server fails to start	323
Spotfire Server runs out of JVM memory	323
Users cannot log in	324
Troubleshooting the Spotfire database	324
Creating a thread dump	325
Memory exhaustion	325
Creating a memory dump	325
Disabling the memory dump feature	326
Creating a troubleshooting bundle	327
Command-based library administration tasks	327

Importing library content by using the command line	328
Exporting library content by using the command line	328
Library content storage outside of the Spotfire database	329
Configuring external library storage in AWS	329
Configuring external library storage in a file system	330
Monitoring external library storage and fixing inconsistencies	330
Forcing Java to use Internet Protocol version 4	331
Upgrading Spotfire	332
Upgrading from Spotfire 7.0 or earlier	332
Setting up the test environment	332
Upgrading Spotfire Server	333
Installation of Spotfire Server during upgrade	333
Applying hotfixes to the server	333
Run the Spotfire Server upgrade tool	334
Running the Spotfire Server upgrade tool interactively	334
Running the Spotfire Server upgrade tool silently	335
Start Spotfire Server	336
Upgrading a cluster of Spotfire Servers	336
Upgrading Spotfire Analyst clients	337
Deploy client packages	337
Upgrading Spotfire Web Player	337
Mapping content of old configuration files to new service configuration files	338
Upgrading scheduled updates	339
Upgrading Spotfire Automation Services	339
Upgrading authentication method	340
Anonymous combined with other authentication method	340
Different authentication methods for Spotfire Server and Web Player	341
Upgrading load balancing	341
Upgrading analysis links	341
Upgrading Web Services API clients	341
Upgrading customizations	342
Upgrading custom visualizations	342
Upgrading cobranding	342
Upgrading from Spotfire 7.5 or later	342
Installation of Spotfire Server during upgrade	343
Preventing Spotfire Servers and node managers from starting automatically	343
Applying hotfixes to the server	344
Run the Spotfire Server upgrade tool	344
Running the Spotfire Server upgrade tool interactively	344

Running the Spotfire Server upgrade tool silently	346
Start Spotfire Server	346
Upgrading nodes	347
Install node manager	347
Installing a node manager interactively during upgrade	347
Run the node manager upgrade tool	348
Running the node manager upgrade tool interactively	348
Running the node manager upgrade tool silently	348
Optional upgrades	349
Upgrading service configurations	349
Upgrading custom-modified log4j.properties files	350
Applying hotfixes to the Spotfire environment	351
Applying hotfixes for services	351
Backup and restore	352
Backup of Spotfire database	352
Backup of Spotfire Server	352
Backup of services	353
Uninstallation	354
Deleting services	354
Revoking trust of nodes	354
Uninstalling node manager	354
Uninstalling Spotfire Server	354
Advanced procedures	356
Custom configurations for managing space needs	356
Changing the default location of the Web Player temporary files	356
Temporary tablespace	357
Virtual memory modification	357
Modifying the virtual memory (server not running as Windows service)	358
Modifying the virtual memory (server running as Windows service)	358
Data source templates	358
Setting up MySQL5 vendor driver	359
Data source template commands	360
XML settings for data source templates	360
JDBC connection properties	366
Advanced connection pool configuration	367
Kerberos authentication for JDBC data sources	368
Creating an Information Services data source template using Kerberos login	368
Verifying a data source template	369
Information Services settings	369

Default join database	371
Spotfire Server public Web Services API's	371
Enabling the Web Services API	371
Generating client proxies	372
Optional security HTTP headers	372
X-Frame-Options	373
X-XSS-Protection	373
HTTP Strict-Transport-Security (HSTS)	374
Cache-Control	374
X-Content-Type-Options	375
Changing how long the server waits before assuming that a node manager is offline	375
Setting the maximum execution time for an Automation Services job	376
Setting the maximum inactivity time for an Automation Services job	376
Absolute session timeout and idle session timeout	376
Setting idle session timeout and absolute session timeout by using the configuration tool	377
Setting idle session timeout by using the command line	378
Setting absolute session timeout by using the command line	378
Changing whether scheduled updates are sent to exhausted service instances	378
Preventing users from opening scheduled update files outside of their schedule window	379
Changing whether recovered rules are automatically enabled	379
Restarting a node manager to terminate its running jobs	380
Increase the number of available sockets on Linux	380
Switching from online to offline administration help	380
Displaying or hiding the Spotfire Server version	381
Contacting support	382
Reference	383
Spotfire Server files	383
Bootstrap.xml file	383
Server.xml file	384
Krb5.conf file	384
Server bootstrapping and database connection pool configuration	385
Database connectivity	385
Database drivers and database connection URLs	386
Command-line reference	390
add-ds-template	390
add-member	391
bootstrap	392
check-external-library	396
clear-join-db	396

config-action-log-database-logger	397
config-action-logger	399
config-action-log-web-service	400
config-anonymous-auth	401
config-attachment-manager	401
config-auth	402
config-auth-filter	404
config-basic-database-auth	405
config-basic-ldap-auth	406
config-basic-windows-auth	406
config-client-cert-auth	407
config-cluster	408
config-csrf-protection	409
config-custom-web-auth	410
config-encryption	411
config-external-auth	412
config-external-scheduled-updates	417
config-import-export-directory	419
config-jmx	419
config-kerberos-auth	421
config-ldap-group-sync	422
config-ldap-userdir	427
config-library-external-data-storage	428
config-library-external-file-storage	429
config-library-external-s3-storage	430
config-login-dialog	431
config-ntlm-auth	433
config-oidc	437
config-persistent-sessions	441
config-post-auth-filter	442
config-public-address	443
config-scheduled-updates-retries	443
config-two-factor-auth	444
config-userdir	445
config-web-service-api	447
config-windows-userdir	447
copy-group-membership	449
copy-library-permissions	451
copy-rules-to-site	452

create-default-config	454
create-jmx-user	454
create-join-db	455
create-ldap-config	456
create-site	474
create-user	475
delete-disabled-users	475
delete-disconnected-groups	476
delete-jmx-user	477
delete-library-content	478
delete-node	478
delete-oauth2-client	479
delete-service-config	480
delete-site	481
delete-user	482
demote-admin	482
enable-user	483
export-config	484
export-ds-template	485
export-groups	486
export-library-content	487
export-rules	488
export-service-config	489
export-users	491
help	492
import-config	492
import-groups	493
import-jaas-config	494
import-library-content	495
import-rules	497
import-scheduled-updates	499
import-service-config	501
import-users	502
invalidate-persistent-sessions	503
list-active-service-configs	504
list-addresses	505
list-admins	505
list-auth-config	506
list-certificates	506

list-configs	507
list-deployment-areas	508
list-ds-template	509
list-groups	509
list-jaas-config	510
list-jmx-users	511
list-ldap-config	511
list-ldap-userdir-config	512
list-licenses	512
list-logging	513
list-nodes	514
list-ntlm-auth	514
list-oauth2-clients	515
list-online-servers	516
list-post-auth-filter	516
list-service-configs	517
list-service-instances	518
list-services	518
list-sites	519
list-userdir-config	519
list-users	520
list-windows-userdir-config	521
manage-deployment-areas	522
modify-db-config	523
modify-ds-template	525
promote-admin	526
register-job-sender-client	526
remove-ds-template	527
remove-jaas-config	528
remove-ldap-config	528
remove-license	529
reset-trust	530
run	530
s3-download	531
set-addresses	532
set-config	533
set-config-prop	533
set-db-config	534
set-license	536

set-logging	536
set-public-address	537
set-server-service-config	538
set-service-config	540
set-site	541
set-user-password	541
show-basic-ldap-auth	542
show-config-history	542
show-deployment	543
show-import-export-directory	544
show-join-database	544
show-library-permissions	545
show-licenses	546
show-oauth2-client	547
switch-domain-name-style	548
test-jaas-config	549
trust-node	550
untrust-node	551
update-bootstrap	552
update-deployment	555
update-ldap-config	556
version	571
Glossary	572

TIBCO Spotfire Server Documentation and Support Services

How to Access TIBCO Documentation

Documentation for TIBCO products is available on the TIBCO Product Documentation website, mainly in HTML and PDF formats.

The TIBCO Product Documentation website is updated frequently and is more current than any other documentation included with the product. To access the latest documentation, visit <https://docs.tibco.com>.

TIBCO Spotfire Server Documentation

The following documents for this product can be found on the TIBCO Documentation site:

- *TIBCO Spotfire® Server and Environment - Installation and Administration*
- *TIBCO Spotfire® Server and Environment - Basic Installation Guide*
- *TIBCO Spotfire® Cobranding*
- *TIBCO Spotfire® Server Release Notes*
- *TIBCO Spotfire® Server Web Services API Reference*
- *TIBCO Spotfire® Server Server Platform API Reference*
- *TIBCO Spotfire® Server Information Services API Reference*
- *TIBCO Spotfire® Server License Agreement*

Release Version Support

Some release versions of TIBCO Spotfire products are designated as long-term support (LTS) versions. LTS versions are typically supported for up to 36 months from release. Defect corrections will typically be delivered in a new release version and as hotfixes or service packs to one or more LTS versions. See also https://docs.tibco.com/pub/spotfire/general/LTS/spotfire_LTS_releases.htm.

How to Contact TIBCO Support

You can contact TIBCO Support in the following ways:

- For an overview of TIBCO Support, visit <http://www.tibco.com/services/support>.
- For accessing the Support Knowledge Base and getting personalized content about products you are interested in, visit the TIBCO Support portal at <https://support.tibco.com>.
- For creating a Support case, you must have a valid maintenance or support contract with TIBCO. You also need a user name and password to log in to <https://support.tibco.com>. If you do not have a user name, you can request one by clicking Register on the website.

System Requirements for Spotfire Products

For information about the system requirements for Spotfire products, visit <http://spotfi.re/sr>.

How to Join TIBCO Community

TIBCO Community is the official channel for TIBCO customers, partners, and employee subject matter experts to share and access their collective experience. TIBCO Community offers access to Q&A forums, product wikis, and best practices. It also offers access to extensions, adapters, solution accelerators, and tools that extend and enable customers to gain full value from TIBCO products. In addition, users can

submit and vote on feature requests from within the [TIBCO Ideas Portal](#). For a free registration, go to <https://community.tibco.com>.

For quick access to TIBCO Spotfire content, see <https://community.tibco.com/products/spotfire>.

Getting started

New TIBCO Spotfire® administrators can begin by learning how a Spotfire® implementation is put together and how it works, or go directly to the basic installation. For experienced Spotfire administrators, the Release Notes describe new features and other changes.



Any updates to this documentation will be available on <https://docs.tibco.com>. To get the latest version of this documentation, click the help button on the TIBCO Spotfire® Server start page (if your implementation allows access to the internet), or go to <https://docs.tibco.com/products/tibco-spotfire-server>.

Experienced Spotfire administrators:

- If you are updating from Spotfire version 7.0 or earlier, you may want to begin with [Introduction to the Spotfire environment](#).
- To get started, see [Upgrading Spotfire](#).

New Spotfire administrators:

- For general information on Spotfire® Server, see [Spotfire Server introduction](#).
- For a description of the Spotfire environment, see [Introduction to the Spotfire environment](#).
- The basic installation takes you through the required steps for a simple configuration of Spotfire Server: the server on one computer, the TIBCO Spotfire® Analyst client on another, the node manager installed, and the TIBCO Spotfire® Web Player and TIBCO Spotfire® Automation Services (if purchased) available on all network computers, user authentication through the Spotfire database.

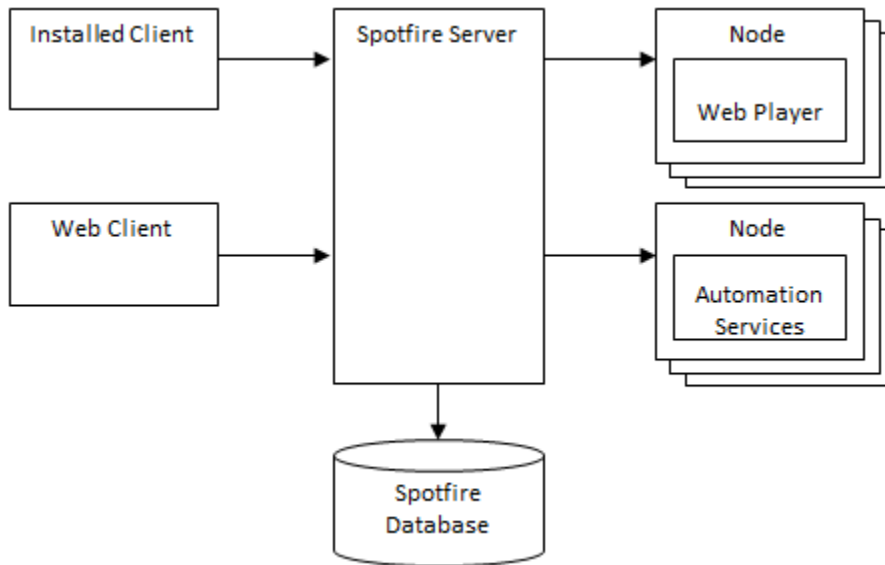


You can also use the basic installation process to complete the initial installation for a more complex implementation. In most cases it is recommended that you have a working basic installation before you add additional servers, load balancers, authentication methods, and so on.

To begin installation, see [Basic installation process for Spotfire](#).

Introduction to the TIBCO Spotfire environment

The TIBCO Spotfire® environment is installed and configured to enable users to analyze their data in the Spotfire® clients.



The Spotfire Server is the central component of the Spotfire environment, to which all Spotfire clients connect. Multiple nodes are installed and connected to Spotfire Server. The Spotfire® Web Player service and Spotfire® Automation Services are installed on nodes to enable the use of Spotfire web clients and the running of Spotfire Automation Services jobs. The server is connected to a Spotfire database that contains a user directory and stores analyses and configuration files. From a Spotfire Server start page, entities in the Spotfire environment can be configured and monitored.

Spotfire Server introduction

Spotfire Server, a Tomcat web application that runs on Windows and Linux operating systems, is the administrative center of any Spotfire environment.

In addition to providing the tools for configuring and administering the Spotfire environment, the Spotfire Server, through the Spotfire clients, enables users to access their data, create visualizations, and share them—with their co-workers or with the world.

Spotfire Server performs the following main functions:

- Authenticates and authorizes Spotfire users.
- Provides access to analyses and data stored in the Spotfire library.
- Provides access to external data sources, including Oracle and SQL Server databases and most JDBC sources, through information links.
- Makes sure that analyses are loaded with updated data according to schedules that are defined by the administrator.
- Provides storage (in the Spotfire database) for configurations, preferences, analyses, and so on.
- Manages the traffic through the Spotfire environment to optimize performance, and in accordance with rules that are defined by the administrator.
- Distributes software updates throughout the implementation.

- Monitors the health and activities of the Spotfire environment and provides diagnostic information both in the server interface and through downloadable logs.

Spotfire database introduction

Spotfire Server requires access to a Spotfire database.

The Spotfire database stores the information that Spotfire Server needs to control the Spotfire environment, including users, groups, licenses, preferences, shared analyses, and system configuration data.

You must have a database server up and running, preferably on a dedicated computer, before installing Spotfire Server. The Spotfire database can be installed on an Oracle Database server or a Microsoft SQL Server.

Nodes and services introduction

Install nodes in the environment to enable the use of Spotfire web clients and Spotfire Automation Services.

With Spotfire Server installed, the installed Spotfire client, called Spotfire Analyst, can be used. To enable the use of Spotfire web clients and Spotfire Automation Services, one or more nodes must also be configured, preferably on dedicated computers.

For each node, the administrator installs and enables services with a specified capability. Each node can have services with the Spotfire Web Player capability, the Spotfire Automation Services capability, or both. The Web Player service allows users to perform analyses in a web browser. Automation Services can be used to automate creation of analysis files, for example, with new data. The capabilities of the enabled services determine the functionality that the node provides to Spotfire end users, through the Spotfire Server. For failover and performance purposes, multiple service instances can be added on each node.

You can scale your Spotfire environment by adding or removing nodes and service instances.

Spotfire clients introduction

Spotfire end users connect to Spotfire Server using either an installed client or a web client.

Spotfire Analyst, a fully-featured client for working with data sources and creating complex analyses, is installed on a user's local computer.

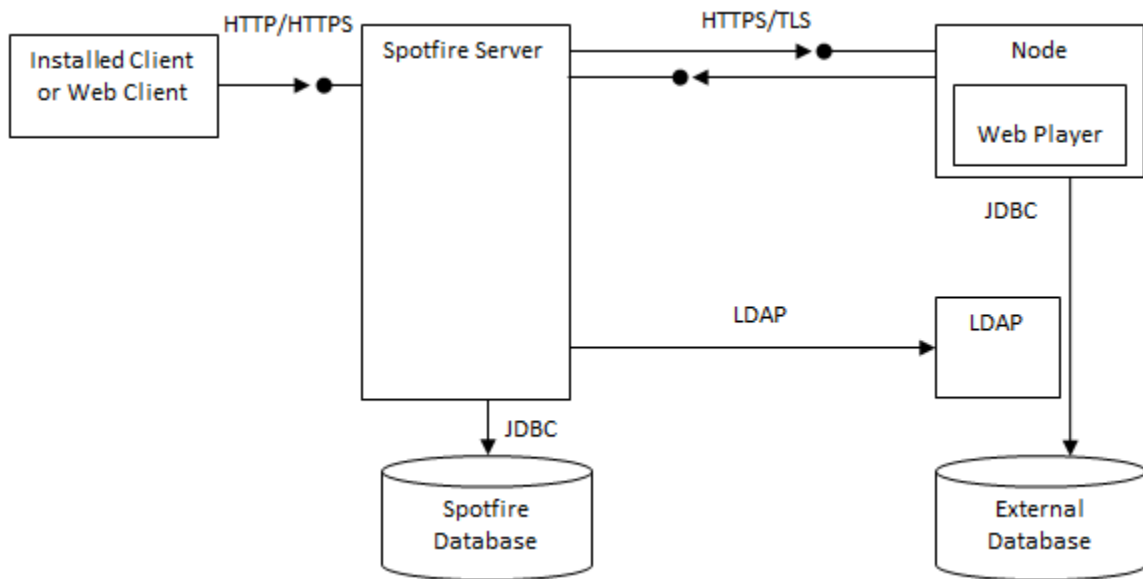
To facilitate interactive analysis in a web browser, a Web Player service generates visualizations that are displayed in the web browser. Depending on which of two licenses a user has, the web client will have different capabilities. With the Consumer license users can view interactive analyses. With the Business Author license users can also create and edit simple analyses.

Environment communication introduction

All back-end communication in a Spotfire environment is secured by HTTPS/TLS, complying with current security standards and industry best practices.

Spotfire Servers listen to incoming traffic from installed clients and web clients on one HTTP or HTTPS port, the front-end communication port.

Spotfire Servers listen to traffic from services on the nodes on another HTTPS port, the back-end communication port.



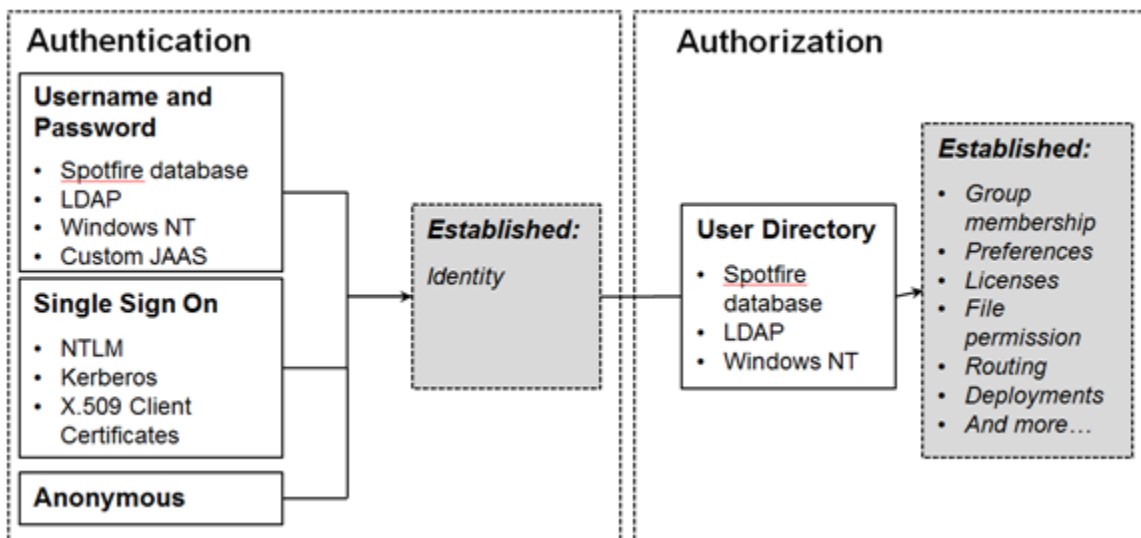
The secured back-end communication is based on certificates. After an administrator has approved the new server or node, the certificates are issued automatically. Without a certificate, a server or a service on a node cannot make requests to, or receive requests from, other entities, except for when requiring a certificate.

After being installed, a node performs a join request to a specific, unencrypted HTTP Spotfire Server port that only handles registration requests. The node remains untrusted until the administrator approves the request by trusting the node. The Spotfire Server start page provides the tools to add nodes to the environment by explicitly trusting them, thereby issuing the certificates. When the node receives its certificate, it can send encrypted communication over the HTTPS/TLS ports and with this it can start to send more than registration requests.

Authentication and user directory introduction

Installed clients, as well as web clients, connect to the Spotfire Server. When users of either client log in to a Spotfire Server, two things happen before they get access: authentication and authorization.

Authentication is the process of validating the identity of a user. Once the identity is validated, the user is authorized in the user directory. Authorizing users determines what their access rights are within the Spotfire environment—in other words, what they are allowed to do.



If username and password is used for authentication, they can be checked against the internal Spotfire user directory, a custom Java Authentication and Authorization Service module, or—the most common option—an external LDAP directory. Spotfire has built-in support for Microsoft Active Directory and the Directory Server product family, which includes Oracle Directory Server, Sun Java Directory Server, and Sun ONE Directory Server. Other LDAP servers can also be used.

For single sign-on, Spotfire supports NTLM, Kerberos, X.509 Certificates, and web authentication.

For anonymous authentication, a preconfigured Spotfire user identity is used to authenticate with the Spotfire Server.

Regardless of how the user was authenticated, the process of authorization is the same. The Spotfire Server checks the Spotfire user directory to determine a user's licenses. Licenses control which functions and analyses users can access with the Spotfire clients.

Optionally, the user and group accounts in the Spotfire user directory can be configured to be synchronized with an external LDAP directory. Spotfire supports the same LDAP servers for directory synchronization as it does for authentication.

In the user directory, users are organized into groups. The user and group information is used to assign permissions, licenses, preferences, and so on to the different resources available within the Spotfire environment.

Users and groups introduction

All Spotfire users are registered in the Spotfire database, where they are organized in groups.

The authentication method of your Spotfire environment determines how users are added to the database and where they are administered:

- If your Spotfire implementation is configured for authentication towards the Spotfire database, the administrator adds and administers user accounts directly in the database by using Spotfire Server and the Administration Manager tool. Administration Manager is accessed from Spotfire Analyst.
- If your implementation uses an external user directory such as LDAP, user accounts are added and administered in that context rather than in the server, and changes are automatically copied to the Spotfire database during synchronization.

Spotfire settings, including access to Spotfire features, which are controlled by licenses, are set at the group level, so all users necessarily belong to at least one group. Any user who is entered into the system automatically becomes a member of the Everyone group; this group cannot be deleted and will always contain all registered users.

In addition to the Everyone group, a user can belong to any number of groups, and has access to all of the features that are enabled for those groups. Groups can be created and managed locally in the Spotfire database, or synchronized from an external source such as an LDAP directory.

Licenses and preferences introduction

Licenses determine which features a group of users should have access to, and preferences set the default behavior of the Spotfire clients.

Licenses determine which features and functionality are available to Spotfire users. License data is stored in the Spotfire database. When a user logs in to Spotfire, the user can only access the features that are enabled for the groups to which the user belongs.

Spotfire administrators can set a wide variety of preferences for the members of a group, such as a default color scheme for analyses or data optimization options.

Licenses and preferences are set in the Administration Manager in Spotfire Analyst. See the Administration Manager documentation for details on license and preference administration.

Deployment introduction

To deploy Spotfire software, the administrator places software packages in a deployment area on Spotfire Server, and assigns the deployment area to particular groups.

If a new deployment is available when a user logs in to a Spotfire client, the software packages are downloaded from the Spotfire Server to the client.

Deployments are used:

- To set up a new Spotfire environment.
- To install a product upgrade, extension, or hotfix provided by Spotfire.
- To install a custom tool or extension.

Administrators can create multiple deployment areas, such as "Production" and "Staging". This allows administrators to test new deployments before rolling them out to the entire client base, or to maintain different deployments for different groups of users.

Spotfire library introduction

The Spotfire database contains the Spotfire library. The library is accessible to Spotfire Analyst, and web clients through the Spotfire Server, allowing users to easily share and reuse their work.

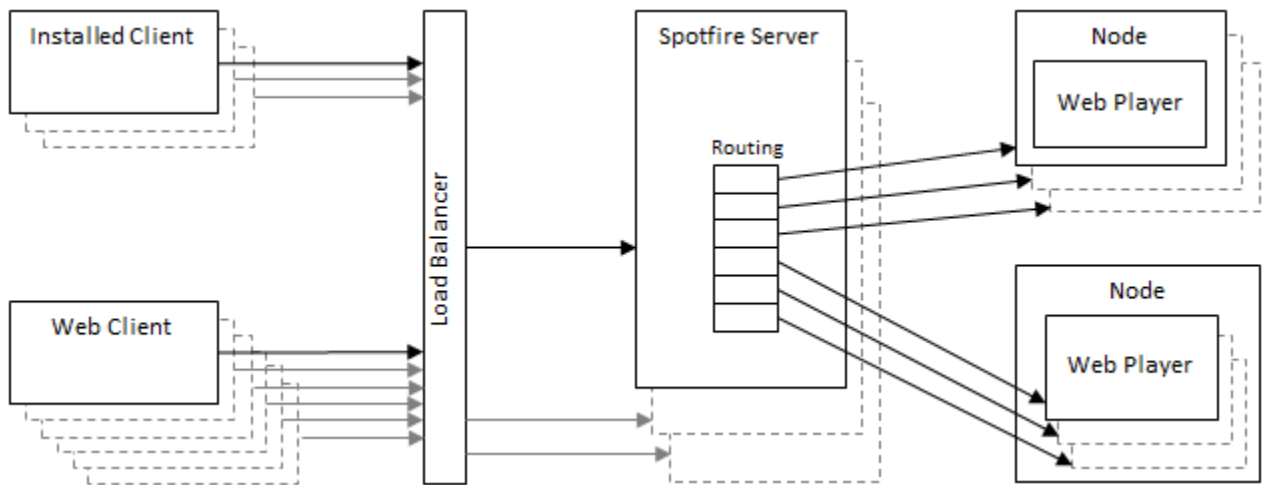
The library stores Spotfire analyses, Spotfire data files, custom Spotfire data functions, information links, shared connections created with Spotfire connectors, and visualization color schemes.

The library is organized into hierarchical folders, which are also used to control access to folder content. The administrator creates the folder structure, and assigns groups with the appropriate read and write permissions to the folders.

Routing introduction

Spotfire provides routing capabilities within the environment.

A cluster of Spotfire Servers in an environment can be fronted by a load balancer to distribute the traffic to the servers. No load balancer is required between Spotfire Server and the nodes because the routing capability of Spotfire Server features built-in load balancing, enabling non-opened analyses to be loaded by the least utilized Web Player service instance.



By default, any Spotfire Server in a cluster can send requests from clients to any Spotfire Web Player service instance. Likewise, any Spotfire Web Player service instance can access any Spotfire Server for library data or to execute information links.

After an analysis has been opened in a client, all subsequent requests for the session are forwarded to the instance that was used for the initialization; thus Spotfire Server routing maintains analysis session affinity.

Default routing improves capacity utilization by forwarding requests for a specific analysis file to the instance or instances of the Spotfire Web Player where it is already opened, thereby serving multiple users with the same service instance. Analysis data is also shared between users, so additional users accessing the analysis file will have a low impact on performance.

In addition to the default routing, administrators can create resource pools and assign any Spotfire Web Player instances to them. The resource pools abstraction enables default routing to be altered by specific routing rules. Rules can be specified for users, groups, or specific analysis files, and are defined and applied in priority order, similar to mail sorting rules. Rules can be sorted, enabled, disabled, and re-mapped to a different resource pool.

There are three health status codes for Web Player instances, used to better route traffic among the instances: Available (or OK), Strained, and Exhausted. The status codes are calculated from the CPU and memory usage on the node running the service instance. The current status can be observed on the diagnostics pages.



It is expected that a service instance that is frequently busy, and has high CPU or memory usage, would remain in the Strained state for long periods of time.

Also, administrators can attach schedules to routing rules that apply to analysis files, effectively turning a routing rule into a scheduled update. Thereby, the administrator can have the analysis pre-loaded on selected instances in a resource pool, and have the analysis refreshed at specified intervals.

Data sources introduction

The Spotfire environment provides several ways for clients to connect to data. The most common ones are: opening a local file, connecting through the information services function of Spotfire Server, or using a Spotfire connector. Users can combine data from multiple sources in a single Spotfire analysis.

Using information services is an option for connecting to enterprise data. In this case, the Spotfire Server makes connections to data sources on behalf of the client, using information links saved in the Spotfire library. The raw data sets are loaded into the memory of the server.

The data sources available are Oracle, Microsoft SQL Server, Teradata, Sybase, SAS/Share, MySQL, DB2, and custom JDBC source types.

Spotfire connectors provide a mechanism for installed clients and service instances to make a direct connection with enterprise data. Depending on the connector, users can choose to load the entire raw data set in the memory of the computer where the client or service instance is installed, or only retrieve aggregated results and make new queries as needed for more detail.

Logging introduction

In addition to the configurable logs for the Spotfire Server, the nodes, and the service instances, the Action Logs and System Monitoring feature helps administrators keep an eye on the health of their Spotfire environment.

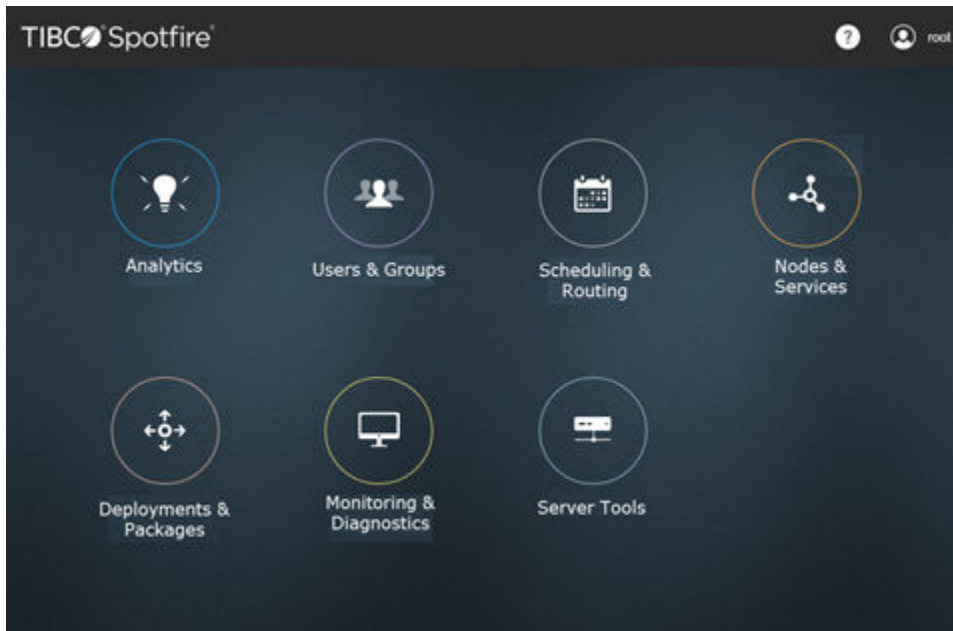
The action logs collect information about system events that are sent through a web service from Spotfire Analyst, Spotfire Automation Services, and the Spotfire Web Player service to the Spotfire Server. These event logs, along with those from the Spotfire Server itself, can be saved either to files or in a database.

System monitoring takes periodic snapshots of key metrics on the Spotfire Server and the Spotfire Web Player services, and stores this information in the same location as the action logs. The logs can then be analyzed in a Spotfire client.

Administrators have many options for how to configure this feature, including which events and system statistics should be logged, from which hosts logging information should be collected, and how the logs are pruned or archived.

Administration interface introduction

The Spotfire Server start page provides access to most administrative tasks and diagnostic information on your Spotfire environment.



- In **Analytics** you can create new analyses, and view and edit analyses that are in the Spotfire library.
- In **Users & Groups** you can create users and groups, add users or groups to groups (including the predefined administrator ones), assign deployment areas to groups, and change user names, passwords, and emails.
- In **Scheduling & Routing** you can schedule updates and monitor their status, date, and time, and create routing rules applicable to groups, users, or specific analysis files.
- In **Nodes & Services** you can review the servers and services setup, add new nodes, services, and service instances, upgrade or rollback existing ones, and create resource pools for routing rules.

- In **Deployments & Packages** you can manage products, upgrades, extensions, and hotfixes by creating or altering deployment areas, adding distributions and packages, and so forth.
- In **Monitoring & Diagnostics** you can monitor the system status, set logging levels, review logs, troubleshoot and download troubleshooting bundle, create memory dumps, and more.
- In **Server Tools** you can download the configuration tool for Spotfire Server.

Library administration, licenses, and preferences are configured in the Administration Manager in the installed Spotfire Analyst client.

Example scenario

This is an example scenario of what happens in the Spotfire environment when a user opens an analysis in a web client.

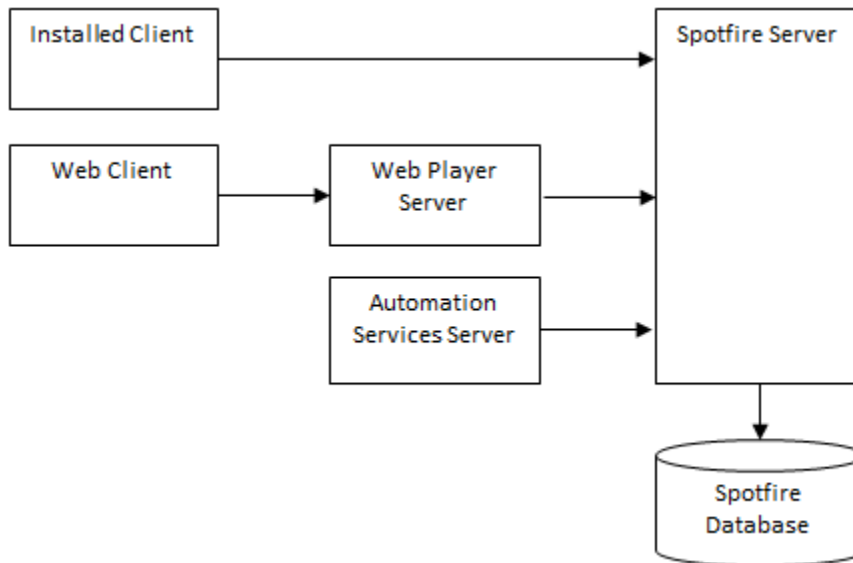
1. The Spotfire web client user receives an email with a link to an analysis that contains interesting information.
2. When the link is opened, an ordinary http (or https) connection is set up from the browser to Spotfire Server. Because the environment is configured for username and password authentication, a login dialog appears.
3. If the username and password are correct, the user also needs to be listed in the user directory. Spotfire Server compares the credentials towards the Spotfire database for verification.
4. A check is made to see that the user has the license privileges to see the analysis, which is stored in the library.
5. The analysis is not already loaded on any Web Player service instance, so the routing logic of Spotfire Server selects the least utilized instance to load the analysis. The request is forwarded to this instance.
6. The Web Player service instance loads the analysis from the library.
7. Data in an analysis can be linked or embedded. This analysis contains linked data, loaded through information services. A request for the data goes back from the Web Player service instance to a Spotfire Server.
8. After the analysis and its data are loaded, Spotfire Server acts as a proxy between the web browser and the Web Player service instance.
9. The user finds the analysis interesting and wants to add an extra visualization. Because the user has the Business Author license, the menu options to do so are visible.
10. After the user has updated and saved the analysis, the user can send a link to interested parties.

Upgrading from Spotfire 7.0 or earlier – an introduction

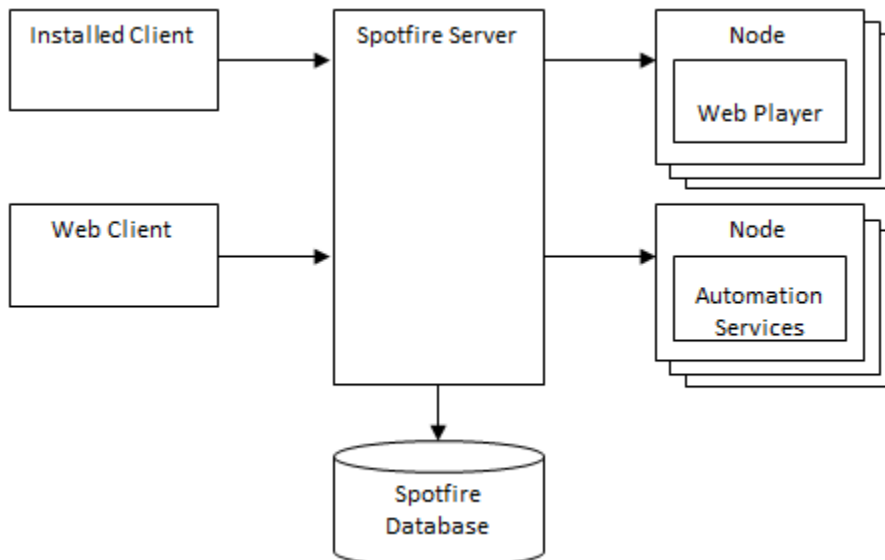
The biggest change from Spotfire 7.0 and earlier versions to Spotfire 7.5 and later is that Spotfire Server now handles all external communication and that Spotfire Web Player and Spotfire Automation Services have become a set of scalable back-end services, installed on nodes.

That means that all web client users connect to Spotfire Server instead of a Spotfire Web Player server, and that Spotfire Automation Services connects to Spotfire Server instead of to an Automation Services server.

A Spotfire 7.0 or earlier environment:



A Spotfire 7.5 or later environment:



When upgrading from Spotfire 7.0 or 6.5, this change mostly affects two things: Spotfire Server now handles all user authentication, regardless of which Spotfire client they use, and no load balancing is required in front of any Spotfire Web Player servers.

Upgrading Spotfire Server is done the same way as in previous versions. You install the new Spotfire Server and use the Spotfire Server Upgrade tool to upgrade the database and, if selected, copy certain files from the old installation of Spotfire Server to the new installation directory.



To be able to upgrade to the new environment, you must have Spotfire Server 6.5.3 HF-008 (or later) or Spotfire Server 7.0.0 HF-002 (or later) installed. If you have an earlier version of Spotfire Server installed, you must first upgrade that server to one of these versions.

To upgrade to the new Spotfire Web Player and Spotfire Automation Services, you apply your applicable existing configurations, install the services on a node, and deploy any extensions.

It is recommended that you set up a staging environment for testing before upgrading.

Some specific things to take into consideration when upgrading are:

- **CPU and memory:** Because Spotfire Server performs more work than in previous versions, it consumes more resources, I/O as well as CPU. All non-client computers in your environment (the computers that host Spotfire Server, and the nodes) require at least 16 GB of memory.
- **Centralized configuration:** All configuration files are now stored in the Spotfire database. This means that a Spotfire Web Player service or Spotfire Automation Services configuration can be centrally applied to all services in your environment. However, this also means that names and content of configuration files have been changed and that old configurations must be copied manually.
- **Authentication:** In Spotfire 7.0 and 6.5, you configure authentication on the Spotfire Server for Spotfire Analyst users and on the Spotfire Web Player server for Spotfire web client users. In the new environment you set up the authentication for all users on Spotfire Server. This means that the same authentication method is used for Spotfire Analyst users as for Spotfire web client users. Therefore, it is no longer supported to use different authentication methods for Spotfire Analyst users and Spotfire web client users. However, anonymous authentication can be combined with another authentication method on the same Spotfire Server. If a custom authentication method was used, this is configured as an external authentication on Spotfire Server.



As of Spotfire version 7.9, you can use sites to configure multiple authentication methods within a single Spotfire environment.

- **Load Balancing:** If your Spotfire 7.0 or 6.5 environment had multiple Spotfire Web Player servers and a load balancer, the load balancer in front of the Web Players is no longer needed. In the new environment, each Web Player service on each node can have multiple instances running. The load balancer in front of the Spotfire Web Players is replaced by the routing capabilities of Spotfire Server. A load balancer can still be used in front of multiple Spotfire Servers.
- **Web Links:** If you have old web links to analyses, these must be updated. Because all users now connect to Spotfire Server, the DNS entry to the former Web Player server must now point to the Spotfire Server.
- **Automation Services:** Existing scheduled Spotfire Automation Services jobs, using the Client Job Sender, must be updated because the configurations have changed and the Client Job Sender now connects to Spotfire Server instead of an Automation Services Server.
- **Extensions and customizations:** API Extensions or customizations, such as custom visualizations or co-branding, must be updated when upgrading to the new environment.

For more information on changes needed, and instructions on how to upgrade your environment, see [Upgrading from 7.0 or earlier](#).

Basic installation process for Spotfire

To get Spotfire up and running in a simple configuration, follow these steps. The resulting simple installation includes the following: the server on one computer, a few Spotfire Web Player instances available for other computers, the Spotfire Analyst client on another computer, and the user directory in the Spotfire database.

Prerequisite

A database server must be up and running, preferably on a dedicated computer. Spotfire supports Oracle Database server and Microsoft SQL Server.



To view the complete system requirements, go to <http://support.spotfire.com/sr.asp>.



If you are running an earlier version of Spotfire Server, see [Upgrading from Spotfire 7.0 or earlier](#).

1. [Download the required software.](#)
2. [Collect the required information.](#)
3. Set up the Spotfire database:
 - [On Oracle](#)
 - [On SQL](#)
4. [Run the Spotfire Server installer.](#)
5. [Apply hotfix.](#)
6. [Create the bootstrap.xml file.](#)
7. [Create and save a basic Spotfire Server configuration.](#)
8. [Create an administrator user.](#)
9. [Start Spotfire Server.](#)
10. [Deploy client software packages to Spotfire Server.](#)
11. [Install a node manager.](#)
12. [Trust the node.](#)
13. [Install Spotfire Web Player instances.](#)
14. [Install Spotfire Automation Services instances.](#)



Alternatively, you can use the command line after step 5 above (see [Manually creating a simple configuration](#)) or run a script that invokes multiple commands (see [Scripting a configuration](#)).

Installation and configuration

Spotfire Server requires that the preparation, installation, database configuration, and server configuration happen in a specific order. Make sure that you follow the steps as described.

See [Basic installation process for Spotfire](#) for the required sequence.

Preparation

Prepare to install Spotfire Server by downloading the required software from the TIBCO eDelivery and Support websites, recording the required system properties, and setting up the Spotfire database on your database server.



Make sure that your system fulfills the requirements listed on the TIBCO Spotfire Server System Requirements page, http://support.spotfire.com/sr_spotfireserver.asp.



If you are upgrading, first read [Upgrading Spotfire](#).

Downloading required software

The first step in installing Spotfire Server is to download the required software to the computer that will run the server.

Prerequisites

You must have access to the required software on the TIBCO eDelivery website and the TIBCO Support website. If you do not have access, contact your sales representative.



As of Spotfire Server version 7.11.4, server hotfixes can be applied only on the specific service pack version that they were created for. Example: If you currently have Spotfire version 7.11.3, you can only apply server hotfixes for the 7.11.3 version, such as 7.11.3 HF-001, 7.11.3 HF-002, and so on. If you want a hotfix of a different service pack level, such as 7.11.5 HF-001, you must first make sure to upgrade to that service pack (7.11.5) before applying the hotfix. (Client hotfixes have not changed.)

Procedure

1. On the [TIBCO eDelivery website](#), go to the TIBCO Spotfire Server page.
2. At the bottom of the page, click **Download**, and then sign in to the site if required.
3. On the server download page, select the latest version and your platform, and select the license agreement check box.
4. Under **Installation Method**, do one of the following:
 - To download the entire product, including language packs and developer software, select **Full Product with Download Manager**, click **Download**, and then follow the instructions.
 - To download fewer files, do the following:
 1. Select **Individual file download**.
 2. Under **SELECT AN INDIVIDUAL COMPONENT**, expand **TIBCO Spotfire Server Software**.
 3. Under **TIBCO Spotfire Server Software**, select either `tib_sfired_server_version_win.zip` (Windows) or `tib_sfired_server_version.tar` (Linux). The software is downloaded to your computer.

The following example shows the approximate location of the required software components for Windows. The Linux options are similar.



4. Expand **TIBCO Spotfire Deployment Kit Software**.
 5. Under **TIBCO Spotfire Deployment Kit Software**, select `TIB_sfire_deploy_version.zip`.
 6. Select any other files that you want to download.
 7. Unzip any zipped files that you downloaded.
5. Optional: If you purchased Spotfire Automation Services, locate and download the product files. For information about installing the product, see the Spotfire Automation Services help.
 6. Download the folder containing the latest hotfix for Spotfire Server:
 1. Sign in to the [TIBCO Support website](#).
 2. Click **Downloads > Hotfixes**.
 3. On the Available Hotfixes page, expand **AvailableDownloads, Spotfire, and Server**.
 4. Select the .zip files containing the hotfixes for your Spotfire Server version (if you are upgrading, select the hotfixes for your new version), and click **Download**. (The .md5 files verify the integrity of the files and do not need to be downloaded.)



The hotfixes are cumulative, so you only have to download the latest one.

5. When the download is complete, unzip the folder's contents.

What to do next

Collect required information

Collecting required information

To set up the Spotfire database, and install and configure Spotfire Server, you must have certain information about the IT system at your site and how you want Spotfire Server to interact with the existing system.

Prerequisites

- A database server must be up and running before you can install Spotfire Server, preferably on a separate computer. The Spotfire Server installer will not install a database server. Spotfire supports Microsoft SQL Server and Oracle Database server.

Procedure

1. Collect the following information about your **database server**:



You may need to contact your database administrator.

Required information	Notes	Your information
Database server type	Either MSSQL or Oracle	
Database server hostname		
Administrator user name		
Administrator password		
Connection identifier	For Oracle only	
Instance name	For MSSQL only	

2. Decide on the following information for the **Spotfire database**:

Required information	Notes	Your information
Spotfire database name	For MSSQL only. The default is spotfire_server.	
Spotfire database user name	If the databases uses Integrated Windows authentication, note this user. If you use Integrated authentication, Spotfire Server must run as this Windows Domain user.	
Spotfire database password		

3. Decide on the following for **Spotfire Server**:

Required information	Notes	Your information
Spotfire Server front-end port	<p>Used for communication with Spotfire clients.</p> <p>The default is 80. If another application on the same computer uses port 80, select a different port number.</p>	
Back-end registration port	<p>Used for key exchange to set up trusted communication between the Spotfire Server and nodes.</p> <p>The default is 9080.</p>	
Back-end communication port (TLS)	<p>Used for encrypted traffic between nodes.</p> <p>The default is 9443.</p>	
Spotfire Server login method	<p>Knowledge about your organization's IT infrastructure is required to set up any login method other than Spotfire database.</p> <p>Available login methods:</p> <ul style="list-style-type: none"> • Username and password: Spotfire database, LDAP, Custom JAAS, Windows NT Domain • Single sign-on: NTLM, Kerberos, X.509 Client Certificate, web authentication 	

Required information	Notes	Your information
Spotfire Server user directory	Knowledge about your organization's IT infrastructure is required to set up any user directory other than Spotfire database. Valid options are: Spotfire database, LDAP, and Windows NT Domain.	
Spotfire Server operating system		
Spotfire Servers hostnames		
Hostname of load balancer, if applicable		

What to do next

[Set up the Spotfire database \(Oracle\)](#)

[Set up the Spotfire database \(SQL Server\)](#)

[Set up the Spotfire database \(SQL Server with Integrated Windows authentication\)](#)

Setting up the Spotfire database (Oracle)

If you are running Oracle Database, follow these steps to set up the Spotfire database before you run the Spotfire Server installer.

Prerequisites

- You have downloaded the Spotfire Server installation kit from the TIBCO eDelivery web site; for instructions, see [Downloading required software](#).
- The following settings must be configured on the Oracle Database server:

- User name and password authentication.



It is also possible to set up Spotfire Server to authenticate with an Oracle Database instance using Kerberos; for instructions, see [Using Kerberos to log in to the Spotfire database](#). In this case, you must run the database preparation scripts manually; see [Running database preparation scripts manually](#).

- National Language Support (NLS) to match the language of the data you will bring into Spotfire.



If the database server NLS cannot be set to match the language of your data, Oracle provides other methods of setting NLS to a specific database or user. For more information, consult your database administrator or see the Oracle database documentation.

- You must also have access to the Oracle Database server. You may need assistance from your database administrator to copy the `install` directory to the database and to provide the database details for the script.






The command-line database tools (for example, sqlplus) must be in the system path of the Oracle Database server.

Procedure

1. Extract the files from the `TIB_sfir_server_version number_win.zip` or `TIB_sfir_server_version number_linux.tar` file to a directory on your desktop.
2. Copy the `oracle_install` directory from the `scripts` directory to the computer running Oracle Database server.
3. On the Oracle Database computer, open the `oracle_install` directory, and then, in a text editor, open the `create_databases` script that corresponds to your platform:
 - Windows: `create_databases.bat`
 - Linux: `create_databases.sh`
 - Windows (Oracle Database running on Amazon RDS): `create_databases_rds.bat`
 - Linux (Oracle Database running on Amazon RDS): `create_databases_rds.sh`
4. In the section under "Set these variables to reflect the local environment", edit the `create_databases` script by providing the appropriate database server details.

Definitions of the variables in `create_databases`

Variable	Description
ROOTFOLDER	<p>Location where the tablespaces will be created. It must be a directory that is writable for the Oracle instance, usually <i>oracle install dir/oradata/SID</i> or <i>oracle install dir/oradata/PDBNAME</i>.</p> <div>  Do not add a slash or backslash after the <SID>.  This variable is not applicable for the Amazon RDS <code>create_databases</code> scripts. </div>
CONNECTIDENTIFIER	Oracle TNS name/SID of the database/service name, for example ORCL or //localhost/pdborcl.example.com.
ADMINNAME	Name of a user with Oracle Database administrator privileges for the database identified in the CONNECTIDENTIFIER , for example "system".
ADMINPASSWORD	Password of the ADMINNAME user.
SERVERDB_USER	Name of the user that will be created to set up the Spotfire database.
SERVERDB_PASSWORD	Password for SERVERDB_USER .
SERVER_DATA_TABLESPACE	Name of the tablespace that will be created. The default value works for most systems.

Variable	Description
SERVER_TEMP_TABLESPACE	<p>Name of the temporary tablespace that will be created. The default value works for most systems.</p> <div>  <p>Conflicting tablespaces can occur if you are creating the Spotfire tablespaces on a database server that is already hosting an Analytics Server or a previous version of Spotfire Server. Make sure that you do not select any names for the new tablespaces and users that conflict with the already hosted tablespaces and users.</p> </div>
INSTALL_DEMODATA	<p>Set to "yes" if you want to install the demo database. The demo database contains example data for learning about Spotfire.</p> <p>If you install the demo database, you must later perform additional steps to make the data available to the users; see Enabling demo database use.</p>
DEMO_DB_USER	Name of the user who will access the demo database. If you change the default user name, the corresponding information layer must be redirected in Information Designer.
DEMO_DB_PASSWORD	Password for DEMO_DB_USER.

Example

This is an example of how the file section might look after modification:

```
rem Set these variables to reflect the local environment:
rem Where should the data be stored on the database server:
set ROOTFOLDER=C:\oracle\app\orcl
rem A connect identifier to the container database or the pluggable database
rem for a pluggable database a service name like //localhost/pdborcl.example.com
rem could be the SID for Oracle 11 or earlier, TNSNAME etc,
rem see the documentation for sqlplus
set CONNECTIDENTIFIER=//localhost/pdborcl.example.com
rem a username and password for an administrator in this (pluggable) database
set ADMINNAME=system
set ADMINPASSWORD=admin123
rem Username and password for the Spotfire instance this user will be created,
rem remember that the password is written here in cleartext,
rem you might want to delete this sensitive info once the script is run
set SERVERDB_USER=spotfire_db
set SERVERDB_PASSWORD=spotfire_db123
rem The spotfire tablespaces, alter if you want to run multiple instances in the
rem same database
set SERVER_DATA_TABLESPACE=SPOTFIRE_DATA
set SERVER_TEMP_TABLESPACE=SPOTFIRE_TEMP
rem Demo data parameters, should it be installed at all
set INSTALL_DEMODATA=no
rem Username and password for the demodata
set DEMO_DB_USER=spotfire_demodata
set DEMO_DB_PASSWORD=spotfire_demodata123
```

5. Save the file and close the text editor.
6. Open a command line and go to the directory where you placed the scripts.
7. Type `create_databases.bat` or `create_databases.sh` and press Enter.
If the parameters are correct, text that is similar to the following text appears in the command-line interface:

```

C:\scripts\oracle\install>create_databases.bat
Creating Spotfire Server tables
Populating Spotfire Server tables
Creating Spotfire Server database user
Spotfire Server demo database user and data will not be created
-----
Please review the log file <log.txt> for any errors or warnings!
C:\scripts\oracle\install

```



The log.txt file is created in the same directory as the create_databases file. Also, if you indicated that you want to download the demo database, log files from the creation of the Spotfire demo data are created. Examine these files to verify that no errors occurred, and retain the logs for future reference.



Because the scripts contain sensitive information, it is good practice to remove them after your Spotfire environment has been installed.

What to do next

Install Spotfire Server

Setting up the Spotfire database (SQL Server)

If you are running Microsoft SQL Server, follow these steps to set up the Spotfire database before you run the Spotfire Server installer.



If you plan to configure Integrated Windows authentication (IWA) between Spotfire Server and the Spotfire database in SQL, see [Setting up the Spotfire database \(SQL Server with Integrated Windows authentication\)](#).

Prerequisites

- You have downloaded and unzipped the Spotfire Server installation kit from the TIBCO eDelivery web site; for instructions, see [Downloading installation software](#).
- The following settings must be configured on the SQL Server:
 - TCP/IP communication listening on a port (the default is 1433).
 - Case-insensitive collation (at least for the Spotfire database).



If your installation of SQL Server uses a case-sensitive collation by default, or your data uses a different collation than Latin1_General_CI_AS, you must edit the create_server_db.sql script before running the create_databases.bat script. See step 2 below.


- The command line database tools (sqlcmd, etc.) must be in the system path.

Procedure

1. Copy the <installation files dir>/scripts/mssql_install directory to the computer running SQL Server.
2. Optional: If your installation of SQL Server uses a case-sensitive collation by default, or if you need to define a different collation, follow these steps:
 - a) On the SQL Server computer, open the mssql_install directory, and then open the create_server_db.sql script in a text editor.
 - b) Locate the line --create database \$ (SERVERDB_NAME) collate Latin1_General_CI_AS;
 - c) Remove the leading dashes (--).

- d) If needed, replace `Latin1_General_CI_AS` with the name of the desired collation, but make sure it is case-insensitive (CI). See the SQL Server documentation for information about available collations.
 - e) Comment out the next line by inserting leading dashes (--), so that the line looks like this: --
`create database $(SERVERDB_NAME)`
 - f) Save the file and close the text editor.
3. On the SQL Server computer, go to the `mssql_install` directory, and open the `create_databases.bat` file in a text editor. If your SQL Server is running on Amazon RDS, open the `create_databases_rds.bat` script in a text editor.
 4. In the section under "Set these variables to reflect the local environment", edit the `create_databases.bat` script by providing the appropriate database server details.

Definitions of the variables in `create_databases.bat`

Variable	Description
CONNECTIDENTIFIER	<p>Replace <code><SERVER></code> with the name of the server running the SQL Server instance, and replace <code><MSSQL_INSTANCENAME></code> with the name of the SQL Server instance.</p> <div>  <p>The default installation of SQL Server creates an unnamed instance of the SQL Server. If your SQL Server is a new installation, delete the "MSSQL_INSTANCENAME" part of the line and enter only the SERVER name. The connection will be made to the unnamed instance.</p> </div>
ADMINNAME	Name of a user with SQL database administrator privileges, usually "sa".
ADMINPASSWORD	Password of the <i>ADMINNAME</i> user.
SERVERDB_NAME	Name of the Spotfire database that will be created; <code>spotfire_server</code> is the default.
SERVERDB_USER	Name of the user that will be created to set up the Spotfire database.
SERVERDB_PASSWORD	Password for <i>SERVERDB_USER</i> .
INSTALL_DEMODATA	<p>Set to "yes" if you want to install the demo database. The demo database contains example data for learning about Spotfire.</p> <p>If you install the demo database, you must later perform additional steps to make the data available to the users; see Enabling demo database use.</p>
DEMODB_NAME	Name of the demo database. If you change the default database name, the corresponding information layer needs to be redirected in Information Designer.
DEMODB_USER	Name of the user that will access the demo database.
DEMODB_PASSWORD	Password for <i>DEMODB_USER</i> .

Example

This is what the `create_databases.bat` file section might look like after modification:

```
rem Set these variable to reflect the local environment:
set CONNECTIDENTIFIER=DBSERVER\MSSQL
set ADMINNAME=sa
set ADMINPASSWORD=admin123
set SERVERDB_NAME=spotfire_server
set SERVERDB_USER=spotfire_db
set SERVERDB_PASSWORD=spotfire_db123

rem Demo data parameters
set INSTALL_DEMODATA=no
set DEMODB_NAME=spotfire_demodata
set DEMODB_USER=spotfire_demodata
set DEMODB_PASSWORD=spotfire_demodata123
```

5. Save the file and close the text editor.
6. Open a command line as an administrator and go to the directory where you placed the scripts.
7. Type `create_databases.bat` and press Enter.
If the parameters are correct, text that is similar to the following text is displayed at the command line:

```
C:\scripts\mssql_install>create_databases.bat
Creating Spotfire Server tables
Populating Spotfire Server tables
Creating Spotfire Server database user
Spotfire Server demo database user and data will not be created
-----
Please review the log file (log.txt) for any errors or warnings!
C:\scripts\mssql_install>
```



Log files are created in the same directory as the `create_databases.bat` file. Examine these files to verify that no errors occurred and retain the logs for future reference.



Because the scripts contain sensitive information, it is good practice to remove them after your Spotfire environment has been installed.

What to do next

[Install Spotfire Server](#)

Setting up the Spotfire database (SQL Server with Integrated Windows authentication)

If you are running Microsoft SQL Server and plan to use Integrated Windows authentication between Spotfire Server and the Spotfire database in SQL, follow these steps to set up the database before you run the Spotfire Server installer.

Prerequisites

- You have downloaded and unzipped the Spotfire Server installation kit from the TIBCO eDelivery web site; for instructions, see [Downloading installation software](#).
- The following settings must be configured on the SQL Server:
 - TCP/IP communication listening on a port (the default is 1433).
 - Case-insensitive collation (at least for the Spotfire database).



If your installation of SQL Server uses a case-sensitive collation by default, or your data uses a different collation than `Latin1_General_CI_AS`, you must edit the `create_server_db.sql` script before running the `create_databases_ia.bat` script. See step 2 below.

- The command line database tools (sqlcmd, etc.) must be in the system path.

With this type of configuration, the Spotfire database will use Windows accounts for authentication. The current user who is running the scripts to create the database must have administrative privileges on the database server, but the Spotfire process should run as a different user when connecting at runtime. Therefore, the scripts have been designed to access the database with a different Windows account when the server is running. This user is assigned to the variable `WINDOWS_LOGIN_ACCOUNT`. Note that the user who ran the scripts to create the database will get database owner permissions (dbo) to the database and will be able to administer the Spotfire database using integrated authentication.

If the user assigned to the `WINDOWS_LOGIN_ACCOUNT` variable already exists as a login on the database server, the `create_server_user_ia.sql` script must be edited. The following rows should then be commented out:

```
use master
GO
CREATE LOGIN [$(WINDOWS_LOGIN_ACCOUNT)] FROM WINDOWS WITH
DEFAULT_DATABASE=[$(SERVERDB_NAME)], DEFAULT_LANGUAGE=[us_english]
GO
ALTER LOGIN [$(WINDOWS_LOGIN_ACCOUNT)] ENABLE
GO
DENY VIEW ANY DATABASE
TO [$(WINDOWS_LOGIN_ACCOUNT)]
```

As mentioned above, the server process should connect as different user than the user that runs this script for security reasons. If you really want to use the same account then you must comment out the following lines from `create_server_user_ia.sql`:

```
CREATE USER [$(SERVERDB_USER)] FOR LOGIN [$(WINDOWS_LOGIN_ACCOUNT)]
GO
```

And, if you have enabled the creation of demo data, the following rows in `create_demo_user_ia.sql` must also be commented out:


```
CREATE USER [$(DEMO_DB_USER)] FOR LOGIN [$(WINDOWS_LOGIN_ACCOUNT)]
GO
```

Procedure

1. Copy the `<installation files dir>/scripts/mssql_install` directory to the computer running SQL Server.
2. If your installation of SQL Server uses a case-sensitive collation by default, or if you need to define a different collation, follow these steps:
 - a) On the SQL Server computer, open the `mssql_install` directory, and then open the `create_server_db.sql` script in a text editor.
 - b) Locate the line `--create database $(SERVERDB_NAME) collate Latin1_General_CI_AS;`
 - c) Remove the leading dashes (--).
 - d) If needed, replace `Latin1_General_CI_AS` with the name of the desired collation, but make sure it is case-insensitive (CI). See the SQL Server documentation for information about available collations.
 - e) Comment out the next line by inserting leading dashes (--), so that the line looks like this: `-- create database $(SERVERDB_NAME)`
 - f) Save the file and close the text editor.
3. On the SQL Server computer, go to the `mssql_install` directory, and then open `create_databases_ia.bat` in a text editor.

4. In the section under "Set these variables to reflect the local environment", edit the `create_databases_ia.bat` script by providing the appropriate database server details. The definitions of the variables are listed at the top of the script.

Definitions of the variables in `create_databases_ia.bat`

Variable	Description
CONNECTIDENTIFIER	<p>Replace <code><SERVER></code> with the name of the server running the SQL Server instance, and replace <code><MSSQL_INSTANCENAME></code> with the name of the SQL Server instance.</p> <div>  <p>The default installation of SQL Server creates an unnamed instance of the SQL Server. If your SQL Server is a new installation, delete the "MSSQL_INSTANCENAME" part of the line and enter only the SERVER name. The connection will be made to the unnamed instance.</p> </div>
WINDOWS_LOGIN_ACCOUNT	The Windows Login Account that should be created as a login on the database server. The server process must run as this user.
SERVERDB_NAME	Name of the Spotfire database that will be created; <code>spotfire_server</code> is the default.
SERVERDB_USER	Name of the user that will be created for the Spotfire database, associated with the <code>WINDOWS_LOGIN_ACCOUNT</code> .
INSTALL_DEMODATA	<p>Set to "yes" if you want to install the demo database. The demo database contains example data for learning about Spotfire.</p> <p>If you install the demo database, you must later perform additional steps to make the data available to the users; see Enabling demo database use.</p>
DEMO_DB_NAME	Name of the demo database. If you change the default database name, the corresponding information layer needs to be redirected in Information Designer.
DEMO_DB_USER	Name of the user that will access the demo database.

Example

This is how the `create_databases_ia.bat` file section might look after modification:

```
rem Set these variable to reflect the local environment:
set CONNECTIDENTIFIER=DBSERVER\MSSQL
set WINDOWS_LOGIN_ACCOUNT=example.com\win_user
set SERVERDB_NAME=spotfire_server
set SERVERDB_USER=spotfire_user

rem Demo data parameters
set INSTALL_DEMODATA=no
set DEMO_DB_NAME=spotfire_demodata
set DEMO_DB_USER=spotfire_demodata
```

5. Save the file and close the text editor.
6. Open a command line as an administrator and go to the directory where you placed the scripts.
7. Type `create_databases_ia.bat` and press Enter.

If the parameters are correct, text that is similar to the following text is displayed at the command prompt:

```
C:\scripts\mssql_install>create_databases_ia.bat
Creating Spotfire Server tables
Populating Spotfire Server tables
Creating Spotfire Server database user
Spotfire Server demo database user and data will not be created
-----
Please review the log file (log.txt) for any errors or warnings!
C:\scripts\mssql_install>
```



Log files are created in the same directory as the `create_databases_ia.bat` file. Examine these files to verify that no errors occurred, and retain the logs for future reference.



Because the scripts contain sensitive information, it is good practice to remove them after your Spotfire environment has been installed.

What to do next

[Install Spotfire Server](#)

Running database preparation scripts manually

If you plan to set up Kerberos authentication between your database and Spotfire Server, you must run the database SQL preparation scripts manually.

Procedure

1. Read through the `create_databases` script to understand how the scripts work.
2. Run the following scripts:

- `create_server_db.sql`
- `populate_server_db.sql`
- `create_server_env.sql`



For Oracle, the `create_databases` script passes the following variables to these scripts. When you run the database Oracle scripts manually, make sure to pass these variables along to the scripts:

- `ROOTFOLDER`
- `CONNECTIDENTIFIER`
- `SERVER_DATA_TABLESPACE`
- `SERVER_TEMP_TABLESPACE`



For SQL, the `create_databases` script passes the following variables to these scripts. When you run the database SQL scripts manually, make sure to pass these variables along to the scripts:

- `SERVERDB_NAME`
- `DEMODB_NAME`

3. If you want to install the demo database tables that are shipped with Spotfire Server, do the following:

a) Run these scripts:

- `create_demotables.sql`
- `create_demodata_env.sql`

b) Using the appropriate load command for your database, load all of the SQL loader files that are in the demodata folder.

Installation

The Spotfire Server installer adds three major components to your system: A Java environment (JDK), a Tomcat application server, and a Spotfire Server web application.



The Spotfire Server should run in an English (United States) language setting, as stated on the TIBCO Spotfire Server System Requirements page, http://support.spotfire.com/sr_spotfireserver.asp.



If you are upgrading, first read [Upgrading Spotfire](#).

The JAVA_HOME of the Apache Tomcat is set to the path of the installed JDK.



For increased security, you may want to install the Java Cryptography Extension (JCE) unlimited strength jurisdiction policy files. It is the user's responsibility to verify that these files are allowed under local regulations.

Select the appropriate installation procedure for your system and level of experience.

Installing the Spotfire Server files (interactively on Windows)

Running the Spotfire Server installer is the second step in the Spotfire Server installation process, after setting up the database.

Prerequisites

The Spotfire database has been set up on your Oracle or SQL Server database; for instructions, see [Setting up the Spotfire database on Oracle](#) or [on SQL Server](#).



For security and product performance reasons, it is recommended that you install Spotfire Server on a different computer than the database.



This procedure is for an interactive installation, using the installation wizard. Alternatively, you can run a silent installation from the command line; for details, see [Installing the Spotfire Server files \(silently on Windows\)](#).

Procedure

1. In the server installation kit that you downloaded from the TIBCO eDelivery site, double-click `setup-win64.exe`.



If you use Microsoft SQL Server with Windows Integrated Authentication, install Spotfire Server as the Domain User that you set up with the script `create_databases_ia.bat`. Also make sure that Spotfire Server always runs as this Domain User. Confirm with the logs that Spotfire Server starts.

2. In the installation wizard Welcome dialog, click **Next**.
3. In the License dialog, read the agreement, select the appropriate radio button, and then click **Next**.
4. In the Third Party Components dialog, if you plan to configure the system for NTLM and you currently have access to the internet, select **Download and install** and then click **Next**.



If you do not currently have access to the internet, you can install the third-party components later; for instructions, see [Downloading third-party components \(JCIFS\) for NTLM authentication](#).

5. In the Destination Folder dialog you can change the location if you want to, and then click **Next**.
6. In the Windows Service dialog, select the option you want and then click **Next**.
7. In the Spotfire Server Port dialog you can specify the front-end port, and then click **Next**.



To check whether a port is in use, open a command prompt, type `netstat -na`, and press Enter.



The ports selected during installation for front-end, back-end communication, and back-end registration ports must be open in the firewall. (The defaults are 80, 9443, and 9080.)

8. In the Backend Communication Ports dialog you can specify the back-end ports, and then click **Next**.
9. In the Node Manager Hosts dialog, select the computer names that can be used by back-end trust. In general you can leave all the listed names as they are.
10. In the Ready to Install dialog, click **Install**.
The Installing dialog tracks the progress of the installation.
11. When the installation is completed, select **Launch the configuration tool** to open the configuration tool, or **Launch the upgrade tool** if you are upgrading.

What to do next

Apply any available hotfixes for Spotfire Server: [Applying hotfixes](#)

Installing the Spotfire Server files (silently on Windows)

Instead of running the installation wizard, you can install the Spotfire Server files silently by running the installer from the command prompt.

Prerequisites

The Spotfire database has been set up within your Oracle or SQL Server database; for instructions, see [Setting up the Spotfire database on Oracle](#) or [on SQL Server](#).



For security and product performance reasons, it is recommended that you install Spotfire Server on a different computer than the database.




To use the interactive installation wizard instead of the command prompt installation, see [Installing the Spotfire Server files \(interactively on Windows\)](#).

Procedure

1. Open a command prompt as an administrator.
2. If necessary, edit the default parameters. Make sure that none of the ports that you select are already in use.

```
setup-win64.exe /s /v"/qn /l*vx TSS_install.log DOWNLOAD_THIRD_PARTY=Yes
INSTALLDIR=C:\tibco\tss\<version> SPOTFIRE_WINDOWS_SERVICE=Create
SERVER_FRONTEND_PORT=80 SERVER_BACKEND_REGISTRATION_PORT=9080
SERVER_BACKEND_COMMUNICATION_PORT=9443
```

Silent installation parameters

Parameter	Description
 DOWNLOAD_THIRD_PARTY This parameter is case sensitive.	The available options are Yes and No. These components are only needed to configure the system for NTLM.
INSTALLDIR	The installation directory.
SPOTFIRE_WINDOWS_SERVICE	The available options are Create and DoNotCreate.
SERVER_FRONTEND_PORT	Used for communication with Spotfire clients. The default is 80.
SERVER_BACKEND_REGISTRATION_PORT	Used for key exchange to set up trusted communication between the Spotfire Server and nodes. The default is 9080.
SERVER_BACKEND_COMMUNICATION_PORT	Used for encrypted traffic between nodes. The default is 9443.

- Specify /qn for quiet installation with no user interface, or /qb for quiet installation with basic user interface.
- Run the installation script.

What to do next

Apply any available hotfixes for Spotfire Server: [Applying hotfixes](#)

Installing the Spotfire Server files (RPM Linux)

If you have root access to the Linux computer on which you want to install Spotfire Server, you can use the RPM-based installer. If you do not have root access, use the Tarball installer instead.

Prerequisites

The Spotfire database has been set up within your Oracle or SQL Server database; for instructions, see [Setting up the Spotfire database on Oracle](#) or [on SQL Server](#).



For security and product performance reasons, it is recommended that you install Spotfire Server on a different computer than the database.

Procedure

- Open a command line and run the following script: `rpm -ivh tss-<version number>.x86_64.rpm`
As the script runs it prompts you for any missing arguments.
- On the command line, run the post-installation script: `/usr/local/bin/tibco/tss/<version number>/configure [-d] [-s] [-r] [-b]` where:
 - d disables the download of third-party components.
 - s specifies the server front-end port.
 - r specifies the back-end registration port.

- -b specifies the back-end communication port.

What to do next

Apply any available hotfixes for Spotfire Server: [Applying hotfixes](#)

Installing the Spotfire Server files (Tarball Linux)

If you do not have root access to the Linux computer on which you want to install Spotfire Server, use the Tarball installer rather than the RPM installer. Both the installation script and a post-installation script are run from the command line.

Prerequisites

The Spotfire database has been set up within your Oracle or SQL Server database; for instructions, see [Setting up the Spotfire database on Oracle](#) or [on SQL Server](#).



For security and product performance reasons, it is recommended that you install Spotfire Server on a different computer than the database.

Procedure

1. Open a command-line interface, go to the directory where you want to install Spotfire Server, and unpack and run the tar file by running the following command: `tar xzf tss-<version number>.x86_64.tar.gz`



The directory must contain the string "tss" in order for start and stop scripts to work.

As the script runs it prompts you for any missing arguments.

2. In the command-line interface, run the post-installation script in the directory where the tar file was unpacked: `./configure [-d] [-s] [-r] [-b]`, where:
 - -d disables the download of third-party components.
 - -s specifies the server front-end port.
 - -r specifies the back-end registration port.
 - -b specifies the back-end communication port.
3. Optional: If you have root access to the computer, configure the server to start when the computer starts by running this command: `./configure-boot`

What to do next

Apply any available hotfixes for Spotfire Server: [Applying hotfixes](#)

Database drivers

DataDirect database drivers work well for test environments, but for production environments, drivers from Oracle or Microsoft SQL are strongly recommended.

Spotfire Server ships with the following database drivers:

- DataDirect drivers for Oracle and Microsoft SQL
- Microsoft SQL Server driver

Spotfire supports the Oracle driver as well, available from the Oracle web site.

Installing the Oracle database driver

If your implementation uses Oracle Database server, it is recommended that you install an Oracle driver (JDBC) for your production environments.

Procedure

1. Download the database driver from the Oracle website.
2. Place the driver in the following directory: `<installation_dir>/tomcat/lib`.

Installing database drivers for Information Designer

The Information Designer tool, available in Spotfire Analyst, allows users to create analyses based on data retrieved from external JDBC sources. These external data sources are accessed using database drivers.

To connect to an external data source, you must also enable a data source template that matches the database and the specific database driver.



The database connection URL, used by the server to connect to the database, may differ for different database drivers; see [Database drivers and database connection URLs](#).

Procedure

1. Download the database driver.
2. Place the driver in the following directory: `<installation_dir>/tomcat/lib`.
3. Restart Spotfire Server.
4. Enable a data source template that matches the database and the specific database driver that you are using. To enable the template, you can use either the configuration tool or the command [add-ds-template](#).

Applying hotfixes to the server

Before you begin configuring Spotfire Server, you must install any available hotfix for this version of the server.

Prerequisites

- You have installed Spotfire Server.
- You have downloaded the latest hotfix for your version of Spotfire Server; for instructions, see [Downloading required software](#), step 6.

Procedure

- Follow the instructions in the `Installation_Instructions.htm` file that was included in the hotfix package that you downloaded.
For more information, see [Overview of hotfixes for TIBCO Spotfire](#) in the TIBCO Community.

What to do next

Configure Spotfire Server; see [Initial configuration](#).

Initial configuration

It is recommended that Spotfire administrators configure a successful basic installation of Spotfire Server before configuring more advanced implementations.



Multiple configurations can be stored in the Spotfire database, but only one can be active

Configuration using the configuration tool

The Spotfire Server configuration tool provides a clear path to a basic installation, and offers the most frequently used configuration options.

The configuration tool must be run by a Spotfire administrator. If the Spotfire administrator does not have access to the computer running Spotfire Server, or if the server cannot display graphics, the configuration tool can be run from a local computer.

Opening the configuration tool

You can use the Spotfire Server configuration tool for the initial configuration of your Spotfire implementation, or for updating your configuration later on.

Procedure

- There are three ways to open the configuration tool:
 - Select the **Launch the Configuration Tool** check box on the last screen of the Spotfire Server installation wizard.
 - On the computer running Spotfire Server, click **Start**, go to the Spotfire Server folder, and click **Configure TIBCO Spotfire Server**.
 - Run the `uiconfig.bat` file (`uiconfig.sh` on Linux). These files are located in the `<installation_dir>\tomcat\bin` directory.



If you cannot run the configuration tool on the Spotfire Server computer, see [Running the configuration tool on a local computer](#).

Running the configuration tool on a local computer

If running the configuration tool on the Spotfire Server computer is impossible or inconvenient, you can run the tool on a local computer.

Prerequisites

Java 8 runtime must be installed on the local computer.

Procedure

1. From the computer where Spotfire Server is installed, copy the `<installation_dir>\tomcat\webapps\spotfire\tools\spotfireconfigtool.jar` file to the local computer.



If Spotfire Server is up and running, you can also access the `spotfireconfigtool.jar` file on the **Server Tools** page.

2. On the local computer, unpack the `.jar` file by doing one of the following:
 - Double-click the `spotfireconfigtool.jar` file.
 - If your system does not recognize the file type, follow these steps:

1. On the local computer, open a command line and go to the directory that contains the `spotfireconfigtool.jar` file.
2. On the command line, enter the following command:

```
java -jar spotfireconfigtool.jar
```

A `spotfireconfigtool` directory is created in the same directory as the `.jar` file.

3. In the newly-created directory, double-click `uiconfig.bat` (Windows) or `uiconfig.sh` (Linux) to open the configuration tool.

Creating the bootstrap.xml file

The `bootstrap.xml` file configures the database connection.

Prerequisites

Spotfire Server is installed.






For Integrated Windows authentication (IWA) between Spotfire Server and the Spotfire database, see [Setting up the Spotfire Server bootstrap file for Integrated Windows authentication](#).

Procedure

1. If the configuration tool is not open, open it; for instructions see [Opening the configuration tool](#). The configuration tool opens to the System Status page, which lists the necessary configuration steps.
2. Click **Create new bootstrap file**. The Bootstrap page is displayed.
3. Enter the following information in the fields:

Path	You may leave the default path as is.
Driver template	Select a template that is compatible with your database server.
Hostname	The Spotfire database host name (the address of the computer on which the SQL or Oracle database is installed).
Port	The Spotfire database port.
Identifier (SID/ database/service)	The Server ID (for Oracle) or the database name (for MS SQL) of the Spotfire database that was created; <code>spotfire_server</code> is the default.
Username	The name of the database account used by Spotfire Server to connect to the Spotfire database. In the <code>create_databases.bat</code> file, this is the value for <code>ADMINNAME</code> .
Password	The password of the database account. Enter correct database login details, as specified earlier. In the <code>create_databases.bat</code> file, this is the value for <code>ADMINPASSWORD</code> .
URL	The JDBC connection URL. This field is pre-populated from selections made but can be edited.
Driver class	This field is pre-populated from selections made, and cannot be edited. To be able to select Oracle, you must also download the JDBC driver. For details, see Database drivers and database connection URLs

Configuration tool password	<p>Enter a configuration tool password of your choice. This will be used to protect the server configuration from unauthorized access.</p> <div>  <p>The configuration tool password will be required when running the configuration tool.</p> </div>
Server alias	Enter any unique name for the Spotfire Server.
Encryption password (optional)	Enter an encryption password of your own choice. This will be used for encrypting other passwords stored in the Spotfire database. The passwords are encrypted with a static key if no encryption password is specified here.
Addresses	<p>These values should match actual hostnames, fully qualified domain names (FQDN), and IP addresses (IPv4 or IPv6) at which the Spotfire Server can be reached by other Spotfire Servers and nodes.</p> <p>If any of these values do not describe the server, or are on a network that will not be used for back-end communication, you should remove them.</p> <p>If you changed the hostname, domain, or IP address, add the new values.</p> <div>  <p>Valid hostnames may only contain alphabetic characters, numeric characters, hyphen and period.</p> </div> <div>  <p>If you want to change these addresses after setting up your environment, use the set-addresses command.</p> </div>
Site	<p>If you plan to use sites in your implementation you should assign the server to a site now. If you have not yet created the sites, see Creating sites. After creating the sites, click Lookup to select a site for this server. For more information, see Sites.</p>

4. Click **Save Bootstrap**.

The configuration tool checks that database drivers are installed and that the database is running. It also checks that the database accepts the given credentials. A message indicates whether the bootstrap file was successfully created. After it is created, the Configuration page of the configuration tool is displayed.

Setting up the Spotfire Server bootstrap file for Integrated Windows authentication

To configure Integrated Windows authentication (IWA) between Spotfire Server and the Spotfire database in SQL, follow these steps.

Prerequisites

You've followed the steps in [Setting up the Spotfire database \(SQL Server with Integrated Windows authentication\)](#).

Procedure

1. Check that the `sqljdbc4.jar` file with Microsoft's vendor JDBC drivers is in the following Spotfire Server folder: `<installation_dir>\tomcat\lib`.
2. Copy the `sqljdbc_auth.dll` file from the `<installation_dir>\tomcat\bin` folder to the `c:\windows\SysWOW64` folder.
3. Change the login for the service to use the Windows account that has login rights to the Spotfire database.

4. In the [bootstrap](#) command, use the following database connection string, substituting actual values for <db_server>, <port>, and <instance>:

```
jdbc:sqlserver://  
<db_server>:<port>;DatabaseName=<instance>;integratedSecurity=true
```

Saving basic configuration data (authentication towards Spotfire database)

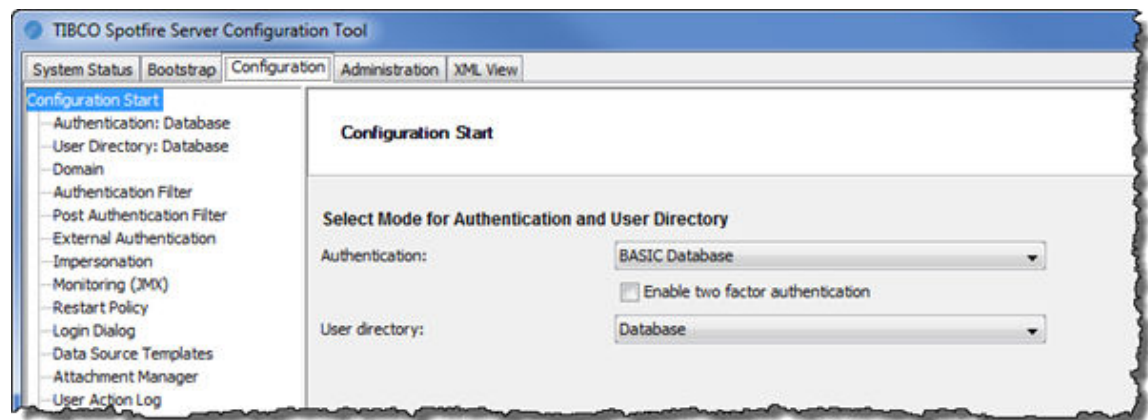
The Configuration page of the configuration tool contains the name of the authentication mode and the user directory for your installation. These instructions are for using the Spotfire database to authenticate users.

Prerequisites

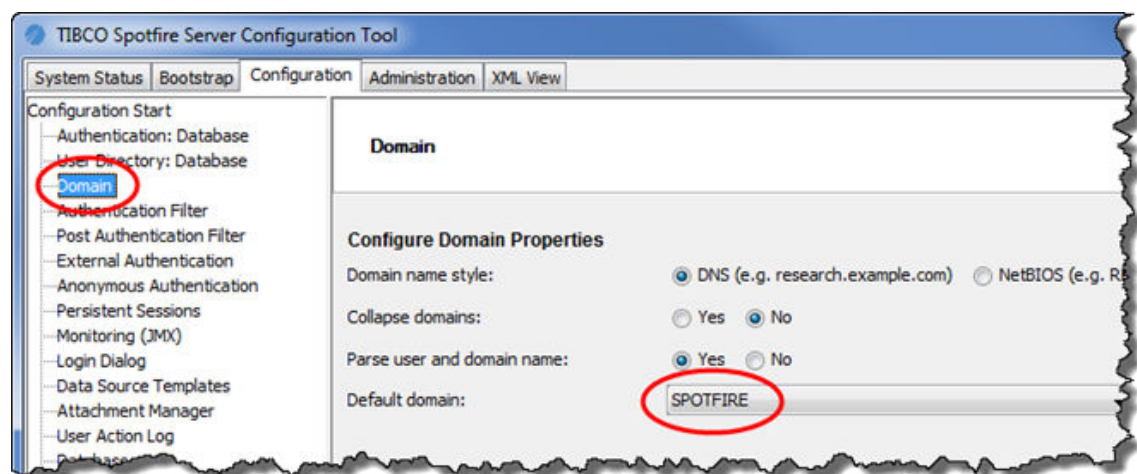
A `bootstrap.xml` file has been successfully saved in the configuration tool (for instructions, see [Creating the bootstrap.xml file](#)).

Procedure

1. On the Configuration page of the configuration tool, verify that **BASIC Database** is selected for **Authentication** and that **Database** is selected for **User directory**.



2. In the left panel of the page click **Domain**, and then verify that **SPOTFIRE** is selected next to **Default domain**.



3. At the bottom of the page, click **Save configuration**.
The Save Configuration wizard is displayed. **Database** is pre-selected as the destination for Spotfire files in the system.
4. Click **Next**.
You are prompted to enter a comment.
5. Enter a comment, and then click **Finish**.

Creating an administrator user

To continue the installation process, the administrator must create an administrator user who has access to all the functionality in the Spotfire implementation.

Prerequisites

Basic configuration data—the authentication mode and user directory for the system—have been saved on the **Configuration** tab of the configuration tool.

Procedure

1. On the Administration page of the configuration tool, under **Create new user**, enter a username and password, and click **Create**.
The new user is displayed in the Users column.
2. Select the new user name and then click **Promote** to add that user to the Administrators group.

What to do next

[Start Spotfire Server](#)

Configuration using the command line

Executing commands on the command line provides greater flexibility and access to options that are not available in the configuration tool. Most administrators use the configuration tool.

The command line can be used in two ways: either by executing commands one-by-one, or by using a script containing several commands that are executed one after the other.

Executing commands on the command line

The command line offers more experienced administrators quick access to a wider variety of options than the configuration tool.

Prerequisites

You must have administrative credentials for Spotfire Server.

Procedure

1. On the computer running Spotfire Server, open a command line as an administrator and change the directory to the location of the `config.bat` file (`config.sh` on Linux). The default location is `<server installation dir>/tomcat/bin`.
This is where you execute commands.

You can also execute commands on a local computer rather than the server computer; for details, see [Executing commands on a local computer](#).
2. Export the active server configuration (the `configuration.xml` file) by using the [export-config](#) command.

Example:

```
config export-config --tool-password=mypassword
```

3. On the command line, enter `config` (`config.sh` on Linux) followed by the command and any required parameters.
4. After you have finished running commands, upload the modified configuration back to the Spotfire database by using the [import-config](#) command. The configuration that you import becomes the active configuration for that server or cluster.

Example:

```
config import-config --tool-password=mypassword --comment=what was changed
```

5. Restart Spotfire Server; for instructions, see [Start or stop Spotfire Server](#).



Because the `configuration.xml` file contains confidential information, you may want to restrict access to it.

Executing commands on a local computer

If it is more convenient, you can execute commands on a local computer rather than on the server computer.

Prerequisites

Follow the steps in [Running the configuration tool on a local computer](#).

Procedure

1. On the local computer, on the System Status page of the configuration tool, create a new bootstrap file.
2. Each time that you run a command on the local computer, specify the location of the bootstrap file by using the `[-b value | --bootstrap-config=value]` option.

Example

To run the command `export-config` on a local computer where the `bootstrap.xml` file was placed on the desktop:

```
config export-config -b=C:\bootstrap.xml
```

Viewing help on configuration commands

You can view information about commands and their parameters from the command line.

Procedure

1. Open a command line and go to the folder that contains the `config.bat` file.



The default location is `<server installation dir>/tomcat/bin`.

2. Type `config help <command name>` and press Enter.

Configuration and administration commands by function

These frequently-used commands are grouped by functional area for easy reviewing.

Command details are available in the [Command-line reference](#). You can also view command details by running the `help` command on the command line (see [Viewing help on configuration commands](#)). The command parameters to use depend on your system setup and environment.

For instructions on using the commands, see [Executing commands on the command line](#).

In general, commands work either towards the server `configuration.xml` file, or work directly on the database. For information about the server configuration files, see [Bootstrap.xml file](#) and [Configuration.xml file](#).

Action log configuration commands

To configure user action logging on the Spotfire Server, use the related command.

All commands in this group work on the `configuration.xml` file, which must be imported using the [import-config](#) command for any changes to take effect.

For instructions on using the commands, see [Executing commands on the command line](#).

Task	Command
Configure the user action database logger.	config-action-log-database-logger
Configure the action log web service.	config-action-log-web-service
Configure the user action logger.	config-action-logger


Administration commands

To perform one of these basic administration tasks, use the related command.

All administration commands connect directly to the Spotfire database and require that the server has been bootstrapped and that an initial configuration has been imported (by using the [import-config](#) command).

For instructions on using the commands, see [Executing commands on the command line](#).

Task	Command
Add a user or group as a member of a specified group.	add-member
Copy group membership from one principal to another.	copy-group-membership
Copy routing rules and schedules from one site to another.	copy-rules-to-site
Create a new user account.	create-user
Delete disabled users.	delete-disabled-users
Delete disconnected groups.	delete-disconnected-groups
Delete a specified OAuth2 client.	delete-oauth2-client
Delete a user account.	delete-user
Revoke full administrator privileges from a user.	demote-admin
Enable or disables a user in the Spotfire database.	enable-user
Export groups from the user directory.	export-groups

Task	Command
Export content from the library.	export-library-content
Export routing rules and schedules from the server.	export-rules
Export users from the user directory.	export-users
Import groups to the user directory.	import-groups
Import content into the library.	import-library-content
Import scheduled updates from Web Player 7.0 and older.	import-scheduled updates
Import users to the user directory.	import-users
Invalidate all persistent sessions.	invalidate-persistent-sessions
List the server administrators.	list-admins
List the deployment areas.	list-deployment-areas
List all groups.	list-groups
List the currently known licenses and license functions.  You must deploy before getting licenses.	list-licenses
List registered OAuth2 clients.	list-oauth2-clients
List all online servers.	list-online-servers
List all users.	list-users
Manage the deployment areas.	manage-deployment-areas
Assign full administrator privileges to a user.	promote-admin
Register a new Automation Services Client Job Sender client.	register-job-sender-client
Remove a license from a group.	remove-license
Set a license and license functions for a group.	set-license
Set a new password for a given user.	set-user-password
Show the current deployment.	show-deployment
Show permissions for a specific directory in the library.	show-library-permissions
Show licenses set on the server.	show-licenses

Task	Command
Show the configuration of a specified OAuth2 client.	show-oauth2-client
Switch the domain names for all users and groups from one style (DNS or NetBIOS) to the other (for all configured domains).	switch-domain-name-style
Update the current deployment.	update-deployment

Authentication commands

To perform an authentication task, use the related command.

These commands are used to configure authentication. All commands in this group work on the `configuration.xml` file, which must be imported using the [import-config](#) command for any changes to take effect.

For instructions on using the commands, see [Executing commands on the command line](#).

Task	Command
Configure the anonymous authentication method.	config-anonymous-auth
Configure authentication and default domain.	config-auth
Configure the authentication filter.	config-auth-filter
Configure the Spotfire database authentication source for use with the BASIC authentication method.	config-basic-database-auth
Configure the LDAP authentication source for use with the basic authentication method.	config-basic-ldap-auth
Configure the Windows NT authentication source for use with the BASIC authentication method.	config-basic-windows-auth
Configure the CLIENT_CERT authentication method.	config-client-cert-auth
Configure custom web authentication.	config-custom-web-auth
Configure the external authentication method.	config-external-auth
Configure the authentication service used with the Kerberos authentication method.	config-kerberos-auth
Configure the authentication service used with the NTLM authentication method.	config-ntlm-auth
Configure authentication using OpenID Connect.	config-oidc
Configure the Persistent Sessions ("remember me") feature.	config-persistent-sessions
Configure the post-authentication filter.	config-post-auth-filter

Task	Command
Configure two-factor authentication.	config-two-factor-auth
Display the current authentication configuration.	list-auth-config
Display the NTLM authentication service configuration.	list-ntlm-auth
Display the current post-authentication filter configuration.	list-post-auth-filter
Show the LDAP authentication source for use with the basic authentication method.	show-basic-ldap-auth

Client configuration command

To configure clients connecting to the Spotfire Server, use this command.

This command works on the `configuration.xml` file, which must be imported using the [import-config](#) command for any changes to take effect.

For instructions on using the commands, see [Executing commands on the command line](#).

Task	Command
Configure the client login dialog behavior.	config-login-dialog

Information Services commands

To perform an Information Services task, use the related command.

All commands in this group work on the `configuration.xml` file, which must be imported using the [import-config](#) command for any changes to take effect.

For instructions on using the commands, see [Executing commands on the command line](#).

Task	Command
Add a new data source template.	add-ds-template
Clear the default join database configuration.	clear-join-db
Configure the default join database.	create-join-db
Export the definition of a data source template.	export-ds-template
List the data source templates.	list-ds-template
Modify a data source template.	modify-ds-template
Remove a data source template.	remove-ds-template
Show the configured default join database.	show-join-database

JAAS commands

To perform a JAAS configuration task, use the related command.

The **test-jaas-config** command connects to the database in a read operation, but all other commands in this group work on the `configuration.xml` file. The `configuration.xml` file must be imported using the [import-config](#) command for any changes to take effect.

For instructions on using the commands, see [Executing commands on the command line](#).

Task	Command
Import new JAAS application configurations into the server configuration.	import-jaas-config
List the JAAS application configurations.	list-jaas-config
Remove the specified JAAS application configurations from the server configuration.	remove-jaas-config
Test a JAAS application configuration.	test-jaas-config

LDAP commands

To manage LDAP configuration for both authentication and the user directory, use the related command.

All commands in this group work on the `configuration.xml` file, which must be imported using the [import-config](#) command for any changes to take effect.

For instructions on using the commands, see [Executing commands on the command line](#).

Task	Command
Configure group synchronization for an LDAP configuration.	config-ldap-group-sync
Create a new LDAP configuration to be used for authentication and/or the user directory LDAP provider.	create-ldap-config
Display LDAP configurations.	list-ldap-config
Remove LDAP configurations.	remove-ldap-config
Update LDAP configurations.	update-ldap-config

Library commands

To configure and administer the Spotfire library, use the related command.

All commands in this group work on the `configuration.xml` file, which must be imported using the [import-config](#) command for any changes to take effect.

For instructions on using the commands, see [Executing commands on the command line](#).

Task	Command
Check for inconsistencies between external storage and Spotfire database.	check-external-library
Configure the library import/export directory.	config-import-export-directory
Configure the external library data storage.	config-library-external-data-storage
Configure the file system storage of library item data.	config-library-external-file-storage
Configure the Amazon S3 storage of library item data.	config-library-external-s3-storage
Copy library permissions from one principal to another.	copy-library-permissions
Delete library content.	delete-library-content
Download the data of library items in Amazon S3 storage.	s3-download
Show the library import/export directory.	show-import-export-directory

Monitoring commands

To configure and administer JMX access to the monitoring component, use the related command.

Except for the **config-jmx** command, which works on the `configuration.xml` file, all monitoring commands connect directly to the database. The configuration must be imported using the [import-config](#) command for any changes to take effect.

For instructions on using the commands, see [Executing commands on the command line](#).

Task	Command
Configure the JMX RMI connector.	config-jmx
Create a new JMX user account.	create-jmx-user
Delete a JMX user.	delete-jmx-user
List all JMX users.	list-jmx-users

Server configuration commands

To perform basic server configuration tasks, use the related command.

Except for the **create-default-config** command, which creates a new `configuration.xml` file, all commands in this group connect directly to the database.

For instructions on using the commands, see [Executing commands on the command line](#).

Task	Command
Create a new server configuration file containing the default configuration.	create-default-config

Task	Command
Export a server configuration from the server database to a file.	export-config
Import a server configuration from a file to the server database.	import-config
List all available server configurations.	list-configs
Set the current server configuration.	set-config
Show the configuration history.	show-config-history

Server database commands

To manage the server database connection pool, use the related command.

The **bootstrap** command creates a new `bootstrap.xml` file and optionally also attempts to connect to the database to test the file. The other commands in this group work on the `configuration.xml` file, which must be imported using the [import-config](#) command for any changes to take effect.

For instructions on using the commands, see [Executing commands on the command line](#).

Task	Command
Bootstrap the server by creating a new bootstrap configuration file.	bootstrap
Configure the encryption of sensitive information such as service account passwords.	config-encryption
Modify the common database connection configuration.	modify-db-config
Set the common database connection configuration.	set-db-config
Update an existing bootstrap configuration file.	update-bootstrap

Services commands

To configure services running on nodes, use the related command.

For instructions on using the commands, see [Executing commands on the command line](#).

Task	Command
Delete a service configuration.	delete-service-config
Export a service configuration.	export-service-config
Import a service configuration.	import-service-config
List active (configured) service configurations.	list-active-service-configs
List available service configurations.	list-service-configs

Task	Command
Set the configuration for a service running in the Spotfire Server (typically the Spotfire Web Player front end).	set-server-service-config
Set the configuration for a service (running on a remote node).	set-service-config

Spotfire collective commands

To manage the Spotfire collective, use the related command.

Most commands in this group connect directly to the database and require that the server has been bootstrapped (by using the [bootstrap](#) command), and that a configuration has been imported using the [import-config](#) command. The **config-cluster** command works on the `configuration.xml` file, which must be imported using the [import-config](#) command for any changes to take effect. Some commands also require a running Spotfire Server to connect to.

For instructions on using the commands, see [Executing commands on the command line](#).

Configure clustering.	config-cluster
Create a new site.	create-site
Delete a specified node.	delete-node
Delete a site.	delete-site
List the addresses of a node.	list-addresses
List the certificates that establish the trust between components within the Spotfire collective.	list-certificates
List logging templates for a specified node.	list-logging
List the nodes in the collective.	list-nodes
List the service instances in the collective.	list-service-instances
List the installed services in the collective.	list-services
List the sites in the collective.	list-sites
Reset the trust within the Spotfire collective.	reset-trust
Set the addresses for a Spotfire Server node.	set-addresses
Set logging for a specified node.	set-logging
Set the site a node should belong to.	set-site
Trust a specified node.	trust-node
Revoke the trust of a specified node.	untrust-node

User directory commands

To configure the user directory, use the related command.

All commands in this group work on the `configuration.xml` file, which must be imported using the [import-config](#) command for any changes to take effect.

For instructions on using the commands, see [Executing commands on the command line](#).

Task	Command
Configure the LDAP user directory.	config-ldap-userdir
Configure the user directory.	config-userdir
Configure the Windows user directory mode.	config-windows-userdir
List the configuration for the user directory LDAP mode.	list-ldap-userdir-config
List the current user directory configuration.	list-userdir-config
List the configuration for the user directory Windows NT mode.	list-windows-userdir-config

Miscellaneous configuration commands

To configure various aspects of the Spotfire Server, use the related command.

All commands in this group work on the `configuration.xml` file, which must be imported using the [import-config](#) command for any changes to take effect.

For instructions on using the commands, see [Executing commands on the command line](#).

Task	Command
Configure the attachment manager.	config-attachment-manager
Configure the CSRF protection.	config-csrf-protection
Configure external scheduled updates for the Spotfire Web Player.	config-external-scheduled-updates
Configure scheduled updates retries.	config-scheduled-updates-retries
Configure the public Web Service API.	config-web-service-api
Set the value of a specific configuration property.	set-config-prop
Configure the public address.	set-public-address

Manually creating a simple configuration

You can configure Spotfire Server by executing a series of commands on the command line.



These instructions are for using the Spotfire database to authenticate users.

Prerequisites

- The Spotfire database has been set up; see [Setting up the Spotfire database \(Oracle\)](#) or [Setting up the Spotfire database \(SQL Server\)](#).
- The Spotfire Server files have been installed; see [Installation](#).

Procedure

1. Run the [bootstrap](#) command to create the connection configuration that Spotfire Server needs for connecting to the database. (For instructions on running commands on the command line, see [Executing commands on the command line](#).)



If you have already run the **bootstrap** command, there is no need to run it again unless you want to use different arguments.

- a) In the following command block, replace the argument values with the appropriate values:

```
> config bootstrap --driver-class="<DRIVER CLASS>"
--database-url="<DATABASE URL>" --username="<DATABASE USERNAME>"
--password="<DATABASE PASSWORD>" --tool-password=
"<CONFIG TOOL PASSWORD>"
```

Argument definitions

--driver-class	The fully qualified class name of the JDBC driver
--database-url	The JDBC connection URL
--username	The name of the database account used by Spotfire Server to connect to the Spotfire database
--password	The password of the database account
--tool-password	Choose a command line password that will be used to protect the server configuration from unauthorized access and/or modification

Example

```
> config bootstrap --driver-class=
"tibcosoftwareinc.jdbc.oracle.OracleDriver"
--database-url="jdbc:tibcosoftwareinc:oracle://MyDBServer:1521;SID=XE"
--username="dbuser" --password="dbpwd" --tool-password="configtoolpwd"
```

A bootstrap.xml file is created in the <installation directory>\tomcat\webapps\spotfire\WEB-INF folder. For more information about this file, see [The bootstrap.xml file](#).

2. Create a default configuration by using the [create-default-config](#) command.
A configuration.xml file is created.
3. Import the configuration to the database by using the [import-config](#) command.
 - a) In the following command block, replace the argument values with the appropriate values:

```
> config import-config --tool-password="<CONFIG TOOL PASSWORD>" --
comment="<DESCRIPTION>"
```

Example

```
> config import-config --tool-password="configtoolpwd" --comment="First config"
```

4. Create a first user by using the [create-user](#) command. This account can be used to log in to Spotfire Server.
 - a) In the following command block, replace the argument values with the appropriate values:

```
> config create-user --tool-password="<CONFIG TOOL PASSWORD>" --username=
"<SPOTFIRE ADMIN USERNAME>" --password="<SPOTFIRE ADMIN PASSWORD>"
```

Example

```
> config create-user --tool-password="configtoolpwd" --
username="SpotfireAdmin" --password="s3cr3t"
```

5. Add the first user to the Administrator group by using the [promote-admin](#) command.

- a) In the following command block, replace the argument values with the appropriate values:

```
> config promote-admin --tool-password="<CONFIG TOOL PASSWORD>" --
username="<SPOTFIRE ADMIN USERNAME>"
```

Example

```
> config promote-admin --tool-password="configtoolpwd" --
username="SpotfireAdmin"
```

When Spotfire Server is running, the first administrator can create other users and add them to the Administrator group.

What to do next

[Start Spotfire Server](#)

[Deploy client packages to Spotfire Server](#)

Scripting a configuration

For more experienced administrators, Spotfire Server includes two prepared configuration scripts that you can use to set up simple configurations. You can also create and run your own scripts.

- The `simple-config.txt` file sets up Spotfire database authentication and the user directory.
- The `simple-config-ldap.txt` file sets up LDAP authentication and the user directory.

These scripts are located in the `<installation_dir>/tomcat/bin` folder.

Example: The simple-config.txt file

The simple-config.txt file, shown below, is divided into three sections:

- The first two lines describe how the script is executed.
- The second section is a list of the variables that are used by the commands.
- The rest of the script contains the commands.

```
# Run this script from the command-line using the following command:
# config run simple-config.txt

# Before using this script you need to set the variables below:
set DB_DRIVER = "tibcosoftwareinc.jdbc.oracle.OracleDriver"
set DB_URL = "jdbc:tibcosoftwareinc:oracle://<server>:<port>;SID=\
<SID>"
#set DB_DRIVER = "tibcosoftwareinc.jdbc.sqlserver.SQLServerDriver"
#set DB_URL = "jdbc:tibcosoftwareinc:sqlserver://
<server>:<port>;DatabaseName=<database name>"
set DB_USER = "<db username>"
set DB_PASSWORD = "<db password>"
set CONFIG_TOOL_PASSWORD = "<config tool password>"
set ADMIN_USER = "<admin username>"
set ADMIN_PASSWORD = "<admin password>"

echo Creating the database connection configuration
bootstrap --no-prompt --driver-class="${DB_DRIVER}" --database-url=\
"${DB_URL}" \
  --username="${DB_USER}" --password="${DB_PASSWORD}" --tool-
password="${CONFIG_TOOL_PASSWORD}"
echo

echo Creating the default configuration
create-default-config
echo

echo Importing the configuration
import-config --tool-password="${CONFIG_TOOL_PASSWORD}" --comment=\
"First config"
echo

echo Creating the '${ADMIN_USER}' user to become administrator
create-user --tool-password="${CONFIG_TOOL_PASSWORD}" --username=\ "${
ADMIN_USER}" --password="${ADMIN_PASSWORD}"
echo

echo Promoting the user '${ADMIN_USER}' to administrator
promote-admin --tool-password="${CONFIG_TOOL_PASSWORD}" --username=\
"${ADMIN_USER}"
echo
```

Editing and running a basic configuration script

To use the simple-config.txt file to set up Spotfire database authentication and user directory, you must modify the script so that it works in your environment.

Prerequisites

- The Spotfire database has been set up; for instructions, see [Setting up the Spotfire database \(Oracle\)](#), [Setting up the Spotfire database \(SQL Server\)](#), or [Setting up the Spotfire database \(SQL Server with Integrated Windows authentication\)](#).
- The Spotfire Server files have been installed; see [Installation](#).

Procedure

1. Open `<installation dir>/tomcat/bin/simple-config.txt` in a text editor and edit the variables:
 - If you use SQL Server, comment out the Oracle variables (“#”) and uncomment the SQL Server variables (remove “#”).
 - For DB_URL, provide the specific values indicated by angle brackets.
 - For DB_USER and DB_PASSWORD, provide the Spotfire database user name and password from the `create_databases.bat` script (described in [Setting up the Spotfire database \(Oracle\)](#) or [Setting up the Spotfire database \(SQL Server\)](#)).
 - For the CONFIG_TOOL_PASSWORD, choose a command line password that will be used to protect the server configuration from unauthorized access and/or modification.
 - For the ADMIN_USER and ADMIN_PASSWORD, first create a user and add it to the Administrators group (see step 4 in [Manually creating a simple configuration](#)), and then provide the use name and password in the script.
2. Save the script. If you do not want to overwrite the existing script, use another name.
3. Open a command line and navigate to `<installation dir>/tomcat/bin`.
4. Type `config run simple-config.txt` and press Enter.
The script executes and creates a basic configuration for Spotfire Server.



The tool is conservative and does not overwrite the `bootstrap.xml` or `configuration.xml` files unless the `--force` flag is used.



it is recommended that you manually remove the `configuration.xml` file when you are done. Do not remove `bootstrap.xml` because it is required to start and run the server.



The `simple-config.txt` file contains sensitive information.

Script language

Spotfire provides a script language that you can use to create a script that runs multiple commands.

# <code>\$</code>	<p>If a hash is the first character on a line, the line is a comment.</p> <p>Example: <code># This is a comment that describes the next section.\$</code></p>
<code>set</code> <code>\$</code>	<p>Defines a variable. The variable name and the value must be separated by an equal character (=).</p> <p>Example: <code>set PASSWORD = "abc123"\$</code></p>
<code>\${Variable}</code> <code>\$</code>	<p>Substitutes the dollar sign and curly braces with the variable value.</p> <p>If there is no matching variable, there is no substitution.</p> <p>Example: <code>--tool-password="\${PASSWORD}"\$</code></p>
<code>\</code> <code>\$</code>	<p>The logical line continues on the next line.</p> <p>Example: <code>bootstrap --no-prompt --driver-class="\${DB_DRIVER}" \ -- database-url="\${DB_URL}" \$</code></p>

<code>echo\$</code>	Writes to console. Example: <code>echo This message will be posted echo\$</code>
<code>\$</code>	Empty rows are allowed\$



Paths and comments that include spaces must be enclosed in straight quotation marks (""). More advanced text editors may change straight quotation marks to smart quotation marks, resulting in errors when the commands are run.

Configuration.xml file

Spotfire Server configurations are stored in the Spotfire database and can be exported to a `configuration.xml` file for editing or sharing.

Certain configuration properties in the Spotfire system are rarely used and cannot be set using commands. To use these properties you must manually edit the `configuration.xml` file. You may also want to work in the configuration file to configure features that require complex commands, such as enabling several authentication options.

The configuration settings can also be exported to file for backup purposes, to be imported into another cluster to set up multiple clusters with similar settings, or to be sent to TIBCO Support for inspection.

You can examine a read-only copy of the `configuration.xml` file on the XML View page of the configuration tool.

If you export the configuration file, make changes, and then import it back to the database, it becomes the active configuration.

Manually editing the Spotfire Server configuration file

Before editing the Spotfire Server configuration file you must export its contents to an XML file.

Procedure

1. On the computer running Spotfire Server, open a command line as an administrator and change the directory to the location of the `config.bat` file (`config.sh` on Linux). The default location is `<installation_dir>/tomcat/bin`.
2. Export the active configuration to a `configuration.xml` file by using the [export-config](#) command. The `configuration.xml` file appears in your working directory.
3. Open `configuration.xml` in an XML editor or a text editor and make your changes.
4. When you've finished, save and close the file.
5. Upload the edited configuration file back to the Spotfire database by using the [import-config](#) command.
6. Restart the Spotfire Server service; for instructions, see [Start or stop Spotfire Server](#).

Result

The imported configuration becomes the active configuration for that server or cluster.

Start or stop Spotfire Server

You must start Spotfire Server after completing initial configuration of the server, before deploying client packages. In addition, you must restart Spotfire Server any time that you change its configuration. The restart causes the server to retrieve a fresh copy of the `configuration.xml` file from the database.

Starting or stopping Spotfire Server (as a Windows service)

After configuring Spotfire Server, you must start it.

Prerequisites

You have successfully completed the initial configuration steps so that the System Status page of the configuration tool shows check marks before the following steps:

- Connect to Database
- Specify Configuration
- Configure Spotfire Server Settings
- Specify Server Administrator

Procedure

1. Log in to the Spotfire Server computer as an administrator.
2. Go to **Control Panel > Administrative Tools > Services** and then, in the Services dialog, locate and select the service called **TIBCO Spotfire Server**.
3. To the left of the services list, click **Start** in the phrase "Start the service".



To stop the service, click **Stop** to the left of the services list.

Result

"Started" appears in the Status column.

What to do next

- Deploy the latest client package to Spotfire Server; for instructions, see [Deploying client packages to Spotfire Server](#).

Starting or stopping Spotfire Server (Windows, no service)

If you did not install a Windows service you must start Spotfire Server manually.

Prerequisites

You have successfully completed the initial configuration steps so that the System Status page of the configuration tool contains four green check marks.

Procedure

1. Log in to the Spotfire Server computer as an administrator.
2. Open a command prompt and go to the following folder: `<installation_dir>/tomcat/bin`.
3. Run the `startup.bat` file.

Result

Spotfire Server starts.



The server will stop running if you close the command prompt or log off from the computer.

Starting or stopping Spotfire Server (Windows, service exists, Integrated Authentication for SQL Server)

If your database server uses Integrated Windows Authentication (IWA) for SQL Server, your Spotfire Server must run as a Windows Domain user that has permission to use the Spotfire database.

Prerequisites

You have successfully completed the initial configuration steps so that the System Status page of the configuration tool contains four green check marks.

Procedure

1. Click **Start > Control Panel > Administrative Tools > Services**.
2. Double-click the service called **TIBCO Spotfire Server**.
The Properties dialog opens.
3. In the Properties dialog, click the **Log On** tab.
4. Select the **This account** radio button and enter the user credentials of the Domain User that was set up with the database preparation script `create_databases_ia.bat`.
5. Click **OK**.
6. Start or stop the service.

Starting or stopping Spotfire Server (Windows, no service, Integrated Authentication for SQL Server)

If your database server uses Integrated Windows Authentication (IWA) for SQL Server, your Spotfire Server must run as a Windows Domain user that has permission to use the Spotfire database.

Prerequisites

You have successfully completed the initial configuration steps so that the System Status page of the configuration tool contains four green check marks.

Procedure

1. Log in to the Spotfire Server computer as the Domain User that was set up with the database preparation script `create_databases_ia.bat`.
2. Open a command prompt and go to the following folder: `<installation_dir>/tomcat/bin`.
3. Run the `startup.bat` file.

Result

Spotfire Server starts.



The server will stop running if you close the command prompt or log off from the computer.

Starting or stopping Spotfire Server (Linux)

On Red Hat and SUSE systems, the Spotfire Server service starts on system startup. Only a user with root user privileges can start and stop the server.

Prerequisites

You have successfully completed the initial configuration steps so that the System Status page of the configuration tool contains four green check marks.

Procedure

1. Log in as root or run with `sudo -s`.
2. Enter the command `/etc/init.d/tss-<version number> start`.



To stop the server, enter the command `/etc/init.d/tss-<version number> stop`.

Clustered server deployments

Large companies often opt for clustered server deployments, where several Spotfire Servers share a database and work together to carry out the server tasks.

Clustered servers provide the following benefits:

- Failover protection if a server goes down.
- Scalability for the growing organization.
- Better performance in a system that handles a high volume of work.

Clustering is *not* enabled by default in Spotfire Server.

Usually a load balancer is added to the deployment to help distribute the workload, but this is not required. A cluster may also contain multiple Spotfire Servers that can be accessed individually through their URLs, but share the same set of node managers. Companies must supply their own load balancer.

There are many configuration options for clustered server deployments; a typical installation features a single load balancer between the Spotfire Servers and the users (on Spotfire Analyst or web client) to optimize the distribution of requests from the clients to the servers.

You can implement clustering using one of the following data grid products:

- Hazelcast (the default) is easy to set up but uses non-secure connections.
- ActiveSpaces requires more configuration but provides secure connections.
- Apache Ignite is easy to set up and provides secure connections.



Apache Ignite is currently only recommended for testing purposes, not for a production environment.

It is generally recommended that you have a working basic installation of a single Spotfire Server before setting up the rest of the cluster; to begin installation, see [Basic installation process for Spotfire](#).

Setting up a cluster of Spotfire Servers

Some deployments that include clustered Spotfire Servers are very complex, and their installation and configuration are best left to a Spotfire consultant. However, if you plan to do it yourself, follow these guidelines.

Prerequisites

- The Spotfire database has been set up on your Oracle or SQL Server database; for instructions, see [Preparation](#).

For general information about Spotfire Server clusters, see [Clustered server deployments](#).

Procedure

1. Install Spotfire Server on each computer; for instructions, see [Installation](#).



For reasons of security and performance, do not install a Spotfire Server on the same computer as the database. (This is true for non-clustered systems as well.)

a) Ensure that all the clustered Spotfire Servers have the same:

- Version number
- Database
- Database drivers
- Encryption password. This is an optional setting on the **Bootstrap** page of the configuration tool.



If you plan to use ActiveSpaces to secure the clustered environment, you must perform the following step on each server computer. If ActiveSpaces is already installed on the server computers, you may want to do it now.

- Copy the file *ActiveSpaces installation dir/lib/as-common.jar* to the following directory: *Spotfire Server installation dir/tomcat/webapps/spotfire/WEB-INF/lib*

2. Apply any available hotfix to each server. For instructions, see [Applying hotfixes to the server](#).
3. Set clustering configuration options in the Spotfire Server configuration. The following steps modify the shared Spotfire Server configuration, so they are only done once.

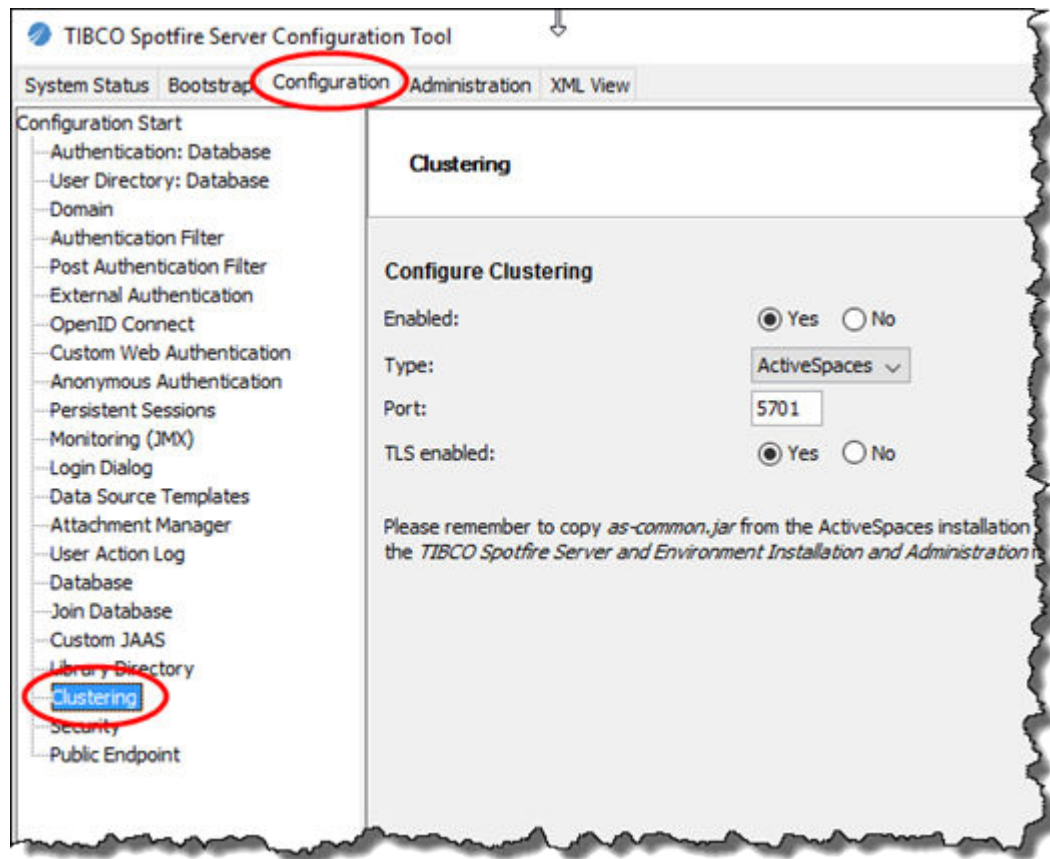


Make sure that none of the servers are running before you change the clustering configuration.




These instructions are for using the configuration tool. Alternatively you can use the [config-cluster](#) command on the command line. For more information, see [Executing commands on the command line](#).

1. If the configuration tool is not open, open it; for instructions see [Opening the configuration tool](#).
2. On the Configuration page, at the bottom of the left pane, click **Clustering**.



3. Under **Configure Clustering**, next to **Enabled**, select **Yes**.
4. Next to **Type**, select **ActiveSpaces** or **Hazelcast**. For information on using ActiveSpaces versus Hazelcast in a clustered implementation, see [Using Hazelcast for clustering](#) and [Using ActiveSpaces for clustering](#).
5. Next to **Port**, enter the TCP/IP port that is used for clustering. This port is the same for all servers in the cluster. (The default is 5701.)

 Make sure that this port is not protected by a firewall.
6. If you selected ActiveSpaces in step d, next to **TLS enabled**, select **Yes**.
7. At the bottom of the page, click **Save configuration**.
4. Start all the servers in the cluster.

Using Hazelcast for clustering

By default, clustered implementations of Spotfire Server use the Hazelcast distributed data grid product to support data clustering.

Hazelcast requires practically no configuration, and in most cases is a sufficient option for clustering.

However, Hazelcast is an unsecure option. To enable data exchange through Hazelcast, a port (by default, 5701) must be open on each Spotfire Server. These ports are not protected by any TLS; Hazelcast uses plain TCP/IP connections for the data exchange between servers.



If you do implement clustering with Hazelcast, the firewalls should be configured for maximum security and, ideally, the ports should be open only to other Spotfire Server instances.



If you have multiple network interfaces on your Spotfire Servers, you may need to configure Hazelcast to Bind to Any Network Interface. To do this, open a command line and export the active server configuration by using the [export-config](#) command. Then run the following command:

```
config set-config-prop --name=clustering.hazelcast.bind-on-any-interface --value=true
```

Then import the configuration back to the Spotfire database by using the [import-config](#) command, and restart the Spotfire Servers sequentially. For additional information on executing commands, see [Executing commands on the command line](#).

If your implementation requires secure connections between the servers in a cluster, you can install TIBCO ActiveSpaces® and configure Spotfire Server to use it for secure TCP/TLS transport. For details, see [Using ActiveSpaces for clustering](#).

For general information about Spotfire Server clusters, see [Clustered server deployments](#).

Using ActiveSpaces for clustering

To enable secure TCP/TLS transport for the exchange of data between clustered Spotfire Servers, install ActiveSpaces and configure the servers to use it as the underlying data grid.

ActiveSpaces is a separate product that must be deployed and configured separately. It is available free-of-charge to purchasers of Spotfire Server.



These instructions are for the baseline scenario of securing TCP/IP transport using TLS certificates/keys, without additional encryption of transmitted data. ActiveSpaces provides various means for securing the cluster; for information on additional options, see the ActiveSpaces documentation.

For general information about Spotfire Server clusters, see [Clustered server deployments](#).

Installing ActiveSpaces

To use ActiveSpaces to secure the connections between clustered servers, ActiveSpaces 2.2.1 must be installed and configured on each Spotfire Server in the cluster. (ActiveSpaces is a separate product that is available free-of-charge to purchasers of Spotfire Server.) After installation, you reconfigure the servers to use ActiveSpaces as the underlying data grid.

For general information about Spotfire Server clusters, see [Clustered server deployments](#).

Procedure

1. On the [TIBCO eDelivery web site](#), go to the TIBCO Spotfire Server page.
2. At the bottom of the page, click **Download** and then sign in to the site, if required.
3. On the server download page, select the latest version and your platform, and select the license agreement check box.
4. Under **Installation Method** in the center of the page, click **Individual file download**.
5. Under **SELECT AN INDIVIDUAL COMPONENT**, expand **TIBCO ActiveSpaces Enterprise Edition Software** and then click either `TIB_activespaces_2.2.1_win_x86_64.zip` (for Windows) or `TIB_activespaces_2.2.1.md5` (for Linux).



The following steps pertain to a Windows installation.

6. After the zipped folder is downloaded, extract the files.
7. Double-click the ActiveSpaces installer to install the product.
8. Copy the file `<ActiveSpaces installation dir>\lib\as-common.jar` to the following directory: `<server installation dir>\tomcat\webapps\spotfire\WEB-INF\lib`.
9. Restart the computer.

10. Repeat these steps for each server computer in the cluster.

What to do next

[Configuring a server cluster with ActiveSpaces \(Windows\)](#)

[Configuring a server cluster with ActiveSpaces \(Linux\)](#)

Configuring a server cluster with ActiveSpaces (Windows)

After installing ActiveSpaces, you must make two changes to the Windows environment variables of each server computer to complete the basic cluster configuration.

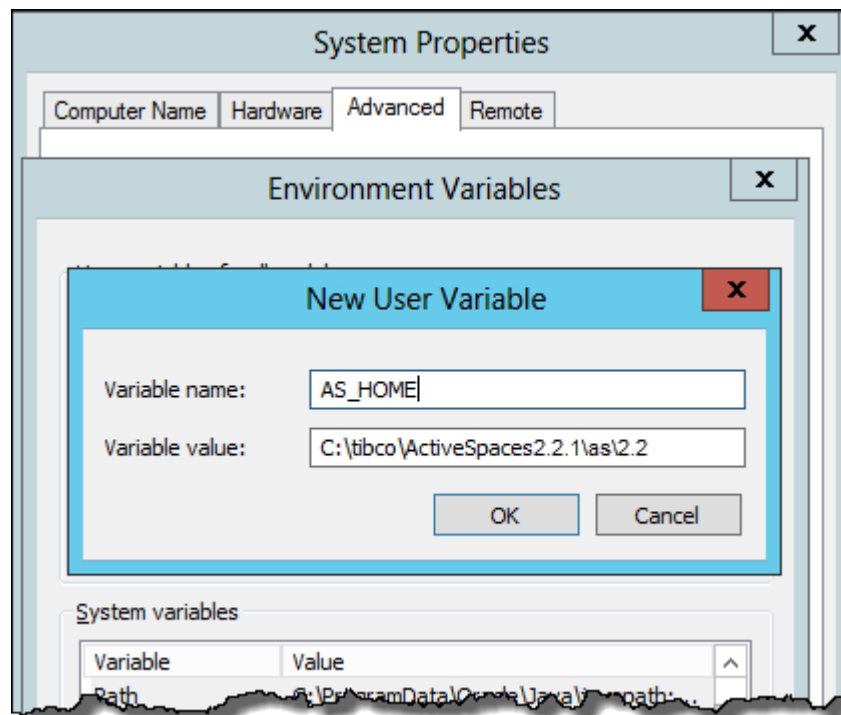
Prerequisites

- You have installed and configured the Spotfire Servers for the cluster as described in [Setting up a cluster of Spotfire Servers](#).
- ActiveSpaces 2.2.1 is installed on each server computer in the cluster; for details, see [Installing ActiveSpaces](#).

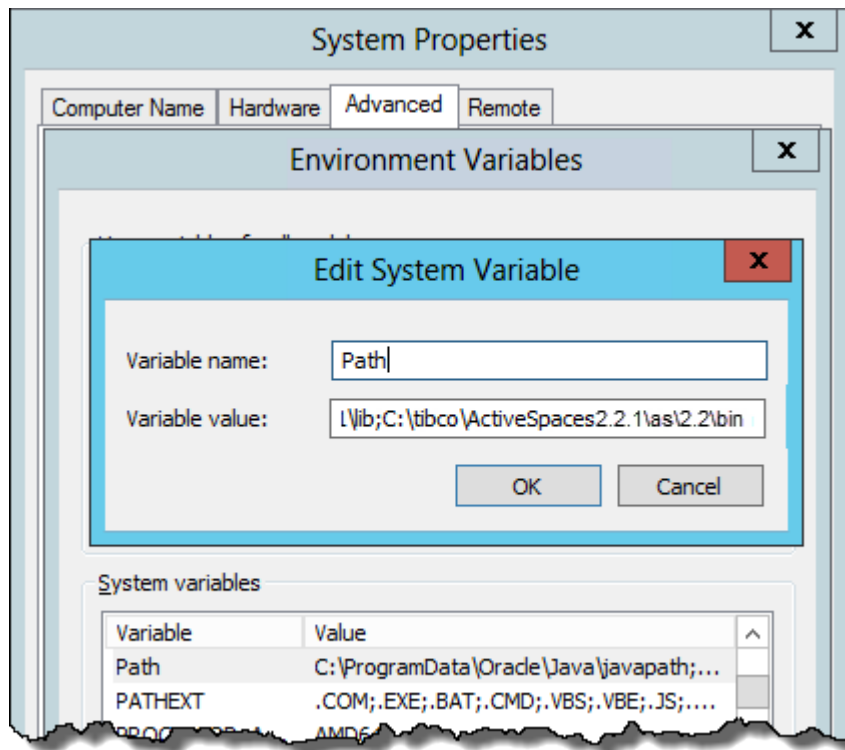
For general information about Spotfire Server clusters, see [Clustered server deployments](#).

Procedure

1. On the Spotfire Server computer, open the Environment Variables dialog.
2. In the "User variables" pane, define AS_HOME as shown in the following example:



3. In the "System variables" pane, add entries to the PATH for the lib folder and the bin folder, as shown in the following example:



4. If you have not done this yet, copy the file `<ActiveSpaces installation dir>\lib\as-common.jar` to the following directory: `<Spotfire Server installation dir>\tomcat\webapps\spotfire\WEB-INF\lib`.
5. Restart the computer.
6. Repeat steps 1-5 for each server computer in the cluster.

What to do next

[Enable secure transport for ActiveSpaces](#)

Configuring a server cluster with ActiveSpaces (Linux)

After setting up the cluster and installing ActiveSpaces, you must do additional configuration if you have a Linux installation. Then ActiveSpaces must be validated on each server computer in the cluster.

Prerequisites

- You have installed and configured the Spotfire Servers for the cluster as described in [Setting up a cluster of Spotfire Servers](#).
- ActiveSpaces 2.2.1 is installed on each server computer in the cluster; for details, see [Installing ActiveSpaces](#).

Procedure

1. On one of the server computers, set the `LD_LIBRARY_PATH` variable to use the ActiveSpaces library by doing one of the following:
 - (Recommended) To permanently set the variable for this computer, follow these steps:
 1. Navigate to the `etc` directory.

2. Open the profile file by entering the following command: `vi profile`
3. Append the following lines to the end of the profile file:

```
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/local/bin/tibco/as/2.2/lib
export AS_HOME=/usr/local/bin/tibco/as/2.2
export PATH=${PATH}:${AS_HOME}/bin:${AS_HOME}/lib
```

where `.../tibco/as/2.2/lib` specifies the path to ActiveSpaces.

4. Save the file and restart the session.

- To set the variable for only the current session, enter the following command:

```
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/local/bin/tibco/as/2.2/lib
```

where `.../tibco/as/2.2/lib` specifies the ActiveSpaces installation directory.



In this case the variable must be reset each time that someone logs in to Spotfire Server on any computer in the cluster, including the current computer.

2. If you have not done this yet, copy the file `<ActiveSpaces install dir>\lib\as-common.jar` to the following directory: `<Spotfire Server install dir>\tomcat\webapps\spotfire\WEB-INF\lib`.
3. Start the Spotfire Server.
4. Repeat steps 1-3 on each server computer.
5. Create the default cluster in ActiveSpaces by using the ActiveSpaces command-line interface (CLI).



The ActiveSpaces CLI should be launched only after all the Spotfire Servers in the cluster are initialized.

1. Open a command window and then open the ActiveSpaces CLI by entering the following commands:

```
cd <ActiveSpaces install dir>\as\2.2\bin
as-admin
```

2. In the ActiveSpaces CLI, create the default cluster in ActiveSpaces as shown in the following example.



The discovery parameter should point to one of the Spotfire Servers in the cluster. Make sure that the clustering port matches the port that you defined in the clustering configuration.

```
as-admin> connect name "spotfire" discovery "tcp://10.90.48.16:5701"
[2015-07-10T15:47:15.428][11524][10356][INFO][transport]
  ip_address=10.98.48.27 port=50000
[2015-07-10T15:47:25.455][11524][10356][INFO][spotfire.metaspaces]
  Connected metaspaces name=[spotfire], listen=[tcp://
10.90.48.16:50000],
  discovery=[tcp://10.98.
48.27:5701], member name=[a62301b-c350] version=2.1.4.011
[2015-07-10T15:47:25.455][11524][8508][INFO][spotfireConnected to
  metaspaces spotfireias-admin> re.$members] member joined:
  member.mydomain.com (a62301b-1645-559fbd18-31d, 10.98.48.16:5701)
[2015-07-10T15:47:25.455][11524][8508][INFO][spotfire.$members]
  member joined: a62301b-c350 (a62301b-c350-559fbed3-1ad,
10.90.48.16:50000)
```



The default (immutable) ActiveSpaces metaspaces name is "spotfire".



For information on the connect command, see the [ActiveSpaces documentation](#).

3. Repeat these steps for each server in the cluster.
6. For verification, list all members of the cluster, as shown in the following example:

```
as-admin> show members
Show Members for Metaspaces 'spotfire' :
```

Cluster Members:

Member Name	IP:Port	Member Role	Member ID
member.mydomain.com	10.90.48.16:5701	manager	a62301b-1645-559fbd18-31d a62301b-c350
10.90.48.16:50000	member	a62301b-c350-559fbed3-1ad	

 member.mydomain.com | 10.90.48.16:5701 | manager | a62301b-1645-559fbd18-31d |
 a62301b-c350 | 10.90.48.16:50000 | member | a62301b-c350-559fbed3-1ad |
 Total Cluster Members: 2



The total number of cluster members should equal the number of running Spotfire Servers plus one (the administration console also joins the cluster as a member).

What to do next

[Enable secure transport for ActiveSpaces](#)

Enabling secure transport for ActiveSpaces

After configuring the Spotfire Servers in the cluster, you must enable ActiveSpaces to use secure transport for communication between the servers.

Prerequisites

You have configured each Spotfire Server in the cluster to use ActiveSpaces; see [Configuring a server cluster with ActiveSpaces \(Windows\)](#) or [Configuring a server cluster with ActiveSpaces \(Linux\)](#).

For additional information on this procedure, see the [ActiveSpaces documentation](#).

For general information about Spotfire Server clusters, see [Clustered server deployments](#).



Steps 1 - 3 are performed on only one server in the cluster.

Procedure

1. On one of the servers in the cluster, open a command window and then open the ActiveSpaces command-line interface (CLI) by entering the following commands:

```
cd ActiveSpaces installation dir/as/2.2/bin
```

```
as-admin
```

2. In the ActiveSpaces CLI, enter the following command:

```
as-admin> create security_policy policy_name "as-policy" policy_file  
"as-policy.txt" encrypt false
```



Do not change the policy name or the policy file name because they are referenced in the Spotfire Server configuration and are immutable.

3. Edit the policy file that you created in the previous step:
 - a) Under the "discovery" attribute of the metaspace_access policy key, list all the members of the cluster.
 - b) Change the metaspace name.
The edited section of the policy file will look similar to this:


```
metaspace_access=metaspace=spotfire;discovery=tcp:  
//10.97.184.60:5701;10.97.184.65:5701
```
 - c) To use traditional, TLS-like transport protection, specify transport_security=integrity. For information on additional options, see the [ActiveSpaces documentation](#).
4. Copy this generated as-policy.txt file to each of the clustered Spotfire Servers, to the folder where the keystore file is located. Typically, the keystore file is located here: <server installation dir>/nm/trust.
5. Start all of the servers.

6. To validate ActiveSpaces, execute the following commands in the ActiveSpaces CLI.

1. Create a security token by entering the following command:

```
as-admin> create security_token domain_name "AS-DOMAIN" policy_file "C:/tibco/tss/version/nm/trust/as-policy.txt" token_file "C:/tibco/tss/version/nm/trust/mytoken.txt"
```

2. Connect to the metaspace with the security token by entering the following command, where the discovery parameter points to one of the Spotfire Servers in the cluster:

```
as-admin> connect security_token "C:/tibco/tss/version/nm/trust/mytoken.txt" name "spotfire" discovery "tcp://10.97.120.65:5701"
```

7. To list the members of the cluster, enter the following command:

```
as-admin> show members
```

Using Apache Ignite for clustering

Apache Ignite clustering requires no manual configuration.



Apache Ignite is currently only recommended for testing purposes, not for a production environment.

Ignite provides TLS version 1.2 for communication, which makes it as secure as ActiveSpaces, and it is faster than the other clustering solutions. In addition, it looks for specific nodes by using their IP address, rather than discovering any node that communicates using multicasting.

By default, Ignite uses these two ports:

- 5701 (this base value is configurable)
- 5702 (base value + 1)

You can change the default clustering ports when you configure the cluster, either in the configuration tool or by using the **config-cluster** command. For details, see [Setting up a cluster of Spotfire Servers](#) or [config-cluster](#).

Configuring NTLM for a cluster of Spotfire Servers

To configure NTLM for clustered servers, first set the options common to all the servers and then set the server-specific options.

For general information about Spotfire Server clusters, see [Clustered server deployments](#).

Procedure

1. Configure the options common to all servers in the cluster. This is performed according to the instructions in [Configuring NTLM authentication for a single server](#), with the following modifications:

- Specify the **DNS domain name** (recommended) or a **domain controller** (not recommended), and possibly also an **AD site name**.



Do not specify the **server**, **account name**, or **password** options at this point.

2. Run the **config-ntlm-auth** command to add the account information for each Spotfire Server in the cluster:

- Run the command once for each server in the cluster.
- Enter the **server**, **account name**, and **password** options. The server option must reflect the server name as defined in the server's `bootstrap.xml` file.

Enabling health check URL for load balanced servers

When using a load balancer in front of a cluster of Spotfire Servers, a health check URL can be set up to show the status of the servers.

For general information about Spotfire Server clusters, see [Clustered server deployments](#).

Procedure

1. Open a command-line interface and export the active configuration by using the [export-config](#) command. (For details on using the Spotfire command line, see [Executing commands on the command line](#).)
2. On the command line, enter the following command:

```
config set-config-prop --name=status-controller.enabled --value=true
```

For information about the command options, see [set-config-prop](#).
3. Import the configuration file back to the Spotfire database by using the [import-config](#) command.
4. Restart the Spotfire Servers in the cluster.

Result

You can now use the URL `/spotfire/rest/status/getStatus` to check the status of the servers in your cluster.

- If the health check URL hasn't been enabled, the HTTP code 404 is returned.
- If the server is up and running, the HTTP code 200 is returned along with the text RUNNING.
- If the server is currently starting or stopping, the HTTP code 503 is returned along with the text STARTING or STOPPING.

Kerberos authentication for clustered servers with load balancer

In a clustered environment where Kerberos authentication is used to authenticate users, the load balancer forwards all Kerberos authentication information to the Spotfire Servers. No configuration on the load balancer is needed, but there are certain considerations to take into account when Kerberos authentication is set up.

These are the special considerations:

- Two Service Principal Names must be created for each Spotfire Server as well as for the load balancer.
- One keytab file must be created. This must use the fully qualified Service Principal Name of the load balancer.
- This keytab file must be copied to each Spotfire Server.
- When Kerberos authentication is set up, the fully qualified Service Principal Name of the load balancer must be provided.

For general information about Spotfire Server clusters, see [Clustered server deployments](#).

X.509 client certificates for clustered servers with load balancer

When using X.509 client certificate authentication in a clustered environment, the clients see the load balancer as the server. The load balancer must therefore be provided and configured with a server certificate and its private key.

The load balancer also needs to be provided and configured with the CA certificate that was used to issue the server certificate.

For general information about Spotfire Server clusters, see [Clustered server deployments](#).

Configuring shared import and export folders for clustered deployments

From the Library Administration tool in Spotfire Analyst, you can import and export library content. The import and export files are stored in a folder specified in the Spotfire Server configuration. In a clustered environment, where the client could be communicating with any of the servers, steps must be taken to ensure that the import and export files are always stored in the same folder.

For general information about Spotfire Server clusters, see [Clustered server deployments](#).

Procedure

- Using Windows shared folder technology, set the location of the import and export folder to a folder that is shared with all the Spotfire Servers in the cluster.

Deploying client packages to Spotfire Server

To install and use the Spotfire Analyst client and Spotfire web client, you must first deploy the following distribution file (.sdn file) to Spotfire Server: `Spotfire.Dxp.sdn`.

For more information about deployments, see [Deployments and deployment areas](#).

Prerequisites

- A Spotfire Server administrator has been created. For instructions, see [Creating an administrator user](#).
- You downloaded the `Spotfire.Dxp.sdn` file from the TIBCO eDelivery site. For details, see [Downloading required software](#).

Procedure

1. Log in to Spotfire Server by going to `http://servername:port/spotfire`, where *port* is the server front-end port (specified in step 7 of [Installing the Spotfire Server files \(interactively on Windows\)](#)).
2. Click **Deployments & Packages**.
3. On the Deployments & Packages page, under **Deployment areas**, select the area you are currently using.
4. In the "Software packages" pane, click **Add packages**.
5. In the "Add packages" dialog, click **Choose File**.
6. Browse to and then double-click the `Spotfire.Dxp.sdn` file.
7. In the "Add packages" dialog, click **Upload**.
After the packages are uploaded to the server (this may take a while), the new software packages are displayed in the "Software packages" pane.
8. At the top of the "Software packages" pane, click **Validate** to check the deployment, and then click **Save**.
9. In the "Save deployment" dialog that opens, verify or edit the details and then click **Save**.

What to do next

[Node manager installation](#)

User authentication

Spotfire supports a variety of user authentication protocols for verifying the identities of users logging in to the program.

To configure authentication, you select both an *authentication method* and a *user directory*.

Spotfire supports the two main types of authentication—user name and password, and single sign-on—as well as two-factor and external methods.

User name and password authentication methods

When users start a Spotfire Analyst client, they select which Spotfire Server to connect to. If that server is configured for a user name and password based authentication method, the users are also prompted for their user name and password.

The user name and password are then sent to Spotfire Server.

The login experience for the Spotfire Analyst client can be customized in several ways, including whether users have the option to save their login information, and whether the dialog contains an RSS feed. For details, see [Login behavior configuration](#).



The credentials that users enter are not encrypted when they are transferred to Spotfire Server unless the server uses TLS. To help counter the risks associated with unencrypted data, enable TLS when configuring a user name and password authentication method.

For all the user name and password methods, an entry for each user is created in the Spotfire database.

- If you configure authentication towards an external user directory such as an LDAP directory, the user list or group hierarchies from the external directory are automatically copied to the Spotfire database.
- If you configure authentication towards the Spotfire database, the user and group information must be manually entered.
- It is possible to combine authentication towards an external user directory with users added manually to the Spotfire database.

Authentication towards the Spotfire database

This authentication method requires that the Spotfire user directory be configured for Spotfire database.

When the user directory is set to **Database**, the administrator usually enters the user names and passwords into the Spotfire database manually. The names and passwords can also be imported from a CSV file, or automatically created as new users log in to the server. The option to automatically create users is available through the *post-authentication filter*.

Authentication towards the Spotfire database is the default configuration for Spotfire Server, so no special configuration is required. It is easy and fast to set up and it is recommended for small implementations.

Authentication towards LDAP

This authentication method integrates with an existing LDAP directory and delegates the actual authentication responsibility to its configured LDAP servers.

The result is that only users with valid accounts in the LDAP directory can log in to Spotfire Server. This setup is recommended for larger implementations.

Spotfire Server supports the following LDAP servers:

- Microsoft Active Directory
- The Directory Server product family (Oracle Directory Server, Sun Java System Directory Server, Sun ONE Directory Server, iPlanet Directory Server, Netscape Directory Server)



Other types of LDAP servers may also work with Spotfire Server, but require more advanced configuration.



When Spotfire Server is authenticating towards a Microsoft Active Directory server, it automatically uses the Fast Bind Control (also known as Concurrent Bind Control) option to minimize the consumed resources on the LDAP server.

LDAP authentication can be combined with either the LDAP user directory or the Spotfire database user directory:

- When the user directory is set to **LDAP**, Spotfire Server can automatically import the user names from the LDAP directory. Passwords remain in the external directory, and Spotfire Server contacts this directory to validate users' passwords. You can set the frequency with which Spotfire Server checks the LDAP directory for updates.



When the user directory mode is set to **LDAP**, Spotfire Server also imports the group names and group membership information. For information on groups, see [Users & groups introduction](#) and [Group administration](#).

- When the user directory mode is set to **Database**, the administrator usually enters the valid user names and passwords into the Spotfire database manually. The names and passwords can also be imported from a CSV file, or be automatically created as new users log in to the server. The option to automatically create users as they log in is available through the [post-authentication filter](#).

Configuring LDAP

When user authentication is configured towards an LDAP directory, Spotfire Server delegates authentication responsibility to the configured LDAP servers. Therefore only users with valid accounts in the LDAP directory can log in to Spotfire Server.

For information about supported LDAP servers and what you need to know about your organization's server, see [Authentication towards LDAP](#).



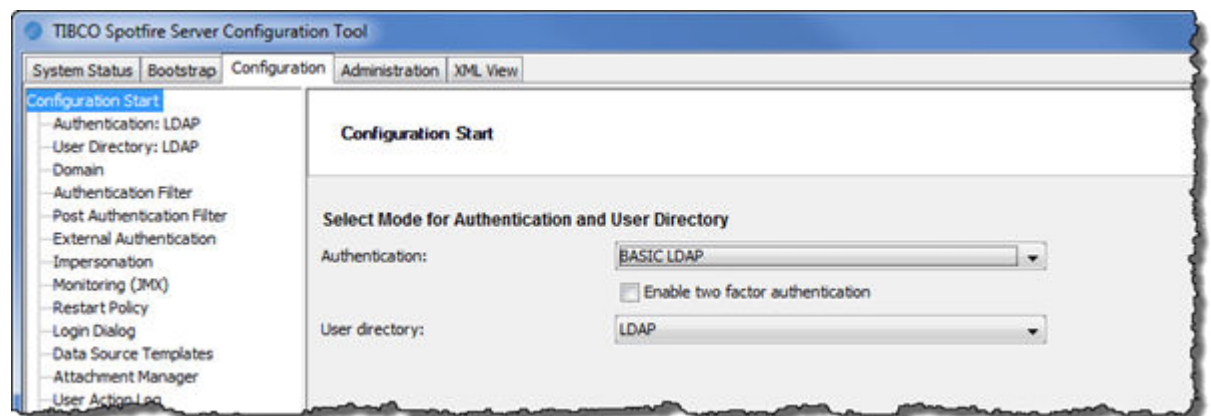
For information about other LDAP implementations, including Kerberos, NTLM, X.509 client certificates, and external authentication, see [User authentication](#).

Prerequisites

- Your organization stores user information in an LDAP directory.
- A `bootstrap.xml` file has been successfully saved in the configuration tool; for instructions, see [Creating the bootstrap.xml File](#).

Procedure

- On the Configuration page of the configuration tool, next to **Authentication**, select **BASIC LDAP**.

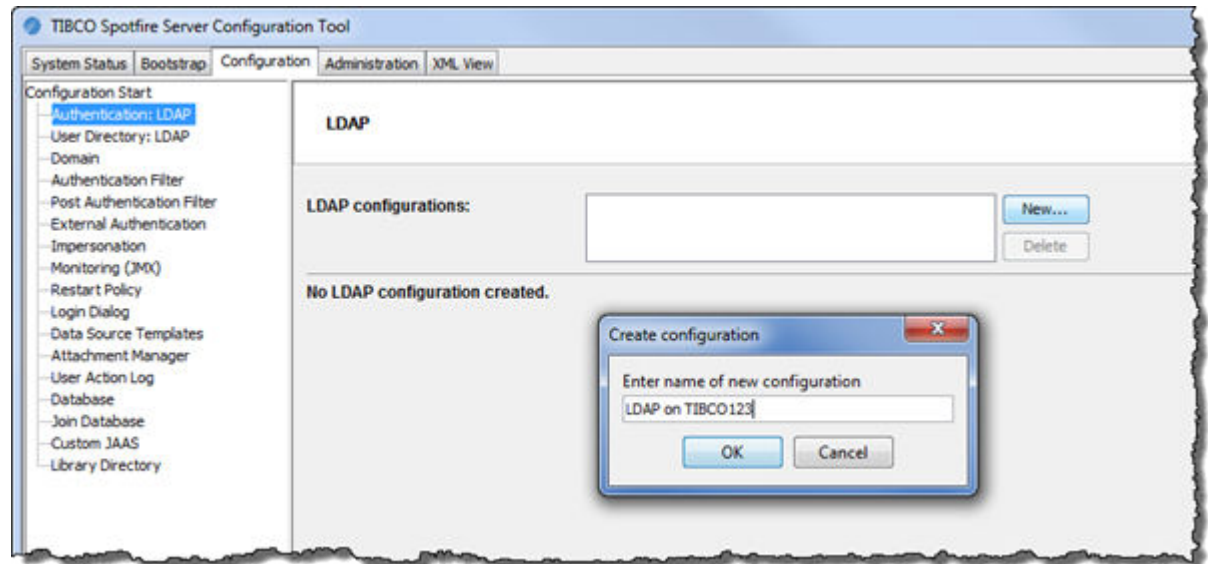


The **User directory** field switches to **LDAP** along with the **Authentication** field. This is because in most cases it is recommended that LDAP authentication be paired with the user directory in LDAP mode.

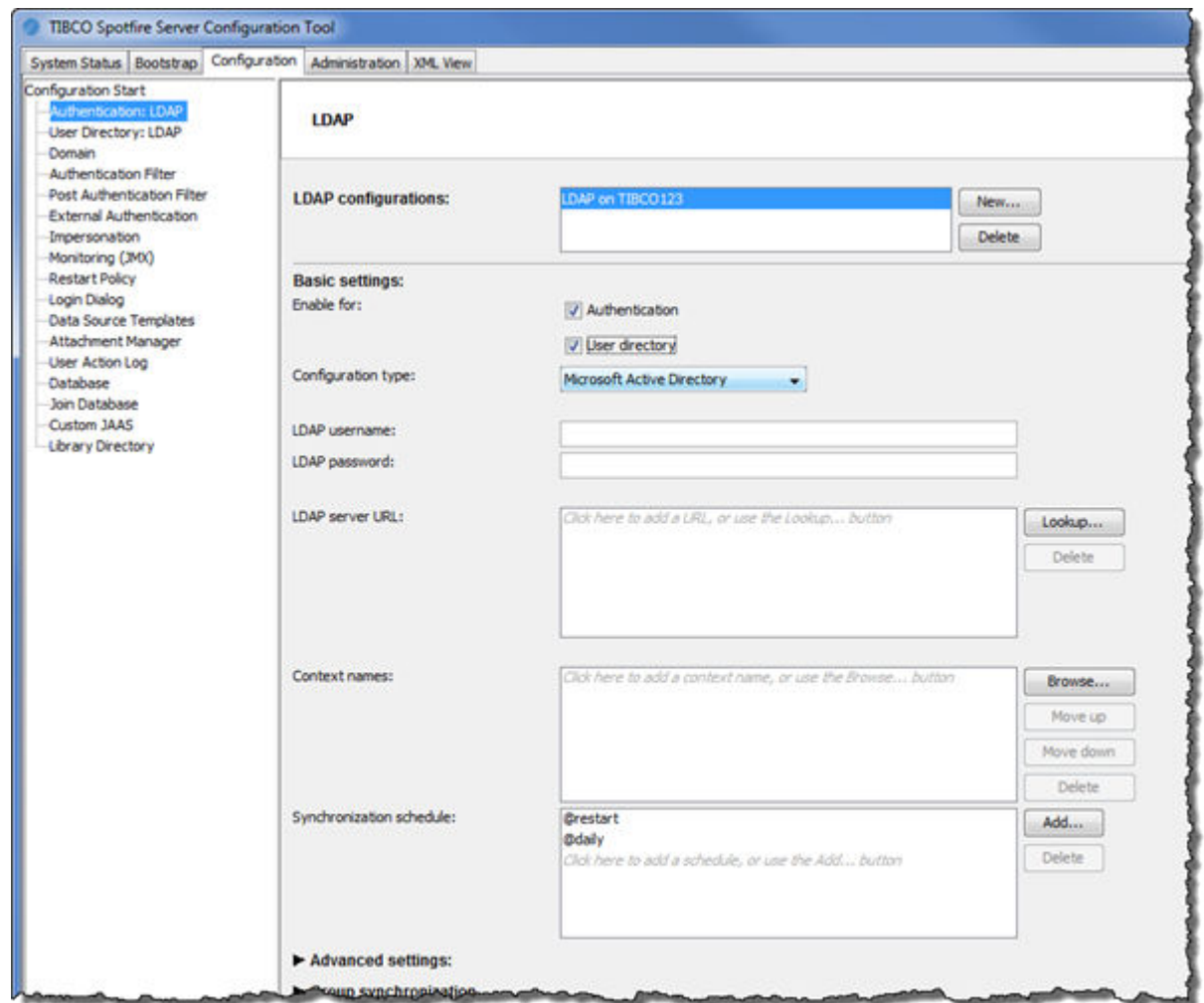


If your LDAP directory contains a very large number of users that are not divided into convenient sub-units (contexts), you may want to use the Spotfire database user directory instead. In this configuration, only users who log in to Spotfire Server are included in the user directory, so there are fewer users for Spotfire Server to track.

2. In the left panel of the page, click **Authentication: LDAP**, and then click **New**.



3. In the Create configuration dialog, enter a name for your LDAP configuration, for example "LDAP on TIBCO123", and then click **OK**.
The LDAP configuration page is displayed.



4. Next to **Enable for**, select both the **Authentication** and **User directory** check boxes. This instructs Spotfire Server to create a user account in the Spotfire database for each user (within the configured scope) in the LDAP directory. When someone tries to log in to the Spotfire system, Spotfire Server accesses their account and then validates their password through the LDAP directory.
5. Next to **LDAP username** and **LDAP password**, enter the user name and password of an LDAP service account with read access to Active Directory.
6. Next to **LDAP server URL**, enter the URL in the form LDAP://server/:port, for example LDAP://computer1.TIBCO.com:389
7. Next to **Context names**, enter the contexts you want to synchronize.
8. Next to **Synchronization schedule** you can change the scheduled synchronization times between the LDAP directory and the Spotfire database. The default is to synchronize whenever Spotfire Server is restarted, in addition to daily. For additional synchronization options, click **Add**.
9. Click **Test connection** to verify your entries.
10. If you set the user directory to **Database** in step 1 above, click **Post Authentication Filter** in the left panel and then, next to **Default filter mode**, select **Auto-create**.
When users log in to Spotfire Server they are added to the Spotfire user directory.
11. When you're finished, click **Save configuration**.

Configuring LDAPS

In an LDAP environment, where the Spotfire system communicates with an LDAP directory server, administrators often secure the LDAP protocol using TLS, if the LDAP directory supports this.

Prerequisites

- The LDAP directory server has been set up to communicate using TLS.

Procedure

1. If you are using a self-signed certificate, set Spotfire Server to trust this certificate:
 - a) Export the certificate to file and copy it to Spotfire Server.
 - b) Open a command-line interface, navigate to the <installation_dir>/jdk/jre/lib/security directory, and run the following keytool command: `../../../../bin/keytool -import -file ldapserver.crt -keystore cacerts -alias spotfire_ldaps`. Replace `ldapserver.crt` with the name of the exported certificate.
 - c) When prompted, enter the password to the `cacerts` keystore. The default password is "changeit" (without quotation marks).
 - d) Verify that the certificate has been successfully added by using the following command: `../../../../bin/keytool -list -keystore cacerts -alias spotfire_ldaps`.
 - e) When prompted, enter the password to the `cacerts` keystore.
2. To activate LDAPS, use the [create-ldap-config](#) or the [update-ldap-config](#) command.

SASL authentication for LDAP

Spotfire Server supports two SASL (Simple Authentication Socket Layer) mechanisms for authentication towards LDAP: DIGEST-MD5 and GSSAPI.

These mechanisms can provide secure authentication of Spotfire Server when it is connecting to LDAP servers by preventing clear text passwords from being transmitted over the network.

GSSAPI can provide secure authentication even over un-secure networks because it uses the Kerberos protocol for authentication.

These instructions apply for Active Directory LDAP configurations. Spotfire Server does not support GSSAPI for other LDAP configurations.

Configuring Spotfire Server for DIGEST-MD5 authentication of LDAP

These instructions apply for Active Directory LDAP configurations. Spotfire Server does not support GSSAPI for other LDAP configurations.

Procedure

- When configuring SASL authentication with DIGEST-MD5, follow these guidelines:
 - The distinguished name (DN) does not work for authentication; the `userPrincipalName` attribute must be used instead.
 - Set the **authentication attribute** option to **userPrincipalName**.
 - Set the **username attribute** option to **sAMAccountName**.
 - All accounts must use reversible encryption for their passwords. This is typically not the default setting for Active Directory.

Configuring Spotfire Server for GSSAPI authentication of LDAP

These instructions apply for Active Directory LDAP configurations. Spotfire Server does not support GSSAPI for other LDAP configurations.

Prerequisites

- Make sure that you have a fully working Active Directory LDAP configuration using clear-text password authentication (also known as simple authentication mechanism).
- Save this fully working Active Directory LDAP configuration to file.
- Make a note of the LDAP configuration's ID.
- Make sure that you have a fully working `krb5.conf` file. The content of the `krb5.conf` file must be the same as when setting up Spotfire Server for Kerberos authentication. See [Configuring Kerberos for Java](#).



Make sure to stop the entire service/Java process before installing the file. If the `krb5.conf` file is modified after Spotfire Server has been started, you must restart the Spotfire Server process for the modifications to take effect.

Procedure

1. Stop Spotfire Server (see [Start or stop Spotfire Server](#)).
2. Copy the fully working `krb5.conf` file to the `<install_dir>/jdk/jre/lib/security` directory on each Spotfire Server in the cluster.
3. Open the configuration tool and go to the LDAP Configuration panel.
4. Update the LDAP user name so that it is a proper Kerberos principal name. Usually it is sufficient to add the name of the account's Windows domain in upper-case letters. Sometimes it is also necessary to include the Windows domain name. Using a name based on a distinguished name (DN) or including a NetBIOS domain name does not work when using GSSAPI.
Examples of correct names:

- `ldapsvc@RESEARCH.EXAMPLE.COM`
- `ldapsvc@research.example.com@RESEARCH.EXAMPLE.COM`

5. Select the specific LDAP configuration to be enabled for GSSAPI and then expand the **Advanced** settings.
6. In the **Advanced** dialog, make the following changes:
 - a) Set the **security-authentication** configuration property to **GSSAPI**.
 - b) Set the **authentication-attribute** to **sAMAccountName** or **userPrincipalName** (whichever works best for your configuration). The default value is empty.



If the `krb5.conf` file contains more than one Kerberos realm, the authentication-attribute must be set to **userPrincipalName**.

- c) Add a custom property with the key `kerberos.login.context.name` and the value **SpotfireGSSAPI**.
7. Click **Save configuration**.
 8. Restart Spotfire Server.

What to do next

Procedure steps related to LDAP configurations must be performed for each LDAP catalogue that you want to enable for GSSAPI. For multiple LDAP configurations, repeat these steps for each configuration.

Authentication towards Windows NT Domain (legacy)

With this authentication method, user authentication is delegated to Windows NT domain controllers.

Spotfire Server must be installed on a computer running Windows and there must be a working Windows NT 4 Server domain controller or a Windows Server 2000 or later domain controller running in mixed mode. This is a legacy solution that should only be used if LDAP cannot be used.

The Windows NT Domain authentication method can be combined with a user directory in either Windows NT Domain mode or in Spotfire database mode.

When combining this authentication method with a Spotfire database user directory mode, the post-authentication filter must be configured for auto-creating mode, so that the users will be automatically added to the user directory. When combining it with a Windows NT Domain User Directory, the default blocking post-authentication filter is already correctly configured.

Combination of LDAP and Spotfire database authentication

If you configure authentication towards an external user directory such as an LDAP directory, or a Windows NT Domain, you can combine this with adding users manually to the Spotfire database.

This feature allow users to access Spotfire eventhough they are not part of the external user directory. The reason for adding such users could for example be if they are temporary users, that you do not want to add to the LDAP directory, or to make sure that administrators can access Spotfire even if the connection to the LDAP directory is lost. These users will be added to the same domain as the groups created in Spotfire.

This feature is enabled by default. For information on how to disable this feature, see [Disabling adding database users when using LDAP](#).



If you switch from Spotfire database authentication to LDAP authentication, all users remaining in the Spotfire database will still have access to Spotfire.

Disabling adding database users when using LDAP

You can disable the possibility to add users to the Spotfire database when authenticating towards an external directory.

Procedure

1. Open a command line and export the active server configuration (the `configuration.xml` file) by using the [export-config](#) command; for additional information, see [Executing commands on the command line](#).

2. On the command line, enter the following command:

```
config set-config-prop --name=user-directory.allow-database-user-creation --value=false
```



To enable the feature again, run the same command but set the value to true.

3. Import the configuration file back to the Spotfire database by using the [import-config](#) command.
4. Restart the Spotfire Server service.

Authentication towards a custom JAAS module

All the user name and password authentication methods that are supported by Spotfire Server are implemented as Java Authentication and Authorization Service (JAAS) modules. Spotfire also supports third-party JAAS modules.

You may therefore use a custom JAAS module, provided that it does the following:

- Validates user name and password authentication.
- Uses JAAS' NameCallback and PasswordCallback objects for collecting the user names and passwords.

When using a custom JAAS module, you must place the jar file in the `<installation_dir>/tomcat/webapps/spotfire/WEB-INF/lib` directory on all Spotfire Servers.

For more information about JAAS, consult the [JAAS Reference Guide](#).

Single sign-on authentication methods

Spotfire Server can be integrated with certain single sign-on systems that are used in enterprise environments.

Spotfire Server can use the NTLM or Kerberos single sign-on authentication methods, where the identity information stored within the user's current Windows session is reused to authenticate the user on the server. Thus, when using these authentication methods, users are never prompted for user name or password when they log in to Spotfire Server. The Kerberos and NTLM authentication methods are commonly referred to as Integrated Windows Authentication.

Spotfire Server can also authenticate users based on X.509 certificates. This requires the server to be configured for mutual TLS, meaning HTTPS with X.509 client certificates.

NTLM authentication

The NTLM authentication method reuses the identity information associated with the user's current Windows session. This identity information is gathered when the user initially logs in to Windows.

When both the client computer and the server computer belong to the same Windows domain or two separate Windows domains with established trust between them, this can provide a single sign-on experience.

If the client computer belongs to a separate Windows domain (without trust established to the server computer's domain), the current Windows session is not valid in the Windows domain of the server computer and the user will be prompted for user name and password. The user must then enter the user name and password of a valid account that belongs to the Windows domain of the server computer.

It is not possible to delegate NTLM authentication; Spotfire Server can not reuse the authentication credentials presented by the client, for example when authenticating against an Information Services data source that also uses NTLM. If you need such functionality, use Kerberos instead.

The NTLM authentication method can be combined with a user directory of either type:

- LDAP (recommended)
- Spotfire database, provided that the default post-authentication filter is configured in auto-creating mode

The following instructions assume that either combination of authentication and user directory is already fully working.

Setting up NTLM authentication involves two steps:

[Creating a computer service account in your Windows domain](#)

[Configuring NTLM authentication](#)

Downloading third-party components (JCIFS) for NTLM authentication

If you plan to use NTLM authentication and did not download the required JCIFS components during server installation, you can manually download them later.

Prerequisites

You have completed a basic installation of Spotfire Server.

Procedure

1. Go to http://public.tibco.com/pub/tibco_oss/jcifs/.
2. Download and extract jcifs_1.3.19.zip to the following directory: <installation directory>\tomcat\webapps\spotfire\WEB-INF\lib.
The required jcifs.jar file appears in the ... \WEB-INF\lib directory.

Creating a computer service account in your Windows domain

To set up NTLM authentication, you first create a computer service account by running a Visual Basic script that is distributed with Spotfire Server.

Prerequisites

- The script must be run on a Windows computer, but does not have to be run on the same computer that the server is installed on.
- You must be logged in to your Windows domain as a member of the group Account Operators or Administrators to run the SetupWizard.vbs script.
- If Spotfire Server is installed on a Linux computer, copy the SetupWizard.vbs script to a Windows computer first.



Alternatively, you can create the computer account manually; see [Creating a computer service account manually](#).

Procedure

1. Double-click the following file: <installation_dir>\tomcat\bin\setupwizard.vbs
2. In the **Domain Controller Hostname** panel, enter the hostname of one of your domain controllers. Click **OK**.
3. In the **Account Name** panel, enter the short name of the computer account to be created. The short name must not exceed 15 characters. Click **OK**.
4. In the **Distinguished Name** panel, enter a distinguished name for the account to be created. We suggest that you use a distinguished name that is based on the short name entered in the previous panel. You should edit this to match your Windows domain, with regards to parameters such as in which Organizational Units (OU) the account should be placed. Click **OK**.
5. In the **Account Password** panel, enter a password for the account to be created. Click **OK**.
A dialog opens with text indicating if the tool was successful. Click **OK**.



If the tool was unsuccessful, make sure that the logged in user has the required permissions to create accounts in the Windows Domain, and that the Domain Controller can be reached.

6. The file SetupWizard.txt, created by the tool in the folder where the tool is located, opens. If it does not, open it manually. The information in the file is required to run the NTLM authentication configuration commands.

Example of a SetupWizard.txt file

```
# Generated by the Jespa Setup Wizard from IOPLEX Software on 2011-04-07

jespa.bindstr = dc.example.research.com
jespa.dns.servers = 192.168.0.1
jespa.dns.site = Default-First-Site-Name
jespa.service.acctname = jespa-svc$@dc.example.research.com
jespa.service.password = Pa33w0rd
```

What to do next

[Configure NTLM authentication using configuration commands](#)

Creating a computer service account manually

If you are setting up NTLM authentication and you are unable to run the `SetupWizard.vbs` script, or you prefer to create the account manually, follow these steps.

Prerequisites

If Spotfire Server is installed on a Linux computer, copy the `SetComputerPassword.vbs` script to a Windows computer first.

Procedure

1. Create the computer account by using the Microsoft Management Console snap-in Domain Users and Computers. Refer to Microsoft documentation for details on how to use this tool.



Make sure to create a new computer account. A user account will not work. Reusing an existing computer account will not work.

2. To set a password for this account, open a command line and run this script with the account name and password as arguments to the command: `<installation dir>/tomcat/bin/SetComputerPassword.vbs`.
`SetComputerPassword.vbs jespa-svc$@dc.example.research.com Pa33w0rd`

What to do next

[Configure NTLM authentication using configuration commands](#)

Configuring NTLM authentication for a single server

These instructions are for configuring NTLM authentication by using the command line.

Prerequisites

You have created a computer service account; see [Creating a computer service account in your Windows domain](#).

Procedure

1. Configure NTLM authentication by using the following commands: [config-ntlm-auth](#) and [list-ntlm-auth](#).

This is the information you must have to run the commands:

Server (optional)	The name of the server instance to which the specified configuration options belong. If no server name is specified, then all parameters will be shared, applying to all servers in the cluster. It is common to use server-specific values for the account name and password configuration options.
Account name (required)	Specifies the fully qualified name of the Active Directory computer account that is to be used by the NTLM authentication service. This account must be a proper computer account, created solely for the purpose of running the NTLM authentication service. It can neither be an ordinary user account, nor an account of an existing computer. Note that the local part of an Active Directory computer account name always ends with a dollar sign, and the local part of the account name (excluding the dollar sign) must not exceed 15 characters. Example: ntlm-svc\$@research.example.com
Password (required)	Specifies the password for the computer account used by the NTLM authentication service.
DNS domain name (optional)	The DNS name of the Windows domain to which the Spotfire Server computer belongs. The specified domain name is automatically resolved into a domain controller hostname. As an alternative to specifying a DNS domain name, it is also possible to specify a domain controller hostname directly. The DNS domain name is recommended because you then automatically get the benefits of fail-over and load-balancing, provided that you have more than one domain controller. The DNS domain name and domain controller arguments are mutually exclusive. Example: research.example.com
Domain controller (optional)	The DNS hostname of an Active Directory domain controller. It is recommended that the DNS domain name option be used instead because that option gives the benefits of fail-over and load-balancing. The domain controller and DNS domain name arguments are mutually exclusive. Example: dc01.research.example.com
DNS servers (optional)	A comma-separated list of IP addresses of the DNS servers associated with the Windows domain. When no DNS servers are specified, the server will fall back to use the server computer's default DNS server configuration. Example: 192.168.1.1,192.168.1.2
AD site (optional)	Specifies the Active Directory site where the Spotfire system is located. Specifying an Active Directory site can potentially increase performance because the NTLM authentication service will then only communicate with the local Windows domain controllers. Example: VIENNA
DNS cache TTL (optional)	Specifies how long (in milliseconds) name server lookups should be cached. The default value is 5000 ms.

Connection ID header name (optional)	This parameter specifies the name of an HTTP header containing unique connection IDs in environments where the server is located behind a proxy or load-balancer that does not properly provide the server with the client's IP address. The specified HTTP header must contain unique connection IDs for each client connection and is thus typically based on the client's IP address together with the connection's port number on the client side.
--------------------------------------	--

2. Import the configuration using the [config-auth](#) command and restart the server to activate the NTLM single sign-on authentication method.

Kerberos authentication

Kerberos is a protocol that allows for secure authentication even over unsecure networks. It can be difficult to set up, but after it is fully working you have a very secure authentication system with the benefits of single sign-on.

It is usually a good idea to first create a working setup where the server uses username and password/LDAP authentication and a user directory in LDAP mode, and then proceed with switching from username and password/LDAP to Kerberos.

Setting up Kerberos authentication on Spotfire Server

If you intend to use the Kerberos authentication method on your system, the first thing you must do is to set up Spotfire Server to use Kerberos.

The following steps are required to configure Spotfire Server for the Kerberos authentication method. Steps 1-3 are performed as a Domain Administrator. Steps 4-7 are performed in Spotfire Server. See step 1 for a list of the prerequisites.

Creating a Kerberos service account

Creating a Kerberos service account is the first step in configuring Spotfire Server for the Kerberos authentication method.


Prerequisites

- Windows Domain Controllers running Windows Server 2008 or later.
- A computer with the Microsoft Active Directory Users and Computers MMC snap-in.
- A computer with the Microsoft Support Tools installed.
- A domain administrator account or a user account which is a member of the built-in Account Operators domain group, or any account with equivalent permissions.
- Windows Domain accounts for all Spotfire users.
- A fully-working user directory, with either of the following options:
 - LDAP (recommended)
 - Spotfire database, provided that the built-in post-authentication filter is auto-creating new users.

Procedure

1. Log in to the computer as a domain administrator or a user who is a member of the built-in Account Operators domain group.
2. Open the Active Directory Users and Computers MMC snap-in.

3. Create an ordinary user account with the following properties:

- Use the same identifier in the **Full name** and **User logon name** (pre-Windows 2000) fields.
 Use only lowercase characters and make sure that there are no spaces in these fields.
- Select the **Password never expires** check box.
- Clear the **User must change password at next logon** check box.
- If you want to use the crypto algorithm aes128-sha1 or aes256-sha1 the account option **This account supports Kerberos AES 128 bit encryption** or **This account supports Kerberos AES 256 bit encryption** must also be selected.

Registering Service Principal Names

Registering Service Principal Names (SPN) is the second step in configuring Spotfire Server for the Kerberos authentication method.

Procedure

1. Log in to the computer as a domain administrator or a user who is a member of the built-in Account Operators domain group.
2. From the Microsoft Support Tools package, use the **setspn.exe** command-line tool to register two SPNs for the Kerberos service account:

- Execute the following two commands, replacing the variables as indicated in the table below the commands:

```
> setspn -S HTTP/<fully qualified hostname>[:<port>] <service account name>
> setspn -S HTTP/<hostname>[:<port>] <service account name>
```

If the Spotfire Server is not listening on the default HTTP port 80 or the default HTTPS port 443, you should execute the **setspn** commands both with and without the port specified:

```
> setspn -S HTTP/<fully qualified hostname>[:<port>] <service account name>
> setspn -S HTTP/<hostname>[:<port>] <service account name>
> setspn -S HTTP/<fully qualified hostname> <service account name>
> setspn -S HTTP/<hostname> <service account name>
```

Variable	Description
fully qualified hostname	The fully qualified DNS hostname of the computer hosting Spotfire Server (in lowercase characters).
hostname	The short DNS hostname, without domain suffix, of the computer hosting Spotfire Server (in lowercase characters).
service account name	The user login name of the previously created Kerberos service account (in lowercase characters).

Variable	Description
port	The TCP port number on which Spotfire Server is listening. This is not required if using the default HTTP port 80 or the default HTTPS port 443.



You must use the name of a DNS A record for Spotfire Server. A CNAME record will not work.



Avoid explicitly specifying the port number if Spotfire Server is using the default HTTP port 80.



It is recommended that you not have multiple Kerberos-enabled HTTP services on one computer.

Registering Service Principal Names for the "spotsvc" Kerberos service account to be used by a Spotfire Server installed on the "spotfireserver.research.example.com" computer and listening on the default HTTP port 80 or the default HTTPS port 443:

```
> setspn -S HTTP/spotfireserver.research.example.com spotsvc
> setspn -S HTTP/spotfireserver spotsvc
```

This creates the following two SPNs for the "spotsvc" service account:

- HTTP/spotfireserver.research.example.com
- HTTP/spotfireserver

To list the resulting Service Principal Names for a Kerberos service account, execute the following command:

```
> setspn -L <service account name>
```

For example, for the "spotsvc" Kerberos service account, the previous command looks like this:

```
> setspn -L spotsvc
```

Creating a keytab file for the Kerberos service account

Creating the keytab file is the third step in configuring Spotfire Server for the Kerberos authentication method.

Procedure

1. Log in to the computer as a domain administrator or a user who is a member of the built-in Account Operators domain group.
2. Execute the following command, replacing the variables with the appropriate values:

```
> ktpass /princ HTTP/<fully qualified hostname>[:<port>]@<realm> /ptype
krb5_nt_principal
/crypto <crypto algorithm> /mapuser <service account name> /out spotfire.keytab
-kvno 0
/pass <service account password>
```



Make sure that the executed command does not have any newlines.



All values are case sensitive.



Older versions of the ktpass.exe tool will fail to create the keytab file when the tool is not run on an actual domain controller.

Variable	Description
fully qualified hostname	The fully qualified DNS hostname of the computer hosting Spotfire Server, which must exactly match the fully qualified hostname used when registering the SPNs (in lowercase characters).
port	The TCP port number on which Spotfire Server is listening (only specified if the port number was explicitly included in the registered Service Principal Names (SPN)). This is not required if using the default HTTP port 80 or the default HTTPS port 443.
realm	The name of the Kerberos realm, which is the DNS domain name written in uppercase characters.
crypto algorithm	Can be one of aes128-sha1, aes256-sha1 or rc4-hmac-nt. Make sure that the selected crypto algorithm is also specified in the krb5.conf file.
service account name	The user login name of the service account with the registered SPNs (written in lowercase characters).
service account password	The password for the service account.



If you change the password of the Kerberos service account, you must re-create the keytab file.



It is not critical to use the name "spotfire.keytab" for the keytab file, but the following instructions assume that this name is used.

Creating a keytab file for the "spotsvc" Kerberos service account in the "research.example.com" domain for Spotfire Server listening on the default HTTP port 80, or the default HTTPS port 443 on the "spotserver.research.example.com" computer:

```
> ktpass /princ HTTP/spotfireserver.research.example.com@RESEARCH.EXAMPLE.COM
/ptype krb5_nt_principal /crypto rc4-hmac-nt /mapuser spotsvc /out
spotfire.keytab -kvno 0
/pass spotsvcpassword
```

Creating a keytab file for the "spotsvc" Kerberos service account in the "research.example.com" domain for Spotfire Server listening on the HTTP port 8080 on the "spotserver.research.example.com" computer:

```
> ktpass /princ HTTP/
spotfireserver.research.example.com:8080@RESEARCH.EXAMPLE.COM
/ptype krb5_nt_principal /crypto rc4-hmac-nt /mapuser spotsvc
/out spotfire.keytab -kvno 0 /pass spotsvcpassword
```

Configuring Kerberos for Java

Configuring Kerberos for Java by editing the `krb5.conf` file is the fourth step in configuring Spotfire Server for the Kerberos authentication method.

Procedure

1. Open the file `krb5.conf` located in the directory `<installation_dir>\jdk\jre\lib\security` (Windows) or `<installation_dir>/jdk/jre/lib/security` (Unix) and edit the following values to reflect your environment.



The arguments are case sensitive.

For more information, see [The `krb5.conf` file](#).

- **MYDOMAIN:** The name of the Kerberos realm, usually the same as the name of the Windows Domain, written in uppercase characters.
- **mydomain:** The name of the Windows Domain, written in lowercase characters.
- **mydc:** The name of the domain controller, written in lowercase characters.

Configuring Kerberos for Java in the "research.example.com" domain, with the two domain controllers "dc01.research.example.com" and "dc02.research.example.com":

```
[libdefaults]
    default_realm = RESEARCH.EXAMPLE.COM
    default_keytab_name = spotfire.keytab
    default_tkt_enctypes = aes128-cts rc4-hmac
    default_tgs_enctypes = aes128-cts rc4-hmac
    forwardable = true

[realms]
    RESEARCH.EXAMPLE.COM = {
        kdc = dc01.research.example.com
        kdc = dc02.research.example.com
        admin_server = dc01.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
```

2. (Optional) If you want to use the crypto algorithm `aes256-sha1`, you must perform the following tasks:
 - a) Add `aes256-cts` as the first option in `default_tkt_enctypes` and `default_tgs_enctypes`.
 - b) Install the Java Cryptography Extension (JCE) unlimited strength jurisdiction policy files on the Spotfire Server .



It is the user's responsibility to verify that these files are allowed under local regulations.

Copying the Kerberos service account's keytab file to Spotfire Server

Copying the keytab file to Spotfire Server is the fifth step in configuring Spotfire Server for the Kerberos authentication method.

Procedure

1. Copy the `spotfire.keytab` file to the directory `<installation dir>\jdk\jre\lib\security` (Windows) or `<installation dir>/jdk/jre/lib/security` (Unix) in Spotfire Server.



Because this file contains sensitive information, it must be handled with care. The file must not under any circumstances be readable by unauthorized users.

To list the contents of the keytab file, use the `klist` command-line tool. It lists the principal name, crypto algorithm, and security credentials. The tool is included in the bundled JDK and is only available when installed on Windows:

```
> <installation dir>\jdk\jre\bin\klist.exe -k -t -e -K <keytab file>
```

To test the keytab file, use the `kinit` command-line tool which is also included in the bundled JDK on Windows platforms:

```
> <installation dir>\jdk\jre\bin\kinit.exe -k -t <keytab file> HTTP/<fully qualified hostname>[:<port>]@<realm>
```

If the keytab file is correctly set up, a ticket cache file is created in the logged-in user's home directory. It can typically be found in the path `C:\Users\<user>\krb5cc_<user>`.

2. As soon as you have verified that the ticket cache was created, you must delete the ticket cache file to prevent future problems.

Using Kerberos authentication with delegated credentials

Users can authenticate to different data sources using single sign-on login information. The server can delegate the user authentication to the data source, either through Information Services, or through a connector. This is possible only if you use the Kerberos single sign-on method.

If you are using a JDBC driver that supports passing the delegated user's Generic Security Standard (GSS) credentials through a connection property, then you can use constrained delegation with Information Services.

To enable constrained delegation for these drivers, add the following connection property to the corresponding Data Source Template.

```
<connection-property>
  <key>spotfire.kerberos.gsscredential.property</key>
  <value>connectionPropertyName</value>
</connection-property>
```

Where `connectionPropertyName` is driver-specific. (Refer to your driver's documentation for more information.)

Prerequisites

For delegation to work, no client user account in the domain can have the setting **Account is sensitive and cannot be delegated**. By default, this setting is not enabled.

Procedure

1. Set up Kerberos authentication as described in [Kerberos authentication](#). Make sure that users can log in with this method.
2. Grant the right to delegate client credentials to the Spotfire Server service account that is used for client authentication.



Only the specified accounts can be delegated by the service account.

- If possible, grant constrained delegation rights to the service account; see [Enabling constrained delegation](#).
- If you cannot use constrained delegation, grant unconstrained delegation rights. See the following topics for more information.
 - [Enabling unconstrained delegation for an account on a domain controller in Windows 2000 mixed or native mode](#).
 - [Enabling unconstrained delegation on a domain controller in Windows Server 2003 mode](#).



As of Spotfire version 7.7, the default delegation policy is "REQUIRE". This means that if Spotfire Server cannot delegate end user credentials, end users will not be able to open analyses in the web client. Prior to this, the default delegation policy was "TRY", which would open analyses using impersonation if delegation failed.

Enabling constrained delegation

This is the second step in the process of setting up Kerberos authentication with delegated credentials for your Spotfire implementation. It allows the Spotfire Server to delegate user credentials to nodes.

Procedure

1. On the domain controller, go to **Administrative Tools**.
2. Select **Active Directory Users and Computers**.
3. Locate the Spotfire Server service account.
4. To open the account properties, right-click the account name and then click **Properties**.
5. On the **Delegation** tab, select **Trust this user for delegation to specified services only**.



The **Delegation** tab is visible only for accounts to which SPNs are mapped.

6. Select **Use any authentication protocol**, and then click **Add**.
7. Click **Users or Computers** and select each user account or machine account that runs the node manager service on your nodes.



If the node manager services are run by user accounts, you must first register SPNs for these. See [Setting up Kerberos authentication on nodes](#).

8. Select the **http** service for each account, and then click **OK**.
9. Click **Apply**.

What to do next

[Enabling constrained delegation on nodes](#)

Enabling unconstrained delegation on a domain controller in Windows Server 2003 mode

This is the second step in the process of setting up Kerberos authentication with delegated credentials for your Spotfire implementation.

Procedure

1. On the domain controller, select **Start > Programs > Administrative Tools**.
2. Select **Active Directory Users and Computers**.

3. Locate the Spotfire Server service account.
4. To open the account properties, right-click the account name and then click **Properties**.
5. On the **Delegation** tab, select **Trust this user for delegation to any service (Kerberos only)**.



The **Delegation** tab is visible only for accounts to which SPNs are mapped.

6. Click **Apply**.

What to do next

[Creating an Information Services data source template using Kerberos login](#)

Enabling unconstrained delegation for an account on a domain controller in Windows 2000 mixed or native mode
This is the second step in the process of setting up Kerberos authentication with delegated credentials for your Spotfire implementation.

Procedure

1. On the domain controller, select **Start > Programs > Administrative Tools**.
2. Select **Active Directory Users and Computers**.
3. Locate the Spotfire Server service account.
4. To open the account properties, right-click the account name and then click **Properties**.
5. On the **Account** tab, in the **Account Options** list, select **Account is trusted for delegation**.
6. Click **Apply**.

What to do next

[Creating an Information Services data source template using Kerberos login](#)

Selecting Kerberos as the Spotfire login method

Selecting Kerberos as the Spotfire login method is the sixth step in configuring Spotfire Server for the Kerberos authentication method. You can use the configuration tool, or use the command line as detailed in this procedure.

Procedure

1. Execute the [config-kerberos-auth](#) command. The command takes the following two parameters:
 - Keytab file: The fully qualified path to the spotfire.keytab file. If the keytab file is named "spotfire.keytab" and has been copied to the recommended directory, the default path \$ {java.home}/lib/security/spotfire.keytab is already correct. The shorthand \$ {java.home} refers to the directory <installation dir>\jdk\jre (Windows) or <installation dir>/jdk/jre (Unix).
 - Service Principal Name: Specify the same Service Principal Name that was used when creating the keytab file. Example: HTTP/spotfireserver.research.example.com
2. Use the [config-auth](#) command to activate the Kerberos SSO authentication method.
3. Import the configuration and restart the server for the changes to take effect.

Disabling the username and password fields in the Spotfire Analyst login dialog

Because the Kerberos authentication method provides single sign-on capabilities, there is no need to prompt the end user for user name and password in the Spotfire Analyst login dialog.



This step is optional.

Procedure

1. Open a command line and export the active configuration (the `configuration.xml` file) by using the `export-config` command; for additional information, see [Executing commands on the command line](#).
2. Execute the `config-login-dialog` command:

```
> config config-login-dialog --allow-user-provided-credentials=false
```
3. Import the configuration file back to the Spotfire database by using the `import-config` command.
4. Restart the Spotfire Server service.



If you are using the configuration tool, select the **Never display login dialog** check box for the **Login dialog** option.

Kerberos authentication for clustered servers with load balancer

In a clustered environment where Kerberos authentication is used to authenticate users, the load balancer forwards all Kerberos authentication information to the Spotfire Servers. No configuration on the load balancer is needed, but there are certain considerations to take into account when Kerberos authentication is set up.

These are the special considerations:

- Two Service Principal Names must be created for each Spotfire Server as well as for the load balancer.
- One keytab file must be created. This must use the fully qualified Service Principal Name of the load balancer.
- This keytab file must be copied to each Spotfire Server.
- When Kerberos authentication is set up, the fully qualified Service Principal Name of the load balancer must be provided.

For general information about Spotfire Server clusters, see [Clustered server deployments](#).

Setting up Kerberos authentication on nodes

After setting up Kerberos authentication on Spotfire Server, you must set it up for the nodes in your environment.



If you use Kerberos delegation, your Spotfire Server and Node Managers must be installed on different computers.

The account used to run the node manager service must be trusted for delegation, and you might need to register Service Principal Names (SPN) for that account. Also, all web client users must be given permission to modify the node manager services folder.

- If the node manager service is run using the local machine account, open the Active Directory Users and Computers MMC snap-in, select the machine account, and then select **Trust this computer for delegation to any service**.

- If the node manager service is run using a specified user account, open the Active Directory Users and Computers MMC snap-in, select the user account, and then select **Trust this user for delegation to any service**.

If the node manager service is run using a specified user account, you must also register Service Principal Names (SPN) for that account.

```
> setspn -S HTTP/<fully qualified node hostname>[:<port>] <node service account name>
```

```
> setspn -S HTTP/<node hostname>[:<port>] <node service account name>
```

For information on how to register SPNs, see [Registering Service Principal Names](#).

All web client user accounts must be given permission to modify the folder nm\services. This permission allows the delegated users to read, write, and delete temp files.



If Spotfire Connectors are used for the Web Player service, all delegated web client users must also have access to the applicable connector drivers.

Enabling constrained delegation on nodes

You must enable constrained delegation for your nodes. It allows the service on the node to delegate user credentials to the Spotfire Server and access external resources.

Prerequisites

You have enabled constrained delegation on Spotfire Server. See [Enabling constrained delegation](#).

Procedure

1. On the domain controller, go to **Administrative Tools**.
2. Select **Active Directory Users and Computers**.
3. Locate the machine accounts or user accounts that runs the node manager services.

Steps 4 through 11 must be performed for each account that runs a node manager service.
4. To open the account properties, right-click the account name and then click **Properties**.
5. On the **Delegation** tab, select **Trust this user for delegation to specified services only**.

The **Delegation** tab is visible only for accounts to which SPNs are mapped. If the node manager services are run by user accounts, you must first register SPNs for these. See [Setting up Kerberos authentication on nodes](#).
6. Select **Use any authentication protocol**, and then click **Add**.
7. Click **Users or Computers** and select any Spotfire Server service account.
8. Select the **http** service for each Spotfire Server service account, and then click **OK**.
9. Click **Users or Computers** and select any machine account or service account for a computer running the external resource you want to delegate to.
10. Select the applicable services for each account, and then click **OK**.

For example the **MSSQLSvc** service for delegation to a Microsoft SQL Server or the **CIFS** service for delegation to a file share.
11. Click **Apply**.

Enable Kerberos authentication for end-users

If you use Kerberos authentication, it must be enabled in the browsers of all end-user computers.

This is applicable for all users accessing Spotfire Server, either from a browser, or Spotfire Analyst.

Enabling Kerberos for Internet Explorer and Spotfire Analyst

Follow these steps on every computer using Internet Explorer or Spotfire Analyst.

Procedure

1. Go to **Tools > Internet Options > Advanced** and select **Enable Integrated Windows Authentication (Requires Restart)**.
2. The Spotfire Server you are connecting to must be located in the **Intranet** security zone.



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



If a client accesses a server belonging to another trusted domain, that server must be added to the **Local Intranet** zone, found under **Internet Options > Security > Local Intranet**. Without this setting, Internet Explorer, or Spotfire Analyst will not be able to authenticate using Kerberos.

For example, if the client `client.emea.example.com` accesses the server `server.na.example.com`, then `server.na.example.com` must be added to the **Local Intranet** zone.

Enabling delegated Kerberos for Google Chrome

Follow these instructions on every computer using Google Chrome.

You must create and set a registry key for Google Chrome.

1. The Spotfire Server you are connecting to must be located in the **Intranet** security zone.
2. In the Registry Editor, go to `[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome]`.
3. Add the String Value `AuthNegotiateDelegateWhitelist`.
4. Modify `AuthNegotiateDelegateWhitelist` and add the URL to the Spotfire Server.

For more information, see the Chromium Projects developer page at <http://dev.chromium.org/administrators/policy-list-3#AuthNegotiateDelegateWhitelist>

Enabling Kerberos for Mozilla Firefox

Follow these steps on every computer using Mozilla Firefox.

Procedure

1. In the Firefox browser address box, type `about:config`.
2. For the following parameters, set the values to the Spotfire Server URL for which you want to activate Negotiate.
 - `network.negotiate-auth.delegation-uris`
 - `network.negotiate-auth.trusted-uris`

Using Kerberos to log in to the Spotfire database

To increase security in your Spotfire implementation, you may want to set up Spotfire Server to authenticate with the Spotfire database using the Kerberos protocol.



This only affects how the database connections are authenticated and is not required for Spotfire Analyst clients or web clients to connect to Spotfire Server using the Kerberos authentication method.

Prerequisites

- Windows Domain Controllers running Windows Server 2008 or later.
- A computer with the Microsoft Active Directory Users and Computers MMC snap-in.
- A computer with the Microsoft Support Tools installed.
- A domain administrator account or a user account which is a member of the built-in Account Operators domain group, or any account with equivalent permissions.
- The database server must already be installed and configured for both Kerberos authentication and user name/password authentication.
- Microsoft Active Directory is used as Kerberos environment.
- If the database is an Oracle database, then download Oracle's latest JDBC driver (`ojdbc7.jar`) from Oracle's web page.
- If the database is a Microsoft SQL Server database, use the bundled Microsoft JDBC driver (`sqljdbc4.jar`). Version 4.0 of the `sqljdbc4.jar` driver introduced the new `authenticationScheme=JavaKerberos` directive, which is required.

Procedure

1. [Create a Windows domain account for the Spotfire database.](#)
2. Create the Spotfire database.
 - If you are using SQL Server database: Edit and run the `create_databases_ia.bat` script. This creates a SQL Server database account and connects it to the previously created Windows domain account. For instructions, see [Setting up the Spotfire database \(SQL Server with Integrated Windows authentication\)](#).
 - If you are using Oracle database: Edit and run the `create_databases.bat` script. This will create a normal Oracle database account that authenticates with user name and password; for instructions on creating the database account, see [Setting up the Spotfire database \(Oracle\)](#).
3. Oracle database only: [Configure the Spotfire database account to the Windows domain account.](#)
4. [Install Spotfire Server.](#)
5. Install a vendor database driver; see [Database drivers](#).
6. [Configure Kerberos for Java.](#)
7. Optional: [Create a keytab file for the Kerberos service account.](#)
8. [Create a JAAS application configuration for the Spotfire database connection pool.](#)
9. [Register the JAAS application configuration file with Java.](#)
10. Connect to the Spotfire database by running the bootstrap command or by using the configuration tool; see [Configuring the database connection for Spotfire Server using Kerberos \(Oracle\)](#) or [Configuring the database connection for Spotfire Server using Kerberos \(SQL Server\)](#).

Creating a Windows domain account for the Spotfire database


Creating a Windows domain account for the database is the first step in setting up Kerberos authentication for database connections.

Prerequisites

See [Using Kerberos to log in to the Spotfire database](#) for the list of prerequisites.

Procedure

1. Log in to Windows with one of the following accounts:
 - A domain administrator
 - A user who is a member of the built-in Account Operators domain group
 - A user with equivalent privileges
2. Launch the Active Directory Users and Computers MMC snap-in and create a normal user account with the following properties:
 - Use the same identifier in the **Full name**, **User logon name**, and **User logon name (pre-Windows 2000)** fields.



Make sure to use only lowercase characters, and leave no spaces in these fields.
 - Select the **Password never expires** check box.
 - Clear the **User must change password at next logon** check box.
 - Recommended: Select the **Account is sensitive and cannot be delegated** check box.

What to do next

- SQL Server database: Edit and run the `create_databases_ia.bat` script. This creates a SQL Server database account and connects it to the previously created Windows domain account. For instructions, see [Setting up the Spotfire database \(SQL Server with Integrated Windows authentication\)](#).
- If you are using Oracle database: Edit and run the `create_databases.bat` script. This will create a normal Oracle database account that authenticates with user name and password; for instructions on creating the database account, see [Setting up the Spotfire database \(Oracle\)](#).

Configuring the Spotfire database account to the Windows domain account

If you are using an Oracle database, this is the third step in setting up Kerberos to log in to the Spotfire database.

Procedure

1. Log in to the Oracle database instance with SYSDBA privileges to manage accounts. Connecting to a database with connection identifier ORCL as sysdba


```
sqlplus sys@ORCL as sysdba
```
2. Alter the Spotfire database account so that it is identified externally by running the following command:


```
SQL> alter user <SERVERDB_USER> identified externally as '<SERVERDB_USER>@REALM';
```

Replace <SERVERDB_USER> and <REALM> with the Spotfire database account name and the Kerberos realm. Make sure to use uppercase letters when specifying the Kerberos realm.

```
SQL> alter user spotuser identified externally as
'spotuser@RESEARCH.EXAMPLE.COM';
```

3. Test the Kerberos-enabled Spotfire database account by opening a command prompt running as the created Windows domain account. It should now be possible to connect to the database using the following command, assuming the connection identifier is ORCL: > sqlplus /@ORCL



It is assumed that Kerberos authentication is already set up for the Oracle client.

Keytab file for the Kerberos service account

There are several methods for creating the keytab file for the Kerberos service account.

Creating a keytab file for the Kerberos service account (using the ktpass.exe command from Microsoft Support Tools)

This method of creating a keytab file uses the **ktpass.exe** command that is included with Microsoft Support Tools.

Procedure

1. On a computer with the Microsoft Support Tools installed (it is not necessary to be logged in as a privileged user), execute the following command, replacing the <database account name>, <REALM>, <crypto algorithm> and <database account password> with the appropriate values. <crypto algorithm> can be one of , aes128-sha1, aes256-sha1 or rc4-hmac-nt. Make sure that the selected crypto algorithm is also specified in the krb5.conf file.



All values are case sensitive.

```
> ktpass /princ <database account name>@<REALM> /ptype krb5_nt_principal /
crypto <crypto algorithm> /out spotfire-database.keytab -kvno 0 /pass <database
account password>
```



It is not critical to use the name "spotfire-database.keytab" for the keytab file, but the following instructions assume that this name is used.

Example of creating a keytab file for the Spotfire database account named "spotuser" in the research.example.com domain:

```
> ktpass /princ spotuser@RESEARCH.EXAMPLE.COM /ptype krb5_nt_principal / crypto
rc4-hmac-nt /out spotfire-database.keytab -kvno 0 /pass spotuserpassword
```

2. Copy the spotfire-database.keytab file to the directory <installation_dir>\jdk\jre\lib\security (Windows) or <installation_dir>/jdk/jre/lib/security (Unix) in Spotfire Server.



Because this file contains sensitive information, it must be handled with care. The file must not under any circumstances be readable by unauthorized users.



If you change the password of the Kerberos service account, you must re-create the keytab file.

Creating a keytab file for the Kerberos service account (using the ktpass.exe command from the bundled JDK)

This method of creating a keytab file uses the **ktpass.exe** command that is included with the bundled JDK.

Procedure

1. On the computer where Spotfire Server is installed, execute the following command: `> ktab -k spotfire-database.keytab -a <database account name>`, replacing the `<database account name>` with the user login name of the Spotfire database account, written in lowercase letters.



All values are case sensitive.



It is not critical to use the name "spotfire-database.keytab" for the keytab file, but the following instructions assume that this name is used.

The tool prompts you for the password of the service account.

2. Enter the password that you used when creating the Spotfire database account.
3. Verify the created keytab by running the `klist` and `kinit` utilities:

```
> klist -k spotfire-database.keytab
> kinit -k -t spotfire-database.keytab <database account name>@<realm>
```



If you change the password of the Kerberos service account, you must re-create the keytab file.

Creating and verifying a keytab file for the "serverdb_user" Spotfire database account in the research.example.com domain:

```
> ktab -k spotfire-database.keytab -a serverdb_user
> klist -k spotfire-database.keytab
> kinit -k -t spotfire-database.keytab serverdb_user@RESEARCH.EXAMPLE.COM
```

4. Copy the `spotfire-database.keytab` file to the Spotfire Server directory `<installation_dir>\jdk\jre\lib\security` (Windows) or `<installation_dir>/jdk/jre/lib/security` (Unix).



Because this file contains sensitive information, it must be handled with care. The file must not under any circumstances be readable by unauthorized users.



If you change the password of the Kerberos service account, you must re-create the keytab file.

Creating a keytab file for the Kerberos service account (using the `ktutil` command on Linux)

This method of creating a keytab file on Linux uses the **ktutil** command.

Prerequisites

- Kerberos is installed on the Linux host where Spotfire Server is installed.
- The tools **ktutil**, **klist**, and **kinit** are available on the Linux host.

Procedure

1. Start the `ktutil` tool by invoking it from the command line without any arguments. Execute the commands below, replacing `<database account name>` with the user login name of the Spotfire database account, written in lowercase letters:

```
> ktutil
ktutil: add_entry -password -p <database account name> -k 0 -e aes128-sha1
Password for <database account name>:
```



```
ktutil: write_kt spotfire-database.keytab
ktutil: quit
```



All values are case sensitive.



It is not critical to use the name "spotfire-database.keytab" for the keytab file, but the following instructions assume that this name is used.

The tool prompts you for the password of the service account.

2. Enter the password that you used when creating the Spotfire database account.
3. Verify the created keytab by running the `klist` and `kinit` utilities:

```
> klist -k spotfire-database.keytab
> kinit -k -t spotfire-database.keytab <database account name>@<realm>
```



If you change the password of the Kerberos service account, you must re-create the keytab file.

Creating and verifying a keytab file for the "serverdb_user" Spotfire database account in the research.example.com domain:

```
> ktutil

ktutil: add_entry -password -p serverdb_user -k 0 -e rc4-hmac-nt
Password for serverdb_user:
ktutil: write_kt spotfire-database.keytab
ktutil: quit

> klist -k spotfire-database.keytab

> kinit -k -t spotfire-database.keytab serverdb_user@RESEARCH.EXAMPLE.COM
```

4. Copy the `spotfire-database.keytab` file to the following Spotfire Server directory:
<installation_dir>/jdk/jre/lib/security.



Because this file contains sensitive information, it must be handled with care. The file must not under any circumstances be readable by unauthorized users.



If you change the password of the Kerberos service account, you must re-create the keytab file.

Creating a JAAS application configuration for the Spotfire database connection pool

Follow these instructions to create a JAAS application configuration for the Spotfire database connection pool.

Procedure

1. Acquire a Kerberos ticket in one of the following ways, and name the file "spotfire-database.login":
 - By using a keytab file; see [Acquiring a Kerberos ticket using a keytab file](#).
 - By using a username and password; see [Acquiring a Kerberos ticket using a username and password](#).
 - By using the identity of the account running the Spotfire Server process; see
2. In Spotfire Server, create the file <install_directory>\jdk\jre\lib\security\spotfire-database.login (Windows) or <install_directory>/jdk/jre/lib/security/spotfire-database.login (Unix) and populate it with the `spotfire-database.login` file.

Acquiring a Kerberos ticket by using a keytab file

This method of acquiring a Kerberos ticket uses a keytab file.

Procedure

- In the following code, replace <service account name> and <realm> with the name of the Spotfire database account and the Kerberos realm. Make sure to



Use lowercase letters for the account name and uppercase letters for the realm name.

```
DatabaseKerberos
{
  com.sun.security.auth.module.Krb5LoginModule
    required
    debug=true
    storeKey=true
    useKeyTab=true
    keyTab="{java.home}/lib/security/spotfire-database.keytab"
    principal="<SERVERDB_USER>@<REALM>";
};
```

Acquiring a Kerberos ticket by using a username and password

This method of acquiring a Kerberos ticket uses a username and password.

Procedure

- In the following code, replace <service account name> and <password> with the name and the password of the Spotfire database account:

```
DatabaseKerberos
{
  com.sun.security.auth.module.Krb5LoginModule
    required
    debug=true
    storeKey=true
    useKeyTab=false
    doNotPrompt=false;
};
```

Acquiring a Kerberos ticket by using the identity of the account running the Spotfire Server process

To make it possible to log in to the Spotfire database as the user currently running the server, the connection pool must be able to acquire the initial Ticket-Granting-Ticket (TGT) from the native Ticket Cache of the Spotfire Server host.

Procedure

- Modify the following registry key so that the TGT session can be exported:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\
Parameters]"allowtgtsessionkey"=dword:00000001
```

```
DatabaseKerberos
{
  com.sun.security.auth.module.Krb5LoginModule
    required
    debug=true
    storeKey=true
    useTicketCache=true
    doNotPrompt=false;
};
```

Registering the JAAS application configuration file with Java

After you have created the `spotfire-database.login` file, it must be registered in Java.

Procedure

- Open the file `<install directory>/jdk/jre/lib/security/java.security` in a text editor and add the following lines to the end of the file:

```
# Register Java Authentication & Authorization Services (JAAS)
configurations
login.config.url.1=file:${java.home}/lib/security/
spotfire-database.login
```

Configuring the database connection for Spotfire Server using Kerberos (Oracle)

If you use an Oracle database, follow these instructions to configure the database connection for Spotfire Server.

Procedure

- To bootstrap Spotfire Server, execute the following bootstrap command, replacing `<database-url>` with the JDBC connection URL.



When using a username and a password to request the Kerberos ticket, make sure to also specify the `-username` and `-password` arguments.

```
> config bootstrap --test --driver-class=oracle.jdbc.OracleDriver --database-
url=<database
url> --kerberos-login-context=DatabaseKerberos -
Coracle.net.authentication_services=
(KERBEROS5)

> config bootstrap --test --driver-class=oracle.jdbc.OracleDriver --database-url=
jdbc:oracle:thin:@research.example.com:1521:orcl --kerberos-login-context=
DatabaseKerberos -Coracle.net.authentication_services=(KERBEROS5)
```

Configuring the database connection for Spotfire Server using Kerberos (SQL Server)

If you use an SQL Server database, follow these instructions to configure the database connection for Spotfire Server.

Procedure

- To bootstrap Spotfire Server, execute the following bootstrap command, replacing `<database url>` with the JDBC connection URL. This URL must include `;integratedSecurity=true;authenticationScheme=JavaKerberos` options.

```
> config bootstrap --test --driver-
class=com.microsoft.sqlserver.jdbc.SQLServerDriver
--database-url=<database url> --kerberos-login-context=DatabaseKerberos

> config bootstrap --test --driver-
class=com.microsoft.sqlserver.jdbc.SQLServerDriver
--database-url=jdbc:sqlserver://db.research.example.com:1433;DatabaseName=
spotfire_server;integratedSecurity=true;authenticationScheme=JavaKerberos
--kerberos-login-context=DatabaseKerberos
```

Authentication using X.509 client certificates

When Spotfire Server is set up with HTTPS and is configured to require client certificates, the information from the certificates can also be used for login purposes.

This method authenticates users by using an X.509 client certificate from the Spotfire client to Spotfire Server.

These are the general steps to configure Spotfire to use X.509 client certificates for authentication:

1. Configure Spotfire Server for HTTPS; see [Configuring HTTPS](#).
2. Install client certificates on each client. For details, see the documentation provided by your operating system vendor.
3. If you have not already done so, import the Certification Authority (CA) certificate(s) to the keystore; see [Installing CA certificates](#).
4. Configure Spotfire Server to require client certificates for HTTPS; see [Configuring Spotfire Server to require client certificates for HTTPS](#).
5. Configure Spotfire Server to use X.509 client certificates to authenticate users; see [Configuring Spotfire Server to use X.509 client certificates to authenticate users](#).

Installing CA certificates

To use X.509 client certificates for authentication, a keystore with CA certificate(s) must be placed in the installation directory.

Procedure

1. If you do not yet have a keystore, follow these steps:
 - a) Create a keystore and import the CA certificate(s) by executing the following command:.

```
><installation_dir>/jdk/bin/keytool -importcert -alias cacert -keystore
<installation_dir>/tomcat/certs/<keystore filename> -file <certificate
filename>
```

CA certificates can be in either PEM format or DER format.

Example for Windows:

```
> C:\tibco\tss\<version>\jdk\bin\keytool -importcert -alias cacert -keystore C:\tibco\tss
\<version>\tomcat\certs\example.jks -file cacert.cer
```

where "example" in *example.jks* is the server hostname.

- b) Repeat the previous step for each additional CA certificate.
2. When you have a keystore containing the CA certificate(s), copy the keystore file to the <installation_dir>/tomcat/certs directory.



The keystore containing the CA certificate(s) can be in either PKCS #12 or JKS format.

Configuring Spotfire Server to require client certificates for HTTPS

This procedure configures the server to require a valid user certificate for all connections.

This is done by editing the `server.xml` file.

Prerequisites

You have performed the first three steps in the topic [Authentication using X.509 client certificates](#).

Procedure

1. Open the following configuration file in an XML editor or a text editor: `<server install dir>/tomcat/conf/server.xml`.
2. Locate the section containing the configuration for the HTTPS connector:

```
<Connector port="443"
    maxHttpHeaderSize="65536"
    connectionTimeout="30000"
    enableLookups="false"
    URIEncoding="UTF-8"
    disableUploadTimeout="true"
    server="TIBCO Spotfire Server"
    compression="on"
    compressableMimeType="text/html,text/xml,text/plain,text/
css,application/json,application/javascript,image/svg+xml,application/xml"
    acceptorThreadCount="2"
    keepAliveTimeout="30000"
    maxKeepAliveRequests="-1"
    maxThreads="2000"
    SSLEnabled="true"
    scheme="https"
    secure="true">
    <SSLHostConfig certificateVerification="none"
        truststoreFile="./certs/[server hostname].jks"
        truststorePass="changeit"
        truststoreType="jks"
        sslProtocol="TLS"
        protocols="+TLSv1.2,+TLSv1.1,+TLSv1"
        honorCipherOrder="true"
        ciphers

        ...
        <Certificate certificateKeystoreFile="./certs/[server hostname].jks"
            certificateKeystorePassword="changeit"
            certificateKeystoreType="jks"
            certificateKeyAlias="[server hostname]" />
    </SSLHostConfig>
</Connector>
```

3. Update the **truststoreFile** parameter with the name of the keystore file containing the CA certificate(s).
4. Set the **truststorePass** parameter to the password for the keystore file containing the CA certificate(s).
5. Set the **truststoreType** parameter to `jks` for a Java keystore or `pkcs12` for a PKCS #12 keystore.
6. Set the **certificateVerification** parameter to `required`.

Configuring Spotfire Server to use X.509 client certificates to authenticate users

This procedure configures the server process for authenticating users with client certificates.

This configuration is done on the command line.

Prerequisites

You have performed the first four steps in the topic [Authentication using X.509 client certificates](#).

Procedure

1. Use the command [config-client-cert-auth](#) to configure the client certificates authentication. For more information, see [Executing commands on the command line](#).
2. Use the command [config-auth](#) to apply the X.509 client certificates single sign-on authentication method.



If you intend to use an LDAP user directory, an attribute in the certificate's Distinguished Name (DN) must match an LDAP account name. By default, the server will use the Common Name (CN) attribute as account name. Use the configuration tool or the [config-client-cert-auth](#) command to configure the server to use another attribute as account name.

Examples

- Using the entire DN as account name:

```
config config-client-cert-auth --name-attribute="DN"
```

This will use the entire DN as account name.

- Using the Subject Alternative Name of type rfc822Name as account name:

```
config config-client-cert-auth --name-attribute="subjectAltName:rfc822Name"
```

This will use a Subject Alternative Name as account name.

Configuring anonymous authentication

Anonymous authentication allows anyone to access public information that is available for viewing on the Spotfire web client without prompting them for a user name or password.

Procedure

1. Export the Spotfire Server basic configuration from the Spotfire database to an XML file, and then open the file in a text editor; for instructions on exporting the file, see [Manually editing the Spotfire Server configuration file](#).
2. Set the `security.anonymous-auth.enabled` configuration property to "true".
3. Save and close the file.
4. Import the file back into Spotfire Server; for instructions, see [Manually editing the Spotfire Server configuration file](#).
5. Enable the guest account by using the [enable-user](#) command in the following form: `config enable-user --username=ANONYMOUS\guest`

Web authentication

When using web authentication, a web browser will be displayed for all users, allowing them to log in to Spotfire using an external authentication provider, such as Google.

By default, the web authentication method supports authentication providers with OpenID Connect support, such as Google. The supported authentication providers can be expanded using the Custom Web Authenticator API. If you configure and enable several authentication providers, users will be allowed to select any of these providers. Users can select to remember the chosen provider, thereby enabling single sign-on, as long as they are logged in on that account.

Web authentication can be combined with username and password authentication.

Configuring OpenID Connect

These instructions are for configuring a default OpenID Connect web authentication provider using the configuration tool.

Prerequisites

- You have configured a public address URL. To do this, go to the Public Address page in the Spotfire Server configuration tool and enable the public address URL `http[s]://<spotfire server>[:<port>]/`.

- You have registered a client at the provider with a return endpoint URL, and received a client ID and a client secret from the provider.
 - The registered client must support the Authorization Code Grant.
 - The registered client must have permission to request the scopes that the server is configured to request. By default, these scopes are "openid", "profile", and "email", but the latter two can be removed and other scopes can be added.

For the default OpenID Connect web authentication providers, use the URL (starting with the configured public address URL):

```
http[s]://<spotfire server>[:<port>]/spotfire/auth/oidc/authenticate
```



When using web authentication, it is recommended to use HTTPS.



It is recommended to use the **Auto-create** option for the post-authentication filter.

Procedure

1. Open the Spotfire Server configuration tool. For information on launching the configuration tool, see [Opening the configuration tool](#).
2. In the configuration tool, select the **Configuration** tab.
3. On the Configuration Start page, select the authentication method **Web authentication**.

If, for example for backward compatibility with older Spotfire clients, you want to combine web authentication with username and password authentication, you should select the **BASIC** authentication method. This way, the launched web browser will have both a username and password alternative, and the alternative to use an external web authentication provider.
4. On the OpenID Connect page, select **Yes** to enable OpenID Connect authentication.
5. To add and configure a new provider, click **Add new provider**.
6. For each added provider, select **Yes** to enable the provider, and specify the **Provider name** (that will be displayed for users when selecting a provider).
7. For each provider, specify the **Discovery document URL**, the **Client ID** and the **Client secret**, as received when registering a client at the provider.
8. Save the configuration and restart the Spotfire Server.

Advanced OpenID Connect settings

More advanced settings can be configured for OpenID Connect, specifying what is displayed for end-users and what is communicated on the end-users between the provider and Spotfire Server.

For more information on these settings, refer to the documentation of the provider and to OpenID Connect, http://openid.net/specs/openid-connect-core-1_0.html.

Option	Description
Domain name	By default, the value of the issuer claim is used. A static name can be specified instead.
Username claim	By default, the value of the sub claim is used. Another claim can be specified.

Option	Description
Scopes	Add scopes to specify what access privileges are being requested. The requested scopes should preferably give access to the name and email claims.
Auth request prompt value	The value to give the prompt request parameter when making the authentication request. Controls how the provider prompts the end-user. May be one of none , login , consent and select_account . This is optional. By default the parameter will be omitted from the request.
Background color	You can specify a background color, as a hexadecimal value, for the added provider on the login page.

Configuring custom web authentication

These instructions are for configuring custom web authentication using the configuration tool.

Prerequisites

- You have implemented the CustomWebAuthenticator API.
- If applicable, you have registered a client at the provider, using a return endpoint URL, and have received a client ID and a client secret from the provider. Use the URL:

```
http[s]://<spotfire server>[:<port>]/spotfire/auth/custom/authenticate
```



When using web authentication, it is recommended to use HTTPS.



It is recommended to use the **Auto-create** option for the post-authentication filter.

Procedure

1. Open the Spotfire Server configuration tool. For information on how to launch the configuration tool, see [Configuration using the configuration tool](#).
2. In the configuration tool, select the **Configuration** tab.
3. On the Configuration Start page, select the authentication method **Web authentication**.



If, for example for backward compatibility with older Spotfire clients, you want to combine web authentication with username and password authentication, select the **BASIC** authentication method. This way, the launched web browser will have both a username and password alternative, and the alternative to use an external web authentication provider.

4. On the Custom Web Authentication page, select **Yes** to enable custom web authentication.
5. Specify the **Authenticator class** - the class implementing the CustomWebAuthenticator API interface.
6. Add any **Initialization parameters** relevant to your custom web authentication implementation.
7. Save the configuration and restart the Spotfire Server.

Two-factor authentication

Spotfire Server supports one form of two-factor authentication. It is possible to combine the chosen primary authentication method with X.509 client certificates.

Typically, the primary authentication method in the two-factor authentication is Basic, but it is also possible to use the other authentication methods.

When two-factor authentication is enabled, the server requires the name of the authenticated user to match the user name in the provided X.509 certificate. For instructions, see [Configuring two-factor authentication](#).

Configuring two-factor authentication

You can configure authentication through X.509 client certificates in addition to your primary authentication method.

Procedure

1. Configure the server to use the chosen primary authentication method.
2. In the configuration tool, on the Configuration page, in the Configuration Start panel, select **Enable two-factor authentication**.
A second Authentication panel is added.
3. In the second Authentication panel, configure the server to use client certificates.

Configuring two-factor authentication using the command line

You can set up two-factor authentication by using the command line or the configuration tool.

Procedure

1. Use the command line to set up the primary authentication method and the client certificates.
2. On the command line, enter the following command:

```
config config-two-factor-auth --enabled=true
```

External authentication

Spotfire clients may access Spotfire Server through an external authentication mechanism, usually a proxy or a load balancer.

When using an external authentication mechanism, Spotfire Server gets the external user name from an HTTP header or a cookie. Getting the external user name from an HTTP header or a cookie could potentially be a security risk and it is strongly recommended that you restrict the permissions to use this feature. It is also recommended to use the external authentication method only when using a load balancer or proxy.

When configuring external authentication, you can add several constraints:

- You can configure Spotfire Server to allow external authentication only when using a secure (TLS) connection.
- You can specify allowed hostnames and/or IP addresses of the client computers that are permitted to log in using external authentication. You can list allowed IP addresses and/or write regular expressions; if you specify both, Spotfire Server first checks in the list and then the regular expression.

In some cases, the proxy or load balancer has already forced the client to authenticate itself. Some proxies and load balancers are capable of forwarding the name of the authenticated user to Spotfire

Server. By enabling external authentication on Spotfire Server, the server can extract the identity of the client so that the client does not have to authenticate twice. Any proxy or load balancer that can propagate the user name so that it is available in the HTTP request to the server as a request attribute, is compatible

Typical scenarios are:

- When both the Spotfire Server cluster and its load balancer are configured for NTLM authentication.
- When the load balancer is configured for X.509 client certificate authentication and propagates the user names extracted from the certificates.
- When the load balancer requires the user to authenticate with username and password in a web form (for example SiteMinder). In this case, you must configure the load balancer to intercept and authenticate requests to, and only to, the path `/spotfire/sf_security_check_external_auth`.

External authentication may be used as a supplementary authentication method that can be used together with the main authentication method, but it can also be used as the main and only authentication method.

- If clients are to always go through a load balancer to reach Spotfire Server, configure external as the main authentication method in the **Authentication** panel. In this case it is not possible to access a Spotfire Server directly. You must also specify a declared authentication method in the **External Authentication** panel.
- Even if a load balancer is used in front of a set of Spotfire Servers, accessing the server directly may be desired. If this is the case, configure another authentication mechanism (any mechanism is allowed) as the main authentication method, and configure external as a supplementary authentication method.

Configuring external authentication



You can configure external authentication by using the configuration tool or the command line.

Procedure

- Use the configuration tool or the [config-external-auth](#) command to set up and enable the external authentication method.

Use the following information to set options:

Enable External Authentication (required)	Specifies whether the external authentication method should be enabled.
Declared authentication method	Select the authentication method used by the load balancer.

Source	<p>Attribute: Enter the name of the HTTP request attribute that contains the name of the authenticated user.</p> <p>Header: Enter the name of the HTTP request header that contains the name of the authenticated user.</p> <p>Cookie: Enter the name of the HTTP request cookie that contains the name of the authenticated user.</p> <p>Custom Authenticator: Enter the name of the class that implements the <code>com.spotfire.server.security.CustomAuthenticator</code> interface.</p> <p>Authentication Filter: Retrieves the user name from the <code>getUserPrincipal()</code> method of <code>javax.servlet.http.HttpServletRequest</code>.</p> <div data-bbox="917 804 959 846">  </div> <div data-bbox="1029 747 1460 909"> <p>The Authentication Filter API has been deprecated. Use the CustomAuthenticator API, the CustomWebAuthenticator API, or a custom login page instead.</p> </div>
Require TLS	Select yes for external authentication to be available for TLS connections only.
Allowed host (hostname or IP address)	A list of hostnames and/or IP addresses of the client computers that are allowed to perform external authentication. If no allowed hosts are specified, all client computers are permitted to perform external authentication.
Allowed IP:s (regular expression)	Add a regular expression that matches the IP addresses of remote hosts that are permitted to perform external authentication. The regular expression shall be written in the syntax supported by <code>java.util.regex.Pattern</code> .
Name filter expression (optional)	<p>A regular expression that can be used to filter the user name that is extracted from the specified request attribute. The value of the regular expression's first capturing group will be used as the new user name.</p> <div data-bbox="917 1669 959 1711">  </div> <div data-bbox="1029 1617 1460 1778"> <p>One use of this feature is to remove the domain names in cases where Spotfire Server is configured to collapse the domains into one single domain within the server.</p> </div> <p>For example, if the attribute contains "domainname\username", you can use the regular expression <code>".*\\"(.*)"</code> to remove "domainname\".</p>

Lower case conversion (optional)

Specifies whether to convert the propagated user name to lowercase. The default is not to convert to lowercase.

External directories and domains

You can configure Spotfire Server to integrate with external directories such as LDAP directories or Windows domains.

Spotfire Server keeps track of which domain every user belongs to. Users who are created by an administrator directly within Spotfire Server belong to the SPOTFIRE domain. When the user directory is configured for **Database**, this is the domain being used.

External users keep their domain name from the external directory, and the domain name appears as part of their user name throughout the Spotfire interface.

The supported external directories can have domain names in two forms:

- DNS domain names, for example "research.example.com". A complete user name looks like this: someone@research.example.com.
- NetBIOS domain names, for example "RESEARCH". A complete user name looks like this: RESEARCH\someone.

When configuring Spotfire Server, the desired domain name style must be set before the server is started for the first time. The domain name style to use is dependent on the combination of authentication method and user directory of your Spotfire implementation.



Be careful when selecting a domain name style for your system; it will affect what information Spotfire Server stores within the Spotfire database. The domain name style can be changed using the [switch-domain-name-style](#) command if the user directory is in LDAP mode and is synchronizing with an Active Directory Server. For other user directory modes, there are no tools to alter that information if the domain name style later needs to be changed.

Below is a matrix showing which domain name style to use for different combinations of authentication method and user directory. Combinations that are not supported are marked " — ".

Spotfire Server will warn and even refuse to start if you try to set up an authentication method and a user directory with incompatible domain name styles. If you for some reason need to go ahead with an officially incompatible configuration, you will need to set the **allow incompatible domain name styles** configuration property to make the server start at all. One way to handle this could be a custom post-authentication filter that creates a bridge between the two originally incompatible domain name styles. (The **allow incompatible domain name styles** option can be set using the [config-userdir](#) command. For information about custom post-authentication filters, see [Post-authentication filter](#).)

Collapse Domains Configuration Property Enabled

User directory type				
Authentication method	Database	LPAD/AD	LDAP/other	Windows NT
Basic database	NetBIOS(DNS)	—	—	—
Basic/LDAP/AD	NetBIOS(DNS)	NetBIOS(DNS)	NetBIOS(DNS)	—
Basic/LDAP/other	NetBIOS(DNS)	NetBIOS(DNS)	NetBIOS(DNS)	—

User directory type				
Authentication method	Database	LPAD/AD	LDAP/other	Windows NT
Basic/Windows NT	—	—	—	NetBIOS(DNS)
NTLM	NetBIOS(DNS)	NetBIOS(DNS)	NetBIOS(DNS)	—
Kerberos	NetBIOS(DNS)	NetBIOS(DNS)	NetBIOS(DNS)	—
X.509 Client Certs.	NetBIOS(DNS)	NetBIOS(DNS)	NetBIOS(DNS)	—

— Unsupported combination of authentication method and user directory.

Collapse Domains Configuration Property Not Enabled

User directory type				
Authentication method	Database	LPAD/AD	LDAP/other	Windows NT
Basic database	NetBIOS, DNS	—	—	—
Basic/LDAP/AD	NetBIOS, DNS	NetBIOS, DNS	#	—
Basic/LDAP/other	NetBIOS, DNS	#	DNS	—
Basic/Windows NT	—	—	—	NetBIOS, DNS
NTLM	NetBIOS, DNS	NetBIOS, DNS	#	—
Kerberos	NetBIOS, DNS	NetBIOS, DNS	DNS	—
X.509 Client Certs.	NetBIOS, DNS	NetBIOS, DNS	DNS	—



NetBIOS is the recommended domain name style, but DNS will also work.

— Unsupported combination of authentication method and user directory.

For this combination of authentication method and user directory, enable the collapse domains option.

A consequence of the new domain tracking is that users may have to provide the domain names as part of their user names when logging in to Spotfire Server. For the Basic/LDAP and Basic/Windows NT authentication methods, the setting of the wildcard domain configuration property decides how the server maps a user to a domain during authentication. When the wildcard domain configuration property is enabled (this is the default), Spotfire Server checks whether the user name contains a domain name, and if it does, that domain name is used. If not, the server attempts to authenticate the user with the provided user name and password in every domain it knows about, until the combination of domain name, user name, and password results in a successful authentication, or until there are no

more domain names to try. If the wildcard domain configuration property is turned off, the domain name must be specified by the user unless it belongs to the configured default domain. This can be configured in the configuration tool.



If the wildcard domain configuration property is enabled and two identically named users in different domains have the same password, there is a risk that the wrong account will be selected when one of these users logs in. Thus, if security has a higher priority than user convenience, make sure to turn off the wildcard domain configuration property. There is also the risk that multiple authentication attempts will lock out the "correct" user.

Spotfire Server provides a configuration property that reverts to the behavior from previous releases. The configuration property is called `collapse-domains` and enabling this means that the external domain of a user is essentially ignored, and that different users with the same user name, but in different domains, will share an account on Spotfire Server. When the collapse domains configuration property is enabled, all external users and groups will be associated with the SPOTFIRE domain, regardless of which domain they belong to in the external directory.

If you want to keep running Spotfire Server without ever caring about domain names, enable both the `collapse-domains` and `wildcard-domain` configuration properties. Doing so will ensure that all users belong to the internal SPOTFIRE domain, and no users will have to enter a domain name when logging in. (The `collapse-domains` configuration property can be set in the configuration tool or by using the `config-userdir` command).



All users will belong to one domain when the `collapse-domains` configuration property is enabled. If there are multiple users with the same account name in different external domains, they will now effectively share the same account within Spotfire Server. If security has a higher priority than user convenience, make sure not to enable the collapse domain configuration property.



It is not recommended to change the `collapse-domains` configuration property after once having synchronized Spotfire Server with an external directory. This creates double accounts with different domain names for every synchronized user and group in the user directory. The new accounts do not inherit the permissions of the old accounts.

LDAP synchronizations

You can schedule when Spotfire Server synchronizes its user directory with LDAP directories. Both users and groups are synchronized in the background, and user and group look-ups query the Spotfire database rather than the LDAP directory.

There are two algorithms that can be used when configuring the recurrence of synchronization tasks: one is based on cron schedules and the other on sleep time between synchronizations.

Sleep time is only used when no cron schedule exists for the LDAP configuration. The sleeping period is configurable and by default it is set to 60 minutes.

New configurations have two default cron schedules: "restart" and "daily". "Restart" runs synchronization at each restart of Spotfire Server; "daily" runs synchronization once a day (at midnight server time). Upgraded configurations may not have these default cron schedules.

Each LDAP configuration has its own schedules. It is possible to use cron schedules for one LDAP configuration and sleep time for another.

User synchronization

By default, the user directory only synchronizes users (not groups) from the LDAP directories.

After an LDAP user has been synchronized and imported to the user directory, the user account becomes a permanent part of the user directory. If the LDAP user is later removed from the LDAP directory, the corresponding user account in the user directory is disabled. Disabled accounts remain visible in the Spotfire system but the user cannot log in.

To prevent user accounts from being disabled by failed synchronization attempts, for example caused by network errors, the `safe-synchronization` option can be enabled. When this option is enabled, no

user accounts are disabled solely because they could not be found during synchronization. By default, this option is not enabled because of the potential security issues.



It is usually not possible to log in as a removed LDAP user anyway because the LDAP directory blocks the authentication attempt if it is also responsible for authenticating users.

User accounts may also be explicitly disabled in the LDAP directories. In this case the user accounts are disabled in the user directory, regardless of the safe synchronization setting.

Group synchronization

Group synchronization mirrors in the user directory the group hierarchies that are in the LDAP directory.

When you set the `group-sync-enabled` option (in the `config-ldap-group-sync` command), the user directory synchronizes groups from the LDAP directory. Synchronizing groups relieves the administrator of the responsibility of managing group memberships. Assigning licenses and privileges to Spotfire groups is still accomplished in the Administrator Manager in Spotfire Analyst.

Synchronized LDAP groups cannot be manually modified in the user directory. Synchronized groups can be placed into manually created groups in the user directory, and thereby be granted permissions. If an LDAP group has been synchronized and it is removed from the list of groups to synchronize, it keeps the members from the last synchronization, but becomes an ordinary group that can be modified in Spotfire.



The user directory does not support cyclic group memberships, where the ancestor of a group is also a descendant of the same group. If the user directory detects a group membership cycle, it will be broken up arbitrarily.

When configuring the groups to be synchronized, specify either the group account names or the distinguished names. The account names and the distinguished names may contain an asterisk (*) as a wildcard character. This wildcard behaves just like the asterisk wildcard in standard LDAP search filters.

It is also possible to specify the distinguished name of an LDAP container containing one or more groups. All those groups will then be synchronized. It is possible to mix all variants.



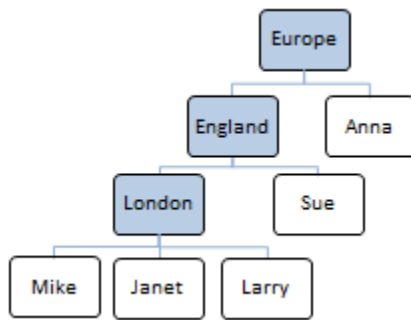
If the `Group synchronization enabled` configuration property is set and no groups or group context names are configured, the user directory synchronizes all groups that it can find in the configured context names.

The synchronized groups can also be used to filter the set of users that are synchronized with the user directory. By enabling the `filter-users-by-groups` option, only users that are members of at least one of the synchronized groups are synchronized with the user directory.

Group-based and role-based synchronization

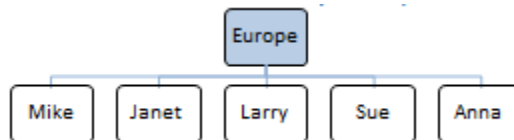
For Active Directory servers, Spotfire Server can synchronize groups. For the Directory Server product family, Spotfire Server can synchronize either groups or roles.

Here are examples of the default behavior of group-based and role-based group synchronization. The examples are based on the following figure:

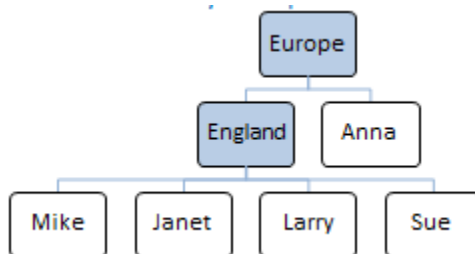


Group-based synchronization:

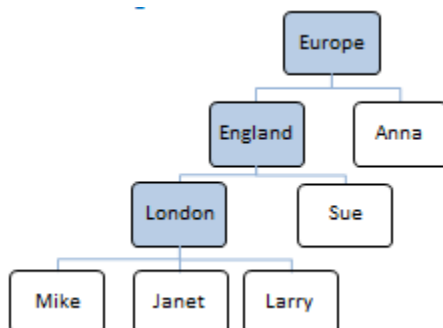
- If you only specify the group "Europe" to be synchronized in your LDAP configuration, the user directory synchronizes according to the figure below. The groups England and London will not be visible because they are automatically replaced with their members:



- If you specify the groups "Europe" and "England" to be synchronized in your LDAP configuration, the user directory will synchronize according to the figure below. The group London will not be visible, but will automatically be replaced with its members:

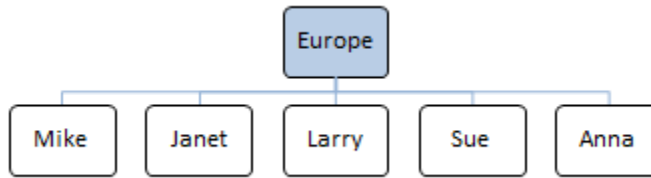


- If you specify the groups "Europe", "England", and "London" explicitly to be synchronized in your LDAP configuration, the user directory will synchronize according to the figure below:

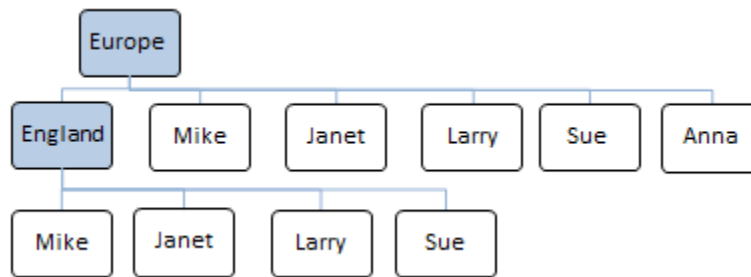


Role-based synchronization:

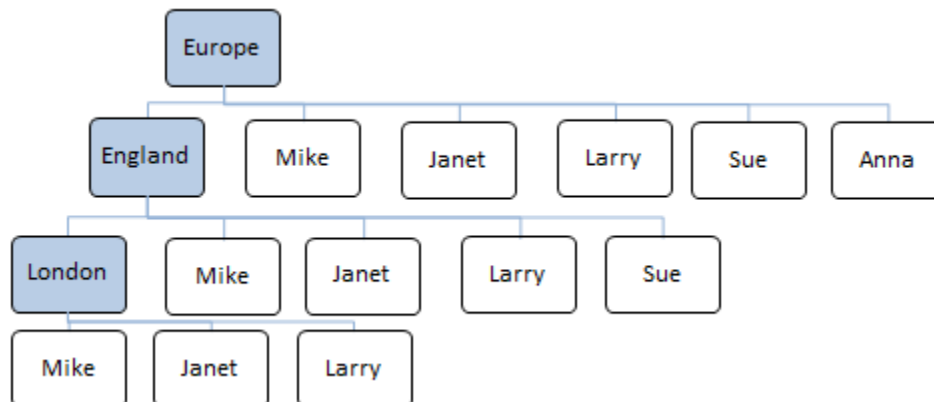
- If you only specify the role "Europe" to be synchronized in your LDAP configuration, the user directory will synchronize according to the figure below. The roles England and London will not be visible, but will automatically be replaced with their members:



- If you specify the roles "Europe" and "England" to be synchronized in your LDAP configuration, the user directory will synchronize according to the figure below. The role London will not be visible. Due to the nature of roles in the Directory Server product family, every role will automatically include all direct members as well as all members of sub roles:



- If you specify the roles "Europe", "England" and "London" explicitly to be synchronized in your LDAP configuration, the user directory synchronizes according to the figure below. Due to the nature of roles in the Directory Server product family, every role automatically includes all direct members as well as all members of sub-roles:



There are two algorithms to choose from when configuring group synchronization: the `memberOf` and the `member` algorithms.

- The `memberOf` algorithm relies on a calculated attribute in the LDAP directory and may induce more load on the LDAP servers. Not all LDAP directories support the `memberOf` algorithm.
- The `member` algorithm performs significantly more LDAP queries, but with much smaller result sets than the `memberOf` algorithm. See the recommendations below for group synchronization on different LDAP servers.

Recommendations

For Microsoft Active Directory server:

- Configure group-based synchronization with the `memberOf` algorithm.

For Sun Java System Directory Server (version 6 and later), do one of the following:

- Configure group-based synchronization with the `memberOf` algorithm.
- Configure role-based synchronization with the `memberOf` algorithm.

For Sun ONE Directory Server (version 5 and earlier), do one of the following:

- Configure role-based synchronization with the `memberOf` algorithm.
- Configure group-based synchronization with the `member` algorithm.



The following combinations do *not* work on Sun ONE Directory Servers:

- Configuring group-based synchronization with the `memberOf` algorithm.
- Configuring role-based synchronization with the `member` algorithm.

LDAP authentication and user directory settings

The following information is required to set up LDAP authentication and user directory mode, including LDAP group synchronization. Contact the LDAP directory administrator if you do not have the required information.

The following table provides an overview of LDAP settings and their applicability. Detailed descriptions of the settings are provided below the table.

- A: Applicable to LDAP as authentication mechanism
- UD: Applicable to LDAP User Directory mode
- GS: Applicable to LDAP User Directory mode with group synchronization
- M: Mandatory
- **: Required by configurations with LDAP server type **Custom**. These options have template values for the non-predefined LDAP server types. The template values can be overridden when necessary.

A	Authentication Attribute	Specifies the name of the LDAP attribute containing a user identity that can be used for authenticating with the LDAP server.
A U M D	LDAP Server Type	Specifies the type of LDAP server: ActiveDirectory, SunOne, SunJavaSystem, or Custom.
A U M D	LDAP Server URLs	A white-space separated list of LDAP server URLs.
A U M D	Context Names	A list of distinguished names (DNs) of the containers holding the user accounts to be visible within Spotfire Server.

A U D	Username The name of the LDAP service account to be used when searching for users and groups in the LDAP directory.
A U D	Password The password for the LDAP service account.
A U D	Security Authentication Specifies the security level to use when binding to the LDAP server. The default value is simple.
A U D	User Search Filter Specifies an LDAP search expression filter to be used when searching for users.
A U D	Referral Mode Specifies how LDAP referrals should be handled.
A U D	Username Attribute Specifies the name of the LDAP attribute containing the user account names.
A U D	Custom LDAP Properties Multiple key-value pairs specifying additional JNDI environment properties to be used when connecting to the LDAP server.
U D	Request Control Specifies the type of LDAP controls to be used when executing search queries to the LDAP server: Probe, PagedResultsControl, VirtualListViewControl or none.
U D	Page Size Specifies the page size to be used with the paged results control or the virtual list view control when performing search queries to the LDAP server. The page size value defaults to 1000 for both the paged results control and the virtual list view control.
U D	Import Limit Specifies a threshold that limits the number of users that can be imported from an LDAP server to Spotfire Server in one query.
U D	Synchronization Schedules Specifies a list of schedules for when the synchronization task should be performed.
G S	Group Synchronization Enabled Specifies whether or not group synchronization should be enabled for this LDAP configuration.

G S	Group Names	Specifies a list of distinguished names (DNs) of either individual groups to be synchronized or a context name where all groups are to be synchronized. If the group synchronization enabled option is set and the list of group names is empty, then all groups that can be found in the LDAP directory will be synchronized.
G * S *	Group Search Filter	Specifies an LDAP search expression filter to be used when searching for groups.
G * S *	Group Name Attribute	Specifies the name of the LDAP attribute containing the group account names
G * S *	Supports memberOf	Specifies whether or not the LDAP servers support a memberOf-like attribute on the user accounts that contain the names of the groups or roles that the users are members of. In general, this is true for all Microsoft Active Directory servers and all types of Sun directory servers.
G * S *	Member Attribute	For all LDAP servers with support for a memberOf-like attribute, this option specifies the name of the LDAP attribute on the user account that contains the names of the groups or roles that the user is a member of.
G * S *	Ignore Member Groups	Specifies whether or not the group synchronization mechanism should recursively traverse the synchronized groups' non-synchronized subgroups and include their members in the search result.

Authentication Attribute

Specifies the name of the LDAP attribute containing a user identity that can be used for authenticating with the LDAP server. This attribute fills no purpose in most common LDAP configurations, but can be useful in more advanced setups where the distinguished name (DN) does not work for authentication or where users should be able to log in using a username that does not map directly to an actual LDAP account. A typical case for using this option is when setting up SASL; see [SASL authentication for LDAP](#).

LDAP Server Type

Specifies the type of LDAP server. There are four valid types: ActiveDirectory, SunOne, SunJavaSystem, and Custom.

When specifying one of the predefined server types, we will assume that default values will be applied for the most fundamental configuration options. It is possible to override the default values. When specifying a Custom LDAP server type, there is no configuration template and all fundamental configuration options must be specified explicitly. The table above shows which configuration options are required for a Custom LDAP server type.

LDAP Server URLs

A whitespace-separated list of LDAP server URLs. An LDAP server URL has the format
`<protocol>://<server>[:<port>]`

- `<protocol>`: Either LDAP or LDAPS
- `<server>`: The fully qualified DNS name of the LDAP server

- `<port>`: An optional number indicating the TCP port the LDAP service is listening on. When using the LDAP protocol, the port number defaults to 389. When using the LDAPS protocol, the port number defaults to 636. Active Directory LDAP servers also provide a Global Catalog containing forest-wide information, instead of domain-wide information only. The Global Catalog LDAP service by default listens on port number 3268 (LDAP) or 3269 (LDAPS).

Spotfire Server does not expect any search base, scope, filter, or other additional parameters after the port number in the LDAP server URLs. Such properties are specified using other configuration options for this command.

Examples of LDAP server URLs:

LDAP://myserver.example.com

LDAPS://myserver.example.com

LDAP://myserver.example.com:389

LDAPS://myserver.example.com:636

LDAP://myserver.example.com:3268

LDAPS://myserver.example.com:3269

Context Names

A list of distinguished names (DNs) of the containers holding the LDAP accounts to be visible within Spotfire Server. When specifying more than one DN, the DN's must be separated by pipe characters (|). If the specified containers contain a large number of users, but only a few should be visible in Spotfire Server, a custom user search filter can be specified to include only the filtered users; see "User Search Filter", below.

Username

The name of the LDAP service account to be used when searching for users and groups in the LDAP directory. This service account does not need to have any write permissions, but it needs to have read permissions for all configured context names (LDAP containers). For most LDAP servers, the account name is the account's distinguished name (DN). For Active Directory, the account name can also be specified in the forms `ntdomain\name` or `name@dnsdomain`.

Examples:

CN=spotsvc,OU=services,DC=research,DC=example,dc=COM

RESEARCH\spotsvc (Active Directory only)

spotsvc@research.example.com (Active Directory only)

Password

The password for the LDAP service account.

Security Authentication

Specifies the security level to use when binding to the LDAP server. The default value is `simple`. Only use this parameter in special cases, and use it with care in production environments.

- To enable anonymous binding, it should be set to **none**.
- To enable plain user name/password authentication, it should be set to **simple**.
- To enable SASL authentication, it should be set to the name of the SASL mechanism to be used. Spotfire Server supports the two SASL mechanisms DIGEST-MD5 and GSSAPI. You can set multiple -C flags to set the additional JNDI environment properties that the SASL authentication mechanism typically requires

A typical case for using this option is when setting up SASL; see [SASL authentication for LDAP](#).

User Search Filter

This parameter specifies an LDAP search expression filter to be used when searching for users.

If only a subset of all the users in the specified LDAP containers should be allowed access to Spotfire Server, a restrictive user search filter can be specified. For instance, the search expression can be configured so that it puts restrictions on which groups the users belong to, or which roles they have.

- For Active Directory servers, the parameter value defaults to `objectClass=user`
- For 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=<firstDN>)(memberOf=<secondDN>))`. Add extra `(memberOf=<groupDN>)` sub-expressions as needed.

Example: `&(objectClass=person)(isMemberOf=cn=project-x,dc=example,dc=com)`

- For any version of the Sun Directory Servers, it defaults to `objectClass=person`.
- 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=<firstDN>)(isMemberOf=<secondDN>))`. Add extra `(isMemberOf=<groupDN>)` sub-expressions as needed.

Example: `&(objectClass=person)(isMemberOf=cn=project-x,dc=example,dc=com)`

- For the Directory Server product family, 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=<firstDN>))(nsRole=<secondDN>)`. Add extra `(nsRole=<roleDN>)` sub-expressions as needed.

Example: `&(objectClass=person)(isMemberOf=cn=project-x,dc=example,dc=com)`

The syntax of LDAP search expression filters is specified by [RFC 4515](#). Consult this specification for information about more advanced filters.

Referral Mode

This argument specifies how LDAP referrals should be handled. Valid arguments are follow (automatically follow any referrals), ignore (ignore referrals) and throw (fail with an error). The default and recommended value is follow.

Username Attribute

Specifies the name of the LDAP attribute containing the user account names. For Active Directory servers the value defaults to `sAMAccountName`. For the Directory Server product family with a default configuration, it defaults to `uid`.

Custom LDAP Properties

Multiple key-value pairs specifying additional JNDI environment properties to be used when connecting to the LDAP server. For instance, specifying the key `java.naming.security.authentication` and the value `simple` have the same result as setting the Security Authentication option to "simple".

Request Control

This option determines the type of LDAP controls to be used when executing search queries to the LDAP server. Valid controls are Probe, PagedResultsControl, VirtualListViewControl, and none.

The default behavior is to probe the LDAP server for the best supported request control. The paged results control is always preferred, since it provides the most efficient way of retrieving the result of the query. The virtual list view control can also be used to retrieve a large number of users, if the paged results control is not supported. The virtual list view control will automatically be used together with a sort control. Both the paged results control and the virtual list view control support a configurable page size, as specified by the page size option.

Page Size

This argument specifies the page size to be used with the paged results control or the virtual list view control when performing search queries to the LDAP server. The page size value defaults to 1000 for both the paged results control and the virtual list view control.

Import Limit

This argument specifies a threshold that limits the number of users that can be imported from an LDAP server to Spotfire Server in one query. This can be used to prevent accidental flooding of Spotfire Server's User Directory when integrating with an LDAP server with tens or even hundreds of thousands of users. By setting an import limit, the administrator can be sure that an unexpected high number of users won't affect the server's performance. 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. Leave this parameter untouched. in most cases.

Group Synchronization Enabled

Specifies whether or not group synchronization should be enabled for this LDAP configuration.

Group Names

Specifies the groups to be synchronized. Groups can be specified with either their account names or their distinguished names (DNs). The account names and the distinguished names may contain an asterisk (*) as a wildcard character. This wildcard behaves just like the asterisk wildcard in standard LDAP search filters. Wildcards work for both account names and distinguished names.

It is also possible to specify the distinguished name of an LDAP container containing multiple groups and thereby synchronizing all those groups. Wildcards can also be used for specifying group containers.

It is possible to mix all variants above. Consider the following when specifying a group to be synchronized:

- Specify either the group's account name or its distinguished name (DN). The account name must match the value of the configured group name attribute.
- It is possible to use an asterisk (*) as a wildcard character s in the account names when specifying group names. If a configured group name contains wildcard characters and matches multiple groups in the directory, all those groups will be synchronized.
- It is also possible to specify the distinguished name of an LDAP container containing one or more groups. All those groups will then be synchronized.
- It is possible to mix all variants.



If the enable group synchronization configuration property is set and the list of group names is empty, then all groups that can be found in the configured context names in the LDAP directory will be synchronized.

Synchronization Schedules

Specifies a list of schedules for when the group synchronization task should be performed. The schedules are specified in the cron format, where each schedule consists of either five fields or one shorthand label.

The five fields are, from left to right, with their valid ranges:

- minute (0-59)
- hour (0-23)
- day of month (1-31)
- month (1-12)
- day of week (0-7, where both 0 and 7 indicate Sunday)

A field may also be configured with the wildcard character (*), indicating that any moment in time matches this field. A group synchronization is triggered when all fields match the current time. If both day of month and day of week have non-wildcard values, then only one of them has to match.

There are also the following shorthand labels that can be used instead of the full cron expressions:

@yearly or @annually: run once a year (equivalent to 0 0 1 1 *)

@monthly: run once a month (equivalent to 0 0 1 * *)

@weekly: run once a week (equivalent to 0 0 * * 0)

@daily or @midnight: run once a day (equivalent to 0 0 * * *)

@hourly: run once an hour (equivalent to 0 * * * *)

@minutely: run once a minute (equivalent to * * * * *)

@reboot or @restart: run every time Spotfire Server is started

Refer to the [Wikipedia overview article on the cron scheduler](#).

Group Search Filter

This parameter specifies an LDAP search expression filter to be used when searching for groups.

- For Active Directory servers, the parameter value defaults to objectClass=group
- For Oracle Directory Servers and Sun Java System Directory Servers, it defaults to objectClass=groupOfUniqueNames
- For Sun ONE Directory Servers, it defaults to &(|(objectclass= nsManagedRoleDefinition)(objectclass=nsNestedRoleDefinition))(objectclass= ldapSubEntry)

Group Name Attribute

Specifies the name of the LDAP attribute containing the group account names:

- For Active Directory servers the value defaults to sAMAccountName
- For any version of the Sun directory servers with a default configuration, it defaults to cn

Supports memberOf

Specifies whether or not the LDAP servers support a memberOf-like attribute on the user accounts that contain the names of the groups or roles that the users are members of. In general, this is true for all Microsoft Active Directory servers and the Directory Server product family.

For some LDAP servers with configurations of type **Custom**, there is no memberOf-like attribute. This is declared by setting the supports memberOf configuration property to "false".

Member Attribute

This parameter value can be set to: memberOf, nsRole, or isMemberOf.

For LDAP configurations with the supports memberOf option set to false, the member attribute option specifies the name of the LDAP attribute on the group accounts that contains the distinguished names (DNs) of its members. In general, this includes LDAP servers with configurations of type Custom and any Sun ONE Directory Servers (version 5 and earlier) when used with group-based synchronization.

For LDAP configurations with the supports memberOf option set to "true", the member attribute option specifies the name of the LDAP attribute on the user accounts that contain the names of the groups or roles that the users are members of. In general, this includes all Microsoft Active Directory servers and all types of Sun Directory Servers version 6 and later. For Sun ONE Directory Servers (version 5 and older), this also applies for roles.

- For Microsoft Active Directory servers, the member attribute value defaults to memberOf.
- For Sun ONE Directory Servers, the member attribute option defaults to nsRole.

- For Sun Java System Directory Server version 6.0 or later, the member attribute option defaults to `isMemberOf`. To use the roles with the Sun Java System Directory Server or later, it is recommended to use the SunONE configuration template instead.



All configurations with the `memberOf` option set to "false" will use a far less efficient group synchronization algorithm that will generate more traffic to the LDAP servers, because Spotfire Server will first have to search for the distinguished names (DNs) of the group members within the groups, and then perform repeated lookups to translate the member DN to the correct account name.

Ignore Member Groups

This argument determines whether or not the group synchronization mechanism should recursively traverse the synchronized groups' non-synchronized subgroups and include their members in the search result.

For Microsoft Active Directory servers, the parameter value defaults to "false" so that all inherited group memberships are correctly reflected. For any version of the Sun Directory Servers, it defaults to "true" because the role and groups mechanisms in those servers automatically include those members.

Post-authentication filter

After a user's identity is validated, Spotfire Server performs an additional check using the *post-authentication filter*.

This filter has two built-in modes:

- **Block.** When the post-authentication filter is set to **Block**, it blocks all users who are not already present in the Spotfire Server user directory. This is the default mode, and the appropriate mode to use with an LDAP user directory.
- **Auto-create.** When the post-authentication filter is set to **Auto-create**, it automatically creates new accounts for any user who logs in to the server for the first time. This mode is valid only when the user directory mode is set to **Database**.

The blocking mode is the default mode. When it is used with a user directory in LDAP/Active Directory mode, it automatically transforms to the domain name of the authenticated user to match the configured domain name style.

The auto-creating mode is typically applied when using an LDAP directory or X.509 certificates for authentication together with the User Directory set up in database mode. The Post-authentication filter will create users with their external domain names, even though the user directory is in database mode, unless the collapse domains configuration property is enabled. This makes it possible to later switch to LDAP or Windows NT mode. If the collapse domains configuration property is enabled, the users will be created within the internal SPOTFIRE domain and it will not be possible to later switch to LDAP or Windows NT mode.

It is also possible to use the Spotfire Server API to create a custom post-authentication filter to perform additional validation. This filter must be installed in the `/tomcat/webapps/spotfire/WEB-INF/lib` directory on all servers. It is enabled using the [config-post-auth-filter](#) command. If a custom filter is used, it will be combined with the built-in filter, meaning that the filters will work together.

HTTPS

By default, Spotfire uses the HTTP protocol for communication between clients and Spotfire Server. To achieve a higher level of security, use the HTTPS protocol instead, ensuring encryption between clients and server.

HTTPS also includes a mechanism for clients to authenticate the server. To have the server authenticate the clients as well, you can enable X.509 client certificate authentication.

To enable encrypted communication using HTTPS, see [Configuring HTTPS](#).

To enable X.509 client certificate authentication, start with [Configuring HTTP](#) and then proceed to [Authentication using X.509 client certificates](#).

Configuring HTTPS

HTTPS ensures that the communication between clients and Spotfire Servers is encrypted.

Prerequisites

Obtain a server certificate and private key, stored in a Java keystore (JKS) or PKCS #12 keystore (P12/PFX).

Procedure

1. Stop Spotfire Server.
2. Copy the keystore file to the `<server installation dir>/tomcat/certs` directory. We suggest using the server's hostname as keystore filename.
3. Open the configuration file `<server installation dir>/tomcat/conf/server.xml` in an XML editor or a text editor and locate the section containing the configuration template for an HTTPS connector:

```
<!--
    <Connector port="443"
        maxHttpHeaderSize="65536"
        connectionTimeout="30000"
        enableLookups="false"
        URIEncoding="UTF-8"
        disableUploadTimeout="true"
        server="TIBCO Spotfire Server"
        compression="on"
        compressableMimeType="text/html,text/xml,text/plain,text/
css,application/json,application/javascript,image/svg+xml,application/xml"
        acceptorThreadCount="2"
        keepAliveTimeout="30000"
        maxKeepAliveRequests="-1"
        maxThreads="2000"
        SSLEnabled="true"
        scheme="https"
        secure="true">
        <SSLHostConfig certificateVerification="none"
            truststoreFile="./certs/[server hostname].jks"
            truststorePass="changeit"
            truststoreType="jks"
            sslProtocol="TLS"
            protocols="+TLSv1.2,+TLSv1.1,+TLSv1"
            honorCipherOrder="true"
            ciphers

            ...
            <Certificate certificateKeystoreFile="./certs/[server hostname].jks"
                certificateKeystorePassword="changeit"
                certificateKeystoreType="jks"
                certificateKeyAlias="[server hostname]" />
        </SSLHostConfig>
    </Connector>
-->
```

(In your installation, [server hostname] is replaced with the actual hostname of your server.)

4. Remove the lines with the comment markers `<!--` and `-->`.
5. Update the **certificateKeystoreFile** parameter with the name of the keystore file containing the server certificate and private key.
6. Set the **certificateKeystorePass** parameter to the password for the keystore file containing the server certificate and private key.
7. Set the **certificateKeystoreType** parameter to `jks` for a Java keystore or `pkcs12` for a PKCS #12 keystore.
8. If the keystore contains more certificates than the server certificate, the **certificateKeyAlias** parameter must be set to the alias for the server certificate and private key.

9. Unless you will enable X.509 client certificate authentication, remove the **truststoreFile**, **truststorePass**, and **truststoreType** parameters.
10. To disable unencrypted HTTP traffic, follow these steps:

1. Locate the section containing the default HTTP connector:

```
<Connector port="[HTTP port]"
maxHttpHeaderSize="16384"
connectionTimeout="30000"
enableLookups="false"
URIEncoding="UTF-8"
disableUploadTimeout="true"
server="TIBCO Spotfire Server" />
```

(In your installation, [HTTP port] is replaced with the HTTP port of your server.)

2. Add comment markers `<!--` and `-->` around the HTTP connector configuration:

```
<!--
<Connector port="[HTTP port]"
maxHttpHeaderSize="16384"
connectionTimeout="30000"
enableLookups="false"
URIEncoding="UTF-8"
disableUploadTimeout="true"
server="TIBCO Spotfire Server" />
-->
```

11. Start Spotfire Server.

Node manager installation

To be able to run services, you must first install and trust one or several node managers, depending on the expected workload. Node managers should not be installed on computers that are running Spotfire Server.

Currently the node manager is capable of running services with two different capabilities: Spotfire Web Player and Spotfire Automation Services.

The installation of the node manager creates a Windows service that runs as the LocalSystem account.



If you change the node manager service account, make sure that the account is a local administrator and that it has read and write access to the node manager installation directory and subdirectories.

There are two principal ways to install and trust a node manager:

- In an interactive installation, you run the `nm-setup.exe` file and then use the administrative tools in Spotfire Server to trust the node and install services and service instances. This is the most common method. For details, see [Installing a node manager interactively](#).
- In a silent installation, you run the installer from the command line. For details, see [Installing a node manager silently](#).

For administrators of large implementations who want to be able to quickly scale their Spotfire system as necessary, an automated method of installing and configuring services and service instances is available. For details, see [Automatically installing services and instances](#).

For more information, see [Nodes and services introduction](#).

Installing a node manager interactively

To make Spotfire Web Player and Spotfire Automation Services available to end users, you first must install a node manager. A Spotfire implementation can contain several nodes, but each one must be installed on a different computer.

Prerequisites

- Spotfire Server is installed and running.
- In the firewall of the computer on which you are installing the node manager, open the ports that will be used for the node manager and the services. (See [step 5](#) below for information on how these ports are used.)



This procedure is for an interactive installation, using the installation wizard. Alternatively, you can run a silent installation from the command line; for details, see [Installing a node manager silently](#).

Procedure

1. Double-click `nm-setup.exe`.



You may be prompted to install Microsoft .NET Framework at this point.

2. On the installation wizard Welcome page, click **Next**.
3. On the License page, read the agreement, select **I accept**, and then click **Next**.
4. On the Destination Folder page you can change the location if you want to, and then click **Next**.



The directory path must not contain spaces.

The Node Manager Ports page opens.

5. On the Node Manager Ports page, enter numbers (or leave the defaults) for the following ports:
 - **Node Manager registration port**—The port that is used to set up secure internal communication channels.



If you are installing the node manager on the same computer as Spotfire Server, this port must be different than the Spotfire Server back-end registration port. The default for the Spotfire Server port is 9080.

- **Node Manager communication port (TLS)**—The port that is used for secure (TLS) communication within the implementation.



If you are installing the node manager on the same computer as Spotfire Server, this port must be different than the Spotfire Server back-end communication port. The default for the Spotfire Server port is 9443.



The selected ports must be available and not blocked by a firewall.



To check whether a port is in use, on a command line enter `netstat -na`.

6. Click **Next**.
The Spotfire Server page opens.
7. On the Spotfire Server page, enter the following information, and then click **Next**.



These values must match the values you used when installing the Spotfire Server files.

- **Server name**—The hostname of Spotfire Server.



Valid hostnames may contain only alphabetic characters, numeric characters, hyphens, and periods.

- **Server backend registration port**—The registration port that you specified during Spotfire Server installation.
 - **Server backend communication port (TLS)**—The back-end communication port that you specified during Spotfire Server installation.
8. On the Network Names page, select the computer names that can be used by back-end trust. In general you can leave all the listed names as they are.
 9. On the Ready to Install page, click **Install**.

What to do next

After the installation wizard finishes running, you must start the new node manager manually; see [Starting or stopping a node manager \(as a Windows service\)](#).

Installing a node manager silently

To make Spotfire Web Player and Spotfire Automation Services available to end users, you first must install a node manager. A Spotfire implementation can contain several nodes, but each one must be installed on a different computer.

Prerequisites

- Spotfire Server is installed and running.
- In the firewall of the computer on which you are installing the node manager, open the ports that will be used for the node manager and the service instances.



To use the interactive installation wizard instead of the command-line installation, see [Installing a node manager interactively](#).

Procedure





1. Open a command line as an administrator.
2. Replace the parameters in the following code:



```
{Installer_Name} /s /v"/qn /l*vx TSS_NM_install.log INSTALLDIR=\"%{INSTALLDIR}\"
NODEMANAGER_REGISTRATION_PORT=%{NODEMANAGER_REGISTRATION_PORT}
NODEMANAGER_COMMUNICATION_PORT=%
{NODEMANAGER_COMMUNICATION_PORT} SERVER_NAME=%{SERVER_NAME}
SERVER_BACKEND_REGISTRATION_PORT=%
{SERVER_BACKEND_REGISTRATION_PORT} SERVER_BACKEND_COMMUNICATION_PORT=%
{SERVER_BACKEND_COMMUNICATION_PORT}
NODEMANAGER_HOST_NAMES=%{HOSTNAME}"
```

Example

```
nm-setup.exe /s /v"/qn /l*vx TSS_NM_install.log INSTALLDIR=\"%C:\tibco\tsnm\"
NODEMANAGER_REGISTRATION_PORT=83
NODEMANAGER_COMMUNICATION_PORT=84 SERVER_NAME=<SpotfireServerName>
SERVER_BACKEND_REGISTRATION_PORT=81
SERVER_BACKEND_COMMUNICATION_PORT=82
NODEMANAGER_HOST_NAMES=<NodeManagerHostNames>"
```

Silent installation parameters

Parameter	Description
INSTALLDIR	<p>The installation directory.</p> <p> The directory path must not contain spaces.</p>
NODEMANAGER_REGISTRATION_PORT	<p>Node manager registration port (Default: 9080) nodemanager.properties: nodemanager.cleartext.port</p> <ul style="list-style-type: none"> Port used for initial setup of internal secure communication channels. Needs only be accessible from Spotfire Server(s). <p> If you are installing the node manager on the same computer as Spotfire Server, this port must be different than the Spotfire Server back-end registration port.</p>
NODEMANAGER_COMMUNICATION_PORT	<p>Node manager communication port (TLS) (Default: 9443) nodemanager.properties: nodemanager.port</p> <ul style="list-style-type: none"> Port used for secure (TLS) internal communication within the environment. Needs only be accessible from Spotfire Server(s). <p> If you are installing the node manager on the same computer as Spotfire Server, this port must be different than the Spotfire Server back-end communication port.</p>
SERVER_NAME	<p>nodemanager.properties: nodemanager.supervisor</p> <ul style="list-style-type: none"> Must match the host name of the Spotfire Server. <p> Valid hostnames may only contain alphabetic characters, numeric characters, hyphens, and periods.</p>
SERVER_BACKEND_REGISTRATION_PORT	<p>Server backend registration port (Default: 9080) nodemanager.properties: nodemanager.supervisor.cleartext.port</p> <ul style="list-style-type: none"> Must match the registration port specified in the Spotfire Server installation.

Parameter	Description
SERVER_BACKEND_COMMUNICATION_PORT	<p>Server backend communication port (TLS): (Default: 9443)</p> <p>nodemanager.properties: nodemanager.supervisor.port</p> <ul style="list-style-type: none"> Must match the back-end communication port specified in the Spotfire Server installation.
NODEMANAGER_HOST_NAMES	<p>A comma-separated list of IP addresses, hostnames, and FQDN names that can be used by back-end trust. These should be for the interface(s) on the computer where the node manager is installed.</p> <div>  Valid hostnames may only contain alphabetic characters, numeric characters, hyphens and periods. </div> <div>  If you do not enter any values, the installer automatically provides values. After installation, confirm that these are correct in the [node manager installation dir]\nm\config\nodemanager.properties file. </div>

- Run the installation script.

What to do next

After installation, you must start the new node manager manually; see [Starting or stopping a node manager \(as a Windows service\)](#).

Starting or stopping a node manager (as a Windows service)

Start or stop the node manager Windows service from the Control Panel on the node manager computer.

Procedure

- Log in as an administrator to the computer on which the node manager is installed.
- Go to **Control Panel > Administrative Tools > Services** and then, in the Services dialog, locate and select the service called **TIBCO Spotfire Node Manager**.
- To the left of the services list, click **Start** in the phrase "Start the service" to start the node manager Windows service.



To stop the service, click **Stop** to the left of the services list.

Result

"Started" appears in the Status column.

What to do next

After starting a node manager you must indicate to the server that you "trust" it; see [Trusting a node](#).

Trusting a node

After installing the node manager, you must indicate in Spotfire Server that you trust the node.

Prerequisites

- You have followed the procedure [Installing a node manager](#).
- Both Spotfire Server and the newly-installed node manager are running.

Procedure

1. Log in to Spotfire Server. (For instructions on accessing the server, see [Starting Spotfire Server](#).)
2. Click **Nodes & Services**, and then click the **Untrusted nodes** tab.
3. Under **Untrusted nodes**, select the check box next to the new node manager and then click **Trust nodes**.
4. In the "Trust node" dialog, click **Trust**.

Result

After a pause, the new node appears on the **Your network** page when you select the **Nodes** view.

What to do next

[Set up services on the node](#)

Automatically trusting new nodes

To speed up the process of adding nodes to your Spotfire implementation, you can configure the system so that all new nodes are automatically trusted by Spotfire Server, or you can limit the automatic trust to specific nodes. In combination with the automatic process for installing services and instances, administrators of large Spotfire implementations in private sub-nets can quickly scale up their system as needed.

Prerequisites

- Spotfire Server is installed and running.
- In the firewall of the computer(s) on which you are installing the node manager, open the ports that will be used for the node manager and the services.

Procedure

1. Open a command line and export the active server configuration (the `configuration.xml` file) by using the [export-config](#) command; for additional information, see [Executing commands on the command line](#).

2. On the command line, enter the following command:

```
config set-config-prop --name=security.trust.auto-trust.enabled --value=true
```

This sets up automatic trust for all new nodes in the Spotfire implementation.

3. Optional: If you want to limit automatic trust to certain nodes, do one of the following:

- To allow one specific node to be automatically trusted, enter one of the following commands:

```
– config set-config-prop --name=security.trust.auto-trust.allowed-hosts-  
config.allowed-hosts.allowed-host --value=example.com
```

where *example.com* is the hostname of the node that will be automatically trusted.

- `config set-config-prop --name=security.trust.auto-trust.allowed-hosts-config.allowed-ip-regexps.allowed-ip-regexp --value=203\.0\.113\.1`
where `203\.0\.113\.1` is a regular expression for the IP address of the node that will be trusted.

- To allow several specific nodes to be automatically trusted, do the following:
 1. Open the `configuration.xml` file in an XML editor or a text editor and locate the `<auto-trust>` section.
 2. Enter an edited version of the following code under `<enabled>true</enabled>`:

```
<allowed-hosts-config>
  <allowed-hosts>
    <allowed-host>host1.example.com</allowed-host>
    <allowed-host>host2.example.com</allowed-host>
  </allowed-hosts>
  <allowed-ip-regexps>
    <allowed-ip>203\.0\.113\.1</allowed-ip>
    <allowed-ip>203\.0\.113\.2</allowed-ip>
  </allowed-ip-regexps>
</allowed-hosts-config>
```

where `hostn.example.com` is the hostname of a node that will be trusted, and `203\.0\.113\.n` is a regular expression for the IP address of a node that will be trusted. These lines can be repeated as often as necessary.



You can also specify a range of regular expressions. The following example allows any IP address between 203.0.113.0 and 203.0.113.255:

```
203\.0\.113\.\d{1,3}
```

3. Save and close the configuration file.
4. Import the configuration file back to the Spotfire database by using the `import-config` command.
5. Restart the Spotfire Server service.

Result

When a new node that is enabled for auto-trust comes online and requests authorization from Spotfire Server, the server trusts the node automatically.

Automatically installing services and instances

To quickly and automatically add services and instances to your Spotfire implementation whenever you add and trust a new node, you can prepare a node template file that is triggered when a new node manager comes online and is trusted. This method is most appropriate for large and growing Spotfire implementations.



If you are configuring an automated deployment in a private subnet, you may also want to automatically trust nodes; for details, see [Automatically trusting new nodes](#).

Prerequisites

- Spotfire Server is up and running.
- In the firewall of the computer on which you are installing the node manager, open the ports that will be used for the service instances.
- You have deployed client packages to Spotfire Server; for instructions, see [Deploying client packages to Spotfire Server](#).
- By default TLS 1.2 is not enabled on Windows Server 2008 R2. For communication to work between a service and Spotfire Server, TLS 1.2 must be enabled. To enable TLS 1.2 on Windows Server 2008 R2, see the section "For later versions of Windows" at <https://support.microsoft.com/en-us/kb/>

245030. For more information about TLS settings in Windows, see <https://technet.microsoft.com/en-us/library/dn786418.aspx>.

Procedure

1. Install and start the node manager(s) but do not trust them; for instructions, see [Node manager installation](#).
2. Open an XML editor or text editor and create a file that contains the following code:

```
{
  "services" : [ {
    "capability" : "WEB_PLAYER",
    "deploymentArea" : "Production",
    "configuration" : "Web Player Configuration",
    "customPrefix" : "Prefix",
    "resourcePool" : "Pool A",
    "instances" : 2,
    "port" : 9501
  }
],
  "strict" : "false"
}
```

3. Edit the default parameters as necessary:

Parameter	Description
capability	The service to install. Current options are WEB_PLAYER or AUTOMATION_SERVICES.
deploymentArea	Name of an existing deployment area.
configuration	<p>Name of an existing configuration (default or otherwise) that is available in the deployment area for the service being deployed.</p> <p>For information on creating new service configurations, see Manually editing the service configuration files.</p>
customName	Name of the new service. If present, this setting overrides any customPrefix setting. This parameter is optional.
customPrefix	Text to add before the name of the service. For example, if the customPrefix value is "Finance Dept.", the new Spotfire Web Player name will be "Finance Dept. Web Player". This parameter is optional.
resourcePool	For Spotfire Web Players, the name of a resource pool that the new instances will join. If the named resource pool does not exist, Spotfire Server creates it. This parameter is optional.
instances	Number of service instances to create. If no number is specified, only the service is created. This parameter is optional.

Parameter	Description
port	Communications port that the instances should use. This parameter is optional.
strict	Changing this parameter to "true" means that the installation will fail if any of the following parameters are not specified or are incorrect: <ul style="list-style-type: none"> • capability • deployment area • configuration



The text between the square brackets can be repeated as often as necessary in the file to create the required services and instances.

4. Name the file `default.conf` and place it in the following directory: `<node manager install directory>/nm/config/`
5. Trust the node manager; for instructions, see [Trusting a node](#).

Result

The services specified in the `default.conf` file are installed and the service instances start running.



After the file is processed, the file's name changes to `default.bak`.

What to do next

For information on the remaining setup tasks, see [Post-installation steps](#).

Login behavior configuration

You can configure various aspects of the Spotfire login dialog.

These are the behaviors that are configurable:

- If the login dialog should be displayed.
- If users should be allowed to work offline or if they always must log in.
- If users can select "Save my login information" in the login dialog and store the login information for future automatic login.
- If users should be forced to log in after working offline for a certain number of days.
- If you want an RSS feed to be shown in the login dialog.
- If users should be able to enter their own credentials in the login dialog.

To configure the login dialog, use the command [config-login-dialog](#).

To change the look and feel of the login dialog and other Spotfire windows, see the TIBCO Spotfire Cobranding help.



For cobranding to work on a Linux system, `cabextract` must be installed.

Enabling an RSS feed in the Spotfire login dialog

Spotfire Server can be configured to display messages to end users in the login dialog, such as news of upcoming scheduled maintenance. One option is to specify a path to an `rss.xml` file that is located on a

Spotfire Server; in this case the XML file is updated manually. The other option is to specify the URL to an external RSS feed.

Procedure

1. If you are using an `rss.xml` file that you will update manually, copy the file to the following directory: `<server install dir.>\tomcat\webapps\spotfire`.
2. Open a command-line interface and export the active configuration (the `configuration.xml` file) by using the `export-config` command. (For details on using the Spotfire command line, see [Executing commands on the command line](#).)
3. On the command line, use the `config-login-dialog` command to set up the feed.



Make sure that the specified RSS feed complies with the standard RSS 2.0 specification, and that the source is available to the end users' clients.



To enable all users see the news in the login dialog, set the display behavior setting (`-s value`) to "always". The login dialog will be shown to all users, even if they opt to save their login credentials for automatic login.

Example using a relative URL on the Spotfire Server:

```
config config-login-dialog -c C:\tibco\tss\tomcat\bin\configuration.xml -s
always -R "/spotfire/rss.xml"
```

4. Import the configuration file back to the Spotfire database by using the `import-config` command.
5. Restart the Spotfire Server service.

Service installation on a node

After installing and trusting a node manager, you configure and install services and service instances on the node.

For each service you install on the node, you select a capability, and the number of instances for that service, Spotfire Web Player or Spotfire Automation Services. For information on how to install a Spotfire Web Player service, see [Installing Spotfire Web Player instances](#). For information on how to install a Spotfire Automation Services service, see [Installing Spotfire Automation Services instances](#).

The services are automatically set up with a default configuration. You can edit the default configuration files manually to create your own service configurations. For more information on how to manually configure the services, see [Manually editing the service configuration files](#).

Preconfiguring Spotfire Web Player services (optional)

You can prepare one or several Spotfire Web Player configurations to apply to new services as you create them. This gives you access to an extended set of Spotfire Web Player options, and simplifies the task of setting up a group of services with identical properties.

Prerequisites

The Spotfire client distribution file (.sdn file) has been deployed to the server; for instructions see [Deploying client packages to Spotfire Server](#).

Procedure

- Follow the steps in [Manually editing the service configuration files](#).

Result

When you install a new Spotfire Web Player, you can select the customized configuration.

Installing Spotfire Web Player instances

After installing and authorizing a node manager, you install the Spotfire Web Player service and indicate the number of Spotfire Web Player instances that you want to make available. The Spotfire Web Player instances can then be accessed on any computer in the network.

Prerequisites

- You have installed and authorized a node manager; for instructions, see [Installing a node manager interactively](#) and [Trusting a node](#).
- Spotfire Server and the node manager are up and running.
- You have deployed client packages to Spotfire Server; for instructions, see [Deploying client packages to Spotfire Server](#).
- By default TLS 1.2 is not enabled on Windows Server 2008 R2. For communication to work between a service and Spotfire Server, TLS 1.2 must be enabled. To enable TLS 1.2 on Windows Server 2008 R2, see the section "For later versions of Windows" at <https://support.microsoft.com/en-us/kb/245030>. For more information about TLS settings in Windows, see <https://technet.microsoft.com/en-us/library/dn786418.aspx>.

Procedure

1. Log in to Spotfire Server and click **Nodes & Services**.
2. Under **Select a view**, select **Nodes**, and then select the node to which you want to add the Spotfire Web Player service. There should be a green circle with a check mark next to the selected node.
3. In the lower-right pane, click **Install new service**.
4. Make your selections in the "Install new service" dialog:
 - a) Under **Deployment area**, select the area you are using.

Administrators generally create a Test deployment area to use as a staging server.
 - b) Under **Capability**, select **Web Player**.
 - c) Under **Configuration**, select the service configuration that you want to apply to the service.

Spotfire Server contains a default service configuration that you can replace later. If you want to prepare a configuration file ahead of time, see [Preconfiguring Spotfire Web Player services](#).
 - d) Under **Number of instances**, enter the number of instances of the service that you want to make available. For more information, see [Multiple service instances on one node](#).
 - e) Under **Port**, you can change the default of 9501 if you want to.
 - f) Enter a name for this service.
5. Click **Install and start**.
To view the progress of the installation, click the **Activity** tab.

What to do next

- If applicable, install Spotfire Automation Services; for instructions, see [Installing Spotfire Automation Services instances](#).
- For information on the remaining setup tasks, see [Post-installation steps](#).

Multiple service instances on one node

Adding more than one Spotfire Web Player instance could be beneficial, particularly on large computers with NUMA architecture.

For failover reasons, it is recommended to have more than one instance in your environment. However, for failover reasons the instances do not have to be on the same node.

There are two main reasons for adding more service instances on the same node:

- If there are unstable analyses that are suspected to result in issues for the process, these analyses can be routed to one dedicated service instance using file routing rules. This isolates the analyses from other instances.
- A very large .NET heap may lead to long duration blocking garbage collections. By distributing analyses that lead to a large .NET memory footprint over more than one service instance, the .NET heap becomes smaller, which leads to quicker garbage collections.

There are two reasons to avoid using too many service instances:

- Each service instance requires some overhead, mostly in terms of memory usage but also some CPU usage.
- There is no data or document sharing between service instances.

You may want to experiment with fewer or more service instances, especially on large computers.

Preconfiguring Spotfire Automation Services (optional)

You can prepare one or several Spotfire Automation Services configurations to apply to new services as you create them. This gives you access to an extended set of Spotfire Automation Services options, and simplifies the task of setting up a group of services with identical properties.

Prerequisites

The Spotfire client distribution file (.sdn file) has been deployed to the server; for instructions see [Deploying client packages to Spotfire Server](#).

Procedure

- Follow the steps in [Manually editing the service configuration files](#).

Result

When you install a new Spotfire Automation Services, you can select the customized configuration.

Installing Spotfire Automation Services instances

After installing and authorizing a node manager, you can install Spotfire Automation Services and indicate the number of instances of this service that you want to make available. Spotfire Automation Services can then be accessed on any computer in the network.



All users that execute Automation Services jobs on the server, using the Job Builder or the Client Job Sender, must be members of the group Automation Services Users.

Prerequisites

- You have installed and authorized a node manager; for instructions, see [Installing a node manager](#) and [Trusting a node](#).
- Spotfire Server and the node manager are up and running.

- You have deployed client packages to Spotfire Server; for instructions, see [Deploying client packages to Spotfire Server](#).
- In Administration Manager in Spotfire Analyst you have assigned *licenses* required by the Automation Services jobs to the `automationservices@SPOTFIRESYSTEM` user, which is the account used to execute the jobs on the service instance.



For a description of the licenses, see the Administration Manager help.

- By default TLS 1.2 is not enabled on Windows Server 2008 R2. For communication to work between a service and Spotfire Server this must be enabled. To enable TLS 1.2 on Windows Server 2008 R2 see section "For later versions of Windows" on <https://support.microsoft.com/en-us/kb/245030>. For more information about TLS settings in windows see <https://technet.microsoft.com/en-us/library/dn786418.aspx>.

Procedure

1. Log in to Spotfire Server and click **Nodes & Services**.
2. In the **Nodes** view, select the node to which you want to add the Spotfire Automation Services service. There should be a green circle with a check mark next to the selected node manager. The words **Installed services** followed by the name of the node manager are displayed in the lower-right pane of the window.
3. Click **Install new service**.
4. Make your selections in the "Install new service" dialog:
 - a) Under **Deployment area**, select the area you are using.

Administrators generally create a Test deployment area to use as a staging server.
 - b) Under **Capability** select **Automation Services**.
 - c) Under **Configuration**, select the service configuration that you want to apply to the service.

Spotfire Server contains a default service configuration that you can replace later. If you want to prepare a configuration file ahead of time, see [Preconfiguring Spotfire Automation Services](#).
 - d) Under **Number of instances**, enter the number of instances of the service that you want to make available.
 - e) Under **Port**, you can change the default of 9501 if you want to.
 - f) Enter a name for this service.
5. Click **Install and start**.
To view the progress of the installation, click the **Activity** tab.

What to do next

For information on the remaining setup tasks, see [Post-installation steps](#).

Automation Services Job Builder and Client Job Sender

Spotfire Automation Services includes the Job Builder tool for creating multi-step jobs, and the Client Job Sender tool for automating jobs that are created in the Job Builder.

The Job Builder requires no installation. It is accessed from Spotfire Analyst.

The Client Job Sender must be installed and then configured to communicate with the Spotfire Server. The job execution schedule is set by using Windows Task Scheduler.

For more information, see the Spotfire Automation Services User's Guide.

Sites

You can create multiple Spotfire environments that share the same Spotfire database, including the library and user directory. These environments, which are called sites, can be configured to reduce latency for multi-geographic deployments. Sites also enable the use of a variety of authentication methods, along with different user directories, within the same deployment.

Each site includes one or more Spotfire Servers along with their connected nodes and services. A site's servers, nodes, and services can only communicate within the site, but because the Spotfire database is shared among the sites, all of the sites have access to the users, groups, and library in your Spotfire implementation.

If the site will contain more than one server, clustering must be enabled for that site; for more information, see [Clustered server deployments](#).



All the sites in an implementation must use the same clustering method.

You assign a Spotfire Server to a site when bootstrapping the server. You can change the assignment afterwards by following the instructions in [Moving a server and its nodes to a different site](#). When you assign a Spotfire Server to a site, any nodes that are connected to the server are automatically included in the site.

As of Spotfire version 7.9, all upgraded servers and nodes belong to the Default site. To assign the upgraded components to a site that you created, use the procedure [Moving a server and its nodes to a different site](#).

The potential reduced latency occurs between the servers and the service instances within a site, resulting in quicker manipulation of data that is already present in the site. To optimize the end-user experience, a best practice when configuring sites is to create scheduled updates so that data and analyses are downloaded from the database before users request them. For more information, see [Scheduled updates to analyses](#).

These are typical uses of Spotfire sites:

- To route user requests from a particular office to the servers and nodes that are physically closest to that office. This reduces the impact of network latency between servers that are located in different geographic regions.
- To enable different authentication methods for different sets of users who share a Spotfire implementation. For example, internal users may use Kerberos authentication while external users such as customers and partners may use username and password authentication.

Administrators who oversee several sites can switch sites from the landing page of the administration interface.

In a deployment that contains sites, the following items are site specific and not shared with any other sites:

- Nodes
- Resource pools
- Schedules
- Scheduled updates and routing rules
- Authentication can be configured to be site specific; see [Setting different authentication methods and user directories for sites](#).
- Public address; set a site's public address when creating the site, or later by using the [set-public-address](#) command.

The following items are "global", so shared among all the sites in a deployment:

- Library
- User directory
- Groups
- Deployments
- Server configuration file
- Service configuration files
- LDAP synchronization
- Signing certificates
- Login page RSS feed

Creating sites

Sites are created on the command line, and then you assign a server to a particular site when you bootstrap the server. In the case of a server that has previously been installed and configured, use the **set-site** command to assign it to a site.

For general information about sites, see [Sites](#).

Procedure

1. Open a command line as an administrator and go to the <server installation directory> \tomcat\bin directory.
2. Run the [create-site](#) command.



It is recommended to specify the public address (the **-a** parameter) when creating a site. If you do not specify the public address now, you can do it later by using the [set-public-address](#) command.

Example

```
config create-site -s MySite -a https://server.example.com/
```

where:

MySite is the name of the site you create.

[https://server.example.com/](#) is the public address of the site (optional).



When using the default port (80 for HTTP, 443 for HTTPS), do not specify the port in the public address.

Setting different authentication methods and user directories for sites

You can configure the sites in your implementation to use different authentication methods and, if necessary, different user directories.

Prerequisites

You have created the sites; for instructions, see [Creating sites](#).

For general information about sites, see [Sites](#).

Procedure

1. On any server computer in the implementation, open a command line as an administrator and export the active configuration by using the [export-config](#) command. For additional information on using the command line, see [Executing commands on the command line](#).
2. To set different authentication methods, do the following:
 1. To set the global authentication method, run the [config-auth](#) command without specifying a site.
 2. To set a different authentication method for a site, run the [config-auth](#) command, specifying the site.

Example

In this example, all of the sites will use LDAP authentication except for the "Tokyo" site, which will use Kerberos.

```
config config-auth -a BASIC -l
```

```
config config-auth -a KERBEROS -s Tokyo
```

3. If all the sites will not use the same user directory, run the [config-userdir](#) command in a similar manner.
4. Import the configuration file by using the [import-config](#) command.
5. Restart the servers.

Moving a server and its nodes to a different site

When moving a server and its nodes from one site to another site, you must edit the `nodemanager.properties` file for each node. This procedure should also be used to move upgraded servers and nodes from the Default site to a site that you created.

Prerequisites

You have created the site to which you want to assign the server; for instructions, see [Creating sites](#).

For general information about sites, see [Sites](#).

Procedure

1. Stop the server and its nodes. For instructions, see [Start or stop Spotfire Server](#) and [Starting or stopping a node manager](#).
2. Assign the server to the new site by using the [set-site](#) command:
 1. On the computer that is running the server, open a command line as an administrator and go to the `<server installation directory>\tomcat\bin` directory.
 2. Run the [set-site](#) command.

Example

```
config set-site -n 1234abcd-ab1-1a23-1234-ab1234c5678 -s Tokyo
```

where:

-n value is the ID of the server.

-s value is the name of the site to which you want to assign the server.



If you do not know the ID of the server, use the [list-nodes](#) command to find the IDs of all the servers and nodes in the environment.

3. Start the server. (Do not start the node managers.)

4. Do the following for each node that is connected to the server:

1. Open the following file in a text editor or XML editor: <node manager installation directory>\nm\config\nodemanager.properties.

Example of the nodemanager.properties file:

```
#Supervisor changed
#Wed Feb 16 22:27:19 CET 2017
nodemanager.host.names=Comp_A,10.101.10.10
nodemanager.communication.port=9443
server.backend.registration.port=9080
nodemanager.registration.port=9080
nodemanager.host=
server.name=Comp_12
nodemanager.supervisor.known=Comp_C:9443-9080,Comp_D:9443-9080,Comp_12:9443-9080
nodemanager.bundle.version=42.0.6127.7990
server.backend.communication.port=9443
```

The nodemanager.supervisor.known property lists the servers in the current site.

2. Delete the line that begins with nodemanager.supervisor.known.
3. Edit the server.backend.registration.port, server.name, and server.backend.communication.port to point to a Spotfire Server in the site to which you are moving.

Example of the edited nodemanager.properties file:

```
#Supervisor changed
#Wed Feb 16 22:27:19 CET 2017
nodemanager.host.names=Comp_A,10.101.10.10
nodemanager.communication.port=9443
server.backend.registration.port=9080
nodemanager.registration.port=9080
nodemanager.host=
server.name=Comp_5
nodemanager.bundle.version=42.0.6127.7990
server.backend.communication.port=9443
```

4. Save and close the file.
5. Start the node manager.

The nodemanager.supervisor.known property is added back into the nodemanager.properties file. It should contain the names of the servers in the new site.

5. In the administrative interface, verify that the node manager comes online in the correct site.



When you move a node, its service instances are removed from any resource pools they may have previously been assigned to.

Sites administration

Sites are administered in the same way as an ordinary Spotfire environment, with the difference that some features are global and some are site specific.

Because the Spotfire database is shared among all the sites, changes made in **Users & Groups** will be global, and affect all sites.

Communication between the Spotfire Server and the nodes only occurs within each site. For this reason, nodes, services, and routing are site specific and administered individually for each site. You can select which site to administer at the top of the Spotfire Server home page.

For general information about sites, see [Sites](#).

Deleting sites

Sites are deleted on the command line. If the site contains servers and nodes, you must specify a site to move them to.

Procedure

1. Stop the servers and node managers in the site that you want to delete. For instructions, see [Start or stop Spotfire Server](#) and [Starting or stopping a node manager](#).
2. Open a command line as an administrator and go to the <server installation directory> \tomcat\bin directory.
3. Run the `delete-site` command.
4. Restart any servers and node managers that were in the site.

Example

```
config delete-site -s "East Coast" -i "Default"
```

where:

East Coast is the name of the site to delete.

Default is the name of the site to which you want to move the deleted site's servers and nodes.

Connectors

With the connectors that are available in Spotfire, users can connect to, and analyze data from, a variety of data sources. This section describes how to configure the connectors for use in Spotfire Analyst, TIBCO Spotfire® Business Author, TIBCO Spotfire Consumer, and TIBCO Spotfire® Automation Services.

The following connectors are currently available:

- Amazon Redshift
- Apache Spark SQL
- Cisco Information Server
- Cloudera Hive
- Cloudera Impala
- Google Analytics
- Hortonworks
- HP Vertica
- IBM DB2
- IBM Netezza
- Microsoft SQL Server
- Microsoft SQL Server Analysis Services
- OData
- Oracle
- Oracle Essbase
- Oracle MySQL
- Pivotal Greenplum

- Pivotal HAWQ
- PostgreSQL
- Salesforce.com
- SAP BW
- SAP HANA
- Teradata
- Teradata Aster

Setting up connectors

Before you can use a data source connector on a Spotfire client, the connector must be installed on the server and the data source driver must be installed on the client computer.

Prerequisites

Client packages have been deployed to Spotfire Server. The connectors are included in the distribution file named `Spotfire.Dxp.sdn`. For information on package deployment, see [Deploying client packages to Spotfire Server](#).



After deployment, make sure to update the clients with the deployed packages. This is done by restarting any open Spotfire clients, logging in as usual, and then clicking **Update now**.

These are the additional required steps for setting up data source connectors.

Procedure

1. On the following computers, install the data source drivers that correspond to the connectors that will be used in your implementation:
 - All computers running Spotfire Analyst.
 - All computers running a node with Spotfire Web Players or Spotfire Automation Services for which connectors should be available.

For information about the required drivers and where to find them, see the system requirements at http://support.spotfire.com/sr_spotfire_dataconnectors.asp.



If you have installed a 32-bit version of the Spotfire Analyst, then you must use the 32-bit version of the data source driver. For Spotfire Web Player services, always use the 64-bit driver.

2. If the connectors should be available for users of Spotfire Web Players or in Spotfire Automation Services, additional configuration on the server is necessary; see [Configuring connectors for use with web clients and Spotfire Automation Services](#).
3. Set the access rights for the users; for details, see [Access to the connectors](#).
4. Some connectors require additional configuration; see, for example, [Configuring the Google Analytics connector](#) and [Installing Oracle Essbase Client on client computers](#).

Configuring connectors for use with web clients and Spotfire Automation Services

If connectors should be available for users of Spotfire web clients, or in Spotfire Automation Services, some configuration on the Spotfire Server is necessary.

This is a suggested workflow; detailed descriptions for each step are available in separate topics.

Procedure

1. Optional: Create a configuration that the service will use, and assign it to the deployment area that the web clients or Automation Services use. For instructions, see [Preconfiguring Spotfire Web Player services \(optional\)](#) or [Preconfiguring Spotfire Automation Services \(optional\)](#), depending on the type of service that you are configuring.



If you have to configure the authentication mode for any of the deployed connectors, this step is required. See [Authentication modes](#) for more information.

2. Install a service and make sure to select the same deployment area as in [Step 1](#). For detailed instructions on installation of services, see [Installing Spotfire Web Player instances](#) or [Installing Spotfire Automation Services instances](#), depending on the type of service you are configuring.



If you created a configuration in [Step 1](#), select that configuration when you install the service.

3. After the service has been installed successfully, test that it is now possible to work with data from the connectors.

Note that some connectors require additional configuration. See for example [Configuring the Google Analytics connector](#) and [Installing Oracle Essbase Client on client computers](#).

Create an analysis in Spotfire Analyst, and configure connections with the connectors that should be available in the web clients. Then save the analysis to the library. Verify that you can successfully open the analysis in a web client.

Create a Spotfire Automation Services job with tasks that use the connectors that should be available for Spotfire Automation Services. Verify that you can run the job successfully.

Authentication modes

You may have to change the authentication mode for some connectors so that they are available for use with Spotfire web clients. This is done in the `Spotfire.Dxp.Worker.Host.exe.config` file.

To change the authentication mode for a connector on a Spotfire Web Player service, you must modify an existing configuration or create a new configuration and assign it to the deployment area on which the `Spotfire.Dxp.sdn` distribution file has been deployed. Instructions are available in [Preconfiguring Spotfire Web Player services \(optional\)](#), but details specific to the connectors are listed here.

- The authentication mode settings are located in the section `<Spotfire.Dxp.Data.Access.Adapters.Settings>`. To edit the configuration file, you must first export it from Spotfire Server using the [export-service-config command](#). For instructions, see [Preconfiguring Spotfire Web Player services \(optional\)](#).
- These are the available authentication modes:
 - Prompt
 - ServiceAccount
 - Kerberos
 - WebConfig

By default, all the connectors use the Prompt mode. To read more about the settings, see [Configuration file examples](#).

- If you are unsure of what a certain connector is called in the configuration file, see [Connector names in configuration file](#).

Connector configuration examples

By default, all Spotfire connectors are listed in the configuration file, `Spotfire.Dxp.Worker.Host.exe.config`, and all connectors use Prompt as authentication mode.

This is the connector section of the configuration file:

```
<Spotfire.Dxp.Data.Access.Adapters.Settings>
  <setting name="WebAuthenticationMode" serializeAs="Xml">
    <value>
      <adapters>
        <adapter name="Spotfire.SqlServerAdapter" mode="Prompt"/>
        <adapter name="Spotfire.TeradataAdapter" mode="Prompt"/>
        <adapter name="Spotfire.OracleAdapter" mode="Prompt"/>
        <adapter name="Spotfire.SsasAdapter" mode="Prompt"/>
        <adapter name="Spotfire.SapBwAdapter" mode="Prompt"/>
        <adapter name="Spotfire.EssbaseAdapter" mode="Prompt"/>
        <adapter name="Spotfire.CompositeAdapter" mode="Prompt"/>
        <adapter name="Spotfire.MySqlAdapter" mode="Prompt"/>
        <adapter name="Spotfire.NetezzaAdapter" mode="Prompt"/>
        <adapter name="Spotfire.PostgreSqlAdapter" mode="Prompt"/>
        <adapter name="Spotfire.VerticaAdapter" mode="Prompt"/>
        <adapter name="Spotfire.TeradataAsterAdapter" mode="Prompt"/>
        <adapter name="Spotfire.HanaAdapter" mode="Prompt"/>
        <adapter name="Spotfire.GreenplumAdapter" mode="Prompt"/>
        <adapter name="Spotfire.ImpalaAdapter" mode="Prompt"/>
        <adapter name="Spotfire.ClouderaHiveAdapter" mode="Prompt"/>
        <adapter name="Spotfire.SparkSqlAdapter" mode="Prompt"/>
        <adapter name="Spotfire.HortonworksAdapter" mode="Prompt"/>
        <adapter name="Spotfire.DB2Adapter" mode="Prompt"/>
        <adapter name="Spotfire.PivotalHdAdapter" mode="Prompt"/>
        <adapter name="Spotfire.ODataAdapter" mode="Prompt"/>
        <adapter name="Spotfire.RedshiftAdapter" mode="Prompt"/>
        <adapter name="Spotfire.SalesforceAdapter" mode="Prompt"/>
        <adapter name="Spotfire.GoogleAnalyticsAdapter" mode="Prompt"/>
      </adapters>
    </value>
  </setting>
</Spotfire.Dxp.Data.Access.Adapters.Settings>
```

The effect that a certain authentication mode has for users who are logging in to a web client depends on the authentication method that was selected for the connection in the analysis. All authentication alternatives are not available for all connectors.

Prompt

Prompt is the default authentication mode. When it is used, web client users are prompted for their username and password when they log in to analyses that contain connections.

Example: `<adapter name="Spotfire.SparkSqlAdapter" mode="Prompt"/>`

ServiceAccount

ServiceAccount is used as authentication mode for connectors that are configured for anonymous authentication (for example Cloudera Hive, Cloudera Impala, Hortonworks, and OData). Web client users are connected to the external data source using the computer account or dedicated user account that is running the node manager.

Example: `<adapter name="Spotfire.ClouderaHiveAdapter" mode="ServiceAccount"/>`

Kerberos

To use Kerberos as authentication method, the following must be true:

- Spotfire Server is configured to use delegated Kerberos.
- In the analysis' connection login dialog, Kerberos is selected as authentication method.

For more information about Kerberos configuration, see [Kerberos authentication](#).

Example: `<adapter name="Spotfire.SqlServerAdapter" mode="Kerberos"/>`

WebConfig

When WebConfig is used as authentication method, you can configure data sources in analyses so that web client users log in automatically with credentials stored in a credentials profile.

Example: `<adapter name="Spotfire.SparkSqlAdapter" mode="WebConfig"/>`

To use WebConfig authentication mode, you must add a credentials profile, which stores a username and password for authentication, in the web client configuration. This is done in the `DataAdapterCredentials` settings section in the configuration file [Spotfire.Dxp.Worker.Host.exe.config](#) file. See the next section, `DataAdapterCredentials`.

You must also specify the credentials profile in the connection data source in the analysis. If you do not specify a credentials profile in the analysis, then web client users must enter their credentials.

DataAdapterCredentials

If WebConfig is selected as WebAuthenticationMode, users log in with a credentials profile that is stored in the web client service configuration. A credentials profile consists of a profile name, a username, and a password. Optionally, you can specify a list of allowed servers and/or connectors in the allowed-usages element, which determines conditions for what you can use the credentials profile for. See [Spotfire.Dxp.Worker.Host.exe.config file](#).

```
<entry profile="profile_name">
  <allowed-usages>
    <entry server-regex="database\.example\.com" />
  </allowed-usages>
  <username>user</username>
  <password>password</password>
</entry>
```

In the example below, two credentials profiles have been added:

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

  <setting name="DataAdapterCredentials" serializeAs="Xml">
    <value>
      <credentials>
        <entry profile="Sales_Dept">
          <allowed-usages>
            <entry server-regex="database\.example\.com" />
          </allowed-usages>
          <username>EMEA\SalesUsers</username>
          <password>MySalesPassword</password>
        </entry>
        <entry profile="Executive">
          <allowed-usages>
            <entry server-regex="another-database\.example\.com" />
          </allowed-usages>
          <username>EMEA\ExecUsers</username>
          <password>MyExecPassword</password>
        </entry>
      </credentials>
    </value>
  </setting>

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

For integrated security, the username should be in the DOMAIN\user format as in the example with EMEA\SalesUsers and EMEA\ExecUsers. The profile is an arbitrary string.

To use the credentials profile for authentication in an analysis, enter the profile name in Spotfire Analyst, on the **Credentials** page of the Data Source Settings dialog. When a credentials profile is specified both in the configuration file and in an analysis in Spotfire Analyst, web client users are not prompted for username and password to the connection when they open the analysis. Instead, the username and password that are defined in the credentials profile of the configuration file are used to log in to the data source.

Connector names in configuration file

This list describes how to refer to the different connectors in the configuration file Spotfire.Dxp.Worker.Host.exe.config.

Official name	Name in configuration file
Amazon Redshift	RedshiftAdapter

Official name	Name in configuration file
Apache Spark SQL	SparkSqlAdapter
Cisco Information Server	CompositeAdapter
Cloudera Hive	ClouderaHiveAdapter
Cloudera Impala	ImpalaAdapter
Google Analytics	GoogleAnalyticsAdapter
Hortonworks	HortonworksAdapter
HP Vertica	VerticaAdapter
IBM DB2	DB2Adapter
IBM Netezza	NetezzaAdapter
Microsoft SQL Server	SqlServerAdapter
Microsoft SQL Server Analysis Services	SsasAdapter
OData	ODataAdapter
Oracle	OracleAdapter
Oracle Essbase	EssbaseAdapter
Oracle MySQL	MySQLAdapter
Pivotal Greenplum	GreenplumAdapter
Pivotal HAWQ	PivotalHdAdapter
PostgreSQL	PostgreSqlAdapter
Salesforce.com	SalesforceAdapter
SAP BW	SapBwAdapter
SAP HANA	HanaAdapter
Teradata	TeradataAdapter
Teradata Aster	TeradataAsterAdapter

Access to the connectors

After you configure the connectors, you must specify access rights to make the connectors available for users of any Spotfire client.

In Spotfire, the access rights to data from connectors are controlled by the following items:

- The data source authentication. See the official help for the data source of interest for more information. For a short summary of which authentication modes are available for a specific connector, you can view the help section for the connector in the *TIBCO Spotfire Analyst – User’s Guide*.
- The licenses enabled for the end user groups. Licenses are set in the Administration Manager in Spotfire Analyst. See the *TIBCO Spotfire Administration Manager – User’s Guide* for detailed instructions.

If the steps in [Configuring connectors for use with web clients and Automation Services](#) are performed on the Spotfire Web Player service, and an analysis using that connection is created, then users of Spotfire web clients can connect to the data source directly.

Installing Oracle Essbase Client on client computers

To use the Oracle Essbase connector, you must also install Oracle Essbase Client on each computer that will run the connector.

Prerequisites

Ensure that you have access to the appropriate Oracle Essbase Client installer and unzip any zipped files on your computer (for example, `ClientInstallers-11122.zip`).

For more information about the supported Oracle Essbase versions, see http://support.spotfire.com/sr_spotfire_dataconnectors.asp.

Procedure

1. In the extracted archive, locate the `EssbaseClient` directory containing the installation program `EssbaseClient.exe`.
2. Double-click `EssbaseClient.exe`.
3. Select the appropriate language and continue.
4. In the installer pane, click **Next**.
5. Make a note of the destination directory; you need it for creating the appropriate environment variables. Click **Next**.
6. In the **Custom Setup** pane, ensure that both **Essbase Client** and **Essbase Client C API** are selected to be installed before you click **Next**.



The Essbase Client C API is not selected by default. You must select it manually.

7. Click **Install**, and then click **Finish** when the installation is completed.



In the **Installed Programs** list of the Control Panel, you can find a listing for Oracle® Hyperion Essbase Client. Use this entry if you must uninstall Oracle Essbase. Also, remember to remove the created environment variables that are listed in [Creating environment variables](#).

Creating environment variables

You must create the required environment variables to access the Essbase Client C API.



The environment variables must be exactly as specified, and they must point to the correct paths. Make sure that no additional blank spaces are added.

Procedure

1. Open the **System Properties** of your computer. (On Windows 7 this is reached from **Control Panel > All Control Panel Items > System > Advanced system settings**.)
2. On the **Advanced** tab, click **Environment Variables**.
3. On client computers, under **System variables**, click **New**, and then create the variable `EPMHOME` and set its value to the home path for the Oracle Enterprise Management System (for example, `C:\oracle\Middleware\EPMSys11R1`).

This home path contains the directories `bin`, `bin-32`, `common`, and `products`.



It is recommended to always use System variables, if possible. For computers running Spotfire Web Player services or Spotfire Automation Services services, the environment variables must be defined as System variables.

4. Create the variable `ARBORPATH` and set it to the destination folder chosen in the installer (for example, `C:\oracle\Middleware\EPMSys11R1\products\Essbase\EssbaseClient` (or `%EPMHOME%\products\Essbase\EssbaseClient`)).
5. Create the variable `ESSBASEPATH` and set it to `%ARBORPATH%`.
6. Add the following to the `PATH` variable (or create the `PATH` variable): `%ARBORPATH%\bin;%EPMHOME%\bin;`

Configuring the Google Analytics connector

To enable the Google Analytics connector for use in web clients, you must create a new project in your Google Analytics instance to obtain the required `ClientID` and `ClientSecret`.

Procedure

1. Log in to <https://console.developers.google.com>.
2. Create a new project.
3. Enable the **Analytics API**.
4. Create credentials.
This will provide you with a client ID and a client secret.
5. Add the following hosts:
 - `http://localhost:55931/authorize/code`
 - `http://localhost:55932/authorize/code`
 - `http://<spotfire_server>/spotfire/wp/oauth2/code`

To learn more about how to work with these settings, refer to the online help in the developer's console .
6. Log in to Spotfire Analyst as a user with administrator rights.
7. Click **Tools > Administration Manager**.
8. On the **Preferences** page, click a group for which you want to enable Google Analytics connectivity.
9. On the **Preferences** tab, expand **Connectors** and click **GoogleAnalytics**.
10. Click **Edit**.
11. In the **ClientID** field, add the client ID obtained in [Step 4](#).
12. In the **ClientSecret** field, add the client secret obtained in [Step 4](#).

13. In the **LocalRedirectPorts** field, enter 55931, 55932.
14. In the Edit Preferences dialog, click **OK**.
15. In the Administration Manager, click **Close**.
16. For the settings to take effect, users must log out of Spotfire and then log in again.

Additional configuration

You can add to or change your Spotfire configuration by using the configuration tool or the command line, or by working directly in the configuration file.

Updating a server configuration in the configuration tool

You can change a Spotfire Server configuration by using the configuration tool.



If you cannot run the configuration tool on the Spotfire Server computer, see [Running the configuration tool on a local computer](#).

Procedure

1. Open the configuration tool and sign in.
2. On the **Configuration** tab, make your changes.
3. Click **Save**.
4. Restart Spotfire Server.

Updating a server configuration on the command line

You can change a Spotfire Server configuration by running a series of commands on the command line.

Procedure

1. Open a command line.
2. Run the [export-config](#) command to export the configuration from the Spotfire database to a configuration file; for additional information, see [Executing commands on the command line](#).

```
> config export-config configuration.xml
```

where "configuration.xml" is optional and the -f (--force) option is not applied.
3. Update the configuration in the configuration file using selected commands. Example:

```
> config config-auth --configuration=configuration.xml --auth-method=BASIC --jaas-database
```

where "--configuration=configuration.xml" is optional.
4. Run the [import-config](#) command to import the updated configuration file into the Spotfire database. Example:

```
> config import-config --comment="Switched to BASIC authentication using the Spotfire Database authentication source" configuration.xml
```

where "configuration.xml" is optional.
5. Restart the server(s).
6. Remove the configuration.xml file or restrict access to it.



Do not remove the bootstrap.xml file.

Manually editing the Spotfire Server configuration file

Before editing the Spotfire Server configuration file you must export its contents to an XML file.

Procedure

1. On the computer running Spotfire Server, open a command line as an administrator and change the directory to the location of the `config.bat` file (`config.sh` on Linux). The default location is `<installation_dir>/tomcat/bin`.
2. Export the active configuration to a `configuration.xml` file by using the [export-config](#) command. The `configuration.xml` file appears in your working directory.
3. Open `configuration.xml` in an XML editor or a text editor and make your changes.
4. When you've finished, save and close the file.
5. Upload the edited configuration file back to the Spotfire database by using the [import-config](#) command.
6. Restart the Spotfire Server service; for instructions, see [Start or stop Spotfire Server](#).

Result

The imported configuration becomes the active configuration for that server or cluster.

Manually editing the service configuration files

The service configuration files give you access to options that are not available in the Spotfire Server administrative interface. You can use the default configuration files as a template to create and import as many customized service configurations as your Spotfire implementation requires. You can then apply the customized configurations to new or existing Spotfire Automation Services or Spotfire Web Player services.

Procedure

1. On the computer running Spotfire Server, open a command line as an administrator and change the directory to the location of the `config.bat` file (`config.sh` on Linux). The default location is `<server installation_dir>/tomcat/bin`.
2. On the command line, export the service configuration that you want to modify from Spotfire Server by using the [export-service-config](#) command. Specify the service's capability and the deployment area, and optionally the configuration name.



By default, all new services receive a "Default" configuration. The properties of the default configuration cannot be changed, but you can edit the configuration files and import the resulting customized configuration with a specified name.



If you are editing a service configuration that has been applied to an existing service, you must verify the name of the active service configuration before you export it. If the name of the active configuration is not "Default", you must specify the name in the **export** command.

Example for exporting the "Default" Spotfire Automation Services configuration that is in the Production deployment area:

```
config export-service-config --capability=AUTOMATION_SERVICES --deployment-area=Production
```

Example for exporting a customized configuration:

```
config export-service-config --config-name=AutomationServicesConfiguration
```

The following configuration files are exported. By default, these files are saved to the `<server installation_dir>\tomcat\bin\config\root` directory.

- `Spotfire.Dxp.Worker.Automation.config` (for Automation Services only)
 - `Spotfire.Dxp.Worker.Core.config`
 - `Spotfire.Dxp.Worker.Host.exe.config`
 - `Spotfire.Dxp.Worker.Web.config`
 - `log4net.config`
3. Edit the exported configuration files in a text editor or XML editor. For details about these files, see [Service configuration files](#).
 4. On the command line, import the customized configuration file back into Spotfire Server and name the configuration by using the `import-service-config` command.



If the configuration to be imported was created from the default configuration, a name *must* be specified.



If you are editing already customized configuration files, specifying a name when importing will create a new service configuration. If you import the changed customized configuration without the `--config-name` parameter, the old customized configuration will be replaced.

```
config import-service-config --config-name=ServiceConfiguration
```

When you install a new service or edit an existing one, you can select the customized configuration.

5. Optional: To activate the customized configuration for an existing service, run the following command on the command line:

```
config set-service-config --service-id=value --config-name=ServiceConfiguration
```



Use the [list-services](#) command to obtain the service ID.



Activating the configuration for a Spotfire Web Player service causes its web clients to restart.

Viewing the name of the active service configuration

You can view the name of a service's current configuration in the Nodes & Services section of Spotfire Server.

Procedure

1. Log in to Spotfire Server and click **Nodes & Services**.
2. On the **Your network** page, under **Select a view**, click **Nodes**, and then select the service whose configuration name you want to view.
3. In the upper-right pane of the page, in the service information list, **Configuration** is the second entry from the bottom:

 Web Player Service HR	
ID	2b1f0459-d895-4e9d-a1a9-f1f6d83533ae
Status	Service installed successfully
Deployment area	Production
Version	7.8.0
Host	Server5A
Capability	Web Player
Number of instances	2
Default port	9501
Configuration	Default
Default resource pool	Unassigned

Service configuration files

There are four files that are used to configure the Spotfire Web Player service and Spotfire Automation Services. Together, these files form service configurations that can be applied to individual services in your Spotfire implementation



For information on working with these files, see [Manually editing the service configuration files](#). For information about the log4net.config file, see [Web Player service logs](#).


- [Spotfire.Dxp.Worker.Automation.config](#)
- [Spotfire.Dxp.Worker.Core.config](#)
- [Spotfire.Dxp.Worker.Host.exe.config](#)
- [Spotfire.Dxp.Worker.Web.config](#)

Spotfire.Dxp.Worker.Automation.config file

This configuration file is used for configurations that are specific to Automation Services .

Setting	Default value	Description
<Spotfire.Dxp.Automation>		
<automation>		
maxWaitTimeForTaskBackgroundJobToFinishSeconds	180	The number of seconds to wait for background thread execution to finish after the task finished executing.

Setting	Default value	Description
maxConcurrentJobs	-1	<p>The number of jobs that are allowed to execute in parallel. If 0 or less, this is set to the number of CPU cores on the machine.</p> <div>  <p>The number of executing jobs can be less than the specified value if the service instance is exhausted. For more information, see WebPlayer_AverageCpuLoadExhaustedLimit in Spotfire.Dxp.Worker.Host.exe.config file.</p> </div>
useKerberos	False	<p>Set to "True" to run Automation Services jobs as a specific Windows account when delegated Kerberos is enabled in the environment. If set to "False", jobs will be run using the node manager service account.</p> <p>To specify the Windows account, add the following section:</p> <pre><kerberosIdentity userName="domain\username" password="password" /></pre> <p>and specify the account username and password.</p>
</automation>		
</Spotfire.Dxp.Automation>		
<Spotfire.Dxp.Automation.Framework>		
<security>		
allowDeleteOfFilesModifiedLastMinutes	30	<p>The Send Email task can delete files after they have been sent. To avoid deleting files that should be kept, only files that have been created and modified in the timeframe specified in this setting can be deleted. The default value is 30 minutes. If set to "0", no files can be deleted. If set to "-1", all files can be deleted.</p>
<allowedFilePaths>		
allowAll	True	<p>By default, Automation Services tasks can read files from, and write files to any directory in the file system. Set this to False to only allow tasks to read from and write to directories specified in the <allowedFilePaths> section.</p> <div>  <p>To be able to restrict the allowed paths for custom tasks, the custom tasks must use the validation function in the Automation Services API.</p> </div>

Setting	Default value	Description
<code><add path="" /></code>		<p>Add an <code><add path="" /></code> row for each directory the Automation Services tasks should be allowed to read from and write to. Paths can be relative to the Automation Service installation directory on the node, local paths, or network paths. For example:</p> <pre> <allowedFilePaths allowAll="false"> <add path=".\\Temp\\" /> <add path="C:\\Temp\\" /> <add path="\\MyServer\\Spotfire Exported PDF\\" /> </allowedFilePaths> </pre> <p> Added allowed paths are compared to all directories and files starting with what was added. For example, if you add C:\\Temp as an allowed path, both the directory C:\\Temp\\ and a file called C:\\Tempfile.txt would be allowed. If you want to make sure that only a specific folder is allowed, add a backslash at the end, for example C:\\Temp\\.</p>
<code></allowedFilePaths></code>		
<code></security></code>		
<code></Spotfire.Dxp.Automation.Framework></code>		
<code><spotfire.dxp.automation.tasks></code>		
<code><smtp></code>		
port	25	The port to use when connecting to the SMTP server.
useTls	False	Set to "True" to use Transport Layer Security (TLS) when connecting to the SMTP server.
timeoutSeconds	100	The maximum number of seconds before the Send command times out.
useWindowsDefaultCredentials	False	Set to "True" to use the windows credentials of the account that executes the node manager when accessing the SMTP server. If username and password is set, this is not used.
username		The username to use when authenticating with the SMTP server.
password		The password to use when authenticating with the SMTP server.

Setting	Default value	Description
<code>useCertificates</code>	False	Set to "True" to use client certificates when accessing the SMTP server.
<code>storeLocation</code>		The store location to take the certificate from [CurrentUser LocalMachine].
<code>storeName</code>		The name of the store to take the certificate from [AddressBook AuthRoot CertificateAuthority Disallowed My Root TrustedPeople TrustedPublisher].
<code>serialNumber</code>		The serial number of the certificate.
</smtp>		
<saveAnalysis>		
<code>forceUpdateBehaviorManualWhenEmbeddingData</code>	True	Set to "True" to force embedding of data function-based data sources, such as On-demand.
</saveAnalysis>		
<preferences>		
<code>Spotfire.Automation.SendMail.SMTPHost</code>		Specify the SMTP Host for Email Notification.
<code>Spotfire.Automation.SendMail.FromAddress</code>		Specify the From Address for Email Notification.
<code>Spotfire.Automation.LibraryImport.TimeoutInSeconds</code>	300	Specify the timeout (seconds) for the library import operation for the Import Library task.
<code>Spotfire.Automation.LibraryExport.TimeoutInSeconds</code>	300	Specify the timeout (seconds) for the library export operation for the Export Library task.
</preferences>		
</spotfire.dxp.automation.tasks>		

Spotfire.Dxp.Worker.Core.config file


This configuration file specifies settings for the service's communication with the Spotfire Server, and if sections in configuration files should be encrypted.

Setting	Default Value	Description
cookies autoTransfer=""		Specify the cookies from the Spotfire Server that should be sent back on all requests in the format of a ; separated list, for example: "ARRAffinity;myCookie;myCookie2".
<authentication hostsToAuthenticate=" " >		<p>This setting is applicable only when the system is set up to use delegated Kerberos.</p> <p>Specify a list of trusted sites/servers that should be allowed to authenticate using Windows credentials. The Spotfire Server is automatically added to this list. Also, the top domain of the computer running this service is added to the list (serv1.b.x.com is added as *.x.com). Add other servers in the format of a ; separated list. To allow wildcard matches, start the host name with a star *.</p> <p>For example:</p> <p>*.a.x.com;serv1.b.x.com;*.y.com;server3</p> <p>This will match <Anything>.a.x.com OR serv1.b.x.com OR <Anything>.y.com OR server3.</p>
<cryptography>		
encryptConfigurationSections	True	Set to true to encrypt sections of configuration files containing sensitive information.



Setting	Default Value	Description
<code>protectSectionEncryptionProvider</code>	<code>DataProtectionConfigurationProvider</code>	Name of the algorithm used when sections are encrypted.
<code></cryptography></code>		

Spotfire.Dxp.Worker.Host.exe.config file

Settings in this configuration file affect both Web Player services and Automation Services.

Setting	Default Value	Description
<code><Spotfire.Dxp.Web.Properties.Settings></code> <code>></code>		
<code>ProxyUsername</code>		<p>If you need to use proxy handling for communication from the Web Player service or Automation Services to Spotfire Server, and the proxy server uses username and password authentication, specify the username in the value tags.</p> <div>  <p>To use these proxy authentication settings, you must also add a proxy section, including the proxy address, to setting <code><system.net><defaultProxy></code></p> </div>
<code>ProxyPassword</code>		If the proxy server uses username and password authentication, specify the password in the value tags.
<code>TibcoSpotfireStatisticsServicesURLs</code>		A list of URLs to Spotfire Statistics Services.
<code>TibcoSpotfireStatisticsServicesUsernames</code>		A list of user names for each of the URLs.
<code>TibcoSpotfireStatisticsServicesPasswords</code>		A list of passwords for each of the user names and URLs.

Setting	Default Value	Description
DataAdapterCredentials		<p>If WebConfig is selected as authentication method for a data connector, you must add at least one credentials profile with username and password information for authentication.</p> <p>In the data connections that will use the credentials profile for authentication, you must specify the name of the credentials profile.</p> <p>You can add multiple profiles with different credentials.</p> <p>Credentials profile reference</p> <p>Each credentials profile entry should be in this format:</p> <pre><entry profile="credentials_profile_name"> <allowed-usages> <entry server- regex="database\.example \.com" /> </allowed-usages> <username>my_username</ username> <password>my_password</ password> </entry></pre> <p>entry profile</p> <p>The name of the credentials profile.</p> <p>The name is used to select the credentials profile for authentication in connection data sources.</p> <p>allowed-usages</p> <p>A list of allowed servers and connectors. You can use the credentials profile for authentication only in connections to the allowed servers, or with the allowed connectors.</p> <p>If allowed-usages is empty, you can use the credentials profile for authentication in connections to any server.</p> <p>Enter allowed servers as regular expressions, in the following format:</p> <pre><entry server-regex="database \.example\.com" /></pre>


Setting	Default Value	Description
		<p>Make sure to specify the allowed servers as valid regular expressions. Values that are not valid regular expressions are ignored. If all servers are invalid, the credentials profile can be used in connections to any server.</p> <p> You can also enter allowed connectors. Then you can use the credentials profile for authentication in any connection that you created with that connector. For example:</p> <pre><entry connector-id="Spotfire.GoogleAnalyticsAdapter" /></pre> <p>You can also specify both a connector id and a server in one allowed-usages entry, to require a specific combination of connector and server. For example:</p> <pre><entry connector-id="Spotfire.SqlServerAdapter" regex="database\.example\.com"></pre> <p>username The username to use for authentication with the data source.</p> <p>password The password to use for authentication with the data source.</p> <p> Spotfire connectors only require that the user has read privileges in the database. When you create a credentials profile, a recommended practice is to use a database user that only has the minimum required privileges for reading the data that you want to analyze in Spotfire.</p>

Setting	Default Value	Description
<code>WebPlayer_AverageCpuLoadExhaustedLimit</code>	90	<p>If a service instance is exhausted, no new users will be routed to that instance. Specify the CPU load limit, in percent, that sets the state of the instance to exhausted.</p> <p>Set to -1 to disable the exhausted limit.</p> <p>Note that this setting is applicable to both Web Player services and Automation Services.</p>
<code>WebPlayer_AverageCpuLoadNotExhaustedLimit</code>	85	<p>Specify the CPU load, in percent, that the instance must get below to leave the exhausted state.</p> <p>Note that this setting is applicable to both Web Player services and Automation Services.</p>
<code>WebPlayer_AverageCpuLoadStrainedLimit</code>	50	<p>If a service instance is strained, new users will be routed to other instances that are not strained or exhausted. If all instances are strained, new users will be routed to the strained instance. Specify the CPU load limit, in percent, that sets the state of the instance to strained.</p> <p>Set to -1 to disable the strained limit.</p> <p>Note that this setting is applicable to both Web Player services and Automation Services.</p>
<code>WebPlayer_AverageCpuLoadNotStrainedLimit</code>	45	<p>Specify the CPU load, in percent, that the instance must get below to leave the strained state.</p> <p>Note that this setting is applicable to both Web Player services and Automation Services.</p>
<code>WebPlayer_AverageCpuLoadCountOnlyCurrentProcess</code>	False	<p>Set to true to only measure the CPU load created by the instance a user is routed to. If set to false, the CPU load will be measured for all instances on the node.</p> <p>Note that this setting is applicable to both Web Player services and Automation Services.</p>
<code></Spotfire.Dxp.Web.Properties.Settings></code>		

Setting	Default Value	Description
<Spotfire.Dxp.Internal.Properties.Settings>		
<Spotfire.Dxp.Application.Properties.Settings>		
Bookmarks_MinimumSynchronizationIntervalSeconds	60	Specify the minimum synchronization interval for bookmarks, in seconds.
WebServerPortAllocationCount	-1	Determines how many ports the internal web server shall bind to. All ports are bound on the loopback interface, localhost. The value for this setting should not be less than the value for ExportRendererCount. If a negative value is specified, this setting defaults to the number of processors on the machine.
WebServerPortFrom	-1	Determines the first (lowest) port that the internal web server shall attempt to bind to. If a negative value is specified, this setting defaults to 8000.
WebServerPortTo	-1	Determines the last (highest) port that the internal web server shall attempt to bind to. If a negative value is specified, this setting defaults to 65535.
ExportRendererCount	-1	Determines how many renderer processes are used to concurrently render pages for PDF export, etcetera. If a negative value is specified, this setting defaults to the number of processors on the machine.
ExportRenderingTimeout	-1	Determines the timeout, in seconds, of an export to PDF operation.
</Spotfire.Dxp.Application.Properties.Settings>		
<Spotfire.Dxp.Data.Properties.Settings>		

Setting	Default Value	Description
DataBlockStorage_MemoryLoadExhaustedLimit	98	If a service instance is exhausted, no new users will be routed to that instance. Specify the memory load limit, in percent, that sets the state of the instance to exhausted. Set to -1 to disable the exhausted limit.
DataBlockStorage_MemoryLoadNotExhaustedLimit	93	Specify the memory load, in percent, that the instance must get below to leave the exhausted state.
DataBlockStorage_MemoryLoadStrainedLimit	75	If a service instance is strained, new users will be routed to other instances that are not strained or exhausted. If all instances are strained, new users will be routed to the strained instance. Specify the memory load limit, in percent, that sets the state of the instance to strained. Set to -1 to disable the strained limit.
DataBlockStorage_MemoryLoadNotStrainedLimit	70	Specify the memory load, in percent, that the instance must get below to leave the strained state.
DataBlockStorageStorageIOSizeKB	64	This setting should not be edited, unless instructed by Spotfire Support.
DataOnDemand_MaxCacheTime	01:00:00	Specify the length of time, in the format HH:MM:SS, for data on demand to be cached. This setting is only used if you configured data on demand to be cached on the web clients.
AllowedFilePaths		Provide the full path to directories or files on a local disk that you want to access in the web clients. Specify each file or directory in a separate <string> tag.
</Spotfire.Dxp.Data.Properties.Settings>		
<Spotfire.Dxp.Data.Access.Properties.Settings>		
AllowCustomQueries	True	Enables custom queries for users on this service.

Setting	Default Value	Description
</Spotfire.Dxp.Data.Access.Properties.Settings>		
<Spotfire.Dxp.Data.Access.Adapters.Settings>		
WebAuthenticationMode	Prompt	<p>Specify the authentication method to use for connectors. Valid options are:</p> <p>WebConfig – Select this to make all users connect with the credentials specified in the Spotfire.Dxp.Web.Properties.Settings/DataAdapterCredentials section.</p> <p>Kerberos – Select this if your system is configured to authenticate users with Kerberos.</p> <p>Prompt – Select this to prompt the users for a username and password for the external data source.</p> <p>ServiceAccount – Select this to make all users connect to the external data source using the computer account or dedicated user account that is used to run the node manager.</p>
</Spotfire.Dxp.Data.Access.Adapters.Settings>		
<system.net>		



Setting	Default Value	Description
<defaultProxy>		<p>If you need to use proxy handling for communication from the Web Player service or Automation Services to Spotfire Server, you must add the following proxy setting inside the defaultProxy tag:</p> <pre><proxy proxyaddress="http:// MyProxyServer:3128" scriptLocation="MyScriptLocation" "/></pre> <p>The proxy setting is a part of the standard .NET Framework. You can find more information about this configuration at the Microsoft Developer Network (MSDN).</p> <p> If the proxy server uses username and password authentication, you must also specify the username and password for proxy server in the <Spotfire.Dxp.Web.Properties.Set setting.</p>
</system.net>		
<runtime>		These settings should not be edited unless instructed by Spotfire Support.
<startup>		These settings should not be edited unless instructed by Spotfire Support.
<system.web>		These settings should not be edited unless instructed by Spotfire Support.
<system.serviceModel>		These settings should not be edited unless instructed by Spotfire Support.

Spotfire.Dxp.Worker.Web.config file


This configuration file specifies Web Player service configurations, some Automation Services configurations, and user interface elements applicable to both the web clients and the library browser on Spotfire Server.



The settings in the sections <application>, <userInterface><pages>, <userInterface><closedAnalysis>, and <userInterface><errorPage>, and the setting maxReceivedMessageSizeMb, which sets the maximum size for file upload, are applicable both to the web client and the library browser on Spotfire Server. If these settings are changed, you must run the [set-service-config](#) command to apply the settings in the web client, and the [set-server-service-config](#) command to apply the settings in the library browser on Spotfire Server.

Setting	Default Value	Description
<spotfire.dxp.web>		
<setup>		
<javascriptApi>		
enabled	True	Controls whether the use of the JavaScript API is enabled or disabled.
domain		<p>Restricts from which domains it is possible to use the JavaScript API.</p> <p>By default, all domains are allowed. A non-empty domain whitelist indicates that only the listed domains can embed Spotfire files in their web site using the JavaScript API. The list is a comma-separated list of domain names.</p>
</javascriptApi>		
<errorReporting>		This section is applicable for both Web Player services and Automation Services.
emailAddress	""	<p>Specify the e-mail address for the Spotfire administrator. When a user encounters certain server related errors, a Report error to your administrator mailto link is displayed. If the user clicks the link, an e-mail addressed to the administrator, including the error log, is created in the default e-mail application.</p> <div>  <p>To apply this setting, you must enable it on the Spotfire Server by running the set-server-service-config command.</p> </div>
maxMailLength	1000	<p>Specify the maximum number of characters in the e-mail that is generated when a user clicks the Report error to your administrator link.</p> <div>  <p>To apply this setting, you must enable it on the Spotfire Server by running the set-server-service-config command.</p> </div>
includeDetailedError Information	False	Set to true to enable detailed error information, like call stacks in messages to end users. For security reasons this should not be enabled by default.

Setting	Default Value	Description
<code>enabledMiniDumpCreationOnError</code>	True	Create a mini dump file if the service goes down unintentionally.
<code>miniDumpPath</code>	" "	Specify the location where the mini dump file should be saved on the computer with the node manager installed. Leave this empty to save the mini dump file to the folder that contains the node manager log files.
<code>miniDumpSizeLarge</code>	False	Set to true to create a full dump. Note that this can create a very large dump file. This setting should not be edited unless instructed by Spotfire Support.
<code>dumpToolPath</code>	C:\Program Files (x86)\Windows Kits\10\Debuggers\x64\cdb.exe	A tool, such as cdb.exe, can be used to automatically capture dumps for hanging service instance processes. To use the cdb.exe tool to capture dumps, it must be installed. Search for "Windows Software Development Kit (SDK) for Windows" and install it. Make sure to include Debugging Tools for Windows when installing. Then verify that cdb.exe is located in this path.
<code>dumpToolFlagsSmall</code>	-c ".dump /mhttpFidcu {0};q" -p {1}	These flags will be used if <code>miniDumpSizeLarge</code> is set to False. For information on the flags, refer to the cdb.exe documentation.
<code>dumpToolFlagsLarge</code>	-c ".dump /ma {0};q" -p {1}	These flags will be used if <code>miniDumpSizeLarge</code> is set to True. For information on the flags, refer to the cdb.exe documentation.
</errorReporting>		
<languages>		This section is applicable for both Web Player services and Automation Services.
<installedLanguages>		This section should not be edited. The list of installed languages will be populated automatically.

Setting	Default Value	Description
<languageMappings>		You can define a mapping from a language preference configured by users in the browser to one of the languages installed on the service. For example, if your users have French (Canada) [fr-CA] as the highest preference language in their web browser, but the service uses French (France) [fr-FR], you can specify that [fr-FR] should be used even if the end users have not added [fr-FR] to their list of supported languages in the browser.
add browserLanguage		For each mapping from a browser language that is not directly supported, add a setting in the <languageMappings> section in the format: <add browserLanguage="en-GB" installedLanguageToUse="en-US"/>
</languageMappings>		
</languages>		
<sbdFCache>		In order to quickly create and share map chart visualizations that use geocoding tables, and to quickly open SBDF files from the library, it is possible to cache and preload the SBDF files stored in the library. The cache is an in-memory cache that keeps recently opened SBDF files from the library open. If files have not been accessed for a specified time, or if memory is low, they will be removed from memory. This section is applicable for both Web Player services and Automation Services.
enabled	True	Set to true to enable the cache.
cacheTimeoutMinutes		Specify the minimum time an SBDF file is stored in the cache. If the preload service is used, this should be a bit longer than the libraryCheckInterval setting.
<preloadSettings>		
enabled	False	Set to true to enable the preload service of SBDF files.  The cache must also be enabled for the preload service to work.

Setting	Default Value	Description
libraryCheckInterval Minutes	10	Specify how often the preloading service will check the library for new content.
librarySearch	MapChart.IsGeocodingTable::true AND MapChart.IsGeocodingEnabled::true	The search string that specifies which SBDF files to cache. The default search string specifies all geocoding tables in the library, you might want to restrict this in order to reduce memory consumption.
</preloadSettings>		
</sbdfCache>		
<scheduledUpdates>		
concurrentUpdates	2	The maximum number of concurrent updates that can be executed at the same time. This is used to limit resources used by the update mechanism. Min value is 1 and max value is 10.
updateIntervalSeconds	60	How often the service should check if any updates should be run. This is set in seconds. Min value is 30, and max value 3600 (=one hour).
useKerberos	False	<p>Set to true to run scheduled updates as a specific Windows account when delegated Kerberos is enabled in the environment. If set to false, schedule updates will be run using the node manager service account.</p> <p>To specify the Windows account, add the following section:</p> <pre><kerberosIdentity userName="domain\username" password="password" /></pre> <p>and specify the account username and password.</p>
customAccount		
<forcedUpdate>		
enabled	True	It is possible to force updates upon users even though the analysis is set to notify the users. This is useful if someone has left an analysis open for a long time and you want to avoid numerous versions of the analysis to be kept simultaneously. To enable forced updates set this key to true.

Setting	Default Value	Description
maximumRejectedUpdates	2	Specify the number of times a user can be notified of new updates without accepting them, before the update is forced on the user.
</forcedUpdate>		
<cacheSettings>		
enabled	False	<p>If the Web Player service is restarted, analyses that are scheduled to be pre-loaded will need to be reloaded. If the data used in the analyses take a long time to load, so will the analyses. Therefore, it is possible to cache data from scheduled analyses on disk to be able to reload the analyses faster on restart.</p> <p>Set this to <code>true</code> to enable caching of data on disk.</p>
path		Specify the path on disk where data is to be stored.
maxDiskSizeMb	0	Specify the maximum disk space used for the cached data. Set this to "0" (zero) to cache data without an upper limit.
maxAgeMinutes	1440	Specify how long a cache entry should be kept on disk if it has not been reloaded by scheduled updates.
</cacheSettings>		
</scheduledUpdates>		
<application>		
helpUrl		You can change the default help link for web client users to point to a locally stored help. Specify the location of the locally stored help here. To use this specified help link, you must also set the <code>useDefaultHelpUrl</code> setting to <code>False</code> .
useDefaultHelpUrl	True	Set this to <code>false</code> and specify a locally stored help in the <code>helpUrl</code> setting to change the target of the help link in the web client. To switch back to the default online web client help, set this to <code>true</code> again.
</application>		

Setting	Default Value	Description
</setup>		
<userInterface>		
<pages>		
showLogout	True	Specify if the Log out menu item is displayed. If <code>true</code> , the menu item is displayed in the top right menu of the web client.
showAbout	True	Specify if the About menu item is displayed. If <code>true</code> , the menu item is displayed in the top right menu of the web client.
showHelp	True	Specify if the Help menu item is displayed. If <code>true</code> , the menu item is displayed in the top right menu of the web client.
showUserName	True	Specify if the user name should appear in the web client user interface, for example in the Modified By section in the library browser and the Analysis Information dialog.
</pages>		
<diagnostics>		This section is applicable for both Web Player services and Automation Services.
errorLogMaxLines	2000	Specify the maximum number of lines from the error log files to display in Monitoring and diagnostics. The range is 1000 - 50000.
</diagnostics>		
<analysis>		
showToolTip	True	Specify if highlighting tooltips should be shown in visualizations in the web client. Setting this value to <code>false</code> will increase performance.
showClose	True	Specify if the Close menu item is displayed. If <code>true</code> , the menu item is displayed in the top right menu of the web client.
showToolBar	True	Specify if the tool bar containing the menu and other controls is displayed in the web client.


Setting	Default Value	Description
showAnalysisInformationTool	True	Specify if the Analysis Information menu item is displayed. If <code>true</code> , the menu item is displayed in the top right menu of the web client.
showExportFile	True	Specify if the Download as DXP file menu item is displayed. If <code>true</code> , the menu item is displayed in the top right menu of the web client.
showExportVisualization	True	Specify if the Export Visualization Image menu item is displayed. If <code>true</code> , the menu item is displayed in the top right menu of the web client.
showUndoRedo	True	Specify if the Undo and Redo menu items are displayed and if undo is available in the visualization. If <code>true</code> , the menu item is displayed in the top right menu of the web client.
showDodPanel	""	Specify the behavior of the Details-on-Demand (DoD) panel. If empty (""), the DoD panel is displayed if the author of the analysis file chooses to display the DoD panel. If <code>true</code> , the DoD panel is always displayed. If <code>false</code> , the DoD panel is never displayed.
showFilterPanel	""	Specify the behavior of the Filter panel. If empty (""), the Filter panel is displayed if the author of the analysis file chooses to display the Filter panel. If <code>true</code> , the Filter panel is always displayed. If <code>false</code> , the Filter panel is never displayed.
showPageNavigation	True	Specify if the Page tabs (or page links) in analyses are displayed. If you set this to <code>false</code> only the currently active Page as saved in the analysis will be displayed.
showStatusBar	True	Specify if the status bar is displayed.
showPrint	True	Specify if the Print menu item is displayed. If <code>true</code> , the menu item is displayed in the top right menu of the web client.

Setting	Default Value	Description
<code>allowRelativeLinks</code>	False	Specify if incomplete links in the Spotfire Web Player should be treated as relative to the library root directory. If <code>false</code> , incomplete links will be prepended with <code>http://</code> .
<code>showShareWithTwitter</code>	True	Specify if users should be able to share analyses on Twitter.
</analysis>		
<customHeader>		
<code>enabled</code>	False	Specify if a custom header is used in the web client or not. Set this to <code>true</code> to enable the custom header.
<code>fileName</code>	Header.htm	If you do not use cobranding in your environment, but still want to use a custom header in the web client, you must specify the name of the file that contains the custom header here. The name must match a custom header file that is placed in the <code><nm installation dir>\nm\services\<service specific folder>\Resources</code> directory.
Height	40	Specify the pixels for the height of the custom header.
</customHeader>		
<closedAnalysis>		
<code>showOpenLibrary</code>	True	Specify if the Open Library link is displayed on the Closed Analysis page.
<code>showReopenAnalysis</code>	True	Specify if the Reopen Analysis link is displayed on the Closed Analysis page.
<code>redirectToLibrary</code>	True	Specify if the Closed Analysis page is displayed after an analysis is closed.
</closedAnalysis>		
<errorPage>		
<code>showOpenLibrary</code>	True	Specify if the Open Library link is displayed on an error page.
<code>showReopenAnalysis</code>	True	Specify if the Reopen Analysis link is displayed on an error page.

Setting	Default Value	Description
</errorPage>		
</userInterface>		
<performance>		
<gcConfiguration>		
sustainedLowLatencyMode	True	This section is applicable for both Web Player services and Automation Services. Enabling <code>sustainedLowLatencyMode</code> should lead to fewer pauses during blocking GC, it may also lead to higher memory usage since GC now becomes less aggressive. When this setting is disabled, the Interactive latency mode is used.
</gcConfiguration>		
<recoverMemory>		
enabled	True	This section is applicable for both Web Player services and Automation Services. Enabling <code>recoverMemory</code> will help the system in the case where memory is exhausted and the last user session is removed. This state may occur if GC was not triggered by the system when freeing up large resources. The action can be specified with an integer depending on the service's memory status: 0. Do nothing. 1. Run garbage collection GC2. 2. Recycle the process.
actionWhenOk	0	Specify action when memory is OK.
actionWhenStrained	1	Specify action when memory is strained.
actionWhenExhausted	2	Specify action when memory is exhausted.
recycleIfScheduledAndCacheEnabled	False	Set to True to allow actions (garbage collection or process recycling) to be triggered even if analyses are cached by scheduled updates, but only if scheduled updates caching is enabled.
recycleEvenIfScheduledAnalyses	False	Set to True to allow actions (garbage collection or process recycling) to be triggered even if analyses are cached by scheduled updates, even if scheduled updates caching is not enabled.

Setting	Default Value	Description
triggerEvenIfUsersLoggedIn	True	Actions (garbage collection or process recycling) may be triggered even if users are logged in.
allowGcEvenIfAnalysesLoaded	False	Set to True to allow GC even if analyses are open.
minMinutesBetweenGc	60	Specify the minimum number of minutes between garbage collections.
minMinutesBeforeRecycle	300	Specify the minimum number of minutes before the process is recycled.
</recoverMemory>		
<documentCache>		
purgeInterval	300	Specify the number of seconds between searches to identify unused, open documents (templates) to be purged. The range is 60 to 3600.
itemExpirationTimeout	00:00:00	Specify the length of time, in the format HH:MM:SS, that a document can remain in the cache when no open analysis is using that document template. Maximum value is 47.00:00:00.
</documentCache>		
<analysis>		
antiAliasEnabled	True	<p>Specify if anti-aliasing is enabled. It is recommended that you leave anti-aliasing enabled in order to produce visualizations that are clear and sharp.</p> <p>All graphics in the web client are rendered with anti-aliasing enabled. However, anti-aliasing does impose a slight performance impact. The performance impact may become noticeable for visualizations that consist of a very large amount of graphical objects.</p>

Setting	Default Value	Description
useClearType	True	Specify if ClearType is enabled. It is recommended that you leave ClearType enabled in order to produce clear and sharp text in visualizations. All graphics in the Spotfire Web Player are rendered with ClearType enabled. However, ClearType does impose a slight performance impact. The performance impact may become noticeable for certain visualizations.
documentStateEnabled	True	Specifies that the state of files is maintained between sessions. If this value is set to true, when users resume working on a file, the file will be in the state in which that user left the file.
closedTimeout	120	Specify how long, in seconds, an analysis session will stay alive when a ping fails. The range is 60 to 4000000 (~46 days).
checkClosedInterval	60	Specify how often, in seconds, a check should be made if an analysis has been closed in the web client. The range is 60 to 300.
inactivityTimeout	02:00:00	Specify the length of time, in the format HH:MM:SS, that an analysis session can be alive when no user activity has been detected, excluding pings. The range is 00:01:00 to Infinite.
checkInactivityInterval	300	Specify how often, in seconds, a check should be made if an analysis session has had no user activity, excluding pings. The range is 60 to 12*3600.
regularPollChangesInterval	500	Specify the base interval, in microseconds, from when a change is made on the web client to when the client polls for a status update. The range is 200 to 1000.
maxPollChangesInterval	3000	Specify the maximum value, in microseconds, by which the poll interval in regularPollChangesInterval is increased for each try until this value is reached. The range is 1000 to 10000.
pollLoadInterval	1000	Specify the interval, in microseconds, between polls when an analysis file is loading. The range is 1000 to 10000.

Setting	Default Value	Description
needsRefreshInterval	15	Specify the frequency, in seconds, with which the web client should ping or poll to keep the analysis alive. The range is 10 to 60.
privateThreadPoolEnabled	True	This setting should not be edited unless instructed by TIBCO Spotfire Support.
privateThreadPoolWorkerCount	1	This setting should not be edited unless instructed by TIBCO Spotfire Support.
toolTipDelay	1000	Specify the length of time, in microseconds, that the client must wait before requesting a visualization highlighting tooltip from the server. The range is 200 to 3000.
undoRedoEnabled	True	Specify if the Undo and Redo functionality is enabled.
maxRenderTimeMs	60000	Specify the time limit, in milliseconds, for each request or render job is allowed to create an image on the web client for a visualization. You can use this setting to prevent long running requests or jobs from making the web client unresponsive.
maxAnalysisShutdownInformations	1024	<p>When an analysis is closed, the reasons why it was closed are stored and used when the analysis is re-opened. This value specifies the maximum number of entries stored.</p> <div>  <p>This setting should not be changed.</p> </div>
</analysis>		
<application>		This section is applicable for both Web Player services and Automation Services.
checkUserSessionTimeoutIntervalSeconds	120	How often to check if a user has timed out on the service.
userSessionTimeout	00:20:00	How long a user is cached on the service.
maxConcurrentWebServiceCallsPerCall	16	Specify how many active web service calls are allowed per CPU core on the service instance.
maxReceivedMessageSizeMb	64	Specify the maximum size of files uploaded to the service (Mb).

Setting	Default Value	Description
maxReaderQuotasSizeKb	256	Specify the maximum size of request and response messages sent to and from the service.
requestTimeoutSeconds	3600	Specify the timeout, in seconds, for requests between the Spotfire Server and the service. This might need to be increased if large files or data sets are uploaded to the service.
</application>		
<performanceCounterLogging>		This section is applicable for both Web Player services and Automation Services.
enabled	True	Enable or disable the logging of the specified performance counters. The result of this logging can be found in the PerformanceCounterLog.txt file specified in the log4net.config file.
cpuAverageTimeSpan	120	Specify the number of seconds to use for a rolling average when calculating the CPU load. The calculated CPU load is used to determine if the service instance is exhausted, strained, or ok.
logInterval	120	Specify the number of seconds between each performance counter logging at INFO level.
counters		Add performance counters you wish to log, at both INFO and DEBUG level, separated by a comma “ , ”. Each counter consists of three parts: category, counter, and instance, separated by a semi-colon “ ; ”. Both standard Windows performance counters, as well as a set of internal TIBCO counters, may be included.
debugLogInterval	15	Specify the number of seconds between each performance counter logging at DEBUG level.
debugCounters		Add additional performance counters you wish to log at DEBUG level, separated by a comma “ , ”.
</performanceCounterLogging>		
<statistics>		This section is applicable for both Web Player services and Automation Services.

Setting	Default Value	Description
flushInterval	60	Specify the number of seconds between each logging.
enabled	True	When true, enables logging of all the other statistics for the service. The result of this logging can be found in the other log files specified in the log4net.config file.
</statistics>		
<hierarchicalClustering>		This section is applicable for both Web Player services and Automation Services.
maxInteractiveElements	2000	Specify the maximum number of rows or columns of a hierarchical clustering that can be started interactively in the web client.
maxElements	30000	Specify the maximum number of rows or columns of a hierarchical clustering that can run on the web client. Scheduled updates can run hierarchical clustering up to this size.
maxInteractiveJobs	2	Specify the maximum number of interactive clustering jobs running in parallel.
cpuFactorInteractiveJobs	0.8	Specify an estimate of the number of threads that clustering will use for interactive jobs on a multi-core server running the Web Player service.
cpuFactorLargeJobs	0.5	Specify an estimate of the number of threads that clustering will use for scheduled update jobs on a multi-core server running the Web Player service.
nativeMemory	500	Specifies a memory limit, in MBytes, for the clustering algorithm. The default value 500 (MBytes) matches maxElements = 30000.
</hierarchicalClustering>		
</performance>		
</spotfire.dxp.web>		

Customizing the service logging configuration

Log4Net.config specifies the logs and logging levels for the Web Player service and Automation Services. To edit this configuration, you must export its contents to an XML file, edit it, import it, and then apply the configuration.

This task walks you through editing the configuration for the Web Player service. You can also edit the configuration for Automation Services, which includes an additional configuration file.

- For an example of editing Automation Services, see [Manually editing the service configuration files](#).
- For a list of the log files and their properties you can customize, see [Service logs](#).

Prerequisites

You must have administrative credentials for Spotfire Server.

Procedure

1. On the computer running Spotfire Server, open a command line as an administrator and change the directory to the path of the config.bat file (config.sh on Linux).

The default file path is `<installation_dir>/tomcat/bin`.

2. Export the configuration using [export-service-conf](#) and passing commands for the service to customize.

For example:

```
config export-service-config --tool-password=mypassword
--capability=WEB_PLAYER --deployment-area=Production c:\temp\config
```

- Provide the appropriate password for the configuration tool.
- The deployment area is usually Production. Check the administration interface page Nodes & Services if you are not sure.
- If the directory where you want to write the configuration files already exists, you can overwrite the contents by using the `--force` flag.

The configuration is exported to the specified directory, creating a `root` subdirectory that contains the following configuration files.

- `log4net.config`
- `Spotfire.Dxp.Worker.Core.config`
- `Spotfire.Dxp.Worker.Host.exe.config`
- `Spotfire.Dxp.Worker.Web.config`

3. Browse to the directory, and then, using a text editor, open and edit the configuration file `log4net.config`.

In the configuration file, each potential log file is specified by an `<appender>` section. Edit each section for the logs to create. For more information about the logs this file can create, see [Web Player service logs](#).

- a) Set the [logging level](#).
- b) Specify the file path to write the log.
- c) Save and close the configuration file.

4. Optional: Customize the user and session statistics, and the performance counter logging, specified in the file `Spotfire.Dxp.Worker.Web.config`, which is also exported and written to the `root` subdirectory.

You can customize the performance counters at both the `INFO` and the `DEBUG` levels. See [Service log levels](#) for more information.

- Return to the command line and import the custom configuration using [import-service-config](#), passing in the configuration name, the tools password, and the path for the configuration.
For example:

```
config import-service-config --tool-password=mypassword
--config-name=SampleConfig c:\temp\config
```

The configuration is successfully imported.

- Set the custom configuration using [set-service-config](#), passing in the service ID and the configuration name.
For example:

```
config set-service-config --tool-password=mypassword
--service-id="VALUE" --config-name=SampleConfig
```



Use the [list-services](#) command to get the service ID. In some cases, you must enclose the service ID in double quotation marks.

A warning is displayed indicating that setting a new service configuration causes all running instances of the service to restart, and you must indicate whether you want to continue. If you press Y, the service restarts and the new configuration is set.

Result

The configuration setting for the Web Player service is displayed in Nodes & Services, and the log files should be written as specified.

Customize statistics and performance counter logging

You can configure the collection of user and session statistics and the performance counters in the file `Spotfire.Dxp.Worker.Web.config`.

The `Spotfire.Dxp.Worker.Web.config` file is exported and imported with other service configuration logging files as described in the task [Customizing the service logging configuration](#).

To customize the information to collect, in the file `Spotfire.Dxp.Worker.Web.config`, find and edit the `<performance>` and `<statistics>` sections. For detailed information about the nodes, see the reference topic for [Spotfire.Dxp.Worker.Web.config](#).

Service log levels

For events occurring for a service, Spotfire Server can provide a log entry that specifies a level of severity. The level applied can provide you with clues about the nature of the log entry.

You can set the log level for each log file you write. The following table lists the log levels and their descriptions. If you set logging the lowest (most severe level), notice that only fatal problems are logged. For each added level of reporting, levels are concatenated, so at the highest, most thorough level, your logs contain detailed information at all levels.

For information about Web Player service logs and their properties, see [Web Player service logs](#).

Log level	Comment
OFF	Specifies that no log should be created.
FATAL	Specifies that fatal problems should be logged.
ERROR	Specifies that fatal problems and errors should be logged.
WARN	Specifies that fatal problems, errors, and warnings should be logged.

Log level	Comment
INFO	Specifies that fatal problems, errors, warnings, and information should be logged.
DEBUG	Specifies the a fine-grained and detailed logging of events.
TRACE	Specifies the an even finer-grained and detailed level of detail for logging of events. Use with caution, because it can degrade server performance if it runs for long.

For a list of server and node logging levels, see [Server and node logging levels](#).

Configuring a specific directory for library import and export

You can change the directory that Spotfire uses for library import and export if the default directory is inconvenient. For most purposes this setting does not need to be changed.

Procedure

- You can set a new library directory by using either the configuration tool or the command line:
 - In the configuration tool, the **Library Directory** panel is at the bottom of the **Configuration** tab.
 - On the command line, use the [config-import-export-directory](#) command.

Enabling cached and precomputed data for scheduled update files

Disk caching and precomputations of data shorten the time it takes for a scheduled update file to reopen in a Spotfire Web Player after the Web Player is restarted. This feature is disabled by default. It is enabled at the service level by editing the `Spotfire.Dxp.Worker.Web.config` file for each installed web client service.

You then have the option of turning the feature off for individual files (see [Disallowing cached and precomputed data in individual scheduled update files](#)).

Procedure

- Open a command line and export the service configuration by using the [export-service-config](#) command.
- Open the `Spotfire.Dxp.Worker.Web.config` file in a text editor or XML editor and locate the following section. By default, the exported configuration file is saved to the `installation dir \tomcat\bin\config\root` directory.


```
<scheduledUpdates concurrentUpdates="2" updateIntervalSeconds="60">
  <forcedUpdate enabled="true" maximumRejectedUpdates="2"/>
  <cacheSettings enabled="false" path="" maxDiskSizeMb="0"
maxAgeMinutes="1440"/>
</scheduledUpdates>
```
- In the line `<cacheSettings enabled="false" path="" maxDiskSizeMb="0" maxAgeMinutes="1440"/>`, make these changes:
 - Set `cacheSettings enabled` to "true".
 - Set `path` to the path on disk where the data is to be stored.

For information on the other settings, see [Spotfire.Dxp.Worker.Web.config](#).

- Import the configuration back into Spotfire Server by using the [import-service-config](#) command.

5. Assign the edited service configuration to the Spotfire Server by using the [set-service-config](#) command.

Example:

```
config set-service-config --service-id=6610a31b-1a2a-4497-b146-cee797f9b6a7
```



Use the [list-services](#) command to obtain the service ID.

Disabling the attachment manager cache

By default the Spotfire attachment manager caches library content and the results of information link executions when downloading or saving large amounts of data. You can disable the attachment manager cache by editing the `configuration.xml` file

Procedure

1. Export and open the Spotfire Server configuration file; for general instructions, see [Manually editing the Spotfire Server configuration file](#).
2. In the `configuration.xml` file, locate the following section and set `<content-caching-enabled>` to "false":

```
<library>
  <import-export-path>default</import-export-path>
  <content-caching-enabled>true</content-caching-enabled>
  <max-number-concurrent-imports-and-exports>3</max-number-concurrent-imports-
and-exports>
</library>
```

3. Then locate the `<information services>` section and set `<result-caching-enabled>` to "false".
4. Import the server configuration file and restart the server(s); for instructions, see [Manually editing the Spotfire Server configuration file](#).

Post-installation steps

After Spotfire Server is installed and configured, the Spotfire administrator must complete these setup tasks before end users can access and work in Spotfire.

1. Install Spotfire Analyst on a computer for the administrator to use.



Steps 3-6 in this list require Spotfire Analyst.

2. Set up users and groups; see [User administration](#) and [Group administration](#) for details.
3. Assign *licenses* and *preferences* to groups; use the Administration Manager in Spotfire Analyst to accomplish these tasks.



For a description of the licenses and preferences, see the Administration Manager help.

4. Set up the Spotfire library by using Spotfire Analyst.
5. Optional: Import demo database files into the library files so that users can experiment with the demo database ; see [Enabling demo database use](#).
6. Optional: Import geocoding tables into the library so that data can be displayed on maps; see [Enabling geocoding tables for map charts](#).

Enabling demo database use

To make the demo database available to end users for practice with Spotfire, you must also import its related ZIP file to the Spotfire library. This ZIP file contains analysis files and an information model that links to the demo data.

Prerequisites

- While setting up the Spotfire database, the administrator chose to install the demo database.
- Spotfire Analyst is installed.

Procedure

1. Copy the file `<Spotfire Server installation kit>/demodata/<mssql or oracle>/demo.part0.zip` to the library folder that is used for importing and exporting files. (By default, this is `<server installation directory>/tomcat/application-data/library`.)
2. Log in to Spotfire Analyst as a Spotfire Administrator or Library Administrator.
3. Click **Tools > Library Administration**.
4. Click **Import** and then browse to and select the file `demo.part0.zip`.
5. Click **OK** twice, and then in the Select Destination Folder dialog, either select an existing folder or create a new one (for example, you can create a "Demo" folder).
6. Click **OK**, wait for the dialog to display the words "Import done", and then click **Close**.

Enabling geocoding tables for map charts

To display data on a Spotfire map, the data must be "geocoded". This involves matching the data to location identifiers in a set of data tables that are known as a geocoding hierarchy. These geocoding tables must be imported into the library before they can be used.

Prerequisites

Spotfire Analyst is installed.

Procedure

1. Copy the file <Spotfire Server installation kit>/geoanalytics/geoanalytics.part0.zip to the library folder that is used for importing and exporting files. (By default, this is <server installation directory>/tomcat/application-data/library.)
2. Log in to Spotfire Analyst as a Spotfire Administrator or Library Administrator.
3. Click **Tools > Library Administration**.
4. Click **Import** and then browse to and select the file geoanalytics.part0.zip.
5. Click **OK** twice, and then in the Select Destination Folder dialog, either select an existing folder or create a new one (for example, you can create a "GeoAnalytics" folder).
6. Click **OK**, wait for the dialog to display the words "Import done", and then click **Close**.

Administration

Administrators can perform most management tasks in Spotfire Server, including creating users and groups, deploying software updates, and managing and monitoring software configurations.

To set licenses and preferences, however, and to manage the library, use Spotfire Analyst.



Spotfire Analyst currently offers the same administrative functionality as its previous version, but as of the 7.5 version, Spotfire Server offers a new, streamlined interface and easy access to both new and existing features.

Opening Spotfire Server

You can access Spotfire Server through a browser on any computer in the domain.

There are two ways to open Spotfire Server:

- On the computer running Spotfire Server, click **Start**, go to the Spotfire Server folder, and click **TIBCO Spotfire Server**.
- On any computer in the domain, go to `http://servername:port/spotfire`.



If you work in a clustered environment, it does not matter which server in the cluster you use. Changes made to one server are stored in the Spotfire database and are available to all servers. If your clustered deployment includes a load balancer, use the load balancer hostname in place of `servername` in the second method.

Nodes, services, and resource pools

In Spotfire Server you can enlarge or scale down your implementation as needed, as well as create and manage *resource pools*. Resource pools are used in *routing rules* to direct Spotfire traffic to specific service instances.

For more information, see [Nodes and services introduction](#), [Node manager installation](#), and [Routing rules](#).

Creating resource pools

If you want a certain analysis, or all analyses requested by certain users, to open on specific instances of the Spotfire Web Player, create a resource pool that contains the selected instances and use it in a routing rule.

Procedure

1. Log in to Spotfire Server and click **Nodes & Services**.
2. On the "Resource pools" page, click **Create resource pool**.
3. In the "Create new resource pool" dialog, enter a name for the pool, and select the check box of each Spotfire Web Player instance that you want to add to the pool.



Each Spotfire Web Player instance can belong to only one resource pool.

4. Click **Create**.
The new pool appears in the Resource pools list.

Adding resources to resource pools

To respond to changing needs in your organization, you can adjust the contents of resource pools at any time.

Procedure

1. Log in to Spotfire Server and click **Nodes & Services**.
2. Click the **Resource pools** tab.
3. In the "Resource pools" table, locate the pool that you want to change and then click the plus sign on the right side of its row.
4. In the "Add instances to resource pool" dialog, select the check box for each instance that you want to add.
5. Click **Add**.

Removing resources from resource pools

To respond to changing needs in your organization, you can adjust the contents of resource pools at any time.

Procedure

1. Log in to Spotfire Server and click **Nodes & Services**.
2. Click the **Resource pools** tab.
3. In the "Resource pools" table, locate the pool that you want to change and then click the down arrow in its "AVAILABLE" box.
This displays a list of the instances that the resource pool currently contains.
4. Above the list of instances, on the right, click the pencil icon.
Check boxes are displayed to the left of each instance.
5. Select the check boxes of the instances that you want to remove from the pool, and then click **Remove**.
The removed instance(s) are added to the "Unassigned instances" section.

Changing the name of a resource pool

You can rename a resource pool directly in the "Resource pools" list.

Procedure

1. Log in to Spotfire Server and click **Nodes & Services**.
2. Click the **Resource pools** tab and then, in the list of resource pools, click the name you want to change.
3. Make your changes, and then click the check mark.

Deleting resource pools

You can delete any resource pool that is no longer being used in a routing rule.

Prerequisites

Make sure that the resource pool is not in use by reviewing the "Resource pool" column of the Rules list in **Scheduling & Routing**.

Procedure

1. Log in to Spotfire Server and click **Nodes & Services**.
2. Click the **Resource pools** tab.
3. In the "Resource pools" table, locate the pool that you want to delete and then click the trash icon on the right side of its row.

Updating node managers

When you add a node manager software update (hotfix) to the appropriate deployment area, an **Update** button is displayed in the information pane for each affected node.

Prerequisites

The software update is in the node manager's deployment area; for instructions, see [Adding software packages to a deployment area](#).

Procedure

1. Log in to Spotfire Server and click **Nodes & Services**.
2. On the "Your network" page, under **Select a view**, click **Nodes**, and then select the node that you want to update.
In the upper-right pane there is an **Update** button.
3. Click **Update**, and then in the confirmation dialog click **Update** again.
A message indicates that the update has started, and then the **Status** line indicates that the node is offline.

Result

When the **Roll back** button appears in the upper-right pane, the update is complete.

If you want to cancel the update and return to the previous node manager version, see [Rolling back a node manager update](#).

Rolling back a node manager update

After updating a node manager, you have the option of undoing the update and returning to the previous version of the node manager.

Procedure

1. Log in to Spotfire Server and click **Nodes & Services**.
2. On the "Your network" page, under **Select a view**, click **Nodes**, and then select the node manager that was updated.
In the upper-right pane there is a **Roll back** button.
3. Click **Roll back**, and then in the confirmation dialog click **Roll back** again.
A message indicates that the rollback has started, and then the **Status** line indicates that the node is offline.

Result

When the **Update** button reappears, the rollback is complete.

Updating services

When you add an update for a service to the appropriate deployment area (or make any other change to a deployment, such as deleting a package or changing the deployment area of a service), an **Update service** button becomes available in the information pane for each affected service.

Procedure

1. Log in to Spotfire Server and click **Nodes & Services**.
2. On the "Your network" page, under **Select a view**, click **Nodes**, and then select the service that you want to update.
In the upper-right pane there is an **Update service** button. You can scan the Packages pane for the orange notes that indicate exactly what has changed from the current deployment.
3. Click **Update service**, and then in the confirmation dialog click **Update**.
In the upper-right pane, the **Status** line indicates that the update has started. The Activity page shows the progress of the update.

Result

When the update is complete, the **Status** line indicates "Service installed successfully". The new service duplicates the settings of the old service, including its name, resource pool, and port. No further requests will be routed to the old service.

If you want to cancel the update and return to the previous service version, see [Rolling back a service update](#).



If you delete the old service you will not be able to roll back the service.

When the update is successful and you are sure that you want to keep the new version, you should delete the old service version. Because Spotfire Server stores a maximum of two versions of a service, if you perform another update on the same service, the first version will be deleted automatically if it is still being stored.

Rolling back a service update

After updating a service, you have the option of undoing the update and returning to the previous version of the service.

Procedure

1. Log in to Spotfire Server and click **Nodes & Services**.
2. On the "Your network" page, under **Select a view**, click **Nodes**, and then select the service that was updated.
The **Show old service** link is visible in the upper-right corner of the page.
3. Click **Show old service**.
In the upper-right pane, information about the old service appears (in a paler font) to the right of information about the new service. A **Roll back** button becomes available in the upper-right corner of the page.
4. Click **Roll back**, and then in the confirmation dialog click **Roll back** again.
The **Status** line indicates "Instances are being modified".
5. When the **Status** line indicates "Service is available but the functionality is limited until rollback is confirmed", click **Confirm rollback** in the upper-right corner of the page. In the confirmation dialog, click **Roll back**.

Result

The **Status** line indicates "Service installed successfully".

Shutting down a service instance

If you want to shut down a service instance because it is not needed, for example, or because you want to run it on a different node, you can shut the service down without disturbing the work of end users. You can also shut it down immediately.

Procedure

1. Log in to Spotfire Server and click **Nodes & Services**.
2. On the "Your network" page, under **Select a view**, select **Nodes**.
3. In the left pane, expand the entries under the node and select the service instance that you want to shut down.
4. In the right pane, click **Shut down** and then do one of the following:

- If you want the instance to continue running for a while, click **Schedule** and then enter the number of hours and minutes you want Spotfire Server to wait before shutting it down.



Before the shutdown, any users on that service instance are notified that the instance will be shutting down; this gives them time to save their work. The instance is then shut down when the user or users close the analysis, or at the scheduled time, whichever is earlier. If no one is using the instance, the instance is shut down immediately.

- If you want the instance to shut down immediately, whether or not it is being used, click **Immediately**.



End users who are on this service instance will lose any unsaved work.

Revoking trust of a node

You may want to remove the authorization of a node because you are upgrading your hardware, for example, or down-scaling your network, or if you see an unusual error and want to reset the computer. This immediately shuts down any services that are running on the node, and disables all management options for the node except re-trusting it.

Procedure

1. Log in to Spotfire Server and click **Nodes & Services**.
2. On the "Your network" page, under **Select a view**, select **Nodes**.
3. In the left pane, select the node whose trust you want to revoke, and in the upper-right pane click **Revoke trust**.

Result

The node moves from the "Your network" page to the "Untrusted nodes" page.

User administration

If the user accounts for your Spotfire implementation are manually added to the database (rather than synchronized with an external directory such as LDAP), user administration takes place in Spotfire Server.



User accounts that are automatically created by Spotfire Server, such as `automationservices@SPOTFIRESYSTEM`, cannot be deleted and their names cannot be changed.

For more information about users, see [Users & groups introduction](#).

Creating new Spotfire users

If your Spotfire implementation is configured for Spotfire database authentication, you can add new users in Spotfire Server. (To import and export users, use the Administrator Manager in Spotfire Analyst.)



Externally synchronized users are managed in that context and not within the Spotfire system..

Procedure

1. Log in to Spotfire Server. (For instructions on accessing the server, see [Opening Spotfire Server](#).)
2. Click **Users & Groups**.
3. Under **Select a category**, select **Users**.
4. At the top of the pane, click **Create new user**.
5. In the New user dialog, enter the user name and password.
6. Re-type the password, enter an email address (optional), and click **Save**.

Result

The new user is displayed in the **Users** list, and the **Groups** list in the lower right pane indicates that the user belongs to the Everyone group.

Adding a user to one or more groups

A user can belong to one or many groups. A user who is an explicit member of a group is also, by inheritance, a member of that group's parent groups.

Procedure

1. Log in to Spotfire Server and click **Users & Groups**.
2. Under **Select a category**, select **Users**.
3. Highlight the name of the user that you want to add to groups.
4. In the **Groups** pane on the right, click **Add**.
5. In the Select groups for user to join dialog, select the check box next to the groups to which you want to add the user.
6. Click **Save**.

Result

The selected groups are displayed in the user's **Groups** list.

Removing a user from one or more groups

You can remove a user from a group to remove the user's access to the licenses that are enabled for that group.

Procedure

1. Log in to Spotfire Server and click **Users & Groups**.
2. Under **Select a category**, select **Users**.
3. In the left pane of the **Users** page, highlight the user who you want to remove from a group.
4. In the lower right pane, under **Groups**, select the check box of the groups from which you want to remove the user.
5. Click **Remove**.

Result

The selected groups no longer appear in the user's **Groups** list.

Changing a user's name, password, or email

You can change user properties in Spotfire Server.



Externally synchronized users are managed in that context and not within the Spotfire system.

Procedure

1. Log in to Spotfire Server and click **Users & Groups**.
2. Under **Select a category**, select **Users**.
3. Highlight the name of the user whose properties you want to change.
4. In the upper-right corner of the page, click **Edit**.
5. In the Edit user dialog, make your changes. (Select the **Change password** check box to create a new password.)
6. When you've finished, click **Save**.

Disabling a user account

Disabling a user account makes it impossible for the user to log in to Spotfire, but keeps their record in the system for reference or for enabling them again in the future.



Externally synchronized users are managed in that context and not within the Spotfire system..

Procedure

- On the command line, use the [enable-user](#) command.
For more information about the command line, see [Configuration using the command line](#).

Deleting users from the system

To permanently remove users from your Spotfire implementation, delete them. However, if you want to deny them access to Spotfire but keep their records in the system, you can disable their accounts instead.



Externally synchronized users are managed in that context and not within the Spotfire system..

Procedure

1. Log in to Spotfire Server and click **Users & Groups**.
2. Under **Select a category**, select **Users**.
3. Select the check box next to the user or users that you want to delete.
4. Click the **Delete checked users** button.

Group administration

Most group administration takes place in Spotfire Server. Managing licenses and preferences, however, takes place in the Administration Manager in Spotfire Analyst.


For groups that are synchronized from an external source such as an LDAP directory, certain tasks including adding and removing members of the synchronized group, take place in the external environment and not within the Spotfire system.





For more information about groups, see [Users & groups introduction](#).

Roles and special groups

Spotfire includes a number of special groups that are present at installation and cannot be removed. They define standard roles for administering and using Spotfire.

Each special group enables a set of licenses that correspond to an administrative or user role. To assign a role to a user, simply add the user to one of the special groups. Note that some roles require not only membership in the special group, but also that a specific license be enabled for the group. Licenses are set in the Administration Manager in Spotfire Analyst.

Role	Description
Administrator	<p>All users who need administrator privileges on Spotfire Server, including the ability to manage users and groups, must belong to this group. Membership in this group grants all permissions described below in addition to administration of preferences, licenses, and the user directory.</p> <div>  <p>This group must also have the Spotfire Administrator license enabled to fully administer the Spotfire system (to access the Administration Manager tool in Spotfire Analyst as well as all areas of Spotfire Server).</p> </div>

Role	Description
Library Administrator	<p>Membership in this group grants full permission to the library. It overrides all folder permissions set in the library, granting full control over content. It also includes the permission to import and export library content. All users and groups that need administrative privileges in the library must belong to this group or the Administrator group.</p> <p> This group must also have the Spotfire Library Administrator license enabled to be able to administer the library (to get access to the Library Administration tool in Spotfire Analyst).</p>
Deployment Administrator	<p>Membership in this group grants permission to deploy packages to the server. Note that these users can deploy to any area on the server, as well as delete any existing deployment.</p> <p>Members of this group can access the Deployments & Packages area of Spotfire Server.</p>
Diagnostics Administrator	<p>Membership in this group grants permission to view server logs and diagnostics, as well as to set logging configurations.</p> <p>Members of this group can access the Monitoring & Diagnostics area of the server.</p>
Scheduling and Routing Administrator	<p>Membership in this group grants permission to create scheduled updates and routing rules.</p> <p>Members of this group can access the Scheduling & Routing area of the server.</p>
Scheduled Updates Users	<p>The account that executed scheduled updates must be a member of this group. By default, the account scheduledupdates@SPOTFIRESYSTEM is a member of this group.</p>
Automation Services Users	<p>Membership in this group grants permission to execute Automation Services jobs on the server, using the Job Builder or the Client Job Sender.</p>
Custom Query Author	<p>Membership in this group grants permission to save scripts written in custom query languages as trusted to the library.</p> <p> An authorized custom query author MUST ALSO have the Custom Query in Connections license enabled to get access to the required UI.</p>
Script Author	<p>Membership in this group grants permission to save scripts as trusted to the library.</p> <p> An authorized script author MUST ALSO have the Author Scripts license enabled.</p> <p> Scripts that are executed by Spotfire Server can essentially do anything that deployed packages can do. Therefore you should only grant this permission to trusted users.</p>
API User	<p>All users who require access to the Spotfire Server public Web Service API must be members of the API User group.</p>

Role	Description
Everyone	This group always contains all users in the Spotfire implementation. No users can be removed from this group, but you can set licenses for the group if you want to.
System Account	This group cannot be edited. It contains the system accounts that are used internally in the Spotfire environment.

Creating a new group

You can create a group at the top level of the groups hierarchy, or as a subgroup of an existing group. A subgroup inherits all the settings of its parent group or groups. (To import and export groups, use the Administrator Manager in Spotfire Analyst.)

Procedure

1. Log in to Spotfire Server and click **Users & Groups**.
2. Under **Select a category**, select **Groups**.
3. At the top of the pane, click **Create new group**.
4. In the Create group dialog, enter a name for the group.
5. Do one of the following:
 - To create a group at the top level, click **Save**.
 - To create a subgroup, select the **Add new group to existing groups** check box, select the check box for the group or groups to which you want to add the new group, and then click **Save**.

Result

The new group is displayed in the **Groups** list. When you highlight the group, any groups to which it belongs are displayed under **Parent groups** in the right pane.

What to do next

Assign licenses to the group.

Licenses and preferences are set in the Administration Manager in Spotfire Analyst.

Adding users to a group

You can add any number of Spotfire users to a group at the same time.



Externally synchronized groups are managed in that context and not within the Spotfire system..

Procedure

1. Log in to Spotfire Server and click **Users & Groups**.
2. Under **Select a category**, select **Groups**.
3. In the left pane of the **Groups** page, highlight the group to which you want to add members.
4. In the **Members** pane on the right, click **Add users**.
5. In the **Select users to add to group** dialog, select the check box next to the user or users that you want to add to the group, and then click **Save**.

Result

The added users are displayed in the **Members** list.

Adding groups to a group

Adding one group to another group creates a hierarchy of groups where a user who is an explicit member of the child group is also, by inheritance, a member of the parent group.



Externally synchronized groups are managed in that context and not within the Spotfire system.

Procedure

1. Log in to Spotfire Server and click **Users & Groups**.
2. Under **Select a category**, select **Groups**.
3. In the left pane of the **Groups** page, highlight the group to which you want to add other groups.
4. In the **Members** pane on the right, click **Add groups**.
5. In the **Select groups to add to group** dialog, select the check box next to the group or groups that you want to add to the group, and then click **Save**.

Result

The added groups are displayed in the **Members** list.

Assigning a primary group to a subgroup

When a group has several parent groups, different values may be set for the same license or preference item in two or more parent groups. To ensure that the child group inherits the default settings of a particular parent group, set that group as the primary group.

Procedure

1. Log in to Spotfire Server and click **Users & Groups**.
2. Under **Select a category**, select **Groups**.
3. Highlight the name of the group to which you want to assign a primary group.
4. In the upper-right pane, click **Edit**.
5. In the Edit group dialog, under **Assign primary group**, select the primary group for the highlighted subgroup.
6. Click **Save**.

Result

In the upper-right pane, the selected group is listed as the primary group.

Assigning a deployment area to a group

For users to have access to a deployment, you must assign the deployment area that contains the deployment to the appropriate groups. If no deployment area is set for a group, the group members are assigned the default deployment area.

For general information, see [Deployments and deployment areas](#).

Procedure

1. Log in to Spotfire Server and click **Users & Groups**.
2. Under **Select a category**, select **Groups**.
3. Highlight the name of the group to which you want to assign a deployment area.
4. In the upper-right pane, click **Edit**.
5. In the Edit group dialog, under **Assign deployment area**, select the deployment area for the group.
6. Click **Save**.

Result

The selected deployment area is displayed under **Deployment area** in the upper-right pane.

Renaming a group

You can rename only those groups that were added to Spotfire Server after installation. The groups that Spotfire creates automatically, such as Administrator and Script Author, cannot be renamed. Also, externally synchronized groups cannot be renamed in the server.

Procedure

1. Log in to Spotfire Server and click **Users & Groups**.
2. Under **Select a category**, select **Groups**.
3. Highlight the name of the group that you want to rename.
4. In the upper-right pane, click **Edit**.
5. In the Edit group dialog, under **Name**, enter the new name.
6. Click **Save**.

Removing members from a group

Members of a Spotfire group can be either users or other groups.



Externally synchronized groups are managed in that context and not within the Spotfire system.

Procedure

1. Log in to Spotfire Server and click **Users & Groups**.
2. Under **Select a category**, select **Groups**.
3. In the left pane of the **Groups** page, highlight the group from which you want to remove members.
4. In the right pane, under **Members**, select the check box of the users or groups that you want to remove.
5. Click **Remove**.

Result

The members you removed no longer appear in the **Members** list.

Deleting groups from the system

Deleting a group does not delete any of its members from Spotfire; only the group itself is deleted. All users and groups that are members of the deleted group remain in the system. Subgroups that lose their parent group are automatically placed at the top level of the group hierarchy.



There is no recursive delete function that deletes an entire branch of the hierarchy.



You cannot delete any of the roles and special groups that Spotfire creates automatically at installation.



Externally synchronized groups are managed in that context and not within the Spotfire system.

Procedure

1. Log in to Spotfire Server and click **Users & Groups**.
2. Under **Select a category**, select **Groups**.
3. In the left pane of the **Groups** page, select the check box next to the group or groups that you want to delete.
4. At the top of the left pane, click **Delete checked groups**.

Result

The deleted groups no longer appear in the **Groups** list.

Deployments and deployment areas

To deploy Spotfire software, the administrator places software packages in a *deployment area* and assigns the deployment area to particular groups.

If a new deployment is available when a user logs in to a Spotfire client, the software packages are downloaded from the server to the client.

Deployments are used:

- To set up a new Spotfire system.
- To install a product upgrade, extension, or hotfix provided by Spotfire.
- To install a custom tool or extension.

A group of software packages (.spk files) can be bundled together into a *distribution* (.sdn file). A distribution can be copied to create a new deployment area, or downloaded for deployment to another Spotfire Server.

Every user is associated with at least one deployment area; by default, this is the Production area that is created when you install Spotfire Server, but you can designate any area as the default.

Some users have access to more than one deployment area because they belong to several groups that are associated with different deployment areas. In this case, users are prompted to choose a deployment area when they log in to the Spotfire client.

Whether a user has access to a particular feature contained in a distribution depends on the licenses that are assigned to that user's groups. For more information, see [Licenses and preferences introduction](#).

Administrators usually create a Test deployment area to use as a staging server; when the new software has been thoroughly tested in their Spotfire environment, the distribution is copied to a production area.

Creating a new deployment area

Deployment areas contain software packages that you make available to certain groups. You can create a new deployment area for a Spotfire update or extension, for custom tools created in your organization, and so on.

For general information, see [Deployments and deployment areas](#).

Procedure

1. Log in to Spotfire Server. (For instructions on accessing the server, see [Opening Spotfire Server](#).)
2. Click **Deployments & Packages**.
3. In the **Deployment areas** pane, click **Add**.
4. In the **Add area** dialog, enter a name for the new area.



Deployment area names are case insensitive and have a maximum length of 25 characters. These are the valid characters:

- a - z
- 0 - 9
- The underline character _
- The dash character -

5. Click **Add area**.

Result

The new deployment area is displayed in the **Deployment areas** list.

Adding software packages to a deployment area

When Spotfire releases updates, or if your company creates custom tools or other software elements, the administrator adds these to a deployment area so that they can be uploaded to Spotfire Server. Then the server distributes the new software to the appropriate groups, as selected by the administrator.

For general information, see [Deployments and deployment areas](#).

Procedure

1. Log in to Spotfire Server and click **Deployments & Packages**.
2. In the left pane, under **Deployment areas**, select a deployment area.



It is recommended that you first test the software on a deployment area that is not in production.

3. Optional: If the deployment area contains any software packages that are not currently needed, delete them. (For instructions, see [Removing packages from a deployment area](#).)
4. In the "Software packages" pane, click **Add packages**.
5. In the "Add packages" dialog, click **Choose File**, locate and select the file you want to add, and click **Open**.
6. In the "Add packages" dialog, click **Upload**.
The added packages are displayed in the **Software packages** pane.



If you want to start over again, you can return to the last saved version of the deployment area by clicking **Revert all**.

7. To confirm that the packages are error-free, in the "Software packages" pane click **Validate**.
8. To save the new packages, click **Save**.
9. In the "Save deployment" dialog, if you want the Spotfire clients to automatically accept the update when they are opened (rather than having the user decide when to accept the update), select the **Force client update** check box.
10. Click **Save**.

Copying a distribution to another deployment area

You can copy a distribution from one deployment area to another when you are ready to move it from a test area to a production area, or if you want to create a new deployment based on an existing one.

Procedure

1. Log in to Spotfire Server and click **Deployments & Packages**.
2. Under **Deployment areas**, select the deployment area that contains the distribution you want to copy.
3. In the Information pane to the right, click **Copy distribution**.
4. In the "Copy distribution" dialog, do one of the following:
 - Select the existing deployment area to which you want to add the distribution, and then click **Copy**.
 - Create a new deployment area to hold the distribution by clicking the **To new area** tab, entering a name for the area, and clicking **Copy**.

Result

When you select the deployment area in the "Deployment areas" pane, the copied software packages are displayed under **Software packages**.

Exporting a distribution

You can download a local copy of a distribution (.sdn file) for deployment to another Spotfire Server.

Procedure

1. Log in to Spotfire Server and click **Deployments & Packages**.
2. Under **Deployment areas**, select the area that contains the distribution that you want to export.
3. In the Information pane to the right, click **Export distribution**.

Changing the default deployment area

The default deployment area is available to all groups for which no deployment area has been set. During installation, Spotfire Server adds a "Production" deployment area and sets it as the default, but you can change the default area to give users access to new software packages.

For general information, see [Deployments and deployment areas](#).

Procedure

1. Log in to Spotfire Server and click **Deployments & Packages**.
2. In the "Deployment areas" pane, select the deployment area you want to set as the default.

3. In the upper-right pane, click **Make default**.

Renaming a deployment area

You can rename any deployment area in your system.

Procedure

1. Log in to Spotfire Server and click **Deployments & Packages**.
2. In the "Deployment areas" pane, select the deployment area you want to rename.
3. In the Information pane to the right, click **Rename**.
4. In the "Rename deployment area" dialog, enter a new name.



Deployment area names are case insensitive and have a maximum length of 25 characters. These are the valid characters:

- a-z
- 0-9
- The underline character _
- The dash character -

5. Click **Rename**.

Removing packages from a deployment area

You can edit the contents of any of your deployment areas.

Procedure

1. Log in to Spotfire Server and click **Deployments & Packages**.
2. In the "Deployment areas" pane, select the deployment area from which you want to remove packages.
3. In the "Software packages" pane, select the check boxes for the packages you want to remove, and then click **Remove packages**.

Clearing a deployment area

If you want to create a new deployment in an existing deployment area, you can clear the area of its contents.

Procedure

1. Log in to Spotfire Server and click **Deployments & Packages**.
2. In the "Deployment areas" pane, select the deployment area that you want to clear.
3. In the "Software packages" pane, click **Clear area**.

Deleting a deployment area

You can delete a deployment area that is no longer needed. The software packages in that area will be removed as well.

Procedure

1. Log in to Spotfire Server and click **Deployments & Packages**.
2. In the "Deployment areas " pane, select the check box in front of the deployment area you want to delete.



It is not possible to delete the area that is set as the default deployment area.

3. In the "Deployment areas " pane, click **Delete**.

Scheduled updates to analyses

For analyses that contain links to large amounts of data, downloading fresh data can take a significant amount of time. Scheduled updates save time by downloading the latest data before users need it.

Based on settings in Spotfire Server, or on messages that the server receives from an external source, selected analyses can be preloaded with fresh data, stored on specific Spotfire Web Player instances, and then made available to users as needed.

For example, in the case of sales data that is tallied at the end of the day, you could schedule the update to occur overnight so that users can quickly access the analysis first thing in the morning, when they log in. Or, in the case of a large analysis that users tend to refer to several times during the day, you could schedule an update every 20 minutes.

You can trigger updates in two ways:

- In Spotfire Server you can create rules that specify the analysis to preload, when to do it, whether the new data is automatically displayed to the end user, and so on.
- Using TIBCO Enterprise Message Service™ (EMS) or a web service, you can create "event-driven updates" that are triggered by an external process. For more information about event-driven updates, see [Creating a scheduled update by using TIBCO EMS](#) or [Creating a scheduled update by using a web service](#).

When scheduling an update in Spotfire Server, you can configure the following options:

- The days of the week that the update runs.
- The times of day between which the updated analysis is available to end users.
- How often the server checks for new data.
- The *resource pool* on which to preload the analysis, and the number of Spotfire Web Player instances that should be available for users opening the analysis.
- Whether the updated data is automatically displayed in the user's copy of the analysis, or the user decides when to refresh the information.
- Whether to allow cached and pre-computed data when the analysis is reopened.

On the Overview page, the "Scheduled updates" pane gives you the basic status of your scheduled updates.

In the **Rules** list you can identify scheduled updates (as opposed to *routing rules*) by their **Type (File)** and the fact that a schedule is displayed under **Schedule** in the list.

You can also view the Activity and Notifications pages in Scheduling & Routing to monitor job status.

Creating a scheduled update by using Spotfire Server

In Spotfire Server, you can configure and run automated data updates to existing analysis files. This saves time for end users because they do not have to wait for the new data to download when they open the analysis.

Prerequisites

- The analysis file to be updated must be in the Spotfire library.
- The scheduled updates user service account (scheduledupdates@SPOTFIRESYSTEM) must have the following library permissions:
 - **Browse & Access** permissions to the analysis.
 - Permissions to access the folder(s) that hold the information link object.
 - Permission to access the data source object.

To set library permissions, use the tools in Spotfire Analyst.



Alternatively, you can use the [copy-library-permissions](#) command to copy library permissions from another user or group.

The following tasks are optional, but you may want to complete them before creating the scheduled update:




- If you want this update to run according to a schedule (or several schedules) that you plan to reuse, create the schedules first; for instructions, see [Creating a reusable schedule](#).
- If you want the updated file to open on specific instances of the Spotfire Web Player, create a *resource pool* containing those instances; for instructions, see [Creating a resource pool](#).



If you are creating a scheduled update for an analysis that is based on data from a prompted or personalized information link, see [Scheduled updates with prompted or personalized information links](#).

For general information, see [Scheduled updates to analyses](#).

Procedure

1. Log in to Spotfire Server and click **Scheduling & Routing**.
 2. In the Rules pane, click **Create rule**.
 3. Under **Type**, select **File**, and then click **Next**.
 4. Enter a name for the rule and select the file that you want to update.
 5. Under **Select resource pool**, do one of the following:
 - If you do not want to set a specific resource pool on which to open the analysis, leave the **System Default** routing selected.
 - If you want the analysis to open on a specific resource pool, select it.
- 

If a scheduled update rule indicates that a file should open on a specific resource pool, this rule overrides any routing rules (for a group or an individual user) that specify a different resource pool for the user who opens the updated file.
6. Optional: Set a priority. This setting comes into effect if two or more scheduled updates are scheduled to occur at the same time. **0** is the highest priority.
 7. To set a schedule, do one of the following:

- To update the analysis based on a schedule that has already been created or several schedules, select **Use saved schedule** and then, in the "Select schedule" dialog, select the schedule or schedules that you want to use.
- To create a "unique schedule" for this rule (a schedule that will not be available for reuse), select **Use custom schedule**. For instructions on setting up the schedule, see [Creating a reusable schedule](#).



Analyses are always updated and loaded at the beginning of each scheduled start time, in addition to the reloads that are set in the **Check for updates every** field. If a scheduled update is scheduled for 24 hours a day/7 days a week, with **Check for updates every** set to 0, the analysis is loaded only once, when the rule is initially executed.

8. If you want the rule to be disabled initially, select the **Disable rule** check box in the bottom right of the dialog. You can enable the rule later, on the Scheduling & Routing page.
9. Optional: If you want to do one of the following, click **Additional properties**:
 - Set the number of Spotfire Web Player instances for this rule.
 - Switch the client update method from automatic to manual.
 - Disallow cached and pre-computed data.

For details, see [Additional settings for scheduled updates](#).

10. In the "Create rule" dialog, click **Save**.



If you are unable to save the information you entered, and your library files are stored externally on Amazon Web Services S3 (AWS), see [Forcing Java to use IPv4](#).

Result

The rule is displayed in the **Rules** list.

Additional settings for scheduled updates

In addition to basic information about the analysis that you want to update and when you want the update to occur, several additional property settings are available in Spotfire Server.

Setting the number of Spotfire Web Player instances to make available for a scheduled update

By default Spotfire Server uses one of the available Spotfire Web Player instances when users open a scheduled update file. To load balance or to change the resource load of a particular analysis, the administrator can set the number of instances on which the updated analysis can open.


Procedure

1. Log in to Spotfire Server and click **Scheduling & Routing**.
2. Do one of the following:
 - If you want to change this property for an existing scheduled update, under **Rules** select the update and click **Edit**.
 - If you are creating a new scheduled update, at the bottom of the second Create rule dialog, click **Additional properties**.
3. In the Additional properties dialog, under **Number of instances** select a number.
4. Click **Update** and then **Save**.

Switching the scheduled update method from automatic to manual

When the scheduled update method is set to manual, users decide when to incorporate new data in the analysis.

Procedure

1. Log in to Spotfire Server and click **Scheduling & Routing**.
2. Do one of the following:
 - If you want to set this property for an existing scheduled update, under **Rules** select the check box next to the update rule and click **Edit**.
 - If you are creating a new scheduled update, at the bottom of the second Create rule dialog, click **Additional properties**.
3. In the Additional properties dialog, under **Update method**, indicate how users should receive the updated data:
 - **Automatic**—The new data is automatically displayed in the analysis when a user opens it.
 - **Manual**—A Refresh icon  on the title bar of the analysis indicates that an updated version is available. When the user clicks the icon, the analysis is updated.
4. Click **Update** and then **Save**.

Disallowing cached and precomputed data in individual scheduled update files

If your Spotfire environment is set up to use disk caching and precomputations of data to shorten the time it takes for an updated analysis to reopen in a Spotfire Web Player after the analysis closes, this setting may prevent the latest data from appearing in the reopened analysis. You can turn this setting off for individual scheduled update files.



By default, cached and precomputed data is *not* enabled. To enable this feature, see [Enabling cached and precomputed data for scheduled update files](#).

Procedure

1. Log in to Spotfire Server and click **Scheduling & Routing**.
2. Do one of the following:
 - If you want to change these properties for an existing scheduled update, under **Rules** select the update, click **Edit**, and then click **Additional Properties**.
 - If you are creating a new scheduled update, at the bottom of the second Create rule dialog, click **Additional Properties**.
3. In the Additional properties dialog, under **Caching**, clear the check boxes of the settings you want to turn off.
4. Click **Update** and then **Save**.

Result

The analysis will always reflect the latest data but it may reopen more slowly.

Scheduled updates with prompted or personalized information links

Scheduled updates are intended mainly for use with analyses that were set up using ordinary information links to load data. If you set up scheduled updates for an analysis that is based on data from a prompted or personalized information link, there are special issues to consider.

When a user opens an analysis that is based on a prompted information link, the user selects a certain view of the data to be loaded. In the same way, when a user opens an analysis that is based on a personalized information link, the data loaded is determined by the permissions of the user who logs in.

However, when a scheduled update of this file occurs, the update causes the analysis to reload based on the prompted values that were specified when the file was originally saved, and the permissions of the user that the administrator set up to programmatically run the scheduled update. This means that users with an analysis already open will see a different selection of data the next time that they update the analysis because the scheduled update has in fact updated the underlying data on the server.

You should be especially careful when setting up scheduled updates for analyses with personalized information links. If the user you specify for the scheduled updates has access to more data than the intended end users of the analyses, these end users may see more data than they have access to; they will see all the data that is available to the user specified for scheduled updates.

Editing a scheduled update

You can edit most properties of a scheduled update at any time. To change the analysis file or the resource pool in a scheduled update, however, you must first disable the rule.

Procedure

1. Log in to Spotfire Server and click **Scheduling & Routing**.
2. In the **Rules** pane, select the scheduled update that you want to edit.
3. Optional: If you want to change the rule's analysis file or resource pool, click **Disable**.
4. In the **Rules** pane, click **Edit** and make your changes.
5. Click **Save**.
6. Optional: If you disabled the rule in step 3, click **Enable** to make it active again.

Creating a reusable schedule

You can create and save schedules that you plan to reuse in scheduled updates to analyses. If a schedule will only be used once, you can set it when you create the update rule.

Procedure

1. Log in to Spotfire Server and click **Scheduling & Routing**.
2. In the "Saved schedules" pane, click **Create schedule**.
3. In the "Create schedule" dialog, enter a name for the schedule.
4. Under **Repeat**, indicate the days on which you want the update to run by selecting the appropriate check boxes.
5. Under **Start** and **End**, enter the times between which the updated analysis should be available to end users (on the days that you indicated in the previous step).
6. Under **Time zone**, select the time zone for the times that you entered in the previous step.

- Under **Check for updates every**, select how often you want Spotfire Server to check whether the analysis file or its underlying data has changed. If the analysis or data has changed, the server updates the pre-loaded file.



Analyses are always updated and loaded at the beginning of each scheduled start time, in addition to the reloads that are set in the **Check for updates every** field. If a scheduled update is scheduled for 24 hours a day/7 days a week, with **Check for updates every** set to 0, the analysis is loaded only once, when the rule is initially executed.

- Click **Save**.

Result

The new schedule is displayed in the **Saved schedules** list.

Manually updating a file outside of its update schedule

If you do not want to wait for a file to be updated according to its schedule, you can trigger an update manually.

Prerequisites

There is a scheduled update for the file that you want to manually update.

Procedure

- Log in to Spotfire Server and click **Scheduling & Routing**.
- On the **Overview** page, under **Rules**, select the file.
- Click **Reload**.

Copying routing rules and schedules from one site to another

You can copy all the routing rules and saved schedules from one site in your Spotfire environment to another site in the same environment by using the **copy-rules-to-site** command. This is helpful when setting up local access points for users who are located in different regions.



This procedure copies rules that were created in the Spotfire Server administration interface. Scheduled updates that are triggered externally, for example by TIBCO Enterprise Message Service (EMS), are not copied.

Procedure

- Open a command line as an administrator and go to the *server installation dir/tomcat/bin* directory.
- On the command line, enter the **copy-rules-to-site** command, specifying the options needed.
Example:

```
config copy-rules-to-site --bootstrap="C:\Work\server\bootstrap.xml" --keystore-
file="C:\Work\nm\trust\keystore.p12" --source-site-name=NewYork --target-site-
name=SanFran --tool-password=Spotfire rule-conflict-resolution=replace --use-
default-resource-pool=true --disabled=false --test-run=false
```

For information on the command options, see [copy-rules-to-site](#).

Result

In this example, the rules and saved schedules from the NewYork site are reproduced in the SanFran site. On the computer where you ran the command, the `impex.rules.log` file, which provides

information about the copy process, is available in the following directory: `<installation_dir>/tomcat/logs`.

Exporting routing rules and schedules for import in a different Spotfire environment

You can export the routing rules and saved schedules from a Spotfire Server to a JSON file. Then, to prepare for a rolling update or to test and validate a new version of Spotfire, you can import the JSON file on a different Spotfire environment.



This procedure exports rules that were created in the Spotfire Server administration interface. Scheduled updates that are triggered externally, for example by TIBCO Enterprise Message Service (EMS), are not exported.

Procedure

1. Open a command line as an administrator and go to the `server installation_dir/tomcat/bin` directory.
2. On the command line, enter the **export-rules** command, specifying the options needed to export the data to a JSON file.

Example:

```
config export-rules --bootstrap-config="C:\Work\Spotfire\bootstrap.xml" --tool-
password=Spotfire --keystore-file "C:\Work\nm\trust\keystore.p12" --force
```

For information on the command options, see [export-rules](#).

Result

In this example, the `rules.json` file containing your scheduled updates and routing rules is available in the `server installation_dir/tomcat/bin` directory.

Importing routing rules and schedules from a different Spotfire environment

After you have exported the routing rules and saved schedules from a Spotfire Server to a JSON file, you can import the JSON file in a different Spotfire environment to prepare for a rolling update, for example, or to test and validate a new version of Spotfire.

Prerequisites

- You have exported the rules and schedules from the original server to a JSON file; for instructions, see [Exporting routing rules and schedules](#).
- At least one server in the target environment is running.
- The analysis files referred to in the rules have been added to the target environment.
- The users and groups referred to in the rules have been created in the target environment.
- If you want the target environment to use resource pools that are named the same as the resource pools in the original environment, and you want the import to use the same resource pool assignments as the original environment, create the resource pools before importing the file.



Your other options are to assign the imported rules to the default resource pool, or to another resource pool; for details, see the `-r` option and the `-u` option in [import-rules](#).

Procedure

1. Open a command line as an administrator and go to the `<server installation_dir>/tomcat/bin` directory.

2. On the command line, enter the **import-rules** command, specifying the options needed.

Example:

```
config import-rules --bootstrap-config="C:\Work\Spotfire\bootstrap.xml" --
keystore-file="C:\Work\nm\trust\keystore.p12" --rule-conflict-resolution=replace
--schedule-conflict-resolution=rename --use-default-resource-pool=true --test-
run=false
```

For information on the command options, see [import-rules](#).



If you want the chance to address import errors up front, you can enable the **--test-run** option. This option provides a preview of any import errors before the actual import takes place.

Result

In the previous example, the rules and saved schedules are imported and assigned to the default resource pool. On the server where you ran the command, the `impex.rules.log` file, which provides information about your import, is available in the following directory: `installation_dir/tomcat/logs`.

Disabling or deleting scheduled updates and routing rules

Disabling a scheduled update or other rule makes the rule inactive until you activate it again. Deleting a rule removes it from the database.

Procedure

1. Log in to Spotfire Server and click **Scheduling & Routing**.
2. Select the check box next to the rule or rules that you want to disable or delete.
3. Click **Disable** or **Delete**.
If you disabled a rule, it appears grayed out in the list.

Deleting schedules

Deleting a schedule removes it from the database and cancels any scheduled updates that use the schedule.

Procedure

1. Log in to Spotfire Server and click **Scheduling & Routing**.
2. Select the check box next to the schedule or schedules that you want to delete.
3. Click **Delete**.



If deleting the schedule will cancel any scheduled updates, Spotfire Server lists the affected rules.

Creating a scheduled update by using TIBCO EMS

You can create scheduled updates that are triggered by messages from TIBCO Enterprise Message Service (EMS). In Spotfire Server, the external updates configuration takes place in the server, and the

updates are sent to the server. Spotfire Server then sends the updates to the appropriate web player service(s).

Prerequisites

- EMS is installed on a computer.
- The following files, which are located in your TIBCO EMS installation in the `lib` folder, must be copied to the Spotfire Server classpath on the server computer. If your implementation is clustered, the files must be copied to each computer in the cluster. If your implementation includes sites, the files must be copied to each server in the sites that will receive scheduled updates via EMS.
 - `jms.jar` or `jms-2.0.jar` (depending on the version)
 - `tlbjms.jar`
 - `tibcrypt.jar`

Procedure

1. On the Spotfire Server command line, use the [config-external-scheduled-updates](#) command to configure the server to accept the EMS messages. (For details on using the Spotfire command line, see [Executing commands on the command line](#).) Include the following parameters:
 - Set the `ems-enabled` value to "true".
 - Set the server and port to the computer and port on which EMS is currently running. Use this configuration:


```
<server-url>tcp://localhost:7222,tcp://localhost:7222</server-url>
```

This enables the reconnect parameters. For more information about this value, see "Fault Tolerance" in the [TIBCO EMS documentation](#).
 - Set the `client-id` value to indicate which server or site will handle the scheduled updates:
 - If your Spotfire implementation includes a clustered server deployment (but not sites), set the `client-id` to a unique value in the cluster. In this case, the first server to connect to EMS will handle all the scheduled updates received via EMS.
 - If your Spotfire implementation includes sites, each site that will receive scheduled updates via EMS must have its own `client-id`.

Command example

```
config config-external-scheduled-updates -e true -s tcp://localhost:7222 -i
clientId1 -t scheduled_updates -S "first site"
```

Example of the resulting section in the server configuration file (`configuration.xml`):

```
</external-updates>
  <external-updates site="first site" operation="override">
    <ems-enabled>true</ems-enabled>
    <server-url>tcp://localhost:7222</server-url>
    <client-id>clientId1</client-id>
    <topic>scheduled_updates</topic>
    <reconnect-attempt-count>10</reconnect-attempt-count>
    <reconnect-attempt-delay-milliseconds>1000</reconnect-attempt-delay-
milliseconds>
    <reconnect-attempt-timeout-milliseconds>1000</reconnect-attempt-timeout-
milliseconds>
    <keep-alive-minutes>10</keep-alive-minutes>
  </external-updates>
```

2. In EMS, create the message. Include the following parameters:
 - Path (required)

- ClientUpdate
- KeepAliveMinutes
- ResourcePoolName



If the following statements are true, the resource pool value in the existing rule takes precedence:

- There is an existing rule for the same file.
- The existing rule was created in Spotfire Server.
- The existing rule specifies a resource pool.
- The existing rule is enabled.



For the ClientUpdate parameter, the value (manual or automatic) that is defined in the external rule takes precedence. If the external update does not specify a value, or if the specified value is invalid, the value from an enabled rule is used, if available.

3. Send the EMS request. For details, see the [TIBCO EMS documentation](#).

Creating a scheduled update by using a SOAP web service

You can create scheduled updates that are triggered by messages from a SOAP web service. In Spotfire Server, the external updates configuration takes place in the server, and the updates are sent to the server. Spotfire Server then sends the updates to the appropriate web player service(s).

Prerequisites

The user calling the web service must have the following:

- Administrator privileges.
- One of the following:
 - Membership in the API User group.
 - The "External updates of analysis in Spotfire web clients" (under "TIBCO Spotfire Consumer") license enabled.

Procedure

1. Edit the Spotfire Server configuration file to enable public web service API access:

```
<public-api>
  <web-services>
    <enabled>true</enabled>
  </web-services>
</public-api>
```

2. Configure the SOAP request using these parameters:

- Web service address: `http://<servername_and_port>/spotfire/ws/pub/UpdateAnalysisService`
- WSDL located at: `http://<servername_and_port>/spotfire/ws/pub/UpdateAnalysisService?wsdl`

You now have the option of setting the *resource pool* (a set of specific Spotfire Web Player instances on which to preload the updated analysis file). However, if the following statements are true, the resource pool value in the existing rule takes precedence:



- There is an existing rule for the same file.
- The existing rule was created in Spotfire Server.
- The existing rule specifies a resource pool.
- The existing rule is enabled.



For the `ClientUpdate` parameter, the value (manual or automatic) that is defined in the external rule takes precedence. If the external update does not specify a value, or if the specified value is invalid, the value from an enabled rule is used, if available.

Sample request

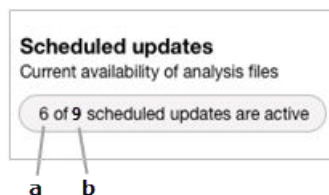
```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ext="http://spotfire.tibco.com/ws/2015/08/externalScheduledUpdate.xsd">
  <soapenv:Header/>
  <soapenv:Body>
    <ext:loadAnalysis>
      <!--Optional:-->
      <updateAnalysis>
        <!--Optional:-->
        <path>/A121-02 BostonMatrix</path>
        <!--Optional:-->
        <clientUpdate>manual</clientUpdate>
        <keepAliveMinutes>5</keepAliveMinutes>
        <!--Optional:-->
        <!--resourcePool>Main</resourcePool-->
      </updateAnalysis>
    </ext:loadAnalysis>
  </soapenv:Body>
</soapenv:Envelope>
```

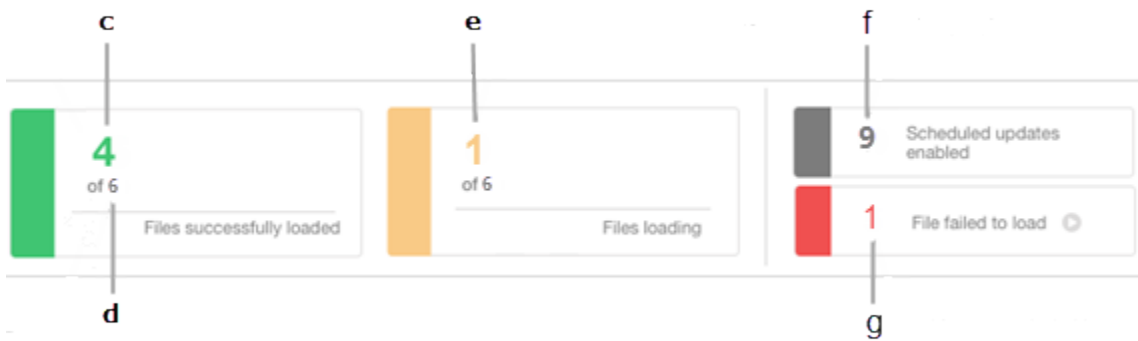
3. Send the request with the user that was configured for this purpose.

Scheduled updates monitoring




The Scheduling & Routing area of Spotfire Server provides several ways of monitoring the success of your scheduled updates.

The "Scheduled updates" pane at the top of the Overview page summarizes the current state of your scheduled updates:





Details about the Scheduled updates summary

a	Number of active scheduled updates <p>The number of scheduled update rules that are enabled and currently within their schedule window. This means that the files that are attached to these rules are scheduled to be loaded now, so that end users can view them without waiting for the data to download.</p>
b	Number of enabled rules <p>The total number of file rules that are enabled in your Spotfire implementation. This includes file rules without schedules.</p>
c	Number of scheduled update rules that ran successfully <p>The number of scheduled update files that end users can currently view without waiting for the data to download. These analyses have been updated (if new data was available) and loaded on at least one Spotfire Web Player instance.</p> <div>  <p>This does not guarantee that the file was loaded on the number of Spotfire Web Player instances that is specified in the rule.</p> </div>
d	The same as a .
e	Number of scheduled update files that are currently being loaded <p>The number of scheduled update files that are currently being loaded and so not yet available to end users.</p> <div>  <p>Scheduled update files that are waiting to load are not counted.</p> </div>
f	The same as b .
g	Number of failed scheduled updates <p>The number of unsuccessful scheduled updates. (The analysis files attached to these rules should have been updated and loaded on at least one Spotfire Web Player instance.)</p> <div>  <p>After a scheduled update fails, it is included in this number until it is scheduled to load again, or until it is manually reloaded.</p> </div>



You can click the large boxes in the Scheduled updates pane to view the scheduled update rules that each box refers to.

On the Activity page, you can view the status, date, and time of each file update attempt. Click the arrow to the left of the line to view additional details, any messages that were generated, and a link to relevant logs.

Important messages are listed on the Notifications page. An information symbol on the **Notifications** tab, and on the Scheduling & Routing image on the main server page, indicates that there is a new notification.

Changing the priority of a rule

Spotfire Server uses rule priorities if two or more rules are executed at the same time.

Procedure

1. Log in to Spotfire Server and click **Scheduling & Routing**.
On the **Overview** page, under **Rules**, the scheduled updates and routing rules are listed in priority order.
2. Select the rule whose priority you want to change and then do one of the following:
 - Drag the rule to a new position in the list.
 - On the right end of the row, click the **More** menu (...) and then select **Move to top** or **Move to bottom**.
 - Click **Edit** and then, in the "Edit rule" dialog, enter a new priority number under **Set a priority**.

Changing the number of retries for failed scheduled updates

By default, Spotfire Server retries a failed scheduled update ten times. Using the command-line interface, you can set a different limit for the number of times that a scheduled update is retried if it initially fails.



This property was previously set by using the `stopUpdatesAfterRepeatedFail` setting in the `Spotfire.Dxp.Worker.Web.config` file.

Procedure

1. Open a command-line interface and export the active configuration (the `configuration.xml` file) by using the `export-config` command. (For details on using the Spotfire command line, see [Executing commands on the command line](#).)
2. Use the `config-scheduled-updates-retries` command to set the retry limit.
Example:

```
config config-scheduled-updates-retries --stop-updates-after-repeated-fail-enabled=true --fails-before-stop=X
```

 where X is the number of times to retry the update.
3. Import the configuration file back to the Spotfire database by using the `import-config` command.
4. Restart the Spotfire Server service.

Changing how often the scheduled update history is cleared

If your organization runs many scheduled updates, history records can quickly pile up in the database. Spotfire Server automatically purges the history once a week, but you can change how often this occurs by editing the `configuration.xml` file.

Procedure

1. Export and open the Spotfire Server configuration file; for general instructions, see [Manually editing the Spotfire Server configuration file](#).
2. Do one of the following:
 - If you are editing a Spotfire Server 7.5 or later configuration file, change the number "7" (which indicates 7 days) in the following section:


```
<scheduled-updates>
  <!-- All scheduled updates details older than the specified number of days
  will be automatically deleted.
  Default: one week, value must be strictly positive.-->
  <purge-history-older-than>7</purge-history-older-than>
</scheduled-updates>
```
 - If you are updating an existing configuration file from a previous version of Spotfire Server, add the entire `<scheduled-updates>` section to the file and then change the number of days between history purges.
3. Save the configuration file and import it back to the server; for instructions, see [Manually editing the Spotfire Server configuration file](#).

Common analysis loading errors

The following are the most common error codes and messages that are displayed when an analysis file does not load successfully.

- SPOT-10001 FileCorruptMissingRequiredEntry
Server was unable to read the uploaded file because it is not a valid DXP file.
- SPOT-10002 IncompatibleVersion
Unsupported file version.
- SPOT-10003 FileCorrupt
Server was unable to read this file because it is not a valid DXP file.
- SPOT-10004 IncompatibleDevelopmentVersion
Server was unable to read the file. The file was saved with a development version of Spotfire and contains features that are not supported by this version.
- SPOT-20000 LoadFileUnknownError
Server was unable to read the file.
- SPOT-20001 IOException
An I/O error occurred when the server attempted to open the file.
- SPOT-30001 LoadFileNoPermissions
Server was denied access to the file.
- SPOT-40001 LoadFileOutOfMemory
Server was unable to load the file due to insufficient memory.
- SPOT-50001 LibraryFailedLoad

Server could not load the analysis.

- SPOT-70001 FailedToExecuteDataSource

Server was unable to execute the data query.

- SPOT-70002 CouldNotCreateDatabaseConnection

Server was unable to access one or more data sources.

- SPOT-70003 FailedToOpenInformationLink

Server was unable to load the information link.

- SPOT-100000 UnknownError

Server was unable to read the file.

Routing rules

A routing rule specifies the *resource pool* on which an analysis opens. You can create routing rules to set a *resource pool* on which to open analyses that are requested by members of a specific group, or by a specific user. You can also set a resource pool for a specific analysis, regardless of who requests it.

You can use routing rules to fine-tune resource management, but their use is optional.

Specific reasons for creating routing rules include the following:

- Define an exclusive resource pool for a critical analysis so that it can be updated and viewed without interference from other analyses and user requests.
- Define a resource pool for management so that they can view and work with analyses without waiting.
- Define a resource pool for users who are trying out a new version of Spotfire.
- Load an analysis on several Spotfire Web Player instances to handle a large number of users.

The default routing rule

The default routing rule indicates the resource pools on which all analyses are opened, unless the analysis itself, or the user who is requesting it, is subject to another routing rule. By default, the default routing rule includes all the services and instances that are available in your Spotfire implementation.

You can edit default routing to include only certain services and instances, but the rule cannot be deleted.

The default routing rule is always displayed at the bottom of the **Rules** list on the **Scheduling & Routing** page.

Creating a routing rule

You can create routing rules that apply to user groups, individual users, or specific analysis files.

Prerequisites


- Create the resource pool that you want to specify for the rule; see [Creating a resource pool](#).
- If you are creating a rule for an analysis file, the file must be in the Spotfire library.

For general information, see [Routing rules](#).

Procedure

1. Log in to Spotfire Server and click **Scheduling & Routing**.
2. In the **Rules** pane, click **Create rule**.
The Create rule dialog opens.

3. Under **Type**, do one of the following and then click **Next**:
 - If you want to set a *resource pool* on which to open analyses that are requested by members of a specific group, select **Group**.
 - If you want to set a resource pool on which to open analyses that are requested by an individual user, select **User**.
 - If you want to set a resource pool on which to open a specific analysis file, select **File**.
4. Enter a name for the rule and then do one of the following:
 - Select the group to which the rule applies.
 - Select the user to which the rule applies.
 - Select the file to which the rule applies.
5. Under **Select resource pool**, select the resource pool on which the analyses that are affected by this rule should open.



If a scheduled update rule indicates that a file should open on a specific resource pool, that rule overrides any routing rules (for a group or an individual user) that specify a different resource pool for the user who opens the updated file.
6. Optional: Set a priority. This setting comes into effect if two or more rules occur at the same time. **0** is the highest priority.
7. If you want the rule to be disabled initially, select the **Disable rule** check box in the bottom right of the dialog. You can enable the rule later on the Scheduling & Routing page.
8. Click **Save**.

Result

The rule is displayed in the **Rules** list.

Monitoring and diagnostics

Spotfire Server provides a wide range of information to help you manage and troubleshoot your implementation.

Server and node logging levels

To help locate and respond to issues that can arise in your Spotfire implementation, you can easily change the amount and types of server and node logs that Spotfire Server collects, without leaving the administration interface .

Spotfire Server provides four logging templates that correspond to the most common logging requirements. Each server and node in your implementation can be set to one of these logging levels.

Logging level	Description
Standard (default)	This logging level captures information-level data about runtime events. The <code>log4j2.xml</code> file controls this logging level.

Logging level	Description
Debug	<p>This level captures detailed debugging information as well as warnings, errors, and other details in the <code>server.log</code>.</p> <p>The <code>sql.log</code> captures detailed SQL Server information.</p> <p>If the server is started from a command prompt or shell, the output to the command prompt or shell is included in the server log. The <code>logging-debug.properties</code> template controls this logging level.</p>
Minimal	<p>This level captures basic information about errors and warnings. The <code>logging-minimal.properties</code> template controls this logging level.</p>
Trace	<p>This level captures more detailed information than the debug level. Because this logging level is very comprehensive, it should be used carefully. The <code>logging-trace.properties</code> template controls this logging level.</p>
Custom	<p>This level is used by Spotfire support. It makes it possible to upload customized logging templates.</p>



Administrators are strongly advised to use the included logging templates. Do not modify or delete these templates.

For a list of logging levels for services, see [Service log levels](#).

Changing server and node logging levels

When Spotfire Server alerts you to an issue in your implementation, you can switch to a more complete logging level from within the Monitoring & Diagnostics area of the administration interface .

Prerequisites

You must have administrative credentials for Spotfire Server.



Alternatively, you can change logging levels by using the [set-logging](#) command. For information on using the command line, see [Executing commands on the command line](#).



It is a good practice to back up the existing logs and clear the logs folder before capturing the debug logs.

Procedure

1. Log in to Spotfire Server and click **Monitoring & Diagnostics**.
2. On the Overview page, select the server(s) or the node(s) whose logging level you want to change.
3. Click **Set log configuration**, select a different logging level, and click **Set**.

Result

The changes appear in the **Log configuration** column.



When the troubleshooting is completed, you should switch back to a lower logging level. You can return quickly to the **Standard (default)** level by selecting the server or node and clicking **Reset log configuration**.

Changing the logging level for a server or node that is not running

When a server or node is not running, you can increase its logging level to capture more troubleshooting data.



Best practice is to back up the existing logs and clear the logs folder before capturing the debug logs.

Procedure

1. On the computer that is hosting the server or node whose logging level you want to change, navigate to the directory that contains the logging templates.
 - For a Spotfire Server, the default location is *server installation dir\tomcat\spotfire-config*.
 - For a node manager, the default location is *node manager installation dir\nm\config\log-config*.
2. If the directory already contains a `logging-levels.properties` file, delete it.
3. Make a copy of the logging template that you want to apply to the server or node, and name the copy "logging-levels.properties". The available templates are `logging-debug.properties`, `logging-minimal.properties`, and `logging-trace.properties`.
4. Open the `logging-levels.properties` file in a text editor or an XML editor.
5. In the `logging-levels.properties` file, add the following line of code to the top of the file, replacing *template name* with the name of the template file that you copied:


```
ActiveConfig=template name
```

Example

```
ActiveConfig=logging-debug.properties
```
6. Save and close the `logging-levels.properties` file.
7. Restart the Spotfire Server service or the Spotfire Node Manager service for the changes to take effect.

Result

The server or node captures the logging information that is indicated in the `logging-levels.properties` file.



When the troubleshooting is completed, switch back to a lower logging level.

Switching back to the Standard (default) logging level

After troubleshooting an issue, you can quickly return to the Standard (default) logging level.

Procedure

1. Log in to Spotfire Server and click **Monitoring & Diagnostics**.
2. On the Overview page, select the server(s) or the node(s) whose logging level you want to return to the default.
3. Click **Reset log configuration**.

Result

The changes appear in the Log configuration column.

Accessing Spotfire Server and node logs

You can view and download various types of Spotfire Server and node logs. For more information about available logs, see the following topics.

- [Spotfire Server logs](#)
- [Node logs](#)
- [Web Player service logs](#)

Procedure

1. Log in to Spotfire Server, and then click **Monitoring & Diagnostics**.
2. On the **Overview** page, under **Spotfire Servers** or **Nodes**, locate the server or node for which you want to access logs, and click **View logs**.
The Logs page opens.
3. In the **Select log file to view** drop-down list, select the log file you want to view.
The selected log file is shown in the "View logs" pane.

You can export the log file by clicking **Download full log file**.

Spotfire Server logs

The server logs store important diagnostic information about the Spotfire Server. The information can help in troubleshooting and resolving issues.

The Spotfire Server runs by default at a basic logging level. This can be elevated when needed; for instructions, see [Changing server and node logging levels](#).

The most important log is the `server.log`. This log file stores information about all activities on the server and can be very handy in troubleshooting issues.

If you encounter an issue with Spotfire Server, provide the server logs to Spotfire Support when you enter the support request.

The following log files are available.

Log file	Description
<code>access.log</code>	Provides information about client access and access attempts to the server and files in the library.
<code>actionslogs\actionlog.log</code>	Provides information about user actions.
<code>catalina.<date>.log</code>	An Apache Tomcat log file.
<code>commons-daemon.<date>.log</code>	An Apache Tomcat procrun log. See https://commons.apache.org/proper/commons-daemon/procrun.html for more information.
<code>impex.log</code>	Provides information about Spotfire library imports and exports.
<code>impex.rules.log</code>	Provides information about importing, exporting, and copying scheduled updates and routing rules between computers running Spotfire Server.

Log file	Description
<code>isusage.log</code>	Provides information about Information Services usage.
<code>library.log</code>	Provides information about Spotfire Library usage.
<code>localhost.<date>.log</code>	An Apache Tomcat log file.
<code>performance.monitoring.log</code>	Spotfire Server performance metrics.
<code>s3request.log</code>	Provides information about Amazon S3 storage.
<code>server-diagnostics.log</code>	Provides diagnostic information about server properties.
<code>server.log</code>	Provides information about all activity on the server except those events recorded in <code>access.log</code> .
<code>sessions.log</code>	Provides information about new sessions and their originating IP-address and user-agent.
<code>soap.log</code>	Provides information about SOAP communication.
<code>sql.log</code>	Provides information about executed SQL queries performed when an information link is executed.
<code>startup.log</code>	Provides information about JAR files loaded on server startup.
<code>tools.log</code>	Information about activity in the configuration tool and on the command line. If you run any configuration commands at the command prompt or use the administration console, this is the log that captures that information.
<code>tssversion-stderr.<date>.log</code>	An Apache Tomcat log file.
<code>tssversion-stdout.<date>.log</code>	An Apache Tomcat log file.
<code>usage.log</code>	Provides information about client access and access attempts to the server.
<code>user-interface.log</code>	Provides information about errors generated by the server web client.

For more information about other available logs, see the following topics.

- [Node logs](#)
- [Web Player service logs](#)

Location of server logs

Find server logs at different locations.

Spotfire Server logs

Spotfire Server logs are located under `<installation_dir>\tomcat\logs` folder.

Example: `C:\tibco\tss\<version>\tomcat\logs`

Spotfire Server Upgrade logs

Spotfire Server Upgrade logs are located under `<installation_dir>\tools\upgrade\logs` folder.

Example: `C:\tibco\tss\<version>\tools\upgrade\logs`

To change these default locations, see [Changing the default location of server logs](#).

Changing the default location of server logs

You can change the default directory location for logs by providing a configuration setting in the Tomcat webapp.

Perform this task on the server where Spotfire Server is installed.

Prerequisites

You must have administrative privileges on the Spotfire Server.

Procedure

1. On the server where Spotfire Server is installed, locate the file `<installation_dir>\tomcat\webapps\spotfire\WEB-INF\web.xml`.
2. Locate and modify the following parameter.

```
<context-param>
  <param-name>log.dir</param-name>
  <param-value>../../logs</param-value>
</context-param>
```

Node logs

The node logs store important diagnostic information. The information can help in troubleshooting and resolving issues.

To view node manager logs, see [Accessing Spotfire Server and node logs](#).

The following table is a partial list available from the **Select log file to view** drop-down list found in the node Log files page. These are the most important node manager log files. You can find information for other logs on this list in the following topics:

- [Spotfire Server logs](#)
- [Service logs](#)

Log file	Description
jetty.log	The output from the jetty container that the node manager runs within (similar to catalina.log).
nm.log, nm.log.n (<i>n</i> is a number between 1 and the maximum number of logs that is configured to roll through.)	Information about all activity on the node.
nodemanager.txt	Generated only when you create a troubleshooting bundle . If you download another troubleshooting bundle at a later time, this log file is overwritten with newer data.

Log file	Description
service-<guid>.log	STDOUT from the service with the specific guid. This is a service instance log, and not an installation log.
winsw.err.log	STDERR output captured by the Windows service handler.
winsw.out.log	STDOUT output captured by the Windows service handler.



If you have an issue with the node manager, the nm.log generally provides the needed details.

Enabling Kerberos debug logging

You can troubleshoot issues with the Kerberos authentication by enabling Kerberos debug logging.



It is a good practice to back up the existing logs and clear the logs folder before capturing the debug logs.

Procedure

1. Export and open the configuration.xml file from <server installation dir>\tomcat\bin folder in an XML editor or a text editor; for details, see [Manually editing the Spotfire Server configuration file](#).
2. In the configuration.xml file, locate the configuration block:

```
<jaas-config>
  <name>spotfirekerberos</name>
  <entries>
    <entry>
      <login-module-name>com.sun.security.auth.module.Krb5LoginModule</login-module-name>
      <control-flag>required</control-flag>
      <options>
        <option>
          <key>debug</key>
          <value>false</value>
        </option>
        <option>
          <key>useKeyTab</key>
          <value>true</value>
        </option>
        <option>
          <key>principal</key>
          <value>HTTP/spotfiretss@TEST.COM</value>
        </option>
        <option>
          <key>storeKey</key>
          <value>true</value>
        </option>
        <option>
          <key>keyTab</key>
          <value>${java.home}/lib/security/spotfire.keytab</value>
        </option>
      </options>
    </entry>
  </entries>
</jaas-config>
```

3. Change the value for debug key from false to true.

```

<jas-config>
  <name>spotfirekerberos</name>
  <entries>
    <entry>
      <login-module-name>com.sun.security.auth.module.Krb5LoginModule</login-module-name>
      <control-flag>required</control-flag>
      <options>
        <option>
          <key>debug</key>
          <value>true</value>
        </option>
        <option>
          <key>useKeyTab</key>
          <value>true</value>
        </option>
        <option>
          <key>principal</key>
          <value>HTTP/spotfirets@TEST.COM</value>
        </option>
        <option>
          <key>storeKey</key>
          <value>true</value>
        </option>
        <option>
          <key>keyTab</key>
          <value>${java.home}/lib/security/spotfire.keytab</value>
        </option>
      </options>
    </entry>
  </entries>
</jas-config>

```

4. Save and close the file.
5. Import the configuration using the [import-config](#) command. For example: `config import-config --comment="Enabled Kerberos Debug Logging"`
6. On the computer that is hosting the server, navigate to the `nm\config` directory. The default location is `<installation_dir>\nm\config`.
7. Do one of the following:
 - If the `logging.properties` file is present in the directory:
 1. Open the `logging.properties` file in an XML editor or text editor.
 2. Replace the current contents of the file with the contents of the `logging-debug.properties-template`.
 3. Save and close the `logging.properties` file.
 - If the `logging.properties` file is *not* present in the directory:
 1. Make a copy of the `logging-debug.properties-template`.
 2. Rename the copy "logging.properties".
8. Restart the Spotfire Server service for the changes to take effect.



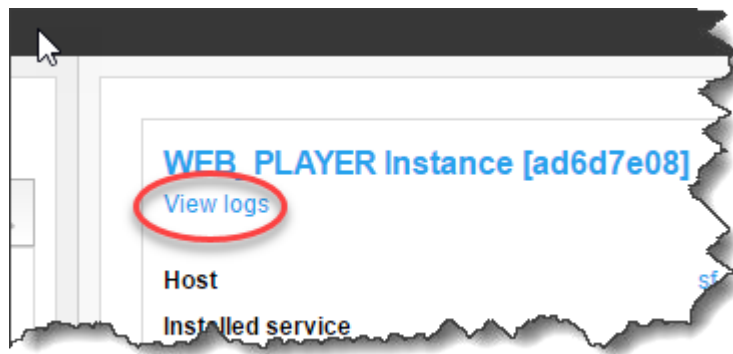
When the troubleshooting is completed, it is recommended to switch back to a lower logging level. You can quickly return to the **Standard (default)** level; for instructions, see [Switching back to the Standard \(default\) logging level](#).

Accessing services logs

Spotfire Server provides easy access to logs for each service. You can select from a list of log files, and you can download the full log file for troubleshooting and working with Spotfire Support. For more information about the logs created for the Web Player, see [Service logs](#). For information about customizing these logs, see [Customizing the service logging configuration](#).

Procedure

1. Log in to Spotfire Server, and then click **Monitoring & Diagnostics**.
2. Click the **Instances** tab.
3. Under Network Diagnostics, select the Automation Services instance or Web Player instance to review.
4. In the area displaying the selected instance, click **View logs**.



The Logs page is displayed in a new browser window.

5. In the **Select log file to view** drop-down list, select the type of log you want to view. The selected log file is shown in the View logs area.

Service logs

The service logs listed in this topic are available for both Web Player services and Automation Services. You can configure the log files listed here in the file `log4net.config`.

To track the resource usage for services, you can enable logging and monitoring of the services by configuring log files in the `log4net.config` file. See [Customizing the service logging configuration](#) for information about exporting and editing this file.



The log4net tool is part of the Apache product family. For more information, see <https://logging.apache.org/log4net/>.

- In the configuration, specify writing all information to a log file by using the default format `%message`.
- For most log files, you can specify the [logging level](#) to write, and which properties to write.

[General logging properties](#) are written into each of the log files listed below. For more detailed information about the additional properties that can be written to each log file, see its linked reference topic.

Log file	Default level	Description
AuditLog.<ID>.txt	INFO	<ul style="list-style-type: none"> At the INFO (default) level, for example, user login and logout, and analysis open and close are logged. At the DEBUG level, state changes (apply and save) are also logged.
DateTimesLog.<ID>.txt	OFF	Time points from the services logs are collected in this file to simplify joins between tables. If logging is set to the DEBUG level, this file can get very large, so time points are not written at the microsecond level.
DocumentCacheStatisticsLog.<ID>.txt	OFF	The cached analyses are sampled regularly.
MemoryStatisticsLog.<ID>.txt	OFF	<p>Writes resource usage per document. Logs the amount of memory used by tables and views, the number of internal document nodes, and the execution time.</p> <ul style="list-style-type: none"> At the INFO level, the total values per document are logged/ At the DEBUG level, detailed information per table is recorded. <p>, and</p>
MonitoringEventsLog.<ID>.txt	INFO	<ul style="list-style-type: none"> At the INFO level, the start up and shut down of the service are logged. At the DEBUG level, session create and remove, analyses open and close, and cached analyses add and remove are also logged.
OpenFilesStatisticsLog.<ID>.txt	OFF	The open analyses sampled regularly.
PerformanceCounterLog.<ID>.txt	INFO	Standard and custom performance counters logged regularly.
Spotfire.Dxp.Worker.Host.Debug.<ID>.log and Spotfire.Dxp.Worker.Host.<ID>.log	n/a	<p>The general purpose log files.</p> <ul style="list-style-type: none"> <code>Spotfire.Dxp.Worker.Host.Debug.<ID>.log</code> writes all logging levels. <code>Spotfire.Dxp.Worker.Host.<ID>.log</code> writes logging levels down to INFO
TimingLog.<ID>.txt	INFO	Logs similar information as the AuditLog, except all events also log a start time, an end time, and a duration.
UserSessionStatisticsLog.<ID>.txt	OFF	The existing sessions are sampled regularly.

For more information about other logs, see the following topics.

- [Spotfire Server logs](#)
- [Node logs](#)

General logging properties

The properties listed here are logged for all service log files.

Property	Description
hostName	The node name.
timeStamp	The local timestamp of the event.
timeStampUtc	The Coordinated Universal Time of the event.
instanceId	The unique ID of the running instance.
serviceId	The unique ID of the running service.

Auditlog

The Auditlog properties listed in this topic are written to the log file named `AuditLog.<ID>.txt`. By default, the logging level is set to INFO.

Property	Description
sessionId	The internal Spotfire session ID.
ipAddress	The IP address of the web client.
userName	The name of the logged on user.
operation	The audit operation, for example "Login".
analysisId	The document id of the currently open document.
argument	An argument for the operation, for example the path of the analysis.
status	Failure or Success.

DateTimesLog

DateTimesLog supports writing to the log file using only the %message format. The default level for DateTimesLog properties is OFF.

This log file compiles all time points from all service logs to simplify joins between tables. If you set this log to the DEBUG level, the resulting log file can be very large, so DateTimesLog does not compile time points at the microsecond level.

DocumentCacheStatisticsLog

The DocumentCacheStatisticsLog properties listed in this topic are written to the log file named DocumentCacheStatisticsLog.<ID>.txt. By default, the logging level is set to OFF.

Property	Description
path	The path of the currently open document.
modifiedOn	The date the document was modified.
referenceCount	The count of concurrent open references to the current document.

MemoryStatisticsLog

The MemoryStatisticsLog properties listed in this topic are written to the log file named MemoryStatisticsLog.<ID>.txt. By default, the logging level is set to OFF.

Property	Description
sessionId	The internal Spotfire session ID.
userName	The name of the logged on user.
analysisId	The unique ID for the analysis.
tableId	The unique ID for the table. This is empty if the value is a total.
analysisPath	The library path for the analysis.
title	The title of the analysis.
type	<p>The type of information. Can be one of the following.</p> <ul style="list-style-type: none"> • SharedApproximateTotalTableSize • SharedApproximateTotalViewSize • DocumentNodeCount • SharedDocumentNodeCount • ApproximateExecutionTime
value	The number of bytes, nodes, or milliseconds depending on type.

MonitoringEventsLog

The MonitoringEventsLog properties listed in this topic are written to the log file named MonitoringEventsLog.<ID>.txt. By default, the logging level is set to INFO.

Property	Description
eventType	The type of event.

Property	Description
argument	Arguments related to the event.
information	Information related to the event.

OpenFilesStatisticsLog

The OpenFilesStatisticsLog properties listed in this topic are written to the log file named AuditLOpenFilesStatisticsLogog.<ID>.txt. By default, the logging level is set to OFF.

Property	Description
sessionId	The internal Spotfire session ID.
filePath	The path of the currently open document.
modifiedOn	The date the document was modified.
fileId	The file ID.
elapsedTime	The time since opened.
inactiveTime	The inactivity time.

PerformanceCounterLog

The PerformanceCounterLog properties listed in this topic are written to the log file named PerformanceCounterLog.<ID>.txt. By default, the logging level is set to INFO.

Property	Description
counterCategory	The category of the performance counter.
counterName	The name of the performance counter.
counterInstance	The instance of the performance counter.
counterValue	The value the performance counter returns.

Spotfire.Dxp.Worker.Host and Spotfire.Dxp.Worker.Host.Debug

The properties for Spotfire.Dxp.Worker.Host and Spotfire.Dxp.Worker.Host.Debug are written to the log files Spotfire.Dxp.Worker.Host.ID.log and Spotfire.Dxp.Worker.Host.Debug.ID.log. These are general purpose log files for all logging levels, and for logging levels down to INFO, respectively. For the properties listed in this topic, you cannot use the standard Apache log4net pattern strings.

Property	Description
pid	The Process ID.
user	The name of the logged on user.

Property	Description
windowsUser	The Windows user.
sessionId	The internal Spotfire session ID.

TimingLog

The TimingLog properties listed in this topic are written to the log file named `TimingLog.<ID>.txt`. By default, the logging level is set to INFO.

Property	Description
endTime	The time the event ends.
duration	The duration of the event.
sessionId	The internal Spotfire session ID.
ipAddress	The IP address of the web client.
userName	The name of the logged on user.
operation	The audit operation, for example "Login".
analysisId	The document id of the currently open document.
argument	An argument for the operation, for example, the path of the analysis.
status	Failure or Success.

UserSessionStatisticsLog

The UserSessionStatisticsLog properties listed in this topic are written to the log file named `UserSessionStatisticsLog.<ID>.txt`. By default, the logging level is set to OFF.

Property	Description
sessionID	The internal Spotfire session ID.
ipAddress	The IP address of the web client.
userName	The name of the logged on user.
browserType	The name and (major) version number of the browser.
cookies	Returns true if cookies are enabled.
loggedInDuration	The duration of time the user has been logged in.

Property	Description
maxOpenFilesCount	The maximum number of open files.
openFileCount	The number of currently open files.

Action logs and system monitoring

Action logs collect user actions. System monitoring collects information about the performance of the Spotfire Server and the services. Information from action logs and from system monitoring is written to the same files or database; therefore, you can use the data you collect to correlate the usage with the system performance.

Action logging and system monitoring are disabled by default.

- To log information from only Spotfire Server, then you must enable writing to files, to a database, or to both files and database only for those actions taking place on the Spotfire Server.
- To also log information from non-server nodes, then you must configure Spotfire Server to accept incoming log events through web service calls.

Action logging and system monitoring	Comments
Writing to files.	Log files are not pruned. By default, a new log file is created every day; although you can change the action log interval , you must manage the space in your file system.
Writing to a database.	You can set an option to remove entries that are older than a certain number of hours. Spotfire provides an Information Model and an analysis file that you can use to start analyzing usage patterns.
Capturing service logs.	You can specify the service or services for which to capture logging information. If you do not configure the web service, only actions performed on the server are logged.

You can enable and configure Spotfire Server for action logging and system monitoring either from the command line or from the configuration tool.

- To enable and configure action logging and system monitoring from the command line, follow the steps in the following tasks.
 1. [Enabling action logging from the command line.](#)
 2. [Configuring logging to a Microsoft SQL Server database with the command line](#) or [Configuring logging to an Oracle database with the command line.](#)
 3. [Configuring the action log web service from the command line.](#)
- To enable and configure action logging and system monitoring from the Spotfire Server configuration tool, follow the steps in the following tasks.
 1. [Setting the action logging to write to a file from the configuration tool.](#)
 2. [Setting the action logging to write to a database from the configuration tool.](#)
 3. [Configuring the action log web service from the configuration tool.](#)

Optionally, you can [import a library into Spotfire Analyst](#) to analyze the action logs.

Configure action logging from the command line

By default, user action logging and system monitoring is not enabled or configured. You can enable and configure it from the server command line.

- You can configure user action logging for actions occurring on Spotfire Server, and for actions occurring on services (Spotfire Analyst, Automation Services, and Spotfire Business Author).
- You can configure the user action and system monitoring logs to write to a file, to a database, or to both.
- Additionally, if you write the logs to a database, you can install a Spotfire Analyst library, which contains Information Links for all available logging categories, and configure it to read the logs from the database to create a Spotfire visualization for analyzing the logs.

Follow the guidance in this section to enable action logging from the command line.

Enabling action logging and system monitoring from the command line

By default, action logging and system monitoring is not enabled. You can enable it from the server command line.

From the command line, running the **enable-action-logging** command is the first step.

Prerequisites

You must have administrative credentials for Spotfire Server.

Procedure

1. Log in to the Spotfire Server, and from the **Start** menu, open a command-line window as administrator.
2. Browse to `<installation dir>\tomcat\bin`.
3. At the command prompt, type the command **config config-action-logger**, passing in the arguments specifying where to record the logs.

- To write the action logs to a file, type the following.

```
config config-action-logger --file-logging-enabled=true --database-logging-enabled=false
```



Log files are not removed automatically. If you enable action logging to write to a file, remember to manage space needs for the resulting log files. By default, log files are written on a daily basis, but the configuration can be changed. See [Setting the action log interval](#) for more information.

- To write the action logs to a database, type the following.

```
config config-action-logger --file-logging-enabled=false --database-logging-enabled=true
```

- To write the action logs to both a file and a database, type the following.

```
config config-action-logger --file-logging-enabled=true --database-logging-enabled=true
```

In these examples, other command-line defaults are accepted. For example, the default configuration enables all categories for logging (**categories="all"**). To limit the enabled categories, provide a comma-separated list. See [Action log categories](#) for a complete list.

For information about all available options for this command, see [config-action-logger](#).

What to do next

- If you specify the database option, configure the action log to write to the database you use.
 - [Configure action logging to a Microsoft SQL Server database.](#)
 - [Configure action logging to an Oracle database.](#)
- To specify which services are allowed for logging on the server, see [configure the action log web service](#).

Configuring logging to a Microsoft SQL Server database with the command line

You can configure action logging to write to a Microsoft SQL Server database, and then run the required additional scripts need for logging to a database. Sample scripts are included in the installation kit for Spotfire Server.

This topic describes the steps required to configure the database for action logging, and to run the configuration scripts from the command line. Alternatively, you can enable and configure the action logging and system monitoring from the Configuration Tool. For more information, see the following topics.

- [Setting the action logging to write to a file from the configuration tool.](#)
- [Setting the action logging to write to a database from the configuration tool.](#)
- [Configuring the action log web service from the configuration tool.](#)

Prerequisites

- You must have administrative credentials for Spotfire Server.
- You must have [enabled logging to a database](#).

Procedure

1. Log in to Spotfire Server, and in the file system, browse to the directory containing the installation kit files.
2. In the installation kit that you downloaded from the TIBCO eDelivery site, browse to the directory containing the scripts to create a new database and schema.

For Oracle, this directory is `/scripts/mssql_install/actionlog`.

3. Using a text editor, open the script file.

The script file to edit is named `create_actionlog_db.bat` (or, for Linux, `create_actionlog_db.sh`).

4. In the script file, edit the section containing the database name `spotfire_actionlog`, setting the variables to reflect your database environment.

You must provide the database password in this script. If you do not have the password, consult your DBA for assistance.



If you want to use the information layer, do not change the user and name, unless you use the **Redirect dependent elements** functionality in Spotfire Analyst Information Designer. See the Spotfire Analyst help topic "Redirecting the Information Model" for more information on this functionality.

5. Optional: If your database is running on Amazon RDS, also edit the script file `create_actionlog_db_rds.bat` (or, for Linux, `create_actionlog_db_rds.sh`), specifying the same information.

6. Run the script to create the database.

Information and error logs are written to a file named `actionlogs.txt` in the directory from where you run the script. If the script takes a very long time, or if it fails, check this text file for more information.

The database is created on the server.

7. Log in to the Spotfire Server, and from the **Start** menu, open a command-line window as administrator.
8. Browse to `<installation dir>\tomcat\bin`.
9. Export the configuration: At the command prompt, type the command **config export-config**.

```
config export-config --force
```

When prompted, supply the tools password. See [export-config](#) for more information.

10. Log in to the Spotfire Server, and from the **Start** menu, open a command-line window as administrator.
11. Browse to `<installation dir>\tomcat\bin`.
12. At the command prompt, type the command **config config-action-log-database-logger**, passing in the arguments specifying the details of the database.
For example, to specify the Microsoft SQL Server database URL, driver class, user name, and password, provide the following.

```
config config-action-log-database-logger --database-url="jdbc:sqlserver://[mycompany]:1433;DatabaseName=[Mydatabase]"
--driver-class="com.microsoft.sqlserver.jdbc.SQLServerDriver" --
username="spotfire_actionlog"
```

When prompted, supply the tools password. See [config-action-log-database-logger](#) for more information.

13. At the command prompt, type the command **config import-config**.

```
config import-config --comment="adding database configuration for action logging."
```

When prompted, supply the tools password. See [import-config](#) for more information.

14. Restart Spotfire Server.

Result

The database is configured.

What to do next

Use the [Information Links and sample analysis file](#) from the installation kit to create a visualization from the action logs.

Configuring logging to an Oracle database with the command line

You can configure action logging to write to an Oracle database, and then run the required additional scripts need for logging to a database. Sample scripts are included in the installation kit for Spotfire Server.

This topic describes the steps required to configure the database and run the configuration scripts from the command line. Alternatively, you can enable and configure the action logging and system monitoring from the configuration tool. For more information, see the following topics.

- [Setting the action logging to write to a file.](#)
- [Setting the action logging to write to a database.](#)

- [Configuring the action log web service from the configuration tool.](#)

Prerequisites

- You must have administrative credentials for Spotfire Server.
- You must have [enabled logging to a database.](#)

Procedure

1. Log in to Spotfire Server, and in the file system, browse to the directory containing the installation kit files.
2. In the installation kit that you downloaded from the TIBCO eDelivery site, browse to the directory containing the scripts to create a new database and schema.
For Oracle, this directory is `/scripts/oracle_install/actionlog`.
3. Using a text editor, open the script file.
The script file to edit is named `create_actionlog_db.bat` (or, for Linux, `create_actionlog_db.sh`).
4. In the script file, edit the section containing the database name `spotfire_actionlog`, setting the variables to reflect your database environment.

You must provide the database password in this script. If you do not have the password, consult your DBA for assistance.



If you want to use the information layer, do not change the user and name, unless you use the **Redirect dependent elements** functionality in Spotfire Analyst Information Designer. See the Spotfire Analyst help topic "Redirecting the Information Model" for more information on this functionality.

5. Optional: If your database is running on Amazon RDS, also edit the script file `create_actionlog_db_rds.bat` (or, for Linux, `create_actionlog_db_rds.sh`), specifying the same information.
6. Run the script to create the database.
Information and error logs are written to a file named `actionlogs.txt` in the directory from where you run the script. If the script takes a very long time, or if it fails, check this text file for more information.
The database is created on the server.
7. On Spotfire Server, from the **Start** menu, open a command-line window as administrator.
8. Browse to `<installation_dir>\tomcat\bin`.
9. Export the configuration: At the command prompt, type the command **config export-config**.
`config export-config --force`
When prompted, supply the tools password. See [export-config](#) for more information.
10. At the command prompt, type the command **config config-action-log-database-logger**, passing in the arguments specifying the details of the database.
For example, to specify the Oracle database URL, driver class, user name, and password. The following example demonstrates the information you must provide.

```
config config-action-log-database-logger
--database-url="jdbc:tibcosoftwareinc:oracle://
some.oraserver.com:1521;ServiceName=pdborcl.example.com"
--driver-class="tibcosoftwareinc.jdbc.oracle.OracleDriver" --
username="spotfire_actionlog"
```

When prompted, supply the tools password. See [config-action-log-database-logger](#) for more information.

11. At the command prompt, type the command **config import-config**.

```
config import-config --comment="adding database configuration for action logging."
```

When prompted, supply the tools password. See [import-config](#) for more information.

12. Restart Spotfire Server.

Result

The database is configured for use.

What to do next

Use the [Information Links and sample analysis file](#) from the installation kit to create a visualization from the action logs.

Configuring the action log web service from the command line

To collect logging from the Spotfire Server and specified services (Spotfire Analyst, Web Player and Automation Services), first enable and configure writing to files or a database, and then enable and configure the action log web service. This task describes configuring the action log web service from the command line.

If you do not configure the action log web service, then only actions performed on Spotfire Server are logged.

Alternatively, you can enable and configure the action log web service from the configuration tool. For more information, see [Configuring the action log web service from the configuration tool](#).

Prerequisites

You must have administrative credentials for Spotfire Server.

You must have completed the following tasks.

- [Enable action logging from the command line](#).
- Configure action logging to write to either [a file](#) or to a database ([Microsoft SQL Server](#) or [Oracle](#)).

Procedure

1. Log in to the Spotfire Server, and from the **Start** menu, open a command-line window as administrator.
2. Browse to `<installation_dir>\tomcat\bin`.
3. At the command prompt, type the command **config config-action-log-web-service**, passing in the arguments specifying the services for which to collect logs.

For example, to enable all categories from all hosts, type the following command.

```
config config-action-log-web-service --allowedHosts=".*" --categories="all"
```

By default, all hosts are allowed and all categories are logged. If you want to reduce the traffic passing between services and the server, replace the default argument values.

- Specify from which host the server should accept logging requests.
- Specify which individual services are allowed for logging. Provide a comma-separated list.

At startup, all configured services check the server for allowed categories. See [Action log categories](#) for a complete list.

Configure action logging using the configuration tool

By default, user action logging and system monitoring is not enabled or configured. You can enable and configure it from the Spotfire Server configuration tool.

- You can configure user action logging for actions occurring on Spotfire Server, and for actions occurring on services (Spotfire Analyst, Automation Services, and Spotfire Business Author).
- You can configure the user action and system monitoring logs to write to a file, to a database, or to both.
- Additionally, if you write the logs to a database, you can install a Spotfire Analyst library, which contains Information Links for all available logging categories, and configure it to read the logs from the database to create a Spotfire visualization for analyzing the logs.

Follow the guidance in this section to enable action logging from the configuration tool.

Setting action logging to write to a file from the configuration tool

If you need to capture action logs, you can set the Spotfire Server configuration file to write the action logs to a file, a database, or both. This topic discusses writing an action log to a file.

Log files are not removed automatically. If you enable action logging to write to a file, remember to manage space needs for the resulting log files. By default, log files are written on a daily basis, but the configuration can be changed. See [Setting the action log interval](#) for more information.

Prerequisites

You must have administrative credentials for Spotfire Server.

Procedure

1. On the computer running Spotfire Server, click **Start**, go to the Spotfire Server folder, and click **Configure TIBCO Spotfire Server**.
2. In the Configuration Start panel, click **User Action log**.
User Action Log configuration options are displayed.
3. For **Enable file logger**, select **Yes**, and then save the configuration.
The Save configuration dialog is displayed, prompting you to write to a database (the recommended default), or to a file.
4. Select **File**, and then click **Next**.
A Save dialog is displayed, prompting you to specify the directory to store the XML configuration files.
5. Browse to a directory to store the files, provide a file name, and then click **Save** to save the configuration.
The action logs are written to the specified file path at the interval specified in the log4j2 configuration file.
6. Optional: [Set the action logs to write to a database from the configuration tool](#).

What to do next

[Configure the web service](#) to log actions from the configuration tool. If you do not configure the web service, only actions that occur on the Spotfire Server are logged.

Save the configuration and restart all services and Spotfire Server for your changes to take effect.

Setting action logging to write to a database from the configuration tool

If you need to capture action logs, you can set the Spotfire Server configuration file to write the action logs to a file, a database, or both. This topic discusses writing an action log to a database. You can configure the action logs by using command-line commands. For more information, see [Enabling action logging and system monitoring from the command line](#).

Prerequisites

- You must have administrative credentials for Spotfire Server.
- You must have a database established to collect the logs.

Procedure

1. On the computer running Spotfire Server, click **Start**, go to the **Spotfire Server** folder, and click **Configure TIBCO Spotfire Server**.
2. In the Configuration Start panel, click **User Action log**. User Action Log configuration options are displayed.
3. For **Enable database logger**, click **Yes**.
4. To set specific categories to log, for **Enable categories**, click **Some Categories**, and from the list, select the categories to log. Only those categories you select are added to the database logger queue. By default all categories are logged.
5. To ensure certain categories are added to the database logger queue, select the Prioritized check box. See [Database logging](#) for more information.
6. Complete the **Database logger configuration** section, specifying the required database connection information. Optionally, change the default configuration settings.
7. Click **Test connection** to make sure the configuration works.
8. Optional: [Set the action logs to write to a file](#) from the configuration tool.

What to do next

[Configure the web service](#) to log actions from the configuration tool. If you do not configure the web service, only actions that occur on the Spotfire Server are logged.

Save the configuration and restart all services and Spotfire Server for your changes to take effect.

Configuring the action log web service from the configuration tool

To collect logging from the Spotfire Server and specified services (Spotfire Analyst, Web Player and Automation Services), first enable and configure writing to files or a database, and then enable and configure the action log web service. This task describes configuring the action log web service from the configuration tool.

Prerequisites

- You must have administrative credentials for Spotfire Server.
- You must have either configured the tool to write to a file or to a database to collect the logs.

Procedure

1. On the computer running Spotfire Server, click **Start**, go to the `Spotfire Server` folder, and click **Configure TIBCO Spotfire Server**.
2. In the Configuration Start panel, click **User Action log**.
User Action Log configuration options are displayed.
3. Set **Enable web service** to **Yes**.
For this option to be enabled, you must have completed the prerequisite to write to a file or database to collect logs.
The Web service configuration section is available.
4. Specify the settings for the web service configuration.
 - Specify the allowed host as a regular expression, if different from the default `.*`. For example, `192\.\168\.[0-9]{1,3}\.[0-9]{1,3}$`
 - Specify which categories to allow to communicate with the server. The default is **All**. If you set this option to **Some Categories**, then you can select from the resulting list box the service categories to allow. See [Action log categories](#) for a complete list.

At startup, a service reads the list and sends to the Spotfire Server user action logger only the user action information for those services that are allowed. If a service is not allowed, then at startup, it has no communication with the Spotfire Server action logger. This setting is useful if you want to remove high-volume services from filling the log files.

If you set the property to enable a service, but you do not set the property to allow it, remember that no communication is sent from the service to the logger.
5. Save the configuration, specifying the configuration destination, and restart all servers and services.

Importing a library to Spotfire Analyst for analyzing action logs

The installation kit includes a downloadable .zip file containing Information Links and a sample analysis file so that you can create a visualization to analyze your user action logs.

Prerequisites

- You must have administrative credentials for Spotfire Server.
- You must have [enabled action logging](#), configured action logging for either an [Oracle database](#) or a [Microsoft SQL Server database](#), and [configured the web service](#) to specify which services to log.

Procedure

1. In the installation kit that you downloaded from the TIBCO eDelivery site, browse to the directory containing the scripts to create a new database and schema.
 - For Oracle, this directory is `/scripts/oracle_install/actionlog`.
 - For SQL Server, this directory is `/scripts/mssql_install/actionlog`.
2. In the installation kit directory, find the .zip file.
 - For Oracle, this file is `logged_user_actions_ora.part0.zip`.
 - For SQL Server, this file is `logged_user_actions_mssql.part0.zip`.
3. On Spotfire Server, open a command line as administrator and go to the `<server installation dir>/tomcat/bin` directory.

4. On the command line, type the command `config import-library-content`, specifying the options needed to import the .zip file.

Example

```
config import-library-content --tool-password=<password> --file-path=/scripts/oracle_install/actionlog/logged_user_actions_ora.part0.zip --conflict-resolution-mode=KEEP_BOTH --user=jdoe
```

See [import-library-content](#) for more information.

5. Open Spotfire Analyst.
6. From the menu, click **Tools > Information Designer**, and then open the Data Source tab.
7. Provide information to connect to the data source, and then save the changes.
You must provide the **Type**, the **Connection URL**, the **Username**, and the **Password**.

Result

The analysis is ready to start reading logging from the database, and the Spotfire Analyst should reflect data read from the system monitoring and the user action logs.

Setting the action log interval

If you set the Spotfire Server configuration to write an action log to a database or a file, then the log is updated on a daily basis, by default. You can change the interval from daily by editing the `log4j2` configuration file.

Log files are not removed automatically, and changing the interval can affect the amount of space required by the files or in the database. Be prepared to manage the space requirements.

Prerequisites

You must have administrative credentials for Spotfire Server.

Before editing the `log4j2` configuration file, make a backup copy.

Procedure

1. On the computer running Spotfire Server, open the following file in a text editor or an XML editor:
`<installation_dir>/tomcat/spotfire-config/log4j2.xml`.
2. Find the appender section specifying `<RollingFile name="actionlog"...>`
3. Edit the `filePattern` entry to specify a different interval.
For detailed information about `filePattern`, see <https://logging.apache.org/log4j/2.x/manual/appenders.html#RollingFileAppender>.
4. Save and close the file.
5. Restart the server service.

Result

Any action logs are written at the new interval.

Database logging

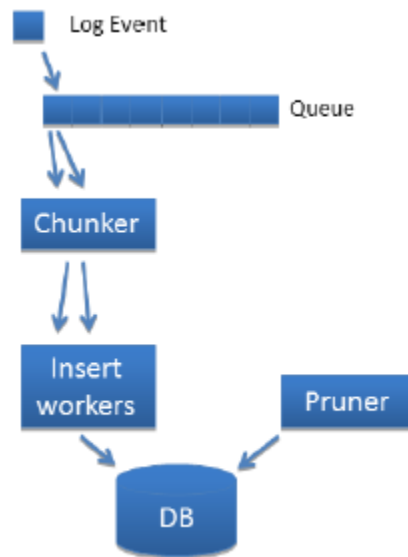
When you configure Spotfire Server to log user actions to a database, you create a dependent and integrated system that you can tune to your logging needs, and you can monitor its health with a JMX-compatible application, such as JConsole.

If you enable database logging, then the server depends on being able to connect successfully to the database. During startup, the database logger attempts to connect to the database. If the database

logger fails to connect, it attempts to reconnect at increasing intervals. If the database logger is not successful after the startup attempts, the server does not run.

Times are logged as GMT by default. To change the logging times value to local time, in the Spotfire Server configuration tool, go to the User Action Log page and set **Log in local time** to **Yes**.

Because several configuration options are available for the database logging, you can tailor the action logging system for your needs. To learn more about how database logging works, follow the steps for event logging.



1. Spotfire Server registers a event and checks if action logging is enabled.
2. If yes, then Spotfire Server checks if the category where the event occurred is enabled for logging.
3. If yes, then the event information is sent to one or two of the loggers.
 - If file logging is enabled, the event is written to the file.
4. Spotfire Server checks if database logging is enabled.
5. If yes, the database logger adds the event to a fixed-size queue. (The queue size is fixed at runtime.)



You can configure the Spotfire Server logging queue to handle the following conditions. See [config-action-log-database-logger](#) for more information.

- Control the maximum number of log events in the queue.
 - If the queue is more than half full, prioritize events so that only certain events are added to the queue.
 - If the queue is full, wait until there is room in the queue.
 - If the queue is full, wait for a given period of time.
6. The chunk worker waits until the configured number of events are available, or until the configured amount of time has passed.
 7. The chunk worker starts an insert worker.

You can configure the number of simultaneous insert workers. If the limit of simultaneous workers is reached, the chunk worker waits for an insert worker to finish. See [config-action-log-database-logger](#) for more information.

8. The insert worker runs a batch insert into the database.

To manage the size and performance of the database, consider the following additional configurations to the action log database logger.

Action	Configuration option in <code>config-action-log-database-logger</code>
If everything must be logged, set the database logger to block for a place in the queue.	<code>--block-on-full-queue=true</code>
Prioritize desired categories. If the queue is more than half full, the database logger adds to the queue only events in the prioritized categories. Other events are discarded.	<code>--prioritized-categories=<value></code>
To ensure that important elements are not discarded, set the queue to wait if it is full.	<code>--wait-on-full-queue-time=<value></code>
If the load is high, set multiple simultaneous insert workers. Otherwise, if you want to sample the system, and you do not want to load a database instance, set the number of insert workers to a low number.	<code>--workers=<value></code>
By default, the database pruner checks every hour for events older than the set number of hours (by default 48 hours). The events that are older are deleted. If you set the number of hours to 0, no pruning takes place, and your database administrator must manage the growth through some other means (for example, by either manually pruning, or by partitioning the table).	<code>--pruning-period=<value></code>
Set a grace period, in seconds, to move events that are in the queue to the database when Spotfire Server is shutting down. Spotfire Server attempts to write these remaining events during this grace period.	<code>--grace-period=<value></code>

The database administrator should monitor the usage regularly to determine if index tables should be rebuilt or dropped.

When you initially configure the action logger to send user action logs to a database, you must run database scripts. These scripts create a new schema and database for the action logs to make it simpler to partition the data table. (See [Configuring logging to an Oracle database with the command line](#) or

[Configuring logging to a Microsoft SQL Server database with the command line](#) for more information about creating a database and schema with these scripts.)

- Events for enabled categories are logged to the table ACTIONLOG, and index tables are created. If you run database searches, you can omit these index tables. (See [Upgrade action logs and system monitoring](#) for more information.) If you include the index tables, and you also set the option for pruning, then your database administrator should consider rebuilding the index tables periodically. See your database administrator for more information.
- Views are created for categories and actions. These views help to interpret the generic columns. If you do not use the views, then you can omit them from the database creation script.

By specifying these options from the command-line command `config config-action-log-database-logger`, you can tune the system for your particular environment and load. Additionally, you can use JMX to tune the system. See [Monitoring](#) for more information about using JMX with Spotfire Server.

In JConsole, under `com.spotfire.server`, you can examine the attributes for `action-log-db-worker`, of type `ActionDBLogger`, to answer the following questions.

Question	JMX Attribute
How many more insert workers can be started?	<code>CurrentNumberOfSpareWorkers</code>
How many events are in the queue?	<code>CurrentQueueSize</code>
What is the minimum number of spare insert workers since the server was started? (0 indicates that all possible workers were started at some point.)	<code>MinimumFreeWorkers</code>
How many events have not been put in the database?	<code>NumberOfFailedLogs</code>
How many events have tried to be logged?	<code>NumberOfLogged</code>
How many items have been pruned from the database?	<code>NumberOfPrunedEntries</code>
How many SQL Exceptions have been encountered?	<code>NumberOfSQLExceptions</code>
How many more events can be queued?	<code>RemainingQueueCapacity</code>

The installation kit also includes an Information Services model and an analysis file, which you can use to gain insight into the usage of the system. See [Importing a library to Spotfire Analyst for analyzing action logs](#) for instructions on downloading and using the visualization.

Action log reference

Spotfire Server action logs capture usage data, such as when a user logs in, opens a file from the library, adds bookmarks, pages through analyses, and so on. Action logs capture events from Spotfire Server, Automation Services, Spotfire Analyst, and Spotfire Business Author.

You can use the action logs to log users' actions in Spotfire, but you cannot use it to log the user state. For example, you can log when a user changes licenses or access permissions for another user (user actions), but you cannot log which actions a user is allowed to perform (user state).

Actions are collected in the logs and stored in files or on a database on Spotfire Server. Actions that do not originate from the server are sent to Spotfire Server through a web service.

- You must enable and configure the web service for actions to log that do not originate from the server.
- When you enable action logging, you must restart all service instances. If you do not restart all service instances, your changes for logging do not go into effect.

Action log data collected

Different levels and types of information are logged when you enable action logs and system monitoring.

Log entries include the following information.

- The time of the action.
- The time the server logged the action.
- The addresses for the server and the computer where the action was performed.
- The user name who performed the logged action.
- The [category](#) of the action, specifying whether the action originated on the Spotfire Server (such as an admin action) or from a service (such as Automation Services).
- The logged action, including [properties](#) (identifying properties or arguments) specific to the action performed. For example, when a user changes a password, the property `uName` is logged to indicate the user name. These properties are displayed in the logged entries as `id1`, `id2`, and arguments `arg1-arg6`.
- Whether the action was completed successfully.
- The session and service instance unique identifiers.

See [Action log entries](#) for more information. See [Sample action log output](#) for an example of a typical set of user actions logged to the action logs.

Logs recorded to a database read the action log column names, and then map them to the fields contained in the database to create a database view. For example, when a user changes a password, the text log entry resembles the following.

```
2017-03-18T09:36:00.381+0100;10.100.32.129;jdoe;2017-03-18T09:36:00,381+0100;10.98.45.189;admin;change_passwd,true;7583cdc4-a6b8-40d4-88e6-90f5d499ff79
```

When the log entry is written to the database, it logs a specific view. For an Oracle database, it is defined as the following.

```
CREATE OR REPLACE VIEW ADMIN_CHANGE_PASSWD AS SELECT
LOGGED_TIME,
MACHINE,
USER_NAME,
ORIGINAL_TIME,
ORIGINAL_IP,
SUCCESS,
SESSION_ID,
```

```
ID1 AS UNAME FROM ACTIONLOG WHERE LOG_CATEGORY = 'admin' AND LOG_ACTION = 'change_passwd'
```

Action log generic entries

Different levels and types of information are logged when you enable action logs and the system monitoring. Regardless of level and type, each of the log entries share the generic information described in this topic.

Log entry	Description	Example
logged_time	The time the event was logged, in the format <i>YYYY-MM-DDTHH:MM:SS:mic+rosc</i> .	2017-03-18T09:36:12.739+0100
machine	The IP address of the computer that performed the logging.	10.100.21.230
user_name	The name of the authenticated user that performed the logged action.	JDOE
original_time	The time the logged event was originally created, in the format <i>YYYY-MM-DDTHH:MM:SS:mic+rosc</i> . This time might differ from the logged time, because it can take time for the log event to be written.	2017-03-18T09:36:12.733+0100
original_ip	The IP address from where the call originates. It can be a proxy.	10.98.25.189
category	The category of the event. See Action log categories for a complete list.	analysis_wp
action	The action performed. For example, change_passwd .	set_page
success	Reports whether the operation succeeded.	true
session_id	A unique ID for the session.	1b15369d63bbcd3a64b576b29d0a34a26f2871b8
service_instance_id	A unique ID for the service instance. This value applies only for the categories with the suffix <i>_wp</i> (Web Player). It is listed as <i>arg5</i> .	bwHPZisVZUeE_Nxj5ybYn-0414411f61_jf2

Action log categories

When you enable action logging, you can enable any of the following categories. When you configure the web service, you can specify from which services to accept requests. When you read the action logs, you can look at these categories for information about where user actions are being logged from. You can specify some or all categories from the command line or from the configuration tool.

category	Description
admin	An administrator request on the server.

category	Description
analysis_as	A Spotfire analysis sent to the server by Automation Services.
analysis_pro	A Spotfire analysis sent to the server by Spotfire Analyst.
analysis_wp	A Spotfire analysis sent to the server by the Web Player (Spotfire Business Author or Spotfire Cloud.)
auth_as	An authorization request sent from Automation Services.
auth_pro	An authorization request sent from the Spotfire Analyst.
auth_wp	An authorization request sent from the Web Player.
automation_job_as	An automation job sent from Automation Services.
automation_task_as	An automation task sent from Automation Services.
data_con_pro	A data connection request sent from Spotfire Analyst.
data_con_wp	A data connection request sent from Web Player.
datafunction_pro	A data function sent from Spotfire Analyst.
datafunction_wp	A data function sent from Web Player.
datasource_pro	A data source request sent from Spotfire Analyst.
datasource_wp	A data source request sent from Web Player.
dblogging	Action logs written only if you log to a database.
ems	A server request for establishing a TIBCO Enterprise Message Service (EMS) connection.
file_pro	A file sent from Spotfire Analyst.
info_link	An information link request on the server.
library	A library request on the server.
library_as	A library request sent from Automation Services.
library_pro	A library request sent from Spotfire Analyst.
library_wp	A library request sent from Web Player.

category	Description
monitoring	A server monitoring measure on the server.
monitoring_w p	A server monitoring request from the Web Player.
routing_rules	A server request related to routing rules.
scheduled_up dates	A server request related to scheduled updates.

admin actions logged on Spotfire Server

Spotfire Server can log actions that an administrator takes to manage users, groups, licenses, preferences, and so on. These actions are logged under the admin category.

The following administration actions are logged on the Spotfire Server. For more information on administrator actions, see [Administration](#).

Action logged	Description
change_passwd	Changed the password for the specified user.
create_group	Created the group with the specified name, display name, and email alias.
create_user	Created the user with the specified user name, display name, and email alias.
group_add_mem ber	Added the specified user name to the specified group name, provide a sorting order, and a grouping ID.
group_remove_m ember	Removed the specified user name from the specified group, providing a sorting order and a grouping ID.
remove_license	Removed the license from the specified group.
remove_principal	Removed the principal with the specified name from the groupingId and sorts the results.
rename_principal	Renamed the principal, replacing the old name with the new name and re-sorts the results.
set_license	Set the license with the specified name to the specified group name.
set_preference	Set the preference with the specified name to the specified type, category, and ID.

auth actions logged from Spotfire Server


Spotfire Server can log user actions for authentication, such as logging in and logging out. Spotfire Server can also log authentication with impersonation credentials. These actions are logged under the category auth.

These authentication actions are logged on the Spotfire Server. For more information about authentication, see [User authentication](#).

Logged action	Description
impersonate	The authentication for the specified user name is from an impersonation.
login	The specified user (email argument and display name) logged in to the specified client type and version.
logout	The specified user logged out.

dblogging actions logged from the database

If you configure your action logs to log to a database, you have an additional category: dblogging. This category has three actions.

Logged action	Description
pruned	Entries are deleted as a result of a pruning action.
startup	The server is started and logging begins.
shutdown	<div> <div>The server is shut down and logging ends.</div> <div>  <div>There is a risk that this action is not logged if the grace period is too short; however, normally it should be logged.</div> </div> </div>

ems action logged from Spotfire Server

Spotfire Server logs connection requests that are sent from TIBCO Enterprise Message Service (EMS). These EMS actions are logged on Spotfire Server from EMS. For more information about EMS, see the help at <https://docs.tibco.com>.

Logged action	Description
create_connection	Created an EMS connection.

info_link actions logged from Spotfire Server

Spotfire Server can log actions that a user takes when using information links. These actions include creating, loading, getting data, and updating the information link. These actions are logged under the category info_link.

These information link actions are logged on Spotfire Server from Spotfire Analyst. For more information about these actions, see the help topics for information links in Spotfire Analyst.

Logged action	Description
create_il	Created an information link in the specified library, with the specified path.
get_data	Retrieved the data for the information link in the specified library, with the specified path.

Logged action	Description
load_il	Loaded the information link in the specified library, with the specified path.
update_il	updated the information link in the specified library, with the specified path.

library actions logged from Spotfire Server

Actions that a user takes that correspond to categories on Spotfire Server or Spotfire Analyst include managing library permissions, creating, importing, exporting, moving, and copying content, loading content and moving content. These actions are logged under the category library on Spotfire Server.

These library actions are logged on Spotfire Server. For more information about these actions, see the help for Library Administration in Spotfire Analyst.

Action logged	Description
clear_perm	Cleared permissions for a folder. Can be recursive.
copy	Copied library content.
create	Created a library.
delete	Deleted an item from the library.
export	Exported an item in the library to the specified path.
import	Imported library content to the specified path.
load_content	Loaded the specified item from the library.
move	Moved an item in the library to the specified path.
remove_perm	Removed permissions for the specified name.
save_content	Saved content to the library.
set_group_perm	Set the group permissions.
set_user_perm	Set the user permissions.

routing_rules actions logged from Spotfire Server

Spotfire Server can log actions that control routing rules.

The following routing rules actions are logged on Spotfire Server. For more information about routing rules, [see Routing Rules](#).

Logged action	Description
create	Created a routing rule.

Logged action	Description
create_schedule	Created a schedule for a routing rule.
delete	Deleted the routing rule.
disable	Disabled the routing rule.
enable	Enabled the routing rule
update	Updated the routing rule.

scheduled_updates actions logged from Spotfire Server

Spotfire Server can log actions that occur as a result of establishing and managing scheduled updates.

The following scheduled update actions are logged on Spotfire Server. For more information about scheduled updates, see [Scheduled updates to analyses](#).

Logged action	Description
adjust_ratio	Analysis load distribution logging.
analysis_update	A server request to update analysis.
cancel_update	A server request to cancel loading analysis.
evaluation	A server request to evaluate scheduled updates.
external_update	An external update request for an analysis.
job_cancel_load	A scheduled update request to cancel loading analysis.
job_execution	A scheduled update job task execution.
job_load	A scheduled update request to load analysis.
job_unload	A scheduled update request to unload analysis.
load	A server request to load analysis.
no_retry	No retry request will be sent.
no_update	No update request will be sent.
reload	A user request to manually load an analysis.
reschedule	A request to reschedule the rule.
retry	A scheduled update request to retry analysis update.

Logged action	Description
retry_exhausted	A scheduled update request to retry on exhausted services.
routing	Route created by scheduled updates.
rule_schedule	A request to schedule a rule.
schedule_change	A server request to change the schedule.
su_evaluation	A server request to evaluate scheduled updates.
su_execution	Scheduled update execution.
su_request	A scheduled update request to process.
task_execution	A scheduled update request to execute a task.
unload	A server request to unload analysis.
update	A server request to update the rule.

Automation Services actions logged from the web service

Spotfire Server logs actions that are performed by Automation Services. They include starting and finishing tasks or jobs, logging in and out, loading content from the library, and applying bookmarks.

For information about each category, see [Action Log categories](#). For more information about Automation Services, see <https://docs.tibco.com>.

analysis_as

Logged action	Description
apply_bookmark	A bookmark with the specified name was applied to the specified library item in the specified path.

auth_as

Logged action	Description
login	The specified user logged in to Spotfire Server.
logout	The specified user logged out from Spotfire Server.

automation_job_as

Logged action	Description
job_finished	The specified Automation Services job finished.
job_started	The specified Automation Services job started.

automation_task_as

Logged action	Description
task_finished	The Automation Services task finished.
task_started	The Automation Services task started.

library_as

Logged action	Description
load	Loaded content from the library specified in Automation Services.

Spotfire Analyst actions logged from the web service

Spotfire Server logs actions that are performed by the user in Spotfire Analyst. Actions are logged according to the category.

For information about each category, see [Action Log categories](#). For more information about the actions, see the help topics in Spotfire Analyst.

analysis_pro

Logged action	Description
apply_bookmark	Applied a bookmark to the specified analysis in Spotfire Analyst.
set_page	Set a page in the specified library item in Spotfire Analyst.

auth_pro

Logged action	Description
login	The specified user logged in to Spotfire Analyst.
logout	The specified user logged out from Spotfire Analyst.

dat_con_pro

Logged action	Description
create_connection	Connected to a data source.
create_source	Created a data source.
get_data	Retrieved data from a data source.
load_connection	Loaded the data connection.
load_source	Loaded the source.
synch_connection	Synchronized the connection.
update_connection	Updated a connection.
update_source	Updated the source.

datafunction_pro

Logged action	Description
execute	Ran a data function in Spotfire Analyst.

datasource_pro

Logged action	Description
execute	Ran an analysis using a data source using the specified parameters

file_pro

Logged action	Description
load	Loaded a file in Spotfire Analyst.

library_pro

Logged action	Description
close	Closed an analysis in Spotfire Analyst.
load	Loaded an analysis in Spotfire Analyst.

Web Player actions logged from the web service

Spotfire Server logs actions that are performed by users of Spotfire Business Author for all categories.

For information about each category, see [Action Log categories](#). For information about Spotfire Business Author, see <https://docs.tibco.com>.

analysis_wp

Action	Description
apply_bookmark	Applied a bookmark to the specified analysis in Spotfire Business Author.
set_page	Set a page in the specified library item in Spotfire Business Author .

auth_wp

Logged action	Description
login	Logged in to Spotfire Business Author.
logout	Logged out from Spotfire Business Author.

dat_con_wp

Logged action	Description
create_connection	Created a data connection in Spotfire Business Author.
create_source	Created a data source in Spotfire Business Author.
get_data	Retrieved data from a data source.
load_connection	Loaded a connection.
load_source	Loaded the source.
synch_connection	Synchronized the connection.
update_connection	Updated the connection.
update_source	Updated the source.

datafunction_wp

Logged action	Description
execute	Executed a data function.

datasource_wp

Logged action	Description
execute	Executed a call to a data source.

file_wp

Logged action	Description
load	Loaded a file.

library_wp

Logged action	Description
clone	Cloned a library entry.
close	Closed a library entry.
load_start	Started loading a library entry.
load	Loaded a library entry.
update_start	Began updating a library entry.
update	Updated a library entry.

Action log actions

This reference lists all possible user actions that are logged by all categories.

Logged action	Categories that can log this action
adjust_ratio	scheduled_updates
analysis_update	scheduled_updates
apply_bookmark	analysis_as analysis_pro analysis_wp

Logged action	Categories that can log this action
cancel_update	scheduled_updates
change_passwd	admin
clear_perm	library
clone	library_wp
close	library_pro library_wp
copy	library
create	library routing_rules
create_connection	dat_con_pro dat_con_wp ems
create_group	admin
create_il	info_link
create_schedule	routing_rules
create_source	dat_con_pro dat_con_wp
create_user	admin

Logged action	Categories that can log this action
delete	library routing_rules
disable	routing_rules
enable	routing_rules
evaluation	scheduled_updates
execute	datafunction_pro datafunction_wp datasource_pro datasource_wp
export	library
external_update	scheduled_updates
get_data	dat_con_pro dat_con_wp info_link
group_add_member	admin
group_remove_member	admin
impersonate	auth
import	library
job_cancel_load	scheduled_updates

Logged action	Categories that can log this action
job_execution	scheduled_updates
job_finished	automation_job_as
job_load	scheduled_updates
job_started	automation_job_as
load	file_pro file_wp library_as library_pro library_wp scheduled_updates
load_connection	dat_con_pro dat_con_wp
load_content	info_link
load_il	dat_con_pro dat_con_wp
load_source	dat_con_pro dat_con_wp
load_start	library_wp
login	auth auth_as auth_pro auth_wp

Logged action	Categories that can log this action
logout	auth auth_as auth_pro auth_wp
move	library
no_retry	scheduled_updates
no_update	scheduled_updates
reload	scheduled_updates
remove_license	admin
remove_perm	library
remove_principal	admin
rename_principal	admin
reschedule	scheduled_updates
retry	scheduled_updates
retry_exhausted	scheduled_updates
routing	scheduled_updates
rule_schedule	scheduled_updates

Logged action	Categories that can log this action
save_content	library
schedule_change	scheduled_updates
set_group_perm	library
set_license	admin
set_page	analysis_pro analysis_wp
set_preference	admin
set_user_perm	library
su_evaluation	scheduled_updates
su_execution	scheduled_updates
su_request	scheduled_updates
synch_connection	dat_con_pro dat_con_wp
task_execution	scheduled_updates
task_finished	automation_task_as
task_started	automation_task_as
unload	scheduled_updates

Logged action	Categories that can log this action
update	library_wp routing_rules scheduled_updates
update_connection	dat_con_pro dat_con_wp
update_il	info_link
update_source	dat_con_pro dat_con_wp
update_start	library_wp

Action log properties

Each action log entry contains generic information, the category of the action, the action logged, and identifying information (id1 and id2), as well as arguments providing more detail about the action. The identifying information and arguments are the properties described in this reference.

For more information about how these properties are reported in a log entry, see [Action log entries](#). For an example of a typical set of user actions and a sample log written as a result, see [Sample action log output](#).

Property	Description	Categories that use this property
analysisId	A unique identifier for the instance of the analysis.	analysis_as analysis_pro analysis_wp library_wp scheduled_updates
analysisPath	The path to the analysis.	scheduled_updates
arguments	Any arguments passed to the server from the EMS.	ems

Property	Description	Categories that use this property
category	Specifies the category of the preference.	admin
clientType	The type of client (for example, Spotfire Analyst).	auth
clientVer	The version of the client that is connecting.	auth
dataSourceInformation	Connector-specific information about the data source. Typically the location of the database.	dat_con_pro dat_con_wp
dataSourceLibraryId	The unique library identifier of the connected data source, if applicable.	dat_con_pro dat_con_wp
dataSourceType	The type of external data source.	dat_con_pro dat_con_wp
destLibraryId	The destination library unique identifier.	library
destPath	The destination library path.	library
destination	The Spotfire Web Player instance URL.	scheduled_updates
destinationList	A list of service URLs. This list is created in the application, based on the scheduled update.	scheduled_updates
destinationName	The name specifying the destination URL.	scheduled_updates
displayName	The display name for a user (for example, John Smith).	admin auth

Property	Description	Categories that use this property
duration	The amount of time the operation or operations took (in ms).	dat_con_pro dat_con_wp datafunction_pro datafunction_wp datasource_pro datasource_wp
email	The e-mail address.	admin auth
excludingFunction	This is a subfunction within a license that is not enabled.	admin
externalQuery	The external query, as generated by the adapter.	dat_con_pro dat_con_wp
gName	The group name.	admin library
groupingId	Operations related to the same operation can share a common grouping identifier. For some operations, this identifier is the same as the job identifier seen in the other logs.	admin info_link library
id	The name of the preference.	admin
internalQuery	The Spotfire query.	dat_con_pro dat_con_wp
jobTaskId	The unique identifier for the job task.	scheduled_updates
jobid	The unique identifier of the job.	automation_job_as automation_task_as scheduled_updates

Property	Description	Categories that use this property
libraryId	The unique identifier for the library item.	analysis_as analysis_pro analysis_wp automation_job_as automation_task_as dat_con_pro dat_con_wp info_link library library_as library_pro library_wp scheduled_updates
libraryPath	The library path.	analysis_pro automation_job_as automation_task_as dat_con_pro dat_con_wp library_wp
libraryType	The type of library. For example, dxp. query.	library
licenseName	The license name.	admin
message	An informational message provided by the rule or the scheduled update.	scheduled_updates routing_rules
name	The name of the entity.	library
newName	The new name.	admin

Property	Description	Categories that use this property
numRows	The number of rows returned.	dat_con_pro dat_con_wp data_source_pro data_source_wp
oldName	The old name.	admin
pageName	The name of the page.	analysis_pro analysis_wp
params	For some operations we do not have the exact functionality, but this information can help identify the action.	datafunction_pro datafunction_wp datasource_pro datasource_wp
path	The path.	analysis_as analysis_wp datafunction_pro datafunction_wp datasource_pro datasource_wp file_wp file_pro info_link library library_as library_pro library_wp
payload	An object or a map containing information related to the specific action.	scheduled_updates
permission	The permission.	library

Property	Description	Categories that use this property
postSize	The size afterwards (in bytes).	library
preSize	The size before (in bytes).	library
prefType	The type of the preference.	admin
processType	The type of the scheduled update process, such as load, unload, or stop_loading.	scheduled_updates
recursive	Indicates whether the performed action was recursive.	library
resourcePool	The resource pool used in the specific scheduled update.	scheduled_updates
ruleName	The name of the rule	scheduled_updates routing_rules
ruleId	The unique identifier of the rule.	routing_rules
scheduleId	The unique identifier for the scheduled update.	routing_rules
scheduleName	The friendly name of the schedule update entry.	routing_rules
serviceUrl	The link to the Spotfire web service. (The web service is the Spotfire Web Player instance on which the scheduled update is running. This can be the same as destination.	scheduled_updates

Property	Description	Categories that use this property
seviceStatus	That status for the scheduled update service. Can be one of the following. Failed Installing Restart Running Starting Stopped Stopping Unreacheable	scheduled_updates
sort	The type (a user or a group).	admin library
taskId	The unique identifier of the task.	scheduled_updates
title	The document title.	datasource_pro datasource_wp
uName	The user name.	admin auth auth_as auth_pro auth_wp library

Property	Description	Categories that use this property
unused	This property is not used.	automation_task_as datafunction_pro datafunction_wp datasource_pro datasource_wp ems file_pro file_wp routing_rules

Action log entries

When you analyze an action log, you can organize the semi-colon separated data into categories, actions, and properties (identifiers, and arguments). You can map these to database columns, which you can display in a Spotfire Analyst visualization.

- See [Action log categories](#) for details about where the logged user action originated.
- [Action log categories](#) also describes the details for actions that apply to the category, and for the identifying information and arguments that apply to the action.

You can configure action logging so that only certain categories are logged. See [Configuring the action log web service from the configuration tool](#) for more information.

Category	Action	id1	id2	arg1	arg2	arg3	arg4	arg5	arg6
admin	change_password	username							
admin	create_group	groupname	displayname	email					
admin	create_user	username	displayname	email					

Category	Action	id1	id2	arg1	arg2	arg3	arg4	arg5	arg6
admin	group_admin_member	name	groupName	sort	groupingId				
admin	group_remove_member	name	groupName	sort	groupingId				
admin	remove_license	groupId	licenseName						
admin	remove_principal	name	sort	groupingId					
admin	rename_principal	oldName	newName	sort					
admin	set_license	groupId	licenseName	excludingFunction					
admin	set_preference	name	prefType	category	id				
analysis_apps	apply_bookmark	libraryId	path	bookmarkName					
analysis_pro	apply_bookmark	libraryId	libraryPath	bookmarkName			analysisId		

Category	Action	id1	id2	arg1	arg2	arg3	arg4	arg5	arg6
analysis_pro	set_page	libraryId	libraryPath	pageName			analysisId		
analysis_wp	apply_bookmark	libraryId	path	bookmarkName		webplayerSessionId	analysisId		
analysis_wp	set_page	libraryId	path	pageName		webplayerSessionId	analysisId		
auth	imPERSONATE	userName							
auth	login	clientType	clientVer	displayName	email				
auth	logout	userName							
auth_as	login	userName							
auth_as	logout	userName							

Category	Action	id1	id2	arg1	arg2	arg3	arg4	arg5	arg6
auth_pro	login	u N a m e							
auth_pro	logout	u N a m e							
auth_wp	login	u N a m e				webplay erSessionId			
auth_wp	logout	u N a m e				webplay erSessionId			
automation_job_as	job_finished	li br ar yId	libraryPath	jobId	status	executionTime	message		
automation_job_as	job_started	li br ar yId	libraryPath	jobId	status	executionTime	message		
automation_task_as	task_finished	li br ar yId	libraryPath	jobId	status	executionTime	message		
automation_task_as	task_started	li br ar yId	libraryPath	jobId	taskClass	unused	taskName		

Category	Action	id 1	id2	arg1	arg2	arg3	arg4	arg5	arg6
dat_con_p ro	creat e_con necti on	li br ar yId d	librar yPath	dataSo urceTy pe	dataSour ceInform ation	dataSour ceLibrar yId			
dat_con_p ro	creat e_sou rce	li br ar yId d	librar yPath	dataSo urceTy pe	dataSour ceInform ation				
dat_con_p ro	get_d ata	li br ar yId d	librar yPath	dataSo urceTy pe	dataSour ceInform ation	internal Query	NumRo ws	duratio n	external Query
dat_con_p ro	load_ conn ectio n	li br ar yId d	librar yPath	dataSo urceTy pe	dataSour ceInform ation	dataSour ceLibrar yId			
dat_con_p ro	load_ sourc e	li br ar yId d	librar yPath	dataSo urceTy pe	dataSour ceInform ation				
dat_con_p ro	synch _con necti on	li br ar yId d	librar yPath	dataSo urceTy pe	dataSour ceInform ation	dataSour ceLibrar yId			
dat_con_p ro	upda te_co nnect ion	li br ar yId d	librar yPath	dataSo urceTy pe	dataSour ceInform ation	dataSour ceLibrar yId			
dat_con_p ro	upda te_so urce	li br ar yId d	librar yPath	dataSo urceTy pe	dataSour ceInform ation				

Category	Action	id 1	id2	arg1	arg2	arg3	arg4	arg5	arg6
dat_con_wp	create_connection	libraryId	libraryPath	dataType	dataSourceInformation	dataSourceLibraryId			
dat_con_wp	create_source	libraryId	libraryPath	dataType	dataSourceInformation				
dat_con_wp	get_data	libraryId	libraryPath	dataType	dataSourceInformation	internal Query	NumRows	duration	external Query
dat_con_wp	load_connection	libraryId	libraryPath	dataType	dataSourceInformation	dataSourceLibraryId			
dat_con_wp	load_source	libraryId	libraryPath	dataType	dataSourceInformation				
dat_con_wp	synchronize_connection	libraryId	libraryPath	dataType	dataSourceInformation	dataSourceLibraryId			
dat_con_wp	update_connection	libraryId	libraryPath	dataType	dataSourceInformation	dataSourceLibraryId			
dat_con_wp	update_source	libraryId	libraryPath	dataType	dataSourceInformation				

Category	Action	id1	id2	arg1	arg2	arg3	arg4	arg5	arg6
datafunction_pro	execute	unused	path	params	duration				
datafunction_wp	execute	unused	path	params	duration				
datasource_pro	execute	unused	path	title	params	duration	NumRows		
datasource_wp	execute	unused	path	title	params	duration	NumRows		
ems	create_connection	unused	unused	arguments					
file_pro	load	unused	path						
file_wp	load	unused	path						
info_link	create_il	libraryId	path						

Category	Action	id1	id2	arg1	arg2	arg3	arg4	arg5	arg6
info_link	get_data	libraryId	path	duration	sizeb	groupingId			
info_link	load_il	libraryId	path	groupingId					
info_link	update_il	libraryId	path						
library	clear_perm	libraryId	path	recursive					
library	copy	libraryId	path	libraryType	destLibraryId	destPath	groupingId		
library	create	libraryId	path	libraryType	preSize	postSize			
library	delete	libraryId	path	libraryType	groupingId				
library	export	libraryId	path	destPath	groupingId				

Category	Action	id1	id2	arg1	arg2	arg3	arg4	arg5	arg6
library	import	libraryId	path	destPath	groupingId				
library	load_content	libraryId	path	libraryType	duration	sizeb	groupingId		
library	move	libraryId	path	libraryType	destLibraryId	destPath	groupingId		
library	remove_perm	libraryId	path	name	sort				
library	save_content	libraryId	path	libraryType	preSize	postSize			
library	set_group_perm	libraryId	path	groupName	permission	groupingId			
library	set_user_perm	libraryId	path	uname	permission	groupingId			
library_as	load	libraryId	path						

Category	Action	id1	id2	arg1	arg2	arg3	arg4	arg5	arg6
library_pro	close	libraryId	path						
library_pro	load	libraryId	path						
library_wp	clone	libraryId	path			webplayerSessionId	analysisId		
library_wp	close	libraryId	path			webplayerSessionId	analysisId		
library_wp	load_start	libraryId	path			webplayerSessionId	analysisId		
library_wp	load	libraryId	path			webplayerSessionId	analysisId		
library_wp	update_start	libraryId	libraryPath			webplayerSessionId	analysisId		
library_wp	update	libraryId	libraryPath			webplayerSessionId	analysisId		
routing_rules	create	ruleId	unused	ruleName	message				

Category	Action	id1	id2	arg1	arg2	arg3	arg4	arg5	arg6
routing_rules	create_schedule	scheduledRuleId	unused	scheduledName	message				
routing_rules	delete	ruleId	unused	ruleName	message				
routing_rules	disable	ruleId	unused	ruleName	message				
routing_rules	enable	ruleId	unused	ruleName	message				
routing_rules	update	ruleId	unused	ruleName	message				
scheduled_updates	adjust_ratio	unused	libraryId	message					
scheduled_updates	analysis_update	taskId	analysisId	destination	message				
scheduled_updates	cancel_update	ruleId	libraryId	ruleName	destination	message			
scheduled_updates	evaluation	unused	unused	serviceUrl	serviceStatus	message			
scheduled_updates	external_update	ruleId	libraryId	analysisPath	resourcePool	message			
scheduled_updates	job_cancel_load	jobTaskId	serviceId	message					

Category	Action	id1	id2	arg1	arg2	arg3	arg4	arg5	arg6
scheduled_updates	job_execution	jobId	taskId	payload	message				
scheduled_updates	job_load	jobTaskId	serviceId	message					
scheduled_updates	job_unload	jobTaskId	serviceId	message					
scheduled_updates	load	ruleId	libraryId	ruleName	destinationList	message			
scheduled_updates	no_retry	unused	libraryId	message					
scheduled_updates	no_update	taskId	libraryId	destination	message				
scheduled_updates	reload	ruleId	libraryId	ruleName	message				
scheduled_updates	reschedule	ruleId	libraryId	ruleName	message				
scheduled_updates	retry	unused	libraryId	destination	message				
scheduled_updates	retry_exhausted	unused	unused	destination	message				

Category	Action	id1	id2	arg1	arg2	arg3	arg4	arg5	arg6
scheduled_updates	routing	unused	libraryId	message					
scheduled_updates	rule_schedule	ruleId	libraryId	ruleName	message				
scheduled_updates	schedule_change	ruleId	libraryId	ruleName	message				
scheduled_updates	subevaluation	ruleId	libraryId	ruleName	message				
scheduled_updates	subexecution	jobId	libraryId	message					
scheduled_updates	subrequest	jobId	libraryId	processType	message				
scheduled_updates	task_execution	taskId	unused	destinationName	message				
scheduled_updates	unload	ruleId	libraryId	ruleName	destinationList	message			
scheduled_updates	update	ruleId	libraryId	ruleName	message				

Example

Every log event is placed on a new row. In the log file, the semicolon specifies a separator. In the database, the information is placed in different columns. Some columns are generic and some columns have different meaning, depending on the category and action. While logging is enabled, the following example is logged.

User action	Log entry
The user "john" changed his password.	2013-05-07T11:55:36.356+0200;10.100.33.227;john;2013-05-07T11:55:36.355+0200;0:0:0:0:0:0:0:1;admin;change_passwd;true;b549dfcf-0059-4d63-b7d0-f710cc10a3cc;john>null
A file originally opened from the library in Spotfire Analyst has been closed.	2013-05-07T11:55:36.356+0200;10.100.33.227;sfa1;2013-04-08T16:20:14.203+0200>null;library_pro;close;true;22154702-8e44-4a26-a102-f1a63121f763;4447a4f7-2c33-43f0-9ed7-edafa152969f;/Demo/Baseball

See [Action log properties](#) and [Action log categories](#) for more information.



If you log to a database, you see an additional category dblogging. See its reference, [dblogging](#), for more information.

Sample action log output

Reading the output from an action log file can be challenging. The sample shown below demonstrates a series of user actions and the resulting log entry that the system provides.

User action	System output
The user jdoe logs in to Spotfire Server.	2017-03-18T09:36:00.381+0100;10.100.32.118;jdoe;2017-03-18T09:36:00,381+0100;10.98.45.199;auth;login;true;7583cdc4-a6b8-40d4-88e6-90f5d499ff79;;;jdoe;;;;
jdoe logs in to Spotfire Business Author. Note the session ID is 1b153....	2017-03-18T09:36:12.152+0100;10.100.32.130;jdoe;2017-03-18T09:36:12,140+0100;10.98.45.199;auth_wp;login;true;21dc38aa-3ec7-4938-8b7e-1dfe218f8655;jdoe;;;1b15369d63bbed3a64b576b29d0a34a26f2871b8;;;;
jdoe loads from the library the DXP contents for the analysis /drafts/ MyAnalysis - first version.	2017-03-18T09:36:12.268+0100;10.100.32.118;jdoe;2017-03-18T09:36:12,267+0100;10.100.32.130;library;load_content;true;21dc38aa-3ec7-4938-8b7e-1dfe218f8655;79c727c3-d70d-43f5-b681-360cee89a821;/drafts/MyAnalysis - first version;dxp;0000000036;0001145557;;;;
The analysis is loaded into Spotfire Business Author. Note that the session ID matches the value above (1b153...), and the analysis ID for the analysis instance is bwHPZ....	2017-03-18T09:36:12.722+0100;10.100.32.130;jdoe;2017-03-18T09:36:12,717+0100;10.98.45.199;library_wp;load;true;21dc38aa-3ec7-4938-8b7e-1dfe218f8655;79c727c3-d70d-43f5-b681-360cee89a821;/drafts/MyAnalysis - first version;AnalysisDxp;1b15369d63bbed3a64b576b29d0a34a26f2871b8;bwhPZisVZUeE_Nxj5ybYn-0414411f61_jf2;;;;

User action	System output
jdoe flips through the pages. Note that the session ID and analysis ID match the values above.	<pre>2017-03-18T09:36:12.739+0100;10.100.32.130;jdoe;2017-03-18T09:36:12,733+0100;10.98.45.199;analysis_wp;set_page;true;21dc38aa-3ec7-4938-8b7e-1dfe218f8655;79c727c3-d70d-43f5-b681-360cee89a821;/drafts/MyAnalysis - first version;Intro;;1b15369d63bbbed3a64b576b29d0a34a26f2871b8;bwhPZisVZUeE_Nxj5ybYn-0414411f61_jf2;;</pre> <pre>2017-03-18T09:36:16.408+0100;10.100.32.130;jdoe;2017-03-18T09:36:16,399+0100;10.98.45.199;analysis_wp;set_page;true;21dc38aa-3ec7-4938-8b7e-1dfe218f8655;79c727c3-d70d-43f5-b681-360cee89a821;/drafts/MyAnalysis - first version;Algebra;;1b15369d63bbbed3a64b576b29d0a34a26f2871b8;bwhPZisVZUeE_Nxj5ybYn-0414411f61_jf2;;</pre> <pre>2017-03-18T09:36:22.044+0100;10.100.32.130;jdoe;2017-03-18T09:36:22,031+0100;10.98.45.199;analysis_wp;set_page;true;21dc38aa-3ec7-4938-8b7e-1dfe218f8655;79c727c3-d70d-43f5-b681-360cee89a821;/drafts/MyAnalysis - first version;Intro;;1b15369d63bbbed3a64b576b29d0a34a26f2871b8;bwhPZisVZUeE_Nxj5ybYn-0414411f61_jf2;;</pre>
jdoe applies a bookmark	<pre>2017-03-18T09:36:22.528+0100;10.100.32.130;jdoe;2017-03-18T09:36:22,514+0100;10.98.45.199;analysis_wp;apply_bookmark;true;21dc38aa-3ec7-4938-8b7e-1dfe218f8655;79c727c3-d70d-43f5-b681-360cee89a821;/drafts/MyAnalysis - first version;geometrics;;1b15369d63bbbed3a64b576b29d0a34a26f2871b8;bwhPZisVZUeE_Nxj5ybYn-0414411f61_jf2;;</pre>
As jdoe closes the analysis, its state is saved to the library.	<pre>2017-03-18T09:36:27.279+0100;10.100.32.118;jdoe;2017-03-18T09:36:27,279+0100;10.100.32.130;library;create;true;21dc38aa-3ec7-4938-8b7e-1dfe218f8655;dbfc821b-0e02-494c-8360-cf8c9c3e07fe;/RelatedItems/AnalysisStates/092a7424-fa68-4179-b762-7f16a5c11e18;analysisstate;0000000000;0000028364;;</pre>
jdoe closes the analysis.	<pre>2017-03-18T09:36:27.288+0100;10.100.32.130;jdoe;2017-03-18T09:36:27,288+0100;10.98.45.199;library_wp;close;true;21dc38aa-3ec7-4938-8b7e-1dfe218f8655;79c727c3-d70d-43f5-b681-360cee89a821;/drafts/MyAnalysis - first version;AnalysisDxp;;1b15369d63bbbed3a64b576b29d0a34a26f2871b8;bwhPZisVZUeE_Nxj5ybYn-0414411f61_jf2;;</pre>
jdoe logs out from Spotfire Server and Spotfire Business Author.	<pre>2017-03-18T09:36:30.884+0100;10.100.32.118;;2017-03-18T09:36:30,884+0100;10.98.45.199;auth;logout;true;7583cdc4-a6b8-40d4-88e6-90f5d499ff79;jdoe;;;;</pre> <pre>2017-03-18T09:36:30.897+0100;10.100.32.130;jdoe;2017-03-18T09:36:30,892+0100;10.100.32.112;auth_wp;logout;true;15966a47-aafd-460e-a649-a80c020a9ca2;jdoe;;;1b15369d63bbbed3a64b576b29d0a34a26f2871b8;;;</pre>

System monitoring reference

System monitoring saves information about the performance of Spotfire Server and the services in the same database or files as the action logs.

System monitoring collects information at regular intervals.

- If you log to a database, to reduce the number of measurements in the database over time, measurements older than a specified amount of time are replaced with average, minimum, and maximum values for a given period of time. The general pruning for the database also affects the monitoring values.
- If you log to file, a file is created every day (the default), so no pruning or averaging is done, and you must manage the space needs of the files.

System monitoring entries

This reference lists all of the entries. When you analyze an action log, you can organize the semi-colon separated data into categories, actions, and properties (identifiers, and arguments). You can map these to database columns, which you can display in a Spotfire Analyst visualization.

Category	Action	id1	id2	arg1	arg2	arg3	arg4
monitoring	average	measure	unused	mean	min	max	
monitoring	measurement	measure	unused	value			
monitoring_wp	average	measure	unused	mean	min	max	
monitoring_wp	counter	measure	wp_id	value	countercategory	countername	counterinstance
monitoring_wp	start_instance						
monitoring_wp	stop_instance						

wp_id is a unique id that identifies the currently-running instance of the Web Player service.

System monitoring properties

Spotfire Server and the Web Player service instance log different properties. The properties are described in this reference.

The tables lists the different properties ([id1](#), [id2](#), [arg1](#), [arg2](#), [arg3](#), [arg4](#)):

Spotfire Server

Measure	Description
cpu	Average CPU load, in percent.

Measure	Description
mem	Heap memory used, in megabytes.
sessions	The number of authenticated HTTP sessions.

Spotfire Web Player service instance (_wp)

Measure	Description
available bytes	The available number of bytes.
cached docs	The number of cached documents.
cpu	Average CPU load, in percent.
disk queue	The length of the disk queue.
mem	The number of bytes used.
network	The total number of bytes transferred per second.
open docs	The number of open documents.
scheduled updates docs	The number of documents controlled by the scheduled updates feature.
uptime	The time in seconds since the service instance was started.

Update action logs and system monitoring

When you update your Spotfire Server to a newer version, remember to consider how an update affects the connection to your database, your database scripts, and the user action logging.

If you have been running user action logging in a previous release of Spotfire Server, then logging continues to work, but you might not be able make full use of the new functionality.

The newer functionality includes further measurements for some log points and properties (for example, CPU usage). Depending on which categories you enabled earlier, you should review the list of services. If you configure user action logs with the configuration tool, selecting categories is easy: you can review and select categories using the check boxes. If you previously selected **all**, the new categories are also selected.

- No changes are necessary if you are logging to a file.
- If you are logging to database, review the rest of this topic.

All enabled categories for user actions and system monitoring are logged to one single table named ACTIONLOG. With no alterations, logging should continue to work, and you should not lose measurements. We have some utilities to help you to analyze the data.

When you update the server, no corresponding automatic SQL update occurs that is related to logging. This design gives full control to you and your database administrator. For example, if you have chosen to implement an advanced management feature, such as partitioning the ACTIONLOG table, this feature remains unchanged.

The database scripts perform the following tasks.

- Create user, schema and database. After an update, you can continue to log to the same target, so do not need to recreate these.
- Create the ACTIONLOG table. This table is still used, and the structure is not altered.
- Create index tables to help searches performed on the ACTIONLOG table. If you configured your earlier installation to omit index tables, then you do not need to change this configuration. With pruning enabled, the ACTIONLOG table has rows both added and deleted, so index tables benefit from being rebuilt regularly. Discuss this task schedule with your database administrator.
- Create views for categories and actions with informative column names, and with the same information as that described in [Action log data collected](#). The views are needed only if you use them for analysis. During an update, these are the only names that must be updated in the database. You can find the information for creating the views in the database installation scripts. These scripts are in the installation kit as follows.

```
./scripts/oracle_install/actionlog
./scripts/mssql_install/actionlog
```

See the following topics for updating the databases.

- [Updating the Oracle database.](#)
- [Updating the Microsoft SQL Server database.](#)

Updating the Oracle database

When you update your Spotfire Server to a newer version, any user action database logging you have configured earlier will most likely continue to work, but to add new views you must perform additional steps.

See also [Update action logs and system monitoring](#).

Prerequisites

You must have credentials to the action log database.

Procedure

1. In the new installation kit directory, browse to \scripts\oracle_install\actionlog.
2. Using a text editor, open the script file create_actionlog_db.bat (on Windows) or .sh (on Linux).
3. In the file, remove the section that creates the tablespace and user. Then, enter the information for CONNECTIDENTIFIER, ACTIONDB_USER, and ACTIONDB_PASSWORD, and run the edited script the same way as when you [enabled the database logging](#).



If you are familiar with SQL utilities, you could instead copy the SQL commands found in create_actionlog_db.sql, log in to the schema spotfire_actionlog and run the SQL directly.

The SQL checks to see whether the table exists, and, if it does, creates only the views.

What to do next

The installation kit also includes a library import file, which contains information links for logging categories, as well as a sample Spotfire analysis file, which you can use to gain insight about your system. See [Importing a library to Spotfire Analyst for analyzing action logs](#) for more information.

Updating the Microsoft SQL Server database

When you update your Spotfire Server to a newer version, any user action database logging you have configured earlier will most likely continue to work, but to add new views you must perform additional steps.

See also [Update action logs and system monitoring](#).

Prerequisites

You must have credentials to the action log database.

Procedure

1. In the new installation kit directory, browse to `\scripts\mssql_install\actionlog`.
2. Using a text editor, open the script file `create_actionlog_db.bat` (on Windows) or `.sh` (on Linux).
3. In the file, remove the section "Create the Spotfire Action log database user". Then, enter the information for `CONNECTIDENTIFIER`, `ACTIONDB_USER`, and `ACTIONDB_PASSWORD`.
4. Run the edited script the same way as when you enabled the database logging.



If you are familiar with SQL tools, you can instead open `create_actionlog_db.sql` for editing, remove the lines above `use $(ACTIONDB_NAME)`, and change this line to `use spotfire_actionlog`. Then, log in to the database `spotfire_actionlog` and run the edited SQL directly.

The SQL checks to see whether the table exists, and, if it does, creates only the views.

What to do next

The installation kit also includes a library import file, which contains information links for logging categories, as well as a sample Spotfire analysis file, which you can use to gain insight about your system. See [Importing a library to Spotfire Analyst for analyzing action logs](#) for more information.

Server monitoring using JMX

You can monitor the Spotfire Server to detect problems with the server itself, with external systems, or with the network. You can also detect misconfigured clients or (in some cases) malicious behavior.

Spotfire Server runs within the Tomcat application server. Tomcat provides the basic functionality needed, the server (Agent level), and a Java Remote Method Invocation (Java RMI) connector (Remote Management level).


Tomcat provides a rich instrumentation set for monitoring and managing the application server. For example, it monitors Tomcat configuration parameters and basic usage statistics. The Java runtime environment that ships with Spotfire Server is also heavily instrumented using JMX. This toolset provides information about CPU and memory usage, garbage collection, and thread pools.

- To monitor the server itself, view and manage logs, and troubleshoot the server, log in to the Spotfire Server administration interface and see the Overview page of Monitoring and Diagnostics.
- To monitor user actions and system events, such as those from Spotfire, Spotfire Web Player, and Spotfire Automation Services, see [Action logs and system monitoring](#).
- To monitor other aspects of the server, use available tools such as TIBCO Hawk®, JConsole (which is included in the Java JDK), or any other Java Management Extensions (JMX)-compliant monitoring tool.

This section provides information on the architecture of the JMX system, types of information captured by JMX, and how to configure and work with JMX-compliant tools to monitor Spotfire Server.

Spotfire Server instrumentation



Spotfire Server components are instrumented to capture detailed information. The following table provides details on the information that the administrator can monitor through instrumentation.

Spotfire Server component	Instrumented information
Server	<ul style="list-style-type: none"> • Server address (IP). • Server hostname. • Server version. • Date and time the server was started. • Uptime time since the server was started, both as a formatted string and in milliseconds since January 1, 1970, 00:00:00 GMT.
Logging	<ul style="list-style-type: none"> • Current log configuration file (configurable). • Available log configuration files (read only). <ul style="list-style-type: none"> – Lists all log configuration files in <installation_dir>\tomcat\webapps\spotfire\WEB-INF. • The number of logging events for the levels set to warn, error, and fatal.
Logger	<p>Information captured depends on the log configuration. It can be set to capture no logs, a single log, or several logs.</p> <ul style="list-style-type: none"> • Log appender name. • Notifications. (Outputs all log statements from a configured log4j appender as JMX notifications.)
Server metrics	<ul style="list-style-type: none"> • Number of attachments on the server. • Number of running Information Services jobs. • Number of authenticated HTTP sessions.
HTTP status codes	<p>The number of HTTP response codes representing client or server errors. Includes the 4xx and 5xx ranges returned from the server.</p> <div>  <p>Responses in these series can be common, even in a system that works well.</p> </div>

Spotfire Server component	Instrumented information
Data source	<p>Records one entry for each currently-running data source on the server, including the server's own data source, as follows.</p> <ul style="list-style-type: none"> • Name. • URL. • Configured minimum number of connections. • Configured maximum number of connections. • Current number of active connections. • Current number of idle connections. • The maximum number of concurrently active connections seen.

JMX configuration security features

Sensitive information can be exposed through JMX and Java. Tomcat and Spotfire Server provide management capabilities to restrict access through authentication, authorization, and encryption security features. Also, as a security measure, the JMX RMI connector is disabled by default, so the administrator must enable it.

Security feature	Description	Default setting
Authentication	Spotfire Server applies the existing database authentication mechanism using a separate database table. Passwords are obscured with hash marks. you can use the same principal names across an entire Spotfire Server cluster.	Enabled.
Authorization	<p>You can configure authorization to specify the level of user permissions.</p> <ul style="list-style-type: none"> • If a user has only read permissions, the user can only read attribute values. • If a user has read-and-write permissions, the user can read and modify any writable attributes. <p>JMX accounts and credentials are separated from Spotfire accounts and credentials. The JMX accounts are used only for monitoring.</p>	<p>Enabled.</p> <div>  <p>Authorization works only with the default authentication implementation.</p> </div>
Encryption	You can configure the Remote Method Invocation (RMI) connector to encrypt the traffic using Transport Layer Security (TLS). This configuration is recommended; otherwise, user names and passwords are transmitted in plain text.	<p>Not enabled.</p> <div>  <p>Encryption configuration requires a certificate.</p> </div>

Security feature	Description	Default setting
Firewall	You can configure a firewall to allow traffic to the desired ports.	The RMI registry and the RMI connector share a common port (1099) to simplify firewall configuration.

JMX configuration commands

Use these commands to configure and administrate JMX access to the monitoring component.

JMX configuration command	Description
<code>config-jmx</code>	Configures the JMX RMI connector.
<code>create-jmx-user</code>	Creates a new JMX user account.
<code>delete-jmx-user</code>	Deletes a JMX user.
<code>list-jmx-users</code>	Lists all JMX users.

Except for the `config-jmx` command, which works on the `configuration.xml` file, all monitoring commands connect directly to the database. You must first import the `configuration.xml` file using the `import-config` command for any changes to take effect. See [Setting up JMX monitoring for JConsole](#) and [import-config](#) for more information.



Click the links in the table for detailed reference for these configuration commands.

JMX levels

A Java Management Extensions (JMX)-compliant monitoring tool, such as TIBCO Hawk® or JConsole, provides three administration levels to Spotfire Server administrators.

The three JMX administration levels are as follows.

JMX administration level	Description
Remote Management level	This level contains connectors and adaptors that provide access to the Agent level.
Agent level	This level is a server that provides applications access to the Instrumentation level.
Instrumentation level	This level provides monitoring information and management operations.

Enabling the JMX logging appender

To monitor the server by using TIBCO Hawk or another Java Management Extensions (JMX)-compliant monitoring tool, you can enable an extra log appender so that the server outputs log events as JMX notifications.

Prerequisites

You must have write access to the server where Spotfire Server is installed.

Perform this task on the computer where Spotfire Server is installed.

Procedure

1. Open the following file in a text editor or an XML editor: `<server installation dir>/tomcat/spotfire-config/log4j2.xml`.
2. Add a new appender definition to the `<Appenders>` section of the `log4j2.xml` file.
For example:

```
<Jmx name="Jmx" description="description of the log">
  <PatternLayout pattern="%X{thread.info} %c{3}: %m%n" />
</Jmx>
```

where the values of the name, description, and pattern attributes can be changed, and the description attribute is optional.

3. In the `<Loggers>` section of the file, locate the loggers for which you want to enable JMX functionality and then add a reference to the JMX appender. See the fourth line of the following example code.

For example:

```
<Logger name="com.spotfire" level="DEBUG" additivity="false">
  <AppenderRef ref="serverlog"/>
  <AppenderRef ref="Console"/>
  <AppenderRef ref="Jmx"/>
</Logger>
```



You can configure multiple JMX appenders, but each one must have a different value for the name attribute.

4. Save and close the file.
5. Restart the server service.

Setting up JMX monitoring for JConsole

This task walks you through setting up JMX monitoring for using JConsole. It does not use Transport Layer Security (TLS).

Prerequisites

- You must have administrative credentials for Spotfire Server. If you are running these commands in Windows, run the command-line interface as administrator.
- You must have access to JConsole.

Perform this task at a command-line prompt on the server, from the directory where the file `config.bat` (on Windows) or `config.sh` (on Linux) is installed. By default, this location is `<server installation dir>/tomcat/bin`.

Procedure

1. Log in to the Spotfire Server, and from the **Start** menu, open a command-line window as administrator.
2. At the command line, run the command `config export-config`.
Provide the tools password when prompted.
The configuration is successfully exported and is ready to change.
3. At the command line, run the command `config config-jmx --enabled=true`.
Provide the tools password when prompted.
4. Import the configuration by running the command `config import-config --comment="Enabling JMX" configuration.xml`.
Provide the tools password when prompted.
5. Create a JMX user by running the command `config create-jmx-user --username=MyJMXUser`.
6. Provide a password for the user *MyJMXUser*.
Provide the tools password when prompted.
7. Restart Spotfire Server.
8. Browse to the JDK directory containing the JConsole executable.
the JConsole executable is in the bin directory of the JDK installation, such as *<Java installation dir>/jdk#. #.#_###/bin*, where *#. #.#_###* represents the version number, such as *1.8.0_121*.
9. Launch the JConsole application.
10. In the JConsole New Connection dialog, select **Remote Process**, enter the *<hostname>:1099*, and then provide the JMX user name and password.



To view the Spotfire information, click the **MBeans** tab, and then select the **com.spotfire.server** domain.

Services monitoring

You can collect and review information on the services running under Spotfire Server using a variety of tools and resources that are provided with your Spotfire Server installation.

Accessing performance data

If your users report to you that the system is slower than they expect, you can begin investigating the problems by examining the performance tracking tools found in Monitoring & Diagnostics.

Prerequisites

You must have administrative privileges on the Spotfire Server.

You can find the performance data for either Automation Services instances or Web Player instances.

Procedure

1. Log in to Spotfire Server, and then click **Monitoring & Diagnostics**.
2. Click the **Instances** tab.
3. Under Network Diagnostics, select the Automation Services instance or Web Player instance to review.

- If you select an Automation Services instance, by default, the Diagnostics area shows **Automation Services Diagnostics** in the drop-down list box and a list of the performance counters.
 - If you select a Web Player instance, by default, the Diagnostics area shows **Analyses and Diagnostics** in the drop-down list box, an Information area containing individual data table instances, and a list of the performance counters.
4. Review the potential problems and troubleshooting suggestions described in [Performance troubleshooting](#).
- The performance counters and information list are diagnostic tools to help you determine if the problems are with the CPU, the RAM, or the .NET memory allocation.

Web Player analyses information - Overview

You can review information about open Web Player instances in **Monitoring & Diagnostics > Instances**. Select the Web Player instance to monitor, and then review the **Overview** tab in the **Information** area.

To access the table, see [Accessing performance data](#).



Click **Refresh** in the **Diagnostics** section to update the list of open analysis.

Overview analysis information

Overview Column head	Description
Title	The title of the analysis. The path of the analysis file is shown in the tooltip.
Instances	The number of open instances of the analysis file.
Average load time	The average time it takes the analysis to load, in seconds.
Execution time	The time spent executing request for the analysis, in seconds. This value is a measure of the CPU load the selected analysis puts on the server.
Total data table size	The total memory size of the data tables in the analysis.
Total data table cells	The total number of cells in the data tables.
Total data view size	<p>This column is displayed only when Show document nodes and view sizes is selected.</p> <p>The total data view size is a measure of the memory required for generating the visualizations of the analysis. The memory required varies depending on the complexity of the data needed for the visualization.</p>

Overview Column head	Description
Total document node count	<p>This column is displayed only when Show document nodes and view sizes is selected.</p> <p>The total number of document nodes. The document node count is a measure of the complexity of the analysis. More visualizations, pages, columns, filtering schemes, markings, and so on, lead to a higher value. If .NET memory is a problem, it is likely that the analyses that use many more document nodes than the others are an issue.</p>
Idle time	The time elapsed since the last user interaction.
Scheduled	Displays Yes if the analysis is scheduled for automatic updates.
Running jobs	The total number of currently running internal analysis jobs.

Web Player analysis information - Details





You can review information about open Web Player instances in **Monitoring & Diagnostics > Instances**. Select the Web Player instance and then review the **Details** tab in the **Information** area.

To access the table, see [Accessing performance data](#).



Click **Refresh** in the **Diagnostics** section to update the list of open analysis.

Details column head	Description
Title	The title of the analysis. The path of the analysis file is shown in the tooltip.
User name	The name of the user that uses the analysis
Load time	The loading time (in seconds) for the analysis.
Execution time	The execution time (in seconds) measures the time spent executing request for the analysis. It is a measure of the CPU load the selected analysis puts on the server.
Shared data table size	The memory size of data tables that are shared between instances of the analysis.
Shared data table cells	The number of data table cells shared between instances of the analysis
Private data table size	The memory size of the data tables that are not shared between instances.
Private data table cells	The number of data table cells that are not shared between instances.

Details column head	Description
Shared data view size	<p>The memory size of the data views that are shared between instances of the analysis.</p> <p>Data view size is a measure of the memory required for generating the visualizations of the analysis. The memory required varies depending on the complexity of the data needed for the visualization.</p> <p> This column is displayed only when Show document nodes and view sizes is selected.</p>
Private data view size	<p>The memory size of the data views that are not shared between instances.</p> <p> This column is displayed only when Show document nodes and view sizes is selected.</p>
Shared document node count	<p>The number of document nodes that are shared between instances of the analysis.</p> <p>The document node count is a measure of the complexity of the analysis. More visualizations, pages, columns, filtering schemes, markings, and so on, lead to a higher value. If .NET memory is a problem, it is likely that the analyses that use many more document nodes than the others are an issue.</p> <p> This column is displayed only when Show document nodes and view sizes is selected.</p>
Private document node count	<p>The number of document nodes that are not shared between instances.</p> <p> This column is displayed only when Show document nodes and view sizes is selected.</p>
Idle time	The time elapsed since the last user interaction.
Scheduled	Yes if the analysis is scheduled for automatic updates.
Running jobs	The total number of currently running internal analysis jobs.

Web Player service performance counters

When you monitor the instance of a Web Player service, you can review the detailed information provided in the **Performance Counters** area to assess the performance measures of open analyses. All memory values are shown in MB.

To access the table, follow the instructions in [Accessing performance data](#).



- To reset the number of cached queries to external data sources, click **Clear cache for all data connections**.
- To run a full garbage collection twice (to clear memory no in use), click **Run a full GC(2)**. Remember that a full garbage collection may take time and the service will be unresponsive during the running.

For information about using performance counters, see [Performance troubleshooting](#).

Performance Counter	Description
# .NET Induced GC	The number of times that an induced GC has been performed. This is .NET Common Language Runtime (CLR) Memory.
% Time In GC	The percentage of processor time spent in GC, this is .NET CLR Memory.
Active threading jobs	The number of active jobs in graphical tables.
Active threads in thread pool	The number of active threads in thread pool (in .NET).
Available memory	The total MBytes available, based on standard performance counter in the category Memory. If this value is low compared to Web Player total working memory , then you might have performance problems related to RAM. See Performance troubleshooting for more information.
Available memory %	Available memory for the Node Manager, as a percentage of total memory.
Avg. disk queue length	The length of the queue for disk input-output. This number should be low.
Current time	The time (in UTC) when the page was updated last time.
Data engine active queries	The number of active data engine queries. The number of active data engine queries. This value should not be far above 0 for very long. Normally, data engine queries do not take very long.
Data engine cache memory	The amount of memory used by the data engine cache. This value can be very high without causing problems because it can be paged out to disk if necessary.
Data engine memory	<p>The amount of memory used by the data engine. This includes all data views and data tables.</p> <ul style="list-style-type: none"> • If this value is a large portion of Web Player total working memory, then you might have performance problems related to RAM. • If this value is only a small portion of the Webplayer total working memory, then you might have performance problems related to .NET memory. <p>See Performance troubleshooting for more information.</p>
Data engine paged in memory	The accumulated amount of paged in memory. This value must be much smaller than Data engine paged out memory
Data engine paged out memory	The accumulated amount of paged out memory. This value can be high, as long as Data engine paged in memory is much smaller.

Performance Counter	Description
Data engine queries finished	The number of finished low level data engine queries.
Data engine query cache memory	The amount of memory used for cached calculations in the data engine.
Idle threads in thread pool	The number of idle threads in thread pool (.NET) that are ready to be used.
May be recycled	Depending on settings for <code>recoverMemory</code> and the current system status, the service instance may send an event to the server that it may recycle the service instance. For more information on <code>recoverMemory</code> , see its entry in Spotfire.Dxp.Worker.Web.config .
Memory health status	<p>According to configured memory limits, this value is displayed as one of the following:</p> <ul style="list-style-type: none"> 0:OK. Indicates that the instance is under no pressure. 5:Strained. Indicates that the instance is under pressure but is not a problem. 8:Exhausted. Indicates that the instance is under a higher load, so avoid routing new users to this instance, but current users can keep working in this instance. <p>Users of analyses in scheduled updates can be routed to a service instance with a status of 8: Exhausted. If you discover that service instances that are used for scheduled updates are often in this state, you should consider adding more service instances to the resource pool.</p> <p>This status is sent to the server to be used for routing decisions. For example, you want to avoid sending many users to service instances that are under a higher load.</p> <p>The limits that determine the health status are configurable for both CPU and memory.</p>
Memory in all .NET heaps	The total MBytes in all .NET heaps, based on .NET CLR Memory.
Network kBytes/sec	The current rate of the network traffic, as measured in kilobytes per second.
Number of shared document nodes	The total number of document nodes that can be shared.
Processor health status	The same as Memory health status above, but for CPU load.
Thread pool queue length	The queue length for the thread pool (in .NET).

Performance Counter	Description
Total average processor %	The average recent CPU % for the node manager, calculated over 120 seconds by default. (For information about tracking the average percentage of CPU usage for a service, see Monitoring CPU usage by services.)
Total processor %	The total processor usage (not just the web client). (For information about tracking the percentage of CPU usage for a service, see Monitoring CPU usage by services.)
Total thread pool requests finished	The total number of thread pool jobs finished (.NET thread pool).
Web Player analyses under scheduled updates control	The number of analyses added to scheduled updates.
Web Player available temp disk space	The amount of free temporary disk space. This value should never approach 0. If the system runs out of temp disk space, all processing halts and any users accessing the server will get no responses. If the value approaches 0, you must add more temp disk space as soon as possible.
Web Player average processor %	The average processor usage recently. Set the time period in <code>cpuAverageTimeSpan</code> , under <code>performanceCounterLogging</code> . See Spotfire.Dxp.Worker.Web.config for more information.
Web Player cached documents	The number of cached analyses.
Web Player current processor %	The processor usage for the web client process.
Web Player image render executions	The number of image-render executions. Typically one image corresponds to one visualization.
Web Player number of users	The number of logged in users.
Web Player open documents	The number of open document instances. (If many users have the same document opened, each copy is counted here.)
Web Player total working memory	The amount of memory used by the web client process. If this value is high compared to Available memory , you might have performance problems related to RAM. See Performance troubleshooting for more information.
Web Player accumulated processor time	The total number of CPU seconds consumed by the web client. If this number is consistently high, you might have performance problems related to CPU consumption. See Performance troubleshooting for more information.
Web Player uptime	The number of seconds since the service instance was started.

Automation Services instance performance counters

When you monitor the instance of Automation Services, you can review the detailed information provided in the **Performance Counters** area to assess the performance measures of the service instance. All memory values are shown in MB.

To access the table, see [Accessing performance data](#).



- To reset the number of cached queries to external data sources, click **Clear cache for all data connections**.
- To run a full garbage collection twice (to clear memory no in use), click **Run a full GC(2)**. Remember that a full garbage collection may take time and the service will be unresponsive during the running.

For information about using performance counters, see [Performance troubleshooting](#).

Performance Counter	Description
# .NET Induced GC	The number of times that an induced GC has been performed. This is .NET Common Language Runtime (CLR) Memory.
% Time In GC	The percentage of processor time spent in GC. This is .NET CLR Memory.
Accumulated processor time	The accumulated number of CPU seconds since the service start. If this number is consistently high, you might have performance problems related to CPU consumption. See Performance troubleshooting for more information.
Active threading jobs	The number of active jobs in graphical tables.
Active threads in thread pool	The number of active threads in thread pool (in .NET).
Available memory	The total MBytes available, based on standard performance counter in the category Memory. If this value is low compared to Total working memory , then you might have performance problems related to RAM. See Performance troubleshooting for more information.
Available memory %	The memory that is still available, as a percentage of the total.
Available temp disk space	The amount of available disk space allocated as temporary.
Average processor %	The average recent CPU percentage for this service instance, calculated over 120 seconds by default. Set the time period in <code>cpuAverageTimeSpan</code> , under <code>performanceCounterLogging</code> . See Spotfire.Dxp.Worker.Web.config for more information. (For information about tracking the average percentage of CPU usage for a service, see Monitoring CPU usage by services .)
Avg. disk queue length	The length of the queue for disk input-output. This number should be low.

Performance Counter	Description
Current processor %	The processor usage for the web client process. (For information about tracking the percentage of CPU usage for a service, see Monitoring CPU usage by services .)
Current time	The time (in UTC) when the page was last updated.
Data engine active queries	The number of active data engine queries. This value should not be far above 0 for very long. Normally, data engine queries do not take very long.
Data engine memory	<p>The amount of memory used by the data engine. This includes all data views and data tables.</p> <ul style="list-style-type: none"> • If this value is a large part of Total working memory, then you might have performance problems related to RAM. • If this value is only a small portion of the Total working memory, then you might have performance problems related to .NET memory. <p>See Performance troubleshooting for more information.</p>
Data engine paged in memory	The accumulated amount of paged in memory. This value must be much smaller than Data engine paged out memory
Data engine paged out memory	The accumulated amount of paged out memory. This value can be high, as long as Data engine paged in memory is much smaller.
Data engine queries finished	The number of finished low level data engine queries.
Data engine query cache memory	The amount of memory used by the data engine cache. This value can be very high without causing problems because it can be paged out to disk if necessary.
Idle threads in thread pool	The number of idle threads in thread pool (.NET) that are ready to be used.
Image render executions	The number of image render executions. Typically one image corresponds to one visualization.
May be recycled	Depending on settings for <code>recoverMemory</code> and the current system status, the service instance may send an event to the server that it may recycle the service instance. For more information on <code>recoverMemory</code> , see its entry in Spotfire.Dxp.Worker.Web.config .

Performance Counter	Description
Memory health status	<p>According to configured memory limits, this value is displayed as one of the following:</p> <ul style="list-style-type: none"> 0:OK. Indicates that the instance is under no pressure. 5:Strained. Indicates that the instance is under pressure but is not a problem. 8:Exhausted. Indicates that the instance is under a higher load, so avoid routing new users to this instance, but current users can keep working in this instance. <p>Users of analyses in scheduled updates can be routed to a service instance with a status of 8: Exhausted. If you discover that service instances that are used for scheduled updates are often in this state, you should consider adding more service instances to the resource pool.</p> <p>The health status is sent to the server to be used for routing decisions. For example, you want to avoid sending many users to service instances that are under a higher load.</p> <p>The limits that determine the health status are configurable for both CPU and memory.</p>
Memory in all .NET heaps	The total MBytes in all .NET heaps, based on .NET CLR Memory.
Network kBytes/sec	The current rate of the network traffic, as measured in kilobytes per second.
Number of users	The number of logged in users.
Processor health status	The same as Memory health status above, but for the CPU load.
Thread pool queue length	The queue length for the thread pool (in .NET).
Total average processor %	The average recent CPU percentage for the node manager, calculated over 120 seconds by default. (For information about tracking the average percentage of CPU usage for a service, see Monitoring CPU usage by services .)
Total processor %	The total processor usage. (For information about tracking the percentage of CPU usage for a service, see Monitoring CPU usage by services .)
Total thread pool requests finished	The total number of thread pool jobs finished (.NET thread pool).
Total working memory	The amount of memory used by the web client process. If this value is high compared to Available memory , you might have performance problems related to RAM. See Performance troubleshooting for more information.
Uptime	The number of seconds since the service instance was started.

Performance troubleshooting

Your users might report that the system is much slower than they expect. System slowdowns can result from one or multiple problems, including system resources and memory. The tools found in Monitoring & Diagnostics can help you track down these types of problems.

By analyzing the problems described in this topic, you can collect information about which analyses are consuming system resources and memory.



Not all performance problems can be traced to the performance issues reported in Monitoring & Diagnostics. If you do not discover the source of the performance problem through the performance counters, you might need to investigate problems with connectivity, network speed, or other external problems.

To find the performance counters and analysis statistical information, follow the instructions in [Accessing performance data](#).

- If a Web Player instance indicates high consumption of resources, you can review the [Analysis information](#) to determine if you have problem analyses causing these issues.
- If an Automation Services instance indicates a high consumption of resources, then review the running analysis for usage information.

You can get additional statistics for a single analysis in the desktop client. You can discover which of its pages or visualizations use most of the resources. See [Examining the statistics of an individual analysis](#) for more information.

1. In the list of [Performance counters](#), find the entry for **Accumulated processor %** (or **Web Player average processor %** for a Web Player instance). Monitor it for a few minutes.
 - If the entry for **Accumulated processor %** (or **Web Player accumulated processor %**) is consistently high, then you have problems with CPU consumption. For a Web Player instance, in the Information area, click the **Overview** tab and review the **Average load time** and **Execution Time** columns. The analyses with the highest values are consuming the most CPU.
 - If the entry for **Web Player accumulated processor** is not consistently high and varies, and your performance problems continue, then check for problems with RAM and .NET memory.
2. To check for problems with RAM or .NET memory, in the list of performance counters, review the following values for the following conditions.
 - The value for **Total working memory** (or **Web Player total working memory** for a Web Player instance) is high, and the value for **Available memory** is low.
 - The value for **Data Engine memory** is a large portion of the value for **Total working memory** (or **Webplayer total working memory**).

If these conditions exist, then memory consumption is the issue. For a Web Player instance, in the Information area, click the **Overview** tab and examine the list of data table instances. The values listed for the columns **Total data table size** and **Total data view size** indicate which analyses are holding the most data table and view memory.

- If an analysis has a large value for **Total data table size**, then the amount of raw data can cause problems. Check the analysis to see if it includes any tables or columns that are not used. If all tables and columns are used, then you need to install more RAM in the Spotfire Server computer.
- If an analysis has a high value for **Total data view size**, or if it appears that the number of document nodes is high, the analysis might be too complicated.



Unused tables, columns, pages, and visualizations generate more document nodes and use data engine memory. However, unused data engine memory can be paged out to disk when available memory becomes low.

3. To check for additional problems with .NET memory, in the list of performance counters, review the entry for **Memory in all .NET heaps**. Click **Run a full GC(2)** twice. This action gives the system a chance to reclaim memory that is released.

For a Web Player instance, in the Information area, click the **Overview** tab and review the **Document Node Count** column. Document nodes are more complicated because they can be different sizes. Analyses that use many more document nodes than the others can cause problems with .NET memory.



Try to perform this action when the server is not very busy, because the system can be unresponsive while running the GC action.

Examining the statistics of an individual analysis

If you have problems with performance of a server, and you suspect one or more analyses of causing the problems on the server, you can examine the suspicious analyses individually using Spotfire Analyst.

See [Performance troubleshooting](#) for advice for identifying any analyses run from the Web Player or through Automation Services that might be causing problems with resource consumption.

Prerequisites

You must have log in credentials for the Spotfire Server for which you want to load the analysis and examine its performance data.

Procedure

1. Log in to Spotfire Analyst and load the analysis to examine.
2. On the menu, click **Help > Support Diagnostics and Logging**.
3. Click the **Diagnostics Information** tab.
Detailed usage information for the analysis is displayed on this tab.

What to do next

Temporarily removing pages, plots, or tables, and then re-examining the resource usage data can provide more insight for troubleshooting, including whether to increase system resources or recommend changes to the analysis.


Logging and exporting monitoring diagnostics

Monitoring diagnostics can be logged, and the logged results can be exported as a Spotfire analysis file that displays the information in the log files.

Procedure

1. Log in to Spotfire Server, and then click **Monitoring & Diagnostics**.
2. On the **Instances** page, under **Network diagnostics**, click the instance for which you want to log and export monitoring diagnostics.
3. Under **Diagnostics**, in the left drop-down list, select the default diagnostics option.
 - For Web Player instances, this option is **Analyses and Diagnostics**.

- For Automation Services instances, this option is **Automation Services Diagnostics**.
4. In the **Logging** drop-down list to the right, select one of the following options.

Option	Description
Enable Monitoring Logging	Start logging to the logs needed for the monitoring analysis on debug level.
Enable Full Monitoring Logging	<p>Start logging, with enabled performance diagnostics, to the logs needed for the monitoring analysis on debug level.</p> <p>This monitoring level is extremely verbose, so do not set this option unless asked to do so by Spotfire Support. After collecting the necessary information from this level, reset logging by selecting Restore Monitoring Logging or by restarting the service instance.</p>
Restore Monitoring Logging	Restore logging levels to what is specified in the <code>log4net.config</code> file.
Export Monitoring Logs and Analysis	<p>Export a snapshot of the log files together with the Spotfire analysis file used to analyze them.</p> <div>  <p>In Spotfire, the Missing File dialog may open. Do the following:</p> <ol style="list-style-type: none"> 1. Select the Apply to all missing files in the analysis check box. 2. Click OK. 3. In the Match Columns dialog that opens, click OK. </div>
Export Monitoring Analysis	Export the monitoring analysis file without the logs. Use this if the logs have been copied in another way.
Export Information	Export diagnostics information to a text file.

Result

Any specified monitoring logs are written to the directory `<installation directory>/nm/logs`.

Viewing node information

You can gather information about a specific node to analyze its available resources and check version details. This information is useful for troubleshooting and working with Spotfire Support.

Prerequisites

You must have administrative credentials for Spotfire Server.

Procedure

1. Log in to Spotfire Server, and then click **Monitoring & Diagnostics**.
2. Click the **Instances** tab.

3. Under Network Diagnostics, select the Automation Services instance or Web Player instance to review.
4. Under Diagnostics, in the left drop-down list box, select **Node**.

Result

The information about the selected node is displayed.

Viewing service configuration information

You can gather information about the service configuration for a node. This information is useful for troubleshooting configuration problems.

Prerequisites

You must have administrative credentials for Spotfire Server.

Procedure

1. Log in to Spotfire Server, and then click **Monitoring & Diagnostics**.
2. Click the **Instances** tab.
3. Under Network Diagnostics, select the Automation Services instance or Web Player instance to review.
4. Under Diagnostics, in the left drop-down list box, select **Service Configuration**.

Result

The configurations and settings that are specified in the `Spotfire.Dxp.Worker.Web.config` file of the service are listed.

Monitoring CPU usage by instances

If you have performance problems, and you expect the CPU usage is an issue, you can monitor the usage for instances. The Spotfire Server Monitoring & Diagnostics tools provide this information.

Prerequisites

You must have administrative credentials for Spotfire Server.

Procedure

1. Log in to Spotfire Server, and then click **Monitoring & Diagnostics**.
2. From Monitoring & Diagnostics, click the **Overview** tab.
The information page for Spotfire Server, Nodes, and service instances is displayed.
3. In the service instances area, look for the column **CPU usage (Avg)**.
The value outside of the parenthesis indicates the percentage of the CPU that the service instance identified in that row is using. The value inside the parenthesis specifies the average CPU usage for that service instance.

What to do next

For general diagnostic information about an instance's node, see [Accessing performance data](#) and [Viewing service configuration information](#).

Viewing assemblies information

You can gather information about the assemblies that are loaded by a specific service. This information is useful for troubleshooting and working with Spotfire Support.

Prerequisites

You must have administrative credentials for Spotfire Server.

Procedure

1. Log in to Spotfire Server, and then click **Monitoring & Diagnostics**.
2. Click the **Instances** tab.
3. Under Network Diagnostics, select the Automation Services instance or Web Player instance to review.
4. Under Diagnostics, in the left drop-down list box, select **Loaded Assemblies**.

Result

The complete list of assemblies for the service is displayed.

Viewing site information

You can gather information about current activity on the web site for a specific service.

Prerequisites

You must have administrative credentials for Spotfire Server.

Procedure

1. Log in to Spotfire Server, and then click **Monitoring & Diagnostics**.
2. Click the **Instances** tab.
3. Under Network Diagnostics, select the Automation Services instance or Web Player instance to review.
4. Under Diagnostics, in the left drop-down list box, select **Site**.

Result

The [Site diagnostics](#) are displayed.

Website diagnostics

The Website diagnostics provide you with details about the current activity of the selected service instance.

Name	Description
Uptime	How long the Web Player service has been running.
Concurrent users	The number of currently logged in users. The number in parentheses indicate the maximum number of concurrent users that is being measured during this uptime.

Name	Description
Number of cached queries for data connections	The number of cached queries to external data sources. This can be reset by clicking Clear cache for all data connections , see Web Player Service Performance Counters .
Cached analyses	The number of currently cached analyses. The number in parentheses indicate the maximum number of analyses that is being measured during this uptime.
Open analyses	The number of currently open analyses.
Current sessions	Lists the currently-active sessions. Current sessions includes the following information. <ul style="list-style-type: none"> • User name(s). • The number of open analyses. The number in parentheses indicate the maximum number of analyses that is being measured during this uptime. • The session ID. • The IP number of the client. • The browser used. • The time the session started.
Current analyses	Lists the currently-open analyses and which users are accessing them. Current analyses includes the following information. <ul style="list-style-type: none"> • The path to the efile. • The time the file was opened. • The analysis ID. • Any pending HTTP requests. • The time since the last ping. • The idle time of the analysis.

Viewing routing

You can get overviews of the routing, such as which instances are used for the different resource pools. You can get this information from both analyses and instances perspectives.

Prerequisites

You must have administrative privileges on the Spotfire Server.

Procedure

1. Log in to Spotfire Server, and then click **Monitoring & Diagnostics**.
2. Click the routing tab to display the information you need.

Option	Description
Routing: Analyses	<p>Displays a list of analyses that are currently active on the server, including the analysis path, the number of users, and the number of instances.</p> <ul style="list-style-type: none"> To view more information about analysis routing, including the instance and the resource pool click the arrow next to the analysis name.
Routing: Instances	<p>Displays a list of Web Player instances currently active on the server, including the resource pools and number of users.</p> <ul style="list-style-type: none"> To view more information about the routing, click the arrow next to the instance name. To view more information about the instance, click its name.

Clicking an instance name from either the Analysis area or the Instance area displays the instance information in Nodes & Services.

Enabling automatic dump capture from non-responsive Web Players

To capture diagnostic information from Spotfire Web Players that stop responding, set up the automatic dump capture.

Procedure

1. On each computer that is running a node manager with the Spotfire Web Player service, download and install the Microsoft Debugging Tools for Windows (WinDbg). This toolkit is available from the following website: <https://developer.microsoft.com/en-us/windows/hardware/windows-driver-kit>.
2. On the server computer, export the active configuration to a `configuration.xml` file by using the `export-config` command. (For details on using the Spotfire command line, see [Executing commands on the command line](#).)
3. Using the `set-config-prop` command, set the `nodemanager.memorydump-after-failures` property to an integer greater than 0. This sets the interval after which the memory dump will occur.

Values for the Web Player auto-dump feature

Value	Description
-0	The Spotfire Web Player automatic dump feature is turned off.
1	The memory dump occurs one interval after the Spotfire Server determines that a service is unreachable. The server performs ten verification steps, so this would cause the dump to occur after 11 failures to communicate with the service.
2	The memory dump occurs two intervals after the Spotfire Server determines that a service is unreachable. This would cause the dump to occur after 12 failures to communicate with the service.

The values continue to increase in the same way.



For a large system, you may want to set a high value because the process may be unresponsive for some time due to blocking garbage collection.

Example:

```
config set-config-prop --name nodemanager.memorydump-after-failures --value 5
```

4. Import the configuration back into the database by using the [import-config](#) command.
5. Do the following on the server computer that you accessed in step 2 above:
 1. Export and open the `Spotfire.Dxp.Worker.Web.config` file for editing; for instructions, see [Manually editing the service configuration files](#).
 2. In `Spotfire.Dxp.Worker.Web.config`, locate the following section:

```
<errorReporting
  emailAddress="" maxMailLength="1000"
  includeDetailedErrorInformation="false"
  enabledMiniDumpCreationOnError="true"
  miniDumpPath=""
  miniDumpSizeLarge="false"
  dumpToolPath ="C:\Program Files (x86)\Windows Kits\10\Debuggers
\x64\cdb.exe"
  dumpToolFlagsSmall="-c &quot;.dump /mhtpFidcu {0};q&quot; -p {1}"
  dumpToolFlagsLarge="-c &quot;.dump /ma {0};q&quot; -p {1}"/>
```

3. Set the `dumpToolPath` to match the location of the `cdb.exe` file that you installed in step 1.
4. (Optional) To configure flags, see the descriptions of the following settings in [Spotfire.Dxp.Worker.Web.config](#): `dumpToolFlagsSmall`, `dumpToolFlagsLarge`, and `miniDumpSizeLarge`.
5. Save the file and then import it back to the server by using the [import-service-config](#) command.
6. Assign the updated configuration to the services by using the [set-service-config](#) command.
6. Restart the server.

Result

If a Spotfire Web Player becomes non-responsive, a dump file with the name `hanging_process_dump_ServiceInstanceID_pidXX.dmp` will be created in the `C:\tibco\tsnm\version number\nm\logs` directory of the node manager computer.

Basic troubleshooting

Spotfire Server provides tools to troubleshoot if you encounter problems in your installation and configuration.

Troubleshooting Spotfire Server

Before diving deeply into logs or contacting support, you can perform some basic steps to check where problems might exist.

From the server where Spotfire Server is installed, perform these basic steps.

Prerequisites

You must have administrative access to Spotfire Server.

Procedure

1. Make sure that Spotfire Server has network connectivity.
2. Make sure that the Spotfire Server service is up and running.
If a custom user account is used to run the Spotfire Server service, ensure that the account credentials are valid and not locked.
3. Verify that no port conflicts with the Spotfire Server ports.
4. Verify that the Spotfire Server administration interface can be accessed outside of the Spotfire Server computer.

If it works correctly on the server machine but is not accessible outside the server, make sure that there is no firewall or proxy blocking server access.

What to do next

If none of these steps solve the problem with Spotfire Server, review all of the [logs](#) and consider [creating a troubleshooting bundle](#) for Spotfire Support to analyze.

Spotfire Server fails to start

If the Spotfire Server fails to start, check the log for the error described in this topic.

```
Error initializing the Spotfire web application. Please contact the
server administrator.
```

The following errors are captured in the server logs.

```
SEVERE: Catalina.start
LifecycleException: service.getName(): "Spotfire"; Protocol handler
start failed: java.net.BindException: Address already in use:
JVM_Bind <null>:
```

Cause

This is an indication of a port conflict.

Resolution

You can check if any of the Spotfire Server ports are blocked by other processes on the Spotfire Server machine. Either stop those services so that Spotfire Server can grab these ports or assign a different port by modifying the `server.xml` file located under `\tomcat\conf` folder.

Spotfire Server runs out of JVM memory

If the Spotfire Server runs out of JVM memory, Spotfire Server can fail or hang. This failure can make new connections impossible, and opening any files can fail.

The following errors are captured in the server logs.

```
Caused by: java.lang.OutOfMemoryError: GC overhead limit exceeded
.....
SEVERE: Exception invoking periodic operation:
java.lang.OutOfMemoryError: Java heap space
```

Cause

This exception indicates that you are out of memory. It is thrown by the garbage collector in the underlying Java and is not specific to Spotfire.

Resolution

You must add more memory. See [Virtual memory modification](#) for more information.

Users cannot log in

Two conditions can cause users to not be able to log into Spotfire Server. The causes and resolutions for these problems are described in this topic.

In both conditions, users are not able to log in to Spotfire Analyst or Spotfire Business Author. Administrators can fail to log into the Spotfire Server administration interface. Both of these conditions result in LDAP errors being generated. You can find the error codes in the server logs.

LDAP error codes	Cause	Resolutions
<code>javax.naming.AuthenticationException: [LDAP: error code 49 - 80090308: LdapErr: DSID-0C090334, comment: AcceptSecurityContext error, data 52e, vece]</code>	This LDAP error code indicates that the log in credentials used for LDAP binding are invalid. This can happen if the password of the LDAP Service Account is expired.	Modify the LDAP configuration with the updated credentials.
<code>javax.naming.AuthenticationException: [LDAP: error code 49 - 80090308: LdapErr: DSID-0C0903A9, comment: AcceptSecurityContext error, data 533, v1db1]</code>	This LDAP error code indicates that the Service Account that is used for LDAP binding can be locked out or disabled.	Enable the Service Account and then try again.

Troubleshooting the Spotfire database

Before diving deeply into logs or contacting support, you can perform some basic steps to check where problems might exist.

From the server where Spotfire Server is installed, perform these basic steps.

Prerequisites

You must have administrative access to Spotfire Server and the Spotfire database.

Procedure

1. Make sure that the Spotfire database is up and running.
2. Validate the database credentials specified in the `bootstrap.xml` file.
3. Ensure that the database user has access to all the required Spotfire database tables and procedures. That is, if the user logs in to the Spotfire Server database with those credentials, the user should be able to browse and access all the contents of the Spotfire database.
4. Make sure there is communication between the Spotfire Server computer and the Spotfire database server.

For example, ping the database server from Spotfire Server.

What to do next

If none of these steps solve the problem with the Spotfire database server, see [Contacting support](#).

Creating a thread dump

Creating thread dumps can be useful. For example, you can use a thread dump to examine problems with servers that appear to be unresponsive, or to investigate why the server is taking an unusual amount of time to respond.

To help troubleshoot such cases, Spotfire Support can examine a dump of thread activity to help determine what is happening. When the Spotfire Server is running as a Windows service, it can be complicated to create this thread dump. This topic describes a simple way to create a thread dump.

Prerequisites

You must have administrative credentials for Spotfire Server.

Procedure

1. Log in to Spotfire Server, and then click **Monitoring & Diagnostics**.
2. Select the Spotfire Server for which you want to download the dump.
3. Click the **More** button (...), and from the resulting drop-down list, click **Download thread dump**. The thread dump is written to a text file and downloaded to the computer.
4. In the server file system where the Spotfire Server is installed, browse to the directory where the text file was written.
The text file name follows the convention `threadDump-<guid>.txt`.

Result

You can open the text file and review the results, and you can share the thread dump with Spotfire Support.

Memory exhaustion

An exhausted memory usually shows an out-of-memory exception in the log. If you are using Microsoft SQL Server, it can manifest itself as a deadlock.

First, try to increase the amount of memory available to the server. For more information, see [Virtual memory modification](#).

If increasing the memory for the server does not solve the problem, you can contact Spotfire Support. Spotfire Support might want to get a dump of the memory to investigate memory leaks. See [Creating a memory dump](#) for instructions.

If your organization handles sensitive information that should not be exposed in a memory dump, you might need to disable this feature. For more information, see [Disabling the memory dump feature](#).

Creating a memory dump

You can create a memory dump to examine problems with exhausted memory.

Perform this task from the Administration interface, and from the file system of the server where Spotfire Server is installed.



When a memory dump is created, the Java Virtual Machine halts for a short period.

Prerequisites

- You must be a member of the Administrator group. It is not sufficient to be only a member of the Diagnostics Administrator group.

- You must have write access to the server's file system where Spotfire Server is installed.

Procedure

1. Log in to Spotfire Server, and then click **Monitoring & Diagnostics**.
2. Select the server for which to create the memory dump.
3. On the right end of the row, click the **More** button (...), and then select **Create memory dump**.

Because memory dumps contain the entire state of the running server, they can contain sensitive information. Therefore, you must prove that you have access to the server.

You are prompted to create a "proof file" in a specific location and with a specific name, and then to return to the Administration interface to resubmit your request.

4. In the server file system where the Spotfire Server is installed, create the specified proof file.
The file does not need to contain content; it merely demonstrates that you are an Administrator with write access to the file system on the server. The memory dump cannot proceed until the file exists.



A new name is generated every time the server is restarted or when a memory dump is made.

5. After you create the proof file as instructed, return to the Administration interface.
The name of the proof file should appear on the page.
6. Click Refresh, and then repeat [Step 3](#).

- A memory dump file is created. This process can take some time.
- Any previous dump file is overwritten.
- When it is completed, the path to the file in the server's file system is displayed.

7. Return to the server file system to retrieve the file.
There is no download functionality on the page.

8. After you have analyzed and solved the memory problem, delete the dump file.
The dump file can contain sensitive information.



On normal termination of the server, the generated heap dump file is deleted automatically.

Disabling the memory dump feature

Because a memory dump can contain sensitive information, you might need to configure the Spotfire Server to never create this artifact.

Perform this task in the file `configuration.xml`, exported from the Spotfire Server.

Prerequisites

- You must have credentials to export, edit, and import the configuration file for Spotfire Server.
- You must export the file `configuration.xml` for editing. See [Manually editing the Spotfire Server configuration file](#) for more information.

Procedure

1. In the file `configuration.xml`, create a new node as follows.

```
<tools>
  <enable-memory-dump>
    <enabled>false</enabled>
  </enable-memory-dump>
</tools>
```

```
</enable-memory-dump>
</tools>
```

2. Save and close the file.
3. Follow the steps for importing the file to the server and then restarting the service.
See [Manually editing the Spotfire Server configuration file](#).

Result

The new imported configuration becomes the active configuration for that server or cluster.

Creating a troubleshooting bundle

You can create a zip archive of different types of logging information. This information can help Spotfire Support assist you with troubleshooting Spotfire Server.

Prerequisites

You must have administrative credentials for Spotfire Server.

Procedure

1. Log in to Spotfire Server, and then click **Monitoring & Diagnostics**.
2. Select the Spotfire Server for which you want to create the troubleshooting bundle.
3. Click **Download troubleshooting bundle**.
A warning dialog is shown advising you that this process can take several minutes.
4. In the Download server troubleshooting bundle dialog, click **OK** to continue.
The troubleshooting bundle is written to a zip archive and downloaded to the server file system.
5. In the server file system where the Spotfire Server is installed, browse to the directory where the zip archive was written.

The zip archive can contain some or all of the following information.

- The entire logs directory.
- A [thread dump](#).
- The results of diagnostics.
- The full configuration history (but not the actual configurations).
- A list of all server startup and shutdown events.
- A list of all nodes in the collective.
- A list of all certificates issued by the internal CA.

What to do next

Contact Spotfire Support for instructions on sharing the troubleshooting bundle.

Command-based library administration tasks

Most library administration tasks are performed in Spotfire Analyst. These include structuring the library and its contents, and setting permissions for library folders. The tasks listed here either can be performed only in Spotfire Server, or can be performed in the server (as well as in Spotfire Analyst) for administrators who prefer using the command line.

For information about library administration in Spotfire Analyst, download the Spotfire [User's Guide](#).

Importing library content by using the command line

Instead of using the Library Administration tool in Spotfire Analyst, you can import content to the library by using the command line.

Prerequisites

You must have administrative credentials for Spotfire Server.

For general information about library administration, download the Spotfire [User's Guide](#)

Procedure

1. Open a command line as an administrator and go to the *server installation dir*/tomcat/bin directory.
2. On the command line, enter the **import-library-content** command, specifying the options needed to import the .zip file.

Example:

```
config import-library-content --tool-password=password --file-path=/
TIB_sfired_server_version_win/demodata/mssql/demo.part0.zip --conflict-resolution-
mode=KEEP_BOTH --user=jdoe --library-path=/
```

For more information, see [import-library-content](#).

Result

The progress of the import is displayed on the command line.

Exporting library content by using the command line

Instead of using the Library Administration tool in Spotfire Analyst, you can export content from the library by using the command line.

Prerequisites

You must have administrative credentials for Spotfire Server.

For general information about library administration, download the Spotfire [User's Guide](#)

Procedure

1. Open a command line as an administrator and go to the *server installation dir*/tomcat/bin directory.
2. On the command line, enter the **import-library-content** command, specifying the options needed to import the ZIP file.

Example:

```
config export-library-content --tool-password=password --file-path=C:/
YearEndAnalyses --user=jdoe --item-type=analysis_files --library-path=/Finals/
Europe
```

For more information, see [export-library-content](#).

Result

The progress of the export is displayed on the command line.

The exported folder and its contents are saved as a ZIP file. The exported items are not removed from the library.

Library content storage outside of the Spotfire database

To minimize the size of your Spotfire database, you can store your organization's Spotfire library content (analyses and analysis data) in the cloud using Amazon Web Services S3 (AWS), or in a file system elsewhere.

In a typical Spotfire installation, the largest part of database storage consists of the library content. When you move the library content to external storage, only the metadata about the library files remains in the database. The other items in database storage (system configuration data, permissions, licenses, and so on) remain where they are.



In this scenario, *all* library content is stored externally; it isn't possible to split storage between the server database and the external site.

Currently there are three main drawbacks to this option:

- Referential integrity is not guaranteed; there is the possibility that content referenced in the Spotfire database will not exist in external storage, and vice versa.
- Your system may run more slowly, such as when loading files.
- A database backup will not back up the library content.

Configuring external library storage in AWS

You can configure external library storage in the cloud using Amazon Web Services S3 (AWS).

Prerequisites

- You must have administrative credentials for Spotfire Server.
- You must have an Amazon S3 account.
- You must have a bucket name. Every server database (or database cluster) should have its own bucket. (Items stored in S3 are identified by their GUIDs. If different servers use the same bucket, importing files to Cluster B—when the files already exist in Cluster A—will overwrite the files in Cluster A.)

Procedure

1. Back up the database.
2. On the command line, export the library using the [export-library-content](#) command. (For details on using the Spotfire command line, see [Executing commands on the command line](#).)
3. Remove the content from the library.



Do not use the `truncate` command in the database because there are hidden folders that should not be removed.

4. To enable external storage and select the type of external storage, use the command [config-library-external-data-storage](#).
5. To configure AWS storage, use the command [config-library-external-s3-storage](#).



You can set the following options when using this command:

- Which AWS regional datacenter the server should connect to.
- Whether large files should be uploaded in chunks, and the details of this behavior.

6. Import the library using the [import-library-content](#) command.



The external library storage system uses the Spotfire library globally unique identifiers (GUIDs) to identify files.

For information on monitoring the external system, see [Monitoring external library storage and fixing inconsistencies](#).

Configuring external library storage in a file system

You can configure external library storage in a file system by using the command line.

Prerequisites

You must have administrative credentials for Spotfire Server.

Procedure

1. Back up the database.
2. On the command line, export the library using the [export-library-content](#) command. (For details on using the Spotfire command line, see [Executing commands on the command line](#).)
3. Remove the content from the library.



Do not use the **truncate** command in the database because there are hidden folders that should not be removed.

4. To enable external storage and to select the type of external storage, use the command [config-library-external-data-storage](#).
5. To specify the path to the storage root, use the command [config-library-external-file-storage](#). Subdirectories for the content files are created under this root.
6. Import the library.



The external library storage system uses the Spotfire library globally unique identifiers (GUIDs) to identify files.

For information on monitoring the external system, see [Monitoring external library storage and fixing inconsistencies](#).

Monitoring external library storage and fixing inconsistencies

Because there is no guarantee of referential integrity when using external library storage, the administrator should regularly check for inconsistencies between the metadata in the Spotfire database and the files in external storage.

Procedure

1. On the command line, enter the command [check-external-library](#) to check for discrepancies. (For details on using the Spotfire command line, see [Executing commands on the command line](#).) A discrepancy report is generated, including where discrepancies occur and any available information to help identify the "orphan" files. This is an excerpt from a report:



2. If a file is found in external storage that is not referenced in the Spotfire database, you can download the file. If it is an analysis file, you can then manually save it to the Spotfire library. If metadata is found for a file that does not exist, you can delete the metadata.

If you want to	Do this
Retrieve an orphan file from Amazon Web Services S3 (AWS)	Download it using the command s3-download .
Retrieve an orphan file from an external file system	Manually copy it from the file system.
Delete files from AWS	Use the command delete-library-content .
Delete files from an external file system	Manually delete the files.
Delete metadata from Spotfire Server	Use the command delete-library-content .

Forcing Java to use Internet Protocol version 4

If your library files are stored on Amazon Web Services S3 (AWS) and you discover instances of the following event in the server logs, you should force Java to use Internet Protocol version 4 (IPv4):

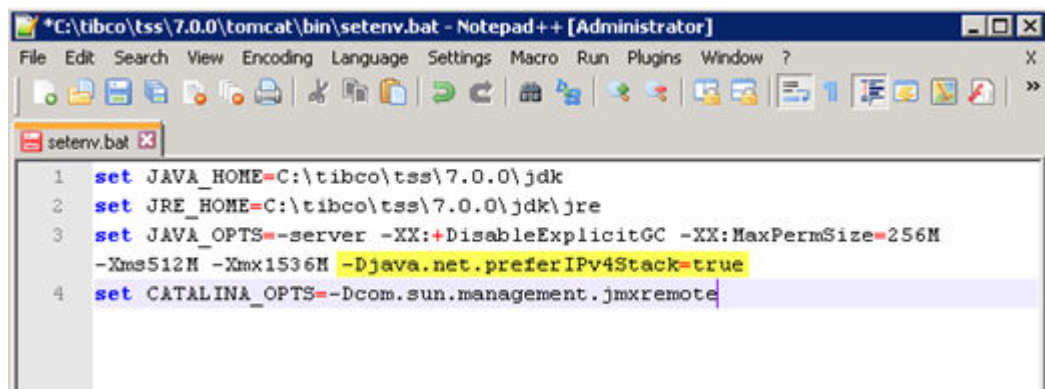
java.net.UnknownHostException: <your bucket name>.s3.amazonaws.com at

java.net.Inet6AddressImpl.lookupAllHostAddr(Native Method)

This parameter is set manually in a Spotfire Server configuration file.

Procedure

1. Open the appropriate file in a text editor:
 - If you are running Spotfire Server as a Windows service, open the <installation dir>/tomcat/bin/service.bat file.
 - If you are *not* running Spotfire Server as a Windows service, open the <installation dir>/tomcat/bin/setenv.bat file.
2. Locate the variable named JAVA_OPTS.
3. Enter the following parameter in the JAVA_OPTS section: -Djava.net.preferIPv4Stack=true
The file will look similar to this (the new parameter is highlighted in yellow):



```

1 set JAVA_HOME=C:\tibco\tss\7.0.0\jdk
2 set JRE_HOME=C:\tibco\tss\7.0.0\jdk\jre
3 set JAVA_OPTS=-server -XX:+DisableExplicitGC -XX:MaxPermSize=256M
  -Xms512M -Xmx1536M -Djava.net.preferIPv4Stack=true
4 set CATALINA_OPTS=-Dcom.sun.management.jmxremote

```

4. Save and close the file.
5. Restart Spotfire Server.

Upgrading Spotfire

There were fundamental architectural changes introduced in Spotfire 7.5. This means that the process of upgrading your Spotfire environment will differ depending on whether you are upgrading from Spotfire 7.0 or earlier or from Spotfire 7.5 or later.

If you are upgrading from Spotfire 7.0 or earlier, see [Upgrading from Spotfire 7.0 or earlier](#).

If you are upgrading from Spotfire 7.5 or later, see [Upgrading from Spotfire 7.5 or later](#).

Upgrading from Spotfire 7.0 or earlier

To upgrade to the latest version of Spotfire from Spotfire 7.0 or 6.5, perform the upgrade tasks applicable to your system.

There are some fundamental changes in the new architecture that affect how you must set up your system to make it behave as it did in the old architecture. The biggest change is that Spotfire Server now handles all external communication. That means that all web client users connect to Spotfire Server instead of a Spotfire Web Player server, and that Spotfire Automation Services jobs are run on Spotfire Server instead of on a Spotfire Automation Services server.

In the 7.5 and later architecture, Spotfire Web Player and Spotfire Automation Services are installed as services on nodes, and Spotfire Server handles the traffic to all instances of these services. When upgrading, these changes mostly affect how authentication and load balancing are set up, as compared to the old architecture.

It is recommended that you set up a Spotfire staging environment for testing before upgrading. See [Setting up the test environment](#).


Related links

[Upgrading a cluster of Spotfire Servers](#)

Setting up the test environment

These are the general steps for setting up the Spotfire test environment and running tests.

Procedure

1. Clone the pre-7.5 production Spotfire database.
 2. Install the new version of Spotfire Servers and node managers.
For more information, see [Basic installation process for Spotfire Server](#).
 3. Install on all servers any available hotfix for the new server. For more information, see [Applying hotfixes to the server](#).
 4. Upgrade the cloned Spotfire database to the new version using the Spotfire Server upgrade tool.
For more information, see [Run the upgrade tool](#).
-  Make sure that it is the cloned database that is upgraded, *not* the production database.
5. Test the system, preferably under conditions similar to production, including any scheduled updates.
 6. After testing is complete, upgrade your pre-7.5 Spotfire environment to the new environment.

Upgrading Spotfire Server

To upgrade Spotfire Server, you install the new version of Spotfire Server and any available hotfixes, and then use the Spotfire Server upgrade tool to upgrade relevant settings, including configurations and node manager trust.

The upgrade tool upgrades the Spotfire database to the current version and, if selected, copies certain files from an old installation of Spotfire Server to the new Spotfire Server installation directory.



If you are upgrading from a pre-7.5 Spotfire Server, you must have Spotfire Server 6.5.3 HF-008 (or later) or Spotfire Server 7.0.0 HF-002 (or later) installed. If you have an earlier version of Spotfire Server installed, you must first upgrade that server to one of these versions.



After the Spotfire database is upgraded, older versions of Spotfire Server will not be able to connect to it. Therefore, stop any older Spotfire Servers connected to the Spotfire database before beginning an upgrade. If you intend to copy information from the old version, do not uninstall it until the new Spotfire Server is in place.



In addition to stopping the older versions of the server, you should prevent the older servers from starting automatically when Windows starts. For instructions for servers running as Windows services, see [Preventing Spotfire Servers and node managers from starting automatically](#).



The upgrade will perform a validation of LDAP configurations. If an invalid LDAP configuration is found, the upgrade will fail. If so, go back to your previous installation, correct the error, and perform the upgrade again.



After the upgrade, make sure that the Administrator group has all licenses, including new ones, assigned to it. Use the Administration Manager in Spotfire Analyst to assign licenses. For a description of the licenses, see the Administration Manager help.

Installation of Spotfire Server during upgrade

When you install Spotfire Server, the upgrade tool is installed as well.

Before installing the new version of Spotfire Server, note the following:

- Configure the new server to use the same ports as the previous installation. This will not cause a port conflict if you have followed steps 1 and 2 in [Upgrading from Spotfire 7.5 or later](#).
- Make sure to install the latest hotfix on all servers before running the upgrade tool.
- Do not start or configure the newly installed server before running the upgrade tool.
- If you intend to copy information from the old version, do not uninstall it until the new version of Spotfire Server is in place.

For general instructions on how to install Spotfire Server, see [Installation](#).

Applying hotfixes to the server

Before you run the upgrade tool, you must install on all servers any available hotfix for the new version of the server.

Prerequisites

- You have installed Spotfire Server.
- You have downloaded the latest hotfix for your new version of Spotfire Server; for instructions, see [Downloading required software](#).

Procedure

- Follow the instructions in the `Installation_Instructions.htm` file that was included in the hotfix package that you downloaded.
For more information, see [Overview of hotfixes for TIBCO Spotfire](#) in the TIBCO Community.

Run the Spotfire Server upgrade tool

The server upgrade tool updates the database. You can run the upgrade tool interactively, or silently by using the command-line interface.



If you have not already done so, make a working backup of your Spotfire database.

For information on how to run the upgrade tool, see [Running the upgrade tool interactively](#) or [Running the upgrade tool silently](#).

Running the Spotfire Server upgrade tool interactively

When you run the Spotfire Server upgrade tool interactively, you are prompted for information about both your older installation and your new installation.



If you are upgrading a cluster of Spotfire Servers, run the upgrade tool on only one server. The Spotfire database will be updated when you run the upgrade tool.



If Spotfire Server is set up to authenticate with the Spotfire database using Windows Integrated Authentication, it is important that you run the upgrade tool as the same user that Spotfire Server authenticates as. Otherwise, the upgrade tool will not be able to authenticate with the database.



The upgrade will perform a validation of LDAP configurations. If an invalid LDAP configuration is found, the upgrade will fail. If so, go back to your previous installation, correct the error, and perform the upgrade again.

Prerequisites

- You have installed the new version of Spotfire Server and any available hotfixes.
- You have a working backup of your Spotfire database.
- If you are using LDAPS, and if the CA certificate is not included in the `cacert` file by default, you must import the CA certificate used to issue the LDAP server's certificate *before* running the upgrade tool. See [Configuring LDAP](#).

Procedure

- If the server upgrade tool is not already open, go to the following directory and double-click `upgradetool.bat` (Windows) or `upgradetool.sh` (Unix): *new version Spotfire Server install dir/tools/upgrade*
By default, the server installation directory is located here: `C:/tibco/tss/version number`.
- The Spotfire Server Upgrade panel is displayed. It provides a reminder to back up or clone the Spotfire database. Click **Next**.
The File Locations panel is displayed. It provides new information and the choice to copy, or not to copy, an existing configuration.
- If you have file access to an old installation, you can select **Previous server installation** and enter the path to its installation directory, for example: `C:/tibco/tss/version number` or `/opt/tss/version number`. Click **Next**.

If there are changes needed after the upgrade, for example, port configuration or the location of TLS certificate, manually edit the `server.xml` file, located in the *Spotfire Server install dir/tomcat/conf* directory.

4. If you did not copy an existing configuration, the Database Type and Driver panel is displayed. Here, specify the database and database driver you are using, and click **Next**.
If you select a database driver type that is not installed in the old installation directory, the message "The selected driver must be installed manually" is displayed. Install the driver manually by placing it in the *new version Spotfire Server install dir/tomcat/lib* directory and restart the upgrade tool.
If you select a database driver type that is not installed and click **Next**, the Database Drivers Not Installed panel is displayed. If this occurs, click **Done** to exit the upgrade tool, then install the database driver and start the upgrade tool again.
The Database Connection Information panel is displayed.
5. Here, provide the Spotfire database **Connection string**, **Username** and **Password**. If your database server uses integrated login, like Windows authentication, select the **Integrated login** check box, to disable the Username and Password fields. Click **Next**.
6. If you did not copy an existing configuration, the Additional Information panel is displayed. Here, specify the configuration tool password, the encryption password, and the server name to use when configuring the Spotfire Server, and click **Next**.
7. If LDAP User Directory mode or Windows NT User Directory mode is used, the User Directory Configuration panel is displayed. Here, select a **domain name style** (DNS or NetBIOS) and a **default domain**.



Make sure to select an accurate domain name style for your system. For more information, see [External directories and domains](#).

The Summary panel is displayed.

8. Click **Upgrade**.
The Upgrade panel is displayed. Here you can see if the upgrade was successful. If there were problems with the upgrade, click **Next** to get information on where the issues have been logged.
9. When the upgrade has been successfully completed (the text "Upgrade done" appears in the panel), click **Finish**.

Running the Spotfire Server upgrade tool silently

As an alternative to running the upgrade tool interactively, you can run it silently using the command line.



If you are upgrading a cluster of Spotfire Servers, run the upgrade tool on only one server. The Spotfire database will be updated when you run the upgrade tool.



If Spotfire Server is set up to authenticate with the Spotfire database using Windows Integrated Authentication, it is important that you run the upgrade tool as the same user that Spotfire Server authenticates as. Otherwise, the upgrade tool will not be able to authenticate with the database.



The upgrade will perform a validation of LDAP configurations. If an invalid LDAP configuration is found, the upgrade will fail. If so, go back to your previous installation, correct the error, and perform the upgrade again.

Prerequisites

- You have installed the new version of Spotfire Server and any available hotfixes.
- You have a working backup of your Spotfire database.

- If you are using LDAPS, and if the CA certificate is not included in the cacert file by default, you must import the CA certificate used to issue the LDAP server's certificate *before* running the upgrade tool. See [Configuring LDAP](#).

Procedure

1. Go to the following directory: *new version Spotfire Server install dir/tools/upgrade*.
2. Open the file `silent.properties` in a text editor or XML editor.
3. Follow the instructions in the file and specify the values of the parameters.
The `from` parameter is the only parameter that you are required to specify.
4. Save the `silent.properties` file.
5. Open a command line.
6. To see the parameters that the upgrade tool will use, do one of the following:
 - On Windows, type `upgradetool.bat -h`.
 - On Linux, type `upgradetool.sh -h`.

The parameters are listed on the command line. Review the list of parameters and specify any that are applicable for your server.
7. To run the upgrade tool silently, do one of the following:
 - On Windows, type `upgradetool.bat -silent silent.properties`.
 - On Linux, type `upgradetool.sh -silent silent.properties`.
8. Press **Enter**.
The upgrade tool runs silently.

Start Spotfire Server

When the upgrade tool has completed without issues, you should start the Spotfire Server.

For information on how to start the Spotfire Server, see [Starting Spotfire Server](#).

To verify that Spotfire Server has been installed and started, launch a browser and go to the Spotfire Server start page: `http://<hostname>:<port>/spotfire`.

Upgrading a cluster of Spotfire Servers

Clustering is disabled by default. Therefore, during the update process, you must enable clustering and reconfigure your cluster-related options.

For general information on upgrading, see [Upgrading](#). For general information on clustering, see [Clustered server deployments](#).



If you have a load balancer that routes based on the `jvmRoute` part of the session id, note that the default value has changed from uppercase to lowercase. If needed, update the load balancer configuration accordingly.

These are the basic steps for upgrading a clustered implementation of Spotfire:

1. Download the required software; see [Downloading required software](#).
2. Install the Spotfire Servers in your cluster; see [Install Spotfire Server](#).
3. Apply the latest hotfix for your version of Spotfire Server (if one is available) to all of the servers; see [Applying hotfixes to the server](#).
4. On only one of the servers, run the upgrade tool; see [Run the upgrade tool](#).

5. On the same server, set your clustering parameters; see [Setting up a cluster of Spotfire Servers](#).
6. Start the same server; see [Start or stop Spotfire Server](#).
7. Start the other servers in the cluster.
8. If you are using ActiveSpaces to secure the connections between clustered servers, you must install and configure ActiveSpaces on every server in the cluster; for details, see [Using ActiveSpaces for clustering](#).

Upgrading Spotfire Analyst clients

Spotfire Analyst clients are upgraded when users connect to a new Spotfire Server on which the new client packages were deployed.



If you use any custom visualizations, these extensions must be modified before you deploy them to Spotfire Server. For more information, see [Upgrading custom visualizations](#).

Deploy client packages

Deploy the new Spotfire client packages to the server.

For information on how to deploy the client packages, see [Deploying client packages to Spotfire Server](#).

After deploying the packages, start a Spotfire client and log in to Spotfire Server. Make sure that the client is upgraded with the new deployment. Verify that the Spotfire library and information model are accessible and work as they did before the upgrade.

Upgrading Spotfire Web Player

Upgrade Spotfire Web Player by installing the Web Player service on a node and applying your configurations.

In the current Spotfire architecture, you no longer install a Spotfire Web Player server that web client users connect to. Now all web client users connect to a Spotfire Server that has a Web Player service installed on a node. You install the Web Player service on a node, apply your Web Player configurations, and deploy any extensions.



Because all web client users connect to the Spotfire Server, authentication is now set up on the Spotfire Server. For more information, see [Upgrading authentication method](#).

Prerequisites

You have a new Spotfire Server up and running.

Procedure

1. Make a copy of your old Web Player server installation directory. This is likely located in a default directory, such as `C:\Program Files\Tibco\Spotfire Web Player\7.0\`. This will contain your `web.config` file, which contains the configuration of your old Web Player server.



If you are using scheduled updates, make sure that you also have a copy of the `ScheduledUpdates.xml` file. For more information, see [Upgrading scheduled updates](#).

2. Deploy the Spotfire distribution to Spotfire Server. For more information, see [Deploying client packages to Spotfire Server](#).
3. Open a command line and export the service configuration files from Spotfire Server by using the `export-service-config` command. Specify the Web Player capability and the deployment area:

```
config export-service-config --capability=WEB_PLAYER --deployment-area=Production
```

The configuration files `Spotfire.Dxp.Worker.Automation.config`,
`Spotfire.Dxp.Worker.Core.config`, `Spotfire.Dxp.Worker.Host.exe.config`, and

Spotfire.Dxp.Worker.Web.config are exported to the <server installation dir>\tomcat\bin\config\root directory.

4. Edit the configuration files in a text editor or XML editor. Use your old web.config file as a reference to replicate your old configuration.
For information on the configuration files, see [Service configuration files](#).
For information on which service configuration files contain the settings from your old web.config file, see [Mapping content of old configuration files to new service configuration files](#).
5. On the command line, import the configuration files to Spotfire Server by using the [import-service-config](#) command. Give the configuration a name. .
Example:

```
config import-service-config --config-name=WebPlayerConfiguration
```
6. On the command line, use the [set-server-service-config](#) command to assign the created Web Player configuration to Spotfire Server to make it available for services:

```
config set-server-service-config --capability=WEB_PLAYER --config-name=WebPlayerConfiguration
```
7. Install the Web Player service on a node as described in [Installing Spotfire Web Player instances](#).
In the Install new service dialog, select the configuration that you imported.
8. Use the Administration Manager in Spotfire Analyst to assign *licenses*. For a description of the licenses, see the Administration Manager help.

Mapping content of old configuration files to new service configuration files

The applicable settings in the old Web Player and Automation Services configuration files are now located in the different service configuration files.

Settings in Web.config

Section	Service configuration file
<Spotfire.Dxp.Services.Settings>	Spotfire.Dxp.Worker.Core.config
<Spotfire.Dxp.Web.Properties.Settings>	Spotfire.Dxp.Worker.Host.exe.config
<Spotfire.Dxp.Data.Properties.Settings>	Spotfire.Dxp.Worker.Host.exe.config
<Spotfire.Dxp.Data.Access.Adapters.Settings>	Spotfire.Dxp.Worker.Host.exe.config
<setup>	Spotfire.Dxp.Worker.Web.config
<userInterface>	Spotfire.Dxp.Worker.Web.config
<performance>	Spotfire.Dxp.Worker.Web.config

Settings in Spotfire.Dxp.Launcher.exe.config

Section	Service configuration file
<Spotfire.Dxp.Automation> <application>	Spotfire.Dxp.Worker.Web.config
<spotfire.dxp.automation.tasks>	Spotfire.Dxp.Worker.Automation.config

Section	Service configuration file
<appSettings>	Spotfire.Dxp.Worker.Automation.config

Upgrading scheduled updates

Scheduled updates are set up using Scheduling & Routing on Spotfire Server.

Old `ScheduledUpdates.xml` files can be imported from a file or the library to the Spotfire database. This is done by running the [import-scheduled-updates](#) command on the command line. Old and new scheduled updates are then configured using Scheduling & Routing on Spotfire Server.

Scheduled updates are run by a pre-defined user account, `scheduledupdates@SPOTFIRESYSTEM`. Make sure that the account `scheduledupdates@SPOTFIRESYSTEM` is a member of the same groups as the old scheduled updates account. If any explicit library permissions were assigned to the old account, these can be copied. To copy library permissions from an old account that is used for scheduled updates to the account `scheduledupdates@SPOTFIRESYSTEM`, use the [copy-library-permissions](#) command.

For more information, see [Scheduled updates to analyses](#). For information on setting up external updates using TIBCO Enterprise Message Service (EMS), see [Creating a scheduled update by using TIBCO EMS](#) and [config-external-scheduled-updates](#).

Upgrading Spotfire Automation Services

Upgrade Spotfire Automation Services by installing Automation Services on a node and applying your configurations.

In the new Spotfire architecture, you no longer install a Spotfire Automation Services server. Now all Automation Services jobs are executed on the node where Automation Services is installed as a service. To upgrade, you install Automation Services as a service on a node, apply your configurations, and deploy any extensions.

Prerequisites

You have a new Spotfire Server up and running.

Procedure

1. Make a copy of your old Spotfire Automation Services server installation directory. Navigate to the `<installation_directory>\webroot\bin` directory. This will contain your `Spotfire.Dxp.Automation.Launcher.exe.config` file, which contains the configuration of your old Automation Services.
2. Deploy the Spotfire distribution to the Spotfire Server. For more information, see [Deploying client packages to Spotfire Server](#).
3. Open a command line as an administrator and export the service configuration files from the Spotfire Server by using the [export-service-config](#) command. Specify the Automation Services capability and the deployment area:

```
config export-service-config --capability=AUTOMATION_SERVICES --deployment-area=Production
```

The configuration files `Spotfire.Dxp.Worker.Automation.config`, `Spotfire.Dxp.Worker.Core.config`, `Spotfire.Dxp.Worker.Host.exe.config`, and `Spotfire.Dxp.Worker.Web.config` are exported to the `<server_installation_dir>\tomcat\bin\config\root` directory.

4. Edit the configuration files in a text editor or XML editor. Use your old `Spotfire.Dxp.Automation.Launcher.exe.config` file as a reference to replicate your old configuration.

For more information on the configuration files, see [Service configuration files](#).

For information on which service configuration files contain the settings from your old `Spotfire.Dxp.Automation.Launcher.exe.config` file, see [Mapping content of old configuration files to new service configuration files](#).

5. On the command line, import the configuration files to the Spotfire Server by using the `import-service-config` command. Give the configuration a name.

Example:

```
config import-service-config --config-name=AutomationServicesConfiguration
```

6. On the command line, use the `set-server-service-config` command to assign the created Automation Services configuration to the Spotfire Server to make it available for services:

```
config set-server-service-config --capability=AUTOMATION_SERVICES --config-name=AutomationServicesConfiguration
```

7. Install Automation Services as a service on a node as described in [Installing Spotfire Automation Services instances](#).

In the Install new service dialog, select the configuration that you imported.

8. Use the Administration Manager in Spotfire Analyst to assign *licenses* required by the Automation Services jobs to the `automationservices@SPOTFIRESYSTEM` user, which is the account used to execute the jobs on the service instance. For a description of the licenses, see the Administration Manager help.
9. Make sure that all users who should execute automation services jobs are members of the group Automation Services Users.
10. Existing scheduled jobs using the Client Job Sender must be updated because the configurations have changed and the Client Job Sender now connects to the Spotfire Server instead of an Automation Services server. For more information, see the Automation Services help.

Upgrading authentication method

Spotfire Server is now used for all authentication.

In the old architecture, you set up authentication on the Spotfire Server for Spotfire Analyst users and on the Spotfire Web Player server for Spotfire web client users. In the new architecture you set up the authentication for all users on the Spotfire Server.

This means that the same authentication method is used for Spotfire Analyst users and Spotfire web client users.

For information on how to set up the authentication method on Spotfire Server, see [User authentication](#).



Impersonation is no longer applicable for single sign-on authentication methods because users now authenticate towards Spotfire Server directly.



If you used custom authentication on the Spotfire Web Player server, see [External authentication](#).

There are, however, some special cases where different authentication methods have been used. See [Anonymous combined with other authentication method](#) and [Different authentication methods for Spotfire Server and Web Player](#).

Anonymous combined with other authentication method

Anonymous authentication can be combined with another authentication method on the same Spotfire Server.

If you previously had a system with multiple Spotfire Web Player servers, where some used Anonymous authentication and some used another authentication method, this is now done on the same Spotfire Server.

To do this, first set up the authentication method you want to use. For more information, see [User authentication](#).

Then also enable Anonymous authentication on the Spotfire Server. For more information, see [Configuring anonymous authentication](#).

Different authentication methods for Spotfire Server and Web Player

It is no longer supported to use different authentication methods for the Spotfire Server and the Spotfire Web Player.

Because all users connect to the Spotfire Server, it is not possible to use different authentication methods for Spotfire Analyst users and Spotfire web client users. If you previously used different authentication methods, you must now decide on one authentication method for all users.



As of Spotfire version 7.9, you can use sites to configure multiple authentication methods within a single Spotfire environment.

Upgrading load balancing

In the new architecture, you no longer need a load balancer between the Spotfire Server and Spotfire Web Players.

If you have a system with multiple Spotfire Web Player servers and a load balancer, the load balancer is no longer needed. In the new architecture each Web Player service on each node can have multiple instances running. The load balancer is replaced by the routing capabilities in the new architecture. For information on how to set up routing of users, see [Creating resource pools](#) and [Routing rules](#).

If you have a cluster of Spotfire Servers, you can still use a load balancer in front of them. For more information, see [Clustered server deployments](#).

Upgrading analysis links

If you have web links to analyses, these must be updated to work in the new architecture.

You no longer install a Spotfire Web Player server that web client users connect to. Now all web client users connect to a Spotfire Server that has a Spotfire Web Player service installed on a node. Therefore, to make old links to web player analysis files continue to work as previously, the DNS entry to the former Web Player server must now point to the Spotfire Server.

If a custom virtual directory (other than the default `SpotfireWeb`) was previously used an additional mapping must be added to the file

```
server installation dir\tomcat\webapps\ROOT\WEB-INF\web.xml.
```

Locate the following section and add all custom directory remappings as a semicolon-separated string.



The target part of the mappings should always be "spotfire/wp".

```
<filter>
  <filter-name>RedirectFilter</filter-name>
  <filter-class>com.spotfire.server.security.RedirectFilter</filter-class>
  <init-param>
    <param-name>rules</param-name>
    <param-value>SpotfireWeb=spotfire/wp;MyCustomVirtualDirectory=spotfire/wp</
param-value>
  </init-param>
</filter>
```

Upgrading Web Services API clients

If you have created clients to the Spotfire Server Web Services API and you plan to activate the CSRF protection that is now available, the clients must be modified to work properly in the new architecture.

If you do not plan to activate the CSRF protection for the public Web Service API, nothing needs to be done.

For more information about the CSRF protection and how the clients should be updated, see the Web Services API documentation on <https://docs.tibco.com/products/tibco-spotfire-server>.

Upgrading customizations

If you have any custom extensions, they must be deployed to the Spotfire Server. Some of them must be edited before deployment to work in the new architecture.

Upgrading custom visualizations

If you are using the custom visualization extension in the Spotfire web client, the extension must be modified to work properly in the new architecture.

Both the C# code and the JavaScript code require changes. For instructions on how to update the code, see the article [Create a Custom Visualization in TIBCO Spotfire](#) on the TIBCO Community site.

After the changes have been made, you must rebuild the custom visualization extension package and deploy it to the Spotfire Server. For more information, see [Adding software packages to a deployment area](#).

Upgrading cobranding

If you have cobranded an earlier version of Spotfire, the cobranding must be updated and then deployed to the server.

For information on the changes and how to cobrand Spotfire, see the TIBCO Spotfire Cobranding help.

Upgrading from Spotfire 7.5 or later

As of Spotfire Server version 7.11.4, server hotfixes can be applied only on the specific service pack version that they were created for. Example: If you currently have Spotfire version 7.11.3, you can only apply server hotfixes for the 7.11.3 version, such as 7.11.3 HF-001, 7.11.3 HF-002, and so on. If you want a hotfix of a different service pack level, such as 7.11.5 HF-001, you must first make sure to upgrade to that service pack (7.11.5) before applying the hotfix. Client hotfixes have not changed.

The Spotfire Server and node manager upgrade tools copy all relevant settings, including configurations and node manager trust, to your new Spotfire environment.

Prerequisites

- Before upgrading, create a working backup of your Spotfire database.
- Download the required software from the [TIBCO eDelivery web site](#) and the [TIBCO Support website](#); for details, see [Downloading required software](#).

Procedure

1. Stop your Spotfire Servers and node managers. For information on how to stop them, see [Start or stop Spotfire Server](#) and [Starting or stopping node manager](#).
2. Set the **Startup type** to **Manual** for your existing Spotfire Servers and node managers to prevent the old installation from starting automatically and causing a port conflict with the new installation. For instructions, see [Preventing Spotfire Servers and node managers from starting automatically](#).
3. Install the new version of Spotfire Server. For instructions and details related to the upgrade, see [Installation of Spotfire Server during upgrade](#).
4. Upgrade the Spotfire Servers by running the Spotfire Server upgrade tool on each server. For more information, see [Run the Spotfire Server upgrade tool](#).



If your servers are clustered, run the upgrade tool on only one of the servers in the cluster.

5. Apply to all the Spotfire Servers any available server hotfix that has the same version number as the new server. For more information, see [Applying hotfixes to the server](#).



Do not apply any hotfixes whose three-digit version number is different from the new server's three-digit version number. Apply only the latest hotfix for the version number.

6. Start the new Spotfire Servers. For information on how to start the Spotfire Server, see [Start Spotfire Server](#).
7. Deploy the Spotfire client packages (`Spotfire.Dxp.sdn`) and node manager packages (`Spotfire.Dxp.NodeManagerWindows.sdn`) to the new Spotfire Server. For more information on how to deploy packages to Spotfire Server, see [Deploying client packages to Spotfire Server](#).
8. Upgrade the nodes by installing the new node manager and running the node manager upgrade tool on each node. For more information, see [Upgrading nodes](#).



When installing the new node managers, specify the same ports that were used by the old node managers.

9. After the upgrade, make sure that the Administrator group has all licenses, including new ones, assigned to it. Use the Administration Manager in Spotfire Analyst to assign licenses. For a description of the licenses, see the Administration Manager help.
10. Start the node managers. For information on how to start the node managers, see [Starting or stopping a node manager \(as a Windows service\)](#).
11. Update all services on all nodes in your environment. For information on how to update the services, see [Upgrading services](#).
12. Optional: Verify or edit changes to service configuration files. Your existing configurations will work in the new version of Spotfire, but some settings have been added or changed and must be updated manually if you do not want to use the default values. For more information, see [Upgrading service configurations](#).

Installation of Spotfire Server during upgrade

When you install Spotfire Server, the upgrade tool is installed as well.

Before installing the new version of Spotfire Server, note the following:

- Configure the new server to use the same ports as the previous installation. This will not cause a port conflict if you have followed steps 1 and 2 in [Upgrading from Spotfire 7.5 or later](#).
- Make sure to install the latest hotfix on all servers before running the upgrade tool.
- Do not start or configure the newly installed server before running the upgrade tool.
- If you intend to copy information from the old version, do not uninstall it until the new version of Spotfire Server is in place.

For general instructions on how to install Spotfire Server, see [Installation](#).

Preventing Spotfire Servers and node managers from starting automatically

When upgrading Spotfire Servers and node managers to the next version, you must prevent the old version of these components from starting automatically when Windows starts. Because the old and new versions use the same communication ports, starting both versions results in a port conflict.

These instructions apply to servers that are running as a Windows service.

Procedure

1. Log in to the Spotfire Server or node manager computer as an administrator.

2. Go to **Control Panel > Administrative Tools > Services** and then, in the Services dialog, locate and select the previous version of the service called **TIBCO Spotfire Server** or **TIBCO Spotfire Node Manager**.
3. Right-click the service and then click **Properties**.
4. In the center of the Properties dialog, next to **Startup type**, select **Manual** and then click **OK**.

Result

When you restart Windows, the server or node manager will not start automatically.

Applying hotfixes to the server

Before you run the upgrade tool, you must install on all servers any available hotfix for the new version of the server.

Prerequisites

- You have installed Spotfire Server.
- You have downloaded the latest hotfix for your new version of Spotfire Server; for instructions, see [Downloading required software](#).

Procedure

- Follow the instructions in the `Installation_Instructions.htm` file that was included in the hotfix package that you downloaded.

For more information, see [Overview of hotfixes for TIBCO Spotfire](#) in the TIBCO Community.

Run the Spotfire Server upgrade tool

The server upgrade tool updates the database. You can run the upgrade tool interactively, or silently by using the command-line interface.



If you have not already done so, make a working backup of your Spotfire database.

For information on how to run the upgrade tool, see [Running the upgrade tool interactively](#) or [Running the upgrade tool silently](#).

Running the Spotfire Server upgrade tool interactively

When you run the Spotfire Server upgrade tool interactively, you are prompted for information about both your older installation and your new installation.



If you are upgrading a cluster of Spotfire Servers, run the upgrade tool on only one server. The Spotfire database will be updated when you run the upgrade tool.



If Spotfire Server is set up to authenticate with the Spotfire database using Windows Integrated Authentication, it is important that you run the upgrade tool as the same user that Spotfire Server authenticates as. Otherwise, the upgrade tool will not be able to authenticate with the database.



The upgrade will perform a validation of LDAP configurations. If an invalid LDAP configuration is found, the upgrade will fail. If so, go back to your previous installation, correct the error, and perform the upgrade again.

Prerequisites

- You have installed the new version of Spotfire Server and any available hotfixes.

- You have a working backup of your Spotfire database.
- If you are using LDAPS, and if the CA certificate is not included in the cacert file by default, you must import the CA certificate used to issue the LDAP server's certificate *before* running the upgrade tool. See [Configuring LDAP](#).

Procedure

1. If the server upgrade tool is not already open, go to the following directory and double-click `upgradetool.bat` (Windows) or `upgradetool.sh` (Unix): *new version Spotfire Server install dir/tools/upgrade*
By default, the server installation directory is located here: `C:/tibco/tss/version number`.
2. The Spotfire Server Upgrade panel is displayed. It provides a reminder to back up or clone the Spotfire database. Click **Next**.
The File Locations panel is displayed. It provides new information and the choice to copy, or not to copy, an existing configuration.
3. If you have file access to an old installation, you can select **Previous server installation** and enter the path to its installation directory, for example: `C:/tibco/tss/version number` or `/opt/tss/version number`. Click **Next**.
If there are changes needed after the upgrade, for example, port configuration or the location of TLS certificate, manually edit the `server.xml` file, located in the *Spotfire Server install dir/tomcat/conf* directory.
4. If you did not copy an existing configuration, the Database Type and Driver panel is displayed. Here, specify the database and database driver you are using, and click **Next**.
If you select a database driver type that is not installed in the old installation directory, the message "The selected driver must be installed manually" is displayed. Install the driver manually by placing it in the *new version Spotfire Server install dir/tomcat/lib* directory and restart the upgrade tool.
If you select a database driver type that is not installed and click **Next**, the Database Drivers Not Installed panel is displayed. If this occurs, click **Done** to exit the upgrade tool, then install the database driver and start the upgrade tool again.
The Database Connection Information panel is displayed.
5. Here, provide the Spotfire database **Connection string**, **Username** and **Password**. If your database server uses integrated login, like Windows authentication, select the **Integrated login** check box, to disable the Username and Password fields. Click **Next**.
6. If you did not copy an existing configuration, the Additional Information panel is displayed. Here, specify the configuration tool password, the encryption password, and the server name to use when configuring the Spotfire Server, and click **Next**.
7. If LDAP User Directory mode or Windows NT User Directory mode is used, the User Directory Configuration panel is displayed. Here, select a **domain name style** (DNS or NetBIOS) and a **default domain**.

Make sure to select an accurate domain name style for your system. For more information, see [External directories and domains](#).

The Summary panel is displayed.
8. Click **Upgrade**.
The Upgrade panel is displayed. Here you can see if the upgrade was successful. If there were problems with the upgrade, click **Next** to get information on where the issues have been logged.
9. When the upgrade has been successfully completed (the text "Upgrade done" appears in the panel), click **Finish**.

Running the Spotfire Server upgrade tool silently

As an alternative to running the upgrade tool interactively, you can run it silently using the command line.



If you are upgrading a cluster of Spotfire Servers, run the upgrade tool on only one server. The Spotfire database will be updated when you run the upgrade tool.



If Spotfire Server is set up to authenticate with the Spotfire database using Windows Integrated Authentication, it is important that you run the upgrade tool as the same user that Spotfire Server authenticates as. Otherwise, the upgrade tool will not be able to authenticate with the database.



The upgrade will perform a validation of LDAP configurations. If an invalid LDAP configuration is found, the upgrade will fail. If so, go back to your previous installation, correct the error, and perform the upgrade again.

Prerequisites

- You have installed the new version of Spotfire Server and any available hotfixes.
- You have a working backup of your Spotfire database.
- If you are using LDAPS, and if the CA certificate is not included in the cacert file by default, you must import the CA certificate used to issue the LDAP server's certificate *before* running the upgrade tool. See [Configuring LDAP](#).

Procedure

1. Go to the following directory: *new version Spotfire Server install dir/tools/upgrade*.
2. Open the file `silent.properties` in a text editor or XML editor.
3. Follow the instructions in the file and specify the values of the parameters.
The `from` parameter is the only parameter that you are required to specify.
4. Save the `silent.properties` file.
5. Open a command line.
6. To see the parameters that the upgrade tool will use, do one of the following:

- On Windows, type `upgradetool.bat -h`.
- On Linux, type `upgradetool.sh -h`.

The parameters are listed on the command line. Review the list of parameters and specify any that are applicable for your server.

7. To run the upgrade tool silently, do one of the following:
 - On Windows, type `upgradetool.bat -silent silent.properties`.
 - On Linux, type `upgradetool.sh -silent silent.properties`.
8. Press **Enter**.
The upgrade tool runs silently.

Start Spotfire Server

When the upgrade tool has completed without issues, you should start the Spotfire Server.

For information on how to start the Spotfire Server, see [Starting Spotfire Server](#).

To verify that Spotfire Server has been installed and started, launch a browser and go to the Spotfire Server start page: `http://<hostname>:<port>/spotfire`.

Upgrading nodes

To upgrade the nodes, install the new node managers on the same computers as the old node managers. Then run the node manager upgrade tool on each new node manager.



Set the **Startup type** to **Manual** for your existing node managers to prevent the old installation from starting automatically and causing a port conflict with the new installation. For instructions, see [Preventing Spotfire Servers and node managers from starting automatically](#).

Install node manager

The node manager upgrade tool is installed along with the new node manager.

You can install a node manager either interactively with a graphical interface or silently by using the command line.

- For the interactive installation, see [Installing a node manager interactively during upgrade](#).
- For the silent installation, see [Installing a node manager silently](#). Then see [Running the node manager upgrade tool silently](#)



Configure the node managers to use the same ports as the previous installation. This will not cause a port conflict if you have followed steps 1 and 2 in [Upgrading from Spotfire 7.5 or later](#).



Do not start the newly installed node manager before running the upgrade tool.

Installing a node manager interactively during upgrade

Install the new node manager on the same computer as the old node manager. You must run the node manager installer with administrative permissions.

Prerequisites

- Spotfire Server is installed and running.

Procedure

1. In the installation kit, right-click `nm-setup.exe` and then click **Run as administrator**.
2. On the installation wizard Welcome page, click **Next**.
3. On the License page, read the agreement, select **I accept**, and then click **Next**.
4. On the Destination Folder page you can change the location if you want to, and then click **Next**. The Node Manager Ports page opens.
5. On the Node Manager Ports page, specify the same ports that were used by the old node manager.
6. Click **Next**. The Spotfire Server page opens.
7. On the Spotfire Server page, enter the following information, and then click **Next**.



These values must match the values you used when installing the Spotfire Server files.

- **Server name**—The hostname of Spotfire Server.



Valid hostnames may contain only alphabetic characters, numeric characters, hyphens, and periods.

- **Server backend registration port**—The registration port that you specified during Spotfire Server installation.

- **Server backend communication port (TLS)**—The back-end communication port that you specified during Spotfire Server installation.
8. On the Network Names page, select the computer names that can be used by back-end trust. In general you can leave all the listed names as they are.
 9. On the Ready to Install page, click **Install**.



Do not start the newly installed node manager before running the upgrade tool.

10. On the Install Wizard Completed page, select **Launch the upgrade tool** and click **Finish**.

What to do next

[Running the node manager upgrade tool interactively](#)

Run the node manager upgrade tool

You can run the node manager upgrade tool interactively, or silently by using the command-line interface.

For information on how to run the node manager upgrade tool, see [Running the node manager upgrade tool interactively](#) or [Running the node manager upgrade tool silently](#).

Running the node manager upgrade tool interactively

When you run the node manager upgrade tool interactively, you are prompted for the installation directory of both your old node manager installation and your new installation.

Prerequisites

You have installed the new node manager.

Procedure

1. If the node manager upgrade tool is not already open, go to the following directory and double-click `upgradetool.bat`: *new node manager installation dir/nm/upgrade*. By default, the node manager installation directory is located here: `C:/tibco/tsnm/version number`. The node manager upgrade tool opens.
2. In the **Upgrade to path** field, specify the location of your new node manager installation directory.
3. In the **Upgrade from** field, specify the location of your old node manager installation directory.
4. Indicate whether you want the upgrade tool to start the node manager Windows service after upgrade.
5. Click **Run Upgrade**.
The result of the node manager upgrade is shown in the text field below the controls.
6. When the node manager is successfully upgraded, close the node manager upgrade tool window.

Running the node manager upgrade tool silently

As an alternative to running the node manager upgrade tool interactively, you can run it silently from the command line.

Prerequisites

You have installed the new node manager.

Procedure

1. On the command line, go to the directory *new node manager installation dir/nm/upgrade*.
2. Run the following command .

```
upgradetool.bat --cmd --from old node manager installation dir --to new node manager installation dir
```

The node manager upgrade tool runs silently.

Optional upgrades

The following upgrades may or may not apply to your Spotfire implementation.

Upgrading service configurations

Service configuration changes require manual updates if you do not want to use their default values.

To get the correct configuration files, it is recommended that you export both the default new service configuration and your old service configuration from Spotfire Server by using the [export-service-config](#) command. Then apply all changes made in the old configuration files to the new configuration files. Then import the new configuration back into Spotfire Server by using the [import-service-config](#) command, and use this configuration for your new services.

For more information on how to edit the configuration files, see [Manually editing the service configuration files](#).

For information on the added or changed settings, see the topics for the appropriate configuration files.

Changes introduced in Spotfire 7.6

[Spotfire.Dxp.Worker.Web.config](#)

Additional service configuration settings were added for the mini-dump creation if a service goes down unintentionally.

In the `<errorReporting>` section, the following settings were added: `miniDumpSizeLarge="false"` and `miniDumpPath=""`.



The `miniDumpSizeLarge` setting can create a very large dump file that should not be edited unless instructed by Spotfire Support.

Changes introduced in Spotfire 7.9

[Spotfire.Dxp.Worker.Host.exe.config](#)

The following proxy handling settings were added, if you need to use proxy handling for communication from the Web Player service or Automation Services to Spotfire Server:

`ProxyUsername`, `ProxyPassword` and `<defaultProxy>`.

[Spotfire.Dxp.Worker.Automation.config](#)

The section `<Spotfire.Dxp.Automation.Framework>` has been added, where you can specify which directories Automation Services tasks can read from, write to, and delete from.

The settings `useKerberos` and `kerberosIdentity` have been added to be able to run Automation Services jobs as a specified Windows account when delegated Kerberos is used in the environment.

[Spotfire.Dxp.Worker.Web.config](#)

The following settings have been added to configure the use of a tool, such as `cdb.exe`, to automatically capture dumps for hanging service instance processes: `dumpToolPath`, `dumpToolFlagsSmall`, `dumpToolFlagsLarge`.

The settings `useKerberos` and `kerberosIdentity` have been added to be able to run scheduled updates as a specified Windows account when delegated Kerberos is used in the environment.

The setting `allowGcEvenIfAnalysesLoaded` has been added. It allows you to run garbage collection even if analyses are open.

The default value of the setting `requestTimeoutSeconds` has been changed from 300 seconds to 3600 seconds.

Upgrading custom-modified `log4j.properties` files

For Spotfire Server 7.9, the logging framework was upgraded from Log4j to Log4j2. If you used a custom-modified `log4j.properties` file in any Spotfire Server version between 7.5 and 7.8, you must manually add these modifications to the new `log4j2.xml` file to continue using the same logging properties.

Note that custom edits to the `log4j2.xml` file are intended for settings that are not available in the administrative interface, such as adding log appenders or changing the log size or rotation.

Procedure

1. Open the `log4j.properties` file from your previous Spotfire Server installation.
2. Open the new version of the following Spotfire Server file in an XML editor or a text editor: *<new Spotfire Server installation dir>/tomcat/spotfire-config/log4j2.xml*.
3. Add the modifications from the old file to the new file, using the new, XML-based format. For full documentation of the new format, see <https://logging.apache.org/log4j/2.x/manual/configuration.html>.
4. Save and close the file.
5. Restart the server.

Applying hotfixes to the Spotfire environment

Any available hotfixes for components of your Spotfire environment should be downloaded and installed.



As of Spotfire Server version 7.11.4, server hotfixes can be applied only on the specific service pack version that they were created for. Example: If you currently have Spotfire version 7.11.3, you can only apply server hotfixes for the 7.11.3 version, such as 7.11.3 HF-001, 7.11.3 HF-002, and so on. If you want a hotfix of a different service pack level, such as 7.11.5 HF-001, you must first make sure to upgrade to that service pack (7.11.5) before applying the hotfix.

Client hotfixes have not changed.

For general hotfix information and links to specific information about each hotfix, see [Overview of hotfixes for TIBCO Spotfire](#) in the TIBCO Community.

Procedure

1. Sign in to the [TIBCO Support website](#).
2. Click **Downloads > Hotfixes**.
3. On the Available Hotfixes page, expand **AvailableDownloads** and **Spotfire**.
4. For each product component in your implementation, locate and select the folder containing the latest hotfix for your product version and click **Download**.



Service hotfixes are in the `Clients (Analyst_WebPlayer_AutomationServices)` folder.

5. When the download is complete, unzip the folder's contents and follow the instructions in the `Installation_Instructions.htm` file.

Applying hotfixes for services

Any available hotfixes for your Automation Services or Web Player services should be downloaded and installed.

Procedure

1. Go to <https://support.tibco.com> to download the latest hotfix for your services. For instructions, see [Applying hotfixes to the Spotfire environment](#).
2. Deploy the downloaded Spotfire distribution to the Spotfire Server. For instructions, see [Deploying client packages to Spotfire Server](#).
3. Update the services. For instructions, see [Updating services](#).

Backup and restore

To enable recovery after a crash or disaster in your Spotfire environment, it is important that information stored in the system is backed up. Most of this information is stored in the Spotfire database, but some of it is stored on the Spotfire Server.

This manual will not describe how to perform backups, only what to back up. It is assumed that you have some sort of backup software for files and computers, and that you use the backup tools provided with the database. Refer to the database documentation for instructions on how to perform backups.

One can only restore to a machine running the same operating system as the backed up system, since there is a bundled Java runtime with binaries for a specific architecture.

Back up each server in the cluster.

The following sections describe what needs to be backed up.

Backup of Spotfire database

The most important part of the Spotfire environment to back up is the Spotfire database.

It contains tables which store the state of the server, for example the library, preferences, and deployments. Most of the server and service configuration files are also stored in the database. Even if only the database has been backed up, it is still possible to restore most of the functionality after a crash. It is therefore vital that you have a valid and current backup of the Spotfire database.



Verify your backups.

Backup of Spotfire Server

A small set of configuration is unique for each Spotfire Server and is stored on the actual Spotfire Server rather than in the database.

This includes information about how Spotfire Server connects to the Spotfire database, which ports the server should listen to, authentication methods such as Kerberos etc.

During installation the server files are essentially all placed in the installation directory. It should be sufficient to back up this directory, of course it is possible to back up the entire file system.

Once a server has been configured or hotfixed there are no further persistent changes. Log files and other temporary files will change, but a restored backup will have the same functionality.

The configuration which is not in the database includes:

- Listening ports configuration. See [The server.xml file](#) for more information.
- Database connection and database drivers. See [Database drivers and database connection URLs](#) for more information.
- Logging configuration. See [Monitoring and diagnostics](#) for more information.
- Memory configuration. See [Virtual memory modification](#) for more information.
- HTTPS. See [HTTPS](#) for more information.
- Authentication such as Kerberos or Client Certificates.
- Any other advanced configuration performed in [Advanced procedures](#). When performing advanced configuration, you should always take backup into consideration.



The `bootstrap.xml` file is not stored in the database either. However, since the `bootstrap.xml` file contains a unique server ID, it can not be re-used if a server is restored on another computer. Therefore, in the event of a server crash where the server is restored on another machine, it is recommended to bootstrap the server again.

Whenever you make any configuration changes or have applied a server hotfix, you should also perform a backup of the Spotfire Server installation directory.

Windows Installations

On Windows installations, there is functionality which will not be restored by only recovering the Spotfire Server installation directory:

- Windows Service
- Uninstall functionality
- Start Menu shortcuts

The Windows Service can be (re-)installed using the bat file `service.bat` located in the `<installation_dir>\tomcat\bin` directory. Run it on the command line with the following arguments: `C:\tibco\tss\<version>\tomcat\bin>service.bat install`.

Uninstallation can be done by removing the service and simply remove the installation directory.

The Start Menu shortcuts can be backed up by copying them to the server installation directory, back that up, and when restoring, copying these files to the start menu directory.

Unix and Linux Installations

On Unix and Linux installations, no essential data is placed outside the installation directory by Spotfire Server. If you have a startup script for the server, it will need to be recreated.

Network Considerations

If you are using Kerberos you should note that configuration needed for this to work is tied to a specific machine and cannot be copied easily to a new one.

You should also consider any other conditions in your environment and their implications, such as IP addresses and firewall rules, LDAP restrictions, and anything else that might affect getting a system back up and running.

Backup of services

The service configuration files are stored in the Spotfire database, so there is no need to make additional backups for the services.

If a node or service must be restored, install it again and select the configuration used for the old service.



Information on which resource pools the service instances should be used for is not stored in the database. The new service instances must be assigned to the old resource pools manually.

Uninstallation

To perform a complete uninstallation of your Spotfire environment, the following steps must be completed, in order.

Deleting services

The first step of uninstalling the Spotfire environment is to delete the installed services.

Procedure

1. Go to the Spotfire Server start page and log in as an administrator.
2. Click **Nodes & Services**.
3. On the **Your network** page, under **Select a view**, select **Nodes**.
4. In the left pane, expand the entries under the node and select the service.
5. In the right pane, click **Delete** for each installed service.

Revoking trust of nodes

The second step of uninstalling the Spotfire environment is to revoke the trust for all installed nodes. For instructions on how to revoke the trust of a node, see [Revoking trust of a node](#).

This must be done for each node in your Spotfire environment.

Uninstalling node manager

The third step of uninstalling the Spotfire environment is to uninstall all node managers.

Uninstallation of the node manager is performed through the regular Windows procedure. On each machine with a node manager installed, click **Start > Control Panel > Programs and Features > Uninstall or change a program**. Then right-click **TIBCO Spotfire Node Manager** and select **Uninstall**.

Uninstalling Spotfire Server

The fourth step of uninstalling the Spotfire environment is to uninstall the Spotfire Server(s).

If you have placed any additional files in the installation directory or any of its subdirectories, such as Spotfire Library export files, you should move these files to a secure location before uninstalling. The installer will remove the installation directory and all its subdirectories.

Windows

Uninstallation of Spotfire Server is performed through the regular Windows procedure. On each computer with a Spotfire Server installed, click **Start > Control Panel > Programs and Features > Uninstall or change a program**. Then right-click **TIBCO Spotfire Server** and select **Uninstall**.

After successful uninstallation, only use-modified files (such as custom JDBC drivers) remain on the computer.

RPM Linux

On each computer with a Spotfire Server installed, uninstall the server by running the command:

```
rpm -e tss-<version number>
```

After a successful uninstallation, only modified files in `tomcat/conf` remain.

Tarball Linux

On each computer with a Spotfire Server installed, uninstall the server by running the following commands:

If the Spotfire Server was configured to start on boot, it must be stopped and removed.

To stop the server, run the command:

```
service tss-<version number> stop
```

To remove the server, run the command:

```
chkconfig --del tss-<version number>
```

Delete added scripts by running the following commands:

```
rm /etc/init.d/tss-<version number>
```

```
rm /etc/sysconfig/tss-<version number>
```



To be able to do this, you must have root access.

The final step is to remove the folder with Spotfire Server files. Do this by running the following command:

```
rm -rf <folder where the tarball was installed>
```

Advanced procedures


These manual procedures are for setting up various features that are supported by Spotfire. Many of the procedures assume prior knowledge of technologies such as LDAP, Kerberos, Apache httpd, and so on.

Custom configurations for managing space needs

If you need more space for library content, log files, information links, or the files that the Web Player service writes to the hard disk, you can change the default settings to store these items in different directories.

For information about the system requirements for Spotfire Server, see <http://support.spotfire.com/sr.asp>.

Links to information for changing settings

Configuration need	For more information
Change the directory where Spotfire Server log files are written.	Follow the instructions in Changing the default location of server logs .
Configure the directory for library imports and exports.	Use the configuration command config-import-export-directory .
 Change the maximum size of the cache for the Web Player service Information Links and library content. If Spotfire Server is configured to cache Information Links and library content, this uses additional disk space. By default, caching is enabled and the max cache size set to 10 GB.	Set the <code>--max-cache-size</code> option for the configuration command config-attachment-manager .
Change the amount of disk space available for all of the log files generated by the Web Player service.	Follow the instructions in Customizing the service logging configuration .
Change the location of the temporary directory that the Web Player service uses for temporary files, paging, and caching data (scheduled updates caching and SBDF caching).	Follow the instruction in Changing the default location of the Web Player temporary files .

Changing the default location of the Web Player temporary files

By default the Web Player service stores temporary files, paging, and caching data (scheduled updates caching and Spotfire Binary Data File (SBDF) caching) in the Temp directory inside the service installation directory. If you need to change the location, or if Spotfire Support suggests that you change it, follow this procedure.

Procedure

1. On the computer running Spotfire Server, open a command line as an administrator and change the directory to the path of the `config.bat` file (`config.sh` on Linux).

The default file path is `<server installation dir>/tomcat/bin`.

2. Export the service configuration by using the [export-service-config](#) command.

Example:

```
config export-service-config --tool-password=mypassword --capability=WEB_PLAYER
--deployment-area=Production
```

3. Open the `Spotfire.Dxp.Worker.Host.exe.config` file in a text editor or XML editor and locate the following section. By default, the exported configuration files are saved to the `<server installation dir>/tomcat/bin/config/root` directory.

```
<Spotfire.Dxp.Internal.Properties.Settings>
  <setting name="TempFolder" serializeAs="String">
    <value>Temp</value>
  </setting>
```

4. Replace the value `Temp` with the path to the new Temp directory.



The Temp directory should be located on a local disk.

Example:

```
<Spotfire.Dxp.Internal.Properties.Settings>
  <setting name="TempFolder" serializeAs="String">
    <value>C:\NewTemp</value>
  </setting>
```

5. Save and close the configuration file.
6. Return to the command line and import the custom configuration using the [import-service-config](#) command.

Example:

```
config import-service-config --tool-password=mypassword --config-
name=SampleConfig
```

7. Apply the custom configuration to specific services by using the [set-service-config](#) command.

Example:

```
config set-service-config --tool-password=mypassword --service-id="VALUE" --
config-name=SampleConfig
```



Use the [list-services](#) command to get the service ID.

Result

The configuration setting for the indicated Web Player service is displayed in Nodes & Services, and the Web Player temporary files should be written as specified.

Temporary tablespace

By default, the tablespaces/database files for Spotfire Server with either an Oracle or SQL database uses autoextend/autogrowth. If this does not meet your needs, alter the settings.

You may want to alter the amount that the files are extended with each increment.

For Oracle, review the maxsize for each table space. For SQL, review the unlimited growth property.

Virtual memory modification

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 computer.

Modifying the virtual memory (server not running as Windows service)

If Spotfire Server is not running as a Windows service, you can modify the virtual memory by following these steps to set up the start script.

Procedure

1. Open the file <installation_dir>/tomcat/bin/setenv.bat or <installation_dir>/tomcat/bin/setenv.sh in a text editor.
2. Locate the line that sets the variable CATALINA_OPTS.
3. Set the following values to the amount of memory you want to allocate:
 - -Xms512M
 - -Xmx4096M
4. Restart the server.

Modifying the virtual memory (server running as Windows service)

If Spotfire Server is running as a Windows service, you can modify the virtual memory by following these steps to set up the start script.

Procedure

1. Stop the Spotfire Server service.
2. On the command line, go to the <installation_dir>/tomcat/bin directory.
3. Enter the following command: `service.bat remove`
4. Open the <installation_dir>/tomcat/bin/service.bat file in a text editor.
5. Locate the following entries and change the numbers to suitable memory values (in MB):
 - `--Jvms 512`
 - `--JvmMx 4096`
6. Save and close the file.
7. Enter the following command: `service.bat install`
8. Start the Spotfire Server service.

Data source templates

Data source templates are used when creating *information links*. Using the Information Designer tool found in Spotfire Analyst, a database administrator can create custom data source templates to define the data sources that are available to users when they create information links.

For more information about the Information Designer, see the Spotfire Analyst help.

Spotfire Analyst includes two data source templates:

- Oracle (DataDirect driver)
- Microsoft SQL Server (DataDirect driver)

Custom data source templates can be based on the following data sources:

- Teradata
- Sybase (JTDS)

- Sybase (DataDirect)
- Sybase
- SQL Server 2005
- SQL Server (JTDS)
- SQL Server (DataDirect)
- SQL Server
- SAS/SHARE
- Composite
- Oracle (delegated Kerberos)
- Oracle (DataDirect)
- Oracle
- MySQL5
- MySQL (DataDirect)
- MySQL
- DB2 (DataDirect)
- DB2



If you add a data source template that does not use the pre-installed DataDirect driver, you must manually install this driver on each Spotfire Server in the cluster before you restart the cluster. Download the appropriate driver JAR file and place it in the `/tomcat/lib` folder of each server.

Setting up MySQL5 vendor driver

For the MySQL5 vendor driver to work with MySQL data sources that include `TIMESTAMPS` that can potentially be null, you must edit the template.

Procedure

1. In the MySQL5 data source template, locate the following section:

```
<connection-properties>
  <connection-property>
    <key>useDynamicCharsetInfo</key>
    <value>>false</value>
  </connection-property>
</connection-properties>
```

2. Within the `connection-properties` tag, add the following code:

```
<connection-property>
  <key>noDatetimeStringSync</key>
  <value>true</value>
</connection-property>
<connection-property>
  <key>zeroDateTimeBehavior</key>
  <value>convertToNull</value>
</connection-property>
```

Data source template commands

You can use these command-line commands to handle data source templates.

If you want to	Use this command	Notes
Add a new data source template	add-ds-template	
Enable, modify, or disable a data source template	modify-ds-template	For a data source template to become available in the Information Designer, it must be enabled.
Remove a data source template	remove-ds-template	Verify that no data sources use the data source template before you remove it. If a data source template is removed, all data sources using that template stop working.

XML settings for data source templates

The following table defines all the available XML settings for data source templates; only the first three are required. All other settings use their default values if not specified.

Setting	Description	Default value
type-name	A unique name for the configuration.	
driver	The JDBC driver Java class used for creating connections.	
connection-url-pattern	A pattern for the connection URL. The 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
sql-filter	Java class that generates SQL.	BasicSQLFilter
sql-runtime	Java class that handles SQL execution.	BasicSQLRuntime


Setting	Description	Default value
fetch-size	A fetch size specifies the amount of data fetched with each database round trip for a query. The specified value is shown as the default value in Information Designer. May be changed at instance level.	10000
batch-size	A batch size specifies the amount of data in each batch update. The specified value is shown as the default value in Information Designer. May be changed at instance level.	100
max-column-name-length	The maximum length of a database column name. This limit is used when creating temporary tables.	30
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\$\$"

Setting	Description	Default value
schema-name-pattern	Determines how a schema name is written in the SQL query	\$\$\$name\$\$
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. A Data Base Administrator may prefer a lower value than the default. Depends on the maximum SQL query size.	10000
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 and schema may be optional (surrounded by brackets).	[\$\$catalog\$\$][\$\$schema\$\$]\$\$table\$\$
procedure-expression-pattern	Determines how a procedure expression is written in the SQL query.	[\$\$catalog\$\$][\$\$schema\$\$]\$\$procedure\$ \$

Setting	Description	Default value
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. This is currently not visible to the user in any UI.	null
date-format-expression	An expression that converts a date field to a string value on the format: YYYY-MM-DD, for example, 2002-11-19. Used in WHERE and HAVING clauses. The tag \$\$value\$\$ is a placeholder for the date field.	\$\$value\$\$
date-literal-format-expression	An expression that converts a date literal on the format YYYY-MM-DD to a date field value. Used in WHERE and HAVING clauses. The tag \$\$value\$\$ is a placeholder for the date literal.	'\$\$value\$\$'
time-format-expression	An expression that converts a time field to a string value on the format: HH:MM:SS, for example 14:59:00. Used in WHERE and HAVING clauses. The tag \$\$value\$\$ is a placeholder for the time field.	\$\$value\$\$
time-literal-format-expression	An expression that converts a time literal on the format HH:MM:SS to a time field value. Used in WHERE and HAVING clauses. The tag \$\$value\$\$ is a placeholder for the time literal.	'\$\$value\$\$'

Setting	Description	Default value
date-time-format-expression	An expression that converts a datetime field to string value on the format: YYYY-MM-DD HH:MM:SS, for example 2002-11-19 14:59:00. Used in WHERE and HAVING clauses. The tag \$\$value\$ is a placeholder for the date-time field.	\$\$value\$\$
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. Used in WHERE and HAVING clauses. The tag \$\$value\$\$ is a placeholder for the date-time literal.	'\$\$value\$\$'
java-to-sql-type-conversions: <ul style="list-style-type: none"> • 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). 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.	VARCHAR(\$\$value\$\$) VARCHAR(255) INTEGER BIGINT REAL DOUBLE PRECISION DATE TIME TIMESTAMP
temp-table-name-pattern	Determines how to format a temporary table name in an SQL command.	\$\$name\$\$

Setting	Description	Default value
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. The syntax may vary between databases. \$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\$\$
drop-temp-table-command	SQL commands for deleting a temporary table. The syntax may vary between databases. \$name\$\$ is a placeholder for the table name	DROP TABLE \$\$name\$\$
data-source-authentication	Default value data source authentication. (boolean). This value can be set (overridden) in the Information Interaction Designer.	false
lob-threshold	Threshold when LOB values used as parameters in a WHERE clause, must be written in temporary tables. The default means no limit.	-1
use-ansi-join	The default generated SQL creates joins with where statements. If this setting is set to true, an attempt is made to rewrite it to standard ANSI format. If this setting is set to false, no attempt to rewrite inner joins will be made and outer joins depend on the value set for use-ansii-style-outer-join.	false

Setting	Description	Default value
use-ansi-style-outer-join	<p>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.</p> <div>  <p>If use-ansi-join is set to true, then this setting has no effect.</p> </div>	false
credentials-timeout	<p>Defines the time in seconds user credentials are cached on the server for a particular data source. Value must be between 900 (15 minutes) and 604800 (1 week). Applicable only if data-source-authentication is set to true.</p>	86400 (24 hours)

JDBC connection properties

The optional `<connection-properties>` parameter block in the 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 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.

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`. This example creates an encrypted connection to the database.

```
<jdbc-type-settings>
  <type-name>oracle</type-name>
  <driver>oracle.jdbc.OracleDriver</driver>
  <connection-
urlpattern>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>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>

```

Advanced connection pool configuration

Information Services uses the same underlying connection pool implementation as Spotfire Server uses for connecting to its own database. The following special parameters are available to configure some of the aspects of that connection pool.

Special parameter	Corresponding common parameter
spotfire.pooling.data.source.scheme	pooling-scheme
spotfire.pooling.data.source.connection.timeout	connection-timeout
spotfire.pooling.data.source.login.timeout	login-timeout
spotfire.kerberos.login.context	kerberos-login-context

For more information, see [Database connectivity](#).

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

Example: Configuring a connection pool for Oracle databases

```

<jdbc-type-settings>
<type-name>oracle</type-name>
<driver>oracle.jdbc.OracleDriver</driver>
<connection-
urlpattern>jdbc:oracle:thin:@<host>:<port1521>:<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</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>

```

Kerberos authentication for JDBC data sources

Configuring Kerberos authentication for JDBC data sources is similar to configuring Kerberos for the connection to the Spotfire database.

For more information, see [Using Kerberos to log in to the Spotfire database](#).

This is an example of configuring a connection pool for Oracle databases:

```
<jdbc-type-settings>
  <type-name>oracle</type-name>
  <driver>oracle.jdbc.OracleDriver</driver>
  <connection-
urlpattern>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.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>
```

Creating an Information Services data source template using Kerberos login

The default Information Services Data Source templates that are included with Spotfire Server are not configured to use Kerberos. You must therefore create a new data source template based on one of the default templates.

Procedure

1. List the existing data source templates by using the [list-ds-template](#) command and select one that matches the database you are setting up, for example Oracle.
2. Export the definition of the selected data source template by using the [export-ds-template](#) command.
3. Open the exported definition file in a text editor.
4. Add the JDBC connection property key `spotfire.connection.pool.factory.data.source` with the value `kerberos.data.source` within the `connection-properties` element. If there is no `connection-properties` element, create one.

There may also be other connection properties you must add; consult the documentation of the database server for more information. For general instructions about adding connection properties, see [JDBC connection properties](#).

Example:

```
<jdbc-type-settings>
  <type-name>oracle</type-name>
  <driver>oracle.jdbc.OracleDriver</driver>
  <connection-urlpattern>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-properties>
  <connection-property>
    <key>oracle.net.authentication_services</key>
```



```
<value>(KERBEROS5)</value>
</connection-property>
</connection-properties>
```

5. Use the [add-ds-template](#) command to add the new data source template with a suitable name, such as "oracle_kerberos", using the modified template definition.
6. Import the configuration and restart the server.

What to do next

[Verify the data source template](#)

Verifying a data source template

Procedure

1. Log in to Spotfire Analyst as an administrator.
2. Select **Tools > Create Information Link**
3. Click **Setup Data Source**.
4. Enter a name for the data source connection.
5. Specify the type of data source.
6. Enter the **connection URL** and **max/min-values** for the connection pool.
7. Enter a username and a password to connect to the database.



This does not apply to Kerberos.

8. Click **Save**.
9. In the left pane, click the **Data sources** tab.

Result

The data source name should appear in the tree to the left, ready for use.

Information Services settings

Information Services provides end users with the ability to access and pivot data from multiple databases simultaneously, without having to know anything about installing database drivers, underlying data schemas or SQL.

End users' access to data from multiple sources can be configured and controlled through settings in Information Services. Below is a list of common settings with short descriptions. For instruction on changing the settings, see [Manually editing the Spotfire Server configuration file](#).

Setting	Description
information-services.jdbc.oracle.use-faster-schema-listing	List all Oracle users as schema list.
information-services.dat.no-sbdf	Use Spotfire text data format or Spotfire binary data format when transferring data from Spotfire Server to a Spotfire client.

Setting	Description
<code>information-services.runtime-query-validation</code>	Validate information link prior to execution.
<code>information-services.dat.data-block-queue-size</code>	Maximum number of queued (not yet consumed by client) data blocks per job.
<code>information-services.dat.idle-limit</code>	Maximum idle time in seconds before a job is garbage collected.
<code>information-services.dat.max-field-size</code>	Maximum size (in Megabytes) for a data cell.
<code>information-services.dat.max-jobs</code>	Maximum number of concurrent jobs.
<code>information-services.dat.max-timeout</code>	Maximum value of timeout parameters; must be at least 60 seconds less than the idle limit.
<code>information-services.dat.pivot.thread-pool-size</code>	Maximum number of pivot worker threads.
<code>information-services.dat.reshape.max-memory-usage</code>	Maximum memory available to a reshape operation.
<code>information-services.dat.retrieve-timeout</code>	Maximum time allowed for retrieve requests, in seconds.
<code>information-services.dat.thread-pool-size</code>	Maximum number of job worker threads.
<code>information-services.ds.credentials-cache-timeout</code>	The default expiration time in seconds for cached data source authentication credentials.
<code>information-services.ds.credentials-provider</code>	The class used to provide credentials for data sources that require authentication.
<code>information-services.jdbc.connection-login-timeout</code>	Login timeout for JDBC database connections.
<code>information-services.jdbc.oracle.temp-table-grantee</code>	Selecting privileges on temporary tables used during query execution will be granted to this user or role. The temporary tables are only valid during the query transaction.
<code>information-services.jdbc.use-inner-select-in-clause</code>	<p>This setting affects the behavior when the number of filter values sent to a jdbc data source exceeds the condition-list-threshold.</p> <p>If set to false (default): all data rows matching any duplicate filter values will be duplicated,</p> <p>If set to true: data rows matching any duplicates will not be duplicated (the same behavior as when the number of filter values is below the condition-list-threshold limit), but there is a large performance penalty.</p>

Default join database

The default join database is used for creating temporary tables and joining the final result when running an information link.

Most often using the standard Spotfire database for the default join database will work fine. However, in certain situations you may want to configure another database to be used. For example, if you prefer to run these operations as a specific user on the database, or if you want to use a database that is specifically optimized for temporary tables.

To set up a default join database use the command [create-join-db](#).

Default join database settings

Option	Description
Type	Sets the type of database and driver you want to use as the default join database. Refers to a data source template.
Connection URL	The connection URL to the database.
Number of Connections	A minimum and maximum number of connections to use when accessing the database.
Username and Password	The username and password that will be used to access the database.

Spotfire Server public Web Services API's

It is possible to build specific functionality that can call Spotfire Server through a set of public Web Services API's.

These can be accessed at:

- [http\[s\]://<tss_host>\[:<port>\]/spotfire/ws/pub/LibraryService](http[s]://<tss_host>[:<port>]/spotfire/ws/pub/LibraryService)
- [http\[s\]://<tss_host>\[:<port>\]/spotfire/ws/pub/SecurityService](http[s]://<tss_host>[:<port>]/spotfire/ws/pub/SecurityService)
- [http\[s\]://<tss_host>\[:<port>\]/spotfire/ws/pub/UserDirectoryService](http[s]://<tss_host>[:<port>]/spotfire/ws/pub/UserDirectoryService)

A description of each web service (a WSDL file) can be retrieved by appending ?wsdl to each web service URL. The WSDL files can be used to generate client proxies which will contain all types and methods that may be used. The implementing classes may not be called directly from Java code.



All user accounts that are going to use the API must be members of the **API User** group.

For more information on the Web Services API, see the Web Services API reference on <https://docs.tibco.com/products/tibco-spotfire-server>.

Enabling the Web Services API

Before the Web Services API can be used, it must be enabled.

To do this, export the server configuration from the database, run the [config-web-service-api](#) command, and import the updated configuration to the database. (For details on using the Spotfire command line, see [Executing commands on the command line](#).)

Procedure

- On the command line, go to the <server installation folder>\tomcat\bin directory, and run the following commands:
 1. `config export-config --force`
 2. `config config-web-service-api --enabled=true`
 3. `config import-config -c "Enabled the public Web Service API"`

Generating client proxies

Proxies can be generated using a tool of your choice.

Here is an example on how to do it using the `wsimport` tool that is included with the Oracle JDK 8.

Procedure

1. Create an authentication file containing the URL of each web service, including a valid user name and password of a user that is a member of the API User group.

Examples of authentication files:

- `http://user:password@tss.example.com:8080/spotfire/ws/pub/LibraryService?wsdl`
- `http://user:password@tss.example.com:8080/spotfire/ws/pub/SecurityService?wsdl`
- `http://user:password@tss.example.com:8080/spotfire/ws/pub/UserDirectoryService?wsdl`

2. Generate the proxies by running `wsimport` for each web service (specifying the authentication file created in the previous step).

Examples on how to generate the proxies, using the authentication files above:

- `wsimport -d bin -s src -Xauthfile auth.txt http://tss.example.com:8080/spotfire/ws/pub/LibraryService?wsdl`
- `wsimport -d bin -s src -Xauthfile auth.txt http://tss.example.com:8080/spotfire/ws/pub/SecurityService?wsdl`
- `wsimport -d bin -s src -Xauthfile auth.txt http://tss.example.com:8080/spotfire/ws/pub/UserDirectoryService?wsdl`

Optional security HTTP headers

The Spotfire Server can be configured to include some extra security-oriented HTTP headers in its responses.

These headers are optional and the only one included by default is the `X-Content-Type-Options` header. Make sure to only enable them if you know exactly how they work and what effects they have.

- [X-Frame-Options](#)
- [X-XSS-Protection](#)
- [Strict-Transport-Security](#)
- [Cache-Control](#)
- [X-Content-Type-Options](#)

X-Frame-Options

The X-Frame-Options HTTP header provides basic protection against some clickjacking attacks (also known as UI redress attacks).

The feature can be switched on by running the following commands in the `<server installation directory>\tomcat\bin` directory on the command line. (For details on using the Spotfire command line, see [Executing commands on the command line](#).)

```
config export-config --force
config set-config-prop -n security.x-frame-options.enabled -v true
config import-config -c "Enabled X-Frame-Options"
```

The feature can be switched off by running the following commands:

```
config export-config --force
config set-config-prop -n security.x-frame-options.enabled -v false
config import-config -c "Disabled X-Frame-Options"
```

When this feature is enabled, the server includes the HTTP header "X-Frame-Options: SAMEORIGIN" in all responses.

The directive can also be customized by running the following commands:

```
config export-config --force
config set-config-prop -n security.x-frame-options.directive -v <value>
config import-config -c "Customized X-Frame-Options directive"
```

<value> can be set to any of the following values:

- DENY: Prevents the rendering of the server web page within a frame.
- SAMEORIGIN: Prevents the rendering of the server web page within a frame if origin mismatch.
- ALLOW-FROM: The server web page will be rendered only when framed from the specified location.
- ALLOWALL: Allows rendering within a frame from any location. (This is a non-standard value which is not supported by all browsers.)

X-XSS-Protection

The X-XSS-Protection HTTP header provides basic protection against some XSS attacks by indicating to the browser clients how they should use their built-in XSS protection filter.



This functionality is enabled by default for new Spotfire Server installations, and for installations upgraded from 7.5 or later, but not for installations upgraded from versions that are earlier than 7.5.

The feature can be switched on by running the following commands in the `server installation dir\tomcat\bin` directory on the command line. (For details on using the Spotfire command line, see [Executing commands on the command line](#).)

```
config export-config --force
config set-config-prop -n security.x-xss-protection.enabled -v true
config import-config -c "Enabled X-XSS-Protection"
```

The feature can be switched off by running the following commands:

```
config export-config --force
config set-config-prop -n security.x-xss-protection.enabled -v false
config import-config -c "Disabled X-XSS-Protection"
```

When this feature is enabled, the server will include the HTTP header "X-XSS-Protection: 1; mode=block" in all responses.

The directive can also be customized by running the following commands:

```
config export-config --force
config set-config-prop -n security.x-xss-protection.directive -v value
config import-config -c "Customized X-XSS-Protection directive"
```

<value> can be set to any of the following values:

- "0"
- "1"
- "1; mode=block"

Make sure to put quotation marks around the last argument on the command line.

HTTP Strict-Transport-Security (HSTS)

The Strict-Transport-Security HTTP header provides support for the HTTP Strict Transport Security (HSTS) standard, as specified by RFC 6797.

It helps to protect against protocol downgrade attacks and cookie hijacking by declaring that user agents, such as web browsers or Spotfire Analyst clients, must interact with the Spotfire Server using secure HTTPS connections.

The feature can be switched on by running the following commands in the <server installation directory>\tomcat\bin directory on the command line. (For details on using the Spotfire command line, see [Executing commands on the command line](#).)

```
config export-config --force
config set-config-prop -n security.hsts.enabled -v true
config import-config -c "Enabled HSTS"
```

The feature can be switched off by running the following commands:

```
config export-config --force
config set-config-prop -n security.hsts.enabled -v false
config import-config -c "Disabled HSTS"
```

When this feature is enabled, the server will include the HTTP header "Strict-Transport-Security: max-age=0" in all responses.

Use the following commands to customize the max-age directive:

```
config export-config --force
config set-config-prop -n security.hsts.max-age-seconds -v <value>
config import-config -c "Customized HSTS max-age directive"
```

<value> can be any positive integer value, representing the number of seconds the HSTS policy should remain in effect.

The includeSubDomains directive is by default not included in the HTTP header, but it can be enabled by running the following commands:

```
config export-config --force
config set-config-prop -n security.hsts.include-sub-domains -v true
config import-config -c "Enabled includeSubDomains directive for HSTS"
```

The includeSubDomains directive can be excluded from the HTTP header by running the following commands:

```
config export-config --force
config set-config-prop -n security.hsts.include-sub-domains -v false
config import-config -c "Disabled includeSubDomains directive for HSTS"
```

Cache-Control

The Cache-Control header controls how the browser caches web resources. To make sure that no sensitive files are ever stored on the file system, enable the Cache-Control header to prevent the files from being cached by the browser.

The feature can be switched on by running the following commands in the <server installation directory>\tomcat\bin directory on the command line. (For details on using the Spotfire command line, see [Executing commands on the command line](#).)

```
config export-config --force
config set-config-prop -n security.cache-control.enabled -v true
config import-config -c "Enabled Cache-Control"
```

The feature can be switched off by running the following commands:

```
config export-config --force
config set-config-prop -n security.cache-control.enabled -v false
config import-config -c "Disabled Cache-Control"
```

When this feature is enabled, the server will include the HTTP header "Cache-Control: no-cache, no-store, must-revalidate" in all responses.

Use the following commands to customize the header directive:

```
config export-config --force
config set-config-prop -n security.cache-control.directive -v <value>
config import-config -c "Customized Cache-Control directive"
```

Replace <value> with any valid cache-control header directive.



You cannot customize the Cache-Control header for files ending with ".html" or attachments with content type "text/html" or "text/plain". These files will always have the value "no-cache, no-store, must-revalidate". They will also get the "Pragma" header set to "no-cache" and the "Expires" header set to "0". The Pragma headers are legacy HTTP 1.0 headers and serve the same purpose as the "Cache-Control" header in HTTP 1.1.

X-Content-Type-Options

The X-Content-Type-Options HTTP header can be used to prevent user agents, such as web browsers or Spotfire Analyst clients, from guessing the MIME content type. Instead, they will always use the declared content type.

The X-Content-Type-Options header is enabled by default.

The feature can be switched off by running the following commands in the <server installation directory>\tomcat\bin directory on the command line:

```
config export-config --force
config set-config-prop -n security.x-content-type-options.enabled -v false
config import-config -c "Disabled X-Content-Type-Options"
```

If switched off, the feature can be switched on again by running the following commands:

```
config export-config --force
config set-config-prop -n security.x-content-type-options.enabled -v true
config import-config -c "Enabled X-Content-Type-Options"
```

For details on using the Spotfire command line, See [Executing commands on the command line](#).

Changing how long the server waits before assuming that a node manager is offline

You can configure the amount of time that Spotfire Server waits for a node manager to signal its presence. If the node manager does not send a signal within the configured time period, the server assumes that the node is offline. For setups that are experiencing a heavy load, you can raise this value to avoid unnecessarily restarting a node manager.

The default value for this property is 12,000 milliseconds (12 seconds).

Procedure

1. Open a command line and export the active server configuration by using the [export-config](#) command; for additional information, see [Executing commands on the command line](#).

2. On the command line, enter the following command:

```
config set-config-prop --name=nodemanager.heartbeat.threshold --value=X
```

where X is the length of time, in milliseconds, that the server will wait for the node manager signal.

3. Import the configuration back to the Spotfire database by using the [import-config](#) command.
4. Restart the Spotfire Server service.

Setting the maximum execution time for an Automation Services job

This Spotfire Server property indicates how long an Automation Services job can run before the server cancels the job. The default setting for this property is 259,200 seconds (72 hours).

Procedure

1. Open a command-line interface and export the active configuration (the `configuration.xml` file) by using the [export-config](#) command.
2. Enter the following command:

```
config set-config-prop --name="automation-services.max-job-execution-time" --value="X"
```

 where "X" is the length of time, in seconds, that an Automation Services job is permitted to run.
3. Import the configuration file back to the Spotfire database by using the [import-config](#) command.
4. Restart Spotfire Server.

Setting the maximum inactivity time for an Automation Services job

This Spotfire Server property indicates how long an Automation Services job can remain inactive before the server cancels the job. The default setting for this property is 259,200 seconds (72 hours).

Procedure

1. Open a command-line interface and export the active configuration (the `configuration.xml` file) by using the [export-config](#) command.
2. Enter the following command:

```
config set-config-prop --name="automation-services.job-inactivity-timeout" --value="X"
```

 where "X" is the time period, in seconds, after which the server will cancel an inactive Automation Services job.
3. Import the configuration file back to the Spotfire database by using the [import-config](#) command.
4. Restart Spotfire Server.

Absolute session timeout and idle session timeout

Absolute session timeout is a recommended security feature, while idle session timeout is mainly a resource management feature.

Absolute session timeout requires all Spotfire users to log in to the program again after the configured amount of time. This is true whether a user has been working in Spotfire the entire time, has left the computer unattended, or has shut the computer down. The data associated with the session remains available to the user so that they can log back in (on the same computer or a different computer) and continue working. The absolute session timeout default is 1,440 minutes (24 hours).

However, because open user sessions tie up system resources that could be used elsewhere, the *idle session timeout* begins its countdown when a user shuts down their computer or the computer is no longer connected to the Spotfire network. If the user does not reactivate their session before the idle session timeout has been reached, the data associated with the session is destroyed and the session's resources become available for other sessions. The idle session timeout default is 30 minutes.



The session is not considered "idle" until the computer shuts down or disconnects from the network because Spotfire Web Player, like many other applications, makes periodic background requests to the server.

Because the login page makes no background requests, when an absolute session timeout occurs, the session data is eventually destroyed when the idle session timeout is reached. This assumes that the user is not immediately logged back in again because they previously selected the **Keep me logged in** check box.

Both idle session timeout and absolute session timeout are set in the `configuration.xml` file. Therefore, in a clustered implementation the setting applies to all the resources in the cluster.

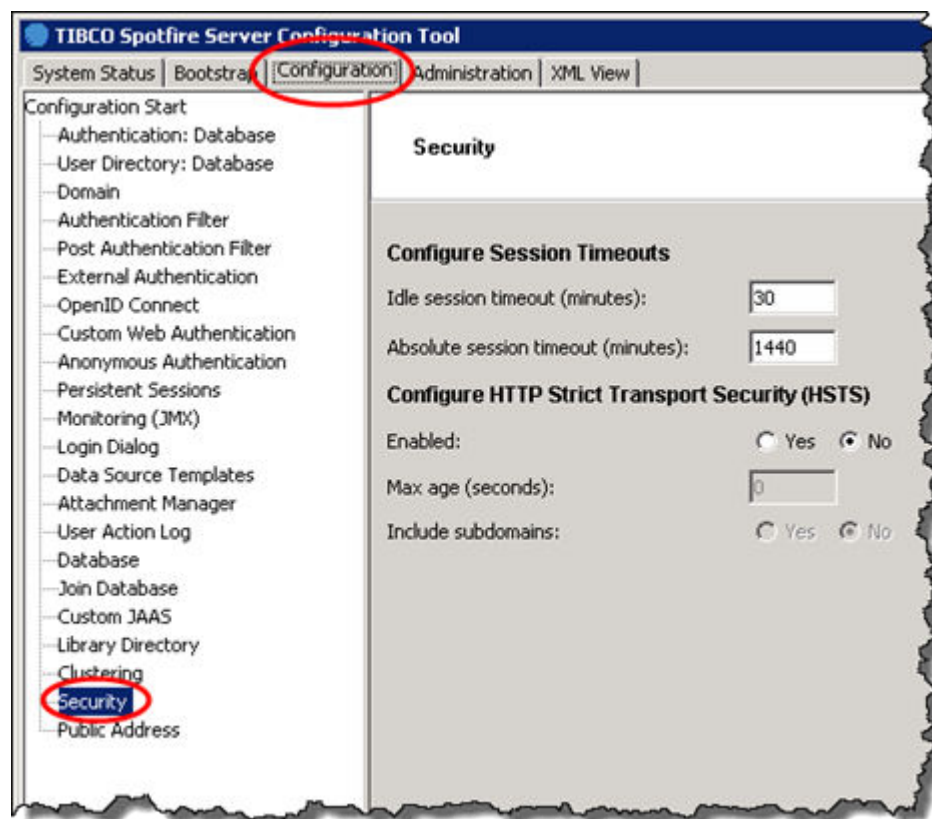
These timeout properties can be configured either in the Spotfire configuration tool or on the command line.

Setting idle session timeout and absolute session timeout by using the configuration tool

Both session timeout values can be adjusted in the **Security** section of the Spotfire configuration tool.

Procedure

1. If the configuration tool is not open, open it; for instructions see [Opening the configuration tool](#).
2. On the Configuration page, at the bottom of the left pane, click **Security**.



3. Under **Configure Session Timeouts** you can change the number of minutes for the idle session timeout and absolute session timeout.
4. Click **Save configuration**.
5. Restart the Spotfire Server.

Setting idle session timeout by using the command line

The primary function of the idle session timeout is to release the resources that are associated with a user session when the computer is inactive for the configured amount of time. The default is 30 minutes.

Procedure

1. Open a command-line interface and export the active configuration (the `configuration.xml` file) by using the `export-config` command. (For details on using the Spotfire command line, see [Executing commands on the command line](#).)
2. On the command line, enter the following command:

```
config set-config-prop -n security.idle-session-timeout -v XX
```

where XX is the number of minutes after which an idle user session will be closed.



A negative value for XX indicates that the idle session timeout value that is configured for the container (in the `web.xml` file) will be used. A value of 0 indicates that a user session will never be closed based solely on its inactivity.

3. Import the configuration file back to the Spotfire database by using the `import-config` command.
4. Restart the Spotfire Server.

Setting absolute session timeout by using the command line

The absolute session timeout indicates the number of minutes after which a user must log in to Spotfire again. The default is 1,440 minutes (24 hours).

Procedure

1. Open a command-line interface and export the active configuration (the `configuration.xml` file) by using the `export-config` command. (For details on using the Spotfire command line, see [Executing commands on the command line](#).)
2. On the command line, enter the following command:

```
config set-config-prop -n security.absolute-session-timeout -v XX
```

where XX is the number of minutes after which a user must log in again.

3. Import the configuration file back to the Spotfire database by using the `import-config` command.
4. Restart the Spotfire Server.

Changing whether scheduled updates are sent to exhausted service instances

By default, if all the Web Player instances in an implementation or a site are listed as "exhausted", scheduled update requests for analyses that are not cached will not be sent to a Web Player instance until one becomes available (no longer exhausted). In the same situation, a scheduled update request for an analysis that is already cached *will* be sent to exhausted instances. You can change these defaults by editing the Spotfire Server configuration file.

Procedure

1. On the server computer, export and open the `configuration.xml` file. For detailed instructions on working with this file, see [Manually editing the Spotfire Server configuration file](#).
2. In the `configuration.xml` file, locate the following section:

```
<scheduled-updates>
  ...
```

```

<performance>
  <load-on-exhausted-instances>false</load-on-exhausted-instances>
  <update-exhausted-instances>true</update-exhausted-instances>
</performance>
...
</scheduled-updates>

```

3. To allow scheduled update analyses that are not cached to use exhausted Web Player instances, change the `load-on-exhausted-instances` value to "true".
4. To prevent scheduled update analyses that are cached from using exhausted Web Player instances, change the `update-exhausted-instances` value to "false".



When a Web Player instance becomes available, the scheduled update is applied only if the rule is still scheduled at that time.

5. Save and close the file.
6. Import the file back to the Spotfire database.
7. Restart the server.

Preventing users from opening scheduled update files outside of their schedule window

Large analysis files are often managed by scheduled updates so that end users can view these files without waiting for them to download. If an end user tries to open one of these scheduled update files outside of its schedule window, however, the file can take a long time to open and may significantly tie up system resources. You can configure the server to block end-user access to these files when the files are not scheduled.



This configuration applies to all scheduled update files. It has no effect on files that are not managed by scheduled updates.

Procedure

1. Open a command-line interface and export the active configuration by using the [export-config](#) command. (For details on using the Spotfire command line, see [Executing commands on the command line](#).)
2. On the command line, enter the following command:

```
config set-config-prop --name=scheduled-updates.performance.deny-open-when-not-scheduled --value=true
```

For information about the command options, see [set-config-prop](#).

3. Import the configuration file back to the Spotfire database by using the [import-config](#) command.
4. Restart the Spotfire Server.

Changing whether recovered rules are automatically enabled

When an analysis file is deleted from the library, any scheduled update or routing rule for that file fails. If the analysis file is then imported back to its previous location, the rule is recovered but it does not run because the rule is, by default, in the "disabled" state. You can switch the default for these recovered rules to "enabled".

Procedure

1. Open a command-line interface and export the active configuration by using the [export-config](#) command. (For details on using the Spotfire command line, see [Executing commands on the command line](#).)

2. On the command line, enter the following command:

```
config set-config-prop --name=scheduled-updates.enable-recovered-rules-automatically --value=true
```

For information about the command options, see [set-config-prop](#).

3. Import the configuration file back to the Spotfire database by using the [import-config](#) command.
4. Restart the Spotfire Server.

Restarting a node manager to terminate its running jobs

Use this procedure to "refresh" a node when its service instances appear to be running jobs that should have terminated.

Procedure

1. Log on with administrator credentials to the computer on which the node manager was installed.
2. Open the Windows Services list and stop the "TIBCO Spotfire Node Manager" service.
3. Open Windows Task Manager and end all the "Spotfire.Dxp.Worker.Host.exe" processes.
4. Restart the "TIBCO Spotfire Node Manager" service.

Increase the number of available sockets on Linux

The Spotfire Server will open many connections, and each will require a file descriptor. For performance and security reasons Linux has a cap on how many connections that can be opened by a process per default. This limit might need to be increased.

To change this limit, edit the `/etc/security/limits.conf` file as root and make the following changes or add the following lines, respectively:

```
spotuser soft nofile 8192
spotuser hard nofile 65000
```

Where `spotuser` is the account that is running the Spotfire Server.

In this example, 8192 files (which includes sockets) can be opened. The setting should be high enough for the system, but not too high. To test the limit without editing the file one can run, for example

```
ulimit -n 32000
```

With a value up to the hard limit to see what the suitable limit is.

The hard limit might be increased if needed but not to more than is given by `/proc/sys/fs/file-max`.

Switching from online to offline administration help

By default, the help button on the administration pages of Spotfire Server opens the online version of this documentation. If you are unable to use the online version, you can switch to the offline version.



Any updates to this documentation will be available at <https://docs.tibco.com/products/tibco-spotfire-server>.

Procedure

1. On the computer running Spotfire Server, open a command-line interface and go to the following directory: `<server installation dir>/tomcat/bin`.
2. On the command line, enter the following commands:

```
config export-config --force
```

```
config set-config-prop -n general.applications.admin.use-online-help -v false
```

```
config import-config -c "Switching to offline administration help"
```

3. Restart the Spotfire Server.

Displaying or hiding the Spotfire Server version

You can configure which users should be able to see information on the Spotfire Server version.

Default mode

By default, information about the Spotfire Server version is present in the About view and in the URL of the online help resources. This information is available to all logged in users. If anonymous authentication is enabled, the information is also available to anonymous users. Users who have not logged in cannot access the version information.

To activate the **default** mode, run the following commands in the <server installation directory> \tomcat\bin directory on the command line:

```
config export-config --force
config set-config-prop -n security.version-settings-mode -v default
config import-config -c "Setting the version settings mode to default"
```

Safe mode

To hide this version information from anonymous users, so that the version information is only available to logged in users, it is possible to activate a **safe** mode.

To active the **safe** mode, run the following commands in the <server installation directory> \tomcat\bin directory on the command line:

```
config export-config --force
config set-config-prop -n security.version-settings-mode -v safe
config import-config -c "Setting the version settings mode to safe"
```

Unsafe mode

To make the version information available to everyone, including anonymous users as well as users who have not logged in, it is possible to active an **unsafe** mode.

To active the **unsafe** mode, run the following commands in the <server installation directory> \tomcat\bin directory on the command line:

```
config export-config --force
config set-config-prop -n security.version-settings-mode -v unsafe
config import-config -c "Setting the version settings mode to unsafe"
```



This configuration setting does not affect the web client. See the showAbout and showHelp settings in the [Spotfire.Dxp.Worker.Web.config](#) configuration file for information on how to disable these features in the web client.

Contacting support

If you encounter an issue that requires assistance from TIBCO Support, consider including the following information (where applicable to your specific issue) when reporting the issue, to help ensure a quick resolution.

- Describe the issue in detail, including any error messages.
- List all products/components and exact versions involved in the issue.
- When was the issue first observed? Has it ever worked in the past? How often does it occur?
- Were any changes made in the environment (on the Spotfire side or externally, such as changes to the operating system/web browser/database/anti-virus software, and so on) around the time that the issue started?
- Are the steps needed to reproduce/trigger the issue known? If so, describe them and, if possible, provide any objects (such as analysis files) that are needed to reproduce it.
- Is the extent of the issue known? For example, does it only affect one/some objects (such as specific servers/analysis files/users), while others work? If so, list any objects that are affected, and also state if there are any known differences between those that work and those that do not.
- Provide logs from the time of the issue. (It is always strongly recommended to submit all available logs). A convenient way to gather the server-side logs is by generating a troubleshooting bundle. For more information, see [Troubleshooting bundle](#).



If you have a way to reproduce the issue, it is recommended to set the logging level to DEBUG (for more information, see [Changing server and node logging levels](#)), reproduce the issue, and then provide the captured logs. Remember to reset the logging level after you are done.

After you have gathered the information, submit your issue to TIBCO Support using the TIBCO Customer Support Portal at <https://support.tibco.com>.

Reference

Spotfire Server files

These files contain configuration information for the server.

For information about the `configuration.xml` file, see [Configuration.xml file](#).

For information about the service configuration files, see [Service configuration files](#).

Bootstrap.xml file

The bootstrap configuration file contains the basic information that Spotfire Server requires to bootstrap itself so that it can connect to the Spotfire database and retrieve its configuration.

The bootstrap configuration file is created by running the [bootstrap](#) command (or using the configuration tool). The file must be created in the `<installation_dir>\tomcat\webapps\spotfire\WEB-INF` directory (Windows) or the `<installation_dir>/tomcat/webapps/spotfire/WEB-INF` directory (Unix). When specifying an alternative bootstrap configuration file path to the bootstrap command, the generated file must be manually copied to this directory before it can be accessed by the server. The file must also be named `bootstrap.xml`.

This is the format of the bootstrap configuration file:

```
<bootstrap>
  <server-name>...</server-name>
  <server>
    <driver-class>...</driver-class>
    <database-url>...</database-url>
    <username>...</username>
    <password>...</password>
  </server>
  <config-tool>
    <driver-class>...</driver-class>
    <database-url>...</database-url>
    <username>...</username>
    <password>...</password>
  </config-tool>
  <server-name>...</server-name>
  <encryption-password>...</encryption-password>
</bootstrap>
```

- The `<config-tool>` section

This section is optional and not required for running the server itself. It is only required for using the configuration commands to access the database. If the commands are not to be used on a specific server, they can easily be disabled by removing this section.

The database password stored in this section is protected by a special configuration tool password that is specified when creating the `bootstrap.xml` file. This tool password must be specified whenever running a command that accesses the database.



The tool password is not related to any administrator user account within the server application itself.

- The `<server-name>` section

This section contains the server name, which is used for identifying the server, for example when specifying server-specific configuration.

- The `<encryption-password>` section

This section is optional. If specified, it contains a password to be used for encrypting other passwords that are stored in the database. If not set, a static password is used.



The same password must be configured for all servers in a cluster.

Server.xml file

Spotfire Server is implemented as a Tomcat web application. For this reason, it uses a standard Tomcat web application configuration file, `server.xml`, to store information it needs when starting. This file is stored in the `<installation_dir>/tomcat/conf/` directory.

In general, there are two reasons that an administrator might edit this file:

- To change port numbers after installation.
- To tweak Tomcat behavior.

Note that each Spotfire Server in a cluster has a `server.xml` file.



The variable `[SpotfirePort]` is set when running the Spotfire Server installer. The variable `[ServerHostname]-srv` is automatically set by the installer by adding the strings `-srv` to the server's hostname. This variable must not contain any characters that need escaping, such as `"`.

For details about the `server.xml` syntax, see Apache Tomcat documentation at <http://tomcat.apache.org/>.

Server hostname example

`spotfireserver1.example.com`



By default Spotfire Server has three pre-configured connectors. Connectors with `connectorType="registration"` and `connectorType="backend"` should not be touched. The public connector (it has no `connectorType` specified explicitly) can be modified or commented out for load balancing and other purposes.

Krb5.conf file

The `krb5.conf` file contains settings for Kerberos. The unmodified version of the file is presented first, followed by a version with example values.

This is the unmodified file:

```
[libdefaults]
    default_realm = MYDOMAIN
    default_keytab_name = spotfire.keytab
    default_tkt_enctypes = aes128-cts rc4-hmac
    default_tgs_enctypes = aes128-cts rc4-hmac
    forwardable = true

[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
```

This is the file with example values:

```
[libdefaults]
    default_realm = RESEARCH.EXAMPLE.COM
```



```

default_keytab_name = spotfire.keytab
default_tkt_enctypes = aes128-cts rc4-hmac
default_tgs_enctypes = aes128-cts rc4-hmac
forwardable = true

[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

```

Server bootstrapping and database connection pool configuration

The Spotfire database holds all user data and most of the configuration for the Spotfire system. To connect to the Spotfire database, Spotfire Server uses a database connection pool.

The `bootstrap.xml` file contains the information that the server needs to connect to the Spotfire database and retrieve the configuration; refer to [The bootstrap.xml file](#). After the server has retrieved the configuration from the database, it re-initializes its database connection pool using information from both the `bootstrap.xml` file, which is present on each server, and any database configuration set for the entire cluster, which is stored as part of the database persisted server configuration.

For the common database configuration tasks, use the commands [modify-db-config](#) and [set-db-config](#).

Database connectivity

The Spotfire Server database connection pool implementation is used for two things: connecting to the Spotfire database and connecting to JDBC compliant data sources through Information Services.

Each connection pool (either for Spotfire Server itself or for fetching data) has many parameters; the following are of general interest:

- The `driver-class` parameter contains the JDBC driver class name; see [Database drivers and database connection URLs](#).
- The `url` parameter contains the JDBC connection URL; see [Database drivers and database connection URLs](#).
- The `username` parameter contains the name of the database user to connect as, if applicable.
- The `password` parameter contains the password for the specified database user, if applicable. The password is always encrypted and must therefore be set using the [bootstrap command](#). It cannot be set manually.
- The `min-connections` parameter contains the minimum number of allocated connections.
- The `max-connections` parameter contains the maximum number of allocated connections. Depending on the pooling scheme, the total number of connections created by the server may be higher than the value of this parameter during high load, 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 as needed.
- The `pooling-scheme` parameter defines the connection pooling algorithm to be used. There are two possible connection pooling algorithms that determine the way the connection pool operates, "DYNAMIC" and "WAIT". The "WAIT" algorithm is the default.

When initialized, the connection pool creates a number of idle database connections equal to the `min-connections` parameter. When the connection pool receives a request for a database connection, it checks if the pool contains any idle connections and uses one of those, if available.

- The "DYNAMIC" pooling scheme—If there are no idle connections in the pool, it automatically creates a new database connection. There is no upper limit for how many connections a connection pool can have open at the same time.
- The "WAIT" pooling scheme—If there are no idle connections in the pool and the number of already open connections is less than the `max-connections` parameter, it creates a new database connection.

If the number of already open connections is equal to the `max-connections` parameter, it 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. In the server logs entries similar to this appear, "Timeout while waiting for database connection after 10 seconds".

Thus, in WAIT mode, the connection pool can never have more open (active or idle) connections than the value of the `max-connections` parameter. Whenever a database connection is returned, it is put in the pool of idle connections, unless it is used immediately to fulfill an already waiting request.

Idle connections in the database connection pool eventually time out if they are not used. The `connection-timeout` parameter defines how long (in seconds) a connection can remain idle in the connection pool before being closed and discarded.

Database drivers and database connection URLs


The following details and examples show how the database connection URL is constructed.

Supported databases and JDBC drivers

Database	Driver name
Oracle (DataDirect Driver)	<code>tibcosoftwareinc.jdbc.oracle.OracleDriver</code>
Oracle (Oracle JDBC Thin Driver, <code>ojdbc7.jar</code>)	<code>oracle.jdbc.OracleDriver</code>
Microsoft SQL Server (DataDirect Driver)	<code>tibcosoftwareinc.jdbc.sqlserver.SQLServerDriver</code>
Microsoft SQL Server (Microsoft JDBC Driver, <code>sqljdbc4.jar</code>)	<code>com.microsoft.sqlserver.jdbc.SQLServerDriver</code>


Database connection URL components



Component	Description
API	Specifies which API to use. This is always <code>jdbc</code> .
Database Driver	Specifies which database driver to use to connect to the database. Default <code>tibcosoftwareinc</code> , which will use the Spotfire DataDirect driver. If you have installed a different driver, you may provide this here.

Component	Description
Server Type	Specifies the type of database server. Either sqlserver or oracle.  Server Type is only applicable when using the DataDirect driver.
Hostname	Specifies the hostname of the database server.
Port	Specifies the port which the database server listens to; for example 1433.
Database name, SID, or service name	Specifies the name (MSSQL), SID (Oracle) or Service Name (Oracle) that defines your Spotfire database.
Options	Specifies further options, separated with semicolons. Only necessary if you want to set something specific for your database server, such as a named Instance in an MSSQL server. See the following examples.

Database connection URL examples

Database driver	URL structure	Examples
Oracle (DataDirect Driver)	[API]:[DBDriver]: [ServerType]://[Hostname]: [Port];SID=[SID]	jdbc:tibcosoftwareinc:oracle:// dbsrv.example.com:1521;SID=s potfire_server
Oracle (DataDirect Driver)	[API]:[DBDriver]: [ServerType]://[Hostname]: [Port];ServiceName=[Service Name]	jdbc:tibcosoftwareinc:oracle:// dbsrv.example.com:1521;Servic eName= pdborcl.example.com
Oracle (Vendor Driver, ojdbc7.jar)	[API]:[DBDriver]: [DriverType]://[Hostname]: [Port];SID	jdbc:oracle:thin:@dbsrv.exempl e.com:1521:orcl
Oracle (Vendor Driver, ojdbc7.jar)	[API]:[DBDriver]: [DriverType]://[Hostname]: [Port]/[ServiceName]	jdbc:oracle:thin:@// dbsrv.example.com:1521/ pdborcl.example.com

Database driver	URL structure	Examples
Microsoft SQL Server (DataDirect Driver)	[API];[DBDriver]: [ServerType]://[Hostname]: [Port];DatabaseName=[DBName]	<p>jdbc:tibcosoftwareinc:sqlserver:// dbsrv.example.com:1433;DatabaseName= spotfire_server</p> <p>Example using Integrated Authentication:</p> <p>jdbc:tibcosoftwareinc:sqlserver:// dbsrv.example.com:1433;DatabaseName= spotfire_server;Authentication Method=ntlm;LoadLibraryPath =c:/tibco/tss/<version>/tomcat/ lib</p> <div>  <p>Make sure that the LoadLibraryPath has the correct path to the tomcat/lib directory in Spotfire Server installation directory.</p> </div>

Database driver	URL structure	Examples
Microsoft SQL Server (Vendor Driver, sqljdbc4.jar)	[API];[DBDriver];//[Hostname]:[Port];DatabaseName=[DBName]	<p>jdbc:sqlserver://dbsrv.example.com:1433;DatabaseName=spotfire_server;selectMethod= cursor</p> <p>Example: Making sure that the driver always returns prevents infinite waits during adverse conditions</p> <p>jdbc:sqlserver://dbsrv.example.com:1433;DatabaseName=spotfire_server;lockTimeout=<X, where X is a good value></p> <div data-bbox="1098 808 1141 850"></div> <p>Due to a restriction in the vendor Microsoft SQL Server driver, you may need to add the option responseBuffering=adaptive to your connection string. This is necessary if you are going to store large analysis files in the library.</p> <p>Example: Using responseBuffering=adaptive</p> <p>jdbc:sqlserver://dbsrv.example.com:1433;databaseName=spotfire_server;selectMethod= cursor;responseBuffering=adaptive</p> <p>Example: Using Integrated Authentication</p> <p>jdbc:sqlserver://dbsrv.example.com:1433;DatabaseName=spotfire_server;selectMethod= cursor;integratedSecurity=true;</p> <div data-bbox="1098 1701 1141 1743"></div> <p>For Integrated Authentication to work, you must place the file sqljdbc_auth.dll in a folder in the system path, such as C:\Windows\System32. This file is included with the</p>

Database driver	URL structure	Examples
		vendor drivers from Microsoft.

Command-line reference

The command-line commands are listed alphabetically here.

Refer to [Configuration and administration commands by function](#) for an easily reviewed functional command grouping, and [Configuration using the command line](#) for information on using the Spotfire command line.

In this reference we use the following symbols:

- Angle brackets (< >) indicate mandatory arguments.
- Square brackets ([]) indicate optional arguments.

Arguments can normally be specified in two different formats. For example, the `max cache size` argument may be entered as `--max-cache-size=<value>` or `-m <value>`.

A negative value must be preceded by a backslash in the second argument format, for example `-m \-7`.

add-ds-template

Adds a new data source template.

```
add-ds-template
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
<-n value | --name=value>
[-e <true|false> | --enabled=<true|false>]
<template definition file>
```

Overview

Use this command to add a new data source template used by Information Services. The name of the template must be unique.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-n value</code> <code>--name=value</code>	Required	none	The name of the data source template to add.
<code>-e <true false></code> <code>--enabled=<true false></code>	Optional	false	Indicates whether the newly created data source template should be enabled.

Option	Optional or Required	Default Value	Description
<template definition file>	Required	none	The path to the file containing the data source template definition.

add-member

Adds a user or group as a member of a specified group.

```
add-member
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
<-g value | --groupname=value>
[-u value | --member-username=value]
[-m value | --member-groupname=value]
```

Overview

Use this command to add an existing user or group as a member of another existing group.

Options

Option	Optional or Required	Default Value	Description
-b value --bootstrap-config=value	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
-t value --tool-password=value	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. See Bootstrap.xml file .
-g value --groupname=value	Required	none	The name of the group to which the member should be added. Unless the group is part of the internal SPOTFIRE domain, the name of the group must include the group's domain name, for example "RESEARCH\group" or "group@research.example.com".

Option	Optional or Required	Default Value	Description
<code>-u value</code> <code>--member-username=value</code>	Required, unless the <code>--member-groupname</code> argument is specified.	none	The name of the user to add as a member of the specified group. Unless the user is part of the configured default domain, the name of the user must include the user's domain name, For example "RESEARCH\user" or "user@research.example.com". The <code>--member-username</code> and <code>--member-groupname</code> arguments are mutually exclusive.
<code>-m value</code> <code>--member-groupname=value</code>	Require, unless the <code>--member-username</code> argument is specified.	none	The name of the group to add as a member of the specified group. Unless the group is part of the internal SPOTFIRE domain, the name of the group must include the group's domain name, for example "RESEARCH\group" or "group@research.example.com". The <code>--member-username</code> and <code>--member-groupname</code> arguments are mutually exclusive.

bootstrap

This command is used to bootstrap the server by creating a new bootstrap configuration file, and a corresponding server node in the database.


To update an existing file, use the [update-bootstrap](#) command.


```
bootstrap
[-f | --force]
[-n | --no-prompt]
[-o | --force-encryption-password]
[-c value | --driver-class=value]
[-d value | --database-url=value]
[-u value | --username=value]
[-p value | --password=value]
[-k value | --kerberos-login-context=value]
{-Ckey=value}
[-E <true|false> | --enable-config-tool=<true|false>]
[-t value | --tool-password=value]
[-e value | --encryption-password=value]
[-a value | --server-alias=value]
[-S value | --site-name=value]
{-Avalue}
[bootstrap configuration file]
```

Overview

Use this command to create a new bootstrap configuration file.

Options

Option	Optional or Required	Default Value	Description
<code>-f</code> <code>--force</code>	Optional	none	Indicates that the tool should overwrite any existing bootstrap configuration file.
<code>-n</code> <code>--no-prompt</code>	Optional	none	Specifies that the tool should not prompt for missing password arguments.
<code>-o</code> <code>--force-encryption-password</code>	Optional		<p>When this flag is specified, the operation will be performed even if the encryption password specified does not match the one currently in use.</p> <div>  <p>This option should only be used to recover from a situation where the encryption password currently in use is lost and where there is no remaining <code>bootstrap.xml</code> file containing it.</p> <p>If a <code>bootstrap.xml</code> file with the current encryption password does exist, use that file together with the config-encryption command to change the encryption password before running this command.</p> </div>
<code>-c value</code> <code>--driver-class=value</code>	Optional	<code>tibcosoftwareinc.jdbc.oracle.OracleDriver</code>	The name of the JDBC driver class.
<code>-d value</code> <code>--database-url=value</code>	Optional	<code>jdbc:tibcosoftwareinc:oracle://localhost:1521;SID=orcl</code>	The JDBC URL to the database. Because this argument usually contains special characters, make sure to escape those characters or enclose the values between quotes.
<code>-u value</code> <code>--username=value</code>	Optional	none	The database account user name.

Option	Optional or Required	Default Value	Description
<code>-p value</code> <code>--password=value</code>	Optional	none	The database account password.
<code>-k value</code> <code>--kerberos-login-context=value</code>	Optional	none	<p>If you use the Kerberos protocol to log in to the database, use this argument to specify the name of the JAAS application configuration to be used for acquiring the Kerberos TGT. This JAAS application configuration must be registered with Java using a <code>login.config.url</code> parameter in the <code><TSS installation directory>\jdk\jre\lib\security\java.security</code> (Windows) or <code><TSS installation directory>/jdk/jre/lib/security/java.security</code> (Unix) file.</p> <div>  <p>The Spotfire Server <code>import-jaas-config</code> command cannot be used for this purpose because the JAAS application configurations that are imported using this command are stored in the database, which prevents Spotfire Server from using them for creating the initial connection to the database.</p> </div>
<code>-Ckey=value</code>	Optional	none	A JDBC connection property. Can be specified multiple times with different keys.
<code>-E <true false></code> <code>--enable-config-tool=<true false></code>	Optional	true	<p>If "true", the <code><config-tool></code> section should be created. Without this section, the configuration tool cannot be used on this computer. See Bootstrap.xml file.</p>

Option	Optional or Required	Default Value	Description
<code>-t value</code> <code>--tool-password=value</code>	Optional	true	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . Can be specified only if a password is given and the argument <code>--enable-config-tool</code> is set to "true".
<code>-e value</code> <code>--encryption-password=value</code>	Optional	none	The password for encrypting passwords that are stored in the database. If you do not set this option, a static password is used. Note that the same password must be configured for all servers in a cluster.
<code>-a value</code> <code>--server-alias=value</code>	Optional	The fully qualified host name as determined when this command is run, but it is only ever used as a unique identifier.	The server alias. Used for identifying the server, for example when specifying server-specific configuration.
<code>-S value</code> <code>--site-name=value</code>	Required unless there is only one site available (in which case the server will be placed in that site).	Default	The name of the site to which the server should belong. The list-sites command can be used to find names of all available sites. New sites can be created using the create-site command.
<code>-Avalue</code>	Optional	The host name(s) and IP address(es) as determined when this command is run.	The possible node backend addresses (host names and IP addresses). Used for internal communication within the Spotfire collective. The addresses will be used in the order they are provided (in cases where there is a need for ordering). This argument may be specified multiple times with different values.
<code>[bootstrap configuration file]</code>	Optional	none	The path to the bootstrap configuration file to create. See Bootstrap.xml file .

Examples

Bootstrap the server to use an Oracle database with the bundled DataDirect JDBC driver:

```
config bootstrap --driver-class=tibcosoftwareinc.jdbc.oracle.OracleDriver
--database-url="jdbc:tibcosoftwareinc:oracle://server:1521;SID=spotfire"
--username=spotuser --password=spotuser
```

Bootstrap the server to use an Oracle database with the Oracle thin JDBC driver:

```
config bootstrap --driver-class=oracle.jdbc.OracleDriver --database-url=
"jdbc:oracle:thin:@server:1521:spotfire" --username=spotuser --password=spotuser
```

Bootstrap the server to use a Microsoft SQL Server database with the bundled DataDirect JDBC driver:

```
config bootstrap --driver-class=tibcosoftwareinc.jdbc.sqlserver.SQLServerDriver
--database-url="jdbc:tibcosoftwareinc:sqlserver://
server:1433;DatabaseName=spotfire_server"
--username=spotuser --password=spotuser
```

Bootstrap the server to use a Microsoft SQL Server database with the Microsoft JDBC driver:

```
config bootstrap --driver-class=com.microsoft.sqlserver.jdbc.SQLServerDriver
--database-url="jdbc:sqlserver://server:1433;DatabaseName=spotfire_server"
--username=spotuser --password=spotuser
```

Specify multiple back-end addresses for the server:

```
config bootstrap -Ahostname.example.com -Ahostname -Aip.x.y.z
```

check-external-library

Checks for inconsistencies between external storage and the Spotfire database.

```
check-external-library
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
```

Overview

Use this command to check the consistency between what is stored in external storage (for example, Amazon S3 or a file system), and what is stored in the Spotfire database.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. See Bootstrap.xml file .

clear-join-db

Clears the default join database configuration.

```
clear-join-db
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
```

Overview

Use this command to clear the default join database configuration, which means that the Spotfire database is used as the default join database (the default behavior).

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

config-action-log-database-logger

Configures the user action database logger.

```
config-action-log-database-logger
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[--driver-class=value]
[-d value | --database-url=value]
[-u value | --username=value]
[-p value | --password=value]
[--commit-period=value]
[--wait-on-full-queue-time=value]
[--wait-on-empty-queue-time=value]
[--grace-period=value]
[--pruning-period=value]
[--queue-size=value]
[--batch-size=value]
[--thread-pool-size=value]
[--workers=value]
[--block-on-full-queue=<true|false>]
[--prioritized-categories=value]
[--monitoring-retention-span=value]
[--monitoring-average-period=value]
[--log-local-time=<true|false>]
```

Overview

Use this command to configure the user action database logger.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

Option	Optional or Required	Default Value	Description
<code>--driver-class=value</code>	Optional	none	The name of the JDBC driver class.
<code>-d value</code> <code>--database-url=value</code>	Optional	none	The JDBC URL to the database. Because this argument usually contains special characters, be sure to escape those characters or enclose the values between quotes.
<code>-u value</code> <code>--username=value</code>	Optional	none	The database account username.
<code>-p value</code> <code>--password=value</code>	Optional	none	The database account password.
<code>--commit-period=value</code>	Optional	none	The frequency (in seconds) that log events should be committed from the queue to the database when the queue is not full.
<code>--wait-on-full-queue-time=value</code>	Optional	none	The time (in milliseconds) to wait before retrying to place a new log event on the queue after being rejected by a full queue.
<code>--wait-on-empty-queue-time=value</code>	Optional	none	Sets the time (in milliseconds) to wait before trying to create a batch from the queue after an empty queue has been encountered.
<code>--grace-period=value</code>	Optional	none	The grace period for the database logger (in seconds). This is the period that the database logger is given at server shutdown to move all items from the queue to the database.
<code>--pruning-period=value</code>	Optional	48 hours	The maximum time (in hours) that logged items are kept in the database. Pruning takes place at server startup, and then at one hour intervals, when all items older than the here-specified number of hours are deleted. To disable pruning, set this argument to 0.
<code>--queue-size=value</code>	Optional	none	The maximum number of log events in the queue.
<code>--batch-size=value</code>	Optional	none	The number of log events that should be moved from the queue to the database in each batch insert.
<code>--thread-pool-size=value</code>	Optional	none	The number of threads available for the batch insert workers.

Option	Optional or Required	Default Value	Description
<code>--workers=value</code>	Optional	none	The maximum number of batch insert workers at any given time.
<code>--block-on-full-queue=<true false></code>	Optional	none	Specifies whether placing a log event on the queue should be allowed to be blocked indefinitely if the queue is full.
<code>--prioritized-categories=value</code>	Optional	none	A comma-separated list of log categories that should have higher priority in the queue.
<code>--monitoring-retention-span=value</code>	Optional	none	The length of time monitoring entries should be saved before they get crunched into averages.
<code>--monitoring-average-period=value</code>	Optional	none	The period between two averaged measurements.
<code>--log-local-time=<true false></code>	Optional	If "false", or not set, timestamps will be in UTC time.	Sets whether timestamps should be in local time or not.

config-action-logger

Configures the user action logger.

```
config-action-logger
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[--categories=value]
[--file-logging-enabled=<true|false>]
[--database-logging-enabled=<true|false>]
[--monitoring-period=value]
```

Overview

Use this command to configure the user action logger.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

Option	Optional or Required	Default Value	Description
<code>--categories=value</code>	Optional	none	A comma-separated list of the categories that should be logged by the user action logger. To enable logging for all categories, specify "all".
<code>--file-logging-enabled=<true false></code>	Optional	none	Specifies whether the user action logger should log to file.
<code>--database-logging-enabled=<true false></code>	Optional	none	Specifies whether the user action logger should log to database.
<code>--monitoring-period=value</code>	Optional	none	Specifies how often monitoring properties are reported.

config-action-log-web-service

Configures the action log web service.

```
config-action-log-web-service
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[--categories=value]
[--allowedHosts=value]
```

Overview

Use this command to configure the action log web service.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>--categories=value</code>	Optional	none	A comma-separated list of categories that should be allowed to log through the web service. To enable all categories, specify "all".
<code>--allowedHosts=value</code>	Optional	none	A regular expression that sets the hosts allowed to use the logger web service. To enable all hosts, specify <code>.*</code>

config-anonymous-auth

Configures the anonymous authentication method.

```
config-anonymous-auth
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-e <true|false> | --enabled=<true|false>]
```

Overview

Use this command to configure anonymous authentication. Anonymous authentication is always combined with another main authentication method, as configured by the [config-auth](#) command. Note that you also must enable the ANONYMOUS\guest account, using the [enable-user](#) command, for anonymous authentication to work.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-e <true false></code> <code>--enabled=<true false></code>	Optional	false	Specifies whether anonymous authentication should be enabled.

config-attachment-manager

Configures the attachment manager.

```
config-attachment-manager
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-e value | --max-cache-expiration-time=value]
[-m value | --max-cache-size=value]
[-E <true|false> | --encryption-enabled=<true|false>]
[-k value | --encryption-key-size=value]
```

Overview

Use this command to configure the attachment manager, which handles data transfer (for instance Library downloads and uploads) to and from Spotfire Server.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-e value</code> <code>--max-cache-expiration-time=value</code>	Optional	86400	The maximum idle time (in seconds) after which cache entries are evicted. Setting this parameter to a negative value disables the cache.
<code>-m value</code> <code>--max-cache-size=value</code>	Optional	10240	The maximum amount of disk space (in megabytes) used by the cache. Setting this parameter to a negative value disables the cache.
<code>-E <true false></code> <code>--encryption-enabled=<true false></code>	Optional	true	Specifies whether the encryption of temp files is enabled.
<code>-k value</code> <code>--encryption-key-size=value</code>	Optional	128	The size of the encryption key used when encrypting temp files.

config-auth

Configures authentication mode and default domain.

```
config-auth
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-a value | --auth-method=value]
[-d | --jaas-database]
[-l | --jaas-ldap]
[-w | --jaas-windows]
[-j value | --jaas-custom=value]
[-D value | --default-domain=value]
[-p <true|false> | --parse-user-and-domain-name=<true|false>]
[-s value | --site-name=value]
```

Overview

Use this command to configure the authentication mode and to set the default domain.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-a value</code> <code>--auth-method=value</code>	Optional	none	The authentication method to use. The following methods are supported: BASIC, CLIENT_CERT, NTLM, Kerberos, and External. The names can be specified in either uppercase or lowercase.
<code>-d</code> <code>--jaas-database</code>	Optional	none	Use the Spotfire database authentication source, as configured in the Spotfire-DBLogin JAAS application configuration. This option is permitted only when using the BASIC authentication method. Also, it is mutually exclusive with all other options related to BASIC authentication sources.
<code>-l</code> <code>--jaas-ldap</code>	Optional	none	Use the LDAP authentication source, as configured in the SpotfireLDAP JAAS application configuration. This option is permitted only when using the BASIC authentication method. Also, it is mutually exclusive with all other options related to BASIC authentication sources.
<code>-w</code> <code>--jaas-windows</code>	Optional	none	Use the Windows NT authentication source, as configured in the SpotfireWindows JAAS application configuration. This option is permitted only when using the BASIC authentication method. Also, it is mutually exclusive with all other options related to BASIC authentication sources.
<code>-j value</code> <code>--jaas-custom=value</code>	Optional	none	Use the custom JAAS application configuration with the specified name. This option is permitted only when using the BASIC authentication method. Also, it is mutually exclusive with all other options related to BASIC authentication sources.

Option	Optional or Required	Default Value	Description
<code>-D value</code> <code>--default-domain=value</code>	Optional	SPOTFIRE	The name of the default domain. A user belonging to the default domain need not specify domain name as part of his or her user name when logging in to the server.
<code>-p <true false></code> <code>--parse-user-and-domain-name=<true false></code>	Optional	true	Indicates whether the user name consists of both a user and a domain part that should be parsed. it is recommended that you avoid changing the default value of "true", except when you are running the user directory in database mode, and the user names are in either NetBIOS name format (domain\user) or email name format (user@domain).
<code>-s value</code> <code>--site-name=value</code>	Optional	none	The name of the site for which the configuration should be applied. Any configuration made with this flag will affect only the specified site.

config-auth-filter

Configures the authentication filter.

```
config-auth-filter
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-f value | --filter-class=value]
{-Ikey=value}
[-s <true|false> | --skip-analyst=<true|false>]
```

Overview

Use this command to configure a custom authentication filter.



The Authentication Filter API is deprecated and will be removed in a future release.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

Option	Optional or Required	Default Value	Description
<code>-f value</code> <code>--filter-class=value</code>	Optional	none	The fully-qualified name of a class implementing the javax.servlet.Filter interface.
<code>-Ikey=value</code>	Optional	none	The initialization parameters provided to the filter when the init(FilterConfig) method is called. Can be specified multiple times with different keys.
<code>-s <true false></code> <code>--skip-analyst=<true false></code>	Optional	false	Indicates whether the Spotfire Analyst client should be handled by the custom authentication filter.

Example

To set the initialization parameter 'debug' to 'true': `config -Idebug=true`

config-basic-database-auth

Configures the Spotfire database authentication source to use the BASIC authentication method.

```
config-basic-database-auth
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-p <true|false> | --parse-user-and-domain-name=<true|false>]
```

Overview

Use this command to configure the Spotfire database authentication source to use the BASIC authentication method. The configuration is stored in the SpotfireDatabase JAAS application configuration.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-p <true false></code> <code>--parse-user-and-domain-name=<true false></code>			This argument is deprecated and is ignored. Use the config-auth command to set the global configuration property.

config-basic-ldap-auth

Configures the LDAP authentication source for use with the BASIC authentication method.

```
config-basic-ldap-auth
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-l value | --ldap-configs=value]
[-w <true|false> | --enable-wildcard-domain=<true|false>]
```

Overview

Use this command to configure the LDAP authentication source to use the BASIC authentication method. The configuration is stored in the SpotfireLDAP JAAS application configuration.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-l value</code> <code>--ldap-configs=value</code>	Optional	none	A comma-separated list of LDAP configuration references. All referenced LDAP configurations must already exist. To create a new LDAP configuration, use the create-ldap-config command. When specifying more than one reference, make sure to enclose the list of references in double quotes.
<code>-w <true false></code> <code>--enable-wildcard-domain=<true false></code>	Optional	none	Indicates whether the server should attempt to authenticate the user in all domains until an authentication attempt succeeds whenever the user omits the domain name in the account name credential.

config-basic-windows-auth

Configures the Windows NT authentication source to use the BASIC authentication method.

```
config-basic-windows-auth
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-d value | --domains=value]
[-w <true|false> | --enable-wildcard-domain=<true|false>]
```

Overview

Use this command to configure the Windows NT authentication source to use the BASIC authentication method. The configuration is stored in the Spotfire Windows JAAS application configuration.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-d value</code> <code>--domains=value</code>	Optional	none	A comma-separated list of domain names. When specifying more than one domain name, make sure to enclose the list of names in quotes.
<code>-w <true false></code> <code>--enable-wildcard-domain=<true false></code>	Optional	none	Indicates whether the server should attempt to authenticate the user in all domains until an authentication attempt succeeds whenever the user omits the domain name in the account name credential.

config-client-cert-auth

Configures the CLIENT_CERT authentication method.

```
config-client-cert-auth
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
<-n value | --name-attribute=value>
[-d <true|false> | --name-attribute-contains-domain=<true|false>]
```

Overview

Use this command to configure the X.509 certificate name attribute used for the CLIENT_CERT authentication method.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

Option	Optional or Required	Default Value	Description
<code>-n value</code> <code>--name-attribute=value</code>	Required	none	<p>The name of the attribute used to extract user names from X.509 certificates.</p> <p>Supported attributes are:</p> <ul style="list-style-type: none"> Any attribute that can occur in the certificate subject's distinguished name (for instance "CN") "DN" (use the whole distinguished name) Any subject alternative name of type "rfc822Name", "dNSName", "directoryName", "uniformResourceIdentifier", "iPAddress", or "registeredID". <p>To use a subject alternative name, make sure the name attribute has the prefix "subjectAltName:". If more than one subject alternative name is present in the certificates, you can add an index prefixed with a pound sign (#).</p>
<code>d <true false></code> <code>--name-attribute-contains-domain=<true false></code>	Optional	false	Indicates whether the specified name attribute contains a fully-qualified account name, with both a user name part and a domain name part.

config-cluster

Configures clustering.


```
config-cluster
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-e <true|false> | --enabled=<true|false>]
[-t value | --type=value]
[-p value | --port=value]
[-s <true|false> | --as-secure-transport=<true|false>]
```

Overview

Use this command to configure clustering.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-e <true false></code> <code>--enabled=<true false></code>	Optional	false	Specifies whether clustering should be enabled.
<code>-t value</code> <code>--type=value</code>	Optional	HAZELCAST	Clustering type: HAZELCAST, ACTIVE_SPACES, or APACHE_IGNITE.  Apache Ignite is currently recommended only for testing purposes, not for a production environment.
<code>-p value</code> <code>--port=value</code>	Optional	5701	The new value for TCP/IP port used for clustering. Shared among all nodes in cluster.
<code>-s <true false></code> <code>--as-secure-transport=<true false></code>	Optional	none	The ActiveSpaces secure transport flag.

Example

To enable clustering in ActiveSpaces mode with a TCP/IP port of 5701:

```
config config-cluster --enabled=true --type=ACTIVE_SPACES
```

config-csrf-protection

Configures the CSRF protection.

```
config-csrf-protection
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-p <true|false> | --public-web-services=<true|false>]
[-l <true|false> | --legacy-soap=<true|false>]
```

Overview

Use this command to configure the CSRF protection. When neither the `-p/--public-web-services` argument nor the `-l/--legacy-soap` argument is provided, the command displays the current configuration.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-p <true false></code> <code>--public-web-services=<true false></code>	Optional	none	Specifies whether the CSRF protection should be enabled for the public Web Service API.
<code>-l <true false></code> <code>--legacy-soap=<true false></code>	Optional	none	Specifies whether the CSRF protection should be enabled for the legacy SOAP clients.

config-custom-web-auth

Configures custom web authentication.

```
config-custom-web-auth
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-e <true|false> | --enabled=<true|false>]
[-a value | --authenticator-class=value]
{-Ikey=value}
```

Overview

This command is used for configuring a custom web authenticator that implements a web-based authentication flow (for example, based on OAuth2).

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-e <true false></code> <code>--enabled=<true false></code>	Optional	true	Specifies whether custom web authentication should be enabled.

Option	Optional or Required	Default Value	Description
<code>-a value</code> <code>--authenticator-class=value</code>	Optional	none	The fully qualified name of a class implementing the <code>com.spotfire.server.security.CustomWebAuthenticator</code> interface.
<code>-Ikey=value</code>	Optional	none	Initialization parameters that will be provided to the custom web authenticator when the <code>init(CustomWebAuthenticatorContext)</code> method is called. If the name of the parameter ends with [SENSITIVE] it will be stored encrypted in the configuration. This argument may be specified multiple times with different keys.

Examples

To set the initialization parameter 'debug' to 'true': `-Idebug=true`

To set a sensitive parameter where the value should be stored encrypted: `-Iclient.secret[SENSITIVE]=secret123`

config-encryption

Configures the encryption of sensitive information such as service account passwords.


```
config-encryption
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-u | --update-encryption-password]
[-p value | --new-encryption-password=value]
[-n | --no-prompt]
[-f | --force]
```

Overview

Use this command to configure the encryption of sensitive information such as service account passwords, including changing the encryption password.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

Option	Optional or Required	Default Value	Description
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. See Bootstrap.xml file .
<code>-u</code> <code>--update-encryption-password</code>	Optional	none	When this flag is specified the encryption password will be updated.
<code>-p value</code> <code>--new-encryption-password=value</code>	Optional	none	The new encryption password. If no encryption password is given and the <code>--update-encryption-password</code> flag is given, then the tool will prompt for the password, unless the <code>--no-prompt</code> flag is given.
<code>-n</code> <code>--no-prompt</code>	Optional	none	When this flag is specified, the tool will not prompt for any missing password arguments.
<code>-f</code> <code>--force</code>	Optional	none	<p>When this flag is specified, the encryption configuration will be updated even if the encryption password in the given bootstrap configuration file does not match the one currently in use.</p> <div>  <p>Any previously configured secret passwords will have to be reconfigured if this option is used.</p> </div>

config-external-auth

Configures the external authentication method.

```

config-external-auth
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-e <true|false> | --enabled=<true|false>]
[-m value | --declared-auth-method=value]
[-a value | --request-attribute=value]
[-r value | --request-header=value]
[-o value | --request-cookie=value]
[-n value | --custom-authenticator-class-name=value]
[-f <true|false> | --use-authentication-filter=<true|false>]
[-x value | --expression=value]
[-d <true|false> | --downcase=<true|false>]

```

```
[ -s <true|false> | --require-tls=<true|false> ]
[ -h value | --allowed-hosts=value ]
{ -Rvalue }
{ -Ikey=value }
```


Overview

This command is used to configure external authentication, which is typically used when a reverse-proxy or similar in front of the Spotfire Server handles authentication. The authentication method can either be used as the main authentication method, as configured by the [config-auth](#) command, or as a complementary authentication method where it is combined with the main method. It is typically used as the main method when the clients only can access the server(s) through a proxy or a load-balancer. It is typically used as a complementary method when the clients can access the server(s) both directly and through a proxy or a load-balancer. To use it as a complementary method, simply configure and enable the method using this command. To use it as the main authentication method, first configure and enable the method using this command and then set it to the main method using the **config-auth** command.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-e <true false></code> <code>--enabled=<true false></code>	Optional	true	Specifies whether the external authentication method should be enabled.
<code>-m value</code> <code>--declared-auth-method=value</code>	Optional	NTLM	The authentication method that should be declared to clients when external authentication is used as the main authentication method. The following methods are supported: CLIENT_CERT, NTLM, KERBEROS, and WEB.
<code>-a value</code> <code>--request-attribute=value</code>	Optional	REMOTE_USER	The name of an HTTP request attribute containing the name of the authenticated user. The <code>--request-attribute</code> , <code>--request-header</code> , <code>--request-cookie</code> , <code>--custom-authenticator-class-name</code> , and <code>--use-authentication-filter</code> arguments are mutually exclusive.

Option	Optional or Required	Default Value	Description
<code>-r value</code> <code>--request-header=value</code>	Optional	none	The name of an HTTP header containing the name of the authenticated user. The <code>--request-attribute</code> , <code>--request-header</code> , <code>--request-cookie</code> , <code>--custom-authenticator-class-name</code> , and <code>--use-authentication-filter</code> arguments are mutually exclusive.
<code>-o value</code> <code>--request-cookie=value</code>	Optional	none	The name of an HTTP cookie containing the name of the authenticated user. The <code>--request-attribute</code> , <code>--request-header</code> , <code>--request-cookie</code> , <code>--custom-authenticator-class-name</code> , and <code>--use-authentication-filter</code> arguments are mutually exclusive.
<code>-n value</code> <code>--custom-authenticator-class-name=value</code>	Optional	none	The name of a class implementing the <code>com.spotfire.server.security.CustomAuthenticator</code> interface that should be used for authentication. Initialization parameters for the Custom Authenticator may be specified using the <code>-I</code> argument. The <code>--request-attribute</code> , <code>--request-header</code> , <code>--request-cookie</code> , <code>--custom-authenticator-class-name</code> , and <code>--use-authentication-filter</code> arguments are mutually exclusive.

Option	Optional or Required	Default Value	Description
<pre>-f <true false> --use-authentication- filter=<true false></pre>	Optional	false	<p>Specifies that the identity of the authenticated user is provided by a custom authentication filter (as the value of the <code>getUserPrincipal()</code> method of <code>javax.servlet.http.HttpServletRequest</code>).</p> <div>  <p>The Authentication Filter API is deprecated and will be removed in a future release; consider using a Custom Authenticator instead.</p> </div> <p>The <code>--request-attribute</code>, <code>--request-header</code>, <code>--request-cookie</code>, <code>--custom-authenticator-class-name</code>, and <code>--use-authentication-filter</code> arguments are mutually exclusive.</p>
<pre>-x value --expression=value</pre>	Optional	none	<p>A regular expression that can be used to filter the username extracted from the specified HTTP request attribute. The value of the regular expression's first capturing group will be used as the new username. A typical scenario is to extract the username from a composite name containing both username and domain name when using the "collapse domains" option.</p> <p>For example, the regular expression <code>"\S+\\<\S+>"</code> can be used to extract the username from a value in the format <code>"domain\username"</code>.</p> <p>Make sure to enclose the specified expression in quotes and to quote all special characters that might otherwise be consumed by the command-line shell.</p>

Option	Optional or Required	Default Value	Description
<code>-d <true false></code> <code>--downcase=<true false></code>	Optional	false	Specifies whether the username should be converted to lower case.
<code>-s <true false></code> <code>--require-tls=<true false></code>	Optional	false	Specifies whether a secure HTTPS connection is required to perform external authentication.
<code>-h value</code> <code>--allowed-hosts=value</code>	Optional	none	<p>A comma-separated list of hostnames and/or IP addresses of the client computers that are permitted to perform external authentication. If this, or at least one -R argument, is not specified, then all client computers are permitted to perform external authentication.</p> <p>Because this is a potential security risk, it is strongly recommended to restrict the permissions to use this feature. Typically, this feature is locked down so that only proxies or load balancers are permitted to use it.</p> <p>A scenario where all client computers can be allowed to use this feature is when a custom post-authentication filter is also in use. Then this filter would be responsible for performing the final authorization, for example by validating additional HTTP headers.</p>
<code>-Rvalue</code>	Optional	none	<p>A regular expression (in the syntax supported by <code>java.util.regex.Pattern</code>) that should match IP addresses of remote hosts that are permitted to perform external authentication. See also the <code>--allowed-hosts</code> argument. This argument can be specified multiple times with different values.</p>

Option	Optional or Required	Default Value	Description
<code>-Ikey=value</code>	Optional	none	<p>Specifies initialization parameters that will be provided to the Custom Authenticator when the <code>init(Map<String, String>)</code> method is called.</p> <p>This argument can only be specified together with the <code>--custom-authenticator-class-name</code> argument, and may be specified multiple times with different keys.</p> <p>Example: To set the Custom Authenticator initialization parameter "debug" to "true":</p> <pre><code>-Idebug=true</code></pre>

config-external-scheduled-updates

Configures external scheduled updates.

```
config-external-scheduled-updates
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-e <true|false> | --ems-enabled=<true|false>]
[-s value | --server-url=value]
[-u value | --username=value]
[-p value | --password=value]
[-i value | --client-id=value]
[-t value | --topic=value]
[-C value | --reconnect-attempt-count=value]
[-D value | --reconnect-attempt-delay-milliseconds=value]
[-T value | --reconnect-attempt-timeout-milliseconds=value]
[-k value | --keep-alive-minutes=value]
[-S value | --site-name=value]
```

Overview

Use this command to configure external scheduled updates via web service or TIBCO EMS.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

Option	Optional or Required	Default Value	Description
<code>-e <true false></code> <code>--ems-enabled=<true false></code>	Optional	false	The value should be "true" if updates triggered by a message sent from TIBCO Enterprise Message Service is enabled.
<code>-s value</code> <code>--server-url=value</code>	Optional, unless <code>--ems-enabled</code> is "true"	none	The URL and, if applicable, the port to the EMS server.
<code>-u value</code> <code>--username=value</code>	Optional	none	The name of the user that will be used to access the EMS server.
<code>-p value</code> <code>--password=value></code>	Optional	none	The password of the user that will be used to access the EMS server.
<code>-i value</code> <code>--client-id=value</code>	Optional, unless <code>--ems-enabled</code> is "true"	none	A unique value to identify the EMS connection. If using multiple sites, a unique value should be assigned to each site.
<code>-t value</code> <code>--topic=value</code>	Optional, unless <code>--ems-enabled</code> is "true"	none	The topic that the EMS durable subscriber should listen to.
<code>-C value</code> <code>--reconnect-attempt-count=value</code>	Optional	10	The number of reconnect attempts to be made if a connect fails.
<code>-D value</code> <code>--reconnect-attempt-delay-milliseconds=value</code>	Optional	1000	The delay for the reconnect attempts.
<code>-T value</code> <code>--reconnect-attempt-timeout-milliseconds=value</code>	Optional	1000	The timeout for the reconnect attempts.
<code>-k value</code> <code>--keep-alive-minutes=value</code>	Optional	10	If a schedule has not been set up for when a file will be pre-loaded, specify the number of minutes the file should be kept alive.

Option	Optional or Required	Default Value	Description
-S value --site-name=value	Optional	none	The name of the site for which the configuration should be applied. Any configuration made with this flag will affect only the specified site. If a site is not given, the EMS configuration will apply to all the sites.

config-import-export-directory

Configures the library import/export directory.

```
config-import-export-directory
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-p value | --path=value]
```

Overview

Use this command to configure the library import/export directory. All library import and export operations are performed from or to this directory. It can be a local directory, or it can reside on a shared disk.

Options

Option	Optional or Required	Default Value	Description
-c value --configuration=value	Optional	configuration.xml	The path to the server configuration file.
-b value --bootstrap-config=value	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
-p value --path=value	Optional	<installation directory>/tomcat/application-data/library	The path to the import/export directory.

config-jmx

Configures the JMX RMI connector.

```
config-jmx
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-e <true|false> | --enabled=<true|false>]
[-a <true|false> | --authentication-enabled=<true|false>]
[-A <true|false> | --authorization-enabled=<true|false>]
[-s <true|false> | --tls-enabled=<true|false>]
[-n <true|false> | --need-client-auth=<true|false>]
[-R value | --registry-port=value]
[-p value | --connector-port=value]
[-j value | --jaas-config=value]
```

Overview

Use this command to configure the JMX RMI connector. This connector can be used for connecting to Spotfire Server for monitoring and management purposes.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-e <true false></code> <code>--enabled=<true false></code>	Optional	false	Specifies whether the RMI connector is enabled.
<code>-a <true false></code> <code>--authentication-enabled=<true false></code>	Optional	true	Specifies whether authentication is enabled for the RMI connector.
<code>-A <true false></code> <code>--authorization-enabled=<true false></code>	Optional	true	Specifies whether authorization is enabled for the RMI connector. Authorization requires authentication to be enabled and works only with the default value of jaas-config.
<code>-s <true false></code> <code>--tls-enabled=<true false></code>	Optional	false	Specifies whether TLS is enabled for the RMI connector.
<code>-n <true false></code> <code>--need-client-auth=<true false></code>	Optional	false	Specifies whether TLS client authentication is required.
<code>-R value</code> <code>--registry-port=value</code>	Optional	1099	The port for the RMI registry.
<code>-p value</code> <code>--connector-port=value</code>	Optional	1099	The port for the RMI connector.
<code>-j value</code> <code>--jaas-config=value</code>	Optional	SpotfireJmx	The JAAS configuration entry to use for authentication. Requires authentication to be enabled. User accounts for the default authentication implementation are created by the create-jmx-user command.

config-kerberos-auth

Configures the authentication service used with the Kerberos authentication method.


```
config-kerberos-auth
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-S value | --server=value]
[-p value | --service-principal-name=value]
[-k value | --keytab-file=value]
[-d <true|false> | --enable-debug=<true|false>]
[-w value | --worker-delegation-policy=value]
```

Overview

Use this command to configure the authentication service used with Kerberos authentication method.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-S value</code> <code>--server=value</code>	Optional	none	The name of the cluster server to which the specified configuration parameters should be applied. If no name is specified, the parameters apply to all servers in the cluster.
<code>-p value</code> <code>--path=value</code>	Required	none	The Kerberos service principal name (SPN) used by the server.
<code>-k value</code> <code>--keytab-file=value</code>	Optional	<code>\${java.home}/lib/security/spotfire.keytab</code>	The path to the Kerberos file containing the keytab entry for the specified SPN. If the specified path contains any Java system properties (for example, as in the default value for this argument), they are automatically expanded.
<code>-d <true false></code> <code>--enable-debug=<true false></code>	Optional	false	Specifies whether extra debug logging should be enabled for the Kerberos authentication service.

Option	Optional or Required	Default Value	Description
<code>-w value</code> <code>--worker-delegation-policy=value</code>	Optional	none	<p>Configures how delegation of Kerberos credentials should be handled when connecting to a service on a node. When a user's credentials are delegated to a service, the service can in turn use these credentials to connect to data sources, assuming the identity of the user. Connections made without delegation can be configured to use impersonation. There are three options:</p> <ul style="list-style-type: none"> • REQUIRE - Do not connect to a service unless delegation succeeds. • TRY - Try delegation; if that fails, log in with impersonation. • NEVER - Do not attempt to delegate; always log in with impersonation. <p> By default, Spotfire Server uses the REQUIRE option.</p>

config-ldap-group-sync

Configures group synchronization for an LDAP configuration.

```
config-ldap-group-sync
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
<--id=value>
[--group-sync-enabled=<true | false>]
[--schedules=value]
[--clear-schedules]
[--group-names=value]
[--clear-group-names]
[--clear-all]
[--filter-users-by-groups=<true | false>]
[--group-search-filter=value]
[--group-name-attribute=value]
[--supports-member-of=<true | false>]
[--member-attribute=value]
[--ignore-member-groups=<true | false>]
```

Overview

Use this command to configure group synchronization for an LDAP configuration used with the User Directory LDAP provider.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>--id=value</code>	Required	none	Specifies the identifier of the LDAP configuration for which to configure group synchronization.
<code>--group-sync-enabled=<true false></code>	Optional	true	Specifies whether group synchronization is enabled for this LDAP configuration.
<code>--schedules=value</code>			This argument was deprecated from version 5.0 and replaced by the similarly-named arguments for the create-ldap-config and update-ldap-config commands because the synchronization schedules are now used for both user and group synchronization.

Option	Optional or Required	Default Value	Description
<code>--clear-schedules</code>			This argument was deprecated from version 5.0 and replaced with the similarly named argument for the update-ldap-config command because the synchronization schedules are now used for both user and group synchronization.
<code>--group-names=value</code>	Optional	none	Specifies the account names or the distinguished names (DNs) of the groups to be synchronized.
<code>--clear-group-names</code>	Optional	none	If you specify this argument, the list of group names synchronized are cleared from the LDAP configuration. This argument can be used with the <code>--group-names</code> argument to remove all old group names before adding the new.
<code>--clear-all</code>	Optional	none	<p>Clears from the LDAP configuration all group synchronization-related configuration options.</p> <p>As of Spotfire Server 5.0 and later, this option does <i>not</i> clear the LDAP synchronization schedules.</p>

Option	Optional or Required	Default Value	Description
<code>--filter-users-by-groups=<true false></code>	Optional	none	Specifies whether users should be filtered by groups, so that only users who are members of the synchronized groups are synchronized.
<code>--group-search-filter=value</code>	Optional, unless the LDAP server type is set to "Custom" using the <code>--type</code> parameter.	For Active Directory servers, the parameter value defaults to <code>objectClass=group</code> . For Sun ONE Directory Servers, it defaults to <code>&((objectclass=nsManagedRoleDefinition)(objectclass=nsNestedRoleDefinition)(objectclass=ldapSubEntry))</code> . For Sun Java System Directory Servers, it defaults to <code>objectClass=groupOfUniqueNames..</code>	Specifies an LDAP search expression filter to use when searching for groups.
<code>--group-name-attribute=value</code>	Optional, unless the LDAP server type is set to "Custom" using the <code>--type</code> parameter.	For Active Directory servers, the value defaults to <code>sAMAccountName</code> . For any version of the Sun Directory Servers with a default configuration, it defaults to <code>cn</code> .	Specifies the name of the LDAP attribute containing the group account names.
<code>--supports-member-of=<true false></code>	Optional, unless the LDAP server type is set to "Custom" using the <code>--type</code> parameter.	none	Specifies whether the LDAP servers support a <code>memberOf</code> -like attribute on the user accounts that contain the names of the groups or roles that the users are members of. In general, this is true for all Microsoft Active Directory servers and all types of Sun Directory Servers.

Option	Optional or Required	Default Value	Description
<code>--member-attribute=value</code>	Optional, unless the LDAP server type is set to "Custom" using the --type parameter.	<p>For Microsoft Active Directory servers, the parameter value defaults to memberOf.</p> <p>For Sun ONE Directory Servers, it defaults to nsRole.</p> <p>For Sun Java System Directory Server version 6.0 or later, it defaults to isMemberOf.</p> <p>To use the roles with the Sun Java System Directory Server, override the default value by setting this argument to "nsRole".</p>	<p>For all LDAP servers with support for a memberOf-like attribute, this argument specifies the name of the LDAP attribute on the user account that contains the names of the groups or roles that the user is a member of. In general, this includes all Microsoft Active Directory servers and all types of Sun Directory Servers.</p> <p>For some LDAP servers with configurations of type Custom, there is no memberOf-like attribute. In those cases, this argument specifies the LDAP attribute on the group account that contains the names of its members.</p> <p>All configurations of this type use a far less efficient group synchronization algorithm that generates more traffic to the LDAP servers because Spotfire Server first has to search for the distinguished names (DNs) of the group members within the groups, and then perform repeated look-ups to translate the member DN to the correct account name.</p>

Option	Optional or Required	Default Value	Description
<code>--ignore-member-groups=<true false></code>	Optional, unless the LDAP server type is set to "Custom" using the <code>--type</code> parameter.	For Microsoft Active Directory servers, the parameter value defaults to "false" so all inherited group memberships are correctly reflected. For any version of the Sun Directory Servers, it defaults to "true" because the role and groups mechanisms in those servers automatically include those members.	Determines whether the group synchronization mechanism should recursively traverse the synchronized groups' non-synchronized subgroups and include their members in the search result.

config-ldap-userdir

Configures the LDAP user directory mode.

```
config-ldap-userdir
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-l value | --ldap-configs=value]
[-s <true|false> | --group-sync-enabled=<true|false>]
[-t value | --sleep-time=value]
```

Overview

Use this command to configure the LDAP user directory mode. If no arguments are specified, the command displays the current configuration.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.n.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-l value</code> <code>--ldap-configs=value</code>	Optional	none	A comma-separated list of LDAP configuration references. All referenced LDAP configurations must already exist. To create a new LDAP configuration, use the create-ldap-config command. When specifying more than one reference, make sure to enclose the list of references in quotes.

Option	Optional or Required	Default Value	Description
<code>-s <true false></code> <code>--group-sync-enabled=<true false></code>	Optional	none	This argument is deprecated and is ignored. Use the config-ldap-group-sync command to enable or disable group synchronization for each LDAP configuration instead.
<code>-t value</code> <code>--sleep-time=value</code>	Optional	60	The number of minutes between each synchronization. The sleep time setting is used only for LDAP configuration entries without group synchronization schedules. If an LDAP configuration entry has a synchronization schedule defined, then this value is ignored.

config-library-external-data-storage

Configures the external library data storage.

```
config-library-external-data-storage
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
<-e <true|false> | --enabled=<true|false>>
[-s value | --external-storage=value]
[-f | --force]
```

Overview

Use this command for general configuration of the external library data storage.

When this feature is enabled, the structure of the library is stored in the Spotfire database, while the actual data of library items is stored elsewhere.

The library must be empty when you switch to or from an external data storage. The prescribed procedure for switching is to export the entire library, empty the library, change the configuration, and then import the library. Switching storage modes with items in the library causes data to be lost.

When you change the external library data storage configuration with this command, a query is made to the Spotfire database to make sure that the library is empty. This check can be overridden by using the `--force` argument.

Currently, Spotfire supports two options for external data storage: storing on the server's file system, or storing on Amazon S3. After enabling this feature, you must configure the storage using the [config-library-external-file-storage](#) command or [config-library-external-s3-storage](#) command.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .
<code>-e <true false></code> <code>--enabled=<true false>></code>	Required	none	Specifies whether external library data storage should be enabled.
<code>-s value</code> <code>--external-storage=value</code>	Optional	none	The external storage to use. The following names are valid: <code>FILE_SYSTEM</code> and <code>AMAZON_S3</code> .
<code>-f</code> <code>--force</code>	Optional	none	Indicates that the tool should change the library configuration even if the library is not empty.

config-library-external-file-storage

Configures the file system storage of library item data.

```
config-library-external-file-storage
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
<-p value | --path=value>
```

Overview

Use this command for configuring file system storage of library data.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	<code>configuration.xml</code>	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

Option	Optional or Required	Default Value	Description
<code>-p value</code> <code>--path=value</code>	Required	none	The path to the directory where library data is stored. Supply the value "DEFAULT" to use the Spotfire Server default location for storing library data on file system.

config-library-external-s3-storage

Configures the Amazon S3 storage of library item data.

```
config-library-external-s3-storage
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[--bucket-name=value]
[--access-key=value]
[--secret-key=value]
[--endpoint=value]
[--threads=value]
[--chunk-size=value]
[--threshold=value]
```

Overview

Use this command for configuring the Amazon S3 storage of library data.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration .xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>--bucket-name=value</code>	Optional	none	The Amazon S3 bucket where library data is stored.

Option	Optional or Required	Default Value	Description
<code>--access-key=value</code>	Optional	none	The access key for connecting to Amazon S3. If set to default, an instance of <code>DefaultAWSCredentialsProviderChain</code> is created. <code>DefaultAWSCredentialsProviderChain</code> can take authentication tokens from environment variables, Java system properties, by way of a config file, through the Amazon EC2 container, or through instance profile credentials delivered through the Amazon EC2 metadata service. For more information see the documentation for <code>DefaultAWSCredentialsProviderChain</code> .
<code>--secret-key=value</code>	Optional	none	The secret key for connecting to Amazon S3.
<code>--endpoint=value</code>	Optional	If not explicitly configured, the default region is used.	The Amazon S3 endpoint to connect to. For example, <code>s3.eu-central-1.amazonaws.com</code> .
<code>--threads=value</code>	Optional	none	The maximum number of threads used for uploading to Amazon S3.
<code>--chunk-size=value</code>	Optional	none	The maximum number of bytes in a chunk when the data is chunked before transfer to Amazon S3.
<code>--threshold=value</code>	Optional	none	Above this value, the number of bytes for the transferred data is split into chunks of a configurable size that are then transferred separately to Amazon S3.

config-login-dialog

Configures the client login dialog behavior.

```

config-login-dialog
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-s value | --show-login-dialog=value]
[-o <true|false> | --allow-work-offline=<true|false>]
[-d value | --offline-days-permitted=value]
[-r <true|false> | --allow-remember-me=<true|false>]
[-u <true|false> | --allow-user-provided-credentials=<true|false>]
[-R value | --rss=value]

```

Overview

Use this command to configure the behavior of the client login dialog.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-s value</code> <code>--show-login-dialog=value</code>	Optional	standard	Controls whether the log in dialog should be displayed. Valid values are: <ul style="list-style-type: none"> always: Show the dialog even if the user selected Save my login information. never: Never show the dialog. <p>Use this option only with one of the single sign-on methods: NTLM, Kerberos, or X.509 Client Certificates.</p> <ul style="list-style-type: none"> standard: Show the dialog only if the user did not select Save my login information.
<code>-o <true false></code> <code>--allow-work-offline=<true false></code>	Optional	true	Controls whether users should be allowed to work offline or if they must always log in.
<code>-d value</code> <code>--offline-days-permitted=value</code>	Optional	-1	Controls how long users can choose to work offline before they are forced to log in. Setting the value to -1 means that users are never forced to connect to Spotfire Server.
<code>-r <true false></code> <code>--allow-remember-me=<true false></code>	Optional	true	Controls whether a user can select to store the log in information for future automatic login, or if he or she must always provide username and password when logging in.

Option	Optional or Required	Default Value	Description
<code>-u <true false></code> <code>--allow-user-provided-credentials=<true false></code>	Optional	true	Controls whether users should be able to enter their own credentials in the login dialog.
<code>-R value</code> <code>--rss=value</code>	Optional	none	The URL to an RSS feed to be shown in the login dialog. The URL may be either an absolute URL or a relative URL (/spotfire/rss.xml) on the Spotfire Server. The feed must be RSS 2.0 compliant. Note that HTML in the RSS feed is not supported.

config-ntlm-auth

Configures the authentication service used with the NTLM authentication method.

```
config-ntlm-auth
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-S value | --server=value]
[-d value | --domain-name=value]
[-D value | --domain-controller=value]
[-a value | --account-name=value]
[-p value | --password=value]
[-n value | --dns-servers=value]
[-s value | --ad-site=value]
[-t value | --dns-cache-ttl=value]
[-i value | --connection-id-header-name=value]
[-L value | --log-level=value]
{-Pkey=value}
[-C value | --domain-trust-cache-values=value]
```

Overview

Use this command to configure the authentication service used with NTLM authentication method.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

Option	Optional or Required	Default Value	Description
-S value --server=value	Optional	none	The name of the cluster server to which the specified configuration parameters should be applied. If no name is specified, the parameters apply to all servers in the cluster. It is typically used to add a server-specific account name (see the --account-name option).
-d value --domain-name=value	Required, unless the --domain-controller argument is specified, or if the --server argument is specified and this parameter is already specified for the global configuration.	none	The DNS name of the Windows domain. The specified domain name automatically resolves into domain controller hostnames. It is also possible to use the --domain-controller argument to specify a domain controller hostname directly. The --domain-name and --domain-controller arguments are mutually exclusive.
-D value --domain-controller=value	Required, unless the --domain-controller argument is specified, or if the --server argument is specified and this parameter is already specified for the global configuration.	none	The DNS hostname of an Active Directory domain controller. It is also possible to use the --domain-name argument to specify a domain name that automatically resolves to domain controller hostnames. The --domain-name and --domain-controller arguments are mutually exclusive.

Option	Optional or Required	Default Value	Description
-a value --account-name=value	Optional, unless the --server argument is specified and this parameter is not already specified for the global configuration.	none	<p>Specifies the fully qualified name of the Active Directory computer account to be used by the NTLM authentication service. This account must be a proper computer account created solely for the purpose of running the NTLM authentication service. It can neither be an ordinary user account, nor an account of an existing computer. Note that the name of an Active Directory computer account always contains a dollar sign, for example, ntlm-svc \$@research.example.com. The local part of the account name (excluding the dollar sign) must not exceed 15 characters. On Linux, the parameter value must be enclosed in single quotes because of the dollar sign.</p> <p>If there is more than one server in the cluster, each server must use its own account. It is recommended to leave the global configuration without account name and password, and only add them to each server's configuration.</p>
-p value --password=value	Optional, unless the --server argument is specified and this parameter is not already specified for the global configuration.	none	<p>Specifies the password for the computer account that is to be used by the NTLM authentication service. It is recommended to leave the global configuration without account name and password, and only add them to each server's configuration.</p>
-n value --dns-servers=value	Optional	none	<p>A comma-separated list of IP addresses for the DNS servers associated with the Windows domain. When no DNS servers are specified, the NTLM authentication service falls back to the server computer default DNS server configuration.</p>

Option	Optional or Required	Default Value	Description
<code>-s value</code> <code>--ad-site=value</code>	Optional	none	The Active Directory site where the Spotfire system is located. Specifying an Active Directory site can potentially improve performance because the NTLM authentication service then communicates only with the local domain controllers.
<code>-t value</code> <code>--dns-cache-ttl=value</code>	Optional	5000 ms.	The length of time (in milliseconds) name server lookups should be cached.
<code>-i value</code> <code>--connection-id-header-name=value</code>	Optional	none	The name of an HTTP header containing unique connection IDs in environments where the server is located behind a proxy or load-balancer that does not properly provide the server with the client IP address. The specified HTTP header must contain unique connection IDs for each client connection and is thus typically based on the client IP address and the connection port number on the client side.
<code>-L value</code> <code>--log-level=value</code>	Optional	1	Specifies the level of logging done for NTLM authentication, an integer value ranging from 0 (no logging) to 4 (debug logging).
<code>-Pkey=value</code>	Optional	none	Specifies additional properties for the Jespa component, in the form of key-value-pairs. For example: <code>-Pjespa.key=value</code> . This argument may be specified multiple times with different keys.

Option	Optional or Required	Default Value	Description
-C value --domain-trust-cache-values=value	Optional	none	Specifies a mapping between NetBIOS and DNS domain names used for canonicalizing domain names when sufficient information is not provided by the local NETLOGON service. The mapping is given as a comma-separated list of NetBIOS:DNS entries, for example "RESEARCH:research.example.com, HR:hr.example.com", and is used for turning a NetBIOS name into a DNS name, or vice versa.

Examples

- Configuring the NTLM authentication service for the research.example.com Windows domain

Windows command prompt:

```
config config-ntlm-auth --domain-name research.example.com --
account-name ntlm-svc$@research.example.com --password 53cr3t
```

Linux command shell:

```
config config-ntlm-auth --domain-name research.example.com --
account-name 'ntlm-svc$@research.example.com' --password 53cr3t
```

- Configuring the NTLM authentication service for using the Active Directory Domain Controller dc.research.example.com

Windows command prompt:

```
config config-ntlm-auth --domain-controller
dc.research.example.com --account-name ntlm-svc
$@research.example.com --password 53cr3t
```

Linux command shell:

```
config config-ntlm-auth --domain-controller
dc.research.example.com --account-name 'ntlm-svc
$@research.example.com' --password 53cr3t
```

- Configuring the NTLM authentication service for the Active Directory Site VIENNA within the research.example.com Windows domain

Windows command prompt:

```
config config-ntlm-auth --domain-name research.example.com --ad-
site=VIENNA --account-name ntlm-svc$@research.example.com --
password 53cr3t
```

Linux command shell:

```
config config-ntlm-auth --domain-name research.example.com --ad-
site=VIENNA --account-name 'ntlm-svc$@research.example.com' --
password 53cr3t
```

config-oidc

Configures authentication using OpenID Connect.

```
config-oidc
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
```

```

[-e <true|false> | --enabled=<true|false>]
[-s | --set-provider]
[-r | --remove-provider]
[-n value | --provider-name=value]
[--provider-enabled=<true|false>]
[--provider-discovery-url=value]
[--provider-client-id=value]
[--provider-client-secret=value]
[--provider-domain-name=value]
[--provider-username-claim=value]
[--provider-id-token-signing-alg=value]
[--provider-id-token-signature-verification-disabled=<true|false>]
[--provider-token-endpoint-auth-method=value]
{-Svalue}
[--provider-auth-request-prompt-value=value]
[--provider-bg-color=value]

```

Overview

Use this command to configure authentication against one or more external providers using OpenID Connect. Authentication using OpenID Connect may be combined with username/password-based authentication and/or custom web authentication.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-e <true false></code> <code>--enabled=<true false></code>	Optional	true	Specifies whether OpenID Connect should be enabled.
<code>-s</code> <code>--set-provider</code>	Optional	none	Indicates that a provider configuration should be set (will replace the configuration for any existing provider with the same name). Cannot be specified together with <code>--remove-provider</code> .
<code>-r</code> <code>--remove-provider</code>	Optional	none	Indicates that a provider configuration should be removed. Cannot be specified together with <code>--set-provider</code> .

Option	Optional or Required	Default Value	Description
<code>-n value</code> <code>--provider-name=value</code>	This argument is optional unless either <code>--set-provider</code> or <code>--remove-provider</code> has been specified.	none	The name of the provider to set or remove. Normally displayed to end users on the login page.
<code>--provider-enabled=<true false></code>	This argument is optional unless <code>--set-provider</code> has been specified.	true	Specifies whether the provider should be enabled.
<code>--provider-discovery-url=value</code>	This argument is optional unless <code>--set-provider</code> has been specified.	none	The URL to the provider's OpenID Connect Discovery document.
<code>--provider-client-id=value</code>	This argument is optional unless <code>--set-provider</code> has been specified.	false	The client ID given by the provider during registration.
<code>--provider-client-secret=value</code>	This argument is optional unless <code>--set-provider</code> has been specified.	none	The client secret given by the provider during registration.
<code>--provider-domain-name=value</code>	Optional	By default the value of the 'issuer' claim is used.	The domain name to assign to the authenticated users.

Option	Optional or Required	Default Value	Description
<code>--provider-username-claim=value</code>	Optional	sub	The name of the claim to use as username for the authenticated users. May for example be 'email', but note that only 'sub' is guaranteed to be a unique and stable identifier.
<code>--provider-id-token-signing-alg=value</code>	Optional	By default all algorithms listed as supported in the Discovery Document will be accepted.	The ID token signature algorithm to expect.
<code>--provider-id-token-signature-verification-disabled=<true false></code>	Optional	false	Indicates that signature verification of ID tokens should be disabled. This should normally only be specified if the provider does not sign the ID tokens.
<code>--provider-token-endpoint-auth-method=value</code>	Optional	By default one of the algorithms listed as supported in the Discovery Document will be used.	The authentication method to use when communicating with the provider's Token Endpoint. May be one of 'client_secret_basic', 'client_secret_post' and 'client_secret_jwt' ('private_key_jwt' is not supported).
<code>-Svalue</code>	Optional	openid, profile, email	A scope to include in the authentication request (besides 'openid' that will always be included). This argument may be specified multiple times with different values.
<code>--provider-auth-request-prompt-value=value</code>	Optional	By default the parameter will be omitted from the request.	The value to give the 'prompt' request parameter when making the authentication request. Controls how the provider prompts the end user. May be one of 'none', 'login', 'consent', or 'select_account'.

Option	Optional or Required	Default Value	Description
<code>--provider-bg-color=value</code>	Optional	none	The normal background color of the provider's button on the login page (when applicable), as a hexadecimal color value.

config-persistent-sessions

Configures the persistent sessions ("remember me") feature.

```
config-persistent-sessions
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-e <true|false> | --enabled=<true|false>]
[-t value | --expiration-time=value]
[-s <true|false> | --sliding-expiration=<true|false>]
```

Overview

Use this command to configure the persistent sessions feature. Persistent sessions allows users to be remembered after a successful login. This means that the user will not have to log in again for a period of time (even if the user, for example, closes the browser).



This feature is only applicable when using username and password based authentication.



This feature is currently only applicable for users (such as Spotfire Web Player users) logging in through a web browser. To configure the behavior of the Spotfire client, use the [config-login-dialog](#) command.



Persistent sessions can be invalidated using the [invalidate-persistent-sessions](#) command.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-e <true false></code> <code>--enabled=<true false></code>	Optional	false	Specifies whether the persistent sessions feature should be enabled.
<code>-t value</code> <code>--expiration-time=value</code>	Optional	2592000	Specifies the time in seconds until a persistent session will expire and the user will have to re-authenticate.

Option	Optional or Required	Default Value	Description
<code>-s <true false></code> <code>--sliding-expiration=<true false></code>	Optional	false	Specifies whether the expiration time should be reset each time the user is authenticated using the persistent session cookie. Note that setting this to "true" means that the user may actually never have to log in again.

config-post-auth-filter

Configures the post-authentication filter.

```
config-post-auth-filter
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-f value | --filter-class=value]
[-s value | --filter-config=value]
[-d value | --default-filter-config=value]
```

Overview

Use this command to configure the post-authentication filter. If no argument is provided, the command simply lists the current configuration and exits.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-f value</code> <code>--filter-class=value</code>	Optional	none	The fully-qualified name of the class implementing the <code>com.spotfire.server.security.PostAuthenticationFilter</code> API. If the argument is none, the current value of this configuration option is cleared.
<code>-s value</code> <code>--filter-config=value</code>	Optional	none	The filter configuration. The semantics of the configuration argument is specific to the actual filter implementation. For example, it could be a configuration name, a file name, or a list of key/value pairs. If the argument is none, the current value of this configuration option is cleared.

Option	Optional or Required	Default Value	Description
<code>-d value</code> <code>--default-filter-config=value</code>	Optional	none	The configuration for the default filter that is always in place. Valid arguments are block and autocreate.

config-public-address

This command has been replaced by **set-public address**.

See [set-public-address](#).

config-scheduled-updates-retries

Configures scheduled updates retries.

```
config-scheduled-updates-retries
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-u value | --update-interval-seconds=value]
[-s <true|false> | --stop-updates-after-repeated-fail-enabled=<true|false>]
[-f value | --fails-before-stop=value]
[-o <true|false> | --stop-only-when-cached=<true|false>]
[-a <true|false> | --always-retry-when-scheduled=<true|false>]
```

Overview

Use this command to configure scheduled updates retries following update failures.



The number of retries was previously set by using the `stopUpdatesAfterRepeatedFail` setting in the `Spotfire.Dxp.Worker.Web.config` file.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-u value</code> <code>--update-interval-seconds=value</code>	Optional	60	How often the server checks whether any scheduled updates should be retried. This is set in seconds. Min value is 30, and max value 3600 (one hour).

Option	Optional or Required	Default Value	Description
<code>-s <true false></code> <code>--stop-updates-after-repeated-fail-enabled=<true false></code>	Optional	true	Set to "true" to limit the number of times the server tries to update an analysis if the update initially fails. If set to "false", the server will retry the update every <code>update-interval-seconds</code> until the analysis is successfully updated.
<code>-f value</code> <code>--fails-before-stop=value</code>	Optional	10	Specify the number of times to retry a scheduled update before stopping. Only applies if <code>stop-updates-after-repeated-fail-enabled</code> is set to "true".
<code>-o <true false></code> <code>--stop-only-when-cached=<true false></code>	Optional	false	<p>If an analysis is not cached and this option is set to "true", the server will retry the scheduled update every <code>update-interval-seconds</code> until the analysis is loaded. In this case, the <code>fails-before-stop</code> setting is ignored.</p> <p>If set to "false", the server will stop trying to update an analysis as specified in <code>fails-before-stop</code>, regardless of whether the analysis is cached.</p> <p>Only applies if <code>stop-updates-after-repeated-fail-enabled</code> is set to "true".</p>
<code>-a <true false></code> <code>--always-retry-when-scheduled=<true false></code>	Optional	true	Set to "true" to reset the counter for <code>fails-before-stop</code> and retry each time the analysis is scheduled to be updated. Only applies if <code>stop-updates-after-repeated-fail-enabled</code> is set to "true".

config-two-factor-auth

Configures two-factor authentication.

```
config-two-factor-auth
[-c value | --configuration=value]
```

```
[-b value | --bootstrap-config=value]
[-e <true|false> | --enabled=<true|false>]
```

Overview

Use this command to configure two-factor authentication. If no argument is provided, the command simply lists the current configuration and exits.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-e <true false></code> <code>--enabled=<true false></code>	Optional	none	Specifies whether or not two-factor authentication should be enabled.

config-userdir

Configures the user directory.


```
config-userdir
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-m value | --mode=value]
[-C <true|false> | --collapse-domains=<true|false>]
[-S <true|false> | --safe-synchronization=<true|false>]
[-s value | --domain-name-style=value]
[-u <true|false> | --unsafe-domain-name-style-allowed=<true|false>]
[-n value | --site-name=value]
```

Overview

Use this command to configure the user directory.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

Option	Optional or Required	Default Value	Description
<code>-m value</code> <code>--mode=value</code>	Optional	database	<p>The name of the user directory mode to use. Supported values are database, ldap, and Windows. The current value will not be changed unless the argument is explicitly specified.</p>
<code>-C value</code> <code>--collapse-domains=value</code>	Optional	false	<p>Indicates whether or not external domains should be collapsed into the internal SPOTFIRE domain, which is the domain used when running the user directory in database mode. The current value will not be changed unless the argument is explicitly specified.</p> <div>  <p>When this feature is enabled, all users will belong to the same domain. If there are multiple users with the same account name from different external domains, they will now share a single Spotfire account. Because this could pose a security problem, this feature should be used with care.</p> </div>
<code>-S <true false></code> <code>--safe-synchronization=<true false></code>	Optional	false	<p>When this option is set to "true", the user directory will not disable users that it cannot find during LDAP or Windows NT synchronization. This flag has no effect if the user directory is running in Database mode. The current value will not be changed unless the argument is explicitly specified.</p>
<code>-s value</code> <code>--domain-name-style=value</code>	Optional	dns	<p>The domain name style used by the server. Supported values are dns and netbios. The current value will not be changed unless the argument is explicitly specified.</p>

Option	Optional or Required	Default Value	Description
<code>-u <true false></code> <code>--unsafe-domain-name-style-allowed=<true false></code>	Optional	false	When this option is set to "true", the server will allow incompatible domain name style settings, instead of refusing to start. This option should be used with care; it can potentially lead to many users and groups being imported to the user directory with invalid domain names.
<code>-n value</code> <code>--site-name=value</code>	Optional	none	The name of the site for which the configuration should be applied. This flag will only have effect when used in conjunction with the <code>--mode</code> flag.

config-web-service-api

Configures the public Web Service API.

```
config-web-service-api
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-e <true|false> | --enabled=<true|false>]
```

Overview

Use this command to configure the public Web Service API. When the `-e/--enabled` argument is not provided, the command displays the current configuration.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-e <true false></code> <code>--enabled=<true false></code>	Optional	none	Specifies whether the public Web Service API should be enabled.

config-windows-userdir

Configures the Windows user directory mode.

```
config-windows-userdir
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-d value | --domains=value]
```

```
[ -t value | --sleep-time=value ]
[ --schedules=value ]
```

Overview

Use this command to configure the Windows user directory mode. If no arguments are specified, the command displays the current configuration.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-d value</code> <code>--domains=value</code>	Optional	none	A comma-separated list of domain names. When specifying more than one domain name, make sure to enclose the list of names in quotes.
<code>-t value</code> <code>--sleep-time=value</code>	Optional	60 minutes	The number of minutes between each synchronization. The <code>--sleep-time</code> and <code>--schedules</code> arguments are mutually exclusive. If neither the <code>--sleep-time</code> argument nor the <code>--schedules</code> argument is specified, the synchronization is performed with a sleep time of 60 minutes.

Option	Optional or Required	Default Value	Description
<code>--schedules=value</code>	Optional	none	<p>A comma-separated list of schedules for when the synchronization should be performed. The <code>--sleep-time</code> and <code>--schedules</code> arguments are mutually exclusive. The schedules are given in a cron-compatible format, where each schedule consists of either five fields or one shorthand label. Make sure to enclose the value in double quotes.</p> <p>The five fields are, from left to right, with their valid ranges: minute (0-59), hour (0-23), day of month (1-31), month (1-12) and day of week (0-7, where both 0 and 7 indicate Sunday). You can configure a field with the wildcard character *, indicating that any moment in time matches this field. An LDAP synchronization is triggered when all fields match the current time. If both day of month and day of week have non-wildcard values, then only one of them has to match.</p> <p>You can use the following shorthand labels instead of the full cron expressions:</p> <p><code>@yearly</code> or <code>@annually</code>: run once a year (equivalent to <code>0 0 1 1 *</code>)</p> <p><code>@monthly</code>: run once a month (equivalent to <code>0 0 1 * *</code>)</p> <p><code>@weekly</code>: run once a week (equivalent to <code>0 0 * * 0</code>)</p> <p><code>@daily</code> or <code>@midnight</code>: run once a day (equivalent to <code>0 0 * * *</code>) <code>@hourly</code>: run once an hour (equivalent to <code>0 * * * *</code>)</p> <p><code>@minutely</code>: run once a minute (equivalent to <code>* * * * *</code>)</p> <p><code>@reboot</code> or <code>@restart</code>: run every time Spotfire Server is started</p> <p>Consult the Wikipedia article for an overview of the cron scheduler: http://en.wikipedia.org/wiki/Cron.</p>

copy-group-membership

Copies group membership from one principal to another.

```
copy-group-membership
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-u value | --oldusername=value]
```

```
[-g value | --oldgroupname=value]
[-n value | --newusername=value]
[-p value | --newgroupname=value]
```

Overview

Use this command to copy the group memberships assigned to an existing user or group to another existing user or group. Only one existing principal to copy from should be given and only one principal to copy to should be given. The principal will only get memberships that it does not already have.



This will not be logged to the Action Log.



Only direct membership will be copied (that is, membership explicitly set for a certain principal and memberships that the principal inherited).

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end user for it on the console. See Bootstrap.xml file for more information.
<code>-u value</code> <code>--oldusername=value</code>	Optional	none	The name of an existing user to copy group membership from. Unless the user is part of the configured default domain, the name of the user must include the user's domain name, for example 'DOMAIN\user' or 'user@domain'.
<code>-g value</code> <code>--oldgroupname=value</code>	Optional	none	The name of an existing group to copy group membership from. Unless the group is part of the configured default domain, the name of the group must include the group's domain name, for example 'DOMAIN\group' or 'group@domain'.

Option	Optional or Required	Default Value	Description
<code>-n value</code> <code>--newusername=value</code>	Optional	none	The name of an existing user to copy group membership to. Unless the user is part of the configured default domain, the name of the user needs to include the user's domain name, for example 'DOMAIN \user' or 'user@domain'.
<code>-p value</code> <code>--newgroupname=value</code>	Optional	none	The name of an existing group to copy group membership to. Unless the group is part of the configured default domain, the name of the group needs to include the group's domain name, for example 'DOMAIN \group' or 'group@domain'.

copy-library-permissions

Copy library permissions from one principal to another.

```
copy-library-permissions
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-u value | --oldusername=value]
[-g value | --oldgroupname=value]
[-n value | --newusername=value]
[-p value | --newgroupname=value]
```

Overview

Use this command to copy library permissions from an existing user or group to another existing user or group. Only one existing principal to copy from should be given and only one principal to copy to should be given. The principal will only get permissions that it does not already have.



This will not be logged to the Action Log.



A permission entry, for example "Browse + Access", counts as two permission entries when summing up how many new permissions have been added.



Only explicit permissions will be copied (permissions explicitly set for a certain principal, and not permissions given through group membership).

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

Option	Optional or Required	Default Value	Description
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. See Bootstrap.xml file .
<code>u value</code> <code>--oldusername=value</code>	Optional	none	The name of an existing user to copy library permissions from. Unless the user is part of the configured default domain, the name of the user must include the user's domain name ('DOMAIN\user' or 'user@domain').
<code>g value</code> <code>--oldgroupname=value</code>	Optional	none	The name of an existing group to copy library permissions from. Unless the group is part of the configured default domain, the name of the group must include the group's domain name ('DOMAIN\group' or 'group@domain').
<code>n value</code> <code>--newusername=value</code>	Optional	none	The name of an existing user to copy library permissions to. Unless the user is part of the configured default domain, the name of the user must include the user's domain name ('DOMAIN\user' or 'user@domain').
<code>p value</code> <code>--newgroupname=value</code>	Optional	none	The name of an existing group to copy library permissions to. Unless the group is part of the configured default domain, the name of the group must include the group's domain name ('DOMAIN\group' or 'group@domain').

copy-rules-to-site

Copies routing rules and schedules from one site to another

```
copy-rules-to-site
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-k value | --keystore-file=value]
<-F value | --source-site-name=value>
<-T value | --target-site-name=value>
[-r value | --resource-pool-name=value]
[-u <true|false> | --use-default-resource-pool=<true|false>]
```

```
[ -d <true|false> | --disabled=<true|false> ]
[ -R value | --rule-conflict-resolution=value ]
[ -S value | --schedule-conflict-resolution=value ]
[ -e <true|false> | --test-run=<true|false> ]
```

Overview

Use this command to copy all the routing rules and schedules from the source site to the target site.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See Bootstrap.xml file help topic for more information.
<code>-k value</code> <code>--keystore-file=value</code>	Optional	none	The location of the keystore containing the certificates used for securing internal communication.
<code>-F value</code> <code>--source-site-name=value</code>	Required	none	The name of the site from which the routing rules and schedules will be copied.
<code>-T value</code> <code>--target-site-name=value</code>	Required	none	The name of the site into which the routing rules and schedules will be copied.
<code>-r value</code> <code>--resource-pool-name=value</code>	Optional	none	A resource pool name that can be used if the resource pool for a given rule is not found.
<code>-u <true false></code> <code>--use-default-resource-pool=<true false></code>	Optional	false	If enabled and the resource pool for a given rule is not found, the default resource pool will be used instead, and the instances count will be automatically reset to one instance.
<code>-d <true false></code> <code>--disabled=<true false></code>	Optional	false	If true, all the rules will be copied in a disabled state.

Option	Optional or Required	Default Value	Description
<code>-R value</code> <code>rule-conflict-resolution=value</code>	Optional	fail	Defines how to handle copying a rule if there already exists a rule with the same name and the same file/user/group in the target site. The argument can be one of: fail (default), replace, or skip.
<code>-S value</code> <code>--schedule-conflict-resolution=value</code>	Optional	rename	Defines how to handle copying a shared schedule if there already exists a shared schedule with the same name in the target site. The argument can be one of: rename (default), or replace. If the schedules are identical, the schedule in the target site will remain as it was.
<code>-e <true false></code> <code>--test-run=<true false></code>	Optional	false	If true, the copy will not actually take place, but the command will produce a preview of the import status of each rule/schedule.

create-default-config

Creates a new server configuration file containing the default configuration.

```
create-default-config
[-f | --force]
[export file]
```

Overview

Use this command to export a default server configuration to a file. The configuration in the file can be edited and then imported into the server database using the [import-config](#) command.

Options

Option	Optional or Required	Default Value	Description
<code>-f</code> <code>--force</code>	Optional	none	Indicates that the tool should overwrite an existing destination file.
<code>[export file]</code>	Optional	configuration.xml	The path to the configuration file that will be created.

create-jmx-user

Creates a new JMX user account.

```
create-jmx-user
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
<-u value | --username=value>
```

```
[-p value | --password=value]
[-l value | --access-level=value]
```

Overview

Use this command to create a new JMX user account. The account can be used only to access status information for the server through the JMX protocol. It cannot be used by users logging in to the server using a Spotfire client or an HTML browser.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .
<code>-u value</code> <code>--username=value</code>	Required	none	The name of the JMX user to create.
<code>-p value</code> <code>--password=value</code>	Optional	none	The new JMX user password.
<code>-l value</code> <code>--access-level=value</code>	Optional	r	The access level for the new user. Can be either r or rw. A user with the rw access level can read and modify any writable attributes.

create-join-db

Configures the default join database.

```
create-join-db
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
<-t value | --type=value>
<-d value | --database-url=value>
<-u value | --username=value>
[-p value | --password=value]
[-i value | --min-connections=value]
[-a value | --max-connections=value]
[-v | --validate]
```

Overview

Use this command to configure the default join database.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--type=value</code>	Required	none	The database type and the driver to use. Must match the type name of one of the enabled data source templates.
<code>-d value</code> <code>--database-url=value</code>	Required	none	The JDBC URL to the database. Because this argument usually contains special characters, be sure to escape those characters or enclose the values in quotes.
<code>-u value</code> <code>--username=value</code>	Required	none	The database account username.
<code>-p value</code> <code>--password=value</code>	Optional	none	The database account password.
<code>-i value</code> <code>--min-connections=value</code>	Optional	0	The minimum number of connections to keep in the connection pool.
<code>-a value</code> <code>--max-connections=value</code>	Optional	0	The maximum number of connections to keep in the connection pool.
<code>-v</code> <code>--validate</code>	Optional	none	Indicates whether the created configuration should be validated by attempting to connect to the database using the specified connection information.

create-ldap-config

Creates a new LDAP configuration for authentication and/or the user directory LDAP provider.

```
create-ldap-config
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
<--id=value>
[--discover]
[-t value | --type=value]
[-s value | --servers=value]
[-n value | --context-names=value]
[-u value | --username=value]
```



```

[-p value | --password=value]
[--schedules=value]
[--user-search-filter=value]
[--user-name-attribute=value]
[--authentication-attribute=value]
[--security-authentication=value]
[--referral-mode=value]
[--referral-mode-root-dse=value]
[--request-control=value]
[--page-size=value]
[--import-limit=value]
[--user-display-name-attribute=value]
[--group-display-name-attribute=value]
{-Ckey=value}
{-Rvalue}
{-Svalue}
[--connection-timeout=value]
[--read-timeout=value]

```

Overview

Use this command to create a new LDAP configuration for authentication and/or user directory back-end.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>--id=value</code>	Required	none	Specifies the identifier for the LDAP configuration to be created.
<code>--discover</code>	Optional	none	Specifies whether to attempt to automatically create an LDAP configuration based on the information available from the DNS service. The discover mode works only when the desired LDAP server has registered SRV records in the DNS service used by the computer where this command is being invoked. This is typically the case for Active Directory LDAP servers. This argument is mutually exclusive with the <code>-t/ --type</code> , <code>-s/--servers</code> , and <code>-n/--context-names</code> arguments.

Option	Optional or Required	Default Value	Description
-t value --type=value	Required, unless the --discover option is used	none	<p>The type of LDAP server. The following names are valid types:</p> <ul style="list-style-type: none"> • ActiveDirectory • SunOne • SunJavaSystem • Custom <p>If you specify any of the first three types, a type-specific configuration template is automatically applied in runtime, so that the most fundamental configuration options are automatically configured.</p> <p>If you specify a "Custom" LDAP server type, there is no such configuration template, and you must specify explicitly all the configuration options. When you use a custom LDAP configuration for authentication or with the User Directory LDAP provider, you must specify the arguments --user-search-filter and --user-name-attribute. If you use such an LDAP configuration for group synchronization, you must also specify additional parameters when running the config-ldap-group-sync command. See the help topic for that command for more information.</p>

Option	Optional or Required	Default Value	Description
-s value --servers=value	Required, unless the --discover option is used	<p>The LDAP protocol port number defaults to 389.</p> <p>The LDAPS protocol port number defaults to 636.</p> <p>Active Directory LDAP servers also provide a Global Catalog containing forest-wide information, instead of domain-wide information only. By default, the Global Catalog LDAP service listens on port number 3268 (LDAP) or 3269 (LDAPS).</p>	<p>A whitespace-separated list of LDAP server URLs. An LDAP server URL has the format <protocol>://<server>[:<port>]:</p> <ul style="list-style-type: none"> • <protocol>: Either "LDAP" or "LDAPS". • <server>: The fully qualified DNS name of the LDAP server. • <port>: Optional. Indicates the port number that the LDAP service is listening on. <p>Spotfire Server does not expect search base, scope, filter, or other additional parameters after the port number in the LDAP server URLs. Such properties are specified using other configuration options for this command.</p> <p>Examples: LDAP server URLs</p> <ul style="list-style-type: none"> • LDAP://myserver.example.com • LDAPS://myserver.example.com • LDAP://myserver.example.com:389 • LDAPS://myserver.example.com:636 • LDAP://myserver.example.com:3268 • LDAPS://myserver.example.com:3269

Option	Optional or Required	Default Value	Description
<code>-n value</code> <code>--context-names=value</code>	Required, unless the <code>--discover</code> option is used	none	<p>A list of distinguished names (DNs) of the containers holding the LDAP accounts to be visible within the Spotfire Server. When you specify more than one DN, you must separate the DNs using pipe characters (<code> </code>).</p> <p>If the specified containers contain a large number of users, of which only a few should be visible in Spotfire Server, you can specify a custom user search filter to include only the designated users (see the <code>--user-search-filter</code> argument).</p> <p>Examples:</p> <ul style="list-style-type: none"> <code>CN=users,DC=example,DC=com</code> <code>OU=project-x,DC=research,DC=example,DC=com</code>
<code>-u value</code> <code>--username=value</code>	Required	none	<p>The name of the LDAP service account to use when searching for users (and optionally also groups) in the LDAP server. This service account does not need to have write permissions, but it must have read permissions for all configured context names (LDAP containers). For most LDAP servers, the account name is the account's distinguished name (DN). For Active Directory, the account name can also be specified in the forms <code>ntdomain\name</code> and <code>name@dnsdomain</code>.</p> <p>Examples:</p> <ul style="list-style-type: none"> <code>CN=spotsvc,OU=services,DC=research,DC=example,dc=COM</code> <code>RESEARCH\spotsvc</code> (Note: Active Directory only) <code>spotsvc@research.example.com</code> (Note: Active Directory only)

Option	Optional or Required	Default Value	Description
<code>-p value</code> <code>--password=value</code>	Optional	none	The password for the LDAP service account.

Option	Optional or Required	Default Value	Description
<code>--schedules=value</code>	Optional	@daily, @restart	<p>A comma-separated list of schedules for when the LDAP synchronization should be performed. The schedules are given in a cron-compatible format, where each schedule consists of either five fields or one shorthand label. Make sure you enclose the value in double quotes.</p> <p>The five fields are, from left to right, with their valid ranges: minute (0-59), hour (0-23), day of month (1-31), month (1-12) and day of week (0-7, where both 0 and 7 indicate Sunday).</p> <p>You can also configure a field with the wildcard character *, indicating that any moment in time matches this field. An LDAP synchronization is triggered when all fields match the current time. If both day of month and day of week have non-wildcard values, then only one of them has to match.</p> <p>You can also use following shorthand labels instead of the full cron expressions:</p> <ul style="list-style-type: none"> • @yearly or @annually: run once a year (equivalent to 0 0 1 1 *) • @monthly: run once a month (equivalent to 0 0 1 * *) • @weekly: run once a week (equivalent to 0 0 * * 0) • @daily or @midnight: run once a day (equivalent to 0 0 * * *) • @hourly: run once an hour (equivalent to 0 * * * *) • @minutely: run once a minute (equivalent to * * * * *) • @reboot or @restart: run every time the Spotfire Server is started

Option	Optional or Required	Default Value	Description
			Refer to the Wikipedia overview article on the cron scheduler .

Option	Optional or Required	Default Value	Description
<code>--user-search-filter=value</code>	Optional, but it must be specified for custom LDAP configurations, either when running this command or the update-ldap-config command.	For Active Directory servers, the parameter value defaults to '(&(objectClass=user)!(objectClass=computer)))'. For any version of the Sun Directory Servers, it defaults to 'objectClass=person'.	<p>Specifies an LDAP search expression filter to use when searching for users.</p> <p>If you need to identify a subset of users in the specified LDAP containers who should be allowed access to Spotfire Server, you can specify a more detailed user search filter. For example, the search expression can be expanded so that it also puts restrictions on which groups the users belong to, or which roles they have.</p> <ul style="list-style-type: none"> For Active Directory servers, access can be restricted to only those users belonging to a certain group by using a search expression with the pattern <code>&(objectClass=user) (memberOf=<groupDN>)</code> where <groupDN> is 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 <code>&(objectClass=user)((memberOf=<firstDN> (memberOf=<secondDN>)).</code> Add extra <code>(memberOf=<groupDN>)</code> sub-expressions as needed. Active Directory example: <code>&(objectClass=person) (isMemberOf=cn=project- x,dc=example,dc=com)</code> For a Sun Java System Directory Server version 6 and later, you can achieve the same effect by using a search expression with the pattern <code>&(objectClass= person) (isMemberOf=<groupDN>).</code> If the users are divided among multiple groups, use the pattern <code>&(objectClass=person)((isMemberOf=<firstDN>)</code>

Option	Optional or Required	Default Value	Description
			<p>(isMemberOf=<secondDN>)). Add extra (isMemberOf=<groupDN>) sub-expressions as needed.</p> <p>Sun Java System Directory Server example:</p> <pre>&(objectClass=person) (isMemberOf=cn=project- x,dc=example,dc=com)</pre> <ul style="list-style-type: none"> For Sun ONE Directory Servers and newer Sun Java System Directory Servers or the older iPlanet Directory Server, you can restrict access 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=<firstDN>) (nsRole=<secondDN>). Add extra (nsRole=<roleDN>) sub-expressions as needed. <p>Sun ONE Directory Servers example:</p> <pre>&(objectClass=person) (isMemberOf=cn=project- x,dc=example,dc=com)</pre> <p>The syntax of LDAP search expression filters is specified by the RFC 4515 document. Consult this documentation for information about more advanced filters.</p>

Option	Optional or Required	Default Value	Description
<code>--user-name-attribute=value</code>	Optional, unless the LDAP server type is set to "Custom" using the --type parameter.	For Active Director servers, the value defaults 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 defaults to 'uid'.	Specifies the name of the LDAP attribute containing the user account names.

Option	Optional or Required	Default Value	Description
<code>--authentication-attribute=value</code>	Optional; use only for advanced setups. It is not set by default.	none	<p>Specifies the name of the LDAP attribute containing a user identity that can be used for binding (authenticating) to the LDAP server. This attribute fills no purpose in most common LDAP configurations, but it can be useful in more advanced setups where the distinguished name (DN) does not work for authentication, or where users should be able to log in using a username that does not map directly to an actual LDAP account.</p> <ul style="list-style-type: none"> If you set up SASL with DIGEST-MD5 in an Active Directory environment, the DN does not work for authentication, and the <code>userPrincipalName</code> attribute must be used instead. The <code>--authentication-attribute</code> argument should then be set to <code>"userPrincipalName"</code> and the <code>--user-name-attribute</code> argument should be set to <code>"sAMAccountName"</code>. (The latter value is the default value for an Active Directory LDAP configuration, so there is no need to set it explicitly.) See also the <code>--security-authentication</code> argument. When you set up SASL with GSSAPI in an Active Directory environment, the DN does not work for authentication and the <code>sAMAccountName</code> or <code>userPrincipalName</code> attribute must be used instead. The <code>--authentication-attribute</code> argument should be set to <code>"sAMAccountName"</code> or <code>"userPrincipalName"</code>, and the <code>--user-name-attribute</code> argument should be set to <code>"sAMAccountName"</code>. (The latter value is the default value for an Active Directory LDAP configuration, so there

Option	Optional or Required	Default Value	Description
			<p>is no need to set it explicitly.) See also the <code>--security-authentication</code> argument.</p> <p>Example:</p> <p>If you set the <code>--user-name-attribute</code> argument to "cn" and the <code>--authentication-attribute</code> argument to "userPrincipalName" in an Active Directory environment, the users can log in to Spotfire Server using their CN attribute values, but underneath the hood, Spotfire Server actually uses the <code>userPrincipalName</code> attribute value of the LDAP account with the matching CN for the actual authentication.</p>

Option	Optional or Required	Default Value	Description
<code>--security-authentication=value</code>	Optional; use only in advanced setups.	simple	<p>Specifies the security level to use when binding to the LDAP server:</p> <ul style="list-style-type: none"> To enable anonymous binding, it should be set to "none". To enable plain username/password authentication, it should be set to "simple". To enable SASL authentication, it should be set to the name of the SASL mechanism to be used, for instance "DIGEST-MD5" or "GSSAPI". Use multiple <code>-c</code> arguments to set the additional JNDI environment properties that the SASL authentication mechanism typically requires. <p>If you set up SASL with DIGEST-MD5 in an Active Directory environment, all accounts must use reversible encryption for their passwords. This is typically not the default setting for the domain controller. The <code>--authentication-attribute</code> argument must also be used to specify the <code>userPrincipalName</code> attribute for the actual authentication to work correctly.</p> <p>If you set up SASL with GSSAPI in an Active Directory environment, the <code>--authentication-attribute</code> argument must be used to specify either the <code>sAMAccountName</code> or the <code>userPrincipalName</code> attribute, and the custom property <code>kerberos.login.context.name</code> must be mapped to the JAAS application configuration <code>SpotfireGSSAPI</code>. This, in turn, requires a fully working Kerberos configuration file at <code>/jdk/jre/lib/security/krb5.conf</code>.</p>

Option	Optional or Required	Default Value	Description
<code>--referral-mode=value</code>	Optional	follow	<p>Specifies how LDAP referrals should be handled. Valid arguments:</p> <ul style="list-style-type: none"> • follow (automatically follow any referrals). Recommended. • ignore (ignore referrals) • throw (fail with an error)
<code>[--referral-mode-root-dse=value]</code>	Optional	If not explicitly set, the value for <code>--referral-mode</code> is used.	<p>Specifies how LDAP referrals should be handled when looking up the RootDSE. Valid arguments are:</p> <ul style="list-style-type: none"> • follow (automatically follow any referrals) • ignore (ignore referrals) • throw (fail with an error)

Option	Optional or Required	Default Value	Description
<code>--request-control=value</code>	Optional	probe	<p>Determines the type of LDAP controls to be used for executing search queries 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, because it provides the most efficient way of retrieving the query result set.</p> <p>You can use the virtual list view control for the same purpose if the paged results control is not supported. The virtual list view control is used automatically, together with a sort control. Both the paged results control and the virtual list view control support a configurable page size, set by the <code>--page-size</code> argument.</p> <ul style="list-style-type: none"> • To explicitly configure the server for probing, set the argument value to "probe". • To configure the server for the paged results control, set the argument value to "PagedResultsControl". • To request the virtual list view control, set the argument value to "VirtualListViewControl". • To completely disable request controls, set the argument value to "none".
<code>--page-size=value</code>	Optional	2000 for both the paged results control and the virtual list view control.	Specifies the page size to be used with the paged results control or the virtual list view control when performing search queries to the LDAP server.

Option	Optional or Required	Default Value	Description
<code>--import-limit=value</code>	Optional	No import limit	<p>Specifies a threshold that limits the number of users that can be imported from an LDAP server to Spotfire Server in one query. This can be used to prevent accidentally flooding the Spotfire user directory when you integrate with an LDAP server with tens or even hundreds of thousands of users.</p> <p>By setting an import limit, you can be sure that an unexpected high number of users will not affect server performance.</p> <p>To request unlimited import explicitly, set the parameter value to "-1". All positive numbers are treated as an import limit. For most cases it is recommended that you leave this parameter untouched.</p>
<code>--user-display-name-attribute=value</code>	Optional	none	Specifies the name of the LDAP attribute containing the user display names.
<code>--group-display-name-attribute=value</code>	Optional	none	Specifies the name of the LDAP attribute containing the group display names.
<code>-Ckey=value</code>	Optional; can be specified multiple times with different keys.	none	<p>Specifies additional JNDI environment properties to use when connecting to the LDAP server.</p> <p>Example: The equivalent of specifying the <code>--security-authentication=DIGEST-MD5</code> argument is - <code>Cjava.naming.security.authentication=DIGEST-MD5</code>.</p>
<code>-Rvalue</code>	Optional; can be specified multiple times with different values.	If this argument is not specified, the Java defaults are used.	<p>Specifies the protocols to be used for LDAPS when connecting to the LDAP server.</p> <p>Example: To enable only TLSv1.2 <code>> -RTLSv1.2</code></p>

Option	Optional or Required	Default Value	Description
<code>-Svalue</code>	Optional; can be specified multiple times with different values.	If this argument is not specified, the Java defaults are used.	Specifies the cipher suites to be used for LDAPS when connecting to the LDAP server. Example: To enable only these two cipher suites <pre>> - STLS_DHE_RSA_WITH_AES_128_GCM_SHA256 - STLS_DHE_RSA_WITH_AES_256_GCM_SHA384</pre>
<code>--connection-timeout=value</code>	Optional	No timeout (see description)	Specifies the connection timeout. The value must be a non-negative integer representing the timeout in milliseconds. A value less than or equal to zero results in no timeout, effectively waiting until the connection times out on the TCP network level.
<code>--read-timeout=value</code>	Optional	No timeout (see description)	Specifies the read timeout. The value must be a non-negative integer representing the timeout in milliseconds. A value less than or equal to zero results in no timeout, effectively waiting until the connection times out on TCP network level.

EXAMPLES

Create an LDAP configuration for Active Directory:

```
create-ldap-config --id="ldap1" --type="ActiveDirectory"
--servers="ldap://dc01.research.example.com:3268 ldap://
dc02.research.example.com:3268" --context-names="OU=project-
x,DC=research,DC=example,DC=com|OU=phbs,DC=management,DC=example,DC=com"
--username="ldapadmin@research.example.com" --password="s3cr3t"
--schedules="@daily"
```

Create an LDAP configuration for SunONE:

```
create-ldap-config --id="ldap1" --type="SunONE"
--servers="ldap://directory.research.example.com:389" --context-names="OU=project-
x,DC=research,DC=example,DC=com|OU=phbs,DC=management,DC=example,DC=com"
--username="ldapadmin" --password="s3cr3t"
--schedules="@daily"
```

Create an LDAP configuration for Sun Java System Directory:

```
create-ldap-config --id="ldap1" --type="SunJavaSystem"
--servers="ldaps://directory.research.example.com:636" --context-
names="OU=project-x,DC=research,DC=example,DC=com|
OU=phbs,DC=management,DC=example,DC=com"
--username="ldapadmin" --password="s3cr3t"
--schedules="@daily"
```

Create an LDAP configuration for a custom LDAP server:

```
create-ldap-config --id="ldap1" --type="Custom"
--servers="ldap://directory.research.example.com" --context-names="OU=project-
x,DC=research,DC=example,DC=com|OU=phbs,DC=management,DC=example,DC=com"
```

```
--user-name-attribute="cn" --search-filter="(&(objectClass=person)
(isMemberOf=cn=projectX,dc=example,dc=com))"
--username="ldapadmin" --password="s3cr3t"
--schedules="@daily"
```

Create an LDAP configuration using the discover mode:

```
create-ldap-config --id="ldap1" --discover
--username="ldapadmin@research.example.com" --password="s3cr3t"
--schedules="@daily"
```

create-site


Creates a new site.

```
create-site
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
<-s value | --site-name=value>
[-a value | --public-address=value]
```

Overview

Use this command to create a new site to which servers may be assigned.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end user for it on the console. See Bootstrap.xml file for more information.
<code>-s value</code> <code>--site-name=value</code>	Required	none	The name of the site that will be created.
<code>-a value</code> <code>--public-address=value</code>	Optional	none	The public address of the site, for example 'http[s]://host[:port]/'. If no public address is set, it will be automatically determined during Spotfire Server startup. To change the value later on, use the set-public-address command.  It is recommended to specify the public address when creating a site.

create-user

Creates a new user account.

```
create-user
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
<-u value | --username=value>
[-p value | --password=value]
[-d value | --display-name=value]
[-e value | --email=value]
```

Overview

Use this command to create a new user account. This user can then be promoted to administrator using the [promote-admin](#) command.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .
<code>u value</code> <code>--username=value</code>	Required	none	The name of the new user.
<code>-p value</code> <code>--password=value</code>	Optional	none	The new user's password.
<code>-d value</code> <code>--display-name=value</code>	Optional	none	The new user's display name.
<code>-e value</code> <code>--email=value</code>	Optional	none	The new user's email address.

delete-disabled-users

Deletes disabled user accounts.

```
delete-disabled-users
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-a <true|false> | --keep-once-active-users=<true|false>]
[-m <true|false> | --keep-group-members=<true|false>]
[-p <true|false> | --keep-users-with-library-permissions=<true|false>]
[-l <true|false> | --keep-library-authors=<true|false>]
[-f | --force]
```

Overview

Use this command to delete disabled user accounts from the user directory.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .
<code>-a <true false></code> <code>--keep-once-active-users=<true false></code>	Optional	true	Indicates whether all users who have logged in at least once should be kept.
<code>-m <true false></code> <code>--keep-group-members=<true false></code>	Optional	true	Indicates whether all users who are members of at least one group should be kept.
<code>-p <true false></code> <code>--keep-users-with-library-permissions=<true false></code>	Optional	true	Indicates whether all users who have explicit library permissions should be kept.
<code>-l <true false></code> <code>--keep-library-authors=<true false></code>	Optional	true	Indicates whether all users who have created or modified any library item should be kept.
<code>-f</code> <code>--force</code>	Optional	none	Indicates that users should be deleted without need for further confirmation.

delete-disconnected-groups

Deletes disconnected groups.

```
delete-disconnected-groups
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-f | --force]
```

Overview

Use this command to delete from the user directory disconnected groups that have been previously synchronized from an LDAP directory.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .
<code>-f</code> <code>--force</code>	Optional	none	Indicates that groups should be deleted without need for further confirmation.

delete-jmx-user

Deletes a JMX user.

```
delete-jmx-user
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
<-u value | --username=value>
```

Overview

Use this command to delete a user who can access the server through JMX.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .
<code>-u value</code> <code>--username=value</code>	Required	none	The name of the user to be deleted.

delete-library-content

Deletes library content.

```
delete-library-content
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
<-i value | --items=value>
[-d | --database]
[-e | --external]
```

Overview

Use this command to delete a library items from the Spotfire database or from external storage on Amazon S3.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .
<code>-i value</code> <code>--items=value</code>	Required	none	A comma-separated list of items (GUIDs) to delete.
<code>-d</code> <code>--database</code>	Optional	none	Deletes entries in the Spotfire library database.
<code>-e</code> <code>--external</code>	Optional	none	Deletes entries in external storage.

delete-node

Deletes a specified node.

```
delete-node
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-k value | --keystore-file=value]
<-i value | --id=value>
```

Overview

Use this command to delete a specified node, after which it will no longer be a part of the collective. To use this command, at least one server in the collective must be running.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end user for it on the console. See Bootstrap.xml file for more information.
<code>-k value</code> <code>--keystore-file=value</code>	Optional	none	The location of the keystore containing the certificates used for securing internal communication.
<code>-i value</code> <code>--id=value</code>	Required	none	The ID of the node that should be deleted. The list-nodes command can be used to find the IDs of all nodes.

delete-oauth2-client

Deletes a specified OAuth2 client.

```
delete-oauth2-client
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-k value | --keystore-file=value]
<-i value | --client-id=value>
```

Overview

Use this command to delete a specified OAuth2 client. To use this command at least one server in the collective must be running.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

Option	Optional or Required	Default Value	Description
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See Bootstrap.xml file for more information.
<code>-k value</code> <code>--keystore-file=value</code>	Optional	none	The location of the keystore containing the certificates used for securing internal communication.
<code>-i value</code> <code>--client-id=value</code>	Required	none	The ID of the client to be deleted. The list-oauth2-clients command can be used to find the IDs of all clients.

delete-service-config

Deletes a service configuration.

```
delete-service-config
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
<-c value | --config-name=value>
```

Overview

Use this command to delete a service configuration. If the configuration is currently assigned to a service, that service will be reverted to the default configuration.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See the Bootstrap.xml file for more information.

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--config-name=value</code>	Required	none	The name of the configuration that should be deleted.

delete-site

Deletes a site.

```
delete-site
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
<-s value | --site-name=value>
[-i value | --target-site=value]
[-f | --force]
```

Overview

Use this command to delete a site. To delete a site that currently contains nodes, the `--target-site` argument must be specified. All nodes in the site will then be moved to the specified site.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end user for it on the console. See Bootstrap.xml file for more information.
<code>-s value</code> <code>--site-name=value</code>	Required	none	The name of the site that will be deleted.
<code>-i value</code> <code>--target-site=value</code>	Optional unless the site being deleted contains nodes. If the argument is not present and there are rules, scheduled updates, or resource pools in the deleted site, these will also be removed.	none	The name of a site into which any nodes, routing rules, scheduled updates, or resource pools in the site being deleted should be moved.

Option	Optional or Required	Default Value	Description
<code>-f</code> <code>--force</code>	Optional	none	Indicates whether the site's routing rules, scheduled updates, and resource pools should be deleted along with the site.

delete-user

Deletes a user account.

```
delete-user
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
<-u value | --username=value>
```

Overview

Use this command to delete a user account.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .
<code>-u value</code> <code>--username=value</code>	Required	none	The name of the user to be deleted.

demote-admin

Revokes full administrator privileges for a user.

```
demote-admin
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
<-u value | --username=value>
```

Overview

Use this command to revoke administrator privileges for a user by removing the user account from the Administrator group.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .
<code>-u value</code> <code>--username=value</code>	Required	none	The name of the user for which to revoke the administrator privileges. Unless the user is part of the configured default domain, the name of the user needs to include the user's domain name, for example <code>DOMAIN\user</code> or <code>user@domain</code> .

enable-user

Enables or disables a user account in the Spotfire database.

```
enable-user
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-u value | --username=value]
[-a | --all]
[-e <true|false> | --enabled=<true|false>]
```

Overview

Use this command to enable or disable a user account in the Spotfire database. A disabled user account does not have access to Spotfire.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See the Bootstrap.xml file for more information about this file.

Option	Optional or Required	Default Value	Description
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .
<code>u value</code> <code>--username=value</code>	Optional	none	The user that should be enabled or disabled. Should not be specified if the <code>-all</code> argument is used.
<code>-a</code> <code>--all</code>	Optional	none	Updates the enabled status for all the users. If this argument is present, no user name should be specified.
<code>-e <true false></code> <code>--enabled=<true false></code>	Optional	true	Specifies whether the user should be enabled.

export-config

Exports a server configuration from the server database to the current working directory as a `configuration.xml` file.

```
export-config
[-f | --force]
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-h value | --hash=value]
[export file]
```

Overview

Use this command to export a server configuration from the server database to a file. The configuration in the file can be edited and then imported back into the server database using the [import-config](#) command.

Options

Option	Optional or Required	Default Value	Description
<code>-f</code> <code>--force</code>	Optional	none	Indicates that the tool should overwrite an existing destination file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

Option	Optional or Required	Default Value	Description
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .
<code>-h value</code> <code>--hash=value</code>	Optional	none	The (possibly abbreviated) hash of the configuration to export. Must consist of at least 6 hexadecimal characters.
<code>[export file]</code>	Optional	configuration.xml	The path to the configuration file that will be created.

export-ds-template

Exports the definition of a data source template.

```
export-ds-template
[-f | --force]
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
<-n value | --name=value>
[template definition file]
```

Overview

Use this command to export to a file the definition of a data source template used by Information Services.

Options

Option	Optional or Required	Default Value	Description
<code>-f</code> <code>--force</code>	Optional	none	Indicates whether the tool should overwrite an existing destination file.
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-n value</code> <code>--name=value</code>	Required	none	The name of the data source template for which to export the definition.
<code>[template definition file]</code>	Optional	template.xml	The path to the definition file to create.

export-groups

Exports groups from the user directory.

```
export-groups
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-m <true|false> | --include-member-groups=<true|false>]
[-u <true|false> | --include-member-users=<true|false>]
[-g <true|false> | --include-guids=<true|false>]
[-s <true|false> | --use-stdf=<true|false>]
[-n <true|false> | --include-name-row=<true|false>]
[export file]
[-f | --force]
```

Overview

Use this command to export all groups from the user directory. The exported groups can be imported on a different server.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .
<code>-m <true false></code> <code>--include-member-groups=<true false></code>	Optional	false	Indicates whether the group hierarchy information (groups in groups) should be included. Can be used in conjunction with the <code>--include-member-users</code> argument to include all information.
<code>-u <true false></code> <code>--include-member-users=<true false></code>	Optional	false	Indicates whether the group hierarchy information (users in groups) should be included. Can be used in conjunction with the <code>--include-member-groups</code> argument to include all information.
<code>-g <true false></code> <code>--include-guids=<true false></code>	Optional	false	Indicates whether the globally unique identifier (GUID) of each group should be included.
<code>-s <true false></code> <code>--use-stdf=<true false></code>	Optional	true	Indicates whether the exported file should be created in Spotfire Text Data Format. If "false", plain CSV format is used.

Option	Optional or Required	Default Value	Description
<code>-n <true false></code> <code>--include-name-row=<true false></code>	Optional	false	Indicates whether the exported file should include a column name row. Applicable only when <code>--use-stdf</code> is set to "false" because STDF always includes a name row.
<code>[export file]</code>	Optional	groups.txt	The path to the file to create.
<code>-f</code> <code>--force</code>	Optional	none	Indicates that the tool should overwrite an existing destination file.

export-library-content

Exports content from the library.

```
export-library-content
[-f | --force]
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
<-p value | --file-path=value>
<-u value | --user=value>
[-a <true|false> | --include-access-rights=<true|false>]
<-i value | --item-type=value>
<-l value | --library-path=value>
```

Overview

Use this command to export content from the library.

Options

Option	Optional or Required	Default Value	Description
<code>-f</code> <code>--force</code>	Optional	none	Indicates that the tool should overwrite any already existing file with the same name as specified in the path argument. All parts of the existing file (path.part0.zip, path.part1.zip, and so on) are also deleted.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the bootstrap.xml file. If the tool password is omitted, the command will prompt the end-user for it on the console. See Bootstrap.xml file help topic for more information.

Option	Optional or Required	Default Value	Description
<code>-p value</code> <code>--file-path=value</code>	Required	none	The file system path to where the item should be exported.
<code>-u value</code> <code>--user=value</code>	Required	none	The user performing the export should be a Library Administrator. The name of the user needs to include the user's domain name, for example DOMAIN\user or user@domain, unless the user is part of the configured default domain.
<code>-a <true false></code> <code>--include-access-rights=<true false></code>	Optional	true	Specifies if access rights should be exported.
<code>-i value</code> <code>--item-type=value</code>	Required	none	<p>Indicates which item types should be exported from the library. It is possible to export all items, or all items of a certain type, from a folder. It is also possible to export a single item of a certain type. When exporting the content of a folder, valid values are: <code>all_items</code>, <code>data_files</code>, <code>analysis_files</code>, <code>data_access</code>, <code>datafunctions</code>, <code>colorschemes</code>, <code>automation_job</code>, and <code>information_model</code>.</p> <p>When exporting a single item, valid values are, for example: <code>dxp</code>, <code>sddf</code>, <code>connectiondatasource</code>, <code>query</code>, <code>asjob</code>, <code>column</code>, <code>procedure</code>, <code>analyticmodel</code>, <code>dxpscript</code>, <code>filter</code>, <code>datafunction</code>, <code>datasource</code>, <code>colorscheme</code>, <code>dataconnection</code>, and <code>join</code>.</p>
<code>-l value</code> <code>--library-path=value</code>	Required	none	The path in the library where the content is exported from. When exporting folder content, a path to the folder must be specified. When exporting a single item, a path to that specific item must be specified. The path must start with a slash (/). If the entire library should be exported, the path should be "/".

export-rules

Exports routing rules and schedules from the server.

```
export-rules
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-k value | --keystore-file=value]
[export file]
[-f | --force]
```


Overview

Use this command to export all the routing rules and schedules from the server. The exported rules may be imported on a different server.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See Bootstrap.xml file help topic for more information.
<code>-k value</code> <code>--keystore-file=value</code>	Optional	none	The location of the keystore containing the certificates used for securing internal communication.
<code>[export-file]</code>	Optional	<code>rules.json</code>	The path to the file to create.
<code>-f</code> <code>--force</code>	Optional	none	The force flag indicates whether the tool overwrites an existing destination file.

export-service-config

Exports a service configuration.

```
export-service-config
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-c value | --config-name=value]
[-a value | --capability=value]
[-d value | --deployment-area=value]
[-f | --force]
[destination directory]
```

Overview

Use this command to export a service configuration for editing. The edited configuration can be imported using the [import-service-config](#) command. Either specify a configuration name or, to export a default configuration, a capability, and a deployment area.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See Bootstrap.xml file for more information.
<code>-c value</code> <code>--config-name=value</code>	Required, unless the <code>--capability</code> and <code>--deployment-area</code> arguments are specified (in which case this argument cannot be specified).	none	The name of the configuration that should be exported.
<code>-a value</code> <code>--capability=value</code>	Required, unless the <code>--config-name</code> argument is specified (in which case this argument cannot be specified).	none	The name of a capability for which the default configuration should be exported. The possible values can be found using the list-service-configs command. This argument must be specified together with the <code>--deployment-area</code> argument.
<code>-d value</code> <code>--deployment-area=value</code>	Required, unless the <code>--config-name</code> argument is specified (in which case this argument cannot be specified).	none	The name of a deployment area for which the default configuration should be exported. This argument must be specified together with the <code>--capability</code> argument.
<code>-f</code> <code>--force</code>	Optional	none	Indicates that the tool should overwrite any existing destination directory.

Option	Optional or Required	Default Value	Description
[destination directory]	Optional	config	The destination directory to which the configuration should be exported.

export-users

Exports users from the user directory.

```
export-users
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-i value | --include-password-hashes=value]
[-s value | --use-stdf=value]
[-g value | --include-guids=value]
[-n value | --include-name-row=value]
[export file]
[-f | --force]
```

Overview

Use this command to export all users from the user directory. The exported users can be imported on a different server.

Options

Option	Optional or Required	Default Value	Description
-b value --bootstrap-config=value	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
-t value --tool-password=value	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .
-i value --include-password-hashes=value>	Optional	false	Indicates whether the exported file should include the password hashes. Passwords are relevant only if you use the Spotfire database for authentication.
-s value --use-stdf=value	Optional	true	Indicates whether the exported file should be created in Spotfire Text Data Format. If <code>false</code> , plain CSV format is used.
-g value --include-guids=value	Optional	false	Indicates whether the Globally Unique Identifier (GUID) of each user should be included.

Option	Optional or Required	Default Value	Description
<code>-n value</code> <code>--include-name-row=value</code>	Optional	false	Indicates whether the exported file should include a column name row. Applicable only when <code>--use-stdf</code> is set to <code>false</code> because STDF always includes a name row.
<code>[export file]</code>	Optional	users.txt	The path to the file to create.
<code>-f</code> <code>--force</code>	Optional	none	Indicates that the tool should overwrite an existing destination file.

help

Displays the help overview or a specific help topic.

```
help
[topic name]
```

Overview

Use this command to display the help overview or a specific help topic.

Options

Option	Optional or Required	Default Value	Description
<code>[topic name]</code>	Optional	none	The name of the help topic to be displayed.

import-config

Imports a server configuration from a file to the server database.

```
import-config
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
<-c value | --comment=value>
[-d <true|false> | --delete-file=<true|false>]
[import file]
```

Overview

Use this command to import a server configuration from a file to the server database and to set it as the current configuration. Such a server configuration file can be generated either by running the [export-config](#) command or by creating a new default configuration by using the [create-default-config](#) command. If an identical configuration file already exists in the server database, the existing configuration will have its description and modification date updated.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See Bootstrap.xml file for more information.
<code>-c value</code> <code>--comment=value</code>	Required	none	A comment describing the reason for the configuration change. Make sure to enclose the specified comment in quotation marks and to quote all special characters that might otherwise be consumed by the command line shell.
<code>-d <true false></code> <code>--delete-file=<true false></code>	Optional	false	Indicates whether the imported configuration file should be deleted from the file system after a successful import.
<code>[import file]</code>	Optional	configuration.xml	The path to the configuration file to import.

import-groups

Imports groups to the user directory.

```
import-groups
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-m <true|false> | --include-member-groups=<true|false>]
[-u <true|false> | --include-member-users=<true|false>]
[-g <true|false> | --include-guids=<true|false>]
[-n <true|false> | --has-name-row=<true|false>]
[import file]
```

Overview

Use this command to import all groups in a given file to the user directory. The groups can be imported including membership information or as a simple list.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	configuration.xml	The path to the configuration file to create.
<code>-m <true false></code> <code>--include-member-groups=<true false></code>	Optional	false	Indicates whether the group hierarchy information (groups in groups) should be included. Can be used in conjunction with the <code>--include-member-users</code> argument to include all information.
<code>-u <true false></code> <code>--include-member-users=<true false></code>	Optional	false	Indicates whether the group hierarchy information (users in groups) should be included. Can be used in conjunction with the <code>--include-member-groups</code> argument to include all information.
<code>-g <true false></code> <code>--include-guids=<true false></code>	Optional	false	Indicates whether globally unique identifiers (GUIDs) in the file should be included.
<code>-n <true false></code> <code>--has-name-row=<true false></code>	Optional	false	Indicates whether the file contains a name row. Applicable only when the file is in plain CSV format because the Spotfire Text Data Format (STDF) always has a name row.
<code>[import file]</code>	Optional	groups.txt	The path to the file to import.

import-jaas-config

Imports new JAAS application configurations into the server configuration.

```
import-jaas-config
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-f | --force]
<-j value | --jaas-config-file=value>
[-n value | --name=value]
```

Overview

Use this command to import new JAAS application configurations into the server configurations.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-f</code> <code>--force</code>	Optional	none	Indicates that the JAAS application configurations should be imported into the server even if other configurations with the same names already exist. When this argument is enabled, the old configurations are overwritten
<code>-j value</code> <code>--jaas-config-file=value</code>	Required	none	The path to the JAAS application configuration file. The file is expected to be in the standard JAAS application configuration format.
<code>-n value</code> <code>--name=value</code>	Optional	none	The names of the JAAS application configurations to be imported into the server. Multiple names must be comma-separated and enclosed between quotes. If this argument is omitted, then all JAAS application configurations within the specified file are imported.

import-library-content

Imports content into the library.

```
import-library-content
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
<-p value | --file-path=value>
<-m value | --conflict-resolution-mode=value>
<-u value | --user=value>
[-e <true|false> | --prune-empty-directories=<true|false>]
[-a <true|false> | --include-access-rights=<true|false>]
[-i value | --item-type=value]
[-l value | --library-path=value]
```

Overview

Use this command to import content into the library.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	true	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See Bootstrap.xml file help topic for more information.
<code>-p value</code> <code>--file-path=value</code>	Required	none	The file system path to the file that should be imported into the library. This should be the result of a previous library export and with a name ending with <code>.part0.zip</code> . If the export consists of several parts (ending with <code>.part1.zip</code> and so on), these must be placed in the same folder.
<code>-m value</code> <code>--conflict-resolution-mode=value</code>	Required	none	Sets the conflict resolution mode that should be used if there is a conflict with existing content in the library path given. The conflict resolution mode is applied for each conflicting item that is imported. Valid values are <code>KEEP_NEW</code> , <code>KEEP_OLD</code> , and <code>KEEP_BOTH</code> .
<code>-u value</code> <code>--user=value</code>	Required	none	The user performing the import should be a Library Administrator. Unless the user is part of the configured default domain, the name of the user needs to include the user's domain name, like <code>DOMAIN \user</code> or <code>user@domain</code> .
<code>-e <true false></code> <code>--prune-empty-directories=<true false></code>	Optional	false	Specifies if empty directories should be created.

Option	Optional or Required	Default Value	Description
<code>-a <true false></code> <code>--include-access-rights=<true false></code>	Optional	true	Specifies if access rights should be imported.
<code>-i value</code> <code>--item-type=value</code>	Optional	all_items	Which item types that should be imported into the library. Valid values are: all_items, colorschemes, information_model, analysis_files, and datafunctions.
<code>-l value</code> <code>--library-path=value</code>	Optional	/	The path in the library where the content is imported. The path must specify an existing folder in the library.

import-rules

Imports routing rules and schedules to the server.

```
import-rules
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-k value | --keystore-file=value]
<exported file>
[-r value | --resource-pool-name=value]
[-u <true|false> | --use-default-resource-pool=<true|false>]
[-d <true|false> | --disabled=<true|false>]
[-s value | --site-name=value]
[-R value | --rule-conflict-resolution=value]
[-S value | --schedule-conflict-resolution=value]
[-e <true|false> | --test-run=<true|false>]
```

Overview

Use this command to import all the routing rules and schedules from the given file to the server.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the bootstrap.xml file. If the tool password is omitted, the command will prompt the end-user for it on the console. See Bootstrap.xml file help topic for more information.

Option	Optional or Required	Default Value	Description
<code>-k value</code> <code>--keystore-file=value</code>	Optional	none	The location of the keystore containing the certificates used for securing internal communication.
<code><exported-file></code>	Required	none	The path to the file containing the rules and schedules to import.
<code>-r value</code> <code>--resource-pool-name=value</code>	Optional	none	A resource pool name that can be used if the resource pool for a given rule is not found. The <code>--resource-pool-name</code> and <code>--use-default-resource-pool</code> arguments are mutually exclusive.
<code>-u <true false></code> <code>--use-default-resource-pool=<true false></code>	Optional	false	If enabled and the resource pool for a given rule is not found, the default resource pool will be used instead, and the instances count will be automatically reset to one instance. The <code>--resource-pool-name</code> and <code>--use-default-resource-pool</code> arguments are mutually exclusive.
<code>-d <true false></code> <code>--disabled=<true false></code>	Optional	false	If true, all the rules will be imported in a disabled state.
<code>-s value</code> <code>--site-name=value</code>		none	The name of a site into which the routing rules and schedules will be imported.
<code>-R value</code> <code>rule-conflict-resolution=value</code>	Optional	fail	Defines how to handle importing a rule if there already exists a rule with the same name and the same file/user/group. The argument can be one of: fail (default), replace, or skip.

Option	Optional or Required	Default Value	Description
<code>-S value</code> <code>--schedule-conflict-resolution=value</code>	Optional	rename	Defines how to handle copying a shared schedule if there already exists a shared schedule with the same name in the target server. The argument can be one of: rename (default), or replace. If the schedules are identical, the schedule in the target server will remain as it was. If the names are the same but the schedules are different, the schedule-conflict-resolution parameter determines whether the schedule in the target server should be renamed or replaced.
<code>-e <true false></code> <code>--test-run=<true false></code>	Optional	false	If true, the import will not actually take place, but the command will produce a preview of the import status of each rule/schedule.

import-scheduled-updates

Imports scheduled updates from previous Spotfire Web Player versions, from either a local file or the library.

```
import-scheduled-updates
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-k value | --keystore-file=value]
[-p value | --local-file-path=value]
[-n value | --library-file-name=value]
[-r value | --resource-pool-name=value]
[-z value | --time-zone-id=value]
[-e <true|false> | --enabled=<true|false>]
[-i value | --instances-count=value]
[-s value | --site-name=value]
```

Overview

Use this command to import scheduled updates from previous Spotfire Web Player versions, from either a local file or the library. At least one Spotfire Server instance must be running.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

Option	Optional or Required	Default Value	Description
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See Bootstrap.xml file for more information.
<code>-k value</code> <code>--keystore-file=value</code>	Optional	none	The location of the keystore containing the certificates used for securing internal communication.
<code>-p value</code> <code>--local-file-path=value</code>	Optional	none	Full path to the local scheduled updates file. Mutually exclusive with the <code>library-file-name</code> .
<code>-n value</code> <code>--library-file-name=value</code>	Optional	none	Name of the scheduled updates file in the library (specified in the previous Spotfire Web Player configuration). Mutually exclusive with the <code>local-file-path</code> .
<code>-r value</code> <code>--resource-pool-name=value</code>	Optional		Optional resource pool for the scheduled updates. If unspecified, default routing applies.
<code>-z value</code> <code>--time-zone-id=value</code>	Optional	none	Optional time zone ID in the Area/City format, for example "America/Los_Angeles" or "Europe/Brussels" (a full list is available in the server). If unspecified, server time zone applies.
<code>-e <true false></code> <code>--enabled=<true false></code>	Optional	false	Optional flag to specify if the scheduled updates are enabled when imported.
<code>-i value</code> <code>--instances-count=value</code>	Optional	1	Optionally specifies on how many Spotfire Web Player instances the scheduled updates should run. '0' means all available.

Option	Optional or Required	Default Value	Description
<code>-s value</code> <code>--site-name=value</code>	Optional	none	The name of the site that the scheduled updates should be imported to. If no site is given, the scheduled updates will be imported to the default site.

import-service-config

Imports a service configuration.

```
import-service-config
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-n value | --config-name=value]
[-d | --delete-directory]
[source directory]
```

Overview

Use this command to import a service configuration. The imported configuration can be assigned to a service using the [set-service-config](#) command.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See the Bootstrap.xml file for more information.
<code>-n value</code> <code>--config-name=value</code>	Optional	none	The name to give to the configuration. If no name is given, the existing configuration will be overwritten. Note that default configurations cannot be overwritten, so if the configuration to be imported was created from a default configuration, a name must be specified.

Option	Optional or Required	Default Value	Description
<code>-d</code> <code>--delete-directory</code>	Optional	none	Indicates whether or not the source directory should be deleted after a successful import.
<code>[source directory]</code>	Optional	config	The source directory containing the configuration that should be imported.

import-users

Imports users to the user directory.

```
import-users
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-i <true|false> | --include-passwords=<true|false>]
[-h <true|false> | --hash-passwords=<true|false>]
[-g <true|false> | --include-guids=<true|false>]
[-n <true|false> | --has-name-row=<true|false>]
[import file]
```

Overview

Use this command to import all users in a given file to the user directory. The users can be imported with or without passwords.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .
<code>-i <true false></code> <code>--include-passwords=<true false></code>	Optional	false	Indicates whether passwords in the file should be included.
<code>-h <true false></code> <code>--hash-passwords=<true false></code>	Optional	false	Indicates whether the included passwords should be hashed during import. Should be false if the users have previously been exported from a Spotfire Server because those passwords are already hashed.

Option	Optional or Required	Default Value	Description
<code>-g <true false></code> <code>--include-guids=<true false></code>	Optional	false	Indicates whether the globally unique identifiers (GUIDs) in the file should be included.
<code>-n <true false></code> <code>--has-name-row=<true false></code>	Optional	false	Indicates whether the file contains a name row. Applicable only when the file is in plain CSV format because the Spotfire Text Data Format (STDF) always has a name row.
<code>[import file]</code>	Optional	users.txt	The path to the file to import.

invalidate-persistent-sessions

Invalidates all persistent sessions.

```
invalidate-persistent-sessions
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-u value | --username=value]
[-a | --all]
```

Overview

Use this command to invalidate persistent sessions for a specified user or for all users.

After the persistent sessions have been invalidated, the user(s) must re-authenticate when they next log in. Currently active sessions will remain active until the next idle timeout or absolute timeout (whichever happens first), after which the user will have to re-authenticate.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See The bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See The bootstrap.xml file for more information.

Option	Optional or Required	Default Value	Description
<code>-u value</code> <code>--username=value</code>	Required, unless the <code>--all</code> flag has been specified	none	The user for which all persistent sessions should be invalidated. Must not be specified together with the <code>--all</code> flag.
<code>-a</code> <code>--all</code>	Required, unless the <code>--username</code> argument has been specified	none	Indicates that all persistent sessions for all users should be invalidated. Must not be specified together with the <code>--username</code> argument.

list-active-service-configs

Lists active (configured) service configurations.

```
list-active-service-configs
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-s value | --site-name=value]
```

Overview

Use this command to list the active (configured) service configurations. See also the [list-service-configs](#) command.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See Bootstrap.xml file for more information.
<code>-s value</code> <code>--site-name=value</code>	Optional	Default	The name of the site for which to list the active service configurations. The list-sites command can be used to find names of all available sites.

list-addresses

Lists the addresses of a node.

```
list-addresses
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-n value | --node-id=value]
```

Overview

Use this command to list the configured addresses of a node. The addresses can be configured using the [set-addresses](#) command.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See Bootstrap.xml file for more information.
<code>-n value</code> <code>--node-id=value</code>	Required	The default value is taken from the file specified with <code>--bootstrap-config</code> .	The ID of the node for which addresses should be listed. The list-nodes command can be used to find the IDs of all nodes in the collective.

list-admins

Lists the server administrators.

```
list-admins
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
```

Overview

Use this command to list the server administrators. Only direct members of the Administrator group are shown.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it. Refer to Bootstrap.xml file .

list-auth-config

Displays the current authentication configuration.

```
list-auth-config
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
```

Overview

Use this command to display the current authentication configuration.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

list-certificates

Lists the certificates that establish the trust between components within the Spotfire collective.

```
list-certificates
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-v | --valid]
[-e | --expired]
[-r | --revoked]
[-p | --pending]
```

Overview

Use this command to list the certificates that establish the trust between components within the Spotfire collective. By default, the tool displays all certificates issued by the internal CA. The output from the tool can be restricted by specifying one or more of the flags.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See Bootstrap.xml file for more information.
<code>-v</code> <code>--valid</code>	Optional	none	When this flag is specified, the tool displays all valid certificates.
<code>-e</code> <code>--expired</code>	Optional	none	When this flag is specified, the tool displays all expired certificates.
<code>-r</code> <code>--revoked</code>	Optional	none	When this flag is specified, the tool displays all revoked certificates.
<code>-p</code> <code>--pending</code>	Optional	none	When this flag is specified, the tool displays all pending certificates.

list-configs

Lists all available server configurations.

```
list-configs
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-i | --include-incompatible]
[-h value | --hash-abbrev=value]
```

Overview

Use this command to list the available configurations. The current configuration is indicated by an asterisk in the left column.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .
<code>-i</code> <code>--include-incompatible</code>	Optional	none	Indicates whether to include configurations incompatible with the current server version.
<code>-h value</code> <code>--hash-abbrev=value</code>	Optional	7	The number of hexadecimal digits (between 6 and 40) to which you want to abbreviate the configuration hash.

list-deployment-areas

Lists the deployment areas.

```
list-deployment-areas
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
```

Overview

Use this command to list the deployment areas as well as display the default deployment area.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it. Refer to Bootstrap.xml file .

list-ds-template

Lists the data source templates.

```
list-ds-template
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
```

Overview

Use this command to list the data source templates.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

list-groups

Lists all groups.

```
list-groups
[-l value | --limit=value]
[-s value | --search-expression=value]
[-m | --list-members]
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
```

Overview

Use this command to list all groups in the user directory.

Options

Option	Optional or Required	Default Value	Description
<code>-l value</code> <code>--limit=value</code>	Optional	20	The maximum number of groups to list.
<code>-s value</code> <code>--search-expression=value</code>	Optional	none	A search expression that can be used to search only for groups with names matching the expression.
<code>-m</code> <code>--list-members</code>	Optional	none	Determines whether to list the members.

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .

list-jaas-config

Lists the JAAS application configurations.

```
list-jaas-config
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[--xml]
[JAAS application configuration name]
```

Overview

Use this command to display the server JAAS application configurations. (It cannot display system JAAS application configurations.)

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>--xml</code>	Optional	none	Specifies if the JAAS application configurations should be displayed in XML format, as it is stored within the <code>configuration.xml</code> file.
<code>[JAAS application configuration name]</code>	Optional	none	The names of the JAAS application configuration to display. Multiple names must be comma-separated and enclosed between quotes. If this argument is omitted, then all JAAS application configurations are displayed.

list-jmx-users

Lists all JMX users.

```
list-jmx-users
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
```

Overview

Use this command to list all users who can access the server through JMX. The result contains the user name and access level of each user.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .

list-ldap-config

Displays LDAP configurations.

```
list-ds-template
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[--xml=value]
[LDAP configuration id]
```

Overview

Use this command to list the data source templates.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

Option	Optional or Required	Default Value	Description
<code>--xml=value</code>	Optional	none	Specifies that the LDAP configuration should be displayed in XML format instead of the standard JAAS application configuration format.
<code>[LDAP configuration id]</code>	Optional	none	Specifies the identifier of the LDAP configuration to be displayed. If no identifier is specified, then all LDAP configurations are displayed.

list-ldap-userdir-config

Lists the configuration for the user directory LDAP mode.

```
list-ldap-userdir-config
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
```

Overview

Use this command to list the configuration for the user directory LDAP mode.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

list-licenses

Lists the currently known licenses and license functions.



To get the licenses, you first must deploy Spotfire.

```
list-licenses
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
```

Overview

Use this command to list the license and license functions.



To get the licenses, you first must deploy Spotfire. Licenses will be listed by their technical names and not their display names (for example, Spotfire.Dxp.WebPlayer, rather than TIBCO Spotfire Consumer).

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See the Bootstrap.xml file for more information.

list-logging

Lists logging templates for a specified node.

```
list-logging
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-k value | --keystore-file=value]
<-i value | --id=value>
```

Overview

Use this command to list available logging templates for a node.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See Bootstrap.xml file for more information.
<code>-k value</code> <code>--keystore-file=value</code>	Optional	none	The location of the keystore containing the certificates used for securing internal communication.

Option	Optional or Required	Default Value	Description
<code>-i value</code> <code>--id=value</code>	Required	none	The ID of the server or node manager for which the logging templates are to be listed. The list-nodes command can be used to find the IDs of all nodes.

list-nodes

Lists the nodes in the collective.

```
list-nodes
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-e | --exclude-trusted]
```

Overview

Use this command to list the nodes in the collective.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See the Bootstrap.xml file for more information.
<code>-e</code> <code>--exclude-trusted</code>	Optional	none	Indicates whether trusted nodes should be excluded.

list-ntlm-auth

Displays the NTLM authentication service configuration.

```
list-ntlm-auth
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-S value | --server=value]
```

Overview

Use this command to display the NTLM authentication service configuration.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-S value</code> <code>--server=value</code>	Optional	none	The name of the cluster server whose configuration should be displayed. If no name is specified, the global parameters common to all servers in the cluster are displayed.

list-oauth2-clients

Lists registered OAuth2 clients.

```
list-oauth2-clients
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-k value | --keystore-file=value]
```

Overview

Use this command to list registered OAuth2 clients. Use the [show-oauth2-client](#) command to see the full configuration of a client. To use this command at least one server in the collective must be running.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end user for it on the console. See Bootstrap.xml file for more information.
<code>-k value</code> <code>--keystore-file=value</code>	Optional	none	The location of the keystore containing the certificates used for securing internal communication.

list-online-servers

Lists all online servers.

```
list-online-servers
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
```

Overview

Use this command to list all servers in the cluster that are currently online.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. See the Bootstrap.xml file .

Output

A table of all servers in the cluster that are currently online. An asterisk in the left column is used to indicate that the server is the current primus server (responsible for handling tasks such as the synchronization of LDAP groups).

Example

```
P  Server Name          IP Address    Version
   server1.example.com  192.0.2.1    7.0.0.70
*  server2.example.com  192.0.2.2    7.0.0.60
   server3.example.com  192.0.2.3    7.0.0.70
```

list-post-auth-filter

Displays the current post-authentication filter configuration.

```
list-post-auth-filter
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
```

Overview

Use this command to display the post-authentication filter configuration.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

list-service-configs

Lists available service configurations.

```
list-service-configs
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-c value | --capability=value]
[-a value | --deployment-area=value]
[-e | --exclude-default-configs]
```

Overview

Use this command to list the available service configurations. The configurations can be exported using the [export-service-config](#) command.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See Bootstrap.xml file for more information.
<code>-c value</code> <code>--capability=value</code>	Optional	none	The name of the capability for which to list configurations.
<code>-a value</code> <code>--deployment-area=value</code>	Optional	none	The name of the deployment area for which to list configurations.

Option	Optional or Required	Default Value	Description
<code>-e</code> <code>--exclude-default-configs</code>	Optional	none	Indicates whether default configurations should be excluded.

list-service-instances

Lists the service instances in the collective.

```
list-service-instances
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-v <true|false> | --verbose=<true|false>]
```

Overview

Use this command to list the service instances in the collective.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .
<code>-v <true false></code> <code>--verbose=<true false></code>	Optional	false	Show verbose information about the service.

list-services

Lists the installed services in the collective.

```
list-services
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-v <true|false> | --verbose=<true|false>]
```

Overview

Use this command to list the installed services in the collective.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See the Bootstrap.xml file for more information.
<code>-v <true false></code> <code>--verbose=<true false></code>	Optional	false	Show verbose information about the service.

list-sites

Lists the sites in the collective.

```
list-sites
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
```

Overview

Use this command to list the sites in the collective.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See the Bootstrap.xml file for more information.

list-userdir-config

List the current user directory configuration.

```
list-userdir-config
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
```

Overview

Use this command to list the current user directory configuration.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

list-users

Lists all users.

```
list-users
[-f | --force-synchronization]
[-l value | --limit=value]
[-s value | --search-expression=value]
[-d | --display-name-search]
[-e <true|false> | --exclude-disabled=<true|false>]
--list-extended-information
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
```

Overview

Use this command to list all users in the user directory. It does not work when using the user directory Windows provider.

Options

Option	Optional or Required	Default Value	Description
<code>-f</code> <code>--force-synchronization</code>	Optional	none	Indicates that the command should force a user directory synchronization before attempting to list the users. This argument has no effect if the user directory is running in database mode.
<code>-l value</code> <code>--limit=value</code>	Optional	100	The maximum number of users to list.
<code>-s value</code> <code>--search-expression=value</code>	Optional	none	A search expression that can be used to search only for users with names matching the expression.

Option	Optional or Required	Default Value	Description
<code>-d</code> <code>--display-name-search</code>	Optional	none	Indicates whether the search expression should be used to match display names rather than user names.
<code>-e value</code> <code>--exclude-disabled=<true false></code>	Optional	false	Indicates whether disabled users should be excluded.
<code>--list-extended-information</code>	Optional	false	Indicates whether extended information such as display name, email, and last login time should be displayed for each user.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. See the Bootstrap.xml file .

list-windows-userdir-config

Lists the configuration for the user directory Windows NT mode.

```
list-windows-userdir-config
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
```

Overview

Use this command to list the configuration for the user directory Windows NT mode.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

manage-deployment-areas

Manages the deployment areas.

```
manage-deployment-areas
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-R | --reset-all-group-areas]
[-r | --reset-group-area]
[-s | --set-group-area]
[-c | --create-area]
[-D | --delete-area]
[-d | --default-area]
[-g value | --group-name=value]
[-a value | --area-name=value]
```

Overview

Use this command to change the deployment area for groups, change the default deployment area, and create and remove deployment areas.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. See Bootstrap.xml file .
<code>-R</code> <code>--reset-all-group-areas</code>	Optional	none	Use if all specified areas for all groups should be removed. This does not affect the default area or any content on the areas. Users are using the default area after running this command. The <code>--reset-all-group-areas</code> , <code>--reset-group-area</code> , <code>--set-group-area</code> , <code>--create-area</code> , <code>--delete-area</code> , and <code>--default-area</code> arguments are mutually exclusive.
<code>-r</code> <code>--reset-group-area</code>	Optional	none	Use if an area for a specific group should be removed. This does not affect the default area or any content on the area. If a user is not a member of any group with a specified area, the default area is used. The <code>--reset-all-group-areas</code> , <code>--reset-group-area</code> , <code>--set-group-area</code> , <code>--create-area</code> , <code>--delete-area</code> , and <code>--default-area</code> arguments are mutually exclusive.

Option	Optional or Required	Default Value	Description
<code>-s</code> <code>--set-group-area</code>	Optional	none	Use if an area should be set for a specific group. A user that is a member of this group gets access to the specified area instead of the default area. The <code>--reset-all-group-areas</code> , <code>--reset-group-area</code> , <code>--set-group-area</code> , <code>--create-area</code> , <code>--delete-area</code> , and <code>--default-area</code> arguments are mutually exclusive.
<code>-c</code> <code>--create-area</code>	Optional	none	Specifies that a new area should be created. The <code>--reset-all-group-areas</code> , <code>--reset-group-area</code> , <code>--set-group-area</code> , <code>--create-area</code> , <code>--delete-area</code> , and <code>--default-area</code> arguments are mutually exclusive.
<code>-D</code> <code>--delete-area</code>	Optional	none	Specifies that an existing area should be deleted. The <code>--reset-all-group-areas</code> , <code>--reset-group-area</code> , <code>--set-group-area</code> , <code>--create-area</code> , <code>--delete-area</code> , and <code>--default-area</code> arguments are mutually exclusive.
<code>-d</code> <code>--default-area</code>	Optional	none	Specifies that the default area should be changed. The <code>--reset-all-group-areas</code> , <code>--reset-group-area</code> , <code>--set-group-area</code> , <code>--create-area</code> , <code>--delete-area</code> , and <code>--default-area</code> arguments are mutually exclusive.
<code>-g value</code> <code>--group-name=value</code>	Optional	none	The name of the group. Applicable for <code>--reset-all-group-areas</code> , <code>--reset-group-area</code> , and <code>--set-group-area</code> .
<code>-a value</code> <code>--area-name=value</code>	Optional	none	The name of the area. Applicable for <code>--set-group-area</code> , <code>--create-area</code> , <code>--delete-area</code> , and <code>--default-area</code> .

modify-db-config

Modifies the common database connection configuration.

```

modify-db-config
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-l value | --login-timeout=value]
[-o value | --connection-timeout=value]
[-i value | --min-connections=value]
[-a value | --max-connections=value]
[-p value | --pooling-scheme=value]
[-q value]
{-Ckey=value}
[-e <true|false> | --clear-connection-properties=<true|false>]

```

Overview

Use this command to modify the common configuration for the connection to the Spotfire Server database. This configuration (which affects all servers) is merged with the configuration in the `bootstrap.xml` file on each server.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-l value</code> <code>--login-timeout=value</code>	Optional	none	The maximum time (in seconds) to wait for a connection to become available.
<code>-o value</code> <code>--connection-timeout=value</code>	Optional	none	The maximum time (in seconds) that a connection can stay idle in the connection pool before being closed and discarded.
<code>-i value</code> <code>--min-connections=value</code>	Optional	none	The minimum number of connections to keep in the connection pool.
<code>-a value</code> <code>--max-connections=value</code>	Optional	none	The maximum number of connections to keep in the connection pool.
<code>-p value</code> <code>--pooling-scheme=value</code>	Optional	none	The connection pooling algorithm to be used. Valid values are: <ul style="list-style-type: none"> • WAIT: The <code>--max-connections</code> parameter is strictly respected. • DYNAMIC: The number of connections can occasionally exceed the configured maximum number.
<code>-q value</code>	Optional	none	An SQL query that should be run directly after a connection has been created.
<code>-Ckey=value</code>	Optional	none	A JDBC connection property that is added to the existing list of connection properties. Several properties can be specified. (Can be specified multiple times with different keys.)

Option	Optional or Required	Default Value	Description
<code>-e <true false></code> <code>--clear-connection-properties=<true false></code>	Optional	false	Clears the existing list of connection properties.

Examples

Setting the maximum number of connections in the pool:

```
config modify-db-config --max-connections=100
```

Setting the pooling scheme:

```
config modify-db-config --pooling-scheme=WAIT
```

Setting the size of the statement pool of the DataDirect driver:

```
config modify-db-config -CMaxPooledStatements=20
```

modify-ds-template

Modifies a data source template.

```
modify-ds-template
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
<-n value | --name=value>
[-e <true|false> | --enable=<true|false>]
[-r value | --rename=value]
[-d value | --definition=value]
```

Overview

Use this command to modify a data source template used by Information Services.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-n value</code> <code>--name=value</code>	Required	none	The name of the data source template to modify.
<code>-e <true false></code> <code>--enable=<true false></code>	Optional	none	Indicates whether the data source template should be enabled. If no argument is given, the value is unchanged.

Option	Optional or Required	Default Value	Description
<code>-r value</code> <code>--rename=value</code>	Optional	none	The name to rename the data source template to. If no argument is given, the value is unchanged.
<code>-d value</code> <code>--definition=value</code>	Optional	none	The path to the file containing a new data source template definition. If no argument is given, the value is unchanged.

promote-admin

Assigns full administrator privileges to a user.

```
promote-admin
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
<-u value | --username=value>
```

Overview

Use this command to promote a user to administrator by adding the user account to the Administrator group.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .
<code>-u value</code> <code>--username=value</code>	Required	none	The name of the user to be promoted to administrator. Unless the user is part of the configured default domain, the name of the user must include the user's domain name, as in "DOMAIN \user" or "user@domain".

register-job-sender-client

Registers a new Automation Services Client Job Sender client.

```
register-job-sender-client
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-k value | --keystore-file=value]
<-n value | --name=value>
```

Overview

Use this command to register a new OAuth2 client that can be used with the Automation Services Client Job Sender. All information needed to use the client, including a client ID and a client secret, will be shown after successful completion of the command. To use this command, at least one server in the collective must be running.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end user for it on the console. See Bootstrap.xml file for more information.
<code>-k value</code> <code>--keystore-file=value</code>	Optional	none	The location of the keystore containing the certificates used for securing internal communication.
<code>-n value</code> <code>--name=value</code>	Required	none	The name of the client to be created. Only used for display purposes, and not guaranteed to be unique.

remove-ds-template

Removes a data source template.

```
remove-ds-template
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
<-n value | --name=value>
```

Overview

Use this command to remove a data source templates.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-n value</code> <code>--name=value</code>	Required	none	The name of the data source template to remove.

remove-jaas-config

Removes the specified JAAS application configurations from the server configuration.

```
remove-jaas-config
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
<-n value | --name=value>
```

Overview

Use this command to remove JAAS application configurations from the server.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-n value</code> <code>--name=value</code>	Required	none	The names of the JAAS application configurations to be removed from the server. Multiple names must be comma-separated and enclosed between quotes.

remove-ldap-config

Removes LDAP configurations.

```
remove-ldap-config
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
<LDAP configuration ids>
```

Overview

Use this command to remove LDAP configurations.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code><LDAP configuration ids></code>	Required	none	Specifies a comma-separated list of identifiers of the LDAP configurations to be removed.

remove-license

Removes a license from a group.

```
remove-license
<-g value | --group=value>
<-l value | --license=value>
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
```

Overview

Use this command to remove a license from a group.

Options

Option	Optional or Required	Default Value	Description
<code>-g value</code> <code>--group=value</code>	Required	none	The group to have its licenses removed.
<code>-l value</code> <code>--license=value</code>	Required	none	The license to remove.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .

reset-trust

Resets the trust within the Spotfire collective.

```
reset-trust
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-d | --delete]
[-f | --force]
```

Overview

Use this command to reset the trust within the Spotfire collective by revoking all the certificates in the internal CA. When the `--delete` argument is provided, the certificates are deleted instead of revoked.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See the Bootstrap.xml file for more information.
<code>-d</code> <code>--delete</code>	Optional	none	When this flag is specified, the tool deletes the certificates in the internal CA instead of just revoking them.
<code>-f</code> <code>--force</code>	Optional	none	When this flag is specified, the tool revokes or deletes the certificates in the internal CA without requiring any confirmation.

run

Runs a configuration script.

```
run
<script file>
```

Overview

Use this command to run a configuration script.

Options

Option	Optional or Required	Default Value	Description
<code><script file></code>	Required	none	The name of the script to be executed.

Script Syntax

Each line must contain the name of a command and its arguments. Arguments can be quoted using either single or double quotation marks. Lines beginning with a hash character (#) are regarded as comments and have no effect. Lines ending with a backslash character (\) are continued on the next line with the backslash character removed before parsing. The special script command "**echo**" can be used to echo messages to the console. See [Script language](#).

s3-download

Downloads the data of library items in Amazon S3 storage.

```
s3-download
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
<-i value | --items=value>
<-d value | --destination=value>
```

Overview

Use this command to download the data of library items in Amazon S3 storage.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it. Refer to Bootstrap.xml file .
<code>-i value</code> <code>--items=value</code>	Required	none	A comma-separated list of the library items (GUIDs) to download.
<code>-d value</code> <code>--destination=value</code>	Required	none	The directory where the downloaded items should be saved.

set-addresses

Sets the addresses for a Spotfire Server node.

```
set-addresses
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-n value | --node-id=value]
{-Avalue}
[-d | --auto-detect]
```

Overview

Use this command to set the (back-end) addresses (host names and IP addresses) of the Spotfire Server node, used for internal communication within the Spotfire collective. Ensure that the node can be reached on all addresses. The back-end ports *must* be reachable through the configured addresses, and the front-end port may be reachable through the configured addresses.



The server being configured must be offline when running the command.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See Bootstrap.xml file for more information.
<code>-n value</code> <code>--node-id=value</code>	Optional	The default value is taken from the file specified with <code>--bootstrap-config</code> .	The ID of the node for which the addresses should be set. The list-nodes command can be used to find the IDs of all nodes in the collective.
<code>-Avalue</code>	Required, unless the <code>--auto-detect</code> flag is specified, and may be specified multiple times with different values.	The default value is the host name(s) and IP address(es) as determined when this command is run.	The possible node backend addresses (host names and IP addresses). Used for internal communication within the Spotfire collective. The addresses will be used in the order they are provided (in cases where there is a need for ordering). The <code>-A</code> and <code>--auto-detect</code> arguments are mutually exclusive.

Option	Optional or Required	Default Value	Description
<code>-d</code> <code>--auto-detect</code>	Required, unless at least one <code>-A</code> argument is specified.	none	If specified, this argument indicates that the addresses should be determined automatically. Must only be specified when configuring the addresses of the server node where the command is run. The <code>-A</code> and <code>--auto-detect</code> arguments are mutually exclusive.

set-config

Sets the current server configuration.

```
set-config
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
<-h value | --hash=value>
<-c value | --comment=value>
```

Overview

Use this command to set the current configuration to one of the existing configurations. See [list-configs](#) for more information.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .
<code>-h value</code> <code>--hash=value</code>	Required	none	The (possibly abbreviated) hash of the configuration to set. Must be at least the first six hexadecimal characters of the hash.
<code>-c value</code> <code>--comment=value</code>	Required	none	A comment describing the reason for the configuration change.

set-config-prop

Sets the value of a specific configuration property.

```
set-config-prop
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
```

```
<-n value | --name=value>
<-v value | --value=value>
[-e <true|false> | --encrypt=<true|false>]
```

Overview

Use this command to set the value of a specific configuration property. There must be at most one such property and the value of the property must be representable as a string.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-n value</code> <code>--name=value</code>	Required	none	The name of the configuration property.
<code>-v value</code> <code>--value=value</code>	Required	none	The new value of the configuration property. This will replace any existing value.
<code>-e <true false></code> <code>--encrypt=<true false></code>	Optional	false	Indicates whether the value should be stored encrypted.

Example

To set the absolute session timeout to one hour:

```
config set-config-prop --name="security.absolute-session-timeout" --value="60"
```

set-db-config

Sets the common database connection configuration.

```
set-db-config
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
[-l value | --login-timeout=value]
[-o value | --connection-timeout=value]
[-i value | --min-connections=value]
[-a value | --max-connections=value]
[-p value | --pooling-scheme=value]
[-q value]
{-Ckey=value}
```

Overview

Use this command to set the common configuration for the connection to the Spotfire Server database. This configuration (which affects all servers) is merged with the configuration in the `bootstrap.xml` file on each server.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-l value</code> <code>--login-timeout=value</code>	Optional	10	The maximum time (in seconds) to wait for a connection to become available.
<code>-o value</code> <code>--connection-timeout=value</code>	Optional	600	A comma-separated list of the library items (GUIDs) to download.
<code>-i value</code> <code>--min-connections=value</code>	Optional	5	The minimum number of connections to keep in the connection pool.
<code>-a value</code> <code>--max-connections=value</code>	Optional	40	The maximum number of connections to keep in the connection pool.
<code>-p value</code> <code>--pooling-scheme=value</code>	Optional	WAIT	<p>The connection pooling algorithm to be used. Valid values are:</p> <ul style="list-style-type: none"> • WAIT: The <code>--max-connections</code> parameter is strictly respected. • DYNAMIC: The number of connections can occasionally exceed the configured maximum number.
<code>-q value</code>	Optional	none	An SQL query that should be run directly after a connection has been created.
<code>-Ckey=value</code>	Optional	none	A JDBC connection property. Several properties can be specified.

Examples

To set the maximum number of connections in the pool:

```
config set-db-config --max-connections=100
```

To set the pooling scheme:

```
config set-db-config --pooling-scheme=WAIT
```

To set the size of the statement pool of the DataDirect driver:

```
config set-db-config CMaxPooledStatements=20
```

set-license

Sets a license and license functions for a group. To see the currently available licenses and license functions, use the `list-licenses` command.

```
set-license
<-g value | --group=value>
<-l value | --license=value>
[-f value | --functions=value]
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
```

Overview

Use this command to set a license and license functions for a group.

Options

Option	Optional or Required	Default Value	Description
<code>-g value</code> <code>--group=value</code>	Required	none	The group that should get the licenses set.
<code>-l value</code> <code>--license=value</code>	Required	none	The license to set. If no license function is provided using the <code>--functions</code> parameter, then all license functions belonging to that license are inherently enabled.
<code>-f value</code> <code>--functions=value</code>	Optional	none	The license functions to enable.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .

set-logging

Set logging for a specified node.

```
set-logging
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-k value | --keystore-file=value]
<-i value | --id=value>
[-p value | --local-file-path=value]
[-n value | --template-file-name=value]
```


Overview

Use this command to set specific logging levels using a custom properties file/template on a specified node.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See Bootstrap.xml file for more information.
<code>-k value</code> <code>--keystore-file=value</code>	Optional	none	The location of the keystore containing the certificates used for securing internal communication.
<code>-i value</code> <code>--id=value</code>	Required	none	The ID of the server or node manager for which the logging templates/file is to be applied. The list-nodes command can be used to find the IDs of all nodes.
<code>-p value</code> <code>--local-file-path=value</code>	Optional	none	The full path of the logging file that will be used to set logging levels.
<code>-n value</code> <code>--template-file-name=value</code>	Optional	none	The template file name which should be used to set the loggers for the node. The list-logging command can be used to find the template files of a node.

set-public-address

Configures the public address.

```
set-public-address
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-s value | --site-name=value]
[-u value | --url=value]
```

Overview

Use this command to configure the public address that should be used when generating absolute URLs. A public address must be configured if the Spotfire Server is accessed through a load balancer or reverse proxy.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See the Bootstrap.xml file for more information.
<code>-s value</code> <code>--site-name=value</code>	Optional if there is a local server (in which case the site of that server will be used) or if there is only one site available (in which case that site will be used).	none	The name of the site for which to set the public address. The list-sites command can be used to find names of all available sites.
<code>-u value</code> <code>--url=value</code>	Optional	none	The public address URL to use, for example "http[s]://host[:port]". If no URL is specified, any existing value will be cleared and the public address will be automatically determined during Spotfire Server startup.

set-server-service-config

Sets the configuration for a service running in Spotfire Server (typically the Spotfire Web Player front-end).

```
set-server-service-config
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-s value | --site-name=value]
```

```
[ -a value | --capability=value ]
[ -c value | --config-name=value ]
```

Overview

Use this command to set the configuration for a service running in Spotfire Server.



After setting the configuration, you must restart the affected servers.

To configure a service running on a remote node, use the [set-service-config](#) command.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See Bootstrap.xml file for more information.
<code>-s value</code> <code>--site-name=value</code>	Optional if there is a local server (in which case the site of that server will be used) or if there is only one site available (in which case that site will be used).	none	The name of the site for which to set the configuration. The list-sites command can be used to find names of all available sites.
<code>-a value</code> <code>--capability=value</code>	Optional	WEB_PLAYER	The name of the capability for which to set the configuration.
<code>-c value</code> <code>--config-name=value</code>	Optional	none	The name of the configuration that should be set. If no configuration name is specified, the service will revert to the default configuration.

set-service-config

Sets the configuration for a service running on a remote node.

```
set-service-config
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-k value | --keystore-file=value]
<-s value | --service-id=value>
[-c value | --config-name=value]
[-f | --force]
```

Overview

Use this command to set the configuration for a service running on a remote node. Note that all running instances (if any) of the service will be restarted.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See Bootstrap.xml file for more information.
<code>-k value</code> <code>--keystore-file=value</code>	Optional	none	The location of the keystore containing the certificates used for securing internal communication.
<code>-s value</code> <code>--service-id=value</code>	Required	none	The ID of the service for which the service should be set.
<code>-c value</code> <code>--config-name=value</code>	Optional	none	The name of the configuration that should be set. If no configuration name is specified, the service reverts to the default configuration.
<code>-f</code> <code>--force</code>	Optional	none	Indicates that the service configuration should be set without need for further confirmation.

set-site

Sets the site to which a node should belong.

```
set-site
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-n value | --node-id=value]
<-s value | --site-name=value>
```

Overview

Use this command to assign a node to a site.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See Bootstrap.xml file for more information.
<code>-n value</code> <code>--node-id=value</code>	Optional	The default value is taken from the file specified with <code>--bootstrap-config</code> .	The ID of the node for which the site should be set. The list-nodes command can be used to find the IDs of all nodes in the collective.
<code>-s value</code> <code>--site-name=value</code>	Required	none	The name of the site to which the node should belong. The list-sites command can be used to find names of all available sites. New sites can be created using the create-site command.

set-user-password

Sets a new password for a given user.

```
set-user-password
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
<-u value | --username=value>
[-p value | --password=value]
```

Overview

Use this command to set the password for a specific user account.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See Bootstrap.xml file for more information.
<code>-u value</code> <code>--username=value</code>	Required	WEB_PLAYER	The name of the user for which the password should be set.
<code>-p value</code> <code>--password=value</code>	Optional	none	The new password.

show-basic-ldap-auth

Shows the LDAP authentication source for use with the BASIC authentication method.

```
show-basic-ldap-auth
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
```

Overview

Use this command to show the LDAP authentication source(s) for use with the BASIC authentication method. The configuration is stored within the Spotfire LDAP JAAS application configuration.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

show-config-history

Shows the configuration history.

```
show-config-history
[-b value | --bootstrap-config=value]
```

```
[-t value | --tool-password=value]
[-h value | --hash-abbrev=value]
```

Overview

Use this command to show the configuration history. The most recent entry is the current configuration.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .
<code>-h value</code> <code>--hash-abbrev=value</code>	Optional	7	The number of hexadecimal digits to abbreviate the configuration hash to. Must be a number between 6 and 40.

show-deployment

Shows the current deployment.

```
show-deployment
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-a value | --area=value]
[-s | --show-ids]
```

Overview

Use this command to show the current deployment in a given area.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .

Option	Optional or Required	Default Value	Description
<code>-a value</code> <code>--area=value</code>	Optional	none	The deployment area for which to show the current deployment. If no area is specified, the deployment of the default area is showed.
<code>-s</code> <code>--show-ids</code>	Optional	none	Indicates whether the package IDs should be included in the output. A package ID is needed to remove a specific package using the update-deployment command. For more information, see update-deployment .

show-import-export-directory

Shows the library import/export directory.

```
show-import-export-directory
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
```

Overview

Use this command to display the library import/export directory. All library import and export operations are done from and to this directory, which can be a local directory or can reside on a shared disk.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

show-join-database

Shows the configured default join database.

```
show-join-database
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
```

Overview

Use this command to show the configured default join database, used by Information Services.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

show-library-permissions

Shows permissions set in the library.

```
show-library-permissions
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
<-l value | --library-path=value>
[-r <true|false> | --recursive=<true|false>]
[-x <true|false> | --expand-groups=<true|false>]
[-d <true|false> | --downward=<true|false>]
[-p value | --path-to-report=value]
[-f <true|false> | --force-overwrite=<true|false>]
```

Overview

Use this command to create a report file that shows the permissions in the library.

Permissions are set on directories. If no permission is set, the directory inherits the permissions from the directory above.

You can use this command in three different ways:

- It can show if any permissions are set explicitly on a directory.
- It can show what permissions are in effect on a certain directory. If no permissions are set on the directory itself, it will continue upwards until it finds the directory from which the permissions are inherited (see recursive option).
- It can be used to report on all directories with permissions explicitly set in a branch of the directory (see the downward option).

The resulting file should be possible to read in Spotfire. It has headers that explain the display in the different columns.

This command may take some time to run. Also, you may need to increase the Java memory allocation to run the command, especially if the users are displayed.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.

Option	Optional or Required	Default Value	Description
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See Bootstrap.xml file help topic for more information.
<code>-l value</code> <code>--library-path=value</code>	Required	none	The path in the library to start to report with (must start with a <code>/</code>).
<code>-r <true false></code> <code>--recursive=<true false></code>	Optional	false	If no permission is set on this directory, continue upwards until permissions are found.
<code>-x <true false></code> <code>--expand-groups=<true false></code>	Optional	false	Specifies whether groups are expanded to show their members. Members of the Administrator and Library Administrator group can see all content. When <code>expand-groups</code> is "true", these implicit rights are also taken into account, and these groups and their members are also displayed.
<code>-d <true false></code> <code>--downward=<true false></code>	Optional	false	Lists permissions on an entire branch of the library, and shows only folders where permissions are set explicitly. (This option takes precedence over the recursive option.)
<code>-p value</code> <code>--path-to-report=value</code>	Optional	none	The name of the report file that should be generated. If not provided, an automatic name is generated.
<code>-f <true false></code> <code>--force-overwrite=<true false></code>	Optional	false	If a name for the report file is provided but a file with that name already exists, set this option to "true" to overwrite the existing file.

show-licenses

Shows licenses set on the server.

```
show-licenses
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-l value | --license=value]
[-x <true|false> | --expand-groups=<true|false>]
[-p value | --path-to-report=value]
[-f <true|false> | --force-overwrite=<true|false>]
```

Overview

Use this command to create a report file that shows the licenses set on the server.

You can read the resulting file in Spotfire. The file has headers that explain the contents displayed in the columns. The column "From Group" contains the group on which the license is explicitly set. For every group that has a license set explicitly, the resulting groups and users (if the expand option is set) are shown once.

Users get the sum of all licenses (and functions). When you analyze the file, note that a user and a license might occur more than once if the user gets its licenses from more than one group with explicit licenses set.

This command may take some time to run. Also, you may need to increase the Java memory allocation to run the command, especially if the users are displayed.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. See Bootstrap.xml file help topic for more information.
<code>-l value</code> <code>--license=value</code>	Optional	none	An optional, comma-separated list of licenses. If provided, the report contains only these licenses. If an invalid entry is given, the valid licenses are displayed.
<code>-x <true false></code> <code>--expand-groups=<true false></code>	Optional	false	Specifies whether groups are expanded to show their members. Members of the Administrator and Library Administrator group can see all content. When <code>expand-groups</code> is "true", these implicit rights are also taken into account, and these groups and their members are also displayed.
<code>-p value</code> <code>--path-to-report=value</code>	Optional	none	The name of the report file that should be generated. If not provided, an automatic name is generated.
<code>-f <true false></code> <code>--force-overwrite=<true false></code>	Optional	false	If a name for the report file is provided but a file with that name already exists, set this option to "true" to overwrite the existing file.

show-oauth2-client

Shows the configuration of a specified OAuth2 client.

```
show-oauth2-client
[-b value | --bootstrap-config=value]
```

```
[-t value | --tool-password=value]
[-k value | --keystore-file=value]
<-i value | --client-id=value>
[-s <true|false> | --show-client-secret=<true|false>]
```

Overview

Use this command to show the full configuration, possibly including the client secret, of a registered OAuth2 client. To use this command at least one server in the collective must be running.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end user for it on the console. See Bootstrap.xml file for more information.
<code>-k value</code> <code>--keystore-file=value</code>	Optional	none	The location of the keystore containing the certificates used for securing internal communication.
<code>-i value</code> <code>--client-id=value</code>	Required	none	The client ID of the client for which to show the configuration. The list-oauth2-clients command can be used to find the IDs of all clients.
<code>-s <true false></code> <code>--show-client-secret=<true false></code>	Optional	false	Indicates whether the client secret should be shown.

switch-domain-name-style

Switches the domain names for all users and groups from one style (DNS or NetBIOS) to the other (for all configured domains).

```
switch-domain-name-style
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
<-n value | --new-domain-name-style=value>
```

Overview

Use this command to switch the domain names for all existing users and groups from one style (DNS or NetBIOS) to the other (for all configured domains). The new domain name style must first be configured using the [config-userdir](#) command. Note that this command is only applicable when using a user directory in LDAP mode against Active Directory.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See the Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. See Bootstrap.xml file .
<code>-n value</code> <code>--new-domain-name-style=value</code>	Required	none	The new domain name style. Valid values are <code>dns</code> and <code>netbios</code> .

test-jaas-config

Tests a JAAS application configuration.

```
test-jaas-config
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-c value | --configuration=value]
<-j value | --jaas-configuration=value>
<-u value | --username=value>
[-p value | --password=value]
```

Overview

Use this command to test a JAAS application configuration by performing a login attempt, using the specified credentials. It can test either a configuration stored in the server database or a configuration stored in an exported configuration file. To test a configuration stored in a configuration file, use the `--configuration` argument. Otherwise the configuration stored in the database is tested. If the JAAS login module requires a connection to the server database, the `--configuration` argument cannot be used.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . Can be specified if a password is given and <code>--enable-config-tool</code> argument is set to <code>true</code> (the default).

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	none	The path to an exported server configuration file. If this parameter is omitted, the application attempts to retrieve the configuration parameters from the server database using the file <code>bootstrap.xml</code> , specified by the <code>--bootstrap</code> argument.
<code>-j value</code> <code>--jaas-configuration=value</code>	Required	none	The name of the JAAS application configuration to test.
<code>-u value</code> <code>--username=value</code>	Required	none	The name of the user to log in as.
<code>-p value</code> <code>--password=value</code>	Optional	none	The password of the user to log in as. If the password is omitted, the command prompts the user for it.

trust-node

Trusts a specified node.

```
trust-node
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-k value | --keystore-file=value]
<-i value | --id=value>
```

Overview

Use this command to trust a specified node, after which it will be a part of the collective. To use this command, at least one server in the collective must be running.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See the Bootstrap.xml file for more information.

Option	Optional or Required	Default Value	Description
<code>k value</code> <code>--keystore-file=value</code>	Optional	none	The location of the keystore containing the certificates used for securing internal communication.
<code>-i value</code> <code>--id=value</code>	Required	none	The ID of the node that should be trusted. The list-nodes command can be used to find the IDs of all nodes waiting to be trusted.

untrust-node

Untrusts a specified node.

```
untrust-node
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
[-k value | --keystore-file=value]
<-i value | --id=value>
```

Overview

Use this command to untrust a specified node, after which it will no longer be a part of the collective. To use this command, at least one server in the collective must be running.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the <code>bootstrap.xml</code> file. If the tool password is omitted, the command will prompt the end-user for it on the console. See Bootstrap.xml file for more information.
<code>k value</code> <code>--keystore-file=value</code>	Optional	none	The location of the keystore containing the certificates used for securing internal communication.
<code>-i value</code> <code>--id=value</code>	Required	none	The ID of the node that should be untrusted. The list-nodes command can be used to find the IDs of all trusted nodes.

update-bootstrap

Updates an existing bootstrap configuration file.

```
update-bootstrap
[-c value | --driver-class=value]
[-d value | --database-url=value]
[-u value | --username=value]
[-p value | --password=value]
[--clear-username-and-password]
[-k value | --kerberos-login-context=value]
[--clear-kerberos-login-context]
{-Ckey=value}
[--clear-connection-properties]
[--disable-config-tool]
[--enable-config-tool]
[-t value | --tool-password=value]
[-a value | --server-alias=value]
[-r | --prompt]
[bootstrap configuration file]
```

Overview

Use this command to update an existing bootstrap configuration file. To create a new file, use the [bootstrap](#) command. Server addresses can be set using the [set-addresses](#) command. The encryption password can be updated by using the [config-encryption](#) command. The site to which the server belongs can be changed by using the [set-site](#) command.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--driver-class=value</code>	Optional	none	This argument specifies the name of the JDBC driver class. If not specified, the previous value is kept. Note that if you change driver you will likely also have to modify the URL (using the <code>--database-url</code> argument).
<code>-d value</code> <code>--database-url=value</code>	Optional	none	This argument specifies the JDBC URL to the database. If not specified, the previous value is kept. Because this argument usually contains special characters, make sure to escape those characters or enclose the values between quotes.
<code>-u value</code> <code>--username=value</code>	Optional	none	This argument specifies the database account's username. If not specified, the previous value (if any) is kept.
<code>-p value</code> <code>--password=value</code>	Optional	none	This argument specifies the database account's password. If not specified, the previous value (if any) is kept. Use the <code>--prompt</code> flag to indicate that the tool should prompt for the password.

Option	Optional or Required	Default Value	Description
<code>--clear-username-and-password</code>	Optional	none	When this flag is specified, any existing username and password will be removed. Use this to switch from username/password-based authentication to Kerberos or NTLM. Cannot be specified together with the <code>--username</code> , <code>--password</code> , or <code>--tool-password</code> arguments.
<code>-k value</code> <code>--kerberos-login-context=value</code>	Optional	none	<p>This argument specifies the name of the JAAS application configuration to be used for acquiring the Kerberos TGT, when using the Kerberos protocol to log in to the database. If not specified, the previous value (if any) is kept unless the <code>--clear-kerberos-login-context</code> flag is specified. The JAAS application configuration must be registered with the JVM using a <code>login.config.url</code> parameter in the <code><server install directory>\jdk\jre\lib\security\java.security</code> file (Windows) or <code><server install directory>/jdk/jre/lib/security/java.security</code> file (Unix).</p> <p>The Spotfire Server import-jaas-config command cannot be used for this purpose because the JAAS application configurations that are imported using this command are stored in the database itself, which prevents the Spotfire Server from using them for creating the initial connection to the database.</p>
<code>--clear-kerberos-login-context</code>	Optional	none	When this flag is specified, any previous Kerberos login context will be cleared. Cannot be specified together with the <code>--kerberos-login-context</code> argument.
<code>-Ckey=value</code>	Optional	none	A JDBC connection property. Several properties may be specified. If not specified, the previous values (if any) are kept unless the <code>--clear-connection-properties</code> flag is specified. This argument may be specified multiple times with different keys.

Option	Optional or Required	Default Value	Description
<code>--clear-connection-properties</code>	Optional	none	When this flag is specified, any previous connection properties will be cleared. Cannot be specified together with the <code>-C</code> argument.
<code>--disable-config-tool</code>	Optional	none	When this flag is specified the <code>config-tool</code> section (if any) will be removed from the bootstrap configuration file. Disables the use of the configuration tool with this bootstrap configuration file. Cannot be specified together with the <code>--enable-config-tool</code> argument. If neither the <code>--disable-config-tool</code> nor the <code>--enable-config-tool</code> argument is specified, the capability will remain as before.
<code>--enable-config-tool</code>	Optional	none	When this flag is specified, a <code>config-tool</code> section will be added to the bootstrap configuration file. Enables the use of the configuration tool with this bootstrap configuration file. Cannot be specified together with the <code>--disable-config-tool</code> argument. If neither the <code>--disable-config-tool</code> nor the <code>--enable-config-tool</code> argument is specified, the capability will remain as before.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	This argument specifies the password needed to execute most configuration tool commands. If not specified, the previous value (if any) is kept. Use the <code>--prompt</code> flag to indicate that the tool should prompt for the password.
<code>-a value</code> <code>--server-alias=value</code>	Optional	none	The server alias. Used for identifying the server, for example when specifying server-specific configuration. If not specified, the previous value is kept.
<code>-r</code> <code>--prompt</code>	Optional	none	When this flag is specified, the tool will prompt for any missing password arguments.
<code>bootstrap configuration file</code>	Optional	none	This argument specifies the path to the bootstrap configuration file to create. See Bootstrap.xml file for more information about this file.

update-deployment

Updates the current deployment.

```
update-deployment
[-b value | --bootstrap-config=value]
[-t value | --tool-password=value]
<-a value | --area=value>
[-c | --clear]
[-r value | --remove-packages=value]
[-v value | --version=value]
[-d value | --description=value]
[-f | --force-update]
[deployment files]
```

Overview

Use this command to add a new deployment or to update the current deployment in a given area.

Options

Option	Optional or Required	Default Value	Description
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>-t value</code> <code>--tool-password=value</code>	Optional	none	The configuration tool password used to decrypt the database password in the file <code>bootstrap.xml</code> . If the tool password is omitted, the command prompts the user for it in the console. Refer to Bootstrap.xml file .
<code>-a value</code> <code>--area=value</code>	Required	none	The deployment area that should be updated.
<code>-c</code> <code>--clear</code>	Optional	none	Indicates that all existing packages should be removed before any new files are added. If no files are provided to add to the deployment, the deployment area is empty.
<code>-r value</code> <code>--remove-packages=value</code>	Optional	none	A comma-separated list of IDs of packages that should be removed from the deployment. The IDs can be determined using the show-deployment command. Should not be specified together with the <code>--clear</code> argument
<code>-v value</code> <code>--version=value</code>	Optional	none	The version of the new deployment. If no value is given, it is taken from the current deployment, or from the last added distribution if one is added.

Option	Optional or Required	Default Value	Description
<code>-d value</code> <code>--description=value</code>	Optional	none	The description of the new deployment. If no value is given it is taken from the current deployment, or from the last added distribution if one is added.
<code>-f</code> <code>--force-update</code>	Optional	none	Indicates that users connecting to the server should be forced to update their clients.
<code>[deployment files]</code>	Optional	none	A comma-separated list of files (packages and distributions) that should be added to the deployment. Note that the paths cannot contain spaces.

update-ldap-config

Updates LDAP configurations.

```
update-ldap-config
[-c value | --configuration=value]
[-b value | --bootstrap-config=value]
<--id=value>
[-t value | --type=value]
[-s value | --servers=value]
[--clear-context-names]
[-n value | --context-names=value]
[-u value | --username=value]
[-p value | --password=value]
[--schedules=value]
[--clear-schedules]
[--user-search-filter=value]
[--user-name-attribute=value]
[--authentication-attribute=value]
[--security-authentication=value]
[--referral-mode=value]
[--referral-mode-root-dse=value]
[--request-control=value]
[--page-size=value]
[--import-limit=value]
[--user-display-name-attribute=value]
[--group-display-name-attribute=value]
{-Ckey=value}
{-Rvalue}
{-Svalue}
[--connection-timeout=value]
[--read-timeout=value]
```

Overview

Use this command to update LDAP configurations.

Options

Option	Optional or Required	Default Value	Description
<code>-c value</code> <code>--configuration=value</code>	Optional	configuration.xml	The path to the server configuration file.
<code>-b value</code> <code>--bootstrap-config=value</code>	Optional	none	The path to the bootstrap configuration file. See Bootstrap.xml file for more information about this file.
<code>--id=value</code>	Required	none	Specifies the identifier for the LDAP configuration to be updated.
<code>-t value</code> <code>--type=value</code>	Optional	none	<p>The type of LDAP server. The following names are valid types:</p> <ul style="list-style-type: none"> • ActiveDirectory • SunOne • SunJavaSystem • Custom <p>When you specify any of the first three types, a type-specific configuration template is automatically applied in runtime so that the most fundamental configuration options are configured automatically.</p> <p>When you specify a Custom LDAP server type, there is no such configuration template and all those configuration options must be specified explicitly. When a custom LDAP configuration is to be used for authentication or with the user directory LDAP provider, the <code>--user-search-filter</code> and <code>--user-name-attribute</code> arguments must be specified. For such an LDAP configuration to be used for group synchronization, additional parameters must also be specified when running the config-ldap-group-sync command. See the help topic for that command for more information.</p>

Option	Optional or Required	Default Value	Description
<code>-s value</code> <code>--servers=value</code>	Optional	none	<p>Specifies a whitespace-separated list of LDAP server URLs. An LDAP server URL has the format <protocol>://<server>[:<port>]:</p> <ul style="list-style-type: none"> • <protocol>: Either LDAP or LDAPS • <server>: The fully qualified DNS name of the LDAP server. • <port>: (Optional) Number indicating the port number the LDAP service is listening on. When using the LDAP protocol, the port number defaults to 389. When using the LDAPS protocol, the port number defaults to 636. Active Directory LDAP servers also provide a Global Catalog containing forest-wide information, instead of domain-wide information only. The Global Catalog LDAP service by default listens on port number 3268 (LDAP) or 3269 (LDAPS). <p>Spotfire Server does not expect any search base, scope, filter or other additional parameters after the port number in the LDAP server URLs. Such properties are specified using other configuration options for this command.</p> <p>Examples of LDAP server URLs:</p> <ul style="list-style-type: none"> – LDAP://myserver.example.com – LDAPS://myserver.example.com – LDAP://myserver.example.com:389 – LDAPS://myserver.example.com:636 – LDAP://myserver.example.com:3268 – LDAPS://myserver.example.com:3269

Option	Optional or Required	Default Value	Description
<code>--clear-context-names</code>	Optional	none	Clears context names from the LDAP configuration. This argument can be used together with the <code>--context-names</code> argument to remove all old context names before adding the new.
<code>-n value</code> <code>--context-names=value</code>	Optional	none	<p>A list of distinguished names (DNs) of containers holding LDAP accounts to be visible within Spotfire Server. When specifying more than one DN, the DN's must be separated by pipe-characters (). The specified context names are added to the context names that are already configured. To set the context names from scratch, use the <code>--clear-context-names</code> argument with the <code>--context-names</code>.</p> <p>If the specified containers contain a large number of users, of which only a few should be visible in Spotfire Server, a custom user search filter can be specified to include only the designated users (see the <code>--user-search-filter</code> argument).</p> <p>Examples:</p> <ul style="list-style-type: none"> • CN=users,DC=example,DC=com • OU=project-x,DC=research,DC=example,DC=com

Option	Optional or Required	Default Value	Description
<u>-u value</u> <u>--username=value</u>	Optional	none	<p>The name of the LDAP service account to be used when searching for users (and optionally also groups) in the LDAP server. This service account does not need to have any write permissions, but it needs to have read permissions for all configured context names (LDAP containers). For most LDAP servers, the account name is the account's distinguished name (DN). For Active Directory, the account name can also be specified in the forms ntdomain\name and name@dnsdomain.</p> <p>Examples:</p> <ul style="list-style-type: none"> • CN=spotsvc,OU=services,DC=research,DC=example,dc=COM • RESEARCH\spotsvc (Active Directory only) • spotsvc@research.example.com (Active Directory only)
<u>--password=value</u>	Optional	none	The password for the LDAP service account.

Option	Optional or Required	Default Value	Description
<code>--schedules=value</code>	Optional	none	<p>A comma-separated list of schedules for when the LDAP synchronization should be performed. The schedules are given in a cron-compatible format, where each schedule consists of either five fields or one shorthand label. Make sure to enclose the value in double quotes. The specified schedules are added to the schedules that are already configured. To set the schedules from scratch, use the <code>--clear-schedules</code> argument with the <code>--schedules</code>.</p> <p>The five fields are, from left to right, with their valid ranges: minute (0-59), hour (0-23), day of month (1-31), month (1-12) and day of week (0-7, where both 0 and 7 indicate Sunday). A field can also be configured with the wildcard character *, indicating that any moment in time matches this field. A group synchronization is triggered when all fields match the current time. If both day of month and day of week have non-wildcard values, then only one of them has to match.</p> <p>There are also the following shorthand labels that can be used instead of the full cron expressions:</p> <ul style="list-style-type: none"> • <code>@yearly</code> or <code>@annually</code>: run once a year (equivalent to <code>0 0 1 1 *</code>) • <code>@monthly</code>: run once a month (equivalent to <code>0 0 1 * *</code>) • <code>@weekly</code>: run once a week (equivalent to <code>0 0 * * 0</code>) • <code>@daily</code> or <code>@midnight</code>: run once a day (equivalent to <code>0 0 * * *</code>) • <code>@hourly</code>: run once an hour (equivalent to <code>0 * * * *</code>) • <code>@minutely</code>: run once a minute (equivalent to <code>* * * * *</code>) • <code>@reboot</code> or <code>@restart</code>: run every time Spotfire Server is started <p>Refer to the Wikipedia overview article on the cron scheduler.</p>

Option	Optional or Required	Default Value	Description
<code>--clear-schedules</code>	Optional	none	Clears from the LDAP configuration the LDAP synchronization schedules. This argument can be used together with the <code>--schedules</code> argument to remove all old schedules before adding the new.

Option	Optional or Required	Default Value	Description
<code>--user-search-filter=value</code>	Optional; must be specified for custom LDAP configurations, either when running this command or the create-ldap-config command. (The parameter is required for all custom configurations.)	For Active Directory servers, the parameter value defaults to '(&(objectClass=user)!(objectClass=computer)))' For any version of the Sun Directory Servers, it defaults to <code>objectClass=person</code> .	<p>Specifies an LDAP search expression filter to be used when searching for users.</p> <p>If only a subset of all the users in the specified LDAP containers should be allowed access to Spotfire Server, a more detailed user search filter can be used. The search expression can, for example, be expanded so that it also puts restrictions on which groups the users belong to, or which roles they have.</p> <ul style="list-style-type: none"> For Active Directory servers, access can be restricted to only those users belonging to a certain group by using a search expression with the pattern <code>&(objectClass=user)(memberOf=<groupDN>)</code>, where <code><groupDN></code> is 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 <code>&(objectClass=user)((memberOf=<firstDN>)(memberOf=<secondDN>))</code>. Add extra <code>(memberOf=<groupDN>)</code> sub-expressions as needed. <p>Active Directory example: <code>&(objectClass=person)(isMemberOf=cn=project-x,dc=example,dc=com)</code></p> <ul style="list-style-type: none"> 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 <code>&(objectClass=person)(isMemberOf=<groupDN>)</code>. If the users are divided among multiple groups, use the pattern <code>&(objectClass=person)((isMemberOf=<firstDN>)(isMemberOf=<secondDN>))</code>. Add extra <code>(isMemberOf=<groupDN>)</code> sub-expressions as needed. <p>Sun Java System Directory Server example: <code>&(objectClass=person)(isMemberOf=cn=project-x,dc=example,dc=com)</code></p>

Option	Optional or Required	Default Value	Description
			<ul style="list-style-type: none"> 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 <code>&(objectClass=person)(nsRole=<roleDN>)</code>. If multiple roles are of interest, use the pattern <code>&(objectClass=person)((nsRole=<firstDN>)(nsRole=<secondDN>))</code>. Add extra <code>(nsRole=<roleDN>)</code> sub-expressions as needed. <p>Sun ONE Directory Servers example: <code>&(objectClass=person)(isMemberOf=cn=project-x,dc=example,dc=com)</code></p> <p>The syntax of LDAP search expression filters is specified by the RFC 4515 document. Consult this documentation for information about more advanced filters.</p>
<code>--user-name-attribute=value</code>	Optional; must be specified for custom LDAP configurations, either when running this command or the create-ldap-config command.	<p>For Active Directory servers the value defaults to <code>sAMAccountName</code>.</p> <p>For a Sun Java System Directory Server (or any older Sun ONE Directory Server or iPlanet Directory Server) with a default configuration, it defaults to <code>UID</code>.</p>	Specifies the name of the LDAP attribute containing the user account names.

Option	Optional or Required	Default Value	Description
<code>--authentication-attribute=value</code>	Optional; should be used only for advanced setups. It is not set by default.	none	<p>Specifies the name of the LDAP attribute containing a user identity that can be used for binding (authenticating) to the LDAP server. This attribute fills no purpose in most common LDAP configurations, but can be useful in more advanced setups, where the distinguished name (DN) does not work for authentication, or where users should be able to log in using a username that does not map directly to an actual LDAP account.</p> <p>When setting up SASL with DIGEST-MD5 in an Active Directory environment, the DN does not work for authentication and the <code>userPrincipalName</code> attribute must be used instead. The <code>--authentication-attribute</code> argument should then be set to <code>userPrincipalName</code> and the <code>--user-name-attribute</code> argument should be set to <code>sAMAccountName</code> (the latter value also happens to be the default value for an Active Directory LDAP configuration, so there's no need to set it explicitly). See also the <code>--security-authentication</code> argument.</p> <p>When setting up SASL with GSSAPI in an Active Directory environment, the DN does not work for authentication and the <code>sAMAccountName</code> or <code>userPrincipalName</code> attribute must be used instead. The <code>--authentication-attribute</code> argument should then be set to <code>sAMAccountName</code> or <code>userPrincipalName</code> and the <code>--user-name-attribute</code> argument should be set to <code>sAMAccountName</code> (the latter value also happens to be the default value for an Active Directory LDAP configuration, so there is no need to set it explicitly). See also the <code>--security-authentication</code> argument.</p> <p>Example: By setting the <code>--user-name-attribute</code> argument to <code>cn</code> and the <code>--authentication-attribute</code> argument to <code>userPrincipalName</code> in an Active Directory environment, the users can log in to Spotfire Server</p>

Option	Optional or Required	Default Value	Description
			using their CN attribute values, but underneath the hood, Spotfire Server actually uses the userPrincipalName attribute value of the LDAP account with the matching CN for the actual authentication.

Option	Optional or Required	Default Value	Description
<code>--security-authentication=value</code>	Optional; should be used only in advanced setups.	simple	<p>This parameter specifies the security level to use when binding to the LDAP server.</p> <ul style="list-style-type: none"> To enable anonymous binding, it should be set to <code>none</code>. To enable plain username/password authentication, it should be set to <code>simple</code>. To enable SASL authentication, it should be set to the name of the SASL mechanism to be used, for example <code>DIGEST-MD5</code> or <code>GSSAPI</code>. Use multiple <code>-C</code> arguments to set the additional JNDI environment properties that the SASL authentication mechanism typically requires. <p>When setting up SASL with <code>DIGEST-MD5</code> in an Active Directory environment, all accounts must use reversible encryption for their passwords. This is typically not the default setting for the domain controller. The <code>--authentication-attribute</code> argument must also be used to specify the <code>userPrincipalName</code> attribute for the actual authentication to work correctly.</p> <p>When setting up SASL with <code>GSSAPI</code> in an Active Directory environment, the <code>--authentication-attribute</code> argument must be used to specify either the <code>sAMAccountName</code> or the <code>userPrincipalName</code> attribute and the custom property <code>kerberos.login.conf-text.name</code> must be mapped to the JAAS application configuration <code>SpotfireGSSAPI</code>. This in turn requires a fully working Kerberos configuration file at <code><installation dir>/jdk/jre/lib/security/krb5.conf</code>.</p>
<code>--referral-mode=value</code>	Optional	follow	<p>Specifies how LDAP referrals should be handled. Valid arguments are <code>follow</code> (automatically follow any referrals), <code>ignore</code> (ignore referrals), and <code>throw</code> (fail with an error).</p>

Option	Optional or Required	Default Value	Description
<code>[--referral-mode-root-dse=value]</code>	Optional	If not explicitly set, the value for <code>--referral-mode</code> is used.	<p>Specifies how LDAP referrals should be handled when looking up the RootDSE. Valid arguments are:</p> <ul style="list-style-type: none"> • follow (automatically follow any referrals) • ignore (ignore referrals) • throw (fail with an error)
<code>--request-control=value</code>	Optional	probe	<p>Determines the type of LDAP controls to be used when executing search queries 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, because it provides the most efficient way of retrieving the query result set. The virtual list view control can also be used for the same purpose if the paged results control is not supported. The virtual list view control is automatically used together with a sort control. Both the paged results control and the virtual list view control supports a configurable page size, set by the <code>--page-size</code> argument.</p> <ul style="list-style-type: none"> • To explicitly configure the server for probing, set the argument value to probe. • To configure the server for the paged results control, set the argument value to PagedResultsControl. • To request the virtual list view control, set the argument value to VirtualListViewControl. • To completely disable request controls, set the argument value to none.

Option	Optional or Required	Default Value	Description
<code>--page-size=value</code>	Optional	The page size value defaults to 2000 for both the paged results control and the virtual list view control.	Specifies the page size to be used with the paged results control or the virtual list view control when performing search queries to the LDAP server
<code>--import-limit=value</code>	Optional	unlimited	Specifies a threshold that limits the number of users that can be imported from an LDAP server to Spotfire Server in one query. This can be used to prevent accidental flooding of the Spotfire Server user directory when integrating with an LDAP server with tens or even hundreds of thousands of users. By setting an import limit, the administrator can be sure that an unexpected high number of users does not affect the server performance. 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.
<code>--user-display-name-attribute=value</code>	Optional	none	Specifies the name of the LDAP attribute containing the user display names.
<code>--group-display-name-attribute=value</code>	Optional	none	Specifies the name of the LDAP attribute containing the group display names.

Option	Optional or Required	Default Value	Description
<code>-Ckey=value</code>	Optional	none	<p>Specifies additional JNDI environment properties to be used when connecting to the LDAP server. Note that it does not add to the previously configured custom properties; it replaces them completely. If you want to keep any of the old custom properties, make sure to specify them once again when adding new ones. This option can be specified multiple times with different keys.</p> <p>Example: The equivalent of specifying the <code>--security-authentication=DIGEST-MD5</code> argument is - <code>Cjava.naming.security.authentication=DIGEST-MD5</code> .</p> <p>Example: Updating the context names <code>update-ldap-config --id="ldap1" --context-names="OU=project-x,DC=research,DC=example,DC=com OU=phbs,DC=management,DC=example,DC=com"</code></p>
<code>-Rvalue</code>	Optional and may be specified multiple times with different values.	If this argument is not specified, the Java defaults are used.	<p>Specifies the protocols to be used for LDAPS when connecting to the LDAP server.</p> <p>Example: To enable only TLSv1.2 <code>-RTLSv1.2</code></p>
<code>-Svalue</code>	Optional and may be specified multiple times with different values.	If this argument is not specified, the Java defaults are used.	<p>Specifies the cipher suites to be used for LDAPS when connecting to the LDAP server.</p> <p>Example: To enable only these two cipher suites</p> <pre>- STLS_DHE_RSA_WITH_AES_128_GCM_SHA256 - STLS_DHE_RSA_WITH_AES_256_GCM_SHA384</pre>

Option	Optional or Required	Default Value	Description
<code>--connection-timeout=value</code>	Optional	no timeout (see description)	Specifies the connection timeout. The value must be a non-negative integer representing the timeout in milliseconds. A value less than or equal to zero results in no timeout, effectively waiting until the connection times out on TCP network level.
<code>--read-timeout=value</code>	Optional	no timeout (see description)	Specifies the read timeout. The value must be a non-negative integer representing the timeout in milliseconds. A value less than or equal to zero results in no timeout, effectively waiting until the connection times out on TCP network level.

version

Displays the current version of the server.

```
version
```

Overview

Use this command to display the current version of the server.

Glossary

Deployments & Packages

deployment area

Deployment areas, which are set up by the Spotfire administrator, make it possible to give different users access to different versions of the Spotfire client, while still using a single Spotfire Server.

distribution

A collection of one or more software packages. The contents of a distribution are distributed to each end user's desktop using the deployment mechanism. A distribution is deployed to a deployment area.

Nodes & Services

node manager

The node manager is the networked software agent that is responsible for managing a set of services on a specific physical or virtual host. This software makes it possible to execute remote commands from the Spotfire Server.

node

All the services and instances that are run by a particular *node manager*.

service

An application that runs on a node manager and provides a particular capability; in the current version of Spotfire Server, Spotfire Web Player and Spotfire Automation Services are the available services. A service is not available to end users until a *service instance* is running.

service instance

A specific realization of a service that is available to Spotfire end users. For example, when a user opens an analysis in the Spotfire Web Player, the user is accessing a particular instance of the Web Player service. (This distinction is invisible to the user.)

resource pool

A set of specific Spotfire Web Player *service instances* (or a single instance) that can be used in a routing rule to define where a given file, or a file requested by a specific user, should preferably open. For example, a rule can specify that company VIPs always view analyses in a particular resource pool.

Scheduling & Routing

rules

There are three types of rules: **File**, **Group**, and **User**.

The Spotfire administrator creates rules to do one of the following:

- Schedule updates to analyses (type of rule = **File**).
- Specify resource pools on which to open analyses that are requested by specific users or members of specific groups (type of rule = **User** or **Group**).
- Specify resource pools on which to open specific analyses (type of rule = **File**).

scheduled update

A rule that sets a schedule for automatically adding fresh data to an existing analysis. The rule also indicates the resource pool on which the analysis should open (Type of rule=**File**).

routing rule

A rule that specifies the resource pool on which an analysis should preferably open.

Users & Groups

primary group

The primary group is the group that determines which licenses and settings apply for a user who belongs to two or more groups.

Miscellaneous

information link

An information link is a structured request for data. Users can create information links to connect to external JDBC databases and thereby access and load data into Spotfire analysis files. Information links and the elements they are created from are stored in the Spotfire database.

license

Licenses determine which features and functionality a user has access to when working in Spotfire. Administrators set licenses at the group level, using the Administration Manager in Spotfire Analyst.

post-authentication filter

The Spotfire Server filter that can either block all users who try to log in but are not already present in the user directory, or automatically create a new account in the user directory for any user who logs in to the server for the first time. It is also possible to use the Spotfire Server api to create a custom post-authentication filter.

preferences

Preferences are default settings for the way that people work, and the analyses they create. Preferences include a wide range of properties, from which toolbars are visible when the user starts Spotfire to the look of tables in visualizations. Administrators set preferences at the group level, using the Administration Manager in Spotfire Analyst.