TIBCO Spotfire® Server Release Notes

Software Release 10.8
Document Updated: February 2020

TIBCO®

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.

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.

Contents

TIBCO 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 Documentation

Documentation for Spotfire Server and related products is available on the Spotfire Server Product Documentation page.

The following documents relevant for this product can be found on the Spotfire Server Documentation site:

- *TIBCO Spotfire® Server and Environment - Quick Start*
- *TIBCO Spotfire® Server and Environment - Installation and Administration*
- *TIBCO Spotfire® Server and Environment Security*
- *TIBCO Spotfire® Server Release Notes*
- *TIBCO Spotfire® Business Author and TIBCO Spotfire® Consumer Release Notes*
- *TIBCO Spotfire® Business Author and Consumer User's Guide*
- *TIBCO Spotfire® Cobranding*
- *TIBCO Spotfire® Qualification Installation and Configuration Manual*
- *TIBCO Spotfire® Qualification User's Guide*
- *Deploying and Using a TIBCO Spotfire® Language Pack*
- *TIBCO Spotfire® Automation Services User's Guide*
- *TIBCO Drivers® - Connecting to an ODBC Data Source Using Spotfire® Analyst*
- *TIBCO Spotfire® Automation Services API Reference*
- *TIBCO Spotfire® Automation Services REST API Reference*
- *TIBCO Spotfire® Server Information Services API Reference*
- *TIBCO Spotfire® Server Library REST API Reference*
- *TIBCO Spotfire® Server Platform API Reference*
- *TIBCO Spotfire® Server Web 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.

TIBCO Spotfire Server Release Notes

The release notes for this product version are provided to inform you of new features, known issues, and issues from previous releases that have been closed.

These release notes are for TIBCO Spotfire® Server version 10.8. They cover Microsoft Windows and Linux installations.

These release notes also cover the Right to Use (RTU) products TIBCO Spotfire® Automation Services and TIBCO Spotfire® Qualification.

Spotfire® Server is a Tomcat web application that runs on Windows and Linux operating systems. It is the administrative center of any TIBCO Spotfire® implementation. In addition to providing the tools for configuring and administering the Spotfire® environment, Spotfire Server facilitates the services that make it possible for users to access, blend, and visualize their data, creating analyses that provide actionable insight.

New Features

The following new features have been added to version 10.8 of TIBCO Spotfire® Server.

What's new in 10.8.1 of Spotfire® Server

New requirements for communication to the Active Directory server

With the Microsoft advisory *ADV190023 | Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing*, new requirements for communication to the Active Directory (AD) server will be introduced. If you use AD server with LDAP, see the section Changes in Functionality for detailed instructions.

What's new in 10.8.0 of Spotfire® Server

SameSite configuration property

Spotfire Server has a configuration property for controlling the `SameSite` cookie attribute for cookies generated by the Spotfire Server.

You might need to change this value in scenarios where the Spotfire Server cookies are used as third party cookies. For example, when using the TIBCO Spotfire JavaScript API. Use the server command-line configuration tool to specify the property.

Example:

```
config export-config --force
config set-config-prop --name="security.cookies.same-site" --value="None"
config import-config -c "Cookies SameSite=None"
```

Valid values for the property are:

- `None`
- `Lax`
- `Unset`

The default is `Unset`, which is a special Tomcat value, and which preserves previous behavior.

The values `None` and `Lax` are defined by rfc6265bis.

Improvements to simplify the server upgrade process with the upgrade tool

The Spotfire® Server upgrade tool has the following improvements.

- Preserves previously configured Java memory properties (JvmMs and JvmMx) within `setenv.sh/setenv.bat`.
- Detects unsupported database versions.
- Detects incompatible driver versions.
- Implements a trust store that supports multiple trust stores. This way, each server to be trusted can have a trust store, separate from the one included with the JRE, which can easily be transferred during upgrades.

Seamless session fail-over

In a Spotfire Server cluster, any server can be taken offline, and all users currently connecting through that server can seamlessly continue their session (through load-balancer rerouting) on another server without re-authenticating. Also, all running analysis sessions in the Spotfire® Web Player can continue without losing their current state.

Improvements to troubleshooting bundle output

The file `routing_rules.txt` in the troubleshooting bundle now includes a new a column, `capability`. This column specifies the type of rule as either `WEB_PLAYER` for Scheduled Update (SU) jobs or `AUTOMATION_SERVICES` for Automation Services (AS) jobs.

New log entry: Create Web Analysis

The log `WebAuditLog` now includes the log entry `Create Web Analysis`. This entry makes it easier to follow analysis life cycles.

Improved library RSS feed

For each analysis, the library RSS feed now provides a link to a page where the user can select to either download the analysis or open the analysis.

Added support for initiating OpenID Connect login from a third party

The OpenID Connect specification describes an optional feature through which a third party (such as an Identity Provider or a portal of some sort) can initiate login on a Service Provider. Examples of third-party Identity Providers are Google, Azure AD, Okta, and so on. See ThirdPartyInitiatedLogin in the *OpenID Connect Core specification* for more information.

Finer control of library items

Direct downloads of library items (through web links) can now be disabled by setting the configuration property `library.direct-downloads.enabled` to `false`.

It is still possible to open files in the Spotfire® Analyst and such even when the property is set to `false`.

New configuration arguments

The configuration scripts file is a normal text file that can include configuration commands and arguments. This version of TIBCO Spotfire Server includes two new arguments.

- Use `-E` to set environment variables.
- Use `-F` to specify that the execution of the script file should fail if an undefined variable is found.

You can specify arguments in the script file in the command `config run <script filename>`. Alternatively, you can set the arguments from the command line using `-Vkey=value`.

For details about new Spotfire features, see What's New in TIBCO Spotfire in the TIBCO Community.

Changes in Functionality

This section describes changes in functionality for this release of Spotfire Server

New requirements for communication to the Active Directory server

With the Microsoft advisory *ADV190023 | Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing*, new requirements for communication to the Active Directory server will be introduced. You can avoid these new requirements by changing certain registry settings on the Active Directory servers. Otherwise, communication between Spotfire Server and the Active Directory servers must use SSL. They should use the LDAPS protocol, and the URI scheme in the configuration should be changed from `LDAP` to `LDAPS`.

Certificates for SSL communication

When a communication is made over SSL, the issuer of the certificate is verified by Spotfire Server. If it is an officially issued certificate, the communication works without changes. In the bundled Java, the following file contains official root certificates:

```
<installation root>/jdk/jre/lib/security/cacerts
```

If a bespoke certificate needs to be issued, then the certificate chain is not to one of these official root certificates. Instead, Spotfire Server must be told to trust this certificate. For earlier releases of Spotfire Server, the only way to make this possible was to import the new certificate into the above-mentioned file, `cacerts`. This method is described in the manual and can still be used.

To facilitate the use of bespoke certificates, you can now use an alternative, easier method, which is described in this section.

Every SSL certificate that is to be trusted can have its own keystore file (in Java Keystore-format, with the suffix `jks`). These files should be placed in the directory *<installation root>*`/tomcat/certs`.

From Spotfire Server 10.3.0 and later, the contents of this directory is copied during an upgrade.

The same password (default `changeit`) is used for the file `cacerts` as for any extra keystore file in `tomcat/certs`. If you must change this password, then you should change the password for all files, including the file `cacerts`.

It is not the private certificate that is needed in these files, so changing the password is not critical, because anyone who can connect to the server can retrieve the public certificate.

The file `cacerts` has the default password `changeit`, and it is assumed that the extra keystore files have the same password. If you must set a new password, the Java startup parameter `javax.net.ssl.trustStorePassword` should be added, either to the start script or to the service. Depending on how Spotfire Server is started, this new password must be set in start scripts or as a parameter for the Windows parameter. For more information on performing this task, in *TIBCO Spotfire® Server and Environment - Installation and Administration* , review the section on changing memory settings. (The steps are the same, even though here it is a startup parameter and not a memory setting.)

Retrieve and create a JKS-file

Below are some hints on how to create a JKS-file. This information works for both Linux and Windows.

Use the forward slash for Linux and the backslash for Windows.

This method works for Spotfire Server version 7.11.10, version 10.3.7, and version 10.6 and later.

The following example shows how to get the certificate for the server *foo.company.com*, which has LDAPS enabled and listens on port 636.

To get the needed certificates installed on Spotfire Server, in the following example, change *foo.company.com* to the server name from which you want to get the certificate, and change *-alias foo* to the alias that should receive the certificate in the keystore. You can run this command toward several servers, and the certificates will be imported and appended to the keystore *trust_foo.jks*, or you can create a new one for each server.

```
<installation root>/jdk/jre/bin/keytool -printcert -sslserver
foo.company.com:636 -rfc | <installation root>/jdk/jre/bin/keytool
-import -noprompt -alias foo -keystore "<installation root>/tomcat/certs/
trust_foo.jks"
-storepass changeit -storetype jks
```

Any readable file with the suffix `jks` should be picked up by the server and the CLI tools.

The relocatable, remote CLI tool does not pick up certificates using this method.

Importing to the cacerts file within the JDK installation

The following command is the only option available for versions of Spotfire Server earlier than version 10.6, except for version 7.11.10 and version 10.3.7.

```
<installation root>/jdk/jre/bin/keytool -printcert -sslserver foo.company.com:636
-rfc | <installation root>/jdk/jre/bin/keytool -import -noprompt -alias foo
-keystore "<installation root>/jdk/jre/lib/security/cacerts" -storepass changeit
-storetype jks
```

The relocatable, remote CLI tool does not pick up certificates installed on the Spotfire Server.

Deprecated and Removed Features

The demodata package is no longer bundled in the Spotfire Server installation.

Migration and Compatibility

Spotfire Server version 10.8 contains detailed instructions for migrating from a previous release.

Spotfire Server

See "Upgrading Spotfire" in the Spotfire Server and Environment - Installation and Administration help.

As of Spotfire Server version 10.3.0, server hotfixes can be applied only on the specific service pack version that they were created for. Example: If you currently have version 10.3.1, you can apply server hotfixes only for the 10.3.1 version, such as 10.3.1 HF-001, 10.3.1 HF-002, and so on. If you want a hotfix of a different service pack level, such as 10.3.2 HF-001, you must first make sure to upgrade to that service pack (10.3.2) before applying the hotfix.

Newer and older versions of Spotfire Analyst client can be used to connect to the current version of Spotfire Server in order to upgrade or downgrade the client packages. However, it is recommended to always run the same version of client and server in production environments. See System Requirements.

Spotfire Automation Services

For instructions on how to upgrade to version 10.8 Spotfire Automation Services, see "Updating Services" in the *Spotfire Server and Environment - Installation and Administration* help.

There were major architectural changes introduced in version 7.5.0. If you are upgrading from a version earlier than 7.5.0, refer to the *Spotfire Automation Services 7.5.0 Release Notes* for more information.

Spotfire Qualification

Version 10.8 of Spotfire Qualification should be installed for compatibility with version 10.8 of TIBCO Spotfire.

For instructions on how to upgrade to version 10.8 of Spotfire Qualification, see the Spotfire Qualification - Installation Guide.

Third Party Software Updates

The following third party software (TPS) components have been added or updated for Spotfire Server version 10.8.

10.8.1, February 2020

TPS	New Version
Apache CXF dependencies	3.3.5
Quartz Enterprise Job Scheduler	2.3.2
Progress DataDirect Connect for JDBC SQL Server Driver	6.0.0.263
Spring Framework	5.2.3

10.8.0, February 2020

TPS	New Version
Amazon Redshift JDBC driver	1.2.37.1061
Angular JS	1.7.9
ASM	7.1
AWS SDK for Java	2.10.33
Apache CXF dependencies	3.3.4
Apache Log4j	2.12.1
Apache Log4j - jul	2.12.0 (New)
Apache Tomcat	9.0.30
Byte Buddy	1.10.5
Jetty	9.4.24.v20191120
MyBatis	3.5.3
MyBatis-Spring	2.0.3

TPS	New Version
Oracle Server JRE	8u241
PostgreSQL JDBC driver	42.2.9
RSyntaxTextArea	3.0.4
Simple Logging Facade for Java - api	1.7.29
Spring Framework	5.2.2

Closed Issues

The following table lists important closed issues in version 10.8 of Spotfire Server.

Spotfire Server 10.8.1, February 2020

Key	Summary
TSS-26590	Improved the logging when inaccessible referrals are encountered during LDAP searches.
TSS-26593	An analysis in Spotfire Web Player failed to trust scripts or queries if the analysis contained a large number of scripts or queries. This issue has been fixed.
TSS-26660	Scheduling and Routing Saved Schedules did not display the correct checked days between sessions.

Spotfire Server 10.8.0, February 2020

Key	Summary
TS-62055	Cancelling a login attempt and then switching between different servers in Spotfire Analyst could sometimes result in an exception and a failed login attempt. This issue has been resolved.
TSS-23526	The `import-rules` command in the CLI now includes the argument `-i`, `--ignore-unavailable-files`. This option specifies ignoring creating rules when library items are invalid.
TSS-24541	Previously, the Scheduled Update cache would clear in less than the specified time if the update was triggered externally using UpdateAnalysisService web service. This issue has been fixed.
TSS-26096	When a user saves an analysis to a new folder in the library, or copies or moves items to a new folder using the library browser, the user no longer has to navigate to the new folder. The new folder in the library is now displayed.
TSS-26150	In some cases, for a failed scheduled update, the end time did not reflect the time of the failure. This issue has been fixed.

Key	Summary
TSS-26212	In some cases, a cancelled scheduled update would not successfully complete its unload process. This problem caused a failure to launch a new scheduled update. This issue has been fixed.
TSS-26226	Previously, the `find-analysis-scripts` command would not list files that contained inline scripts but no other scripts, data functions, or custom queries. It now lists those files.
TSS-26228	A missing JDBC driver can no longer block the creation of a Troubleshooting Bundle.
TSS-26283	Output was missing from the upgrade tool due to the process ending before the output pipe was read. An improvement to the reader was added such that the error and output (if any present) should be gathered and displayed/logged.
TSS-26296	The documentation was unclear regarding not installing TIBCO® Enterprise Runtime for R - Server Edition on the same node or computer as other services, such as Spotfire Web Player. This issue has been clarified.
TSS-26308	Previously, when the user imported an Information Services data source with a cached information link containing a cache validation query, and if the data source changed ID (due to conflicts) during the import, then the reference from the cache validation query was not remapped properly. This issue has been fixed.
TSS-26443	In some cases, a scheduled update that had been deleted could stay in the cache, resulting in a SQL exception in the cleanup. This issue has been fixed.

Known Issues

The following table lists known issues in version 10.8 of Spotfire Server.

Key	Summary
TSS-21408	In Spotfire environments with an Oracle database, Spotfire occasionally uses more cursors than are available. This can occur in a variety of situations, but in all cases the following error appears in the server log: `ORA-01000 maximum open cursors exceeded`, and the server stops functioning. Workaround: If this occurs, try setting the **`OPEN_CURSORS`** property in Oracle to at least 500, and then restart the server.
TSS-23602	In the Automation Services area of the administration interface, if an Automation Services job is in the IN_PROGRESS state, and all of the servers in the cluster stop running or are restarted, the job will remain in the IN_PROGRESS state in the Activity view even after the servers are back online. Workaround: Clear the job activity from the Activity view by right-clicking the activity and then clicking **Clear selected activity**.

Key	Summary
none	If your Spotfire implementation uses Web authentication through OpenID Connect or custom web authentication, Spotfire Package Builder cannot be used to deploy extensions to the server. Workaround: Deploy the extension package by using the Deployments & Packages area of Spotfire Server.
TS-58033	In the following situation, Spotfire users cannot view certain analysis files in the web client: • The user is authenticated using Kerberos with delegation. • The user wants to view an analysis that accesses a TERR node. Workaround: Give Read permission for the private key of the Web Player Node certificate to users. Procedure: 1. On the computer running the Web Player node manager, open a command window as an administrator. 2. Enter `mmc`. 3. In the Console dialog that opens, click **File** > **Add/Remove Snap-ins**. 4. In the Add or Remove Snap-ins dialog, select **Certificates** and click **Add**. 5. In the Certificates snap-in dialog, select **Computer account** and click **Next**. 6. In the Select Computer dialog, click **Finish**. 7. In the Add or Remove Snap-ins dialog, click **OK**. 8. In the Console Root window, click **Certificates (Local Computer)** to view the certificate stores for the computer. 9. Go to Certificates (Local Computer)\Personal\Certificates, and then right-click the certificate that was issued by "TIBCO Spotfire Signing CA". 10. Select **All Tasks** > **Manage Private Keys**. 11. In the Permissions dialog, under **Group or user names**, select a group that contains all Spotfire users that need to run analyses using the TERR service. 12. Under **Permissions for** ***Name***, select the **Allow** check box in the **Read** row, and then click **OK**. 13. In the Spotfire administration interface or in the Windows Services dialog, restart the Web Player node.
TS-62137	Python packages that are installed by the Administrator (through an SPK) take precedence over packages installed using the Python Tools from the Spotfire Analyst Tools menu. If users attempt to update a package previously installed by an SPK, then the package update is installed, but the update is ignored.