TIBCO Spotfire® Server Release Notes

Software Release 12.0 LTS (12.0.5)

Contents

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 12.0. They cover Microsoft Windows and Linux installations.

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 in version 12.0 of TIBCO Spotfire® Server.

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

Key	Version	Summary
TSS-32099	12.0.4	**Improved troubleshooting of sites and resource pools** Additional site and routing information for the resource pool has been added to the descriptive files in the troubleshooting bundle.
TSS-31887	12.0.3	**New cli command to delete Web Player state** The new cli command `delete-analysis-states` can be used to remove stale or unwanted personalized views for each web client user from analyses in the library.
SPOT-1491	12.0.0	**Spotfire library version history** It is now possible to utilize version history in the Spotfire library. With history enabled, you can view previous analysis versions and go to any previously-saved version (either to restore the version, or to save a previous version as a new file). For new installations, library version history is enabled by default and a new version is created each time a file is updated in the library. Version history is available, not only for analysis files, but for all visible Spotfire library items, like data sources, data functions, color schemes, SBDF files, mods, etc. As an administrator, you can disable version history entirely, or for certain item types only. You can view and manage the version history of a library item. From the **Library**, right-click the item and select **View version history**. From the Version history tab, you can delete, restore, or save a copy of a specific version. For easier identification of versions and for change management, you can add a version name and a comment for any specific version. **Note:** Each version is a complete copy of the item, not an incremental one. Depending on your Spotfire usage, the Spotfire storage (the Spotfire database or object storage) utilization might increase very fast (for example, if you have many users who frequently save their analyses with embedded data, or if you have frequently running Automation Services jobs). For such situations, automated pruning using the `delete-library-versions` command is strongly recommended. For TIBCO Cloud™ Spotfire®, all versions are kept at least 30 days. Non-named versions can be deleted after this period.
SPOT-1670	12.0.0	**Library compression** Library items imported into, or exported from, the Spotfire library are now compressed using the gzip format. This change provides more efficient use of library space, whether the library is stored in the Spotfire database or in an external storage mechanism. Library compression works with all supported databases.
TSS-30946	12.0.0	**Delete old versions from Library version history** It is possible to delete old library versions with the new command `delete-library-versions`. You can control whether you want to keep library item versions • with comments, • with names, • based on a specified library search expression for the keyword `created`. For example, newer than "a month ago" or "2 weeks ago", • by content size. For example, smaller than "500KB".

Key	Version	Summary
SPOT-1592	12.0.0	**TIBCO Spotfire Automation Services is supported on Linux** Debian 11 is now supported as the operating system for the TIBCO Spotfire Automation Services service. Note that ASP.NET Core Runtime 6 LTS is required when running on Linux. See also the System Requirements. **Known limitations** The following two job tasks are not supported on Linux: • Set Data Source Credentials • Set Credentials for External Connection See also Running Web Player or Automation Services on Linux.
SPOT-1657	12.0.0	**External actions using TIBCO Cloud Integration** The new feature lets you take action in your business systems directly from the visualizations. You can now trigger business processes, update databases, control Internet of Things devices and much more, without having to leave your Spotfire analysis. This is made possible by integrating with TIBCO Cloud™ Integration, TCI. TCI offers connectivity to a wide range of applications, databases and collaboration platforms, including custom applications reached by standard communication protocols. With a hybrid cloud architecture, actions can be used in any Spotfire environment, both in the cloud and on premises. This also applies to the systems that actions can integrate with. Actions are created with no-code user interfaces, both when building the integration apps in TIBCO Cloud Integration and when configuring them in Spotfire. A security mechanism is provided to protect your sensitive data. Before an action can be applied, it must be trusted, either by the person running the action, or indirectly by the administrator specifying action configurators as trusted signers. **Note:** External actions are not supported in the current versions of Spotfire mobile apps (TIBCO Spotfire® for Apple iOS 2.13.0 and TIBCO Spotfire® for Android 1.4.5).
SPOT-794	12.0.0	**TIBCO Spotfire Web Player is supported on Linux** Debian 11 is now supported as the operating system for the TIBCO Spotfire Web Player service. Note that ASP.NET Core Runtime 6 LTS is required when running on Linux. See also the System Requirements. **Known limitations** • Kerberos is not supported. • Some data connectors are not supported: Vertica, SAP, Oracle Essbase & Microsoft SQL Server Analysis Services (SSAS) • Windows Metafile formats (WMF & EMF) are not supported. See also Running Web Player or Automation Services on Linux.
SPOT-1460	12.0.0	**TIBCO Spotfire deployment in Kubernetes** As with previous Spotfire releases, you can create your own recipes for deploying TIBCO Spotfire® using containers and Helm charts on a Kubernetes cluster. Now, you can also use the recipes from Cloud Deployment Kit for TIBCO Spotfire® as they are, or as the reference starting point for your own recipes.

Key	Version	Summary
SPOT-1801	12.0.0	**New command for automating creation of the Spotfire database** You can now automate creating a Spotfire database with the command line command `create-db`. You can also automate creating the Spotfire action log database schema with the command line command `create-actionlogdb`. The commands `create-db` and `create-actionlogdb` work with all supported databases listed in the System Requirements. **Note**: As before, the Spotfire database, user, and schemas can be created with the provided database scripts. Now, you can also perform the same steps directly from the command line, without using the scripts.
TS-69136	12.0.0	**Read connector credentials profiles from files** It is now possible to read connector credentials profiles from files on the computer running the Worker host service. The directory containing the files is defined by the `DataAdapterCredentialsFilesDirectory` setting in `Spotfire.Dxp.Worker.Host.exe.config`.
TSS-26171	12.0.0	**Spotfire Server now supports a graceful shutdown from command line** You can now order a delayed or graceful shutdown of the Spotfire Server from the command line, which informs all back-end services that the instance should be considered off line and should not be used for new requests. Use the following syntax to perform a graceful shutdown from the command line: `/opt/tibco/tss/<version>/tomcat/spotfire-bin/graceful-shutdown.sh --minimum-draining-seconds=<minimum-period-seconds> --draining-timeout-seconds=<delay-seconds>` The command calls for a scheduled shutdown of the Spotfire Server with the specified delay `<delay-seconds>` in seconds. Use the argument `<minimum-period-seconds>` to prevent premature shutdowns. **Note:** Without support for draining front-end sessions in the load balancer/reverse proxy, front-end requests and session can still be disrupted. The health check URL responds with a 200 status and `DRAINING` in the response payload while the server is in this state.
TSS-28794	12.0.0	**The upgrade tool includes a lock to prevent simultaneous executions** The upgrade tool now includes a transient lock that prevents simultaneous executions of the upgrade. This lock is useful for scripted scenarios when running the upgrade tool in silent mode. The lock is valid for a short while (default 120 seconds) so that a later run of the execution should proceed, even if a first execution of the upgrade was terminated before the cleanup of the lock was executed.
TSS-29576	12.0.0	**Browser-based public API clients in OAuth2 Authorization Server** The built-in OAuth2 Authorization Server now supports browser-based public API clients (registered using the existing `register-api-client` command). The new type of client is primarily intended for use with the JavaScript API.
TSS-29923	12.0.0	**New data source template setting use-get-schemas** With this setting, Information Services data sources use the `getSchemas` function to fetch schemas instead of the `getTables` and `getProcedures` functions. The `getSchemas` function improves performance. However, it shows all schemas regardless of whether these schemas have tables/procedures. The `getSchemas` function is only available for JDBC versions 4.1 and later.

Key	Version	Summary
TSS-29966	12.0.0	**New details panel in the library view** You can now view more information about a selected item in the library by opening the details panel. The details are shown to the right of the table, after clicking the *Open details panel* icon above the table. Resize the panel by clicking and dragging the splitter left or right.
TSS-30476	12.0.0	**Copy item to other folder in the library** You can now copy library items into other folders in the library directly, by clicking **Copy** and navigating into the desired folder.
TSS-30502	12.0.0	**Spotfire Server now includes a system overview in Troubleshooting Bundle** The troubleshooting bundle now contains a new file, which provides a system overview of the Spotfire environment.
TSS-30528	12.0.0	**Silent update of the database only** When running the upgrade tool in silent mode you can now choose to update only the database. See the file `silent.properties` for details.
TSS-30619	12.0.0	**Edit a library item's description from the Library page** You can now edit the description of an item directly from the *Library* (*Browse*) web administration page by clicking the pen icon in the details panel.
TSS-30661	12.0.0	**New command for removing imported certificates** You can now use the command `remove-code-signing-root-certificate` to delete imported root certificates for code trust.
TSS-31203	12.0.0	**Create an action log database using the CLI** A new command, `create-actionlogdb`, has been added, which can make it easier to create the action log database in many cases. Use of this command does not require installation of the command line tools for the database. Instead, the command uses `jdbc` to connect to the database.
TSAS-1112	12.0.0	**Configurable file system path in Automation Services tasks** Automation Services tasks can now use a new substitution field, `exportPath`. During execution, the field is replaced by an actual path specified in the service configuration.
TSS-15985	12.0.0	**Better overview of ports** In the web administration *Nodes & Services, Network* page, you can now clearly see the purpose of the used ports (Communication port/Registration port) when viewing details about a node manager or a server.
TSS-8819	12.0.0	**More information in Deployments & Packages** In the Deployments & Packages, Deployment areas page, you can now also see a *Published by* column in the Software packages table.

Changes in Functionality

The following are important changes in functionality in version 12.0 of Spotfire Server.

Key	Version	Summary
TSS-31995	12.0.4	**Authentication flag for a Kerberos data source set to false** The authentication flag for a Kerberos data source is now set to false by default. With this change, if the user context is Kerberos, an Information Link does not prompt for credentials.
TSS-32069	12.0.4	**Disable digest verification** You can now disable digest verification for the Library contents.
TSS-31905	12.0.3	**The option `--testrun` is no longer available for Oracle databases** In the Upgrade Tool, the option `--testrun` is no longer available when you perform a full rollback of an Oracle database because it is not possible to perform a full rollback with the option enabled.
TSS-31674	12.0.2	**New rule defaults to lowest priority** In the *Scheduling & Routing* page, when creating a new rule, the default is now that the new rule gets the lowest priority instead of the highest (where 0 is the highest priority). This means that the new rule will show up at the bottom of your rules list, if no manual changes are done to the priority.
SPOT-1751	12.0.0	**Updated Spotfire artwork** The Spotfire icon and artwork have been updated in Spotfire 12.
SPOT-1757	12.0.0	**Updated requirements for PostgreSQL as the database** PostgreSQL 11 is no longer supported as the Spotfire database.
SPOT-1758	12.0.0	**Updated operating system requirements** Microsoft Windows Server 2012 and Microsoft Windows Server 2012R2 are no longer supported as the operating system for the following Spotfire products: • TIBCO Spotfire Server • TIBCO Spotfire Web Player • TIBCO Spotfire Automation Services • TIBCO Spotfire Statistics Services • TIBCO Enterprise Runtime for R - Server Edition • TIBCO Spotfire Service for Python • Citrix with TIBCO Spotfire® Analyst & Desktop • Remote Desktop Services with TIBCO Spotfire® Analyst & Desktop

Key	Version	Summary
SPOT-1790	12.0.0	**CentOS 8 is no longer supported as an operating system** CentOS 8 is no longer a supported operating system for the following Spotfire products. • TIBCO Spotfire® Server • TIBCO Spotfire® Statistics Services • TIBCO® Enterprise Runtime for R - Server Edition • TIBCO Spotfire® Service for Python
TSS-25117	12.0.0	**Search for both display name and username** When searching for users, the search query now automatically tries to match either the user's display name or username without having to toggle between the two.
TSS-30164	12.0.0	**Easier to edit rules** In the Scheduling & Routing Rules page, when editing a rule for an analysis, user or group, you can now browse for other analyses, users or groups directly by clicking the input and not only by clicking on the *Browse* button.
TSS-30215	12.0.0	**Changes in handling of trusted signers and items** When viewing information about trusted signers and items in the *My Account* page, or in the *Trusted signers and items* page for a specific user or group, you can now view and edit trusted certificates and users based on the role that the trust has been granted for: mod developer or action configurator. Where applicable, you can also view and edit trust for individually trusted visualization mods and action configurations.
TSS-30268	12.0.0	**Updated tables in the server web administration pages** • The tables in the Spotfire Server web administration pages now support selecting or clearing rows using the **Ctrl** and **Shift** keys. • Tables that support selection (i.e., where the rows have a check box) will now keep the selected rows when refreshing the data in the table. Previously, the selected rows were cleared upon refresh.
TSS-30572	12.0.0	**Changes to queue behavior for Automation Services instances and jobs** • Jobs in the (in-memory) queue are now processed according to `lastModified`. • By default, TIBCO Spotfire Automations Services jobs can now always be queued, even if no Spotfire Automation Services instances are installed. This change allows "scale to zero". To revert to the previous behavior, set the property `automation-services.compatibility.queue-when-no-services-deployed` to `false`. • Automation Services jobs are not assigned a destination until there is a destination with available slots. To revert to the previous behavior, where a job is assigned a destination when queued, set the property `automation-services.compatibility.assign-destination-before-queueing` to `true`. • Previously, EXHAUSTED Automation Services instances would continue to process jobs, but no new jobs were assigned to an exhausted instance. Now, exhausted instances no longer claim unassigned jobs in the queue. This means that queue processing of Automation Services jobs can stop if these instances cannot get out of the exhausted state. Therefore, if no automatic scaling is configured, you can instead set the property `automation-services.compatibility.claim-on-exhausted-instances` to `true`, to allow exhausted Automation Services instances to claim tasks.

Key	Version	Summary
TSS-30742	12.0.0	**Empty defaults for dump configuration on Windows** The `dumpToolPath`, and related flags, are now empty in the default configuration. Examples and instructions are available both in config file comments and in the Server and Environment - Installation and Administration manual. The reason for this change is because the old default values do not make sense for non-Windows platforms and that the Windows configuration will not work out-of-the-box anyway, because installation and path adjustments are usually needed.
TSS-31120	12.0.0	**Response validity time for OSCP increased** The default value of Online Certificate Status Protocol (OCSP) response validity has been increased from 60 seconds to 3600 seconds. This change addresses potential problems with network traffic and load.
TSS-31157	12.0.0	**New argument for delete-library-content** The command-line command `delete-library-content` has the new argument `-u | --username`, which accepts the user name of the library administrator.

Deprecated and Removed Features

Deprecated features

The table lists features that are deprecated and will be removed in a future release of Spotfire.

Key	Version	Summary
TSS-28133	12.0.0	The CLI parameter `-t` or `--tool-password` of the `s3-download` command is deprecated and will be removed in a future version. Using this parameter results in a warning message about the deprecation. Deprecated since Spotfire 11.4.0.
TSS-29565	12.0.0	The `getReturnEndpoint()` method of the `CustomWebAuthenticatorInitContext` API class is deprecated and will be removed in a future release. Please use the new method with the same name in the `WebAuthenticationContext` API class instead. Deprecated since Spotfire 11.6.0.
TSS-30402	12.0.0	In a future release an upgrade will be done to the namespaces defined in the Jakarta EE 9 project. If you have custom code deployed on the Spotfire server, this means that some of your code might need to be altered and rebuilt. Several important third party components are upgraded to use new namespaces defined in the Jakarta EE 9 project. A future release will start using these upgraded components. When using the upgraded components it is important to know that some, but not all, imports of `javax.` must be changed to `jakarta.`. For example, `javax.servlet.http.HttpServletRequest` must be changed to `jakarta.servlet.http.HttpServletRequest`. A list of components that will be changing namespace can be found here: https://wiki.eclipse.org/Jakarta_EE_Maven_Coordinates Deprecated since Spotfire 10.10.11, 11.4.6 & 11.8.0.
TSS-31202	12.0.0	The following API methods have been deprecated. They contain references to Java EE 8 and that will not work in a future version of TIBCO Spotfire Server based on the newer Jakarta EE 9 or later: • `Object AuthenticationContext.getAttribute(String name)`: The usage of the attribute name `javax.servlet.request.X509Certificate` is deprecated. The attribute name and the returned class type will both change to `jakarta.servlet.request.X509Certificate` in Jakarta EE 9 or later. • `Enumeration<String> getAttributeNames()`: The attribute name `javax.servlet.request.X509Certificate` is deprecated. It will change to `jakarta.servlet.request.X509Certificate` in Jakarta EE 9 or later. • `Cookie[] getCookies()`: The method is deprecated as the returned class type `javax.servlet.http.Cookie` will change to `jakarta.servlet.http.Cookie` in Jakarta EE 9 or later. Use the `String getHeader("Cookie")` method invocation instead. Deprecated since Spotfire 12.0.0.

Removed features

The following features have been removed in this version of Spotfire.

Key	Version	Summary
TSS-32172	12.0.4	**TIBCO ODBC drivers for Apache Spark SQL, Apache Cassandra, and MongoDB** The TIBCO Drivers package, which includes ODBC drivers for Apache Spark SQL, Apache Cassandra, and MongoDB, is removed. The drivers are no longer included with Spotfire. If you use any of these drivers for accessing data in Spotfire today, it is recommended that you use different drivers. As you prepare to migrate, you can continue using the TIBCO ODBC drivers that you have already downloaded, but no new versions will be released to address potential issues. **Migration instructions** The following are recommendations for how you can migrate to using a different driver. *Apache Spark SQL* To access data with the connector for Apache Spark SQL, install one of the other supported drivers. See the system requirements. • Install the new driver on all computers where you will access the data in Spotfire. You do not need to edit your data connections in Spotfire when you change drivers. *MongoDB* To access data from MongoDB in Spotfire, use the connector for MySQL with the ODBC driver for MongoDB Connector for BI. See the system requirements. 1. Install the MongoDB Connector for BI driver on all computers where you will access data from MongoDB in Spotfire. 2. In a Spotfire installed client, create a new data connection to your MongoDB data with the connector for MySQL (**Connect to > MongoDB Connector for BI**). Save the data connection to the library, for reuse in all your analysis files. 3. Open the analysis file you need to update. On the **Data canvas**, replace your old MongoDB data source with data from your new connection in the library. *Apache Cassandra* To access data from Apache Cassandra, you must use a different driver. 1. After installing the new driver, create a new DSN for the data you need to access. 2. Share the DSN, and install the driver, on all computers where you will access the data in Spotfire. 3. In a Spotfire installed client, open the analysis file you need to update. 4. On the **Data canvas**, replace your old Apache Cassandra data source, and use **Load data from ODBC, OLE DB, or ADO.NET data provider** to connect to your new Apache Cassandra data DSN.
TSS-31245	12.0.0	The API class `com.spotfire.server.security.AbstractPostAuthenticationFilter` is no longer supported.

Third Party Software Updates

The following third party software (TPS) components have been added or updated in version 12.0 of Spotfire Server.

Key	Version	Summary
TSS-32557	12.0.5	The following JDBC drivers have been updated: • Redshift JDBC driver to version 2.1.0.14 • Progress DataDirect Oracle driver to version 6.0.0.000977 • Progress DataDirect DB2 driver to version 5.1.4.000413 • Progress DataDirect MySQL driver to version 5.1.4.000266 • Progress DataDirect SQL Server driver to version 6.0.0.001071
TSS-32360	12.0.5	• Amazon AWS SDK updated to 2.20.61 • Apache Commons FileUpload updated to 1.5 • Apache Log4j2 updated to 2.20.0 • Apache Tomcat updated to 9.0.74 • ASM updated to 9.5 • Azure blob storage updated to 12.22.0 • FasterXML Jackson Core updated to 2.15.0 • Jetty updated to 9.4.51.v20230217 • Metrics Core updated to 4.2.18 • MigLayout updated to 11.1 • Nimbus Jose + JWT updated to 9.31 • PostgreSQL JDBC driver updated to 42.6.0 • RSyntaxTextArea updated to 3.3.3 • Simple Logging Facade for Java updated to 2.0.7 • Spring Framework updated to 5.3.27 • UAP-java updated to 1.5.4 • Oracle JDK updated to 17.0.7
TSS-32502	12.0.5	• AngularJS updated to 15.2.8 • Autoprefixer updated to 10.4.14 • ngx-toastr updated 16.1.1 • Reactive Extensions Library for JavaScript updated to 7.8.1 • tslib updated to 2.5.0 • worker-timers updated to 7.0.65 • zone.js updated to 0.13.0

Key	Version	Summary
TSS-31918	12.0.4	- Amazon AWS SDK updated to 2.19.15 - Apache Tomcat updated to 9.0.71 - Azure Storage blob updated to 12.20.2 - FasterXML Jackson updated to 2.14.1 - FasterXML Woodstox updated to 6.4.0 - Java Microbenchmark Harness updated to 1.36 - Jetty updated to 9.4.50.v20221201 - Metrics Core updated to 4.2.15 - Netty Reactor Http updated to 1.0.26 - Netty Resolver DNS updated to 4.1.86Final - Nimbus JOSE+JWT updated to 9.28 - Oracle JDK updated to 17.0.6 - RSyntaxTextArea updated to 3.3.1 - Simple Logging Facade for Java (SLF4J) updated to 2.0.6 - Spring Framework updated to 5.3.24 - XMLUnit updated to 2.9.1
TSS-31919	12.0.4	- Angular updated to 15.0.4 - ngx-toastr updated to 16.0.1 - Reactive Extensions Library for JavaScript updated to 7.8.0 - worker-timers update to 7.0.60 - zone.js updated to 0.12.0
TSS-31792	12.0.3	- Angular updated to 14.2.9 - Autoprefixer updated to 10.4.13 - ngx-toastr updated to 15.2.1 - Reactive Extensions Library for JavaScript updated to 7.5.7 - tslib updated to 2.4.1 - worker-timers update to 7.0.58
TSS-31790	12.0.3	- Apache Tomcat updated to 9.0.69 - FasterXML Jackson Core updated to 2.14.0 - Azure Storage Blob updated to 12.20.1 - PostgreSQL JDBC Driver updated to 42.5.1 - Reactor Netty Http updated to 1.0.24 - SnakeYAML updated to 1.33

Key	Version	Summary
TSS-31569	12.0.2	• Amazon AWS SDK updated to 2.17.292 • ANTLR4 updated to 4.11.1 • Apache Commons Text updated to 1.10.0 • Apache CXF updated to 3.5.4 • Apache Ignite updated to 2.14.0 • Apache Tomcat updated to 9.0.68 • ASM updated to 9.4 • Azure Blob Storage updated to 12.20.0 • BlueConic/browscap-java updated to 1.3.13 • Dropwizard Metrics Core updated to 4.2.12 • FasterXML/Jackson Databind updated to 2.13.4.2 • FasterXML/Jackson Core updated to 2.13.4 • Jetty updated to 9.4.49.v20220914 • Log4j updated to 2.19.0 • Nimbus JOSE + JWT updated to 9.25.6 • Oracle JDK updated to 17.0.5 • PostgreSQL JDBC Driver updated to 42.5.0 • RSyntaxTextArea updated to 3.3.0 • Simple Logging Facade for Java updated to 2.0.2 • Spring Framework updated to 5.3.23
TSS-31576	12.0.2	• Angular updated to 14.2.6 The following included NPM packages are updated in this release: • autoprefixer updated to 10.4.12 • ngx-toastr updated to 15.2.1 • Reactive Extensions Library for JavaScript updated to 7.5.7 • worker-timers updated to 7.0.54 • zone.js updated to 0.11.8
TSS-31710	12.0.2	• Progress DataDirect Connect for JDBC MySQL Driver updated to 5.1.4.000265 • Progress DataDirect for JDBC for Oracle Driver updated to 6.0.0.000840
TSS-31467	12.0.1	The following JDBC drivers have been updated: • Redshift JDBC driver to 2.1.0.9 • Progress DataDirect Oracle driver to 6.0.0.000790 • Progress DataDirect SQLserver driver to 6.0.0.000998

Key	Version	Summary
TSS-31368	12.0.1	- Amazon AWS SDK updated to 2.17.258 - Apache CXF updated to 3.5.3 - Apache Log4j updated to 2.18.0 - Apache Tomcat updated to 9.0.65 - Jetty updated to 9.4.48.v20220622 - Metrics Core updated to 4.2.11 - Microsoft Azure Blob Storage updated to 12.19.0 - Nimbus José JWT updated to 9.23 - Oracle JDK updated to 17.0.4 - PostgreSQL JDBC driver updated to 42.4.1 - Spring Framework updated to 5.3.22 - User Agent Parser updated to 1.5.3
TSS-31369	12.0.1	- AngularJS updated to 14.1.1 - Reactive Extensions Library for JavaScript updated to 7.5.6 - toastr updated to 15.0.0 - Zones for Javascript updated to 0.11.7
TSS-30424	12.0.0	Angular updated to 13.3.9
TSS-30868	12.0.0	Apache Ignite updated to 2.13.0
TSS-30790	12.0.0	Progress DataDirect Connect for JDBC SQL Server updated to 6.0.0.000827
SPOT-1721	12.0.0	The following Spotfire products and components now use Java 17.0.3: - TIBCO Spotfire® Server - TIBCO Spotfire® node manager - TIBCO Spotfire® Service for Python (Python service) - TIBCO® Enterprise Runtime for R - Server Edition (TERR service)
TSS-31053	12.0.0	Updated JDBC drivers: - Progress DataDirect Oracle driver updated to 6.0.0.000707 - Progress DataDirect Sybase driver updated to 5.1.4.000135 - Redshift JDBC updated to 2.1.0.7

Key	Version	Summary
TSS-30423	12.0.0	- Amazon Redshift JDBC driver updated to 2.1.0.5 - ANTLR4 updated to 4.10.1 - Apache CFX updated to 3.5.2 - Apache Ignite updated to 2.13.0 - Apache Log4j Core updated to 2.17.2 - Apache Tomcat updated to 9.0.63 - ASM updated to 9.3 - AspectJ Weaver updated to 1.9.9.1 - AWS SDK for Java updated to 2.17.195 - Azure Active Directory Library for Java updated to 12.14.4 - Byte Buddy updated to 1.12.10 - Jackson Core updated to 2.13.3 - Jetty updated to 9.4.46.v20220331 - JSON Small and Fast Parser updated to 2.4.8 - Metrics Core updated to 4.2.9 - Nimbus JOSE + JWT updated to 9.22 - PostgreSQL JDBC Driver updated to 42.3.5 - Progress DataDirect Connect for JDBC SQL Server updated to 6.0.0.000827 - RSyntaxTextArea updated to 3.2.0 - Simple Logging Facade for Java updated to 1.7.36 - Spring Framework updated to 5.3.20

Closed Issues

The table lists important closed issues in version 12.0 of Spotfire Server.

Key	Version	Summary
TSS-32305	12.0.5	When the system property `java.io.tmpdir` is set to `relative`, unpacking cobranding packages in the `.cab` format fails.
TSS-32320	12.0.5	Inefficient search index updates can lead to poor performance after a large number of very small library items are imported.
TSS-32323	12.0.5	Excessive path look-ups can lead to poor performance after a large number of very small library items are imported.
TSS-32402	12.0.5	A SQL query that is used when deleting library items (or library item versions) is inefficient and can lead to a high database CPU load.
TSS-32411	12.0.5	The following library compression configuration properties are missing from the help topic: • `activities.compression.max-concurrent` • `activities.prune-tasks-older-than-seconds` • `library.compression.migration.batch` • `library.compression.migration.wait`
TSS-32414	12.0.5	In TIBCO Cloud Spotfire, on the *My Account* page, the user's display name and email are not correct.
TSS-32454	12.0.5	When you redirect an Information Services data source (for example from a MySQL instance to a Microsoft SQL Server instance) from a data source that does not use schemas, to another data source that does use schemas, any dependent elements are not updated correctly.
TSS-32456	12.0.5	The external Ignite process always binds to all available network interfaces, even if it is configured not to so using the `clustering.apacheignite.bind-on-any-interface` configuration property.
TSS-32477	12.0.5	If you have enabled the legacy feature SOAP logging, logging to the file `informationservices/soap.log` does not work as expected for Information Services data sources that have *User authentication* selected.
TSS-32478	12.0.5	A Content Security Policy set in HTML makes it hard to configure a custom policy.
TSS-32517	12.0.5	The help topic for Spotfire.Dxp.Worker.Host.dll.config is not available.
TSS-32551	12.0.5	The `--keep-created-after` argument of the `delete-library-versions` command is not interpreted as intended (specifying it will lead to all versions being kept).
TSS-31921	12.0.4	Clicking the "Open in installed client" button in the Analysis Redirect page has no effect.

Key	Version	Summary
TSS-32039	12.0.4	If you have an Oracle Spotfire Server database, and if 1,000 or more activities have failed to compress more than twice, then compressing any other library items fails.
TSS-32076	12.0.4	Users do not get redirected to their initial target pages after authenticating, when they have selected the *Remember my choice* checkbox and they are using an OpenID Authentication provider.
TSS-32077	12.0.4	Fixed users and external users cannot be enabled or disabled in the Users app.
TSS-32094	12.0.4	The installation scripts for Microsoft SQL Server can fail with an error similar to the following: `Introducing FOREIGN KEY constraint 'FK_LIB_RESOLREQUI_1B29035F' on table 'LIB_RESOLVED_DEPEND_VER' may cause cycles or multiple cascade paths."` The same failure with a similar message can occur during an upgrade if you are using a Microsoft SQL Server database.
TSS-32096	12.0.4	When using sites with Oracle as the database backend for the Spotfire Server, a routing rule from another site can be used incorrectly, which makes it impossible to open analysis files.
TSS-32151	12.0.4	Deleting library item versions takes more time than necessary. This issue primarily affects import validation of Information Services elements, where the imported elements are typically rewritten and the original version is deleted.
TSS-32169	12.0.4	When migrating data from one PostgreSQL database to another PostgreSQL database, the migration tool cannot migrate large objects.
TSS-32245	12.0.4	Specifying an empty value for a `CustomCredentialsProvider` initialization parameter in an Information Services data source template results in an error during Spotfire Server startup.
TSS-31775	12.0.3	When the configuration property `scheduled-updates.failover-delay.enabled` is set to `true`, the server fails to serialize an object.
TSS-31822	12.0.3	The CLI command `delete-library-versions` returns a null pointer exception when you use a library search query that references a user.
TSS-31839	12.0.3	Direct links to bookmarks within analyses do not work.
TSS-31886	12.0.3	If you use Microsoft SQL Server as the Spotfire Server database, and if the Spotfire Server database was created with a non-default SQL Server collation, then library delete operations can fail.
TSS-31505	12.0.2	In rare circumstances, Automation Services jobs are stuck and not retried when an instance is running at full capacity.
TSS-31564	12.0.2	The example script for configuring a Spotfire Server using a script does not include using PostgreSQL.
TSS-31584	12.0.2	Import of an exported library folder sometimes fails due to incorrect handling of declared dependencies.

Key	Version	Summary
TSS-31585	12.0.2	Members of the *Scheduling and Routing Administrator* group, who are not also members of the *Administrator* group, cannot create user rules, create group rules, or view the *Scheduled updates activity* page in the Spotfire Server web administration pages.
TSS-31588	12.0.2	Upgrade of the Spotfire database fails if there are broken items (items without any content) in the library.
TSS-31613	12.0.2	The remove-code-signing-certificate command removes the desired root certificate from the database.
TSS-31639	12.0.2	During a library export/import process, some metadata for the library item is not imported correctly, which results in a content mismatch warning in Spotfire Analyst.
TSS-31640	12.0.2	There is no documentation about how to handle a Spotfire Server using RC4_HMAC after the 3DES and RC4_HMAC encryption algorithms were deprecated in Java and became disabled by default for Kerberos (cf. https://www.oracle.com/java/technologies/javase/17-relnote-issues.html). To enable RC4_HMAC, you must perform some manual steps. See Standards and Algorithms in the *TIBCO Spotfire® Server and Environment Security* guide for more information.
TSS-31648	12.0.2	When you work with on-demand data from information links, and you use more than one parameter, `Timestamp` and `Time` columns with milliseconds precision sometimes cause errors.
TSS-31663	12.0.2	For some system combinations, where SQL Server is used as the Spotfire Server database and using different locales, unicode characters are not displayed correctly in the *Scheduling & Routing* page.
TSS-31672	12.0.2	A user name or password that contains special characters (for example, + or *) does not work for logging in using the cobranding custom login.
TSS-31680	12.0.2	The landing page is displayed for users who only have access to a single Spotfire Server web page, or to the library and the Spotfire web client only, instead of navigating directly to the accessible page or to the web client.
TSS-31692	12.0.2	There is no way to stop users from accessing an analysis file that is configured for caching but is not available in the cache. This can cause an unnecessarily high load on the server by repeated attempts to access the file. The issue has been fixed by including information about analysis loading status, and scheduled updates status when denying access to an analysis. In addition, it is now also possible to ignore an analysis that is currently being loaded, when denying access, by setting `scheduled-updates.performance.deny-open-when-not-ready` to `true` in the server configuration.
TSS-31694	12.0.2	Using a copied URL to a Spotfire web client analysis in another user session results in a blank screen.
TSS-31752	12.0.2	In scenarios with a lot of concurrent users, and when having a personalized view for each web client user, the database sometimes gets too high database contention (because multiple processes try to access the same data), which can lead to system instabilities. The risk for this to happen has now been reduced.
TSS-31754	12.0.2	In scenarios with a lot of concurrent users, code trust queries affect the Spotfire Server database load. The risk for this to happen has now been reduced.

Key	Version	Summary
TSS-31756	12.0.2	The job that compresses library items, which runs in the background, keeps a database result set open longer than necessary.
TSS-31758	12.0.2	Library searches that use custom parameters are slower in Spotfire 12.0 than in earlier versions.
TSS-31321	12.0.1	If issues prevent communication between the node manager and a service, the service is sometimes not informed that it should shut down gracefully, and it takes too long to stop the service. Calls to the service should be retried, at least for a short period of time, to reduce the number of such cases.
TSS-31391	12.0.1	If a Library search includes an open bracket ('['), the search fails for a SQL Server database.
TSS-31393	12.0.1	Library searches do not use function-based indexes in case-sensitive databases such as Oracle and PostgreSQL.
TSS-31401	12.0.1	For the PostgreSQL database, deleting a library item that has multiple versions does not delete the content for all versions.
TSS-31412	12.0.1	Opening or accessing an imported column causes Spotfire Analyst to fail unexpectedly.
TSS-31416	12.0.1	A database upgrade can fail if a library item's properties are not going to be versioned.
TSS-31418	12.0.1	In the library, the context menu option **Copy link** is missing for analysis files and Information Link files.
TSS-31450	12.0.1	The sentence about differences in calculation results between Windows and Linux in the *TIBCO Spotfire® Server and Environment - Installation and Administration* guide is incorrect.
TSS-31457	12.0.1	From the Monitoring & Diagnostics page, when you select a node, and from the Nodes & Services > Network page, when you select a node, service, or server, the link to the deployment area is broken.
TSS-31458	12.0.1	On the *Monitoring & Diagnostics, Routing: Analyses* page, if multiple analyses have the same path, then only the first occurrence of an analysis is duplicated, and the other analyses with the same path are ignored.
TSS-31459	12.0.1	The same trusted entities, but with a different trust source ("Trusted by"), are presented as duplicate entries on the My Account page and under User > Trusted signers and items.
TSS-31462	12.0.1	Running a configuration script can fail if the script contains many database calls.
TSS-31478	12.0.1	It is not possible to search for External Updates in the *Scheduling & Routing, Activity* table in the TIBCO Spotfire Server web administration pages.
TS-37791	12.0.0	The documentation states that the *Administrator* user group includes the permissions from all other system groups. In fact, the *Administrator* group does not include permissions from the *Script Author* and *Custom Query Author* groups.

Key	Version	Summary
TS-69399	12.0.0	Long timeouts for OCSP requests in node services can cause node services to be unresponsive.
TSAS-1107	12.0.0	The Spotfire Analyst and the Automation Services service can become unresponsive if they are provided with very low values for height or width in the tasks "Export Image" and "Send Email."
TSS-15080	12.0.0	It is not possible to remove a primary parent group in the settings for a group.
TSS-27047	12.0.0	Library items with duplicated names, and of the same type and in the same folder, can be created if they are saved at the same time.
TSS-29769	12.0.0	After changing the deployment area for a group, it is no longer possible to go back to the state where the group always uses the current default deployment area.
TSS-29962	12.0.0	The selection in tables in the web administration pages is not maintained when refreshing the table data.
TSS-29973	12.0.0	Logging to the export log for the Spotfire Analyst client is interrupted due to a concurrency issue. The job continues and is unaffected; only logging is interrupted.
TSS-30166	12.0.0	In the Scheduling & Routing app, when you navigate from a rule with a name containing a character that requires URL encoding (such as '&', '+', '%', and so on) to its corresponding activity, you can encounter incorrect search results, or you can be redirected to the landing page.
TSS-30201	12.0.0	The error message and status code shown in the Spotfire Server web administration pages when a circular membership exception occurs is incorrect.
TSS-30261	12.0.0	You are not allowed to add multiple saved schedules with identical configurations, nor to add new schedules with identical configurations when creating or editing a rule.
TSS-30336	12.0.0	When deleting a used deployment area, it should not be allowed to move nodes and services to an empty deployment area.
TSS-30347	12.0.0	Failing to upload a package in a deployment area results in an unfriendly error message.
TSS-30400	12.0.0	The dialog showing information about pre- and post-service rollback for an updated service permanently shows the spinner and does not load data.
TSS-30452	12.0.0	Error code 3 is returned when executing the command `config run simple-config-ldap.txt`, due to a superfluous backslash in the file.
TSS-30455	12.0.0	While moving one or more items in the library, and the *Move* banner is displayed at the top of the page, the last item in the library is no longer visible.
TSS-30508	12.0.0	The documentation does not specify that you must configure HTTPS if you want to set the cookie attribute SameSite to None.
TSS-30512	12.0.0	The documentation incorrectly states that default value for the Web Player service configuration setting `maxReceivedMessageSizeMb` is 64 MB. The actual default value is 1024 MB.

Key	Version	Summary
TSS-30513	12.0.0	The `config-external-ignite-process` erroneously removes all of the JVM options from the configuration if no options are specified while updating another value.
TSS-30518	12.0.0	Blocked users, certificates and items should be highlighted with an error icon in the tables that show information about trust, that is, on the following pages: My Account (Trusted signers and items section), Group details (Trusted signers tab), User details (Trusted signers and items tab)
TSS-30519	12.0.0	Blocked users and certificates should not be possible to be added as trusted signers for a group.
TSS-30527	12.0.0	Data functions cannot be seen in the library, and *Data function* is not an available type when filtering in the library.
TSS-30537	12.0.0	Running nodes on Windows Server 2022 with a connection to the Spotfire Server through HTTPS and TLS 1.3 can cause stability issues.
TSS-30578	12.0.0	The `create-deployment-area` CLI command does not provide validation according to the rules in the documentation.
TSS-30595	12.0.0	The Welcome dialog and the installation steps dialog for the TIBCO Cloud Spotfire Library do not fit on a small screen.
TSS-30612	12.0.0	When you use Information Services, errors can occur when you load several information links with Date, Time, and/or DateTime columns at the same time.
TSS-30623	12.0.0	It is not possible to remove all groups from a specific group.
TSS-30690	12.0.0	The value displayed in the *Last start time* column of the Scheduling & Routing Rules page is incorrect.
TSS-30692	12.0.0	When trying to view a specific rule's job activity, the result can be imprecise and list more than one job because the search filter uses the rule name only.
TSS-30740	12.0.0	In the library, it is not possible to delete items which have dependencies (where other items depend on them).
TSS-30743	12.0.0	Setting the level of the `com.spotfire.ws.soap.SOAP` logger to `DEBUG` does not enable SOAP logging.
TSS-30756	12.0.0	The Options documentation for the command-line command `set-sensitive-config-prop` documentation mistakenly includes the flag `--encrypt=value`.
TSS-30776	12.0.0	When you edit a user's profile, If you leave **Display name** empty, an error is displayed.
TSS-30788	12.0.0	In the Monitoring & Diagnostics Instances page, if you search by instance ID, you will get incorrect search results.
TSS-30789	12.0.0	In the Scheduling & Routing Rules page and Activity page, when a resource pool is not available, an inconsistent name is used for the resource pool.
TSS-30799	12.0.0	When the Library settings specify that the search input must not be present on the Library page, the **Create folder** icon button is not displayed.

Key	Version	Summary
TSS-30820	12.0.0	When a very high maximum number of connections is configured for a data source, an excessive amount of memory is allocated.
TSS-30821	12.0.0	In the unlikely event that a user logs in and out at the same time, a potential deadlock can occur.
TSS-30835	12.0.0	In the library, you cannot move a folder to another folder whose name starts with the same characters as the folder you try to move.
TSS-30843	12.0.0	In the *Scheduling & Routing*, *Rules* page, the resource pool name should be used instead of the resource pool ID when filtering.
TSS-30847	12.0.0	In the action log, the `sessions` metric incorrectly shows the total number of sessions that have been created instead of the current number of active sessions.
TSS-30850	12.0.0	When using TIBCO Cloud Spotfire and trying to download the Spotfire Analyst client or other resources from the Downloads page, this is sometimes not possible because the download link has expired.
TSS-30851	12.0.0	An error is shown when editing a rule's custom schedule.
TSS-30854	12.0.0	The instructions for verifying a data source template contain incorrect information.
TSS-30865	12.0.0	The filter option 'Default routing' is missing for the **Resource pool** filter in the *Scheduling & Routing*, *Rules* page.
TSS-30915	12.0.0	The Spotfire Server starts even if it cannot bind to one or more ports.
TSS-30924	12.0.0	In the *TIBCO Spotfire Server Installation and Administration* guide, the topic Configuring HTTPS should be clarified for administrators who do not use X.509 client certificates.
TSS-30945	12.0.0	External authentication does not work when connecting with a web client.
TSS-31010	12.0.0	The `find-analysis-scripts` command does not properly trust multi-line custom queries.
TSS-31048	12.0.0	The help topic Configure LDAPS in the TIBCO Spotfire Server and Environment - Installation and Administration Manual should use the command `-importcert` rather than `-import`.
TSS-31142	12.0.0	External scheduled updates are not listed in the *Scheduled updates activity* table in the Spotfire Server web administration pages.
TSS-32111	12.0.0	The system requirements topic for installing Web Player did not explicitly state that the requirement applied to the Windows operating system only.

Known Issues

The following are known issues in version 12.0 of Spotfire Server:

Key	Version	Summary
TSAS-1123	12.0.0	**Encrypting services' configuration files not supported on Linux** You cannot encrypt configuration files for Automation Services and Web Player Services on Linux.
TSS-21408	12.0.0	**Using more cursors than are available can cause the server to stop responding and displays an error** 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 error occurs, try setting the OPEN_CURSORS property in Oracle to at least 500, and then restart the server.
TSS-23602	12.0.0	**A Spotfire Server restart affects jobs being executed by Automation Services** 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 remains in the IN_PROGRESS state in the Activity view even after the servers are back online. **Workaround:** Right-click the activity, and then click **Clear selected activity** to clear the job activity from the Activity view.
TSS-26972	12.0.0	**Java changes affect updating node manager from 10.9 to 10.10 or later** Updating the node manager from Nodes & Services from a 10.9 or earlier release to a 10.10 release or later is not supported due to updated Java versions. **Workaround:** To update the node manager to version 10.10 or later, you must install it on each computer, and then run the node manager upgrade tool.

Key	Version	Summary
TSS-29819	12.0.0	**Users authenticated through Kerberos with delegation require special handling for accessing certain services** In the following situations, 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 service 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 box that opens, click **File > Add/Remove > Snap-ins**. 4. In the Add or Remove Snap-ins dialog box, select **Certificates**, and then click **Add**. 5. In the Certificates snap-in dialog box, select **Computer account**, and then click **Next**. 6. In the Select Computer dialog box, click **Finish**. 7. In the Add or Remove Snap-ins dialog box, 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 box, 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 box, restart the Web Player node.
TSS-30350	12.0.0	**Very high display resolution affects ability to repair or uninstall Spotfire Server** Repair or uninstallation of the Spotfire Server and/or the node manager does not work on computers with a high display resolution, such as 3840 x 2160 pixels. The repair/uninstall dialogs in the installers are not shown as expected and there is no way to proceed with the repair/uninstallation. **Workaround:** Temporarily switch to a lower display resolution, such as 1920 x 1080 pixels.
TSS-30734	12.0.0	**Proxy server configuration** When using a proxy server between the Spotfire Server and a Web Player or Automation Services service deployed on Linux, the services will use the operating system proxy configuration. Only the username and password for the proxy can be configured in the configuration files of the services.

Key	Version	Summary
TSS-31285	12.0.0	**Network-related issues and unexpected attempts to reconnect in containerized Spotfire Server and Spotfire Web Player**

When the `spotfire-webplayer` is under heavy load, or if the load increases suddenly, you can experience spotfire-webplayer pod `livenessProbe` failures or network-related issues between the spotfire-server and spotfire-webplayer pods, and the spotfire-webplayer pod can restart prematurely. Usually, this problem is caused by CPU throttling in Kubernetes/Linux cgroups/Completely Fair Scheduler. When this situation occurs, users can experience reconnection attempts.

Workaround

To avoid or minimize CPU throttling, ensure that the spotfire-webplayer and spotfire-server do not specify a value for `resources.limits.cpu`, and increase the spotfire-webplayer `livenessProbe` failure window by increasing the values for `periodSeconds` and/or `failureThreshold`.

Depending on the scenarios you observe, you can decrease the spotfire-webplayer CPU strained levels (see `WebPlayer_AverageCpuLoadStrainedLimit` in `Spotfire.Dxp.Worker.Host.dll.config` and `cpuAverageTimeSpan` in `Spotfire.Dxp.Worker.Web.config`) so that the load is distributed earlier among the running spotfire-webplayer pods, or so that analyses are put in scheduled updates.

In addition, increasing `System.Threading.ThreadPool.MinThreads` in `Spotfire.Dxp.Worker.Host.runtimeconfig.json` to a larger value, (for example,100 or 200, depending on the load) helps in some scenarios.

Example

Spotfire.Dxp.Worker.Host.runtimeconfig.json

```json
{
  "runtimeOptions": {
    "tfm": "net6.0",
    "frameworks": [
      {
        "name": "Microsoft.NETCore.App",
        "version": "6.0.0"
      },
      {
        "name": "Microsoft.AspNetCore.App",
        "version": "6.0.0"
      }
    ],
    "configProperties": {
      "System.Drawing.EnableUnixSupport": true,
      "System.GC.Server": true,
      "System.Reflection.Metadata.MetadataUpdater.
IsSupported": false,
      "System.Runtime.Serialization.
EnableUnsafeBinaryFormatterSerialization": true,
      "System.Threading.ThreadPool.MinThreads": 100
    }
  }
}
```

For a containerized Spotfire Server (CDK), see the README files for information about exporting the current file, and then apply it after modification using a command like the following:

```
helm upgrade ... --set-file=config.'Spotfire\.Dxp\.Worker\.Host\.
runtimeconfig\.json'=Spotfire.Dxp.Worker.Host.runtimeconfig.json
```

Migration and Compatibility

The documentation 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

Version 12.0 of Spotfire Automation Services should be installed for compatibility with version 12.0 of TIBCO Spotfire.

For instructions on how to upgrade to version 12.0 Spotfire Automation Services, see "Updating Services" in the *Spotfire Server and Environment - Installation and Administration* help.

Spotfire Qualification

Version 12.0 of Spotfire Qualification should be installed for compatibility with version 12.0 of TIBCO Spotfire.

For instructions on how to upgrade to version 12.0 of Spotfire Qualification, see the Spotfire Qualification - Installation Guide.

TIBCO Documentation and Support Services

For information about the Spotfire products, you can read the documentation, contact TIBCO Support, and join the TIBCO Community.

How to Access TIBCO Documentation

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

The website is updated frequently and is more current than any other documentation included with the product.

TIBCO Spotfire Documentation

The documentation for all Spotfire products is available on the TIBCO Spotfire® Documentation page. This page takes you directly to the latest version of each document.

To see documents for a specific Spotfire product or version, click the link of the product under 'Other versions', and on the product page, choose your version from the top right selector.

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

Get an overview of TIBCO Support. You can contact TIBCO Support in the following ways:

- 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.

Legal and Third-Party Notices