

TIBCO® API Exchange Manager

Administration

Software Release 2.1.1
November 2014

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.

This document contains confidential information that is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of TIBCO Software Inc.

TIBCO, Two-Second Advantage, TIBCO Hawk, TIBCO Rendezvous, TIBCO Runtime Agent, TIBCO ActiveMatrix, TIBCO ActiveMatrix BusinessWorks, TIBCO ActiveMatrix Service Gateway, TIBCO ActiveSpaces, TIBCO Administrator, TIBCO API Exchange, TIBCO API Exchange Gateway, TIBCO BusinessEvents, TIBCO BusinessConnect, TIBCO BusinessConnect Trading Community Management, TIBCO Designer, TIBCO Spotfire, and TIBCO Spotfire Web Player are either registered trademarks or trademarks of TIBCO Software Inc. in the United States and/or other countries.

Enterprise Java Beans (EJB), Java Platform Enterprise Edition (Java EE), Java 2 Platform Enterprise Edition (J2EE), and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle Corporation in the U.S. and other countries.

All other product and company names and marks mentioned in this document are the property of their respective owners and are mentioned for identification purposes only.

THIS SOFTWARE MAY BE AVAILABLE ON MULTIPLE OPERATING SYSTEMS. HOWEVER, NOT ALL OPERATING SYSTEM PLATFORMS FOR A SPECIFIC SOFTWARE VERSION ARE RELEASED AT THE SAME TIME. SEE THE README 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.

Copyright © 2013-14 TIBCO Software Inc. ALL RIGHTS RESERVED.

TIBCO Software Inc. Confidential Information

Contents

Preface	v
Related Documentation	vi
TIBCO® API Exchange Documentation	vi
TIBCO® API Exchange Gateway Documentation	vi
TIBCO® API Exchange Manager Documentation	vi
Other Documentation	vii
Typographical Conventions	viii
Connecting with TIBCO Resources	x
How to Join TIBCOCommunity	x
How to Access TIBCO Documentation	x
How to Contact TIBCO Support	x
Chapter 1 Administration	1
Portal Administration	2
Managing User Roles	2
Managing Environments and Gateways	2
Managing Subscriptions	4
Managing OAuth 2.0 Scopes	5
Product Management	6
Managing APIs	6
Managing Products and Associated Plans	7
Partner Management	8
Managing Organizations	8
Managing Users	8
Managing Applications	8
Managing Subscriptions	9
Managing Throttle Quotas	9
Logging	10
Setting Up SSL Support for the Developer Portal	11
Chapter 2 API Analytics	15
Overview	16
Configuration	17
Viewing the Dashboard	24

Index **27**

Preface

TIBCO API Exchange Manager allows service providers and product managers to create service gateways and application environments that enable development of software products and associated APIs.

Topics

- [Related Documentation, page vi](#)
- [Typographical Conventions, page viii](#)
- [Connecting with TIBCO Resources, page x](#)

Related Documentation

This section lists documentation resources you might find useful.

TIBCO® API Exchange Documentation

The TIBCO API Exchange Documentation contains:

- *TIBCO API Exchange Concepts*. Read this document to get an overview of API Exchange concepts, workflow, and deployment.
- *TIBCO API Exchange Getting Started*. Read this document for a tutorial on installing and configuring TIBCO API Exchange and running the sample project provided with the product.

These documents are included as part of the TIBCO API Exchange Manager documentation.

TIBCO® API Exchange Gateway Documentation

The following documents form the TIBCO API Exchange Gateway documentation set:

- *TIBCO API Exchange Gateway Installation*. Read this manual for instructions on site preparation and installation.
- *TIBCO API Exchange Gateway User's Guide*. Read this manual for instructions on how to configure and use this product.
- *TIBCO API Exchange Gateway Release Notes*. Read the release notes for a list of new and changed features. This document also contains lists of known issues and closed issues for this release.

TIBCO® API Exchange Manager Documentation

The following documents form the TIBCO API Exchange Manager documentation set:

- *TIBCO API Exchange Manager Installation*. Read this manual for instructions on site preparation and installation.
- *TIBCO API Exchange Manager Administration*. Read this manual for information on how to set up users and user groups, add APIs, and manage products and plans.

- *TIBCO API Exchange Manager Release Notes* Read the release notes for a list of new and changed features. This document also contains lists of known issues and closed issues for this release.

Other Documentation

You might find it useful to read the documentation for the following:

- Joomla! - See <http://docs.joomla.org>.
- Example project hosted on GitHub: *Adapter Code for TIBCO API Exchange and Joomla!*. See <https://github.com/API-Exchange/JoomlaAdapter/wiki>.




Typographical Conventions

The following typographical conventions are used in this manual.

Table 1 General Typographical Conventions

Convention	Use
<i>ENV_NAME</i> <i>TIBCO_HOME</i> <i>ASG_HOME</i> <i>ASG_CONFIG_HOME</i>	<p>TIBCO products are installed into an installation environment. A product installed into an installation environment does not access components in other installation environments. Incompatible products and multiple instances of the same product must be installed into different installation environments.</p> <p>An installation environment consists of the following properties:</p> <ul style="list-style-type: none">• Name Identifies the installation environment. This name is referenced in documentation as <i>ENV_NAME</i>. On Microsoft Windows, the name is appended to the name of Windows services created by the installer and is a component of the path to the product shortcut in the Windows Start > All Programs menu.• Path The folder into which the product is installed. This folder is referenced in documentation as <i>TIBCO_HOME</i>. <p>TIBCO API Exchange installs into a directory within a <i>TIBCO_HOME</i>. This directory is referenced in documentation as <i>ASG_HOME</i>. The default value of <i>ASG_HOME</i> depends on the operating system. For example on linux platform, the value of <i>ASG_HOME</i> is /home/asg/tibcoasg/asg/2.1.</p> <p>TIBCO API Exchange stores the configuration files in a directory which is separate from the installation directory. This directory is referenced in documentation as <i>ASG_CONFIG_HOME</i>. For example on linux platform, the value of <i>ASG_CONFIG_HOME</i> is: /home/asg/tibcoasgconfig/tibco/cfgmgmt</p>
code font	<p>Code font identifies commands, code examples, filenames, pathnames, and output displayed in a command window. For example:</p> <p>Use MyCommand to start the foo process.</p>
bold code font	<p>Bold code font is used in the following ways:</p> <ul style="list-style-type: none">• In procedures, to indicate what a user types. For example: Type admin.• In large code samples, to indicate the parts of the sample that are of particular interest.• In command syntax, to indicate the default parameter for a command. For example, if no parameter is specified, MyCommand is enabled: MyCommand [enable disable]

Table 1 General Typographical Conventions (Cont'd)

Convention	Use
<i>italic font</i>	<p>Italic font is used in the following ways:</p> <ul style="list-style-type: none">• To indicate a document title. For example: See <i>TIBCO ActiveMatrix BusinessWorks Concepts</i>.• To introduce new terms For example: A portal page may contain several portlets. <i>Portlets</i> are mini-applications that run in a portal.• To indicate a variable in a command or code syntax that you must replace. For example: <code>MyCommand <i>PathName</i></code>
Key combinations	<p>Key name separated by a plus sign indicate keys pressed simultaneously. For example: Ctrl+C.</p> <p>Key names separated by a comma and space indicate keys pressed one after the other. For example: Esc, Ctrl+Q.</p>
	<p>The note icon indicates information that is of special interest or importance, for example, an additional action required only in certain circumstances.</p>
	<p>The tip icon indicates an idea that could be useful, for example, a way to apply the information provided in the current section to achieve a specific result.</p>
	<p>The warning icon indicates the potential for a damaging situation, for example, data loss or corruption if certain steps are taken or not taken.</p>

Connecting with TIBCO Resources

How to Join TIBCOCommunity

TIBCOCommunity is an online destination for TIBCO customers, partners, and resident experts. It is a place to share and access the collective experience of the TIBCO community. TIBCOCommunity offers forums, blogs, and access to a variety of resources. To register, go to <http://www.tibcommunity.com>.

How to Access TIBCO Documentation

You can access TIBCO documentation here:

<http://docs.tibco.com>

How to Contact TIBCO Support

For comments or problems with this manual or the software it addresses, contact TIBCO Support as follows:

- For an overview of TIBCO Support, and information about getting started with TIBCO Support, visit this site:

<http://www.tibco.com/services/support>

- If you already have a valid maintenance or support contract, visit this site:

<https://support.tibco.com>

Entry to this site requires a user name and password. If you do not have a user name, you can request one.

Chapter 1 Administration

The portal administrator or the manager, performs administrative tasks such as managing environments, users, APIs, products, subscriptions, viewing logs, and so on. The portal administrator can also configure and view API Analytics.



A sample Developer Portal is available when you install the GitHub project *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1* in your environment.

Topics

- [Portal Administration, page 2](#)
- [Product Management, page 6](#)
- [Partner Management, page 8](#)
- [Logging, page 10](#)
- [Setting Up SSL Support for the Developer Portal, page 11](#)

Portal Administration

Portal administrators have full access to all product features and all functions on the portal. Their primary role is to create environments and add gateways to the environments, manage users and user roles, and manage APIs, products, subscriptions and scopes. Portal administrators can also view API usage data on the analytics dashboard.



The Developer Portal is available if *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1* is installed in your environment. The portal administrator can use the portal to perform management tasks. Refer to the *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1* documentation for detailed instructions.

Managing User Roles

The portal administrator is responsible for creating organizations, manager roles, and for managing users and subscriptions. Portal administrators are also responsible for creating and managing products, APIs, and product plans.



If you have installed *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1* in your environment, the portal administrator can create the users and user roles in the Joomla! Administrator back-end.

Managing Environments and Gateways

An environment defines an area in which products and applications can function; for example, “test,” “development,” and so on. Physically, an environment maps to a TIBCO API Exchange Gateway cluster. The environment defines a base path, which typically represents a load balancer in the network, and includes a protocol, host, port number, and a path. For example, `http://localhost:8080/base_path_to_api`. APIs that are deployed in this environment can be accessed by applications using this base path.

The portal administrator creates an environment and specifies information such as the type of environment and base path URL, and then adds one or more gateways to the environment. The portal administrator can also view and update the configuration for the gateway clusters contained in the environment.



If you have installed *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1* in your environment, the portal administrator can access the TIBCO API Exchange Gateway Config UI from the Developer Portal.

Master Configuration

Master configuration (also referred to as *master copy*) is the complete set of configuration provisioned by the portal engine to the gateway cluster for a subscription. If the local configuration of one or more gateway instances is out-of-sync, they can be fully re-provisioned with the master configuration.

The master configuration for a gateway cluster is composed of two parts: base and access.

- **Base configuration** is set by the portal administrator (API provider) and does not change when application developers push updates from the portal. Base configuration is not environment specific.
- **Access configuration** is updated when API subscriptions are created, and used by partners and applications. It contains information controlling the access to an API by certain organizations, users, and applications, which are environment-specific entities.

To use the master configuration for the first time, copy the entire set of the cluster configuration to

`ASG_CONFIG_HOME/environments/<env_name>/<gateway_name>/<project_name>`.

After that, any change to the base configuration must be made on both master configuration and the gateway instances' local configuration.

When moving the gateway configuration from a development environment to a production environment, you must move the base configuration manually. Do not move the access configuration in the development environment, because it might differ from the configuration in the production environment.

Use the tool, **asg-tools**, provided by API Exchange Gateway to export or import the base configuration from the development environment and then import it into the production environment. Access configurations in each environment remain unaffected. See *TIBCO API Exchange Gateway Release Notes* for details on using the tool **asg-tools**.

By default, the master copy is not maintained on the portal-engine. This is not recommended for a development environment.

For a production environment, you can choose to maintain the master copy in the portal engine by enabling master configuration from the gateway configuration UI > Portal Engine Properties.



If you are using the *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1*, you can access the gateway configuration UI can be accessed from the Developer Portal page that manages environments and gateways. You can use the gateway configuration UI in the portal to publish the master configuration to each gateway instance.

Managing Subscriptions

Portal administrators can create a subscription on behalf of an organization. For a given product and plan, the portal administrator specifies the start date and end date, and sets the status for the subscription.

An organization must have a valid subscription to a product before an application can use it. If needed, an application developer or manager must request a subscription to a product's plan. Depending on the subscription type specified for the plan, the portal administrator might need to approve the request.

Subscription Request for a Plan with Auto-provisioning

When an application developer or manager places a request for a plan with auto-subscription enabled, the plan is automatically approved and a subscription for the organization that the requestor belongs to is created. By default, the validity for the subscription is set to five years.



If you are using the *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1*, the portal administrator can modify the start date and end date for the plan from Joomla. See the *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1* documentation for details.

Approve Subscription Request for a Plan Without Auto-provisioning

When an application developer or manager places a request for a plan without auto-subscription enabled, an email notification is sent to the portal administrator and the requestor.



If you are using the *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1*, the portal administrator can choose to nominate one or more members as portal administrators by adding them to the SuperUsers group in the Joomla Admin utility. In this case, the email notification is sent to all the portal administrators. See the *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1* documentation for details.

Approve Subscription Request for a Custom Plan

If an application developer or manager places a request for a custom plan, an email notification is sent to the portal administrator and requestor. The portal administrator needs to create the custom plan and provision it for the requestor.



If you are using the *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1*, refer to the *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1* documentation for details.

Managing OAuth 2.0 Scopes

TIBCO API Exchange supports OAuth 2.0 for authentication and authorization. See the TIBCO API Exchange Gateway documentation for details on setting up the OAuth infrastructure.

The portal administrator can define a scope by specifying the name and description for the scope. If scopes are enabled for the Developer Portal, the application developers can add one or more scopes to their applications, if they choose to use OAuth.

Product Management

Product management is typically performed by product managers, or by portal administrators in the absence of a product manager. The product manager or portal administrator creates and manages APIs, products, and product plans.



In the current release, the portal administrator performs the product management tasks.



The Developer Portal is available if *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1* is installed in your environment. The portal administrator can use the portal to perform the management tasks. Refer to the *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1* documentation for detailed instructions.

Managing APIs

Managing APIs consists of creating and publishing APIs and operations for the portal users to browse and test.

The portal administrator first creates one or more APIs, which are then associated with products. When creating the APIs, the portal administrator specifies the following information:

- The type of API — REST or SOAP.
- The environments in which the APIs are usable; the APIs must be provisioned in the selected environments.
- Any specification artifacts used by the API (Swagger specifications for REST APIs or WSDL specifications for SOAP APIs). Ensure that the specification artifacts are available for upload.



The REST API resource paths specified must be unique for a product.

If you are using *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1*, specifying duplicate resource paths may result in the swagger specifications being displayed incorrectly in the API explorer.

- Downloadable documentation.
- Available inline documentation.

Managing Products and Associated Plans

Once the APIs are created, the portal administrator can create products and associate APIs with the products. When creating a product, the portal administrator also specifies the information such as product category, documentation, and any product specific terms or conditions.

The portal administrator can add one or more plans to a product. When creating a plan, the portal administrator specifies information such as the plan name, level, subscription method, price, rate limit, quota limit, and so on.

Partner Management

Partner managers (also referred to as *managers*) utilize self-service registration of users, create applications, explore APIs, and request subscriptions or request additional keys for applications.



The Developer Portal is available if *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1* is installed in your environment. The portal administrator can use the portal to perform the management tasks. Refer to the *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1* documentation for detailed instructions.

Managing Organizations

Portal administrators can create organizations and add users to the organizations. In order to use an application, users must belong to an organization associated with the application.

While creating an organization, the portal administrator specifies information such as name of the organization, contact person for the organization, email address and telephone number of the contact person, APIs, products, and applications that are owned by the organization. The portal administrators can also add members and subscriptions to the organization.

Managing Users

Portal administrators can add new or existing users to user groups and grant them access to specified environments. They can also create an organization administrator for an organization.



If you are using the *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1*, TIBCO recommends that you do NOT change the pre-configured user groups and access levels in the Joomla! Administrator back-end.

Managing Applications

Managing applications consists of creating applications and requesting keys for applications. Partner managers and application developers create applications, assign products to the applications, and associate subscriptions with the applications.

The manager or a developer can also request for a replacement key for an application. This may be necessary if the existing key has been compromised. When you obtain a replacement key for an application, the original key is disabled and the replacement key is enabled.

Managing Subscriptions

The portal administrator or manager can place a request for a subscription to an existing plan or request a custom plan. Upon approval, a subscription for the organization that the requestor belongs to is created with the specified validity period. See [Managing Subscriptions, page 5](#) for details.

Managing Throttle Quotas

When registering products or applications, the portal administrator can specify throttle quotas. A throttle quota is a percent value that sets a quota for usage of the product or application. If you implement throttle quotas, then the dashboard for an application and the Dashboard tab in the Developer Portal shows a bar graph that indicates the throttle quota usage for the product, application, or subscription. In addition, the system generates alerts when a throttle quota has been exceeded and the alerts are displayed on Dashboard pages.

Logging

The log file `asg-portal.log` available at `<ASG_CONFIG_HOME>\logs` includes a log of all the events occurring on the portal engine. By default, the logging level is set to INFO.

To change the logging level:

- Edit the file `<ASG_CONFIG_HOME>\asg_portal.properties` and update the property `tibco.clientVar.ASG/Logging/MinLogLevel` to set it with one of the following log levels:
 - 0: DEBUG
 - 1: INFO
 - 2: WARN
 - 3: ERROR
 - 4: No Logging
- Edit the file `<ASG_HOME>\2.1\bin\asg-portal.cdd` to enable the `<log-configs>` property and set the logging level. For example:


```
<log-configs>
  <log-config id="logConfig">
    <enabled>true</enabled>
    <roles>*:info</roles>
    ...
  </log-config>
</log-configs>
```

If you are using the *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1*, the portal administrator can view a log of the responses received from the server on the Joomla! Administrator user interface. See *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1 Administration* for details.

Setting Up SSL Support for the Developer Portal

You can set up the API Exchange portal engine and the Developer Portal to communicate using a Secure Sockets Layer (SSL) connection over HTTPS.

Configuring the portal engine and the Developer Portal for SSL includes the following tasks:

- [Task A, Make Sure the Portal Engine and the Gateway Engine are Running Over SSL, page 11.](#)
- [Task B, Set up Apache to Run on SSL, page 12.](#)
- [Task C, Specify Settings for SSL in the Apache httpd.conf File, page 12.](#)
- [Task D, Configure SSL in the Joomla Administrator, page 12.](#)
- [Task E, Edit the asg_portal.properties File to Specify SSL Settings, page 13.](#)
- [Task F, Import the Joomla Security Certificates into the cacerts Keystore, page 14.](#)
- [Task G, In the Developer Portal, Specify SSL for Environment and Gateway Configuration, page 14.](#)

Task A Make Sure the Portal Engine and the Gateway Engine are Running Over SSL

Ensure that the gateway engine and the portal engine are configured to run over SSL:

1. Enable HTTPS on the API Exchange Gateway.
For information on enabling HTTPS on the API Exchange Gateway, see “Enable Facade HTTPs Transport” in Chapter 4 of the *TIBCO API Exchange Gateway User’s Guide*.
2. Edit the `asg-portal.properties` file on the host where the API Exchange Manager component is running to ensure that the Developer Portal runs over SSL.

For information on this task, see [Task E, Edit the asg_portal.properties File to Specify SSL Settings, page 13.](#)

Task B Set up Apache to Run on SSL

To set up the Apache Web Server to run on SSL, follow these steps:

1. Review the Apache documentation for information on setting up Apache for SSL. You can find basic documentation on setting up Apache for SSL at the following URL:

http://httpd.apache.org/docs/2.4/ssl/ssl_howto.html

2. Locate the `<APACHE_HOME>/conf/extra/httpd-ssl.conf` file.
3. Edit the `httpd-ssl.conf` file and ensure that it contains the following lines:


```
SSLEngine on
SSLProxyEngine on
SSLProxyVerify none
SSLProxyCheckPeerCN off
SSLProxyCheckPeerName off
```

Task C Specify Settings for SSL in the Apache httpd.conf File

Edit the `httpd.conf` file and make sure the following settings are specified:

1. Uncomment the line that reads:


```
#LoadModule ssl_module modules/mod_ssl.so
```
2. Uncomment the lines that point to the `httpd-ssl.conf` file:


```
# Secure (SSL/TLS) connections
#Include conf/extra/httpd-ssl.conf
```
3. Edit any lines that specify ProxyPass settings and ensure that they specify HTTPS URLs and the port number for SSL (9133).

For example:

```
ProxyPass /apiKey https://developer.company.com :9133/apiKey
ProxyPassReverse /apiKey https://developer.company.com:
9133/apiKey
```

Task D Configure SSL in the Joomla Administrator

Follow these steps to configure SSL for Joomla:



Make sure that the API Exchange Gateway component is configured to run on SSL. See “Enable Facade HTTPs Transport” in Chapter 4 of the *TIBCO API Exchange Gateway User’s Guide*.

1. Log into the Joomla Administrator user interface.

2. Select **System > Global Configuration**.
3. Click the **Server** tab.
4. From the pull-down menu for Force SSL, select **Entire Site**.
5. Click **Save**.

Task E Edit the `asg_portal.properties` File to Specify SSL Settings

To configure the portal engine for SSL, follow these steps:

1. Go to the `<directory path for asg_portal.properties file>` directory.
2. Edit the `asg_portal.properties` file.
3. Locate the section that is labelled `#Facade HTTPS Channel`.
4. Specify the HTTPS configuration settings as required.

For detailed information, see the section on “Connection Parameters for HTTPs Channel (Facade)” in Table 15, “Core Engine Properties” in Chapter 3 of the *TIBCO API Exchange Gateway User’s Guide*, “Core Engine Configuration.”

5. Edit the lines that specify the Swagger specification document location and the portal server URL prefix, and make sure that they specify an HTTPS URL, as follows:

```
# Portal Engine Swagger specification document location URL
prefix
https://asg.portal.engine.swagger.spec.url.prefix =
https://<portal_engine_hostname>/joomla/uploads/swaggerSpecs/
# Portal Server URL prefix
asg.portal.url.prefix = https://<portal_engine_hostname>/joomla
```

6. Uncomment the following line and ensure that it specifies the hostname of the server running the portal engine, as follows:

```
asg.portal.server.hostname=<portal-engine-server-hostname>
```

7. If you will use Spotfire to output analytic data for API Exchange APIs, add the following lines:

```
#SSL Properties for Spotfire
asg.portal.spotfire.ssl.property.file.path=
<path_to_spotfire_ssl_properties_file>
```

8. Save the `asg_portal.properties` file.

Task F Import the Joomla Security Certificates into the cacerts Keystore

Import the certificates used by Joomla into the TIBCO cacerts keystore. this ensures that the portal engine trust the certificate presented by Joomla.

Follow these steps to import the certificates:

1. Import the certificates used by Joomla into the
<TIBCO_HOME>/tibcojre64/1.7.0/lib/security/cacerts keystore so that the portal engine trusts the certificate presented by Joomla

```
keytool -import -keystore %jre_home%\lib\security\cacerts -alias  
<alias_name> -file <your_cert_file>
```

where *alias_name* is the name of the SSL alias and *your_cert_file* is the filename of your certificate file.

Task G In the Developer Portal, Specify SSL for Environment and Gateway Configuration

When you are configuring the Developer Portal, specify SSL for any environments or gateways that you create:

1. When you create a new environment using the Create New Environment page:
 - a. Make sure that you check the **SSL** check box under the Basepath field.
 - b. If you choose **Yes** for the Managed by Gateway setting, then select **Yes** for the SSL Enabled selection, and specify an HTTPS URL for the Management URL.
2. After you save the environment, then when you create a gateway for the environment on the Create New Gateway page, check the **SSL** check box under the Management URL field.

Chapter 2 **API Analytics**

API Analytics presents statistical information about API usage, for use by the API providers and consumers. The analytical data can be viewed by portal administrators, managers, and developers. This feature requires licensed versions of TIBCO® Spotfire Server and TIBCO® Spotfire Web Player.



The Developer Portal (also referred to as portal) is available if you install the GitHub project *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1* in your environment.

Topics

- [Overview, page 16](#)
- [Configuration, page 17](#)
- [Viewing the Dashboard, page 24](#)

Overview

Analytics for TIBCO® API Exchange Manager requires the following software:

- TIBCO Spotfire® Server
- TIBCO Spotfire® Web Player

These products are distributed and installed separately. Refer to the respective product documentation for instructions to install and configure the software.

Configuration

After you install TIBCO API Exchange, complete the following tasks to configure the various components required to view the API Analytics dashboard.

Task A Configuring TIBCO Spotfire Server

1. Install and configure TIBCO Spotfire Server. Refer to *TIBCO® API Exchange Gateway User's Guide* for instructions to configure the TIBCO Spotfire Server and Client.



If you are using the *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1* component, ensure that the TIBCO Spotfire Web Player instance and the Joomla server are hosted on machines whose fully qualified name share a common suffix that includes the domain name. For example:

joomla.a.b.c.group-g.companyname.com and
spotfirewp.x.group-g.companyname.com

2. Enable Impersonation using the TIBCO Spotfire Configuration Tool.
3. Create a user **asgwebplayer** and add the user to the Impersonator group. This user will be used in [Task B](#) to authenticate TIBCO Spotfire Web Player.
4. Ensure that the Central Logger data is available at the following locations:
 - For MySQL: Database named **asgstat**.
 - For SQLServer: Database named **asgstat**
 - For Oracle: Schema named **asguser**
5. Copy the content of the installed folder that matches your database type into `<TIBCO_SPOTFIRE_SERVER_HOME>\tomcat\application-data\library`:
 - templates/spotfire/mysql
 - templates/spotfire/oracle
 - templates/spotfire/sqlserver
6. Using the **TIBCO Spotfire Client > Tools > Library Administration** menu follow these steps:
 - a. Import `ASG_CL.part0.zip` to the root of the library.
 - b. Choose the option to replace the existing item.

If you choose to keep the existing permissions, you might see warning messages about missing users. You can ignore these warnings.



Do NOT move or rename the imported resource **ASG_CL**.

7. Using the **TIBCO Spotfire Client > Tools > Information Designer > Elements** menu, right-click on the resource **/ASG_CL**, choose **Edit**, and update the data source with your actual connection parameters. Provide valid credentials for authentication.



Do NOT move or rename the imported resource **ASG_CL**.

8. Using the **TIBCO Spotfire Client > Tools > Library Administration** menu, import **ASG.part0.zip** to the root of the library.
9. Open the resource **/ASG/Host** using **File > Open from > Library....**
10. If the information link is not resolved, use the **Browse** option to locate that information link under **/ASG/links/unfiltered**.
11. Click **File > Save as > Library Item...** to save the changes.
12. Open the resource **/ASG/Partner** using **File > Open from > Library....**
13. If any information link is not resolved, use the **Browse** option to locate the information link under **/ASG/links/filtered**.
14. Click **File > Save as > Library Item...** to save the changes.
15. Ensure that the Impersonator group has read access to the **/ASG** directory and the files under it.
16. If needed, you can now move or rename the **/ASG** directory and the **/ASG_CL** resource. If you move or rename the **/ASG** directory (for example, to */new_directory*), update the property `asg.portal.spotfire.library.path.prefix` in `asg-portal.properties` to */new_directory*. This lets the portal gateway know the path of the directory that contains the **Host** and **Partner** resources.



Do not rename the resources **Host** and **Partner** in the TIBCO Spotfire Library. If needed, you can move these resources to a common directory. Ensure that both the resources are available in a common directory. By default, these resources are available in the **/ASG** directory.

Task B Installing and Configuring TIBCO Spotfire Web Player

1. Install TIBCO Spotfire Web Player to enable Web Player connection to the TIBCO Spotfire Server configured in [Task A, Configuring TIBCO Spotfire Server](#).

During Web Player installation, do the following:

- a. When prompted to enter the Virtual directory to create in IIS:
Spotfire Web Player URL pattern:
`http[s]://<servername>/APIXAnalytics/`
- b. Make sure that you specify the virtual directory as shown in the example above, as **APIXAnalytics**.

The name you type here will be part of the Spotfire Web Player URL.

For additional information, see the *TIBCO Spotfire® Web Player 6.0 Installation and Configuration* document—"Installer Options" in the Section 1.6 "Pre-Installation Checklist," and Section 3.2, "Run the Installer."

2. Configure authentication as follows:
 - a. Specify authentication either as Anonymous or as Basic Authentication. If you are using Basic Authentication, update the section on authentication and authorization in `<TIBCO_SpotfireWebPlayer_root>/web.config` as indicated in the following code sample.

```
<!-- ***** AUTHENTICATION: ***** -->
  <!-- Forms authentication: -->
  <!--   <authentication mode="Forms" > -->
  <!--     <forms loginUrl="~/Login.aspx" cookieless="UseCookies"
defaultUrl="~/Default.aspx" slidingExpiration="true"
timeout="525600" /> -->
  <!--   </authentication> -->
  <!-- Windows: -->
  <!--   <identity impersonate="true"/> -->
  <!--   <authentication mode="Windows"> -->
  <!--   </authentication> -->
  <!-- Anonymous/None: (In this case the username and password
from spotfire.dxp.web/authentication/impersonator are used) -->
  <!--   <authentication mode="None"> -->
  <!--   </authentication> -->
  <!-- ***** Copy applicable parameters from above and
replace below: ***** -->
  <authentication mode="None"></authentication>
  <authorization>
    <!--Remove next line <deny users="?">, when using Anonymous
Authentication-->
    <!--<deny users="?" />-->
    <allow users="*" />
  </authorization>
```

- b. Enable Impersonation in the Web Player. Specify the credentials for the user **asgwebplayer** created in [Task A, Configuring TIBCO Spotfire Server](#) for the impersonation.

```
<!--Impersonation: -->
  <!-- This is the username and password or certificate serial
number used for impersonation. -->
  <setting name="ImpersonationUsername" serializeAs="String">
    <value>asgwebplayer</value>
  </setting>
  <setting name="ImpersonationPassword" serializeAs="String">
    <value>asgwebplayer</value>
  </setting>
```

- c. Enable Basic Authentication on the IIS server.

Refer to *TIBCO Spotfire Web Player Installation* > 3.3.1 *Username and Password* and *TIBCO Spotfire Web Player Installation* > 3.3.2 *Anonymous (Pre-configured) Access* for details.

3. Configure the JavaScript API.
 - a. Enable the JavaScript API.
 - b. If you are using the *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1*, set the domain name to the common part of the fully qualified name of the Joomla server and the TIBCO Spotfire server. For example, if you are using `joomla.a.b.c.group-g.companyname.com` and `spotfirewp.x.group-g.companyname.com`, set the domain name to either `companyname.com` or `group-g.companyname.com`.

Refer to section 6.2, “Advanced Web.Config Settings,” in *TIBCO Spotfire Web Player Installation* for details.

Task C Configuring TIBCO® API Exchange Gateway

1. Configure the TIBCO Spotfire Domain to the same values as in [Task B Step 3 b](#).



If you have installed *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1*, you can configure the TIBCO Spotfire Domain with the same value as specified in [Task B Step 3 b](#). above from the Joomla! Administrator > System > Control Panel > Global Configuration > API Manager Configuration and Email Templates.

2. Update the file `asg-portal.properties` located at `<ASG_CONFIG_HOME>` and edit the following properties:
 - Update `asg.portal.spotfire.url.prefix` to specify the hostname and port number of the TIBCO Spotfire Web Player. For example:
`http://hostname:port`
 - If you selected Basic Authentication for TIBCO Spotfire Web Player, update the properties `asg.portal.spotfire.username` and `asg.portal.spotfire.password` to specify the username and password.
 - If you moved or renamed the `/ASG` directory in [Task A step 16](#), update the property `asg.portal.spotfire.library.path.prefix` with the new location.
3. Update the configuration file `TargetOperation.cfg` located at `<ASG_CONFIG_HOME>\PortalProject\` and edit the host name and port number for the service request to provide the TIBCO Spotfire Web Player URL. If you use Basic Authentication, enter the username and password.



If you have installed *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1*, you can access the configuration for the Portal Project from the Developer Portal. Navigate and update the following URIs:

- Portal Project > Routing > Facade Operations > Request > Operation URI to point to the TIBCO Spotfire Web Player.
- Portal Project > Routing > Facade Operations > RequestGet > Operation URI to point to the TIBCO Spotfire Web Player.
- Portal Project > Routing > Target Operations > Request and Portal Project > Routing > Target Operations > Request to point to the TIBCO Spotfire Web Player.
- Portal Project > Routing > Target Operations > Request and Portal Project > Routing > Target Operations > RequestGet to point to the TIBCO Spotfire Web Player.

4. Configure the proxies for the server that proxies requests between the browser and the portal gateway. Edit the file `<apache_home>\conf\httpd.conf` to update the following:

```
ProxyPass /Analytics http://developer.company.com
:9122/SpotfireWeb
ProxyPassReverse /Analytics http://developer.company.com
:9122/SpotfireWeb
ProxyPass /SpotfireWeb http://developer.company.com
:9122/SpotfireWeb
ProxyPassReverse /
SpotfireWeb http://developer.company.com :9122/SpotfireWeb
```

where *developer.company.com* represents the URL used by your company.

Task D (Optional) Set Up One-Way SSL from the Spotfire Server to the Developer Portal

If you will use SSL for communication between the Spotfire server and the Developer Portal, specify SSL configuration settings in the following configuration files:

- The `asg_portal.properties` file
- The `TargetOperation.cfg` file of the Portal project.

Follow these steps to set up one-way SSL for the Spotfire server:

1. Edit the `asg_portal.properties` file:
 - a. Make sure the following URL is an HTTPS URL as in the following example:


```
asg.portal.spotfire.url.prefix=https://<spotfire_hostname>:<spotfire_https_port>
```
 2. Set the `asg.portal.spotfire.ssl.property.file.path` value to specify the absolute path to the SSL properties used for the Spotfire server, as follows:


```
asg.portal.spotfire.ssl.property.file.path=<absolute-path-to-ssl.properties>
```

 For example:


```
asg.portal.spotfire.ssl.property.file.path=/opt/tibcoasgconfig/tibco/cfgmgmt/asg/PortalProject/wss/ssl.properties
```
3. Add an `ssl.properties` file to the directory as stated above.

[Example 1](#) shows a sample `ssl.properties` file.

Example 1 Sample `ssl.properties` File for Spotfire

```
com.tibco.trinity.runtime.core.provider.identity.trust.enableTrustStoreAccess=true
```



```

com.tibco.trinity.runtime.core.provider.identity.trust.trustStores
erviceProvider=class:com.tibco.trinity.runtime.core.provider.credent
ntial.keystore
com.tibco.trinity.runtime.core.provider.credential.keystore.keySto
reLocation=/root/Desktop/AllCerts/SpotfireServerCert.pfx
com.tibco.trinity.runtime.core.provider.credential.keystore.keySto
rePassword=password
com.tibco.trinity.runtime.core.provider.credential.keystore.keySto
reProvider=
com.tibco.trinity.runtime.core.provider.credential.keystore.keySto
reRefreshInterval=60000
com.tibco.trinity.runtime.core.provider.credential.keystore.keySto
reType=PKCS12

```

4. Edit the PortalProject configuration found under the *TIBCO_CONFIG_HOME* directory, and make sure the *TargetOperation.cfg* file contains a line configuring the HTTPS service for Spotfire, as in the following example:

```

service_Request|HTTPS|||20000,0,0,0|||||/APIXAnalytics|gov-w
as.na.tibco.com|443|Administrator|!tlseasy|*,{uri_suffix},{query_s
tring}|POST|ssl.properties|true
service_RequestGet|HTTPS|||20000,0,0,0|||||/APIXAnalytics|go
v-was.na.tibco.com|443|Administrator|!tlseasy|*,{uri_suffix},{quer
y_string}|GET|ssl.properties|true

```

5. Import the Spotfire certificate into the cacerts keystore found at:
<TIBCO_HOME>/tibcojre64/1.7.0/lib/security/cacerts.

To import the certificate, use the **keytool** command as shown below:

```

keytool -import -keystore %jre_home%\lib\security\cacerts -alias
<alias_name> -file <your_cert_file>

```

where *alias_name* is the name of the SSL alias and *your_cert_file* is the filename of your certificate file.

Viewing the Dashboard

Portal administrators, managers, and application developers can view the dashboard from the Developer Portal. The Developer Portal is available if the GitHub project *Adapter Code for TIBCO API Exchange and Joomla! 2.1.1* is installed in your environment.



To view the dashboard, access the Developer Portal using a host name that matches the domain name configured in the Joomla! Administrator back-end and in TIBCO Spotfire Web Player. For example, if the domain specified in the configuration is `companyname.com`, the portal web site must be accessed using `http://hostname.a.b.companyname.com`.

The dashboard provides two views - host and partner, and each view contains multiple pages. All the pages can be customized using TIBCO Spotfire.

Depending on the role, a user is presented with one or both the views:

- If the user is a **member of an organization**, the user is presented with the partner view for his/her organization. For example, developers and managers of the same organization are presented with the same view.
- If the user is a portal administrator, the user is presented with the host view and partner views for all the partners.

Figure 1 illustrates an example page on the dashboard.

Figure 1 Sample Page on the Dashboard



Filtering Data on the Dashboard

The dashboard provides information on the API usage for an organization across applications and products.

The data on the dashboard can be filtered in one of the following ways:

- By options: Select one or more of the options such as applications, products, operations, time interval, or status.
- By different areas: Select different areas on the graph also act as filters.

Index

A

API analytics [15](#)
 configuration [17](#)
 viewing the dashboard [24](#)

C

customer support [x](#)

P

partner management [8](#)
portal administration [2](#)
product management [6](#)

S

support, contacting [x](#)

T

technical support [x](#)
TIBCO_HOME [viii](#)