TIBCO® API Exchange Manager Administration

Software Release 2.3
September 2016

Two-Second Advantage®

Important Information

Contents

TIBCO Documentation and Support Services

Documentation for this and other TIBCO products is available on the TIBCO Documentation site. This site is updated more frequently than any documentation that might be included with the product. To ensure that you are accessing the latest available help topics, please visit:

https://docs.tibco.com

Product-Specific Documentation

Documentation for TIBCO products is not bundled with the software. Instead, it is available on the TIBCO Documentation site. To directly access documentation for this product, double-click the following file:

`TIBCO_HOME/asg/2.3/doc/manager/index.html`

where *TIBCO_HOME* is the top-level directory in which TIBCO products are installed. On Windows, the default *TIBCO_HOME* is `C:\tibco`. On UNIX systems, the default *TIBCO_HOME* is `/opt/tibco`.

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

- *TIBCO API Exchange Manager Installation*
- *TIBCO API Exchange Manager Administration*
- *TIBCO API Exchange Manager Release Notes*
- *TIBCO API Exchange Concepts*
- *TIBCO API Exchange Getting Started*

How to Contact TIBCO Support

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

- 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.

How to Join TIBCOmmunity

TIBCOmmunity 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. TIBCOmmunity offers forums, blogs, and access to a variety of resources. To register, go to the following web address:

https://www.tibcommunity.com

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! 2.2.0 in your environment.

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! 2.2.0 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! 2.2.0 documentation for detailed instructions: http://github.com/API-Exchange/JoomlaAdapter/wiki.

User Roles Management

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! 2.2.0 in your environment, the portal administrator can create the users and user roles in the Joomla! Administrator backend.

Environments and Gateways Management

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! 2.2.0 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**

The base configuration is set by the portal administrator, also referred to as the API provider, and does not change when application developers push updates from the portal. Base configuration is not environment specific.

- **Access configuration**

The 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 the master configuration and the gateway instances' local configuration.

When moving the gateway configuration from a development environment to a production environment, 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 advisable 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 Adapter Code for TIBCO API Exchange and Joomla! 2.2.0, you can access the gateway configuration UI 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.

Admin Subscription Management

When you log in to the Joomla! Administrator back-end as an administrator, you can view the active and inactive subscriptions by clicking the **Subscriptions** tab.

In the **Subscriptions** tab, you can achieve the following operations:

- View the subscription name, start date, end date and current status for all of your accepted subscriptions.
- Create a new subscription by clicking **Create New Subscription**, and then fill out the creation form.
- Edit an existing subscription by clicking the subscription name, and then click **Edit** on the Subscription Details page.
- Approve or reject your pending subscriptions. To approve and reject a subscription request, move your mouse pointer over the **Subscriptions** tab, and then click **Request**. After reviewing the request details, if you want to approve the request, enter a start date, end date, and an optional note, and then click **Confirm Approval**; otherwise, add a note, and then click **Confirm Rejection**.

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 Adapter Code for TIBCO API Exchange and Joomla! 2.2.0, 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! 2.2.0* 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 Adapter Code for TIBCO API Exchange and Joomla! 2.2.0 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 A*dapter Code for TIBCO API Exchange and Joomla! 2.2.0* 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 Adapter Code for TIBCO API Exchange and Joomla! 2.2.0 refer to the *Adapter Code for TIBCO API Exchange and Joomla! 2.2.0* documentation for details.

OAuth 2.0 Scopes Management

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: http://docs.tibco.com.

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 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! 2.2.0 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! 2.2.0* documentation for detailed instructions.

APIs Management

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

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, that is, 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! 2.2.0, specifying duplicate resource paths might result in the swagger specifications being displayed incorrectly in the API explorer.

- Downloadable documentation.
- Available inline documentation.

Products and Associated Plans Management

After 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! 2.2.0 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! 2.2.0* documentation for detailed instructions.

Organizations Management

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.

Users Management

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 Adapter Code for TIBCO API Exchange and Joomla! 2.2.0, it is best practice that you do **not** change the pre-configured user groups and access levels in the Joomla! Administrator back-end.

Applications Management

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 might 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.

Subscriptions Management

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.

Throttle Quotas Management

When registering products or applications, the portal administrator can specify throttle quotas.

A throttle quota is an absolute 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 the usager alert threshold value exceeds. The alerts are displayed on Dashboard pages.

In addition, the Product Page allows for flexibility in the throttle time range for proxy. You can create product plans which contains monthly or yearly flexibility information.

Logging

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

- Edit the *<ASG_CONFIG_HOME>*`\asg_portal.properties` file and update the `tibco.clientVar.ASG/Logging/MinLogLevel` property to set it with one of the following log levels:
  - 0: `DEBUG`
  - 1: `INFO`
  - 2: `WARN`
  - 3: `ERROR`
  - 4: `No Logging`
- Edit the *<ASG_HOME>*`\2.1\bin\asg-portal.cdd` file 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 Adapter Code for TIBCO API Exchange and Joomla! 2.2.0, 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! 2.2.0 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. You can configure the portal engine and the Developer Portal for SSL.

You might experience troubleshooting the very first time the HTTPS call is invoked from the API Explorer when the certificate is not already installed in the browser. To resolve the issue complete the following steps:

1. Get the Portal Engine, Gateway and Joomla all on HTTPS.
2. Login as a developer.
3. Request a subscription.
4. Send a request through the API Explorer.

Ensuring 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.

Procedure

1. Enable HTTPS on the API Exchange Gateway.

   See "Enable Facade HTTPs Transport" in the *TIBCO API Exchange Gateway User's Guide* for information on enabling HTTPS on the API Exchange Gateway.

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.

Setting up Apache Web Server to Run on SSL

You can set up Apache Web Server to Run on SSL.

Procedure

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
```

Specifying Settings for SSL in the Apache httpd.conf File

Procedure

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
```

Configuring SSL in the Joomla Administrator

Make sure that the API Exchange Gateway component is configured to run on SSL. See "Enable Facade HTTPs Transport" in *TIBCO API Exchange Gateway User's Guide* for more details.

Procedure

1. Log in to 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**.

Configuring the Portal Engine for SSL

Procedure

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.

   See the "Connection Parameters for HTTPs Channel (Facade)" and "Core Engine Properties" sections in *TIBCO API Exchange Gateway User's Guide* for more details.
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
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 host name of the server running the portal engine, as follows:

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

7. If you 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.

Importing the Joomla Security Certificates into TIBCO Cacerts Keystore

Import the certificates used by Joomla to the keystore so that the portal engine trusts the certificate presented by Joomla.

Procedure

1. Import the certificate used by Joomla into the `TIBCO_HOME/tibcojre64/1.7.0/lib/security/cacerts` directory by using the following command:

   `keytool - import -trustcacerts - alias alias_name -file filename - keystore keystore_name`

   where:

   alias_name is the name of the SSL alias.

   filename is the name of the certificate file.

   keystore_name is the `jre_home\lib\security\cacerts` directory.
2. In Developer Portal, specify the SSL for Environment and Gateway Configuration.

Configuring the Developer Portal and Specifying SSL for any Environments or Gateways

Procedure

1. Make sure that you select the **SSL** check box under the **Base path** field.
2. 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.
3. After you save the environment, create a gateway for the environment on the Create New Gateway page, by selecting the **SSL** check box under the **Management URL** field.

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 the portal, is available if you install the GitHub project *Adapter Code for TIBCO API Exchange and Joomla! 2.2.0* in your environment.

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.

Configuring TIBCO Spotfire Server

Configure TIBCO Spotfire Server.

Procedure

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 Adapter Code for TIBCO API Exchange and Joomla! 2.2.0 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 by using the TIBCO Spotfire Configuration Tool.
3. Create a user **asgwebplayer** and add the user to the Impersonator group.

   This information is needed 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 the *`TIBCO_SPOTFIRE_SERVER_HOME`*`\tomcat\application-data\library` directory:

   ```
   templates/spotfire/mysql
   templates/spotfire/oracle
   templates/spotfire/sqlserver
   ```
6. Under the **TIBCO Spotfire Client** > **Tools** > **Library Administration** menu, complete the following steps:

   a) Import the `ASG_CL.part0.zip` file to the root of the library.
   b) 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. Under the **TIBCO Spotfire Client** > **Tools** > **Information Designer** > **Elements** menu, right-click on the resource **/ASG_CL**, click **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. Under the **TIBCO Spotfire Client** > **Tools** > **Library Administration** menu, import the `ASG.part0.zip` file to the root of the library.
9. Open the resource **/ASG/Host** by clicking **File** > **Open from** > **Library** . If the information link is not resolved, use the **Browse** option to locate that information link under **/ASG/links/unfiltered**.
10. Click **File** > **Save as** > **Library Item** to save the changes.
11. Open the resource **/ASG/Partner** by clicking **File** > **Open from** > **Library** . If any information link is not resolved, use the **Browse** option to locate the information link under **/ASG/links/filtered**.
12. Click **File** > **Save as** > **Library Item** to save the changes. Ensure that the Impersonator group has read access to the `/ASG` directory and the files under it.

    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, rename it to /*new_directory*), update the property `asg.portal.spotfire.library.path.prefix` in the `asg_portal.properties` file to /*new_directory*. This makes 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 TIBCO Spotfire Library. If it is required, 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.

Installing and Configuring TIBCO Spotfire Web Player

Install and configure TIBCO Spotfire Web Player.

Procedure

1. Install TIBCO Spotfire Web Player to enable the Web Player connection to TIBCO Spotfire Server.
   a) When you are prompted to enter the Virtual directory to create in IIS, type the following text:

   ```
   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 is part of the Spotfire Web Player URL.

      See the “Pre-Installation Checklist” and “Run the Installer” sections in *TIBCO Spotfire® Web Player 6.0 Installation and Configuration* for more information.

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 `the` *`TIBCO_SpotfireWebPlayer_root`*`/web.config` file 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 WEb Player. Specify the credential for the user **asgwebplayer** 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.

See *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 more details, which are available on http://docs.tibco.com.

3. Configure the JavaScript API.

a) Enable the JavaScript API.

b) If you are using Adapter Code for TIBCO API Exchange and Joomla! 2.2.0, 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`.

See “Advanced Web.Config Settings” in *TIBCO Spotfire Web Player Installation* for more details.

Configuring TIBCO® API Exchange Gateway

Configure TIBCO API Exchange Gateway.

Procedure

1. Configure TIBCO Spotfire Domain.

> If you have installed Adapter Code for TIBCO API Exchange and Joomla! 2.2.0, you can configure the TIBCO Spotfire Domain under **Joomla! Administrator** > **System** > **Control Panel** > **Global Configuration** > **API Manager Configuration and Email Templates** .

2. Update the asg-portal.properties file, which is located at *`ASG_CONFIG_HOME`* and edit the following properties:

   - Update the `asg.portal.spotfire.url.prefix` property to specify the host name 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 `asg.portal.spotfire.username` and `asg.portal.spotfire.password` properties to specify the user name and password.
- If you moved or renamed the **`/ASG`** directory to update the `asg.portal.spotfire.library.path.prefix` property with the new location.

3. Update the `TargetOperation.cfg` configuration file that is located under the *`ASG_CONFIG_HOME`*`\PortalProject` directory 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 user name and password. Under **Project** > **Routing**, complete the following operations:

   - In the **TargetOperations** tab, set URI, Host, Port and optionally user name and password if basic authentication is enabled for Operations Request and RequestGet.
   - In the **Facade Operation** tab, set the Operation URI to the URI that is set in TargetOperation for Operations Request and RequestGet.

   > Access the gateway configuration either through the API management portal or by directly launching it in a browser as `http://host:port/ConfigUI`. The host is the machine where ConfigUI is running and the port is on which the Config UI is running. By default, these are `localhost` and `9200` respectively.

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

```
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` is the URL used by your company.

Setting Up One-Way SSL Communication Between Spotfire and the Developer Portal (Optional)

You can set up one-way SSL for the Spotfire server with the `asg_portal.properties` and `TargetOperation.cfg` files of the Portal project.

Procedure

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 value of the `asg.portal.spotfire.ssl.property.file.path` property to the absolute path to the SSL properties used for the Spotfire server, for example:

```
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 previously.

   The following example shows the `ssl.properties` file.

```
com.tibco.trinity.runtime.core.provider.identity.trust.enableTrustStoreAccess=tru
e
com.tibco.trinity.runtime.core.provider.identity.trust.trustStoreServiceProvider=
class:com.tibco.trinity.runtime.core.provider.credential.keystore
com.tibco.trinity.runtime.core.provider.credential.keystore.keyStoreLocation=/
root/Desktop/AllCerts/SpotfireServerCert.pfx
com.tibco.trinity.runtime.core.provider.credential.keystore.keyStorePassword=pass
word
com.tibco.trinity.runtime.core.provider.credential.keystore.keyStoreProvider=
com.tibco.trinity.runtime.core.provider.credential.keystore.keyStoreRefreshInterv
al=60000
com.tibco.trinity.runtime.core.provider.credential.keystore.keyStoreType=PKCS12
```

4. Edit the `PortalProject` configuration that is located under the *`TIBCO_CONFIG_HOME`* directory, and make sure the `TargetOperation.cfg` file contains a line configuring the HTTPS service for Spotfire, for example:

```
service_Request|HTTPS|||20000,0,0,0||||||||||/APIXAnalytics|gov-
was.na.tibco.com|443|Administrator|!t1seasy|*,{uri_suffix},{query_string}|POST|
ssl.properties|trueservice_RequestGet|HTTPS|||20000,0,0,0||||||||||/
APIXAnalytics|gov-was.na.tibco.com|443|Administrator|!t1seasy|*,{uri_suffix},
{query_string}|GET|ssl.properties|true
```

5. Import the Spotfire certificate into the `cacerts` keystore that is located in *`TIBCO_HOME`*`/tibcojre64/1.7.0/lib/security/cacerts` directory by using the following command:

```
keytool - import -trustcacerts - alias alias_name -file filename - keystore keystore_name
```

where:

alias_name is the name of the SSL alias.

filename is the name of the certificate file.

keystore_name is the *`jre_home`*`\lib\security\cacerts` directory.

Dashboard View

Portal administrators, managers, and application developers can view the dashboard from the Developer Portal. The Developer Portal is available if the Adapter Code for TIBCO API Exchange and Joomla! 2.2.0 GitHub project 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.

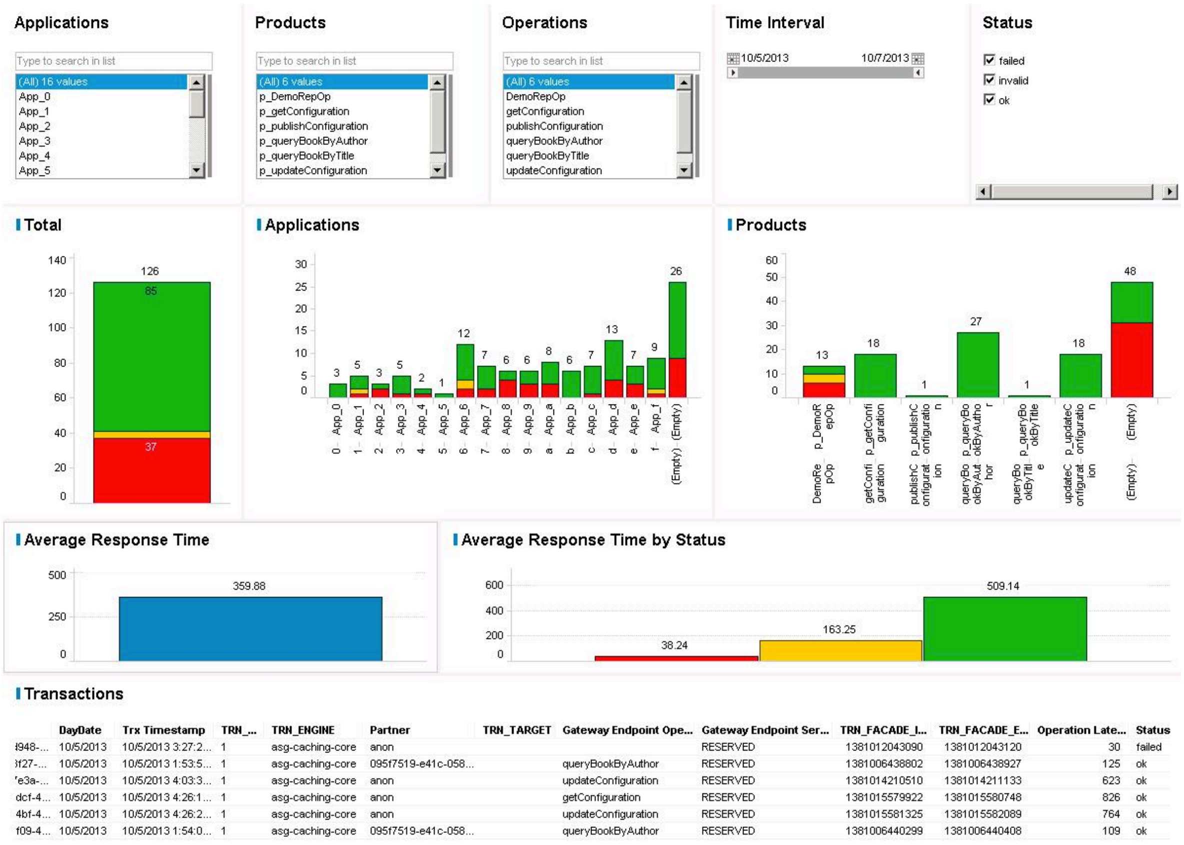
Depending on the role, a user is presented with one or both the views:

- If the user is a **member of an organization**, the user is presented with the partner view for his or 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.

  See "Log Request Headers" in *TIBCO® API Exchange Gateway User's Guide* for more details regarding the logging and viewing request headers on Spotfire dashboard,.

The following figure illustrates an example page on the dashboard.

Sample Page on the Dashboard



	DayDate	Trx Timestamp	TRN_...	TRN_ENGINE	Partner	TRN_TARGET	Gateway Endpoint Ope...	Gateway Endpoint Ser...	TRN_FACADE_I...	TRN_FACADE_E...	Operation Late...	Status
948-...	10/5/2013	10/5/2013 3:27:2...	1	asg-caching-core	anon			RESERVED	1381012043090	1381012043120	30	failed
f27-...	10/5/2013	10/5/2013 1:53:5...	1	asg-caching-core	095f7519-e41c-058...		queryBookByAuthor	RESERVED	1381006438802	1381006438927	125	ok
e3a-...	10/5/2013	10/5/2013 4:03:3...	1	asg-caching-core	anon		updateConfiguration	RESERVED	1381014210510	1381014211133	623	ok
dcf-4...	10/5/2013	10/5/2013 4:26:1...	1	asg-caching-core	anon		getConfiguration	RESERVED	1381015579922	1381015580748	826	ok
4bf-4...	10/5/2013	10/5/2013 4:26:2...	1	asg-caching-core	anon		updateConfiguration	RESERVED	1381015581325	1381015582089	764	ok
f09-4...	10/5/2013	10/5/2013 1:54:0...	1	asg-caching-core	095f7519-e41c-058...		queryBookByAuthor	RESERVED	1381006440299	1381006440408	109	ok

Editing the Number of Alerts Displayed on the Dashboard

You can edit the number of alerts displayed on the dashboard. The count of alert message number can be set at the backend.

Procedure

1. Login to the Joomla backend Administrator as Admin 2.
2. Navigate to **System > Global Configuration**.
3. Select the API Manager Configuration and Email Templates.
4. Edit the **Show Alerts Count** field as required.

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.