



Adapter Code for TIBCO® API Exchange and Joomla!

Administration Guide

*Version 2.3.4
November 2021*



Contents

Contents	2
Administration from the Joomla! Administrator User Interface	4
Global Configuration	4
Updating the API Manager Configuration	4
API Manager Mail Server Configuration	5
API Manager Email Templates	6
Changing Columns Displayed on API Manager Logs	6
User Management	7
Managing User Password Parameters	7
Changing a User's Email Address	9
Enabling SSL Certificate Download for Developer Portal Users	10
Enabling OAuth and Scopes Configuration	12
API Manager Portal Administration	14
Managing User Roles	14
Creating an Organization	14
Adding a Member to the Organization	15
Creating a Manager Role	16
Viewing an Organization's Information	16
Managing Environments and Gateways	17
Creating an Environment	17
Adding a Gateway to an Environment	20
Managing Environment Configurations	20
Managing Subscriptions	22
Viewing Subscription Requests	22
Viewing Subscriptions	23
Creating a Subscription	25
Approving Subscription Requests	26

Managing Scopes	28
Creating a Scope	28
Managing APIs	29
Creating an API	29
Adding an Operation	31
Managing Portal REST API	31
Managing Products and Associated Plans	32
Creating a Product	32
Creating a Product Plan	33
Associating a Base path with a Product	35
Adding a Product Category	35
Administering Developer Forums	36
Configuring the Developer Portal for Developer Forum Comments	36
Editing Comments	39
Using the Application Dashboard	39
Viewing the API Analytics Dashboard	41
Contacting Support	42
TIBCO Documentation and Support Services	43
Legal and Third-Party Notices	45

Administration from the Joomla! Administrator User Interface

The portal administrator can update the global configuration for API Manager properties using the Joomla! Administrator back-end. By using the portal administrator through Joomla! Administrator, you can manipulate the user interface, such as managing users, updating global configurations, and modifying templates.

Global Configuration

If you have followed the installation instructions provided in *Adapter Code for TIBCO® API Exchange Manager and Joomla! Installation*, the Administrator back-end is available at `http://<host>:<port>/joomla/administrator`.

Updating the API Manager Configuration

Procedure

1. Log in to the Joomla! administrator back-end as an administrator.
2. Go to **System > Global Configuration > API Manager Configuration and Email Templates**.
3. Update the properties as described in the following table.

Table System > Global Configuration Properties

Field	Description
TIBCO Spotfire® Domain	<p>Specifies the common domain suffix for the machines hosting the Joomla server and TIBCO Spotfire® Web Player.</p> <p>This property enables the loading of analytical data from the hosts that share the common domain suffix.</p>

Field	Description
ConfigUI URL	Specifies the URL of the TIBCO® API Exchange Gateway Config UI.
Show Ping	Select YES to provide an option to log in to the API Portal using Ping identity for authentication.
Ping URL	Specifies the URL of the Ping Identity Server.

4. Click **Save** to save your changes, or **Save & Close** to save your changes and return to the Joomla! Administrator welcome page.

API Manager Mail Server Configuration

You can configure the mail server that is used to send the notification emails. Email notifications are sent to the portal administrators when certain events occur. For example, when an application developer places a request for a plan, or when a portal administrator approves the request and creates a subscription for the requestor, or when a user logs a support request.

Procedure

1. Log in to the Joomla! administrator back-end as an administrator.
2. Go to **System > Global Configuration** and click the **Server** tab.
3. Update the fields under Mail Settings with your mail server details:
 - **Mailer** Select a tool to send emails from the portal: PHP Mail, Sendmail, or SMTP.
 - **From email** Enter the sender's email to be used to send site emails.
 - **From Name** Enter the sender's name to be used when sending site emails.
 - **Sendmail Path** Enter the directory path to the sendmail program on the host server.
 - **SMTP Authentication** Choose **YES** if your SMTP host requires authentication.
 - **SMTP Security** Select the security model to be used by the SMTP server from the drop-down list: SSL or TLS.

- **SMTP Port** Enter the port number for the SMTP server. Typically, the port number for most non-secure servers is 25, and for most secure servers it is 465.
 - **SMTP Username** Enter the user name to access the SMTP host.
 - **SMTP Password** Enter the password for the SMTP host.
 - **SMTP Host** Enter the name of the SMTP host.
4. Click **Save** to save your changes, or **Save & Close** to save your changes and return to the Joomla! Administrator welcome page.

API Manager Email Templates

You can update the email templates. The content of the notification emails is based on a template and can be modified to suit your needs.

Procedure

1. Login to the Joomla! administrator back-end and navigate to **Components > API Manager Components & Email Templates**.
All the available email templates are listed.
2. Click on the **Subject** of the email template to open the template for editing.
3. Update the content of the email template, ensuring that you do not modify the variables specified between braces (for example, {USER}). You can also update the email subject and type of email: text or HTML.



Note

It is best practice that you do NOT modify the email alias.

4. Click **Save & Close** to update the template, or click **Save & New** to save your changes and open a form for a new template.

Changing Columns Displayed on API Manager Logs

The responses received from the server are logged and can be viewed by selecting **Components > API Manager Log**.

From the Filter option, you can choose to view all logs or deleted logs.

From the Search Option, you can search the logs based on the **User ID** or **Content** fields and retrieve a subset of the logs that match your search criteria.

Procedure

1. Log in to the Joomla! Administrator back-end and navigate to **System > Global Configuration > API Manager Log**.
2. By default, all the fields are set to **Yes**. Update the value for the fields that you do not want to display.

User Management

The portal administrator is a member of the Super Users group and has the highest level of access. After selecting **Users > User Manager**, the portal administrator can perform the following user management tasks:

- Assign users to user groups.
- Update the group membership of existing users.
- Activate or de-activate a user.
- Enable or disable a user.



Warning

Do not use the Joomla! User Manager page to create new users. Users should register using the self-registration feature of the Developer Portal. Also, do **not** modify the access levels defined for the User Groups.

Refer to the Joomla! documentation for details on user management.

Managing User Password Parameters

You can set password parameters for Developer Portal users through the Joomla administration utility. You can specify the following parameters:

- Minimum Password Length
- Password Minimum Integers
- Password Minimum Symbols
- Password Upper Case Minimum

Procedure

1. Log in to the Joomla! Administrator back-end and navigate to **Users > User Manager**.
The User Manager page appears.

- At the upper right of the page, click **Options**.

The User Manager Components page appears, as shown in the following figure:

The screenshot shows the Joomla! User Manager Components Options page. The 'Component' tab is selected. The settings are as follows:

- Allow User Registration:** Yes (selected)
- New User Registration Group:** - Registered
- Guest User Group:** - Guest
- Send Password:** Yes (selected)
- New User Account Activation:** Self
- Notification Mail to Administrators:** No (selected)
- Capcha:** - Use Default -
- Frontend User Parameters:** Show (selected)
- Frontend Language:** Hide (selected)
- Change Login Name:** No (selected)
- Maximum Reset Count:** 10
- Time in Hours:** 1
- Minimum Password Length:** 4
- Password Minimum Integers:** 0
- Password Minimum Symbols:** 0
- Password Upper Case Minimum:** 0

- Leave the first ten fields set to the default.
- Change the following parameters as required:
 - Minimum Password Length** Specify the minimum required password length.
 - Password Minimum Integers** Specify the minimum number of integers required in the user password.
 - Password Minimum Symbols** Specify the minimum number of special characters required in password.

- **Password Upper Case Minimum** Specify the minimum number of uppercase letters required in passwords.

5. Click **Save**.

Changing a User's Email Address

You can change a user's email address. Email addresses are created when a user registers as a Developer Portal user from the self registration interface. Using the User Manager interface in the Joomla back-end, you can change a user's email address as needed.

Procedure

1. In the Joomla Administrator, go to **Users > User Manager**.
2. Locate the record for the user whose email you wish to change, and note the user's ID. For example, for the Host Administrator, this ID is 129.
3. Click on the user's name to go to the Edit page for their Joomla user record.
4. Update the user's email address and click **Save**. If the user's user name is an email address, change it to the new email address at this time.

5. In the MySQL database, locate the record ID for this user by using the following query:

```
SELECT `record_id` FROM `openapi_js_res_record_values` WHERE `field_id`=77 AND `field_value`=<ID_FROM_STEP_2>
```

where <ID_FROM_STEP_2> is the ID of the Joomla user record identified in Step 2.

For the Host Administrator, this should return 219 as the record_id.

6. Locate the actual record for the user profile with the following query:

```
SELECT `fields` FROM `openapi_js_res_record` WHERE `id`=<ID_FROM_STEP_4>
```

where <ID_FROM_STEP_4> is the record_id returned as the result of the query in step 4.

This returns JSON code that looks similar to the following code:

```
{"77":"129","88":
["Manager"],"113":null,"101":"admin","102":"admin@local.host","121":
{"country":"1","region":"650","tel":"8461000","ext":""},"45":"Host","46":"SuperAdmin","47":"68","50":["68"]}
```

7. Change the value of field '102' in the JSON code from its current email address to the new email address.

8. Locate the record for the email address of the user profile with the following query:

```
SELECT * FROM `openapi_js_res_record_values` WHERE `field_id`=102 AND
`record_id`=<ID_FROM_STEP_4>
```

where <ID_FROM_STEP_4> is the result of the query in Step 4.

9. Change that record's 'field_value' column from the old email address to the new email address.

10. Locate the record for the user name of the user profile with the following query:

```
SELECT * FROM `openapi_js_res_record_values` WHERE `field_id`=101 AND
`record_id`=<ID_FROM_STEP_4>
```

where <ID_FROM_STEP_4> is the result of the query in step 4.

11. If the 'field_value' for this record is an email address, change the 'field_value' from the old email address to the new email address.

Enabling SSL Certificate Download for Developer Portal Users

You can enable SSL certificate download. After initial installation of the Developer Portal, when users attempt to view the defined APIs provided with API Exchange Manager, they are not able to see the APIs.

To enable Developer Portal users to see the APIs, you must use the Joomla administration utility to configure the installation to allow users to download SSL certificates.

Procedure

1. Log in to the Joomla! Administrator back-end and navigate to **Components > Cobalt 8 > Sections**.
2. In the list of sections, click **Products**.


The Edit section products page appears.

3. At the bottom of the page, click **Toggle Editor**.

A window appears that displays the current XML coding for the initial login screen.

4. Select the existing XML code.
5. Change the code to contain additional section tags and text similar to the following code:

```
<div class="section-description">
<h3>Browse our API Catalog</h3>
<div class="guests-only"><a title="Contact us"
href="index.php/component/users/?view=registration">Register</a>
for an account, request a plan, create an API key and build your
app.</div>
<div class="registered-only">In order to use our APIs in the API
Explorer, you will first need to install our certificate in your
browser. <a href="https://<apiserver.com>/" target="_blank">Click
Here</a> and the accept the certificate in the new page to
install it in your browser.</div>
</div>
```

Note  The *apiserver.com* URL value shown in the code example above is a sample URL. You must specify the actual URL of the host in your installation that is running the Developer Portal.

6. Click **Toggle Editor**.

The formatted version of the XML code appears in the XML window, similar to the following label:

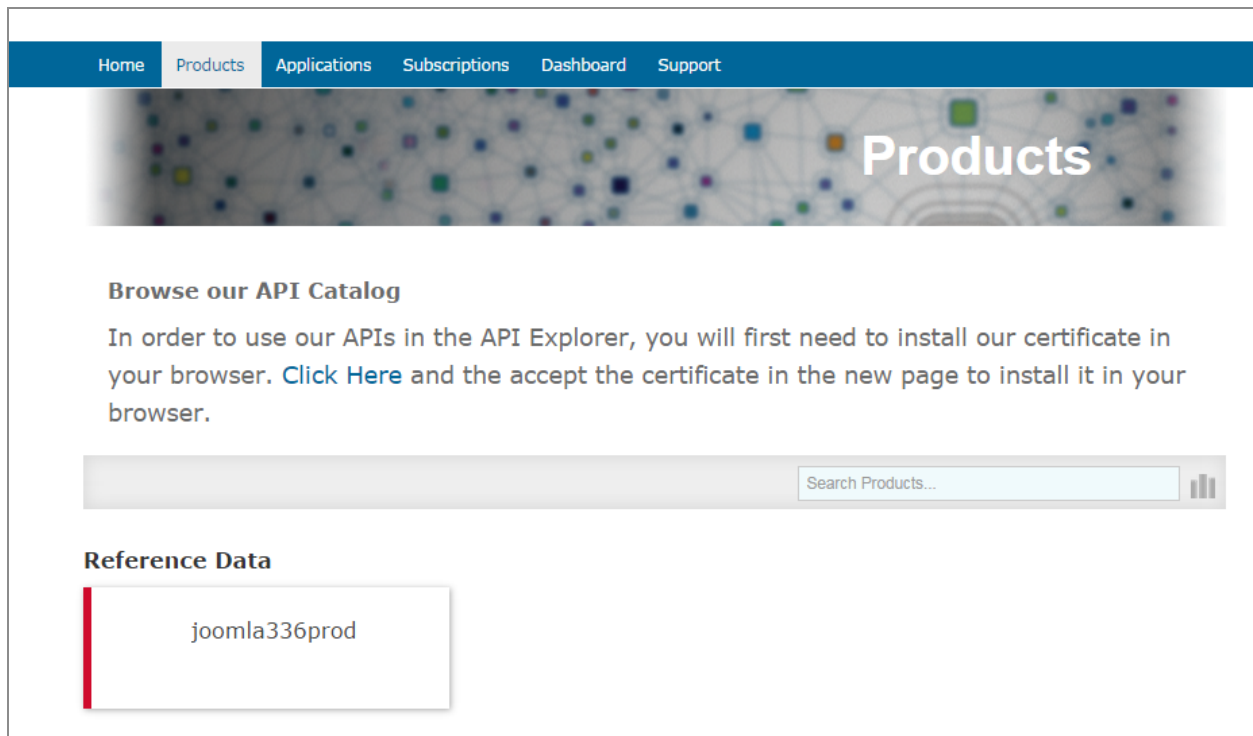
Browse our API Catalog

Register for an account, request a plan, create an API key and build your app.

In order to use TIBCO APIs in the API Explorer, you must install TIBCO certificate in your browser. Click **Here** and the accept the certificate in the new page to install it in your browser.

7. Click **Save**.

When users log in and navigate to the Products page, they see the specified text, as shown in the following figure:



Enabling OAuth and Scopes Configuration

You can enable OAuth and scopes configuration. By default, after initial installation of the Developer Portal, OAuth authorization and the associated scopes configuration for users who access applications that require OAuth authorization are turned off.

If your organization is using OAuth authorization to enable access to services provided by third-party vendors, you can configure OAuth in the Joomla administration utility. When you turn on OAuth authorization, API developers have the option of specifying OAuth authorization for the application when they register it, and the **Scopes** tab is active in the Developer Portal.

Procedure

1. Log in to the Joomla! administrator back-end as an administrator.
2. Go to **System > Global Configuration > API Manager Configuration and Email Templates**.

The API Manager page appears:

The screenshot shows the Joomla! Administrator User Interface. The top header is dark blue with the Joomla! logo and the title "API Manager Configuration & Email Templates Manager Options". Below the header is a light gray bar with four buttons: "Save" (green), "Save & Close" (green), "Cancel" (red), and "Help" (blue). The main content area is divided into two columns. The left column is a sidebar with a menu. The right column contains configuration options for the "Component" tab.

SYSTEM	Component
Global Configuration	
COMPONENT	
Banners	TIBCO Spotfire® Domain
Cache Manager	ConfigUI URL
Checkin	Enable OAuth
Cobalt 8	
Contacts	Show Ping
Articles	
API Manager Configuration and Email Templates	Ping URL
Smart Search	Show Alerts Count
Installation Manager	
Joomla! Update	Re-Sync DB with portal
Language Manager	
API Manager Log	

By default, the Default APIKey setting is active.

3. Click the **Default OAuth** setting next to Enable OAuth and then click **Save**.

Developer Portal users see the OAuth configuration section on the Register Application interface, and the Scopes tab is active.

For information on setting OAuth in the Developer Portal, see “Registering and Application” in the **Adapter Code for TIBCO API Exchange and Joomla User’s Guide**.

API Manager Portal Administration

The Developer Portal (also referred to as the portal) provides an interface for portal administrators to perform tasks such as creating environments and adding gateways, and managing users, subscriptions, and scopes.

Managing User Roles

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

Creating an Organization

Actor: Portal Administrator

Procedure

1. Log in to the Developer Portal as a portal administrator.
2. Click the **Organizations** tab, and then click **Create New Organization**.
The Create New Organization interface appears.
3. Specify the following information to identify the organization:
 - **Title** Enter a short and unique name for the organization.
 - **Description** Enter a description for the organization.
 - **Organization Type** Choose the organization type from the options in the drop-down list: host and partner.



Note

Ensure that only one organization is defined as a host organization.

- **Email** Enter a contact email address for the organization contact person. This email is used for notifications and may represent a single user or a distribution group.

- **Threshold** Enter a number between 0 and 100 that specifies a threshold usage percentage at which you will receive an alert notification.
 - **Contact Details**
 - Address Fields** Enter address details for the organization contact.
 - Instant Contacts** Enter a telephone number for the organization contact.
4. Click **Save** to create the organization.
- An organization detail page appears for the organization.
- The newly created organization is listed on the **Organizations** tab.

Adding a Member to the Organization

Actor: Portal Administrator

After creating an organization, the portal administrator can add members and update additional information for the organization.

Procedure

1. Log in to the API Manager Portal as a portal administrator.
2. Click the **Organizations** tab and then click the name of the organization.
3. Click **New Member** under Members.

The Create a New User profile interface appears.
4. Specify the following information to identify the user:
 - **User profile title** Enter a name for the user profile. This name is used to display the user name on the UI.
 - **System User** Select an existing Joomla! (system) user to associate with this user profile. Use this field only when there is an existing Joomla! user in the system for which there is no user profile created.
 - **User type** Choose the user type from the options in the drop-down list: Developer, Contact, or Manager.
 - **Email** Enter the email address for the user.
 - **First name** Enter the user's first name.
 - **Last name** Enter the user's last name.
 - **Contact phone number** Enter the user's contact phone number.

- **Member of organizations** Displays the organization the user belongs to. This value is assigned automatically when a new user is created.
 - **Contact for organizations** Click **Choose**, and from the dialog that appears, select the organizations for which this user can be the contact person, and then click **APPLY**.
5. Click **Save** to create the user profile.

Creating a Manager Role

Actor: Portal Administrator

The portal administrator is responsible for creating manager roles.

To create a manager role, follow the steps described in the Adding a Member to the Organization section and in the **User type** field, choose **Manager**.

Viewing an Organization's Information

Procedure

1. Click the **Organizations** tab.
2. Select the organization whose information you want to view.

The organization detail page for the organization appears. The organization detail page shows the following features:

- **Applications** Lists the applications owned by the organization, and shows the plans and percentage of usage for the plan.
- **Alerts** The Alerts area of the screen displays alert messages, such as quota threshold alerts. Quota threshold alerts appear when usage for a particular plan exceeds the quota threshold limit specified for a subscription.

The following alert shows a sample quota threshold alert for a subscription:

Subscription Coke Coke-Deals-Economy(ID 252) has exceeded the quota threshold. The current usage is 15.0%

- **Subscriptions** Lists the active subscriptions for the organization, shows the subscription period for each subscription, and indicates the plans associated with the subscription and the percentage of usage for each plan.

- **Statistics** Click **Show Dashboard** to go to the analytics page for the organization. For information on using the Dashboard, see Using the Application Dashboard section.
 - **Members** Lists the members of the organization.
3. If you want to add a new member to the organization, click **New Member**.
For information on adding a member, see Adding a Member to the Organization section.

Managing Environments and Gateways

The portal administrator first creates one or more environments, and then associates them with gateways. The environments are then registered in the portal so that APIs and products can be provisioned in one or more environments.

Creating an Environment

Actor: Portal Administrator

Procedure

1. Log in to the API Manager Portal as portal administrator.
2. Choose the **Environments** tab and then click **Create New Environment**.
The Submit New Environment interface appears.
3. Enter the basic information to set up the new environment:
 - **Environment Name** Enter a short name for the environment. The name is displayed on the product page within the portal.
 - **Description** Enter a description for the environment.
 - **Type** Choose the environment type from the options in the drop-down list: Development, Production, Sandbox, Staging, or Testing. The type is for informational purposes only.
 - **Basepath** Enter a URL that represents the public endpoint for services running in the environment. Often this is an IP load balancer, For example, enter `http://localhost:8080/basepath`.
4. Specify whether the environment is managed by a Gateway:

- To retain the default setting (**Yes**), leave the Yes check box selected.

If the environment is managed by a Gateway, then the basic settings for API operations executed through the Gateway are configured on the API Exchange Gateway, using the Gateway Configuration interface.

- To specify that the environment is managed by the portal, select **No**.

Selecting **No** configures proxy pass-through configuration for the environment. With proxy pass-through, the basic settings for API operations in the environment are specified in the Developer Portal interface.

5. If you selected **No** to indicate that the environment is not managed by a Gateway, complete these steps:

Enter the following information:

Organization	The organization that will use the target operation.
User name	User name with BASIC authentication for HTTP authentication.
Password	Password with BASIC authentication for HTTP authentication.
timeout	Timeout (in milliseconds) to use when accessing the target operation.
Retry Count	The interval between the HTTP(s) connection retries. A value of 0 indicates no retry.
Retry Interval	The interval between HTTP(s) connection retries. A value of 0 indicates no retry.
Retry Timeout	The timeout value on each attempt of the HTTP connection. This value is specified in milliseconds. A value of 0 indicates no timeout.
Headers to Forward	This field allows users to copy header information from the northbound incoming

	<p>request and forward it to the southbound side.</p> <p>If the value of Headers To Forward is specified as (*), all the headers are copied.</p> <p>If the Headers To Forward contains "*,-SoapAction", any incoming SOAP Action header is removed from the incoming headers and the value set on the endpoint is ignored.</p>
Operation Features	<p>The list of keywords identifying the features required by the operation. For information on the supported features, see “Target Operation” in the <i>TIBCO API Exchange Gateway User’s Guide</i>.</p>

Specify whether the environment will use SSL.

- To enable SSL, leave the default setting (**Yes**) enabled.
- To disable SSL, choose **No**.

If you specify SSL, enter the following information:

- **Property File** Enter the directory path and filename for the SSL property file.
- **Anonymous SSL** To enable anonymous SSL, click **Yes**. To disable anonymous SSL, click **No**.

6. Click **Save** to save the environment.

An environment page for the new environment appears. This page lists the settings that you have configured for the environment.

If you specified that the environment is not managed by a Gateway, then on this page you can click **Add Gateway** to add a gateway to the environment or click **Configure** to specify additional environment configuration settings.

For information on adding a gateway to the environment, see Adding a Gateway to an Environment section.

For information on specifying additional environment configuration settings, see Managing Environment Configurations section.

Adding a Gateway to an Environment

Actor: Portal Administrator

After creating an environment, the portal administrator can add one or more gateways to the environment.

Procedure

1. Log in to the API Manager Portal as portal administrator.
2. Choose the **Environments** tab and click on an environment name.
3. Click **Add Gateway** under Gateways.
The Create New Gateway interface appears.
4. Enter the information to identify the gateway:
 - **Gateway name** Enter a name for the gateway.
 - **Description** Enter a description for the gateway.
 - **Environment** Displays the name of the environment that the gateway is being added to.
 - **Management URL** Enter the URL to connect to the TIBCO API Exchange Gateway server. If the Management URL is to be accessed using Secure Sockets Layer (SSL), select the **SSL** check box.
To add additional URLs, click the Add URL button to display additional fields for adding URLs and enter the URL information for the URLs.
5. Click **Save** to add the gateway to the environment.

Managing Environment Configurations

After an environment has been created, you can view detailed information about the environment and specify additional configuration settings for the environment.



Note

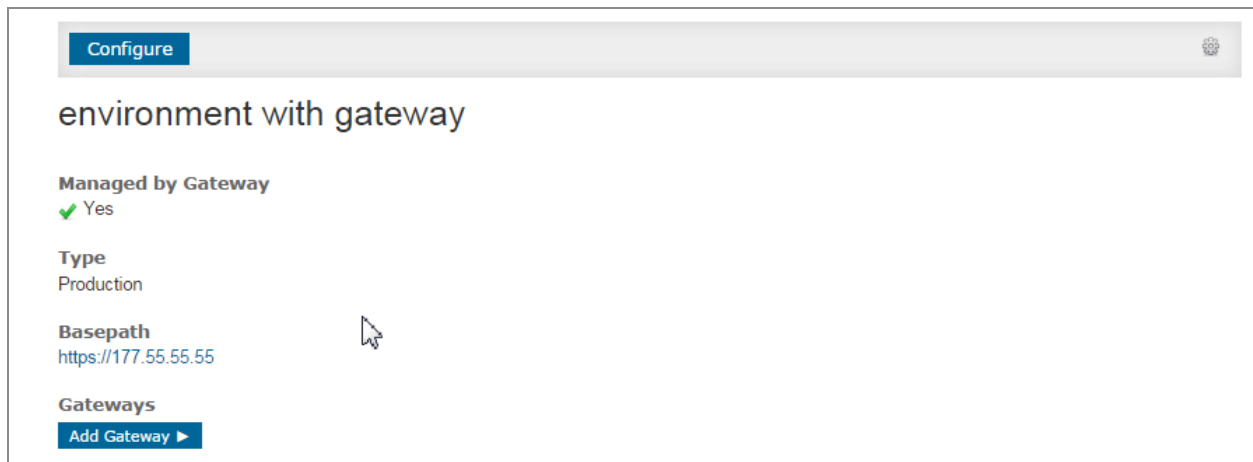
To access the master configuration from the portal, ensure that the portal-engine is started after the Global Configuration setting **Enable Master Configuration** is set to **on**. This property is set in the `asg_portal.properties` file.

Procedure

1. Log in to the API Manager Portal as portal administrator.

2. Choose the **Environments** tab and click on an environment name.

A summary page showing the environment configuration appears:



The summary page shows the environment's description, type, and base path. If the environment is configured to be managed by a gateway, the summary page shows the associated gateways.

3. To view information about a gateway, click on a gateway name.
4. To add additional gateways, click **Add Gateway**.
5. To configure the environment, click **Configure**.

The gateway configuration UI appears.

6. To update the master configuration, follow these steps:

If you need to update the gateway configuration for a particular project, click the name of a project.

The gateway configuration is maintained on the ASG gateway host. From the Developer Portal display, you can add a new project configuration, duplicate, rename, or validate the configuration, delete the configuration, or publish the configuration.

To view the projects for another environment, click **Advanced Settings**, and then select the environment and the cluster whose configuration is to be updated. The projects available in that cluster are displayed.

Click on a project to view the configuration. Update the configuration as required.

Click the save icon  to save the changes locally.

7. To publish the updates on the master configuration to the gateway instance configuration:

Hover over the project name to see the menu options.

Click the **Update Project Configuration** icon .

This updates the configurations for the registered gateway instances of the cluster.

Note For more detailed information on how master configurations are maintained, see the **i** “Portal Administration” section in the *TIBCO API Exchange Manager Administration* document. The master configuration is discussed in the “Master Configuration” section.

The APIs section of the page lists the APIs currently associated with the environment.

8. To view detailed information about an API, click an API name.
9. To view detailed information about a product, click a product name.

Managing Subscriptions

Portal administrators can create subscriptions for a selected product and plan. Also, when an application developer places a request for a plan, the portal administrator can create the subscription and make it available to its requesters.

Subscriptions also allows you to manage the access to APIs through API Exchange Gateway. However, managing the access to APIs in the portal often resulted in restricting APIs to users with an account, provided a limited beta program, and restricted use to partner specific APIs. In release 2.2.0, you can use **Access Levels and Categories to manage the access to APIs in the portal. For more details, see "Managing Access Levels and Categories in the Portal."**

Viewing Subscription Requests

Actor: Portal Administrator

You can view, accept or reject subscription requests using the **Requests** tab in the Developer Portal.

Procedure

1. Click the **Subscriptions** tab and from the pull-down menu, choose **Requests**.

The Manage Requests page appears, as shown in the following figure.

Manage requests				
Search Organization...				All ▾
Subscribing organization	Request ID	Requested	Updated	Status
John Doe rbiell@tibco.com	▶ 3	30 Oct 2014	30 Oct 2014	● Approved
	▶ 2	30 Oct 2014	30 Oct 2014	● Approved
John Smith rbiell888@gmail.com	▶ 4	31 Oct 2014	31 Oct 2014	● Pending
	▶ 1	30 Oct 2014	31 Oct 2014	● Rejected

The Manage Requests page shows the current subscription requests. The stoplight indicator next to each subscription indicates the status of the subscription request. The subscription request status can be one of the following statuses:

- **Pending** The subscription request has been submitted by a user, and is pending approval.
- **Approved** The subscription has been approved.
- **Rejected** The subscription request was rejected.
- **Cancelled** The subscription was approved but has been cancelled by an application developer.

2. To display details about a subscription request, click the subscription status for the request in the Status column.

The Request ID, subscription type (for example, Custom), and details about the subscription appear (the configured number of calls per day and number of calls per second).

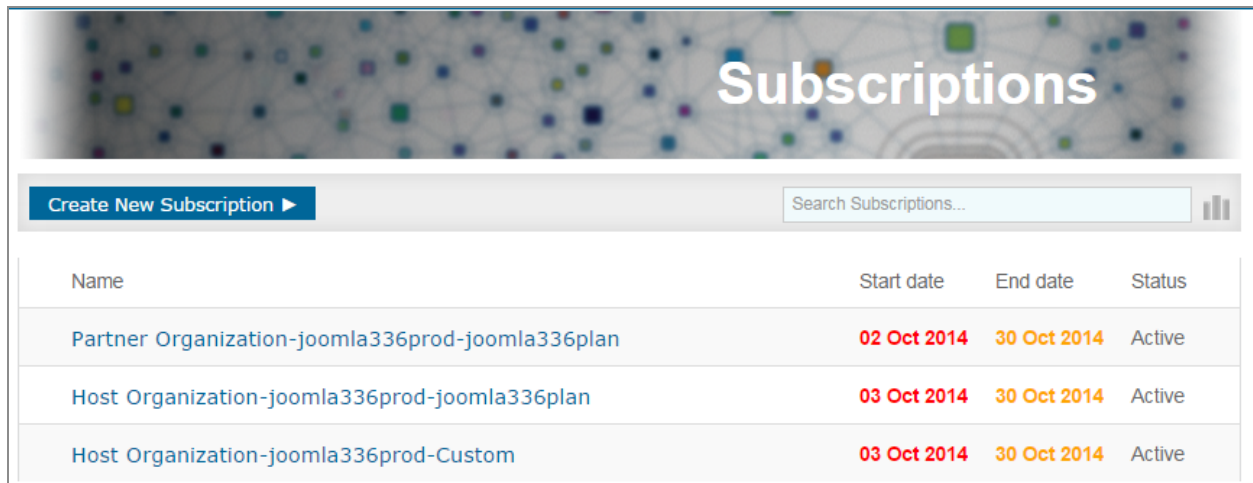
Viewing Subscriptions

Actor: Portal Administrator

Procedure

1. Log in to the API Manager Portal as portal administrator.
2. Click the **Subscriptions** tab.

The Subscriptions page appears, as shown in the following figure:

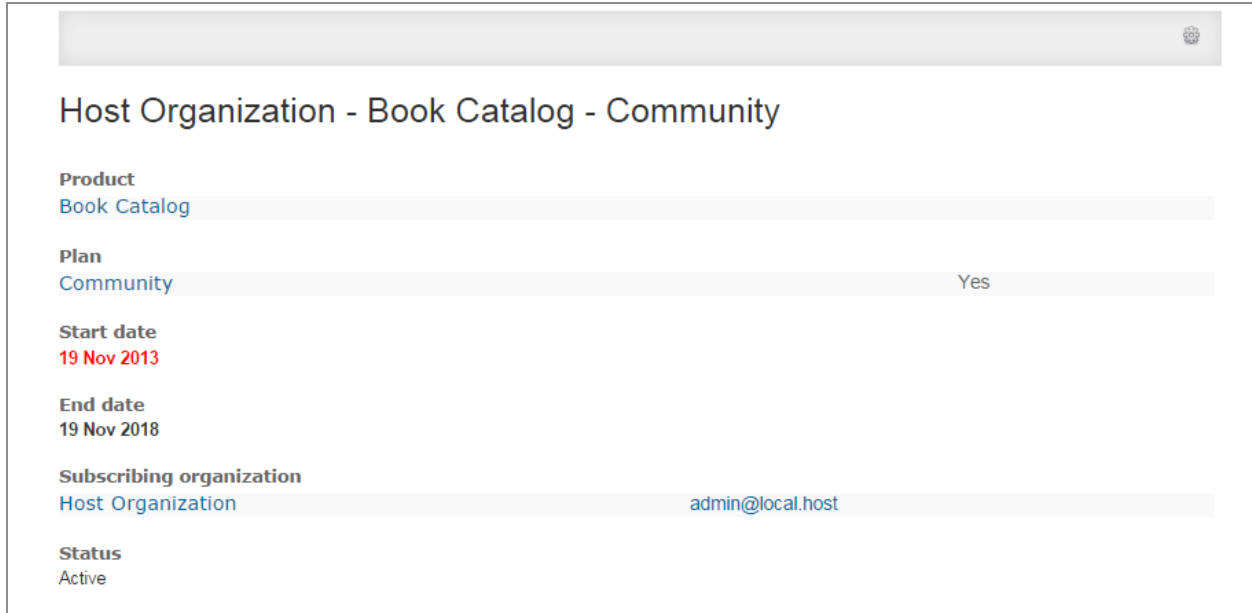


Name	Start date	End date	Status
Partner Organization-joomla336prod-joomla336plan	02 Oct 2014	30 Oct 2014	Active
Host Organization-joomla336prod-joomla336plan	03 Oct 2014	30 Oct 2014	Active
Host Organization-joomla336prod-Custom	03 Oct 2014	30 Oct 2014	Active

The **Subscriptions** tab shows all subscriptions in the system database, and includes the following information:

- The name of the subscribing organization
 - The name of the product subscribed to
 - The name of the plan subscribed to
 - The start and end date for the subscription
3. To view details about a subscription, click on the subscription name.

The system displays details about the subscription, as shown the following figure:



Host Organization - Book Catalog - Community

Product
Book Catalog

Plan
Community Yes


Start date
19 Nov 2013

End date
19 Nov 2018

Subscribing organization
Host Organization admin@local.host

Status
Active

You can review the details of the subscription, or edit it if needed.

4. To edit the subscription, click the tools icon  and select **Edit**.
5. The Edit Subscription page appears. For information on the fields for setting up a subscription, see Creating a Subscription section.
 - To activate a subscription, click **Active**.
 - To inactivate a subscription, click **Inactive**.
6. Click **Save**.

Creating a Subscription

Actor: Portal Administrator

Procedure

1. Log in to the API Manager Portal as portal administrator.
2. Click the **Subscriptions** tab and then click **Create New Subscription**.
The Create new Subscription interface for the selected product and plan appears.
3. Specify the following information:
 - **Description** Enter a description for the subscription.

- **Contact** Contact person for the subscription. This value is automatically assigned to the contact for the organization.
 - **Product** Displays the product selected.
 - **Plan** Displays the plan selected.
 - **Start date** Specify the start date for the subscription. By default, the start date is set to today's date.
 - **End date** Specify the end date for the subscription. By default, the end date is set to today's date.
 - **Subscribing organization** Click **Choose**, and from the Attach Existing dialog, choose the organizations that subscription is applicable to, and then click **Apply**.
 - **Status** Set the status of the subscription to active or inactive.
4. Click **Save**.

The subscription is created with a name in the following format:

<organization_name>-<product_name>-<plan_name>

Approving Subscription Requests

When an application developer submits a request, an email containing the details of the request is sent to the portal administrator.

Plan with Auto-Provisioning

The subscription for a plan with auto-provisioning is created automatically when an application developer places a request.

Plan without Auto-Provisioning

To create a subscription for a requested plan, follow these steps:

Procedure

1. Click on the URL provided in the email containing the details of the request.
2. Log in to the API Manager Portal as portal administrator, if needed. The Create New Subscription interface appears and contains the values for the requested plan.
3. Update the **Start Date** and **End Date** for the subscription, and the **Status** of the subscription.
4. Click **Save** to create the subscription.

Custom Plan

A custom plan does not exist in the system when it is requested. The portal administrator needs to create a plan and then add a subscription for the requestor. For details, see the [Creating a Product Plan](#) section and [Creating a Subscription](#) section.

Managing Access Levels and Categories in the Portal

You can access levels control which users can view objects including **Menus and Product Categories**.

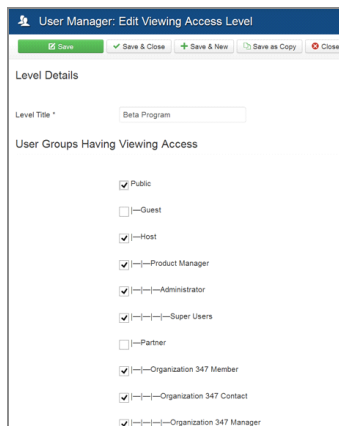
In order to access level controls through Menus and Product Categories, complete the following steps:

Procedure

1. Assign Users to Groups by clicking **Menu Users > Groups**.
2. Assign Groups to Access Levels by clicking **Menu Users > Access Levels**.

Each organization has three groups which consists of:

- Organization <ID> Member
- Organization <ID> Contact
- Organization <ID> Manager

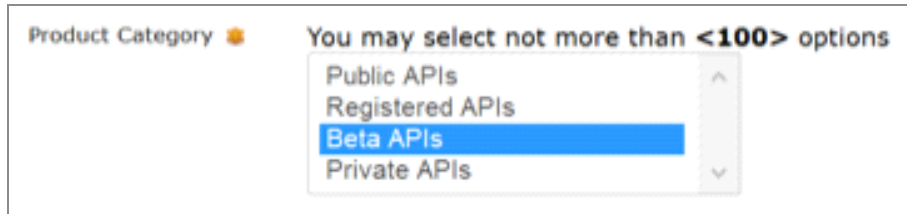


Each organization also has three Access Levels, which are as follows:

- Organization <ID> Member
- Organization <ID> Contact
- Organization <ID> Manager

To ensure you are managing access levels and categories successfully, ensure that the host has access as well.

Product visibility is controlled by Product Categories. Different users are able to access different view of this.



Managing Scopes

Actor: Portal Administrator

Scopes are used to restrict access to applications. The portal administrator creates a scope, which can then be used by application developers.

i The **Scopes** tab appears only if OAuth authorization is enabled. For information on **Note** enabling OAuth authorization, see Enabling OAuth and Scopes Configuration section.

Creating a Scope

Procedure

1. Log into the Developer Portal as portal administrator.
2. Click the **Scopes** tab and then click **Create New Scope**.
The Create New Scope interface appears.
3. Specify the following information:
 - **Scope name** Name of the scope.
 - **Description** Description of the scope.
4. Click **Save & Close** to create the scope.

Managing APIs

The portal administrator creates and publishes APIs and operations, which are then associated with products. These products are used for the application developers to create applications.

Creating an API

Actor: Portal

Procedure

1. Log in to the API Manager Portal as a portal administrator.
2. Select the **APIs** tab and click **Create New API**.
The Create New API page appears.
3. Enter the information to define the API:
 - **API name** Enter a name for the API.
 - **Description** Enter a description for the API.
 - **API Type** Choose the API type from the options in the drop-down list: **REST** and **SOAP**. The default API type is **REST**.
4. Specify whether to create a proxy for the API:
 - To create a proxy for the API, click **Yes** in the Create Proxy for API selection.
In order to create a proxy, when you choose an environment for the API to run in, you must choose an environment that has been with the Managed by Gateway setting set to No.
 - To accept the default (do not create a proxy), click **No**.
5. Upload the API spec and documentation for the API:



Note

Specification artifacts must be available for upload.

Upload REST API Spec If the API is a REST API, to add a REST API specification, click **Add files**, and then browse for and select the Swagger specification files to be added. Ensure that the file format is JSON. Once the files are selected, click **Start upload** to upload the selected files.

Upload WSDL API Spec If the API is a SOAP API, to add WSDL API specification, click **Add files**, and then browse for and select the WSDL specification files to be added. Once the files are selected, click **Start upload** to upload the selected files.

REST resource path Enter the REST resource path for the REST API. This field is applicable to REST APIs and can be left empty for APIs of type SOAP.



Note

The REST API resource paths specified must be unique for a product. Specifying duplicate resource paths might result in the swagger specifications being displayed incorrectly in the API explorer.

Environment Click **Choose** and select an environment in which the APIs are provisioned and are usable.

If you chose Yes for the Create Proxy for API setting, choose an environment that has the Managed by Gateway setting set to **No**.

Target Environment This selection appears only if you choose **Yes** for the Create Proxy for API setting. If you chose **Yes** for the Create Proxy for API setting, then click **Choose** and then select an environment in which the APIs are provisioned and are usable. This is an environment that is not managed by a gateway.

If you chose **Yes** for the Create Proxy for API setting, choose a target environment that has the Managed by Gateway setting set to **No**.

6. Enter information for the API documentation:

- **Attached Documentation Files** Click **Add files** to add one or more documentation files for the API and then click **Start upload** to upload the selected files.
- **Inline documentation** Enter inline documentation text as required.

7. Click **Save**.

An API detail page for the new API appears. This page shows the API specification, Description, API type, and resource path for the API.

8. Specify the following information.

- **Contact** Contact for the API. Click **Create New** to create a new contact or click **Choose** and choose the contact for the API.
- **Owner organization** Name of the organization that owns the API. The value is assigned automatically.
- **Contained in products** Click **Choose**, and then from the list of products, choose the products that will use the API.

- **Operations** Operations can be added to the API after the API is created. Depending on the type of the API, the portal administrator might need to add operations to the newly created API:

For REST APIs, the operations are picked up from the specification and automatically added to the API. However, the operations are not picked up from the specification for SOAP APIs. The portal administrator must manually add operations to the SOAP APIs after creating them.

See Adding an Operation section for details.

Adding an Operation

Actor: Portal Administrator

You can add an operation manually; however, an operation added manually cannot be deleted by Archiving the API. The operation must be deleted manually.

Procedure

1. Log in to the API Manager Portal as a portal administrator.
2. Select the **APIs** tab and then select an existing API. The API details page appears.
3. Under the "Operations" section, click **Add Operation**.
The Create New Operation interface appears.
4. Enter the information to identify the operation:
 - **Operation name** Enter a name for the operation.
 - **Description** Enter description for the operation.
 - **URI path** Enter the REST operation's path or the endpoint URI for the WSDL.
 - **REST method** Select a method for the REST operation from the drop-down: DELETE, GET, POST, or PUT.
 - **SOAP Action** If the API is a SOAP API, enter the SOAP action for the SOAP operation.
5. Click **Save** to add the operation to the API.

Managing Portal REST API

To use the REST API functionality, complete the following steps:

Procedure

1. In the API Exchange Joomla Adapter folder, open the RestAPI folder.
2. Select the `com_API` and `plg_restapi`.zip files from the RestAPI folder and install them by using Joomla Extension Manager. Install the `com_api`.zip file first.
3. Use the Joomla back end to manage APIX web services and toggle it to be enabled in the status column.
4. In the **Global Configuration** tab, ensure that **Use Rewrite URLs** is selected.
5. Edit the base code in the `.htaccess` file to enable restapi, which is included in the installation of the Joomla adapter. You have to configure restapi to your setup.



Note

- Ensure that the base path is the same with the one where API Exchange is hosted.
- Ensure that the rewrite rule urls are changed.
- Ensure that your Virtual Host is set to **ALL** with whatever stack you use, such as LAMP, WAMP, and XAMP.

To see the swagger implementation of the Rest APIs, you must change the path for two files in the Joomla installation:

Procedure

1. Navigate to `apidocs` and open `index.html`, where a bracket called `joomlahostname` for the `url` variable is located. Fill out the `url` variable with your domain name in this bracket.
2. In the **apidocs > V.1 > apixrestapiswagger** folder, change the host name to your `joomlahostname` without any `http://`.

Managing Products and Associated Plans

After the APIs are created, the portal administrator can create products and associate APIs with the products. The portal administrator can then add new plans to the products.

Creating a Product

Actor: Portal Administrator, Product Manager

Procedure

1. Log in to the Developer Portal as a Portal Administrator.
2. Click the **Products** tab and click **Create New Product**.
The Create New Product interface appears.
3. Enter information to identify the product:
 - **Name of the Product** Enter a name for the product.
 - **Description** Enter a description for the product.
 - **Product Category** Select a product category from the drop-down list.
See Adding a Product Category section for instructions on adding a new category from the Joomla! Administrator back-end.
 - **Upload product thumbnail** Upload an image to display the product thumbnail.
4. To associate the product with APIs, click **Choose** and from the list of APIs that appears, select one or more APIs for your product. Then click **Apply**.
5. Enter information for the product documentation:
 - **Inline documentation** Enter the inline documentation text for the product, if any.
 - **Attached Documentation Files** Click **Add files** to add one or more documentation files for the product and then click **Start upload** to upload the selected files.
 - **Product-specific terms & conditions** Enter the text for product-specific terms and conditions, if any.
6. Click **Save** to create the product.

Creating a Product Plan

Actor: Portal Administrator

Procedure

1. Log in to the API Manager Portal as a partner administrator.
2. Click the **Products** tab and select an existing product from the list of products. The product details page appears.
3. Click the **Plans** tab and then click **Add Plan**.

The Create New Plan interface appears.

4. Specify the following information to set up the plan:

- **Plan name** Enter a name for the plan.
- **Level** Specifies the ordering of the plan in the list of product plans, where the plans are placed in the increasing order of the level. Choose a level from the drop-down menu: custom, Level 1, Level 2, Level 3, Level 4, and Level 5.



After they have been created, custom plans are not displayed on the UI. However, the custom plans can be selected when creating a subscription.

- **Subscriptions** After you create the plan, you can add a subscription to it.
- **Price or keyword** Enter a price or a keyword to be highlighted for the plan.
- **Contact** Contact for the plan.
- **Product** Displays the product name for which the plan is to be created.
- **Auto subscribed** Select **Yes** to create a plan that can be auto-provisioned.
- **Plan details** Enter the details of the plan.
- **Rate Limit** Specifies the number of requests to the API allowed per second.
- **Quota Limit** Specifies the number of requests to the API allowed per day for products using the plan.
- **Concurrent Limit** Controls how many concurrent users, or users at the same time, the plan allows for access to its APIs. An optional field that does not have a default value. You have to set a number in the **Concurrent Limit** field in the **Plan Details Page** for this feature to become active. By default, it is not set. The maximum length of the number is 10.
- **Description** Enter a description for the plan.

5. If the system administrator has configured a routing key that should be applied to the plan, enter it as the plan type in the **Plan Type** field.

The value specified for the Plan Type is written to the Facade Access configuration file on the API Exchange Gateway and can be used to identify a routing key that routes requests from APIs that belong to the application to target operations that facilitate specific processing. For example, based on the routing key enabled using the Plan Type, customers can route requests to different URL destinations that enable specific processing desired for the Plan Type.

6. Click **Save** to save the plan and add it to the selected product.

The newly created plan appears on the product page for the product.

After creating a product and adding a plan, you must associate an environment with the product. See Associating a Base path with a Product section for details.

Associating a Base path with a Product


Procedure

1. Log in to the API Manager Portal as a portal administrator.
2. Click the **Products** tab and select an existing product from the list of products. The product details page appears.
3. Under the section **Base paths**, click **Choose**. The Attach Existing dialog appears.
The pull-down menu for base paths presents a list of base paths. These correspond to base paths created when a environments are created; for example “Production Environment.” The basepath value indicates the URL for a base path. Often this is an IP load balancer.
4. Select the base path (environment) and click **APPLY**. The base path field on the product details page displays the selected environment and base path URL.

Adding a Product Category

Actor: Portal Administrators:

Procedure

1. Log in to the Joomla! Administrator back-end as portal administrator.
2. Navigate to **Components > Cobalt 8 > Sections**.
3. For the **Products** section, click on  and then select **Manage Categories**. The Product Categories page appears.



Note

If needed, you can edit or delete existing product categories from this page.

4. Click **New** to open the form for a new category.
5. Enter the information to define the category.

6. Save the information to create the new category.

Administering Developer Forums

Users can use the comment on and discuss products and applications by using the Portal Administration interface, through the Developer Forums that you set up.

You can set up discussion forums, control what types of users can post and view comments, edit comments, and delete comments if needed.

Configuring the Developer Portal for Developer Forum Comments

Procedure

1. Log into the Joomla administration interface.
2. From the Dashboard page, choose **Components > Cobalt 8 > Records**.
The Records page appears.
3. At the left of the page, click **Types**.
4. Click **Product**.
5. Click **Comments Parameters**.

The Comments page appears, as shown in the following figure:

Define Comments Provider

[Learn how to add your own comment adapter](#)

Comments provider: Cobalt - Built-In Comments ▼

General Parameters

Captcha for public users	No Yes
Require admin approval	No Yes
Show Be first to post message	No Yes

Comments Rules

Who can post comments	Registered ▼
Who can set comments access	Host Administrator ▼
Who can view comments	Public ▼
Who can moderate comments	Host Administrator ▼
Language mode	Comments submitted on any ▼
Require admin approval	No Yes
Article author can moderate	No Yes
Article author can disable	No Yes
Comment author can edit	No Yes
Comment author can delete	No Yes

- Set the parameters as shown in the figure. This specifies that comments can be made by registered users, controlled by the host administrator, viewed by all public users, and be moderated by the host administrator.
- Scroll down to the next section of parameters, shown in the following figure:

Private Comments

Who can post private comments	Registered ▼
Who can view private comments	Host Administrator ▼
Article author can view private comments	<input type="button" value="No"/> <input checked="" type="button" value="Yes"/>

Rating

Who can rate comments	Registered ▼
Who can view rating	Public ▼
Auto unpublish	100

Attachments

Who can attach	Default View Level (Public) ▼
Overwrite if exists	<input type="button" value="No"/> <input checked="" type="button" value="Yes"/>
Show downloads num	<input type="button" value="No"/> <input checked="" type="button" value="Yes"/>
Show size	<input type="button" value="No"/> <input checked="" type="button" value="Yes"/>
Allowed formats	pdf, zip, doc, jpg, jpeg, png, gz, tar, .
File max size (Byte)	2097152
Maximum files to attach	3

8. Set the parameters as shown in the figure.

9. Click **Save**.

Comments are now enabled for products administered in the Developer Portal.

10. To verify the comments are enabled, follow these steps:

Log into the Developer Portal as an application developer or as a product manager.

Go to the **Products** tab and verify that the Comments window is active.

Enter a comment and verify that it is saved.

Log in as another user and enter a response to the initial comment.

Verify that the response is saved.

Editing Comments

The back-end Portal Administrator can edit or delete comments. In addition, the administrator can unpublish a comment. Unpublishing a comment removes it from the Comments displayed in the Developer Portal, but it does not delete it permanently; at a later time the administrator can republish it.

Procedure

1. Log into the Joomla administration interface.

2. Choose **Components > Cobalt 8**.

3. On the Records page, click **Comments**.

The Comments page appears. The Comments page displays the existing Comments records.

4. To edit a comment, select the comment in the list of records and then edit it.

5. Click **Save and Close** to save the comment.

The comment is now changed and Developer Portal users see the new version of the comment when they log in.

6. To delete a comment, select the check box next to the comment and then click **Delete**.

7. To unpublish a comment, select the check box next to the comment and then click **Unpublish**.

The comment is no longer visible to Developer Portal users.

8. To publish a comment that has been unpublished, select the check box next to the comment and then click **Publish**.

The comment is now visible in the Comments area for the products.

Using the Application Dashboard

With the application dashboard on the Developer Portal, you can view the following features:

- Quota usage for the applications defined for the installation
- Quota threshold alerts
- Information on subscribed products
- Statistics by application or by product
- Contact information for members of organizations that own applications

Procedure

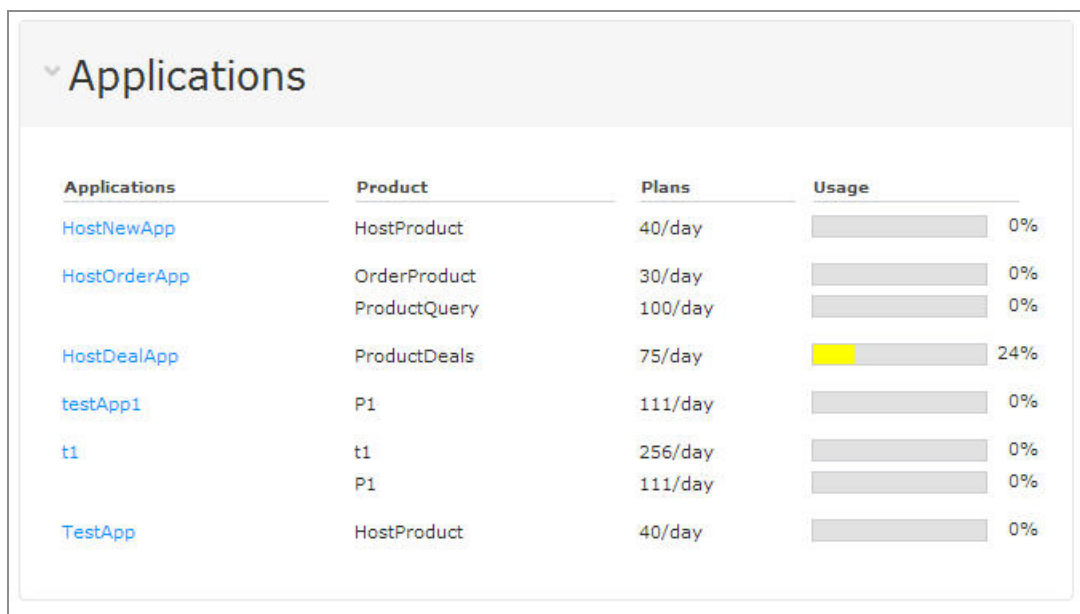
1. Click the **Dashboard** tab.

The Application Dashboard appears.

You can toggle display of the dashboard sections by clicking on the section title. For example, to toggle display of application quota usage on or off, click **Applications**.

2. To re-sync the portal, click **Re-Sync**.
3. To view application quota usage, click **Applications** (if application quota usage is not already active).

A list of applications with quota usage information appears, as shown in the following figure.



The screenshot shows the 'Applications' section of the dashboard. It contains a table with four columns: Applications, Product, Plans, and Usage. The 'Usage' column includes a bar graph and a percentage value. The bar for 'HostDealApp' is highlighted in yellow, indicating it is over its configured threshold.

Applications	Product	Plans	Usage
HostNewApp	HostProduct	40/day	<div></div> 0%
HostOrderApp	OrderProduct	30/day	<div></div> 0%
	ProductQuery	100/day	<div></div> 0%
HostDealApp	ProductDeals	75/day	<div></div> 24%
testApp1	P1	111/day	<div></div> 0%
t1	t1	256/day	<div></div> 0%
	P1	111/day	<div></div> 0%
TestApp	HostProduct	40/day	<div></div> 0%

- The bar graph for usage indicates the percent utilization of the usage quota. If the usage is over its configured threshold, the bar changes color.

The Alerts area displays any alerts that are active.

4. To view Subscriptions information, click **Subscriptions** (if Subscriptions information is not shown already).

A list of the active subscriptions appears. Next to each subscription the threshold quota usage for the subscription is indicated as a percentage and in a bar graph.

To add a new subscription, click **New Subscription**. For information on adding a new subscription, see Managing Subscriptions section.

5. To view statistics, click **Statistics** (if the statistics display is not already active).
6. To view information about members, click **Members** (if the members display is not already active).
7. To add a new member, click **Add Member**.

For information on adding a member, see Adding a Member to the Organization section.

Viewing the API Analytics Dashboard

Actors: Portal Administrator, Manager, Application Developer:



Note

Ensure that the components required to display the analytics dashboard are configured correctly. Refer to the *TIBCO API Exchange Manager Administration* guide for detailed instructions.

Procedure

1. Log in to the Developer Portal.
2. Choose the **Organizations** tab and click on the name of organization for which you want to view the analytical data.

The organization details page for the organization appears.

3. Click Statistics, in the details area.
4. Click **Show Dashboard** to open the Analytics dashboard.

Depending on the role, the user is presented one or two views. The portal administrator is presented with the host view and partner views for all the partners.

The pages in both host and partner views can be customized using TIBCO Spotfire.

Contacting Support

To contact customer support for the Developer Portal, click the **Support** tab, type a query, and then click **Send Your Query**.

TIBCO Documentation and Support Services

For information about this product, you can read the documentation, contact TIBCO Support, and join 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 [TIBCO Product Documentation](#) website is updated frequently and is more current than any other documentation included with the product.

Product-Specific Documentation

Documentation for Adapter Code for TIBCO® API Exchange and Joomla! is available on the [Adapter Code for TIBCO® API Exchange and Joomla! Product Documentation](#) page.

To directly access documentation for this product, double-click the following file:

`TIBCO_HOME/release_notes/TIB_api-exchange-joomla-adapter_2.3.4_docinfo.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 in the TIBCO Documentation site:

- Adapter Code for TIBCO® API Exchange and Joomla! Installation
- Adapter Code for TIBCO® API Exchange and Joomla! Administration Guide
- Adapter Code for TIBCO® API Exchange and Joomla! User's Guide
- Adapter Code for TIBCO® API Exchange and Joomla! Release Notes

How to Contact TIBCO Support

You can contact TIBCO Support in the following ways:

- For an overview of TIBCO Support, visit <http://www.tibco.com/services/support>.
- For accessing the Support Knowledge Base and getting personalized content about products you are interested in, visit the TIBCO Support portal at <https://support.tibco.com>.

- For creating a Support case, you must have a valid maintenance or support contract with TIBCO. You also need a user name and password to log in to <https://support.tibco.com>. If you do not have a user name, you can request one by clicking Register on the website.

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>.

Legal and Third-Party Notices

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

TIBCO, the TIBCO logo, the TIBCO O logo are either registered trademarks or trademarks of TIBCO Software Inc. in the United States and/or other countries.

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

This document includes fonts that are licensed under the SIL Open Font License, Version 1.1, which is available at: <https://scripts.sil.org/OFL>

Copyright (c) Paul D. Hunt, with Reserved Font Name Source Sans Pro and Source Code Pro.

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.

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

Copyright © 2016-2021. TIBCO Software Inc. All Rights Reserved.