

IBM Cúram Social Program Management
Version 7.0.0

*Cúram Portlet Deployment Guide For
WebSphere Portal Server*



Note

Before using this information and the product it supports, read the information in “Notices” on page 19

Edition

This edition applies to IBM Cúram Social Program Management v7.0.0 and to all subsequent releases unless otherwise indicated in new editions.

Licensed Materials - Property of IBM.

© **Copyright IBM Corporation 2012, 2016.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

© Cúram Software Limited. 2011. All rights reserved.

Contents

Figures	v
--------------------------	----------

Tables	vii
-------------------------	------------

Deploying Portlets on IBM WebSphere

Portal Server	1
--------------------------------	----------

Introduction	1
Introduction	1
Prerequisites	1
Audience	1
Chapters in this Guide	1
Cúram Portlet Overview	2
Cúram Portlets	2
Access Control of Cúram Portlets	2
Current limitations of Cúram Portlets	2
Building the Portlet WAR File	2
Configuring Cúram Portlets	2
Configuring Cúram Portlets	3
Configuring the base URL in Cúram Portlets	3
Configuring the display characteristics of each Cúram Portlet	4
Building WAR file	4
Deploying Cúram Portlets	4
Configuring Cúram Portlet content	4
Setting up Users and Groups For Portal Resources	5
Deploying Portlets on Portal Pages	6
Single Sign On Curam Portlet Configuration.	6
Introduction	6
Manual WebSphere Portal Server Configuration	6
Starting the Portal Server	6

The Administrative Console	6
Creating the Data Source Login Alias	7
Configure DB2 Data Sources	7
Save the Master Configuration	8
Configure Administration Security	8
Configure Users	9
Disable Cross Cluster Authentication	10
Save the Changes	10
Specific Server Configuration	10
Configure your JNDI lookup port	10
Configure your ORB Pass By Reference	10
Configure your Java Virtual Machine	10
Configure your Timer Service	11
Set up the Port Access	11
Configure Session Security Integration	12
Bus Configuration	13
Setup the Service Integration Bus	13
JMS Configuration	14
Setup the JMS Connection Factories	14
Setup the Application Queues	14
Setup the Application Topics	15
Configure Historical Log Files	15
Completion	16
Configuring Portal Server to reuse JSESSIONID	16
Manual Application Deployment	16

Notices	19
--------------------------	-----------

Privacy Policy considerations	20
Trademarks	21

Figures

Tables

1. Selecting Cúram Pod.	5	2. Exception Destination Settings	15
---------------------------------	---	---	----

Deploying Portlets on IBM WebSphere Portal Server

Cúram portlets show information about a Cúram application. There is a 1:1 mapping between the content of certain Cúram pods and Cúram portlets. A number of steps are required to deploy Cúram Portlets. A portlet WAR file is required. The content of the Cúram portlets must be configured before deployment.

Introduction

Introduction

This guide describes the process of configuring Cúram portlets, and deploying them to a portal page on a Portal Server.

Prerequisites

To successfully deploy and administer Cúram portlets, the reader will need the following:

- Be familiar with configuring IBM® WebSphere® Application Server and/or IBM WebSphere Portal Server;
- Must have read the *Cúram Third-Party Tools Installation Guide for Windows* document to know what software is needed to configure Cúram portlets;
- A basic understanding of the Cúram application, and Cúram application development.

Audience

This document is a technical guide for individuals who are responsible for administering resources on a Application Server and/or a Portal Servers.

Chapters in this Guide

The following list describes the chapters within this guide:

Cúram Portlet Overview

This chapter gives an overview of what constitutes a Cúram portlet.

Building the Portlet WAR File

This chapter describes how to configure the Cúram portlets and build the `CuramPortlets.war` file before the Cúram portlets can be deployed.

Deploying Cúram Portlets

This chapter describes how to configure the content of Cúram portlets and also how to deploy Cúram portlets.

Single Sign On Cúram Portlet Configuration

This appendix describes how the manually configure the Portal Server and manually deploy the Cúram application so that a user can enable Single Sign On (SSO) portlets.

Cúram Portlet Overview

Cúram Portlets

Cúram portlets are portlets that display information pertaining to a Cúram application. There is a 1:1 mapping between the content of certain Cúram pods and Cúram portlets - with some slight differences - therefore there is a strong relationship between the content displayed in Cúram portlets and Cúram pods, see the *Cúram Pod Developers Guide* for more details on pods. Cúram portlets have been developed in accordance with the JSR 286 specification. However, it is important to note that this does not mean that Cúram portlets currently exhibit all the JSR 286 features, such as inter-portlet communication.

It is important to realize that Cúram portlets are not delivered out-of-the-box as ready to deploy portlets. There are some important steps that must be undertaken before Cúram portlets can be deployed on a portal page, and which are described in the following chapters. Furthermore if it is requirement that Cúram portlets must be SSO (described in “Access Control of Cúram Portlets”) compliant, then the instructions specified in “Single Sign On Cúram Portlet Configuration” on page 6 must be undertaken.

Access Control of Cúram Portlets

There are currently two supported ways of controlling access to Cúram portlets:

- **Single Sign On Cúram Portlets**

Refer to Single Sign On in order to see more details about the SSO Specification. This means that once a user starts a new portal session (by logging in), they will *not* be required to login into each Cúram portlet on a portal page, after a portal page containing Cúram portlet is initially loaded.

- **Non SSO Cúram Portlets**

This means that once a user starts a new portal session (by logging in), they *must* then log into each Cúram portlet on a portal page after the page is initially loaded in order to be able to use the portlets. This is assuming that a user has not already logged in a the Cúram application within the same browser session. Refer to the Chapter on Session Management in the *Cúram Web Client Reference Manual* in order to find out more information on browsers sessions and session management of the Cúram application.

Current limitations of Cúram Portlets

These are the current limitations of Cúram portlets:

- **Localization**

Cúram portlets are currently only supported in the English locale.

- **Web Browser Support**

Cúram portlets are currently supported by the web browsers which are supported by the Cúram application. Refer to the *Cúram v6 Supported Prerequisites* document to see supported version of these browsers.

Building the Portlet WAR File

Configuring Cúram Portlets

Configuring SSO Cúram Portlets: If SSO Cúram portlets are required, then the Cúram application (IBM Cúram Social Program Management must be manually

configured and deployed on the Portal Server. The instructions to do this are described in “Single Sign On Curam Portlet Configuration” on page 6. Otherwise a Cúram application that has been deployed on an Application Server will suffice - refer to the chapter on *Deployment* for in the *Cúram Deployment Guide for WebSphere Application Server* for more details on this.

The Cúram portlets must be configured before generating the CuramPortlets.war file. They can be configured by updating the relevant property files in the client core component.

Note: The current supported way to configure Cúram portlets is to update the property files within the webclient/components/core/PortletConfig directory. It should be noted that updating the property files in this way, conflict's with the policy of customizing files in the custom component and is a limitation that will be addressed in a future release.

Configuring Cúram Portlets

The value of the portlet.ids property key in the PortletConfig.properties file is used to configure what portlets get packaged in the CuramPortlets.war file. The value of this property must be formatted so that it meets the following criteria:

- **It must be a comma delimited string**

It must be a comma separated string, with each part of the string corresponding to the ID (identifier) of a Curam Pod.

- **It's comma delimited substrings must map to a properties file**

The value of each these comma delimited substrings maps to a properties file within the PortletConfig/resources directory.

If the value of the portlet.ids property does not conform to these criteria, then an error will occur when the generating the CuramPortlets.war file. By default the value of this property contains the full list of supported Cúram portlets. It is recommended that the default value of this property should not be updated. It is also recommended that the property files in the resources directory are left as they are in the installation even if the value of the portlet.ids property has been modified.

Configuring the base URL in Cúram Portlets

The base URL is part of the absolute (Uniform Resource Locator) URL used by each portlet to access pages in the Cúram application. The base URL is common to all Cúram portlets. Refer to the RFC 3986 if you wish to find out more information about URL specification. The value of the base.url property key in the PortletConfig.properties file is used to configure the base URL for Cúram portlets.

The default value for the base.url property key is **https://localhost:9044/Curam/**. The base URL of Cúram portlets can be configured in the following supported way:

- **Scheme/Protocol**

This is the first part of the property value and is used to configure the protocol that will be used to access pages in the application from a Cúram portlet. As can be seen in the default value of the property value it contains the value **https** which configures a portlet to access the Cúram application securely by using the Hypertext Transfer Protocol through a Secure Socket Layer (HTTPS). It is strongly recommended to leave this value as is.

- **Domain**

This must be used to configure the host name or ip address of the server on which the WebSphere system is running and where the Cúram application has been deployed. The default domain is "localhost" as can be seen above. The domain should be fully qualified if the default value is not being used - e.g., server1.xxx.com

- **Port Number**

The port number must be configured to the same port number that has been specified to host the Cúram application. If this part of the URL is omitted from the configured property value, then default port number 80 will be used.

- **Application Name**

This part of the base URL is the application as specified by the context root of the application when deploying the Cúram application on a host.

Configuring the display characteristics of each Cúram Portlet

Each of the property files within the PortletConfig/resources directory maps to each of the Cúram portlets that are packaged in the WAR file. So the properties within any of these property files can be used to configure the way in which a particular Cúram portlet will be displayed. The property keys that start with "javax" are used to configure title text and labels on the portlet and are specified in the portlet specification. Refer to JSR 286 for more information. The value of the portlet.height property key configures the height of a Cúram portlet. All of the properties within each of the property files within the PortletConfig/resources directory is mandatory.

Building WAR file

Build the CuramPortlets.war file by running **build portlet-war** from the installation_dir /webclient directory.

The CuramPortlets.war file is generated in the installation_dir /webclient/build/CuramPortlets directory.

Deploying Cúram Portlets

Configuring Cúram Portlet content

After the CuramPortlets.war file has been generated, the content of the Cúram portlets must be configured before they are ready to deploy.

The following steps describe how to configure the content of a Cúram portlet:

1. Log into the Admin application
2. **Navigate to Personalised Pod Pages**

Select the "Personalised Pod Pages" link from the "User Interface" Category from the Shortcut Panel.

3. **Configure a Personal page**

Select the "New Personalised Page.." page action control. This action will cause a modal dialog page to appear with a wizard progress bar.

On the wizard progress bar on the modal dialog page there are a number of steps which must be completed as follows:

- **Page ID**

On the first step of the wizard enter the same page ID that has been specified for the particular Cúram portlet that is being configured. For example, if the content of the QuickLinksPortlet portlet is being configured -

as specified in the value of the portlet.ids property key in the PortletConfig.properties file, then “QuickLinksPortlet” must be entered into the text input field provided. See ID of Cúram portlets listed in Table 1.

- **User Role**

On the second step of the wizard select the “SUPERROLE” option using the radio button.

- **Available Pods**

On the third step of the wizard, you need to select the appropriate pod from a list (by ticking the relevant checkbox), so that the correct pod content will be displayed within a particular Cúram portlet. The following table describes which pod name should be selected, based on the Cúram portlet (by ID) being configured:

Table 1. Selecting Cúram Pod

Cúram Portlet ID	Cúram Pod Name
MyTasksPortlet	My Tasks
QuickLinksPortlet	Quicks Links
MyAppointmentsPortlet	My Appointments
WorkQueuesPortlet	Work Queues
RecentNotiPortlet	Recent Notifications
OrgSummaryPortlet	Organization Summary
MyCurrentCasesPortlet	My Current Cases
MyTasksChartPortlet	My Task Charts
CaseloadSummaryPortlet	My Case Summary

- **Default Pods**

On the fourth step of the wizard select the option presented by ticking the checkbox.

- **Page Layout**

On the final step of the wizard enter 1 in the text input field and click on the “Save” button to complete the configuration for the portlet.

Layout issues: If text other than 1 is entered into the text input field provided, then layout issues will manifest themselves when the Cúram portlets are deployed.

Setting up Users and Groups For Portal Resources

The administrator of the Portal Server should create user groups and users so that they are granted access to Cúram specific portal resources (i.e portal pages hosting Cúram portlets). Furthermore there should be a direct mapping between the users of the portal resources and the users of the Cúram application (IBM Cúram Social Program Management) - i.e. admin and caseworker users. Refer to the **Administering > Users And Groups > Creating new users and groups** section of the WebSphere Portal Server documentation on details of how to create users and user groups. The users can be added to the All Authenticated Portal Users group or a new group that distinguishes that the group are users of Cúram portlets.

Note: The User ID and Password for these users, must match the User name and Password for users of the Cúram application.

Deploying Portlets on Portal Pages

There are basically two steps in deploying a Cúram portlet to a portal page, which are documented in the **Administering > Managing portlets and portlet applications > Installing a portlet** section of the WebSphere Portal Server documentation:

- Installing the CuramPortlets.war file containing the Cúram Portlets, into the Web Modules repository on the Portal Server
- Create an instance of a Cúram portlet on a portal page.

The appropriate user can open a portal page with Cúram portlets, by opening an instance of a web browser and pointing it at: `http://domain:WpsHostPort/WpsContextRoot/MyPortalPage"/>`.

For example if the default values for the portal server installation and default values of the Cúram portlet configuration are used (and assuming that there is a portal page created called MyPortalPage which has Cúram portlets), then the browser would be pointed at: `http://localhost:10039/wps/myportal/MyPortalPage"/>`

Single Sign On Curam Portlet Configuration

Introduction

The sections in this appendix describe the manual steps required to configure Cúram Single Sign On Portlets on a Portal Server. The Portal Server will first have to be manually configured, then the EAR files for the application will have to be manually deployed on the Server.

Manual WebSphere Portal Server Configuration

Starting the Portal Server

To start WebSphere_Portal, the startServer.bat, located in the wp_profile/bin directory of the WebSphere installation, should be used:

<WEBSHERE PORTAL INSTALL DIR>/wp_profile/bin/startServer WebSphere_Portal.
The default profile name during installation is "wp_profile", if you have customized the profile name then that must be used instead of "wp_profile" above.

Alternatively, the Administrative Console can be started from **Start > Programs > IBM WebSphere > Portal Server Version > Start the Server.**

The Administrative Console

To open the Administrative Console, a web browser should be pointed at:
`https://domain:10032/ibm/console"/>`

Alternatively, the Administrative Console can be started from **Start > Programs > IBM WebSphere > Application Server Network Deployment Version > Profiles > wp_profile > Administrative console.** The **Start the server** and **Stop the server** commands can also be used from this menu to start and stop the servers.

Each time the Administration Console is opened, a username and password will be requested for login. These credentials will be those that were used when installing the Portal Server. The Administration Console is divided into two sections. The left hand side contains a tree hierarchy for navigating the console and the right hand

side displays the information related to the current node selected in the tree. When instructed to **Navigate to**, the tree hierarchy should be traversed to the relevant node.

Creating the Data Source Login Alias

The Administrative Console can be used to configure a login alias for both the DB2 and data sources as follows:

1. Navigate to **Security > Global security**;
2. Expand the **Java Authentication and Authorization Service** option in the **Authentication** section and select the **J2C authentication data** option;
3. Click **New** to open the Configuration screen;
4. Set the following fields:
Alias = dbadmin
User ID = *<database username>*
Password = *<database password>*
Description = The database security alias
where *<database username>* and *<database password>* are set to the username and password used to login to the database;
5. Click **OK** to confirm the changes.

Configure DB2 Data Sources

Set up DB2 Environment Variable:

1. Navigate to **Environment > WebSphere variables**;
2. Select the **DB2UNIVERSAL_JDBC_DRIVER_PATH** link from the list of environment variables. This will open the configuration screen for this variable;
3. Set the **Value** field to point to the directory containing the Type 4/Type 2 drivers. This is normally the drivers directory under the SDEJ installation, e.g. **D:\Curam\CuramSDEJ\drivers**;
4. Click **OK** to confirm the changes.

Set up the Database Driver Provider:

1. Navigate to **Resources > JDBC > JDBC providers**;
2. *Note:* The appropriate scope where the data source is to be defined should be selected at this point.
3. Click **New** to add a new driver. This will open a configuration screen;
4. Select **DB2** from the list in the **database type** drop down supplied;
5. Select the **DB2 Universal JDBC Driver Provider** from the list in the **Provider type** drop down supplied;
6. Select the **XA data source** from the list in the **Implementation type** drop down supplied;
7. Click **Next** to continue;
8. Review the properties on the configuration screen that opens. There should be no need to change any of them unless you are planning to connect to a **zOS** database. If so, verify that **\${DB2UNIVERSAL_JDBC_DRIVER_PATH}** field is pointing at the correct directory for your system. For example, it should point at the directory containing the DB2 Connect license jar, **db2jcc_license_cisuz.jar** provided by IBM for **zOS** connectivity;
9. Click **Next** and then **Finish** to confirm the changes.

Set up the Database Driver DataSource: The following steps should be repeated for each of the application Data Sources, substituting `curamdb`, `curamsibdb` and `curamtimerdb` for `<DataSourceName>` (without the angle brackets):

1. Select the DB2 Universal JDBC Driver Provider (XA) now displayed on the list of **JDBC Providers**. This will open the configuration screen for the provider;
2. Select the **Data sources** link under **Additional Properties**;
3. Click **New** to add a new data source;
4. Set the fields as follows:
Data source name : `<DataSourceName>`
JNDI name : `jdbc/<DataSourceName>`
5. Click **Next** to continue;
6. Set the fields as follows:
Driver type : 2 or 4 as required;
Database name : The name of the DB2 database. (This will be equivalent to the `curam.db.name` property in the `Bootstrap.properties` file);
Server name : The name of the DB2 database server. (This will be equivalent to the `curam.db.servername` property in the `Bootstrap.properties` file);
Port number : The DB2 database server port. (This will be equivalent to the `curam.db.serverport` property in the `Bootstrap.properties` file);
Leave all other fields untouched unless a specific change is required and click **Next**;
7. Set the **Component-managed authentication alias** drop down value to: `<valid for database>`;
Set the **Mapping-configuration alias** drop down value to:
`DefaultPrincipalMapping`
Set the **Container-managed authentication alias** drop down value to: `<valid for database>`;
where the `<valid for database>` alias used is the one set up in “Creating the Data Source Login Alias” on page 7;
Leave all other fields untouched unless a specific change is required and click **Next** to continue.
8. Click **Finish** to confirm the changes and continue;
9. Select the newly created `DataSourceName` data source from the displayed list;
10. Select the **Custom Properties** link under **Additional Properties**;
11. Select the `fullyMaterializeLobData` entry;
12. Set the value to be `false`;
13. Click **OK** to confirm the change.

Save the Master Configuration

A *Save* can be performed by clicking the **Save** link in the **Message(s)** box. This box is displayed only after configuration changes have been made.

Configure Administration Security

The default user registry used by the application is the default WebSphere file-based user registry.

1. Navigate to **Security > Global security**;
2. Set the **Available realm definitions** to be **Federated repositories** and click the **Configure** button;
3. Set the **Primary administrative username** to be `websphere`;

4. Select the **Automatically generated server identity** radio button;
5. Select **Ignore case for authorization** and click **OK**;
6. Enter the password for the default administrative user, e.g. websphere, enter the confirmation and click **OK** to confirm the changes;
7. Set the **Available realm definitions** to be **Federated repositories** and click the **Set as current** button;
8. Select **Enable administrative security**;
9. Select **Enable application security**;
10. Select **Use Java 2 security to restrict application access to local resources** and **Warn if applications are granted custom permissions**;
11. Click the **Apply** button to confirm the changes;
12. Navigate to **Security > Global security**;
13. Select the **Custom Properties** link;
14. Click **New** and set the name and value as follows:
 Name= `com.ibm.ws.security.web.logoutOnHTTPSessionExpire`
 Value= `true`
15. Click **OK** to add the new property.
16. Navigate to **Security > Global security**;
17. Select **Web and SIP Security > Single sign-on (SSO)**;
18. Ensure the **Requires SSL** check box is unchecked;
19. Ensure that the value of the **Domain Name** field is set to the fully qualified domain name that will be used to access the application e.g. `xxx.com`. It should be configured similar to that specified in “Configuring the base URL in Cúram Portlets” on page 3;
20. Click **OK** to confirm the change.
21. Navigate to **Security > Global Security**;
22. Select **Custom properties**;
23. Add `com.ibm.ws.security.addHttpOnlyAttributeToCookies` with value `true`;
24. Click **OK** to confirm the change.
25. Save the changes to the master configuration.

Configure Users

The configured WebSphere Portal Server user registry is used for authentication of administrative users and the database user. The WebSphere Portal Server administrative users and the database user must be manually added to the user registry as follows.

- Navigate to **Users and Groups > Manage Users**;
- Click the **Create** button;
- Fill in the details for the Portal Server administrative user and click the **Create** button.
- Repeat the steps for the database user.
- For each user of a Cúram application (e.g admin application) the equivalent user should be set up as a user of the Portal Server. At a minimum the admin and caseworker users should be set up. The admin user should be set as follows:
 - The value of the User ID field must be set to `admin`
 - The value of the First name field could be set to `admin`
 - The value of the First name field could be set to `worker`

- The value of the Password and Confirm password fields must be set to the value of the password that will be used to access the admin application.

Note: If Portal Server administrative security was enabled when creating the profile the administrative user may already be defined in the registry.

Disable Cross Cluster Authentication

This property determines the behavior of a single sign-on LTPA Token2 login. The property `com.ibm.ws.security.webChallengeIfCustomSubjectNotFound` is set to `false` to ensure that web sessions can seamlessly transfer between two servers in a cluster (for example, in a fail over scenario) without being asked for security credentials.

1. Navigate to **Security > Global security**;
2. Click on **Custom properties** and select `com.ibm.ws.security.webChallengeIfCustomSubjectNotFound` property from the list of available properties.
3. Under General Properties, change the value of the `com.ibm.ws.security.webChallengeIfCustomSubjectNotFound` property to *false*
4. Click **OK** to confirm the addition;

Save the Changes

Save the changes to the master configuration as described in “Save the Master Configuration” on page 8.

Specific Server Configuration

This section describes how to configure the specific target with respect to the server scope i.e WebSphere_Portal.

Configure your JNDI lookup port

1. Navigate to **Servers > Server Types > WebSphere application servers**;
2. Select the relevant server from the list, e.g. WebSphere_Portal;
3. Expand **Ports** in the **Communications** section and click the **Details** button;
4. Select the **BOOTSTRAP_ADDRESS** entry and set the **Port** to match the value of the property `curam.server.port` in your `AppServer.properties` file;
5. Click **OK** to apply changes;
6. Save the changes made to the master configuration using the **Save** option as before.

Configure your ORB Pass By Reference

1. Navigate to **Servers > Server Types > WebSphere application servers**;
2. Select the relevant server from the list, e.g. WebSphere_Portal;
3. Expand **Container Services** in the **Container Settings** section and click the **ORB service** link;
4. Select the **Pass by reference** option from the **General Properties** section.
5. Click **OK** to apply changes;
6. Save the changes made to the master configuration using the **Save** option as before.

Configure your Java Virtual Machine

1. Navigate to **Servers > Server Types > WebSphere application servers**;
2. Select the appropriate server from the list i.e WebSphere_Portal;
3. In the **Server Infrastructure** section expand **Java and Process Management**;

4. Select the **Process definition** link;
5. In the **Additional Properties** section Select the **Java Virtual Machine** link;
6. Set the fields as follows:
Initial heap size :512
Maximum heap size :1024
Click **Apply** to set the values;
7. In the **Additional Properties** section Select the **Custom Properties** link;
8. Click **New** and set the properties as follows:
Name : com.ibm.websphere.security.util.authCacheCustomKeySupport
Value : false
Click **OK** to add the property;
9. *The following step is only required on non-Windows platforms.*
Click **New** and set the properties as follows:
Name : java.awt.headless
Value : true
Click **OK** to add the property;
10. Save the changes made to the master configuration using the **Save** option as before.

Configure your Timer Service

1. Navigate to **Servers > Server Types > WebSphere application servers**;
2. Select the appropriate server from the list i.e WebSphere_Portal;
3. In the **Container Settings** section expand **EJB Container Settings**;
4. Select the **EJB timer service settings** link;
5. In the Scheduler Type panel Select the **Use internal EJB timer service scheduler instance** option;
6. Set the fields as follows:
Data source JNDI name :jdbc/curamtimerdb
Data source alias : <valid for database>
where the alias used is the one set up in “Creating the Data Source Login Alias” on page 7;
7. Click **OK** to confirm the changes;
8. Save the changes made to the master configuration using the **Save** option as before.

Set up the Port Access

1. Navigate to **Servers > Server Types > WebSphere application servers**;
2. Select the appropriate server from the list i.e WebSphere_Portal;
3. Select the **Ports** link in the **Communications** section;
4. Click the **details** button;
5. Click **New** and set the following fields for the Client TCP/IP port:
User-defined Port Name : CuramClientEndPoint
Host : *
Port : 9044
Click **OK** to apply the changes;
6. Click **New** and set the following fields for the WebServices TCP/IP port:
User-defined Port Name : CuramWebServicesEndPoint

Host : *

Port : 9082

Click **OK** to apply the changes;

7. Navigate to **Servers > Server Types > WebSphere application Servers**;
8. Select the relevant server from the list i.e WebSphere_Portal;
9. Expand the **Web Container Settings** branch in the **Container Settings** section;
10. Select the **Web container transport chains** link;
11. Click **New** and set the following fields for the Client transport chain:
Name : CuramClientChain
Transport Chain Template : WebContainer-Secure
Click **Next**
Use Existing Port : CuramClientEndPoint
Click **Next** and **Finish**
12. Click **New** and set the following fields for the WebServices transport chain:
Name : CuramWebServicesChain
Transport Chain Template : WebContainer
Click **Next**
Use Existing Port : CuramWebServicesEndPoint
Click **Next** and **Finish**
13. Select the newly created **CuramClientChain**;
14. Select the **HTTP Inbound Channel** link;
15. Ensure the **Use persistent keep alive connections** check box is checked;
16. Click **OK** to confirm the addition;
17. Navigate to **Environment > Virtual hosts**;
18. Click **New** to add a new Virtual Host by setting the following fields;
Name = *client_host*
Repeat this step using the replacing *client_host* with *webservices_host*;
19. Select the **client_host** link from the list of virtual hosts;
Select the **Host Aliases** link in the **Additional Properties** section;
Click **New** to add a new Alias by setting the following fields;
Host Name = *
Port = 9044
where 9044 is the port used in step 5. Repeat this step for the other Virtual Host and port used (e.g. webservices_host, 9082);
20. Click **OK** to confirm the addition;
21. Save the changes to the master configuration as described in "Save the Master Configuration" on page 8.

Configure Session Security Integration

1. Navigate to **Servers > Server Types > WebSphere application servers**;
2. Select the relevant server from the list i.e WebSphere_Portal;
3. Click the **Session management** in the **Container Settings** section
4. Select the **Security integration**, *un-check. Note: Please make sure security integration is un-checked.*
5. Click **OK** to apply changes;

6. Save the changes made to the master configuration using the **Save** option as before.
- 7.

Note: This above setting is required for web applications.

Bus Configuration

Setup the Service Integration Bus

1. Navigate to **Service integration > Buses**;
2. Click **New** and in **Step 1** set the following field:
Name : CuramBus
 Leave everything else as the default and click **Next**;
3. Entering the **Configure bus security** Wizard, Step 1.1, click **Next**;
 In **Step 1.2** of the **Configure bus security** Wizard take the default setting and click **Next**;
 In **Step 1.3** of the **Configure bus security** Wizard take the default setting, as appropriate, and click **Next**;
 In **Step 1.4** of the **Configure bus security** Wizard review your settings and click **Next**;
4. In Step 2 click **Finish** to apply the changes.
5. Select the **CuramBus** now displayed on the list of Buses. This will open the configuration screen;
6. Select **Bus members** in the **Topology** section;
7. Click **Add** to open the **Add a New Bus Member** Wizard;
8. Select the server to add to the Bus and click **Next**;
9. Select **Data store** and click **Next**;
10. Select the option to **use existing data source** and set the options as follows:
Data source JNDI name = jdbc/curamsibdb
Schema name = *username*
 Where *username* is the database username.
 Deselect the **Create tables** option;
 Leave everything else as the default and click **Next**;
11. Take the default tuning parameters as appropriate and click **Next**;
12. Click **Finish** to complete and exit the Wizard;
13. Navigate to **Service integration > Buses**;
14. Select the **CuramBus** now displayed on the list of Buses. This will open the configuration screen;
15. Select **Security** in the **Additional Properties** section;
16. Select **Users and groups in the bus connector role** in the **Authorization Policy** section;
17. Click **New** to open the **SIB Security Resource Wizard**;
18. Select the **The built in special groups** radio button and click **Next**;
19. Select the **Server** and **AllAuthenticated** check boxes and click **Next**;
20. Click **Finish** to complete and exit the Wizard.
21. Save the changes to the master configuration as described in "Save the Master Configuration" on page 8.

JMS Configuration

Setup the JMS Connection Factories

1. Navigate to **Resources > JMS > JMS providers**;
2. *Note:* The appropriate scope where the JMS resources are to be defined should be selected at this point.
3. Select the **Default messaging provider** link;
4. Select the **Connection factories** link in the **Additional Properties** section;
5. Click **New** and set the following fields:
Name : CuramQueueConnectionFactory
JNDI Name : jms/CuramQueueConnectionFactory
Description : The factory for all connections to application queues.
Bus Name : CuramBus
Authentication alias for XA recovery : Same as for the jdbc/curamdb data source (e.g. <SERVERNAME> /dbadmin)
Mapping-configuration alias : DefaultPrincipalMapping
Container-managed authentication alias : Same as for the Authentication alias for XA recovery.
Leave everything else as the default and click **OK** to apply the changes;
6. Click **New** and set the following fields:
Name : CuramTopicConnectionFactory
JNDI Name : jms/CuramTopicConnectionFactory
Description : The factory for all connections to application queues.
Bus Name : CuramBus
Authentication alias for XA recovery : Same as for the jdbc/curamdb data source (e.g. <SERVERNAME> /dbadmin)
Mapping-configuration alias : DefaultPrincipalMapping
Container-managed authentication alias : Same as for the jdbc/curamdb data source (e.g. <SERVERNAME> /dbadmin)
Leave everything else as the default and click **OK** to apply the changes;
7. Save the changes to the master configuration as described in “Save the Master Configuration” on page 8.

Setup the Application Queues

Perform the following steps, substituting <QueueName> (without the angle brackets) with each of the following queue names: DPEnactment, DPError, CuramDeadMessageQueue, WorkflowActivity, WorkflowEnactment and WorkflowError.

1. Navigate to **Service integration > Buses > CuramBus**;
2. Select the **Destinations** link in the **Destination resources** section;
3. Click **New** to open the “Create new destination” wizard;
4. Select **Queue** as the destination type and click **Next**;
5. Set the following queue attributes:
Identifier : SIB_ <QueueName>
Leave everything else as the default and click **Next**;
6. Use the **Selected Bus Member** and click **Next**;
7. Click **Finish** to confirm the queue creation.

8. Select the newly added SIB_ <QueueName> queue now displayed on the list of existing providers. This will open the configuration screen again;
9. Use the following table to set the Exception Destination via the **Specify** radio button and associated text field;

Table 2. Exception Destination Settings

Queue Name	Exception Destination
SIB_CuramDeadMessageQueue	System
SIB_DPEnactment	SIB_DPErrors
SIB_DPErrors	SIB_CuramDeadMessageQueue
SIB_WorkflowActivity	SIB_WorkflowErrors
SIB_WorkflowEnactment	SIB_WorkflowErrors
SIB_WorkflowErrors	SIB_CuramDeadMessageQueue

10. Click **OK** to apply the changes.
11. Navigate to **Resources > JMS > JMS providers**;
12. Select the **Default messaging provider** link;
13. Select the **Queues** link in the **Additional Properties** section;
14. Click **New** and set the following fields:
 - Name** : <QueueName>
 - JNDI Name** : jms/ <QueueName>
 - Bus Name** : CuramBus
 - Queue Name** : SIB_ <QueueName>
 - Delivery Mode** : Persistent
 Leave everything else as the default and click **OK** to apply the changes.

Save the changes to the master configuration as described in “Save the Master Configuration” on page 8.

Setup the Application Topics

1. Navigate to **Resources > JMS > JMS providers**;
2. Select the **Default messaging provider** link;
3. Select the **Topics** link in the **Additional Properties** section;
4. Click **New** and set the following fields:
 - Name** : CuramCacheInvalidationTopic
 - JNDI Name** : jms/CuramCacheInvalidationTopic
 - Description** : Cache Invalidation Topic
 - Bus name** : CuramBus
 - Topic space** : Default.Topic.Space
 - JMS Delivery Mode** : Persistent
 Leave everything else as the default and click **OK** to apply the changes.
5. Save the changes to the master configuration as described in “Save the Master Configuration” on page 8.

Configure Historical Log Files

This is an optional step. It is possible to configure the maximum number of historical log files maintained by a particular server. To do this

1. Navigate to **Servers > Server Types > WebSphere application servers**;

2. Select the relevant server from the list of servers;
3. Select **Logging and Tracing** from the **Troubleshooting** section;
4. Select **JVM Logs** from the **General Properties** list;
5. Change the **Maximum Number of Historical Log Files** field to 30 for both the System.out and System.err files;
6. Click **OK** to apply the changes;
7. Save the changes to the master configuration.

Completion

The Portal Server is now configured and ready to install an application on it. Log out of the Administration Console and restart the Portal Server.

Configuring Portal Server to reuse JSESSIONID

In order to enable Single Sign on between an the Cúram application and Cúram Portlets, the JSESSIONID information must be maintained. In order to do this, the following must be done:

- Navigate to **Servers > ServerTypes > WebSphere application servers > WebSphere_Portal > Server Infrastructure > Java and Process Management > Process Definition > Java Virtual Machine > Custom Properties > New;**
- Set HttpSessionIdReuse as the value of the Name field and set true as the value of the Value field.
- Click the **OK** to apply the changes.
- Save the changes to the master configuration

Manual Application Deployment

To install an enterprise application in WebSphere, the Administration Console can be used. The steps below describe how to install an application, EJB component, or Web module using the Administrative Console.

Note: Once the install has been started, the **Cancel** button must be used to exit if the installation of the application is aborted. It is not sufficient to simply move to another Administrative Console page without first clicking **Cancel** on an application installation page.

1. Navigate to **Applications > New Application;**
2. Select **New Enterprise Application;**
3. Click the appropriate radio button and specify the full path name of the source application file or EAR file, optionally via the **Browse** button, in the Path to the new application panel and click **Next;**
The default location for the application EAR files is:
`%SERVER_DIR%/build/ear/WAS/Curam.ear`
4. Select the **Fast Path - Prompt only when additional information is required** radio button in the How do you want to install the application? panel and click **Next;**
5. Leave the defaults as they are for step 1, *Select installation options* and click **Next;**
6. In step 2, **Map modules to servers**, for every module listed, select a target server or a cluster from the **Clusters and Servers** list. To do this, tick the check box beside the particular module(s) and then select the server or cluster and click **Apply.**

7. Click **Next** and then **Finish** to complete the installation. This step may take a few minutes and should finish with the message *Application Curam installed successfully*.
8. Save the changes to the Master Configuration. (See “Save the Master Configuration” on page 8 for more details.)
9. Navigate to **Applications > Application Types > WebSphere enterprise applications** and select the newly installed application.
10. Select the **Class loading and update detection** option from the **Detail Properties** section.
11. Set the **Class loader order** to be **Classes loaded with local class loader first (parent last)**.
12. Set the **WAR class loader policy** to be **Single class loader for application**.
13. Click **OK**.
14. Select the **Security role to user/group mapping** option from the **Detail Properties** section and map the mdbuser role to a username and password as per these steps:

Note: The username you use to map to the mdbuser role must already be defined in your user registry.

- a. Check **Select** for the mdbuser role and click **Map users**;
- b. Enter the appropriate username in the **Search String** field and click **Search**;
- c. Select the ID from the **Available:** list and click >> to add it to the **Selected:** list and click **OK**.
- d. Click **OK**.
15. Having mapped the mdbuser role you can now update the user RunAs role by selecting the **User RunAs roles** option from the **Detail Properties** section.
16. Enter an appropriate username and password in the **username** and **password** fields, respectively. Check **Select** for the mdbuser role and click **Apply**.
17. Click **OK**.
18. Save the changes to the master configuration.
19. After deployment it is necessary to start the application before it can be used. Navigate to **Applications > Application Types > WebSphere enterprise applications**, tick the check box for the newly installed application, and click the **Start** button. This step may take a few minutes and should finish with the application status changing to indicate it has been started.
20. Finally, test the application deployment. For example, point a Web browser at the URL for the deployed application e.g. <https://localhost:9044/Curam>.

Notices

This information was developed for products and services offered in the United States.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing IBM Corporation North Castle Drive, MD-NC119 Armonk, NY 10504-17

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing Legal and Intellectual Property Law IBM Japan Ltd. 19-21, Nihonbash

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Privacy Policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings

can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies or other similar technologies that collect each user's name, user name, password, and/or other personally identifiable information for purposes of session management, authentication, enhanced user usability, single sign-on configuration and/or other usage tracking and/or functional purposes. These cookies or other similar technologies cannot be disabled.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at <http://www.ibm.com/privacy> and IBM's Online Privacy Statement at <http://www.ibm.com/privacy/details> the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at <http://www.ibm.com/software/info/product-privacy>.

Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at " Copyright and trademark information " at <http://www.ibm.com/legal/copytrade.shtml>.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java[™] and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other names may be trademarks of their respective owners. Other company, product, and service names may be trademarks or service marks of others.



Printed in USA