SYBASE®
An SAP® Company

Installation Guide

Sybase Brand Mobiliser 1.3

DOCUMENT ID: DC01971-01-0130-01
LAST REVISED: June 2013

Sybase, Inc., One Sybase Drive, Dublin, CA 94568.

Contents

Getting Started

You can install Sybase® Brand Mobiliser in both development and production environments. Brand Mobiliser runs in an OSGi-compliant container.

Before you install Brand Mobiliser, familiarize yourself with the supported hardware and software—see the *Brand Mobiliser Release Bulletin*.

Although Brand Mobiliser works closely with the Mobiliser Platform, the Brand Mobiliser installation is independent of the Mobiliser Platform installation. You can install Brand Mobiliser on a server or on a developer workstation.

New Installations

If no earlier version of Brand Mobiliser is installed, install Brand Mobiliser version 1.3. After you install, the system is ready to run in a development environment.

Upgrades

If Brand Mobiliser version 1.2 and a production database (DB2 or Oracle) are already installed:

1. Install Brand Mobiliser version 1.3.
2. Upgrade the database.

See also

- *Installing Brand Mobiliser* on page 3
- *Setting Up a Production System* on page 7
- *Upgrading the Brand Mobiliser Database* on page 9

Installing Brand Mobiliser

Install Brand Mobiliser on AIX, Linux, or Windows machines. After you install Brand Mobiliser, it is ready to run as a development system, using the embedded Apache Derby database.

Prerequisites

Verify that you are running a supported version of the JDK or JRE on the installation system —see the *Brand Mobiliser Release Bulletin*.

Task

The Brand Mobiliser distribution binary is `aims-brand-mobiliser-1.3.1.zip`.

1. Copy `aims-brand-mobiliser-1.3.1.zip` from the distribution medium to the installation location.
2. In the installation location, run:

   ```
   unzip aims-brand-mobiliser-1.3.1.zip
   ```

   The *BRAND_HOME* installation directory is created with these contents:
   - `bin/` – Apache Felix kernel and main subsystem bundles.
   - `bundle/` – OSGi bundles.
   - `conf/` – configuration files.
   - `derby/` – embedded Apache Derby database.
   - `license/` – open source license information.
   - `sql/` – database scripts.
   - `thirdparty/` – third-party libraries and manifest.
   - `upload/` – default folder for uploading subscribers.
   - `README.html` – software documentation updates.
3. In a Web browser, read the release notes in *BRAND_HOME*`/README.html`.

Next

For development, start the server.

See also

- *Hashing the Admin Password* on page 20

Starting the Server

Start the Brand Mobiliser server.

Prerequisites

Install Brand Mobiliser.

Task

The start-up scripts (`run.sh` and `run.bat`) expect the location of the `java` application to be in the PATH. If you plan to run a start-up script in production, modify the script to reflect your system architecture. You need not have root privilege to execute a start-up script.

Change to the *BRAND_HOME* directory, and run the command or commands for your platform:

Platform	Command
Windows	`bin\run.bat`
AIX or Linux	`chmod 755 bin/run.sh` `bin/run.sh start`

See also

- *Configuring the Event Scheduler JDBC Driver* on page 17

Launching the Brand Mobiliser Web UI

Use a Web browser to launch the Brand Mobiliser Web UI and log in to the server.

Prerequisites

Start the Brand Mobiliser server.

Task

1. Open a browser and navigate to either:
   - `http://localhost:8080/brand`, or
   - `http://server:8080/brand`, where *server* is the name of the server on which Brand Mobiliser is running.
2. Log in to the Brand Mobiliser Web UI.

   The default login credentials are:

- User Name – `admin`
- Password – `Brand!23`

If you created a new admin password, use it to log in.

Setting Up a Production System

Install Brand Mobiliser on an AIX, Linux, or Windows machine to run in a production system.

Some steps vary depending on enterprise IT policies and deployment landscape; use them as a starting point for consultation and discussion with your system architect.

1. *Installing Brand Mobiliser*

   Install Brand Mobiliser on AIX, Linux, or Windows machines. After you install Brand Mobiliser, it is ready to run as a development system, using the embedded Apache Derby database.

2. *Hashing the Admin Password*

   Run the password-hashing tool for the admin user password, and insert it into the database script that creates the admin user. The hashed password is stored in the database.

3. *Configuring New Database Installations*

   Brand Mobiliser installs with an embedded Apache Derby database that you can use for development and testing. For production, use either an IBM DB2 or an Oracle database.

4. *Enabling Encryption*

   After you enable encryption, you can encrypt any Brand Mobiliser property value. By default, encryption is disabled.

5. *Configuring Authentication*

   By default, when you log in to the Brand Mobiliser Web UI, authentication is performed using the built-in database model (authentication.bean=AuthenticationManager). You can reconfigure authentication to use an LDAP system.

6. *Configuring the Event Scheduler JDBC Driver*

   To manage events that trigger event applications, configure the JDBC database driver that the event scheduler uses. The event scheduler is based on the Quartz scheduler.

7. *Starting the Server*

   Start the Brand Mobiliser server.

8. *Launching the Brand Mobiliser Web UI*

   Use a Web browser to launch the Brand Mobiliser Web UI and log in to the server.

Upgrading the Brand Mobiliser Database

Before you upgrade the Brand Mobiliser database from version 1.2 to version 1.3, back up the database.

Prerequisites

- Back up the database.
- Consult the DBA who maintains the Brand Mobiliser database to find out about any customizations to the existing schema, such as the tablespace or users.

Task

1. Change to the *BRAND_HOME*/`sql/`**database**`/Upgrade_1.2` directory, where **database** is either db2 or oracle.
2. Log in to the database, and run:
   ```
   03b-BrandMobiliser-Objects.sql
   ```

Configuring New Database Installations

Brand Mobiliser installs with an embedded Apache Derby database that you can use for development and testing. For production, use either an IBM DB2 or an Oracle database.

Prerequisites

Install a DB2 or an Oracle database—see the *Brand Mobiliser Release Bulletin* for supported database versions.

Task

A database administrator (DBA) should install, configure, and support a production database. Installation procedures vary by database platform; review them with your DBA. To support Brand Mobiliser, run database scripts to create a tablespace, database objects, and the initial data.

1. Review the database scripts that are included with Brand Mobiliser for compliance with corporate policies.
2. Perform the appropriate tasks for your database:

Database	Perform These Tasks
IBM DB2	• *Configure the DB2 Database* on page 12 • *Enable the DB2 JDBC Driver* on page 13
Oracle	• *Configure the Oracle Database* on page 14 • *Install the Oracle JDBC Driver* on page 15 • *Enable the Oracle JDBC Driver* on page 16

Note: Derby scripts are provided for a standalone Derby installation, also known as a network server. Test and certify a Derby network server installation before deploying it to a production environment.

See also

- *Hashing the Admin Password* on page 20
- *Enabling Encryption* on page 19

IBM DB2 Database

You can use an IBM DB2 database in a Brand Mobiliser production system.

Install an IBM DB2 database version that has been tested and certified for Brand Mobiliser —see the *Brand Mobiliser Release Bulletin*.

Configuring DB2 Databases

Configure an IBM DB2 database for new Brand Mobiliser installations.

Prerequisites

1. Install the DB2 database.
2. Create a new hashed password for the admin user, and save it in the `/sql/common/1.3.1/04-BrandMobiliser-Base-Data.sql` script.

Task

To complete this task, you must either be a root user or have sudo privileges. DB2 database scripts are located in the *BRAND_HOME*`/sql/db2/1.3.1` directory.

1. To add system groups, on the command line, run:

```
groupadd -g 999 db2iadm1
groupadd -g 998 db2fadm1
groupadd -g 997 dasadm1
```

2. To add system users, run:

```
useradd -u 1004 -g db2iadm1 -m -d /home/mwiz2 mwiz2
useradd -u 1003 -g db2fadm1 -m -d /home/db2fenc1 db2fenc1
useradd -u 1002 -g dasadm1 -m -d /home/dasusr1 dasusr1
```

3. For each new user, change the password:

```
passwd mwiz2
passwd db2fenc1
passwd dasusr1
```

   The default password for each user is “sql.”

4. Create a DB2 instance:

```
$ pwd
/opt/IBMdb2/V9.7/instance/
$ ./db2icrt -a server -u db2fenc1 mwiz2
```

5. Verify the database installation:
   a) Log in as mwiz2, using the password set in step 3.
   b) Start the database manager:

```
db2star
```

c) Create the sample database:
```
db2sampl
```
d) Start the DB2 command line processor:
```
db2
```
e) Connect to the sample database:
```
connect to sample
```

6. Create the **brandmob** database and grant DBA privileges to the mwiz2 user, by running:
```
01-BrandMobiliser-DB_DB2.sql
```
Ensure that the current DB2 instance has write privileges to the data directory, which the script assumes is `/home/db2`.
7. Connect to the newly created **brandmob** database as the mwiz2 user:
```
db2 connect to brandmob user mwiz2 using sql
```
8. Insert initial data and create the admin user:
```
04-BrandMobiliser-Base-Data.sql
```

Next
Enable the DB2 JDBC driver.

See also
- *Enabling the DB2 JDBC Driver* on page 13

Enabling the DB2 JDBC Driver
To use an IBM DB2 database, enable the JDBC driver that is installed with Brand Mobiliser.

Prerequisites
Configure the DB2 database.

Task

1. Open the *BRAND_HOME*`/conf/cfgbackup/service.dsprovider.properties` file.
2. Remove the comment indicators from the DB2 configuration, and enter the password you created for the mwiz2 user:
   - If the password is encrypted, replace `XXX` with the encrypted password.
   - If the password is plain text, replace `{enc}XXX` with the password.
```
# DB2
driverClassName=com.ibm.db2.jcc.DB2Driver
url=jdbc:db2://localhost:60000/brandmob
username=mwiz2
```

```
password={enc}XXX
validationQuery=select 1 from sysibm.sysdummy1
```

3. Comment out the Derby configuration, and save the file:

```
# DERBY EMBEDDED  - For development and Testing only!!!!!
#driverClassName=org.apache.derby.jdbc.EmbeddedDriver
#url=jdbc:derby:mwiz2
#username=mwiz2
#password=sql
#validationQuery=select 1 from sysibm.sysdummy1
```

See also

- *Configuring DB2 Databases* on page 12
- *Encrypting Property Values* on page 20

Oracle Database

You can use an Oracle database in a Brand Mobiliser production system.

Install an Oracle database version that has been tested and certified for Brand Mobiliser—see the *Brand Mobiliser Release Bulletin*.

Configuring Oracle Databases

Configure an Oracle database for new Brand Mobiliser installations.

Prerequisites

1. Install an Oracle database.
2. Create a new hashed password for the admin user, and save it in the `/sql/common/1.3.1/04-BrandMobiliser-Base-Data.sql` script.

Task

Consult your DBA for a custom installation using an existing tablespace or user for the Brand Mobiliser schema.

1. Edit the *BRAND_HOME*`/sql/oracle/1.3.1/02-BrandMobiliser-Users.sql` script, and replace `XXX` with a password for the mwiz2 user:

```
create user mwiz2 identified by XXX;
```

2. As a user with DBA privileges, log in to the database.
3. Create a tablespace:

```
/sql/oracle/1.3.1/01-BrandMobiliser-Tablespaces.sql
```

4. Create the mwiz2 user:

```
/sql/oracle/1.3.1/02-BrandMobiliser-Users.sql
```

5. As the mwiz2 user, create a schema:
   ```
   /sql/oracle/1.3.1/03a-BrandMobiliser-Objects.sql
   ```
   Perform all remaining steps as the mwiz2 user.
6. Create another schema:
   ```
   oracle/1.3.1/03b-BrandMobiliser-Objects.sql
   ```
7. Insert initial data and create the admin user:
   ```
   /sql/common/1.3.1/04-BrandMobiliser-Base-Data.sql
   ```
8. Configure the JDBC connection in `conf/cfgback/service.dsprovider.properties`.

Next

Install the Oracle JDBC driver.

See also

- *Installing Oracle JDBC Drivers* on page 15
- *Enabling the Oracle JDBC Driver* on page 16
- *Encrypting Property Values* on page 20

Installing Oracle JDBC Drivers

To use an Oracle database, install an Oracle JDBC driver.

1. Download the Oracle JDBC driver from the Oracle Web site at *http://www.oracle.com/technetwork/database/features/jdbc/index-091264.html*.
2. Unzip the downloaded package and find `ojdbc6.jar`.
3. Copy `ojdbc6.jar` to the `thirdparty/oracle` directory.

   There should be a manifest file in the directory called `oraclemanifest`.
4. Update the manifest in `ojdbc6.jar` with `oraclemanifest`:
   a) Change to the `thirdparty/oracle` directory.
   b) Run:
      ```
      jar -umvf oraclemanifest ojdbc6.jar
      ```
5. Copy the modified `ojdbc6.jar` to the `bundle/application` directory, and rename it `oracle-jdbc-osgi_11.2.0.2.0-1.0.0.jar`:
   ```
   cp ojdbc6.jar ${BRAND_HOME}/bundle/application/oracle-jdbc-osgi_11.2.0.2.0-1.0.0.jar
   ```
   where BRAND_HOME is set to the Brand Mobiliser installation directory.
6. Configure the location of the Oracle JDBC driver:
   a) Open the `conf/config.properties` file.
   b) Under the #JDBC drivers section, add this line:

```
${aims.app.dir}/oracle-jdbc-osgi_11.2.0.2.0-1.0.0.jar
```

Next

Enable the Oracle JDBC driver.

See also

- *Configuring Oracle Databases* on page 14
- *Enabling the Oracle JDBC Driver* on page 16

Enabling the Oracle JDBC Driver

To use an Oracle database, enable the Oracle JDBC driver that you installed.

Prerequisites

- Configure an Oracle database.
- Install an Oracle JDBC driver.

Task

1. Open the *BRAND_HOME*`/conf/cfgbackup/service.dsprovider.properties` file.
2. Remove the comment indicators from the Oracle configuration, and enter the password you created for the mwiz2 user:
   - If the password is encrypted, replace `XXX` with the encrypted password.
   - If the password is plain text, replace `{enc}XXX` with the password.

```
# Oracle
driverClassName=oracle.jdbc.driver.OracleDriver
url=jdbc:oracle:thin:@localhost:1521:xe
username=mwiz2
password={enc}XXX
validationQuery=select 1 from DUAL
```

3. Comment out the Derby configuration, and save the file:

```
# DERBY EMBEDDED  - For development and Testing only!!!!!
#driverClassName=org.apache.derby.jdbc.EmbeddedDriver
#url=jdbc:derby:mwiz2
#username=mwiz2
#password=sql
#validationQuery=select 1 from sysibm.sysdummy1
```

See also

- *Configuring Oracle Databases* on page 14
- *Installing Oracle JDBC Drivers* on page 15
- *Encrypting Property Values* on page 20

Configuring the Event Scheduler JDBC Driver

To manage events that trigger event applications, configure the JDBC database driver that the event scheduler uses. The event scheduler is based on the Quartz scheduler.

The event scheduler persists schedules in the database. The event scheduler uses a JDBC driver different from the one Brand Mobiliser uses, and you must configure it separately.

1. Open the *BRAND_HOME*`/conf/cfgbackup/service.event.quartz.properties` file.
2. For your database, enable the JDBC driver, and save the file:
   - For Oracle databases, uncomment this line:

```
#jobStore.driverDelegateClass=org.quartz.impl.jdbcjobstore.oracle.OracleDelegate
```

   - For most other databases, use the default driver:

```
jobStore.driverDelegateClass=org.quartz.impl.jdbcjobstore.StdJDBCDelegate
```

   - For other databases that do not work with the default driver, see the Quartz documentation at *http://www.quartz-scheduler.org/documentation/quartz-1.x/configuration/ConfigJobStoreTX*.

See also

- *Configuring Authentication* on page 22
- *Starting the Server* on page 4

Security

To secure passwords and other properties, you can encrypt them. To secure the admin password, use the hashing tool, and store the hashed version in the database.

See also

- *Enabling Encryption* on page 19
- *Encrypting Property Values* on page 20
- *Hashing the Admin Password* on page 20
- *Enabling SSL* on page 21
- *Configuring Authentication* on page 22

Enabling Encryption

After you enable encryption, you can encrypt any Brand Mobiliser property value. By default, encryption is disabled.

1. Open the *BRAND_HOME*`/conf/system.properties` file.
2. Uncomment this line, and replace `samplesecret` with a new value for `decryptionkey`:

```
# com.sybase365.arf.container.system.decryptionkey=samplesecret
```

3. (Optional) Uncomment this line, and set `decryptionkeylength` to a higher value, for example, 256 or 512, and save the file:

```
# com.sybase365.arf.container.system.decryptionkeylength=128
```

   - If the line remains commented out, the default value, 128, is used.
   - If you uncomment the line, and set the value to 256 or higher, you must install the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6. See *http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html*. Do not set the decrpytion key length to a value greater than 2048.

4. Stop and restart Brand Mobiliser.

See also

- *Encrypting Property Values* on page 20
- *Configuring New Database Installations* on page 11
- *Configuring Authentication* on page 22
- *Hashing the Admin Password* on page 20
- *Enabling SSL* on page 21

- *Security* on page 19

Encrypting Property Values

You can encrypt property values in Brand Mobiliser configuration files using its encryption tool. Passwords are the most commonly encrypted values, but you can encrypt any value.

Prerequisites

Enable encryption.

Task

1. Go to *BRAND_HOME*/`bin`, and run:

   ```
   ../encrypt.sh decryptionValue password
   ```

   where:
   - *decryptionValue* is the value of `decryptionkey`, defined in `system.properties`.
   - *password* is the property value to encrypt.

   The result of running the `encrypt.sh` command is an encrypted and Base64-encoded value, for example:

```
x9CJt8qwgXSuDN7FY21mVOIZ1WiwIRiJoX9CatjqQiYRPjmj7NdeAchigFmxQKX4
```

2. In the configuration file, enter the encrypted value, prepended with `{enc}`, for example:

```
password={enc}x9CJt8qwgXSuDN7FY21mVOIZ1WiwIRiJoX9CatjqQiYRPjmj7NdeAchigF
mxQKX4
```

   `{enc}` alerts the configuration manager to unencrypt the property value before using it.

See also

- *Enabling Encryption* on page 19
- *Hashing the Admin Password* on page 20
- *Enabling SSL* on page 21
- *Configuring Authentication* on page 22
- *Security* on page 19

Hashing the Admin Password

Run the password-hashing tool for the admin user password, and insert it into the database script that creates the admin user. The hashed password is stored in the database.

To comply with SAP® security requirements, the script for creating the admin user is disabled. The admin password in the `/sql/common/1.3.1/04-BrandMobiliser-Base-`

`Data.sql` script is a hashed version of `Brand!23`. Replace this password with a new hashed password.

1. To generate a hashed password, navigate to the `/bin` directory, and run:

   ```
   ./passwordtool.sh password
   ```

   where *password* is the password to hash.
2. Edit the `04-BrandMobiliser-Base-Data.sql` script, uncomment these lines, and replace `$2a$10$xVTSvw3hcCFtZ2DnMav.Te/WsOMBtLC1MV0QLi/z.ziUyJY/T.d0i` with the newly hashed password:

```
--INSERT INTO M_USERS (ID,USERNAME,PASSWORD,DISABLED)
--VALUES (1,'admin','$2a$10$xVTSvw3hcCFtZ2DnMav.Te/WsOMBtLC1MV0QLi/z.ziUyJY/T.d0i',0);
```

See also

- *Installing Brand Mobiliser* on page 3
- *Configuring New Database Installations* on page 11
- *Enabling Encryption* on page 19
- *Encrypting Property Values* on page 20
- *Enabling SSL* on page 21
- *Configuring Authentication* on page 22
- *Security* on page 19

Enabling SSL

Enable SSL for the Brand Mobiliser Web UI (HTTPS).

Brand Mobiliser embeds Jetty for its javax.servlet container capability. Configure Jetty for SSL, and use the X.509 certificate, which SAP® recommends.

1. Create a keystore if one does not yet exist:
   a) On the command line, enter:

```
keytool -keystore keystore -alias jetty -genkey -keyalg RSA
```

   b) Follow the onscreen instructions. Enter the first and last name to match your machine host name.
   c) Copy the keystore file to the *BRAND_HOME*`/conf/keystore` directory.
2. In the `conf/cfgbackup` directory, create an `org.ops4j.pax.web.properties` file (if it does not already exist), and add these lines:

```
# Enable SSL
org.osgi.service.http.secure.enabled=true

# SSL Port
```

```
org.osgi.service.http.port.secure=8443

# Keystore created to hold SSL certificate
org.ops4j.pax.web.ssl.keystore=conf/keystore

# Keys to access Keystore and SSL certificate
org.ops4j.pax.web.ssl.password=password
org.ops4j.pax.web.ssl.keypassword=keypassword
```

3. To encrypt the properties **org.ops4j.pax.web.ssl.password** and **org.ops4j.pax.web.ssl.keypassword**, run the encryption tool.
4. Enter the encrypted passwords, as in the example, below:

```
# Keys to access Keystore and SSL certificate
org.ops4j.pax.web.ssl.password={enc}cMYSsdsyRNzhyKlrBzbLIUH1z0tux5jykXWx
Pn76RlU=
org.ops4j.pax.web.ssl.keypassword={enc}$2a$10$xVTSvw3hcCFtZ2DnMav.Te/
WsOMBtLC1MV0QLi
```

5. Stop and restart Brand Mobiliser.
6. Verify the connection at https://*hostname*:8443/brand, where *hostname* is the name of the machine on which Brand Mobiliser is running.

For more information about configuring Jetty for SSL, see *http://www.eclipse.org/jetty/documentation/current/*

See also

- *Enabling Encryption* on page 19
- *Encrypting Property Values* on page 20
- *Hashing the Admin Password* on page 20
- *Configuring Authentication* on page 22
- *Security* on page 19

Configuring Authentication

By default, when you log in to the Brand Mobiliser Web UI, authentication is performed using the built-in database model (authentication.bean=AuthenticationManager). You can reconfigure authentication to use an LDAP system.

1. Open the *BRAND_HOME*`/conf/cfgbackup/service.webui.security.properties` file.
2. Set the value of `authentication.bean` to either:
   - `AuthenticationManager` – database authentication, database-role authorization, or
   - `LdapAuthenticationManager` – LDAP authentication, database-role authorization.

3. If you set the value of `authentication.bean` to `LdapAuthenticationManager`:
   a) Add these lines to the file:
   ```
   username=admin
   pwd=brandldap
   ```
   b) Reconfigure the `ldap.*` properties to connect to the LDAP system provided by your enterprise IT administrator.
   ```
   ldap.host=localhost
   ldap.port=389
   ldap.userpath=uid={uid},ou=people,o=sybase365
   ldap.security.authentication=SIMPLE
   ```
4. Stop and restart Brand Mobiliser.

See also

- *Enabling Encryption* on page 19
- *Configuring the Event Scheduler JDBC Driver* on page 17
- *Encrypting Property Values* on page 20
- *Hashing the Admin Password* on page 20
- *Enabling SSL* on page 21
- *Security* on page 19

Users

The admin user is automatically created in the embedded Derby database when you install Brand Mobiliser. The admin user is created in a production database when you run the Brand Mobiliser database scripts. The admin user has the SUPER_ADMIN role and unlimited access to the system.

The initial password for the admin user is `Brand!23`. In a production system, the admin user should change the password. The admin user is the platform administrator. Some tasks, such as creating workspaces, and restarting and configuring channels, can be performed only by the platform administrator. In practice, the platform administrator generally creates and configures workspaces, and grants the ADMIN role to users.

A user with the ADMIN role can administer workspaces, create users, and assign workspaces to users. A user with the ADMIN role who is assigned to more than one workspace is the administrator for all those workspaces.

You cannot delete users from the Brand Mobiliser Web UI; however, you can deactivate them using the Manage User screen. When an inactive user tries to log in, he or she sees `Invalid user ID or password`.

Adding Users

On the Manage Users screen, administrators can add new users, and assign roles and workspaces to them.

1. On the Brand Mobiliser Web UI navigation bar, select **Workspace Administration**.
2. Select **Manage Users**, then select **Add New User**.
3. Enter:

Property Name	Description
User name	Login name for the user.
Password	Password for the user.
Reenter Password	Reenter the password.
Roles	• To assign a role to the user, select the role from the Available list, and click the right arrow. • To remove a role, select it in the Selected list, and click the left arrow.

Property Name	Description
Workspaces	• To assign a workspace to the user, select the workspace in the Available list, and click the right arrow. • To unassign a workspace from the user, select the workspace in the Selected list, and click the left arrow.

4. Click **Save**.

Workspaces

A Brand Mobiliser workspace is a logical grouping of applications, users, and other artifacts. When you install Brand Mobiliser, the default workspace, which you can use for development, is created automatically.

Brand Mobiliser workspaces meet both development and deployment needs. In the development environment, a workspace provides the logical grouping of users who are collaborating on projects or tasks. A workspace can also be used for partitioning development, QA, and production environments.

Index

R

S

U

W