SYBASE®
An SAP® Company

System Administration

Sybase Brand Mobiliser 1.3

DOCUMENT ID: DC01972-01-0130-01
LAST REVISED: June 2013

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

Contents

Introduction **1**
Security **3**
Enabling Encryption 3
Encrypting Property Values 4
Enabling SSL 4
Configuring Authentication 5
Users **7**
Adding Users 7
Editing User Properties 8
Deactivating Users 9
User Roles 9
Deleting Users 11
Communication Channels **13**
Configuring SMPP Inbound Channels 13
Configuring SMPP Outbound Channels 14
Configuring JMS Channels 15
Workspaces **17**
Creating Workspaces 18
Opening Workspaces 19
Default Menu 19
Configuring Default Menus 20
Deleting Workspaces 21
Categories **23**
Subscribers **25**
Creating Empty Subscriber Sets 26
Uploading Subscriber Sets 26
Reports **29**
Generating Traffic Reports 29
Generating Subscriber Reports 30
Maintenance and Tuning **31**
System Configuration Files 31

Editing Configuration Files 32
Log Files 33
Database Table Maintenance 33
Default Ports 34
Brand Mobiliser Processing Engine 35
Monitoring Sessions 37
Viewing Processing Engine Logs 37
Processing Engine Performance 37
Index 41

Introduction

Sybase® Brand Mobiliser administrators configure platform components and ensure that the production system works efficiently as a result of that configuration.

Brand Mobiliser defines three types of administrators: system administrators, platform administrators, and workspace administrators.

Typically, system administrators:

- Are IT professionals
- Install software
- Secure production systems
- Start and stop the server
- Configure Brand Mobiliser properties
- Monitor and tune the system

A platform administrator:

- Is created in the production database when you run the database scripts: one in each Brand Mobiliser installation
- Has the SUPER_ADMIN role; user name is admin
- Is the first user to log in to the Brand Mobiliser Web UI
- Creates workspaces and default menus
- Adds and configures users
- Sets up communication channels

Workspace administrators:

- Are created by the platform administrator: one for each workspace
- Have the ADMIN role
- In their workspaces, create users, manage default menus and categories, and generate reports

Security

To secure a production system, Brand Mobiliser provides encryption capability, SSL connections, and choices for a system-authentication manager.

See also

- *Communication Channels* on page 13
- *User Roles* on page 9

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 4

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 3
- *Enabling SSL* on page 4

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

- *Encrypting Property Values* on page 4

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.

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**.

See also

- *Editing User Properties* on page 8
- *Deactivating Users* on page 9
- *User Roles* on page 9

Editing User Properties

You can edit properties for users in the current workspace.

Although an administrator can have access to multiple workspaces, only users in the workspace that he or she is currently logged in to appear.

1. On the Brand Mobiliser Web UI Navigation bar, select **Workspace Administration**.
2. Select **Manage Users**.
3. Select the user whose properties you want to edit.
4. You can edit these properties:

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.
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.

5. Click **Save**.

See also

- *Adding Users* on page 7
- *Deactivating Users* on page 9
- *User Roles* on page 9

Deactivating Users

Deactivate users to prevent them from accessing applications.

1. On the Brand Mobiliser Web UI Navigation bar, select **Workspace Administration**.
2. Select **Manage Users**.
3. Select the user you want to deactivate.
4. Select **Actions > Disable User**.

   You can also deactivate users by assigning them to the default workspace, which removes their assigned roles. Users can still log in, but cannot access an active workspace.

See also

- *Adding Users* on page 7
- *Editing User Properties* on page 8
- *User Roles* on page 9

User Roles

Brand Mobiliser roles restrict access to screens and controls.

SUPER_ADMIN

The default user (admin) has the SUPER_ADMIN role. Do not change this configuration, but do change the password. The default password is `Brand!23`. The admin user is created in the production database when you run the Brand Mobiliser database scripts.

A user with the SUPER_ADMIN role is the platform administrator, has unlimited access to the system, and exclusive access to the Workspace Administration screen, which can be used to:

- Create and manage workspaces
- Create the QA workspace, and assign it to the workspace administrator
- Configure channels
- Start, stop, and restart the processing engine

A SUPER_ADMIN user can also perform any function available to other roles.

ADMIN

A user with the ADMIN role is called the workspace administrator. Each workspace should have an assigned workspace administrators who can create users for the workspace, set up the default menu, and manage sessions.

In a development environment with no active channels, you can assign the ADMIN role to an application developer. A user with the ADMIN role can:

- Access all Workspace Administration screens, except Manage Workspace and Manage Channel Configuration.
- Create and manage workspace users in the Manage User screen.
- Manage active sessions that are created for interactive applications, using the Managing Sessions screen.
- Monitor the Brand Mobiliser Processing Engine (processing engine) log using the Processing Engine Logs screen.
- Generate traffic reports for a workspace.

ADMIN users can also perform any function available to the APP_ADMIN and APP_OWNER roles.

APP_ADMIN

The APP_ADMIN role is assigned to team members of the QA team who are working in a QA environment.

Users with this role work with applications, events, and subscribers. They have full access to development functions, including create, modify, approve, simulate, and delete. They also can access to the Manage Categories screen.

Assign the APP_ADMIN role to testers, so they can import, activate, and test applications.

APP_OWNER

Typically, the APP_OWNER role is assigned to QA team members and application developers in the production environment, when necessary.

Application owners can create applications, but they cannot activate them. Access is restricted to read-only functionalities.

To allow business analysts to view traffic reports from testing, and to troubleshoot reported bugs, assign the APP_OWNER role to them.

See also

- *Adding Users* on page 7
- *Editing User Properties* on page 8
- *Deactivating Users* on page 9

Deleting Users

To delete a user, first unassign all roles and workspaces, except the default workspace, from the user.

Prerequisites

Back up the database.

Task

Note: This task can be performed only by a system administrator or a DBA.

1. In the Brand Mobiliser Web UI, log in as a user who has the ADMIN role, and who is assigned to the workspace.
2. Navigate to the Manage User page, and unassign all roles and workspaces, except the default workspace, from the user.
3. Using the database management tool:
   a) In the `M_USERS` table, find the ID of the user you want to delete (for example, ID = 100).
   b) In the `M_CLIENTS_USERS` table, delete the row where USERS_ID = 100.
   c) In the `M_USERS` table, delete the row where ID = 100.

Communication Channels

A Brand Mobiliser communication channel is the conduit for receiving inbound and delivering outbound messages.

Short Message Peer-to-Peer (SMPP) – connections are used to send and receive SMS messages.

Built-in channel types are:

- SmsOutDummy – the loopback channel, which is used for simulation tests in a development environment, and requires no configuration. When a new workspace is created, the SMS outbound channel is automatically assigned to SmsOutDummy.
- Short Message Peer-to-Peer (SMPP) – uses the SMPP protocol to deliver inbound and outbound messages to short message service centers (SMSC) and external short messaging entities.
- Java Message Service (JMS) – delivers inbound and outbound messages via the message-oriented middleware.

The platform administrator can configure SMPP (inbound and outbound) and JMS channels to have one or more connections, and set these connections to active or inactive. An active connection on an inbound channel receives incoming messages. An active connection on an outbound channel delivers outgoing messages. Channels are defined at the platform level, and are shared by all workspaces.

Configuring SMPP Inbound Channels

Incoming messages on an SMPP inbound connection can target any workspace. The destination workspace is determined by the short code of the incoming message.

1. In the Brand Mobiliser Web UI navigation bar, select **Workspace Administration**, then select **Manage Channel Configurations**.
2. On the Manage Channels screen, select the **SMPP IN** tab, and enter values for these parameters:

Parameter	Description
Name	Unique name for the channel.
URL	Host name of the short message service center (SMSC).
Port	Port number for the listener.
Username	User name for authentication.

Parameter	Description
Password	Valid password for the user name.
System type	Identifier for SMSC.
Keep Alive (ms)	Frequency for sending enquire-link requests, in milliseconds; required to keep the SMPP connection alive. SMPP protocol setting.
Active	To activate the channel, select the check box; to deactivate, unselect the check box.

Note: Adding, deleting, or modifying a channel requires that you restart all active channels, which impacts all running applications in all workspaces.

3. To restart channels, select **Channel Actions > Restart Channels**.

See also

- *Configuring SMPP Outbound Channels* on page 14

Configuring SMPP Outbound Channels

SMPP outbound connections are specific to a workspace—one connection per workspace. Brand Mobiliser makes outbound connections to short message service centers (SMSC) and SMS gateways.

1. On the Manage Channels screen, select the **SMPP OUT** tab, and enter values for these parameters:

Parameter	Description
Name	Unique name for the channel.
URL	Host name of the short message service center (SMSC).
Port	Port number to create a connection to.
Username	User name for authentication.
Password	Valid password for the user name.
System type	Identifier for the SMSC.
Dest Ton	Destination-number type.
Dest Npi	Destination numbering plan identification.
Src Ton	Source-number type.
Src Npi	Source numbering plan identification.

Parameter	Description
Delay (ms)	Message delay before sending next message, in milliseconds.
Keep Alive (ms)	Frequency for sending enquire-link requests, in milliseconds; required to keep the SMPP connection alive. SMPP protocol setting.
Permanent	Whether connections persist or a new connection is created for each message. To persist connections, select the check box; to create new connections, un-select the check box.
Active	Whether this channel is active or not. To activate, select the check box; to deactivate, unselect the check box.

Note: Adding, deleting, or modifying a channel requires that you restart all active channels, which impacts all running applications in all workspaces. In addition, when you switch a channel from "active" to "not active," the channel is detached from its workspaces during the restart process, leaving these workspaces without an outbound channel.

2. To restart channels, select **Channel Actions > Restart Channels**.

See also

- *Configuring SMPP Inbound Channels* on page 13

Configuring JMS Channels

A single JMS channel supports both inbound and outbound traffic.

The JMS queue names define whether messages on the queue are inbound or outbound. The Brand Mobiliser JMS message format is proprietary. To use this channel mechanism, consult with your SAP Support contact.

1. On the Manage Channels screen, select the **JMS Connector** tab, and enter values for these parameters:

Parameter	Description
Name	Unique name for the channel.
URL	JMS broker to connect to.
Username	User name for authentication.
Password	Valid password for the user name.
In Queue	Queue name to look for inbound messages.
Out Queue	Queue name to look for outbound messages.

Parameter	Description
Active	To activate the channel, select the check box; to deactivate, unselect the check box.

Note: Adding, deleting, or modifying a channel requires that you restart all active channels, which impacts all running applications in all workspaces. In addition, when you switch a channel from "active" to "not active," the channel is detached from its workspaces during the restart process, leaving these workspaces without an outbound channel.

2. To restart channels, select **Channel Actions > Restart Channels**.

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.

After you create a workspace, you can assign users to it. You can assign a user to more than one workspace. The default installation of the platform has a predefined workspace called `default` and a user called `admin`, who is assigned to the `default` workspace. The `admin` user has the SUPER_ADMIN role, and is the platform administrator.

Warning! Do not delete the `default` workspace or the `admin` user.

In a deployment environment, you must configure a workspace with at least one unique short or long code. Short codes are special telephone numbers, significantly shorter than full telephone numbers, which you can use to address SMS and MMS messages from some mobile phones and fixed phones, and are limited to national borders. Long codes are longer numbers that you can use for international calls. The processing engine uses unique short codes or long codes to dispatch incoming messages to a corresponding workspace. In the remainder of this topic, code refers to either a short code or a long code.

You can assign more than one code to a workspace, but you cannot use a code in multiple workspaces. If there is more than one code assigned to a workspace, the processing engine uses the code flags, `Default` and `Use for Reply`, to determine which code to assign to the **Origination MSISDN** property in responses (outbound messages). As an example, a workspace has short codes: A, B, and C. When an inbound message is sent to any of these short codes, the processing engine sets the value of the **Origination MSISDN** property in the response, based on the status of the short code's flags. Mobile operators require **Origination MSISDN** values.

Short Code	Selected Short-Code Flag	Value Assigned to Origination MSISDN in Responses	Reason for Origination MSISDN Value
A	Default	A	A is the default short code.
B	Use for Reply	B	The Use for Reply flag is selected.
C	None	A	The Use for Reply flag is not selected, so the system selects the default short code.

Each workspace can have only one outbound channel connection. Inbound channels are not workspace specific. An incoming message from any channel is evaluated and routed to its corresponding workspace, based on the destination short or long code in the message.

For best results:

- Do not assign any users to the `default` workspace. Preserve the initial setup of the workspace (assigned to the admin user). Treat the `default` workspace as a guest workspace, so when users are inadvertently assigned to it, no damage is done.
- Do not assign any short codes to the `default` workspace, because short codes cannot be reused across workspaces.
- To prevent unintended traffic flow, do not set up any channels on the `default` workspace.

Creating Workspaces

A workspace is a logical grouping of applications, users, and, other artifacts. In addition to a unique name, a workspace also has a unique short or long code.

1. To create a workspace, on the Brand Mobiliser Web UI navigation bar, select **Workspace Administration**.
2. In the Workspace and User list, select **Manage Workspaces**.
3. On the Workspaces screen, select **Add New Workspace**.
4. On the Manage Workspace screen, enter values for these parameters, and click **Save**:
   - Name – unique name of the workspace.
   - Short Name – name and short name can be the same, but they must be unique in the system.
   - Select an outbound channel from the list.
5. Select the **Shortcode** tab, and enter a short code.

   After you add a short code to a workspace, all incoming messages with a destination MSISDN equal to the short code are sent to the workspace.
6. (Optional) To determine the value of the **Origination MSISDN** property in outbound messages, set one of these flags:
   - **Default** – if this flag is set and the Use for Reply flag of the incoming-message's short code is not set, the value of **Origination MSISDN** in outbound messages is set to this short code
   - **Use for Reply** – if this flag is set for the short code to which the inbound message is sent, the value of **Origination MSISDN** in outbound messages is set to this short code.
7. Click **Add**.
   The short code is added to the workspace. To add another short code, repeat steps 5–7.

You can edit an existing workspace by selecting it from the Manage Workspace screen.

See also

- *Opening Workspaces* on page 19
- *Configuring Default Menus* on page 20
- *Default Menu* on page 19

Opening Workspaces

Workspace administrators can assign Brand Mobiliser Web UI (Brand UI) users to multiple workspaces, and users can open their workspaces individually. After logging in to the Brand UI, one of your workspaces opens. The name of the current workspace appears on the Login Status Bar.

1. To open a different workspace, on the Login Status Bar, expand the **Workspace** list, and select the workspace.
2. To confirm the change, click **OK**.

The new workspace opens, and the main window (Dashboard) appears. Each workspace has unique artifacts, such as short codes, channels, and applications. By design, you cannot see or access resources from multiple workspaces at the same time.

See also

- *Creating Workspaces* on page 18
- *Configuring Default Menus* on page 20
- *Default Menu* on page 19

Default Menu

A Brand Mobiliser default menu responds to keywords that are sent to a workspace but not assigned to an application. Each workspace must have a default menu. Typically, the workspace administrator sets up the default menu.

Responses on a default menu are in menu form. For example, in a workspace with three interactive applications, the response message for an unrecognized keyword may be:

```
Choose: 1 – for banking; 2 – for payment; 3 – for weather.
```

When you set up a default menu, you associate applications with the menu. The menu is generated automatically. When a workspace receives an unrecognized keyword, it sends an automatically generated response to the mobile consumer, using default-menu settings. Mobile consumers can respond with options in the menu index.

Functionalities available on the Setup Default Menu screen are:

- Default Menu – displays the menu that is sent in response to unrecognized keywords. The order of the menu items determines the generated menu indexes. You can change the order

using the up and down arrows to move applications. Application names are links to the corresponding application screens.

- Add Application to Default Menu – provides a list of all applications that can be added to the default menu. The list displays all interactive applications that are currently active. For information about developing applications, see the *Brand Mobiliser Developer Guide*.
- Response Messages – displays two messages: the text that is prepended to the default menu, and the message that is sent as a response when the default menu is empty. The prepended text can be as simple as "Choose," or a welcome message. When there are no applications assigned to the default menu, an alternate response is sent to mobile subscribers, for example, a keyword that is valid for one of the applications in the workspace.
- Activate Default Menu – when you create a new workspace, you must activate the default menu.

See also

- *Creating Workspaces* on page 18
- *Opening Workspaces* on page 19
- *Configuring Default Menus* on page 20

Configuring Default Menus

Set up and activate a default menu for each workspace. When a consumer selects an option in the default menu, the associated application starts.

A default menu can have a maximum of five menu items.

1. In the Brand Mobiliser Web UI navigation bar, select **Actions > Set Up Default Menu**.
2. Add an application to the default menu:
   a) Select an application from the list.

      The selected application appears as the last item in the default menu.
   b) Click **Add to Menu**.

      When there are five applications in the menu, Add to Menu is disabled.
3. (Optional) Change the order of applications in the menu:
   a) In the Default Menu list, select an application, and click the up or down arrow to change the order.
   b) To remove an application from the list, select the **X** that corresponds to the application.
4. (Optional) Edit the response message:
   a) Under Text Prepended to Menu, enter explanatory text that mobile consumers see above the list of applications in the menu.

b) Under Message when Default Menu is Empty, enter the text that mobile consumers see when there are no applications in the menu, for example, a keyword that is assigned to an application in the workspace.

c) Click **Save**.

5. Click **Activate**.

   Any subsequent changes you make to the default menu require you to reactivate the menu before the changes take effect.

Note: The default menu is designed to be active at all times. If there is an issue, you must either fix it, or remove all linked applications, so that no menu is created. As a last resort, stop the default menu by disconnecting the outbound channel from the workspace.

See also

- *Creating Workspaces* on page 18
- *Opening Workspaces* on page 19
- *Default Menu* on page 19

Deleting Workspaces

Before you delete a workspace, remove all applications running in the workspace and unassign all users from the workspace.

Prerequisites

Back up the database.

Task

Note: This task can be performed only by a system administrator or a DBA.

1. In the Brand UI, log in as a user who has the ADMIN role, and who is assigned to the workspace you want to delete.
2. Navigate to the Set Up Default Menu page.
   a) Remove all applications assigned to the default menu.
   b) Approve the default menu.
3. Go to the Assets page, and remove all applications from the workspace.
4. Navigate to the Manage User page, and unassign all users from this workspace, including the user who logged in.

   If the logged-in user is assigned only to this workspace:

   a) Assign the logged-in user to a different workspace.
   b) Unassign the logged-in user from the current workspace.

5. Using the database management tool, log in to the database, and delete the workspace data.
   a) In the `M_CLIENTS` table, find the workspace ID (for example, 200). The workspace name is in the NAME column.
   b) In the `M_CLIENT_MSISDNS` table, find the ID where CLIENTS_ID = 200. In this example, `M_CLIENT_MSISDNS`.ID = 222.
   c) In the `M_MESSAGE_LOG` table, delete all rows where CLIENTS_MSISDNS_ID = 222.
   d) In the `M_CLIENT_MSISDNS` table, delete the row where ID = 222.
   e) In the `M_SESSIONS_ACTIVE` table, delete all rows where CLIENTS_ID = 200.
   f) In the `M_SESSIONS` table, delete all rows where CLIENTS_ID = 200.
   g) In the `M_MESSAGE_RECEIVERS` table, delete all rows where CLIENTS_ID = 200.
   h) In the `M_MENU_PAGES` table, get the value of ID where CLIENTS_ID = 200. In this example, `M_MENU_PAGES`.ID = 444.
   i) In the `M_MENU_PAGES_LANGS` table, delete all rows, where ID = 444.
   j) In the `M_MENU_PAGES` table, delete all rows where CLIENTS_ID = 200.
   k) In the `M_CLIENTS` table, delete the row, where ID = 200.

Categories

You can assign categories to applications and events. Categories are primarily used for filtering in the Brand Mobiliser Web UI.

You can create new categories, and edit and delete existing categories on the Manage Category screen.

In the Brand Mobiliser Web UI navigation bar, select **Actions > Manage Categories**.

You cannot delete a category if it is assigned to an application or event.

Subscribers

The data model for Brand Mobiliser mobile-subscribers storage is called subscribers. A group of subscribers and their attributes is called a set. The Subscribers screen lists all subscriber sets in the workspace.

Subscribers storage is available to all Brand Mobiliser applications. You can use subscribers storage as the system of record for small-scale implementations. Ideally, use subscribers storage as temporary storage, for staging, or as in-transit storage, pending batch transfer to a system of record. The database schema used by subscribers storage is not fully optimized for large-scale or more domain-specific purposes, such as for customer relationship management (CRM), or enterprise resource planning (ERP).

A subscribers set name is not required to be unique, but to avoid confusion, SAP recommends that it is. A set is made up of a list of rows with 21 fields. The **KEY** field is the unique key, and the remaining 20 fields are free form. The first free-form field, **ATTRIB1**, can store up to 1000 characters; the remaining free-form fields can store up to 320 characters each.

The set model is designed to store lists of subscribers. In a subscriber list, the **KEY** field stores a mobile subscriber's unique MSISDN. You can use the remaining free-form fields to store additional attributes related to the subscriber. You can use these attributes in different ways; for example, to dynamically "mail-merge" into the SMS message template, to send customized SMS messages based on attributes, or to filter the number of SMS messages sent, based on specific attributes. Since SMS messages are limited to about 160 characters (varies based on the character-encoding type), Brand Mobiliser automatically breaks a long message into smaller pieces, and sends each piece as a separate SMS message.

You can use the Brand Mobiliser Web UI to generate a subscriber-set report, by exporting the set to a comma-separated value (CSV) file. You can also use a CSV file to transfer a set to a permanent system of record. CSV files can be read by spreadsheet programs, uploaded to databases, imported into reporting applications, and processed by custom-built applications.

If you need an automated process to transfer a set, you can create a Brand Mobiliser application using custom plug-in states, to send or upload the set in batch mode to the target system. To schedule a batch process, use the Brand Mobiliser event system. You can populate a set by uploading a CSV file on the Upload Subscriber screen, or you can create an empty set on the New Subscriber Set screen, and populate it automatically using Brand Mobiliser applications. For example, you can develop Brand Mobiliser applications to pull subscribers from:

- A CRM system
- Twitter followers
- Facebook friends
- LinkedIn connections

You can also add mobile subscribers who respond to a short code to opt in. You can use subscriber lists to collect customer data for real-time analytics and reporting.

Create and populate subscriber sets by:

- Creating an empty set – then populate using either the Upload Merge or the Add Subscriber application state.
- Uploading a subscriber file – either a CSV file or a compressed CSV file.

See also

- *Generating Subscriber Reports* on page 30

Creating Empty Subscriber Sets

A subscriber set is a group of subscribers. The Subscribers screen lists all the subscriber sets in the workspace. A set has a unique ID and a name.

Although a set name is not required to be unique, SAP recommends that you use unique names to distinguish each set from others in the system.

1. In the Brand Mobiliser Web UI Navigation bar, select **Subscribers**.
2. Select **Create Empty Set**.
3. On the New Subscriber Set window, select the **Set Details** tab, and enter:
   - Set Name – a unique name for the subscriber set.
   - Attributes Metadata – (optional) a comma-separated list of attribute names to assign to the subscriber set free-form fields; maximum number of fields is 20.
4. Click **Save**.

Uploading Subscriber Sets

You can upload subscriber sets from both comma-separated value (CSV) files and compressed CSV files. CSV files contain comma-separated attribute names on the first row, and comma-separated values in remaining rows. Each set has a unique ID and a name.

Uploading compressed files is the preferred method, especially for files containing a large number of subscribers. Compression can significantly reduce the upload streaming time. Compressed CSV files have a `.zip` extension.

Brand Mobiliser version 1.3 does not have virus-scanning capability. All uploaded files are checked to verify that they conform to specific formats; otherwise, they are not processed.

Tip: Scan for viruses before uploading files.

1. In the Brand UI Navigation bar, select **Subscribers**.

2. Select **Upload Subscriber**.
3. Enter the set name.
4. Click **Browse**, select the file, and click **Open**.
5. Click **Upload**.
6. Wait until streaming is complete and a success message appears beneath the Upload button, then click **Subscribers**.

Uploading a file is a two-step process: streaming the file to the server, then processing and uploading the file contents to the database. Depending on the file size and system utilizations, the latter may take several minutes. However, once the file is stored on the server, the subscriber set is created, enabling users to track the uploading process from the Subscribers screen. The process states change in this order: Not Started, Load In Progress, and Load Success. During the Load In Progress state, you can see the number of subscribers increase.

Reports

You can access the Reports screen from the Brand Mobiliser Web UI navigation bar.

In the Reports screen, you can export data to comma-separated value (CSV) files, which can be imported into more sophisticated reporting tools or applications. You can also import CSV files into permanent systems of record. Currently, Brand Mobiliser cannot display reports graphically.

Generating Traffic Reports

The Brand Mobiliser Traffic Reports screen provides simple search and filter tools to extract reports of incoming and outgoing messages, as well as acknowledgements from SMS providers.

The Traffic Reports screen is a tool for filtering messages, and displays a preview of up to 2000 results. You can export traffic reports to comma-separated value (CSV) files, in which case all rows are exported. CSV files can be read or imported by analysis and reporting tools.

1. In the Brand UI navigation bar, select **Reports**.
2. On the Standard Reports screen, select **Traffic Report**.
3. Select the sender in the list, or select **Advanced** to narrow results:
   - Start and End Dates – narrows results to the dates messages were sent.
   - Application Name – filters messages based on the interactive or event application name.
   - Message Direction – filters incoming and outgoing messages, based on their direction, in, out, or in-and-out.
   - Receiver – returns messages with a specific customer MSISDN. This is helpful for customers who use interactive applications.
4. Click **Search**.
   You see a maximum of 2000 rows.
5. Select **Export CSV**.

   This link appears only when there are results to show.
6. Select **Save File**, and click **OK**.

See also

- *Monitoring Sessions* on page 37
- *Processing Engine Performance* on page 37

Generating Subscriber Reports

You can export Brand Mobiliser subscriber sets to comma-separated value (CSV) files. In the Subscribers screen, you can preview and export subscriber sets. You can export all rows in a set; the maximum number of rows you can preview is 2000.

Exporting lets you create subscriber sets by merging multiple files, and save the combined content. A subscriber set may have been created as an empty set, and later populated by applications, using options such as opt-in, subscribe, or log for reporting. Exporting lets you transfer data to the system of record, for reporting. You can also develop an automated system to perform the transfer, using applications and custom states.

1. In the Brand UI navigation bar, select **Reports**.
2. On the Standard Reports screen, select **Subscriber Report**.
3. Click the set you want to export.
   You see attributes for each subscriber in the set.
4. Click **Export CSV**.
5. Select **Save File**, and click **OK**.

See also

- *Subscribers* on page 25

Maintenance and Tuning

You can monitor, maintain, and tune Brand Mobiliser components. The frequency of required maintenance frequency depends on traffic volume (number of messages).

System Configuration Files

Configure system components in Brand Mobiliser configuration files.

Brand Mobiliser Configuration Files

Brand Mobiliser configuration files are located in the *BRAND_HOME*/`conf` directory. `config.properties` and `system.properties` are required to start the server:

- `config.properties` contains Advanced Interactive Message Server (AIMS) configurations that are based on the Apache Felix implementation. You need not change most of these settings, as they pertain to the Brand Mobiliser platform. You may need to make changes if you apply a patch; follow the step-by-step instructions provided with the patch.
- `system.properties` contains subsystem configurations, such as logging, the Jetty HTTP server, and encryption settings. If you plan to encrypt configuration property values, enable encrypting in `system.properties`.

Brand Mobiliser Web UI

The user interface for Brand Mobiliser is configured in the `service.brand_webapp.properties` file.

AIMS System Web Console

During development, use the AIMS System Web console to inspect the OSGi container, deployed bundles, and register configurations. The Web console does not meet production standards, so to prevent unintended deployment to production, it is by default, disabled.

Jetty Servlet Container

The Jetty servlet container hosts Web applications, and is configured in the `org.ops4j.pax.web.properties` file. As described on the Apache Jakarta Web site, AJP13 is a connector component that communicates with a Web connector via the AJP protocol. AJP13 may be useful if you want to invisibly integrate Tomcat 4 (or Jetty) into an Apache installation, and you want Apache to handle the static content contained in the Web application, or to use Apache SSL processing. In many application environments, using an AJP13 component results in better overall performance than running your applications under Tomcat alone using the HTTP/1.1 connector. For details about the `jetty.xml` file, see *http://www.eclipse.org/jetty/documentation/current/*.

Log4j
Logging is controlled by the `org.ops4j.pax.logging.properties` file; the properties are dynamic and use the log4j configuration format. See *http://logging.apache.org/log4j/1.2/manual.html* .

Editing Configuration Files

You can copy configuration files to a location where Brand Mobiliser reloads them automatically. You can also track configuration-file changes.

1. To make changes to a system configuration file, and have those changes take effect without restarting Brand Mobiliser:
   a) Change the configuration file in the `conf/cfgbackup` folder.
   b) Copy the modified file to the `conf/cfgload` folder.

   Brand Mobiliser loads the file automatically, and moves it back to the `conf/cfgbackup` folder. By default, changes are not logged.
2. To track configuration-file changes:
   a) Edit the `conf/cfgbackup/org.ops4j.pax.logging.properties` file.
   b) Change the value of **log4j.logger.com.sybase365.arf.container.system** from WARN to INFO:

```
log4j.logger.com.sybase365.arf.container.system=INFO, main,
osgi:VmLogAppender
log4j.additivity.com.sybase365.arf.container.system=false
```

When the property file is reloaded, the log is written to `log/felix.log`. The following example displays log entries that resulted from reloading the `service.webui.security.properties` file.

```
16:15:53,507 | INFO | Thread-1 | cm-loader | ldap.port:389
16:15:53,513 | INFO | Thread-1 | cm-loader |
ldap.userpath:uid={uid},ou=people,o=sybase365
16:15:53,513 | INFO | Thread-1 | cm-loader |
ldap.security.authentication:SIMPLE
16:15:53,513 | INFO | Thread-1 | cm-loader | ldap.host:localhost
16:15:53,513 | INFO | Thread-1 | cm-loader |
service.pid:service.webui.security
16:15:53,513 | INFO | Thread-1 | cm-loader |
authentication.bean:AuthenticationManager
16:15:53,513 | INFO | Thread-1 | cm-loader |
arf.filename:service.webui.security.properties
```

See also

- *Monitoring Sessions* on page 37
- *Default Ports* on page 34
- *Processing Engine Performance* on page 37

Log Files

If you encounter issues running Brand Mobiliser, check the log files in the *BRAND_HOME*/`logs` directory. Brand Mobiliser creates log groups for its various subsystems.

Log File	Description
`brand.log`	Primary log file for Brand Mobiliser applications
`felix.log`	Server kernel and miscellaneous log for all nonapplication issues
`pax-web.log`	Pax-Web and Jetty servlet container log
`persist.log`	Persistence log
`spring.log`	Dependency injection (DI) application framework used by Brand Mobiliser applications

Database Table Maintenance

Database tables store logins, and persist configurations, transactions, and session data. Logging tables require regular archiving when traffic volume is high.

The information presented here is intended to help the DBA incorporate application tables into the overall database maintenance plan. As always, regular backups are essential for recovery in the event of unexpected failure.

Note: The DBA should review these guidelines, and define archiving and purging schedules based on company policy.

Table 1. Logging Tables

Table Name	Description	Archive and Purge
`M_CORE_STATUS_LOG`	Engine logs	Purge based on the TIMESTAMP2 column.
`M_LOGIN_HISTORY`	User logins	Purge based on the TIMESTAMP2 column.
`M_MESSAGE_LOGS`	Size increases with number of subscribers and traffic	Purge based on the TIMESTAMP2 column.

Table Name	Description	Archive and Purge
M_MESSAGE_RECEIVERS	Size increases with number of subscribers and traffic	Purge based on MARKED_DELETED = 1 AND if there are no references in the M_MESSAGE_LOG table.
M_MESSAGE_ATTRIBUTES	Number of rows increase with traffic and session data	Purge before purging the M_SESSIONS table, and based on the SESSIONS_ID column.
M_SESSIONS	Number of rows increase with traffic and session data	Purge based on the CLOSED_DATE column.
M_SMAPP_TRANSITION_LOG	Number of rows increase with traffic and session data	Purge based on the TIMESTAMP2 column.

Default Ports

The Brand Mobiliser installation sets up default ports. Consult your IT system architect, and adjust values if conflicts occur, or disable if not needed.

Port Value	Port Key
5366	JMX remote connection port enables monitoring and management from a remote system. In the /bin directory, set the RMI_PORT in the start-up script, run.sh or run.bat. See Monitoring and Management Using JMX Technology at: *http://docs.oracle.com/javase/6/docs/technotes/guides/management/agent.html*.
5365	Telnet port from localhost enables connecting to OSGi shell console using Telnet. In the /bin directory, edit the start-up script, run.sh or run.bat, and set the value of TELNET_PORT.
8080	Set the HTTP port for Brand Mobiliser Web UI in the conf/org.ops4j.pax.web.properties file.

See also

- *Processing Engine Performance* on page 37
- *Editing Configuration Files* on page 32
- *Monitoring Sessions* on page 37

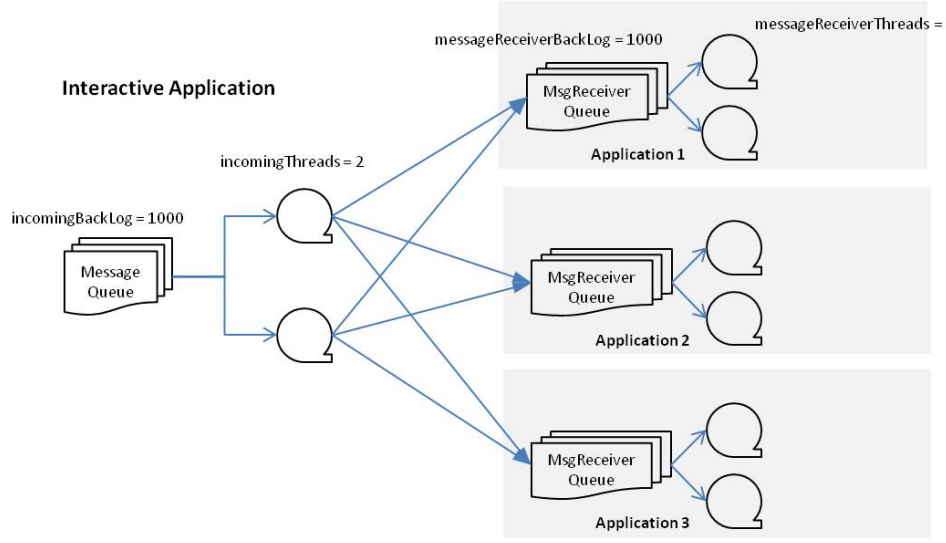
Brand Mobiliser Processing Engine

Understanding the internal mechanism and configuration parameters of Brand Mobiliser may help you tune the Brand Mobiliser Processing Engine (processing engine) for optimal performance.

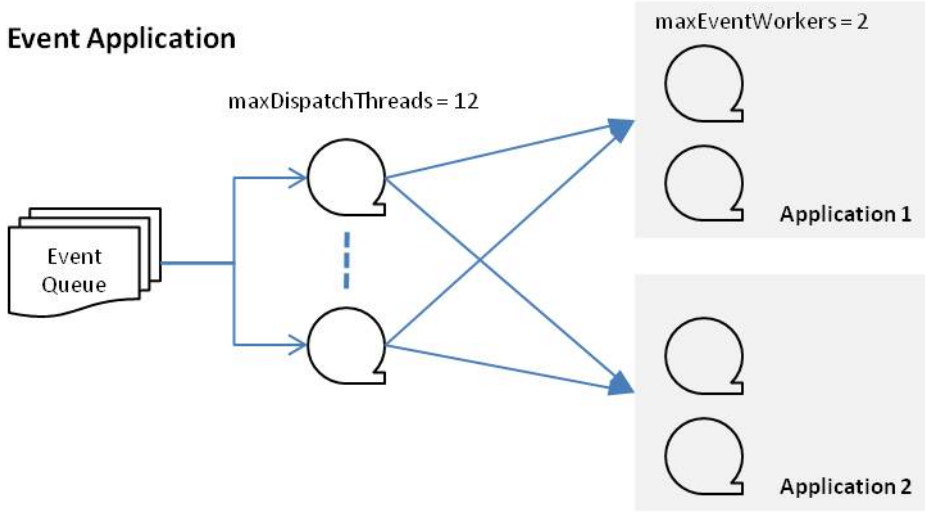
The processing engine powers mobile commerce solutions, and lets you scale your services. The processing engine is designed to serve the continued growth of mobile traffic, which demands instant interactions with mobile applications.

The processing engine processes interactive applications somewhat differently than it processes event applications, as shown below.

Interactive Application Processing



Event Application Processing



Processing Engine Configuration File

In the `/conf/cfgbackup/service.coreprocessing.properties` configuration file, you can tune the processing engine and queues for increased throughput, based on specific hardware configurations and channel throughput.

```
# Configuration for Incoming Queue – Interactive Application
# Number of threads to handle the dispatch of the incoming queue.
# Note that this should not exceed the messageReceiverThreads
incomingThreads=2

# Configuration for Incoming Queue – Interactive Application
# Maximum number of messages allowed in the incoming queue. This is a
global queue
# that handles all incoming messages before dispatching to a specific
message
# receiver.
incomingBackLog=1000

# Configuration for Message Receiver – Interactive Application
# A message receiver is created for each active Brand Mobiliser
application
# Configure the number of threads to handle the message queue for
each message
# receiver.
messageReceiverThreads=2

# Configuration for Message Receiver – Interactive Application
# Maximum number of messages allowed in each message receiver
queue
# There is one queue for each message receiver.
messageReceiverBackLog=500
```

```
# Configuration for Event Application, used in Campaign
# Maximum number of dispatching thread to process the event queue
maxDispatchThreads=12

# Configuration for Event Application, used in Campaign
# Number of Processor per event application
maxEventWorkers=1

# Batch size in processing the subscriber file
batchLoadSize=100
```

Monitoring Sessions

The processing engine creates a session for each incoming message. On the Manage Sessions screen, the workspace administrator can monitor active sessions and terminate them if necessary.

1. To display the currently active sessions, click **Refresh**.
2. To end an active session, select the session, and click **Close Session**. Active sessions are automatically terminated when the application ends, or if the session times out.

Warning! The list of active sessions includes all sessions, including those for other workspaces. Close sessions carefully.

See also

- *Generating Traffic Reports* on page 29
- *Processing Engine Performance* on page 37
- *Editing Configuration Files* on page 32
- *Default Ports* on page 34

Viewing Processing Engine Logs

The processing engine logs both start-up and shutdown messages.

1. On the Brand Mobiliser Web UI navigation bar, select **Workspace Administration**.
2. Select **Processing Engine Logs**.

Processing Engine Performance

Depending on the hardware configuration and the host server, you may be able to tune the processing engine to increase throughput if necessary.

The default performance configuration, which is defined in the `service.coreprocessing.properties` file, works for typical scenarios.

Note: Always run performance tests on a new configuration before deploying it to the production system. Changes to the `service.coreprocessing.properties` file do not take effect until you restart the Brand Mobiliser server.

Performance testing has been conducted using this system configuration:

- Hardware – HP DL 360 G6; 1U standalone; 2x Intel X5450; 8x 2GB (16GB).
- Server configurations – one dedicated server for the database and another for Brand Mobiliser.

Software Configuration for Interactive Application Performance Test

Processing Engine	Datasource
messageReceiverThreads=10 messageReceiverBackLog=50000 incomingThreads=10 incomingBackLog=50000	maxIdle=50 (50 maximum performance) maxActive=25 (50 maximum performance)

Results for Interactive Application Performance Test

Load	Result
10,000 messages	110 messages/second

Software Configuration for Event Application Performance Test

Processing Engine
maxDispatchThreads=12 maxEventWorkers=4

Results for Event Application Performance Test

Messages	Rate
Up to 88	88 messages/second
Up to 3,520	93 messages/second
Up to 52,695	92 messages/second
Up to 174,668	94 messages/second
Up to 3,576,594	82 messages/second
Up to 4,999,899	97 messages/second

See also

- *Generating Traffic Reports* on page 29
- *Monitoring Sessions* on page 37

- *Default Ports* on page 34
- *Editing Configuration Files* on page 32

Index

A

ADMIN role 9
admin user 7
administrator types 1
AIMS System Web console
    configuring 31
APP_ADMIN role 9
APP_OWNER role 9
assigning
    roles to users 7
    workspaces to users 7

B

Brand Mobiliser Web UI
    configuring 31
    securing 5
brand.log file 33

C

categories 23
channels
    communication 13
    JMS, configuring 15
    SMPP inbound, configuring 13
    SMPP outbound, configuring 14
communication channels 13
config.properties file 31
configuration files 31
    editing 32
    tracking changes in 32
configuring
    AIMS System Web console 31
    Brand Mobiliser Web UI 31
    default menus 20
    Jetty servlet container 31
    JMS channels 15
    log4j 31
    ports 34
    SMPP inbound channels 13
    SMPP outbound channels 14
creating
    categories 23
    empty subscriber sets 26
    users 7
    workspaces 18

D

databases
    subscribers 25
    table maintenance 33
deactivating users 9
default menus
    configuring 20
    defined 19
deleting
    categories 23
    users 11
    workspaces 21

E

editing
    categories 23
    configuration files 32
    user properties 8
    workspaces 18
enabling
    encryption 3
    SSL 4
encrypt.sh encryption tool 4
encrypting property values 4
encryption, enabling 3

F

features, security 3
felix.log file 33
files
    logging 33

J

Jetty for SSL, configuring 4
Jetty servlet container
    configuring 31
JMS channels, configuring 15

L

log4j 31
logging 33
    configuring log4j 31
    database tables 33
    processing engine 37

M

maintenance
    and tuning 31
    database tables 33
monitoring sessions 37

O

opening a workspace 19
org.ops4j.pax.logging.properties file 31
org.ops4j.pax.web.properties file 31

P

passwords
    encrypting 4
    initial 7
pax-web.log file 33
performance 37
persist.log file 33
platform administrator 7
platform administrators 1
ports 34
processing engine 35
    logs, viewing 37
    performance 37
    sessions, monitoring 37
processing log 37
property values, encrypting 4

R

reports 29
    subscribers, generating 30
    traffic, generating 29
restarting channels 14
roles
    assigning to users 7
    user 9

S

securing Brand UI 5
security
    enabling encryption 3
    enabling SSL 4
    encrypting properties 4
    features 3
service.brand_webapp.properties file 31
sessions, monitoring 37
sets, subscriber 25
SMPP channels
    inbound, configuring 13
    outbound, configuring 14
spring.log file 33
SSL, enabling 4
subscriber reports 30
subscriber sets
    empty, creating 26
    uploading 26
subscribers 25
SUPER_ADMIN role 9
system administration 34
system administrators 1
system.properties file 31

T

tracking configuration-file changes 32
traffic reports, generating 29
tuning and maintenance 31

U

uploading
    subscriber sets 26
user roles 9
users 7
    adding 7
    deactivating 9
    deleting 11
    editing properties 8

W

workspace administrators 1

workspaces
creating 18
default menus 19
defined 17
deleting 21
opening 19