ABC Company Mobile Message Server Administration 2

SMMS Architecture

This section of the SMMS Administrator Guide provides an overview of how SMMS functions and how to configure it. Use this section to learn about:

Client/Server Architecture

SMMS is a client/server system that allows the web-server based client activity to be carried out on a web-server machine and the underlying server activity to be carried out on a different machine. SMMS uses the Sun Microsystems Remote Procedure Call (RPC) to communicate between the client and server. All SMMS installations require an RPC system to be in place. Under UNIX environments, this is generally a service called `rpcbind` or `rpcd`. On Windows systems, this is a pair of services: the Remote Procedure Call Service and Remote Procedure Call Locator.

The SMMS client and server may be run on different physical machines. In this case, the SMMS client must be configured to know what machine on which the SMMS server is running.

In order to configure an SMMS client to connect to an SMMS server on a different machine, see the *SMMS Installation Guide*.

The SMMS server can run on one machine, or it can be configured to use multiple machines. In high-availability or high-load environments, the SMMS server will always be running on more than one machine.

Configuration of this type of installation is covered in the server configuration section below.

SMMS Client Functionality

The SMMS client is a web application that runs either as a cgi-bin executable or a module to a specific web server, for example an Apache server module, an NSAPI server module for UNIX machines, and an ISAPI server module for NT machines. The simplest and most common SMMS installations use the cgi-bin, but high-load installations should use one of the server modules for improved performance.

The SMMS client is responsible for handling interactions between the user's browser and the SMMS server. This includes reading form data or other request methods from a client request, turning this information into a request to the SMMS server, and formatting of the request for the user's browser.

The client has two types of configuration: a catalog file and a set of HTML template files. The catalog file is a standard method for customizing a binary at run-time, and includes general interface configuration information such as the directories where templates and images can be found for the SMMS interface. The catalog file also contains localization information for some of the underlying interface configuration. The HTML template files contain the layout and flow information for the interface itself. For the most part, localization takes place by editing the template files.

If the browser being used does not handle tables well, it could affect the load time for the SMMS pages. In this case, modify the template files to display in something other than tables.

For details about customizing these templates, see the *Template Modification Guide*.

When a user has successfully logged in to the SMMS server, the client records the user name, password, SMMS server name, and SMMS child server number in a cookie, encrypted using 3DES, and passed back to the user's browser. For each subsequent action, this cookie is read to determine what SMMS child server the user is connected to, and to reauthenticate with the SMMS server if necessary (see SMMS Server Functionality, below, for information about SMMS Child servers).

Important: When a user completes the session, it is crucial that they use the Logout link provided in the SMMS interface. This ensures that the authentication information stored in the cookie is removed, and the SMMS session is removed from the browsers cache.

SMMS Server Functionality

The SMMS server is a UNIX daemon process or an NT service that is responsible for two general areas of functionality: load balancing and user activity.

Load balancing is carried out either within one machine by the use of multiple server instances or across multiple machines, depending on the configuration of the server.

The primary task of the SMMS server is supporting user activity. This includes connecting to and authentication with the mail servers, preserving the state of a users session, and carrying out all user-requested activity.

The SMMS server is configured using a text configuration file, named `smms.conf`. The configuration file has areas for general configuration as well as load balancing information and connection information for each of the mail and directory servers to be used.

When the SMMS server is started, it reads the configuration file to determine the number of servers that should be available to service user requests. It then starts these servers (known as child servers) as well as the server responsible for load balancing between child servers and remote (master) SMMS servers (called the Switchboard server for multiple server installations). The original

server is known as the monitor server; it is responsible for restarting any of the master or child servers that become inactive or disconnected during the course of operations.

Because of these different functions, when starting a SMMS server you will see two more SMMS server processes than the number of child servers specified in the configuration file.

SMMS User Accounts

SMMS does not have any control over accounts that are allowed to use the system. It relies on the mail servers that have been configured to provide authentication for users. Once a user has been authenticated with the mail server, they are allowed to use all SMMS functionality.

When a user performs any personalization activity, such as changing preferences or adding addressbook entries, a preference directory is created for that user. All changes are stored in this directory and are available any time the user logs back into SMMS.

SMMS and Cookies

SMMS 1.0 includes a method for encoding user information in cookies stored at the browser. This works using the following:

- When user and session authentication information is stored in a cookie, it is encrypted with Triple-DES (3DES);
- The IP address of the browser is included in this information; it is tested each time the cookie is received by the client. If the current IP address of the request does not match the original stored in the cookie, a security violation is assumed and the user if forcibly logged out and invited to re-login.

Because of this, laptop users who move from one location to another without logging off must re-authenticate. Users logging in from internet cafes or university common rooms must log out in order to sever the connection.

Catalog Files

The SMMS client uses a binary format catalog file to store information that is required for all invocations. Catalog files are formatted using the UNIX `gencat` command, which converts a text format file into a binary format for faster lookup. Use any simple text editor to create or edit the catalog file.

The catalog source file is formatted as a list of sets, each of which contains one or more entries. For instance, a catalog with two entries in Set 1 and one entry in Set 3 might look like:

```
$  sample catalog file- catalog.src
$set 1
$ default LDAP search and scope
252 objectClass=organizationalPerson
253 one
$set 3
$ image directory
3 /smms/images
```

Once you have made your changes, use the `gencat` utility to convert the catalog source to the binary format. Differing operating systems' native `gencat` catalog compilers have varying requirements for catalog file formatting. The `cleancat` utility takes the SMMS catalog file as input, and generates a "clean" catalog format which, if used with the `-s` switch, breaks no known gencat formatting rules. For example:

```
cleancat -s smms.cat.dirty smms.cat.clean
```

The gencat utility is invoked with the name of the binary file to be created followed by the name of the source file to use. For instance:

```
gencat smms.cat smms.cat.clean
```

The `smms.cat` file must be placed in the same directory where the SMMS CGI-BIN executable is located, or in the server root of the web server if a module is being used.

"Complete Catalog Entry List" on page 40 contains a list of all sets, including the message numbers and the default messages associated with those numbers.

The following catalog file entries are the most commonly used to configure SMMS.

Interface options

- `Set 1, entry 300- List of character sets available to the user.`

  Character sets are listed separated by commas. If an interface should support English and Japanese text, this entry would be set with a line such as "300 iso-8059-1,shift_jis". When a user selects a character set from the list, this choice gets saved with their preferences on the SMMS server. If a user has a character set selected, the SMMS client will attempt to load a catalog file called `SMMS-[charset].cat`. In the case of shift_jis, this file would be `SMMS-shift_jis.cat`. This allows the SMMS administrator to customize all of the messages, images, and templates for each supported character set.

- `Set 1, entry 252- default LDAP search`
  `Set 1, entry 253- default LDAP search scope`

  The two entries above configure the LDAP search that is performed when the user first loads the "Directory" screen. The scope is set to either "sub" or "one" to indicate whether the scope of the search includes sub searches of the base hierarchy, or only the base level.

- `Set 3, entry 3- image directory`
  `Set 3, entry 75- template directory`

  The two entries above allow the administrator to specify a different directory for loading images or templates. The default image directory is "/.smms" off of the document root of the web server. The default template directory is "templates" off of the directory where the SMMS client is running.

Functionality options

- `Set 3, entry 63- Enable postponing of messages.`

  If this option is set to No, users who are connected to an IMAP server will not have the option of postponing (saving as draft) messages.

- `Set 3, entry 58- Enable user-selected number of messages to load at once.`

  This value is set to a number that specifies the maximum number of messages the user is allowed to load at once. When this catalog entry is present, the default behavior of presenting the user with a link is replaced with an entry box and a button that the user can click when they have entered the number of messages they wish to load in the entry box.

- `Set 3, entry 59- Disable "Dangerous" Javascript`

  If this entry is set to Yes this entry disables printing of Javascript calls that are considered dangerous when they occur in an email message. These calls include **`form.submit, document.load, document.replace,`** and **`window.open`**.

- `Set 3, entry 73- Suppress printing of port number along with SMMS client URL.`

  In certain cases the site configuration uses a proxy server to connect to the SMMS client on a port other than the default (80). This catalog entry tells the SMMS client to act as if it is running on the default port. If this entry is not in place and the web server under which the SMMS client is running is listening on port 88, the template function `print_script_url` prints `http://webserver.example.com:88`. If this entry is in place, the function prints `http://webserver.example.com`.

URL options

- `Set 3, entry 64- page to send user to for Login page`
  `Set 3, entry 71- page to send user to on Login error`
  `Set 3, entry 50- page to send user to on Logout.`

  The default behavior of SMMS is to use the template `Login.thtml` during any of the above requests. Under certain conditions, a site administrator may wish to send users to another page on Logout, or to keep the Login and Login Failure pages under their complete control.

Language Customization

SMMS allows the administrator to create catalog files for character sets for languages that use characters other than the default. This is done in catalog file set 1 entry 300. For example, if users needed to view messages in Japanese characters, the administrator would add the following character set label to this catalog file.

```
$set1
300 iso8859_1,Shift_JIS
```

Adding this label will provide the users with a drop down list of languages to choose from. This list is found in the Mailbox Options Preferences Screen.

Templates

SMMS uses HTML template files to control the interface that is presented to the user. A default set of templates is shipped with the SMMS documentation.

You can modify existing templates and present the users with your own corporate branding. See the *Template Modification Guide* for complete details about customizing your templates.

SMMS Device Lookup Table

A device lookup table allows the SMMS client to associate a user agent with a content-type and a set of templates. It also determines whether or not the device has support for HTTP cookies. For SMMS, this table (by default `smms_devices`) is a plain text file located in the same directory as the default catalog file.

If no match is found or no table exists, the default values are used.

Separate fields with a whitespace with entries separated by a newline or carriage return. If the field text contains a space, encase the text in quotation marks.

If a user-agent matches more than one regex, the first matching entry in the list is used.

SMMS device lookup table fields are shown in Table 2-1.

Table 2-1 Device lookup table fields

Field	Description	Default
User Agent Regex	A regular expression that SMMS uses to match the agent's HTTP_USER_AGENT string.	
Content-Type	The content type that this device expects for text; for example, text/html, text/vnd.wap.wml, or text/x-hdml.	text/html
Template Extension	The extension that the device type templates must have. Templates for all devices are stored in the same directory, so it is important that all devices which have their own templates must have unique extensions for them. The leading dot (.) is optional.	.thtml
Cookie Support	(optional) Yes/Y if the device supports cookies, No/N if not.	Yes
Device UID	(optional) Some devices without cookie support post a UID each request. The device UID is the name of that ID. This field should only be used if cookie support is set to no.	