

SA Server

Sending OTPs by SMS User Guide

All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© Copyright 2008 Gemalto N.V. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

GEMALTO, B.P. 100, 13881 GEMENOS CEDEX, FRANCE.

Tel: +33 (0)4.42.36.50.00 Fax: +33 (0)4.42.36.50.90

Printed in France.

Document Reference: DOC116968A

May 28, 2008

Preface		v
	Who Should Read This Book	v
	For More Information	v
	Conventions	vi
	Contact Our Hotline	vi
Chapter 1	Sending OTPs by SMS	1
	Overview	1
	From the User's Point of View	1
	How to Implement this Feature	1
	Managing SMS Profiles	2
	Viewing All SMS Profiles	2
	Adding an SMS Profile	4
	Add an SMS Profile	6
	Creating the OATH Policy	6
	SMS Devices	6
	Virtual Devices	7
	Checking the User Details	8
	Checking the Role	9
	Modifying the SMS Message	10

List of Figures

Figure 1 - Manage SMS Profiles Window	2
Figure 2 - View All SMS Profiles	3
Figure 3 - View SMS Profile	3
Figure 4 - Add An SMS Profile	4
Figure 5 - Add An HTTP Type SMS Profile	5
Figure 6 - Delete SMS Profiles	6
Figure 7 - Create OATH Policy - SMS Devices	7
Figure 8 - Create OATH Policy - Virtual Devices	7
Figure 9 - View User Window	8
Figure 10 - View Role Window	9
Figure 11 - The "Other Settings" Window	10

The Gemalto two-factor authentication solution provides strong authentication based on smart cards for the enterprise, banking, and internet service provider (ISP) markets.

This solution enables organizations to deploy a strong authentication solution for their end users, whether local or remote. The system can service a broad range of deployments, from small corporations with less than 100 users to ISPs with potentially millions of users.

Who Should Read This Book

This guide is intended for system administrators and integrators responsible for configuring and managing the SA Server and related third-party products. In particular it describes how to configure the system to send virtual one-time passwords (OTPs) to customers as SMS text messages.

Administrators should be familiar with:

- The SA Server system architecture, as explained in this guide.
- Administrative tasks on the selected platform.

For More Information

For a complete list of the documentation for the Gemalto Strong Authentication (SA) Server, refer to the release notes (README.txt) on the Gemalto SA Server CD

For more information about other supported components, see the manufacturer's documentation for those products.

Conventions

The following conventions are used in this document:

Numeric values

By default, numeric values are expressed in decimal notation.

- Hexadecimal numbers are followed by the 'h' character. For example, the decimal value 13 is expressed in hexadecimal as **0Dh**.

In this manual, the following *highlighting styles* are used:

- **Bold** — In instructions, commands, file names, folder names, key names, icons, menus, menu items, field names, buttons, check boxes, tabs, registry keys and values.
- *Italic* — Variables that you must replace with a value, book titles, new or emphasized terms.

In this manual, *hyperlinks* are marked as described below:

- Internal Links — Displayed in quotation marks. When viewing this book online, click an internal link to jump to a different section of the book.
- [External Links](#) — Displayed in blue, underlined text. When viewing this book online, click an external link to launch your default browser (or email program) to navigate to that Web address or compose an email.

In this manual, *notes* and *cautions* are marked like this:

Note: Information that further explains a concept or instruction, tips, and tricks.

Caution: Information that alerts you to potentially severe problems that might result in loss of data or system failure.

Contact Our Hotline

If you do not find the information you need in this manual, or if you find errors, contact the Gemalto hotline at <http://support.gemalto.com/>.

Please note the document reference number, your job function, and the name of your company. (You will find the document reference number at the bottom of the legal notice on the inside front cover.)

Sending OTPs by SMS

Overview

You can enable users to receive OTPs by SMS on their mobile phones. There are two main scenarios:

- The user has an **SMS device** and SMS is the normal way of sending OTPs to the user.
- The user is issued a **virtual device** because he or she has lost their device and SMS is chosen as the way of communicating the OTPs to the user.

From the User's Point of View

These are the steps the user takes to receive OTPs by SMS:

- 1 The user logs on to the web portal of the company or bank or Internet Service Provider and in the Login page clicks **Request OTP by SMS** (as can be demonstrated in SA Server's User Portal).
- 2 The user enters his or her user ID and password and makes sure that his or her mobile phone is switched on.
- 3 The user clicks **Submit** to generate the OTP request, and shortly afterwards receives the OTP as an SMS.

How to Implement this Feature

To implement this feature in your SA Server, you will need to follow these steps:

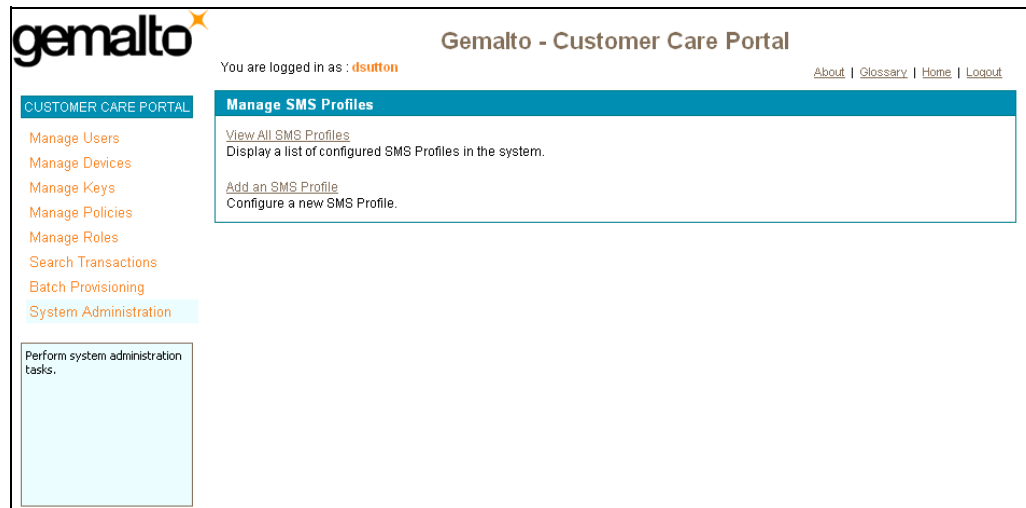
- 1 Create an SMS profile as described in "Adding an SMS Profile" on page 4. The SMS Profile is where you define the parameters relating to the SMS environment.
- 2 Create an OATH SMS policy for your devices. Please refer to "Creating the OATH Policy" on page 6.
- 3 Check the user details for each user who is to receive OTPs by SMS. Make sure each user record has a valid value in the field **Mobile Phone #**. Refer to "Checking the User Details" on page 8.
- 4 Make sure that the role assigned to the user has the privilege **Generate SMS OTP** checked. Refer to "Checking the Role" on page 9.

Managing SMS Profiles

In order to send OTPs to users via an SMS, you will need to configure an SMS profile for your system. This profile describes the SMS environment. You can in fact have as many SMS profiles as you like, but only one can be active at any time.

To access this section, click **Manage SMS Profiles** in the **System Administration** menu. This displays the **Manage SMS Profiles** window as shown in “Figure 1”.

Figure 1 - Manage SMS Profiles Window



From this window you can:

- View All SMS Profiles
- Add an SMS Profile

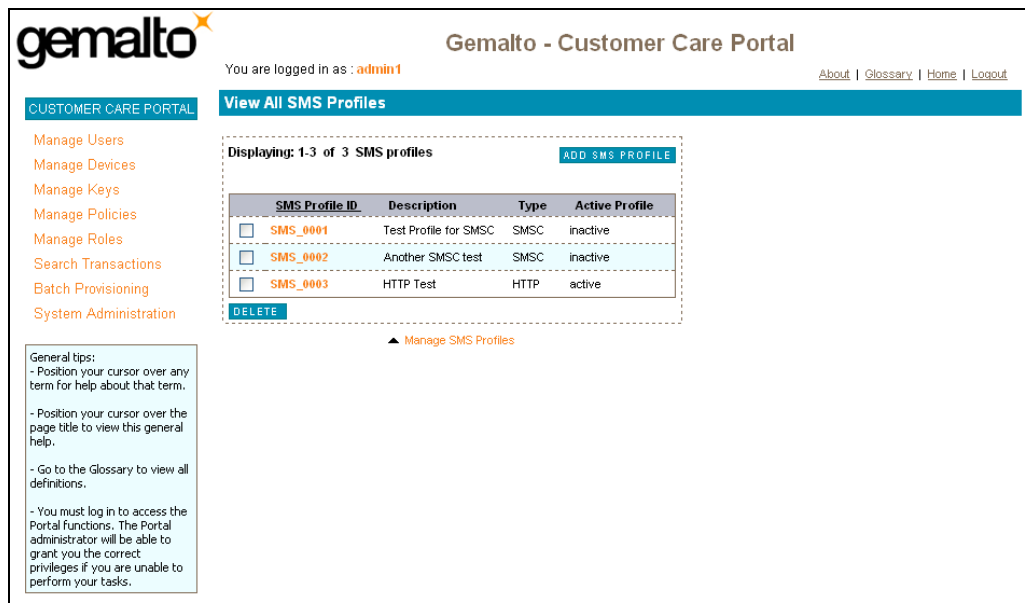
Viewing All SMS Profiles

This function enables you to:

- See a list of the SMS profiles currently available in your system
- Update the details of a particular SMS profile
- Add an SMS profile to the list
- Delete an SMS Profile from the list

To access these functions, click **View All SMS Profiles** in the **Manage SMS Profiles** window, shown in “Figure 1”. This action displays the window shown in “Figure 2” on page 3.

Figure 2 - View All SMS Profiles



The window displays a list of the SMS profiles currently available in your system.

To update the details of an SMS profile:

- 1 In the **View All SMS Profiles** window, click the SMS profile that you want to update. This displays the **View SMS Profile** window with that module's details of the module as shown in "Figure 3".

Figure 3 - View SMS Profile



- 2 Modify the parameters in the window, then click **Update**. If the update is successful, a message displays to tell you this.

The parameters are described in "To add an SMS profile to the list:" on page 4.

Adding an SMS Profile

To add an SMS profile to the list:

- 1 From the **View All SMS Profiles** window in “Figure 2” on page 3, click **Add an SMS Profile**. This displays the window shown in “Figure 4”.

Figure 4 - Add An SMS Profile

The screenshot shows the 'Add an SMS Profile' form in the Gemalto Customer Care Portal. The form is titled 'Add an SMS Profile' and is part of the 'CUSTOMER CARE PORTAL'. It shows a form for creating a new SMS profile with the following fields:

- SMS Profile ID: SMS_0001
- Description: Test Profile for SMSC
- Active Profile:
- * Type: SMSC (dropdown)
- * Originating Address: 01 23 45 67 89
- * Data Coding Scheme: 0
- * Protocol ID: 0
- * Validity Period: 1024
- * System ID: TestID
- * Password: [text input]
- * Confirm Password: [text input]
- * TCP1 Address: 123.123.123.123
- * TCP1 Port: 8080
- * TCP2 Address: 321.321.321.321
- * TCP2 Port: 8081

At the bottom of the form are two buttons: 'CREATE' and 'START OVER'. Below the buttons is a link: 'View All SMS Profiles'. On the left side of the form, there is a sidebar with navigation links: 'Manage Users', 'Manage Devices', 'Manage Keys', 'Manage Policies', 'Manage Roles', 'Search Transactions', 'Batch Provisioning', and 'System Administration'. Below these links is a 'Create Tips' box with the following text:

Position your cursor over any term for help about that term. Position your cursor over the page title to view the Create Tips.

Create Tips:

- Required fields are marked by an asterisk.
- Complete all required fields, then click the CREATE button to save the information and create the new item.
- Click START OVER to erase all entries and begin again.

- 2 In **Description**, you can if you choose enter text to describe your SMS profile.
- 3 In **Active Profile**, check the box if you want this profile to be the active one. As only one SMS profile can be active at any time, you cannot choose this if another profile is currently active in the system. You can of course create the profile as “inactive” and modify the profiles afterwards.
- 4 In **Type**, either select **SMSC** or **HTTP** according to your type of SMS service provider. If you choose **HTTP**, the window changes to the one in “Figure 5” on page 5. In that case, complete the rest of that window as described in “To add an HTTP type SMS profile to the list:” on page 5.
- 5 If you chose **SMSC**, complete the rest of the window as follows:
 - In **Originating Address** enter the phone number of the SMS sender. This must contain only numbers, the + sign or spaces.
 - In **Data Coding Scheme**, enter a number from 0 to 255.
 - In **Protocol ID**, enter a number from 0 to 255.
 - In **Validity Period**, enter the validity period for the SMS messages in seconds. If the SMS-C cannot send the message in this time, it discards the message.
 - In **System ID**, enter the user ID that SA Server uses to log in to the SMS-C service.
 - In **Password** and **Confirm Password**, enter the password that SA Server uses to log in to the SMS-C service.
 - In the remaining fields enter the TCP IP addresses and port numbers for the SMS-C connection.

- 6 When you have completed the window, click **Create**. If the creation is successful, a message displays telling you this

Note: If you want to begin again, before you click **Create**, you can clear your parameters by clicking **Start Over**.

- 7 If you want to add further SMS profiles, enter the details of the next module and click **Create**.

To add an HTTP type SMS profile to the list:

- 1 If you have not already done so, from the **View All SMS Profiles** window in “Figure 2” on page 3, click **Add an SMS Profile**. In **Type**, choose **HTTP**. This displays the window shown in “Figure 5”.

Figure 5 - Add An HTTP Type SMS Profile

The screenshot shows the 'Add an SMS Profile' window in the Gemalto Customer Care Portal. The user is logged in as 'dsutton'. The window title is 'Add an SMS Profile'. The form contains the following fields and options:

- SMS Profile ID:** SMS_0003
- Description:** Test Profile for HTTP
- Active Profile:**
- Type:** HTTP (dropdown menu)
- URL:** http://www.sms-server.com/send?user=gemalto&password=xxx&receiver=%2b15122574004&sender=%2b15122573000
- Dynamic URL configuration:** The following tags are place holders for dynamic content in the URL string. The server will replace them with the appropriate content when generating an SMS message. Configure your URL by embedding the tags where it is appropriate.
 - <RECEIVER_MSISDN> - place holder for the destination address
 - <CONTENT_MSG> - place holder for the message content
- Example:**
 - Static URL: http://www.sms-server.com/send?user=gemalto&password=xxx&receiver=%2b15122574004&sender=%2b15122573000&content=testing123
 - Dynamic URL: http://www.sms-server.com/send?user=gemalto&password=xxx&receiver=<RECEIVER_MSISDN>&sender=5122573000&content=<CONTENT_MSG>
- Expected Result:** SUCCESS
- Active Proxy Server:** Enabled Disabled
- Proxy Server Address:** 123.123.123.123
- Proxy Server Port:** 8080

Buttons: **CREATE**, **START OVER**, [View All SMS Profiles](#)

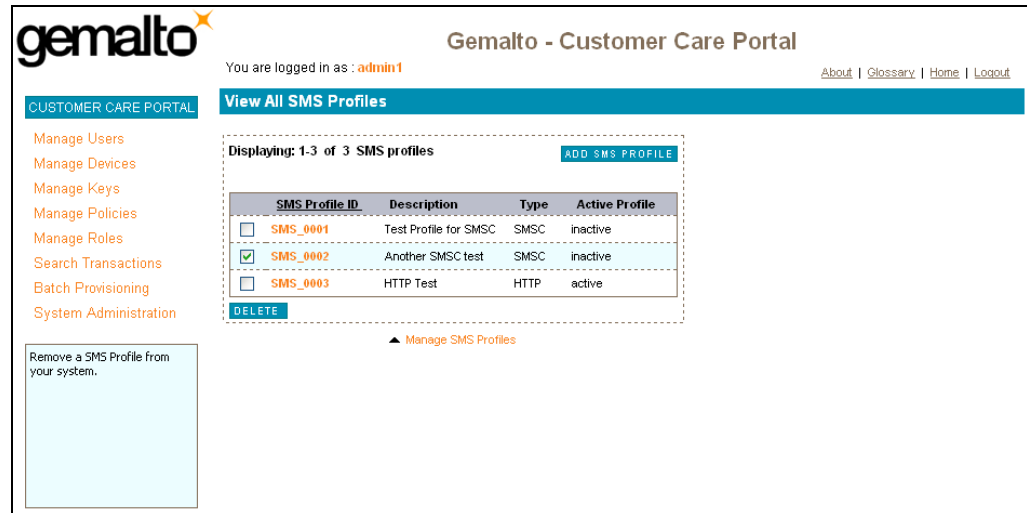
- 2 Complete the rest of the window as follows:
- In **URL** enter the dynamic URL of the HTTP SMS server, using the embedded tags shown in the window.
 - In **Expected Result**, enter the string that you want to appear if the SMS is sent successfully.
 - In **Active Proxy Server**, choose **Enabled** or **Disabled** depending on whether or not your system uses a proxy server.
 - The last two fields appear only if you choose **Active Proxy Server** enabled. Enter the IP address and Port number for the Proxy Server.
- 3 When you have completed the window, click **Create**. If the creation is successful, a message displays telling you this

Note: If you want to begin again, before you click **Create**, you can clear your parameters by clicking **Start Over**.

- 4 If you want to add further SMS profiles, enter the details of the next module and click **Create**.

To delete an SMS profile from the list:

- 1 From the **View All SMS Profiles** window, check the boxes next to the SMS profiles that you want to delete, as shown in “Figure 6”.

Figure 6 - Delete SMS Profiles

- 2 Click **Delete**. If successful, a message displays telling you this and the SMS profile(s) are removed from the system.

Add an SMS Profile

You can add an SMS profile directly from the **Manage SMS Profiles** window, shown in “Figure 1” on page 2. This opens the same window as that shown in “Figure 4” on page 4. Follow the same instructions.

Creating the OATH Policy

You need to create a policy for each type of scenario described at the beginning of this document:

- One for devices that receive OTPs by SMS as the standard method.
- One for virtual devices, where the user has lost their real device and wishes to receive his or her virtual OTP by SMS.

For full details on how to create OATH policies, please refer to the *Customer Care Portal Guide*.

SMS Devices

When you create the OATH policy for SMS devices, (**Manage Policies > Create OATH Policy**), set the **Device Mode** to **SMS** as shown in “Figure 7” on page 7.

Figure 7 - Create OATH Policy - SMS Devices

The screenshot shows the 'Create OATH Policy' form in the Gemalto Customer Care Portal. The user is logged in as 'dsutton'. The form includes a sidebar with navigation options like 'Manage Users', 'Manage Devices', and 'Manage Policies'. The main form area contains the following fields and options:

- Policy Name:** Text input field.
- Device Mode:** Dropdown menu set to 'SMS'.
- Key Mode:** 'Random Key'.
- Send Mode:** 'SMS'.
- OTP Length:** Radio buttons for 6, 7, and 8 (8 is selected).
- Use Password Rule:** Radio buttons for 'Enabled' (selected) and 'Disabled'.
- Applet Version:** Text input field.
- Max OTP Lock:** Text input field with value '0'.
- Check Dates:** Checked checkbox.
- OTP Life Period (seconds):** Text input field with value '0'.

Buttons for 'CREATE' and 'START OVER' are at the bottom. A note on the left explains the 'Maximum one-time password attempts' field.

The **Send Mode** is automatically set to **SMS** for SMS devices.

Virtual Devices

When you create the OATH policy for Virtual devices, (**Manage Policies > Create OATH Policy**), set the **Device Mode** to **Virtual** as shown in "Figure 8".

Figure 8 - Create OATH Policy - Virtual Devices

The screenshot shows the 'Create OATH Policy' form in the Gemalto Customer Care Portal. The user is logged in as 'admin1'. The form includes a sidebar with navigation options like 'Manage Users', 'Manage Devices', and 'Manage Policies'. The main form area contains the following fields and options:

- Policy Name:** Text input field.
- Device Mode:** Dropdown menu set to 'Virtual'.
- Key Mode:** 'Random Key'.
- Send Mode:** Dropdown menu set to 'Display'.
- Default Policy:** Unchecked checkbox.
- OTP Length:** Radio buttons for 6, 7, and 8 (8 is selected).
- Use Password Rule:** Radio buttons for 'Enabled' (selected) and 'Disabled'.
- Applet Version:** Text input field.
- Sync Window:** Text input field with value '100'.
- Resync Window:** Text input field with value '500'.
- Max OTP Lock:** Text input field with value '0'.
- Check Dates:** Radio buttons for 'Disabled', 'Fixed Date' (selected), and 'Life Period'.
- Number of Virtual OTPs:** Text input field with value '10'.

Buttons for 'CREATE' and 'START OVER' are at the bottom. A note on the left explains the 'Maximum resynchronization window' field.

In **Send Mode** choose **SMS**.

Checking the User Details

For details on how to view user records, please refer to the *Customer Care Portal Guide*.

Here the important thing to note is that for a user to receive an OTP via SMS, the Mobile Phone# must be present and valid in the user record as shown in "Figure 9"

Figure 9 - View User Window

gemalto Gemalto - Customer Care Portal

You are logged in as : dsutton [About](#) | [Glossary](#) | [Home](#) | [Logout](#)

CUSTOMER CARE PORTAL **View User**

- Manage Users
- Manage Devices
- Manage Keys
- Manage Policies
- Manage Roles
- Search Transactions
- Batch Provisioning
- System Administration

Refresh the data on the screen.

USER INFORMATION

User ID: dsutton

First Name: David

Last Name: Sutton

Email Address: [Redacted]

Mobile Phone #: 06 11 22 33 44

User State: Active

Role: Admin [INFO](#)

Password Attempts: 0

QA Attempts: 0

Creation Date: 26-Apr-2008 16:34:19

Last Modified Date: 27-May-2008 03:31:35

[UPDATE](#) [BLOCK](#) [REVOKE](#)

[RESET PASSWORD](#) [LOST OR FORGOTTEN DEVICE](#)

ASSOCIATED DEVICES

Smart Card ID #	Device State	Expires
[Redacted]	<input type="checkbox"/> Encrypted LINK	

[ACTIVATE](#) [REMOVE](#) [BLOCK](#) [UNBLOCK](#) [REVOKE](#)

USER TRANSACTION HISTORY						
#	Smart Card ID	Action	Action Result	Performed by	Start Time	End Time
1		Update User	Operation was successful.	dsutton	27-May-2008 03:31:35	27-May-2008 03:31:35
2		Authenticate by Password	Operation was successful.	dsutton	27-May-2008 01:40:23	27-May-2008 01:40:24
3		Authenticate by Password	Operation was successful.	dsutton	20-May-2008 06:25:58	20-May-2008 06:25:58
4		Authenticate by Password	Operation was successful.	dsutton	20-May-2008 04:14:44	20-May-2008 04:14:44
5		Authenticate by Password	Operation was successful.	dsutton	20-May-2008 03:16:42	20-May-2008 03:16:42
6		Authenticate by Password	Operation was successful.	dsutton	20-May-2008 03:08:00	20-May-2008 03:08:00
7		Authenticate by Password	Operation was successful.	dsutton	20-May-2008 02:52:31	20-May-2008 02:52:31
8		Authenticate by Password	Operation was successful.	dsutton	19-May-2008 07:31:29	19-May-2008 07:31:29
9		Authenticate by Password	Operation was successful.	dsutton	16-May-2008 08:05:39	16-May-2008 08:05:39
10		Authenticate by Password	Operation was successful.	dsutton	16-May-2008 07:06:09	16-May-2008 07:06:09

Show last 10 transactions [REFRESH](#)

[Return to View User](#)

Checking the Role

For details on how to view role details, please refer to the *Customer Care Portal Guide*. Here the important thing to note is that for a user to receive an OTP via SMS, the role assigned to him or her must have the **Generate SMS OTP** privilege as shown in “Figure 10”.

Figure 10 - View Role Window

The screenshot shows the 'View Role' window in the Gemalto Customer Care Portal. The role name is 'Admin' and its description is 'Built-in default admin role'. The 'Privileged Role' is set to 'Yes'. The number of associated users is 3, and the creation and last modified dates are both 28-Apr-2008 16:29:51. The 'Generate SMS OTP' privilege is highlighted with a red circle. The sidebar on the left includes options like 'Manage Users', 'Manage Devices', 'Manage Keys', 'Manage Policies', 'Manage Roles', 'Search Transactions', 'Batch Provisioning', and 'System Administration'. A note in the sidebar says 'View the users associated with the current role.'

ROLE INFORMATION			
Role Name:	Admin		
Role Description:	Built-in default admin role		
Privileged Role:	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Number of Associated Users:	3 VIEW USERS		
Creation Date:	28-Apr-2008 16:29:51		
Last Modified Date:	28-Apr-2008 16:29:51		
UPDATE ROLE DELETE ROLE COPY ROLE			
Privileges: Please select role privileges from the list below. <input type="checkbox"/>			
<input checked="" type="checkbox"/> Register User	<input checked="" type="checkbox"/> View My Transaction History	<input checked="" type="checkbox"/> Change My Answers	<input checked="" type="checkbox"/> Resync My Device
<input checked="" type="checkbox"/> Update My Account	<input checked="" type="checkbox"/> Change My Password	<input checked="" type="checkbox"/> Reset My Password	<input checked="" type="checkbox"/> Lost My Device
<input checked="" type="checkbox"/> View My Account	<input checked="" type="checkbox"/> Generate SMS OTP		
<input checked="" type="checkbox"/> Create User	<input checked="" type="checkbox"/> Unlock User	<input checked="" type="checkbox"/> Change User Role	<input checked="" type="checkbox"/> Lost Device
<input checked="" type="checkbox"/> Update User	<input checked="" type="checkbox"/> Block User	<input checked="" type="checkbox"/> Reset User Password	<input checked="" type="checkbox"/> Link Device to User
<input checked="" type="checkbox"/> Delete User	<input checked="" type="checkbox"/> Unblock User	<input checked="" type="checkbox"/> Reset QA Attempts	<input checked="" type="checkbox"/> Activate Device
<input checked="" type="checkbox"/> Search User	<input checked="" type="checkbox"/> Revoke User	<input checked="" type="checkbox"/> Reset Password Attempts	<input checked="" type="checkbox"/> Remove Device from User
<input checked="" type="checkbox"/> Create Device	<input checked="" type="checkbox"/> Block Device	<input checked="" type="checkbox"/> Reset OTP Attempts	<input checked="" type="checkbox"/> Link Key to Device
<input checked="" type="checkbox"/> Update Device	<input checked="" type="checkbox"/> Unblock Device	<input checked="" type="checkbox"/> Unlock Device	<input checked="" type="checkbox"/> Link Policy to Device
<input checked="" type="checkbox"/> Delete Device	<input checked="" type="checkbox"/> Revoke Device	<input checked="" type="checkbox"/> Resync Device	<input checked="" type="checkbox"/> Expire Devices
<input checked="" type="checkbox"/> Search Device			
<input checked="" type="checkbox"/> Authenticate User	<input checked="" type="checkbox"/> Authenticate Device	<input checked="" type="checkbox"/> Authenticate User-Device	
<input checked="" type="checkbox"/> Authenticate by Password	<input checked="" type="checkbox"/> Access Customer Care Portal	<input checked="" type="checkbox"/> Access System Administration Portal	

Modifying the SMS Message

When users receive an OTP by SMS, the message has some accompanying text, for example “Please use the following SMS 1-time key to access SA Server. This value expires on”. You can change this message by modifying it in the appropriate XML file. There is one file for SMS devices and one for virtual devices.

These files can be accessed via the System Administration part of the Customer Care Portal. They are located in **Home > Manage System Settings > Other Settings**:

Figure 11 - The “Other Settings” Window

The screenshot displays the 'Other settings' window in the Gemalto Customer Care Portal. The page header includes the Gemalto logo, the user's login name 'dsutton', and navigation links for 'About', 'Glossary', 'Home', and 'Logout'. The main content area is titled 'Other settings' and contains a table with the following data:

File Name	Last Updated	
Mail engine settings	Monday, May 12, 2008 9:35:54 AM CDT	REPLACE
Generate virtual OTP email template	Monday, May 12, 2008 9:35:55 AM CDT	REPLACE
Generate virtual OTP SMS template	Monday, May 12, 2008 9:35:55 AM CDT	REPLACE
Self-generate virtual OTP email template	Monday, May 12, 2008 9:35:54 AM CDT	REPLACE
Request OTP by SMS template	Monday, May 12, 2008 9:35:54 AM CDT	REPLACE
Database connection pool settings	Monday, May 12, 2008 4:34:44 PM CDT	REPLACE
SQL engine settings	Monday, May 12, 2008 4:34:46 PM CDT	REPLACE
Security engine settings	Monday, May 12, 2008 4:34:46 PM CDT	REPLACE

Below the table is a link for 'Manage System Settings'. On the left side of the page, there is a sidebar with navigation options: 'Manage Users', 'Manage Devices', 'Manage Keys', 'Manage Policies', 'Manage Roles', 'Search Transactions', 'Batch Provisioning', and 'System Administration'. At the bottom left, there is a button labeled 'Click to download the file'.

For details on how to replace these files, refer to the *System Administration Guide*.