SafeNet Authentication Service (SAS)

Service Provider Branding Guide

gemalto
security to be free

Document Part Number: 007-012405-002, Rev. F

Release Date: June 2016

Contents

Preface

This guide describes the various ways in which the appearance of SafeNet Authentication Service (SAS) can be customized.

Users are encouraged to read this guide in the order in which information is presented, as successive chapters often rely on information and concepts presented in prior chapters.

Audience

This guide is intended for SafeNet Authentication Service Administrators, Product Managers, and Marketing Managers responsible for how managed authentication services are delivered, and for configuring SAS to reflect the organization's brand.

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—A cloud-based service of SafeNet, Inc.
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**—The software used to build an authentication service.
- **SafeNet Authentication Service – Private Cloud (SAS-PCE)**—A term used to describe the implementation of SPE on customer premises.

Terminology

Several terms and their meaning are important to understanding the information presented in this guide:

- **SAS**—All versions of SafeNet Authentication Service; the technology and infrastructure upon which the authentication service is delivered.
- **Service Providers**—These are accounts that, in addition to having their own virtual server, are able to create and manage subordinate accounts, Virtual Service Providers, and/or Subscribers.
- **Subscriber**—When the term "subscriber" is presented in lowercase, it applies to all accounts that you create and manage. When capitalized, the term "Subscriber" refers to accounts that are not Service Providers.
- **Virtual Server**—This term refers to an individual account's virtual authentication server.
- **Virtual Service Providers**—These are service provider accounts that have a Service Provider as a parent.

Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	

1
Branding Your Service

Overview

An important strategy for developing, promoting, and sustaining your cloud authentication service is the promotion of your brand in the marketplace. This document describes the many options available to customize and brand the service you deliver to your Subscribers. These options include:

- **Fonts**—Customize font type, color, and weight
- **Logos**—Apply your logo to the Management interface, Self-Service, and Enrollment web pages. Add background images to Self-Service and Enrollment pages.
- **Colors**—Apply colors to pages, tables, and input fields on Self-Service and Enrollment web pages.
- **Buttons**—Select from a range of graphic buttons, use HTML buttons, or upload your own buttons for use on all pages.
- **Email and SMS Messages**—These messages can be customized to use text or HTML, and to include graphics and hyperlinks.

Inheritance

By default, every account you "on-board" automatically inherits all branding and SMS gateway customizations you have applied to your virtual server. Refer to the *Service Provider Administrator Guide* for instructions to remove or prevent inheritance.

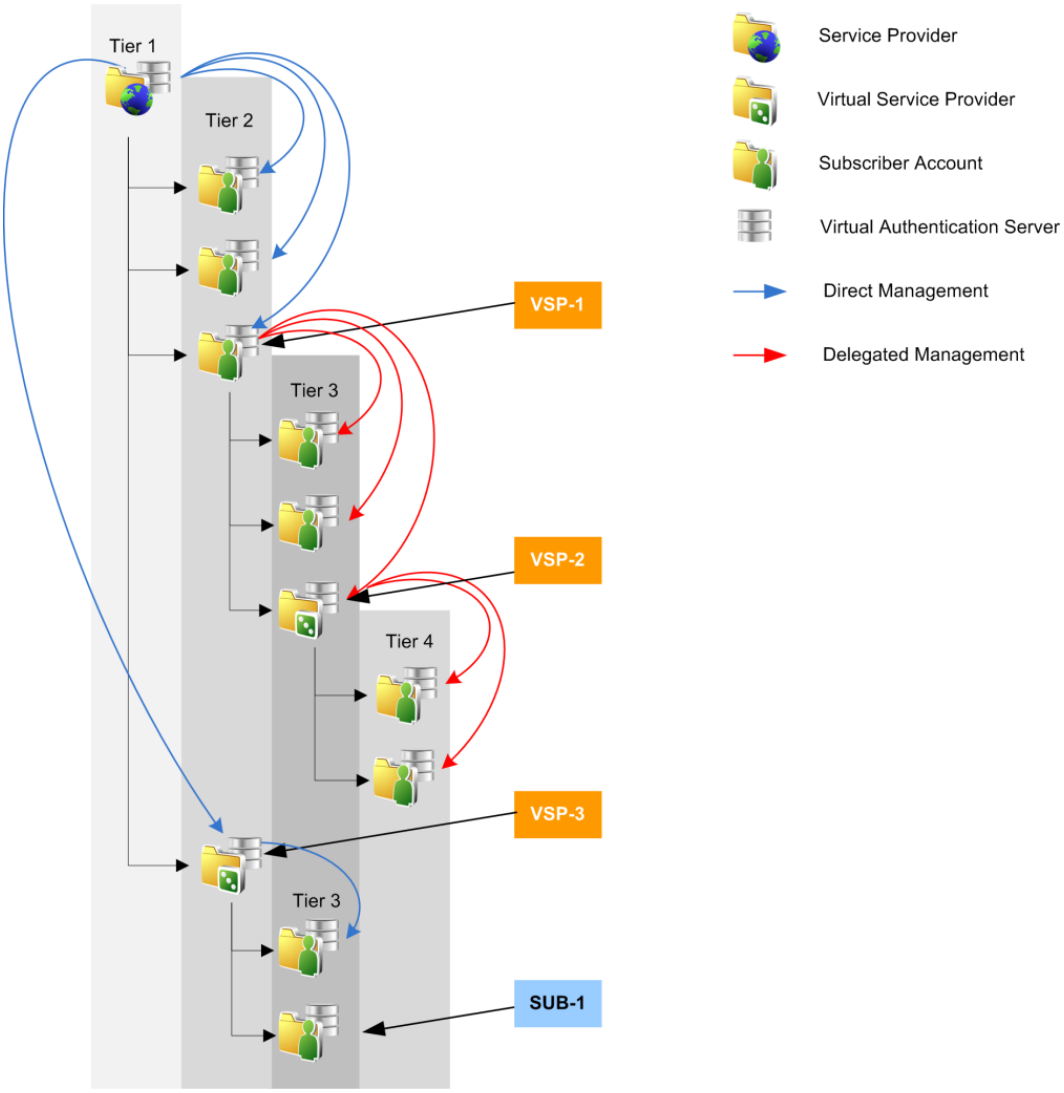

Figure 1: Branding and Customization Inheritance

In Figure 1: Branding and Customization Inheritance, all child accounts in Tier 2 inherit the branding and customization settings configured by the Host Account.

If VSP-1 modifies the branding for a customization configuration in its virtual server, all of its child accounts in Tier 3 inherit the new branding and customizations.

When VSP-1 adds VSP-2 to its accounts, it can disable VSP-2's ability to modify branding and customization. In that case, VSP-2 and all of its child accounts in Tier 4 inherit VSP-1's branding and customization.

Similarly, VSP-3 inherits the Host Account's branding and customization configuration. If VSP-3 makes no changes, all of its child accounts in Tier 3 inherit the Host Account's branding and customization configuration.

SUB-1 can modify the branding and configuration it inherited from VSP-3 to reflect its own requirements.

Note that a change at any time to VSP-3's branding and customization configuration is inherited only by its child accounts that have not applied their own customizations.

Custom URLs

SAS generates unique URLs for the Management logon and Self-Service pages of each virtual server. Each subscriber must use their own unique Management logon and Self-Service URLs. Management UI logon can also take place at the default logon page (http://serviceURL/console), where default branding will be visible.

These URLS are displayed in the **Custom Branding** module (**COMMS** tab **> Custom Branding**) and **Self-Service** section of the **Automation** module (**Policy** tab **> Automation** module **> Self-Service** hyperlink) respectively. Only at these URLs will branding be visible and will Self-Service functions succeed.

Enrollment page URLs are generated on the fly for each user that is part of a provisioning task. URLs are included in the notification email message to the user.

Overriding Inheritance

Each of your on-boarded accounts has its own Virtual Server that can be configured to override inherited customizations. This is beneficial should your client require their own brand or, as a Virtual Service provider, wish to resell your service under their brand.

Note that if an on-boarded account applies a customization to their virtual server, it will no longer inherit any new customizations that you apply to your virtual server.

No Override

To prevent your on-boarded account from overriding the inherited or custom branding you applied to their Virtual Server, do one of the following:

- Do not create an Administrator account to be used by your client to log in to the Management interface of their virtual server. If they cannot log in, they cannot apply changes.
- To allow your client to log in to the management interface of their virtual server but not to modify customizations:
    - Do not use the **Add Administrator** function on the **ON-BOARDING** tab to add your client as an Operator, as this gives them the right to make modifications.
    - Instead, create a role that denies access to the **Branding** module. (To prevent changes to SMS gateways, email servers, and message contents, ensure that the role denies access to the **Communications** module.)
    - Add the client as a User, assign a token, and then promote the client to Operator, having created the role in the previous bullet.

Refer to the *Virtual Service Provider Administrator Guide* for information on creating and assigning Operators to Roles, customizing email and SMS messages, and configuring SMS gateways and SMTP servers.

2
Applying Your Brand

Custom Branding Module

The appearance and branding of the virtual server Management UI, Self-Service, and Enrollment web pages can be customized for colors, fonts, logos, and titles.

The virtual server generates a unique URL for each customized page:

- **Customized Management UI Logon Page URL**—This is the Operator login URL reference in the **Custom Branding** module.
- **Customized Self-service URL**—This is the Self Service Unique URL found in the **Self-Service** tab **> Configuring Self-Service** module.
- **Customized Enrollment pages**—This is the Self Service Unique URL found in the **Self-Service** tab **> Configuring Self-Service** module.

To customize:

1. On the **Custom Branding** window, click the **Set Customization Inherit** hyperlink.
2. Clear the **Use Customizations Inherit** option.
3. Click **Apply**.

The module displays options for customizing fonts, colors, buttons, logo images, titles, labels, and product name.

To discard customizations:

- Select the **Set Customization Inherit** option.

If **Use Customizations Inherit** is subsequently re-enabled, the virtual server inherits the system defaults and not the defaults from the Service Provider.

Custom Fonts

To select custom fonts:

1. Click the **Custom Fonts** hyperlink.
2. In the **Font-family** field, select a font family.
3. Set the font for the remaining fields as desired.

   Your settings will be applied for preview to the **Sample** text.

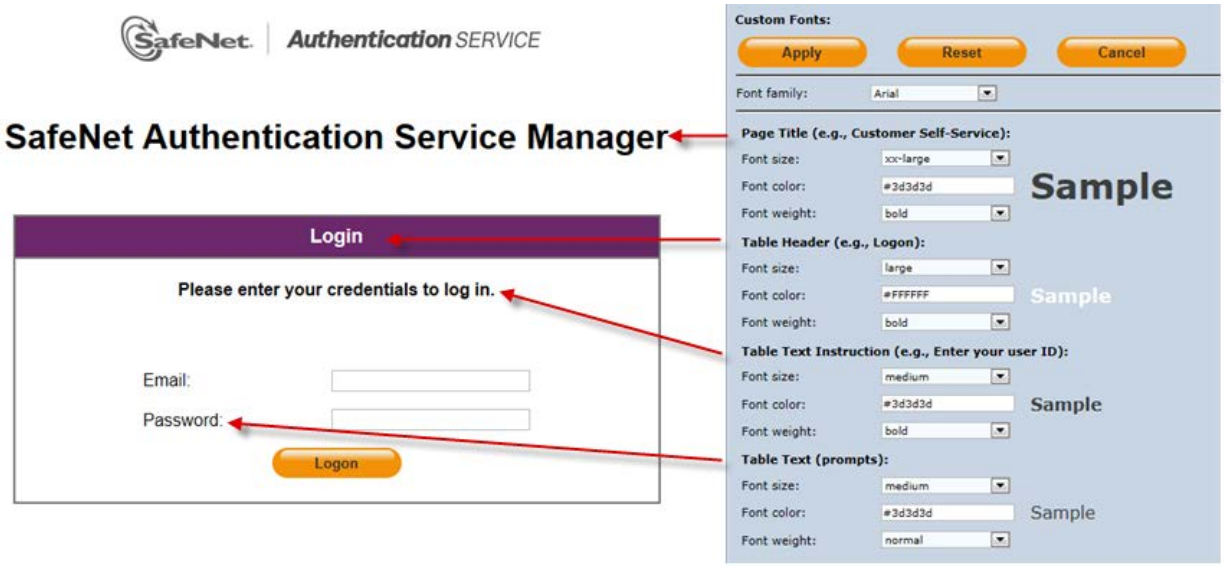

Figure 2: Custom Fonts

Custom Colors

To select custom colors:

Click the **Custom Colors** hyperlink. Select the font-family from the drop-down list. Enter colors using standard names (red, green, blue, etc.) or use hex values (#F80000, #CC6600, etc.).

Custom Colors – Logon Page

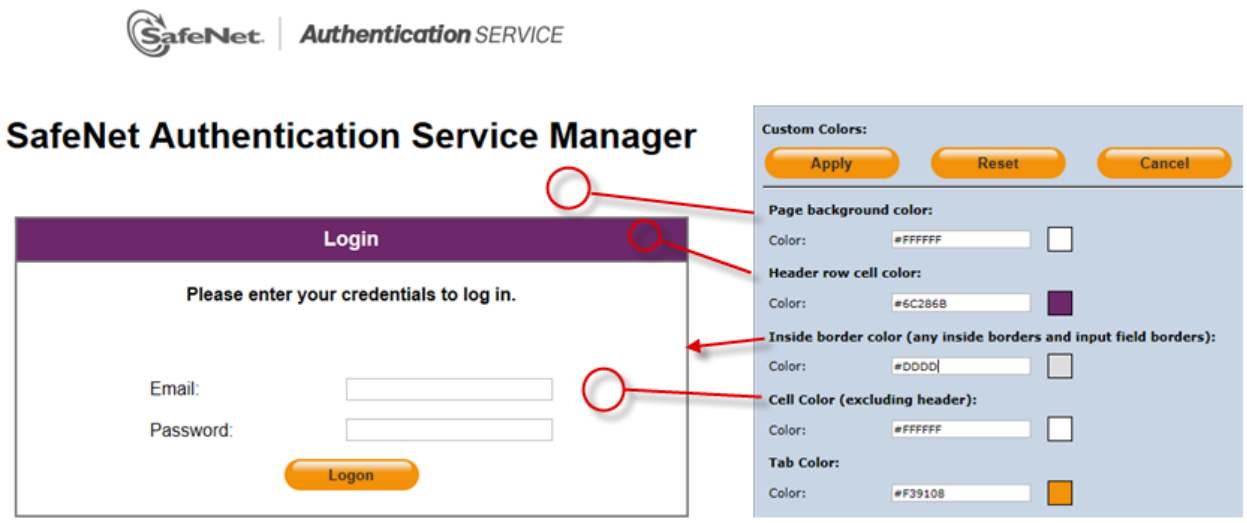

Figure 3: Custom Colors - Logon Page

Custom Colors – Management UI

Figure 4: Custom Colors - Management UI

Custom Buttons

To begin, click the **Custom Buttons** hyperlink. To select a preset graphic button, click the corresponding radio button and click **Apply**. To use an HTML button, enter a color value (red, green…) or a color HEX value (#F80000, #00C800…).

For normal and hover button text size, color and weight can be customized by configuring the **Button Text** and **Button Hover Text** options. As above, use standard color values or enter a HEX value for font color.

Custom graphic buttons can also be used. Buttons must be 120 x 28 px in PNG, JPG or GIF format. First upload the button in the **Custom Logo Images** module, then return to this page and select the button, text, hover, etc.

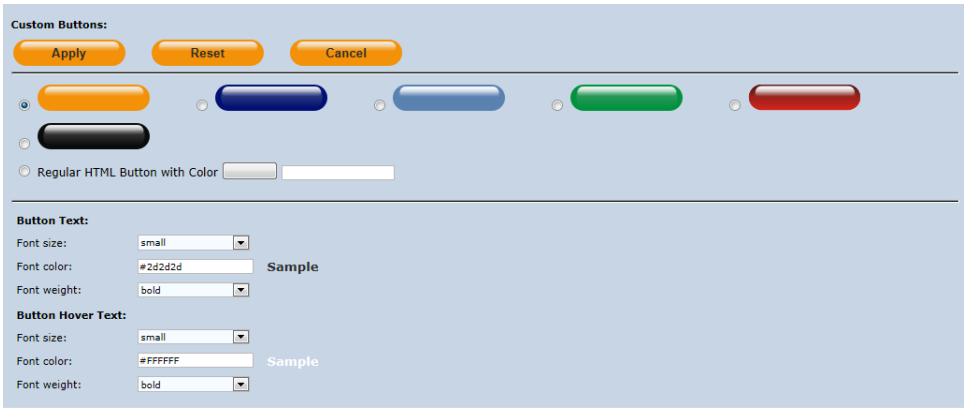

Figure 5: Custom Buttons

Custom Logo Images

To begin, click the **Custom Logo Images** hyperlink. Select the images then click the **Upload** button. Images can be replaced with the defaults by clicking the **X** to the right of any custom image or replaced by simply uploading a new image.

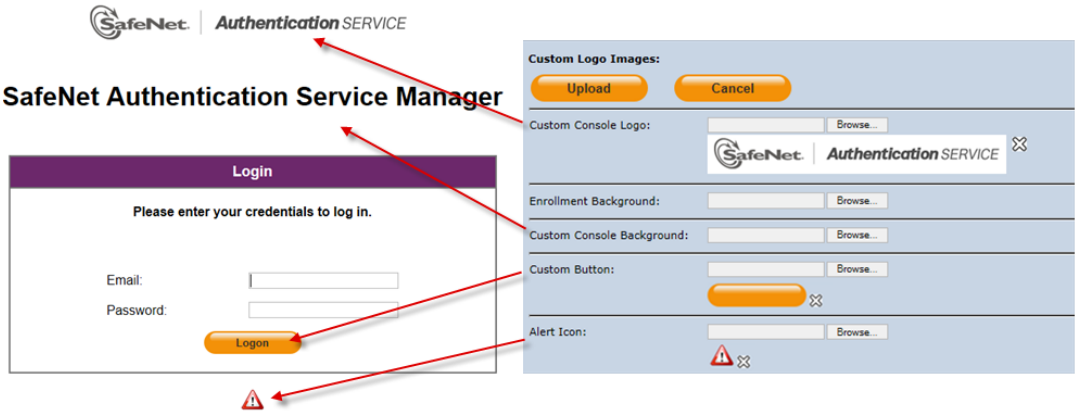

Figure 6: Custom Logo Images (with custom button uploaded)

- The Custom Console Logo must be in no larger than 400 x 100 px in png, jpg, or gif format.
- The Alert Icon must be 30 x 30 px in PNG, JPG or GIF format.

The recommend background size is 1800 x 1100 px in PNG, JPG or GIF format. To maintain page loading speed image size should be less than 50kB.

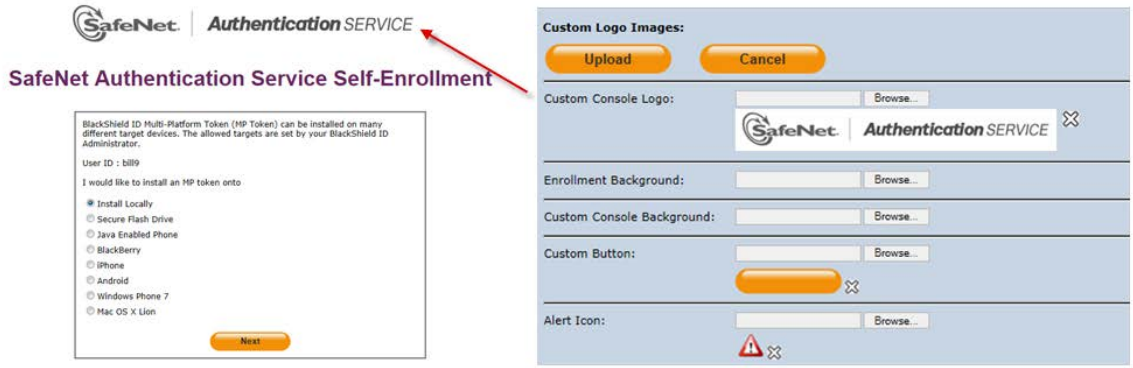

Figure 7: Custom Logo - Enrollment Pages

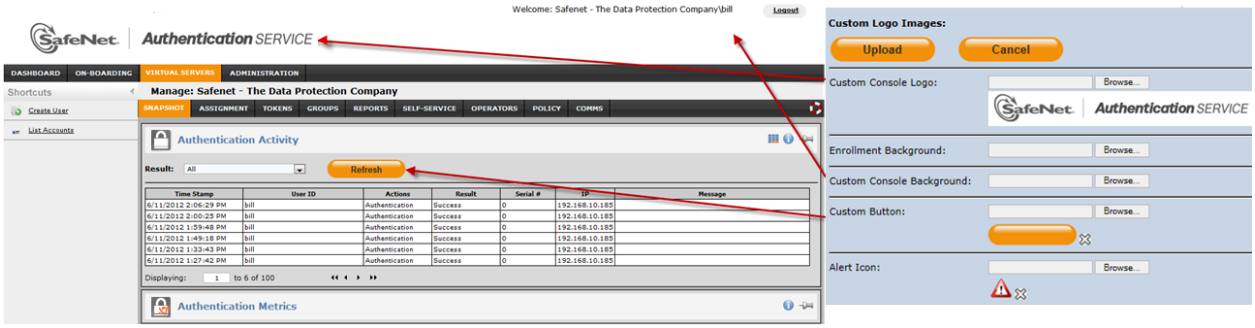

Figure 8: Custom Logo - Management UI

Custom Titles

Modify the text in the corresponding fields to replace the titles on the console management logon, self-enrollment and self-service pages.

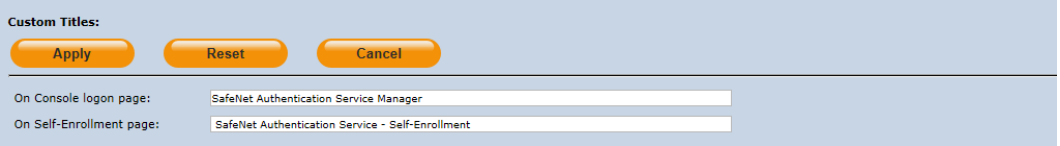

Figure 9: Custom Titles

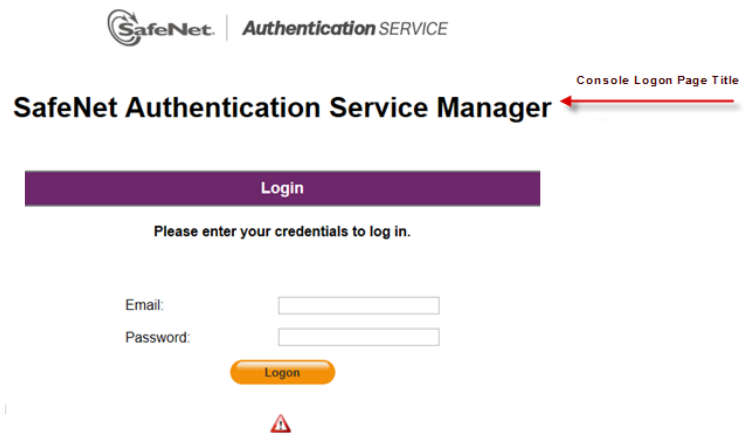

Figure 10: Console Logon Title

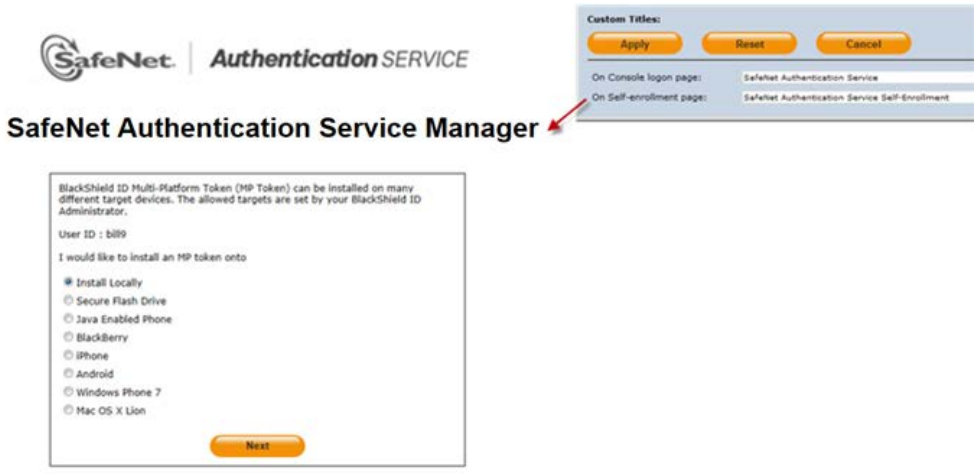

Figure 11: Self-enrollment Page Title

Custom Labels

Use this module to change the custom # labels displayed in the UI, where:

Figure 12: Custom Labels

- **User Custom**—Refers to **Custom #1**, **Custom #2**, and **Custom #3** field labels displayed in **User Detail** (Virtual Server) and in user related reports and tables. An example use would be to change **Custom #1** to an employee number or other identifier that could be used to link reports and user information in SAS to the external system.
- **Account Custom**—Refers **to Custom #1**, **Custom #2**, and **Custom #3** field labels displayed in **Accounts Detail** (On-Boarding) and in account related reports and tables. An example use would be to change **Custom #1** to an account number or other identifier that could be used to link reports and customer information in SAS to the external system.

Custom Product Name

Use this function to change all occurrences of the default product name (SafeNet Authentication Service) used in email and SMS templates (refer to **COMMS** Tab > **Communications** module > **SMS Messages** / **E-mail Messages**).

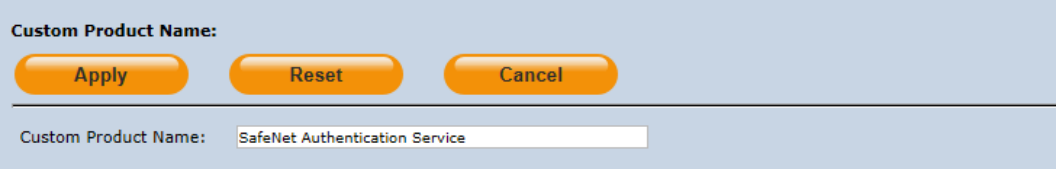

Figure 13: Custom Product Name

Custom Organization Name

Use this function to change all occurrences of the default organization name used in email and SMS templates (refer to **COMMS** Tab > **Communications** module > **SMS Messages** / **E-mail Messages**).

This name is only used with Push OTP, and is included in the login request details on a user's mobile device. By default, this is the **Account Name** that is displayed in the SAS Management Console.

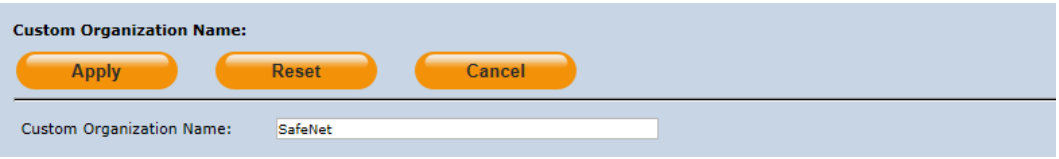

Figure 14: Custom Organization Name

Custom SMS Messages

You can customize the various SMS/OTP messages that are sent by the Virtual Server. Start from the Virtual Server **COMMS** tab **> SMS Messages** hyperlink **> Custom** option, and then select an **SMS Message Type**. The message content is displayed in the **Message** window.

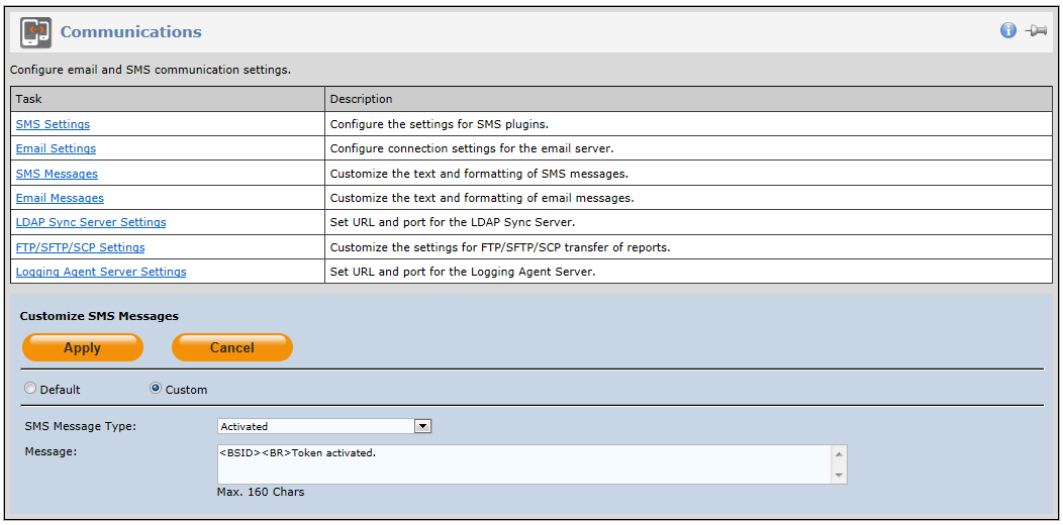

Figure 15: Customize SMS Messages

> **NOTE:** You can add **!MUTE!** to the beginning of any SMS or e-mail message to prevent it from being sent.

Customizing SMS Messages

Message content can be modified as required, bearing in mind that SMS messages greater than 160 characters in length (including spaces) will be split into two or more messages.

Tags are used to insert information from the Virtual Server into your message content. The following tags are used.

Tag	Description
** **	Text following this tag is on a new line.
<NEW_PIN>	New PIN value set by Operator or via Self-Service
<NEXT_OTP>	OTP
<USER_ID>	User ID
<PIN>	PIN
<TEMP_PIN>	Temporary Password (Token suspended by Operator)
<BSID>	This value is replaced by the values in the Custom Product Name field.

The following is a list of SMS messages and corresponding events that cause the messages to be sent:

Message	Event	Valid Tags
Activated	Sent when suspended token is Unlocked by Operator	<BSID>
Activated New PIN	Sent when suspended token is Unlocked by Operator and a New PIN is set.	<BSID> <NEW_PIN>
New Challenge/Response	Sent when SMS token in challenge/response mode is provisioned.	<BSID> <USER_ID>
New Challenge/Response with no PIN	Sent when SMS token in challenge/response mode is provisioned and no PIN is required.	<BSID> <USER_ID>
New PIN	Sent when a new PIN is set by an Operator.	<BSID> <NEXT_OTP><PIN>
New PIN Change Next	Sent when a new PIN is set by an Operator and PIN change on first use is required.	<BSID> <NEXT_OTP><PIN>
New QUICKLog	Sent when SMS token in QUICKLog mode) is provisioned.	<BSID> <USER_ID><NEXT_OTP><PIN>
New QUICKLog with no PIN	Sent when SMS token in QUICKLog mode is provisioned and a PIN is not required to use the token.	<BSID> <USER_ID><NEXT_OTP>
Next OTP	Sent after successful SMS/OTP authentication for tokens in QUICKLog mode.	<BSID> <NEXT_OTP>
Next OTP with no PIN	Sent after successful SMS/OTP authentication for tokens in QUICKLog mode and a PIN is not required to use the token.	<BSID> <NEXT_OTP>
Suspended	Sent when the SMS/OTP token is Suspended.	<BSID>
Suspended Temp Password	Sent when the SMS/OTP token is Suspended and a temporary password is set for the user.	<BSID> <TEMP_PIN>
Test Successful	Sent when testing SMS Settings.	<BSID>

Custom Email Messages

Message content can be modified as required. Select the Text or HTML option to send content using plain text or HTML respectively.

Tags are used to insert information from the Virtual Server into your message content. Many tags are available for specific messages only. The following tags may be used:

Tag	Use
** **	Text following this tag is on a new line
<accountName />	Company name associated with Virtual Server
<remaining />	The remaining (unused) capacity in the Virtual Server
<total />	The total capacity allocated to the Virtual Server
<active />	Virtual Server service as set by Service Provider (enabled / disabled)
<type />	Virtual Server service type (account, Virtual Service Provider, Evaluation)
<daysLeft />	Day before Service stop date
<stepDate />	Service stop date as set by Service Provider
<dateTime />	Timestamp of an event
<firstName>	First name of a User
<lastName>	Last name of a User
<blackberryURL />	Unique URL for self-enrollment of MP-1 token on BlackBerry generated by Virtual Server
<reportName />	Name of a report
<name />	User ID
<taskeID />	Provisioning task number generated by Virtual Server
<count />	Number of users that did not complete self-enrollment before the Provisioning Task expiration
<username />	A User's UserID (User Detail)
<Uaddress />	Address (User Detail)
<Ucity />	City (User Detail)
<Uprovince />	State/Province (User Detail)

<Upostal />	Postal/Zip (User Detail)
<Ucountry />	Country (User Detail)
<orgName />	Account Name (Virtual Server)
<Oaddress />	Account address (Virtual Server)
<Oprovince />	Account State/Province (Virtual Server)
<Opostal />	Account Postal/Zip (Virtual Server)
<Ocountry />	Account country (Virtual Server)
<otaURL />	Unique URL for self-enrollment to install MP-1 generated by Virtual Server
<tokenPIN />	PIN for MP-1 token enrollment on Java phone
<capLeft />	Remaining Virtual Server license capacity
<capTotal />	Total Virtual Server license capacity
<expiryDate />	Server license expiration date
<expiryTime />	Days remaining before license expires
<capLeft />	Service capacity remaining
<capTotal />	Service capacity total
<tokenList />	Serial numbers of tokens no longer associated with users
<freeSpace />	Disk space remaining
<diskSize/>	Total disk space
<percentageFree />	Percentage of available space versus total disk size
<consoleLink />	Unique URL for Operator Validation and logon to management UI
<username />	Unique UserID used by Operator to logon to management UI
<unlockTime/>	Time a user account will automatically unlock
<organization />	Account to which a user belongs
<state />	Operator account status. (active, pending, suspended)
<remaining />	Quantity of SMS Credits in Virtual Server inventory
<selfEnrollURL />	Unique URL sent to user for self-enrollment

<addList />	List of users added by synchronization with an external user data source
<ignoreList />	Total number of users not updated during synchronization as users already exist in the Virtual Server
<updateList />	Total number of users removed by synchronization, as users no longer exist in the external data source
<removeList />	List of users removed by synchronization as users no longer exist in the external data source
<totalMarkforRemoval />	Total number of users not found in external data source during synchronization. These users will be removed from the Virtual Server after 24 hours have elapsed.
<markedList />	List of users not found in external data source during synchronization. These users will be removed from the Virtual Server after 24 hours have elapsed.
<tokenType />	Type of token. (KT, MP…)
<time />	Date/Time of request by user to be issued a token
<oldState />	State of token (assigned, active…) when token was assigned to user
<newState />	The State a token is moved to by the Virtual Server when the user to which it was assigned can no longer be found
<serial />	Serial number of a token
<remaining />	Quantity of a type of token remaining in inventory
<total />	Total quantity of tokens registered in the Virtual Server
<failAttempts />	Quantity of consecutive failed logon attempts

The following is a list of SMS messages and corresponding events that cause the messages to be sent where:

- **SP Alert**—These alerts are only available to accounts where the Service Type is Virtual Service Provider.
- **Alert**—These alerts are available in all account Service Types.
- **HAlerts**—These are system alerts and are valid only for the hosting service.
- **Enrollment**—These messages are sent as part of a Provisioning and/or Self-enrollment process.

Customizing Email Messages

Account Capacity	
Type	SP Alert
Event	Sent when Virtual Server capacity falls below configured event threshold
Subject	SafeNet Authentication Service Account Capacity
Body	The account <accountName /> is approaching their capacity with <remaining /> remaining of <total /> allocated to them
SMS Content	Account <accountName /> approaching capacity. <remaining />/<total /> left

Account Removed	
Type	SP Alert
Event	Sent when an Account (Virtual Server) is removed
Subject	SafeNet Authentication Service Account Removed
Body	The account <accountName /> has been removed by <operator />
SMS Content	Account <accountName /> removed by <operator />

Account Status Change	
Type	SP Alert
Event	Sent when a Virtual Server account is enabled or disabled
Subject	SafeNet Authentication Service Account Status Change
Body	The account <accountName /> has changed to an <active /> <type />
SMS Content	Account <accountName /> changed to an <active /> <type />

Account Stop Date	
Type	SP Alert
Event	Sent X days in advance of Service stop date
Subject	SafeNet Authentication Service Account Stop Date
Body	The account <accountName /> is approaching their stop date. There are <daysLeft /> day(s) till the stop date on <stopDate />
SMS Content	<daysLeft /> day(s) till stop on <stopDate /> for account <accountName />

Active Evaluation Stop Date	
Type	SP Alert
Event	Sent X days in advance of Service stop date for evaluation accounts
Subject	SafeNet Authentication Service Evaluation Stop Date
Body	The account <accountName /> is approaching their evaluation stop date. There are <daysLeft /> day(s) till the stop date on <stopDate />
SMS Content	<daysLeft /> day(s) till stop on <stopDate /> for eval account <accountName />

Android Token	
Type	Enrollment
Event	Sent to User enrolling MP-1 on an Android device
Subject	Over-The-Air (OTA) Installation for Android Device
Body	<firstName /> <lastName />: Follow these 2 easy steps to install the MP-1 token on your Android device: Step 1: Tap the icon below to download the MP-1 from Android Market. Step 2: Now that the MP-1 is installed, you can click the URL below to install the MP-1 token profile. <otaURL />
SMS Content	The MP-1 token Download URL: <otaURL />

Auth Node Changes	
Type	SP Alert
Event	Sent if an element of the service is downgraded or unavailable.
Subject	SafeNet Authentication Service Auth Node Changes
Body	The Auth Node <nodeName /> in account <accountName /> was <action /> by <changedBy />
SMS Content	Auth Node <nodeName /> in <accountName /> <action /> by <changedBy />

Auth Service Down	
Type	SP Alert
Event	Sent if an element of the service is downgraded or unavailable
Subject	SafeNet Authentication Service Authentication Service Error
Body	This message is to report that the SafeNet Authentication Service authentication service was found to be unresponsive at <dateTime />, during a scheduled check of the service
SMS Content	SafeNet Authentication Service down at <dateTime />

BlackBerry PIN	
Type	Enrollment
Event	Sent to Users receiving BlackBerry token by e-mail. First of two messages.
Subject	SafeNet Authentication Service Auth Node Changes
Body	<firstName /> <lastName />: This e-mail will assist you in the installation and activation of your new SafeNet token into your Blackberry. Step one is to install the Token Authenticator and Token Attachment handler application on your BlackBerry. Step two is the installation and activation of the actual token. Please make note of the PIN below, as it is required to activate your token. To install the Token Authenticator "Over-the-Air", browse to the URL below with your BlackBerry. If the application is installed via Desktop Manager (USB) or Blackberry Enterprise Server, this step is not necessary. Again, please make note of your token activation PIN. Your token will be issued to you shortly. <blackberryURL /> Your token activation PIN is: <tokenPIN />
SMS Content	

BlackBerry Token	
Type	Enrollment
Event	Sent to Users receiving BlackBerry token by e-mail. Second of two messages
Subject	SafeNet Authentication Service Blackberry Token
Body	<firstName /> <lastName />: Your new SafeNet BlackBerry token is attached. To install the token, move the cursor to the attached file at the bottom of this message. Click the trackwheel or trackball and then select the Load Token option on the menu. It will pop up the SafeNet BlackBerry token installation wizard and prompt for the user name and activation PIN. Use the activation PIN received in the previous e-mail. If you have not received an activation PIN, contact your HELP Desk.
SMS Content	

Completed Report	
Type	Alert
Event	Sent to recipients receiving reports by e-mail
Subject	SafeNet Authentication Service Report Results
Body	<accountName /> Results of the report <reportName /> are attached.
SMS Content	

Enrollment Lockout	
Type	Alert
Event	Sent when a User exceeds the maximum number of attempts to self-enroll.
Subject	Enrollment Lockout
Body	<accountName />, The user <name /> has been locked out of self enrollment at <dateTime /> because there have been too many failed attempts to enroll.
SMS Content	User <name /> has been locked out of self enrollment

Enrollment Out of Band	
Type	Enrollment
Event	Sent when a User during enrollment of a token provisioned using a shipping authority.
Subject	Enrollment Validation
Body	This email is to validate an ongoing enrollment attempt. Your validation code is <code />. If you are not in the process of enrolling a token, this e-mail can be ignored.
SMS Content	Your enrollment validation code is <code />.

Expired Reservation	
Type	Alert
Event	Sent when a Provisioning Task expires before all Users in the task have completed self-enrollment.
Subject	SafeNet Authentication Service Reservation is Expired
Body	Provisioning task <taskID /> has expired in account <accountName /> with <count /> users still pending enrollment. They will no longer be able to complete enrollment.
SMS Content	Reservation expired for user <userName />

Hardware Assignment Notification	
Type	Alert
Event	Sent when manually assigning a hardware token.
Subject	SafeNet Authentication Service Token Assignment Notification
Body	A hardware token has been assigned <firstName /> <lastName />: <userName /> At: <Uaddress /> <Ucity /> <Uprovince /> <Upostal /> <Ucountry /> In company: <orgName /> At: <Oaddress /> <Ocity /> <Oprovince /> <Opostal /> <Ocountry />
SMS Content	

Hardware Provisioning Notification	
Type	Alert
Event	Sent when auto-provisioning a hardware token.
Subject	SafeNet Authentication Service Token Provisioning Notification
Body	A hardware token has been provisioned <firstName /> <lastName />: <userName /> At: <Uaddress /> <Ucity /> <Uprovince /> <Upostal /> <Ucountry /> In company: <orgName /> At: <Oaddress /> <Ocity /> <Oprovince /> <Opostal /> <Ocountry />
SMS Content	

iPhone Token	
Type	Enrollment
Event	Sent to User enrolling MP-1 on iPhone or iPad.
Subject	Over-The-Air (OTA) Installation for iPhone Device
Body	<firstName /> <lastName />: Follow these 2 easy steps to install the MP-1 token on your iPhone, iPod, iTouch or iPad: Step 1: Tap the icon below to download the MP-1 from App Store. Step 2: Now that the MP-1 is installed, you can click the URL below to install the MP-1 token profile. <otaURL />
SMS Content	The MP-1 token Download URL: <otaURL />

Java ME OTE	
Type	Enrollment
Event	Sent to User enrolling MP-1 on Java phone.
Subject	SafeNet Authentication Service MP Token for Java-enabled Mobile Device
Body	<firstName /> <lastName />: This e-mail will assist you in the Over-the-Air (OTA) installation and activation of your new SafeNet Authentication Service Multi-Platform (MP) token on your Java-enabled Mobile Device. Initial PIN: <tokenPIN /> Download URL: <otaURL />
SMS Content	New SAS MP token: PIN:<tokenPIN /> Download URL: <otaURL />

Java ME USB	
Type	Enrollment
Event	Sent to User enrolling MP-1 on Java phone via USB desktop connection.
Subject	SafeNet Authentication Service MP Token for Java-enabled Mobile Device
Body	<firstName /> <lastName />: This e-mail will assist you in the desktop suite (USB) installation and activation of your new SafeNet Authentication Service Multi-Platform (MP) token on your Java-enabled Mobile Device. Initial PIN: <tokenPIN /> ========== Download Nokia PC Suite: http://www.nokia.ca/get-support-and-software/software/pc_suite/download MP token installation on Nokia Phone: <nokiaHelpURL /> ==========
SMS Content	

Java ME USB	
Type	HAlert
Event	Sent when Service capacity falls below minimum threshold.
Subject	SafeNet Authentication Service License Capacity Warning
Body	This message is a warning that your SafeNet Authentication Service system is nearing its maximum license capacity. Remaining Active Token Capacity: <capLeft /> / <capTotal /> If you require more capacity, contact SafeNet to expand your license.
SMS Content	System Capacity warning: <capLeft /> / <capTotal />

License Expiry	
Type	HAlert
Event	Sent X days before license expires.
Subject	SafeNet Authentication Service License Expiry Warning
Body	This message is a warning that your SafeNet Authentication Service system is nearing its license expiry. Your license expires on <expiryDate />. You have <expiryTime /> day(s) left before SafeNet Authentication Service shuts down. Contact SafeNet to get your license extended.
SMS Content	License expiry warning: Your license expires on <expiryDate />

License Accounts	
Type	Alert
Event	Sent when remaining account capacity falls below minimum threshold.
Subject	SafeNet Authentication Service License Capacity Warning
Body	This message is a warning that your SafeNet Authentication Service system is nearing its maximum account capacity.
SMS Content	

List of Token Users Not Found	
Type	Alert
Event	Lists token(s) no longer associated with users caused when users are removed from external user source before revoking token.
Subject	List of SafeNet Authentication Service Token Users Not Found
Body	The following list contains tokens that have had their state set to <newState /> because the users they were assigned to can no longer be found by SAS. <tokenList />
SMS Content	Tokens have been orphaned in SAS. Log in to see the details.

Low Disk Space	
Type	HAlert
Event	Sent when disk space falls below minimum threshold.
Subject	SafeNet Authentication Service Low Disk Space Warning
Body	This message is to report that the free disk space on system drive <driveLetter /> is low. Details: Time of Report: <dateTime /> Free Space: <freeSpace /> bytes. Disk Size: <diskSize /> bytes. Percentage Free: <percentageFree />
SMS Content	Low disk space warning. <percentageFree />% free on <driveLetter />

Mail Test	
Type	Alert
Event	Sent when testing email/SMTP settings.
Subject	SafeNet Authentication Service E-mail Configuration Test
Body	E-mail configuration is correct if you have received this message.
SMS Content	SMS configuration is correct if you have received this message.

MP PIN	
Type	Enrollment
Event	Sent to users receiving MP-1 token by email. First of two messages.
Subject	SafeNet Authentication Service E-mail Configuration Test
Body	<firstName /> <lastName />: This e-mail will assist you in the installation of your new SafeNet Authentication Service MP token. Please make note of the PIN below, as it is required to activate your token, which will be issued to you shortly. Your token activation PIN is: <tokenPIN />
SMS Content	

Operator E-mail Validation	
Type	Enrollment
Event	Sent to user when promoted to Virtual Server Operator.
Subject	SafeNet Authentication Service E-mail Validation
Body	To activate your Operator account in the SafeNet Authentication Service Authentication Manager you must logon by following the link and using the e-mail address indicated below: Logon link: <consoleLink /> E-mail: <userName />
SMS Content	Welcome to SafeNet Authentication Service. Logon at <consoleLink />

Operator Lockout Alert	
Type	Alert
Event	Sent to Operator when a user account becomes locked. (Account Lockout/Unlock Policy)
Subject	SafeNet Authentication Service User Lockout Alert
Body	Attention: The following user has been locked out of authentication access until <unlockTime />, following <failedAttempts /> consecutive failed logon attempts: Name: <firstName /> <lastName /> Username: <userName /> Account: <organization />
SMS Content	Account <userName /> in organization <organization /> has been locked.

Operator Unlockout Alert	
Type	Alert
Event	Sent to Operator when a user account becomes unlocked. (Account Lockout/Unlock Policy)
Subject	SafeNet Authentication Service User Unlock Alert
Body	Attention: The following user's authentication access has been unlocked: Name: <firstName /> <lastName /> Username: <userName /> Account: <organization />
SMS Content	Account Unlock Alert: User: <userName /> Organization <organization />

Operator Status Change	
Type	Alert
Event	Sent when an Operator's status changes. (active, pending, suspended)
Subject	Operator Status Change
Body	Attention: The following operator's state has been changed to <state /> User Account: <userName /> Account: <accountName />
SMS Content	<organization />: <userName />'s operator status changed to <state />

Organization Capacity	
Type	Alert
Event	Sent when Virtual Server capacity falls below threshold.
Subject	SafeNet Authentication Service Capacity
Body	<accountName /> You are approaching your maximum capacity. <remaining /> left out of <total />
SMS Content	Approaching capacity: <remaining /> left of <total />

Organization SMS Credits	
Type	Alert
Event	Sent when Virtual Server SMS Credits falls below threshold.
Subject	SafeNet Authentication Service SMS Credits
Body	<accountName />, Your available SMS credits are getting low. You have <remaining /> left.
SMS Content	SMS Credits low. <remaining /> left

Provisioning Cancelled	
Type	Alert
Event	Self-enrollment instructions sent to users as part of a provisioning task.
Subject	SafeNet Authentication Service Provisioning Cancelled
Body	<firstName /> <lastName />, your pending token provisioning has been cancelled. The enrollment link you received in a previous email is no longer active.
SMS Content	Your token provisioning has been cancelled.

Push Notification Rejection Internal Operator Alert	
Type	Alert
Event	Sent to the Operator when a user rejects a push notification.
Subject	SafeNet Authentication Service Push Notification Rejection Alert
Body	The user account <userid /> in organization <organization /> denied and reported a push notification: Organization name: <organizationName /> Resource name: <resourceName /> Client IP address: <clientIP /> Location: <clientLocation />
SMS Content	Account <userid /> in <organizationName /> denied and reported a push notification.

Push Notification Rejection User Alert	
Type	Alert
Event	Sent to the user when he rejects a push notification.
Subject	SafeNet Authentication Service Auto-send Rejection Alert
Body	<firstName /> <lastName />, this auto-send authentication request was denied from your <deviceOS /> <deviceType /> device, and reported to your administrator: Organization name: <organizationName /> User ID: <userid /> Resource name: <resourceName /> Client IP address: <clientIP /> Location: <clientLocation />
SMS Content	Auto-send was denied from your <deviceOS /> <deviceType /> device.

SafeNet Authentication Service MP Token	
Type	Enrollment
Event	Sent to Users receiving MP-1 token by e-mail
Subject	SafeNet Authentication Service MP Token
Body	<firstName /> <lastName />: Your new SafeNet Authentication Service MP token is attached. To install, double click on the attached token. This will launch the SafeNet Authentication Service Software Tools installation wizard and prompt you for the activation PIN. Use the activation PIN received in the previous e-mail. If you have not received an activation PIN, or you do not have the SafeNet Authentication Service Software Tools installed, please contact your Help Desk or Administrator.
SMS Content	

Self-Enrollment	
Type	Enrollment
Event	Self-enrollment instructions sent to users as part of a provisioning task.
Subject	SafeNet Authentication Service Self-enrollment
Body	<firstName /> <lastName />: Your self-enrollment account has been created. If you are enrolling a hardware token, and do not have your token yet, please contact your system administrator.
SMS Content	SafeNet Authentication Service Self Enrollment: Enroll at <selfEnrollURL />

Self Service Report Lost Token	
Type	Enrollment
Event	Self-service Confirmation of Lost Token
Subject	SafeNet Authentication Service Self-enrollment
Body	<firstName /> <lastName />: Please click the following link to confirm your lost token report. <url /> If the above link does not work, please copy and paste this url to your web browser. Please confirm your lost token report within the next 10 minutes.
SMS Content	Please click the following link to confirm your lost token report. <url />. Please confirm your lost token report within the next 10 minutes.

Self Service Request Token	
Type	Enrollment
Event	Sent when a user initiated token request is received from self-service.
Subject	Self-service Confirmation of Token Request
Body	<firstName /> <lastName />: Please click the following link to confirm that you requested a token. <url /> If the above link does not work, please copy and paste this url to your web browser. Please confirm your request within the next 10 minutes.
SMS Content	Please click the following link to confirm that you requested a token. <url />. Please confirm your request within the next 10 minutes.

Self Service Temp Password	
Type	Enrollment
Event	Sent when a user requests a sign-in credential for the self-service site.
Subject	Self-service Temporary Sign in Password
Body	<firstName /> <lastName />: Your self-service temporary sign in password is: <password /> Please use this password to sign in within the next 10 minutes.
SMS Content	Your self-service temporary sign in password is: <password />. Please use this password to sign in within the next 10 minutes.

Service Notification	
Type	Alert
Event	Sent when a service notification is enabled by a Service Provider and delivery method is email.
Subject	SAS Service Notification
Body	SAS Service Notification – contents of this message should be changed to reflect the notification.
SMS Content	SAS Service Notification

SIM Service Failed	
Type	Alert
Event	Sent when a SIM/OTA service is unable to provision a user.
Subject	SIM Provisioning Failed
Body	Task <taskID /> to MSISDN <MSISDN /> for user <userName /> has failed after <attempts /> attempt(s).
SMS Content	SAS Service Notification

SIM Service Retry	
Type	Alert
Event	Sent when a SIM/OTA service retries a provisioning task.
Subject	SIM Provisioning requires retry
Body	Task <taskID /> to MSISDN <MSISDN /> for user <userName /> has not been completed after <attempts /> attempt(s). It will be attempted <remaining /> more times.
SMS Content	Task <taskID /> for <userName />@<MSISDN /> has failed after <attempts /> attempt(s).

Sync Notification	
Type	Alert
Event	Sent whenever an LDAP sync task updates the virtual server.
Subject	LDAP Sync notification
Body	The following actions have been processed for <orgName />: The following <totalAdded /> new users have been added: <addList /> The following <totalUpdated /> existing users have been updated: <updateList /> The following <totalRemoved /> users have been removed: <removeList /> The following <totalMarkForRemoval /> users have been marked for deletion: <markedList /> They will continue to exist for 24 hours, during which period they have been marked as disabled. If this was a result of a misconfiguration, fixing the configuration will re-enable the users. Note: If you have deleted a user in LDAP, re-creating a new user with the same user name will NOT restore the existing user.
SMS Content	Task <taskID /> for <userName />@<MSISDN /> has failed after <attempts /> attempt(s).

Token Request Ack	
Type	Enrollment
Event	Sent to user to acknowledge request to be issued a token.
Subject	SafeNet Authentication Service Token Request Acknowledged
Body	This message is to confirm that your request for a <tokenType /> token has been received as of <time />.
SMS Content	Your request for a SAS token has been received.

Token Request Deny	
Type	Enrollment
Event	Sent to user when request to be issued a token is denied.
Subject	SafeNet Authentication Service Token Request Denied
Body	This message is to inform you that your request for a <tokenType /> token has been denied.
SMS Content	Your request for a SAS token has been denied.

Token User Not Found	
Type	Alert
Event	Sent when token state is change when the user to which it was assigned is not found.
Subject	SafeNet Authentication Service Token User Not Found
Body	The token <serial /> which was assigned to user <userName /> has been changed from state <oldState /> to <newState /> This has occured because the user <userName /> can no longer be found by SAS.
SMS Content	Token <serial /> has been orphaned as user <userName /> cannot be found.

Token User Replaced	
Type	Alert
Event	Sent when a User (UserID) with an assigned token is overwritten with an user from a different user source with an identical UserID. For example, a manually created userID is overwritten during LDAP synchronization which includes an identical UserID.
Subject	SafeNet Authentication Service Token User Replaced
Body	The token <serial /> which was assigned to user <userName /> has been changed from state <oldState /> to <newState /> This has occured because the user <userName /> has been overwritten by a new user <userName />.
SMS Content	Token <serial /> orphaned because user <userName /> was over written.

Token Request Approval 2	
Type	Enrollment
Event	Sent to Approver 2 Authorities when a token request is approved by an Approver 2 Authorities (if enabled)
Subject	<productName /> Self-service token request
Body	LEVEL 2 APPROVAL The following user has requested a token in <accountName />. User: <userName /> First Name: <firstName /> Last Name: <lastName /> E-mail: <email /> Token type requested: <typeRequested /> To approve this request click on this link: <approveURL />. To reject this request click on this link: <rejectURL />. This request can also be approved or rejected by logging into the SAS Manager.
SMS Content	Self-service token request <taskID />. Click URL or logon to approve or reject.

Token Request Issuer	
Type	Enrollment
Event	Sent to Issuing Authorities when a token request has all necessary approvals.
Subject	<productName /> Self-service token request
Body	The following user has requested a token in <accountName />. User: <userName /> First Name: <firstName /> Last Name: <lastName /> E-mail: <email /> Token type requested: <typeRequested /> To issue this request click on this link: <issueURL />. This request can also be issued by logging into the SAS Manager.
SMS Content	Self-service token request <taskID />. Click the URL or logon to issue or reject.

Token Request Receipt	
Type	Enrollment
Event	Sent to the requesting user to confirm receipt of the request from the self-service site.
Subject	<productName /> Token request receipt notification
Body	REQUEST RECEIPT PROCESSING <firstName /> <lastName />, Your request for a token has been received and is awaiting approval. Your request will be processed within the next <expireLength /> days.
SMS Content	Your request for a token has been received.

Token Request Shipper	
Type	Enrollment
Event	Sent to the shipping authority once the token request has received the Issuing Authority approval (if enabled.)
Subject	<productName /> Self-service token request
Body	The token for the following request needs to be shipped in <accountName />. User: <userName /> First Name: <firstName /> Last Name: <lastName /> E-mail: <email /> Token type requested: <typeRequested /> After the token required for this request has been shipped, the request can be marked as shipped by logging into the SAS Manager.
SMS Content	Self-service token request <taskID /> ready for shipping.

Token Request Validation	
Type	Enrollment
Event	Sent to the requesting user to require their confirmation of a request for a token from the self-service site.
Subject	Token Request Validation
Body	<P>Click on the link below or paste link into a browser to validate your token request.</P> <P>Requests that are not validated with <Days /> are automatically rejected.</P> <P>Validation URL: <URL /></P>
SMS Content	Go to <URL /> to validate token request.

Token Sub Capacity	
Type	Alert
Event	Sent when remaining quantity of tokens in inventory falls below the minimum threshold.
Subject	SafeNet Authentication Service Token Capacity
Body	<accountName />, You are approaching your remaining capacity available to you. <remaining /> left out of <total />
SMS Content	Approaching capacity: <remaining /> left of <total />

User Lockout Alert	
Type	Alert
Event	Sent to user when their account becomes locked due to excessive failed consecutive logon attempts
Subject	SafeNet Authentication Service User Lockout Alert
Body	<accountName />, You are approaching your remaining capacity available to you. <remaining /> left out of <total /<firstName /> <lastName />, you have been locked out of authentication access until <unlockTime />, following <failedAttempts /> consecutive failed logon attempts.
SMS Content	Your SAS account has been locked until <unlockTime />

User Unlock Alert	
Type	Alert
Event	Sent to user when their account becomes unlocked.
Subject	SafeNet Authentication Service User Unlock Alert
Body	<firstName /> <lastName />, you can again attempt to logon to the authentication service.
SMS Content	Your SAS account has been unlocked.

Windows Phone 7 Token	
Type	Enrollment
Event	Sent to User enrolling MP-1 on Windows Phone 7 device.
Subject	Over-The-Air (OTA) Installation for Windows Phone 7 Device
Body	<firstName /> <lastName />: Follow these easy steps to install the MP-1 token on your Windows Phone 7 device: Step 1: Tap the icon below to download the MP-1 from Windows Phone Marketplace. Step 2: Now that the MP-1 is installed, please complete the following steps: 1. Copy the code below by tapping it, and then drag the arrows at each end of the highlighted text to include the first and last characters, up to and including the trailing BSID characters at the end of the code. <otaURL /> 2. Tap Copy. 3. Open the MP-1, and then tap the Import button. 4. Tap inside the text box and then tap the Paste button to paste the download code. 5. Tap the Done button to complete the installation of the token.
SMS Content	The MP-1 token Download code: <otaURL />