All information herein is either public information or is the property of and owned solely by Gemalto 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.

© 2018 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto 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.

**Document Number:** 007-012402-002, Rev. F

**Release Date:** January 2018
## Contents

### Preface
- Audience ................................................................................................................................. 5
- Terminology ................................................................................................................................. 5
- Support Contacts .......................................................................................................................... 6
  - Customer Support Portal ........................................................................................................... 6
  - Telephone Support ...................................................................................................................... 7

### 1 Overview ................................................................................................................................. 8

### 2 Self-Service Site ......................................................................................................................... 10
- Self-Service Site Appearance ...................................................................................................... 11
- Inheritance ....................................................................................................................................... 12
- Service Configuration ...................................................................................................................... 12
- Languages ........................................................................................................................................ 13
- Authorities ......................................................................................................................................... 13
- Workflow .......................................................................................................................................... 13
- Provisioning Tasks ............................................................................................................................ 13
- Reporting .......................................................................................................................................... 14

### 3 Configuring Self-Service .............................................................................................................. 15
- Self-Service Policy ........................................................................................................................... 16
- Set Customization Inherit ............................................................................................................... 16
- Configure Self-Service Appearance ................................................................................................ 16
- Configure Self-Service Buttons and Icons ...................................................................................... 18
- Configure Self-Service Fonts ............................................................................................................ 19
- Configure Self-Service Modules ..................................................................................................... 20
  - Self-Service Module Options ...................................................................................................... 20
  - Language Set .................................................................................................................................. 21
  - Default Elements ............................................................................................................................ 22
  - My Profile ...................................................................................................................................... 23
  - Request a Token .............................................................................................................................. 28
  - Reset PIN ....................................................................................................................................... 35
  - Reset PIP ........................................................................................................................................ 39
  - Resync Token ................................................................................................................................. 40
  - Resend SMS .................................................................................................................................... 43
  - Sign In ............................................................................................................................................. 44
- Configure Self-Enrollment Pages ..................................................................................................... 48
  - Default/Common Page ..................................................................................................................... 48
  - Software Token Page ....................................................................................................................... 49
  - Custom Token Page .......................................................................................................................... 50
Contents

Hardware Token Page ........................................................................................................................... 51
Password Page ...................................................................................................................................... 52
MobilePASS Page .................................................................................................................................. 53
Self-Service Authorities .......................................................................................................................... 54
Configuring Authorities ........................................................................................................................... 55
Out-of-Band Enrollment .......................................................................................................................... 56
Request and Approval Queue Processing ............................................................................................... 57
Configure Request and Approval Queue Processing ............................................................................ 57
Language ...................................................................................................................................................... 58

4 Queue Management .............................................................................................................................. 59
Token Requests Report .......................................................................................................................... 60
Preface

This guide describes the self-service functionality of the SafeNet Authentication Service (SAS) platforms. It describes all of the processes required to:

- Customize the Self-Service site
- Automate workflow related to fulfilling user requests for tokens/authentication methods
- Generate, schedule, and automatically deliver relevant reports to workflow and security stakeholders

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 responsible for how managed authentication services are delivered to accounts, and for configuring SAS to reflect the Service Provider’s internal business processes, Service Level Agreements, and management hierarchy.

Terminology

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SafeNet Authentication Service Platforms</td>
<td>This term refers to the capability of the application software used in the SafeNet’s Cloud service, Service Provider Edition used by service providers to delivery their own cloud authentication service and by Enterprises for SPE/PCE requirements for internal use and/or extension to enterprises and individuals with whom they interact (Private Cloud).</td>
</tr>
<tr>
<td>Virtual Server</td>
<td>This term refers to an individual Enterprise’s authentication service delivered by SafeNet Authentication Service (Cloud).</td>
</tr>
<tr>
<td>Subscriber</td>
<td>When presented in all lowercase, the term “subscriber” applies to all accounts that you create and manage. When presented with initial caps, the term “Subscriber” refers to accounts that are not Service Providers.</td>
</tr>
<tr>
<td>Service Providers</td>
<td>These are accounts that, in addition to having their own Virtual Server, are able to create and manage additional accounts.</td>
</tr>
<tr>
<td>Virtual Service Providers</td>
<td>These are service provider accounts that have a service provider as a parent.</td>
</tr>
</tbody>
</table>
Support Contacts

If you encounter a problem while installing, registering, or operating this product, refer to 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.

Customer Support Portal

The Customer Support Portal, at https://supportportal.gemalto.com, is a where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

NOTE: You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the REGISTER link.
# Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Customer Support by telephone. Calls to Customer Support are handled on a priority basis.

<table>
<thead>
<tr>
<th>Region</th>
<th>Telephone number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>+1-410-931-7520</td>
</tr>
<tr>
<td>Australia</td>
<td>1800.020.183</td>
</tr>
<tr>
<td>China</td>
<td>North: 10800-713-1971</td>
</tr>
<tr>
<td></td>
<td>South: 10800-1301-932</td>
</tr>
<tr>
<td>France</td>
<td>0800-912-857</td>
</tr>
<tr>
<td>Germany</td>
<td>0800-181-6374</td>
</tr>
<tr>
<td>India</td>
<td>000.800.100.4290</td>
</tr>
<tr>
<td>Israel</td>
<td>180-931-5798</td>
</tr>
<tr>
<td>Italy</td>
<td>800-786-421</td>
</tr>
<tr>
<td>Japan</td>
<td>0066 3382 1699</td>
</tr>
<tr>
<td>Korea</td>
<td>+82 2 3429 1055</td>
</tr>
<tr>
<td>Netherlands</td>
<td>0800.022.2996</td>
</tr>
<tr>
<td>New Zealand</td>
<td>0800.440.359</td>
</tr>
<tr>
<td>Portugal</td>
<td>800.863.499</td>
</tr>
<tr>
<td>Singapore</td>
<td>800.1302.029</td>
</tr>
<tr>
<td>Spain</td>
<td>900.938.717</td>
</tr>
<tr>
<td>Sweden</td>
<td>020.791.028</td>
</tr>
<tr>
<td>Switzerland</td>
<td>0800.564.849</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>0800.056.3158</td>
</tr>
<tr>
<td>United States</td>
<td>(800) 545-6608</td>
</tr>
</tbody>
</table>
The SafeNet Authentication Service (SAS) **Self-Service** site enables organizations to:

- Empower users to perform simple authentication management functions, such as resetting PINs and viewing authentication history, which helps to reduce the workload and user reliance on the help desk.

**NOTE:** To report a lost token, users must contact their administrator or help desk.

- Invite users to request a token. This is particularly useful for organizations servicing consumers of online subscription services. Users can now request a token as part of their subscription for other services.
- Create a customized yet automated workflow for approving token requests, and fulfilling and shipping tokens to users.
- Offer a complete user-centric service, including multi-language support, customized prompts, messages, help, and navigation—all optimized for the user based on how they are interacting with self-service (browser type, screen resolution etc.).

Self-service functionality is exposed by the SafeNet Authentication Service platform as a web service (WSDL), giving developers the tools necessary to build some or all of the self-service functionality into a corporate portal. For more information about the self-service WSDL, contact SafeNet or your local vendor.

Typically, authentication self-service has been limited to extending some token management functionality to “users”; specifically, PIN management, OTP resend, and token resync. The focus is almost always “token-centric”, assuming that all users are the same, have tokens, and that the only issues self-service need resolve are token-related. In fact, many enterprises want to extend self-service functionality to people that:

- May or may not have tokens. In many organizations, the idea that users should be able to request a token (and/or services) makes sense, perhaps as part of some other service to which the user is subscribing. The concept then is “pull”.
- May or may not be known to the organization. Commonly, users belong to an organization. But this is not always the case. At a simple level, external parties, such as contractors or business partners, may require the service. The separation between the enterprise and the possible user community may broaden. Think of a user becoming a subscriber to your service for the first time. Until they sign up and are approved, the user is completely unknown. Therefore, self-service must accommodate communities that may become legitimate users of the service but are unknown to the service provider prior to “signing-up.”
- May have very diverse requirements, not the least of which is language. It’s difficult to contemplate providing a “global” self-service capability without considering the diversity of the community. It is very unlikely that users will all speak the same language or that hardware tokens shipped from Toronto will arrive in Montreal...
and Shanghai in the same timeframe. In other words, self-service needs to accommodate diversity in such a way as to maximize the simplicity of the user experience, regardless of language, logistics, and authentication method.

It is quickly apparent that the “pull” world demands a new set of tools by which administrators of authentication services can extend self-service functions to current and potential users, determine the validity of requests, how each is to be handled and how, throughout the process, the user is kept informed.

The key elements to producing an effective and highly marketable self-service capability depend on:

- Ensuring that the approval process reflects the enterprise’s desired workflow
- Sufficient visibility at all stages of the workflow as to the status of a request
- Effective and simple workflow and communication with the user

All self-service functionality, from what is presented to the user to back-office workflow, is configured through the Self-Service tab of the SAS Management Console.

Self-service then is best viewed as three functional areas:

- The Self-Service website, through which users perform common functions.
- Presentation services, through which administrators customize the services, languages, and other aspects of self-service presented to users on the Self-Service site.
- Back-end workflow, through which administrators manage the services presented to users through the Self-Service website.
Self-Service configuration and management is performed from **Virtual Servers > Self-Service**:

- **Configuring Self-Service**—Provides access to all of the functions related to customizing the site for appearance, user services, and back-office workflow, including approving and fulfilling user requests for tokens.

- **Queue Management**—Provides lists of outstanding tasks related to user requests for tokens. Operators with appropriate “authorities” can view and process requests for tokens.

![Figure 1: Self-Service Tab](image-url)
The **Self-Service** site can present users with the following services:

<table>
<thead>
<tr>
<th>Service</th>
<th>Default Icon</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Request a Token</strong></td>
<td>![Token Icon]</td>
</tr>
<tr>
<td>This service allows users to request a token by type from a list of approved token types and authentication methods. This service accommodates both existing users, as well as creation of new user accounts. This service is not published by default.</td>
<td></td>
</tr>
</tbody>
</table>

| **Reset PIN** | ![PIN Icon] |
| This service allows users to modify their server-side PIN without the assistance of the help desk. PIN changes must comply with the PIN policy. This service is published by default. |

| **Reset PIP** | ![PIP Icon] |
| This service allows users to modify the PIP (personal identification pattern) associated with their GrID authentication method without the assistance of the help desk. The new PIP must comply with the PIP policy. This service is published by default. |

| **Resync Token** | ![Resync Icon] |
| This service allows users to test and resync their token with the server without the assistance of the help desk. This service is published by default. |

| **My Profile** | ![Profile Icon] |
| This service can allow users to modify basic information about their account such as address, telephone number, etc. It also presents basic statics about their authentication activity and allows them to manage challenge/response questions valid (if enabled) for sign-on to the Self-Service site. This service is not published by default. |

| **Resend SMS** | ![Resend SMS Icon] |
| This service allows a user to request an SMS/OTP resend to their registered mobile device. |

**Self-Service Site Appearance**

The Self-Service site is highly customizable within each virtual server. This includes:

- Navigation and other buttons
- Logos and icons
- Fonts
- Colors
Inheritance

By default, when a Subscriber account is on-boarded, (for example, a child account created by the Service Provider), it inherits all customizations applied to the Service Provider’s Self-Service site. Subscriber accounts can override these customizations and independently configure their Self-Service site.

Figure 2: Self-Service Site Inheritance

To override default or Service Provider customizations:

1. Click Virtual Servers > Self-Service > Configuring Self-Service > Set Customizations Inherit.
2. De-select User Inherit Customizations and then click Apply.

To revert to the default site settings which do not inherit from the Service Provider customizations, select the option and then click Apply to commit the change.

Service Configuration

The user options and supported languages for each service are configured independently.

Figure 3: “Request a Token” Service Configuration Example
Languages

The Self-Service site can be configured to provide services in any number of languages. The default service is based on an English language set. Administrators can create additional language sets using the English set as a guide.

Authorities

Authorities are special privileges assigned to Operators for the purpose of managing user requests for tokens received from the Self-Service site. There are four possible Authorities:

- **Approval Level 1**—This Authority approves or denies user requests for tokens received from the Self-Service site. At least one Operator must have this Authority if the Request a Token service is enabled on the Self-Service site.
- **Approval Level 2**—This Authority approves or denies user requests for tokens that have been approved by Approval Level 1 authorities. This is an optional Authority.
- **Issuing Authority**—Requests for tokens that have received the required approvals are fulfilled by the Issuing Authority. This function is the equivalent of using the Provision functions available on the Assignment tab unless a Shipping Authority has been created. At least one Operator must have this authority if the Request a Token service is enabled on the Self-Service site.
- **Shipping Authority**—The Shipping Authority is a special function that serves two purposes:
  - It can be used to coordinate the delivery of enrollment instructions with receipt of the physical token by the user.
  - It can be used to increase the security of enrollment by requiring the user to provide an additional code during enrollment that is delivered separately and out-of-band (“OOB”) with respect to all other enrollment instructions.

Shipping authorities are applied by token type. Token requests for affected token types that have been approved by the Issuing Authority must be completed by the Shipping Authority. This is an optional authority.

Workflow

Requests for tokens include workflow that incorporates appropriate messaging and alerts for the users making requests for tokens and for each Authority involved in the approval and fulfillment process. Alerts and messages can be customized and sent by email and/or SMS. In addition, all requests can be viewed and managed from the Queue Management module.

Provisioning Tasks

A provisioning task is created for each fulfillment. Tasks can be viewed by clicking the Provisioning Tasks link in the Shortcuts section on the Assignment tab. A provisioning task shows the date the enrollment reservation was created, the date by which enrollment must be completed, and the status of the enrollment. Tasks may be cancelled or modified prior to user enrollment, and an alert can be generated for expired enrollments. For more information on provisioning tasks, refer to the SAS Service Provider Administrator Guide.
**Reporting**

All self-service requests for tokens and subsequent processing by authorities are available in reports (Reports tab) including:

- **Provisioning Task Attempts**—Reports details of attempts to use provisioning tasks by users.
- **Provisioning Tasks**—Reports details of provisioning tasks.
- **Provisioning Tasks – Outstanding**—Lists all outstanding provisioning tasks.
Configuring Self-Service

Virtual Servers > Self-Service > Configuring Self-Service includes the following tasks:

- Self-Service Policy—View or modify the Self-Service site’s unique URL.
- Set Customization Inherit—Override site customizations inherited from the Service Provider or revert to default settings.
- Configure Self-Service Appearance—Configure the overall site “look and feel”, including colors, logos, and banner images.
- Configure Self-Service Buttons and Icons—Modify navigation items, such as buttons, button text, and icons.
- Configure Self-Service Fonts—Select font types and styles used throughout the site.
- Configure Self-Service Modules—Customize each of the services published to the Self-Service site, including language sets, required/optional fields, and user help and instructions.
- Configure Self-Enrollment Pages—Customize instructions presented to the user during token enrollment. Instructions and messages can be created independently for each token type.
- Self-Service Authorities—Add one or more Authorities to Operators.
- Out-of-Band —Require an additional authentication factor during enrollment, delivered to the user “out of band”.
- Request and Approval Queue Processing—Customize the message content and delivery method provided to users that have requested a token and to Authorities.
- Language—Select the Self-Service default language.
Self-Service Policy

This section defines the base and unique URLs for the Self-Service site (see Figure 4). These URLs are automatically created when the virtual server account is activated. Do not modify these URLs unless you want to link to an alternate, stand-alone Self-Service site.

The **Self-Service Unique URL** must be provided to users; clicking the link displays the Self-Service Home page (see Figure 6).

![Image](https://example.com/image.png)

**Figure 4: Self-Service Policy URL**

Set Customization Inherit

Use this section to either accept or override customizations inherited from the Service Provider site. To override the settings on the Service Provider site, clear the **Use Inherit Customizations** option and then click **Apply**.

![Image](https://example.com/image.png)

**Figure 5: Self-Service Customization Option**

Configure Self-Service Appearance

Use **Virtual Servers > Self-Service > Configuring Self-Service > Configure Self-Service Appearance** to change the colors and logos used on the Self-Service site. The options include:

- **Self-Service Logo**—The logo that displays at the top-center of Self-Service site. Format: png, jpg, or gif. Dimensions: 387 x 70 pixels.
- **Logo Background Color**—The color behind the logo; spanning the width of the page. Dimensions: page width x 70 pixels.
- **Banner Image**—The image in the banner area, which includes the navigation buttons. Dimensions: page width x 80 pixels.
- **Banner Color**—The color behind the banner image; spanning the width of the page. Dimensions: page width x 80 pixels.
- **Homepage Background**—The image on the home page background. Dimensions: page width x 80 pixels (max).
- **Homepage Color**—The color displayed behind the Homepage Background image.
- **Page Background**—The background image used on all pages other than the home page.
- **Page Color**—The color displayed behind the Page Background image on all pages other than the home page.
• **Language Icon**—An optional icon displayed in the page footer to provide language selection options on the page.

• **Help Text Background**—The background color for help text.

• **Error Text Background**—The background color for error messages.

• **Input Field Border Color**—The color of the border surrounding input fields.

• **Input Field Background Color**—The background color for input fields.

Go to Virtual Servers > Self-Service > Configuring Self-Service > Self-Service Policy and click on the Self-Service Unique URL to display the Self-Service Home page and view the effect of your settings (see Figure 6).

![Figure 6: Self-Service Home Page Example](image)

From the Self-Service Home page, click on any one of the service icons (for example, **My Profile**) to display the service page and view the effect of your **Page Background** and **Page Color** settings (see Figure 7).

![Figure 7: Self-Service <Service> Page Example](image)
Configure Self-Service Buttons and Icons

Use this section to change the buttons and icons used on the Self-Service site:

- **Small Button**—Used for navigation throughout the site. Button images can be uploaded, selected from a list of available buttons, or configured as an HTML button. Dimensions 120 x 28 pixels.
- **Button Text**—Select the font, size, color, and weight for the text on small buttons.
- **Button Hover Text**—Modify the appearance of the button text when hovering over the button.
- **Large Button**—Some options, such as choosing the type of token, use a large button. Button images can be uploaded, selected from a list of available buttons, or configured as an HTML button. Dimensions: 400 x 28 pixels.
- **Icons**—Service icons can be replaced with uploaded images. Format: png, jpg, or gif. Dimensions: 100 x 100 pixels.
- **Language Icon**—The language icon can be replaced with an image or text. Dimensions: 96 x 20 pixels.

![Configure Self-Service Buttons and Icons](image)

Figure 8: Configure Self-Service Buttons and Icons
Configure Self-Service Fonts

Use this section to change the fonts used on the Self-Service service pages.

- **Site Title**—The title displayed in the banner area.
- **Page Title**—The title below the banner area and to the left of the | separator.
- **Page Service**—The title below the banner area and to the right of the | separator.
- **Field Label**—The font used throughout the site for field labels.
- **Help Text**—The font used in help panels.
- **Error Text**—The font used for error messages.
- **Footer Text**—The font used in the footer.

![Configure Self-Service Fonts](image)

**Figure 9: Configure Self-Service Fonts**
Configure Self-Service Modules

This section describes how to configure the Self-Service services: Default Elements, My Profile, Request a Token, Reset PIN, Reset PIP, Resync Token, Resend SMS, and Sign In. These options and services are located at Virtual Servers > Self-Service > Configuring Self-Service > Configure Self-Service Modules.

Self-Service Module Options

A service is published to the Self-Service site if it is enabled. Referring to Figure 10:

- **Enable <Service Name>**—To change the publication status of a service, select or clear the Enable option and then click Apply.

- **Require the User to Sign in**—For security reasons, some services, such as My Profile or Change PIN, should require the user to authenticate before access is granted. To require authentication, select this option and then click Apply.

- **Use Page – (not shown)**—Most services contain several pages; however depending on your requirements, it may not be necessary to publish all pages. For example, the My Profile service includes pages that display token requests made by the user. As this is an information page only, it is not necessary to publish the page.

- **Show Help**—Help is available for most pages; however, it can be removed from the site by clearing this option.

- **Required – (not shown)**—Some pages, such as My Profile, allow users to input or update information. The Required option, if enabled, requires the user to enter data into the field. If this option is not selected, the field is not displayed.

Figure 10: Self-Service Module Options
Language Set

This section supports the viewing and creation of multiple language sets for each of the Self-Service services, and all of the pages, error messages, and help text available with each service.

To view a language set, select it from the language list, and then click View.

To add a language set, type the name for the set in the Language set field, and then click Add. Next, modify all of the labels, default text, help text, and error messages for each of the pages in the service. For example, to create a French language set:

1. Add French to the list.

2. Select a service from the Module list.
3. Select a page from the Pages list and then modify the text and labels.

4. Click Apply to save the set. Repeat steps 2 and 3 until all pages have been modified.
Default Elements

This module has only one page and includes the basic information presented on the Self-Service home page. User access to customized Terms of Use policies and documentation can be provided by placing these on a publicly accessible location and updating the corresponding URLs in this module.

The **Language** icon can be replaced with text or a custom image (see Figure 6).

The **Help Desk** link in the footer area should contain information that assists the user in contacting your help desk for assistance.

Figure 11: Default Elements Module
**My Profile**

This service enables users to modify basic information about their account such as address and telephone number. It also presents basic statistics about their authentication activity and enables them to manage challenge/response questions valid (if enabled) for sign on to the Self-Service site. There are five pages in this service. Each service contains a section for error messages and/or help text.

This service requires sign in to the self-service site.

**Select to Proceed Page**

This is the first page displayed when My Profile is selected by the user.

**View my Logon Statistics**

This displays information about authentication activity by the user including last logon date, number of logons: today, this week this month and this year. This page can be unpublished.
View and Update my Profile

The user can update basic personal information that is stored in the virtual server. Note that this service cannot be used to update information obtained by the virtual server from an external user source such as LDAP. Only users that have been manually created or imported from a flat file can update their information through this service.

This service lists the fields that will accept user input. Some are mandatory (no options), others can be required (made mandatory). It also contains sections for customizing error messages and adding help text relevant to this page.

Figure 14: View and Update My Profile
Update my Security Questions and Answers

Security Questions and Answers can be used as an alternative sign-in method for the self-service site. This service allows the administrator to create a series of questions. The user will be required to create a set of answers to these questions. During sign-in the user will have the option of supplying the previously recorded answers to the questions as an alternative sign-in method if this method is enabled. This page can be unpublished.

![Figure 15: Update my security Questions and Answers](image)

Question Management Page

Use this page to create questions from which the user will select as an alternate self-service site sign in method.

![Figure 16: My Profile Service | Update my security questions and answers | Question Management](image)
In this service:

- **Question Management Dropdown**
  This dropdown provide access to three pages used to configure security question and answers:
  
- **Question Management**
  Use this page to create questions.

Use the **Edit** button to modify a highlighted question from the defined question list, including the minimum and maximum answer length, case sensitivity and trivial answer control options.

Use the **Add** button to add a question created in the **Question** field to the **Defined Questions** list.

### Question Sets Page

Use this page to define the number of question groups that will be displayed to the user. Users must answer one question from the list of questions contained in a Question Set.

![Figure 17: My Profile Service | Update my security questions and answers | Question Sets](image)

Use the arrows to add or remove question sets to or from the **Defined Question Sets** list. Sets in this list are displayed to the user.
Question Assignment

Use this page to group questions created in Question Management into one or more of the sets enabled in Question Sets.

![Figure 18: My Profile Service | Update my security questions and answers | Question Assignment](image)

To add one or more questions to a set, select the set from the dropdown list, then using the arrows move the questions to be included in the set to the Questions in Sets list, then click the Update button to commit the change.

- Minimum answer length
  Sets the minimum number of characters allowed as an answer.

- Maximum answer length
  Sets the maximum number of characters allowed as an answer.

- Answers are case sensitive
  If checked, answers are case sensitive.

- Disallow trivial answers
  If checked, answers comprised of triplets (for example, 111, aaa) or 3 character sequential strings (for example, 123, abc) are disallowed.

Use the Add button to add questions to the list. To edit or remove a question, highlight it in the list then click the Edit or Remove button respectively.

My Token Request

This page displays a list of outstanding token requests.
Request a Token

This service provides the ability for a user to request a token. It is also where outbound messages to users and authorities are configured. To make this service available on the Self-Service site, the following must be in place:

- The virtual server must have at least one Operator.
- **Enable Request a Token** must be selected here and under the **Self-Service Authorities** service.

Although both options must be enabled for the **Request a Token** button to be available on the Self-Service site, enabling the option here (under the **Request a Token** service) allows you to show or hide the **Request a Token** button on the home page on the Self-Service site. However, it has no effect on the function itself, which will continue to run while the same option is enabled under **Configuring Self-Service > Self-Service Authorities**. Hiding the button simply prevents users from requesting new tokens, allowing administrators time to process existing requests that are currently in the token request queue.

**Figure 19: Request a Token Page**

There are six (6) pages in this service:

- User Type Page – page 29
- Create Account Page – page 30
- Token Type Page – page 31
- Confirmation Page – page 32
- Validation Page – page 33
- User Page – page 33
User Type Page

This is the first page presented to the user when accessing this service. Users that have an account and an assigned authentication method, such as a token, can sign in to the Self-Service site and request an additional token.

This page also allows users that do not have an account in the virtual server to create an account (pending approval) as part of the token request process.

Figure 20: Request a Token - User Page
Create Account Page

If enabled, the user will be able to submit a request to create an account in the virtual server during the “request a token” process. The request must be approved by Approval Level 1 (and Approval Level 2 if enabled) before the account is created.

Figure 21: Request a Token - Create Account Page

The fields **First Name**, **Last Name**, **User ID**, and **E-mail address** are mandatory if this page is enabled. Other fields can be displayed by selecting the corresponding **Required** option.

To unpublish (hide) the **Create Account** page, clear the **Use Page** option.
Token Type Page

This page displays a list of token types that may be requested by the user. Each type in the list has a corresponding enrollment class. For example, the MP for iPhone/iPad would use the **Software** enrollment class. The class selection determines which notification and enrollment instructions the user will receive for the selected token type.

![Token Type Page](image)

**Figure 22: Request a Token - Token Type Page**

To publish or unpublish a token type, select or clear the corresponding field option respectively, and then click **Apply**.

**To add a token type:**

1. Click the **Add Token Type** button.
2. Enter a description and select a class from the list.
3. Select the **Field** option.
4. Click **Apply**.
Confirmation Page

The **Confirmation** page is used to configure messages that are displayed to the user immediately following token selection.

![Confirmation Page](image)

**Figure 23: Request a Token - Confirmation Page**

Only one of the messages will display, corresponding to the type of validation required/available.
Validation Page

The Validation page is used to configure messages that will be displayed to the user for token validation. If enabled, the user must confirm their request for a token by replying to a message delivered to them via email and/or SMS. To enable or disable the validation requirement, select or clear the Use Page option and then click the Apply button.

![Figure 24: Request a Token - Validation Page](image)

User Page

This page is displayed when the user selects the I am an Existing User option. It requires the user to provide their User ID when signing in to the Self-Service site.

- **User ID**: The label for the User ID input field.
- **Error**: The error message displayed if the User ID is not valid.
- **Next**: Text for the Next button.

![Figure 25: Request a Token - User Page](image)
Figure 26: Request a Token Workflow
Reset PIN

This service provides the ability for a user to reset the server-side PIN associated with a token assigned to them. There are five (5) pages in this service. Each page contains a section for error messages and/or help text.

User Page

This is the content of the first page served to the user when accessing the Reset PIN facilities. If the page is set to require the user to sign in, they will be directed to the Sign In page before being presented with the User page.

![Figure 27: Reset PIN - User Page](image)
Select a Token Page

If a user has more than one token, this page provides a list from which the user can select the token. PIN reset applies to the selected token.

Figure 28: Reset PIN - Select a Token Page
Create New PIN Page

This page is presented when the user has supplied their UserID and the serial number of a token assigned to their account and the PIN associated with the token allows the user to generate a new PIN (for example, server-side, user select). It requires the user to enter and verify a new PIN.

Figure 29: Reset PIN - Create New PIN Page
Server-side PIN Page

This page is displayed if the token issued to a user requires a server-side PIN that is set by the server (for example, server-side, server select).

![Server-side PIN Page](image)

Figure 30: Reset PIN – Server-side PIN Page

Confirmation Page

This page is presented when the user has successfully changed their PIN.

![Confirmation Page](image)

Figure 31: Reset PIN - Confirmation Page
Reset PIP

This service provides the ability for a user to reset the PIN associated with their GrID authentication method. There are three pages in this service. Each page contains a section for error messages and/or help text.

User Page

This is the first page displayed to the user when accessing the Reset PIP facilities. If the page is set to require the user to sign in, they are directed to the Sign In page before being presented with the User Page.

If directed to sign in, the user should only provide their UserID. If an OTP field is displayed on the sign in page, it should be left blank. A valid userID and empty OTP field will generate a new page with a GrID and OTP field, allowing the user to authenticate and sign in.

![Figure 32: Reset PIP - User Page]

Select Pattern Page

This page displays for a valid UserID provided on the User page and requires the user to provide their PIP.

![Figure 33: Reset PIP - Select Pattern Page]
Confirmation Page

The confirmation page is presented on successfully resetting a PIP.

![Confirmation Page](image)

**Figure 34: Reset PIN - Confirmation Page**

Resync Token

This service provides the ability to resync a token with the server and confirm the ability to authenticate with the token. There are six (6) pages in this service. Each page contains a section for error messages and/or help text.

User Page

The user page is served up to the user in two parts—the first requires the UserID, which, if found on the server, generates the second part requesting the token serial number.

![User Page](image)

**Figure 35: Resync Token - User Page**
Auth Resync Page

This page is presented when the selected token supports resynchronization using two consecutive OTPs.

![Auth Resync Page](image)

Figure 36: Resync Token - Auth Resync Page

Time-based Resync Page

This page is presented when the selected token is time-synchronous and supports resynchronization using two consecutive OTPs.

![Time-based Resync Page](image)

Figure 37: Resync Token – Time-based Resync Page
3 – Configuring Self-Service

**Challenge/Response Page**

The challenge/response page is presented when a token fails resynchronization using all other available methods. In this method the user must key the displayed challenge into their token to generate a passcode or “response”, and then enter the response in the indicated field.

![Challenge/Response Page](image)

**Figure 38: Resync Token - Challenge/Response Page**

**Confirmation Page**

The confirmation page displays the outcome of the synchronization attempt whether successful (Confirmation), failed (Error) or not processed (No Token Error).

![Confirmation Page](image)

**Figure 39: Resync Token - Confirmation Page**
Resend SMS

The Resend SMS page enables a user to send a new SMS Token code to their mobile device.

Figure 40: Resend SMS - User Page
Sign In

This service controls the options for signing into the self-service site. There are five (5) pages in this service. Each page contains a section for error messages and/or help text. The Sign In button is replaced with a Sign Out button when a user successfully authenticates to the Self-Service site.

Authenticate Page

This page presents the allowed methods for authenticating into the Self-Service site. The remaining pages in this service provide the user experience and process necessary for the method selected by the user.

Figure 41: Sign In - Authenticate Page
Authenticate to Process Page

This page handles authentication using tokens, grids and static passwords. It includes additional prompts to deal with authentication exceptions. In most cases a user authenticating using a token will provide their OTP and gain access to the site. However, it is possible that another policy will be triggered altering this workflow.

For example, if there is a server policy that requires the user to change their PIN every 30 days and this happens to coincide with their authenticating to the self-service site, successful authentication will be followed with a requirement to create a new PIN before access to self-service is permitted. This page provides prompts that deal with such situations.

![Figure 42: Sign In - Authenticate to Process Page](image-url)
Send Password by E-mail Page

This selection sends a one-time password, valid only for the Self-Service site to the email address associated with the userID. It includes error messages to handle cases where email cannot be sent or the userID cannot be found.

Figure 43: Sign In - Send Password by Email Page

Send Password by SMS Page

This selection sends a one-time password, valid only for the self-service site to the SMS number associated with the userID. It includes error messages to handle cases where SMS cannot be sent or the userID cannot be found.

Figure 44: Sign In - Send Password by SMS Page
Sign in using Questions and Answers

This option allows a user to sign in using answers to questions provided when configuring their profile.

Figure 45: Sign In using Questions and Answers
Configure Self-Enrollment Pages

Self-enrollment pages are presented to users so that they can bind and activate their tokens. Different token types and authentication methods require different enrollment steps/pages, as described below.

Default/Common Page

This page contains elements that are used in all enrollment processes. The use of these elements varies, depending on the token type and enrollment process. For example, UserID and Activation code may be prompts on an enrollment page, or may be used as labels in enrollment emails/SMS messages.

These prompts and labels should be translated for each language set to be supported on the Self-Service site (see Language Set).

Figure 46: Self-Enrollment - Default/Common Page
Software Token Page

This page contains the prompts, error messages, and instructions for enrolling MP-1 software tokens for each of the supported target devices, including: iOS, Android, BlackBerry, JAVA, Windows, and OS X.

These prompts and labels should be translated for each language set to be supported on the Self-Service site (see Language Set).

![Software Token Page](image)

**Figure 47: Self-Enrollment - Software Token Page**
Custom Token Page

This page contains all of the prompts and labels for enrolling custom tokens. These prompts and labels should be translated for each language set to be supported on the Self-Service site (see Language Set).

![Custom Token Page](image)

Figure 48: Self-Enrollment - Custom Token Page
Hardware Token Page

This page contains the prompts and labels for enrolling hardware tokens (RB-1, KT-x, eTokenPASS, RADIUS tokens, and third-party tokens).

These prompts and labels should be translated for each language set to be supported on the Self-Service site (see Language Set).

![Hardware Token Page](image)

**Figure 49: Self-Enrollment - Hardware Token Page**
Password Page

This page contains all of the prompts and labels for enrolling a static password. These prompts and labels should be translated for each language set to be supported on the Self-Service site (see Language Set).

Figure 50: Self-Enrollment - Password Page
MobilePASS Page

This is a lengthy page which contains all of the prompts and instructions for enrolling MobilePASS tokens for each of the possible target devices (iOS, Android, BlackBerry, JAVA, Windows, and Mac OS X).

The Multi-Device Instructions section may be useful to:

- Provide assistance to users when the device where the page is loaded is not a selected allowed target. Allowed Targets Settings are designed to allow the user to choose the instructions related to his/her chosen device type, and are selected in POLICY > Token Policies, and
- Provide instructions to users who may be loading the Self-Enrollment page on a device that is not their intended device for enrolling the token (and wish to only review the instructions).

The Multi-Device Instructions section will be displayed only if the Enable Multi-Device Instructions check box is selected in POLICY > Automation Policies > Self-Enrollment Policy.

- For new accounts created in SAS v3.5 (and higher), this option is enabled by default.
- For existing customers, after an upgrade to SAS v3.5, this option is disabled by default.

These prompts and messages should be translated for each language set to be supported on the Self-Service site.

Figure 51: Self-Enrollment - MobilePASS Page
Self-Service Authorities

Authorities are special privileges assigned to Operators for the purpose of managing user requests for tokens received from the Self-service site. There are four possible Authorities:

- **Approval Level 1**—This authority approves or denies user requests for tokens received from the Self-Service site. At least one Operator must have this authority if the Request a Token service is enabled on the Self-Service site.

- **Approval Level 2**—This authority approves or denies user requests for tokens that have been approved by Approval Level 1 authorities. This is an optional authority.

- **Issuing Authority**—Requests for tokens that have received the required approvals are fulfilled by the Issuing Authority. This function is the equivalent of using the Provision functions available on the Assignment tab unless a Shipping Authority has been created. At least one Operator must have this authority if the Request a Token service is enabled on the Self-Service site.

- **Shipping Authority**—The Shipping Authority is a special function that serves two purposes:
  - It can be used to coordinate the delivery of enrollment instructions with receipt of the physical token by the user.
  - It can be used to increase the security of enrollment by requiring the user to provide an additional code during enrollment that is delivered separately and Out-of-Band (OOB) with respect to all other enrollment instructions.

Shipping authorities are applied by token type. Token requests for affected token types that have been approved by the Issuing Authority must be completed by the Shipping Authority. This is an optional authority.
Configuring Authorities

Begin from the Configuring Self-Service module > Self-service Authorities link. This will display a list of Operators that can be assigned one or more authorities. To enable an authority for an Operator, select the appropriate authority option, and then click the Apply button to commit.

There must be at least one Operator with Approver Level 1 Authority and/or Issuing Authority to activate Enable Request a Token. Enable the Request a Token option for it to display on the Self-Service site.

Likewise, if a token is in the Shipping Authority Required list, at least one Operator with Shipping Authority is required.

![Figure 52: Configure Self-Service Authorities](image)

At least one Approval Level 1 and Issuing Authority must be enabled.

![Figure 53: Self-Service Workflow](image)

To add a shipping authority to a token type, first ensure that at least one Operator has been given this authority. Refer to “Configuring Authorities” on page 55. Next, select the token type from the Not Required window and, using the arrow, move it to the Shipping Authority Required window. Repeat this step for each token type that will require a shipping authority.
Out-of-Band Enrollment

Out-of-band (OOB) enrollment requires that the user provide an additional factor during enrollment to further validate their identity. This normally is in the form of an activation code. The code can be delivered by email, SMS, or output to a file.

OOB can be used with both hardware and software tokens. To enable OOB, select the tokens to which it will apply and the activation code delivery methods, and then click the **Apply** button.

![Figure 54: Out of Band Enrollment](image)

<table>
<thead>
<tr>
<th>Type</th>
<th>Self-service only</th>
<th>Send Activation Code by Email</th>
<th>Send Activation Code by SMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>eToken</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GOLOD</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RG</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OAITH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SecurID</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MP</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>GoDiware</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MobilePASS</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Request and Approval Queue Processing

This service contains a page for each of the messages that is sent to the user and authorities during the approval and provisioning process. Use the messages to inform users of the status of their request and to notify authorities when action is required of them.

Each message has an enable/disable option. If enabled, the message is sent at the appropriate point in the process. If disabled, the message is not sent.

Configure Request and Approval Queue Processing

The following configuration options are available in this service:

- **Auto-delete unapproved requests after X days**—If set to 0, unapproved requests will not be automatically removed from the Approval queue. Any other value will automatically remove an unapproved request the indicated number of days after it was received.

- **Allow approval by Email/SMS**—Check the delivery method(s) the system will use to send status and action alerts to authorities. If none are checked, status and action alerts will not be sent but the request will be listed in the appropriate queue.

This service contains several notifications. Use the menu in the Configure Queue Processing section to select the message. Each message has three sections — two for email (Subject, Body) and one for SMS (SMS Content). Most messages contain variables (for example, `<email />`) that must not be removed or modified. Otherwise, modify any other element of each notification according to your needs.

There is a 160-character limit (including spaces) in SMS messages. To prevent a multi-part SMS message, avoid exceeding this limit.

Click **Apply** after each message modification to commit the change.

![Figure 55: Request and Approval Queue Processing](image-url)
Language

This service is used to specify the default language for the Self-Service site. The English and French language sets are pre-configured, with English as the default. Additional language sets can be created using any existing language set as a guide. It should be noted that log files will always be presented in the English language.

To specify a language, select it from the Self-Service Default Language list and then click Save.

Figure 56: Language Configuration

If a user wishes to set their own personal language preference for the Self-Service site, they can do so on the Self-Service site Login page and Home page. At the bottom of the page, a text or icon link for languages will be displayed, based on configuration of the Self-Service service (the default links are shown below).

To switch to another language, click the languages link and then select the language from the list. All text in the Self-Service site will be converted to the selected language upon log in for that user only.

<table>
<thead>
<tr>
<th>To change the default user language</th>
<th>Languages text link</th>
<th>Languages icon link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a link on the Self-Service site home page…</td>
<td>Languages</td>
<td>SELECT A COUNTRY/REGION</td>
</tr>
<tr>
<td>…and then select a language.</td>
<td></td>
<td>English Français</td>
</tr>
</tbody>
</table>
The **Queue Management** module provides the interface for each of the authorities to process requests. Use the **State** menu to select the **Authority Queue** to be viewed. Note that an Operator is not able to view a queue for which they do not have the corresponding authority.

![Queue Management](image)

**Figure 57: Queue Management**

Select a **Request State** from the list, and then click **Search** to update the list for the selected state.

All queues have a list containing requests waiting processing. Each row in the list shows:

- **Request ID**—This is a unique number that identifies this request through all of the queues. As soon as a request has been issued, a provisioning task is created using the same ID number. Provisioning tasks track the user’s enrollment activity.

- **Submit Date**—This is the date and time the user submitted the request.

- **User ID**—This is the user ID associated with the request. Click the link to view information about the user. This will correspond with the data for this user ID found under **Assignment > User Detail**.

- **First Name**—This is the user’s first name.

- **Last Name**—This is the user’s surname.

- **Email**—This is the email address associated with this user.

- **Token Type**—This is the token type requested by the user.

- **Process State**—This indicates the state of the request. Currently, the only option is **Pending Approval**.

- **Approval Level 1**—Displays a list of all requests awaiting this approval. Select one or more requests then click Level 1 Approve or Reject.
  
  - If the request is approved and Approval Level 2 is enabled, the request will be removed from this list and appear in the Approval Level 2 queue, otherwise it will appear in the Issuer queue.

  - If enabled, the user will receive a “Request Approved” or “Request Rejected” notification corresponding to the Authorities decision. If approved and enabled, the next Authority in the processing sequence will receive a notification.

- **Approval Level 2**—Displays a list of all requests awaiting this approval. Select one or more requests then click Level 2 Approve or Reject to approve or reject the request respectively.
• If the request is approved the request will be removed from this list and appear in the Issue queue.

• If approved and enabled, the next Authority in the processing sequence will receive a notification.

• **Issue**—Displays a list of all requests awaiting this approval. Select one or more requests then click Issue Approve or Reject to approve or reject the request respectively.

  • If the request is approved and Shipping Authority is enabled for the requested token type, the request will be removed from this list and appear in the Shipping queue, otherwise the enrollment messages will be sent to the user.

  • If approved, a Provisioning Task will be created. The task tracks the status of the enrollment, including enforcement of enrollment policies such as last date to enroll.

• **Shipping Queue**—Displays a list of all requests awaiting this approval. Select one or more requests then click Issue Approve or Reject to approve or reject the request respectively.

  • The must receive an out of band activation code/instructions. The method of delivery is determined by the selection by token type.

  • If approved, a Provisioning Task will be created. The task tracks the status of the enrollment, including enforcement of enrollment policies such as last date to enroll. Tasks may be view from the Assignment > Provisioning Tasks.

### Token Requests Report

Token requests data and related workflow activity is recorded in the database. A number of reports are available to extract this data:

This report captures all requests and their progress through the workflow including:

• Request ID
• User ID
• First Name (user)
• Last Name (user)
• Email (user)
• Token Type (requested)
• Request State (Approval 1, Approval 2, Issue, Ship)
• Request Date
• Approval Date
• Approved By
• Issued Date
• Issued By
• Shipped Date
• Shipped By

Other relevant reports are the Provisioning Task Attempts, Provisioning Tasks and Provisioning Tasks Outstanding reports. Refer to the SAS Service Provider Administrator Guide for additional information.