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: 007-012406-003, Rev. B

Release Date: January 2018
Contents

Preface .................................................................................................................................. 5
Applicability .......................................................................................................................... 5
Introduction .......................................................................................................................... 5
Additional Reading .............................................................................................................. 6
Support Contacts .................................................................................................................. 6
   Customer Support Portal .................................................................................................. 6
   Telephone Support .......................................................................................................... 7

1 On-boarding an Account .................................................................................................. 8
   Overview ......................................................................................................................... 8
   Activating the Service ..................................................................................................... 9
   Account Type .................................................................................................................. 9
   Service Period ............................................................................................................... 10
   Auth Nodes .................................................................................................................... 10
   Delegated Management ................................................................................................. 10
   Allocation ....................................................................................................................... 11
      Allocation Options ...................................................................................................... 11
      Using the Allocation Wizard ..................................................................................... 13
      Allocation Wizard for Sale, ICE, and SMS Transactions ........................................... 17
   Create Operator ............................................................................................................. 18
   Auth Nodes .................................................................................................................... 18
   Contacts ......................................................................................................................... 19

2 Managing Virtual Servers ............................................................................................... 20
   Adding Users .................................................................................................................. 20
      Manually Adding Users ............................................................................................. 21
      Importing Users ......................................................................................................... 21
      Synchronization .......................................................................................................... 21
      LDAP Integration ....................................................................................................... 21
   Provisioning Users with Tokens .................................................................................... 22
      Bulk Provisioning ........................................................................................................ 22
      Automated Provisioning ............................................................................................. 22
      Manually Assigning and Managing Tokens .............................................................. 24

3 Reporting ....................................................................................................................... 30
   Overview ......................................................................................................................... 30
   Available Reports Module ............................................................................................. 31
      Customize Report ....................................................................................................... 33
   My Report List Module ................................................................................................. 34
   Schedule Report ............................................................................................................ 34
Preface

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—A cloud authentication service of Gemalto.
- **SAS – Service Provider Edition (SAS-SPE)**—The software used to build an authentication service.
- **SAS – Private Cloud Edition (SAS-PCE)**—The on-premises implementation of SAS-SPE.

Introduction

The SafeNet Authentication Service management interface gives administrators the tools and workflow automation to on-board, activate, and provision subscriber accounts in a matter of minutes. It also provides a great deal of flexibility in constructing Operator Roles and Scope; essentially which actions can be performed on which accounts.

Chapter 1 of this guide steps through a typical on-boarding process and assumes that the Operator performing the tasks has access to the entire management UI. These steps include:

- Adding accounts
- Activating services
- Allocating inventory
- Creating subscriber account administrators
- Activating Auth Nodes
- Adding account contacts

Chapter 2 provides an overview of common Virtual Server management tasks that you may perform on an account’s Virtual Server. As a Service Provider, this section will be useful to your help desk or other groups responsible for day-to-day management activities to be performed on behalf of the account, such as:

- Adding users
- Provisioning users with tokens
- Suspending tokens
- Assigning temporary passwords
- Generating reports

Chapter 3 explains how to customize, schedule, and deliver audit, usage, compliance, and billing reports.
Additional Reading

This document reflects a substantially reduced subset of the functionality of SafeNet Authentication Service. Refer to the SAS Service Provider Administrator Guide for complete documentation and examples.

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>
1 – On-boarding an Account

On-boarding an Account

Overview

On-boarding is the process of creating an account, establishing the type of service to be provided, allocating token inventory and capacity, and adding Auth Nodes. If the account will be self-managed, on-boarding may also encompass adding an Operator.

NOTE: A Virtual Server has been created during the installation and configuration process and can be managed from the Virtual Servers tab. The remainder of the information in this guide applies only if you intend to create and manage additional organizations and authentication servers.

All on-boarding activities are performed from the ON-BOARDING tab of the Service Provider management interface. The process begins by clicking the Create Account hyperlink in Shortcuts and then completing the Create Account form.

When adding a new account, keep the following in mind:

- The Account name must be unique.
- The Custom #1 field can be used to link the account to an external system. A typical use is to add the account number generated by your billing system for the account in this field. This allows all reports to be linked to the billing number and account name or both. The Custom #2 and Custom #3 fields can be used for similar purposes.
Activating the Service

Once an account has been created, the next step is to configure its type of service, duration, and other basic parameters from the Services module.

Account Type

In most cases, the Account Type selection will be Subscriber. This type of account is ideal for those accounts that will add users to the service manually, by import, or by LDAP synchronization from a single LDAP server. This account type is not permitted to create or manage additional accounts.

To allow an account to create, manage, and share resources with subordinate accounts, or to support LDAP synchronization with multiple LDAPs, it must be configured as a Service Provider. Typically, this option will be selected:

- Where the Account is reselling your service to its customer base and therefore will create and possibly manage its own accounts.
- Where the subscribing organization wants to on-board subsidiary companies or segregate management and services between internal groups or where multiple LDAP servers will be synchronizing users on the service.

The Evaluation check box does not affect the type of account but it does add a flag that can be used in reporting to distinguish “paying” customers from those evaluating the service. It can also be used to generate an alert to Account Managers a defined number of days before the service stops, allowing the Account Manager to proactively manage the account while it is still active.
Service Period

The Service Period uses the start/stop dates to limit the period of availability of the service to the account. These dates are modified by the Account Status option, which, if set to Active, makes the service available for the period commencing with the start date and ending on the stop date. If the Account Status is set to Not Active, the service is disabled regardless of the Service Period.

Billing frequency is simply a flag to Account Managers and reproduced in reports. In conjunction with the other information in this module, this allows Account Managers to ascertain the service and billing commitments with the account without referring to contracts.

Auth Nodes

SafeNet Authentication Service will receive and process authentication requests from VPNs, applications and so on, collectively referred to as Auth Nodes, configured for this account. This setting allows the service provider to limit the number of devices or applications that can authenticate against the service. The minimum value is 1. In general setting this value to reflect the minimum account requirements is recommended. Service Providers can use this setting to create up-sell opportunities, attaching a service cost for additional Auth Nodes.

Delegated Management

Though, in most cases, a Service Provider will manage the accounts they create, there are situations where they may wish to delegate management responsibility to their parent organization. SP2 has created and can manage SUB1; however, SP2 has also delegated management of SUB1 to SP1. This allows SP1 to manage the SUB1 account on behalf of SP2. Some useful applications of delegated management include:

- Supporting intermediate sales channels (for example, SP2 is purely as sales organization with no support capability, whereas SP1 is able to provide a full range of support functions).
- SP2 is a customer with several subsidiary organizations, LDAP domains, etc. (SUB1, SUB2, SUB(N)) but all user and account management is to be performed by SP1.

Checking the Delegated Management Option immediately delegates management to the Service Provider’s parent. The Primary Contact and Telephone fields can be populated to add a point of contact reference at the parent (SP1).
Allocation

ON-BOARDING > Allocation enables you to allocate tokens and capacity to the account. This process moves inventory into the account’s Virtual Server. A summary of your inventory available for allocation to an account can be found in the Inventory module on the Dashboard. Capacity determines the maximum number of tokens that can be in use (assigned to users).

The Allocation module displays a table showing the capacity and quantity of all token and authentication types allocated to the account’s Virtual Server, where:

- **Maximum**—Shows the total, by capacity and authentication method, allocated to the account.
- **In Use**—Shows the capacity and authentication methods consumed by the account or, in the case of Virtual Service Providers, for their own use or allocated to accounts they manage.
- **Available**—Shows unconsumed capacity and authentication methods.

Allocation Options

Rental

The Rental option is applied to accounts that will pay a recurring fee per user for capacity or some combination of capacity and tokens. This option ensures that the ownership of tokens does not transfer to the account.

Choose Capacity if you are migrating an account from an in-house system with tokens that are compatible on the SafeNet Authentication Service. Essentially, this option allows you to bill for the service without billing for tokens.

Choose Tokens, Transaction Type Rental, and Automatically add Capacity with this allocation. Also specify if the account will be paying a fee per user for the service including a token per user.
Sale

The sale option transfers ownership of tokens to the account. This option is ideal where the account wishes to own the tokens rather than have that cost bundled into their recurring cost per user.

Choose **Tokens, Transaction Type Sale** if the Account is purchasing tokens and does not require additional capacity. Example uses include an Account replacing owned tokens that have been lost or replacing one token type with another.

Choose **Tokens, Transaction Type Sale and Automatically add Capacity with this allocation** where the Account requires an equal amount of additional capacity to support the purchased tokens. Note that this option is the equivalent of two separate allocation transactions: **Tokens, Transaction Type Sale** and **Capacity Only**.

ICE (In Case of Emergency)

ICE is a service you can offer your accounts to allow them to increase capacity and issue tokens for a limited period of time after which capacity returns to pre-ICE levels. ICE includes MP-1 software tokens equal to the ICE capacity. These tokens can be deployed to any MP-1 target, such as PCs, iPhones™, and BlackBerrys. Expiration of ICE stops the authentication service only for users with ICE tokens.

Though only one (1) ICE license can be activated at a time, additional ICE licenses can be allocated at any time to replace a consumed license or replace an in-use license prior to expiration.

In addition, only one (1) ICE license can be in use at a time. Activation of an ICE license replaces an in-use license; it does not extend an in-use license.

SMS Credits

The **SMS Credits** option is used to charge accounts in advance for use of SMS services. Each SMS message sent by the account uses one (1) credit (assuming customized message lengths do not exceed the SMS character limit resulting in two (2) or more SMS transmissions per message). SafeNet Authentication Service decrements the account’s SMS credits inventory every time a message is sent.

Use this option if the account will be using SMS/OTP or if it will be configured to send alerts via SMS.

This option is available only if the Virtual Server has a configured SMS gateway or SMS modem, or if you are a Service Provider and have SMS credits in your inventory.

SafeNet Authentication Service can send an alert to an Account Manager if an account’s remaining SMS credits fall below a specified threshold.
Using the Allocation Wizard

Each type of token and/or capacity is allocated to an account in separate transactions.

To start the Allocation Wizard, click **On-Boarding > (select the account) > Allocation > Allocate.**

![Allocation Wizard](image)

The number of steps in the wizard depends on the type of allocation. In general, allocation includes:

- Selecting the type of allocation – Rental, Sales, ICE, or SMS Credits
- Indicating the quantity of inventory to be allocated
- Creating a billing reference – the amount to be charged for the transaction or unit of transaction, billing triggers, customer reference, and comments.

**Allocation Wizard Step 1 – Determine Allocation Type**

1. Select the transaction type and sub options. For example if your service bundles capacity and tokens into a single cost/user/month, select **Tokens.**

![Determine Allocation Type](image)

2. Select the **Transaction Type, Rental**, and then check the **Automatically add Capacity with this allocation** option.
   - **Capacity Only**—Indicates that tokens are not included in this allocation. A typical use of this option would be to allow an account to use tokens they already own, and will import or initialize into their **Virtual Server.**
1 – On-boarding an Account

- **Tokens**—Allocates a specific quantity and type of token.
  - **Sale**—Indicates that token ownership is transferred. Inventory that is not owned cannot be allocated in a sale transaction.
  - **Rental**—Indicates that ownership will not transfer. This transaction type can allocate from token inventory containing sale and rental tokens.
- **Token Type**—Indicates the type of token to be allocated.
- **Automatically add Capacity with this allocation**—Allocates corresponding rental capacity with the sale tokens.
- **ICE**—Indicates the quantity of ICE to be allocated to the account.
- **SMS Credit**—Transfers a quantity of SMS credits to the account.

3. Click **Next** to continue.

### Allocation Wizard Step 2 – Select Inventory for Allocation

The next step is to select the inventory to be allocated. The list selections will vary depending on how your inventory is managed:

#### Table: Allocation Wizard Step 2 – Select Token

<table>
<thead>
<tr>
<th>Container</th>
<th>Indicates the container from which token inventory should be allocated. The Default holds all tokens unless additional containers have been created and inventory added to them.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rental/Sale</td>
<td>Used to limit the tokens displayed in the list to Rental or Sale. Note that Sale tokens can be allocated as sale or rental, while Rental tokens can only be allocated as rental.</td>
</tr>
<tr>
<td>Serial #</td>
<td>Used to select a specific token from inventory by serial number.</td>
</tr>
<tr>
<td>Available</td>
<td>Indicates the quantity available for allocation.</td>
</tr>
<tr>
<td>Quantity</td>
<td>Indicates the quantity to be selected.</td>
</tr>
</tbody>
</table>

Enter the quantity to be allocated and then click **Search**. The list displays inventory that matches the search criteria. Select the inventory in the list by selecting the corresponding check box(es), and then click **Next**.

You can use the **Remove** button to remove checked inventory from the **Allocated** list.
## Allocation Wizard Step 3 – Create Billing References

Billing references are used in reporting to indicate how the transaction should be billed, and to link the transaction to customer references, such as purchase order numbers.

### Billing Basis

The billing method associated with the transaction. Options are:

- **Allocation** - Billing occurs on the date the inventory is allocated to the account.
- **Activate** - Billing occurs when the token/method is assigned to a user. This could be a user of this account or any account to which it transfers the token.
- **Authentication** - Billing is based on token usage; each authentication incurs a charge.
- **Transfer** - Billing commences when this account (Virtual Service Provider) allocates inventory to an account it creates and manages. Transfer provides a mechanism to bill for the entire transaction or only the quantities transferred.

### Billing Start

This date modifies the **Billing Basis** to indicate a date other than the transaction date to start billing. This is useful for allowing a grace period before billing commences. For example, on allocation, the **Billing Start** could allow 30 days after allocation before billing commences whereas on Transfer, the **Billing Start** date could mean commence billing on this date whether or not the inventory has been transferred.

### Rate/Month

The charge to be applied per unit being transferred. Note that a character that is not easily used within the external billing system (for example, $, £) should not be included in this field.

### Reference

Information related to the allocation, such as the purchase or sales order number; used to link the transaction to external processes such as order fulfillment.

### Warranty Replacement

Indicates that the allocation is to replace product under warranty. This is helpful for distinguishing between new orders, billable product and no-charge warranty replacements when producing billing reports.

Use the **Reference** field to record the RMA (Return Material Authorization) number with the warranty replacement.

### Evaluation

Indicates that the allocation is provided for evaluation purposes.

### Comment

Freeform text area in which to include comments related to the transaction. Comments form a permanent part of the transaction record.
Allocation Wizard Step 4 – Confirm Allocation

This is the last step, which provides the opportunity to verify before committing the entire transaction.

![Allocation Wizard Step 4](image)

The **Allocation** table is updated when the wizard finishes.

![Allocation Table](image)
Allocation Wizard for Sale, ICE, and SMS Transactions

Sale Transactions

The process for Sale transactions is identical to the Rental example in the preceding pages except as follows:

- Only inventory available for sale can be used in a Sale transaction.
- Tokens can be allocated without capacity. Choose this option if replacing lost or damaged tokens owned or rented by the account.
- Tokens can be allocated with a corresponding quantity of rental capacity. This option is the equivalent of two separate transactions: Rental > Capacity Only and Sale > Token (without capacity).

ICE Transactions

To allocate ICE tokens: select ICE, click Next, enter a quantity in the Allocate field to reflect the required ICE capacity, and then follow the wizard steps described in “Using the Allocation Wizard” on page 13.

All ICE licenses have a duration of 30 days from activation on the account’s Virtual Server.

SMS Credits Transactions

To allocate SMS Credits, select the SMS Credits option, enter the quantity of SMS credits to allocate to the account, and then follow the steps described in “Using the Allocation Wizard” on page 13.

The SMS Credits Inventory will be Unlimited if, as a Service Provider, you have configured an SMS Gateway in the Virtual Server.

Setting this field to 0 indicates that, as a Virtual Service Provider, you have not configured an SMS Gateway and have either not purchased or have consumed all SMS credits allocated to your account by your Service Provider.
Create Operator

As soon as you create an account, you are able to manage every aspect of the service and the account’s Virtual Server from the Manage tab.

You can optionally create an Operator for Subscribers and/or Virtual Service Providers - to enable the accounts to log in to the management console to manage their Virtual Server without your involvement. This process sends enrollment and activation messages to the user that is configured as the Account Operator.

Auth Nodes

An Auth Node is any of the account’s devices (for example, VPN and web applications such as Outlook Web Access) that send authentication requests to the service. An entry in the Auth Nodes table must be created for every Auth Node. The number of Auth Nodes cannot exceed the allowed number set in the Services module. SAS will not process authentication requests received from devices or applications that are not in the list.

Auth Nodes become active within minutes of configuration.

To configure the Auth Node, click On-Boarding > Auth Nodes (module) > Auth Nodes (task) > Add and enter at least the following:

- For RADIUS clients, such as SSL VPNs:
  - A descriptive name of the device in the Auth Node Name field
  - The IP address of the RADIUS client
  - The RADIUS shared secret (this must be identical in both SAS and the RADIUS client)

- For SAS Agents, such as Agent for Outlook Web Access:
  - A descriptive name of the device in the Auth Node Name field
  - The IP address of the RADIUS client

NOTE: By default, if left empty, the Resource Name field will be populated with the Auth Node Name value. In push notifications, the Resource Name identifies the auth node that it relates to, so the user can recognize that it is a valid node to
authenticate.
If authentication nodes are shared, the Resource Name is inherited from the parent account. If authentication nodes are shared with child accounts, make sure that the **Resource Name** is also meaningful to users of these child accounts.

SafeNet Authentication Service can be configured to send an activation alert as soon as it is ready to accept authentication requests from the newly configured Auth Node.

Some RADIUS clients are not fully RADIUS compliant and do not support “challenge-response”, which is a requirement for server-side PIN changes. If your RADIUS client does not support challenge-response, and you have configured your server-side PIN policy to require the user to periodically change their PIN, enable the **Exclude from PIN change requests** option to prevent a forced PIN change with the non-compliant RADIUS client.

**Contacts**

The **Contacts** module is simply a place to add reference contacts related to the account, such as technical and accounts payable contacts.
Managing Virtual Servers

This chapter provides an overview of common Virtual Server management tasks that you may perform on an account’s Virtual Server. As a Service Provider, this section will be useful to your help desk or other groups responsible for day-to-day management activities to be performed on behalf of the Account such as:

- adding users
- provisioning users with tokens
- suspending tokens
- assigning temporary passwords
- generating reports

Adding Users

Once an account has been activated and inventory has been allocated, it’s time to add users and provision them with tokens. Begin by clicking the account’s hyperlink in the Managed Account list on the Virtual Server tab. The work area in the management UI will change to show the account’s Virtual Server management tabs.

The Assignment tab provides access to all of the user management and provisioning tasks for the selected account’s Virtual Server. This tab contains all of the modules necessary to:

- Manually add or import users into the account’s Virtual Server
- View users with tokens in individual transactions or in batches
- Apply individual user authentication activity and metrics without running reports
- Apply time/day logon access restrictions to individual users
- Manage individual user group membership for the purpose of authorization
- Apply individual user RADIUS attributes for the purpose of authorization
Manually Adding Users

Users can be added manually by clicking the “Create User” hyperlink under Shortcuts and completing the User information form. The minimum requirement is First Name, Last Name, User ID and e-mail address.

Importing Users

Multiple users can be imported into the system by using the Import Users hyperlink under Shortcuts. The import wizard can accommodate a wide range of delimited files (tab, csv etc.), with or without a header row.

- The minimum requirement is First Name, Last Name, User ID, and e-mail address.
- Missing data, such as country code, which is required for SMS messaging, can be populated within the wizard. For example, if all mobile numbers in the import file are registered in North America but none include the country code 1, the wizard can force the addition of 1.

Synchronization

Users can be automatically added, suspended or removed from the Account’s Virtual Server by utilizing the SafeNet Authentication Service Synchronization Agent, eliminating the need to manually create and manage users. In addition to basic user information, synchronization includes the users Active Directory group membership which in turn can be used for:

- Automatic provisioning of tokens to users
- Automatic revocation of tokens from users
- LDAP pre-authentication and authorization

Note that SafeNet Authentication Service supports manual creation of users concurrent with LDAP synchronization, bearing in mind that manually created users will not be modified in any way by an LDAP synchronization provided there is no overlap in UserID. If an overlap occurs, any tokens assigned to the manually created UserID are revoked and the UserID is replaced by the overlapping LDAP UserID.

LDAP Integration

Users can be automatically added, suspended, or removed from the account’s Virtual Server by configuring LDAP integration, eliminating the need to manually create and manage users. In addition to basic user information, synchronization includes the users Active Directory group membership, which, in turn, can be used for:

- Automatic provisioning of tokens to users (refer to “Automated Provisioning” on page 22)
- Automatic revocation of tokens from users
- LDAP pre-authentication and authorization
- Chained authentication

Note that for performance reasons LDAP integration is not recommended where the directory server and SafeNet Authentication Service are communicating across the internet. If integration over the internet is required it must be across a high speed, low latency connection with guaranteed availability.
Provisioning Users with Tokens

There are several ways to provision users with tokens:

- **Bulk Provisioning**—Whereby any number of users are provisioned in one simple, time-saving step.
- **Automated Provisioning**—Whereby rules are used to evaluate when a user should be issued a token and what type of token. If the rule evaluates true for a user, a token is issued. If false, the token is revoked. Automated provisioning is usually used in conjunction with LDAP Synchronization and LDAP Integration.
- **Manual Provisioning**—Used to manually provision users, one user at a time.

**Bulk Provisioning**

This process is used to provision each of any number of users with a token in a simple point-and-click process.

To provision one or more users:

1. Click **Virtual Servers > Assignment**.
2. Use **Search User** to refine the list of users to be provisioned.
3. Select the token type.
4. Confirm the provisioning task.

Bulk provisioning sends a self-enrollment notification containing instructions for receiving, installing (if necessary) and activating their token to all users in the provisioning task.

Provisioning tasks can be modified or recalled for all or some users in the task by clicking **Provisioning Tasks** in the Shortcuts panel of the **Assignment** tab.

**Automated Provisioning**

This method evaluates rules configured in **Virtual Servers > Policy > Automation Policies**. While complex rules can be configured, the most common practice is to provision a user with a token based on their Group membership. During LDAP synchronization, user information is updated, adding or removing users from the Account’s Virtual Server and adding or updating their Virtual Server’s copy of LDAP group membership. If during update a user is found to be a member of a group to which tokens should be provisioned, the user will automatically be sent the appropriate self-enrollment notification.
The main advantage of Auto Provisioning is that by virtue of adding or removing users from LDAP and LDAP groups, SafeNet Authentication Service can take the appropriate provision/de-provision action with no manual intervention.

To configure auto provisioning:

2. Enter a Rule Name, choose the Token Type to be provisioned, and select the (LDAP) Target Group(s) to which a user must belong to cause SAS to start the provisioning process.
3. In addition to group membership, you can refine the rule conditions as follows:
   - To prevent multiple tokens from being issued to a user because they belong to more than one valid group or already have a token, clear the Issue Duplicate Types check box.
   - To automatically revoke all tokens provisioned to the user under this rule if the rule evaluates false (such as the user is no longer a member of valid group) check the Auto Revoke option. If you alter an existing provisioning rule that includes the Auto Revoke option (for example, adding another group to the rule), make sure that the rule still evaluates for users who are already enrolled. If it does not, tokens will be automatically unassigned from these users.
   - To restrict the rule to users that reside in Container in the Virtual Server, select the container from the Container list. Note that all users reside in the Default container unless specifically moved to a different container.
   - To define a rule that includes multiple groups, users must belong to each group that is selected in the Use by rule window. For example, if GroupA, AND GroupB, AND GroupC are selected, users must
belong to groups A, B, and C. If only one group should apply to a rule, create a separate provisioning rule, and only assign that group to the rule.

If the Virtual Server has been allocated ICE capacity, then use the Assign as ICE Token option to automatically issue ICE tokens if the rule evaluates true.

Manually Assigning and Managing Tokens

Tokens Module

Use the Virtual Servers > Assignment > (Search User) > User ID > Tokens module to:

- Add a token to a user.
- Provision a token to a user.
- Assign a temporary static password to a user.
- Manage all tokens associated with a user.

The tokens module lists all tokens associated with a user where:

- **Manage**—Provides access to all management functions for the corresponding token.
- **Type**—Displays the authentication method assigned to the user.
- **Serial #**—Displays the serial number of the token or the word Password if a static password is allowed.
- **State**—This is the state of the token/authentication method where:
  - **Active**—This method can be used to authenticate.
  - **Suspended**—The authentication method is associated with the user but has been suspended by an Operator, preventing it from being used to authenticate until the method is reactivated by an Operator.
  - **Locked**—Indicates that the user has exceeded the maximum number of consecutive failed logon attempts. The token will remain locked until the unlock policy is triggered or an Operator reactivates the token.
  - **Assigned**—Indicates that the token has been assigned to the user but has not yet been used to authenticate.
- **Initial PIN**—This is the initial PIN value to be given to the user when using Assign to issue a token. By default, the initial PIN value must be changed by the user during their first authentication. The initial PIN value displayed in this field is cleared from the display as soon as the user completes the PIN change.

Note that the Password button is disabled if the user has any other assigned authentication methods.
Managing a Token

To manage a user's token, begin by clicking the Manage hyperlink for the corresponding token.

![Tokens Table]

Suspend

Use this option to suspend the token, making it invalid for authentication but leaving it assigned to the user. This button is disabled if the token is not in the Active state.

![Suspend Token]

Depending on policy, the following options may be available when suspending a user's token:

- **No Static Password**—The user's token will be suspended and the user will not be given a temporary static password.

- **Accept LDAP Password**—The user's token will be suspended and the user will be allowed to use their LDAP password to authenticate. Note that this option requires LDAP integration.

- **Set Temporary Static Password**—The user's token will be suspended and the user will be given a temporary static password which can be used to authenticate:
  - **Generate button**—Use this to generate a static password that complies with the established policy.
  - **Change static password on first use option**—If checked, the user must change the provided static password to a new value known only to them and which complies with the established policy.
  - **No Static Password after**—Use this option to limit the life of the temporary password.
- **Comment**—Use this area to enter a brief explanation for suspending the token. This forms part of the permanent token record and can be viewed by other Operators managing this user’s account.

**Unlock**

Use this option to reactivate a token that is in the locked state, making it valid for authentication. Its use varies depending on the PIN mode:

- If the token is locked due to excessive consecutive failed authentication attempts, click **Activate** to reactivate the token. Select the **Set a New PIN** option to create a new PIN for the user for this token or use the **Random** button to generate a PIN that complies with the policy.

- A token initialized with a token-side PIN which has been locked by the user by exceeding the maximum allowed PIN attempts may be unlocked using this function, provided the token was initialized with the unlock token option enabled. This function should only be used if you are certain that the person in possession of the token is the rightful owner.

- To use this function the user must generate an unlock challenge. The method for doing this varies with token type. Refer to the SafeNet Authentication Service – Tokens Guide. For MP-1 tokens, for example, enter this value into the **Challenge displayed on token** field, and then click **Unlock** to display an unlock code. Give this to the user to enter into their token. If correctly entered, the user will be required to generate a new PIN, after which the token can be used to authenticate.
New PIN

This option is available where the PIN is evaluated by the server (server-side PIN). This function sets a new PIN value for this token according to the configured PIN policy. Use the Generate button to automatically create a new PIN that meets the minimum policy requirements.

Resync

Use this option to resync a token or test the token if there are repeated failed authentication attempts with this token. Generally, resync is not required. If necessary, however, resync does not require the user or Operator to reveal the PIN associated with a token.

The Resync methods vary depending on the type of token.

For Challenge/Response resynchronization:

Have the user key the Challenge into their token after enabling resync to generate a Response. Enter the resulting response into the Response field, and then click Resync. The response provided by the user's token for the displayed challenge should result in a successful test. If so, the token is working properly and in sync with the server. (Refer to the SafeNet Authentication Service Tokens Guide.)
For OATH, SafeNet GOLD/Platinum tokens:
Have the user generate two (2) passcodes and enter them in the correct order. A message will be displayed confirming the success or failure of the resync process.

**Initialize**

Use **Initialize** to generate new token seeds and change the operating parameters of hardware tokens. The current token template is applied during initialization. The appropriate token initializer must be connected to the PC. This button is available only if a hardware token is selected.

**Issue**

Use **Issue** to create an MP-1 token profile (token seed and operating parameters) in conjunction with the **Assign** function.
Revoke

Use Revoke button to revoke a token. A revoked token can no longer be used to authenticate. If the Revoke Password option is not selected, the user can still authenticate using an assigned static password. The user can also authenticate with any other active token associated with their account.

- **Return to Inventory, Initialization Required**—Select this option for hardware tokens issued with a token-side PIN or if the token seed and operating parameters must be changed before the token is reissued. This option is typically used with RB-1 PIN Pad tokens.
- **Return to Inventory, token does not need to be reinitialized**—Select this option for all other cases where the token is being returned.
- **Lost**—Returns the token to inventory in the Lost state. Tokens in this state cannot be reissued unless they are recovered and reinitialized.
- **Faulty**—Returns the token to inventory in the Faulty state. Tokens in this state cannot be reissued unless they are successfully reinitialized.
Reporting

Overview

Every Virtual Server has a reporting engine that provides an extensive range of usage, compliance, inventory management and billing reports. Reports can be customized, scheduled and automatically delivered to recipients or viewed and downloaded through the management UI.

Reporting consists of four modules:

- **Available Reports Module**—This module lists all of the standard reports available in the Virtual Server. Reports from this list can be customized and copied to the My Customized Reports module.

- **My Report List**—This module lists all reports that can be run on the Virtual Server. Reports in this module can be scheduled to run once or periodically at regular, predefined intervals. Delivery options and recipients are defined in this module.

- **My Scheduled Reports**—All scheduled reports appear in the My Scheduled Reports list. Schedules can be modified and reports can be run now without modifying the normal schedule.

- **My Report Output**—This module lists all reports that are currently in the run state or have completed. From this list, Operators can view or download reports in a variety of formats.

Operator roles determine which modules are available to an Operator, and whether or not they can modify report parameters.

Scheduled reports and report output will display only those reports to which the Operator is entitled. Reports can be customized, scheduled and delivered to the account, the Service Provider and to external parties, such as auditors.
Available Reports Module

All reports that are available in a Virtual Server are listed in the Available Reports module. To view the entire list of available reports use the navigation controls below the list or expand the number of rows displayed using the customization icon in the module bar. The report class dropdown selects reports corresponding to:

- **Security Policy**—This group of reports deals with alert history, container management, Operator roles and scope, and Auth Nodes and RADIUS attributes.
- **Compliance**—This group of reports covers user authentication activity, Operator activity and other factors important to internal and external security auditors.
- **Billing**—This group of reports provides details of all transactions including capacity, tokens, SMS credits, and their related billing terms.
- **Inventory**—This group of reports provides detailed information on tokens, token ownership, states, and other general inventory information.

To add a report to the My Report List module, begin by selecting a report from the list, and then click the Add button.
### Reporting

**SafeNet Authentication Service**: Service Provider Quick Start Guide

**Document Number**: 007-012406-003, Rev. B, © 2018 Gemalto

<table>
<thead>
<tr>
<th>Report Columns:</th>
</tr>
</thead>
<tbody>
<tr>
<td>TimeStamp</td>
</tr>
<tr>
<td>User ID</td>
</tr>
<tr>
<td>Uset Name</td>
</tr>
<tr>
<td>FirstName</td>
</tr>
<tr>
<td>LastName</td>
</tr>
<tr>
<td>Source IP</td>
</tr>
<tr>
<td>Agent</td>
</tr>
<tr>
<td>Token</td>
</tr>
<tr>
<td>Action</td>
</tr>
<tr>
<td>Result</td>
</tr>
<tr>
<td>Credential Type</td>
</tr>
<tr>
<td>Message</td>
</tr>
</tbody>
</table>

**Authorization:**

| Access to Report Not Enabled: |
| Access to Report Enabled:    |

**External Authorization:**

| Access to Report Not Enabled: |
| Access to Report Enabled:    |

**Authorization Role:**

| Access to Report Not Enabled: |
| Access to Report Enabled:    |

**Email Recipients:**

| Add |

- Email small reports (less than 2000 rows)
Customize Report

The options for report customization vary depending on the type of report selected. In general:

- **Report Section**—Customize the name of the report and its description. These changes will appear in the My Report List module. Note that report names must be unique.

- **Filters**—If available, filters provide a way to limit the scope of a report, such as the reporting period.

- **Report Columns**—This shows default fields included in the report. To include/exclude fields, select/deselect fields using the corresponding check boxes.

- **Authorization**—The **Access to Report not Enabled** field lists all Operators that are potential report recipients. The **Access to Reports Enabled** field lists all Operators that will receive the reports. To add or remove selections from the **Recipient** list, highlight the Operators (Use Ctrl+Click to select multiple Operators), and then click the appropriate arrow to move.

- **External Authorization**—The **Access to Report not Enabled** field lists all Service Providers that are potential report recipients. The **Access to Reports Enabled** field lists all Service Providers that will receive the reports. To add or remove from the recipient list, highlight the Service Providers (Use Ctrl+Click to select multiple Service Providers), and then click the appropriate arrow to move.

- **Email Recipients**—The server can send the report by e-mail to addresses in the recipients list. Use this option to send reports to people that are not Operators or Service Providers and therefore cannot log in to the management UI to view and download reports. To add recipients, enter their e-mail address then click the **Add** button. To remove recipients, highlight their e-mail address then click the **Remove** button.

- **Email small reports (less than 2000 rows)**—This option must be selected if you want SAS to e-mail the report. If selected, SAS e-mails reports to the configured roles (for example, Account Managers and Operators) as well as to the addresses entered in the **E-mail Recipients** field. Reports can also be downloaded from the management UI or by using BSIDCA.

---

**NOTE:** The reports are unencrypted. Use secure transfer methods such as scp/sftp or download via https.

---

**NOTE:** The number of rows in small reports can be configured for PCE installations only; the default is 2000.

---

Click the **Finish** button to commit the customizations and add the report to the **My Report List** module.
My Report List Module

This module lists all customized reports. It is from this list that you schedule reports to run.

To schedule a report, select the report then click the Schedule button.

Schedule Report

The schedule report options are:

- **Run Now**—The run now option adds the report to the report processing queue. Reports in the queue are run in chronological order.
- **Schedule Begins**—The report will not run prior to this date.
- **Frequency**—Reports can be scheduled to run on specific days of the week by selecting the **Days/Week** option, then selecting the specific days. Alternatively, the report can be scheduled to run on a monthly basis by selecting the **Months/Year** option, then selecting the specific months. If **Months/Year** is selected, the **On day** option is enabled. Use this option to specify a day in each month that the report should run. Reports will not run after the date specified in the **Expiration Date** field. By default, report schedules do not expire.
- **Run Time**—The time at which the report should begin executing.
- **Expiration**—The date after which the report will be removed from the **My Scheduled Reports** list.
To commit the report schedule, click the **Finish** button. This adds the report to the **My Scheduled Reports** module.

Operators with appropriate role permissions can use the **Edit** hyperlink to modify the report criteria or remove the report from the **My Report List** using the **Remove** hyperlink.

### My Scheduled Reports Module

Scheduled reports to which the Operator is entitled appear in the **My Scheduled Reports** List. The list shows the report name, run frequency, run time and expiration date. Clicking the report name hyperlink displays the report criteria. Operators can modify a report schedule or run a report now. The **Run Now** option adds the report to the report processing queue.

Reports in the queue are run in chronological order. The reporting service checks the queue every 5 minutes and after each report is generated. This means that all reports will be processed in order however if no reports are detected, up to five (5) minutes may elapse before the service will check the queue for new report additions. The **Run now** option does not alter the report’s regular schedule.

Operators with appropriate role permissions can make changes to the reports schedule by clicking the **Edit** hyperlink, or remove the report from the schedule by clicking the **Remove** hyperlink.

Reports that are running or have completed running are added to the **My Report Output** module.

### My Report Output

All reports that are running or have completed to which the Operator is entitled are listed in the **Report Output** table.

Reports can be viewed in the browser by clicking the report name hyperlink. Alternatively they may be downloaded for local processing by clicking any of the **CSV**, **Tab**, or **HTML** hyperlinks. Reports that are no longer required can be deleted from the list by clicking the **Remove** hyperlink.