SafeNet Authentication Service
Subscriber Account Operator Guide
Trademarks and Disclaimer

Trademarks, Copyrights, and Third-Party Software
Copyright 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.

Disclaimer
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, the confidentiality and proprietary legend and this full warning notice appear in all copies.
> This document shall not be posted on any publicly accessible 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.
CONTENTS

PREFACE .................................................................................................................. 8
Terminology .............................................................................................................. 8
Additional Reading ................................................................................................. 8
Support Contacts .................................................................................................... 9
Customer Support Portal ......................................................................................... 9
Telephone Support .................................................................................................. 9
Email Support .......................................................................................................... 9

1 Introduction ......................................................................................................... 10
SafeNet Authentication Service ............................................................................... 10
Management Console ............................................................................................. 12
Conventions ............................................................................................................. 12
SafeNet Authentication Service + SafeNet Trusted Access .................................... 13

2 Virtual Service Functions ..................................................................................... 15

3 SNAPSHOT ........................................................................................................... 16
Authentication Activity ............................................................................................. 16
Authentication Metrics ............................................................................................. 18
Token States ............................................................................................................. 18
SMS Credits ........................................................................................................... 19
Allocation ................................................................................................................ 19
References ................................................................................................................ 21

4 ASSIGNMENT ..................................................................................................... 22
About Adding Users ................................................................................................. 22
Create User (shortcut) .............................................................................................. 23
Import Users (shortcut) ............................................................................................ 24
Provisioning Tasks (shortcut) .................................................................................. 25
Search User .............................................................................................................. 27
Search Fields ........................................................................................................... 27
Search for Users ...................................................................................................... 28
Search Result Fields ................................................................................................. 28
Additional ASSIGNMENT Modules .......................................................................... 29
User Detail ................................................................................................................ 31
Tokens ....................................................................................................................... 31
Assign ...................................................................................................................... 32
Provision .................................................................................................................. 34
Suspend ...................................................................................................................... 37
Unlock ....................................................................................................................... 38
New PIN ..................................................................................................................... 39
Resync ....................................................................................................................... 40
This guide is for SAS Service Providers responsible for delivering authentication services to accounts and for configuring the service to reflect the account’s internal business processes, Service Level Agreements, and management hierarchy. This guide describes the functionality of:

- **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.

**Terminology**

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Provider / Account Manager</td>
<td>The top-level organization that:</td>
</tr>
<tr>
<td></td>
<td>&gt; Installed and owns SAS, SAS-SPE, or SAS-PCE.</td>
</tr>
<tr>
<td></td>
<td>&gt; Manages their own Virtual Server.</td>
</tr>
<tr>
<td></td>
<td>&gt; Is able to create and manage additional Virtual Service Provider and Subscriber accounts.</td>
</tr>
<tr>
<td></td>
<td>Every other organization is either a Virtual Service Provider or Subscriber.</td>
</tr>
<tr>
<td>subscriber</td>
<td>All accounts that you create and manage, including Service Provider accounts.</td>
</tr>
<tr>
<td>Subscriber</td>
<td>Accounts that are not Service Providers.</td>
</tr>
<tr>
<td>Virtual Server</td>
<td>An individual account’s virtual authentication server.</td>
</tr>
<tr>
<td>Virtual Service Provider / Operator</td>
<td>An organization that:</td>
</tr>
<tr>
<td></td>
<td>&gt; Has a Service Provider as a parent.</td>
</tr>
<tr>
<td></td>
<td>&gt; Manages their own Virtual Server.</td>
</tr>
<tr>
<td></td>
<td>&gt; Is able to create and manage additional Virtual Service Provider and Subscriber accounts.</td>
</tr>
</tbody>
</table>

**Additional Reading**

The SafeNet Authentication Service document suite includes:

- Service Provider Quick Start Guide
- Service Provider Administrator Guide
- Operator Guide for Subscribers
- Synchronization Agent Configuration Guide
- Branding and Customization Guide
- Service Provider Billing and Reporting Reference Guide
- SafeNet Trusted Access Operator Guide
Support Contacts

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. 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 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 Gemalto Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support via email at technical.support@gemalto.com.
SafeNet Authentication Service

SafeNet Authentication Service (SAS) is an enterprise-class authentication server designed to extend authentication services to users in a single organization or across an unlimited number of entities. These entities can be almost anything, from divisions or cost centers within a company, to subsidiaries or completely independent organizations. Its multi-tier, multi-tenant structure accommodates just about any hierarchy, reporting structure, business structure, security segregation, or other delineation.

Figure 1: SafeNet Authentication Service Delivery Platform

SafeNet Authentication Service is available as:

> **SAS**: Gemalto’s cloud-based highly secure, software as-a-service authentication platform with no hardware requirements, providing 24/7 availability. By leaving security to the experts, organizations can have peace of mind knowing their systems are secure, and always available, in a trusted cloud environment. In addition, using one cloud-based platform to manage, maintain, and provision a wide-range of tokens, SAS can grow with your organization’s requirements—securing an infinite number of users in a variety of token form factors.
> **SAS – Service Provider Edition (SPE):** Providing organizations with a highly economical and effective cloud-based authentication management service.

> **SAS – Private Cloud Edition (PCE):** Providing organizations with an on-premises authentication management solution.

SAS can be used to extend authentication services beyond the corporate perimeter. By supporting SAML (Security Assertion Markup Language), many cloud applications—from Google Apps and Salesforce to Box.net and web SSO services—can be protected by SAS. Better yet, users will authenticate with the same user ID and token(s) that they use for the corporate network—providing a single, consistent, and familiar login experience.

Throughout this guide, the term “Service Provider” is used to convey the notion of delivering authentication as a service; whether SAS is installed on-premises or as a cloud service. While authentication methods and interoperability remain significant factors, there is a strong focus in SAS on using automation to simplify and streamline user and authentication management; driving the cost of service delivery significantly lower. Key features include:

> **Workflow Automation**—Easy-to-configure policy engines that can manage users, provisioning tasks, access control, and much more based on changes in LDAP.

> **Management by Exception**—Alerts delivered through the UI, SMS, and email in response to business, security, and workflow events and thresholds.

> **Branding**—Complete customization of all user facing emails, web pages, alerts and URLs.

> **Billing**—Flexible inter- and intra-company billing for services.

> **Granular Security Roles and Scope**—Control over who can do what and to whom, captured in the database for extensive audit control, and alerts for real-time notification of changes to security settings.

No matter how many entities you add to your service, each will appear to have a discrete enterprise authentication server, what is referred to throughout this documentation as a “Virtual Server.”

When you, as a Service Provider, log in to the management console, you’ll be able to view and manage all of your accounts and their Virtual Servers independently. While you will likely standardize on a few service offerings, this independence means that you can customize your service for individual accounts without affecting any other account’s service. This includes pricing, billing, branding, and much, much more.

SafeNet Authentication Service does not obligate you to manage all aspects of an account’s service. In fact, you can allow some or all of your accounts to manage their own Virtual Server.

SafeNet Authentication Service includes workflow automation and management tools that can reduce your on-boarding and management costs to near zero. For example, by combining LDAP synchronization with provisioning rules, each time your account adds a user in their LDAP server, within minutes SAS will automatically create the user account in their Virtual Server and provision the user with a token—all of this without your staff clicking a mouse button.

Finally, you can use SafeNet Authentication Service to create Virtual Service Providers. As a Virtual Service Provider, your account can create and manage Subscribers. You can use Virtual Service Providers to create additional sales channels that resell your service under your banner or under their brand. Of course, Virtual Service Providers are not limited to being resellers. They can also be large, complex end-users accounts that need to independently extend and manage the service delivered to many subsidiaries or cost centers, or to accommodate multiple LDAPs and user data sources, or to share access to protected resources across organizational boundaries.
Management Console

The Management Console presents a row of tabs where you can perform all management functions.

**Figure 1: Subscriber Console (with Subscriber-configurable Customizations)**

Conventions

- **Tabs** group business, service, and management functions.
- **Modules** group specific functions, such as token management and user management.
  - Click a module name to toggle the module open/closed.
  - Unpinned modules close whenever another module is opened.
  - Modules that are pinned open will not close when another module is opened.
  - Click the information icon on the module bar to display context-sensitive help.
  - Modules that contain lists display a customization icon with which you can change the number of rows displayed in the list. An item count at the bottom of each list shows the number of items displayed and the total number of items that meet the search criteria. Use the arrows beside the item count to navigate through a long list of items.
- **Actions/tasks** enable you to add, view, edit, and delete accounts, users, and tokens.
Navigation arrows enable you to: go to the first; previous; next; or last page respectively, in cases where there are multiple pages of information.

**SafeNet Authentication Service + SafeNet Trusted Access**

STA (not available with SAS PCE/SPE) provides user and group access to cloud applications via context-aware policies that specify appropriate credentials.

SAS authenticates the STA users and groups as well as managing users, groups, and tokens.

When configured for your account, you open STA from SAS Shortcuts:

The components that apply when traffic is directed to either STA or SAS are shown in the figure that follows.
### Application Traffic Directed to STA

<table>
<thead>
<tr>
<th>STA</th>
<th>Policies</th>
<th>Applications</th>
<th>Dashboard</th>
<th>Smart SSO</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Tenant Creation and Mgmt</td>
<td>User Creation/Sync</td>
<td>Operators</td>
<td>Permission Control</td>
</tr>
<tr>
<td></td>
<td>Token provisioning</td>
<td>Token Authentication</td>
<td>AD Password Sync</td>
<td>AD Password Validation</td>
</tr>
<tr>
<td></td>
<td>SAS Logs</td>
<td>SAS Reports</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Application Traffic Directed to SAS

<table>
<thead>
<tr>
<th>SAS</th>
<th>Policies</th>
<th>Applications</th>
<th>Dashboard</th>
<th>Smart SSO</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Tenant Creation and Mgmt</td>
<td>User Creation/Sync</td>
<td>Operators</td>
<td>Permission Control</td>
</tr>
<tr>
<td></td>
<td>Token provisioning</td>
<td>Token Authentication</td>
<td>AD Password Sync</td>
<td>AD Password Validation</td>
</tr>
<tr>
<td></td>
<td>SAS Logs</td>
<td>SAS Reports</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When access attempts for an application are directed to STA, the STA policies fully govern the authentication requirements. In such cases, the SAS pre-authentication rules and Contextual Authentication policies do not apply.

SAS Operator tasks related to STA include:

> Provision Operators, roles, and permissions.

> Provision or synchronize your users. If domain passwords are used, use the SAS Synchronization Agent to synchronize your users and their domain password from an Active Directory.

> Provision tokens for the users.

In addition, SAS Administrator tasks related to STA are described in the *SAS Service Provider Administrator Guide*.
This chapter describes the functionality in the Virtual Server tabs, where you can perform the following tasks:

- Manage an account's virtual server.
- Manage an account's users.
- Provision users with tokens.
- Generate account specific security, compliance, billing, and inventory reports.
- Customize provisioning, enrollment, email, SMS, and other account specific processes.
The following modules are available on the SNAPSHOT tab:

> **Authentication Activity**—Lists up to 100 of the most recent authentications including diagnostic information.

> **Authentication Metrics**—Displays authentication activity metrics over various periods of time.

> **Token States**—Displays all tokens registered in the Virtual Server by state.

> **SMS Credits**—Displays the current SMS credit balance, alert level and SMS sent message count.

> **Allocation**—A complete listing of Virtual Server capacity and token inventory, including detailed transaction records.

> **References**—Displays the custom product name and version number, and URLs from which agents, software, documentation and terms of use can be downloaded or viewed.

**Figure 1: SNAPSHOT**

<table>
<thead>
<tr>
<th>Authentication Activity</th>
<th>Assignment</th>
<th>Tokens</th>
<th>Groups</th>
<th>Reports</th>
<th>Self-Service</th>
<th>Operators</th>
<th>Policy</th>
<th>Comms</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Authentication Activity**

The **Authentication Activity** module displays a list of the most recent authentications, up to a maximum of 100 records. Opening the module automatically refreshes the list.

**Figure 1: SNAPSHOT > Authentication Activity**

Entries in the list can be filtered according to the following **Result** values:

> **All (default)**—Displays all authentication activity.
> **Failure**—Displays only failed authentications. Note that push notifications that are rejected (the user tapped *It wasn’t me!* ) are listed as a **Failure**, with a message to indicate that it was due to user rejection.

> **Success**—Displays only successful authentications. Note that push notifications that are accepted (the user tapped APPROVED) are listed as a **Success**.

> **Challenge**—Displays SMS, Push, GrIDsure, CR token, and ID First authentication events. In the case of a challenge-response configured token, SAS sends the user a request for: an OTP (SMS); OTP (Push); GrIDsure image; or an 8-digit challenge (CR). Note that for push OTP challenges, additional information like geolocation and resource name are displayed in the message column.

Notes about **Push Notification** results:

- Push notifications are listed as **Challenge**.
- Push notifications that are accepted (“approved”) by the user are listed as **Success**.
- Push notifications that are rejected by the user are listed as **Failure**, with a message to indicate that it was due to user rejection.
- Push notifications that are ignored by the user do not result in another entry after the **Challenge**.

**NOTE** Push OTP is not available with SAS PCE/SPE.

> **Server PIN Provided**—Displays authentication events where the server has generated a PIN for the user.

> **User PIN Change**—Displays authentication events where the user has been prompted to change their PIN.

> **Outer Window Authentication**—The user provided a correct OTP value, but one that was outside of the inner window. Outer window success indicates that the user provided the next expected OTP. (Refer to "Synchronization" on page 101).

> **Change Static Password**—Displays events where the user was required to change their temporary static password. (Refer to "Token Policies > Global or Groups PIN Change" on page 100).

> **Password Change Failed**—Displays events where password change failed.

> **PIN Change Failed**—Displays events where user PIN change failed.

> **Skipped**—Displays authentications which are not required from the user due to policy settings; such as when the user requests access from a known network and/or device.

Click **Refresh** to sort the results according to revised criteria, or simply to update the list to include any authentications which occurred since the module was opened.

A count of records shown versus total records found is displayed at the bottom of the list. Click the **Customization** button on the module bar and enter a new number of rows in the text field to reset the number of records displayed.

The table of Authentication Activity results includes:

> **Time Stamp**—Displays the time stamp for each authentication event.

> **UserID**—Displays the userID provided by the user attempting to authenticate.

> **Actions**—Displays the action performed during the authentication.

> **Result**—(See the list of possible values at the beginning of this section.)

> **Credential Type**—Displays the type of credential used to authenticate.
SNAPSHOT

> **Serial #**—Displays the serial number of the token used to successfully authenticate. If the value is 0 and authentication succeeded, this indicates the use of a static password to authenticate.

> **IP**—Displays the IP address of the authentication request. Depending upon configuration, this could be the user’s access point (for example, VPN gateway) or agent (for example, OWA) IP address.

> **Message**—Displays a brief description about the authentication attempt.

---

**Authentication Metrics**

The Authentication Metrics module displays a list of pass, fail, and total authentications over various periods:

**Figure 1: SNAPSHOT > Authentication Metrics**

<table>
<thead>
<tr>
<th>Result</th>
<th>Today</th>
<th>Week-to-Date</th>
<th>Last Week</th>
<th>Month-to-Date</th>
<th>Last Month</th>
<th>Year-to-Date</th>
<th>Last Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass</td>
<td>5</td>
<td>12</td>
<td>19</td>
<td>11</td>
<td>30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fail</td>
<td>12</td>
<td>11</td>
<td>15</td>
<td>16</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>17</td>
<td>23</td>
<td>34</td>
<td>17</td>
<td>35</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

> **Today**—Lists values for the current day from 00:00:01, to the time at which the module was opened or most recently refreshed.

> **Week to**—Lists values from 00:00:01 on Monday of the current week, to the time the module was opened or most recently refreshed.

> **Last Week**—Lists values from 00:00:01 on Monday to 24:00:00 on Sunday of the previous week.

> **Month to Date**—Lists values from 00:00:01 on the 1st day of the current month, to the time the module was opened or most recently refreshed.

> **Last Month**—Lists values from 00:00:01 on the 1st day, to 24:00:00 on the last day of the previous month.

> **Year to Date**—Lists values from 00:00:01 on January 1 of the current year, to the time the module was opened or most recently refreshed.

> **Last Year**—Lists values from 00:00:01 on January 1 to 24:00:00 on December 31 of the previous year.

---

**Token States**

The token states module provides a count of all token types in the Accounts inventory by state:

**Figure 1: SNAPSHOT > Token States**

<table>
<thead>
<tr>
<th>Type</th>
<th>Initialize</th>
<th>Inventory</th>
<th>Assigned</th>
<th>Active</th>
<th>Suspended</th>
<th>Locked</th>
<th>Lost/Faulty</th>
</tr>
</thead>
<tbody>
<tr>
<td>MP</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gridtrue</td>
<td>0</td>
<td>19</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MobilePASS</td>
<td>0</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Password</td>
<td>0</td>
<td>87</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

> **Initialize**—Tokens that must be reinitialized before they can be assigned or provisioned.
Inventory—Tokens that are available for assignment or provisioning.

Assigned—Tokens that are assigned to a user but not yet used to authenticate.

Active—Tokens that are assigned to users and have been used to authenticate.

Suspended—Tokens that have been suspended by an Operator, preventing their use for authentication by the user to whom they are assigned.

Locked—Tokens that are in a locked state as a result of excessive consecutive failed authentication attempts.

Lost/Faulty—Tokens that have been marked as lost or faulty by an Operator.

**SMS Credits**

The SMS Credits module displays the current SMS Credits Balance, the low Balance Alert Level and the total SMS Messages Sent by this Account where:

**Figure 1: SNAPSHOT > SMS Credits**

> The **SMS Credit Balance** is decremented each time an SMS message is sent.

> The **SMS Messages Sent** value is incremented each time an SMS message is sent.

> The messages sent count resets to zero on the 1 millionth message sent.

> An alert is generated when the **SMS Credit Balance** equals the **Low Balance Alert Level**.

**Allocation**

The **Allocation** module summarizes server inventory. The Transaction Log displays a detailed list of all allocations and deallocations related to an account.
In the Allocation table:

> **Maximum**—This lists the maximum number of users that can authenticate against the server. Users may have multiple tokens and the total number of tokens issued to users may exceed server capacity. In all cases, these values are decremented as capacity and tokens/authentication methods are consumed. Note that some authentication methods consume the same resource. For example, all tokens consume a unit of capacity when assigned to a user. Likewise, MP-1/SMS, GridID, and Password consume a token license, therefore every time any one of these token/authentication methods is assigned to a user, totals for each token type in this class are decremented.

> **In Use**—This lists the capacity consumed as well as totals for all token/authentication methods that are in use.

> **Available**—List capacity and tokens available for assignment to users.

In the Transaction Log:

> **Transaction ID**—This is a unique number assigned by the server to each allocation by the Service Provider. The Transaction ID is a hyperlink if the transaction includes tokens. Clicking the hyperlink displays a list of all tokens by serial number included in the transaction.

> **Reference**—This is a value entered by the Service Provider when allocating the token, generally to aid in identifying the transaction when communicating with the account. This value may have meaning only to the Service Provider.

> **Allocate to**—This is the account which received the inventory allocation. For example, when a service provider allocates inventory, the value in this field will be the name of the account that received the inventory. Conversely during deallocation inventory is returned to the service provider and therefore the service provider name will appear in this field.

---

1 Prior to v3.2, capacity determined the maximum number of tokens and/or authentication methods that could be assigned to users.
> **Allocated From**—This is the account that allocated the inventory. The values in this field are the opposite of “Allocate to”.

> **Date**—This is the date and time of the allocation.

> **Quantity**—This indicates the item quantity of the transaction, usually tokens or SMS credits.

> **Product**—This indicates the primary item in the transaction. If the transaction contains tokens, this will display the token family such as KT, RB etc. A transaction cannot contain more than one token type.

> **Type**—This indicates Rental or Sale. Rental indicates that the allocation of tokens/authentication methods is part of a subscription, incurring a periodic charge for usage. Sale indicates that tokens/authentication methods have been purchased.

> **Capacity**—This indicates the quantity of capacity included in the transaction. Note that capacity is always a rental transaction even when included in a transaction with tokens marked as Sale.

> **Changed by**—This is the name of the Account Manager that performed the allocation.

Any transaction that came from a parent to a child can be used to allocate tokens to the child’s child if and only if all tokens, capacity, and credits that came with the transaction from the parent are available to be allocated.

**References**

The **References** module lists:

> The Custom Product Name set under COMMS > Custom Branding > Custom Product Name.

> The version number, retrieved from the file system, which is not configurable.

> URLs from which agents, software, documentation and terms of use can be downloaded or viewed. The values in this module are configured by the Service Provider. These values are automatically inherited by all on-boarded accounts. All virtual service providers can modify these values for their child accounts.

**Figure 1: SNAPSHOT > References**
The **ASSIGNMENT** tab enables you to manage all user: authentication methods/metrics, access restrictions, group memberships, and RADIUS attributes.

**Figure 1: ASSIGNMENT > Search User**

In addition to the Search User module, the following shortcuts display:

- **Create User**—Manually add users.
- **Import Users**—Import users from a .csv or tab delimited flat file.
- **Provisioning Tasks**—Remove users from tasks or extend tasks “time-to-live”.

**About Adding Users**

This chapter describes how to add and manage users. SAS enables you to add users in the following ways:

1. Manually, one user at a time, using the Create User shortcut.
2. Manually, importing one or more user records from a flat file.
3. Automatically by synchronizing with your Active Directory/LDAP server.

You can add users to the Virtual Server using both manual and automated methods, provided that UserIDs are unique. This allows you to extend authenticating to users that exist in your LDAP directory such as employees, as well as users that do not, such as contractors or business partners.

Consider using Automated Provisioning if you are using automated user creation in conjunction with an external LDAP/AD user source. Automated Provisioning can save administration time by automatically provisioning users with tokens, revoking tokens when users are deleted and applying authorizations based on LDAP groups and much more. (Refer to “Time Zone Offset” on page 125.)
Create User (shortcut)

Click the Create User shortcut to manually create a user record. Clicking the shortcut opens the Create User wizard.

Figure 1: Create User

The minimum requirement for adding a user is First Name, Last Name, User ID and email address. The Add button is disabled until these fields are populated. When the four required fields have been completed, clicking Add creates the record and opens the User Detail page (refer to “ASSIGNMENT” on page 30).

- **UserID**—Must be unique. If an identical UserID already exists, an error message is displayed.
- **E-mail**—Address is required. It is used in provisioning and self-enrollment.
- **Mobile/SMS**—This field is required to provision the user with the SMS/OTP authentication method and should contain the SMS number of recipient’s mobile device. The number must always begin with the country code.

  For example:
  
  In North America, the entry +1-613-599-2441 would result in a message delivery to: 16135992441 where 1 is the country code, 613 is the area code and the remaining 7 digits the phone number.
  
  In the UK, the entry 44 870 111 2222 would result in an entry in the format: 4408701112222 where 44 is the country code, 870 the city code and the remaining digits the phone number.

- **Container**—Use this option to place the user in a container.

- **Phone**—This is an optional field which may contain spaces, periods (.), dashes (-) and plus signs (+) in addition to digits.

- **Custom #1, Custom #2, and Custom #3**—These are optional fields that can be used to store additional data related to the user. The Custom #1 field is displayed in the User list. Note that the “Custom #x” labels can be changed from the Branding module, Custom labels section.

- **Alias #1, #2**—Aliases can be used to create additional pseudo-UserIDs for a user, allowing the user to log on using their UserID or aliases and any of the tokens assigned to the user. A common application of aliases would be for a person with two domain UserIDs and two roles. For example, Bob and bob-sysadmin, the former being a standard user account, the latter being an account with elevated privileges. In this example, either ID can use the same token.
Import Users (shortcut)

Bulk import of users is a convenient way to add many users in a single operation. To import users, begin by clicking the Import Users shortcut.

Figure 1: Import Users Wizard - Step 1

Select the import file format and field qualifiers (if any), and then click Next. Browse to and select the user data import file. Clear the File has a header row option if the import file does not include a header row, and then click Next.

Figure 2: Import Users Wizard - Step 2

In the Confirm Field Mappings and Import pane, select the appropriate Database field for each Import Data field. There are four required Database fields in the Confirm Field Mappings and Import pane (FirstName, LastName, UserID, and E-mail), each marked by an asterisk (*). UserID * entries must be unique.

Optionally, use Add Field and select the appropriate unused field name from the drop-down list to add further rows. Add Field can be used to force data not contained in the import file into the database. Default values can be created for any added fields.

Data entered into any of the Default Value fields will be used to populate user records that do not have data in the corresponding import file field.
Figure 3: Import Users Wizard - Step 3

Select the container into which users should be imported. The **Do not import if the UserID exists in the database** prevents a user record from being imported if it already exists in the database.

The **Update user record if the UserID exists in the database** will overwrite fields in the database with data from corresponding fields in the import file if a matching UserID is found in the database. Note that populated fields in the database will not be overwritten if a corresponding field is not included in the import file.

Click **Import** to complete the process. When import is finished the server will display the result of the import, showing users that were imported and/or any errors that occurred.

Figure 4: Import Users Wizard – Step 4

### Provisioning Tasks (shortcut)

The server creates a Provisioning Task each time the provision function is used.

To manage provisioning tasks:

1. Click the **Provisioning Tasks** shortcut.

   **ASSIGNMENT > Provisioning Task Management** displays.
The following functions and fields display:

<table>
<thead>
<tr>
<th><strong>Task</strong></th>
<th>This is a unique number generated by the server for each task. Click this link to view the task details.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operator</strong></td>
<td>This is the UserID of the Operator that created the provisioning task.</td>
</tr>
<tr>
<td><strong>Emailed to</strong></td>
<td>This is the last email address a provisioning task was sent to.</td>
</tr>
<tr>
<td><strong>Start Date</strong></td>
<td>This is the date the task was created.</td>
</tr>
<tr>
<td><strong>Stop Date</strong></td>
<td>This is the date by which all users must have completed self-enrollment.</td>
</tr>
<tr>
<td><strong>Count</strong></td>
<td>This is the number of users included in the provisioning task.</td>
</tr>
</tbody>
</table>
Edit | Use this link to modify the task for one or more users included in the task.
---|---
Remove | Use this link to remove a task from the list. Once a task is removed, any users in the task that have not completed enrollment will no longer be able to self-enroll.
Status | Indicates the status of each user’s enrollment:
| Active—User may still enroll the token.
| Completed—User has enrolled their token and used it to authenticate at least one time.
| Locked—User attempted and failed to enroll token within the maximum allowed attempts.
| Expired—User did not enroll token before the stop date.
Serial Number | The serial number of the enrolled token.

A provisioning task which has been completed (all tokens have been enrolled) is not displayed in this list. Its data is maintained for reporting purposes only.

**Edit a Provisioning Task**

To change a task, click the corresponding **Edit** link.

> **Remove**—This option will remove selected users from the task, and their ability to enroll will be canceled. Check the e-mail notification option to advise users that their enrollment has been canceled. This action cannot be reversed.

> **New Stop Date**—This option can be used to extend or shorten the enrollment period. Click **Apply** to complete the change or **Cancel** to abort changes.

**Search User**

You use the Search User module to:

> Find users that match a variety of search criteria.

> Manage individual users and their tokens.

> Provision tokens for multiple users in a single operation (see "Provision" on page 34).

**Search Fields**

The following fields in the Search User section of the module can be used to refine your search:

> **User ID**—The value the user types to identify themselves when logging in. Use * as a wildcard.

> **Last Name**—The surname of the user. Use * as a wildcard.

> **Auth Method**—The authentication method assigned to users:
  
  • **Any**—Include users that authenticate with any method.
  
  • **Token**—Include only users that authenticate with tokens.
  
  • **Password**—Include only users that authenticate with a static password set in the authentication server.
  
  • **External Credentials**—Include only users that are allowed to authenticate with credentials not validated by the server, such as a pass-through to an LDAP server. This option applies only to LDAP integration; it does not apply to LDAP synchronization.

> **Email**—The email address of the user.
> **Container**—The container within which you want to restrict the search. See "Container Maintenance" on page 65.

> **Account State**—Locked or Unlocked. For more information see "Search Result Fields" below.

**Search for Users**

To display a list of users in the Virtual Server:

1. Type the search criteria that apply in the fields provided (for example, type * in the User ID field).
2. Click the **Search** button.

   SAS displays a list of users that meet the search criteria.

**Search Result Fields**

**Figure 1: Search Result Fields**

The following fields display in the search results:

> **User ID**—Click to display additional modules that describe a user.

> **Last Name**—The user’s surname.

> **First Name**—The user’s first name.

> **Custom #1**—One of three fields that can be populated with custom data to distinguish the user from other similarly named users. Examples include employee number, department etc. Note that the label “Custom #1” can be changed in the Branding module of the virtual server.

> **Auth Method**—An indication of the primary authentication method assigned to the user. Options include PwD (Password stored with the user account in the Virtual Server), Token (indicates a two-factor authentication method is assigned).
> **RADIUS Attr**—Indicates whether or not RADIUS attributes have been set for the user. This does not reflect RADIUS attributes applied to a group to which the user may belong.

> **Auth State**—Set to Active if the user can authenticate against the service. Set to Locked if authentication failures exceed the Account Lockout/Unlock Policy (refer to "Account Lockout/Unlock Policy" on page 90). Set to Assigned if the user has not authenticated with the assigned token. If multiple tokens are associated with the user, state precedence in the list is Locked, Active, Assigned.

> **Account State**—Locked or Unlocked. Locked when an account is in breach of the dormant account policy (see "Dormant Account Lockout Policy" on page 91). When an account is locked, the user's authentication attempts fail, regardless of the Auth State. When you unlock an account, you must also verify that the auth state is unlocked. The lock state of the account is local to SAS and is different from the LDAP lock state.

> **Container**—Displays the container in which the user account resides. See "Container Maintenance" on page 65.

> **Provision** (Button)—Provision all selected users in the list with tokens in one simple operation. See "Provision" on page 34.

> **Delete** (Button)—Delete all selected users (excluding LDAP integrated and LDAP synchronized).

> **Account Unlock** (Button)—Unlock an account.

### Additional ASSIGNMENT Modules

To display comprehensive information about a user:

1. Click the desired **UserID** from the search results (see "Search Result Fields" on the previous page).

   Additional ASSIGNMENT modules display.
The additional ASSIGNMENT modules are:

> **User Detail**—This module displays basic user information. User detail can be modified for all users that were manually created or imported. User accounts created by LDAP integration/synchronization must be modified in the LDAP directory.

> **Tokens**—Use this module to assign, provision and manage all tokens associated with an individual user.

> **Authentication Metrics**—Displays the individual user’s authentication metrics over various periods of time.

> **Authentication Activity**—Displays authentication history for up to 100 of the user’s most recent authentication.

> **Access Restrictions**—Use this to set specific times/days and periods during which the user is allowed to authenticate or prevent a user from being authenticated.

> **Group Membership**—Use this module to add or remove group memberships for the selected user. Groups can be used to automate provisioning and/or determine if the user is allowed to authenticate and/or be granted access to specific resources.

> **RADIUS Attributes (user)**—Use this module to apply RADIUS attributes to the selected user.

> **SAML Services**—Use this module to manual enable a user to authenticate at one or more configured SAML Service Providers. Service Providers must be configured before this module can be used. See "SAML Service Providers" on page 165.
User Detail

The User Detail module displays basic information about a user. If the user account was manually created or imported, the Edit button will be active, allowing the information to be updated. If the user account is synchronized or integrated with LDAP, the Edit button will be disabled and required edits to the user account information must be made in LDAP.

Figure 1: User Detail

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Container</td>
<td>This is the container in which the user account resides and can be changed by selecting from the drop-down list and applying the change.</td>
</tr>
<tr>
<td>Custom #1, 2, 3</td>
<td>These fields are available for holding additional information about the user.</td>
</tr>
<tr>
<td>Alias #1, 2</td>
<td>These are alternate login credentials that can authenticate with the user's tokens.</td>
</tr>
</tbody>
</table>

Tokens

Use the ASSIGNMENT > Tokens module to:

> Manage (add, provision) user tokens.
> Assign a temporary static password to a user.
> View the tasks associated with a user to determine if the user is to be provisioned with a token.

Figure 1: ASSIGNMENT > Tokens

The Tokens module provides the following functions and information about a user’s tokens:

> Assign (button)—Typically used to manually issue hardware tokens, one user at a time.
> **Provision** (button)—Issue any token type (hardware, software, SMS, GrID) to 1 or more users simply. This option works hand-in-hand with self-enrollment. Provisioning provides major time-savings for administrators and is the recommended method for associating a token with a user.

> **Change Log** (button)—View the last five token management tasks performed for this user.

> **Password** (button)—Assign a temporary static password to a user that does not have an active token. Disabled if the user has any other assigned authentication method.

> **Manage**—Provides access to all management functions for the token.

> **Type**—Displays the authentication method assigned to the user.

> **Target**—Device to which a token is deployed (e.g., Windows™ PC, iPhone™, BlackBerry™, etc.)

> **Serial #**—Displays the serial number of the token or “Password” if a static password is allowed.

> **State**—The state of the token/authentication method:

  - **Active**—Can be used to authenticate.
  - **Suspended**—Cannot be used to authenticate until it is reactivated by an operator.
  - **Locked**—Cannot be used to authenticate until the unlock policy is triggered or until it is reactivated by an operator. The user has exceeded the maximum number of consecutive failed logon attempts.
  - **Assigned**—Issued to the user, but not yet used to authenticate.

> **Provisioning Rule**—Displays the method by which a token was provisioned: <Rule Name>, "Manual", or blank space (if SAS is unable to determine the rule name).

> **Initial PIN**—The 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. SAS clears the Initial PIN field as soon as the user completes the PIN change.

### Assign

To assign a token to a user:

1. Click **Assign**.

![Tokens](image)

2. To refine the inventory list of tokens available for assignment, do one of the following:

   - Select from the **Token Type** drop-down list.
   - Type a partial serial number.
3. Click **Search**. The tokens are listed.

![Tokens](image1)

4. Click **Select** for the token to assign. The Assign Token options are displayed.

![Tokens](image2)

5. Click **Assign** to save the selection.

The token is now assigned to the user.

![Tokens](image3)

If this is a hardware token, you should give this to the user now along with the initial PIN shown in the last column of the list. The default policy requires the user to change this PIN on first use of the token to a value known only to them. The value in the **Initial PIN** field is cleared when the user completes their PIN change.

If this is a software token, you must ensure that the MP-1 application is installed on the user’s PC, BlackBerry™, iPhone etc. before proceeding.
6. To assign an MP-1 token, click the **Manage** hyperlink, and then click the **Issue** button.

Select the delivery method for the token profile.

- **Save the token file**—This saves the token profile to a location specified by the Operator. The file must be transferred to the user’s device.
- **E-mail the token and PIN to the user**—Choose this option to e-mail the token and initial PIN to the user. Typically this method is used for installation of the MP token on a laptop.

**Provision**

You can automatically provision and securely deliver tokens to one or more users, regardless of their physical location, in a single bulk operation. This process has significant advantages:

> It saves a tremendous amount of time for Operators.
> It is secure because only the intended recipient can enroll and activate their token.
> It can be used with hardware and software tokens.
> It is not necessary to deliver a specific hardware token to each user.
> It can be time-limited, requiring users to enroll their tokens on or before a specified date.
It can be used to coordinate migrating users from static passwords to token authentication without interruption of service.

To use the provision function, begin by selecting one or more users from the **Users** list, and then click the **Provision** button.

**Figure 2: Selecting Users for Provisioning**

This will refine the list to include only those users selected for provisioning. Once you’ve verified the list of selected users, click **Provision** again. Next, select the type of token to be issued to each of the users in the list. You can add a comment about this provisioning task in the **Description** field.

- **Available**—Indicates the quantity tokens by type in inventory and available for provisioning
- **Reserved for Provisioning Tasks**—Specific tokens (i.e., serial numbers) are not removed from inventory until enrollment is complete. This column represents the amount of inventory that has been committed by other provisioning tasks.
Select the Token Type to be Provisioned

Click **Provision > Confirm** to complete the process and create a Provisioning Task.

**Self-Enrollment**

Each user in the provisioning task will receive an email with instructions for enrollment. The content of the email message varies, depending on the token type. Message content can be customized including the use of HTML and images (see “SAS Service Provider Branding Guide”).

**Figure 3: Default MP Token Enrollment Message**

```
James Brown:
Your self-enrollment account has been created.

If you are enrolling a hardware token, and do not have your token yet, please contact your system administrator.

Please, go to the following URL to enroll with BlackShield ID:


If the above link does not work, please copy and paste this url to your web browser.
```
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.

Figure 4: Suspend a Token

If a user has multiple active tokens, the various password options will not be available. If the user has only one active token and the virtual server temporary password policy allows assignment of a password, (refer to "Token Policies > Global or Groups PIN Change" on page 100) 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/AD Password**—The user’s token will be suspended and the user will be allowed to use their LDAP/Active Directory password to authenticate. Note that this option is displayed only if the SAS LDAP Integrator service is set up in SAS PCE/SPE, or if Active Directory Password Sync is set up for SAS Cloud, (requires SAS v3.5.1 or later) and the user has a synchronized Active Directory password. Refer to **Enable password synchronization** in the *Synchronization Agent Configuration Guide* for additional details.

**NOTE** Currently, SAS does not synchronize the password expiry state. The AD password is handled as a cached credential, where the credential remains valid until the user updates it through the domain controller.
NOTE The Account Lockout policy (defined in POLICY > User Policies) temporarily locks a user’s AD password if the Account lock threshold is exceeded. The AD password is automatically unlocked after the configured Account lock duration. Assigned AD passwords appear in the user’s token list, and can also be manually unlocked by the Operator. However, the Operator cannot manually unlock unassigned AD passwords that can be used in pre-authentication rules or STA password validation. Both assigned and unassigned AD passwords are always automatically unlocked according to the Account Lockout policy. (Refer to "Account Lockout/Unlock Policy" on page 90.)

> 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. (Refer to “Temporary Password Policy” on page 100.)
- **Change 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, clicking **Unlock** will reactivate the token. Check 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.

**Figure 5: Unlock a Token**

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. (Refer to "POLICY > Token Policies" on page 93.) 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 the token type. Refer to the SafeNet Authentication Service Tokens Guide. For example, for an MP-1 token, 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.

**Figure 6: Unlock Token Example**

![Unlock Token Example](image)

**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.

**Figure 7: New PIN**

![New PIN](image)

The **Change PIN on first use** option is disabled if the change PIN policy is set to prevent Operator override. If enabled, the Operator can remove the requirement to change PIN on first use.
Resync

Use this option to resync a token or test a token if there are repeated failed authentication attempts with it. Generally, a resync is not required. 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.)

![Resync Example](image)

- **For OATH, SafeNet Gold/Platinum tokens**—Have the user generate two passcodes and enter these in the correct order. A message will be displayed confirming the success or failure of the resync process.

![OATH Resync Example](image)

Initialize

Use initialize to generate new token seeds and change the operating parameters of hardware tokens. The current token template (refer to "Token Templates" on page 94) 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.
**Warning** MP-1 tokens are deprecated. Please refer to the End-of-Sale announcement for full details.

**Figure 8: Initialize Token**

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

**Figure 9: Revoke Token**

Use this button to revoke a token. A revoked token can no longer be used to authenticate.

If the Authentication Type is Password, and the Revoke Password check box is not selected, the user can still authenticate using a previously assigned static password. The user can also authenticate with any other active token associated with their account.

- **Return to Inventory, Initialization Required**—Choose 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. Generally, this option is used with RB-1 PIN Pad tokens.
- **Return to Inventory, token does not need to be reinitialized**—Choose 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.
View a User’s Tasks

Use the Tokens module to view the outstanding provisioning tasks that apply to the user’s tokens.

**Figure 10: ASSIGNMENT > Tokens**

![Tokens module screenshot]

The **Provisioning Tasks** table is not displayed if there are no outstanding tasks. The Provisioning Tasks table cannot be edited.

In the **Provisioning Tasks** table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task</td>
<td>If the operator has provisioning management permissions, this is a hyperlink to the Provisioning Task Management module where the selected task is expanded.</td>
</tr>
<tr>
<td>Operator</td>
<td>This is the UserID of the Operator that created the provisioning task.</td>
</tr>
<tr>
<td>Start Date</td>
<td>This is the date the task was created.</td>
</tr>
<tr>
<td>Stop Date</td>
<td>This is the date by which the user must have completed self-enrollment.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates the status of the user’s enrollment.</td>
</tr>
</tbody>
</table>

Resend a Token Provisioning Task

An Operator can resend a provisioning task message to a user:

1. Click **Virtual Servers > Assignment > Tokens**.
2. Select the User ID of the user whose provisioning task you want to resend.
3. In the **Tokens** section, under **Provisioning Tasks**, click **Edit**.
4. Click **Resend**.

By default, the email address saved in the user’s SAS profile is automatically entered into the **E-mail** field. You can specify an alternate email address if necessary; however, this email address will not be retained in the system once the provisioning task is resent. Note that only active provisioning tasks can be resent. The **Stop Date** for the task will be adjusted based on the Self-Enrollment Policy.
Figure 11: Resend Provisioning Task

Authentication Metrics
This module displays authentication metrics for the user reflecting pass, fail and total authentication results for the current day, current week, previous week, month to date, previous month, year to date, and previous year.

Figure 1: ASSIGNMENT > Authentication Metrics

Authentication Activity
This module is identical to the Authentication Activity module on the SNAPSHOT tab (refer to "Authentication Activity" on page 16) with the exception that all data is for the selected user.
Figure 1: ASSIGNMENT > Authentication Activity

Access Restrictions

Use this module to set time, day, or date restrictions on when a user can authenticate. By default, restrictions are disabled.

**NOTE** If the Virtual Server is configured for LDAP integration, consider using Active Directory time, day, or date restrictions. Any changes to restrictions in Active Directory will automatically be applied by the authentication server.
1. Select the **Enable Restrictions** check box.

2. Specify the date, time, or day restrictions:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Start Date</strong></td>
<td>The user cannot authenticate prior to this date.</td>
</tr>
</tbody>
</table>
| **Stop Date** | The user cannot authenticate starting on this date. For example, to specify one day of access on 2017/09/01:  
|               | > Start Date: 2017/09/01  
|               | > Stop Date: 2017/09/02                                                     |
| **Start Time**| The user cannot authenticate prior to this time of day, within the Start Date and Stop Date range.  
|               | For example, to specify authentication between 17:00-22:00 on 2017/09/01:  
|               | > Start Date: 2017/09/01  
|               | > Stop Date: 2017/09/02  
|               | > Start Time: 17:00  
|               | > Stop Time: 22:00                                                        |
| **Stop Time** | The user cannot authenticate after this time of day, within the Start Date and Stop Date range.  
| **On the following days** | The user can authenticate on only the checked days.  |

3. Click the **Apply** button.
4. To view up to the last five (5) changes that were made to this user’s access restrictions, click the **Change log** button.

The change log includes the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modified Time</td>
<td>Indicates the time and date stamp of the applied change.</td>
</tr>
<tr>
<td>Change By</td>
<td>Displays the UserID of the Operator who applied the change.</td>
</tr>
<tr>
<td>Change by Account</td>
<td>Displays the name of the account that applied the change.</td>
</tr>
</tbody>
</table>

**Group Membership**

Use this module to manage the user’s group memberships. Groups can be used for auto-provisioning and for authorization (RADIUS attributes and/or pre-authentication rules). Click the **Add** button, select the group membership, and then click **Apply**. To remove a membership, click the corresponding **Remove** link and confirm the action.

**Figure 1: ASSIGNMENT > Group Membership**

To modify the memberships of many users at a time, use the **Group Membership** module on the **GROUPS** tab instead.

**RADIUS Attributes (user)**

Use this module to apply RADIUS attributes to the user. Note that user attributes take precedence over attributes applied to groups to which the user belongs. The functionality of this module is identical to the **RADIUS Attributes** module on the **Groups** tab except that changes applied here are applied to the user. (Refer to “RADIUS Attribute (Group)” on page 64.)

To define user-based RADIUS attributes, you can use the SAS FreeRADIUS Agent or Microsoft NPS. The FreeRADIUS Agent and Microsoft NPS are capable of returning RADIUS attributes defined in SAS to the RADIUS client.

By default, RADIUS return attributes are defined for all Auth Nodes, or they can be restricted to selected Auth Nodes by using the **Restrict To Auth Nodes** check box.
When authenticating with a RADIUS token, SAS also passes RADIUS attributes to the RADIUS client that were received from an external RADIUS server. This is beneficial for authentication requests that may go to a third-party authentication service and then return through SAS. This is also useful for migrations where an external RADIUS server continues to authenticate users that are not yet migrated to SAS. With this feature, the RADIUS client can receive the same external attributes during the migration phase than before migration (without SAS).

Also, refer to "Block RADIUS Authentication" on page 161.

NOTE  SAS returns the attributes received from the external server after attributes that are configured in SAS. If the same attribute is configured in the external server and in SAS but with different values, it is up to the RADIUS client as to how this is interpreted. It is advised to avoid conflicting attribute definitions in SAS and the external RADIUS server.

SAML Services
Use this module to manually enable a user to authenticate against one or more SAML Service Providers.
To manage SAML services, click **ASSIGNMENT > Search User > (User ID) > User Detail: (User ID) > SAML Services**. The following functions are available:

- **Service**—Lists all of the configured SAML Service Providers. See "SAML Service Providers" on page 165.
- **SAML Login ID**—The User ID that is returned to the service provider in the SAML assertion. If your service provider (e.g., Salesforce) requires a user ID of name@domain.com, and this is identical to the user’s email address, choose the **E-mail** option. Doing so allows the user to consistently use their user ID to authenticate regardless of the service provider’s requirements. Typically, a service provider will require either the user ID or e-mail. For all other cases, choose the **Custom** option and enter the required user ID to be returned.

You can automate the creation/removal of SAML Services for users by creating a SAML provisioning rule. Refer to "SAML Provisioning Rules" on page 131.
The TOKENS tab enables you to view, import, bulk-assign, and initialize tokens.

<table>
<thead>
<tr>
<th>Snapshot</th>
<th>Assignment</th>
<th>Tokens</th>
<th>Groups</th>
<th>Reports</th>
<th>Self-Service</th>
<th>Operators</th>
<th>Policy</th>
<th>Comms</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>View Change Log</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Display the last five changes to the token properties; including: date and time of change, Operator ID, and changed values (&quot;View Change Log (shortcut)&quot; below).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>List Lost Tokens</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Display a list of tokens that have been marked as lost or faulty by an Operator (&quot;List Lost Tokens (shortcut)&quot; on the next page).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>List Locked Tokens</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Display a list of tokens that are in a locked state as a result of excessive consecutive failed authentication attempts (&quot;List Locked Tokens (shortcut)&quot; on the next page).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tokens</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>List registered tokens and move tokens between containers (&quot;Tokens&quot; on the next page).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Import SafeNet Tokens</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Import records for unallocated tokens that have a .btk, .dat, or .xml file (&quot;Import SafeNet Tokens&quot; on page 53).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bulk Assign Third Party Tokens</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Automatically assign a token by serial number to an existing UserID (&quot;Import Third Party Tokens&quot; on page 55).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Import Third Party Tokens</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Import RSA/SecurID AES time-based tokens serial number records (&quot;Configure the Window Size for a Time-based Token’s First Authentication&quot; on page 54).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Initialize Token</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Initialize or change the operating parameters of hardware tokens on your server, such as OTP length and strength (&quot;Initialize Token&quot; on page 58).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

View Change Log (shortcut)

The View Change Log shortcut opens TOKENS > Tokens to display the record of changes to token properties; including: date and time, Operator ID, and values.
Figure 1: View Change Log (Shortcut)

List Lost Tokens (shortcut)

The List Lost Tokens shortcut opens TOKENS > Tokens to display the search results for tokens that have been placed in a lost or failed state by the Operator (State = Lost/Failed).

List Locked Tokens (shortcut)

The List Locked Tokens shortcut opens TOKENS > Tokens to display the search results for tokens that are locked due to excessive consecutive failed authentication attempts (State = Locked).

Tokens

TOKENS > Tokens enables you to find/view details about all registered tokens.

<table>
<thead>
<tr>
<th>Section</th>
<th>Field/Action</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Log</td>
<td></td>
<td></td>
<td>Display the last five token management operations in the Virtual Server. The log displays a row for each token operation that includes the token</td>
</tr>
<tr>
<td>Section</td>
<td>Field/Action</td>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Search</td>
<td>Token Type</td>
<td></td>
<td>Refine the list to a specific type of token.</td>
</tr>
<tr>
<td>Search</td>
<td>State</td>
<td></td>
<td>Refine the list to tokens in a selected state.</td>
</tr>
<tr>
<td>Search</td>
<td></td>
<td>All</td>
<td>List all tokens; include every state.</td>
</tr>
<tr>
<td>Search</td>
<td></td>
<td>Inventory</td>
<td>The token is available for assignment to users.</td>
</tr>
<tr>
<td>Search</td>
<td></td>
<td>Initialize</td>
<td>A hardware token in inventory that must be initialized before it becomes available for assignment.</td>
</tr>
<tr>
<td>Search</td>
<td></td>
<td>Assigned</td>
<td>The token is no longer in inventory. It has either been manually assigned to a user but not activated or is part of a bulk provisioning operation and has not yet been enrolled by a user.</td>
</tr>
<tr>
<td>Search</td>
<td></td>
<td>Active</td>
<td>The token is assigned to a user and has been enrolled or used to authenticate.</td>
</tr>
<tr>
<td>Search</td>
<td></td>
<td>Suspended</td>
<td>This indicates that an Operator has placed the token in a suspended state, making it invalid for authentication but leaving it assigned to a user. This is usually done if there is a security concern such as a lost or misplaced token. Suspended tokens can be reactivated by an Operator when the security concern has been resolved.</td>
</tr>
<tr>
<td>Search</td>
<td></td>
<td>Locked</td>
<td>This state occurs when a user exceeds the maximum consecutive failed logon attempts threshold. A locked token can be reactivated by an Operator. The automatic locking and unlocking of tokens is controlled by the Account Lockout/Unlock Policy.</td>
</tr>
<tr>
<td>Search</td>
<td></td>
<td>Lost/Failed</td>
<td>This is a state applied by an Operator when revoking a token. Revoked tokens are returned to Inventory in this state where they can be permanently removed or if the token is subsequently found or determined to function properly, it can be reinitialized into the Inventory state.</td>
</tr>
<tr>
<td>Search</td>
<td>Serial #</td>
<td></td>
<td>Search by partial or complete serial number to find a range or specific token.</td>
</tr>
<tr>
<td>Search</td>
<td>Container</td>
<td></td>
<td>Lists only the tokens that are held in the selected container. (Refer to &quot;Container Maintenance&quot; on page 65.)</td>
</tr>
<tr>
<td>Search</td>
<td></td>
<td>All</td>
<td>List all tokens; include every container.</td>
</tr>
<tr>
<td>Search</td>
<td></td>
<td></td>
<td>Search for the values placed in the Token Type, State, Serial #, and Container fields.</td>
</tr>
<tr>
<td>Search</td>
<td></td>
<td></td>
<td>Clear the contents of the fields in the Search section.</td>
</tr>
</tbody>
</table>

**Token Search Results**

The result of a search is displayed in the Token List.
Figure 1: TOKENS > Search Results

From this list you can:

> **Move**—Move the selected tokens to a different container.

> **Reset PIN Policy**—Apply the current Server-side PIN policy to the selected range of tokens. This function is not available for tokens initialized with Token-side PINs. Tokens must be in the Inventory state.

> **Delete**—Remove the selected token from the Virtual Server Inventory. Delete cannot be used with rented tokens. Rented tokens must be deallocated by the Service Provider.

> **Serial Number**—Click to display the token operating parameters, in-use statistics, organizational ownership, and MobilePASS app details (the target OS, Push OTP state, and the device type), as shown in Figure 2. Under **Mobile App**, the **Push OTP** field displays only if the push feature is enabled in **POLICY > Token Policies**. If the push feature is enabled, the state of the Push OTP feature is displayed here. Push OTP is not available with SAS PCE/SPE. The states are:

  - **Enabled**—Displays if the user has permitted Push OTP notifications on the device.
  - **Disabled**—Displays if the user has not permitted Push OTP notifications on the device, but the application is push capable (for example, on MobilePASS+).
  - **Not Applicable**—Displays if the application is not push capable (for example, on MobilePASS 8).

> **User ID**—Click to access the user’s record and management functions. The additional **ASSIGNMENT** modules display (see "Additional ASSIGNMENT Modules" on page 29).

> **Close**—Hide the Token List section.
Figure 2: Token Detail

Import SafeNet Tokens

**TOKENS > Import SafeNet Tokens** enables you to import .btk and .dat files into inventory for a variety of tokens. You can also import .xml files (available for SAS SPE/PCE only).

<table>
<thead>
<tr>
<th>Action/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import</td>
<td>Import tokens from a selected file into inventory. By default, token templates force a user-selected PIN on imported tokens. By default GOLD/eTokens do not have PINs, unless their token template policy is changed.</td>
</tr>
<tr>
<td>Action/Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>NOTE</strong></td>
<td>Import will fail for tokens with a serial number that already exists in the Virtual Server. Token seed records can be re-imported after duplicates are removed from the Virtual Server inventory. The maximum file size is 10 Mb.</td>
</tr>
<tr>
<td>Save Log</td>
<td>Store the import results (also displayed on the import token UI) to the default web browser download folder.</td>
</tr>
<tr>
<td>Container</td>
<td>The container into which token inventory will be allocated. The “Default” container holds all tokens unless additional containers have been created and inventory added to them. For more information about containers refer to “Container Maintenance” on page 65.</td>
</tr>
<tr>
<td>Import File</td>
<td>The file containing the tokens to be imported.</td>
</tr>
<tr>
<td>Browse</td>
<td>Locate the file to be imported.</td>
</tr>
</tbody>
</table>

### Configure the Window Size for a Time-based Token’s First Authentication

You can configure an expanded evaluation window (maximum value = 300) that applies only to the first authentication attempt after a token record is imported - to adjust for token drift - so that the time-based tokens can be conveniently synchronized. Subsequent authentication attempts with the tokens will be restricted to the Inner window (maximum = 10) and Outer window (maximum = 100) values. See "Synchronization" on page 101 for information about Inner/Outer windows.

To configure the window size for a time-based token’s first authentication:

1. Click **POLICY > Token Policies > Synchronization**. The Synchronization section displays.
2. Type a value in the field provided for the “First authentication time-based OTP window size”.

   **NOTE** The recommended size for a first-authentication time-based OTP window is “200”. A too-small value will result in unexpected challenges for additional authentication from SAS. A too-large value may reduce the security of your authentication process.

3. Click **Apply** to save your changes.

   **NOTE** If multiple first-authentication attempts fail, verify that the “First authentication time-based OTP window size” is set correctly. Next, to reset the affected tokens, delete them from SAS and re-import the file with the tokens.

### Import SafeNet Tokens

To import SafeNet Tokens (this feature is available for SAS SPE/PCE only):

1. Click **TOKENS > Import SafeNet Tokens**.
2. Click **Choose File**.
3. Browse to the file location.
4. Double-click the file to be imported (maximum file size = 10 Mb).

   The file name displays in the “Choose File” field.
5. Click **Choose File**. The file name displays in the “Selected File” field.

6. (For xml files only) SAS prompts for a password. Type your password in the field provided.

7. Click **Import**. SAS displays the result (for example, a list of the tokens that were added).

8. (Optional) Click **Save Log** to save the import results to your default web browser Download folder.

   An example of the import results log follows:

   * The following tokens have been successfully added:
     Total: 2 tokens added.
     Token: 1, Serial: GAKT00040D6D, Type: eToken
     Token: 2, Serial: GAKT00040D6E, Type: eToken

   The following tokens already exist.

     Total: 2 tokens exist.
     Token: 1, Serial: GAKT00040D6F, Type: eToken
     Token: 2, Serial: GAKT00040D71, Type: eToken

9. Click the **Tokens** module. The Search section displays.

10. Select **eToken** from the drop-down menu in the Token Type field.

11. Click **Search**. A list of the search results displays.

12. Click a **Serial #** from the Token List. SAS displays details about the token.

**Import Third Party Tokens**

**TOKENS > Import Third Party Tokens** enables a host service provider to import tokens into inventory. Tokens are automatically bound to an existing UserID in SAS if the import file contains a matching UserID; otherwise the tokens are placed in inventory.
<table>
<thead>
<tr>
<th>Action/Field</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import</td>
<td></td>
<td>Import tokens from a selected file into inventory. By default, the imported tokens do not have PINs unless their token template policy is changed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE</strong> Import will fail for tokens having a serial number that already exists in the Virtual Server. Token seed records can be re-imported after duplicates are removed from the Virtual Server inventory. The maximum file size is 10 Mb.</td>
</tr>
<tr>
<td>Save Log As</td>
<td></td>
<td>Store the provisioning results (also displayed on the import token UI) to the default web browser download folder.</td>
</tr>
</tbody>
</table>
| Token Type   | RADIUS | Use with any token type, provided the third-party authentication server will accept authentication requests via RADIUS from SAS. To automatically bind a specific token to a user during import:  
> Ensure that the UserID already exists in SAS.  
> Ensure that a record in the import file contains the corresponding UserID and token serial number. Each record in the import file must be in the format:  
   UserID,SerialNumber,yyyy/mm/dd  
   Where: **Serial Number** is 12 characters (pad with leading 0 if necessary).  
If a UserID is omitted in the import record, the token will be imported and placed in inventory. Though the token can be assigned or provisioned to a user in SAS, care must be taken to ensure that the same token is assigned to the same user in the third-party RADIUS server. Use containers to segregate imported tokens that will be allocated to Subscriber Accounts. |
|              | SecurID | Use with SecurID tokens, provided the RSA Authentication Manager is configured to accept authentication requests via RADIUS from SafeNet Authentication Service. To automatically bind a specific token to a user during import:  
> Ensure that the UserID already exists in SafeNet Authentication Service.  
> Ensure that a record in the import file contains the corresponding UserID and token serial number. Each record in the import file must be in the format:  
   UserID,SerialNumber,yyyy/mm/dd,#  
   Where: **Serial Number** is 12 characters (pad with leading 0 if necessary).  
   # is the length of the generated passcode. Allowed values are 6 or 8. If omitted, 6 is assumed.  
If a UserID is omitted in the import record, the token will be imported and placed in inventory. Though the token can be assigned or provisioned to a user in SafeNet Authentication Service care must be taken to ensure that the same token is assigned to the same user in the RSA Authentication Manager. |
| Container    |        | The container from which token inventory should be allocated. Default holds all tokens unless additional containers have been created and inventory added to them. For more information refer to "Container Maintenance" on page 65. |
| Import File  |        | The file containing the tokens to be imported. Click Browse to navigate to the file. |
Typically, OATH-compliant tokens work fine with SAS. However, support can only be provided on a best effort approach as long as the 3rd party tokens have not been fully validated. You may be instructed to work with the token vendor for a resolution.

For SAS Cloud: All 3rd party token seed records must be provided to Gemalto for import into SAS Cloud.

For SAS PCE/SPE: All token seed records (except those in XML format) must be provided in an unencrypted format and converted to .btk file format by Gemalto. XML token seed records can be imported directly.

### Bulk Assign Third-Party Tokens

The tokens must exist in inventory prior to using this module.

This module is available to Virtual Service Provider and Subscriber account and allows tokens from various manufacturers to be managed by SafeNet Authentication Service. Tokens will automatically be bound to an existing UserID in SafeNet Authentication Service if the token import record contains a matching UserID.

The token records must be added to your token inventory by your Service Provider. Your Service Provider will require a file containing a record for each token. Refer to “RADIUS Tokens”.

If an import record does not contain a UserID, the token will be imported and placed in inventory.

**Figure 1: TOkENS > Bulk Assign Third-Party Tokens**

Options include the following:

> **RADIUS Tokens**—This import method can be used with any token type including RSA/SecurID, provided the third-party authentication server will accept authentication requests via RADIUS from SAS.

**Step 1**: Provide a **Third-Party Token Import** file to your service provider.

- This file must be comma delimited file (.csv) and contain a record for each token being imported. Each record must be in the following format:
  
  SerialNumber,yyyy/mm/dd

- Note the leading “,”

  Serial Number is 12 characters (pad with leading 0 if necessary)

  These tokens will appear in your token inventory when the Service Provider has completed the import process.

**Step 2**: To automatically bind a specific token to a user during import:

- Ensure that the UserID already exists in SafeNet Authentication Service.
• Ensure that a record in the import file contains the corresponding UserID and token serial number. This file must be comma delimited file (.csv). Each record in the import file must be in the format:

UserID,SerialNumber,yyyymm/dd

Where: **Serial Number** is 12 characters (pad with leading 0 if necessary)

If a UserID is omitted in the import record, the token will be imported and placed in inventory. Though the token can be assigned or provisioned to a user in SafeNet Authentication Service, care must be taken to ensure that the same token is assigned to the same user in the third-party RADIUS server.

**SecurID Tokens**—Not available to Virtual Service Provider or Subscriber accounts.

**OATH Token**—Third-party OATH tokens can be imported into SafeNet Authentication Service, however, these must be converted to a special .btk format prior to import. Contact Gemalto for instructions.

## Initialize Token

This module can be used with CRYPTOCard/SafeNet RB and KT series hardware tokens. It applies the corresponding series template which determines the operating characteristics of the token such as passcode length, strength, PIN options and so on. (Refer to **"POLICY > Token Policies" on page 93.**)

**Figure 1: TOKENS > Initialize Token**

This process requires an RB and/or KT token initializer attached to a USB port on the operator’s PC. The necessary drivers can be downloaded and installed using the links displayed in the module.

**NOTE** The installation procedure will install a Windows service (Token Initialization Service) on the operator’s PC. This service requires local administrator permissions on the PC.

## Preparing the KT Series Token for Initialization

Starting with the KT-x off, press and hold the button until the display shows “Init” (approximately 3-4 seconds). Release and press the button again. The display will show the prompt: **RDY 4 IR.** Insert the token in the
initializer with the LCD display facing the front of the initializer. Click the **Initialize** button. Note that the KT-x will remain in the RDY 4 IR state for approximately 15 seconds. The token cannot be initialized while in any other state. Initialization will complete in 7-10 seconds.

### Preparing the RB Series Token for Initialization

Place the RB-x token in the initializer with the LCD display down and facing the front of the initializer. The RB-x does not need any other preparation before initialization. Click **Initialize** in the **Token Mgt** group to complete the process. Initialization will complete in 7-10 seconds.

**Figure 2: RB Series Token Initializer**

---

### Troubleshooting

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I’m experiencing communication problems.</td>
<td>Ensure the SAS Token Initialization Service is running. To test whether it is working correctly, browse to <a href="http://localhost:19857/Initializer/ReadInformation">http://localhost:19857/Initializer/ReadInformation</a> on the client machine on which you are trying to initialize the token. Performing this step with a token that is ready to be initialized should return information about the token. Error code descriptions are provided in the return. Here is a sample of the information that is returned if the SAS Token Initialization Service is running and there is no initializer plugged in:</td>
</tr>
<tr>
<td>Issue</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>{ &quot;CurrentFirmware&quot;:&quot;-2&quot;, &quot;CurrentModelNumber&quot;:&quot;-2&quot;, &quot;CurrentSerial&quot;:&quot;-2&quot;, &quot;ErrorCodes&quot; :</td>
</tr>
<tr>
<td></td>
<td>[ {&quot;Key&quot;:1,&quot;Value&quot;:&quot;Generic Error&quot;}, {&quot;Key&quot;:2,&quot;Value&quot;:&quot;No Initializer Detected&quot;}, {&quot;Key&quot;:3,&quot;Value&quot;:&quot;No Token Detected&quot;},</td>
</tr>
<tr>
<td></td>
<td>{&quot;Key&quot;:4,&quot;Value&quot;:&quot;Couldn't read serial number&quot;}, {&quot;Key&quot;:5,&quot;Value&quot;:&quot;Enter serial manually&quot;} ]</td>
</tr>
<tr>
<td></td>
<td>The &quot;No initializer or installed drivers. Token initialization failed.&quot; message is displayed after installing the <strong>Initializer Drivers</strong> software.</td>
</tr>
<tr>
<td></td>
<td>1. Disconnect and reconnect the USB initializer.</td>
</tr>
<tr>
<td></td>
<td>2. Verify that Windows completes the <strong>Driver Software Installation</strong> by confirming the device is recognized. In <strong>Control Panel &gt; Devices and Printers</strong>, the device should be listed under <strong>Unspecified</strong>.</td>
</tr>
<tr>
<td></td>
<td>For example, you should see <strong>CRYPTOCARD KT Token USB Initializer</strong> or <strong>CRYPTOCARD RB Token USB Initializer</strong>.</td>
</tr>
</tbody>
</table>
GROUPS provides access to functions that enable you to:

- Create and Manage Groups (Group Maintenance module)
- Manage User Group Memberships (Group Membership module)
- Apply RADIUS Attributes to Groups (RADIUS Attribute (Group) module)
- Create and Manage Containers (Container Maintenance module)
- Manage Container Objects (Container Members)

**Group Maintenance**

Groups are attributes that can be attached to a UserID and used for authorization during the authentication process. Group attributes provide a way to distinguish between valid users (all users that can authenticate) and those that should be allowed to authenticate to gain access to a particular resource.

For example, assume you have two (2) valid users User1 and User2 both of which can authenticate. However, one of your protected resources is the HR network which should only be available to User1. By creating and adding User1 to the “HR” group, then creating a firewall rule or a Pre-Authentication rule (refer to "Pre-Authentication Rules" on page 151) in the Virtual Server, only User1 will be able to authenticate to the HR network. This of course is a simple example. Complex requirements are also accommodated using a combination of Group Membership and Pre-Authentication rules.

**Internal and Synchronized Groups**

You can have two types of groups on the Virtual Server:

- **Internal Groups**—Groups that you create and to which you add members.
> **Synchronized Groups**—Groups that exist on an external source such as Active Directory. The Synchronization Agent can be used to “synchronize” Active Directory group(s) in the Virtual Server. Synchronization not only synchronizes AD groups, it also retains each synchronized user’s group membership.

- AD groups can be used for authorization. Simply by adding or removing a user from an AD group, the Virtual Server using Pre-authentication rules can allow or deny access to resources based on user group membership attributes.
- Auto-provision users with tokens based on their AD group membership. For example, if in AD there were three groups: remote access, KT and MP, the Virtual Server could automatically provision users that belong to the remote access and KT groups with a KT hardware token, and those that belong to the remote access and MP groups with a software token.
- By utilizing a combination of Groups, Pre-authentication, and auto-provisioning the Virtual Server can accomplish most authentication management functions (creating users, authorization, assigning tokens, revoking tokens) without any administration.

Synchronized users can belong to both Synchronized and Internal groups.

To create an internal group, select the **Internal** option, and then click **New**.

**Figure 1: Add Group**

![Add Group Form](image)

Type a group name and a brief description of its purpose in the fields provided, and then click **Add**. This adds the group and updates the **Internal Groups** List.

Group names and descriptions can be edited by clicking **Edit**, or removed by clicking **Remove**.
Group Membership

This module is used to display all members of a group or to modify the memberships of one or more users. Note that the memberships for an individual user can also be managed from the Group Membership module on the ASSIGNMENT tab.

Figure 1: Group Membership List

To view group membership, use the search function in conjunction with:

- **Is a member of option**—Refines the list to users that are members of any group or the specified group.
- **Is not a member of option**—Refines the list to users that are not members of any group or the specified group.

You can further refine the list by adding the User’s last name or User ID to the search criteria.

Click **User ID** to display the corresponding **User Detail**.

Add Users to a Group (Internal)

To add users to a group, use the check box options to select one or more users, and then click the **New** button. This will open the **Add Membership** window. Use the drop-down list to select the group membership to add to the user, and then click the **Add** button.

Synchronized Group Membership

Synchronized Group membership cannot be added or removed from users in the management UI. This is because synchronized group membership is obtained from the AD/LDAP or other external user source. However, you can use the **Search Synchronized** tab in **Group Membership** to view groups and group memberships.
RADIUS Attribute (Group)

This module allows RADIUS Attributes to be attached to a group. The attribute will be returned for each member of the group when they authenticate. Note that attributes assigned to users have precedence over attributes assigned to a group to which the user belongs.

By default, group-based RADIUS attributes are defined for all Auth Nodes, or they can be restricted to selected Auth Nodes (excluding shared Auth Nodes) by using the **Restrict To Auth Nodes** check box.

When authenticating with a RADIUS token, SAS also passes RADIUS attributes to the RADIUS client that were received from an external RADIUS server. This is beneficial for authentication requests that may go to a third-party authentication service and then return through SAS. This is also useful for migrations where an external RADIUS server continues to authenticate users that are not yet migrated to SAS. With this feature, the RADIUS client can receive the same external attributes during the migration phase than before migration (without SAS).

Also, refer to "Block RADIUS Authentication" on page 161.

NOTE  SAS returns the attributes received from the external server after attributes that are configured in SAS. If the same attribute is configured in the external server and in SAS but with different values, it is up to the RADIUS client as to how this is interpreted. It is advised to avoid conflicting attribute definitions in SAS and the external RADIUS server.

Set RADIUS Attribute (Group)

To set RADIUS attributes, select the appropriate Internal or Synchronized Group, and then click the **New** button.
The options and input values will vary depending upon your selection from the various drop-down lists. Consult your network equipment vendor’s documentation for guidance on which attributes to use.

Once the attribute is set, click the **Add** button. This will add the attribute to the Group. Repeat as necessary to add more attributes.

**View RADIUS Attribute (Group)**

Select the group to view using the internal or synchronized group option, and then click Search. A list of attributes assigned to the group will be displayed in a list. The **Edit** link for each attribute can be used to modify the corresponding attribute. Likewise, the **Remove** link is used to remove the group attribute.

**Container Maintenance**

Containers are used to separate objects (users, tokens or both) for the purposes of management. Objects can only reside in one container at a time. When a user is moved between containers, all of the user’s assigned tokens are moved at the same time.

Containers define an Operator’s scope – what it is they can manage. If a container is not in an Operator’s scope, then all of the objects in the container are also not in scope and consequently cannot be viewed or managed by the Operator.
Containers can be used to segregate:

> Management:
  - Operator A can see/manage objects in Container A
  - Operator B can see/manage objects in Container B
  - Operator C can see/manage objects in Containers A and B

> Inventory:
  - Cost center A purchases tokens which are placed in Container A
  - Cost center B purchases tokens which are placed in Container B
  - Operator A can only view/manage tokens in Container A
  - Operator B can only view/manage tokens in Container B
  - Operator C can view/manage tokens in Containers A and B

The Virtual Server has a default container into which users and tokens are automatically placed unless a different selection is made at the time the users and/or tokens were added.

**Create a Container**

To create a new container, click the **New** button, then enter a unique container name and brief description of its purpose, and then click **Add**. The new container will appear in the **Containers List**.

Click the **Edit** link or the **Remove** link respectively to edit the container information or remove it. Note that all objects must be removed from a container before it can be removed.
Container Members

Containers and their members can be viewed and members moved between containers using this module.

Figure 1: GROUPS > Container Members

The Containers View includes two tabs: Users and Unassigned Tokens. To view objects by type, select the appropriate tab. Recall that tokens assigned to users always reside in the container with the user.

To view the members of a container, select the appropriate Source Container and then click Search. The resulting list displays all objects in the container. Clicking the UserID or Serial Number links displays the object’s details.

Move Objects

To move objects to a different container, select the objects in the list using the check box option, then select the target container from the Move to Container list, and then click the Move button.
The Service Provider reporting engine 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.

Figure 1: REPORTS

<table>
<thead>
<tr>
<th>Snapshot</th>
<th>Assignment</th>
<th>Tokens</th>
<th>Groups</th>
<th>Reports</th>
<th>Self-Service</th>
<th>Operators</th>
<th>Policy</th>
<th>Comms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Reports</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>My Report List</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>My Scheduled Reports</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>My Report Output</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

These reports do not include user-specific information, but rather cumulative information for billing and reporting purposes. For example, a report may include the name of all organizations below the service provider and a count of tokens by type and their state. But, reports do not include username, user ID, token assignment, etc. Detailed reports including user-specific information must be generated at each virtual server. This mechanism provides a way for the subscriber account to protect confidential information from the service provider.

The REPORTS modules include:

- **Available Reports**—Displays the standard reports available in SAS for Service Providers. Reports from this list can be customized and copied to the My Reports List module.

- **My Report List**—Displays the reports that can be run on by the Service Provider. 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**—Displays the scheduled reports. Schedules can be modified and reports can be run “Now” without modifying the normal schedule.

- **My Report Output**—Displays the reports that are currently in the run state or have completed. From this list Account Managers can view or download reports to which they are entitled in a variety of formats.

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

My Scheduled Reports and My Report Output display only those reports to which the Operator is authorized. Reports can be customized, scheduled, and delivered to the account, the Service Provider, and to external parties such as auditors.

### Available Reports

To access the reports that are available to you, click REPORTS > Available Reports.
Figure 1: Available Reports

The Report Class drop-down filters reports corresponding to:

- **Account Management**—Account usage, service terms, and overall operations.
- **Compliance**—Account Manager activities related to managing accounts and operations performed through the management console.
- **Billing**—All transactions including capacity, tokens, SMS credits, and their related billing terms.
- **Service Metrics**—Information similar to that provided with DASHBOARD > Subscriber Metrics.
- **Asset Management**—The state and usage of tokens: in Inventory and allocated to accounts.

To add a report to My Report List:

1. Select a report from the list.
2. Click Add.

   The Customize Reports options are displayed.
Customize Report

When customizing reports, only the Report Columns check boxes that are currently active are displayed by default. The More Columns/Less Columns toggle button enables you to view or hide additional column selections.

- Click the More Columns button to display additional column check boxes that are currently inactive.
- Click the Less Columns button to hide the column checkboxes that are currently inactive.
- Changes that are made to the Report Columns check boxes will take effect after clicking Finish.
- In cases where there is only one unselected check box, the toggle button is not displayed.

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

- **Report**—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. Filters will vary depending upon the nature of the report. Common filters include:
• **Child Only or ALL**—Child only includes data from accounts on-boarded by the Service Provider. All includes data for from all account in the tree below the Service Provider (for example, child, grandchild, etc.).

• **Date Range**—This can be a specific range, or for regular reports, can be options such as this month, last month, last 3 months, etc.

> **Report Columns**—Displays 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 Report Enabled** field lists all Operators that will receive the reports. To add or remove from the recipient list, highlight the Operators (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 Report Enabled** field lists all Service Providers that will receive the reports. To add or remove from the recipient list, highlight the Service Providers (CTRL+click to select multiple Service Providers), and then click the appropriate arrow to move.

> **E-mail 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 into the management UI to view and download reports. To add recipients, enter their e-mail address then click **Add**. To remove recipients, highlight their e-mail address then click **Remove**.

> **E-mail 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.

<table>
<thead>
<tr>
<th><strong>NOTE</strong></th>
<th>The number of rows in small reports can be configured for PCE installations only; the default is 2000.</th>
</tr>
</thead>
</table>

| **NOTE** | For security and compliance reasons, use a secure method, such as SFTP/SCP. |

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

**My Report List**

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

To schedule a report:

1. Select the report.
2. Click Schedule.

Figure 2: My Report List > Schedule Report

3. Select the desired options:
7 • Schedule to Run Now—This 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 option 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 Expiration Date. 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.

4. Click Finish to add the report to the My Scheduled Reports module.

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

My Scheduled Reports

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 link 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 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.

Figure 1: REPORTS > My Scheduled Reports

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

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 My Report Output table.

The data retention period for reports is set to 365 days for SAS Cloud. SAS-PCE administrators can configure the data retention period in the System > Logging > Archiving module.

Figure 1: REPORTS > My Report Output

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 links. Reports that are no longer required can be deleted from the list by clicking the Remove link.

Outdated reports are automatically removed from the My Report Output list after the number of days specified in the Auto Remove module. See "Auto Remove" on page 134.
SAS Self-service enables organizations to:

> Empower users to perform simple authentication management functions such as resetting PINs, reporting lost tokens or viewing their authentication history, and in the process, reduce the workload and end user reliance on the help desk.

> Invite users to request a token. This is particularly useful for organizations servicing consumers of on-line 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, 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.)

For more information, refer to Configuring Self-Service in the SafeNet Authentication Service Self-Service Administrator Guide.

Figure 1: SELF-SERVICE > Configuring Self-Service

![Configuring Self-Service](image)
Virtual Servers are managed by Operators, of which there are two types:

- **Internal Operator**—User accounts in the Virtual Server that have been promoted to Operator status.
- **External Operator**—Operator accounts created for the Service Provider, allowing Service Provider management access to the Virtual Server.

Both types of Operators are managed from the **OPERATORS** tab.

**Figure 1: OPERATORS**

<table>
<thead>
<tr>
<th>Snapshot</th>
<th>Assignment</th>
<th>Tokens</th>
<th>Groups</th>
<th>Reports</th>
<th>Self-Service</th>
<th>Operators</th>
<th>Policy</th>
<th>Comms</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Internal Operator" /></td>
<td><img src="image2" alt="Internal Operator" /></td>
<td><img src="image3" alt="Internal Operator" /></td>
<td><img src="image4" alt="Internal Operator" /></td>
<td><img src="image5" alt="Internal Operator" /></td>
<td><img src="image6" alt="Internal Operator" /></td>
<td><img src="image7" alt="Internal Operator" /></td>
<td><img src="image8" alt="Internal Operator" /></td>
<td><img src="image9" alt="Internal Operator" /></td>
</tr>
<tr>
<td><img src="image10" alt="External Operator" /></td>
<td><img src="image11" alt="External Operator" /></td>
<td><img src="image12" alt="External Operator" /></td>
<td><img src="image13" alt="External Operator" /></td>
<td><img src="image14" alt="External Operator" /></td>
<td><img src="image15" alt="External Operator" /></td>
<td><img src="image16" alt="External Operator" /></td>
<td><img src="image17" alt="External Operator" /></td>
<td><img src="image18" alt="External Operator" /></td>
</tr>
</tbody>
</table>

**Internal Operator**

Any user added to a Virtual Server to which you’ve assigned a token or password can be promoted to Internal Operator, allowing them to log into and perform management functions. Operators appear in the Internal Operator list. Operators cannot modify their own role, scope or access restrictions.

**Figure 1: OPERATORS > Internal Operator**

Each row in the list displays:

- **User ID**—This is the User ID of the Operator. Click the link to reveal additional user detail.
- **Role Name**—This is the role assigned to the Operator. Roles determine what an operator is able to do through the management UI.
State—There are three (3) possible states:

Pending Validation—User has not yet validated their email address.
Active—Operator is able to log on to the management UI. Click the State link to suspend.
Suspended—Operator account has been suspended. Click the State link to re-activate.
Edit—Click this link to edit the Operator’s role, scope and access restrictions.
Remove—Click this link to remove this user as an Operator.

Add an Internal Operator

To add an Internal Operator, begin by clicking the New button in the Internal Operator module. This will produce a list of users that are eligible for promotion to Operator status. Only users with active tokens appear in the search results. Use the Last Name and/or UserID criteria and the Search button to refine the list. Click Next to select a Role.

Figure 2: List of Potential Operators

You can select multiple users for promotion, bearing in mind that the same Role, Scope, and Access Restrictions will be applied to all selected users.

Assign a Role

Roles determine the task an Operator can perform (refer to "POLICY > Role Management" on page 113). Select a Role and then click Next.
Assign Scope

Containers define an Operator’s Scope—what it is they can manage. If a Container is not in an Operator’s Scope, then all of the objects in the container are also not in Scope and consequently cannot be viewed or managed by the Operator. Select one or more Containers from the list, and then click Next.

Access Restrictions

Access Restrictions are used to limit when an Operator is allowed to log into the Virtual Server management UI. If no restrictions are to be applied, click Finish, or, enable restrictions, and then click Finish.
Figure 5: Assign Access Restrictions

If Access Restrictions are required, begin by clicking the **Enable Restrictions** option, then:

- **Start Date**—Operator cannot log into the Virtual Server management UI prior to this date.
- **End Date**—Operator cannot log into the Virtual Server management UI after this date.
- **Start Time**—Operator cannot log into the Virtual Server management UI prior to this time of day.
- **Stop Time**—Operator cannot log into the Virtual Server management UI after this time of day.
- **On the following days**—Operator logon is restricted to the checked days of the week.

**Operator E-mail Validation**

Operators log into the management UI using the e-mail address associated with their UserID. Before an Operator can logon, they must confirm they own the email account to which the validation message is sent.

Figure 6: Customizable Operator E-mail Validation

```
Allen Ladd,

To activate your Operator account in your Virtual Server, you must logon by following the link and using the e-mail address as your User ID indicated below:

E-mail: aladd@acme.com


After validation you can log into the management UI at:
http://209.1.1.100/console/
```

Note that a validation message will be resent if the Operator’s e-mail address associated with their UserID changes.
External Operator

An external Operator is an account that is automatically created for the Service Provider when the Virtual Server is created. It is through this account that Account Managers are able to access the account’s Virtual Server (via the VIRTUAL SERVERS tab).

- As with Internal Operators, External Operators have an assigned role, which by default is Operator, allowing access to all of the VIRTUAL SERVERS tabs, modules, and actions.

- A role other than Operator can be assigned to an External Operator. By applying a different role, the account can limit the functionality available to the Service Provider through the UI, including denying access to the Virtual Server. To prevent this, the Service Provider must modify all Internal Operator roles to deny access to the External Operator module.

- All External Operator activity is recorded in the Virtual Server for audit and reporting purposes.

- An additional External Operator account is created for each Service Provider account to which management of the Virtual Server has been delegated. External Operator accounts can have different roles.

In the External Operator list:

- **Account**—This is the name of the Service Provider account.
> **Primary Contact**—This field is populated using information provided in the **Primary Contact** field in the Services module on the ON-BOARDING tab.

> **Telephone**—This field is populated using information provided in the **Primary Contact** field in the Services module on the ON-BOARDING tab.

> **Role**—This is the role assigned to the External Operator account. Refer to "POLICY > Role Management" on page 113.

> **Realming**—Empty field indicates the external operator has not been added to the realm.

  - **Enabled** indicates the external operator has been added to the realm and can authenticate. Clicking the link allows the status to be changed to **Disabled**.

  - **Disabled** indicates the external operator has been added to the realm but is not allowed to authenticate. Clicking the link allows the status to be changed to **Enabled**.

> **Edit**—Allows an Internal or External Operator with sufficient rights to modify the role assigned to this account.

> **Remove**—Allows an Internal or External Operator with sufficient rights to modify the role assigned to this account.

Operators cannot modify or delete their own role.

Delegation is most commonly used in a multi-tier sales and service model, where the intermediary sales channel On-boards the account but does not have the capacity or business interest to manage the account’s Virtual Server. If the delegation option is selected in the Services module (ON-BOARDING tab), then two External Operator accounts are automatically created, one for the Service Provider and one for the delegated Service Provider.

### Add an External Operator Account (Delegation)

An External Operator account can be created for each Service Provider to which management of the Virtual Server should be delegated. Each Service Provider account must provide a delegation code. This code will be used to create an External Operator account for their exclusive use.

To add an external operator account, click **New**.

#### Figure 2: OPERATORS > External Operator > New

![External Operator](image)

Enter the delegation code provided by the Service Provider, and then click **Verify** to confirm the Service Provider name in the **Managing Account** field. Click **Next** to continue.
Figure 3: OPERATORS > External Operator > Assign Role

Select the role (for more details about roles, see "Role Management" on page 113) to be applied to this account, and then click Next.

Figure 4: Configure Scope

Select the containers to which this role should have access, and then click Next.

Figure 5: Configure Access Restrictions
To limit when the Service Provider can log in and manage the Virtual Server, turn on access restrictions, and configure the conditions where:

- **Enable Restrictions**—If checked, restrictions are enabled. If cleared, no time/day/date range restrictions are applied.
- **Start Date**—Management UI logon is denied before this date.
- **End Date**—Management UI logon is denied after this date.
- **Start Time**—Management UI logon is denied before this time.
- **End Time**—Management UI logon is denied after this time.
- **On the following days**—Management UI logon is permitted on checked days only.

Note that Account Manager Restrictions apply only to Account Manager Management UI logons. It does not affect any logon by the user.

**Figure 6: New External Operator**

The new External Operator account is added to the list.

Click **Enable** and then **Apply** to confirm the delegation.

The account’s Virtual Server displays in the accounts list on their **VIRTUAL SERVERS** tab.

**Figure 7: Server Provider Confirmation**
Modify and Remove External Operators

The process to modify or remove External Operators is identical to that for Internal Operators.
The **POLICY** tab enables you to configure an account’s security policy; to enforce a consistent login experience and protect against denial of service, brute force, and other account credential attacks.

<table>
<thead>
<tr>
<th>Snapshot</th>
<th>Assignment</th>
<th>Tokens</th>
<th>Groups</th>
<th>Reports</th>
<th>Self-Service</th>
<th>Operators</th>
<th>Policy</th>
<th>Comms</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Create User" /> Create User</td>
<td>(Shortcut) Add a user record to an account (&quot;Create User (shortcut)&quot; on page 23).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><img src="image" alt="Authentication Policies" /> Authentication Policies</td>
<td>Configure the authentication behavior (&quot;Authentication Policies&quot; below).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><img src="image" alt="User Policies" /> User Policies</td>
<td>Configure a user’s access to the authentication service (&quot;User Policies&quot; on page 90).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><img src="image" alt="Token Policies" /> Token Policies</td>
<td>Configure a token’s interaction with the authentication service (&quot;Token Policies&quot; on page 93).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><img src="image" alt="Role Management" /> Role Management</td>
<td>Configure operator roles, alerts, alert thresholds, and the console language (&quot;Role Management&quot; on page 113).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><img src="image" alt="Automation Policies" /> Automation Policies</td>
<td>Auto-provision users with tokens and configure self-enrollment/service (&quot;Automation Policies&quot; on page 124).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Authentication Policies

**POLICY > Authentication Policies** enables you to configure one Contextual Authentication policy per Virtual Server to flexibly adapt (apply/skip) credential requirements for SAML-protected web-based applications.
<table>
<thead>
<tr>
<th>Section</th>
<th>Field/Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POLICY IMPACT</td>
<td>No Impact (default)</td>
<td>Define whether or not SAS applies the Contextual Authentication policy.</td>
</tr>
<tr>
<td>AFFECTED USERS</td>
<td>All Users</td>
<td>Apply the policy to all users.</td>
</tr>
<tr>
<td></td>
<td>Users in Specific Groups</td>
<td>Type the group name(s) containing the subset of users to which the policy will apply.</td>
</tr>
<tr>
<td>CONTEXT CONDITIONS</td>
<td>Trusted Network</td>
<td>The IP address to which the policy applies. SAS considers the originating public IP address of the request only.</td>
</tr>
<tr>
<td></td>
<td>IPv4, IPv6, or CIDR address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ending address</td>
<td>(Optional) The end IP address of a range.</td>
</tr>
<tr>
<td></td>
<td>Known Device</td>
<td>The number of days before SAS requires users to fully authenticate.</td>
</tr>
<tr>
<td></td>
<td>Retention period</td>
<td></td>
</tr>
<tr>
<td>RE-AUTHENTICATION PERIOD</td>
<td>Every 30 days (default)</td>
<td>The number of days before users must authenticate with their full credentials; to ensure that users don’t forget their full login credentials and to protect against malicious use of a known device.</td>
</tr>
</tbody>
</table>
Configure a Contextual Authentication Policy

To configure a Contextual Authentication policy:

1. Click **POLICY > Authentication Policies > Contextual Authentication Policy**.

2. Define the POLICY IMPACT on the authentication process; select one of the following options:
   - **No Impact**—(Default) The Contextual Authentication policy will NOT be applied. SAS WILL prompt the user for their full credentials at each login.
   - **Skip OTP**—If all of the policy conditions are met and unless the end of the RE-AUTHENTICATION PERIOD has been reached, SAS will NOT prompt the user for their credentials (for example, static password or One Time Password) as part of the authentication process.

3. Define the AFFECTED USERS to whom the policy applies:
   - **All Users** (Default)
   - **Users in Specific Groups**—Type the name of the group(s) in the field provided.

   **NOTE**  A group must exist to be added to the list. If a local and a synced group have the same name, both groups are added to SAS when the policy is saved. If a list of groups exists in the RBA Policy and an operator switches to "All Users" the list of groups becomes inactive but is not erased from the database unless the policy is saved. The policy applies to the child groups of each parent group. Changes are not saved if no groups are added or removed.

4. (Optional) Define a Trusted Network of IP addresses:
   a. Select **Trusted Network** in the CONTEXT CONDITIONS section.
   b. Type a trusted IP address in the left-most of the two fields provided. If this is the first address of a range, type the start/lowest IP address in this field.
   c. (Optional) If this is the last address of a range, type the end/highest IP address in the right-most of the two fields provided.

   **NOTE**  The following IP address formats are supported: IPv4, IPv6, or CIDR. SAS considers the originating IP address of the request only. For example, if the user requests a protected application from a public IP address, SAS ignores the user’s internal enterprise network IP address (if any). Changes to the Trusted Network option are logged.
5. (Optional) Allow Known Devices (user-device-browser combinations from which users have ‘recently’ successfully authenticated) to qualify for the policy:
   a. Select Known Device in the CONTEXT CONDITIONS section.
   b. Type the Retention period (1 - 365 days), in the field provided, throughout which SAS will remember the browser-device combination. The Retention period is continuously restarted upon each successful authentication within the Retention period. Default = 7 days.

   **NOTE** If the user attempts to authenticate after the configured Retention period is exceeded, the user must provide credentials; even if POLICY IMPACT = Skip OTP. Upon successful authentication by the user, the Retention period is restarted.

The Known Device condition is specific to the combination of user, device, and browser. For example, a user may meet the Known Device rule on one browser (e.g., Google Chrome) on their computer, but not on another browser on the same computer – depending on the authentication history of the browser being used.

The Known Device condition will be applied to a user on a given device-browser pair only if they have selected the Remember Me on this Device check-box on the SAML login page and successfully authenticated.

The Known Device condition relies on cookies and is effective only if cookies are allowed on the browser from which the user is authenticating.

If the user on a Known Device fails to type their correct User ID at the login prompt, SAS then prompts the user with a false challenge (but does not reveal to the user that their User ID was invalid).

6. Type the number of days (1 - 90), in the RE-AUTHENTICATION PERIOD, until which SAS will require the user to authenticate with all of their credentials. Default = 30 days.
NOTE The re-authentication is enforced separately on each device-browser that the user is using. If POLICY IMPACT = Skip OTP, after the configured number of days, and upon the next authentication request, SAS will prompt the user for full credentials and deny the user access to the SAML-protected resource until the user provides their full credentials. Upon successful authentication by the user, SAS will restart the Re-authentication period. If POLICY IMPACT = No Impact, then the Contextual Authentication policy (including the re-authentication period) will NOT be applied and SAS WILL prompt the user for their full credentials at each login.

7. Click Apply to save your changes or click Cancel to cancel your changes.

View the Change Log
When you save changes to “Users in Specific Groups” and/or “Trusted Network”, SAS updates the Operator logs in the console.

Enable Contextual Authentication
Contextual Authentication is disabled, by default, and must be enabled on a per SAML Service Provider basis using the SAML 2.0 Setting.

NOTE Pre-authentication rules do not apply to SAML authentications where Enhanced User Login and/or Contextual Authentication are used. For more information, see “Pre-Authentication Rules” on page 151.

To enable the Contextual Authentication for a SAML Service Provider:
1. Click COMMS > SAML Service Providers > SAML 2.0 Settings > Add/Edit > Add/Edit SAML 2.0 Setting.
2. In the USER LOGIN SETTINGS section, select both:
3. Click Apply to save your changes or click Cancel to cancel your changes.

NOTE You can select “Enable Contextual Authentication” only if “Enhanced User Login” is also selected for the same SAML Service Provider. If “Enable Contextual Authentication” is selected and you deselect “Enhanced User Login”, then “Enable Contextual Authentication” becomes ineffective (grayed out) but retains its settings.
**Figure 1: SAML Service Providers > SAML 2.0 Settings**

![SAML 2.0 Settings](image)

**User Policies**

This module contains policies that affect user accounts.

**Figure 1: POLICY > User Policies**

![User Policies](image)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Lockout/Unlock Policy</td>
<td>Set the conditions under which the server will automatically lock and/or unlock a user account.</td>
</tr>
<tr>
<td>Dormant Account Lockout Policy</td>
<td>Set conditions for locking accounts which have become dormant.</td>
</tr>
<tr>
<td>Push OTP Rejection Policy</td>
<td>Enable sending email alerts when users reject OTP push notifications.</td>
</tr>
</tbody>
</table>

**Account Lockout/Unlock Policy**

The Virtual Server uses this policy to determine how to handle consecutive failed logon attempts.
Figure 2: User Policies > Account Lockout/Unlock Policy

> **Apply** (button)—Save changes to the policy. Active until changes to the policy are saved or canceled.
> **Cancel** (button)—Clear unsaved changes to the policy and close the module.
> **Change Log** (button)—Display the last 5 changes to the policy; including: date and time of change, Operator ID, and changed values.
> **Account lock threshold**—The maximum number of consecutive failed login attempts permitted for a user. If this value is exceeded, SAS locks the account. To disable this function, set the value to 0. Default value: 3
> **Alert User on account lockout**—If checked, SAS sends an alert to the User when the User’s account changes state from Unlocked to Locked.
> **Alert User on account unlock**—If checked, SAS sends an alert to the User when the User’s account changes state from Locked to Unlocked.
> **Account lock duration**—The time in seconds, minutes, or hours that must elapse after locking the account, after which the User’s account will automatically unlock. If set to 0, the account will not automatically unlock. Default value: 15 minutes.

**Dormant Account Lockout Policy**

Some compliance regulations require that dormant user accounts be automatically locked and not be permitted to authenticate. A dormant account is one that has not logged on for a defined period of time.

The Virtual Server uses the **Dormant Account Lockout Policy** to determine how long after the last successful logon an account is considered to be dormant and becomes locked.
Figure 3: User Policies > Dormant Account Lockout Policy

> **Apply Button**—Active when the policy is modified. Use to commit policy change.

> **Cancel**—Clears any uncommitted change to the policy and closes the module.

> **Change Log**—Displays a list of the last 5 changes to this policy, including the date and time of each change, changed by Operator ID, and the value that was specified.

> **Dormant Account Threshold**—Allowed range in days is: 0 (default, threshold disabled) to 365. Input limited to integers in this range.

**Push OTP Rejection Policy**

This feature is not available with SAS PCE/SPE.

The Virtual Server uses the **Push OTP Rejection Policy** to send push notifications only to registered devices with currently active, push-enabled tokens. If a user receives a push notification that he or she did not initiate and the notification is rejected, enabling this option will automatically email a Push Notification Rejection Alert to the user.

**NOTE** If the user’s account gets locked due to this Push OTP rejection, the body of this alert is appended to the User Lockout Alert that is sent to the user.
Figure 4: User Policies > Push OTP Rejection Policy

> **Apply** (button)—Active when the policy is modified. Use to commit policy change.
> **Cancel** (button)—Clears any uncommitted change to the policy and closes the module.
> **Change Log** (button)—Displays a list of the last 5 changes to this policy as follows, including the date and time of each change, changed by Operator ID, and the value that was specified.
> **Alert user on OTP push notification rejected**—If checked, an alert regarding the User’s Account that a push notification was denied (from the User’s device) will be sent by email to the User.

**Token Policies**

This module contains policies that affect token usage and operation.

Figure 1: POLICY > Token Policies
Token Templates

Templates are the operating parameters for each type of token. A template is applied every time a hardware token is initialized, an MP token is assigned/provisioned, or an SMS/OTP or Grid is generated. You can adjust token templates, and therefore token operation, to adapt to changes in your security policy.

Figure 2: POLICY > Token Policies > Token Templates

Token templates are the operating characteristics, such as passcode strength, to be applied to all hardware tokens of a given type during initialization, to MP tokens when they are assigned/provisioned to users, and to SMS/OTP passcodes. A template modification does not affect tokens that are already initialized and does not affect tokens assigned to users.

Token templates are provided for: KT-1, KT-2/3, KT-4, KT-5; RB; MP; Legacy 4.x, 5.x, 6.x; SMS, OATH, RADIUS, SecureID, Gridsure, GOLD, eToken, and MobilePASS software tokens.

The options presented in a template vary depending upon the token type. In addition, the selection of one option may preclude the availability of another option.

By default, all tokens use AES 256-bit encryption. Certain third-party tokens use 3DES or OATH. SAS applies the strongest algorithm supported by the token type.

Passcode Policy

- **Mode**—Tokens can operate in either Challenge-Response or Quick Log mode. Quick Log mode is recommended because it greatly simplifies the User logon experience and strengthens security by eliminating the requirement to have the user key a challenge into a token to get an OTP. Default value: Quick Log.

- **Complexity**—The OTPs generated by the token can be comprised of numbers, letters, and additional characters as follows:
  - **Decimal**—Token generates passcodes comprised of digits from 0-9.
• **Hexadecimal**—Token generates passcodes comprised of digits and letters from 0–9 and A–F.
• **Base32**—Token generates passcodes comprised of digits and letters from 0-9 and A-Z. (Default value).
• **Base64**—Token generates passcodes comprised of digits and letters from 0-9 and Aa-Zz, as well as punctuation.

> **Length**—This option determines the number of characters displayed as the OTP. Options are 5, 6, 7 or 8 characters. Default value: 8.

> **Synchronization**
  - **Time-based**—Determines the number of seconds the user has to authenticate, before another Passcode needs to be generated.
  - **Event-based**—Determines the number of clicks the user has to authenticate, before another Passcode needs to be generated.

> **Display Mask**—If set to Telephone Mode, the fourth character of the OTP will always be a dash (“-”). Typically, this is used with a decimal OTP, length of 8. Example OTP: 123-5678. If set to **None**, the fourth character is unmodified. Example OTP: 12345678. Telephone mode can be used with any token complexity and length setting. Default value: None.

> **Password/Cycle**—This option is used in conjunction with Operation Policy (Manual Shut-Off, Auto Shut-Off). Tokens can be limited to generating 1 password per cycle or allow multiple passwords to be generated in a cycle. Default value: Single.

For tokens with a **No PIN** or **Server-side** PIN policy, the selection of **Single** in combination with **Manual Shut-Off** set to **Disabled** means that the token will not generate another password until the **Auto Shut-Off** value has expired. For example, if the value is 60 seconds, the user must wait 60 seconds before another password can be generated.

For tokens with a **Fixed** or **User selected** PIN, selection of **Manual Shut-off** set to **Disabled** means that the token will not generate another password until the **Auto Shut-Off** value has expired and the user enters their PIN into the token.

**Operation Policy**

> **Manual Shut-Off**—If Enabled, the user can clear the OTP from the display and turn the token off at any time by pressing the appropriate button, depending on the token type. If **Disabled**, the OTP will be displayed until the Auto Shut-off value expires. Default Value: Disabled.

> **Auto Shut-Off**—This value determines the length of time the password will be displayed, 30, 60 or 90 seconds. On expiration of this value, the token automatically clears the display and shuts off. Default Values: 60.

**NOTE** Gemalto recommends using the **Operation Policy Group** default settings for RB and KT series tokens configured for QUICKLog operation. Doing so ensures that the user must wait at least 60 (default) seconds before the token will generate another passcode.

**PIN Policy**

> **PIN Type**—This setting determines the type of PIN to be used with the token:
• **No PIN**—Means that the user will not use a PIN. The token generated password will be sufficient for authentication.

• **Fixed PIN**—Means that the PIN generated for the token during initialization is permanent and cannot be changed without reinitializing the token. This PIN must always be keyed into the token before a password is generated.

• **User-selected PIN**—Means that the user must change the PIN generated for the token during initialization before a password will be generated. Thereafter, the user can change the PIN at any time. Note that the PIN change must conform to the minimum requirements for PIN Length, Complexity and Maximum PIN Attempts.

• **Server-side Fixed**—Means that the PIN generated for the token at initialization is permanent and cannot be changed without reinitializing the token. This PIN type is evaluated at SafeNet Authentication Service.

• **Server-side User Select**—Means that the PIN generated for the token can be changed by the User. The new PIN must conform to the minimum requirements set in the Server-side PIN policy.

• **Server-side Server Select**—Means that the PIN generated for the token can be changed, however, the new PIN will be generated by SAS and will conform to the minimum requirements set in the Server-side PIN Policy Group on the Policy Admin tab.

  Server-side PINs require the user to append or prepend the PIN to the token generated password during login, allowing the PIN to be evaluated by the Virtual Server. For example, if the user PIN is ABCD, and it must be prepended to the password 12345678, the user would enter ABCD12345678 at the password prompt.

  All other PIN types require the user to key the correct PIN into the token before a password is generated. In this case, the user provides only the password at the password prompt. For example, if the user PIN is 8432 and the password is 12345678, the user will enter 12345678 at the password prompt. Generally, server-side PINs are used with KT tokens.

> **Initial PIN**—Determines the nature of the initial PIN created for a token during initialization. If Random, SafeNet Authentication Service will generate a random PIN that conforms to the minimum PIN Policy options set in the drop-downs for this group for each token during initialization. If Fixed, all tokens will be initialized with the same PIN. Default value: Random

> **Min. PIN Length**—Determines the minimum PIN length that can be used with the token.

  • This option is disabled if PIN Type is set to No PIN. The user will not be required to use a PIN at any time.

  • This option is disabled if PIN Type is set to Server-side Fixed, Server-side User Select, or Server-side Server Select. The user will be required to use a PIN according to the options set in the Server-side PIN Policy Group.

  • This option is enabled if PIN Type is set to Fixed PIN or User selected PIN. This requires that any PIN set for the token meets the indicated minimum number of digits. The range is 1 to 8 digits.

> **Allow Trivial PINs**—If enabled, a PIN may be three (3) or more consecutive numbers (for example, 1234), or three (3) or more identical digits (for example, 2222). Default value: Cleared.

> **Max. PIN Attempts**—Determines the maximum number of consecutive failed PIN attempts permitted by the token. If this number is exceeded, the token will enter the Locked state and cannot be used for authentication until it is reinitialized. This option is available only if PIN Type is set to Fixed PIN or User selected PIN.
Click the **Apply** button to apply changes to the template. Changes to the template will be applied to their respective token types during initialization. Previously initialized tokens will be unaffected by changes to a template.

**PIN Complexity**—If **PIN Complexity** is set to **Decimal** and **Allow Trivial PINs** is selected, the user can use a PIN with any consecutive or repeated characters. For example, 1111, 1234, 6543, abcd, aaaa.

- If **PIN Complexity** is set to **Decimal** and **Allow Trivial PINs** is **disabled**, the user can use either a Numeric or an alphanumeric PIN, as long as it does not consist of consecutive or repeated characters. For example, aaaa or 1234 are not permitted while 9946, 123682, 321aaa, i6gfaa are permitted.
- If **PIN Complexity** is set to **Alphanumeric**, the user must use an alphanumeric PIN that includes at least one uppercase and one lowercase character, and one number. For example, 1Qazxs8, ajUys36.

**Allow Biometric PIN**—If enabled, subscribers can use a fingerprint sensor instead of typing a PIN to access their MobilePASS+ token. Default value: **Disabled**. This option requires that:

- **Token Type** is set to **MobilePASS**.
- **PIN Type** is set to **User-selected PIN**.

The Biometric PIN (Touch ID for iOS) policy setting on SAS is applied to tokens at the time of enrollment only. After a token is enrolled, policy changes on SAS do not affect the availability of the Biometric PIN (Touch ID for iOS) feature on that token.

---

**View/Edit a Token Template**

To view or modify a template:

1. Click **Token Templates**.
2. Select a token type.
3. Click **Edit** and modify the settings, if needed.
4. Click **Apply** to apply changes to the template.

---

**Token Passcode Processing Policy**

There are global settings that determine how the server will evaluate OTPs and support off-line authentication.

**Figure 3: Token Policies > Token Passcode Processing Policy**

---

*NOTE* Changes to the template are applied to tokens during initialization. Previously initialized tokens are not affected by later changes to a template.*
> **Ignore case in Hexadecimal and Base 32 token codes**—This is a usability enhancement. If enabled, users will be able to enter OTPs using either uppercase and/or lowercase letters. If unchecked, users must enter Base32 token codes using only uppercase letters.

> **Allow disconnected authentication**—This option is used in conjunction with the SafeNet Authentication Service Authentication Agent for Windows Logon. If enabled, users will be able to log in to their Windows computers using an OTP, even if the computer is not connected to a network. The number of disconnected authentications is the maximum number of times a user can log in to their computer before they must connect to the network and authenticate against the Virtual Server.

**Server-side PIN Policy**

You can configure how the server will evaluate PINs that are appended or prepended to the token code.

**Figure 4: (SAS Cloud Only) Token Policies > Server-side PIN Policy**

The Server-side PIN Policy options are:

> **Change PIN on first use is required (Operator cannot override)**—Force the user to change the initial PIN set for the token during initialization or set by an Operator before they can logon. For example, if the initial PIN is ABCD and the password is 12345678, the user will attempt to logon with ABCD12345678. Assuming this combination successfully authenticates against SafeNet Authentication Service, the user will then be prompted to change their PIN to a new value that meets the minimum requirements of the Server-side PIN. If this option is checked, the Operator cannot override this policy when resetting a User's PIN. If this option is cleared, the Operator can choose whether or not to force a PIN change on first use after resetting the User's PIN. Default value: checked.

> **Force Random PINs (Operator cannot override)**—If selected: 1) the Virtual Server generates random PINs that meet the Server-side PIN policy requirements for each User; 2) the Operator cannot choose the PIN to be given to a User. If cleared, the Operator can create a PIN that conforms to the policy or request a PIN be generated by the Server. Default: selected.

> **Mask Initial PIN**—(SAS SPE/PCE Only) Allows to mask Token PINs on User Detail and Token Detail pages in the SAS Administrator portal. If the checkbox is cleared, token PINs are displayed in clear text when configured using either of the method (using the SAS Console or executing the WSDL BSIDCA API). By
default, the PIN masking will be off. Administrators or Operators (those who can access POLICY > Token Policies) will only be able to change this setting.

> PIN Processing Order—Determines whether the PIN must be appended to the end of the token code or prepended to the beginning of the token code.

The PIN Strength options are:

> Minimum Length—The minimum number of characters in a PIN. Range is 3 – 15 characters.
> Maximum Length—The maximum number of characters in a PIN. Range is 4 – 16 characters.
> Default Generated Length—The number of characters in a PIN auto-generated by the server.
> Change Frequency—How frequently a user must change their Server-side Server Select or Server-side User Select PIN. This period begins with the last PIN change date for a token. Default: 30 days.

> Minimum Complexity—The combination of characters that must be used in a PIN. Default: Numeric.
  - Numeric—A PIN comprised of digits 0-9.
  - Alphanumeric—A PIN that contains at least 1 digit and 1 uppercase letter; for example, 0-9, A-Z.
  - Strong Alphanumeric—A PIN that contains at least 1 digit, 1 uppercase letter, and 1 lowercase letter; for example, 0-9, Aa-Zz.
  - Complex Alphanumeric—A PIN that contains at least 1 digit, 1 letter, and 1 special character; for example, 0-9, Aa-Zz, and punctuation.

The following table illustrates the application of PIN complexity rules, using MobilePASS as an example:

<table>
<thead>
<tr>
<th>Server-side PIN Policy</th>
<th>Client Message</th>
<th>Pass Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Numeric: (Minimum) PIN comprises digits 0-9.</td>
<td>“Token PIN should contain X decimal or alphanumeric characters.”</td>
<td>abc123, 1111, abcd, or Pass12</td>
</tr>
<tr>
<td>Alphanumeric: (Minimum) PIN comprises at least 1 digit and 1 uppercase letter.</td>
<td>“Token PIN should contain X alphanumeric characters and have at least one numeral, lowercase and uppercase character.”</td>
<td>12aA or 12Aa</td>
</tr>
<tr>
<td>Strong Alphanumeric: (Minimum) PIN comprises at least 1 digit, 1 uppercase letter and 1 lowercase letter.</td>
<td>“Token PIN should contain X alphanumeric characters and have at least one numeral, lowercase, and uppercase character.”</td>
<td>12aA or 12Aa</td>
</tr>
<tr>
<td>Complex Alphanumeric: (Minimum) PIN comprises at least 1 digit, 1 letter and 1 special character (for example, punctuation).</td>
<td>Not applicable for MobilePASS</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE** Alphanumeric PINs are typically more secure than numeric PINs.
Global or Groups PIN Change

This determines if the Server-side PIN Policy settings are global settings. Global PIN changes are applied immediately, and the group’s users who have server-side PIN-enabled tokens are required to change their Server-side PINs during their next authentication.

**Figure 5: Token Policies > Global or Groups PIN Change**

Temporary Password Policy

This section applies to temporary static passwords assigned to user accounts using the Password button (Tokens module > ASSIGNMENT tab). As with Server-side PIN Policy, these Options set global temporary password policy. Click Apply in the Actions group to apply changes to these values.

**Figure 6: Token Policies > Temporary Password Policy**
Temporary Password Allowed—This option determines whether a static password can be assigned. When checked, an Operator can assign a temporary password to a user, provided the user does not currently have an active token. If cleared, Operators may not assign a temporary password to a user. Default value: Enabled.

Change Password on first use required—This option forces the user to change the static password assigned by an Operator before they can logon. The user must first provide the assigned password and then is prompted to replace the password. If this box is checked, all users assigned a static password will be required to change it on first use. The Operator cannot override this policy. If cleared, the Operator has the option of requiring a password change on first use. Default value: checked.

Minimum Length—This is the minimum number of characters required in the temporary password. Range is 3 to 15 characters. Default value: 8.

Maximum Length—This is the maximum number of characters permitted in the temporary password. Range is 4 to 16 characters. This value must be greater than or equal to the minimum length. Default value is 16 characters.

Minimum Complexity—This determines the combination of characters that must be used in a password. Default value: Complex alphanumeric.

- **Numeric**—The minimum requirement is a password comprised of digits 0-9.
- **Alphanumeric**—The minimum requirement is a password that contains at least 1 digit and 1 uppercase letter. 0-9, A-Z.
- **Strong Alphanumeric**—The minimum requirement is a password comprised of at least 1 digit, 1 uppercase letter and 1 lowercase letter. 0-9, Aa-Zz.
- **Complex alphanumeric**—The minimum requirement is a password comprised of at least 1 digit, 1 letter and 1 special character. 0-9, Aa-Zz, and other printable characters.

Change Frequency—This determines how frequently a user will be required to change their static password. This period commences with the last static password change date for a token. Default value: 30 days.

Force Random Passwords—This determines whether an Operator can choose the password to be given to a user. If cleared, the Operator can manually create or generate a password that conforms to the policy. If checked, the Virtual Server must generate the temporary password. Default value: cleared.

Force Maximum Lifetime—This determines how long a temporary password will remain active. Possible values are in minutes, hours, days or weeks. Default value: disabled.

**Synchronization**

Synchronization provides a secure mechanism through which the server and token can automatically resynchronize when a user authenticates.
**Figure 7: Token Policies > Synchronization**

The Synchronization options are:

> **Inner event-based OTP window size**—The number of passwords the server will "look-ahead" from the last successful logon by the user. Using the example above, the server would be expecting passcode number 1 even though the user provides passcode number 2. Assuming the default inner window value of 3, the server would look from passcode 1 to 3 until a match is found (in this case at passcode 2). If a match is found, the user is authenticated and any unused passcodes are discarded. The next valid passcode on the server would be passcode 3. Default value: 10.

> **Outer event-based OTP window size**—This handles situations where the user’s passcode is not found in the inner window. In this case, the server will look ahead up to the indicated value (by default 100). If a match is found in this window, the user is prompted to provide the next passcode in sequence. For example, if the user provides passcode 4, the user will be prompted for and must provide passcode 5. In essence this window has an effective size of 1. Default value: 100.

> **First authentication time-based OTP window size**—An expanded evaluation window (maximum value = 300) that applies only to the first authentication attempt after a token record is imported - to adjust for token drift - so that the time-based tokens can be conveniently synchronized. Subsequent authentication attempts with the token will be restricted to the Inner window (maximum = 10) and Outer window (maximum = 100) values. For more details, see "Configure the Window Size for a Time-based Token’s First Authentication" on page 54.

> **Inner time-based OTP window size**—This handles time drift for time-based tokens. This value determines the number of token ticks the token can be out of sync with the server. An OTP found inside this window will be accepted and the server is updated to adjust for this token’s time drift. Default: 5.

![NOTE] Token ticks are defined in the token profile (under Time Period). The default is 30 seconds.

> **Outer time-based OTP window size**—This handles time drift for time-based tokens. This value determines the number of token ticks the token can be out of sync with the server if the OTP is not found in the inner window. If the OTP is found in the outer window, the user must provide the next OTP in sequence to successfully authenticate. Default value: 25.

![NOTE] Token ticks are defined in the token profile (under Time Period). The default is 30 seconds.
NOTE When a user is resyncing a token on the Self-Service site, or an admin is resyncing a token on the Token window of the SAS Management Console, the outer window is three times the setting, up to a maximum of 300. The actual outer window value, up to a maximum of 100, is only used during an authentication with an agent.

Synchronization supports the following token types:

- QUICKLog (event-based) Tokens configured for QUICKLog do not rely on time to remain synchronized with the server. Instead, each time an event-based token is activated a new token code is generated. For each login “event”, the server compares the submitted passcode with the expected passcode. Occasionally, a user may generate a passcode without using it, causing the token to be “ahead of” or out of sync with the server during the next login.
- CRYPTOCard/SafeNet KT series (time-based)
- SafeNet GOLD/Platinum
- MobilePASS
- eToken PASS
- Third-party OATH

**Display the Synchronization Policy Change Log**

To display the Synchronization Policy Change Log:

1. Click **POLICY > Token Policies > Synchronization**. The Synchronization section displays.
2. Click **Change Log** to display a record of the changes to the Synchronization fields.

<table>
<thead>
<tr>
<th>Change Time</th>
<th>Changed by Account</th>
<th>Changed by Account</th>
<th>Inner event-based OTP window</th>
<th>Outer event-based OTP window</th>
<th>First authentication time-based OTP window</th>
<th>Inner time-based OTP window</th>
<th>Outer time-based OTP window</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/19/2017 9:52:51 AM</td>
<td>Burryn</td>
<td>misa</td>
<td>10</td>
<td>100</td>
<td>5</td>
<td>5</td>
<td>25</td>
</tr>
<tr>
<td>12/19/2017 9:52:46 AM</td>
<td>Burryn</td>
<td>misa</td>
<td>10</td>
<td>100</td>
<td>15</td>
<td>5</td>
<td>25</td>
</tr>
<tr>
<td>12/19/2017 9:52:34 AM</td>
<td>Burryn</td>
<td>misa</td>
<td>10</td>
<td>100</td>
<td>5</td>
<td>5</td>
<td>25</td>
</tr>
<tr>
<td>12/19/2017 9:52:22 AM</td>
<td>Burryn</td>
<td>misa</td>
<td>15</td>
<td>100</td>
<td>5</td>
<td>5</td>
<td>25</td>
</tr>
</tbody>
</table>

3. Click **Close** to hide the Change Log.

**SMS/OTP**

This policy determines how the server will generate and deliver OTPs by SMS to users.
> **OTPs per SMS**—From one to five OTPs can be sent in an SMS message. This method applies only if the SMS token is issued in QUICKLog mode (refer to "POLICY > Token Policies" on page 93). In this mode the user receives an SMS message immediately after each successful authentication. By including more than 1 OTP, users that are temporarily outside of an SMS delivery zone will be able to authenticate until all OTPs in the message have been consumed.

If the SMS token is issued in Challenge/Response mode, the OTP is not sent until the user attempts to logon. SMS Challenge/Response is usually combined with Single Sign-on, whereby the user must first successfully authenticate with the Active Directory password, after which the Virtual Server automatically sends the OTP necessary to complete the authentication and logon process.

> **Resend OTP on Challenge**—If checked, the Virtual Server will send an OTP to the user if an empty or 1 character password is submitted in the **OTP/password** field during authentication.

> **Request Interval**—This setting determines the number of minutes that must elapse between Resend OTP on challenge requests. Requests received during this period are ignored by the server.

> **Challenge Time to Live**—This setting determines the lifespan of an OTP issued in Challenge/Response mode. An OTP that is unused after this period cannot be used to authenticate.

> **Send SMS messages via E-mail**—If enabled, all SMS token passcodes are sent via SMTP server. Use this option to deliver OTPs to an email address or to send OTPs using email to SMS. If disabled, all OTPs are sent via SMS gateway or modem.

> **Use the following method**—The options are **Replacement** and **Suffix**.

  - **Replacement**—OTPs are sent using the address from the field selected in the Use the following value option (described below). Typically, this will be a valid email address.

  - **Suffix**—OTPs are sent to an address that is the combination of the data in the Mobile/SMS field (User Detail) and the data contained in field selected in Use the following value option. For example, if Mobile/SMS contains 16135992441 and Custom #2 (selected) contains @na.rogers.com, the email will be sent to 16135992441@na.rogers.com.

> **Use the following value**—This selection determines the field used to provide the data for **Replacement** and **Suffix**. Options are **Email**, **Custom #1**, #2, or #3.

### Software Token Push OTP Setting

This policy determines if Push OTP communication is enabled for MobilePASS+.

This feature is not available with SAS PCE/SPE.
Figure 9: Token Policies > Software Token Push OTP Setting

![Software Token Push OTP Setting](image)

- **Apply Button**—Active when the policy is modified. Use to commit policy change.
- **Cancel**—Clears any uncommitted change to the policy and closes the module.
- **Change Log**—Displays a list of the last 5 changes to this policy as follows, including the date and time of each change, changed by the Account and Operator ID, and the value that was specified.
- **Enable Push OTP communication with MobilePASS+**—(not available with SAS PCE/SPE) This selection enables Push OTP communication for MobilePASS+. It applies to this Virtual Server.

When enabled, the **Allowed Targets Settings** options display the OS types where users can enroll MobilePASS tokens. The settings that you select in this policy will determine which targets are presented to users during MobilePASS token self-enrollment. Enrolled and active tokens cannot be transferred between the two apps.

**NOTE** These selections can also be made in "Allowed Targets" on the next page.

- **Enhanced Approval Workflow**—(not available with SAS PCE/SPE) Significantly accelerate the authentication process for MobilePASS+ (version 1.4 or higher) tokens and enable users to manage push login requests without unlocking their mobile device.

**NOTE** It is highly recommended that you either enforce a device PIN or enable a PIN setting in the MobilePASS token template so that only the device owner or token assignee can approve a push request.
NOTE If Enhanced Approval Workflow is enabled, users with incompatible versions of MobilePASS+ will receive an error message when the application opens. Enhanced Approval Workflow can be disabled at any time, restoring full functionality with earlier MobilePASS+ versions.

For new accounts created in SAS v3.5 (and higher), by default, iOS and Android are configured to MobilePASS+, and all other platforms are configured to MobilePASS 8.

For existing accounts, after the upgrade to SAS v3.5, all platforms are selected to deploy for MobilePASS 8 by default. You will need to enable iOS or Android (or both) for MobilePASS+.

Only one MobilePASS application per OS type can be selected. For example, you can enable iOS for either MobilePASS+ or MobilePASS 8, but not both.

MobilePASS+
- **Android**—If enabled, the token may be installed on Android O/S 4.x and 5.x.
- **iOS**—If enabled, the token may be installed on iPhones and iPads running iOS 7+.

MobilePASS 8
- **Android**—If enabled, the token may be installed on Android O/S 2.3+
- **iOS**—If enabled, the token may be installed on iPhones and iPads running iOS 6+
- **Mac OS X**—If enabled, the token may be installed on devices running OS 10.9 and 10.10.
- **Windows Phone**—If enabled, the token may be installed on devices running Windows Phone 8.1+
- **Windows**—If enabled, the token may be installed on Windows 7, 8, 8.1, and 10.
- **Windows RT**—If enabled, the token may be installed on Windows tablets running 8.1+
- **BlackBerry 10**—If enabled, the token may be installed on devices running OS 10.2+
- **BlackBerry Java**—If enabled, the token may be installed on these devices/specfied operating systems:
  - BB Curve 9320/OS 7.1
  - BB Torch 9800/OS 6.0
  - BB Bold Touch 9900/OS 7.0
  - BB Torch 9860/OS 7.1
  - BB 9700 (Bold)/running v5.0.0.979
  - BB 9810 (Torch)/running v7.1.0.714
  - BB 9900/OS 7.1

**Allowed Targets**
This policy is used to select the OS types where users can enroll MobilePASS and MP-1 tokens.
**WARNING** MP-1 tokens are deprecated. Please refer to the End-of-Sale announcement for full details.

MobilePASS

Figure 10: Token Policies > Allowed Targets Policy – MobilePASS

The MobilePASS tab consists of two sections—one for MobilePASS 8 target settings, and one for MobilePASS+ target settings. The settings that you select in this policy will determine which targets are presented to users during MobilePASS token self-enrollment. Enrolled and active tokens cannot be transferred between the two apps.

Note that one MobilePASS application per OS type can be selected. For example, you can enable iOS for either MobilePASS+ or MobilePASS 8, but not both.

For additional details on these selections, please refer to "Software Token Push OTP Setting " on page 104.

MP-1

**WARNING** MP-1 tokens are deprecated. Please refer to the End-of-Sale announcement for full details.
MP-1 tokens can be installed on a wide range of devices (targets).

- **Allow user to edit phone number and e-mail address during enrollment**—If enabled, the user will be able to modify the email address and/or mobile phone number to which the token enrollment message is delivered. By default, this option is disabled, forcing enrollment to occur through address and number in the users account detail.

- **Require Phone Description**—If selected, a list of devices configured in the MP Token Devices module (refer to "MP Token Devices" on the next page) will be displayed during the self-enrollment process.

- **Show MP target selector as a drop-down list**—If selected, targets are displayed in a drop-down list. If not selected, targets are displayed as radio button options.

- **Allow Install Locally**—If enabled, the user will have the option to install the MP on their PC, supported on Windows Desktop, up to Windows 8.x.

- **Allow Java Enabled Phone**—If enabled, the user will be able to install the token on mobile phones running the Java O/S. Options include USB/desktop and Over-the-Air (OTA) token installation. The type of method that can be used is determined by the phone manufacturer.

- **Allow Smart Card**—This option is disabled in this version.

- **Allow BlackBerry**—If enabled, the token may be installed on BlackBerry devices.

- **Allow Secure Flash Drive**—If enabled, the token may be installed on supported secure Flash Drives such as IronKey™ Enterprise and SafeStick™. Refer to the SafeNet website for a list of supported products and versions.

- **Allow iPhone**—If enabled, the token may be installed on iPhones and iPads running iOS 4.3+.

- **Allow Android**—If enabled, the token may be installed on devices running Android O/S 2.2+.

- **Allow Mac OS X**—If enabled, the token may be installed on devices running OS X 10.7 (Lion) or higher.

- **Allow Windows Phone 8**—If enabled, the token may be installed on devices running Windows Phone 7 or higher.
The device names presented to users during self-enrollment can be modified by changing the corresponding text in the **MP Token Targets** section.

**MP Token Devices**

This section allows the messages presented in the browser to the user during self-enrollment to be customized for both content and graphics. The messages will apply to the type of device selected in the **Type** list. Use this module to add instructions and support for target devices, such as specific models of mobile phones and USB drives.

**Figure 12: Token Policies > MP Token Devices**

![MP Token Devices](image_url)

An entry is added to the list for each custom device. Use the **Edit** and **Remove** links to edit and remove custom messages.

**Third-Party Authentication Options**

This policy determines the operation of the GrIDsure authentication method and RADIUS tokens.
Figure 13: Token Policies > Third-Party Authentication Options

**Gridsure Method**

This method presents a matrix of characters to the user during authentication. The user’s passcode is determined by overlaying their “PIP” (personal identification pattern) on the matrix and using the corresponding characters in the order the PIP was created. The white squares in the following image have been added to demonstrate the concept of a PIP, and a resulting passcode, in this case 87982, bearing in mind that the user might have created the PIP pattern in any order.

In other words, had the user created it right to left, the passcode for would have been 28978. There is no restriction on the order in which a pattern is created and indeed some cells in the pattern could have been used more than once. For example, assume left to right, repeating every second cell would mean that the passcode for this PIP would be: 8779882. The PIP can be combined with a PIN for an additional level of security.

**Figure 14: Gridsure method demonstrating a PIP**

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>1</td>
<td>7</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>9</td>
<td>1</td>
<td>7</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>6</td>
<td>9</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>7</td>
<td>2</td>
<td>0</td>
<td>6</td>
</tr>
</tbody>
</table>

To modify, select **Gridsure** from the list and then click **Edit**.
Figure 15: Token Policies > Modify GrIDsure method

> **Allow Trivial PINs**—If enabled, the user can select a row, column or 4 corners of the grid as their PIP.

> **Use Numbers, lowercase letters, uppercase letters, symbols**—Grids will contain characters from the enabled options. Note that the grid size is set under Token Templates (refer to "POLICY > Token Policies" on page 93), as is the requirement for a PIN, as well as the passcode that corresponds to the PIP.

> **Minimum PIP Length**—Specify the minimum number of characters for a PIP. Default: 4

**RADIUS Method**

RADIUS is a configuration that can be used with any third-party token. Its purpose is to provide enterprises with a simple and effective migration path from their existing third-party vendor’s authentication product to SAS and, in the process, extend most of the SAS Management UI functionality including PIN management, automated provisioning, authentication history and reporting and pre-authentication rules to users with the third-party tokens.

This method bears similarity with RADIUS proxy but there are substantial differences:

<table>
<thead>
<tr>
<th>Similarities</th>
<th>Differences</th>
</tr>
</thead>
<tbody>
<tr>
<td>SafeNet Authentication Service is configured as a RADIUS Client to the third-parties RADIUS server. Configuration is standard RADIUS – IP, port #, shared secret.</td>
<td>In RADIUS proxy, all user, token management, authentication history, reporting etc. must be done at the third-party RADIUS server. However, in RADIUS Token mode, all management can be done through SafeNet Authentication Service except for reassignment of third-party tokens.</td>
</tr>
</tbody>
</table>

Any tokens imported into SafeNet Authentication Service (refer to "Import Third Party Tokens" on page 55) using the RADIUS option automatically use the method as configured in this module.
**Figure 16: Migration using "RADIUS" Token**

To modify, select **RADIUS** from the list and then click **Edit**.

**Figure 17: Configure "RADIUS" Third-Party Token Support**
> **RADIUS IP**—This is the IP address of the third-party authentication server’s RADIUS server. During authentication, SafeNet Authentication Service will pass the OTP via this connection to the third-party server for passcode verification.

> **Secondary RADIUS IP**—Provides redundancy for the RADIUS IP setting above. This setting is optional but recommended.

> **RADIUS Port**—The port number on to be used for RADIUS requests. Default is 1812. This value must match the settings at the third-party authentication server.

> **RADIUS Shared Secret**—This is the shared secret used to encrypt RADIUS traffic. It must be identical in both SafeNet Authentication Service and the third-party RADIUS server.

> **User Name**—User ID. Must exist in both SAS and the third-party RADIUS server. In addition, the token assigned to the user must have been imported as a “RADIUS” token and must be the same token assigned to the user in the third-party server.

> **User Password**

> **Test**—Provides a way to test the configuration before saving the changes. Displays the results of the authentication test.

### Role Management

Use this module to manage Operator roles, alerts, and alert thresholds, and to select the SAS Management Console language.

**Figure 1: POLICY > Role Management**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role Management</td>
<td>Create roles by grouping management functions found on tabs and modules.</td>
</tr>
<tr>
<td>Alert Management</td>
<td>Set which email and/or SMS event alerts that operators will receive, according to their role.</td>
</tr>
<tr>
<td>External Alerts Recipients</td>
<td>Create a list of external recipients for email and/or SMS event alerts.</td>
</tr>
<tr>
<td>Event Thresholds</td>
<td>Set the conditions under which alerts will be sent.</td>
</tr>
<tr>
<td>Language</td>
<td>Set the language</td>
</tr>
<tr>
<td>Allowed Management IP Range</td>
<td>Restrict login to an account's SAS management UI to a specified IP range</td>
</tr>
</tbody>
</table>

### Role Management (task)

A role is a combination of tabs, modules, and actions within modules that are available to an Operator. Access to tabs and modules can be disabled. Where access to tabs and modules is allowed, the actions within any module can be restricted through policy settings.
For example:

- Disabling the Add function in the Tokens module on the ASSIGNMENT tab and the Access function in the Provisioning module removes the ability to assign or provision a token.
- Disabling the OPERATORS tab removes access to this tab and all of its modules.

This high degree of granularity means that operational security can easily be customized for each Virtual Server and role. The Operator role is always assigned to the person added through the Create Operator module on the ON-BOARDING tab. If a different role is required, create the user from within the Virtual Server (ASSIGNMENT tab, Create User shortcut), then promote the user to Operator status from the OPERATORS tab, selecting an appropriate role.

Roles are specific to the Virtual Server in which they are configured. The Operator role grants unrestricted rights to manage the Virtual Server. Existing roles are displayed in the roles list. Use the Edit or Remove links to edit or remove the corresponding role.

**Create an Operator Role**

All roles except the default Operator role can be edited or removed.

1. Click POLICY > Role Management and then click the Role Management task.
2. Click **Add**.

For similar roles, click **Duplicate** to make a copy of an existing role that you can edit.

3. Type the **Role Name**, and then click **Next**.
4. Select the access permissions for the tabs, modules, and actions.

<table>
<thead>
<tr>
<th>Role Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditor</td>
<td></td>
</tr>
<tr>
<td>Help Desk</td>
<td></td>
</tr>
<tr>
<td>Operator</td>
<td>Grants unrestricted rights to manage this authentication service (Default)</td>
</tr>
<tr>
<td>Snapshot Reports</td>
<td></td>
</tr>
</tbody>
</table>

Displaying: 1 to 4 of 4

<table>
<thead>
<tr>
<th>Display</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Close</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Role Name: Operator

Description: Grants unrestricted rights to manage this authentication service (Default)

<table>
<thead>
<tr>
<th>Module</th>
<th>Access</th>
<th>Edit</th>
<th>Delete</th>
<th>Add</th>
<th>Import</th>
<th>Export</th>
<th>View Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Activity</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication Metrics</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Snapshot Tab Token States</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMS Credits</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allocation</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>References</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Module</th>
<th>Access</th>
<th>Edit</th>
<th>Delete</th>
<th>Add</th>
<th>Import</th>
<th>Export</th>
<th>View Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create User</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Search User</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>User Detail</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Tokens</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Authentication Activity</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication Metrics</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Restrictions</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Group Membership</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>RADIUS Attributes</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Provisioning</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>SAML Services</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Import Users</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Module</th>
<th>Access</th>
<th>Edit</th>
<th>Delete</th>
<th>Add</th>
<th>Import</th>
<th>Export</th>
<th>View Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Token Search</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Import SafeNet Tokens</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Bulk Assign Third-Party Tokens</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Initialize Hardware Tokens</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Module</th>
<th>Access</th>
<th>Edit</th>
<th>Delete</th>
<th>Add</th>
<th>Import</th>
<th>Export</th>
<th>View Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Maintenance</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Group Membership</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>RADIUS Attributes Group</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Container Maintenance</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Container Member</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>
CAUTION! It is a best practice to limit a role with Remote Services access to a specific API user. A user whose role includes Remote Services has full access to the management API, regardless of any other limitations that are imposed on the user.

5. Click Save to commit the role configuration.

Add or Edit a Role
To add a role or edit an existing role, click the Add button or Edit hyperlink respectively. If adding, you will be prompted to create a role name and a role description, after which you’ll be presented with the Role configuration page.

The Role configuration page ("Create an Operator Role" on page 114) is split into several horizontal sections, each representing a different Virtual Server tab. Within each section is a table listing all modules available on the tab and a corresponding set of actions available for each module. Clearing a check box removes the tab, module, or action from the role.

Module Actions
Choose from the following actions for each module, by selecting the associated checkbox:

> Access—Displays the module.
> **Edit**—Enables the Role to access edit functions.
> **Delete**—Enables the Role to access delete or remove functions.
> **Add**—Enables the Role to access add functions.
> **Import**—Enables the Role to access import functions.
> **Export**—Enables the Role to access export functions.
> **View Log**—Enables the Role to access the View Log function.

**Alert Management**

The Virtual Server can generate alerts when a condition or threshold is detected or exceeded. By default an alert policy with all alerts disabled is attached to every role when the role is created. Edit the default policy for each role to enable the desired alert and delivery method.

To configure alerts:

1. Click **Policy > Role Management > Alert Management**.

2. Click **Edit** corresponding to a role.
Alerts can be delivered by e-mail and/or SMS message. To enable an alert, check the corresponding check box according to the method of delivery. Commit the changes by clicking the **Apply** button.

- **Organization Capacity**—If enabled, an alert will be sent when the Virtual Server capacity falls below the threshold. (Refer to “Alert Management” on the previous page on page "Alert Management" on the previous page.)

- **Account SMS Credits**—If enabled, an alert will be sent when available SMS Credits falls below the threshold.

- **Operator Status Change**—If enabled, an alert will be sent when an Operator’s status is changed to/from Active, Suspended, Removed.

- **Expired Reservation**—If enabled, an alert is generated for each user in a provisioning task who has not enrolled their token before the stop date.

- **Enrollment Lockout**—If enabled, an alert is generated if the user exceeds the maximum number of attempts to enroll their token. (Refer to “Self-Enrollment Policy” on page 129 on page "Self-Enrollment Policy" on page 129.)

- **Hardware Assignment Notification**—If enabled, an alert including the User detail is sent when a hardware token is assigned to a user.
> **Hardware Provisioning Notification**—If enabled, an alert including the User detail and address is sent when a hardware token is assigned to a user. This option is useful for alerting a third-party fulfillment service with information necessary to deliver the hardware token to the user.

> **LDAP Sync Notification**—If enabled an alert is sent each time LDAP synchronization results in an update to the server. A sync notification alert indicates why user synchronization failed—it lists all affected users and the error that caused the failure, so that the user data can be corrected in the user source.

If the alert has been customized, the failure information can be added by manually inserting the following text into the alert template after the `<removeList />` section:

The following `<totalProblemUsers />` users have properties that prevented a successful sync:

```xml
<problemUserList />:
```

NOTE It is recommended that you set this alert. For more information, see the SafeNet Authentication Service Synchronization Agent: FAQS.

> **Service Notifications**—If enabled, service notifications are delivered by the selected method. Note that service notifications are created by the Service Provider and are always published to the management logon page.

> **Provisioning Notification**—If enabled, an alert is sent each time a provisioning task is created.

> **Operator Lockout Alert**—If enabled, an alert is sent when an Operator account becomes locked.

> **Operator Unlock Alert**—If enabled, an alert is sent when an Operator account becomes unlocked.

> **Auth Node Changes**—If enabled, an alert is delivered sent when an Auth Node is added, modified or removed from the Virtual Server.

> **Allocation/Deallocation Alert**—If enabled, an alert is sent whenever inventory (Capacity, tokens, SMS credits, ICE) are add to or removed from the Virtual Server.

> **Lost Token Report**—If enabled, an alert is sent when user reports a lost token.

> **Dormant Account Alert**—If enabled, an alert is sent when the user is approaching their Dormant Account Lockout threshold.

> **Organization Stop Date**—If enabled, an alert is sent when the Account Service Stop date is within X days of the current date. The threshold should be adjusted accordingly.

> **Sync Host Notification**—If enabled, an alert is sent indicating that permissions should be edited to allow the SAS server to accept syncs from the Synchronization Agent. This option is enabled by default when creating a new Virtual Server. The alert is only sent when a newly added agent attempts a sync for the first time.

> **Push Notification Rejection Operator Alert**—If enabled, an alert is sent to the Operator when a user denies a push notification request from their device.

**External Alerts Recipients**

Use this policy to configure alerts and delivery method(s) for recipients that are not Operators. Configuration of this policy is similar to **Alert Management Policy** with the following exceptions:

> **Alert Name**—Use this to classify the set of alerts.
Alert Recipients—This is a list of recipients. A valid address or mobile number must be entered if alert delivery will be by email or SMS message respectively. Click the Add button to update the recipient list.

Figure 3: Role Management > External Alerts Recipients > Set Event Recipients
Event Thresholds

Figure 5: Role Management > Event Thresholds > Set Event Thresholds

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Threshold</th>
<th>Alert Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization Capacity</td>
<td>0</td>
<td>Send alert when available capacity falls below X.</td>
</tr>
<tr>
<td>Account SMS Credits</td>
<td>0</td>
<td>Send alert when SMS credits falls below X.</td>
</tr>
<tr>
<td>Allocation/Deallocation Alert</td>
<td>1</td>
<td>Send an alert when an allocation or deallocation involving at least X tokens or capacity occurs.</td>
</tr>
<tr>
<td>Organization Stop Date</td>
<td>30</td>
<td>Send alert X days before Stop Date.</td>
</tr>
</tbody>
</table>

Use this policy to configure the server to monitor for specific alerts and thresholds where:
> **Organizational Capacity**—This is related to the capacity of the virtual server. An alert is generated if the value falls below the threshold.

> **Account SMS Credits**—This is related to the number of SMS credits in inventory. An alert is generated if the value falls below the threshold.

> **Allocation/Deallocation Alert**—An alert is generated whenever inventory (Capacity, tokens, SMS credits, ICE) are add to or removed from the virtual server.

> **Organization Stop Date**—An alert is generated X days before the stop date.

**Language**

Use this policy to set the default language of the SAS Management Console. Currently, only the English language can be designated as the default language.

**Figure 6: Role Management > Language**

![Language Configuration](image)

While English is currently the only language available as the default language for the SAS Management Console, Operators can specify their own language preference if desired, which will take effect upon login. There are two locations in SAS where an Operator can set their language preference:

> **SAS Login page**—At the bottom of the SAS Login page, links are provided for English and Français.

![SAS Login Page](image)

> **SAS Management Console Home page**—On the SAS Management Console Home page, a **Language** option is provided at the top of the page. Placing the mouse cursor over the Language button will present the options English and Français, as well as any other language sets that may have been created.

![Language Option](image)
All text in the Console will be switched to the selected language, including fields, buttons, tabs, menus, and descriptions (as shown in the example below). It should be noted that log files will always be presented in the English language.

**Allowed Management IP Range**
Use this policy to restrict an account's SAS logon to a specific IP range.

**Figure 7: Role Management > Allowed Management IP Range**

<table>
<thead>
<tr>
<th>Allowed Management IP Range:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply</td>
</tr>
<tr>
<td>Enable Allowed Management IP Range:</td>
</tr>
</tbody>
</table>

No Records

To add a range in which the account's SAS Management UI logon is allowed, click **Add**.

**Figure 8: Role Management > Allowed Management IP Range > Add IP Range**

<table>
<thead>
<tr>
<th>Allowed Management IP Range:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply</td>
</tr>
<tr>
<td>Enable Allowed Management IP Range:</td>
</tr>
</tbody>
</table>

No Records

Add IP Range

- **Name**—This is a friendly name for this range.
- **Start IP**—This is the beginning of the IP address range to be enabled or disabled.
- **End IP**—This is the end of the IP address range to be enabled or disabled.

**Automation Policies**
Automation policies are used to auto-provision users with tokens, and to control the self-enrollment and self-service functions.
**Time Zone Offset**

Use this policy to control the offset from Coordinated Universal Time (UTC) of the time recorded for a reported activity.

- **Apply**—Use to commit policy change.
- **Cancel**—Use to cancel any uncommitted change to the policy and close the module.
- **Adjust Time Zone relative to UTC**—Select the offset in hours from the UTC.

Time adjustments are local to the Virtual Server.

**Time Zone Offset affects:**

- Date/Timestamps used in all reports
- The scheduled Run Time of a report
- Date/Timestamp of Provisioning Tasks
- Enrollment Date/Timestamp
- Snapshot/Authentication Activity Date/Timestamp
- Date/Timestamp of Allocation/Deallocation
- Date/Timestamp of Operator Activity
- Date/Timestamp of External Operator Activity in Virtual Server
- Pre-Auth Rules using time/date:
  - Start/stop of rule
• Account day/time restrictions (authentication)

The **Time Zone Offset** is automatically inherited from the parent at the time of account creation.

If an account has no parent (the first account on a system), its offset is based on the local server time. The local server time of account in the cloud is UTC 0.

When an account’s **Time Zone Offset** is changed, the upcoming scheduled reports are not affected. Only after a scheduled report is run will a recurring report be scheduled using the new offset.

If the account is a Subscriber, time stamp changes affect the virtual server only.

If the account is a Service Provider, time stamp changes affect the Service Provider’s virtual server AND all reports and activities performed at the Service Provider level (for example, Administration | Reports, Allocation/deallocation Date/Time Stamp, all view log data).

A **Time Zone Offset** adjustment may impact the date of an activity.

### Provisioning Rules

One of the most powerful features of the server, provisioning rules determine under what conditions tokens will be automatically issued and revoked. Combine provisioning rules with pre-authentication rules to seamlessly migrate users from static passwords to token authentication without service interruption and with little to no administration.

Rules are triggered when group memberships and other user attributes change. For example, if a user is added to a group included in a rule, SAS will provision the user with a token. Conversely, if a user is removed from a group included in the rule, SAS will revoke the token.

Provisioning rules can be used with internal groups or LDAP synchronized groups. By combining provisioning rules with LDAP synchronization or integration, the server can automatically issue and revoke tokens based on changes made in LDAP without the intervention of an Operator.

### Create a Provisioning Rule

To create a provisioning rule:

1. Click **POLICY > Automation Policies > Provisioning Rules**.
2. Click **New Rule**.

The “Add New Provisioning Rule” section displays.
The following options are available:

> **Rule Name**—This is a unique, descriptive name for the rule.

> **Token Type**—This is the type of token to be provisioned when the rule evaluates true.

> **Issue Duplicate Types**—If unchecked, a user will not be provisioned with the selected token type if they already have one of the same type as a result of manually assigning a token or a different rule evaluating true.
> **Auto Revoke**—If checked, the token issued by this rule will be revoked if the rule evaluates false for the user such as when a user has been removed from the monitored group(s).

![NOTE] This option should only be selected in the case that a user remains synced to SAS but the provisioning rule no longer applies. If a user is removed from SAS (for example because they are no longer part of a sync group) all of their tokens are revoked whether or not Auto Revoke is selected.

> **Notify Users With Active Provisioning Revoke**—If checked, users are notified if their auto provisioned tokens are revoked by the provisioning rule.

> **Container**—The user must reside in the selected container for the rule to evaluate true.

> **Require Expiring**—Enable this option to provision a replacement token N days before the expiration date of any assigned tokens. Enabling **Auto Revoke** results in the replaced token being revoked immediately upon the user completing enrollment of the replacement token.

> **Require In-Service Expire**—This option is used to replace tokens that have been in the field for an extended period of time and are likely to need battery replacement. Enable this option to provision a replacement token for any assigned tokens that has been in use for more than N years. Enabling **Auto Revoke** results in the replaced token being revoked immediately upon the user completing enrollment of the replacement token.

> **Assign as ICE Token**—This option is available only if ICE capacity has been added to the server. If checked, the user will be provisioned with an ICE token which after enrollment can only be used to authenticate during the life of the ICE license.

> **Target Groups**—The group(s) to which the rule will apply.

> **Affected Group Members**

  - **Users that belong to ANY of the target groups. (OR Logic. Highly Recommended.)**
    
    If one or more groups are selected for a rule, users that belong to any of the selected groups will be included in the rule.

  - **Users that belong to ALL of the target groups. (AND Logic. Use with Caution.)**
    
    If multiple groups are selected for a rule, only the users that belong to all of the selected groups will be included in the rule. For example, if GroupA, GroupB, and GroupC are selected, only users that belong to GroupA, AND GroupB, AND GroupC will be included in the rule.

**About Affected Group Members**

Consider the case where you create provisioning rule “One” for Group A. Initially, the rule applies to all users in that group. However, that may change if you add a group to the original rule, depending upon whether you apply OR logic or AND logic, as described in the scenarios that follow.

![CAUTION!] If you add a group to an existing provisioning rule, you may dramatically and unexpectedly change the effect of the rule.

For example, if you add a group to an AND logic provisioning rule which has provisioned tokens and Auto Revoke selected, then all users from the original group(s) that are not also members of the added group will have their tokens revoked.
Scenario 1: Select “Users that belong to ANY of the target groups. (OR Logic. Highly Recommended.)”

If you select “Users that belong to ANY of the target groups” and apply rule “One” to Group B (i.e., add Group B to rule “One”); the rule will apply to ALL users from Group A and Group B, as shown in the following table.

<table>
<thead>
<tr>
<th>Group</th>
<th>Users</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Alfred, Betty, Carson, Diane, Emil, Fred</td>
<td>After you add Group B to rule “One”, the users to which the rule applies is expanded to include Cory, Debbie, and Ernest (i.e., the users that belong to ANY of the groups listed in the rule).</td>
</tr>
<tr>
<td>B</td>
<td>Betty, Cory, Debbie, Ernest, Fred</td>
<td>If Auto Revoke is a condition of the rule, none of the users from Groups A and B will have their tokens revoked.</td>
</tr>
</tbody>
</table>

Scenario 2: Select “Users that belong to ALL of the target groups. (AND Logic. Use with Caution.)”

If you select “Users that belong to ALL of the target groups” and apply rule “One” to Group B (i.e., add Group B to rule “One”); the rule will apply to only the users whom belong to both Group A AND Group B, as shown in the following table (i.e., Betty and Fred).

<table>
<thead>
<tr>
<th>Group</th>
<th>Users</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Alfred, Betty, Carson, Diane, Emil, Fred</td>
<td>After you add Group B to rule “One”, the users to which the rule applies is reduced to Betty and Fred (i.e., the only users that belong to ALL groups listed in the rule). If Auto Revoke is a condition of the rule, the users that were previously assigned tokens by rule “One” that don’t belong to ALL groups (i.e., Alfred, Carson, Diane, and Emil) will have their tokens revoked.</td>
</tr>
<tr>
<td>B</td>
<td>Betty, Cory, Debbie, Ernest, Fred</td>
<td></td>
</tr>
</tbody>
</table>

Self-Enrollment Policy

Use this policy to control self-enrollment thresholds and alerts.
**Self-Enrollment base URL**—This is the URL to which the user will be directed as a result of a provisioning task and is included in the enrollment email instructions to the user. Do not modify this value unless you have installed a stand-alone enrollment web server.

**To enforce self-service over SSL, replace http with https in the Self-Enrollment Base URL field. Do not modify this value unless you have installed a stand-alone enrollment web server and have a valid certificate installed.**

**Activation Code Format**—This option determines the strength of the activation code included in the enrollment message and encoded in the enrollment URL. Options are numeric, alphabetic or Alphanumeric formats.

**Reservation time to live**—This is the maximum number of days the user has to complete enrollment commencing with the start date of the provisioning task. This value is added to the provisioning task start date to generate the provisioning task stop date. If set to 0, a provisioning task will never expire. The default value is 10 days.

**Enrollment lockout after**—This value determines the number of failed enrollment attempts by a user. When this threshold is exceeded, the user will be unable to enroll their token.

**Days Before Expiry To Warn**—This value allows you to send a provisioning reminder via email to the user a specified number of days (0-31) before expiration of their provisioning task. The default setting is 0, which will not send a reminder. You can modify the email message template called EnrollmentExpiring to customize the content of the expiry reminder email sent to the user.

**Enable Multi-Device Instructions**—If checked, the Multi-Device Instructions section in SELF-SERVICE > Configure Self-Enrollment Pages is enabled in the self-enrollment policy for MobilePASS tokens. Multi-Device Instructions 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 that are related to their chosen device type and selected in POLICY > Token Policies.
• 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).

> **Display QR Code**—If checked, the enrollment email sent to the user will include the link to the page on the SAS Self-Service module where the QR code is displayed.

• The QR code will display only if a supported device is selected in the device selection drop down menu of the enrollment email.

### SAML Provisioning Rules

For a user to authenticate against a SAML Service Provider (for example, Google Apps, Salesforce), they must be given the appropriate rights. SAML Provisioning Rules are designed to replace the manual process (refer to "SAML Services" on page 47) of creating SAML associations.

In effect, a rule automatically creates the appropriate associations based on user attributes such as group membership. For example, the action of adding or removing a user from an Active Directory security group will cause the rule to automatically create or remove SAML associations affected by the rule.

To configure or edit a rule, click the **New Rule** button or the **Edit** link respectively.

**Figure 6: POLICY > Automation Policies > SAML Provisioning Rules**

> **Rule Name**—A name that describes the rule.
> **User is in container**—Users affected by this rule must be in the selected container.

> **Server Groups**—Users in these groups are not affected by this rule.

> **Rule Groups**—Users must be in one or more of these groups to be affected by this rule.

> **Relying Parties**—Service Providers in this section are not affected by this rule. This list contains all configured "SAML Service Providers" on page 165.

> **Rule Parties**—Users that belong to one or more of the Rule Groups will be able to authenticate against Service Providers in this section.

> **SAML Login ID**—The User ID that is returned to the service provider in the SAML assertion. If your service provider (e.g., Salesforce) requires a User ID of name@domain.com, and this is identical to the user’s email address, choose the **Email** option. Doing so allows the user to consistently use their user ID to authenticate regardless of the service provider’s requirements. Typically, a service provider will require either the user ID or e-mail. For all other cases, choose the **Custom** option and enter the required user ID to be returned.

### Role Provisioning Rules

Use this function to automatically add an Account Manager and grant access to the management UI based on attributes such as Active Directory group membership. Conversely an Account Manager can be automatically removed if the rule that promoted the user to Account Manager evaluates false.
To add a rule, click the **New Rule** button, where:

- **Rule Name**—This must be a unique name which identifies the rule.
- **Auto Revoke**—If selected, the Account Manager created by this rule will be automatically removed if the conditions (for example, group membership) are no longer valid.
- **Containers**—This is container where the user must reside for the rule to evaluate true.
- **Role**—This is the role that will be assigned to the Account Manager. The list includes all configured roles.
- **Scope**—Account management groups list all configured groups. The Account Manager will have access to groups listed in the **Applied by Rule** window. Use the arrow keys to move highlighted groups between the two windows.
- **Groups Filter**—The **Virtual Server** groups window lists all groups in the virtual server. Users that are members of one or more of the groups in the **Used by rule** window will be promoted to Account Manager. Use the arrow keys to move highlighted groups between the two windows.
Auto Remove

Auto remove is used to automatically remove reports and alerts that are no longer required based on their age. This function only removes the entries in the various lists. Data is retained in the system and available by running the report again, if necessary.

Figure 8: POLICY > Automation Policies > Auto Remove

Provisioning Policy

Auto-provisioning can be enabled for users in nested groups.

Figure 9: POLICY > Automation Policies > Provisioning Policy

Provisioning Rules will use nested group relations — Select this option to enable this policy. When enabled, provisioning rules for a parent group will be applied to all of its nested groups in SAS, and all users that are in the nested groups will receive an email for token activation. This policy applies to user and role provisioning. SAML service provisioning applies to users in nested groups regardless of this setting.
The COMMS tab contains the following modules:

- **Communications**—Configure/Customize SMS gateways, SMTP email, and content of outbound SMS and Email messages.
- **LDAP**—Configure LDAP integration.

  **NOTE** LDAP integration is available only on SAS SPE/PCE. For SAS Cloud, refer to "LDAP Sync Server Settings" on page 142.

- **Authentication Processing**—Configure Pre-authentication rules, LDAP Synchronization, and Agent key files.
- **Auth Nodes**—Configure Auth Nodes, Sharing, and Realms.
- **SAML Service Providers**—Configure SAML Service Providers.
- **Custom Branding**—Customize the appearance of the SAS console.

**Figure 1: COMMS**
Communications

Figure 1: COMMS > Communications

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS Settings</td>
<td>Configure the settings for SMS plugins.</td>
</tr>
<tr>
<td>Email Settings</td>
<td>Configure connection settings for the email server.</td>
</tr>
<tr>
<td>SMS Messages</td>
<td>Customize the text and formatting of SMS messages.</td>
</tr>
<tr>
<td>Email Messages</td>
<td>Customize the text and formatting of email messages.</td>
</tr>
<tr>
<td>LDAP Sync Server Settings</td>
<td>Set URL and port for the LDAP Sync Server.</td>
</tr>
<tr>
<td>FTP/SFTP/SCP Settings</td>
<td>Customize the settings for FTP/SFTP/SCP transfer of reports.</td>
</tr>
<tr>
<td>Logging Agent Server Settings</td>
<td>Set URL and port for the Logging Agent Server.</td>
</tr>
</tbody>
</table>

SMS Settings

SMS gateways are used to send SMS/OTPs and alerts. There are two options for sending SMS messages:

> **Default**—In this option, SMS messages will be sent via your Service Provider’s SMS gateway. This option can be used only if you have been allocated SMS credits by your Service Provider. You can verify this from the **Allocation** module on the **SNAPSHOT** tab under the SMS Credits column.

> **Custom**—Select this option to configure the Virtual Server to send SMS messages via a gateway service to which you’ve subscribed or SMS modem installed at your site. You can verify the ability to send SMS messages by entering the number of a device capable of receiving SMS messages in the **SMS Mobile Number** field. SMS phone numbers must contain only digits and must begin with a country code.

Figure 2: COMMS > Communications > SMS Settings (Default)

**Custom SMS Settings**

To configure the Virtual Server to use an SMS gateway service or modem, start by selecting the Custom option, and then provide details about the SMS provider you are using:

> **Gateway**—Select to configure a primary and failover SMS service provider.
• **SMS Plugin**—The list includes a number of preconfigured providers. If the SMS provider you are using is not listed, select the **Generic HTTP(s) SMS Plugin** option. See “Using a Generic HTTP(s) SMS Plugin” on the next page.

**Figure 3: COMMS > Communications > SMS Settings (Custom)**

The options for configuration will vary depending on your SMS plug-in selection. Your gateway service provider will supply the necessary configuration information.

**NOTE** For the Clickatell SMS Plugin, if you purchased the "customization" feature from Clickatell, you can use an alternate Sender ID. When you select **Clickatell SMS Plugin**, a message next to the **Sender ID** field indicates the requirements for this optional functionality.

Other configuration options that may be available, depending on your network and SMS gateway service provider:

> **Use Proxy**—If you will be sending SMS messages via a Proxy Server, select **Yes**, and then add the Proxy URL, Proxy Port, Proxy Username, and Proxy Password.

> **Use Flash SMS**—Use this option if the gateway supports Flash SMS and you do not want SMS messages stored on the receiving device.

> **Use Overwrite SMS**—Use this option if the gateway supports Overwrite SMS, causing the previous SMS message stored on the receiving device to be overwritten by each new message.
Using a Generic HTTP(S) SMS Plugin

Select the Generic HTTP(s) SMS Plugin option to configure communications with SMS service providers not included in the SMS Plugin list. Refer to the provider’s documentation for guidance on formatting entries in SAS. Available configuration options include the following:

> **Method Name**—Select GET or POST, based on what your SMS service provider requires.

> **Add parameters to URL**—When set to True, this function will encode a space as a "+" sign, as specified in URLEncode(). If set to False, a space is encoded as "%20". Check with your SMS provider as to which setting is recommended. Most SMS providers support both encodings, while some will only support one of the two available options.

> **SMS URL**—Enter the SMS URL. For example: http://api.<SMS provider>.com/http/sendmsg

  - If the selected method is GET, the SMS message is sent as a page request with the parameters on the same line as the URL. They are appended to the page name with a ?, followed by the key, followed by an =, and then the value. Use & to add another key-value pair.

  - If the selected method is POST, the SMS message is sent as a page request with the parameters attached as a query string included in the message body (rather than with the URL).

> **Destination Parameter Name**—Enter the name (a key, as described above in SMS URL) the SMS provider wants for the cellphone number.

> **Message Parameter Name**—Enter the name (a key, as described above in SMS URL) the SMS provider wants for the message to be sent.

> **Success Message Contains String**—Enter the text string SAS sends back for a success message.

> **Use Proxy**—If you will be sending SMS messages via a Proxy Server, select Yes, and then add the Proxy URL, Proxy Port, Proxy Username, and Proxy Password.

If additional parameters are required, click Add Parameter, and enter them as key-value pairs. You will notice below that you can also flag a field as a password to hide the contents of a field.
E-mail Settings

SMTP servers are used to send enrollment messages and alerts. There are two options for sending e-mail messages:

> **Default**—Send email messages via your Service Provider’s SMTP server.

E-mail sent via the Service Providers SMTP server will not appear to come from your account. In addition, any failed deliveries (for example, invalid e-mail address) will be sent to the Service Provider’s e-mail server.

> **Custom**—Send email messages via the account’s SMTP server. E-mail sent via the account’s SMTP server will appear to come from the account. Any failed delivery notices will be sent to the account’s e-mail server. You can verify the Virtual Server’s ability to send e-mail messages by entering a valid e-mail address in the **Test To Address** field, and then clicking the **Test** button.

If using a third-party email server, you can modify the **From Address** by choosing the **Custom** option in the **From Address** group then enter a custom address.
**Custom E-mail Settings**

To configure the Virtual Server to use the account’s SMTP server, start by selecting the **Custom** option.

**SMS Messages**

You can customize the various SMS/OTP messages that are sent by the Virtual Server. Start by selecting the **Custom** option, and then select an **SMS Message Type** from the list. The message content is displayed in the **Message** box.
NOTE You can add !MUTE! to the beginning of any SMS or e-mail message to prevent it from being sent.

Refer to the SAS Service Provider Branding Guide for information about customizing SMS messages.

**Email Messages**

You can customize the various e-mail messages that are sent by the Virtual Server. Start by selecting the **Custom** option, and then select an **E-mail Message Type** from the list. The message content is displayed in the **Message** box.

Messages that are sent in response to an alert can be sent by e-mail, SMS, or both (refer to "Alert Management" on page 118). The **SMS Content** field is presented for messages that support both types of delivery. SMS messages greater than 160 characters including spaces will span multiple SMS messages.

Note that an SMS Credit is consumed for each SMS alert message unless the Virtual Server is configured to use an SMS gateway.

Refer to the SAS Service Provider Branding Guide for information about customizing email messages.
LDAP Sync Server Settings

This function is used to change the default location of the LDAP synchronization server. Synchronization agents will transmit to this location. Do not modify the default settings unless you have installed and configured a separate synchronization server.
FTP/SFTP/SCP Settings

Reports generated by the virtual server can be sent by FTP, SFTP, or SCP. This module defines the location and connection information to the remote FTP, SFTP, or SCP server.

Figure 9: Communications > LDAP Sync Server Settings

**WARNING** MP-1 tokens are deprecated. Please refer to the End-of-Sale announcement for full details.

**NOTE** For SFTP connections, the following SSH ciphers and MACs are supported:
- Key Exchange: diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1
- Cipher: 3des-cbc, aes128-cbc
- MAC: hmac-md5
Logging Agent Server Settings

To configure settings for a Logging Agent server other than the default, select Custom.

Figure 11: COMMS > Communications > Logging Agent Server Settings

Inbound is the Logging Agent server address to which Logging Agents “send” data. Outbound is the Logging Agent server address from which the agent “receives” packets. This information is also displayed under COMMS > Authentication Processing > Logging Agent.

- **Primary Host/IP** — This is the FQDN host name or IP address of the Logging Agent server.
- **Failover Host/IP** — This is the FQDN host name or IP address of the alternate Logging Agent server if the primary server selection is not available.
- **Port** — This is the port number to connect to the Logging Agent server.

LDAP (SAS SPE/PCE Only)

**NOTE** LDAP integration is available only on SAS SPE/PCE. SafeNet Authentication Service - SAS subscribers must use the Synchronization Agent. See "LDAP Sync Server Settings" on page 142.

Use the COMMS > LDAP module to configure LDAP integration. In SAS PCE/SPE v3.4 and later, LDAP integration is implemented as a service, replacing the Direct LDAP Integration feature that was included in earlier releases of SAS PCE/SPE.

LDAP integration should be configured only where a high speed, permanent connection is assured, and LDAP failover is configured. The loss of connection between the Virtual Server and all LDAP user sources will result in an authentication service outage.
The SAS LDAP Integrator service enables SAS to make a direct connection to LDAP without the need for an external agent. The service runs automatically on startup. It scans LDAP users and groups every five minutes, and updates the SAS database to match the contents of LDAP. The scan interval is not configurable.

The user information is stored internally in the SAS database, and SAS is not required to make connections to LDAP for each authentication demand, which results in efficient performance. SAS can continue to operate even when LDAP is disconnected or non-responsive.

Configuring LDAP integration enables users to be automatically added, suspended, or removed from an account’s Virtual Server, which eliminates the need to manually create and manage users or to use a synchronization agent.

With integration, UserIDs, group membership, and other LDAP/AD user attributes are validated against the LDAP source for every user lookup and authentication that is performed in the Virtual Server. Integration supports additional functionality, such as chained authentication (LDAP authentication followed by OTP authentication) and static password validation against Active Directory.

In addition to basic user information, synchronization includes the users’ Active Directory group membership, which can be used for:

- Automatic provisioning of tokens to users (Refer to “Time Zone Offset” on page 125)
- Automatic revocation of tokens from users
- LDAP pre-authentication and authorization
- Chained authentication
Configure the LDAP User Source

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.

If your LDAP/AD does not use a default schema, you must configure a compatible schema in the Virtual Server before you configure the LDAP User Source. Do this from the Schema Management link. (See “Schema Management” on page 148.)

1. Select Comms and expand the LDAP module.

2. Click LDAP User Source.

3. Configure the Virtual Server to connect directly to your LDAP/Active Directory.
   - **Host name or IP Address**—The FQDN host name or IP address of your LDAP/AD.
   - **Port**—The port number allowed to connect to LDAP/AD.
   - **Use TLS for LDAP connection**—Check this option if you have a certificate installed on your LDAP/AD server.
   - **Number of Failover Hosts**—The number of failover LDAP/AD servers to which the Virtual Server will attempt to connect in the event the primary LDAP/AD cannot be reached.
   - **Connection Timeout (secs)**—The time in seconds before the connection terminates.

4. Click Next.

5. Select an LDAP Schema from the list, and then click Next.
6. Provide a valid user account that can be used by the Virtual Server to connect to your LDAP/AD.

The Virtual Server does not write to LDAP. The account privileges need only be sufficient to allow the Virtual Server to connect and browse the schema.

After a connection is established, the Virtual Server automatically detects all DNs containing users that will be integrated with the Virtual Server. Users added or removed from these DNs are automatically added or removed from the Virtual Server.

7. To remove DNs from integration with the Virtual Server, select the **Manually edit searched containers** option.

8. To use the Virtual Server to authenticate users in your LDAP/AD user source, as well as users that are not in that user source, select the **Use Local Database** option.

9. The Virtual Server can simultaneously support LDAP integration or LDAP synchronization, and the creation and management of users in its SQL database.

10. Click **Done** to save the configuration.

Users in your LDAP/AD directory will automatically be populated in the Virtual Server.
Schema Management

You can add a custom schema to the Virtual Server.

1. Click **Schema Management**.

2. In the **Schema** drop-down list, select a default schema that is most like your custom schema.

   ![Schema Configuration](image)

   The page displays the default schema mappings.

3. Adjust the defaults to map your schema to the **User** and **Group Attributes**, **Object Class**, and **Custom Fields** where:
   - **User Attributes** and **Custom Fields**
     These are the fields that appear in the User detail.
The Virtual Server in conjunction with LDAP Pre-auth Rules can take advantage of additional attributes found in Active Directory including:

- **userAccountControl**—The Virtual Server will not authenticate a User whose account is disabled in Active Directory.
- **lockoutTime**—The Virtual Server will authenticate a user only during the **Days/Times** set in Active Directory.
- **memberOf**—The Virtual Server will authenticate a user based on their Active Directory group membership. This is usually combined with source IP and other attributes in Pre-authentication rules.
- **accountExpires**—The Virtual Server will not authenticate an expired Active Directory user account.

**LDAP Synchronization**

Users can be automatically added, suspended, or removed from the account’s Virtual Server by using the LDAP Synchronization Agent, eliminating the need to manually create and manage users. The agent comes with support for standard Active Directory, eDirectory, and SunOne. The agent can be configured to support non-standard schemas.

This method requires the installation of a Synchronization Agent, normally somewhere on the same network as the AD/LDAP directory.

**Figure 3: LDAP/AD Synchronization Agent**

The Agent is configured to monitor the specified LDAP containers (DNs) and groups for changes such as adding or removing a user, synchronizing and applying these changes at the Virtual Server.

Synchronization can be coupled with other workflow automation policies such as:

> Automatic provisioning of tokens to users (Refer to "Time Zone Offset" on page 125)
> Automatic revocation of tokens from users
> LDAP pre-authentication and authorization

SAS 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 marked as lost with a comment, and the UserID is replaced by the overlapping LDAP UserID.

To configure your system for LDAP synchronization, see the *SAS Synchronization Agent Configuration Guide*. 

---

SafeNet Authentication Service Subscriber Account Operator Guide
Release 3.7.15 007-012406-003 Rev. G March 2018
## Authentication Processing

Figure 1: COMMS > Authentication Processing

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-authentication Rules</td>
<td>Set filter attributes to be evaluated before validating credentials.</td>
</tr>
<tr>
<td>Authentication Agent Settings</td>
<td>Generate encryption keys required for remote authentication agents.</td>
</tr>
<tr>
<td>LDAP Sync Agent Settings</td>
<td>Confirm or clear LDAP Sync Agent settings.</td>
</tr>
<tr>
<td>ICE Activation</td>
<td>Activate ICE License</td>
</tr>
<tr>
<td>LDAP Sync Agent Hosts</td>
<td>List of all remote host names/ips of servers syncing to SafeNet Authentication Service</td>
</tr>
<tr>
<td>Logging Agent</td>
<td>List of all logging Agents</td>
</tr>
<tr>
<td>Migrate SafeNet Authentication Servers</td>
<td>Settings in this section will allow the server to migrate users and tokens from other SafeNet Authentication Servers.</td>
</tr>
<tr>
<td>Block RADIUS Authentication Without Attributes</td>
<td>Enable this session to block the RADIUS authentication if no RADIUS return attribute is defined for the user or group.</td>
</tr>
</tbody>
</table>

In this module:

> **Pre-Authentication Rules**—Determines the conditions that must be satisfied before a user is allowed to authenticate.

> **Authentication Agent Settings**—Generates a unique encryption file used by agents to authenticate against the Virtual Server.

> **Remote Service Settings**—Generates a unique encryption file to be used by Remote Services against the Virtual Server.

> **NOTE** Remote Service Settings is available only on SAS SPE/PCE.

> **LDAP Sync Agent Settings**—Generates a unique encryption file to be used by the LDAP Sync Agent to synchronize LDAP/AD user sources with the Virtual Server.

> **ICE Activation**—Activates ICE capacity allowing MP-1 ICE tokens and capacity to be used to accommodate a short term requirement to increase the number of users that can authenticate against the system.

> **LDAP Sync Agent Hosts**—Use this function to add allowed LDAP sync agents to the virtual server by name and source IP address.

> **Logging Agent**—Use this function to add logging agents by name and source IP address.

> **Migrate SafeNet Authentication Servers**—Use this function to allow the server to migrate users and tokens from other SafeNet authentication servers (such as SafeWord and CryptoServer). For more information, refer to the SafeWord to SafeNet Authentication Service Migration Guide.

> **Block RADIUS Authentication Without Attribute**—Use this function to block the RADIUS authentication if no RADIUS return attribute is defined for the user or group.
Pre-Authentication Rules

Just because a user is able to provide a valid one-time passcode does not necessarily mean that they should be granted access to the network. Other conditions—such as network access point, group membership, account status, and other attributes—might be important in allowing or denying access.

Note that to authenticate against an LDAP user source, a direct LDAP connection must be used from SAS. LDAP authentication is not supported through the Sync Agent.

Security Administrators can use Pre-authentication Rules to apply additional conditions that must be met for authentication to succeed.

The key advantages of Pre-authentication Rules are:

- Rules can be applied to LDAP/Active Directory user account attributes.
- Rules can be applied to user accounts maintained in the internal SQL user data source.
- Rules can be applied based on network access points (source IP, Agent).
- Rules can be used to modify the authentication sequence (OTP, LDAP, LDAP + OTP).
- Changes to user attributes made in LDAP or the internal user data source are immediately effective on SafeNet Authentication Service.
- Rules can have a fixed day of week, start and/or stop date, and/or start and/or stop time; a useful feature for transitioning from static passwords to OTP authentication.

There are few limitations to how Pre-authentication Rules can be used. Rules can be relatively simple, checking a single attribute such as time of day restrictions, or they can be complex, checking multiple attributes such as group membership, network access point and token state.

The authentication proceeds in the following sequence:

- UserID is validated. If valid:
  - Pre-authentication rules are applied. If any rule is satisfied:
    - Password is validated. If valid, access is granted.

The key concepts to consider when creating rules are:

- Multiple rules may be configured, however a user’s attributes need only satisfy one rule for authentication to proceed.
- Initially, SAS is configured with an **Allow All** rule. Pre-Authentication Rules must be enabled to provide the restrictions.

Configure Pre-Authentication Rules

Begin by clicking the **Pre-authentication Rules** link, and then the **New Rule** button. Enter a name and description for the rule, and then select a filter from the drop-down list. Possible filters include:

- Agent is
- Date Restrictions
- Day of week restrictions
- IP
- LDAP/AD Password Validation (prior to SAS v3.5.1, this was named **LDAP password pass-through**)
- Time of day restrictions
User is a member of

Select the Enable Pre-Auth Rules check box enables the enforcement of pre-authentication rules. This allows an administrator to spend time creating the rules, and when ready, this feature can be enabled, and the rules will become enforced. If the feature is enabled and there are no pre-authentication rules defined, then all authentications will be blocked/fail.

**Figure 2: COMMS > Authentication Processing > Pre-authentication Rules**

<table>
<thead>
<tr>
<th>Filter: Agent is</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication API</td>
<td>Required to allow authentication from 3rd party applications that added authentication using the SafeNet Authentication Service Authentication API.</td>
</tr>
<tr>
<td>Citrix</td>
<td>Required to allow authentication via the SafeNet Authentication Service Agent for Citrix Web Interface.</td>
</tr>
<tr>
<td>Console</td>
<td>Required to allow remote management connections to SafeNet Authentication Service server</td>
</tr>
<tr>
<td>IAS</td>
<td>Required to allow authentication via the SafeNet Authentication Service Agent for IAS / NPS</td>
</tr>
<tr>
<td>IIS</td>
<td>Required to allow authentication via the SafeNet Authentication Service Agent for IIS</td>
</tr>
<tr>
<td>Filter: Agent is</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Remote Management API</td>
<td>Required to allow the Command Line Interface (CLI) to connect to SafeNet Authentication Service server.</td>
</tr>
<tr>
<td>Juniper / Funk SBR</td>
<td>Required to allow authentication via the SafeNet Authentication Service Agent for Juniper/Funk Steel Belted RADIUS</td>
</tr>
<tr>
<td>Windows Logon</td>
<td>Required to allow authentication via the SafeNet Authentication Service Agent for Windows Domain Logon.</td>
</tr>
</tbody>
</table>

**Date Restrictions**

This filter is used to limit the lifetime of a rule. This rule is always used in conjunction with another filter. For example, it could be used with the “LDAP/AD Password Validation” filter to facilitate migration from LDAP passwords to token authentication, whereby LDAP passwords would be valid against SafeNet Authentication Service until the rule expires or a token is activated.

<table>
<thead>
<tr>
<th>Filter: Date Restrictions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Begin this rule on</td>
<td>If enabled, the rule will not be active until the indicated date. If disabled, the rule is immediately effective.</td>
</tr>
<tr>
<td>Expire this rule on</td>
<td>If enabled, the rule will stop being enforced on this date. If disabled, the rule will remain active.</td>
</tr>
</tbody>
</table>

**Day of Week Restrictions**

If enabled, SafeNet Authentication Service will process authentication requests only on the selected days of the week. Unlike the Access Restrictions module on the **ASSIGNMENT** tab, this rule can be used to enforce restrictions on groups or destinations.

<table>
<thead>
<tr>
<th>Filter: Day of week restrictions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day of week</td>
<td>If enabled, the rule will be enforced on the selected days of the week.</td>
</tr>
</tbody>
</table>

**IP**

If enabled, SafeNet Authentication Service will not process authentication requests from NAS devices such as VPNs and firewalls that have an IP address outside of the defined range. This filter is usually used in conjunction with another filter. For example, if combined with a group membership attribute, only members of a specific group could authenticate at a NAS device in the IP range. Conversely, in the absence of any other contravening rule, members of the group would not be able to authenticate at a NAS device not in the IP range. This filter supports IPv4 and IPv6 addressing.

<table>
<thead>
<tr>
<th>Filter: IP</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is equal to</td>
<td>Specifies a single valid IP address</td>
</tr>
<tr>
<td>Is in the range</td>
<td>Specifies an IP address range</td>
</tr>
<tr>
<td>Is in mask</td>
<td>Specifies an IP address range using a mask</td>
</tr>
</tbody>
</table>
**LDAP/AD Password Validation**

This filter determines when SafeNet Authentication Service should validate a password or pass it through to LDAP for validation. It also determines how SafeNet Authentication Service will handle LDAP authentications that fail.

![NOTE] This function is available with SAS PCE/SPE with a direct LDAP connection, or, it is available with SAS Cloud, through Active Directory password synchronization (this requires SAS v3.5.1 or later).

![NOTE] MSCHAPv2 authentication protocol is not supported for LDAP/AD passwords.

The primary purpose of this filter is transparent migration of users from static passwords to token authentication. For users that meet the conditions, authentication will “pass through” SafeNet Authentication Service to LDAP or use the synchronized Active Directory password for validation. This filter also determines the action to be taken by SafeNet Authentication Service after LDAP authentication. This filter is often combined with Date Restrictions and Agent or IP attributes.

For example, enabling **LDAP/AD Password Validation** if a user has no token or temporary password would mean that any user with a token must use it to authenticate while those without could continue to use their LDAP password until they received or enrolled their token or until the Date restriction disabled this attribute.

<table>
<thead>
<tr>
<th>Filter: LDAP/AD Password Validation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>All passwords will be passed to LDAP for validation/verified against the AD hash.</td>
</tr>
<tr>
<td>When user has no SafeNet Authentication Service token/password</td>
<td>Passwords will be passed to LDAP for validation/verified against the AD hash only if the user <em>does not have</em> a token in the Active, Suspended, or Locked state, or a SAS temporary password.</td>
</tr>
<tr>
<td>When user has an active SafeNet Authentication Service token/password</td>
<td>Passwords will be passed to LDAP for validation/verified against the AD hash only if the user <em>has</em> a token in the Active, Suspended or Locked state or SAS temporary password</td>
</tr>
<tr>
<td>If LDAP authentication fails, reject the authentication</td>
<td>Access is denied if LDAP authentication fails.</td>
</tr>
<tr>
<td>If LDAP authentication fails, forward request back to SafeNet Authentication Service</td>
<td>SafeNet Authentication Service attempts to validate the password.</td>
</tr>
<tr>
<td>If LDAP authentication succeeds, the user is authenticated</td>
<td>SafeNet Authentication Service grants access based on the AD password alone.</td>
</tr>
<tr>
<td>If LDAP authentication succeeds, force challenge response</td>
<td>SafeNet Authentication Service challenges the user to authenticate with their SAS token/password</td>
</tr>
</tbody>
</table>
**Time of Day Restrictions**

If enabled, SafeNet Authentication Service will process authentication requests only within the selected time range. Unlike the Access Restrictions module on the ASSIGNMENT tab, this rule can be used to enforce restrictions on groups or destinations.

<table>
<thead>
<tr>
<th>Filter: Time of day restrictions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start time</td>
<td>If enabled, the rule will not be active until the indicated time. If disabled, the rule is immediately effective.</td>
</tr>
<tr>
<td>End time</td>
<td>If enabled, the rule will stop being enforced at this time. If disabled, the rule will remain active.</td>
</tr>
</tbody>
</table>

**User is a member of**

This filter is used to require group membership for authentication to proceed. It is normally used in conjunction with Agent or IP filters so that a user must be a member of a specified LDAP group when authenticating at the defined agent or IP address.

This filter does not require group membership to be configured in SafeNet Authentication Service. Users LDAP group memberships can be checked with each authentication. This means that group memberships can manage from LDAP. Use “*” as a wildcard to filter available groups.

<table>
<thead>
<tr>
<th>Filter: User is a member of</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User is a member of</td>
<td>User must be a member of the specified group in the list. To create a list, separate LDAP group names with a semi-colon “;”</td>
</tr>
</tbody>
</table>

**Authentication Agent Settings**

SafeNet Authentication Service agents send authentication requests to the Virtual Server. Security sensitive data sent between the server and agents is protected by AES 256 encryption. To encrypt the traffic and to prevent unauthorized agents, the Virtual Server requires that each agent use an identical encryption key file.

A default encryption key file is automatically created by the Virtual Server.

The default encryption key files are provided to ease initial setup. For best security practices, it is recommended to replace all default agent encryption key files with newly created ones.

To create an Agent Key File, click the Authentication Agent Settings link, and then click the Create button.
Download the newly created key file and use it when prompted during configuration of any SafeNet Authentication Service agent that will authenticate against the Virtual Server. For information about individual agents and configuration, go to www.safenet-inc.com.

**NOTE** By design, when a new key is created in SAS (for the encryption of communication between SAS and an authentication agent), the old key becomes invalid.

**Remote Service Settings**

**NOTE** Remote Service Settings is available only on SAS SPE/PCE.

Remote Service allows command line clients to send management instructions to the Virtual Server. Security sensitive data sent between the server and agents is protected by AES 256 encryption. To encrypt the traffic and to prevent unauthorized command line clients, the Virtual Server requires that each client use an identical encryption key file.

A default encryption key file is automatically created by the Virtual Server.

For optimum security a new encryption key file should be created and used to replace all default Remote Service key files.

To create a Remote Service Key File, begin by clicking the Remote Service Settings hyperlink, and then clicking the Create button.

**Figure 4: COMMS > Authentication Processing > Remote Service Settings > Create**

Download the newly created key file and use it when prompted during configuration of any SafeNet Authentication Service agent that will authenticate against the Virtual Server.

**LDAP Sync Agent Settings**

The LDAP Sync Agent Settings generates an encryption key file that is required by the LDAP Sync Agent to encrypt data transmitted between the sync agent and the Virtual Server. This section also includes settings that determine how the Virtual Server handles Operator accounts under certain conditions described below.

Begin by clicking the LDAP Sync Agent Settings hyperlink, enable/disable the options, then download the Sync Agent key file and install with your LDAP Sync Agent.
> **Persist Operators Against Sync**—By default, synchronized user accounts are removed from the Virtual Server when removed from a synchronized group in your external data source (LDAP/AD). If this option is unchecked, users that have been promoted to Operator will also be removed. Checking this option ensures that unintended changes to the LDAP account do not prevent the Operator from logging into the Virtual Server management UI. If checked, Operator accounts must be manually removed.

> **Use Delayed Sync Removal**—By default, this option delays the removal of synchronized LDAP user accounts flagged for deletion from the SAS Virtual Server for 24 hours. Conversely, if this option is disabled, accounts deleted in the LDAP directory are removed immediately and permanently from the SAS user database upon synchronization, along with all user/token associations.

When this option is enabled, it provides a “safety net” that protects against accidental or erroneous deletions, and saves the time and effort of re-establishing valid user accounts. The deleted user accounts will be marked as “disabled” during the 24-hour period, and these users will not be able to authenticate. However, Operators will have the ability to either re-enable the account or expedite the deletion manually if they are certain the removal is valid.

When used in conjunction with this option, enabling sync notifications provides the Operators with the opportunity to review synchronization activities and determine the validity of user account changes and deletions. (Refer to "Alert Management" on page 118.) If a sync event is detected, the Virtual Server will send an alert to Operators indicating that all detected changes will occur in 24 hours unless they intervene.

**ICE Activation**

This option is available only if an ICE (In Case of Emergency) capacity has been allocated to the Virtual Server. ICE is used to temporarily increase the Virtual Server capacity and quantity of MP-1 tokens and therefore the number of users that can authenticate against the Virtual Server in response to an extraordinary situation or event.

**WARNING** MP-1 tokens are deprecated. Please refer to the End-of-Sale announcement for full details.
All ICE licenses are valid for 30 days from activation and can be activated one time only. Once activated, the license will persist for 30 days or until overwritten by a new ICE license. Unused time or capacity is not retained.

Users that have been provisioned with ICE MP-1 tokens will be able to self-enroll at any time prior to activation or after activation of the ICE license. However, on expiration of ICE, they will not be able to authenticate. Note that their ICE tokens remain valid for use if a subsequent ICE license is activated.

To activate an ICE license, click the **ICE Activation** link, and then click the **Activate** button.

### LDAP Sync Agent Hosts

This lists all LDAP sync agents that are allowed to synchronize with this virtual server.

**Figure 7: COMMS > Authentication Processing > LDAP Sync Agent Hosts**

Click **Add** to create a new entry in the table, and then enter the name of the remote agent and its source IP address. The sync agent can send LDAP changes when **Sync Permissions** are set to **Allowed**. Use the following links:

- **Sync Permissions**—Toggle between Allowed and Denied.
- **Remove**—Remove a sync agent from the list.

### View Sync History

View synchronization activity. On this report, the **Processed Groups** column displays the number of changed groups that were processed during the sync batch. The **Processed Users** column displays only the number of users in this batch sent to be synced since the last successful sync. Each synchronization batch contains up to 500 attributes. How many users fit into a batch depends on how many attributes are configured for syncing.

### Logging Agent

This function lists all logging agents for the selected virtual server. The IP address and port information for each agent is displayed, providing convenient access to information required for firewall configuration between the Logging Agent and the SAS server.
Figure 8: COMMS > Authentication Processing > Logging Agents

Click **Add** to create a new entry in the table, enter the logging agent address, and then click **Apply**. Click **Download** to download and save the logging agent configuration file (*LoggingAgentConfigFile.bmc*), and then manually load it in the client. The logging agent can receive logging information from the server when Permissions are set to Allowed.

- **Permitted**—Toggles between **Allowed** and **Denied**.
- **Remove**—To remove a logging agent from the list.

Migrate SafeNet Authentication Servers

The settings in this section allow the SAS server to migrate users and tokens from legacy SafeNet products, such as SafeWord and CRYPTOCard.

Figure 9: COMMS > Authentication Processing > Migrate SafeNet Authentication Servers

Settings in this section allow the server to migrate users and tokens from other SafeNet authentication servers. From the **Server** list, select the server you want users and tokens to migrate from.
For CryptoServer 5.32 or CryptoServer 6.4, prerequisites are:

- Ensure that the capacity of the account in SAS supports an equal or greater number of tokens as the CRYPTO-Server license, to ensure that all tokens are imported and activated for all users. If the capacity of this account is too low, the import will not take place for any users, operator, token, or group.

- An existing ODBC data source should be configured in SAS to connect to the corresponding CRYPTO-Server database (i.e., MySQL ODBC data source configured in SAS to connect to a MySQL database on the CRYPTOAdmin server). In SAS, install the ODBC driver required to connect to the 6.x or 5.32 CRYPTO-Server database (MySQL, MS SQL, or Oracle). Configure the ODBC driver to connect to the 6.x or 5.32 CRYPTO-Server database.

If using MySQL, a grant statement must be added to allow a connection from SAS. Add the following SQL statements to the MySQL server used by CRYPTO-Server:

- grant all privileges on ".*" to root@IP_Address_of_SAS identified by 'password';
- grant all privileges on ".*" to root@DNS_Name_of_SAS identified by 'password';
- grant all privileges on ".*" to root@Hostname_of_SAS identified by 'password';
- flush privileges;

- RADIUS attributes and clients from a 6.4 server will not be imported; these must be manually created in the SAS Agent-enabled IAS/NPS or Steel-Belted RADIUS software.

- 6.4 CAP Protocol-enabled agents are not supported in SAS (CRYPTO-Logon, CRYPTO-Web, CAP PAM, and certain Citrix Web Interface agents); they must be updated to SAS Agents.

- CRYPTO-Server software tokens are imported and marked as legacy tokens in the database. Users with old versions of CRYPTOCard Software Tools installed can authenticate against SAS without changing their client-side software. This does not include CRYPTO-Server agents such as CRYPTO-Logon.

- RADIUS attributes and clients from a 6.4 server will not be imported. These must be manually created in the SAS Agent-enabled IAS/NPS or Steel-Belted RADIUS software.

- 6.4 CAP Protocol-enabled agents are not supported in SAS (CRYPTO-Logon, CRYPTO-Web, CAP PAM and certain Citrix Web Interface agents); they must be updated to SAS Agents.

- CRYPTO-Server software tokens are imported and marked as legacy tokens in the database. Users with old versions of CRYPTOCard Software Tools installed can authenticate against SAS without changing their client-side software. This does not include CRYPTO-Server agents such as CRYPTO-Logon.

- If during the migration a duplicate serial number is detected, a new serial number will be assigned to the token, which can then be assigned to the user. This change in the serial number does not affect a migrated user's ability to authenticate against SAS.

- If SAS is configured to use LDAP, tokens are assigned and activated during the migration when it finds a match between the CRYPTOCard server token name and the LDAP user logon name. If a match is not found, the token is imported but placed into inventory. Static-password-enabled users will not be enabled as static password users in SAS.

- KT-1 tokens with a serial number 3120xxxx or earlier and RB-1 tokens with a serial number 2020xxxx or earlier will be migrated into SAS but it might not be possible to reinitialize these tokens. These older tokens may need to be replaced with more recent models due to firmware compatibility issues.

- Serial initializers are not supported in SAS. Serial token initializers must be upgraded to USB token initializers. Installing SAS on an existing 6.x CRYPTO-Server is not recommended due to RADIUS Port conflicts between the CRYPTO-Protocol (CAP and RADIUS) service and IAS/NPS.
Parameters for CryptoServer 5.32 or CryptoServer 6.4 migrations:

- **ODBC Name**—the name of the ODBC data source as configured in the ODBC configuration of the Administrator tools section of the Control Panel. (REQUIRED FOR CryptoServer 5.32 or CryptoServer 6.4)
- **Secret**—(CryptoServer 5.32 only) This is the text contained in the 'ccsecret' file on the 5.32 CRYPTO-Server
- **Oracle**—Forces alternate SQL syntax to migrate from Oracle databases
- **User Name**—Optional user name if the ODBC connection settings do not specify one.
- **Password**—Optional password if the ODBC connection settings do not specify one.

**NOTE** The Add Parameter button can be used to add optional custom ODBC attributes to pass to the ODBC data source if required for them to connect.

SafeWord requirements are as follows:

- A valid license must have been imported.
- An empty account must exist to migrate into with enough capacity for the tokens that will be migrated.

Parameters for SafeWord migration:

- **Ldif file**—The path to the decrypted SafeWord export LDIF to migrate.
- **Database Password**—An optional password that was used to encrypt the contents of the database. This password is 8 to 16 characters long.
- **Sccsigners file**—A required file used to decrypt the ldif database file.
- **User CSV file**—An optional file containing additional user information.

### Block RADIUS Authentication

This setting will allow you to block (and reject) RADIUS authentication if no RADIUS return attribute is defined for the user or group. This feature works only when authenticating through FreeRADIUS agent since RADIUS attributes defined for users and groups are returned to FreeRADIUS agents only.

To block RADIUS authentication:

1. Select **COMMS > Authentication Processing > Block RADIUS** authentication without return attribute.
2. Click **Apply**.

**Figure 10: COMMS > Authentication Processing > Block RADIUS Authentication Without Attributes**
When authenticating with a RADIUS token, SAS also passes RADIUS attributes to the RADIUS client that were received from an external RADIUS server. This is beneficial for authentication requests that may go to a third-party authentication service and then return through SAS. If this feature is applied, authentication request to SAS will check the combined list of attributes (RADIUS token attributes and SAS-defined attributes) to block authentication requests.

Auth Nodes

An Auth Node is any RADIUS client, Agent or application (for example, VPN and web applications such as Outlook Web Access) that will send authentication requests to the Virtual Server. This module displays a list of configured Auth Nodes and allows adding, editing and removal.

Figure 1: COMMS > Auth Nodes

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 by your Service Provider. The Virtual Server will not process authentication requests received from devices or applications that are not in the list.

Configure Auth Nodes

To configure an Auth Node, click the Add button and enter at least the following:

For RADIUS clients such as SSL VPNs:

> Descriptive name of the device in the Auth Node Name field
> IP Address of the RADIUS client
> RADIUS shared secret (this must be identical in both SafeNet Authentication Service and the RADIUS client)

For SafeNet Authentication Service Agents, such as Outlook Web Access:

> Descriptive name of the device in the Auth Node Name field
> IP Address of the Agent
The **Resource Name** field identifies in a push notification which authentication node it relates to, so the user can be sure he is authenticating a valid node. By default, this is the **Auth Node Name**. Unlike **Auth Node Name**, the **Resource Name** does not have to be unique. 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.

**Figure 2: COMMS > Auth Nodes > Edit Auth Node > Auth Nodes**

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, select the option **Exclude from PIN change requests** to prevent a forced PIN change with the non-compliant RADIUS clients.

### Sharing and Realms

Sharing and Realms is an optional service feature that allows an Auth Node to be shared with two or more organizations or Virtual Servers. Essentially, a Realm is a group of Virtual Servers. For example, Org 1 manages a Web Application and its own users for authentication. Org 1 wants users from three of its subsidiaries (Org 2, Org 3, Org 4), each with its own Virtual Server, to be able to log into the Web App. In addition, each Org has protected applications to which only its users should have access. Using Sharing and Realms, Org 1 can share the Web App with other Orgs while restricting access to other Auth Nodes to its own users.
To configure, click the **Sharing and Realms** tab, configure as necessary, and then click **Save** to commit the configuration.

**Figure 4: COMMS > Auth Nodes > Edit Auth Node > Sharing & Realms**

- **Allow account lookup based on user name**—The submitted UserID will be used to authenticate the user. The Virtual Server will search the **Shared Auth Node** list in descending order. The first matching UserID will be used to authenticate the user. Use the up/down arrows to move a selected realm up or down in the priority list. Effectively, this means that all UserIDs must be unique across all Realms.
> **Enable Realms**—Use this option where UserIDs may not be unique across all realms. If enabled, additional UserID information will be used to determine to which realm the user belongs. Typically, the UserID will be an email address. Use this feature in conjunction with the **Selected Account** and **Realm Identifier** options. See “Sharing and Realms” on page 163 for additional information.

> **Strip Realm from UserID**—Strips all data starting with the delimiter character from the UserID. This allows a submitted UserID, such as an email address (UserID@myco.com), to be authenticated as UserID.

> **Delimiter Instance**— Specifies where to split up when multiple delimiter characters are present. Uses the first instance of the delimiter (left to right) or the last instance of the delimiter (right to left). In the example `user@realm1@realm2`:

  - Split at First delimiter instance: `user | realm1@realm2`
  - Split at Last delimiter instance: `user@realm1 | realm2`

> **Realm First**—Specifies which part of the string is the realm versus the userID, after splitting at the delimiter character. In the `DOMAIN\user` example, the delimiter character is \. When Realm First is enabled, `user` is sent, and when Realm First is disabled `DOMAIN` is sent.

An account’s Auth Node can be shared with an External User Account Manager only if it is within the External User account’s scope.

### SAML Service Providers

SAML Service Providers (for example, Google Apps, Salesforce, Box.net) can rely on SafeNet Authentication Service for authentication. Use this module to add Service Providers to the Virtual Server. For configuration examples using popular cloud applications, refer to the separate document *SAML Authentication Quick Start Guide*. 
Figure 1: COMMS > SAML Service Providers > SAML 2.0 Settings > Add (Part 1)

The remaining fields (Return Attributes and Custom Login UI) that display in the Add/Edit SAML 2.0 Setting section continue on the next page.
The information displayed in the **SAML 2.0 Settings** section will be required by your Service Provider.

To insert a service provider into the list:

1. Click **Add**.
2. Complete the following fields:
   - **Service Provider Name**—The name you assign to the Relying Party for easy identification. This is used for administration purposes and must be unique within a virtual server. This name displays in
SAML Services lists under **ASSIGNMENT > SAML Services** and under **POLICY > Automation Policies > SAML Provisioning Rules**.

- **Resource Name**—(Push OTP is not available with SAS PCE/SPE) Push notifications include the SAML service where a push was initiated. To ensure users easily recognize the source of the push notification, this field enables Operators to customize the SAML service name that displays. This field defaults to the **SAML Service Provider Name** after the SAS upgrade, and when a new SAML service is added.
- This name is included in the Push notification instead of the Auth Node Resource Name.
- **SAML 2.0 Metadata**

**Upload Existing Metadata File**—An XML file that is generated by your SAML Service Provider.

**Create New Metadata File**—Some SAML Service Providers do not provide a metadata file, but instead provide only their Entity ID and location (essentially the resource being accessed). Use this option to have the virtual server create and add a metadata file based on this information.

![NOTE](image)

When a SAML metadata file is provided, SAS will validate the Location URL in the metadata file. If the server cannot reach the URL, a warning message will be displayed, which provides the user with the option to either continue with the current file, or cancel the action.

If the user clicks Continue, the upload will continue with the current file, and the SAML configuration will be added.

If the user clicks Cancel, the SAML panel will close, and the SAML configuration will not be added.

- **Entity ID**—The Relying Party ID of the SAML Service Provider, typically in the form of a URL. This value will be provided by the SAML Service Provider or can be extracted from the metadata (XML file) provided by the SAML Service Provider.

  For example:
  ```xml
  <?xml version="1.0" encoding="UTF-8"?>
  <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  entityID=https://mycompany.salesforce.com
  ```

- **Enable Enhanced User Login**—The check box that controls whether Enhanced User Login or Classic User Login displays.

- **Return Attributes**—(not available with SAS PCE/SPE) Return attributes are used to enable SAML applications to integrate with SAS and to authorize the user based on the attribute values. Operators must define all SAML return attributes for their SAML services in SAS. Note that after a SAS upgrade (to SAS v3.5.1 or later), any existing SAML service providers will automatically be configured to their existing behavior. Attributes that are not needed can be deleted.

![NOTE](image)

For newly created SAML services, the SAS Operator must add all required attributes. There are no default attributes. The agent will not send attributes that are not added.
To add a return attribute:

1. Click **Add attribute**.
2. Define the **Name** for the attribute.
3. Select the attribute type from the **Value** menu.
4. (If a custom value is needed) Select **Custom** from the **Value** menu and type the value.

To delete a return attribute, click **X** adjacent to the attribute.

The most commonly used return attributes are:

- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
- http://schemas.xmlsoap.org/claims/EmailAddress
- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
- http://schemas.xmlsoap.org/claims/givenname
- http://schemas.xmlsoap.org/claims/.CommonName
- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier
- principal

The options in the **Custom Login UI** section are used to customize the appearance of the login page.

- **Logo**—The image that displays as the logo on the login form.
- **CSS**—Modify the CSS and then upload it to customize the appearance of the page. For more information, see "CSS Customization" on page 175.

**NOTE** Some of the following fields include recommended line lengths. Do not exceed the recommended length to ensure that the text is displayed correctly.

- **Background Image**—(available with SAS Cloud - Enhanced User Login only) The image that displays as the background on the login form.
- **Button Image**—(available with SAS Cloud - Classic User Login only) The image that displays as the login button on the login form.
- **Page Title**—The title displayed on the browser tab.
- **Icon**—The icon displayed on the browser tab.
- **Enable Push/Manual OTP Selector**—(not available with SAS PCE/SPE) The check box that controls whether the Push OTP or Manual OTP option displays on the SAML login page.
> **Push/Manual OTP Selector Text**—(not available with SAS PCE/SPE) This field displays if the Enable Push/Manual OTP Selector check box is selected. This is the "I want to:" text to display on the SAML Login page. Recommended length: 20 characters

> **Push OTP Button Text**—(not available with SAS PCE/SPE) This field displays if the Enable Push/Manual OTP Selector check box is selected. This is the text to display for the option to use Push OTP. Recommended length: 29 characters

> **Manual OTP Button Text**—(not available with SAS PCE/SPE) This field displays if the Enable Push/Manual OTP Selector check box is selected. This is the text to display for the option to use a manual OTP. Recommended length: 29 characters

> **Push OTP Processing Text**—(not available with SAS PCE/SPE) This is the text to display when a Push OTP request is processing and waiting for a response from the user. Recommended length: 30 characters

> **Push OTP Cancellation Text**—(not available with SAS PCE/SPE) This is the text to display on the button that is used to cancel a Push OTP request. Recommended length: 40 characters

> **Push OTP Cancellation Link**—(not available with SAS PCE/SPE) This is the text to display when a Push OTP request is cancelling. Recommended length: 10 characters

> **Push OTP Authenticating Text**—(not available with SAS PCE/SPE) This is the text to display when a Push OTP request is authenticating. Recommended length: 22 characters

> **Login Header Text**—This field is no longer used.

> **Login Button Text**—This is the text displayed on the logon button. Recommended length: 10 characters

> **Login Message**—This field is no longer used.

> **Username Text**—This is the label for the user name field. Recommended length: 20 characters

> **Password Text**—This is the label for the password field. Recommended length: 20 characters

> **Remember Me Text**—(available with SAS Cloud - Enhanced User Login only) The label for the Remember me on this device field. Recommended length: 35 characters or less. This parameter is used only when Enhanced User Login is set to ON.

> **Remember Me Help Text**—(available with SAS Cloud - Enhanced User Login only) The text displayed after the Help icon (next to the Remember me on this device check box) is clicked. Recommended length: 80 characters or less. This parameter is used only when Enhanced User Login is set to ON.

> **Forget Me Text**—(available with SAS Cloud - Enhanced User Login only) The label for the Forget Me on this Device field. Recommended length: 40 characters or less. This parameter is used only when Enhanced User Login is set to ON.
> **SIGN-IN Text**—(available with SAS Cloud - Enhanced User Login only) The text that displays at the top of the authentication dialog box next to the application name (Resource Name). Recommended length: 24 characters or less. This parameter is used only when Enhanced User Login is set to ON.

> **SIGN-OUT Text**—(available with SAS Cloud - Enhanced User Login only) The text that displays upon signing out. Recommended length: 24 characters or less. This parameter is used only when Enhanced User Login is set to ON.

> **OR Text**—(available with SAS Cloud - Enhanced User Login only) The text that displays in between the Push OTP progress message and the manual Passcode field prompt – the default is the conjunction “or”. Recommended length: 20 characters or less. This parameter is used only when Enhanced User Login is set to ON.

### Enhanced User Login

Enhanced User Login (available with SAS Cloud v3.5.3 and later, but not with SAS PCE/SPE) improves the user experience relative to the Classic User Login for SAML authentications in the following ways:

> The user provides their User Name only; after which SAS prompts them for additional credentials.

> SAS initiates the appropriate challenge (Push, SMS or GrIDsure) for a user whom is remembered from previous successful authentication(s) on the same device + browser combination.

> SAS pre-populates the User Name field for users whom choose to be remembered from previous successful authentication(s) on the same device + browser combination.

> SAS displays the name of the requested application during login.

> SAS displays the User Name during login.

#### Figure 3: Comparison of Login Pages

<table>
<thead>
<tr>
<th>Enhanced User Login</th>
<th>Classic User Login</th>
<th>SAS PCE</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Enhanced User Login" /></td>
<td><img src="image2.png" alt="Classic User Login" /></td>
<td><img src="image3.png" alt="SAS PCE" /></td>
</tr>
</tbody>
</table>

### Activate the Enhanced User Login

To activate the Enhanced User Login feature for a SAML Service Provider:

1. Login to the SAS console.
2. Select the account that you are managing from “List Accounts” in the Shortcuts column.
3. Navigate to **COMMS > SAML Service Providers > SAML 2.0 Settings**.
4. Click **Add** to create a SAML Service Provider
   or
   Select a SAML Service Provider from the Service Provider Name table (if present).

5. Select the **Enable Enhanced User Login** check box.

**Switch Between Login Types**
You can enable/disable Enhanced User Login individually for each SAML SP so as to roll out the feature only after users are trained and your feature customizations are completed.

For SAML Service Providers configured prior to the introduction of the Enhanced User Login feature, the feature is OFF by default and the Classic User Login experience displays.

For SAML Service Providers configured after the introduction of the Enhanced User Login feature, the feature is ON by default and the Enhanced User Login experience displays. If the feature is thereafter set to OFF, the Classic User Login experience displays.

**Remember me on this Device**
The **Remember me on this device** function enables users to login to a specific device (for example, desktop PC, tablet, or mobile phone) + browser (for example, Chrome, Internet Explorer, or Safari) combination multiple times without typing their user ID (that is, SAS pre-populates the User Name field) if they have previously logged in to the specific device + browser combination. This function also enables SAS to recognize users so that in later authentications it can, under certain conditions, automatically initiate a Push, GrIDsure or SMS challenge.

**Figure 4: SAML Login - Remember Me on this Device**

SAS will not pre-populate the User Name field or recognize the user if the user attempts to login:

> To a device other than that which they used when **Remember me on this device** was last selected.

> Using a browser other than that which they used when **Remember me on this device** was last selected.

See ""If the User Chooses to be Remembered" below" for further details.

**If the User Chooses to be Remembered**
If the user selected **Remember me on this device** and successfully authenticated on the device + browser combination that they are currently using; then, in response to a login request from the user, SAS sends a Push, SMS or GrIDsure challenge appropriate to the user’s token type whenever all of the following conditions
apply:

1. **Enable Enhanced User Login** is selected.
2. The user has not selected **Forget me on this device** since last selecting **Remember me on this device**.
3. The user is provisioned with one type of token only (for example, MobilePASS+ with Push enabled, SMS or GrIDsure).

**Customize the Remember Me Text**
You can customize the “Remember me on this device” text that displays on the login page next to the check-box that enables a user to select whether they want to be remembered on the device + browser combination that they are currently using.

1. Navigate to **COMMS > SAML Service Providers > SAML 2.0 Settings**.
2. Type a customized message in the **Remember Me Text** field.

*Figure 5: Remember Me Text Field*

**Customize the Remember me Help Text**
You can customize the text that displays on the login page when a user clicks on the question mark icon next to the “Remember me on this device” option.

1. Navigate to **COMMS > SAML Service Providers > SAML 2.0 Settings**.
2. Type a customized message in the **Remember Me Help Text** field.

*Figure 6: Remember Me Help Text Field*

**Forget me on this Device**
The **Forget me on this device** function enables users to be forgotten on the device + browser combination that they are currently using - in the context of SAML authentication; not just for the current login attempt but for all login attempts until they select “Remember me on this device”.
Figure 7: SAML Login - Forget Me on this Device

![SAML Login Interface](image)

After selecting **Remember me on this device** (whereby the User Name field is pre-populated), a user can choose to be prompted for their User Name (i.e., type their User Name) on subsequent logins, by selecting **Forget me on this device**.

**Customize the Forget Me Text**
You can customize the “Forget me on this device” text that displays on the login page as a link that enables the user to be forgotten for the device + browser combination that they are currently using.

1. Navigate to **COMMS > SAML Service Providers > SAML 2.0 Settings**.
2. Type a customized message in the **Forget Me Text** field.

Figure 8: Forget Me Text Field

![Forget Me Text Field](image)

**Display Enhancements**
To add context to the authentication process, the following information displays on the login page:

- The name of the requested application (at the top of the authentication dialog box).
- The User Name of the authenticating user.

The name that SAS displays for the requested application is configured using **COMMS > SAML Service Providers > SAML 2.0 Settings > Resource Name** for each SAML Service Provider.
Figure 9: SAML Service Providers > SAML 2.0 Settings

Add SAML 2.0 Setting:
[Apply] [Cancel]

SERVICE PROVIDER CONFIGURATION

Service Provider Name: 
Resource Name: 

Login Page Customization
The Enhanced User Login for SAML feature introduces the following User Interface (UI) elements:

> Background Image
> Remember Me Text
> Remember Me Help Text
> Forget Me Text
> SIGN-IN Text
> SIGN-OUT Text
> OR Text

In the case of a SAML Service Provider application that was previously configured in SAS with some or all of the text or image fields customized, when Enable Enhanced User Login is selected, the customized values are retained and (where applicable) are applied to the Enhanced User Login experience.

CSS Customization
You can customize both the Enhanced User Login and the Classic User Login user interface by uploading a custom CSS file. To obtain a copy of the default CSS file:

1. Go to http://www2.gemalto.com/sas/implementation-guides.html
2. Click “SafeNet Authentication Service Cloud” to display a list of SAS Cloud documents.
3. Click “CSS for SAML Enhanced User Login” under the heading with the same name.

The bsid.css file displays. The Classic User Login classes are defined within the “Non ID First” section and the Enhanced User Login classes are defined within the “ID First” section.

NOTE Custom CSS files are always applied on top of the default CSS file, as such, classes specified in the custom CSS files will override classes of the same name in the default CSS file.
As you switch from Classic User Login to Enhanced User Login, or vice-versa, by changing the Enable Enhanced User Login setting, a previously uploaded custom CSS file is retained. However, since CSS classes for Enhanced User Login are distinct from CSS classes for Classic User Login, a previously applied custom CSS file created strictly to customize the UI for Classic User Login will have no effect on the User Interface for Enhanced User Login.

Restrictions and Limitations
The Enhanced User Login feature is not compatible with SAS Pre-Authentication rules.

In cases where the Enhanced User Login feature is enabled, if a Virtual Server is configured for Pre-Authentication rules, those rules are ignored in the context of a SAML authentication; but continue to be applied in all other contexts.

Custom Branding
The appearance and branding of the Virtual Server management console, Self-Service, and Enrollment web pages can be customized for colors, fonts, logos, titles, labels, and product name. Refer to the SAS Service Provider Branding Guide for information about customizing these SAS elements.

Figure 1: COMMS > Custom Branding (Operator View)

Figure 2: COMMS > Custom Branding (Account Manager View)
APPENDIX A
Compliance with PCI-DSS

Gemalto’s SafeNet Authentication Service can be leveraged by customers looking to comply with PCI-DSS to provide a strong and reliable authentication method to systems containing or processing card payment data.

Below are highlighted a number of key requirements for PCI-DSS which need to be met to obtain compliance that can be achieved using the SafeNet Authentication Service. However, action is required by an administrator during the simple configuration process to enable the required functionality.

Requirement 8.1.6b

Gemalto recommends the implementation of built-in system policies to protect customer login credentials from brute force attack methods. For customers leveraging SafeNet Authentication Service for use with PCI-DSS compliance, it is recommended that the SAS Server policy be configured for “Account Lockout/Unlock Policy” to enforce that no more than six attempts can be made to access an account with incorrect credentials before that account is disabled. See "Account Lockout/Unlock Policy" on page 90.

Requirement 8.2.3b

Gemalto recommends the use of a PIN in conjunction with a token policy of at least six digits to provide strong multi-factor authentication for your users. When customers look to leverage the SafeNet Authentication Service to comply with PCI DSS, it is recommended that a “Server-Side” PIN be selected for the token and the associated complexity for this PIN be alphanumeric.

For customers looking to not leverage a PIN, we recommend that the token template for your specific token be updated prior to deployment to at minimum a seven character OTP which is alphanumeric in its display. See "Server-side PIN Policy" on page 98 and "Token Templates" on page 94.

Requirement 8.2.4b

Gemalto recommends to never use a static password where a One Time Password (OTP) is available. When leveraging the SafeNet Authentication Service for PCI-DSS compliance customers must implement at least a periodically changing password and notify the user under what circumstances this must be changed (for example, every X days). The simplest way to comply with this action is to leverage an OTP which automatically changes the passcode at every login attempt. It is also recommended that the Temporary Password Policy be configured to force a change of Temporary passwords to maintain compliance for any non-OTP users. See "Temporary Password Policy" on page 100.

Requirement 8.2.5b

Gemalto recommends to never use a static password where a One Time Password (OTP) is available. For customers whom wish to leverage the SafeNet Authentication Service to comply with PCI-DSS, it is recommended that temporary passwords be disabled within the system to enforce an OTP-based
authentication. See “Temporary Password Policy” on page 100.