



SafeNet Authentication Service

CUSTOMER RELEASE NOTES

Version: 3.4 PCE/SPE
Build: 3.4.233.28627
Issue Date: 21 April 2015
Document Part Number: 007-012947-001, Rev. A

Contents

Product Description	3
Release Description.....	3
New Features and Enhancements.....	3
New Features.....	3
French Language Support.....	3
Differential Synchronization.....	5
Sync History Report	5
Sync Host Notification Alert.....	5
Enhancements	6
Support for Syncing LDAP Users from Nested Groups.....	6
Ability to Delete Audit Role Removed	6
Ability to Delete Root Operator Removed	7
Auth Nodes – Enhancements to ‘Strip Realm from UserID’ Function	7
Customizable Sender ID with Clickatell SMS Plug-In.....	8
Logging Server IP Addresses Displayed in SAS Console.....	8
Migrate Third Party Authentication Servers.....	9
SAML 2.0 Settings – Active Hyperlink for Identity Provider Certificate Download	10
Support for BlueCoat, f5, and Palo Alto RADIUS Attributes.....	10
Token Enrollment Enhancements	11
Tooltip to Resolve Truncated List Display Issues.....	11
Auto-Provisioning Updates.....	11
Service Metrics Total Active Users per Month Report.....	12
SAS LDAP Integrator Service	12
Self-Enrollment Support for BlackBerry 10.....	13
Support for MobilePASS 8.4 for Windows RT and MobilePASS 8.4 for Windows Phone 8	13
Provisioning Task Management – Days Before Expiry to Warn.....	14
Resend Token Provisioning Tasks.....	15

Self-Service Base URL Field Length Increased	15
Token Inventory Performance Improvements	15
Limiting FreeRADIUS to Specified TLS Versions.....	15
External RADIUS Attribute Pass-Through.....	15
MS SQL Server Support.....	16
Advisory Notes.....	16
Database Backup before Upgrade	16
Email Notifications.....	16
Resolved and Known Issues.....	17
Resolved Issues.....	17
Known Issues.....	22
Compatibility and Upgrade Information.....	23
Interoperability	23
Supported Tokens.....	23
Supported Mobile Devices	23
Supported Browsers.....	24
Supported Directories.....	24
Upgrade Instructions.....	24
Upgrading the Synchronization Agent.....	24
Product Documentation	25
Support Contacts.....	25

Product Description

SafeNet Authentication Service (SAS) delivers fully automated, authentication management solution, with flexible token options tailored to the unique needs of your organization, substantially reducing the total cost of operation.

Strong authentication is made easy through the flexibility and scalability of SafeNet Authentication Service's automated workflows, vendor-agnostic token integrations, and broad APIs. In addition, management capabilities and processes are fully automated and customizable—providing a seamless and enhanced user experience.

SafeNet Authentication Service enables a quick migration to a multi-tier, multi-tenant cloud environment, protecting everything, from cloud-based and on-premises applications to networks, users, and devices.

Release Description

SafeNet Authentication Service - Version 3.4 PCE/SPE is a major release including new features, enhancements, and fixes.

New Features and Enhancements

New Features

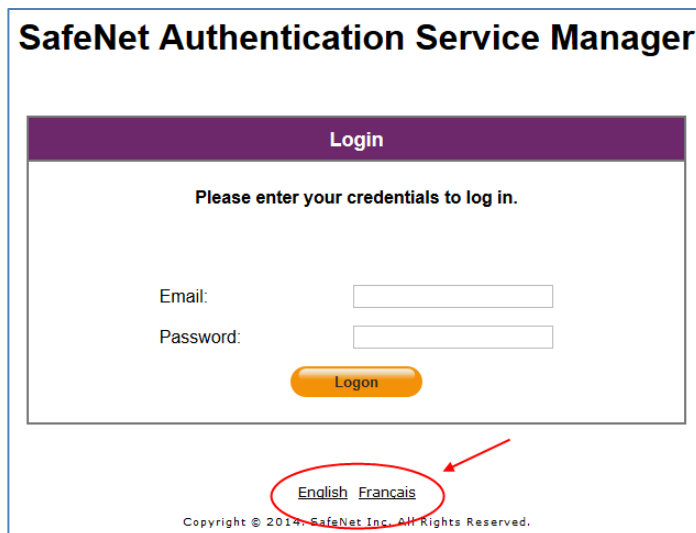
French Language Support

Support for the French language has been added to SAS. This support encompasses both the SAS Management Console and the Self-Service website.

While English is currently the only language available as the default language for the Management Console, Operators can specify their own language preference if desired, which will take effect upon login. If the Operator language is set to French, the API responses will also be in French.

There are two locations in SAS where an Operator can set their language preference:

- **SAS Login page**—Links are provided for **English** and **Français** at the bottom of the SAS **Login** page.



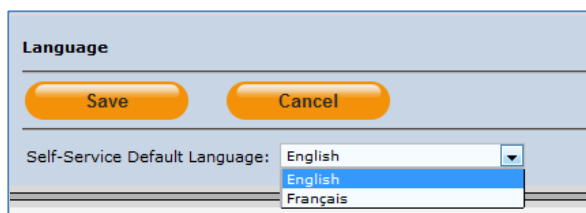
- **SAS Management Console Home page**—On the SAS Management Console **Home** page, a **Language** option is provided at the top of the page. Placing the mouse cursor over the **Language** button will present the options **English** and **Français**, as well as any other language sets that may have been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




NOTE: All text in the user interface will be switched to French, 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.



Setting the default language for the Self-Service site is done under **Virtual Servers > Self-Service > Configuring Self-Service > Language**. To switch to the French language, select **Français** in the **Self-Service Default Language** field, and then click **Save**.



If an Operator wishes to set their own personal language preference for the Self-Service site, they can do so on the **Self-Service Login** page. At the bottom of the page, a text or icon link for languages will be displayed, based on configuration of the Self-Service module (the default links are shown below). To switch to the French language, click the languages link and then select **Français** from the list. All text in the Self-Service site will be converted to French for that user only.

To change the default user language	Languages text link	Languages icon link
Select a link on the Self-Service site home page...	Languages	
...and then select a language	<div style="border: 1px solid black; padding: 5px;"> <p style="color: red; margin: 0;">SELECT A COUNTRY/REGION:</p> <p style="margin: 0;">English Français</p> </div>	

Differential Synchronization

In previous versions of SAS, a full sync of all user records was performed for each and every sync event. With this version, the SAS Synchronization Agent has been enhanced so that only changed user records, including additions and deletions, are synchronized, resulting in less network traffic and reduced sync time. This is referred to as “differential synchronization.” Reduced system load also increases the reliability of synchronization services.

User records are sent in “batches” to the SAS user store. With differential synchronization, the initial sync may take longer to complete as it builds up its local information store, but subsequent syncs typically complete much faster.

Differential syncing occurs in parallel with scanning the user store. This means that new users can typically start using authentication before all users are synchronized. If the agent cannot connect to the server, the sync is retried with the next user store scan. Differential synchronization also re-enables scan intervals less than 60 minutes down to a minimum of 20 minutes, and instant synchronization by stopping and starting the agent.

Sync History Report

In support of differential synchronization, the **Sync History Report** (available through the SAS Management Console) has been updated. The **User’s Total** column heading has been changed to **Processed Users** and the **Group’s Total** column heading has been changed to **Processed Groups**.

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 batch contains up to 40 users or groups.

The **Sync History Report** is viewed in the SAS Management Console by clicking **COMMS > Authentication Processing > LDAP Sync Agent Hosts**. Click the **View Sync History** link. User changes appear in the report incrementally as they occur.

Sync Host Notification Alert

A new alert option called **Sync Host Notification** can now be enabled for SAS operators. When enabled, an alert will be sent via email or SMS indicating that permissions should be edited to allow the SAS server to accept syncs from the Synchronization Agent. This option is configured under **Virtual Servers > Policy > Role Management > Alert Management** and is enabled by default when creating a new Virtual Server. The alert is only sent when a newly added agent attempts to synchronize for the first time.

Enhancements

Support for Syncing LDAP Users from Nested Groups

The SAS Synchronization Agent has been enhanced to allow syncing of LDAP users from nested groups. The agent will sync LDAP users within nested groups, where users may be members of a group that is a member of another group. The nested groups themselves are not synced, and their users do not retain group memberships in SAS by default setting. The **Group Sync Options** setting (see below) allows retention of group membership attributes for users.

SAS syncs users and groups that are visible in LDAP. SAS is not aware of trust relationships in Active Directory.

After the **Synch Groups** list has been created, the option selected below will determine how these groups and users are filtered, and thus added to SAS.

Group Sync Options

The **Group Sync Options** setting determines how groups are synchronized to SAS, and which group memberships users have in SAS. This setting does not affect which users are synchronized. With all options, all users in Synch Groups and any nested groups therein are synchronized.

In the **Groups to sync** field, select one of the following options:

- **Groups with users only**— Groups are synchronized that contain users from any Synch Groups or any nested groups therein. The group memberships for all users are retained.
- **Filter groups only**— Only the group designations contained in the **Synch Groups** list will be synchronized. Users' group memberships are maintained for Synch Groups only. This option is the default setting.
- **None**— Group designations will not be synchronized and thus group memberships will not be maintained. Users from Synch Groups or any nested groups therein will be synced to a single, inclusive SAS users list.



NOTE: In SAS, the **Assignment** tab will display group membership attributes for a user's parent group(s). However, auto-provisioning rules trigger only on "direct" group membership, which means that nested groups require their own auto-provisioning rules. For example, Group A contains Group B as a nested group, and User1 is a user in Group B. The **Assignment** tab will show that User1 is a member of Groups A and B; however, an auto-provisioning rule on Group A does not apply to User1 but an auto-provisioning rule on Group B will apply.



NOTE: SAS syncs all nested groups that are visible in LDAP. SAS is not aware of trust relationships in Active Directory.

Before updating the Synchronization Agent, it is recommended to verify that LDAP groups configured for syncing do not contain nested groups with users you do not intend to sync. After upgrading, all users of nested groups will be synced automatically.

Additional information can be found in the *SafeNet Authentication Service Synchronization Agent Configuration Guide*.

Ability to Delete Audit Role Removed

In previous versions, under **Administration > Account Manager Roles**, a **Remove** link was available for the **Audit** role. This link has been removed as this role should not be deleted.

VIRTUAL SERVERS		ADMINISTRATION	
Account Manager Roles			
Add		Change Log	
Role	Description		
Account Manager	Default - This role cannot be removed or modified and allows access to all Service Provider tabs, module and actions.		
Audit	This role cannot be removed and allows read-only access to all Service Provider tabs, modules, and actions.	Edit	

Ability to Delete Root Operator Removed

In previous versions, under **Virtual Servers > Operators > External Operator**, a **Remove** link was available for the **Root** operator account. This link has been removed as this account should not be deleted.

Auth Nodes – Enhancements to ‘Strip Realm from UserID’ Function

In previous versions, the function to strip realm (domain) prefixes from user IDs did not work consistently. Changes have been implemented to correct those issues.

In support of these updates, a new field called **Realm First** has been added to the **Sharing & Realms** tab under **VIRTUAL SERVERS > COMMS > Auth Nodes**. When this field is enabled, the UserID is accepted as **DOMAIN\user**; when disabled, **user@domain**. In this example, the “\” symbol must be specified in the **Delimiter character** field.

Add Auth Node

Auth Nodes | **Sharing & Realms**

Allow account lookup based on user name
 Enable Realms

Strip Realm from UserID

Delimiter character:
 Delimiter instance:

Realm First:

Customizable Sender ID with Clickatell SMS Plug-In

In previous versions, the Clickatell SMS Plugin did not accept customization of the Sender ID. Any value placed in the **Sender ID** field under **VIRTUAL SERVERS > COMMS > Communications > SMS Settings** was blocked during SMS routing from Clickatell to the carrier. With this release of SAS, an alternate Sender ID may be used as long as the “customization” feature has been purchased from Clickatell. When **Clickatell SMS Plugin** is selected under **SMS Settings**, you will now see a message next to the **Sender ID** field indicating the requirements for this optional functionality, as shown in the image below.

SMS Settings

Apply Cancel

Default Custom

Gateway: Primary SMS gateway provider

SMS Plugin: Clickatell SMS Plugin

UserName:

Password:

SMS URL:

API ID:

Sender ID: Sender ID must be registered with Clickatell before entering it here. SMS messages may not be delivered on mobile networks that don't support Sender ID.

Use Proxy: Yes No

Message Options: None Use Flash SMS Use Overwrite SMS

SMS Mobile Number: Test

Country code followed by number.

Logging Server IP Addresses Displayed in SAS Console

In the **Communications** module, under **COMMS > Communications > Logging Agent Server Settings**, when specifying “custom” server settings, the column labels have been changed for clarity - **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.

Logging Agent Server Settings:

Apply Cancel

Default Custom

"Inbound" is the Logging Agent Server address to which Logging Agents send data to. "Outbound" is the Logging Agent Server address that the agent receives packets from. This information is displayed also under Authentication Processing / Logging Agent task.

	Inbound	Outbound
Primary Host/IP:	<input type="text"/>	<input type="text"/>
Failover Host/IP:	<input type="text"/>	<input type="text"/>
Port:	<input type="text"/>	<input type="text"/>

The IP address and port information is also displayed under **COMMS > Authentication Processing > Logging Agent**, providing convenient access to the information required for firewall configuration between the Logging Agent and the SAS server.

Authentication Processing

Use these settings to configure Context Pre-auth rules, download or generate authentication, remote service and LDAP Sync Agent encryption keys.

Task	Description
Context Evaluation Rules	Set the Context Filters to be evaluated before authentication.
Authentication Agent Settings	Generate encryption keys required for remote authentication agents.
Remote Service Settings	Generate encryption keys required for remote service agents.
LDAP Sync Agent Settings	Confirm or clear LDAP Sync Agent settings.
ICE Activation	Activate ICE License
LDAP Sync Agent Hosts	List of all remote host names/IPs of servers syncing to SafeNet Authentication Service
Logging Agent	List of all logging Agents
Migrate SafeNet Authentication Servers	Settings in this section will allow the server to migrate users and tokens from other SafeNet Authentication Servers.

Logging Agent:

Add Download Cancel

Firewall configuration for Logging Agent to connect with Logging Agent Server:

Source	Destination	IP	Port
Agent	SAS	cloudlog1.safenet-inc.com	8459
Agent	SAS	cloudlog2.safenet-inc.com	8459
SAS	Agent	109.73.120.145	8458
SAS	Agent	69.20.230.196	8458

Remote Host	First Instance	Last Instance	Permitted	
0.0.0.44	13/06/2014 11:20:09 AM	13/06/2014 11:20:09 AM	alllog	Remove

Displaying: 1 to 1 of 1

Migrate Third Party Authentication Servers

The **Task** and **Description** text for the **Migrate Third Party Authentication Servers** function under **VIRTUAL SERVERS > COMMS > Authentication Processing** has been changed as shown below. The new wording accurately reflects the selections in the **Server** list, which are legacy SafeNet products rather than third-party products.

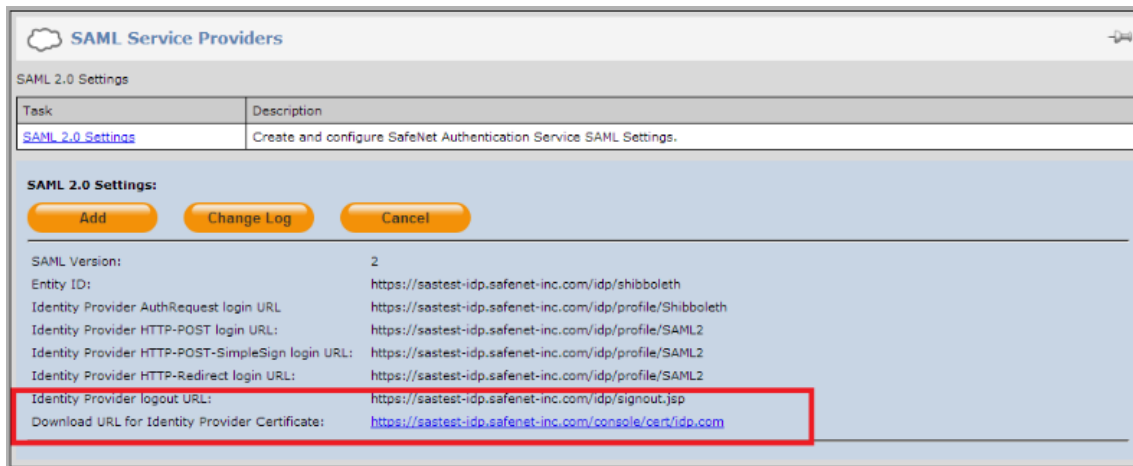
Authentication Processing

Use these settings to configure Context Pre-auth rules, download or generate authentication, remote service and LDAP Sync Agent encryption keys.

Task	Description
Authentication Agent Settings	Generate encryption keys required for remote authentication agents.
LDAP Sync Agent Settings	Confirm or clear LDAP Sync Agent settings.
ICE Activation	Activate ICE License
LDAP Sync Agent Hosts	List of all remote host names/IPs of servers syncing to SafeNet Authentication Service
Agent SSL Certificate	Agent SSL certificate for Domain Validation Agent
Logging Agent	List of all logging Agents
Migrate SafeNet Authentication Servers	Settings in this section will allow the server to migrate users and tokens from other SafeNet Authentication Servers.

SAML 2.0 Settings – Active Hyperlink for Identity Provider Certificate Download

Under **COMMS > SAML Service Providers > SAML 2.0 Settings**, the **Download URL for Identity Provider Certificate** hyperlink is now an active link that will initiate downloading of the certificate. In previous versions, you were required to copy and paste the URL into a browser to initiate the download process.



Support for BlueCoat, f5, and Palo Alto RADIUS Attributes

Under **Virtual Server > Assignment > User > RADIUS Attributes**, SAS now allows the selection of vendor-specific RADIUS attributes for BlueCoat, f5, and Palo Alto, as shown below.

Vendor: BlueCoat
Attribute: Blue-Coat-Authorization
Format: Blue-Coat-Authorization
Value: No-Access

Vendor: f5
Attribute: F5-LTM-Audit-Msg
Format: F5-LTM-Audit-Msg
Value: F5-LTM-User-Console
F5-LTM-User-Context-1
F5-LTM-User-Context-2
F5-LTM-User-Info-1
F5-LTM-User-Info-2
F5-LTM-User-Partition
F5-LTM-User-Role
F5-LTM-User-Role-Universal
F5-LTM-User-Shell

Vendor: PaloAlto
Attribute: PaloAlto-Admin-Access-Domain
Format: PaloAlto-Admin-Access-Domain
Value: PaloAlto-Admin-Role
PaloAlto-Panorama-Admin-Access-Domain
PaloAlto-Panorama-Admin-Role
PaloAlto-User-Group

Token Enrollment Enhancements

The **Configure Self-Enrollment pages** function, under **Virtual Servers > Self Service**, now includes options that allow for customization of the **Software Token** self-enrollment pages presented to the user, as shown in the example below. For example, in an upgrade scenario, where the Software Tools app is already installed, the self-enrollment page can be configured to not include this link and skip to setting a PIN.

Tooltip to Resolve Truncated List Display Issues

In previous versions, list items could not be viewed in their entirety if the value exceeded the display range. To resolve this issue, “tooltip” functionality has been implemented that will display the full name by clicking the list item.

Auto-Provisioning Updates

Auto-Provisioning is implemented as a service in SAS 3.4 PCE/SPE. It manages the creation of provisioning tasks and revocation of previously assigned tokens

SAS 3.4 PCE/SPE resolves a number of longstanding defects with auto-provisioning. This function now works as originally intended - auto-provisioning rules are checked periodically and new provisioning tasks are created for users that match the rule conditions until they enroll a token.

Users will receive new provisioning notification emails after their previous provisioning tasks expire (10 days by default). This stops when they have completed enrollment for the token and as long as the user remains associated with the provisioning rule; typically, this means as long as the user stays in the same group.

Service Metrics Total Active Users per Month Report

The Service Provider report called Service Metrics Total Active Users per Month (Rolling YTD) has been extended. This report provides the total active users by account type on a rolling YTD basis. A new unique account **ID** column can be added and a new filter, **Child Only**, allows inclusion of all or only child accounts. This report is accessed via **ADMINISTRATION > Report and Billing Management > Available Reports**. In the **Report Class** field, select **Service Metrics**.

Customize Report

Finish Cancel

Select and move a username to the Access to Report Enabled field to authorize output.

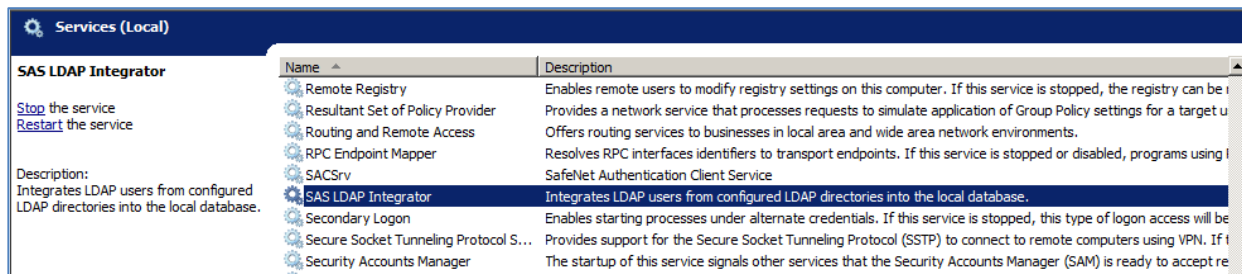
Report:
Name: Service Metrics - Total Active Users per Month (Rolling YTD)
Description: Reports total active users by account type (rolling YTD)

Filters:
Service Type: All
Evaluation: All
Child Only: Child Only

Report Columns:
 Account
 2014-10
 2014-9
 2014-8
 2014-7
 2014-6
 2014-5
 2014-4
 2014-3
 2014-2
 2014-1
 2013-12
 2013-11
 Id

SAS LDAP Integrator Service

LDAP integration is implemented as a service in SAS 3.4 PCE/SPE, replacing the Direct LDAP Integration feature included in earlier releases of SAS PCE/SPE.



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 start-up. It scans LDAP users and groups periodically, updating the SAS database to match the contents of LDAP.

As the information is now stored internally in the SAS database, SAS is no longer required to make connections to LDAP for each authentication demand, resulting in a significant improvement in performance. SAS can now continue operating even when LDAP is disconnected or non-responsive.

To choose your primary LDAP user source, select **COMMS > LDAP > LDAP User Source**, and then enter the **Host Name** (or **IP Address**) and the **Port**.

Self-Enrollment Support for BlackBerry 10

A new section for **MobilePASS BlackBerry 10** has been added to the **MobilePASS** page under **Virtual Servers > Self-Service > Configuring Self-Service > Configure Self-Enrollment Pages**.

The download link directs BlackBerry 10 users to the Android converted app in the BlackBerry World app store. To enroll a token, the user must copy and paste the enrollment code from the self-enrollment page into the app.

Alternatively, MobilePASS for BlackBerry 10 is a native app for deployment through BlackBerry Enterprise Server (BES). It is currently not published in the BlackBerry World app store. If so desired, it is possible to remove the **<DownloadLink />** tag in the **MobilePASS Top Message** section of the self-enrollment page and add full links to the platform-specific client sections.

The MobilePASS client links can be found at <http://www2.safenet-inc.com/sas/getmp.html>.

With the BlackBerry 10 native app, the user can simply click on the auto-enrollment link to enroll the token.

This enhancement also resolves issues for BlackBerry users on pre-OS 10 devices.

For MobilePASS BlackBerry Java app users, clicking on the auto-enrollment link now again opens the app to enroll the token (refer to issue SAS-6316 under "Resolved Issues" on page17).

For details about deploying MobilePASS for BlackBerry, refer to the *MobilePASS for BlackBerry Deployment Guide*.

Configure Self-Enrollment pages

Use this module to configure Self-Enrollment pages.

MobilePASS

MobilePASS Windows:	Once the application has been installed, select the link below to install the token on your device. Enroll your MobilePASS token
MobilePASS Windows RT:	Once the application has been installed, select the link below to install the token on your device. Enroll your MobilePASS token
MobilePASS Windows Phone:	Once the application has been installed, select the link below to install the token on your device. Enroll your MobilePASS token
MobilePASS BlackBerry Java:	Once the application has been installed, select the link below to install the token on your device. Enroll your MobilePASS token
MobilePASS BlackBerry 10:	Once the application has been installed, select the link below to install the token on your device. Enroll your MobilePASS token
MobilePASS Common:	Copy the following string, open the MobilePASS application, select Automatic Enrollment, and then paste (on some platforms, may already be pasted): <code>

<Base64 /></code>

Support for MobilePASS 8.4 for Windows RT and MobilePASS 8.4 for Windows Phone 8

SAS now provides support for MobilePASS 8.4 for Windows RT and MobilePASS 8.4 for Windows Phone 8. Users visiting the self-enrollment page with a Windows RT device will be directed to download the MobilePASS app from the Windows Store. Users visiting the self-enrollment page with a Windows Phone device will be directed to download the MobilePASS app from the Windows Phone Store

Within SAS, you can configure the self-enrollment page for MobilePASS Windows RT as shown below. This function is accessed via **VIRTUAL SERVERS > Self-Service > Configuring Self-Service > Configure Self-Enrollment Pages**.

```
MobilePASS Windows RT:
Once the application has been installed, select
the link below to install the token on your
device.<br><br><a
href="MobilePASS:enrollment=<Base64
/>">Enroll your MobilePASS token</a><p>In
```

Provisioning Task Management – Days Before Expiry to Warn

A new field called **Days Before Expiry to Warn** has been added under **VIRTUAL SERVERS > POLICY > Automation Policies > Self-enrollment Policy**. This field allows a provisioning reminder to be sent via email to the selected 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.

Self-Enrollment Policy

Apply Cancel

Self-Enrollment Base URL:

Activation code format:

Reservation time to live: (0-31) Days (0 = will not expire)

Enrollment lockout after: (1-30) Attempts

Days Before Expiry To Warn: (0-31) Days (0 = will not warn)

A new email message template has also been added called **Enrollment Expiring**, which allows customization of the content of the expiry reminder email sent to the user. This template is accessed via **VIRTUAL SERVERS > COMMS > Communications > Email Messages**. Select **Custom** and then select **Enrollment Expiring** from the **Email Message Type** list.

Customize Email Messages

Apply Cancel

Default Custom

Applying defaults (clicking Default then Apply) resets all messages to those of your parent service provider.

Email Message Type:

Format: Text HTML

Subject:

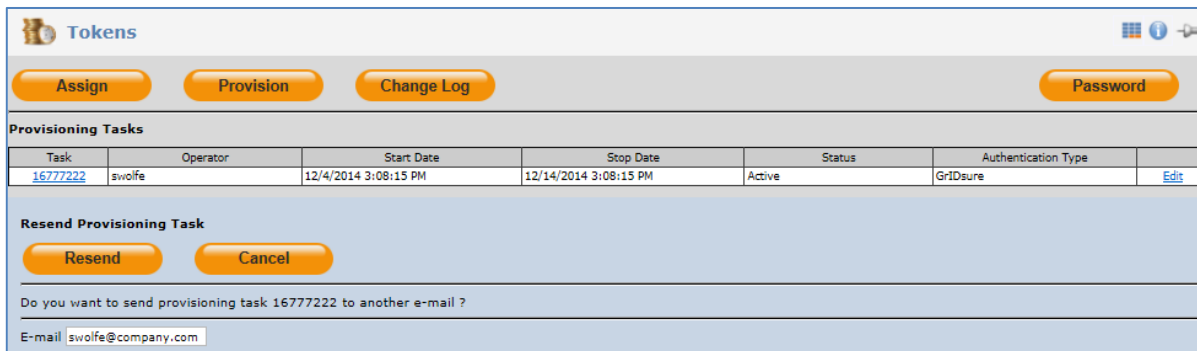
Body:

SMS Content:

Max 160 chars.

Resend Token Provisioning Tasks

SAS now provides the ability for an Operator to resend a provisioning task message to a user. This function is accessed via **Virtual Servers > Assignment > Tokens**. Select the User ID of the user whose provisioning task you want to resend. In the **Tokens** section, under **Provisioning Tasks**, click the **Edit** link for the task, and then click the **Resend** button. By default, the email address saved in the user's SAS profile is automatically entered into the **E-mail** field. An alternate email address can be specified; 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.



The screenshot shows the 'Tokens' management interface. At the top, there are buttons for 'Assign', 'Provision', 'Change Log', and 'Password'. Below this is a table titled 'Provisioning Tasks' with columns for Task, Operator, Start Date, Stop Date, Status, and Authentication Type. A single task is listed with ID 16777222, operator 'swolfe', and status 'Active'. Below the table is a 'Resend Provisioning Task' section with 'Resend' and 'Cancel' buttons. A confirmation dialog asks 'Do you want to send provisioning task 16777222 to another e-mail?' with an 'E-mail' field containing 'swolfe@company.com'.

Task	Operator	Start Date	Stop Date	Status	Authentication Type	
16777222	swolfe	12/4/2014 3:08:15 PM	12/14/2014 3:08:15 PM	Active	Gridsure	Edit

Self-Service Base URL Field Length Increased

The field length for the **Self-Service Base URL** field has been increased from 64 to 128 characters to make it consistent with the **Self-Enrollment Base URL** field.

Token Inventory Performance Improvements

Performance improvements have been made to SAS to determine if certain token types are available in inventory.

Limiting FreeRADIUS to Specified TLS Versions

After installing or upgrading to FreeRADIUS Updater 1.04, a secure TLS-based channel for processing authentication requests to SAS is enforced by default. This is required as a consequence of the reported POODLE vulnerability in SSL.

For more details: <https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566>

External RADIUS Attribute Pass-Through

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



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.

MS SQL Server Support

Microsoft SQL Server 2012 and 2012 R2 are now supported

Advisory Notes

Database Backup before Upgrade



CAUTION: It is strongly recommended to back up the database before upgrading to SAS 3.4 PCE/SPE. Failure to do so could result in serious data loss.

Email Notifications

After upgrading to SAS PCE/SPE 3.4, operators may be receiving additional email notifications. The primary reason is that this release resolves numerous defects.

Most of these emails should be related to one of the following:

Auto-Provisioning Tasks (pending tasks in the system)

Provisioning tasks may be stuck in a pending state for extended periods of time (SAS-4091, SAS-4695). This is now fixed, hence outstanding provisioning tasks will be sent shortly after the upgrade.

Users are receiving provisioning notifications since they are a member of auto-provisioning tasks that are pending and have not been completed by these users.

They will continue to get these provisioning emails every 10 days (by default) until the task has been completed.

There are three ways to resolve this:

- The user completes enrollment.
- The user is removed from the group synchronized to the auto provisioning rule.
- The auto provisioning rule is removed from the system.

External Operator Alerts

External Operators did not always receive the alerts they were configured to receive (SAS-4979). This is now fixed; hence External Operators are receiving notifications for alerts enabled under **Account Manager Role Alert Management**. Operators will continue to receive alerts for the settings enabled.

There are the following ways to resolve this:

- Disable alerts as appropriate under **Account Manager Role Alert Management**.
- Acknowledge the alerts, as these are intended to notify the External Operators for the activity related to their child accounts.

External Operators are receiving notifications for alerts enabled under **Account Manager Role Alert Management**.

Operators will continue to receive alerts for the settings enabled.

There are the following ways to resolve this:

- Disable alerts as appropriate under **Account Manager Role Alert Management**.
- Acknowledge the alerts, as these are intended to notify the External Operators for the activity related to their child accounts.

Resolved and Known Issues

Resolved Issues

Issue	Synopsis
Various	Internally reported issues relating to elimination of resource contention.
SAS-6519 SAS-6316	For MobilePASS BlackBerry Java app users, clicking on the auto-enrollment link now again opens the app to enroll the token. For more information, refer to “Self-Enrollment Support for BlackBerry 10” under “Enhancements” on page 13.
SAS-6167	When using a Generic HTTP(s) SMS Plugin , SAS is now able to send OTPs via SMS to users whose mobile number is prefixed with the + symbol.
SAS-5832	The customization for Self-Enrollment pages is now supported for MobilePASS for Windows Store (RT).
SAS-5788	Resolved medium severity security issue found using the security analysis tool.
SAS-5654	The Provisioning Task list is now updated correctly when a task is removed.
SAS-5640	Users who have already been manually provisioned with a Gridsure token are now excluded from the auto-provisioning process and no longer appear under the list of users who were not enrolled.
SAS-5630	CSV user imports succeed with large number of users being imported.
SAS-5563	After migrating from BlackShieldID 2.7 to SAS 3.4, the grid size of the imported Gridsure tokens changed from 6x6 to 5x5 after first use.
SAS-5549	SAML assertion no longer fails authentication when using aliases.
SAS-5548	Error related to Sync Server Connection Issues under E-mail Message Templates in the Synchronization Agent has been corrected.
SAS-5531 SAS-5542	Capacity calculation error could cause provisioning and assignment errors. The calculation of capacity was counting Expired , Cancelled , and Completed provisioning tasks.
SAS-5540	Import of users fails when Save Log As is used.
SAS-5531	An error that occurred when provisioning tokens in specific virtual servers has been corrected.
SAS-5493	Sharing an Auth Node with a child account and then attempting to log on using an alias of a user in one of the shared child accounts now works correctly.
SAS-5436	The button labeled Set as Default under Virtual Servers > Self-Service > Configuring Self-Service > Configure Self-Service Modules has been removed as it conflicted with the Self-Service Default Language setting under Virtual Servers > Self-Service > Configuring Self-Service > Languages .
SAS-5263	In some instances, MobilePASS was loaded onto a device but was not activated in SAS. This has been corrected.
SAS-5251	Multiple auto-provisioning emails are no longer sent to users when the Role Provisioning rule is applied.

Issue	Synopsis
SAS-5250	Setting up an Auto Provisioning Rule for a password token with Auto Revoke enabled now revokes the token when an AD user is removed from a group.
SAS-5215	Syncing an Operator user with no mobile number defined no longer prevents the user record from being updated.
SAS-5193	To address the Poodle vulnerability, the FreeRADIUS Agent is limited to TLS versions of SSL without reverting to SSL V3.0 or SSL V2.0.
SAS-5184	Requests made through the Self-Service site for token activation codes to be sent via SMS are now processed correctly.
SAS-5121	Alias name transfer no longer occurs when creating a new user with an existing username in a virtual server.
SAS-5113	A display issue with the Shortcut link in the SAS Management Console has been corrected.
SAS-5105	An issue where provisioning tasks were created for users who had already been provisioned with a token has been corrected.
SAS-5101	The First OTP and Second OTP fields are now available for the time-based MobilePASS resync functionality in the SAS Administration Console .
SAS-5022	Error messages have been added to SAS when attempting to save an image file that the system will not accept (for example, when uploading images for icons on the Self-Service site).
SAS-5021	An error that occurred when removing and re-importing users has been corrected.
SAS-5010	An XSS vulnerability with the file upload functionality has been resolved.
SAS-5006	SAS no longer enters a state where an old synced group cannot be removed, yet the users can be removed.
SAS-4998	A display issue with the users table on the ASSIGNMENT tab has been corrected. This list now displays 10 users per page as intended.
SAS-4991	The Billing – Users by custom field report (formerly named the Count Unique User report), located under Administration > Reports and Billing Management , no longer includes duplicate or erroneous users.
SAS-4979	External Operators were not receiving sync host notification alerts.
SAS-4887	The Count Unique User ID report has been renamed to Billing – Users by custom field , which more accurately reflects the data generated by this report, which includes users in child accounts filtered by the Custom #1 field.
SAS-4880	Under Configure Self-Service Modules , when setting the VPN URL field for the Default Elements module, IP addresses are no longer required to be preceded by http://www .
SAS-4867	Changes to Auth Nodes were not reflected in the Auth Node Change Log . A blank report was generated.
SAS-4747	Security updates to address OpenSSL vulnerabilities have been added to SAS.
SAS-4742	Removed "Incomplete Auto reservation" message; available only in debug mode

Issue	Synopsis
SAS-4741	"Illegal user provisioning" error did not indicate organization for which the error occurred.
SAS-4695	The Auto Provisioning Service generated errors and then terminated unexpectedly.
SAS-4615	When importing users, it was possible to select Address2 as an option for database field but it did not appear in User Detail on ASSIGNMENT tab.
SAS-4579	Could not change Container or Alias fields of a synchronized user.
SAS-4524	A SAS server upgrade error on the Security Answers table was resolved.
SAS-4521	COMMS tab returned an error on user access.
SAS-4518	Self-service in languages other than English no longer produces an error message.
SAS-4506	Failed to import SafeNet 3300 tokens.
SAS-4493	GrIDsure token self-enrollment failed.
SAS-4490	The Linux packages for SAS Agent for FreeRADIUS and FreeRADIUS Updater are now signed.
SAS-4476	Users were able to select new passwords after exceeding license limit but were not able to authenticate on the Self-Service portal.
SAS-4472	SAS communicated incorrectly with a sync client when no sync was required due to the 1-hour delay. This did not apply to Differential Sync functionality as 1-hour delays are not supported.
SAS-4430	User IDs did not allow capital letters.
SAS-4391	MP token enrollment using an activation code did not request PIN code change.
SAS-4359	Performance improved when moving tokens with the BSIDCA API MoveTokens feature.
SAS-4349	Defined realm value was case sensitive. Could not authenticate if user entry did not match exactly.
SAS-4318	Editing an External Operator no longer causes Delegated Management rights to be removed.
SAS-4286/4255	Logging addresses are now displayed in the Virtual Servers > Comms > Logging Agent window. This has been documented in the <i>SAS Remote Logging Agent Configuration Guide</i> .
SAS-4271	Security patches were included for OpenSSL 1.0.1h and OpenSSL 0.9.8za. See http://www.safenet-inc.com/technical-support/security-updates/ for more information.
SAS-4196	Errors that occurred when attempting to install a license file into SAS have been resolved.
SAS-4165	Architectural changes were made to increase efficient management of users and groups.
SAS-4142	After configuring SMTP settings, the Apply button was disabled and it was not possible to continue with configuration.
SAS-4130	MP-1 application on MAC reported that its certificate has expired
SAS-4129	When working with Self-Service , after time-out, the user is now directed to the correct portal.

Issue	Synopsis
SAS-4100	In the MP-1 Token Template window, the Time Complexity field is now labelled correctly.
SAS-4091	Provisioning rules with expiration dates did not work as expected.
SAS-4048	RADIUS service now correctly detects SAS server availability.
SAS-4041	The target is now properly reset after a provisioned MobilePASS token is revoked.
SAS-3947	The <i>SAS Self-Service Administrator Guide</i> stated that lost tokens could be reported through the Self-Service site, which is not the case. The guide has been updated to state a user must contact their administrator or help desk to report a lost token.
SAS-3938	After clicking on Custom Labels , the window and field descriptor are now displayed correctly.
SAS-3937	The <i>SAS Service Provider Administrator Guide</i> has been updated to provide clarification of the Add parameters to URL field for Custom SMS settings.
SAS-3927	SAS validation of MP-1 on latest version of OS X.
SAS-3924	Users can now create User IDs in the console or using the Import Users feature using uppercase letters. Limitation: Lowercase letters in existing User IDs cannot be changed to uppercase.
SAS-3887	Token allocation and de-allocation queries are no longer slowing authentication performance.
SAS-3865	An issue where -0 was appended to the serial numbers for imported SafeNet GOLD tokens has been corrected.
SAS-3811	Sync of server SQL statements causing long wait time.
SAS-3798	Resolved issue that some operators do not have visibility of Assignment and Tokens tabs
SAS-3763	In certain instances, large amounts of data were unnecessarily retrieved from the database.
SAS-3742	Following migration from SafeWord to SAS, the correct token types are now displayed in the SAS Allocation window.
SAS-3697	The SafeNet eToken 3200 (Gold) upload file is now imported correctly.
SAS-3670	Improvements to moving users into containers when auto provisioning rules have been enabled
SAS-3623	Performance improvements to token allocation
SAS-3620	Restored a missing text label from the allocation user interface
SAS-3601	Custom email setting no longer reverts back to default
SAS-3539	Error messages that were encountered when viewing reports in the Event Viewer have been resolved.
SAS-3482	Improved support for long group names in the SAS Management Interface
SAS-3480	Changes in MP-1 enrollment workflow; self-enrollment not configurable.

Issue	Synopsis
SAS-3415	Error received during automatic provisioning for user groups in multiple provisioning rules.
SAS-3370	Could not find any recognizable digits.
SAS-3327	Stability improvements to self-enrollment for date/time handling.
SAS-2966	Operators that did not have “remove” privileges in their role definition were able to delete provisioning tasks.
SAS-2533	An issue existed where SAS allowed assignment and activation of tokens without the available token capacity. When this occurred, all logins to SAS failed until the user logged in with Microsoft credentials and added additional token capacity. This issue has been corrected.
SAS-2484	The “Duplicate key value” error message in log files has been resolved.
SAS-2435	Ability to customize enrollment screen when choosing Install Locally for MP token.
SAS-2345	An option to remove the I am a new user button from the Request a Token module in the Self-Service portal is now supported.
SAS-2145	Corrected an issue to allow operators with delegated access to download reports
SAS-1954	The <i>SAS Service Provider Administrator Guide</i> and the <i>SAS Subscriber Account Operator Guide</i> have been updated to provide the correct default values for the inner and outer window synchronization parameters.
SAS-1847	When attempting to display the group list from AD after having added many groups in which some authenticate with CRYPTOCARD and some do not, the IIS 7 agent crashed.
SAS-1398	When provisioning an MP-1 token and installing locally, an erroneous error message was sometimes displayed, even though the process was successful.
SAS-1397	Logon failed when a user was provisioned with SMS and required the PIN to be changed at first logon.
SAS-1176	Enrollment notification strings containing ‘\’ or ‘/’ characters cannot be copied.
SAS-1042	The SMS URL value in SMS Settings only allowed 64 characters.

Known Issues

Issue	Synopsis
SAS-6198	<p>Summary: Windows authentication cannot be used with the MS SQL Server</p> <p>Workaround: None.</p>
SAS-6001	<p>Summary: Attempting to run reports sometime fails as a result of inadequate MS SQL server capacity.</p> <p>Workaround: Increase the data size allowed for replication. It is recommended to increase the data size to 20mb. For information about increasing the data size in MS SQL, refer to the following Microsoft documentation: https://msdn.microsoft.com/en-us/library/ms179573.aspx</p>
SAS-5814 SAS-5830	<p>Summary: In some instances, generated reports cannot be viewed. When selecting a report under My Report Output, the SAS Management Console closes unexpectedly and the user must log in again.</p> <p>Workaround: Log in to SAS with an Account Manager role. Click the VIRTUAL SERVERS tab and then select a virtual server. Next, click the ADMINISTRATION tab, click Report Output, and then select a generated report.</p>
SAS-5813	<p>Summary: Fixed Passwords: By default, user passwords in SafeWord are case insensitive and are stored in upper case. This may lead to problems when migrating to SAS.</p> <p>Workaround: For authentication to succeed following migration to SafeNet Authentication Service, the passwords must be entered in all upper case or be reset. If the SafeWord user passwords are set as case-sensitive, they will continue to operate correctly following migration.</p>
SAS-5017	<p>Summary: When adding multiple logging agents in the SAS Console, only the first agent added receives logging events, even after it is removed. This means that only one logging agent can be used.</p> <p>Workaround: None.</p>
SAS-4953	<p>In the SAS Console, under Assignment > User > Tokens > Manage > Resync, the First OTP and Second OTP fields are now displayed when performing a time-based resync for a MobilePASS token.</p>
SAS-4827	<p>Summary: UserIDs with UTF-8 characters do not display properly.</p> <p>Workaround: This issue exists in certain versions of Internet Explorer only. Using another browser will avoid this display issue..</p>
SAS-4766	<p>Summary: Allowing one logging agent host for a Virtual Server allows all logging agent hosts.</p> <p>Workaround: None</p>
SAS-3920 SAS-2708	<p>Summary: Error when adding SAML SP if DNS/Host URL is unresolvable.</p> <p>Workaround: None</p>
SAS-1852	<p>Summary: When the Change password at first logon policy was set for a user with a fixed password, the user's attempt to change the password at first logon failed.</p> <p>Workaround: None</p>

Issue	Synopsis
SAS-1318	<p>Summary: After entering a non-standard RADIUS attribute (SAS Console > Virtual Servers > Radius Attribute > New), the Attribute value is displayed as 1, not the value entered.</p> <p>Workaround: To work around this issue, click a specific attribute “after” clicking a non-standard type. This interface display will update successfully.</p>
SAS-1257	<p>Summary: If a token is deleted during the provisioning process, it continues to be displayed in the Provisioning Task Manager.</p> <p>Workaround: The provisioning task can be deleted manually.</p>
SAS-1152	<p>Summary: When editing a Provisioning Task in Virtual Servers > Assignment > Provisioning Task Management, and setting the Stop Date to the current date, no error message displayed and the Edit window closes normally, with the previous Stop Date remaining unchanged.</p> <p>Workaround: Select the day after today’s date. This sets the end date to 12:00:01 a.m. on the next day (i.e., midnight of “today”).</p>

Compatibility and Upgrade Information

Interoperability

Supported Tokens

- **Hardware tokens:** KT-4, KT-5, RB, eToken PASS time-based, eToken PASS event-based, SafeNet GOLD, SafeNet Silver, eToken 3410, eToken 3400, CD-1
- **Software tokens:**
 - **MP-1:** Clients are included for Android, iOS, BlackBerry, Java, Windows Desktop, and Mac OS X.
 - **MobilePASS:** Clients are included for Android, iOS, BlackBerry, Windows Desktop, Windows Phone, and Windows Store (RT).

Supported Mobile Devices

- Android devices running OS 2.2 or later
- Devices running iOS 5.0 or later
- BlackBerry devices running OS 6 or later
- BlackBerry devices running OS 10
- BlackBerry devices running Java v7.x
- Windows Phone
- Windows RT

Supported Browsers

- Chrome 33 and later
- Firefox 3.5 and later
- Internet Explorer 8 and later



NOTE: Internet Explorer versions 10 and later do not support hardware token initialization.

Supported Directories

LDAP

- Active Directory
- Novell eDirectory 8.x
- SunOne 5.x

SQL

- MS-SQL
- MySQL
- Oracle

Upgrade Instructions

Upgrading the Synchronization Agent

Existing Synchronization Agents will continue to work but the scan interval will be limited to once every 60 minutes (instead of every 20 minutes), even if the agent is manually stopped and restarted.

It is recommended to upgrade the Synchronization Agent to v3.4 in order to obtain the benefits of differential synchronization and regain a scan interval of every 20 minutes. Restarting the synchronization service in the agent initiates scanning and synchronization.

Product Documentation

See <http://www2.safenet-inc.com/sas/implementation-guides.html> for documentation associated with this product. We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet 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 SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

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