SafeNet Authentication Service

CUSTOMER RELEASE NOTES

Version: 3.20 SAS PCE GA

Build: 3.20.0.3092

Issue Date: June 2024

Document Part Number: 007-001478-001 Rev L

Contents

Product Description

SafeNet Authentication Service (SAS) delivers fully automated, highly secure authentication-as-a-service, 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 SAS 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.

SAS 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 Information - SafeNet Authentication Service 3.20 PCE

General Availability Release

Release Summary - June, 2024
This general availability release introduces the following features and resolves the issues listed below:

Visual location display in MobilePASS+ push notifications

Push notifications now include the authentication attempt's location. In this security enhancement, the push login request includes a map view to show the location where the login attempt is originated from, allowing users to verify the legitimacy of authentication requests. This feature is supported in MobilePASS+ versions 2.4 and above. Additionally, you can view the live location in the SAS PCE console under **Snapshot** -> **Authentication Activity** or under **Virtual Server** -> **Assignment** -> {User Id} -> **Authentication Activity**.

MobilePASS+ push with number matching

SAS PCE provides number matching in SafeNet MobilePASS+ to enhance the security of push authentications, guarding against MFA fatigue or push bombing attacks. With number matching, users gain control over each login request by selecting the number displayed during authentication. This feature is supported in MobilePASS+ versions 2.5 and above. Refer to the **Token Policies** > **Software Token and Push OTP Settings** section in *SafeNet Authentication Service 3.20 Service Provider Administrator Guide* for details about how to enable this feature.

Support for MySQL 8.0.33

SAS PCE now supports MySQL 8.0.33 database. All commonly supported deployments are expected to work. This feature ensures that the upgrade from older SAS-supported MySQL versions work seamlessly.

Support for Microsoft SQL Server 2022

SAS PCE now supports Microsoft SQL (MS SQL) Server 2022. This feature ensures that the upgrade from older SAS-supported MS SQL versions work seamlessly.

SSO for non-standard Web applications

This release introduces integration between **SafeNet App Gateway** and **SAS PCE** to enable secure access to the non-standard web applications, that is, non-SAML or non-OIDC based web applications. In this integration, **Keycloak** (an open-source product) acts as the Identity Provider (IdP) and SAS PCE provides Multi-factor authentication (MFA). The Single Sign-On (SSO) works similar to the existing SafeNet App Gateway integration with STA.

Resolved Issues

This table provides resolved issues as of the latest release.

Issue	Synopsis
SAS-63144	Previously, when the admin reduced the license capacity, the provisioning would still happen at the original capacity, leading to a negative capacity. However, now, tokens are activated based on the latest license capacity.
SAS-68114	Users now have the option to choose whether to retain a persistent cookie. An application setting called **RemovePersistentCookie** has been introduced for self-service functionality. By default, this setting is `False`, permitting the use of persistent cookies. However, changing the value to `True` will replace the persistent cookie with a session-based cookie. For more details, refer to **Persistent cookie settings for Self-Service portal** section in *SafeNet Authentication Service 3.20 Installation Guide*.
SAS-64355	A restriction on the use of special characters in configuring the SAS Server Side PIN Policy has been implemented. The acceptable special characters include: (`!@#$%&*?`). For more details, refer to *SafeNet Authentication Service 3.20 Service Provider Administrator Guide*.
SAS-54412	The outdated information regarding the **SAS Server Restore** is now removed from the documentation. The updated steps to import the Cipher key has been tested with all the supported databases. For more details, refer to the *SafeNet Authentication Service 3.20 Installation Guide*.
SAS-69260	In macOS Sonoma 14.4.1, users were getting an error while enrolling a MobilePASS token (with the system culture other than en-US). Now, the MobilePASS enrollment supports all the system culture.

Known Issues

This table provides list of known issues as of the latest release.

Issue	Synopsis
SAS-69399	The SAS Token Management console does not reflect the reduced token count for **GrIDsure** and **MobilePASS** after downgrading the license (for example, from 20 to 10 capacity license).
SAS-67267	**GetReportOutput** gives an empty response if level parameter is other than **Subscriber**.

Issue	Synopsis
SAS-68944	**Summary**: After importing the site(s) from primary to secondary SAS, administrator is not able to remove the site of secondary SAS from primary server and can access virtual server data from secondary SAS. **Workaround**: To remove the secondary machine site, uninstall SAS from secondary site.
SAS-68710	Operator is able to re-send the token provisioning email even if the operator role only allows deletion role (since with deletion role, edit permission/role gets added currently).
SAS-69824	User is able to configure non-numeric value in Fixed PIN even if Server-side PIN Policy has ***Numeric*** Minimum Complexity.

> **NOTE** Click here to access Customer Release Notes of previous releases.

Advisory Notes

Setting up MS SQL with Windows Domain User

> **NOTE** In case of Site Import, if the SAS servers are in different domains, all SAS servers must be in the trusted domain. For more details, refer to the *Installation Guide*.

Migrating to MS SQL Database Server

> **NOTE** If migrating to MS SQL database (from any database server) with the SAS Database Migrator utility, please select the checkbox if using the Windows domain user account.

Database Backup

> **CAUTION!** It is strongly recommended to back up the database before upgrading to the latest version of the SAS. Failure to do so could result in serious data loss.

MobilePASS+ Software Authenticator

The SAS 3.5 (and later) PCE supports Thales next-generation software authenticator, *MobilePASS+*, in addition to MobilePASS v8. Both applications use the same MobilePASS token allocation, and a new Allowed Targets policy allows to select either application for new enrollments. By default, enrollments on iOS and Android are with *MobilePASS+*, and with MobilePASS v8 for all other supported device platforms.

Upgrading Synchronization Agent

Synchronization Agent 3.3.2 (and earlier) will continue to work but the scan interval is 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 version 3.4 (or later) to obtain the benefits of differential synchronization and a scan interval of every 20 minutes. Restarting the synchronization service in the agent initiates scanning and synchronization.

Compatibility and Component Information

Supported Tokens

Hardware Tokens

- KT-4, KT-5, RB, eToken PASS time-based, eToken PASS event-based, SafeNet GOLD, eToken 3410, eToken 3400, CD-1, SafeNet OTP 110, IDProve 100, SafeNet OTP Display Cards.

Software Tokens

- **MobilePASS+**: Supported for Android, iOS, macOS, Apple Watch, Windows Mobile, and Windows Desktop.
- **MobilePASS v8.4.6**: Supported for Android, iOS, Windows Mobile, Windows Desktop, and Mac OS X.
- **MP-1**: SafeNet Authentication Service support for MP-1 tokens software has been phased out and is no longer supported.

Supported Browsers

- Microsoft Edge Chromium
- Chrome™
- Firefox®
- Safari 5 and later on iOS
- Safari 10.1 and later on macOS

> **NOTE** For hardware token initialization, Internet Explorer versions 10 and below may result in a lesser user experience. It is recommended to use the latest versions of the supported browsers for token initialization.

Supported Directories

LDAP

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

SQL

- MS SQL
- MySQL

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 Thales Customer Support.

Thales 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 Thales 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.thalesgroup.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

The support portal also lists telephone numbers for voice contact (Contact Us).