SafeNet Authentication Service

CUSTOMER RELEASE NOTES

Version: 3.19 SAS PCE SP1

Build: 3.19.02564.2564

Issue Date: February 2024

Document Part Number: 007-001478-001 Rev K

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 3.19 PCE

The following release has been issued for SafeNet Authentication Service 3.19 PCE

> Service Pack 1 Release

> General Availability Release

Service Pack 1 Release

Release Summary - February, 2024
This service pack release includes all the features of 3.19 GA release and introduces the following security enhancement. It also addresses the issues listed below:

Security Enhancement

Issue	Synopsis
SAS-67539	A session management issue was detected in SAS PCE. This issue allowed an authenticated user to gain access to another organization's account. To exploit this vulnerability required a malicious user to be authenticated and logged in to an active session, and to access the user's information in the other organization. For details on how to temporarily disable the SAS PCE Self-Service portal until an upgrade to Hotfix version SAS PCE 3.19 SP1 is possible, see **KB0028251** on the **Customer Support Portal**.

Resolved Issue

Issue	Synopsis
SAS-66347	When the token was re-synced using the API, the second OTP allowed user authentication, but now it displays an error message.
SAS-67716	Earlier, when SAS PCE was installed with a custom setup, the site import into a secondary site failed, but it is operating accurately now.

Issue	Synopsis
SAS-67889	Earlier, the license upgrade from evaluation to production was not visible because the service start date and service stop date under **On-Boarding** > **Services** section remained unchanged. However, this change is now visible.
SAS-66350	When the SAS was setup with MySQL using manual replication, the user federation via Keycloak did not work. However, it is now functioning correctly.

Known Issue

Issue	Synopsis
SAS-68232	Non-essential logs are observed in the DBupgrade.logs file during the fresh installation or upgrade of SAS PCE.

General Availability Release

Release Summary - November, 2023
This general availability release introduces the following features and resolves the issues listed below:

FIPS Compliance Enhancement

With new modifications in cryptographic algorithms and security compliance, SafeNet Authentication Service now leverages Federal Information Processing Standards. This compliance ensures that FIPS-enabled machines protect the sensitive data on the SAS server and allows secure authentication operations. For more details, refer to the **Security and Compliance** chapter in the *SAS 3.19 Installation Guide* or **Installation** section on Thalesdocs.

Thalesdocs

SAS PCE documentation is now online at https://thalesdocs.com/sas/latest. With all the product related content housed at one place, Thales makes it easier for you to access, consume and share the required information effortlessly.

From v3.20 onwards, SAS PCE documentation will only be available on Thalesdocs. PDFs will no longer be part of our subsequent releases.

LUNA HSM Support

SAS PCE v3.18 and above are now compatible with on-premise LUNA HSM 7 devices, which augments the protection against cryptographic keys and data-sensitive operations. For more information on supported platforms or LUNA HSM integration, refer to *LUNA HSM Integration Guide* or **Integration** section on Thalesdocs.

FreeRADIUS Windows Service Removal

BlackShield ID FreeRADIUS windows service and freeradconfig web service are no longer a part of SAS PCE. As part of this change, all the references of BlackShield ID FreeRADIUS and freeradconfig service have been removed from the product and documentation.

Agent and SDK Updates

This release includes the following updated agent documents:

- Microsoft Active Directory Federation Service (ADFS) 2.43
- Microsoft Network Policy Server (NPS) 3.0.2
- Microsoft Outlook Web Application (OWA) 2.1.5
- SafeNet Agent for Epic 3.0.4
- SafeNet Agent for FreeRADIUS 3.2.1
- SafeNet Agent for Remote Logging 1.06
- SafeNet Agent for Windows Logon 3.6.2
- SafeNet Authentication API for Java 1.3.0
- SafeNet Synchronization Agent 3.8.7

Documentation Improvements

- Added more detailed information on communication and flow of data between SAS server and its agents, authentication apps and APIs.
- Revised references of Azure Active Directory (Azure AD) to Microsoft Entra ID in *SAS 3.19 Subscriber Account Operator Guide* as per Microsoft's name change guidelines.
- Revised references of Microsoft Office 365 to Microsoft 365 in *SAS 3.19 Push OTP Solution Guide*, *MobilePASS+ for Android User Guide*, *MobilePASS+ for iOS User Guide*, *MobilePASS+ for Windows User Guide* and *MobilePASS+ for Chrome User Guide* in accordance with Microsoft's name change undertaking.

Resolved Issues

This table provides resolved issues as of the latest release.

Issue	Synopsis
SAS-65825	EMET 5.52, the Microsoft security toolkit leveraged by SAS in previous versions, is removed from the application.
SAS-61583	After successful enrollment, the GrIDsure token is displaying under the **Authentication Methods** module as expected. Previously, the GrIDsure token would still be listed under **Provisioning Tasks** post enrollment.
SAS-55079	The administrator was not able to update HSM user PIN in the SAS console. Implemented license validation cashing to fix the issue for expected behavior.
SAS-65578	*SAS 3.19 Push OTP Solution Guide*, *SAS 3.19 System Requirements Guide* and *SafeNet Agent for FreeRADIUS Installation and Configuration Guide* are improved with comprehensive data flow and networking information.
SAS-65103	Timestamp format issue pertaining to the RLA authentication logs displayed in the Syslog server is fixed.

Known Issues

This table provides known issues as of the latest release.

Issue	Synopsis
SAS-66270	**Summary:** Post installation, SAS HA Controller Service, which is expected to be disabled by default, is enabled. **Workaround:** Before upgrading to a new version, determine the state of the SAS HA Controller Service, and then make sure to retain the same state after the upgrade as well.
SAS-66402	**Summary:** Alert mails are not being sent to the operator when the Account Capacity and Remaining Account Capacity fall below the specified threshold values.
SAS-50466	**Summary:** With latest **SMS + Email** delivery method, when the end user does not have enough credits to receive OTP via SMS, the OTP isn't received on Email also. **Workaround:** In case of insufficient credits, the **SMS/Email/Voice OTP Delivery Methods** can be switched to **Email**. The OTP is received successfully.
SAS-60212	**Summary:** When **Pin Policy** in MobilePASS/MobilePASS+ is set to **Change PIN on first use is required** option, the user is not getting prompted to change the pin after first successful login.
SAS-65113	**Summary**: When using a long customized message with special characters during authentication with an SMS token, the message content is splitting into two parts. **Workaround**: When using the default SMS format, the entire message is delivered in one SMS as expected.

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 Mac OS

> **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
- Oracle

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).