SafeNet Agent for NPS 3.0.2

CUSTOMER RELEASE NOTES

Build Number: 3.0.2.569
Issue Date: June 2022
Document Part Number: 007-013943-002, Rev. C

Contents

Product Description 2
Resolved and Known Issues 2
Issue Severity and Classification 2
Release Description 2
Release Summary – SafeNet Agent for NPS 3.0.2 2
Release Summary – SafeNet Agent for NPS 3.0.1 3
Release Summary – SafeNet Agent for NPS 3.0.0 3
Release Summary – SafeNet Agent for NPS 2.1.0 4
Release Summary – SafeNet Agent for NPS 2.0 4
Advisory Notes 5
Administrator Credentials Required 5
Logging with Push OTP 5
Known Issues 5
Compatibility and Upgrade Information 6
System Requirements 6
Authentication Protocols 6
Push OTP 6
Upgrade 6
Product Documentation 7
Support Contacts 7
Customer Support Portal 7
Telephone Support 7
Email Support 7

Product Description

The SafeNet Agent for NPS adds strong authentication to Microsoft's Network Policy Server (NPS) environments, by transferring RADIUS requests received by the NPS to the SafeNet server.

NPS is the Microsoft implementation of a Remote Authentication Dial-In User Service (RADIUS) server, and is included in the Windows Server 2012, 2016 and 2019 families. The NPS performs centralized connection authentication, authorization, and accounting for many types of network access, including wireless, authenticating switch, remote access (dial-up and VPN), and router-to-router connections.

Resolved and Known Issues

Issue Severity and Classification

The following table serves as a key to the severity and classification of the issues listed in the **Resolved Issues** table and the **Known Issues** table, which can be found in the sections that follow.

Severity	Classification	Definition
C	Critical	No reasonable workaround exists
H	High	Reasonable workaround exists
M	Medium	Medium-level priority problems
L	Low	Low-level priority problems

Release Description

Release Summary – SafeNet Agent for NPS 3.0.2

The SafeNet Agent for NPS 3.0.2 release introduces a new registry key and resolves some customer-reported issues.

Resolved Issues

This section describe the issues resolved in the SafeNet Agent for NPS v3.0.2 release:

Severity	Issue	Synopsis
H	SASNOI-15812	**Summary:** While validating with NTRadPing, triggers were not working even if the pre-auth rule was set. A new registry key, **AllowPreAuthRule**, is now added to support the use of pre-authentication rules for the Active Directory (AD) users.
H	SASNOI-14991	**Summary:** The radius return attribute **Mapped-IP-Address** was causing the NPS agent to crash due to not being able to fetch the correct IP Address. Now, the agent captures the correct IP Address, which is correctly displayed on NTRadPing as well.

Release Summary – SafeNet Agent for NPS 3.0.1

The SafeNet Agent for NPS 3.0.1 release resolves some customer-reported issues.

Resolved Issues

This section describe the issues resolved in the SafeNet Agent for NPS v3.0.1:

Severity	Issue	Synopsis
H	SASNOI-12340	**Summary:** The SafeNet Agent for NPS installed on Windows Server 2012R2 now does not crash if the initial RADIUS request contains some attributes (such as Event-Timestamp, Stripped-User-Name, Realm) from the FreeRADIUS server.
H	SASNOI-12025	**Summary:** The NPS agent throwing the error "Network Policy Server discarded the Push token request when radius attribute **ratAuthenticator** value is empty" is now resolved. The authentication is working fine now.

Release Summary – SafeNet Agent for NPS 3.0.0

The SafeNet Agent for NPS 3.0.0 introduces new features and resolves a known issue.

New Features and Enhancements

Enhanced Security

The **AES-GCM** encryption algorithm is now used to provide faster and a more secure way to protect the data exchange.

Thales Branding

The SafeNet Agent for NPS 3.0.0 has been redesigned with the Thales branding. With this release, the installer name is also changed to **SafeNet Agent for NPS**.

Extended Operating System Support

The SafeNet Agent for NPS 3.0.0 now supports **Windows Server 2019 (64-bit)**.

Resolved Issues

This section describe the issues resolved in the SafeNet Agent for NPS v3.0.0:

Severity	Issue	Synopsis
H	SASNOI-10366	**Summary:** The SafeNet Agent for NPS does not intercept the authentication requests that comes to the NPS server if the Connection Request Policy is set to **Authenticate requests on this server**.
H	SASNOI-10519	**Summary:** The authentication works correctly in the migration mode when NPS agent is installed on the NPS migration server.

Release Summary – SafeNet Agent for NPS 2.1.0

The SafeNet Agent for NPS 2.1.0 introduces new features and resolves a known issue.

New Features and Enhancements

Support for Transport Layer Security v1.2

Support for Transport Layer (TLS) v1.2 protocol has now been added.

Extended Operating System Support

The SafeNet NPS Agent now supports Windows 2016 (64-bit).

Security Enhancements

To better secure the communication between channels, the SafeNet NPS Agent 2.1.0 contains certain security enhancements at infrastructure and agent level.

Upgrade from Version 2.0

The SafeNet Agent for NPS 2.1.0 supports upgrade from version 2.0.

Resolved Issues

This section describe the issues resolved in the SafeNet Agent for NPS v2.1.0:

Severity	Issue	Synopsis
M	SASNOI-3600	**Summary:** SafeNet Agent for NPS now works correctly when receiving an authentication request using the MS-CHAP-v2 protocol.

Release Summary – SafeNet Agent for NPS 2.0

The SafeNet Agent for NPS 2.0 introduces new features and repairs several known issues.

New Features and Enhancements

Support for Push OTP

The SafeNet Agent for NPS 2.0 supports the Push OTP function with MobilePASS+ (new generation mobile authenticator) when SAS Authentication Server Cloud Edition 3.9.1 and later versions become available.

Support for Return Attributes

The SafeNet Agent for NPS 2.0 supports the use of SafeNet server defined user or group RADIUS Return Attributes.

Gemalto Branding

The SafeNet Agent for NPS 2.0 has been updated with Gemalto branding.

Upgrade from Version 1.31

The SafeNet Agent for NPS 2.0 supports upgrade from version 1.31.

Resolved Issues

This section describe the issues resolved in the SafeNet Agent for NPS v2.0:

Severity	Issue	Synopsis
L	SASIL-2640	**Summary:** SafeNet Agent for NPS now works correctly when receiving an authentication request from Aruba ClearPass.

Advisory Notes

Administrator Credentials Required

The SafeNet Agent for NPS must run with administrator credentials. This applies to the installation of the agent and to running **SafeNet Agent Management Console** options.

Logging with Push OTP

When logging to a website supporting the Push OTP function, the user enters the Username, leaves the password field empty, and clicks the login button. The user will then receive a prompt on their MobilePASS+ app, to accept or reject the logon request. On accepting the logon request, the user is logged in to the website.

Known Issues

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

Severity	Issue	Synopsis
H	SASNOI-3589	**Summary:** Authentication fails using challenge-response token if CHAP or MS-CHAP-v2 protocol is employed. **Workaround:** None. Will be fixed in a future release.
H	SASNOI-3533	**Summary**: The **Server Status Check** always reports that the Secondary (Failover) Server is off-line, even if it is running correctly. **Workaround:** None. Will be fixed in a future release.
H	SASNOI-3499	**Summary**: An error message is encountered while installing the NPS agent on non-English Operating Systems. **Workaround:** None. Will be fixed in a future release.
H	SASNOI-3366	**Summary**: Push functionality does not work when NPS is configured using the Token Validator Proxy (TVP) Agent. **Workaround**: Add an exception that when NPS is configured with Proxy, connection to the TVP should route directly.
H	SASIL-3183	**Summary**: If SafeNet Agent for NPS is working via a proxy server, when running the **Server Status Check** procedure (**SafeNet Agent Management Console > Authentication Test**) the SafeNet server is reported as being off-line, even though it is running correctly. **Workaround:** None. Will be fixed in a future release.

Compatibility and Upgrade Information

System Requirements

Prerequisites

Microsoft .NET Framework 4.5.2 (or above) must be installed on the same computer as the SafeNet Agent for NPS.

Operating Systems

- Windows Server 2012 R2 (64-bit)
- Windows Server 2016 (64-bit)
- Windows Server 2019 (64-bit)

Authentication Management Platforms

- SafeNet Authentication Service PCE/SPE 3.9.1 and later
- SafeNet Trusted Access (earlier, SAS Cloud)

Authentication Protocols

The SafeNet Agent for NPS supports the following authentication protocols:

- PAP
- CHAP
- MS-CHAP-v2

The following restrictions apply when working in Challenge/ Response mode:

- Tokens in Challenge/ Response mode are supported only for PAP.
- GrIDSure tokens are supported only for PAP and MS-CHAP-v2. MS-CHAP-v2 requires SAS 3.9.1 or later.

> **NOTE:** To use GrIDSure with the SafeNet Agent for NPS, the user must utilize an external GrIDSure service (for example SAS Self Service Portal).

Push OTP

The SafeNet Agent for NPS supports the Push OTP function when working with MobilePASS+.

> **NOTE**: Push OTP is currently not supported for SAS PCE/SPE.

Upgrade

The SafeNet Agent for NPS **v3.0.2** supports upgrade from **v2.0** onwards.

Upgrade from versions earlier than 2.0 is not supported.

> **NOTE:** Upgrade is not supported on Windows Server 2019.

Product Documentation

The following documents is associated with this release:

- *SafeNet Agent for NPS v3.0.2: Installation and Configuration Guide*

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 refer to the documentation. 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 the **REGISTER** link.

Telephone Support

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

Email Support

You can also contact technical support by email at technical.support.DIS@thalesgroup.com.