

SafeNet Agent for Internet Information Services

CUSTOMER RELEASE NOTES

Version: 2.1.0
Build: 2.1.0.69
Issue Date: May 2025
Document Part Number: 007-000454-002 Rev. C

Contents

| | |
|---|---|
| Product Description | 2 |
| Release Information | 2 |
| Release Summary – SafeNet Agent for Microsoft IIS 2.1.0 | 2 |
| Release Summary – SafeNet Agent for Microsoft IIS 2.0.3 | 2 |
| Release Summary – SafeNet Agent for Microsoft IIS 2.0.1 | 3 |
| Release Summary – SafeNet Agent for Microsoft IIS 2.0.0 | 3 |
| Release Summary – SafeNet Agent for Microsoft IIS 1.1.0 | 4 |
| Release Summary – SafeNet Agent for Microsoft IIS 1.06 | 4 |
| Advisory Notes | 4 |
| Upgrade Limitations | 4 |
| Known Issues | 5 |
| Compatibility and Component Information | 5 |
| Authentication Server | 5 |
| Network | 5 |
| Supported Architecture | 5 |
| Supported Web Servers | 5 |
| Supported Applications and Objects | 5 |
| Supported IIS Authentication Type | 6 |
| Supported Web Browsers | 6 |
| Additional Software Components | 6 |
| Additional Web Browser Requirements | 6 |
| Supported Authentication Methods | 6 |
| Product Documentation | 6 |
| Support Contacts | 8 |

Product Description

The SafeNet Agent for Internet Information Services is designed for Terminal Services Web (TS Web), but can also be used for IIS websites and resources where the authentication method is configured to use the Microsoft authentication. The agent ensures web-based resources are accessible only to authorized users, whether working remotely or behind a firewall, by prompting for additional credentials during logon.

By default, logon to the TS Web requires that the user provide a correct user name and password. The SafeNet Agent for Microsoft IIS augments this logon mechanism with strong authentication by adding a requirement to provide a One-Time Password (OTP) generated by a Thales Group token.

Release Information

Release Summary – SafeNet Agent for Microsoft IIS 2.1.0

The following release has been issued for SafeNet Agent for Microsoft IIS v2.1.0:

General Availability Release - May, 2025

This release provides the following support and resolves a customer-reported issue.

ASP.NET-based Applications Support

The agent now supports ASP.NET-based applications, such as, SharePoint and CyberArk, enabling seamless integration for the web apps built on the ASP.NET framework. This enhancement ensures better performance, scalability, and ease of use for ASP.NET-based application architectures.

Removed Support for Agent Migration

Agent migration for version 2.1.0 and above is no longer supported.

Resolved Issues

| Issue | Synopsis |
|--------------|--|
| SASNOI-20480 | Users can now access the SharePoint and CyberArk applications when the IIS agent is enabled. |

Release Summary – SafeNet Agent for Microsoft IIS 2.0.3

The following release has been issued for SafeNet Agent for Microsoft IIS v2.0.3:

General Availability Release - July, 2024

The SafeNet Agent for Microsoft IIS 2.0.3 release introduces the product re-branding and a security fix.

Thales Branding

The SafeNet Agent for Microsoft IIS has been redesigned with the Thales branding.

Security Fix

This release introduces a security fix for the most secure version of SafeNet Agent for Microsoft IIS. For more details, please refer the security bulletin (ref: 20240726).

Release Summary – SafeNet Agent for Microsoft IIS 2.0.1

The SafeNet Agent for Microsoft IIS 2.0.1 release introduces two new features.

FIPS Support

It introduces support for:

- > The FIPS mode within the operating system with AES-GCM and RSA key standards.
- > The FIPS mode for decrypting the agent's BSID key.

Upgrade Support

The SafeNet Agent for Microsoft IIS 2.0.1 release now supports the upgrade from 2.0.0. To upgrade, run the installation wizard and select appropriate options when prompted.

NOTE You must update the new agent configuration file using the management console, once it gets downloaded. Once the upgrade is complete, the IIS server restarts. The upgrade should be performed during non-peak hours to avoid disruption of services.

Release Summary – SafeNet Agent for Microsoft IIS 2.0.0

The SafeNet Agent for Microsoft IIS 2.0.0 release introduces an enhancement and resolves some customer-reported issues.

Enhanced Security

The **AES-GCM** encryption algorithm is now used to provide faster and a more secure way to protect data exchange between the SafeNet Agent for Microsoft IIS and the SAS solution. Enabled by enhanced security, the agent delivers a more robust, and dependable authentication experience. A more secure key standard, like **AES-GCM**, can also help you comply with your organization's security policy requirements.

This feature is supported on **SAS Cloud** and **SAS PCE/SPE v3.9.1** onwards.

NOTE To use the **AES-GCM** key standard, the administrator has to download a new *Agent.bsidkey* file from the SAS, and update the same (in the agent) at **Configuration Management > Communications > Agent Encryption Key File**.

Resolved Issues

Please find below details of the solutions provided.

| Issue | Synopsis |
|-------------|---|
| SASNOI-9886 | Time stamp format of the secured URL has been updated to be more generic. |

Release Summary – SafeNet Agent for Microsoft IIS 1.1.0

The SafeNet Agent for Microsoft IIS 1.1.0 introduces a new feature, in addition to resolving customer reported/ known issues.

Security Enhancements

Several security issues have been resolved, including hardening of the directory permissions level.

Support for Transport Layer Security 1.1/1.2

Support for Transport Layer Security (TLS) 1.1 and 1.2 protocols has now been added.

Extended Operating System Support

With this release, users will be able to seamlessly install, configure and execute the agent in a **Windows Server 2016** (64-bit) operating system environment. In addition, the **Windows Server 2008** operating system is no longer supported.

Resolved Issues

Please find below details of the solutions provided.

| Issue | Synopsis |
|-------------|---|
| SASNOI-7974 | Secured the vulnerability that made the agent susceptible to cross-site scripting attacks. |
| SASNOI-7418 | AD password is now removed from the logs files of the agent. |
| SASNOI-7351 | The agent now authenticates IIS web resources successfully with Mozilla Firefox version 57 browser. |

Release Summary – SafeNet Agent for Microsoft IIS 1.06

The SafeNet Agent for Microsoft IIS v1.06 introduces security enhancements, in addition to resolving a customer reported/ known issue.

Resolved Issues

Please find below details of the solutions provided.

| Issue | Synopsis |
|------------|--|
| SASIL-1944 | A user without privileges no longer has access to the SafeNet Agent for Microsoft IIS installation directory following installation by the domain administrator. |

Advisory Notes

Upgrade Limitations

Upgrade from earlier versions of the SafeNet Agent for Microsoft IIS to version 2.0.0 is not supported.

Known Issues

| Issue | Synopsis |
|--|---|
| SASNOI-21966 | Summary: After authentication, when accessing the protected application, the Thales favicon appears instead of the application's favicon. Workaround: Replace the default Thales icon with the customized <company> icon at the agent installed location (\GEMALTO\IIS\SupportFiles\basic). It will be resolved in a future release. |
| SASNOI-4089 | Summary: There is no documented procedure for customizing the SafeNet Agent for Microsoft IIS user interface. Workaround: None, will be resolved in a future release. |
| SASNOI-22168 | Summary: While authenticating with the GridSure token, users need to re-enter the Grid OTP. Workaround: None. This is an intermittent issue and will be fixed in a future release. |
| SASNOI-21953 SASNOI-22013 | Summary: Logging issue. While accessing a protected site of SharePoint, the log files are not created at the default log location for the application. Workaround: None. It will be resolved in a future release. |

Compatibility and Component Information

Authentication Server

- > SafeNet Authentication Service PCE/SPE 3.9.2 and later
- > SafeNet Authentication Service Cloud

Network

- > TCP Port 443

Supported Architecture

- > 64-bit

Supported Web Servers

- > IIS 10

Supported Applications and Objects

- > Terminal Services Web Sites
- > Virtual Directories
- > Applications

Supported IIS Authentication Type

- > Microsoft Authentication (Basic Authentication)

Supported Web Browsers

- > Microsoft Edge
- > Mozilla Firefox
- > Google Chrome

NOTE If the Auth Node is configured with an **IPv4** address, **Mozilla Firefox** might default to using **IPv6**, leading to authentication failures. To ensure compatibility, modify the Firefox settings by performing the following steps:

1. Open Firefox and type **about:config** in the address bar.
2. Click **Accept the Risk and Continue** (if prompted).
3. In the search bar, type **network.dns.disableIPv6**.
4. Set this option to **true** by double-clicking it or using the toggle button.
5. Restart Firefox.

Additional Software Components

- > Microsoft .NET Framework 4.8 (or above) must be installed.
- > Following ASP .NET versions (Server role component) must be installed:
 - Windows Server 2016 – ASP .NET 4.8 (or above)
 - Windows Server 2019 – ASP .NET 4.8 (or above)
 - Windows Server 2022 – ASP .NET 4.8 (or above)
- > IIS 6 Management Compatibility Role Service (and its sub components) must be installed.

Additional Web Browser Requirements

- > Cookies must be enabled.
- > JavaScript must be enabled.
- > ActiveX plug-ins (software token detection only).

Supported Authentication Methods

- > All tokens and authentication methods supported by SafeNet sever.

NOTE MobilePASS token is not supported in Quick Log mode.

Product Documentation

The following product documentation is associated with this release:

- > SafeNet Agent for Internet Information Services: 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 when 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 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](#)).