SafeNet Agent for Windows Logon 4.1.2

CUSTOMER RELEASE NOTES

Build Number: 4.1.2.1492
Issue Date: May 2025
Document Part Number: 007-000281-003, Rev. D

Contents

Product Description

The SafeNet Agent for Windows Logon is a Two-Factor Authentication (2FA) solution to help Microsoft enterprise customers ensure that valuable resources are accessible only to authorized users. It delivers a simplified and consistent user login experience, reduces support calls related to password management, and helps organizations comply with regulatory requirements.

The use of 2FA when accessing network resources, in place of traditional static passwords, is a critical measure for information security.

For a list of existing issues as of the latest release, refer to Known Issues.

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 Windows Logon 4.1.2

The SafeNet Agent for Windows Logon v4.1.2 resolves some customer-reported issues.

> **Correction:**
> In the WLA 4.1.1 documentation, for Error 1721, the affected Windows version was incorrectly mentioned as “22H2”.
> This has been corrected to **Windows 11, version 24H2** in the WLA 4.1.2 documentation.

Resolved Issues

<table>
<tr><th>Severity</th><th>Issue</th><th>Synopsis</th></tr>
<tr><td>H</td><td>SASNOI-22047</td><td>Login attempts were failing if the username included "<b>!,~,`,!,^,(,),{,} ,’</b>", displaying the error message "Username cannot be blank or contain any of the following special characters: /\[]:;|=+*?<>@". This issue is now resolved. The supported special characters are <b>a-z,A-Z,0-9,.,-,_,$,%,&,#,~,`,!,^,(,),{,},'</b></td></tr>
<tr><td>C</td><td>SASNOI-21794</td><td>An <b>Error 1721</b> appeared while installing or upgrading the agent on Windows 11, version 24H2 and above (mentioned in the KB article here). The issue is now fixed and the agent’s dependency with WMIC has been removed.</td></tr>
</table>

Release Summary – SafeNet Agent for Windows Logon 4.1.1

The SafeNet Agent for Windows Logon v4.1.1 introduces security fixes and resolves a customer-reported issue.

Security Fix

This release introduces some security fixes for the SafeNet Agent for Windows Logon.

Resolved Issues

Severity	Issue	Synopsis
H	SASNOI-21362	The silent uninstallation of the agent was not completed properly because certain actions were triggered incorrectly, resulting in a non-zero return code. This issue has now been resolved.

Release Summary – SafeNet Agent for Windows Logon 4.1.0

The SafeNet Agent for Windows Logon v4.1.0 introduces the following new features and resolves some customer-reported issues.

Language selection and customization

The agent now operates in multiple languages, which allows administrators to choose the display language for the Windows Logon agent as per the user's preference. A new registry setting, **PreferredLanguage**, is introduced that facilitate the agent to support a number of languages, including English (Default), French, German, and more.

The default text messages of a specific language file (for example, en.json) that is available at *C:\Program Files\SafeNet\Windows Logon\Languages* can also be customized.

> **NOTE**: While uninstalling or upgrading the agent, ensure to take a backup of the **ccl** files. You will need to manually edit the key values in the required JSON files to match the previous customization. For the detailed information on the key-value pairs, refer to this annexure.

Local admin MFA privilege control

In WLA, administrators had rights to modify the WLA registry settings locally, such as disabling the agent, which allowed users to bypass two-factor authentication (2FA). To mitigate this issue and enhance security, a new registry setting called **RegEditCount** has been introduced to restrict admins' ability to make local modifications.

This feature enables enterprises to control the privileges of a local admin user on a WLA-installed machine. Its count specifies the maximum number of logon attempts a local admin user can use with modified sensitive registry settings. Once the logon attempt reaches the set threshold (the RegEditCount value), any local changes to the registry settings will be reverted to their original values, and the modifications will not be retained.

For more details, see the **RegEditCount** setting in the **Registry Settings** section in *SafeNet Agent for Windows Logon 4.1.0: Installation and Configuration Guide*.

Push UI Enhancement

The MobilePASS+ Push screen and user messaging within the existing UI/UX have been improved throughout the entire user authentication journey.

Resolved Issues

Severity	Issue	Synopsis
C	SASNOI-21050 SASNOI-21365 SASNOI-21437	On Windows 10, after installing Microsoft's Windows update **KB5043064 (OS Builds 19044.4894 and 19045.4894)**, the WLA users authenticating with SafeNet MobilePASS+ authenticator were facing critical issues affecting the PUSH authentication. For more details, refer to the KB article here on the support portal. This issue is now resolved.
H	SASNOI-21378	The agent was sending wrong IP address of the client machine during push authentication. This issue is now fixed.
H	SASNOI-18389	After customizing the cursor size, when the user locks the machine and logs back in, the mouse pointer resets to the smallest size. This issue is now fixed.
H	SASNOI-20812	Login attempts failed if the username included a blank space (for example, "local admin"), displaying the error message "Username cannot be blank or contain any of the following special characters: / \ [ ] : ; = @ + * < >" ". After the fix, the error no longer appears, and the username field supports blank spaces.
C	SASNOI-17617	After deploying WLA, CredCryptoHelper errors and WLANotificationService warnings appeared in the event viewer and agent log due to database failure and runtime exceptions. Now, on enabling the **Debug** mode in the WLA management console, the event viewer logs provide more specific and detailed information.
H	SASNOI-20854	An **Error 1722** message appeared while uninstalling the agent through the control panel due to insufficient user permissions. This issue is now resolved and the agent can be uninstalled successfully via the control panel.
H	SASNOI-20598	Users were unable to install the agent due to improper cleanup of the required registry entries. It displayed an error "Upgrade from current installed WLA agent is not supported. Please uninstall the agent before running". This issue is now fixed.
H	SASNOI-8625	During logon, if a user long presses the **Enter** key without providing a **Passcode**, WLA sends a large number of authentication requests to the SafeNet Authentication Server. To prevent multiple authentication requests to the server, auto-focus is disabled after submission of the blank **Passcode**. The users can proceed with their journey through the mouse click on the displayed message.
L	SASNOI-19218	The "Exempt Local/Domain Administrator strong authentication" feature was not working for the users of a custom domain group who are also a nested member of any of the following built-in groups. 1. Domain Admins 2. Enterprise Admins 3. Schema Admins 4. Group Policy Creator Owner In this case, the users were not able to bypass the SafeNet OTP and they need to login via MFA. This issue is now fixed.

Release Summary – SafeNet Agent for Windows Logon 4.0.0

The SafeNet Agent for Windows Logon v4.0.0 introduces the following new feature.

Passwordless Windows Logon

The **Passwordless Windows Logon** feature is based on SafeNet Agent for Windows Logon (STA version). It enhances secured access to Windows machines by eliminating the need to provide a password for machine access and beyond, by replacing the password with a certificate-based authentication mechanism. It further eliminates the end-user friction, as users no longer need to manage or remember their passwords.

However, this feature is not available for SAS PCE customers. For detailed information, refer to the online documentation on thalesdocs.

Resolved Issues

Severity	Issue	Synopsis
H	SASNOI-14902	After upgrading the agent, the password caching feature was not working when logging into a WLA-protected machine, even if **Enable Microsoft Password Caching** is selected in the **SafeNet Windows Logon Agent Manager > Policy** tab. This issue is now fixed.

Release Summary – SafeNet Agent for Windows Logon 3.7.0

The SafeNet Agent for Windows Logon v3.7.0 introduces the following significant features and resolves a customer-reported issue.

Number Matching

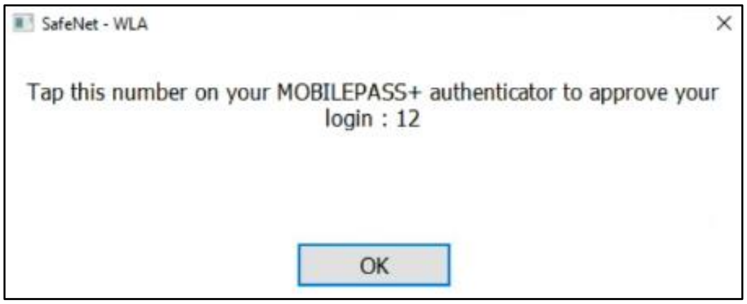
WLA now supports **MobilePASS+ push with number matching** feature, which secures push authentications to protect against MFA fatigue or push bombing attacks.

Number matching gives control to the user for every login request, because they must select the number in the push notification on their MobilePASS+ application as is displayed on the WLA login screen.

For more details, refer to **Running the Solution** section in *SafeNet Agent for Windows Logon: Installation and Configuration Guide*.

Limitation

While accessing an application via **Run as different user** (in outgoing RDP or shared folder access use cases), the WLA-agent installed machine displays the following UI (different than the number matching UI displayed in all other use cases):



Tap this number on your MOBILEPASS+ authenticator to approve your login : 12

Kiosk Support

The agent is now supported in Kiosk mode for **Windows 10** and **Windows 11** (64-bit) operating systems.

Resolved Issues

Severity	Issue	Synopsis
C	SASNOI-19577	**Summary**: If interactive logon policy **Display user information when the session is locked** is set to *Do not display user information* and **Skip OTP on Unlock** is enabled, and the user provides an empty username and password during unlock, the user is blocked from accessing the machine as all subsequent authentication with the correct credentials fail. This issue is now fixed.

Release Summary – SafeNet Agent for Windows Logon 3.6.3

The SafeNet Agent for Windows Logon v3.6.3 resolves some customer-reported issues.

Resolved Issues

Severity	Issue	Synopsis
C	SASNOI-17859	**Summary**: During logon or unlock, the user credential fields are displayed with a delay of few (20-30) seconds, due to which a domain user is not able to login into the machine. This behavior is observed during network latency or when the domain controller is inaccessible and was reported in WLA v3.6.0. This issue is now fixed.
C	SASNOI-19195	**Summary**: After upgrading the agent from version **3.5.x** to **3.6.x**, users are able to login in offline mode only after at least one successful online authentication. This issue is now fixed and the users can login in offline mode without the need of an online authentication.
C	SASNOI-19226	**Summary**: WLA fails to authenticate a user whose username contains "**$**" and displays an error. After the fix, the username field supports "$" as a valid special character.
C	SASNOI-19578	**Summary**: If **Don't display username at sign-in** interactive logon windows policy is enabled, and the user enters an incorrect username while unlocking the machine, the **Username** field is not displayed again to enter the correct credentials. In this case, the user is blocked from accessing the machine. After the fix, the login flow is working as expected.
H	SASNOI-18183	**Summary**: If a user switches from online to offline mode and attempts to launch an application via "Run as administrator" that must use an OTP, then the user is not prompted for an OTP. After the fix, the authentication is working as expected in offline mode.
H	SASNOI-18237	**Summary**: After changing the AD password, the users were not able to login with the changed password. This is now fixed and the users can successfully log in with the changed password.

H	SASNOI-13324	**Summary**: During offline authentication, the agent did not accept emergency password for the user assigned with a GrIDsure token. This issue is fixed and the user with a GrIDsure token can use the emergency password for offline authentication.

Release Summary – SafeNet Agent for Windows Logon 3.6.2

The SafeNet Agent for Windows Logon v3.6.2 release resolves some customer-reported issues.

Resolved Issues

Severity	Issue	Synopsis
C	SASNOI-18390	**Summary**: While unlocking or logging into a WLA 3.6.1 protected machine, the login screen flickers due to which a user is unable to access the machine. UI flickering is now fixed and the users are presented with the appropriate login screen.
H	SASNOI-17922	**Summary**: During logon/unlock, OTP and password fields are simultaneously displayed for a few (10-20) seconds due to which a user is not able to login to the machine. This issue was reported in WLA v3.6.0. This is now fixed and appropriate user credential fields (OTP and password) are displayed during the logon/unlock.

Release Summary – SafeNet Agent for Windows Logon 3.6.1

The SafeNet Agent for Windows Logon v3.6.1 release introduces the following security fix and resolves some customer-reported issues.

Security Fix

This release introduces a security fix for the most secure version of SafeNet Agent for Windows Logon.

For more details, please refer the security bulletin (ref: *20230704*).

Resolved Issues

Severity	Issue	Synopsis
H	SASNOI-16785	**Summary**: If “Microsoft Password Caching” is enabled and user enters incorrect password while executing an application with administrator privileges, then WLA caches the incorrect password. The user does not get the password prompt to provide the correct password anymore and hence is unable to execute the application. This is fixed now and WLA does not cache the password if incorrect.
H	SASNOI-16386	**Summary**: Offline authentication does not work for domain users added in a local group after restart. This is now fixed by caching the users’ appropriate group and the offline authentication works as expected.

Severity	Issue	Synopsis
H	SASNOI-17409	**Summary**: If a user provides "*@domain" in the username field, and the log level is set to DEBUG, all the usernames of the domain are written in the agent's log file. This issue has been fixed by restricting the username field to only support valid username characters or formats.

Release Summary – SafeNet Agent for Windows Logon 3.6.0

The SafeNet Agent for Windows Logon v3.6.0 offers some improvements and introduces the following features.

Agent Deployment via Microsoft Endpoint Configuration Manager

Along with the existing agent deployment methods, Group Policy Object (GPO) and Intune, the agent can now also be deployed via a Windows-centric endpoint management tool, **Microsoft Endpoint Configuration Manager**, formerly known as **Microsoft System Center Configuration Manager** (SCCM). It enables the admins to deploy the agent on the client machines within or outside the corporate network.

For detailed information, refer to **Chapter 5: Deploying the agent via Microsoft Endpoint Configuration Manager** in *SafeNet Agent for Windows Logon 3.6.0: Installation and Configuration Guide*.

Enhancements

- The **Credential Provider** in **Policy** tab of the SafeNet Windows Logon Agent Manager now defaults to **Windows V2 Password Credential Provider**. To wrap any other external (third-party) credential provider, for example, Microsoft Credential Provider V1, select **Other Credential Provider**, and enter its GUID in the subsequent text field. For more details, refer to the **Policy Tab** section in *Installation and Configuration Guide*.

  Additionally, the **WLAasV1Provider** registry setting has been removed from the ADML and ADMX template.
- The user messaging has been improved in the existing login UI/UX for near native Windows experience. For new screens, refer to **Chapter 7: Running the Solution** in *Installation and Configuration Guide*.
- The **Use GrIDsure Token** link, displayed on the login screen is now renamed to **Use a grid pattern**.
- A new parameter, **AGENTSTATUS** is added to enable or disable the agent while installing the agent silently.

Release Summary – SafeNet Agent for Windows Logon 3.5.2

The SafeNet Agent for Windows Logon v3.5.2 release introduces an enhancement and resolves some customer-reported issues.

Enhanced Data Protection

The agent is now compatible with Microsoft Windows native FDE tool, **BitLocker**.

Extended Operating System Support

The SafeNet Agent for Windows Logon now adds support of **Windows Server 2022**.

Resolved Issues

Severity	Issue	Synopsis
M	SASNOI-8458	**Summary**: The **EmergencyPassword** registry entry was missing in the WLA ADMX template. This registry entry has now been added in the ADML and ADMX template.
C	SASNOI-14179	**Summary**: The **More choices** option was not visible while accessing an application with elevated privileges. This issue is fixed and the **More choices** option is now visible in the sign-in window for the user with elevated privileges.
H	SASNOI-16626	**Summary**: In some rare scenarios, after restarting the machine, the end-users were not able to authenticate in offline mode. This is fixed and the WLA offline authentication is now working correctly.

Release Summary – SafeNet Agent for Windows Logon 3.5.1

The SafeNet Agent for Windows Logon v3.5.1 release introduces a security fix and the following security improvement.

Security Improvement

A new registry setting, **SetCachingToCurrentUser**, is introduced to augment the secured storage of a user's cached Microsoft password.

Security Fix

This release introduces a security fix for the most secure version of SafeNet Agent for Windows Logon.
For more details, please refer the security bulletin (*ref: 18052022)*.

Release Summary – SafeNet Agent for Windows Logon 3.5.0

The SafeNet Agent for Windows Logon v3.5.0 release introduces the following new features and resolves some customer-reported issues.

Azure Active Directory (AD) Support

SafeNet Agent for Windows Logon is now supported for pure and hybrid **Azure AD** joined machines.

Intune support for deployment of WLA is added. For detailed information, see *SafeNet Agent for Windows Logon: Installation and Configuration Guide*.

Limitations

Following are the limitations of WLA agent for Azure AD joined machines:

- The **Exempt Local/Domain Administrator strong authentication** will not work with pure **Azure AD** joined machines for domain admins. However, this feature will work as expected for the local admins.
- The **Group Filter** feature will not work with pure **Azure AD** joined machines for domain groups. However, this feature will work as expected for the local groups.
- Third-party federation services with Azure AD joined machines are not supported.

Support of Interactive Logon Windows Policies

SafeNet Agent for Windows Logon now supports the following interactive logon windows policies:

- Do not display last user name
- Display user information when the session is logged

Microsoft Credential Provider V1 Support

The Microsoft Credential Provider V1 is now only supported for **Windows Server 2012**.

Resolved Issues

Severity	Issue	Synopsis
H	SASNOI-14865	**Summary**: WLA did not retain existing users' cached password after an MFA exempted user logs in to the machine. Subsequently, user/s of the machine are prompted for password on their next login. This is now fixed and the password caching functionality is working as expected.
H	SASNOI-14887	**Summary**: WLA failed to bypass the SafeNet OTP authentication on system unlock when the windows policy was set to hide the username at login/unlock screen. After adding the support for **Interactive Logon Windows Policies**, this issue is resolved. **NOTE**: If the windows policy is set to hide the username, the screen will display a generic message "If you normally use a Token, please enter your PIN + OTP otherwise your Windows Password in Password Field".

Release Summary – SafeNet Agent for Windows Logon 3.4.5

The SafeNet Agent for Windows Logon v3.4.5 release offers support of Windows 11 and resolves a customer-reported issue.

Extended Operating System Support

The SafeNet Agent for Windows Logon now adds support of **Windows 11 (64-bit)**.

Resolved Issues

Severity	Issue	Synopsis
H	SASNOI-14353	**Summary**: After rebooting the WLA installed machine, the end-users were not able to authenticate in offline mode if the domain was not accessible. This is now fixed and the WLA offline authentication is working correctly.

Release Summary – SafeNet Agent for Windows Logon 3.4.4

The SafeNet Agent for Windows Logon v3.4.4 release introduces some security fixes and improvements.

- The Microsoft password of the domain administrators are no longer cached and stored by SafeNet Agent for Windows Logon.
- The Microsoft password of other users are now protected with additional layers of encryption.

Security Fix

This release introduces security fixes for the most secure version of SafeNet Agent for Windows Logon.
For more details, please refer the security bulletin (*ref: 2021112)*.

Release Summary – SafeNet Agent for Windows Logon 3.4.3

The SafeNet Agent for Windows Logon v3.4.3 release resolves some customer-reported issues.

Security Fix

This release introduces a security fix for the most secure version of SafeNet Agent for Windows Logon.
For more details, please refer the security bulletin (*ref: 14102021)*.

Resolved Issues

Severity	Issue	Synopsis
H	SASNOI-12798	**Summary:** WLA ignored the users in the **exempted group** and prompted for multi-factor authentication for all the users after a machine restart. This is now fixed and WLA does not prompt for MFA for users who are in the exempted group.
H	SASNOI-12894	**Summary**: When a user initiated an RDP session from a WLA protected machine, the “more choices” option was not visible thereby inhibiting the Switch User functionality. This is fixed, now the “more choices” option is visible and the Switch User functionality is accessible.
C	SASNOI-12787	**Summary**: Multi-factor authentication was bypassed when the group filter is selected to “Only selected groups must use SafeNet” by entering a username in an incorrect email format. For more details please refer the security bulletin (*ref: 14102021)*.
H	SASNOI-13543	**Summary**: For user logins configured to “Skip OTP on Unlock”, the WLA protected machine used to hang during system unlock, if the user provides the correct password preceded by two incorrect password attempts. After the fix, the machine no longer hangs for the above scenario.

Release Summary – SafeNet Agent for Windows Logon 3.4.2

The SafeNet Agent for Windows Logon v3.4.2 release resolves a customer-reported issue.

Resolved Issues

Severity	Issue	Synopsis
C	SASNOI-12926	**Summary**: The WLA offline authentication is now working correctly.
H	SASNOI-12391	**Summary**: The WLA login does not hang even if it does not have access to the VPN. The offline authentication works correctly in this case.
C	SASNOI-13027	**Summary**: The login screen flickering issue in Windows 10 is now resolved.

Release Summary – SafeNet Agent for Windows Logon 3.4.1

The SafeNet Agent for Windows Logon v3.4.1 release resolves a customer-reported issue.

Resolved Issues

Severity	Issue	Synopsis
H	SASNOI-12650	**Summary**: The SafeNet Agent for Windows Logon now correctly accepts and displays the special characters/accents in the WLA login screen.

Release Summary – SafeNet Agent for Windows Logon 3.4.0

The SafeNet Agent for Windows Logon v3.4.0 release supports the below new feature.

Thales Branding

The SafeNet Agent for Windows Logon has been redesigned with the Thales branding.

With this release, the Management Console name is changed to **SafeNet Windows Logon Agent Manager**.

Reduced Operating System Support

The SafeNet Agent for Windows Logon 3.4.0 has now stopped the support for Windows 7 (32-bit, 64-bit) and Windows Server 2008 R2 (64-bit).

Release Summary – SafeNet Agent for Windows Logon 3.3.3

The SafeNet Agent for Windows Logon v3.3.3 release resolves some customer-reported issues.

Resolved Issues

Severity	Issue	Synopsis
H	SASNOI-12141	**Summary**: The Windows 2019 machine now does not hang when the user (who is not a part of MFA group) logins successfully through WLA after 2-3 wrong attempts initially.
H	SASNOI-12257	**Summary**: The login functionality now works correctly and the user does not get prompted for an OTP again if they enter a wrong AD password.

Release Summary – SafeNet Agent for Windows Logon 3.3.2

The SafeNet Agent for Windows Logon v3.3.2 release resolves some customer-reported issues.

Resolved Issues

Severity	Issue	Synopsis
H	SASNOI-11688	**Summary:** On cancelling the PUSH authentication from the WLA login screen, the request took longer than expected to go back to the normal logon screen. Code refactoring has been done to resolve the issue.
M	SASNOI-11427	**Summary:** The PUSH message on the Windows Logon Agent did not show where the request was coming from. Now, the PUSH authentication request successfully displays a proper message on the pop-up window.

Release Summary – SafeNet Agent for Windows Logon 3.3.1

The SafeNet Agent for Windows Logon v3.3.1 release introduces the below feature and resolves some customer-reported issues.

Extended Operating System Support

The SafeNet Agent for Windows Logon v3.3.1 now supports **Windows Server 2019 (64-bit)**.

Resolved Issues

Severity	Issue	Synopsis
C	SASNOI-8729	**Summary:** The Remaining off-line authentication count is now displayed correctly in the SafeNet Windows Logon Agent Manager window.
C	SASNOI-10819	**Summary:** The authentication delay for users bypassing the MFA is now fixed.

Release Summary – SafeNet Agent for Windows Logon 3.2.0

The SafeNet Agent for Windows Logon v3.2.0 release introduces major updates to the agent mode that works with SafeNet Trusted Access (application management) and for this mode, resolves the below customer-reported issues.

Resolved Issues

Severity	Issue	Synopsis
H	SASNOI-10179	**Summary:** Group filtering on SafeNet Agent for Windows Logon is now working correctly.
H	SASNOI-6639	**Summary:** WLA server status check and Authentication from console is working fine now with TVP (Enable SSL Certificate Check).

Release Summary – SafeNet Agent for Windows Logon 2.3.6

The SafeNet Agent for Windows Logon v2.3.6 release resolves the below customer-reported issue.

Resolved Issues

Severity	Issue	Synopsis
C	SASNOI-10566	**Summary:** The users logged in the system using only the Windows password, bypassing the Push OTP if the authentication attempt is timeout. Now, the login functionality works correctly, and the SafeNet Authentication with the PUSH OTP is not bypassed erroneously.

Release Summary – SafeNet Agent for Windows Logon 2.3.5

The SafeNet Agent for Windows Logon v2.3.5 introduces support for the FIPS mode within the operating system with RSA key standard.

Release Summary – SafeNet Agent for Windows Logon 2.3.4

The SafeNet Agent for Windows Logon v2.3.4 introduces support for the FIPS mode for decrypting the agent’s BSID key.

Release Summary – SafeNet Agent for Windows Logon 2.3.3

The SafeNet Agent for Windows Logon v2.3.3 introduces support for the FIPS mode within the operating system. This is currently applicable only for the agent authentication flow for the **AES-GCM** key standard.

Release Summary – SafeNet Agent for Windows Logon 2.3.2

The SafeNet Agent for Windows Logon 2.3.2 release resolves some customer-reported issues.

Resolved Issues

Severity	Issue	Synopsis
H	SASNOI-8920	**Summary:** The agent now enforces Local Administrator Accounts through GPO or Registry.
H	SASNOI-9013	**Summary:** The domain security group are not excluded from Two-Factor Authentication (2FA).
H	SASNOI-9761	**Summary:** If logged in user's user ID is single character, the agent not display offline OTP count.

Release Summary – SafeNet Agent for Windows Logon 2.3.1

The SafeNet Agent for Windows Logon 2.3.1 release resolves some customer-reported issues.

Resolved Issues

Severity	Issue	Synopsis
H	SASNOI-9046	**Summary:** The agent now enforces 2FA for users who login using alternate UPN suffix.
H	SASNOI-9045	**Summary:** The Windows Logon screen does not become unresponsive on losing the network connection. Code refactoring has been done, ensuring that if the login functionality does not work, the users are authenticated using the offline mode.
H	SASNOI-8855	**Summary:** The group membership functionality now applies correctly, ensuring that the members in the bypass SafeNet authentication group can now login using only their AD credentials.
H	SASNOI-8849	**Summary:** Some code modifications have been made, improving the login speed of the agent.
M	SASNOI-8839	**Summary:** If an internet timeout error is encountered, the users are authenticated using the offline mode.
H	SASNOI-8269	**Summary:** Credential providers do not go back to the login screen, if the Microsoft API calls take longer than expected to respond. Code refactoring has been done for the **getGroup** functionality, ensuring that if the functionality times out, the users are authenticated using the offline mode.

Release Summary – SafeNet Agent for Windows Logon 2.3.0

The SafeNet Agent for Windows Logon 2.3.0 release introduces two new features.

Bypass SafeNet Authentication on System Unlock

The SafeNet Agent for Windows Logon now allows the administrators to bypass SafeNet OTP authentication on system unlock. The feature, **Skip OTP on Unlock** reduces friction of entering OTP every time a user unlocks a machine. For more details, refer the *SafeNet Agent for Windows Logon: Installation and Configuration Guide*.

Bypass SafeNet Authentication for All Applications

The SafeNet Agent for Windows Logon now allows the administrators to bypass SafeNet OTP authentication for all applications at once, by adding a wildcard, an asterisk (*) in the ***FilterProcess*** Registry flag. The feature is useful in instances where an administrator does not explicitly want to add all the applications that must be excluded from the OTP authentication. For more details, refer the *SafeNet Agent for Windows Logon: Installation and Configuration Guide*.

Release Summary – SafeNet Agent for Windows Logon 2.2.8

The SafeNet Agent for Windows Logon 2.2.8 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 Windows Logon and the SAS/STA 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 **SafeNet Trusted Access (STA)** 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

Severity	Issue	Synopsis
C	SASNOI-8871	**Summary:** Leading and trailing spaces in usernames will now be removed by the agent, and only the trimmed values will be passed to the Active Directory for group lookup. This ensures that the group filter functionality applies correctly, and the SafeNet authentication is not bypassed, erroneously.
H	SASNOI-8651	**Summary:** MSI silent installation documentation enhanced. For details, refer *SafeNet Agent for Windows Logon: Installation & Configuration Guide*.
C	SASNOI-8622	**Summary:** The SafeNet Agent for Windows Logon will now correctly authenticate users via the offline mode even during network connectivity issues or unavailability of the Domain Controller. The issue was encountered since the user groups were getting partially fetched due to network disruptions, leading to authentication bypasses.
H	SASNOI-8309	**Summary:** Users will now be able to successfully authenticate to their machines after a **Sleep** operation.

Severity	Issue	Synopsis
C	SASNOI-6646	**Summary: Group Filter** functionality (available on the **Policy** tab of the SafeNet Windows Logon Agent Manager now works for users in the external domain, allowing administrators to enforce or bypass the SafeNet authentication, as per their requirements.
M	SASNOI-3115/ SASIL-3852	**Summary:** Administrators will now be able to successfully authenticate to a user's machine (as the user) using the emergency password.

Release Summary – SafeNet Agent for Windows Logon 2.2.7

The SafeNet Agent for Windows Logon 2.2.7 release introduces new features and resolves some customer-reported issues.

Exclude Credential Filters

Administrators can modify the ***CompatibleFilters*** registry entry to add Credential Filters of specific Credential Providers, which are compatible and can be wrapped with our custom Credential Provider. For more details, refer the *SafeNet Agent for Windows Logon: Installation and Configuration Guide*.

Bypass SafeNet Authentication

To prevent applications from applying the SafeNet authentication, administrators can modify the ***FilterProcess*** registry entry. For more details, refer the *SafeNet Agent for Windows Logon: Installation and Configuration Guide*.

Resolved Issues

Severity	Issue	Synopsis
H	SASNOI-8245	**Summary:** A correct error message is displayed when SAS/STA service is timed out during the logon process.
M	SASNOI-8237	**Summary:** Users can configure **Communication Timeout** field up to **1** second.
	SASNOI-8234	**Summary:** ACL vulnerability is now fixed for WLA agent.
H	SASNOI-7855	**Summary:** Users can logon using the WLA agent with maximum supported PIN length and number of disconnected authentications.
H	SASNOI-6858	**Summary:** Incompatible Filter warning is removed for SpecOps ureset client when accessing SafeNet Windows Logon Agent Manager console.

Release Summary – SafeNet Agent for Windows Logon 2.2.6

The SafeNet Agent for Windows Logon 2.2.6 release resolves some customer-reported issues.

Resolved Issues

Severity	Issue	Synopsis
H	SASNOI-8143	**Summary:** The **Communication Timeout** setting will now work even if there is congestion or blockage in the underlying network.

Severity	Issue	Synopsis
H	SASNOI-8069	**Summary:** Users will now be able to successfully login, after a reboot or from the lock screen, using the V2 credential provider. The SafeNet Agent for Windows Logon now submits authentication requests in the correct format, *REALM\username*.

Release Summary – SafeNet Agent for Windows Logon 2.2.5

The SafeNet Agent for Windows Logon 2.2.5 release resolves some customer-reported/ known issues.

Resolved Issues

Severity	Issue	Synopsis
C	SASNOI-7773	**Summary:** It is now possible to switch between users even if the SafeNet Agent for Windows Logon is in the *enabled* state.
C	SASNOI-7623	**Summary:** The **Username** field cannot be edited after providing an incorrect AD password, ensuring that login attempts by any other user are not possible.
H	SASNOI-7506	**Summary:** The credential tile provider, Courion AD Password Reset (Core Security, SecureAuth), now wraps correctly with the SafeNet Agent for Windows Logon v2.2.1.

Release Summary – SafeNet Agent for Windows Logon 2.2.4

The SafeNet Agent for Windows Logon 2.2.4 release includes a feature enhancement, and resolves some known issues.

Domain Groups not Nested in Local Groups

The option, **Domain groups are not nested in Local group**, if selected indicates that no Nested Groups (Domain groups are nested in the Local group) are present inside the **Selected Groups** field. Domain lookup is skipped in such a case, helping improve the login delay time.

To enable this option, navigate to **SafeNet Windows Logon Agent Manager** > **Policy** > **Group Authentication Exceptions**.

Resolved Issues

Severity	Issue	Synopsis
	SASNOI-7340	**Summary:** The SafeNet Agent for Windows Logon now switches over to the primary SAS/STA server (if it becomes available) before the timeout if the secondary SAS/STA server is not configured, or is unavailable.
C	SASNOI-7230	**Summary:** The performance of the SafeNet Agent for Windows Logon is enhanced, ensuring that it logins faster.
H	SASNOI-7022	**Summary:** The SafeNet Agent for Windows Logon now allow users to successfully authenticate (using Offline authentication) using Windows 10 machines when connected through a Wi-Fi network, not connected to the LAN.

Severity	Issue	Synopsis
C	SASNOI-6901	**Summary:** The SafeNet Agent for Windows Logon v2.1 now allow users to login successfully using certificate/ smartcard based authentications.
H	SASNOI-6328	**Summary:** All exempted AD users of nested groups are now correctly bypassed from SafeNet OTP authentication.
M	SASNOI-3012	**Summary:** Since .NET 3.5 Framework is deprecated for Windows 8.1/10, the dependency to install it for running the agent, is now removed. The SafeNet Agent for Windows Logon works on .NET 4.5 Framework.

Release Summary – SafeNet Agent for Windows Logon 2.2.1

The SafeNet Agent for Windows Logon 2.2.1 resolves a customer-reported defect.

Resolved Issues

Severity	Issue	Synopsis
	SASNOI-7200	**Summary:** Normal users will now be able to access the SafeNet Agent for Windows Logon console without any error.
C	SASNOI-6710	**Summary:** After a user's password reset, the user will now be able to change his or her password at the time of next login.

Release Summary – SafeNet Agent for Windows Logon 2.2.0

The SafeNet Agent for Windows Logon 2.2.0 introduces a new feature and resolves some customer-reported defects.

Third Party Network Provider Software Compliance

It provides the following two options:

- **Allow all applications**: This option allows you to install the agent without updating the registry keys under [**`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order`**]. This option is selected by default on the Management console.

  > **NOTE:** Sometimes, selecting this option creates a conflict between the SafeNet Agent for Windows Logon and the third-party network provider software. In such a case, you need to uninstall the third-party network provider software and remove its registry entry. Before executing this operation, you need to perform the following steps:
  >
  > 1. Ensure that the **Allow all applications** option is selected, and click **Apply**.
  > 2. Close the Management console.

- **Allow only SafeNet compliant applications**: This option allows you to reset the registry key under [**`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order`**] to **"ProviderOrder"=" RDPNP,LanmanWorkstation,webclient "**.

Resolved Issues

This release resolves some known issues. Please find below details of the solutions provided.

Severity	Issue	Synopsis
H	SASNOI-6691	**Summary:** User will now be able to add local groups in the SafeNet Agent for Windows Logon.
H	SASNOI-6601	**Summary:** After the agent installation or while opening the Windows Logon Agent console, the network provider doesn’t get changed automatically.
C	SASNOI-6563	**Summary:** The SafeNet Agent for Windows Logon is now working as per the proxy server settings.

Release Summary – SafeNet Agent for Windows Logon 2.1

The SafeNet Agent for Windows Logon 2.1 introduces new features and resolves some customer-reported defects.

Allow Network Path without OTP

A capability to allow enabling/ disabling network path access without OTP is added to **Policy** tab of **SafeNet Windows Logon Agent Manager**. The **Allow windows explorer without OTP** check box, if enabled, allow Windows explorer to run without SafeNet Authentication (bypassing the SafeNet OTP option).

Extended Operating System Support

The SafeNet Agent for Windows Logon 2.1 now supports Windows Server 2016 (64-bit).

Support for Credential Providers

Support for the following Credential Providers is added:

1. Microsoft Credential Provider Tile Version 1 (V1)
2. Microsoft Credential Provider Tile Version 2 (V2)
3. Other [external (third-party)] Credential Provider(s) (like, ServiceNow)

> **NOTE:** To view supported Operating System (OS) versions, click here.

Wrap Third-Party Credential Providers

By default, the SafeNet Agent for Windows Logon wraps Microsoft Credential Provider. A new setting enables an administrator to wrap other external providers as well.

Display Other Credential Providers

By default, the SafeNet Agent for Windows Logon filters out (do not display) any other credential provider. Using **DoNotFilter** registry entry, the administrators can enable a view where other credential providers can also be displayed.

Resolved Issues

This release resolves some known issues. Please find below details of the solutions provided.

Severity	Issue	Synopsis
H	SASNOI-6583	**Summary:** Users will now be able to successfully login to Windows 10 machines via RDP using AD credentials. **Allow outgoing RDP connection without OTP** functionality is fixed, ensuring that SafeNet authentication can be bypassed, if required, when making an outgoing RDP connection.
H	SASNOI-6554	**Summary:** The cursor now positions back to the **Password** field after an unsuccessful login attempt.
H	SASNOI-6327	**Summary:** Unlocking a Windows 10 machine (after the SafeNet Agent for Windows Logon 2.1 installation, but on a machine not having ServiceNow) now displays the login screen. Earlier, it used to display only a blank screen.
H	SASNOI-6318	**Summary:** Login Tiles on a Windows 7 machine (after the SafeNet Agent for Windows Logon 2.1 installation, but on a machine not having ServiceNow) are now displayed even after entering ServiceNow GUID in *WrapCredentialProvider* registry entry.
H	SASNOI-6256	**Summary:** Users will now be able to access the network shared path on Windows 8 (and 8.1) machines.
H	SASNOI-6225	**Summary:** The **Hide Microsoft credential tile** option (of **Credential Tile Filter** dropdown menu in the Policy tab) now hides the Windows credential tile from the user.
H	SASNOI-6220	**Summary:** The **Username** field is now available with non-English languages on Windows 10 machines.
H	SASNOI-6169	**Summary:** The authentication conflict between the SafeNet Agent for Windows Logon and Govt CAC Smart Card login is now resolved by adding capability that allows to enable/ disable network path access without OTP. The **Allow windows explorer without OTP** check box, if enabled, allow Windows explorer to run without SafeNet Authentication (bypassing the SafeNet OTP option).
M	SASNOI-6133	**Summary:** The message, **If you normally use a Token, please enter your PIN + OTP otherwise your Windows Password in Password Field** now also displays for Windows 7 login screens, making it consistent with Windows 8 and Windows 10 login screens.
M	SASNOI-6131	**Summary:** The **Other User** tile, which was earlier displayed when a user attempted to log-off/ switch user on a Windows 7 machine, is now removed. When a user now attempts to log-off/ switch user on a Windows 7 machine, the user will directly be prompted for an OTP to unlock the machine.
H	SASNOI-2890	**Summary:** The SafeNet Agent for Windows Logon 2.1 now supports .NET 4.5 package, thus resolving the TLS 1.1/1.2 issue over Hyper Text Transfer Protocol Secure (HTTPS) connections.
H	SASNOI-2721	**Summary:** The support for Microsoft Credential Provider Tile Version 2 ensures that third-party password reset tools now displays password reset text link while the SafeNet Agent for Windows Logon is enabled and working.

Release Summary – SafeNet Agent for Windows Logon 2.0

The SafeNet Agent for Windows Logon 2.0 introduces new features and repairs several customer-reported defects.

Push Authentication

The SafeNet Agent for Windows Logon 2.0 supports Push OTP when working with MobilePASS+.

> **NOTE:** Push Authentication is supported when working with STA Edition. For SAS PCE/SPE, Push Authentication is only supported with version 3.9.1 (and onwards).

ADMX Support

The SafeNet Agent for Windows Logon 2.0 supports the use of ADMX files for defining the Administrative Template policy settings in the Windows Group Policy tools.

Active Directory Search

Performance of the Active Directory Search feature has been enhanced.

Proxy Server Settings

Proxy server settings can now be configured in the Configuration Management interface.

Gemalto Branding

The SafeNet Agent for Windows Logon Management user interface has been redesigned with Gemalto branding.

Resolved Issues

This release resolves some known issues. Please find below details of the solutions provided.

Severity	Issue	Synopsis
H	SASNOI-2882	**Summary:** The SafeNet Agent for Windows Logon now supports TLS 1.1/1.2 on Windows 7 with the agent configured without TVP.
H	SASNOI-3132	**Summary:** Windows password is now validated correctly in Windows 10 Spanish.
H	SASNOI-2963	**Summary:** The Exempt Administrator feature now functions as expected.
M	SASNOI-2892	**Summary:** Windows 10 now remembers the previous user name.
H	SASNOI-2907	**Summary:** Performance has been greatly enhanced when logging on with the SafeNet Agent for Windows Logon.
H	SASNOI-3113	**Summary:** Performance has been greatly enhanced when logging on with the SafeNet Agent for Windows Logon.
H	SASNOI-2896	**Summary:** In Windows 8 the Switch User option is now supported.
M	SASNOI-2897	**Summary:** The GrIDsure logon grid is now displayed at an appropriate size and with a high visual quality.
M	SASNOI-3122	**Summary:** The failover setting (selected or not selected) configured during the installation process is now applied correctly in the Configuration Management window following installation.
M	SASNOI-2978	**Summary:** The Windows Group Policy security settings option **Do not display last user name** now functions correctly.

Advisory Notes

Proxy Settings Following Upgrade

If proxy was activated in the SafeNet Agent for Windows Logon 1.13, to continue working with proxy following upgrade to version 2.0, go to **Configuration Management > Communications > Proxy Settings**, enter the credentials (username and password) and click **Apply**.

Known Issues

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

Severity	Issue	Synopsis
H	SASNOI-22272	**Summary:** On uninstalling the agent via control panel, an intermittent **Error 1306** is displayed. **Workaround:** Restart the machine. It will be fixed in a future release.
M	SASNOI-22305	**Summary:** Modify option in the installer does not work as expected and authentication fails. **Workaround:** Either re-upload the bsid key file in the management console or uninstall and install the agent.
M	SASNOI-22357	**Summary:** AD user authentication with the username format "Domain\username@domain" fails and an offline access error "For offline access, please contact your administrator. Ignore this message if offline access is not needed" displays. **Workaround:** None. It will be fixed in a future release.
M	SASNOI-22369	**Summary:** On performing the credUI operations, such as, outgoing RDP or accessing an application as run as different user in offline mode, the remaining offline authentication count does not decrement on the login screen. **Workaround:** None. It will be fixed in a future release.
H	SASNOI-22331	**Summary:** WLA fails to authenticate a AD user whose UPN username contains the special characters **/ | = + * ? < >** and displays an error. **Workaround:** None. It will be fixed in a future release. For now, the supported characters for UPN username are **a-z,A-Z,0-9,.,-,_,$,%,&,#,~,`,!,^,(,),{,},'**
M	SASNOI-21384	**Summary:** The placeholder text for the **Username** and **Passcode** fields remains in English, despite the application being configured for a different language. **Workaround:** None. It will be fixed in a future release.
M	SASNOI-20077	**Summary:** [Legacy] In Windows 11, if a user attempts to launch an application via "Run as different user", then the user is not prompted for 2FA. **Workaround:** None. It will be fixed in a future release.
H	SASNOI-19527	**Summary:** Offline authentication does not work after the agent upgrade from v3.4.x. **Workaround:** The end-users need to perform at least one successful online authentication for subsequent offline login attempts.
H	SASNOI-8630	**Summary:** It is not possible to enforce SafeNet authentication on nested groups over an external domain. **Workaround:** None, will be fixed in a future release.
H	SASNOI-2825	**Summary:** In Windows 8, 10, Server 2012 and Server 2012 R2, the **Autoadminlogon** feature does not function. **Workaround:** None, will be fixed in a future release.

Severity	Issue	Synopsis
M	SASNOI-3323	**Summary:** Hybrid Mode is not supported when a Local User is included in a Domain Group. **Workaround:** None, will be fixed in a future release.

Compatibility and Upgrade Information

Prerequisites

- Microsoft .NET 4.8 and above

Supported Upgrade Version

The Document Subject v4.1.2 supports upgrade from v3.4.x (and above).

> **NOTE:** For consistent behavior, we highly recommend you to upgrade the agent in online mode or when STA is available.

Supported SAS/STA Releases

- SAS PCE/SPE 3.9.1 and later
- SafeNet Trusted Access (STA) Edition

> **NOTE:** Push Authentication is supported when working with STA Edition. For SAS PCE/SPE, Push Authentication is only supported with version 3.9.1 (and onwards).

Supported Operating Systems

- Windows 10
- Windows 11
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Product Documentation

The following product documentation is associated with this release:

- *SafeNet Agent for Windows Logon 4.1.2: Installation and Configuration Guide*

> **NOTE:** Perform installation and migration in **Run as Administrator** mode.

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 before contacting support. If you cannot resolve the issue, contact your supplier or Thales Group Customer Support.

Thales Group 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 Group 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 a 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 Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales Group Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

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