



# SafeNet Authentication Service Agent for Windows Logon

## CUSTOMER RELEASE NOTES

**Version:** 1.13  
**Build:** 549  
**Issue Date:** 7 March 2016  
**Document Part Number:** 007-012564-001, Rev. H

### Contents

Product Description.....	2
Release Description.....	2
New Features and Enhancements.....	2
Security Enhancements .....	2
Support for Windows 10.....	2
Advisory Notes.....	2
Upgrade Not Supported .....	2
Realm Stripping Settings.....	3
Offline Functionality after Migration.....	3
Localization Not Supported .....	4
RDP with Administrator Account .....	4
Resolved and Known Issues.....	4
Resolved Issues.....	4
Known Issues.....	5
Compatibility and Upgrade Information.....	6
Prerequisites .....	6
SafeNet Authentication Service.....	6
Operating Systems Supported by SAS Agent for Windows Logon 1.13 .....	6
Installation.....	7
Migration from SAS Agent for Windows Logon 1.11/1.12 to version 1.13.....	7
Product Documentation .....	9
Support Contacts .....	9

## Product Description

---

The SafeNet Authentication Service (SAS) Agent for Windows Logon is a two-factor authentication 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 two-factor authentication when accessing network resources, in place of traditional static passwords, is a necessary measure for information security.

## Release Description

---

SAS Agent for Windows Logon 1.13 repairs several customer-reported defects, enhances security, and introduces new features.

## New Features and Enhancements

---

### Security Enhancements

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

### Support for Windows 10

Windows 10 has been added to the list of supported operating systems.

## Advisory Notes

---

### Upgrade Not Supported

SAS Agent for Windows Logon 1.13 does not support upgrade from earlier versions. Instead, the configuration from the older version must be saved, using the Configuration Export/Import Utility (WLAAgentConfigUtility.exe), and then imported into the new installation.

See “Migration from SAS Agent for Windows Logon 1.11/1.12 to version 1.13” on page 7.

For versions of SAS Agent for Windows Logon earlier than 1.11, neither upgrade nor migration to version 1.13 is supported.



**NOTE:** For versions of SAS Agent for Windows Logon earlier than 1.11, neither upgrade nor migration to version 1.13 is supported.

---

## Realm Stripping Settings

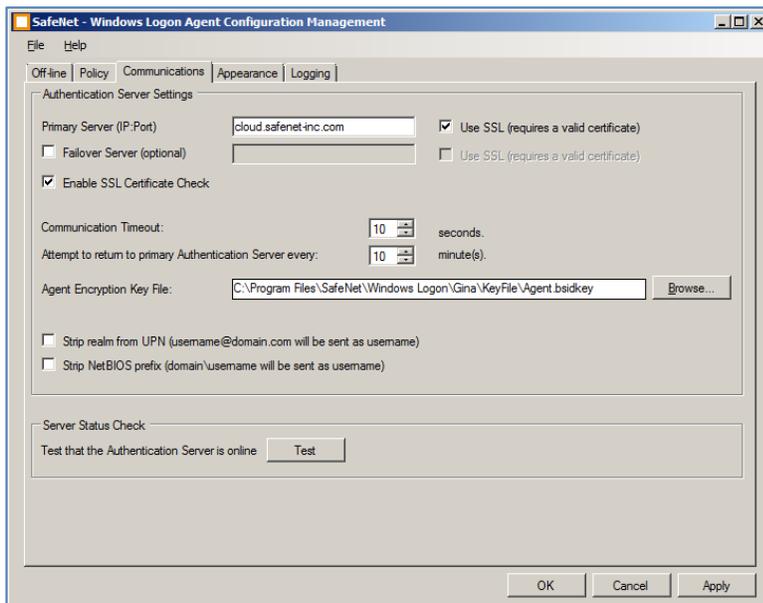
To work with a short SAS username format (for example, bill instead of Domain\bill or [bill@domain.com](mailto:bill@domain.com)), after installation, activate the strip function in the in the **SafeNet – Windows Logon Agent Configuration Management > Communications** tab.



**NOTE:** Alternatively, the realm-stripping feature can be configured in the **SafeNet Authentication Service, Auth Node Module**. For details, see the *SafeNet Authentication Service, Service Provider Administrator Guide*.

To select the strip function in SAS Agent for Windows Logon:

1. From the **SafeNet – Windows Logon Agent Configuration Management** window, select the **Communications** tab.



2. Select one or both of the following and click **OK**:
  - **Strip realm from UPN (username@domain.com will be sent as username):** Select if the SAS username is required without the suffix **@domain**.
  - **Strip NetBIOS prefix (domain\username will be sent as username):** Select if the SAS username is required without the prefix **domain\**.



**NOTE:** The realm-stripping feature applies to SAS usernames only. Active Directory usernames are not affected.

## Offline Functionality after Migration

After successful migration to SAS Agent for Windows Logon 1.13, to work offline (with offline OTPs) you must log in through SAS (for example, using online OTP) or manually replenish offline OTPs (admin functionality). Previously replenished OTPs will be removed following migration.

## Localization Not Supported

Localization is not supported in SAS Agent for Windows Logon 1.12 or 1.13, and the localization tab does not appear in the **SafeNet – Windows Logon Agent Configuration Management** window.

The localization tab is present in SAS Agent for Windows Logon 1.11, but the localization settings are not migrated to version 1.13.

## RDP with Administrator Account

On a host computer, where organizational IT policies determine that there are no access permissions for Domain Administrators via RDP, the Fast User Switch must be disabled.

**To disable the Fast User Switch on the host computer:**

1. In Windows registry, navigate to **HKEY\_LOCAL\_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Policies \ System**
2. Create a DWORD (32-bit) Value named **HideFastUserSwitching**.
3. Set the Value data for **HideFastUserSwitching** to 1.



**NOTE:** Logging onto the host computer with a different user must be done during the RDP connection initiation.

## Resolved and Known Issues

### Resolved Issues

Issue	Synopsis
SASIL-2347	Grid authentication now operates correctly when working on Windows 10.
SASIL-2173	When customizing SAS Agent for Windows Logon with a custom logo, the SafeNet or CryptoCard logo no longer overlays the customer's logo.
SASIL-2171	The SAS Agent for Windows Logon logo can now be customized correctly.
SASIL-2084	After installing SAS Agent for Windows Logon on Windows Server 2008 R2 with XenApp 6.5, the local drives are now visible to the user.
SASIL-2065	When locking the Windows user session (Windows Logo Key+L), the logo (Gemalto or custom) is now displayed.
SASIL-2055	When changing the Windows password, by pressing Ctrl+Alt+Delete and selecting Change Windows Password, the following erroneous message is no longer displayed: "If you normally use a Token, Please enter your PIN + OTP otherwise your Windows Password in Password field."
SASIL-2016	When installing or running a program as Administrator, the agent no longer suppresses the User Account Control (UAC), nor causes consent.exe to run in the background, consuming many computer resources.
SASIL-2008	The <i>SAS Agent for Windows Logon Configuration Guide</i> has been updated to remove the Localization tab, which is no longer included in the SafeNet-Windows Logon Agent Management window.

## Known Issues

Issue	Synopsis
SASIL-2616	<p><b>Summary:</b> When accessing the Outlook Web APP (OWA) console, the user is prompted for an OTP password, even though the Active Directory (AD) password is required.</p> <p><b>Workaround:</b> Does not affect functionality. Enter the AD logon credentials. Will be fixed in a future release.</p>
SASIL-2421	<p><b>Summary:</b> Following installation, even though a secondary server is not included, in the <b>Communications</b> tab &gt; <b>Authentication Server Settings</b>, the <b>Failover Server</b> field is automatically populated with <b>Localhost</b></p> <p><b>Workaround:</b> Uncheck <b>Failover Server</b>.</p>
SASIL-2296	<p><b>Summary:</b> When logging on to SAS Agent for Windows Logon, the user is prompted for a token. This is incorrect as the AD password is required. In addition, the screen shows the SafeNet Authentication Service (SAS) logo, which is not appropriate for the Active Directory (AD) logon.</p> <p><b>Workaround:</b> Does not affect functionality. Enter the AD logon credentials. Will be fixed in a future release.</p>
SASIL-2177	<p><b>Summary:</b> Sometimes, SAS Agent for Windows Logon takes a long time (more than ten seconds) to search through the groups in Active Directory (AD).</p> <p><b>Workaround:</b> None. Will be fixed in a future release.</p>
SASIL-2100	<p><b>Summary:</b> Sometimes, when using SAS Agent for Windows Logon with SAS Cloud, with the SafeNet Token Proxy Validator Agent deployed at the customer's premises, the login process is slow.</p> <p><b>Workaround:</b> None. Will be fixed in a future release.</p>
SASIL-1990	<p><b>Summary:</b> The Windows Group Policy security settings option "Do not display last user name" does not work.</p> <p><b>Workaround:</b> None. Will be fixed in a future release.</p>
SASIL-1170	<p><b>Summary:</b> The Windows 2008 login screen does not refresh to show the correct domain.</p> <p><b>Workaround:</b> None. Will be fixed in a future release.</p>
SASIL-712	<p><b>Summary:</b> SAS Agent for Windows Logon prompts for the PIN, not the full OTP, on computers with a SafeNet software token installed. An option to change this behavior is not supported.</p> <p><b>Workaround:</b> None. Prompting for PIN-only is the expected behavior. However, for organizations that wish to use the full OTP, support for this configuration will be included in a future release of SAS Agent for Windows Logon.</p>
SASIL-693	<p><b>Summary:</b> SAS Agent for Windows Logon sometimes fails to enforce OTP bypass on a domain-level Administrator nested within a Local Administrator Group.</p> <p><b>Workaround:</b> None. Will be fixed in a future release.</p>
SASIL-692	<p><b>Summary:</b> When the user locks their session, a message prompts the user that only the administrator or a different user (not currently logged on) can unlock the session.</p> <p><b>Workaround:</b> Ignore. The user can log on successfully, despite the message.</p>

Issue	Synopsis
SASIL-531	<p><b>Summary:</b> The user must log in at least once before the administrator can replenish offline OTPs for the user. If the user has not logged in, an “Unknown User” message is displayed.</p> <p><b>Workaround:</b> The user must log in at least once before performing replenishment.</p>
SASIL-138	<p><b>Summary:</b> SAS Agent for Windows Logon does not operate when the Microsoft Threat Management Gateway (TMG) web proxy is in use.</p> <p><b>Workaround:</b> None. Will be fixed in a future release.</p>

## Compatibility and Upgrade Information

### Prerequisites

- Microsoft .Net 3.5
- Microsoft GDI+ VC User gdi Plus RTL x86
- MSXML 6.0 SP1

### SafeNet Authentication Service

- SafeNet Authentication Service PCE/SPE 3.3.2 and later
- SafeNet Authentication Service Cloud

### Operating Systems Supported by SAS Agent for Windows Logon 1.13



**NOTE:** SAS Agent for Windows Logon 1.13 does not support Windows XP or Windows Server 2003. For these operating systems, use SAS Agent for Windows Logon 1.12.

- Windows Vista SP2 (32-bit, 64-bit)
- Windows 7 (32-bit, 64-bit)
- Windows Server 2008 (32-bit)
- Windows Server 2008 R2 (64-bit)
- Windows 8 (32-bit, 64-bit)
- Windows 8.1 (32-bit, 64-bit)
- Windows Server 2012 (64-bit)
- Windows Server 2012 R2 (64-bit)
- Windows 10 (32-bit, 64-bit)

## Installation

For installation details, see the *SAS Agent for Windows Logon Configuration Guide*.



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

---

## Migration from SAS Agent for Windows Logon 1.11/1.12 to version 1.13

Automatic upgrade to SAS Agent for Windows Logon 1.13 from versions 1.11 and 1.12 is not supported. Instead, the configuration from the older version must be saved, using the Configuration Export/Import Utility (WLAAgentConfigUtility.exe), and then imported into the new installation.



**NOTE:** The Configuration Export/Import Utility, and the installation process, must be run in **Run as Administrator** mode.

---

The utility is used to export the registry parameter settings from the currently installed version (1.11 or 1.12). These settings are then imported into SAS Agent for Windows Logon 1.13.



**NOTE:** The Configuration Export/Import Utility (WLAAgentConfigUtility.exe) must be run separately on each computer where SAS Agent for Windows Logon 1.13 is being installed with settings imported from an earlier version.

---

1. Place the Configuration Export/Import Utility (**WLAAgentConfigUtility.exe**) in a temporary location, to where the backup file will be exported.
2. From the command line, run the export command **-e**  
For example:  
**C:\tempWLABackup>WLAAgentConfigUtility.exe -e**  
The settings are saved to the **WLAConfig.xml** file.
3. Make a copy of **C:\tempWLABackup** including folder contents and save in a different location for later use.
4. Uninstall SAS Agent for Windows Logon (1.11 or 1.12).
5. Manually delete the remnants of the agent installation folder.
6. Install SAS Agent for Windows Logon 1.13.
7. Place the Configuration Export/Import Utility (**WLAAgentConfigUtility.exe**) in the folder where the backup file (**WLAConfig.xml**) is located, for example **C:\tempWLABackup**.
8. From the command line, run the import command **-i**  
For example:  
**C:\tempWLABackup>WLAAgentConfigUtility.exe -i**
9. Reboot the computer.

## Registry Parameters Backup

SAS Agent for Windows Logon settings are placed in the OS registry under **HKEY\_LOCAL\_MACHINE\SOFTWARE\CRYPTOCARD** as follows:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\CRYPTOCARD\AuthGINA**

**HKEY\_LOCAL\_MACHINE\SOFTWARE\CRYPTOCARD\AuthGINA\Users**

The Configuration Export/Import Utility (WLAAgentConfigUtility.exe) backs up registry settings to the **WLACONFIG.XML** file. By default, the backup files are created in the current working directory. However, this can be controlled by a command line by supplying additional optional parameters, including the full path to the backup filename.

## Backup Resource files

After export is performed, the directory containing the Configuration Export/Import Utility (WLAAgentConfigUtility.exe) contains the following files:

**agent.dsidkey**

**authgina.ini**

**authotp.ini**

**LogonClient.ccl**

**softTokenMessages.ccl**

**WLACONFIG.XML**

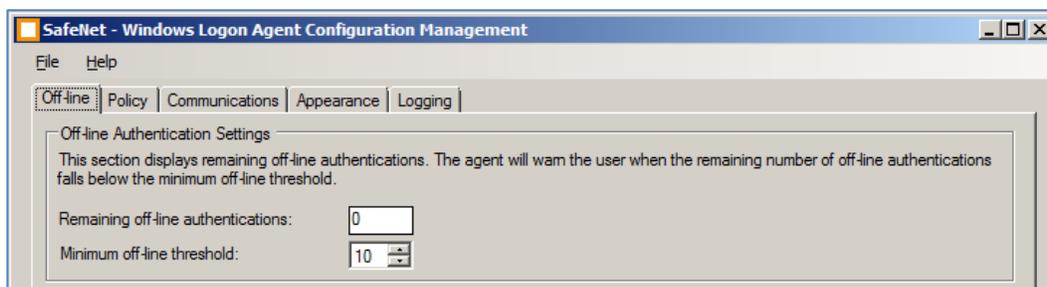
## Migration Limitation - Minimum Off-Line Threshold

**Minimum offline threshold** determines when the maximum number of off-line authentications permitted. When this number is reached, SAS Agent for Windows Logon sends a warning message to the user to authenticate against SAS or to perform a manual replenishment.

When migrating the settings from SAS Agent for Windows Logon 1.11 to version 1.13, the **Minimum off-line threshold** setting is not migrated, but will be set at the default value of 10. To change this value, configure the setting manually after migration.

**To set the Minimum off-line threshold manually:**

1. In the **SafeNet–Windows Logon Agent Configuration Management** window, open the **Off-line** tab.



2. In the **Minimum Off-line threshold** field, set to the required number to between 5 and 99. The default is 10.

# Product Documentation

---

The following documentation is available:

- *SafeNet Authentication Service Agent for Windows Logon Configuration Guide*  
(PN: 007-012394-002)
- *SafeNet Authentication Service Agent for Windows Logon Frequently Asked Questions*  
(PN: 007-013453-001)

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 make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto 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 Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	<a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a> Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	