All information herein is either public information or is the property of and owned solely by SafeNet Inc. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of SafeNet’s information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, SafeNet makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, SafeNet reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

SafeNet hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall SafeNet be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

SafeNet does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. In no event shall SafeNet be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating SafeNet products. SafeNet disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2016 SafeNet. All rights reserved. SafeNet and the SafeNet logo are trademarks and service marks of SafeNet N.V. and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

**Product Version:** 1.13

**Document Part Number:** 007-012394-002, Rev. D

**Release Date:** 7 March 2016
Contents

Audience ......................................................................................................................................................... 5
Related Documents........................................................................................................................................ 5
Support Contacts......................................................................................................................................... 6

1 CHAPTER 1 ................................................................................................................................................. 7
2 Overview ................................................................................................................................................... 7
   Environment................................................................................................................................................ 7
   SafeNet Authentication Service Windows Logon – Domain Authentication ............................................ 8
   SafeNet Authentication Service Windows Logon – Workgroup Authentication ....................................... 9
   SafeNet Authentication Service Windows Logon – Offline Authentication ............................................ 10
   Modes of Operation .................................................................................................................................. 11
   Offline Authentication .............................................................................................................................. 11

3 CHAPTER 2 ................................................................................................................................................. 12
4 Installation and Migration ......................................................................................................................... 12
   Prerequisites ............................................................................................................................................ 12
   Installing SAS Agent for Windows Logon ................................................................................................. 12
   Silent Installation ...................................................................................................................................... 17
   Realm Stripping Settings ............................................................................................................................ 18
   Upgrade Not Supported .............................................................................................................................. 18
   Migration from SAS Agent for Windows Logon 1.11/1.12 to version 1.13 ............................................... 18
      Registry Parameters Backup ............................................................................................................ 19
      Backup Resource files ......................................................................................................................... 19
      Migration Limitation - Minimum Off-Line Threshold ........................................................................ 20
   RDP with Administrator Account ............................................................................................................ 20

5 CHAPTER 3 ................................................................................................................................................. 21
6 Configuration .............................................................................................................................................. 21
   SAS Agent for Windows Logon Configuration Management ....................................................................... 21
   Offline Tab ............................................................................................................................................ 22
      Offline Authentication Settings ........................................................................................................... 22
      Manually Replenish ............................................................................................................................... 23
      Authentication Test ............................................................................................................................... 23
   Policy Tab ............................................................................................................................................... 24
      Authentication Processing ....................................................................................................................... 24
      Credential Tile Filter .............................................................................................................................. 25
      Group Authentication Exceptions .......................................................................................................... 26
   Communications Tab .............................................................................................................................. 27
      Authentication Server Settings ............................................................................................................ 27
Contents

Appearance Tab ........................................................................................................................................... 29
Logging Tab ........................................................................................................................................... 30
  Logging Level ................................................................................................................................... 30
  Log File Location ............................................................................................................................. 30

7  CHAPTER 4 ........................................................................................................................................ 31

8  Advanced Configuration ........................................................................................................... 31
  Remote Users with a Depleted Offline Authentication Store ............................................................ 31
  Remote Users Who Have Lost or Forgotten their Token ................................................................. 31
  Refining Administrator Group Exclusions ...................................................................................... 32
  Configuring Num Lock Settings ...................................................................................................... 32
Preface

Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure.

All products manufactured and distributed by SafeNet, Inc. are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

Related Documents

The following documents contain related information:

- SafeNet Authentication Service Agent for Windows Logon Customer Release Notes (PN: 007-012564-001)
- SafeNet Authentication Service Agent for Windows Logon Frequently Asked Questions (PN: 007-013453-001)
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.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
</table>
| Address             | Gemalto, Inc.  
4690 Millennium Drive  
Belcamp, Maryland 21017, USA                   |
| Phone               | US  1-800-545-6608  
International 1-410-931-7520            |
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. |
CHAPTER 1: Overview

Overview

The SafeNet Authentication Service Agent for Windows Logon is designed to help Microsoft enterprise customers ensure that valuable resources are accessible only by authorized users. It delivers a simplified and consistent user login experience, virtually eliminates help desk calls related to password management, and helps organizations comply with regulatory requirements.

The use of two-factor authentication instead of just traditional static passwords to access a Windows environment is a necessary critical step for information security.

Environment

<table>
<thead>
<tr>
<th>Environment</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Windows Versions</td>
<td><strong>NOTE:</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>• Windows Vista SP2 (32-bit, 64-bit)</td>
</tr>
<tr>
<td></td>
<td>• Windows 7 (32-bit, 64-bit)</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 (32-bit)</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>• Windows 8 (32-bit, 64-bit)</td>
</tr>
<tr>
<td></td>
<td>• Windows 8.1 (32-bit, 64-bit)</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>• Windows 10 (32-bit, 64-bit)</td>
</tr>
<tr>
<td>Additional Software Prerequisites</td>
<td>• Microsoft .Net 3.5</td>
</tr>
<tr>
<td></td>
<td>• Microsoft GDI+ VC User gdi Plus RTL x86</td>
</tr>
<tr>
<td></td>
<td>• MSXML 6.0 SP1</td>
</tr>
<tr>
<td>Supported Networking Environments</td>
<td>• Microsoft Domain</td>
</tr>
<tr>
<td>Supported Architecture</td>
<td>• 32-bit</td>
</tr>
<tr>
<td></td>
<td>• 64-bit</td>
</tr>
</tbody>
</table>
Environment | Description
---|---
**Network** | - TCP Port 80 or 443

**Supported Tokens** | All tokens supported by SafeNet Authentication Server.

**Unsupported Tokens** | 4.x legacy, 5.x legacy, 6.x legacy, UB, IronKey, SafeStick, Smart Cards.

**Note:** Microsoft CBA Login is not supported by the agent, but it can run in parallel.

**Unsupported Tokens in Offline Authentication Mode** | Challenge-response-enabled tokens, SMS, Gridsure, and time-based tokens

---

**SafeNet Authentication Service Windows Logon – Domain Authentication**

**Windows Logon Agent – Domain Authentication**

1. The user is presented with a SafeNet Authentication Service Windows Logon prompt, and then clicks **Ctrl+Alt+Del**.
2. The user enters their user name, OTP, and, if applicable, the logon domain. If the user is part of a domain group authentication exception, the credentials are passed to Active Directory; otherwise, the user name and OTP are sent to SafeNet Authentication Service for verification.
3. If the SafeNet Authentication Service credentials are valid, the user is prompted for their Microsoft password. If **Microsoft Password Caching** mode is enabled, the user is prompted for the Microsoft password only the first time they log on. Subsequently, the SafeNet Authentication Service Windows Logon agent will cache the Microsoft Windows password, furnishing it as required.
4. If the Microsoft password is valid, the user is logged on to the workstation.
SafeNet Authentication Service Windows Logon – Workgroup Authentication

1. The user is presented with a SafeNet Authentication Service Windows Logon prompt, and then clicks Ctrl+Alt+Del.
2. The user enters their user name and OTP. If the user is part of a local group authentication exception, the credentials are passed to the local workstation; otherwise, the user name and OTP are sent to SafeNet Authentication Service for verification.
3. If the SafeNet Authentication Service credentials are valid, the user is prompted for their Microsoft password. If Microsoft Password Caching mode is enabled, the user is prompted for their Microsoft password only the first time they log on. Subsequently, the SafeNet Authentication Service Windows Logon agent will cache the Microsoft Windows password, furnishing it as required.
4. If the Microsoft password is valid, the user is logged on to the workstation.
SafeNet Authentication Service Windows Logon – Offline Authentication

Windows Logon Agent – Offline Authentication

1. The offline user is presented with a SafeNet Authentication Service Windows Logon prompt, at which they click Ctrl+Alt+Del.

   **NOTE:** To use offline authentication, the user must log on at least once online. When the user logs on online, offline data is replenished. While online, the user can top up or replenish the account anytime using the management tool. Management tools also show the number of offline authentications available and the warning threshold the user can set for the replenishment reminder.

2. The offline user enters their user name, OTP and, if applicable, the logon domain. If the offline user is part of a local group authentication exception, the credentials are passed to the local workstation; otherwise, the user name and OTP are verified by the offline authentication one-time password store on the local workstation.

3. If the SafeNet Authentication Service credentials are valid, the user is prompted for their Microsoft password. If Microsoft Password Caching mode is enabled, the user is prompted for the Microsoft password only the first time they log on. Subsequently, the SafeNet Authentication Service Windows Logon Agent will cache the Microsoft Windows password, furnishing it as required.

4. If the Microsoft password is valid, the user is logged on to the workstation.
Modes of Operation

There are two modes of operation for the SAS Agent for Windows Logon. The mode of operation is selected during installation but, if required, can be modified afterwards. The modes of operation are:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dual Password Mode</td>
<td>In <strong>Dual Password</strong> mode, each user authenticates with a token-generated one-time password and then logs on with their Microsoft password. The user is prompted for the Microsoft password every time they log on.</td>
</tr>
<tr>
<td>Microsoft Password Caching Mode</td>
<td>In <strong>Microsoft Password Caching</strong> mode, each user authenticates with a token-generated one-time password and then logs on with their Microsoft password. The user is prompted for the Microsoft password only the first time they log on. Subsequently, the SafeNet Authentication Service Windows Logon agent will cache the Microsoft Windows password, furnishing it as required. However, the user will be prompted to supply a new password if/when Active Directory or the local workstation enforces a password change policy.</td>
</tr>
</tbody>
</table>

Offline Authentication

By default, SafeNet Authentication Service supports offline authentication; that is, the facility for a user to log on with a SafeNet one-time password when there is no connection to SAS. For details about disabling offline authentication, see the **SafeNet Authentication Service Administrator’s Guide**.

The SafeNet Authentication Service Windows Logon Agent permits end-user workstations that may be offline periodically to authenticate. The normal SafeNet Authentication Service Windows Logon Agent authentication process requires that the user furnish a token-generated one-time password for transmission to the SafeNet Authentication Service. When offline, there is no communication with the SafeNet Authentication Service, only the local SafeNet Authentication Service Windows Logon Agent. However, two-factor authentication is preserved; the user must have the token and must know a PIN.

Offline authentication is supported in both SafeNet Authentication Service Windows logon modes of operation (**Dual Password** and **Microsoft Password Caching**) with any account using the supported token types.

The token can be enabled (for example, using one-time passwords for logon) or disabled (for example, using a SAS static password for logon). However, offline authentication logon can only be done if the last logon before disconnecting from the network was done with a one-time password. The same applies if the user has been configured to use a SAS static password.
CHAPTER 2
Installation and Migration

Prerequisites

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

- Ensure that TCP port 80 or 443 is open between the SAS Agent for Windows Logon and SAS Server.
- Administrative rights to the Windows system are required during installation of the SAS Windows Logon Agent.
- The following must be installed before installation:
  - Microsoft .Net 3.5
  - Microsoft GDI+ VC User gdi Plus RTL x86
  - MSXML 6.0 SP1.Net 2.0 and MSXML 6 if not already present.

Installing SAS Agent for Windows Logon

1. Locate and run one of the SafeNet Authentication Service installers below as applicable:
   - SafeNet Authentication Service Windows Logon Agent for Vista-2008-7 x64.exe (64-bit)
   - SafeNet Authentication Service Windows Logon Agent for Windows 8-10.exe (Windows 8 and later 32-bit)
   - SafeNet Authentication Service Windows Logon Agent for Windows 8-10 x64.exe (Windows 8 and later 64-bit)
2. On the **Welcome** window, click **Next**.

3. On the **License Agreement** window, select **I accept the terms in the license agreement** and then click **Next**.
4. On the **Customer Information** window, complete the **User Name** and **Organization** boxes as appropriate, and then click **Next**.

5. On the **Destination Folder** window, click **Next** to select the default installation destination folder, or click **Change** to browse to and select a different destination folder. Click **Next** to continue.
6. On the **Authentication Service Setup** window, provide the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Location</strong></td>
<td>Enter the hostname or IP address of the primary SafeNet Authentication Service server.</td>
</tr>
<tr>
<td><strong>Connect using SSL (HTTPS)</strong></td>
<td>Select this option if SAS has been configured to accept incoming SSL connections.</td>
</tr>
<tr>
<td><strong>Specify failover SAS Authentication Server</strong></td>
<td>Select this check box if a failover SAS is being used. If selected, you must also complete the <strong>Location</strong> field.</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>Enter the hostname or IP address of the failover SAS server.</td>
</tr>
<tr>
<td><strong>Connect using SSL (HTTPS)</strong></td>
<td>Select this option if the failover SAS server has been configured to accept incoming SSL connections.</td>
</tr>
</tbody>
</table>

![Authentication Service Setup](image)

7. On the **Windows Logon Setup** window, provide the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Exempt Local and Domain Administrator groups from SafeNet Authentication Service Authentication</strong></td>
<td>Select this option to allow administrators to log on without providing SafeNet credentials.</td>
</tr>
<tr>
<td><strong>Logon Mode</strong></td>
<td>Select one of the following logon modes:</td>
</tr>
<tr>
<td></td>
<td>- Users will enter both SAS and Windows credentials with each logon</td>
</tr>
<tr>
<td></td>
<td>- SAS will cache Windows passwords after the first use</td>
</tr>
<tr>
<td><strong>Display an option for users to logon with GrIDsure tokens</strong></td>
<td>Select this option if required.</td>
</tr>
</tbody>
</table>
8. Click **Next**.

9. On the **Ready to Install the Program** window, click **Install**.

---

SafeNet Authentication Service Agent for Windows Logon 1.13: Configuration Guide
Document PN: 007-012394-002, Rev. D. Copyright © 2016 SafeNet, Inc., All rights reserved.
10. When the installation process is completed, the **Installshield Wizard Completed** window is displayed. Click Finish.

![Installshield Wizard Completed]

**Silent Installation**

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

A SafeNet Authentication Service Windows Logon **msi** installation package can be launched from the command line. The **msi** files have the same prefixes as the SAS installer **exe** files.

```
msiexec /i "SafeNet Authentication Service Windows Logon Agent for Windows 8 x64.msi" /quiet
```

To set options, the property name is used in name value pairs with spaces in between each pair.

For example, to set the Primary SafeNet Authentication Service to **192.168.10.200** with SSL and enabled Microsoft **Password Caching** mode, you would run the following command:

```
msiexec /i "SafeNet Authentication Service Windows Logon Agent for Windows 8 x64.msi" /quiet
TOKENVALIDATORLOCATION=192.168.10.200 USESSL=s LOGONMODE=1
```
Realm Stripping Settings

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

See “Communications Tab” on page 27.

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

Upgrade Not Supported

SAS Agent for Windows Logon 1.13 does not support upgrade from earlier versions (1.11/1.12). Instead, the configuration must be migrated from the earlier version.

See the next section “Migration from SAS Agent for Windows Logon 1.11/1.12 to version 1.13” on page 18.

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

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

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.

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.


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.

For information about setting the Minimum off-line threshold, see “Offline Authentication Settings” on page 22.

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.
CHAPTER 3: Configuration

SAS Agent for Windows Logon Configuration Management

Use the SAS Agent for Windows Logon Configuration Management Tool to configure the various options available within the agent.

The Offline, Policy, Communications, Appearance, and Logging tabs are available only to users who are part of the Local Administrators and Domain Administrators groups. All other groups will see only the Offline tab.

NOTES:

- To use all features of the Configuration Manager you must be working in Run as Administrator mode.
- When working in User mode, the user can access the Offline tab only.
- To use the Configuration Manager you must be working in Run as Administrator mode.
- The Configuration Management Tool cannot be opened by a domain administrator from a trusted domain using administrator rights.
Offline Tab

The Offline tab deals primarily with end-user offline authentication settings. It displays the current amount of offline authentication attempts, allows for the customization of the minimum warning notification threshold, the ability to replenish manually the offline one-time password store, and to test authentication requests against SAS.

Offline Authentication Settings

The SAS Agent for Windows Logon allows users to log in to their workstations when SAS is not available.

- **Remaining offline authentications**: The amount of SafeNet authentications available before the user must authenticate against SAS or perform a manual replenish. The offline authentications value is a global configuration setting configured within the **Policy Admin, Authentication Policy** section of the SAS Manager. The default value is **100**.

- **Minimum offline threshold**: The user will see a warning to authenticate against SAS or perform a manual replenish if this value is reached. The value may be between **5** and **99**. The default value is **10**.
Manually Replenish

NOTE: The User Name format needs to be the same as defined for use in the SAS Server.

The offline store is automatically replenished when a user returns and logs in to the corporate network, but if the offline store expires while the user is still at a remote location, the Manually Replenish option allows a user to refill their offline authentication store remotely.

To replenish an offline authentication store manually:

1. Establish a VPN connection to the corporate network.
2. Open the SAS Agent for Windows Logon Configuration Tool.
3. Enter your SafeNet credentials into the Passcode field, and then click Connect.
4. The SAS Agent for Windows Logon contacts SAS to verify the logon credentials. If the credentials are valid, the offline authentication is restored; otherwise, the user will receive a warning message to retry the authentication attempt.

Authentication Test

This allows administrators to test authentication between the agent and SAS.

NOTE: The User Name format needs to be the same as defined for use in the SAS Server.
Policy Tab

The Policy tab allows SafeNet authentication exclusions to be applied to the SAS Agent for Windows Logon.

![Policy Tab Image]

Authentication Processing

Authentication Processing is the process of authenticating information received from authentication sources.

- **Enable Agent**: This option turns the SAS Agent for Windows Logon on or off. The default setting is Enabled.

- **Enable Emergency Password**: This option turns the emergency password feature on or off. The default setting is Enabled. This feature is an authentication method that allows an administrator to authenticate to a user’s computer as the user without entering a SafeNet one-time password. This only applies under two conditions:
  - The emergency password is enabled and the offline authentication store is empty.
  - The emergency password is enabled and the Windows system is unable to communicate with the SafeNet Authentication Service at the time of authentication.

Each user will have a unique emergency password, which is set on the Secured Users tab of the SAS Manager. The emergency password can be used until the workstation regains contact with SAS, at which point it will be randomized.
• **Enable Local/Domain Administrator strong authentication exemption:** This option allows the Local and Domain Administrator groups to be exempt from SafeNet authentication during login. The default value is determined during installation of the agent.

• **Enable Microsoft password caching:** This option enables or disables Microsoft Password Caching mode.

• **Enable GrIDsure Tokens (2008, Vista and Windows 7 only):** This option enables or disables the Use GrIDsure Token option displayed in the Windows Logon dialog prompts. This is required if users have been assigned GrIDsure tokens.

• **Allow outgoing RDP Connection without OTP:** Enables SAS authentication to be bypassed when making an RDP connection.

  **NOTE:** The Allow outgoing RDP Connection without OTP feature is not effective if the Microsoft parameter enablecredsspsupport:i:0 that controls credentials usage on OS level for RDP is set to null.

**Credential Tile Filter**

The **Credential Tile Filter** assesses whether a list of credential providers should be allowed to provide credential tiles.

• **Only display SafeNet credential Tile:** All credential tiles presented to the user will enforce SafeNet authentication.

• **Hide Microsoft credential Tile:** The Microsoft credential tile is hidden from the user. Only the SafeNet credential tiles and third-party credential tiles are displayed.

• **Hide SafeNet credential tile and show all available:** This option disables the SafeNet credential tile and displays any third-party and/or Microsoft credential tiles.
Group Authentication Exceptions

The **Group Authentication Exceptions** section omits single and/or multiple local or domain groups from performing SafeNet authentication. Only one group filter option is valid at any given time, and it cannot overlap with another group authentication exception. The default setting is **Everyone must use SafeNet**.

- **Everyone must use SafeNet**: All users must perform SafeNet authentication.
- **Only selected groups will bypass SafeNet**: All users are required to perform SafeNet authentication, except for the Microsoft group(s) defined.
- **Only selected groups must use SafeNet**: Users are not required to perform SafeNet authentication, except for the Microsoft group(s) defined.
- **From this location**: This option displays local or domain search results.
- **Enter the group name to select**: This option is used in conjunction with **Check Names** or **Show All**, and allows searches for Microsoft groups.
- **Highlight already selected groups in search results**: If a Microsoft group has already been configured in the exception, it will appear as a highlighted result.
Communications Tab

This tab deals primarily with the connection options for SafeNet Authentication Service.

![Communications Tab](image)

**Authentication Server Settings**

- **Primary Server (IP:Port):** This setting is used to configure the IP address/hostname of the primary SafeNet Authentication Service. The default port is 80. Alternatively, **Use SSL** can also be selected. The default TCP port for SSL requests is 443.

- **Failover Server (Optional):** This setting is used to configure the IP address/hostname of the failover SafeNet Authentication Service. The default port is 80. Alternatively, **Use SSL** can also be selected. The default TCP port for SSL requests is 443.

  NOTE: In a new installation, the Failover Server option is selected by default.

- **Enable SSL server certificate check:** Clear to disable the SSL server certificate error check.

  If selected, the agent checks if the certificate from the SAS server is correct. If not selected the certificate is not checked. The SSL certificate check is enabled by default. This supports backward compatibility for customers using the on-premises deployment of SAS.
NOTE: The use of SSL certificates is strongly recommended.

- **Communication Timeout**: This setting specifies the maximum timeout value for authentication requests sent to the SafeNet Authentication Service.
- **Attempt to return to primary Authentication Server every**: This setting specifies the Primary Authentication server retry interval. This setting only takes effect when the Agent is using the Failover Server entry.
- **Agent Encryption Key File**: This setting is used to specify the location of the SafeNet Authentication Service Agent Key File.
- **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.

- **Server Status Check**: This function is used to run a communication test to verify a connection to SafeNet Authentication Service.
Appearance Tab

This tab allows for the customization of the logo displayed during authentication.

The custom logo must be a bitmap of 110 x 110 pixels. Solid white will be used as the transparent color if the image is smaller than 110 x 110 pixels.

NOTE: The logo file must be saved on the local computer. We recommend saving in the SAS Agent for Windows Logon installation folder or any other protected location.

The Restore option will revert to the default SafeNet Authentication Service logo.
CHAPTER 3: Configuration

Logging Tab

Logging Level
This setting adjusts the logging level. For log levels 1, 2, and 3, only the initial connection between the Agent and the server and any failed connection attempts are logged. The default setting is 3.

Log File Location
This setting specifies the location of the log files. The log files are rotated on a daily basis. The default locations are as follows:

- **2008/2008R2/Vista/7**: C:\Program Files\ SafeNet\Windows Logon\Gina\Log
- **Windows 8 and later**: C:\Program Files\ SafeNet\Windows Logon 8\AuthGINA
CHAPTER 4: Advanced Configuration

Remote Users with a Depleted Offline Authentication Store

The following steps should be taken if the emergency password is enabled and the offline authentication store is empty, resulting in the user being unable to log in to their workstation:

1. The user contacts the SafeNet Authentication Service administrator or operator.
2. The SAS administrator or operator logs in to the SafeNet Authentication Service Manager, finds the user on the Secured Users tab, and makes note of the emergency password.
3. The SAS administrator or operator provides the user with the emergency password.
4. The user logs in to their workstation using the emergency password.
5. The user establishes a VPN connection to the network.
6. The user launches the SafeNet Authentication Service Windows Logon Configuration tool and performs a manual replenish with their SafeNet credentials to restore their offline authentication store. Do not attempt to replenish with the emergency password, as this will fail.
7. The user may now log in with their SafeNet credentials while offline.

Remote Users Who Have Lost or Forgotten their Token

The following steps should be taken if the emergency password is enabled and the workstation is unable to communicate with the SafeNet Authentication Service at the time of authentication:

1. The user contacts the SafeNet Authentication Service administrator or operator.
2. The SafeNet Authentication Service administrator or operator logs in to the SafeNet Authentication Service Manager, finds the user on the Secured Users tab and makes note of the emergency password.
3. The SafeNet Authentication Service administrator or operator provides the user with the emergency password.
4. The user logs in to their workstation using the emergency password.
5. The SafeNet Authentication Service administrator or operator assigns the user a new token or enables a SafeNet Authentication Service static password.
6. The user establishes a VPN connection to the network.
7. The user launches the SafeNet Authentication Service Windows Logon Configuration Tool and performs a manual replenish with the new token or SafeNet Authentication Service static password.
8. The user may now log in with their SafeNet credentials while offline.
Refining Administrator Group Exclusions

During the installation of the SAS Agent for Windows Logon, an option can be enabled to exempt the Local and Domain Administrators groups from performing SafeNet authentication. In certain cases, restrictions may only be needed for the Local Administrators group or the Domain Administrators group rather than all Administrator groups. The following can be carried out to achieve this goal:

1. During the installation of the SAS Agent for Windows Logon, deselect the option Exempt Local and Domain Administrator groups from SafeNet Authentication Service Authentication.
2. Log in to the SafeNet Authentication Service Windows Logon protected workstation with SafeNet credentials and then Microsoft credentials.
3. Right-click on the SafeNet Authentication Service Windows Logon Configuration Tool and then select Run as administrator.
4. Click the Policy tab. In the Group Authentication Exceptions section, select Only selected groups will bypass SafeNet. Add the administrator group(s) to be excluded from SafeNet authentication.
5. Log out and then log in again.

Configuring Num Lock Settings

The Num Lock setting can be controlled from the Registry. If required, perform the following steps:

1. Click Start > Run.
2. In the Open box, type regedit, and then click OK.
3. In the Registry, open one of the following:
   - For a single user: HKEY_CURRENT_USER > Control Panel > Keyboard
   - For all users: KEY_USERS\Default > Control Panel > Keyboard
4. Edit the string value named InitialKeyboardIndicators as follows:
   - Set to 0 to set NumLock OFF.
   - Set to 2 to set NumLock ON.