SafeNet Authentication Service

Windows Logon Agent Configuration Guide

SafeNet
THE DATA PROTECTION COMPANY

Document Information

Document Part Number	007-012394-002, Rev. C
Release Date	September 2014

Trademarks

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

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.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contents

Preface

Purpose of this Guide

This document describes how to install and configure SafeNet Authentication (SAS) Windows Logon Agent. It contains the following chapters:

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—a cloud authentication service of SafeNet, Inc.
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**—the software used to build a SafeNet authentication service.
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—On-premises implementation of SAS.

Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure. This includes SAS users and security officers, the key manager administrators, and network administrators. It is assumed that the users of this document are proficient with security concepts.

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.

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 SafeNet Customer Support. SafeNet 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 SafeNet 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	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	

CHAPTER 1
Overview

The SafeNet Authentication Service Agent for Microsoft® Windows® two-factor authentication solution 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.

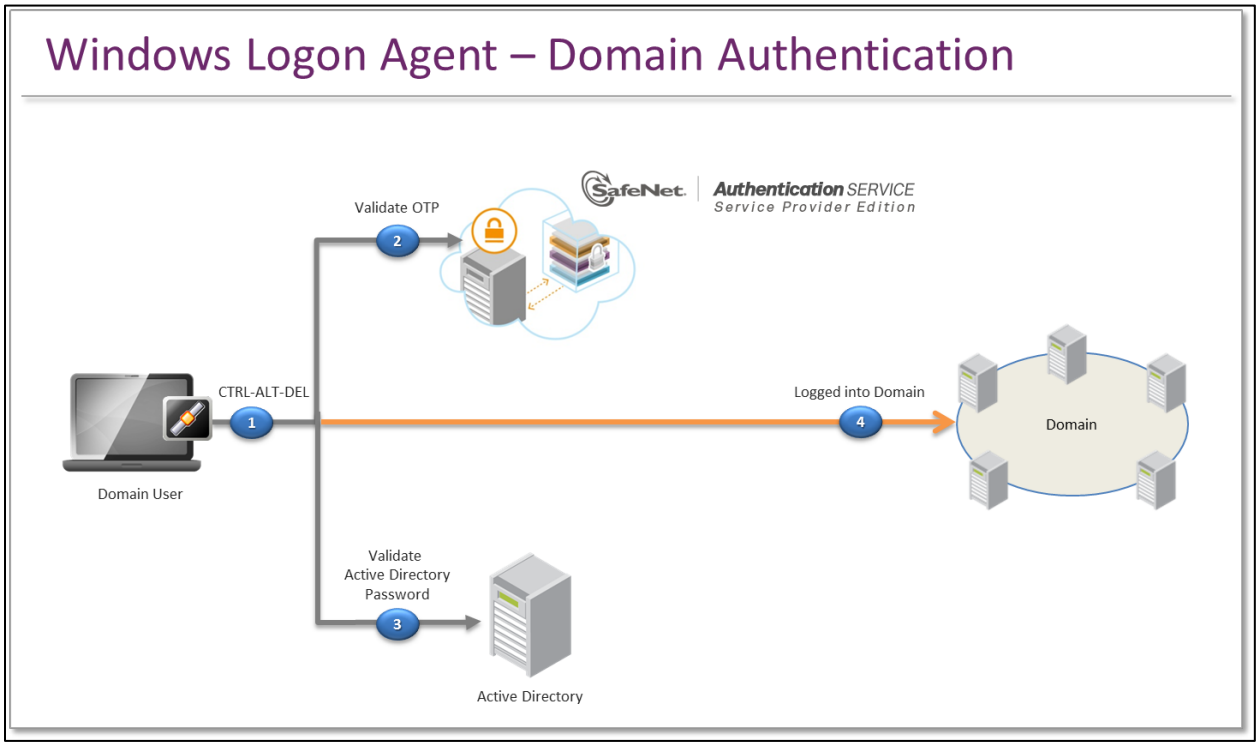
The use of two-factor authentication instead of just traditional static passwords to access a Windows environment is a necessary critical step for information security.

Environment

Environment	Description
Supported Windows Versions	• Windows XP • Windows 2003 and Windows Terminal Server 2003 • Windows 2008 SP2 and Windows 2008 R2 • Windows 2008 SP2 and Windows 2008 R2 Terminal Server • Windows Vista SP2 • Windows 7 • Windows 8 • Windows 8.1 • Windows Server 2012 • Windows Server 2012 R2
Additional Software Components	.Net 2.0
Supported Networking Environments	• Microsoft Domain • Microsoft Workgroup
Supported Architecture	• 32-bit • 64-bit
Network	TCP Port 80 or 443

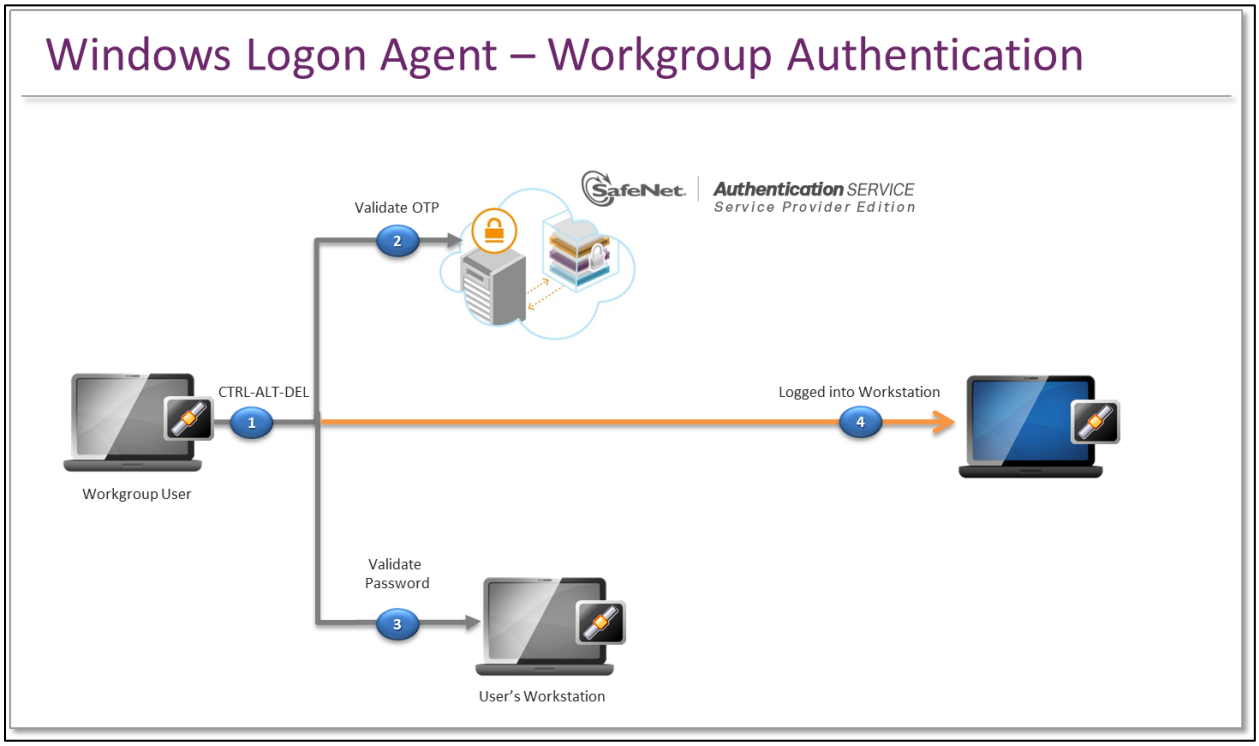
Environment	Description
Supported Tokens	KT Series, RB Series, CD-1, SMS, MP-1, GrIDsure (Vista/2008/7 only), SafeNet GOLD, Platinum, and eTokenPASS, MobilePASS
Unsupported Tokens	4.x legacy, 5.x legacy, 6.x legacy, UB, Smart Cards, IronKey, SafeStick
Unsupported Tokens in Offline Authentication Mode	Challenge-response-enabled tokens, SMS, GrIDsure, and time-based tokens.

SafeNet Authentication Service Windows Logon – Domain Authentication



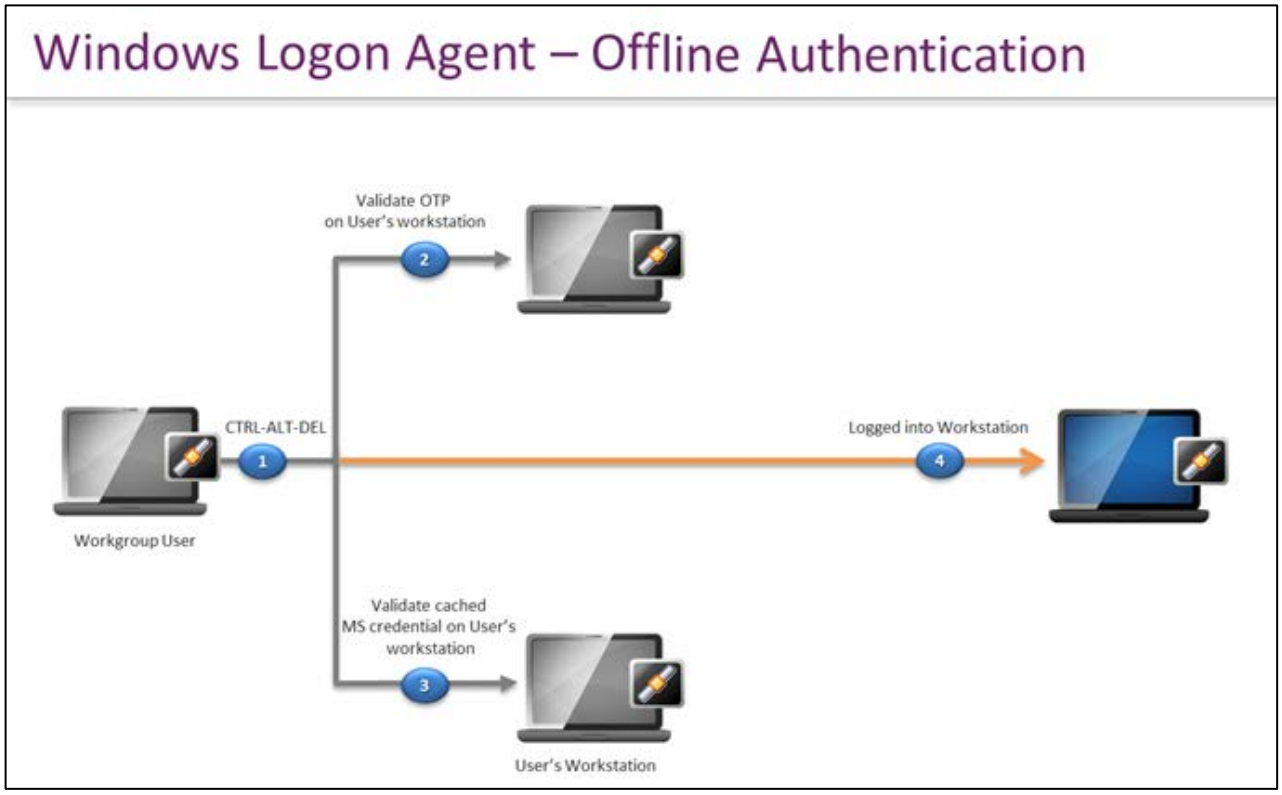
1. The user is presented with a SafeNet Authentication Service Windows Logon prompt, and then presses **Ctrl+Alt+Del**.
2. The user enters their user name, OTP, and, if applicable, the logon domain. If the user is part of a domain group authentication exception, the credentials are passed to Active Directory; 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 presses **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



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

> **NOTE:** In order 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, an administrator can top up or replenish an account anytime using the management tool. Management tools also show the number of offline authentications available and the warning threshold that can be 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 Windows Logon Agent. The mode of operation is selected during installation but can be modified afterwards if necessary. The modes of operation are:

Mode	Description
Dual Password Mode	In **Dual Password** 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.
Microsoft Password Caching Mode	In Microsoft **Password Caching** 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 SAS 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.

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 SAS Windows Logon Agent permits end-user workstations that may be offline periodically to authenticate. The normal SAS Windows Logon Agent authentication process requires that the user furnish a token-generated one-time password for transmission to SAS. When offline, there is no communication with SAS, only the local SAS 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 SAS 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

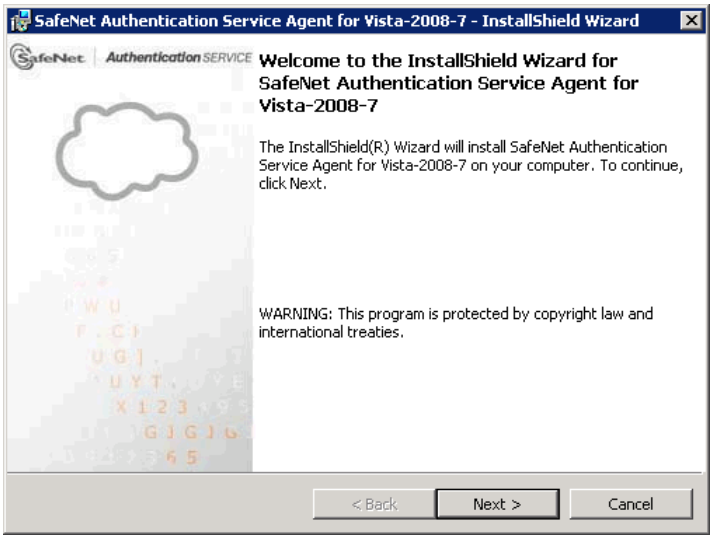
Preparation and Prerequisites

- Ensure that TCP port 80 or 443 is open between the SAS Windows Logon Agent and SafeNet Authentication Service.
- Administrative rights to the Windows system are required during installation of the SAS Windows Logon Agent.
- The SAS Windows Logon Agent will attempt to download and install .Net 2.0 and MSXML 6 if not already present. Alternatively, if this is not possible, these packages can be found in the SafeNet Authentication Service distribution package.

Installing SAS Windows Logon Agent

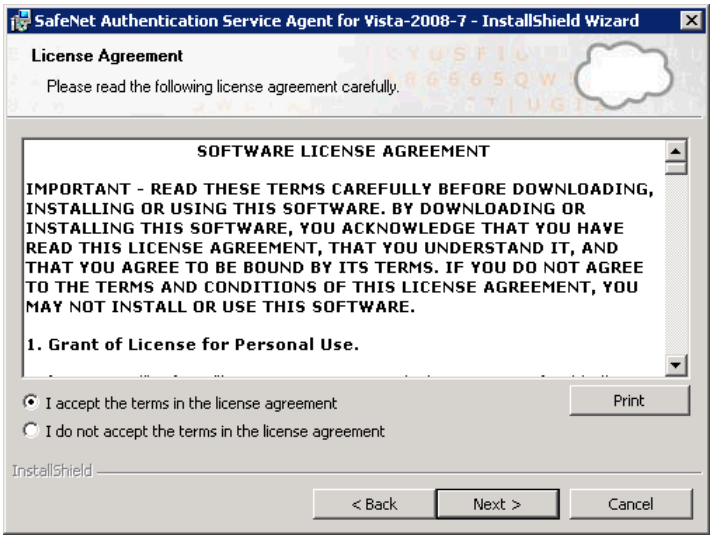
1. Log on to the Windows system.
2. Locate and run one of the installers listed below:
    - SafeNet Authentication Service Agent for Window 8 x64.exe
    - SafeNet Authentication Service Agent for Window 8 x64.msi
    - SafeNet Authentication Service Agent for Window 8.exe
    - SafeNet Authentication Service Agent for Window 8.msi
    - SafeNet Windows Logon Agent for Vista-2008-7 x64.exe
    - SafeNet Windows Logon Agent for Vista-2008-7 x64.msi
    - SafeNet Windows Logon Agent for Vista-2008-7.exe
    - SafeNet Windows Logon Agent for Vista-2008-7.msi
    - SafeNet Windows Logon Agent for XP-2003 x64.exe
    - SafeNet Windows Logon Agent for XP-2003 x64.msi
    - SafeNet Windows Logon Agent for XP-2003.exe
    - SafeNet Windows Logon Agent for XP-2003.msi

The **Welcome** window opens.



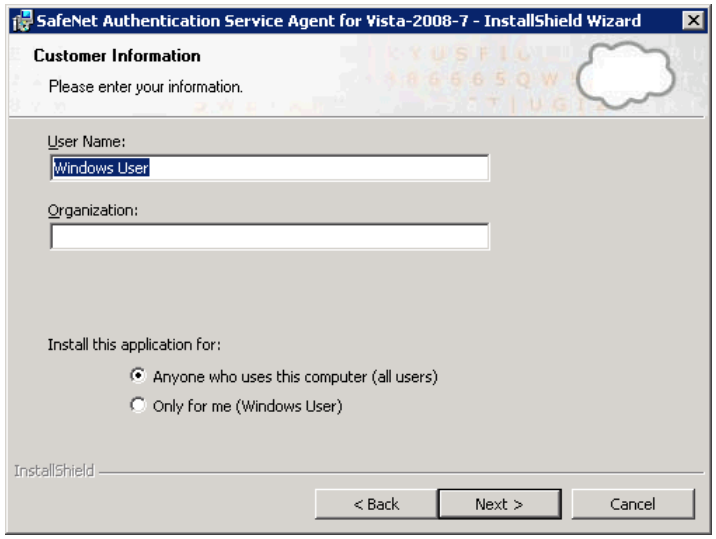
3. Click **Next**.

   The **License Agreement** window opens.



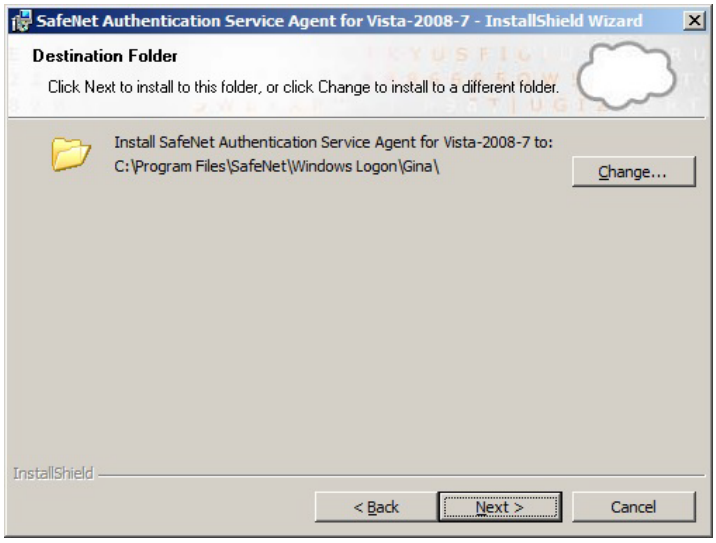
4. Select **I accept the terms in the license agreement**, and then click **Next**.

The **Customer Information** window opens.



5. Complete the **User Name** and **Organization** boxes as required, and then click **Next**.

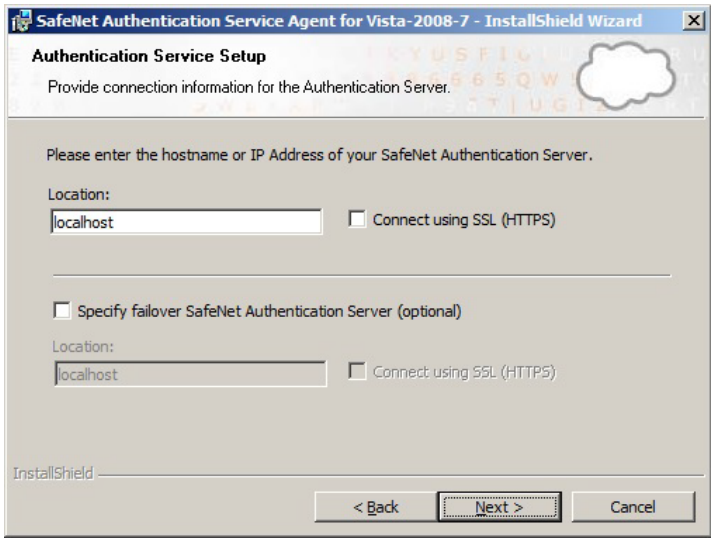
   The **Destination Folder** window opens.



6. Do one of the following:

   - Click **Next** to select the default installation destination folder and continue.
   - Click **Change** to browse to and select a different folder, then click **Next** to continue.

The **Authentication Service Setup** window opens.



7. Enter the following information and click **Next**:

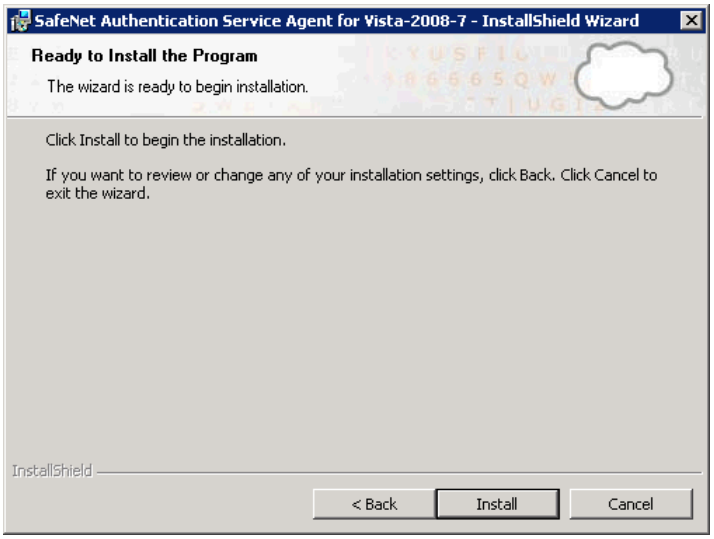
Location	Enter the hostname or IP address of the primary SafeNet Authentication Service.
Connect using SSL (HTTPS)	Select this option if SAS has been configured to accept incoming SSL connections.
Specify failover SafeNet Authentication Server	Select this option if a failover SAS is being used. If selected, you must also complete the **Location** field.
Location	Enter the hostname or IP address of the failover SAS, if applicable.
Connect using SSL (HTTPS)	Select this option if the failover SAS has been configured to accept incoming SSL connections.

The **Windows Logon Setup** window opens.

8. Enter the following information and click **Next**:

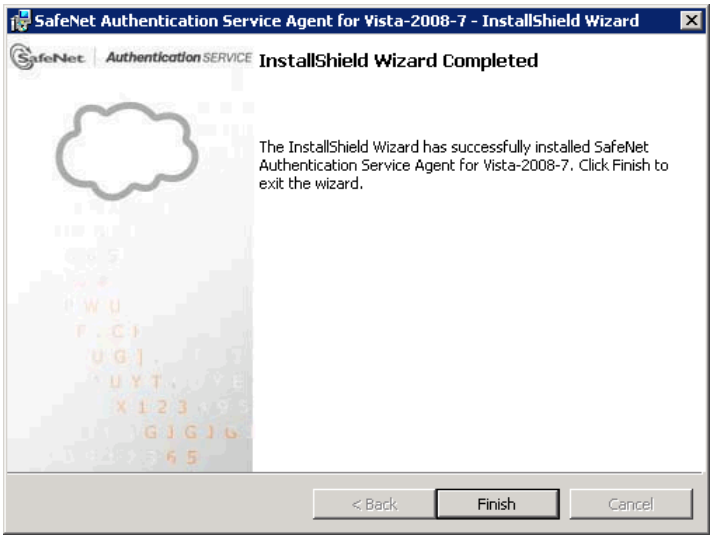
Exempt Local and Domain Administrator groups from SafeNet Authentication Service Authentication	Select this option to allow administrators to log on without providing SafeNet credentials.
Logon Mode	Select one of the following logon modes: • Users will enter both SAS and Windows credentials with each logon • SAS will cache Windows passwords after the first use
Display and option for users to logon with GrIDsure tokens	Select this option if required.

The **Ready to Install the Program** window opens.



9. Click **Install**

When the installation process is complete, the **Installshield Wizard Completed** window is displayed.



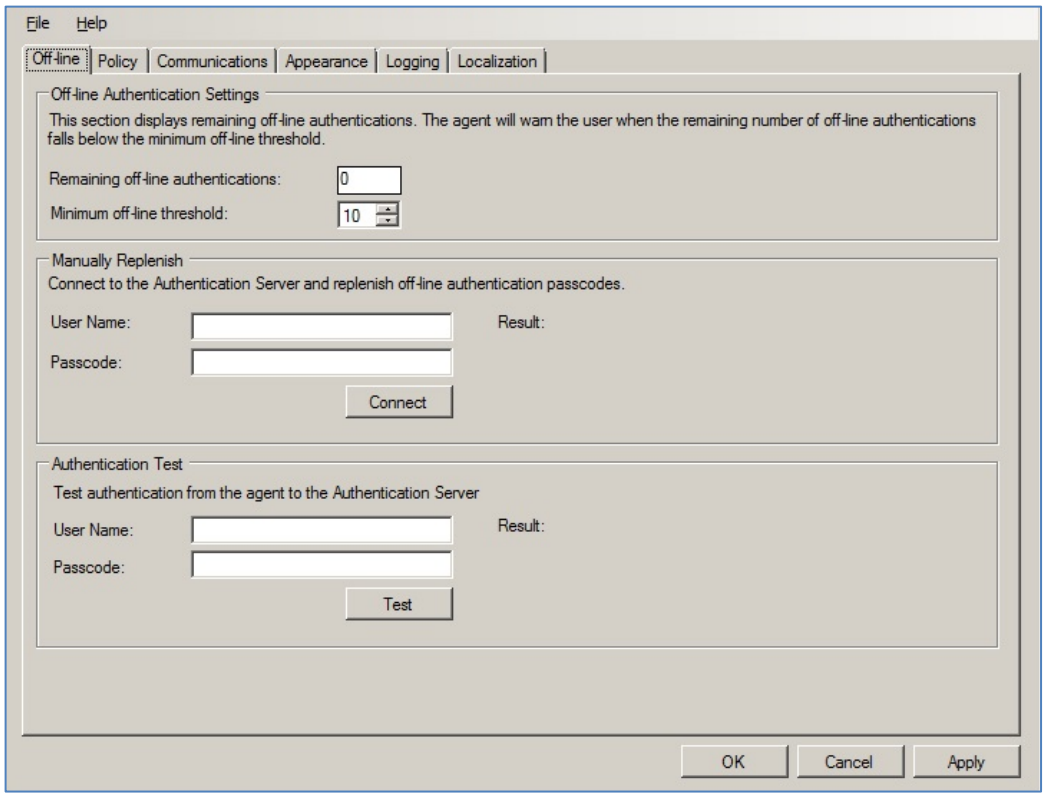
10. Click **Finish** to exit the installation wizard.

CHAPTER 3
Configuration

SAS Windows Logon Agent Configuration Tool

The SAS Windows Logon Agent Configuration Tool allows for the customization of various options available within the SAS Windows Logon Agent.

The **Off-line**, **Policy**, **Communications**, **Appearance**, **Logging**, and **Localization** tabs are available only to users who are part of the **Local Administrators** and **Domain Administrators** groups. On the **Off-line** tab, non-admin users will only have access to the **Minimum off-line threshold** setting in the **Off-line Authentication Settings** section.

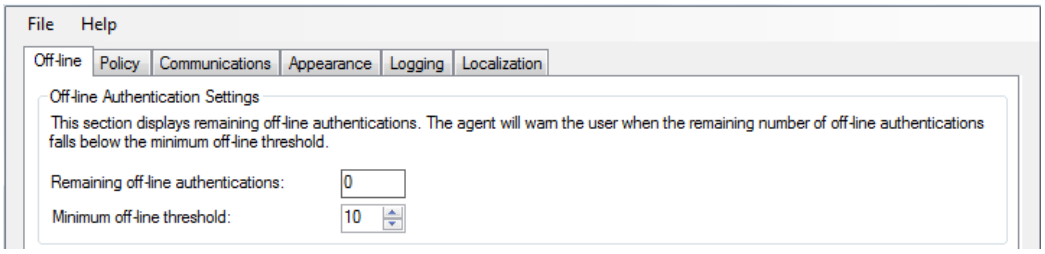


Off-line Tab

The **Off-line** tab is available only to users who are part of the **Local Administrators** and **Domain Administrators** groups. This 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 manually replenish the offline one-time password store, and to test authentication requests against SAS. Non-admin users will only have access to the **Minimum off-line threshold** setting.

Off-line Authentication Settings

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



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

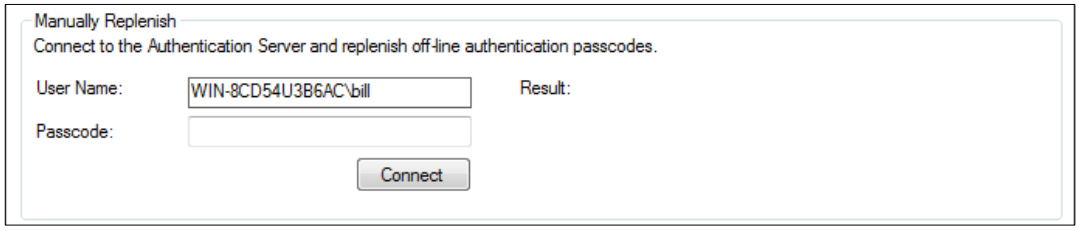
The Off-line store is automatically replenished when a user returns and logs in to the corporate network but, on rare occasion, the Off-line store may expire while the user is still at a remote location. The **Manually Replenish** option allows an administrator to refill an Off-line authentication store remotely. This function is available only to users who are part of the **Local Administrators** and **Domain Administrators** groups.

To manually replenish an Off-line authentication store:

1. Establish a VPN connection to the corporate network.
2. Open the SAS Windows Logon Agent Configuration Tool.
3. Enter your SafeNet credentials into the **Passcode** field and then click **Connect**.

NOTE: The administrator must provide the domain prefix as part of the user name when performing a manual replenishment; for example, **MYDOMAIN\user1**.

4. The SAS Windows Logon Agent 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.

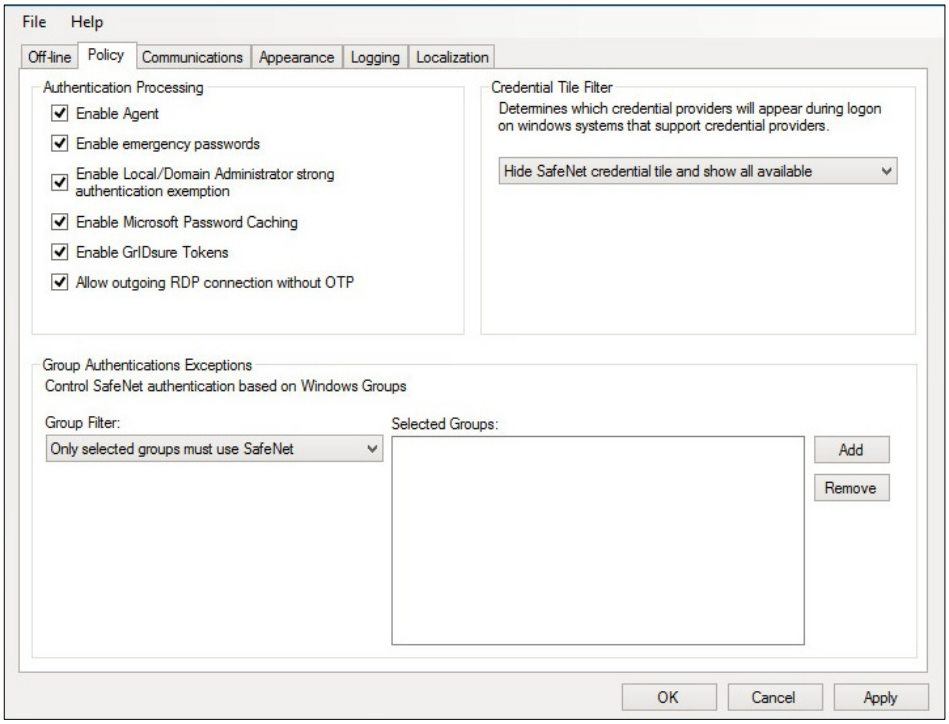


Authentication Test

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

Policy Tab

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

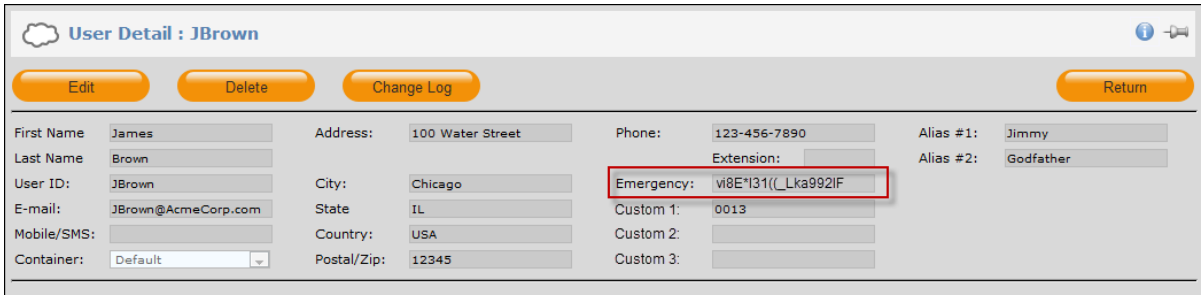


Authentication Processing

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

- **Enable Agent**: This option turns the SAS Windows Logon Agent 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 SafeNet Authentication Service at the time of authentication.

  Each user will have a unique emergency password, which is specified on the **Secured Users** tab of the SafeNet Authentication Service Manager. The emergency password can be used until the workstation regains contact with SafeNet Authentication Service, 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.

Credential Tile Filter

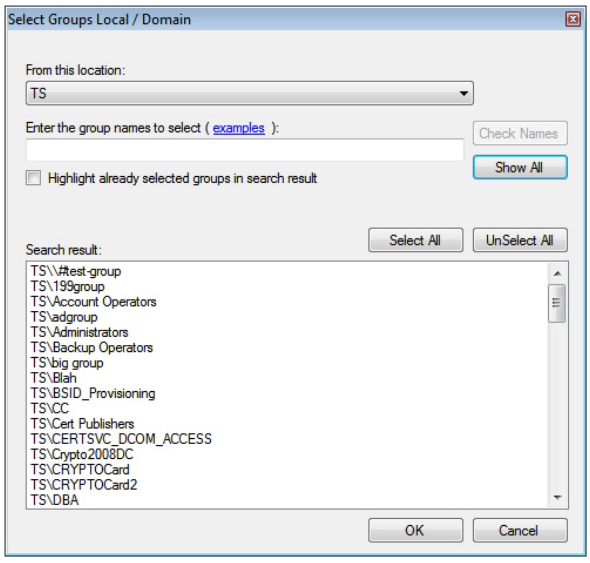
The **Credential Tile Filter** assesses whether a list of credential providers should be allowed to provide credential tiles:

- **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

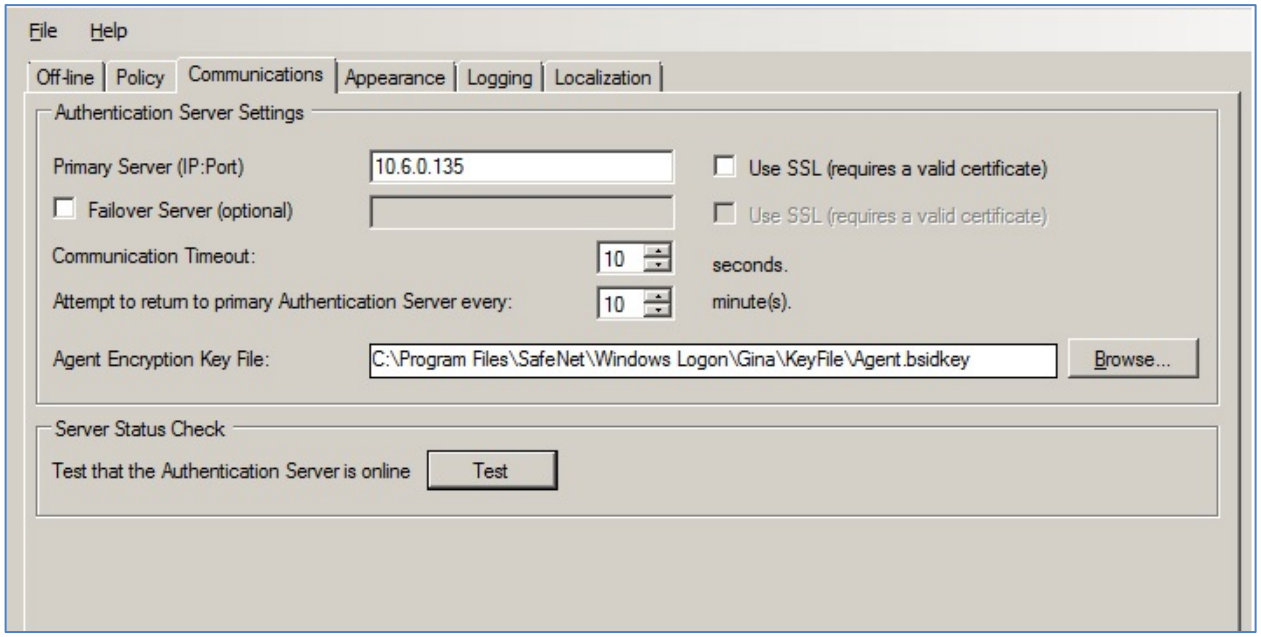
The **Group Authentication Exceptions** section omits single and/or multiple local or domain groups from performing SafeNet authentication. Only one group filter option is valid at any given time, and it cannot overlap with another group authentication exception. The default setting is **Everyone must 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 the Microsoft group(s) defined.
- **Only selected groups must use SafeNet:** All users are not required to perform SafeNet authentication except 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.



Authentication Server Settings

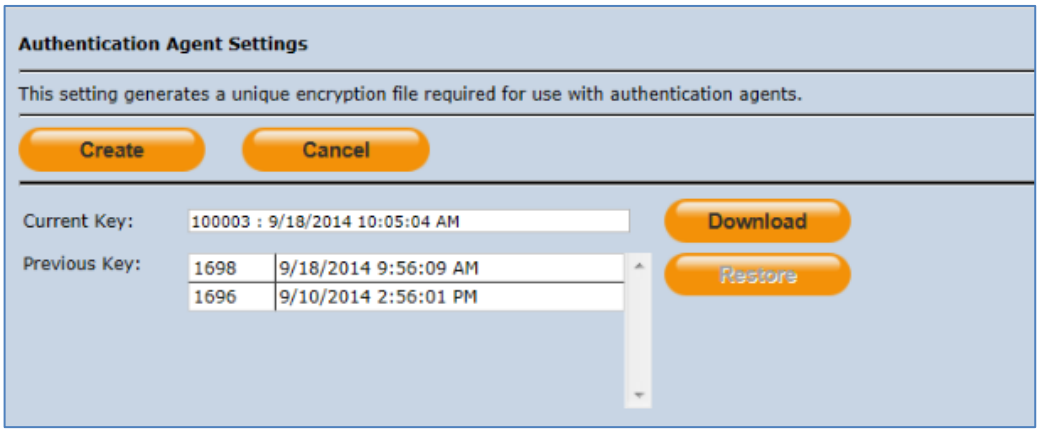
- **Primary Server (IP:Port):** This setting is used to configure the IP address/hostname of the primary SafeNet Authentication Service. The default port is **80**. Alternatively, **Use SSL** can also be selected. The default TCP port for SSL requests is **443**.
- **Failover Server (Optional):** This 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**.
- **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. You can replace the default unified key file (provided during installation) with a unique key file downloaded from the SAS server. To create a new key file, open the SAS Management Console. Click **Virtual Servers > COMMS > Authentication Processing > Authentication Agent Settings**, and then click the **Create** button.

  Once a new key is created, all other computers running Windows Logon Agent should download and use this key. To download the key file, open the SAS Management Console. Click **Virtual Servers > COMMS > Authentication Processing > Authentication Agent Settings**. Click the **Download** button.

  When downloading the new key, one of the following actions should be performed:

  - Replace the previous key with the new key (rename or delete the previous key)
  - Place the new key in a different directory, and then update the agent to reference the new key path

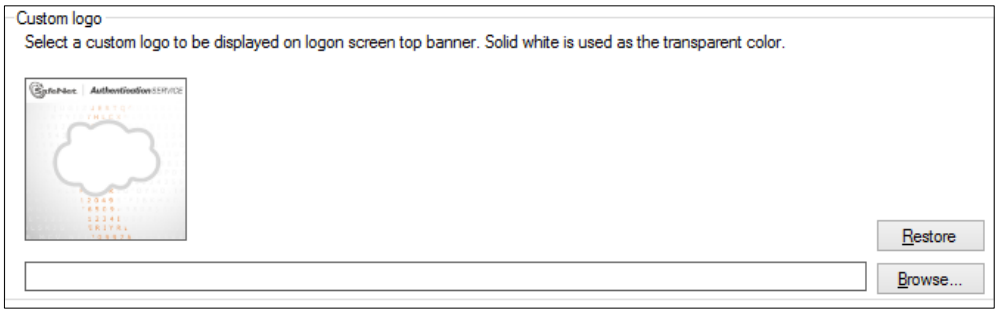


- **Server Status Check:** This function performs a communication test to verify a connection to the SafeNet Authentication Service.

Appearance Tab

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

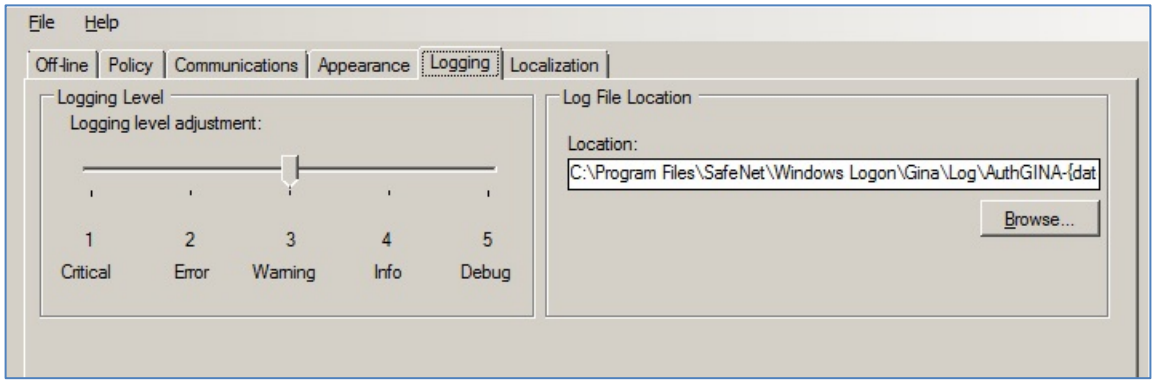
The custom logo must be a bitmap of 110 x 110 pixels. Solid white will be used as the transparent color if the image is smaller than 110 x 110 pixels.



The **Restore** option will revert to the default SAS logo.

A SafeNet watermark will appear when a custom logo is used.

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.

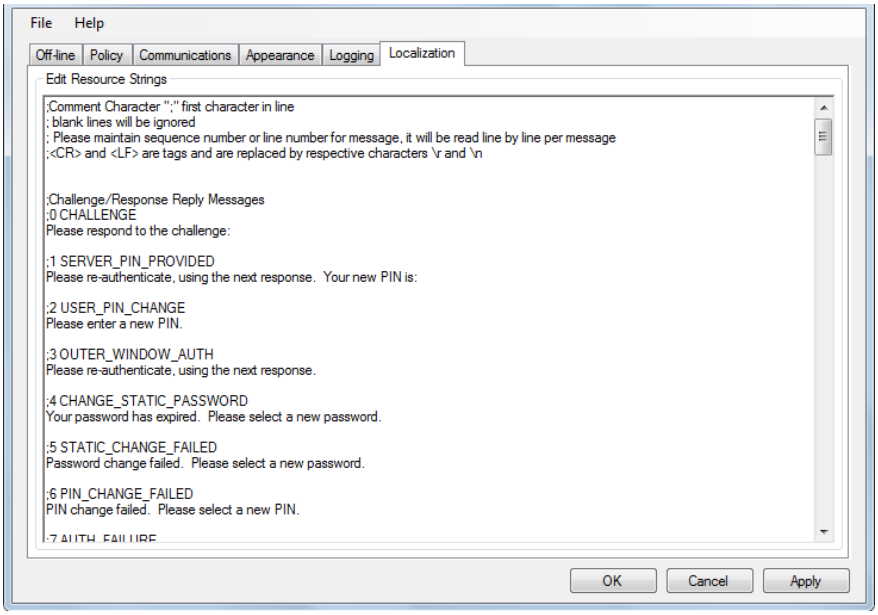
The default locations are as follows:

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

Localization Tab

The settings on this tab represent the prompts and information messages provided by the SAS Windows Logon Agent. These messages can be modified as necessary to improve usability. The **LogonClient.ccl** message file can also be manually modified outside of the configuration tool. The default locations are:

- **2008/2008R2/Vista/7:** C:\Program Files\SafeNet\Windows Logon\Gina\languages\en
- **Windows 8 and later:** C:\Program Files\SafeNet\Windows Logon 8\languages\en



Migrating from CRYPTO-Logon 6.x

The following information is for CRYPTO-Server 6.x customers who are currently using the CRYPTO-Logon 6.x Agent.

Architecture Changes

- The SAS-Logon for Domain Controller package is no longer required. The SAS Windows Logon package communicates directly with SafeNet Authentication Service.
- The SAS Windows Logon package is supported in a Domain and/or Workgroup environment.
- The SAS Windows Logon package is not compatible with CRYPTO-Server 6.x.
- The network traffic used by the SAS Windows logon Agent has changed. The SAS Windows Logon Agent uses TCP port 80 or 443. Previously, the CRYPTO-Logon 6.x used TCP port 5742.
- For supported environments, see page 6.
- CRYPTO-Logon 6.x **Static Password** mode has been renamed **Dual Password** mode. CRYPTO-Logon 6.x **Password Manager** mode has been renamed to **Microsoft Password Caching** mode.

- **Disconnected** authentication has been renamed to **Offline** authentication.
  - Disconnected (Offline) authentication is no longer enabled on a per-token basis. Disconnected (Offline) authentication is a global option, enabled by default, for all supported tokens.
  - The disconnected (offline) authentication **Warning Message Threshold** is now customizable. Previously, this setting was hard-coded to **10**. The **Warning Message Threshold** value can be set between 5 and 99.
- Smart card and USB tokens are not supported in the SAS Windows Logon package.

Feature Changes

- CRYPTO-Logon 6.x Static Password mode has been renamed Dual Password mode. CRYPTO-Logon 6.x Password Manager mode has been renamed to Microsoft Password Caching mode.
- The SafeNet Authentication Service Windows Logon Agent includes a client-side configuration tool to allow customizations that were previously only available via the Registry.
- SafeNet authentication exclusions can be added for specific Microsoft groups.
- Local and Domain Administrator groups can be exempt from SafeNet authentication during login. This option is selectable during installation and can be disabled within the SafeNet Authentication Service Windows Logon configuration tool.
- The Agent provides the ability to control which authentication credential tiles are visible to users (Windows 2008/Vista/7 only).
- A silent install can be performed using the MSI installer package.
- Custom logos are supported.
- Various messages provided to the end user are now customizable.
- The SafeNet Authentication Service Windows Logon Agent includes the ability for a user to manually replenish their offline authentication information.
- An emergency password feature has been added. This feature is an authentication method that enables an administrator to authenticate to a user's computer as the user without entering a SafeNet one-time password. See "Authentication Processing" on page 20 for more details.

Upgrading to the SAS Windows Logon Agent

- The SAS distribution package includes a 6.x migration tool that will copy all user, token, and operator information from CRYPTO-Server 6.x into SafeNet Authentication Service.
- The default **Inner Window** value of **10** on the **Policy Admin** tab of the SafeNet Authentication Service Manager should be changed to **99.** The **Outer Window** value of **100** should be changed to **200**. Modifying these settings will keep SafeNet tokens in sync between each SafeNet server as Windows workstations are migrated to the SAS Windows Logon package.
- The CRYPTO-Logon 6.x Desktop client must be uninstalled prior to installing the SAS Windows Logon Agent.

- The 6.x CRYPTOCard Software Tools must be upgraded to the SafeNet Authentication Service Software Tools. Do not remove the 6.x CRYPTOCard Software Tools as this will remove any software tokens installed. During the installation of the SafeNet Authentication Service Software Tools, any existing ST tokens will automatically be detected and imported. Once the tokens have been imported, the 6.x CRYPTOCard Software Tools package can be uninstalled. If a software token needs to be re-deployed at a later date, an MP token must be issued to the user.
- The SAS-Logon for Domain Controller package should be the last component to uninstall after all workstations have been migrated to the SAS Windows Logon Agent.
- If smart card or USB tokens are being used, contact your SAS account manager for more information.

Advanced Configuration

SAS Windows Logon Silent Installation

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

The following is a list of options that can be specified. If the option is not specified, it will be set to the default value, which is equivalent to clicking **Next** on all pages of the installer dialog.

TOKENVALIDATORLOCATION	**Value**
Primary SafeNet Authentication Service	IP address or Hostname Default Value: localhost
USESSL	
Enable SSL to Primary SafeNet Authentication Service	**S** otherwise omit **USESSL** Default Value: Disabled
TOKENVALIDATORLOCATION2	
Secondary SafeNet Authentication Service	IP address or Hostname Default Value: Disabled
USESSL2	
Enable SSL to Secondary SafeNet Authentication Service	**S** otherwise omit **USESSL2** Default Value: Disabled

TOKENVALIDATORLOCATION	Value
EXEMPTADMINS	
Logon Mode of Operation	**1** for yes, **0** for no Default Value: Dual Logon (0)
LOGONMODE	
Logon Mode of Operation Default Value: Dual Logon (0)	0 for “users will supply both passwords each time” 1 for “Microsoft password caching”

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 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 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 SAS 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 SafeNet Authentication Service at the time of authentication:

1. The user contacts the SAS 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 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 SAS Windows Logon Configuration Tool and performs a manual replenish with the new token or SAS static password.
8. The user may now log in with their SafeNet credentials while offline.

Refining Administrator Group Exclusions

During the installation of the SafeNet Authentication Service Windows Logon Agent, 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 SafeNet Authentication Service Windows Logon Agent, deselect the option **Exempt Local and Domain Administrator groups from SafeNet Authentication Service Authentication**.
2. Log in to the SAS Windows Logon-protected workstation with SafeNet credentials and then Microsoft credentials.
3. Right-click the **SAS 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, Inc.** Add the administrator group(s) to be excluded from SafeNet authentication.
5. On Windows 2003/XP, reboot the workstation for the setting to take effect; otherwise, log out and then log in again.

Advanced Windows Login Settings

The **Do not display last user name** setting determines whether the name of the last user to log on to the computer is displayed in the Windows logon screen. This setting can be changed through the local or domain policy.

1. Click **Start > Run**.
2. In the **Open** box, enter **mmc** and then click **OK**.
3. On the **Console** menu, click **File > Add/Remove Snap-in**.
4. Click **Add**.
5. Click the **Group Policy** snap-in and then click **Add**.
6. Click the target Group Policy object (GPO). The default setting is the local computer. Click **Browse** to select other GPOs that are available on the network. Click **Finish**.
7. Click **Close** and then click **OK**.
8. Expand the **Computer Configuration** node, the **Windows Settings** node, and the **Security Settings** node.
9. Expand the **Local Policies** node, and then click **Security Options**.
10. In the right pane, under **Logon Screen**, double-click **Interactive logon: the Do not display last user name** or **Do not display last user name**.
11. Click **Enabled**.
12. Click **OK**.
13. Close the **Group Policy** console.
14. Restart the workstation or server for the settings to take effect.

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**.