SafeNet Authentication Service

Configuration Guide

SAS Agent for Microsoft SharePoint

Document Information

Product Version	SAS Agent for or Microsoft SharePoint version 1.04
Document Part Number	007-012485-001, Rev. B
Release Date	24 March 2015

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.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Introduction

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Microsoft SharePoint. Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Overview

The SafeNet Authentication Service Agent for SharePoint is designed to help Microsoft enterprise customers ensure that SharePoint resources are accessible only by authorized users, whether working remotely or inside the firewall. It delivers a simplified and consistent user login experience and helps organizations comply with regulatory requirements.

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

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)** — A term used to describe the implementation of SAS-PCE/SPE.

Environment

Authentication Server	• SafeNet Authentication Service PCE/SPE 3.3.2 and later • SafeNet Authentication Service Cloud
Network	• TCP Port 80 or 443
Supported Web Servers	• IIS 7.0 • IIS 7.5 • IIS 8.0 • IIS 8.5
Supported SharePoint Server Version	• Microsoft SharePoint 2010 • Microsoft SharePoint 2013
Supported Web Browsers	• Internet Explorer 9, 10, 11 • Chrome • Firefox
Additional Web Browser Requirements	• Cookies must be enabled • JavaScript must be enabled • ActiveX plug-ins (software token detection only)
Supported Authentication Methods	All tokens and authentication methods supported by SafeNet Authentication Service

Authentication Modes

There are two modes of operation for the SAS Agent for Microsoft SharePoint. By default, Split Authentication mode is enabled. The authentication mode can be modified after installation using the SafeNet Authentication Service SharePoint Agent Configuration Tool.

Mode	Description
Standard Authentication Mode	Standard Authentication Mode enables a single stage login process. Microsoft and SafeNet Authentication Service credentials must be entered into the SharePoint login page.
Split Authentication Mode	Split Authentication mode enables a two-stage login process. In the first stage, users provide their Microsoft credentials. In the second stage, users provide their SAS credentials. This mode allows administrators to control authentication dialogs based on Microsoft groups or token type (such as GrIDsure). This is the preferred mode when migrating from static to one-time passwords (OTPs).

Standard Authentication Mode (Hardware and Software)

1. The user enters the SharePoint URL into their web browser.
2. The SafeNet Authentication Service SharePoint Agent examines the incoming request against its **IP Range Exclusions/Inclusions** list to determine if SafeNet Authentication Service authentication can be ignored.
3. If IP address exclusion is detected, SafeNet Authentication Service credentials are not required. The user authenticates using Microsoft credentials.
4. If IP address exclusion is not detected, a SafeNet Authentication Service form-based login page is displayed.
5. If a software token is detected, the SharePoint login page will display **Token**, **PIN**, **Microsoft Password**, and **Microsoft Domain** fields. An option to toggle between **Hardware** and **Software** token mode is available.
6. If a software token is not detected, the SharePoint login page will display **Microsoft Username**, **Microsoft Password**, and **OTP** fields.
7. The user enters their Microsoft and SafeNet Authentication Service credentials into the login page. If both sets of credentials are valid, the user is presented with their SharePoint site; otherwise, the attempt is rejected.

Standard Authentication Mode (Hardware, Software, and GrIDsure/SMS)

1. The user enters the SharePoint URL into their web browser.
2. The SafeNet Authentication Service agent examines the incoming request against its **IP Range Exclusions/Inclusions** list to determine if SafeNet Authentication Service authentication can be ignored.
3. If IP address exclusion is detected, SafeNet Authentication Service credentials are not required. The user authenticates using Microsoft credentials.
4. If IP address exclusion is not detected, a SafeNet Authentication Service form-based login page is displayed.
5. If a software token is detected, the SharePoint login page will display **Token**, **PIN**, **Microsoft Password**, and **Domain** fields. The option to toggle between hardware, software, and GrIDsure/SMS token mode is available.
6. If a software token is not detected, the SharePoint login page will display **Microsoft Username**, **Microsoft Password**, and **OTP** fields. The option to toggle between hardware and GrIDsure/SMS challenge-response token mode is available.
7. The user enters their Microsoft and SafeNet Authentication Service credentials into the login page. If both sets of credentials are valid, the user is presented with their SharePoint site; otherwise, the attempt is rejected.
8. In GrIDsure/SMS Challenge-response mode the user enters their Microsoft credentials into the login page. If the Microsoft credentials are valid, the user is presented with a GrIDsure grid or provided with an OTP via SMS. If the SafeNet Authentication Service credentials entered are valid, the user is presented with their SharePoint site; otherwise, the attempt is rejected.

Split Authentication Mode

1. The user enters the SharePoint URL into their web browser.
2. The SafeNet Authentication Service agent examines the incoming request against its **IP Range Exclusions/Inclusions** list to determine if SafeNet Authentication Service authentication can be ignored.
3. If IP address exclusion is detected, SafeNet Authentication Service credentials are not required. The user authenticates and logs in to the SharePoint site using their Microsoft credentials.

4. If IP address exclusion is not detected, the user is presented with **Microsoft Username** and **Microsoft Password** fields. If the Microsoft credentials are valid, the user is allowed to continue; otherwise, the attempt is rejected.
5. The SafeNet Authentication Service agent examines the Microsoft username against its **Group Authentication Exceptions** list to determine if SafeNet Authentication Service authentication can be ignored.
6. If a group authentication exception is detected, SafeNet Authentication Service credentials are not required. The user is presented with their SharePoint site.
7. If a group authentication exception is not detected, the SafeNet Authentication Service agent examines the Microsoft username against its GrIDsure and SMS authentication group list.
8. If a GrIDsure or SMS authentication group match is detected, the user is presented with their GrIDsure grid or provided with an OTP via SMS. If the SafeNet Authentication Service credentials are valid, the user is presented with their SharePoint site; otherwise, the attempt is rejected.
9. If a software token is detected, the SharePoint login page will display a **PIN** field. The option to toggle between **Hardware** and **Software** token mode is available.
10. If a software token is not detected, the SharePoint login page will display an **OTP** field.
11. The user enters their SafeNet Authentication Service credentials into the login page. If the credentials are valid, the user is presented with their SharePoint site; otherwise, the attempt is rejected.

Prerequisites

- Ensure that users are able to log in to SharePoint using their Microsoft credentials prior to deploying the agent.
- Ensure that TCP port 80 or 443 is open between the SafeNet Authentication Service Agent for SharePoint and the SafeNet Authentication Service server.
- Administrative rights to the Windows system are required during installation of the SafeNet Authentication Service SharePoint Agent.
- Download the SafeNet Authentication Service Agent for SharePoint. A link to the agents and other software can be found on the **Snapshot** tab in the **References** module for users of SAS.
- The SafeNet Authentication Service Agent for SharePoint requires that each SharePoint site is configured to use **Basic authentication**. Prior to enabling the SafeNet Authentication Service agent, the following must be performed within SharePoint:
- Log in to the SharePoint Central Administration website.
- Select **Security**.
- In the **General Security** section, select **Specify Authentication Providers**.
- Select the web application and then select the zone.
- If the SharePoint site is using **Classic Mode authentication**, clear the **Integrated Windows authentication** option and select **Basic authentication**. If the SharePoint site is using Claims Based Authentication, select the **Basic authentication** option.

Installing the SAS Agent for SharePoint

1. Log on to the SharePoint server as a user with administrative privileges.
2. Locate and run the **SAS Agent for SharePoint x64.exe** installation package as administrator.
3. Follow the installation instructions.

Enabling the SAS Agent for SharePoint

The following instructions are required for the basic configuration of the agent. For more in-depth information on each setting, refer to the "SAS SharePoint Agent Configuration Tool" on page 9.

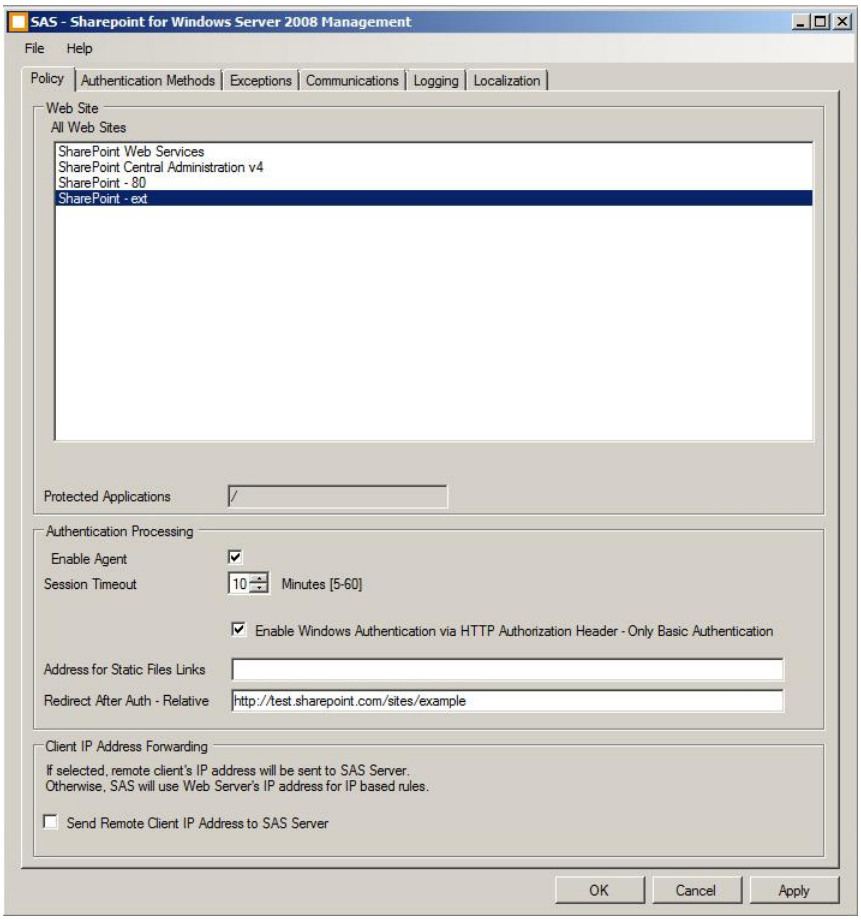
1. Click **Start > All Programs > SafeNet Authentication Service > SafeNet Authentication Service Agent for SharePoint > SharePoint Agent Configuration**.
2. On the **Policy** tab, select the SharePoint website. Select **Enable Agent** and any additional settings required.
3. Click the **Communications** tab. Modify the **Authentication Server Settings** to reflect the location of SAS.
4. Verify that all other tabs meet your requirements.
5. Apply the settings.
6. Restart the IIS server for the settings to take effect.

SAS SharePoint Agent Configuration Tool

The SAS SharePoint Agent Configuration Tool allows for the modification of various features available within the SAS Agent for SharePoint.

Policy Tab

The **Policy** tab deals primarily with enabling the SharePoint Agent and defining the website settings. When a website is selected, all settings selected within each tab apply to the specific website. If another website is selected, all tabs revert to their customized or default settings, allowing the selection of different settings within each tab.



Web Site Group

- **Web Site Name:** Allows the selection of a SharePoint website. Default value: None.
- **Protected Applications:** Specifies the top level directory of the SharePoint Server. Default value: /

Authentication Processing Group

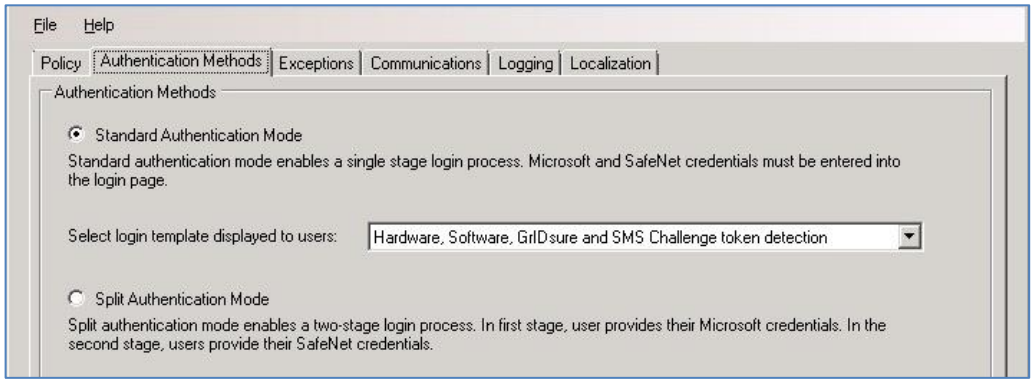
- **Enable Agent:** Turns the SAS Agent for SharePoint on or off. Default value: Disabled.
- **Session Timeout:** Specifies the time-out in minutes.
- **Enable Windows Authentication via HTTP Authentication Header - Only Basic Authentication:** If the user is using Basic Authentication, selecting this option will bypass the Basic Authentication screen in the agent and will prompt only for OTP, if required.
- **Address for Static Files Links:** If you work in a Proxy environment, and there is a problem with displaying site content (for example, images do not display correctly) the static file link must be configured in the following format**: protocol://host:port.application/**
- **Redirect After Auth – Relative:** The agent protecting the specific SharePoint site will redirect the user to this location after a successful authentication. The redirected site must be part of the specific SharePoint-protected site.

Client IP Address Forwarding Group

If selected, the remote client IP address will be sent to SAS; otherwise, the SharePoint IP address will be sent to SAS. Default value: Enabled.

Authentication Methods Tab

The **Authentication Methods** tab allows for the selection of the login authentication method and web page authentication layout presented to the user.



Authentication Methods Group

Standard Authentication Mode: This mode enables a single-step login process. Microsoft and SafeNet Authentication Service credentials must be entered into a single login page. Default value: Disabled.

Standard Authentication Mode provides the option to select one of two login templates:

- **Hardware and Software Token Detection:** If a software token is detected, the login page will display Token, **PIN**, **Microsoft Password**, and **Microsoft Domain** fields; otherwise, **Microsoft Username**, **Microsoft Password**, and **OTP** fields are displayed. The option to toggle between **Hardware** and **Software** token mode will be available if a software token is detected on the local workstation.
- **Hardware, Software, GrIDsure, and SMS Challenge Token Detection:** If a software token is detected, the login page will display **Token**, **PIN**, **Microsoft Password**, and **Microsoft Domain** fields. If required, a set of radio button options will allow the user to select a different token type. If no software

token exists, the user will be presented with **Microsoft Username**, **Microsoft Password**, and **OTP** fields, along with an option to enable a GrIDsure\SMS Challenge login page.

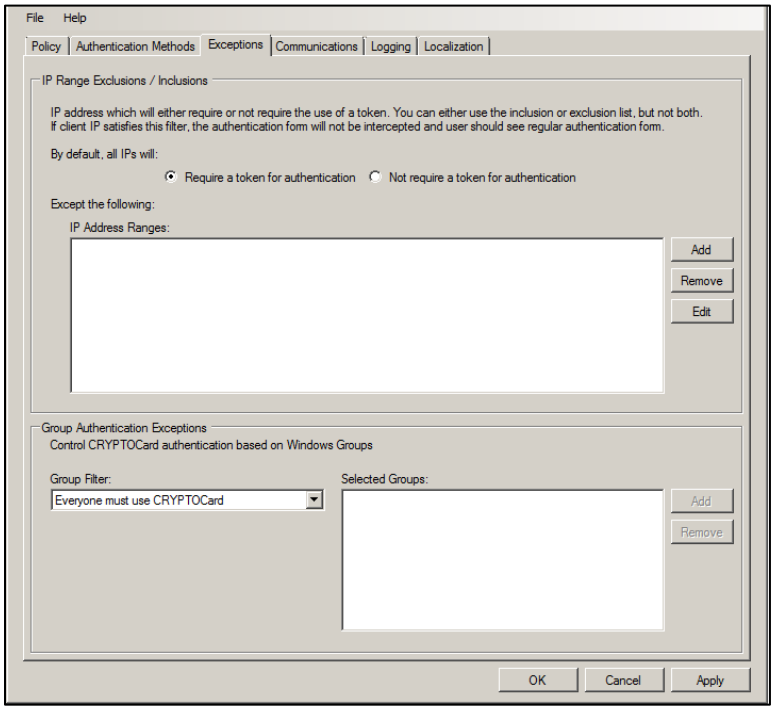
Split Authentication Mode: enables a two-stage login process. In the first stage, users provide their Microsoft credentials. In the second stage, users provide their SafeNet Authentication Service credentials. Default value: Enabled.

This mode provides the following advantages over **Standard Authentication Mode**:

- Microsoft group exclusions may be used to slowly migrate users from static passwords to a combination of static and one-time passwords.
- Allows administrators to specify via Microsoft groups, users who have been provided with GrIDsure or SMS challenge-response tokens. This allows for a seamless login experience as the agent displays exactly what is required from the user.
- **GrIDsure Tab (Optional):** Allows an administrator to specify a Microsoft group, which contains SafeNet Authentication Service users who have been assigned a GrIDsure token. When the agent detects a user within this group, it will automatically display a GrIDsure grid after they have provided valid Microsoft credentials.
- **SMS Challenge-Response Tab (Optional):** Allows an administrator to specify a Microsoft group, which contains SafeNet Authentication Service users who have been assigned an SMS challenge-response token. When the agent detects a user within the group, it will automatically provide them with a one-time password via SMS after they have provided valid Microsoft credentials.

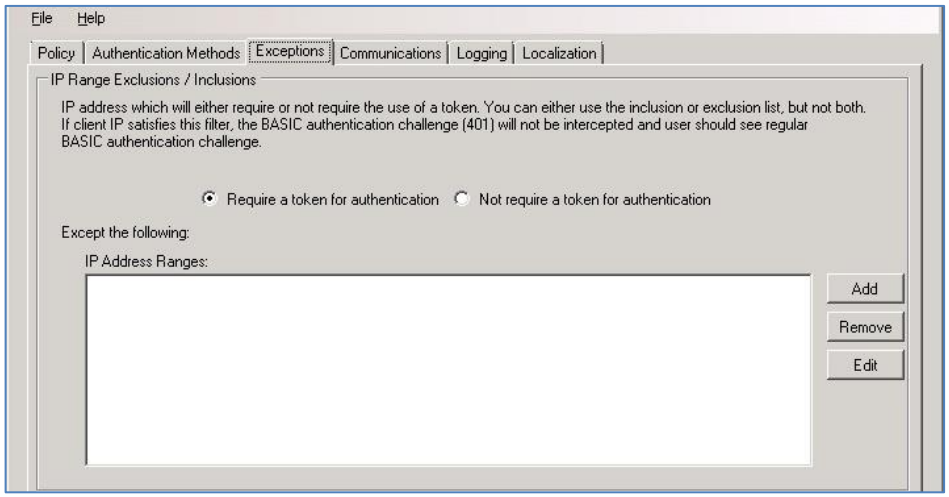
Exceptions Tab

The **Exceptions** tab allows specific Microsoft groups or network traffic to bypass SafeNet Authentication Service authentication. By default, all users are required to perform SafeNet Authentication Service authentication unless otherwise defined by exclusion.



IP Range Exceptions/Inclusions Group

Allows an administrator to define which network traffic requires SAS authentication. By default, all networks are required to perform SAS authentication.

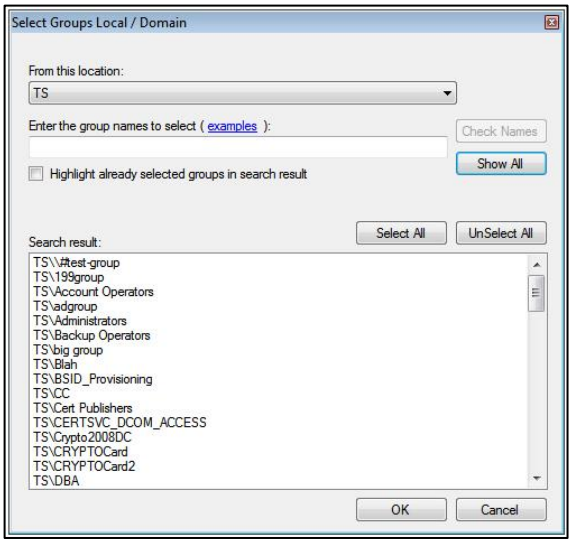


Group Authentication Exceptions Group

Group authentication exceptions omit single and/or multiple domain groups from performing SafeNet Authentication Service authentication. Only one group filter option is valid at any given time, and it cannot overlap with another group authentication exception. Default value: Everyone must use SafeNet Authentication Service.

The following group authentication exceptions are available:

- **Everyone must use SafeNet Authentication Service:** All users must perform SafeNet Authentication Service authentication.
- **Only selected groups will bypass SafeNet Authentication Service:** All users are required to perform SafeNet Authentication Service authentication except the Microsoft Group(s) defined.
- **Only selected groups must use SafeNet Authentication Service:** All users are not required to perform SafeNet Authentication Service authentication except the Microsoft Group(s) defined. Adding a group authentication exception entry will display the following:

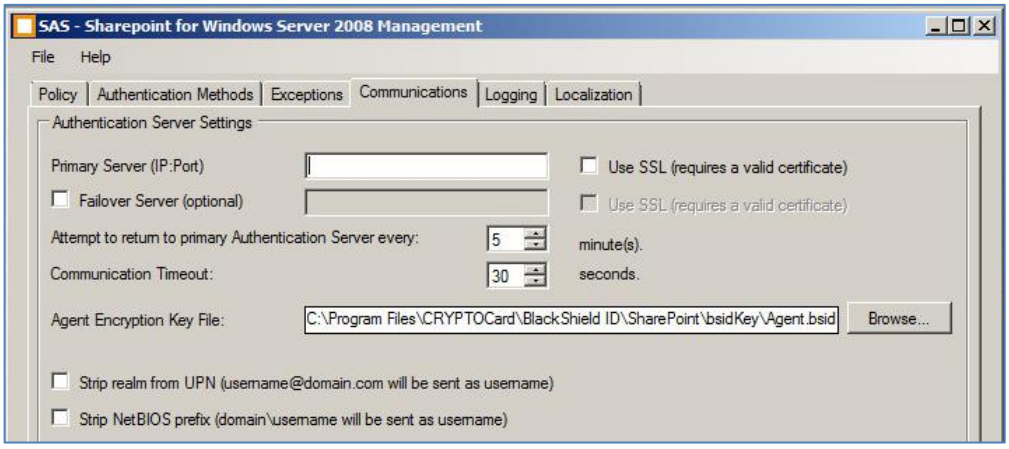


- **From this location:** Select the location from which the results will be searched.
- **Enter the group name to select:** Used in conjunction with **Check Names** or **Show all**. Allows searches for Microsoft groups.
- **Highlight already selected groups in search results:** If a Microsoft Group 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 Group



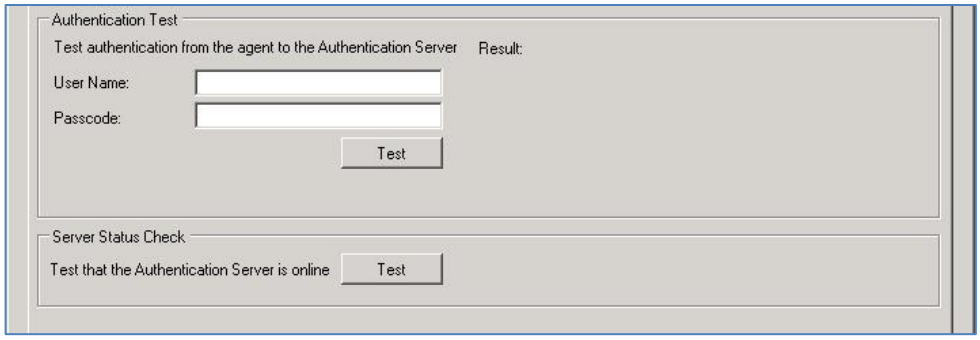
- **Primary Server (IP:Port):** Used to configure the IP address/hostname of the primary SafeNet Authentication Service. Default is port **80**. Alternatively, **Use SSL** can also be selected. Default TCP port for SSL requests is **443**.
- **Failover Server (Optional):** Used to configure the IP address/hostname of the failover SafeNet Authentication Service. Default is port **80**. Alternatively, **Use SSL** can also be selected. Default TCP port for SSL requests is **443**.
- **Attempt to return to primary Authentication Server every:** Sets the Primary Authentication Server retry interval. This setting only takes effect when the agent is using the **Failover Server** entry.
- **Communication Timeout:** Sets the maximum timeout value for authentication requests sent to SAS.
- **Agent Encryption Key File:** Used to specify the location of the SAS 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.

Once stripping has been activated or deactivated for a SharePoint site, the agent stores these values and uses them as default for each new SharePoint site protected by the agent.

Authentication Test Group

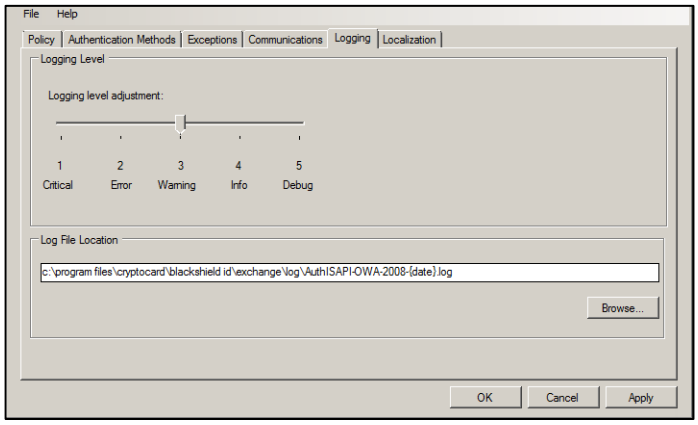
Allows administrators to test authentication between the agent and SafeNet Authentication Service.



Server Status Check Group

Performs a communication test to verify a connection to SafeNet Authentication Service.

Logging Tab



Logging Level Group

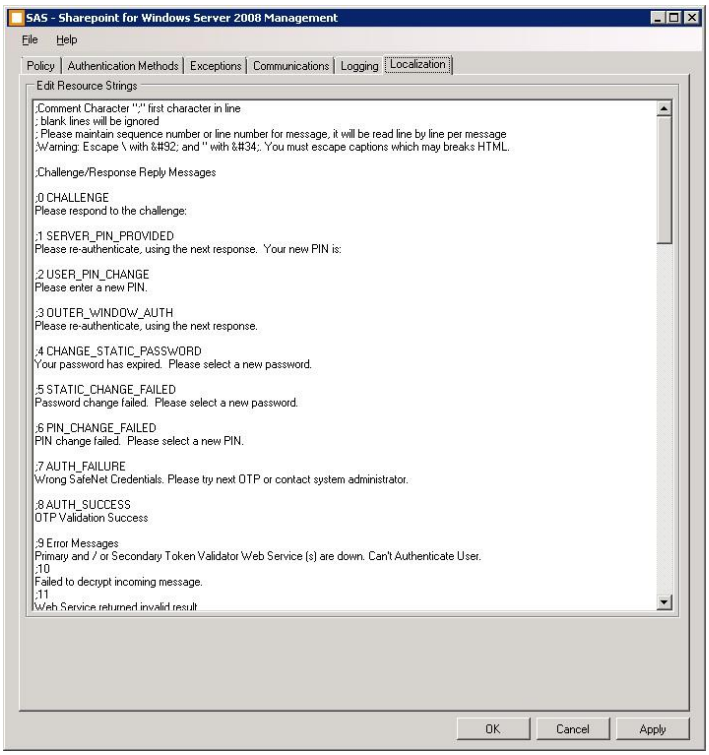
Adjusts the logging level. For log levels 1, 2, and 3, only the initial connection between the agent and the server, and any failed connection attempts, are logged. Log level 5 sets the agent into debug mode. Default value is **3**.

Log File location Group

Specifies the location of the log files. The log file is rotated on a daily basis. The default location is **\Program Files\CRYPTOCard\SAS \Exchange\Log**.

Localization Tab

NOTE: English is the only language supported in the current release.



The settings in this tab represent the prompts and information messages provided by the SAS agent. These can be modified as necessary to improve usability. The **Messages.txt** file can also be manually modified outside of the configuration tool. This file can be found in the **\Program Files\CRYPTOCard\SAS \Exchange\LocalizedMessages** folder.

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 phone support is available to you.

Table 1: Support Contacts

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.	