SafeNet Authentication Service

Configuration Guide

SAS Agent for Microsoft Internet Information Services (IIS)

Document Information

Product Version	1.05
Release Date	13 April 2015
Product Number	007-012393-002, Rev D

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

By default, logon to Microsoft Terminal Services Web (TS Web) and Remote Desktop Web (RD Web) requires that a user provide a correct user name and password. This document describes the steps necessary to augment this logon mechanism with strong authentication by adding a requirement to provide a one-time password generated by a SafeNet token.

NOTE: In Windows Server 2012 and Windows Server 2012 R2, Terminal Services Web Access (TS Web Access) and Remote Desktop Web (RD Web) are included as part of Remote Desktop Web Access (RD Web Access).

The SafeNet Authentication Service (SAS) Agent for Microsoft Internet Information Services (IIS) is designed for Terminal Services Web (TS Web) and Remote Desktop Web (RD Web), but may also be used for IIS websites where the authentication method is configured to use Microsoft authentication. The agent ensures web-based resources are accessible only by authorized users, whether working remotely or inside the firewall, by prompting for additional credentials during logon.

Applicability

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 Applications and Objects	• Remote Desktop Web • Terminal Services Web Sites, Virtual Directories, Applications
Supported IIS Authentication Type	Microsoft Authentication (Basic Authentication)
Supported Web Browsers	• Internet Explorer 9,10,11 • Firefox • Chrome
Additional Web Browser Requirements	• Cookies must be enabled • JavaScript must be enabled • ActiveX plug-ins (software token detection only)

Authentication Modes

There are two login authentication modes available in the SAS Agent for Microsoft Internet Information Services (IIS).

Mode	Description
Standard Authentication Mode	Standard Authentication Mode enables a single-stage login process. Microsoft and SafeNet credentials must be entered into the SafeNet 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 SafeNet 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.

By default, **Split Authentication Mode** is enabled. The authentication mode can be modified after installation using the **SAS Agent for Microsoft IIS Configuration Tool**.

Standard Authentication Mode (Hardware and Software)

1. The user enters the URL into their web browser.
2. The SAS Agent for Microsoft IIS examines the incoming request against its **IP Range Exclusions/Inclusions** list to determine if SafeNet authentication can be ignored.
3. If IP address exclusion is detected, SafeNet credentials are not required. The user authenticates using Microsoft credentials.
4. If IP address exclusion is not detected, a SafeNet-enabled login page appears.
5. If a software token is detected, the SafeNet 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 SafeNet login page will display **Microsoft Username**, **Microsoft Password**, and **OTP** fields.
7. The user enters their Microsoft and SafeNet credentials into the login page. If both sets of credentials are valid, the user is presented with their website; otherwise, the attempt is rejected.

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

1. The user enters the URL into their web browser.
2. The SAS Agent for Microsoft IIS examines the incoming request against its **IP Range Exclusions/Inclusions** list to determine if SafeNet authentication can be ignored.
3. If IP address exclusion is detected, SafeNet credentials are not required. The user authenticates using Microsoft credentials.
4. If IP address exclusion is not detected, a SafeNet-enabled login page appears.
5. If a software token is detected, the SafeNet 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 SafeNet 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 credentials into the login page. If both sets of credentials are valid, the user is presented with their website; 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 credentials entered are valid, the user is presented with their website; otherwise, the attempt is rejected.

Split Authentication Mode

1. The user enters the URL into their web browser.
2. The SAS Agent for Microsoft IIS examines the incoming request against its **IP Range Exclusions/Inclusions** list to determine if SafeNet authentication can be ignored.
3. If IP address exclusion is detected, SafeNet credentials are not required. The user authenticates and logs in to the website 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 SAS Agent for Microsoft IIS examines the Microsoft username against its **Group Authentication Exceptions** list to determine if SafeNet authentication can be ignored.
6. If a group authentication exception is detected, SafeNet credentials are not required. The user is presented with their website.
7. If a group authentication exception is not detected, the SAS 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 credentials are valid, the user is presented with their website; otherwise, the attempt is rejected.
9. If a software token is detected, the SafeNet login page will display the token name and a **PIN** field. The option to toggle between hardware and software mode is available.
10. If a software token is not detected, the SafeNet login page will display an **OTP** field.
11. The user enters their SafeNet credentials into the login page. If the credentials are valid, the user is presented with their website; otherwise, the attempt is rejected.

Installation

Prerequisites

- If the web site is configured to use Basic Authentication ensure that NTLM is disabled.
- If the web site is configured to use Windows Authentication ensure that NTLM is enabled.
- Ensure that TCP port 80 or 443 is open between the SAS Agent for Microsoft IIS and the SAS server.
- Administrative rights to the Windows system are required during installation and configuration of the SAS for Microsoft IIS Agent.
- Add an Auth Node in SafeNet Authentication Service (SAS)
  - In the **SAS Management Console**, select **VIRTUAL SERVERS > COMMS > Auth Nodes**. Enter the name or IP address of the computer where SAS Microsoft IIS Agent is installed.
  - For details, refer to the *SAS Service Provider Administrator Guide*.

Installing the SAS for Microsoft IIS Agent

1. Log on to the IIS web server as a user with administrative privileges.
2. Locate and run the **SAS Agent for IIS 7 x64.exe** installation package.

NOTE: The **SAS Agent for IIS 7 x64.exe** installation package supports both IIS 7.x and IIS 8.x.

3. Accept the license agreement.
4. Select the installation destination folder, and then proceed with the installation.

Configuring IIS for Use with the SAS for Microsoft IIS Agent

The SAS for Microsoft IIS Agent requires that Terminal Services Web and Remote Desktop Web are configured to use Basic Authentication or Windows Authentication. Prior to enabling the SAS Agent for Microsoft IIS, the following steps must be performed.

Basic Authentication

Remote Desktop Web

1. Launch the IIS Manager from **Administrative Tools**.
2. Click **Computer Name > Sites > Default Web Site > RDWeb**.
3. Select **Pages**. In the **IIS** section of the **Features View** pane, select **Authentication**.
   - Disable **Anonymous** and **Forms Authentication**.
   - Enable **Basic Authentication**.
4. In the **Edit Basic Authentication Settings** window, in the **Default domain** field, enter a default domain or leave it blank. Users who do not provide a domain when they log on to your site are authenticated against this domain.
5. .In the Realm text box, enter a realm or leave it blank. In general, you can use the same value for the realm name that you used for the default domain.

Caution: If you enter the default domain name in the **Realm** text box, your internal Microsoft Windows domain name may be exposed to external users during the user name and password challenge.

6. Click **OK** to close the **Edit Basic Authentication Settings** window.

Terminal Services Web

1. Launch the IIS Manager from **Administrative Tools**.
2. Click **Computer Name > Sites > Default Web Site**.
3. Select **TS**.
4. In the **IIS** section of the **Features View** pane, select **Authentication**.
   - Disable **Windows Authentication**.
   - Enable **Basic Authentication**.
5. In the **Edit Basic Authentication Settings** window, in the **Default domain** field, enter a default domain or leave it blank. Users who do not provide a domain when they log on to your site are authenticated against this domain.
6. .In the Realm text box, enter a realm or leave it blank. In general, you can use the same value for the realm name that was used for the default domain.

> **Caution:** If you enter the default domain name in the **Realm** text box, your internal Microsoft Windows domain name may be exposed to external users during the user name and password challenge.

7. Click **OK** to close the **Edit Basic Authentication Settings** window.

Windows Authentication

Terminal Services Web

1. Launch the IIS Manager from **Administrative Tools**.
2. Click **Computer Name > Sites > Default Web Site**.
3. Select **TS**.
4. In the **IIS** section of the **Features View** pane, select **Authentication**.
   - Enable **Windows Authentication**.
   - Disable **Basic Authentication**.
5. In the **Edit Windows Authentication Settings** window, in the **Default domain** field, enter a default domain or leave it blank. Users who do not provide a domain when they log on to your site are authenticated against this domain.
6. .In the Realm text box, type a realm or leave it blank. In general, you can use the same value for the realm name as you used for the default domain.

> **Caution:** If you enter the default domain name in the **Realm** text box, your internal Microsoft Windows domain name may be exposed to external users during the user name and password challenge.

7. Click **OK** to close the **Edit Basic Authentication Settings** window.

Enabling the SAS Microsoft IIS Agent

These basic instructions are required to enforce SafeNet authentication during logon to Terminal Services Web or Remote Desktop Web. For more in-depth information on each setting, refer to the “Configuring the SAS Agent for Microsoft IIS section, on page 12.

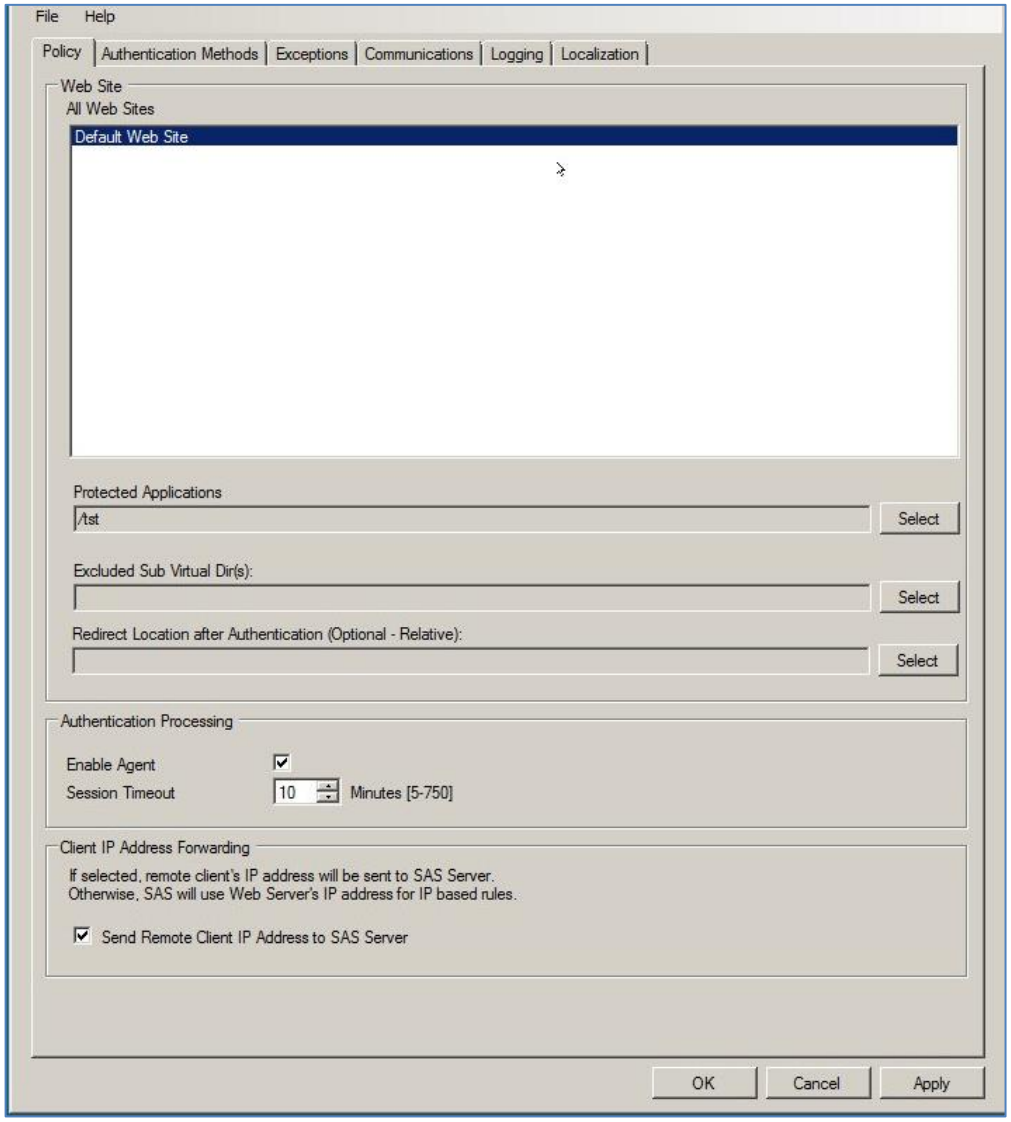
1. Click **Start > All Programs > SafeNet > SAS Agent for IIS 7 > IIS 7 Agent Configuration**.
2. On the **Policy** tab, under **All Web Sites**, select **Default Web Site**.
   a. Under **Protected Applications**, select **/RDWeb/Pages** for Remote Desktop Web or **/TS** for Terminal Services Web.
   b. Select **Enable Agent**, and then select any additional settings required.
3. Click the **Communications** tab. Verify that the **Authentication Server Settings** reflect the location of the SAS server.
4. Verify that all other tabs meet your requirements.
5. Apply the settings. The IIS server will restart for the settings to take effect.

Configuring the SAS Agent for Microsoft IIS

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

Policy Tab

The **Policy** tab provides the ability to select a website and then protect web-based resources with SafeNet authentication. When a website is selected, all settings defined within each tab apply to the specific website. If another website is selected, all tabs revert to their customized or default settings allowing a different configuration to be applied.



Website

- **All Websites:** Allows the selection of the website. The website selection will determine the list displayed within **Protected Applications**.
- **Protected Applications:** Allows the selection of an application or virtual directory (single or multiple).

Authentication Processing

- **Enable Agent:** Turns the SAS Agent for Microsoft IIS on or off. The default value is **Disabled**.
- **Session Timeout:** Specifies the amount of time in minutes that the user may remain idle before they are required to re-authenticate with their SafeNet credentials. The default value is **10** minutes.

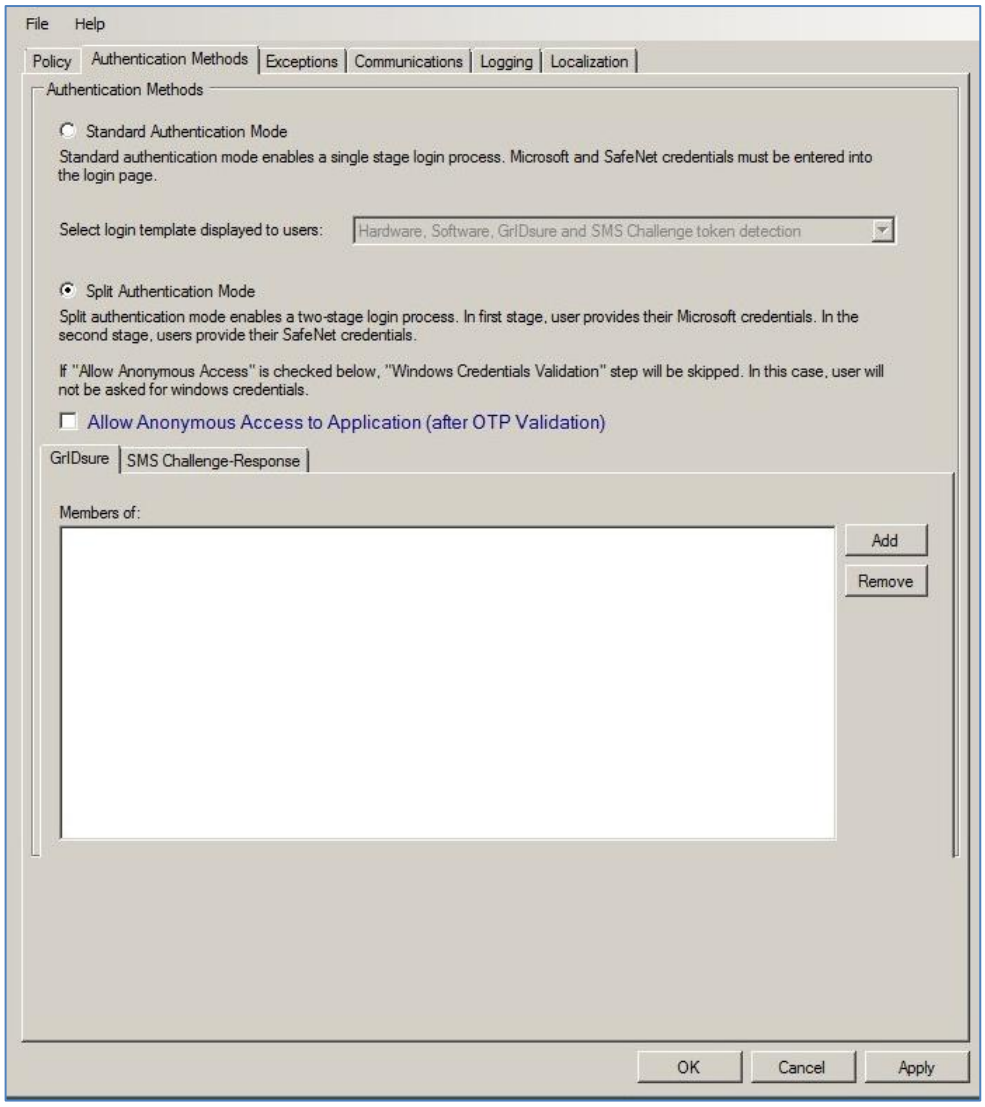
Client IP Address Forwarding

If selected, the remote client IP address will be sent to the SAS server. Otherwise, the web server's IP Address will be used. The default value is **Enabled**.

Note: Due to a known defect, the **Client IP Address Forwarding** option is not visible with low resolution screens.

Authentication Methods Tab

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



Authentication Methods

The following authentication modes are available:

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

  This 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.

Note: When logging in, the default settings are those of the Hardware token.

- **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 can be used to select a different token type. If a software token does not exist, 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.

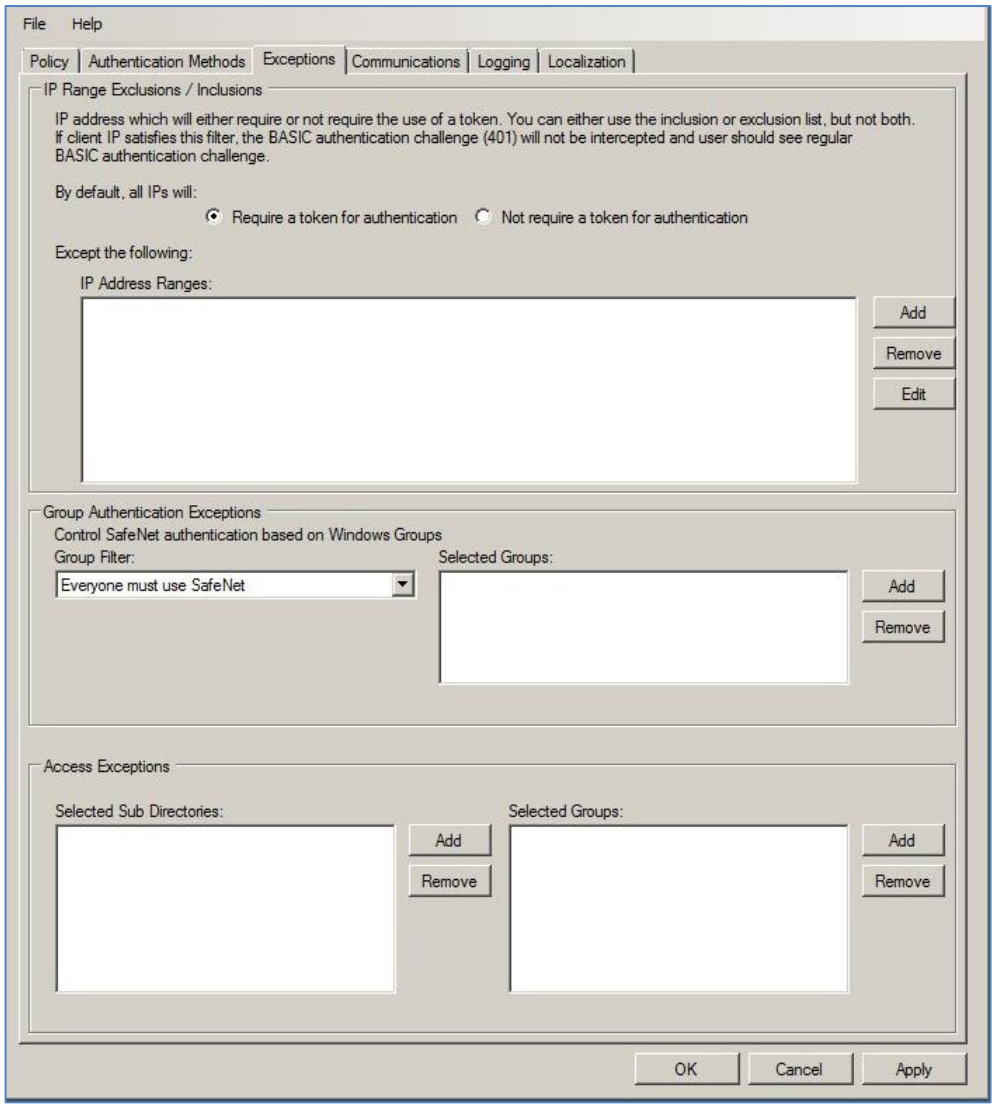
- **Split Authentication Mode:** This mode enables a two-stage login process. In the first stage, users provide their Microsoft credentials. In the second stage, users provide their SafeNet credentials. The default value is **Enabled**.

  This mode provides the following advantages over Standard Authentication mode:

  - Microsoft group exclusions may be used to migrate users incrementally 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 provides 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 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 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. By default, all users are required to perform SafeNet authentication unless otherwise defined by exception.



IP Range Exceptions/Inclusions

This function allows an administrator to define which network traffic requires SafeNet authentication. By default, all networks are required to perform SafeNet authentication.

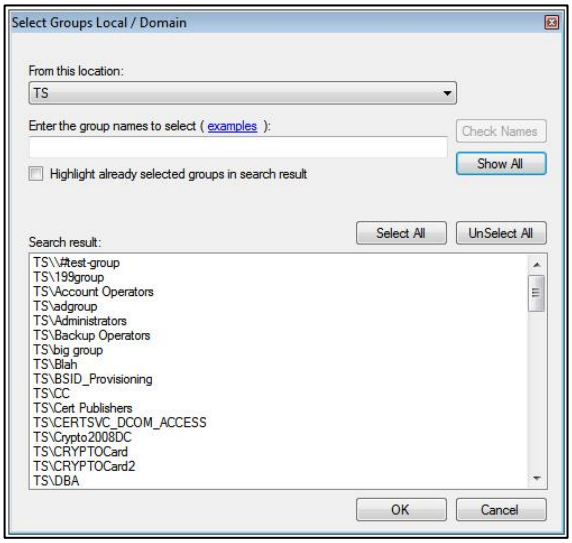
Group Authentication Exceptions

Group authentication exceptions omit single and/or multiple 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**.

The following group authentication exceptions are available:

- **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.

After you enter a group authentication exception, the **Select Groups local/Domain** window opens:



- **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.

Access Exceptions

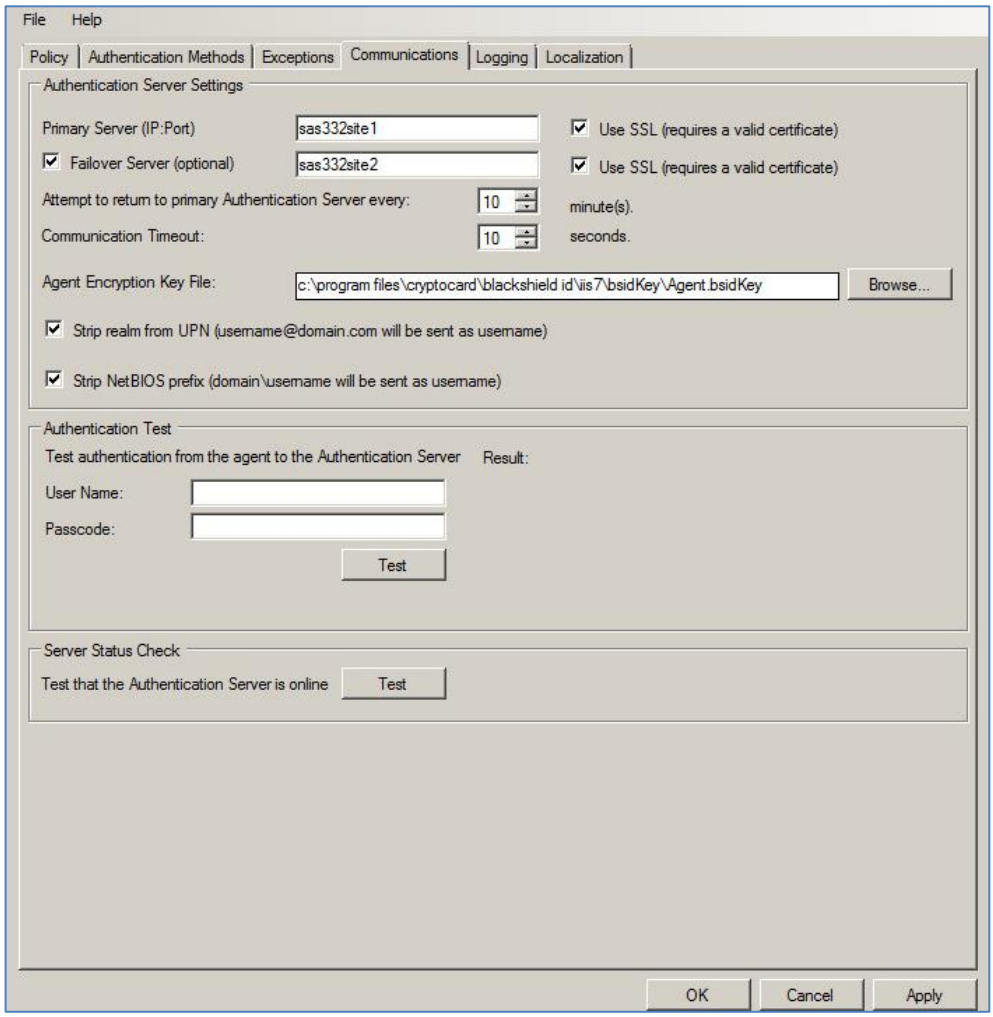
Access Exceptions blocks access to specified subdirectories in the website selected in the **Policy** tab.

- **Selected Sub Directories:** Select the required subdirectory.
- **Selected Group:** Select the groups for which access to the selected website sub-directories.

Users who are members of the selected groups will receive an error message when attempting to access the blocked location, as follows: “Access to this URL is blocked by the system administrator.”

Communications Tab

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



Authentication Server Settings

- **Primary Server (IP:Port)**: Used to configure the IP address/hostname of the primary SAS server. The default is port 80. Alternatively, **Use SSL** can also be selected. The default TCP port for SSL requests is **443**.
- **Failover Server (Optional):** Used to configure the IP address/hostname of the failover SAS server. The default is port **80**. Alternatively, **Use SSL** can also be selected. The default TCP port for SSL requests is **443**.
- **Attempt to return to primary Authentication Server every:** Sets the Primary Authentication server retry interval in minutes. This setting only takes effect when the agent is using the **Failover Server** entry.
- **Communication Timeout:** Sets the maximum timeout value in seconds for authentication requests sent to the SAS server.
- **Agent Encryption Key File:** Used to specify the location of the SAS for Microsoft IIS 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 an IIS site, the agent stores these values and uses them as default for each new IIS site protected by the agent.

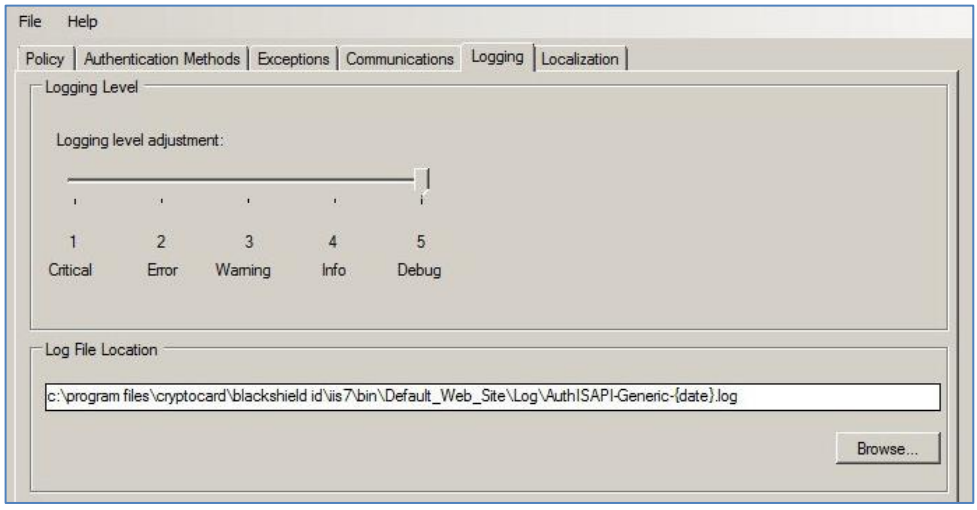
Authentication Test

This function allows administrators to test authentication between the SAS for Microsoft IIS Agent and the SAS server.

Server Status Check

This function performs a communication test to verify a connection to the SAS server.

Logging Tab

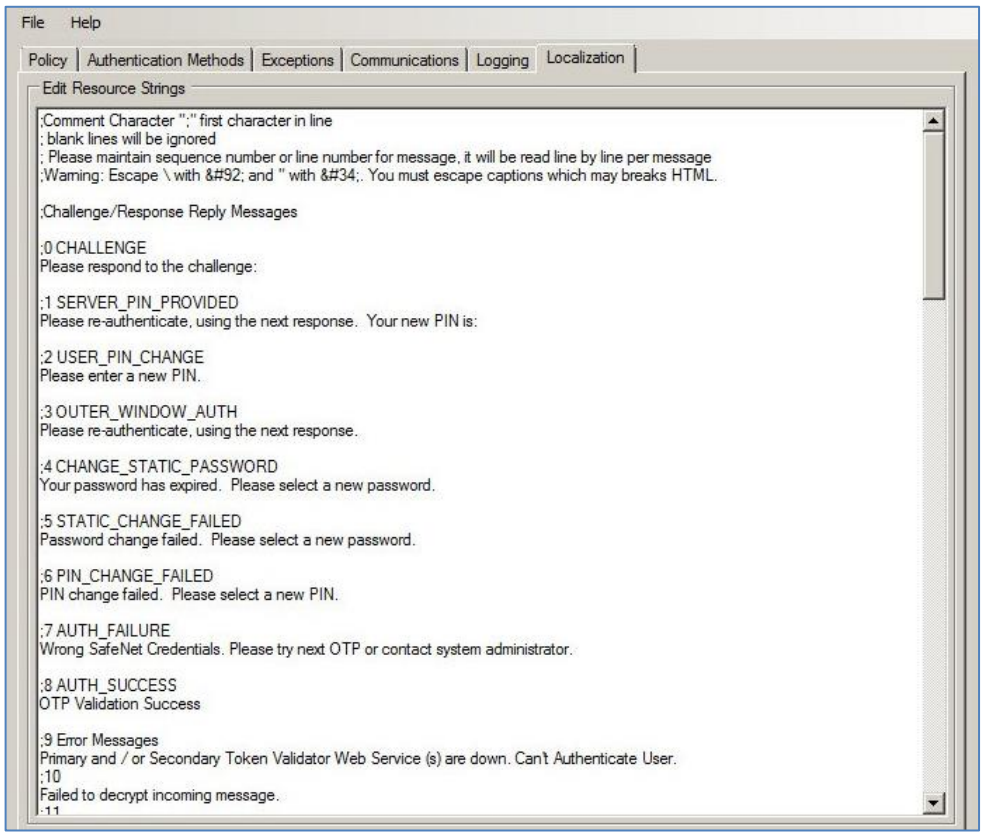


The **Logging** tab contains the following settings:

- **Logging Level:** Adjusts the logging level. For log levels 1, 2, and 3, only the initial connection between the agent and server attempts are logged. Log level 5 sets the agent in debug mode. The default value is **3**.
- **Log File Location:** Specifies the location of the log files. The log file is rotated on a daily basis. The default log file location is **\Program Files\SafeNet\SAS\IIS7\bin\Web_Site_Name\Log**.

Localization Tab

The settings on this tab represent the prompts and information messages supplied by the 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 folder **\Program Files\SafeNet\SAS\IIS7\LocalizedMessages**.



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.

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
Email	support@safenet-inc.com	
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.	