All information herein is either public information or is the property of and owned solely by Gemalto NV. 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 Gemalto’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, Gemalto 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, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto 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 Gemalto 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.

Gemalto 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. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto 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.

© 2015 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto 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: 1.06
Document Part Number: 007-012393-002, Rev. E
Release Date: 28 January 2016
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audience</td>
<td>4</td>
</tr>
<tr>
<td>Related Documents</td>
<td>4</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>5</td>
</tr>
<tr>
<td>Introduction</td>
<td>6</td>
</tr>
<tr>
<td>Applicability</td>
<td>7</td>
</tr>
<tr>
<td>Authentication Modes</td>
<td>8</td>
</tr>
<tr>
<td>Standard Authentication Mode (Hardware and Software)</td>
<td>8</td>
</tr>
<tr>
<td>Standard Authentication Mode (Hardware, Software and GrIDsure/SMS)</td>
<td>9</td>
</tr>
<tr>
<td>Split Authentication Mode</td>
<td>9</td>
</tr>
<tr>
<td>Installation</td>
<td>10</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>10</td>
</tr>
<tr>
<td>Installing SAS Agent for IIS</td>
<td>10</td>
</tr>
<tr>
<td>Replacing Previously Installed Versions</td>
<td>11</td>
</tr>
<tr>
<td>Importing Configuration Settings from an Earlier Version of the Agent</td>
<td>11</td>
</tr>
<tr>
<td>Transferring Localization Settings</td>
<td>12</td>
</tr>
<tr>
<td>Importing Configuration Settings from the Same Version of the Agent</td>
<td>12</td>
</tr>
<tr>
<td>Configuring IIS for Use with SAS Agent for IIS</td>
<td>13</td>
</tr>
<tr>
<td>Activating Basic Authentication</td>
<td>13</td>
</tr>
<tr>
<td>Terminal Services Web</td>
<td>13</td>
</tr>
<tr>
<td>Configuring SAS Agent for IIS</td>
<td>14</td>
</tr>
<tr>
<td>Policy Tab</td>
<td>15</td>
</tr>
<tr>
<td>Website</td>
<td>15</td>
</tr>
<tr>
<td>Authentication Processing</td>
<td>16</td>
</tr>
<tr>
<td>Client IP Address Forwarding</td>
<td>16</td>
</tr>
<tr>
<td>Authentication Methods Tab</td>
<td>17</td>
</tr>
<tr>
<td>Authentication Methods</td>
<td>17</td>
</tr>
<tr>
<td>Exceptions Tab</td>
<td>19</td>
</tr>
<tr>
<td>IP Range Exceptions/Inclusions</td>
<td>19</td>
</tr>
<tr>
<td>Group Authentication Exceptions</td>
<td>19</td>
</tr>
<tr>
<td>Access Exceptions</td>
<td>20</td>
</tr>
<tr>
<td>Communications Tab</td>
<td>21</td>
</tr>
<tr>
<td>Authentication Server Settings</td>
<td>21</td>
</tr>
<tr>
<td>Authentication Test</td>
<td>22</td>
</tr>
<tr>
<td>Server Status Check</td>
<td>22</td>
</tr>
<tr>
<td>Logging Tab</td>
<td>22</td>
</tr>
<tr>
<td>Localization Tab</td>
<td>23</td>
</tr>
</tbody>
</table>
Preface

Audience

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

The document describes how to install and deploy Microsoft Internet Information Services (IIS) with SafeNet Authentication Service.

All products manufactured and distributed by Gemalto, 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:

- SAS Agent for Microsoft Internet Information Services Configuration Guide (PN: 007-012393-002)
- SAS Agent for Microsoft Internet Information Services Frequently Asked Questions (PN: 007-013419-00)
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>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>Gemalto, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland  21017, USA</td>
</tr>
<tr>
<td><strong>Phone</strong></td>
<td><strong>US</strong></td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td><strong>International</strong></td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td><strong>Technical Support</strong></td>
<td><strong>Customer Portal</strong></td>
</tr>
<tr>
<td></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
Introduction

SafeNet Authentication Service Agent for Microsoft Internet Information Services (SAS Agent for IIS) is designed for Terminal Services Web (TS Web), but may also be used for IIS websites, resources are accessible only to authorized users, whether working remotely or behind a firewall, by prompting for additional credentials during logon.

By default, logon to TS Web requires that the user provide a correct user name and password. SAS Agent for IIS augments this logon mechanism with strong authentication by adding a requirement to provide a one-time password generated by a Gemalto token.
### 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                        | Terminal Services Web Sites, Virtual Directories, Applications |
| Supported IIS Authentication Type                         | Microsoft Authentication (Basic Authentication)       |
| Supported Web Browsers                                    | Internet Explorer 9,10,11                             |
|                                                           | Microsoft Edge                                       |
|                                                           | Firefox                                               |
|                                                           | Chrome                                                |
| 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 login authentication modes available in SAS Agent for IIS.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Authentication Mode</td>
<td>Standard Authentication Mode enables a single-stage login process. Microsoft and SafeNet credentials must be entered into the SafeNet login page.</td>
</tr>
<tr>
<td>Split Authentication Mode</td>
<td>Split Authentication Mode enables a two-stage login process:</td>
</tr>
<tr>
<td></td>
<td>• In the first stage, users provide their Microsoft credentials.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>

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

**Standard Authentication Mode (Hardware and Software)**

1. The user enters the URL into their web browser.
2. 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. 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. 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. 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, 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

**NOTE:** Administrative rights to the Windows system are required during installation and configuration of SAS Agent for IIS.

- 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 SAS Agent for IIS and the SAS server.
- 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 Agent for IIS is installed.
  - For details, refer to the **SAS Service Provider Administrator Guide**.

Installing SAS Agent for IIS

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

**NOTE:** 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.
Replacing Previously Installed Versions

- Automatic upgrade from earlier versions of SAS Agent for IIS to version 1.06 is not supported. Instead, the configuration from the older version must be saved, using the Export Utility, and then imported into the new installation. See “Importing Configuration Settings from an Earlier Version of the Agent” on page 11.

- In addition, the Localization settings of the older version must be saved and used in the newly installed SAS Agent for IIS to version 1.06. See “Transferring Localization Settings” on page 12.

- If SAS Agent for IIS 1.06 is to be uninstalled and the same version re-installed, the configuration from the original installation must be saved. See “Importing Configuration Settings from the Same Version of the Agent” on page 12.

Importing Configuration Settings from an Earlier Version of the Agent

To keep the settings from SAS Agent for IIS 1.04 or 1.05 for use in version 1.06, use the Export Configuration Utility (ExportIISAgentUtility.exe).

NOTE: The Export Configuration Utility (ExportIISAgentUtility.exe) is included in the software package.

The utility is used to export the configuration settings from the currently installed version (1.04 or 1.05). These settings are then imported into 1.06 using the Load Saved Configuration feature.

To Import settings from an earlier installation of SAS Agent for IIS:

1. Place the Export Configuration Utility (ExportIISAgentUtility.exe) in the installation path of the previously installed version of SAS Agent for IIS.
   By default the installation directory is C:\Program Files\CRYPTOCARD\BlackShield ID\IIS7\bin
2. Run the Export Configuration Utility:
   a. Double click on ExportIISAgentUtility.exe
   b. When the window opens, press Enter.
   A file of the settings (Backup.bsidConfig) is created.
3. Make a copy of Backup.bsidConfig and save in a different location for later use.
4. Uninstall SAS Agent for IIS 1.04 or 1.05.
5. Delete the installation folder of the agent manually.
6. Install SAS Agent for IIS 1.06
7. In SAS Agent for Microsoft IIS Configuration Tool window, select File > Load Saved Configuration.
8. Navigate to the saved configuration file (Backup.bsidConfig) and click Open.
   The saved configuration is imported into the newly installed SAS Agent for IIS 1.06.

NOTE: The export and import of the configuration file (ExportIISAgentUtility.exe) must be performed from the same location. By default, the path is C:\Program Files\CRYPTOCARD\BlackShield ID\IIS7\bin. If a non-default directory was used in the original installation, the same path must be used for the new installation.
Transferring Localization Settings

To preserve changes made to the localization settings in the earlier installation, the messages.txt file must be saved and used in the new installation.

To Import localization settings from an earlier installation of SAS Agent for IIS:

1. Before uninstalling the previous installation of SAS Agent for IIS, make a copy of the messages.txt file (Default: C:\Program Files\CRYPTOCARD\BlackShield ID\IIS7\LocalizedMessages) and save in a different location for later use.

2. After installing SAS Agent for IIS and after importing the configuration, replace the messages.txt file in the same directory (Default: C:\Program Files\CRYPTOCARD\BlackShield ID\IIS7\LocalizedMessages).

Importing Configuration Settings from the Same Version of the Agent

If you uninstall SAS Agent for IIS 1.06 and re-install the same version, you can use the agent’s Export Current Configuration and Load Saved Configuration functions to transfer the configuration. The Export Configuration Utility is not required.

To transfer configuration settings when re-installing SAS Agent for IIS 1.06:

1. On the previously installed SAS Agent for IIS 1.06, select File>Export Current Configuration. A file of the settings (Backup.bsidConfig) is created.
2. Make a copy of Backup.bsidConfig and save in a different location for later use.
3. Uninstall the previously installed SAS Agent for IIS 1.06.
4. Delete the installation folder of SAS Agent for IIS 1.06 manually.
5. Install SAS Agent for IIS 1.06.
6. In SAS Agent for Microsoft IIS Configuration Tool window, select File > Load Saved Configuration.
7. Navigate to the saved file Backup.bsidConfig and click Open.
   The saved configuration is imported into the newly installed SAS Agent for IIS.
Configuring IIS for Use with SAS Agent for IIS

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

Activating Basic Authentication

1. Launch the IIS Manager from Administrative Tools.
2. Navigate to Computer Name > Sites > Default Web Site.
3. In the IIS section of the Features View pane, select Authentication.
4. Enable Basic Authentication and ensure that all other authentication types are disabled.

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. Unusually, 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.
Enabling SAS Agent for IIS

These basic instructions are required to enforce SafeNet authentication during logon to Terminal Services Web. For more information on each setting, refer to the “Configuring SAS Agent for IIS section, on page 15.

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 the websites that you want to protect
   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 SAS Agent for IIS

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

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 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 Tab](image)

**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**: Not all users are required to perform SafeNet authentication; only 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 SAS Agent for IIS 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 SAS Agent for IIS and the SAS server.

### Server Status Check

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

### Logging Tab

![Logging Tab](image)

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`. 

![Localization Tab Image](image-url)