



# SafeNet Agent for Internet Information Services 2.0.1

## INSTALLATION AND CONFIGURATION GUIDE



All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates 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 Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as "Thales") 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, Thales 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, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

**Thales 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 Thales 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.**

**Thales 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 Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales 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.**

Copyright © 2018-2020 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and affiliates and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the properties of their respective owners.

# CONTENTS

Preface: About the SafeNet Agent for Internet Information Services Guide .....	5
Customer Release Notes .....	5
Audience .....	5
Document Conventions .....	5
Command Syntax and Typeface Conventions .....	5
Notifications and Alerts .....	6
Support Contacts .....	7
<b>Chapter 1: Introduction .....</b>	<b>8</b>
Overview .....	8
Compatibility and Component Information .....	8
Authentication Server .....	8
Network .....	8
Supported Architecture .....	8
Supported Web Servers .....	8
Supported Applications and Objects .....	8
Supported IIS Authentication Type .....	8
Supported Web Browsers .....	9
Additional Software Components .....	9
Additional Web Browser Requirements .....	9
Supported Authentication Methods .....	9
Authentication Modes .....	9
Standard Authentication Mode .....	10
Split Authentication Mode .....	10
Prerequisites .....	11
<b>Chapter 2: Installing the SafeNet Agent for Internet Information Services .....</b>	<b>12</b>
Installing the Agent .....	12
Configuring Internet Information Services .....	17
Activating Basic Authentication .....	17
Configuring Terminal Services Web .....	17
Enabling the Agent .....	17
Uninstalling the Agent .....	18
Configuring Transport Layer Security .....	18
<b>Chapter 3: Configuring the SafeNet Agent for Internet Information Services .....</b>	<b>19</b>
Policy .....	19
Web Site .....	20
Authentication Processing .....	21
Client IP Address Forwarding .....	21
Authentication Methods .....	22

---

Authentication Methods .....	22
Exceptions .....	24
IP Range Exclusions / Inclusions .....	24
Access Exceptions .....	25
Communications .....	26
Authentication Server Settings .....	26
Authentication Test .....	27
Server Status Check .....	27
Logging .....	28
Logging Level .....	28
Log File Location .....	28
Localization .....	29
Chapter 4: Configuring Initialization File for Specific Request Headers (Optional) .....	30
Chapter 5: Upgrading the SafeNet Agent for Internet Information Services .....	31
Migrating the Agent .....	31
Chapter 6: Testing the SafeNet Agent for Internet Information Services .....	33
Hardware / Software .....	33
GrIDSure / SMS Challenge .....	34

# **PREFACE:** About the SafeNet Agent for Internet Information Services Guide

## Customer Release Notes

---

The Customer Release Notes (CRN) provide important information about this release that is not included in the customer documentation. It is strongly recommended that you read the CRN to fully understand the capabilities, limitations, and known issues for this release.

## Audience

---

This document is intended for personnel responsible for maintaining your organization's security infrastructure. This includes SafeNet Authentication Service (SAS) / SafeNet Trusted Access (STA) users and security officers, 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 Thales Group 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.

## Document Conventions

---

This section describes the conventions used in this document.

### Command Syntax and Typeface Conventions

This document uses the following conventions for command syntax descriptions, and to highlight elements of the user interface.

Format	Convention
<b>bold</b>	The bold attribute is used to indicate the following: <ul style="list-style-type: none"> <li>&gt; Command-line commands and options that you enter verbatim (Type <b>dir /p</b>.)</li> <li>&gt; Button names (Click <b>Save As</b>.)</li> <li>&gt; Check box and radio button names (Select the <b>Print Duplex</b> check box.)</li> <li>&gt; Dialog box titles (On the <b>Protect Document</b> dialog box, click <b>Yes</b>.)</li> <li>&gt; Field names (<b>User Name</b>: Enter the name of the user.)</li> <li>&gt; Menu names (On the <b>File</b> menu, click <b>Save</b>.) (Click <b>Menu &gt; Go To &gt; Folders</b>.)</li> <li>&gt; User input (In the <b>Date</b> box, type <b>April 1</b>.)</li> </ul>
<i>italics</i>	In type, the italic attribute is used for emphasis or to indicate a related document. (See the <i>Installation Guide</i> for more information.)
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[optional] [<optional>]	Represent optional <b>keywords</b> or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.
{a b c} {<a> <b> <c>}	Represent required alternate <b>keywords</b> or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.
[a b c] [<a> <b> <c>]	Represent optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.

## Notifications and Alerts

Notifications and alerts are used to highlight important information or alert you to the potential for data loss or personal injury.

### Tips

Tips are used to highlight information that helps to complete a task more efficiently.

**TIP** This is some information that will allow you to complete your task more efficiently.

### Notes

Notes are used to highlight important or helpful information.

**NOTE** Take note. Contains important or helpful information.

## Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss.

**CAUTION!** Exercise caution. Contains important information that may help prevent unexpected results or data loss.

## Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury.

**\*\*WARNING\*\*** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.

## Support Contacts

---

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or [Thales Group Customer Support](#).

Thales Group 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 Thales Group and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

### Customer Support Portal

The Customer Support Portal, at <https://supportportal.gemalto.com>, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

**NOTE** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

### Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales Group Customer Support by telephone at [+1 410-931-7520](tel:+14109317520). Additional local telephone support numbers are listed on the support portal.

### Email Support

You can also contact technical support by email at [technical.support@gemalto.com](mailto:technical.support@gemalto.com).

# CHAPTER 1: Introduction

## Overview

---

The SafeNet Agent for Internet Information Services is designed for Terminal Services Web (TS Web), but can also be used for IIS websites and resources where the authentication method is configured to use the Microsoft authentication. The agent ensures web-based 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 the TS Web requires that the user provide a correct user name and password. The SafeNet Agent for Microsoft IIS augments this logon mechanism with strong authentication by adding a requirement to provide a One-Time Password (OTP) generated by a Thales Group token.

## Compatibility and Component Information

---

### Authentication Server

- > SafeNet Authentication Service PCE/SPE 3.9.2 and later
- > SafeNet Authentication Service Cloud

### Network

- > TCP Port 80 or 443

### Supported Architecture

- > 64-bit

### Supported Web Servers

- > IIS 8.5
- > IIS 10

### Supported Applications and Objects

- > Terminal Services Web Sites
- > Virtual Directories
- > Applications

### Supported IIS Authentication Type

- > Microsoft Authentication (Basic Authentication)



## Supported Web Browsers

- > Internet Explorer 11
- > Microsoft Edge
- > Firefox
- > Chrome

## Additional Software Components

- > Microsoft .NET Framework 4.5.2 (or above) must be installed.
- > Following ASP .NET versions (Server role component) must be installed:
  - 2012 R2 – ASP .NET 4.5 (or above)
  - Windows Server 2016 – ASP .NET 4.6 (or above)
- > IIS 6 Management Compatibility Role Service (and its sub components) must be installed.

## 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 Modes

There are two login authentication modes available for the SafeNet Agent for Microsoft IIS.

By default, **Standard Authentication Mode** is enabled. The authentication mode can be modified after installation using ["Configuring the SafeNet Agent for Internet Information Services" on page 19](#) > ["Authentication Methods" on page 22](#) tab.

Mode	Description
<b>Standard Authentication Mode</b>	Standard Authentication Mode enables a single-stage login process. Microsoft and SafeNet credentials must be entered in the SafeNet login page to access resources.
<b>Split Authentication Mode</b>	<p>Split Authentication Mode enables a two-stage login process:</p> <ul style="list-style-type: none"> <li>&gt; In the first stage, users provide their Microsoft credentials.</li> <li>&gt; In the second stage, users provide their SafeNet credentials.</li> </ul> <p>This mode allows administrators to control authentication dialogs based on Microsoft groups or token type (such as GrIDSure).</p> <p>This is the preferred mode when migrating from static to One-Time Passwords (OTPs).</p>

## Standard Authentication Mode

1. The user enters the URL into a web browser.
2. The SafeNet Agent for Microsoft IIS examines the incoming request against its "**IP Range Exclusions / Inclusions**" on page 24 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 their Microsoft credentials.
4. If IP address exclusion is not detected, a SafeNet-enabled login page appears.
5. The agent's authentication page is displayed with the following fields:
  - [Domain\]User Name
  - Password
  - OTP

**NOTE** By default, the **Hardware / Software** token option is selected. If you toggle to the **GrIDsure / SMS Challenge** token option, the **OTP** field (from the above list) becomes unavailable.

6. 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.

**NOTE** For **GrIDsure/ SMS Challenge** option, 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 a web browser.
2. The SafeNet Agent for Microsoft IIS examines the incoming request against its "**IP Range Exclusions / Inclusions**" on page 24 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 SafeNet Agent for Microsoft IIS examines the Microsoft username against its "**Exceptions**" on page 24 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 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.
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.

## Prerequisites

---

- > If the website is configured to use **Basic Authentication**, ensure that NTLM (a suite of challenge-response authentication and session security protocols) is disabled.
- > If the website is configured to use **Windows Authentication**, ensure that NTLM is enabled.
- > Ensure that **Dot Net Framework 4.5.2** and above must be installed on the SafeNet Agent for Microsoft IIS machine.
- > Add an Auth Node in the SAS: In the **SAS Management Console**, select **VIRTUAL SERVERS > COMMS > Auth Nodes**. Enter the name or IP address of the computer where the SafeNet Agent for Microsoft IIS is installed. For details, refer *SAS Service Provider Administrator Guide*.

# CHAPTER 2: Installing the SafeNet Agent for Internet Information Services

## Installing the Agent

**NOTE** Administrative rights to the Windows system are required during installation, migration, upgrade, configuration and uninstallation of the SafeNet Agent for Microsoft IIS.

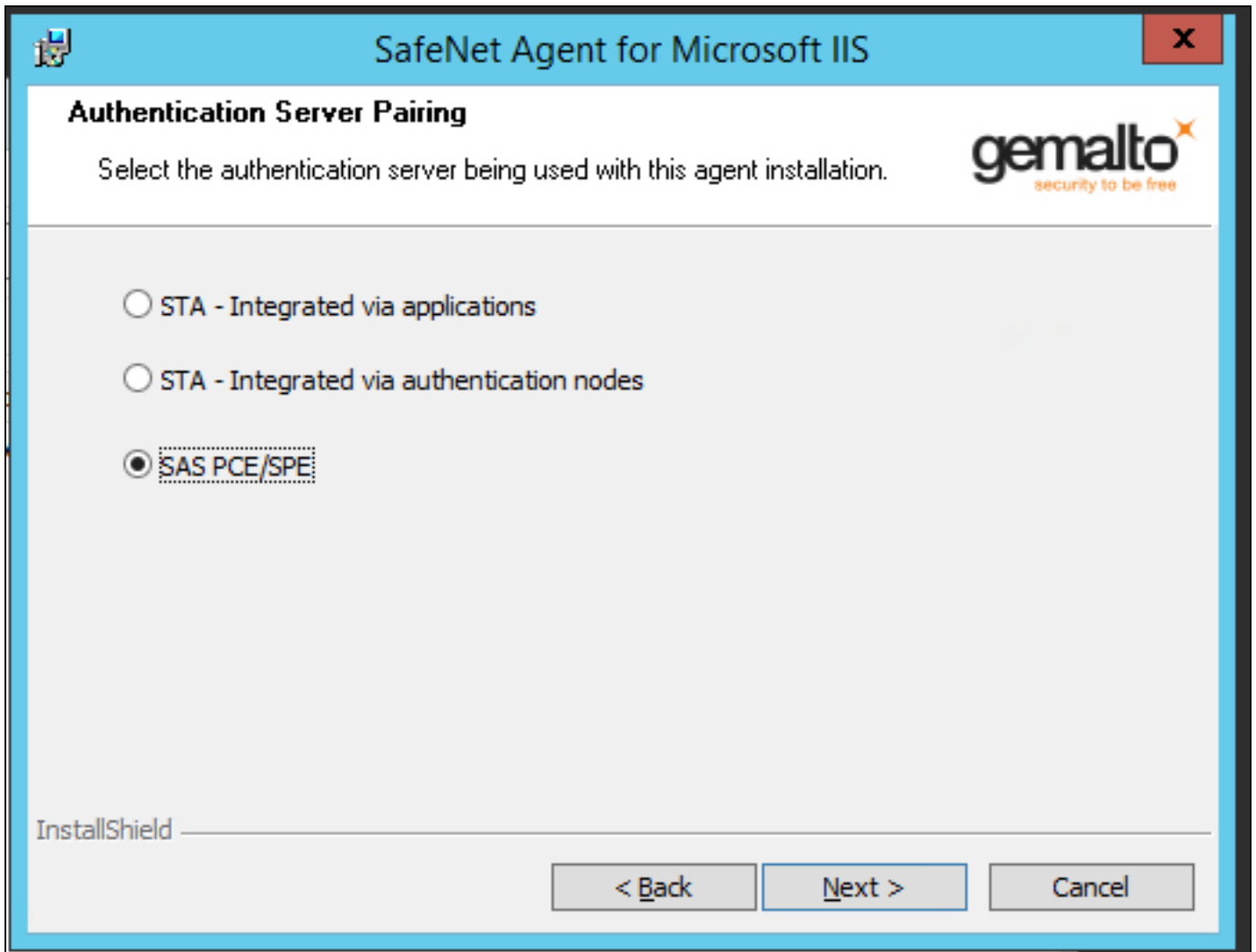
1. Log on to the Microsoft IIS web server as a user with administrative privileges.
2. Locate and execute the following installation package:  
`Safenet Agent for Microsoft IIS.exe`
3. On the **Welcome to the InstallShield Wizard...** window, click **Next**.



- On the **License Agreement** window, select **I accept the terms in the license agreement**, and click **Next**.



- Authentication Server Pairing:** Select the **SAS PCE/SPE** option from the following Authentication Server types, and click **Next**.

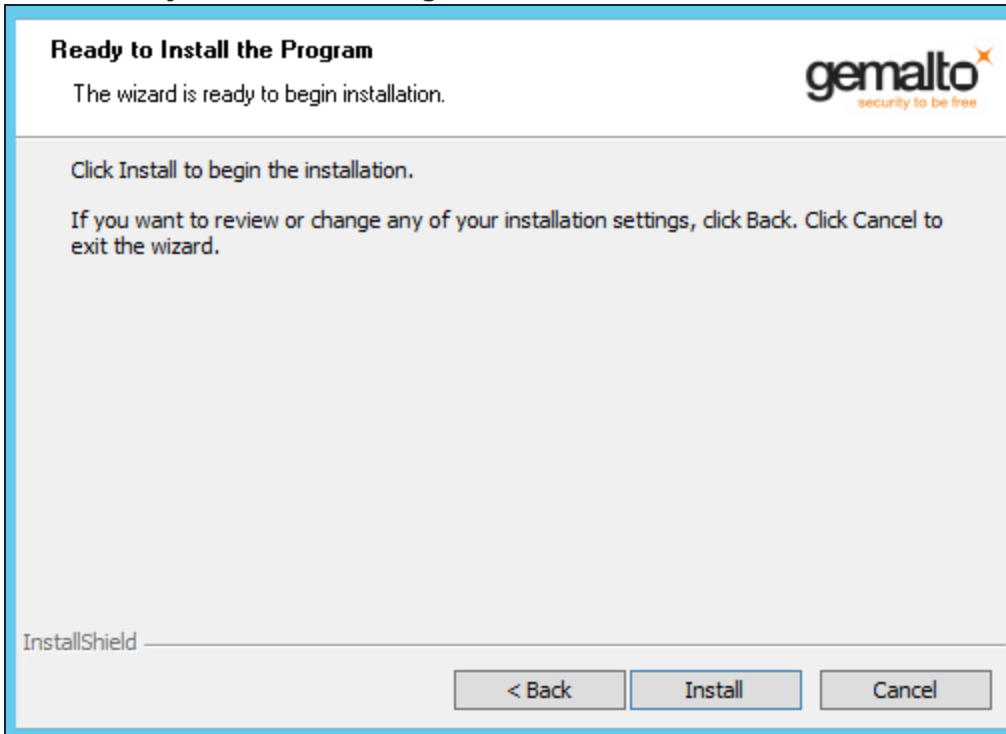


6. On the **Customer Information** window, enter **User Name** and **Organization** (any names can be used) and click **Next**.

**NOTE** To determine who will have access to the application, select one of the following:  
**Anyone who uses this computer (all users)** or **Only for me (Windows User)**

7. On the **Destination Folder** window, perform one of the following steps:
- > To change the installation folder, click **Change** and navigate to the required folder, and then click **Next**.
  - > To accept the default installation folder as displayed, click **Next**.

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



9. Once the installation is completed, the **InstallShield Wizard Completed** window is displayed. Click **Finish** to exit the wizard.





## Configuring Internet Information Services

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

### Activating Basic Authentication

To prevent superfluous prompts for credentials when logging in, set the web pages to 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.

### Configuring 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**.
  - a. Disable **Windows Authentication**
  - b. Enable **Basic Authentication**
5. At the **Edit Basic Authentication Settings** window, enter a default domain (or leave it blank) in the **Default domain** field. 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). Usually, 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 the Agent

The following basic instructions are required to enforce SafeNet authentication during logon to Terminal Services Web. For more information on each setting, refer "[Configuring the SafeNet Agent for Internet Information Services](#)" on page 19.

1. Click **Start > All Programs > SafeNet > Agents > IIS Agent Configuration Tool**.
2. On the "[Policy](#)" on page 19 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 select any additional settings, if required.
- 3.** Click the **"Communications"** on **page 26** tab. Verify that the **Authentication Server Settings** reflect the location of the SafeNet 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.

## Uninstalling the Agent

---

**NOTE** Administrative rights to the Windows system are required during installation, migration, configuration and uninstallation of the SafeNet Agent for Microsoft IIS.

To uninstall the SafeNet Agent for Microsoft IIS, perform the steps:

- 1.** Navigate to **Start > Control Panel > Programs and Features**.
- 2.** Select the *SafeNet Agent for Internet Information Services* program.
- 3.** Click **Uninstall**.

## Configuring Transport Layer Security

---

To configure TLS 1.1/ 1.2 support on the SAS Microsoft IIS Agent v2.0.1.53, set the registry settings as follows:

- > HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client DisabledByDefault => 0x0
- > HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client DisabledByDefault => 0x0

**NOTE** The agent will always connect with the highest enabled protocol.

# CHAPTER 3: Configuring the SafeNet Agent for Internet Information Services

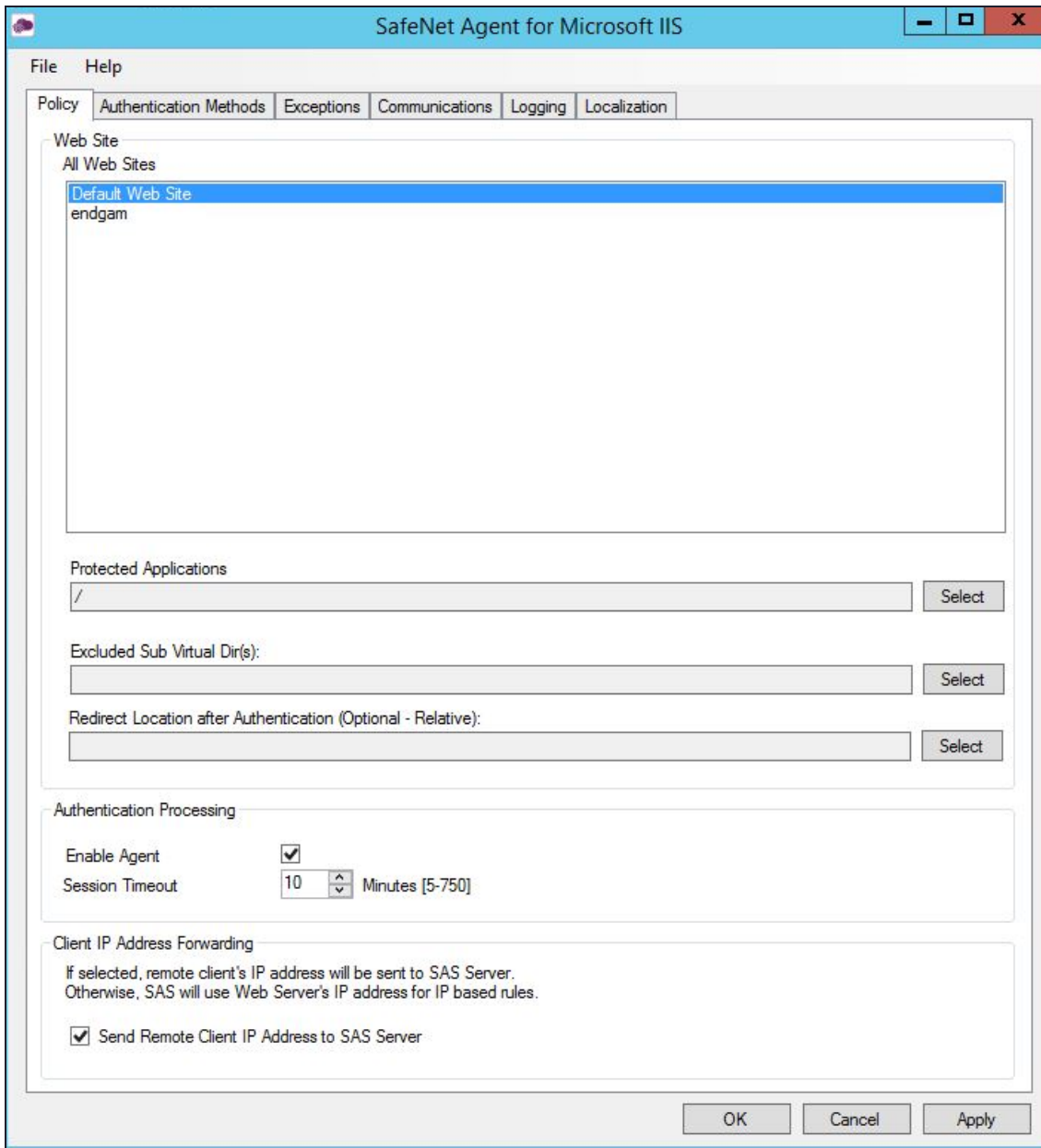
The SafeNet Agent for Microsoft IIS Configuration Tool allows for the modification of various features available within the agent.

**NOTE** Administrative rights to the Windows system are required during installation, migration, configuration and uninstallation of the SafeNet Agent for Microsoft IIS.

## Policy

---

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.



## Web Site

- > **All Web Sites:** 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 a virtual directory (single or multiple).
- > **Excluded Sub Virtual Dir(s):** Allows to select the sub virtual directories that you want to be excluded from the authentication.
- > **Redirect Location after Authentication (Optional – Relative):** Allows to select the URL to which you want to redirect, after the successful authentication.

## Authentication Processing

- > **Enable Agent:** Turns the SafeNet 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**.

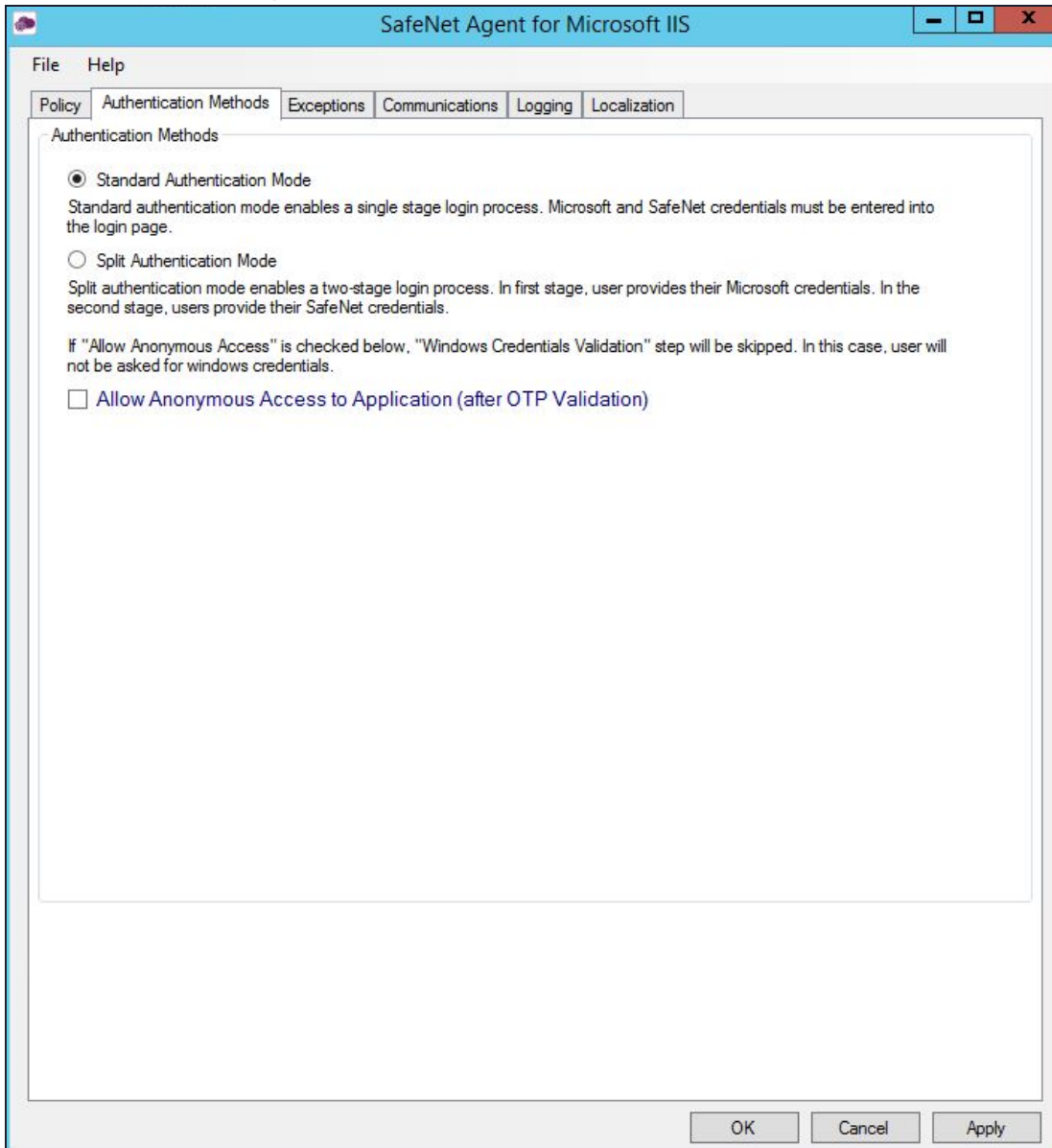
## Client IP Address Forwarding

If selected, the remote client IP address will be sent to the SafeNet 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 on low-resolution screens.

## Authentication Methods

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:

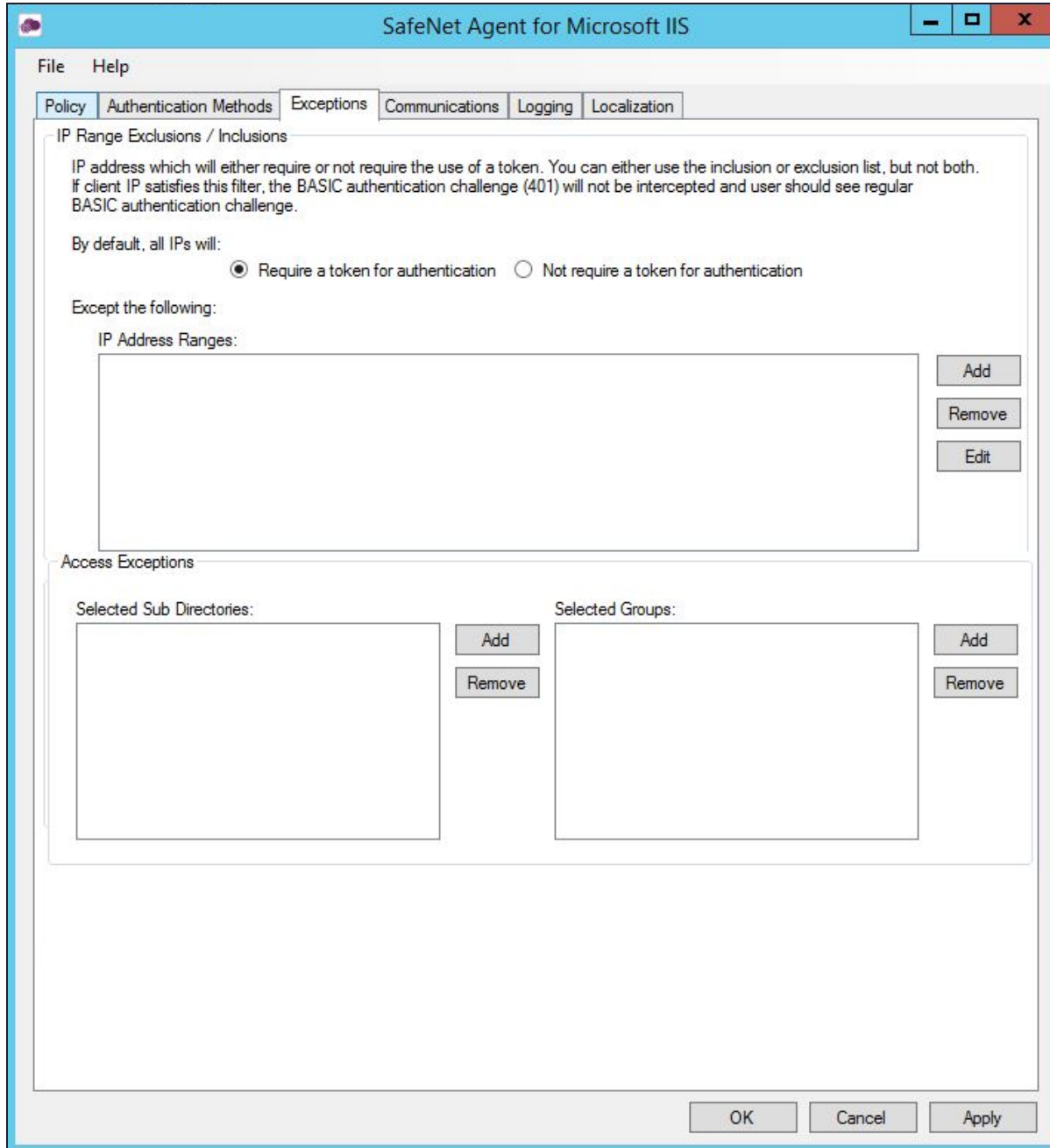
- > **Standard Authentication Mode:** This mode enables a single step login process. Microsoft and SafeNet credentials must be entered in a single login page. The default value is **Disabled**.
- > **Split Authentication Mode:** This mode enables a two-stage login process. In the first stage, users provide 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 (OTPs).
- 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 an OTP via SMS after they have provided valid Microsoft credentials.

## Exceptions

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 Exclusions / Inclusions

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



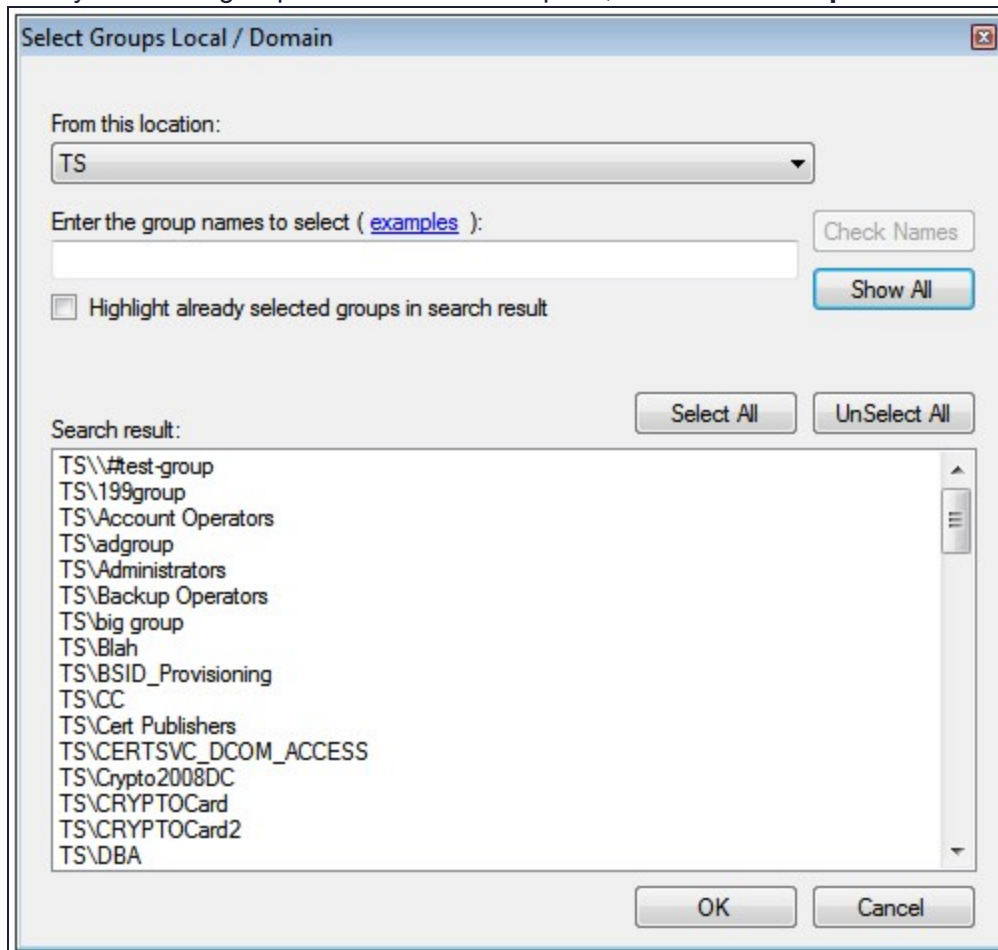
## Access Exceptions

Access Exceptions blocks access to specified subdirectories in the website selected in the "Policy" on page 19 tab.

- > **Selected Sub Directories:** Select the required subdirectory.
- > **Selected Groups:** Select the required groups. Users who are members of the selected groups will receive the following error message when attempting to access the blocked location: **"Access to this URL is blocked by the system administrator."**

Group Exceptions omits 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.

After you enter a group authentication exception, the **Select Groups Local / Domain** window is displayed:



- **From this location:** Select the location from which the results will be searched.
- **Enter the group names to select:** Used in conjunction with **Check Names** or **Show all**. Allows searches for Microsoft groups.
- **Highlight already selected groups in search result:** If a Microsoft group has already been configured in the exception, it will appear as a highlighted result.

## Communications

This tab primarily deals with connection options for the SafeNet.

The screenshot shows the 'Communications' tab of the SafeNet Agent configuration window. The 'Authentication Server Settings' section is expanded, showing the following options:

- Primary Server (IP:Port):** 10.164.46.158
- Failover Server (optional):** (empty field)
- Attempt to return to primary Authentication Server every:** 10 minute(s)
- Communication Timeout:** 10 seconds
- Use SSL (requires a valid certificate)** (checked for both Primary and Failover)
- Agent Encryption Key File:** c:\program files\gemalto\is\bsidKey\Agent.bsidKey
- Strip realm from UPN (username@domain.com will be sent as username)**
- Strip NetBIOS prefix (domain\username will be sent as username)**

The 'Authentication Test' section includes fields for 'User Name' and 'Passcode', and a 'Test' button. The 'Server Status Check' section includes a 'Test' button. At the bottom right, there is a watermark 'Activate Go to Syst' and buttons for 'OK', 'Cancel', and 'Apply'.

### Authentication Server Settings

- > **Primary Server (IP:Port):** Used to configure the IP address/ hostname of the primary SafeNet server. The default is port **80**. Alternatively, **Use SSL** checkbox 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 SafeNet server. The default is port **80**. Alternatively, **Use SSL** checkbox 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**.
- > **Communication Timeout:** Sets the maximum timeout value (in seconds) for authentication requests sent to the SafeNet server.

- > **Agent Encryption Key File:** Used to specify the key file location for the SafeNet Agent for Microsoft IIS. The encrypted key file is used to communicate between the agent and the authentication server. This file is used to encrypt / decrypt the data, ensuring that all authentication attempts made against the server are from valid, recognized agents. The key file can be downloaded from the SafeNet server, by following the steps:
  - a. Login to your SAS account, and navigate to **COMMS > Authentication Processing** section.
  - b. Under the **Task** list, click **Authentication Agent Settings** link and download the key.
  - c. The key file must be kept at a location accessible by all the authorized users:
    - i. Using Windows Explorer, change your current working directory to the **bsidKey** directory by typing "**[INSTALLDIR]\bsidKey**" in the address bar, where **[INSTALLDIR]** represents the install directory of this agent.
    - ii. Copy and paste the agent key file at the location.
- > **Strip realm from UPN (username@domain.com will be sent as username):** Select if the SafeNet username is required without the suffix **@domain**.
- > **Strip NetBIOS prefix (domain\username will be sent as username):** Select if the SafeNet username is required without the prefix **domain\**.

**NOTE** The realm-stripping feature applies to SafeNet usernames only. Active Directory usernames are not affected.

**NOTE** Once stripping has been activated or deactivated for an Microsoft IIS site, the agent stores these values and uses them as default for each new Microsoft IIS site protected by the agent.

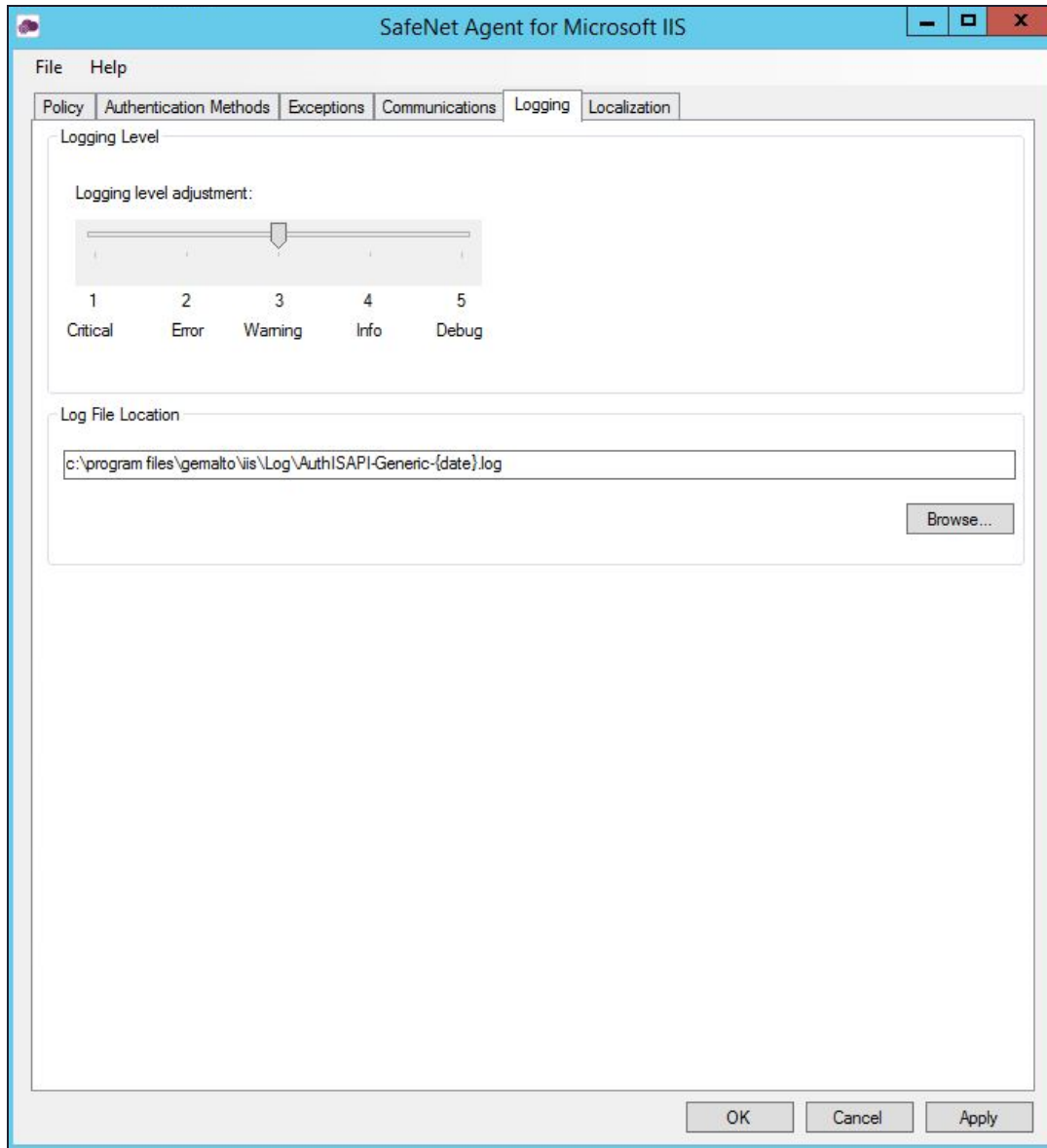
## Authentication Test

This function allow administrators to test authentication between the SafeNet Agent for Microsoft IIS and the SafeNet server.

## Server Status Check

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

## Logging



### Logging Level

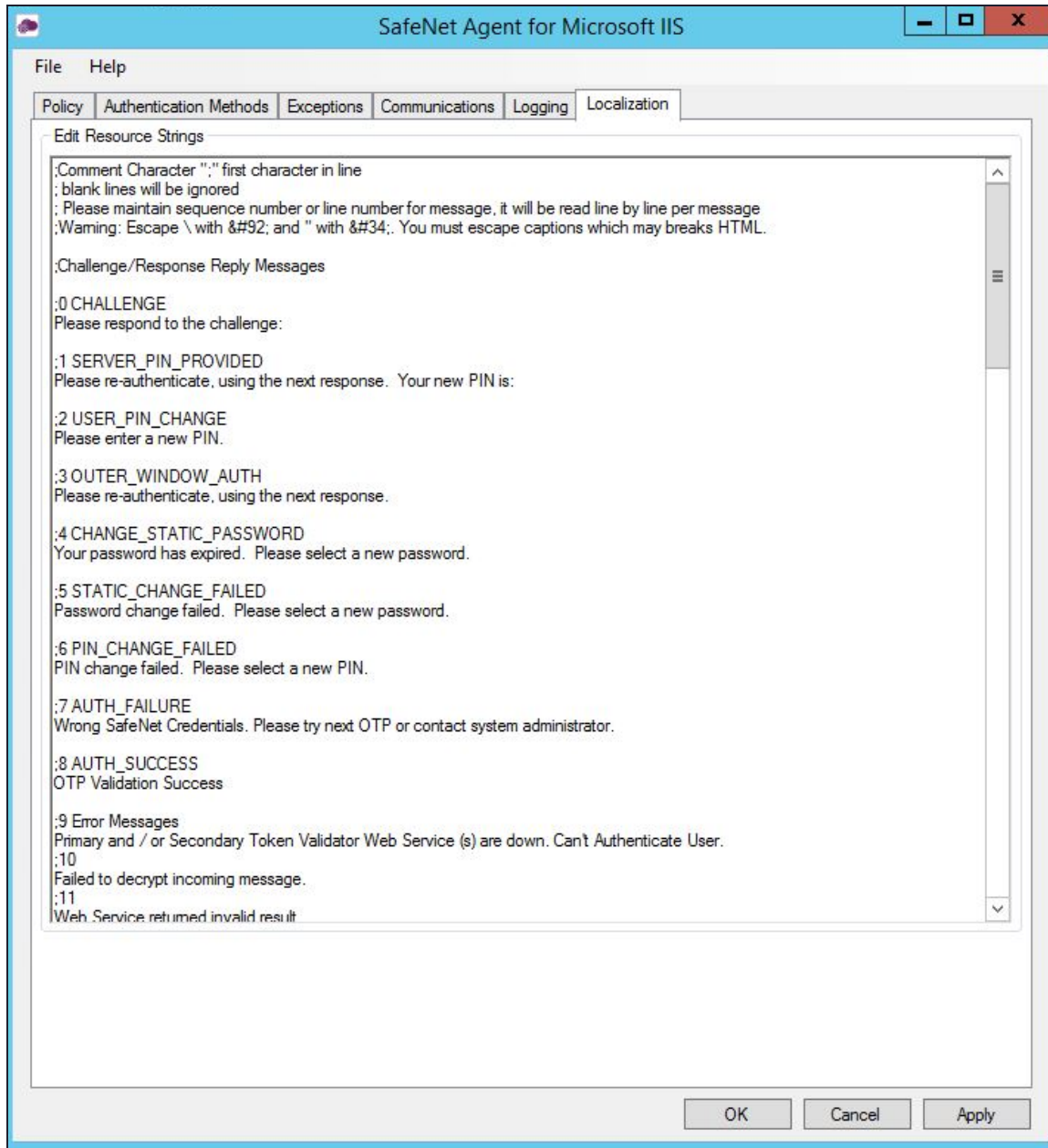
It helps adjust the logging level. For log levels 1, 2, and 3, only the initial connection between the agent and server attempts are logged. Log level 5 sets the agent in the debug mode. The default value is **3**.

### Log File Location

It helps specify the location of the log file. The log file is rotated on a daily basis. The default log file location is:  
 Program Files\GEMALTO\IIS\Log<Web\_Site\_Name>\AuthISAPI-Generic-{date}.log

## Localization

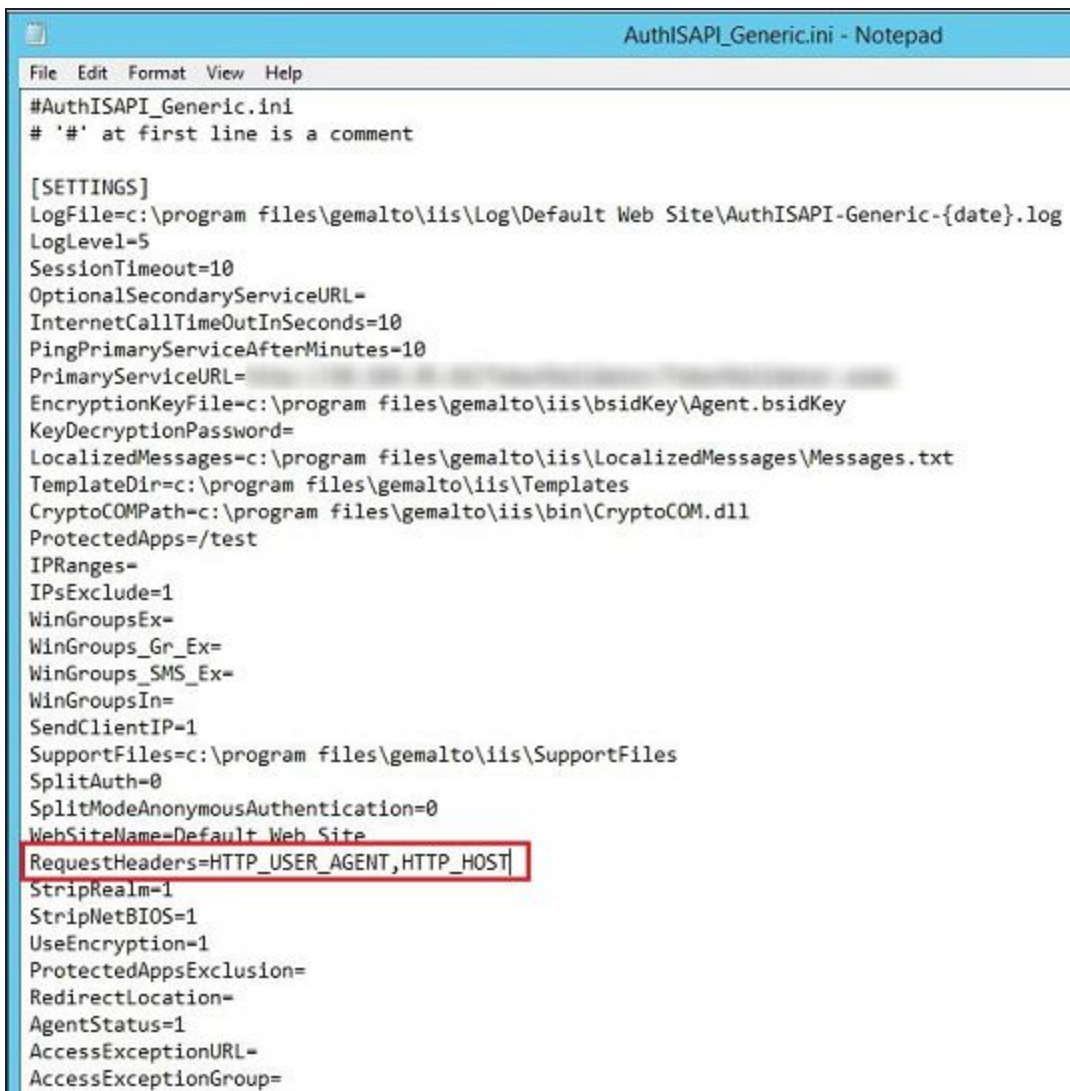
The settings on this tab represent the prompts and information messages supplied by the agent. These can be modified as necessary to improve usability. The **Messages.txt** file can be modified manually outside of the configuration tool. The default location of this file is: `Program Files\GEMALTO\IIS\LocalizedMessages`



# CHAPTER 4: Configuring Initialization File for Specific Request Headers (Optional)

The Initialization (*.INI*) file is used to set parameters for operating systems and programs.

Using the *.INI* file, users can also skip validation checks for specific Request Headers. To skip, add the required validation checks in the **AuthISAPI\_Generic.ini** file (default located at `Installation\Bin\<Application_Pool>\`) under **RequestHeaders** column by specifying comma-separated header values.



```
AuthISAPI_Generic.ini - Notepad
File Edit Format View Help
#AuthISAPI_Generic.ini
# '#' at first line is a comment

[SETTINGS]
LogFile=c:\program files\gemalto\iis\Log\Default Web Site\AuthISAPI-Generic-{date}.log
LogLevel=5
SessionTimeout=10
OptionalSecondaryServiceURL=
InternetCallTimeOutInSeconds=10
PingPrimaryServiceAfterMinutes=10
PrimaryServiceURL=
EncryptionKeyFile=c:\program files\gemalto\iis\bsidKey\Agent.bsidKey
KeyDecryptionPassword=
LocalizedMessages=c:\program files\gemalto\iis\LocalizedMessages\Messages.txt
TemplateDir=c:\program files\gemalto\iis\Templates
CryptoCOMPPath=c:\program files\gemalto\iis\bin\CryptoCOM.dll
ProtectedApps=/test
IPRanges=
IPsExclude=1
WinGroupsEx=
WinGroups_Gr_Ex=
WinGroups_SMS_Ex=
WinGroupsIn=
SendClientIP=1
SupportFiles=c:\program files\gemalto\iis\SupportFiles
SplitAuth=0
SplitModeAnonymousAuthentication=0
WebSiteName=Default Web Site
RequestHeaders=HTTP_USER_AGENT,HTTP_HOST
StripRealm=1
StripNetBIOS=1
UseEncryption=1
ProtectedAppsExclusion=
RedirectLocation=
AgentStatus=1
AccessExceptionURL=
AccessExceptionGroup=
```

# CHAPTER 5: Upgrading the SafeNet Agent for Internet Information Services

**NOTE** Administrative rights to the Windows system are required during installation, migration, upgrade, configuration and uninstallation of the SafeNet Agent for Microsoft IIS.

Upgrade from earlier versions of the SafeNet Agent for Microsoft IIS to version 2.0.0 is not supported. For migrating agent settings within same version and on different environments, see "[Migrating the Agent](#)" below.

The SafeNet Agent for Microsoft IIS 2.0.1 supports upgrade from 2.0.0. To upgrade, run the installation wizard and select appropriate options when prompted.

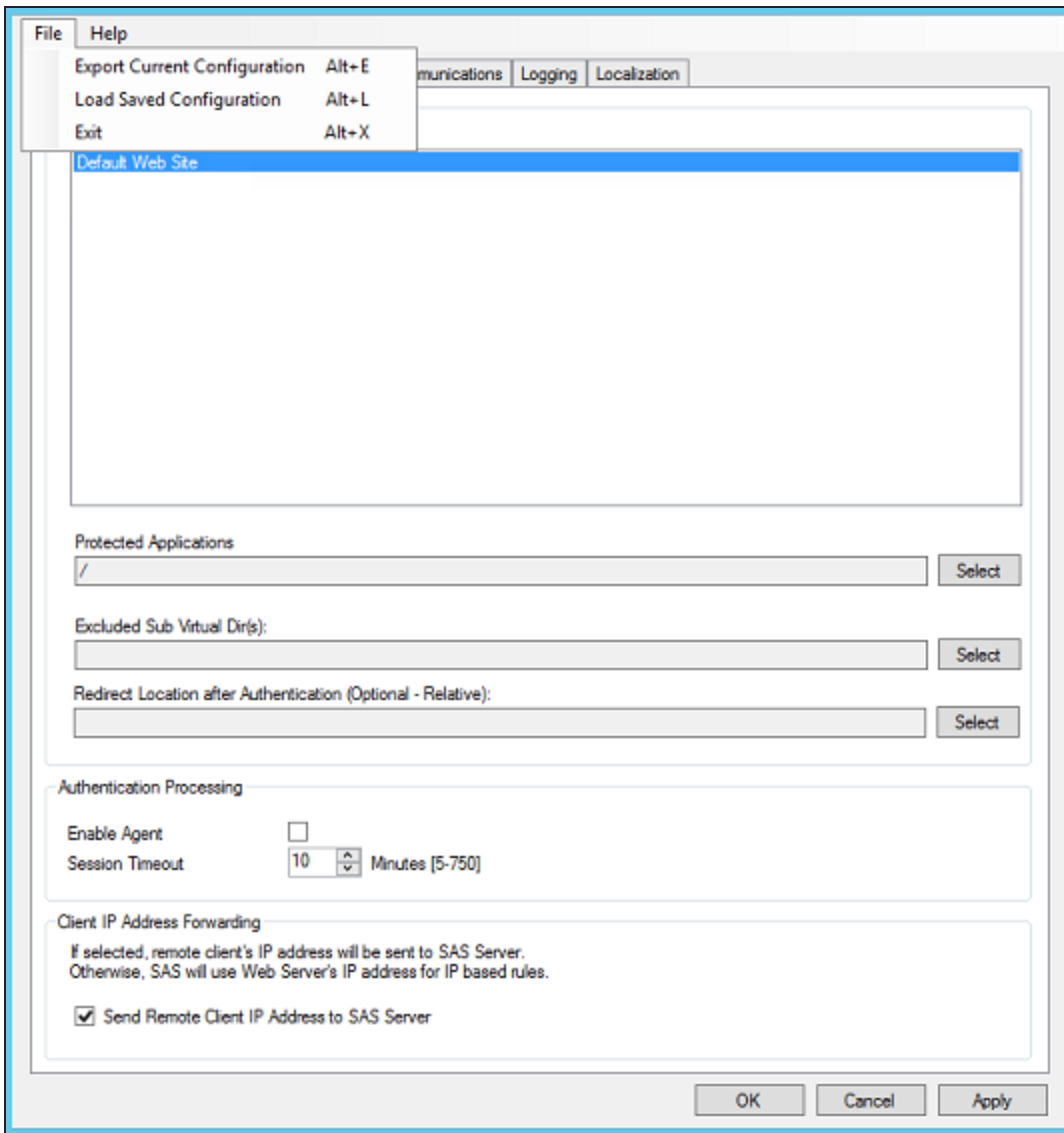
**NOTE** You must update the new agent configuration file using the management console, once it gets downloaded. Once the upgrade is complete, the IIS server restarts. The upgrade should be performed during non-peak hours to avoid disruption of services.

**TIP** Ensure that the SafeNet Agent for Microsoft IIS Configuration Tool is closed while upgrading the agent.

## Migrating the Agent

In the existing setup of the agent, perform the following steps:

1. Open the agent's Management Console, and navigate to **File > Export Current Configuration**. A file of the settings (***Backup.bsidConfig***) is created.
2. Make a copy of the ***Backup.bsidConfig*** file, and save it to the new environment.
3. Install the agent version you wish to migrate on the new environment.
4. Open the newly installed agent's Management Console, and navigate to **File > Load Saved Configuration**.
5. Import the configuration file (as saved in step 2). Navigate to the saved file, ***Backup.bsidConfig***, click **Open** and import the configuration into the agent.
6. Click **Apply** to apply the settings.





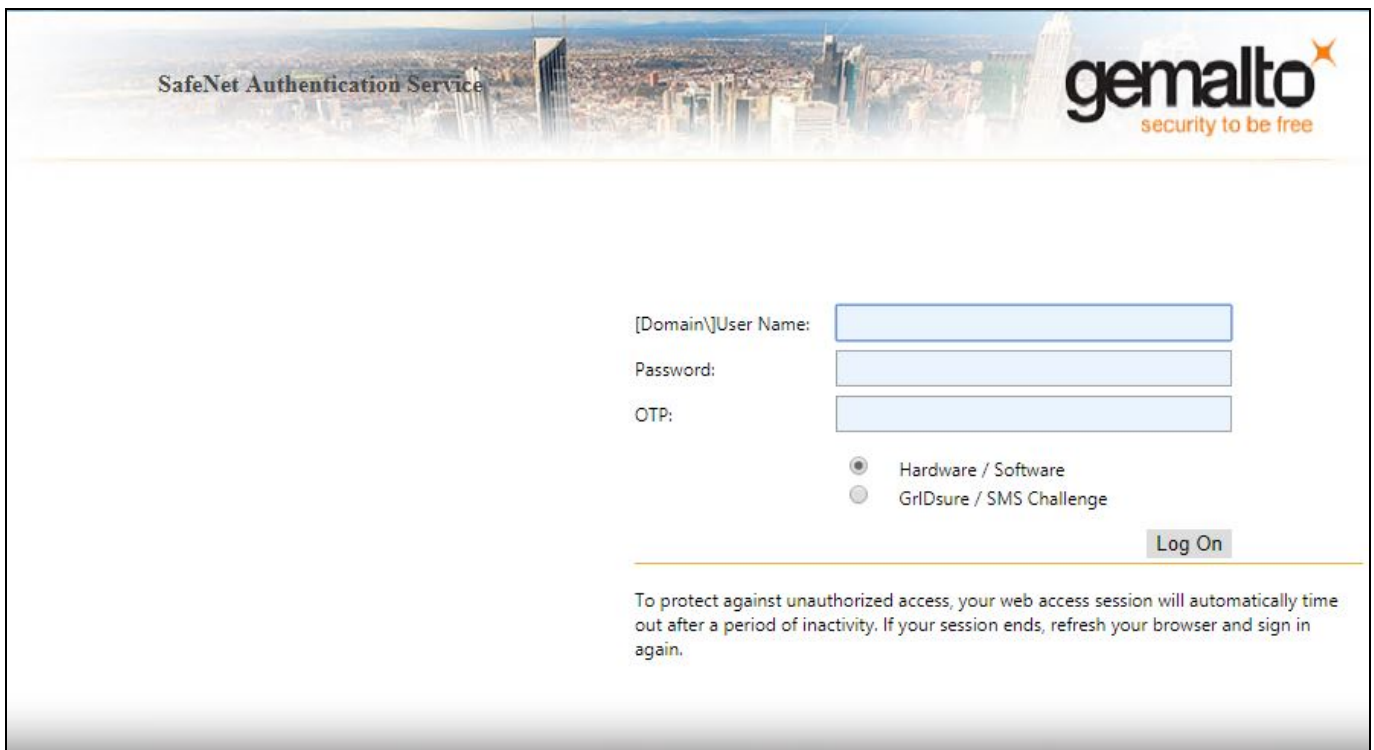
# CHAPTER 6: Testing the SafeNet Agent for Internet Information Services

The flow of running the agent solution and verifying the authentication, is based on the selected token type. The following authentication token options are available:

- > [Hardware / Software](#)
- > [GrIDsure / SMS Challenge](#)

## Hardware / Software

1. In the agent's authentication page, enter **[Domain]\User Name**, **Password** and **OTP**.



SafeNet Authentication Service

gemalto  
security to be free

[Domain]\User Name:

Password:

OTP:

Hardware / Software  
 GrIDsure / SMS Challenge

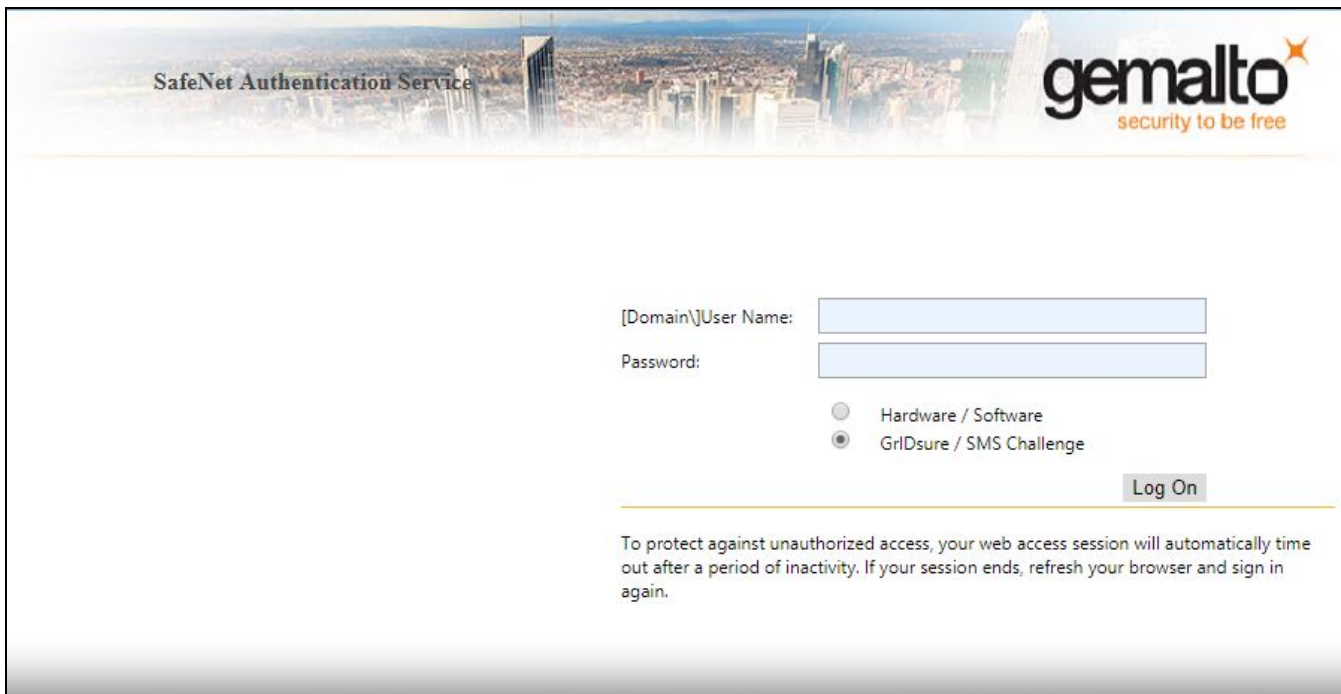
Log On

To protect against unauthorized access, your web access session will automatically time out after a period of inactivity. If your session ends, refresh your browser and sign in again.

2. Click **Log On**.
3. If both sets of credentials (Microsoft and SafeNet credentials) are valid, the user is presented with their website, otherwise, the attempt is rejected.

## GrIDSure / SMS Challenge

1. In the agent's authentication page, enter **[Domain]User Name**, and **Password**.



SafeNet Authentication Service

gemalto  
security to be free

[Domain]User Name:

Password:

Hardware / Software

GrIDSure / SMS Challenge

Log On

To protect against unauthorized access, your web access session will automatically time out after a period of inactivity. If your session ends, refresh your browser and sign in again.

2. Click **Log On**.
3. If the Microsoft credentials are valid, you will be 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.