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 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 the 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.

© 2017 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.

**Document Part Number:** 007-013748-001

**Version:** 1.1

**Release Date:** March 2017
# Table of Contents

Preface ........................................................................................................................................... 5  
Customer Release Notes .................................................................................................................. 5  
Audience ........................................................................................................................................ 5  
Third-Party Software Acknowledgement ......................................................................................... 5  
Support Contacts ............................................................................................................................ 6  

1 Introduction ................................................................................................................................... 7  
Overview ....................................................................................................................................... 7  
Applicability ................................................................................................................................... 7  
Environment ................................................................................................................................... 8  

2 SafeNet Authentication Service Agent for Outlook Web App 2010 ............................................. 9  
Authentication Modes ...................................................................................................................... 9  
Setting Authentication Mode ........................................................................................................... 9  
Standard Authentication Mode - Hardware/Software ...................................................................... 10  
Standard Authentication Mode - GrIDsure/SMS Challenge ............................................................. 11  
Split Authentication Mode ............................................................................................................... 12  
Prerequisites .................................................................................................................................. 14  
Installing SAS Agent for OWA 2010 ................................................................................................. 14  
Upgrading SAS Agent for OWA 2010 ............................................................................................... 16  
Installing SAS Agent for OWA 2010 Using Previous Configurations ........................................... 16  
SafeNet Microsoft Exchange OWA Manager .................................................................................. 19  
Policy Tab ...................................................................................................................................... 19  
Authentication Methods Tab ........................................................................................................... 20  
Exceptions Tab ................................................................................................................................. 21  
Communications Tab ...................................................................................................................... 24  
Logging Tab .................................................................................................................................... 25  
Localization Tab ............................................................................................................................... 26  

3 SafeNet Authentication Service Agent for Outlook Web App 2013 .............................................. 27  
Authentication Modes ...................................................................................................................... 27  
Setting Authentication Mode ........................................................................................................... 27  
Standard Authentication Mode - Hardware/Software ...................................................................... 28  
Split Authentication Mode ............................................................................................................... 28  
Prerequisites .................................................................................................................................. 30  
Installing SAS Agent for OWA 2013 ................................................................................................. 31  
Upgrading SAS Agent for OWA 2013 ............................................................................................... 32  
Installing SAS Agent for OWA 2013 Using Previous Configurations ........................................... 33  
SafeNet Microsoft Exchange OWA Manager .................................................................................. 35  
Policy Tab ...................................................................................................................................... 35  
Authentication Methods Tab ........................................................................................................... 36  
Exceptions Tab ................................................................................................................................. 37  
Communications Tab ...................................................................................................................... 39  
Logging Tab .................................................................................................................................... 40  
Localization Tab ............................................................................................................................... 41  

SafeNet Authentication Service Agent for Microsoft Outlook Web App: Installation and Configuration Guide  
Document PN: 007-013748-001, Rev. A, © Gemalto 2017. All rights reserved.  
Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and are registered in certain countries.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 SafeNet Authentication Service Agent for Outlook Web App 2016</td>
<td>42</td>
</tr>
<tr>
<td>Authentication Modes</td>
<td>42</td>
</tr>
<tr>
<td>Setting Authentication Mode</td>
<td>42</td>
</tr>
<tr>
<td>Standard Authentication Mode - Hardware/Software</td>
<td>43</td>
</tr>
<tr>
<td>Split Authentication Mode</td>
<td>43</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>45</td>
</tr>
<tr>
<td>Installing SAS Agent for OWA 2016</td>
<td>46</td>
</tr>
<tr>
<td>Installing SAS Agent for OWA 2016 Using Previous Configurations</td>
<td>47</td>
</tr>
<tr>
<td>SafeNet Microsoft Exchange OWA Manager</td>
<td>50</td>
</tr>
<tr>
<td>Policy Tab</td>
<td>50</td>
</tr>
<tr>
<td>Authentication Methods Tab</td>
<td>51</td>
</tr>
<tr>
<td>Exceptions Tab</td>
<td>52</td>
</tr>
<tr>
<td>Communications Tab</td>
<td>54</td>
</tr>
<tr>
<td>Logging Tab</td>
<td>56</td>
</tr>
<tr>
<td>Localization Tab</td>
<td>57</td>
</tr>
</tbody>
</table>
This document describes how to install and configure the Gemalto SafeNet Authentication Service (SAS) Agent for Microsoft Outlook Web App (OWA).

Customer Release Notes

The Customer Release Notes (CRN) document provides important information about this release that is not included in other 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 targeted at system administrators who are familiar with OWA, and are interested in adding Multi-Factor Authentication (MFA) capabilities using the SAS solution.

All products manufactured and distributed by Gemalto 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.

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Microsoft OWA. Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged.
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 the 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>
</table>
| Address                 | Gemalto
                           4690 Millennium Drive
                           Belcamp, Maryland 21017 USA                         |
| Phone                   | United States | 1-800-545-6608
                           International | 1-410-931-7520                                    |
| Technical Support       | https://serviceportal.safenet-inc.com                    |
| Customer Portal         | Existing customers with a Technical Support Customer Portal account can login to manage incidents, get latest software upgrades, and access the Gemalto Knowledge Base. |
| Documentation           | All SAS Agents documentation can be found at the SafeNet Authentication Service Downloads page. |
|                         | All SAS documentation (Cloud, PCE, SPE, Token and Integration) can be found at the SafeNet Knowledge Base page. |
Overview

Authentication is the process of proving that a user is who he or she claims to be. An Access System enables the user to configure authentication rules in the policy domains that protect the resources. Authentication rules contain authentication schemes, which provide the methods for performing verification of a user's identity.

The Outlook Web App (OWA) is Microsoft Exchange Server's web-based email client, allowing users to access email messages, contacts, and calendar using web browsers, without setting up a full email client.

The Gemalto SafeNet Authentication Service (SAS) delivers fully automated, highly secure authentication-as-a-service, with flexible token options tailored to the unique needs of different organizations, substantially reducing the total cost of operation. Strong authentication is easily achievable through the flexibility and scalability of SAS’s automated workflows, vendor-agnostic token integrations, and broad APIs. In addition, management capabilities and processes are fully automated and customizable—providing a seamless and enhanced user experience. The SAS solution also enables a quick migration to a multi-tier, multi-tenant cloud environment, protecting everything, from cloud-based and on-premises applications to networks, users, and devices.

The SAS Agent for OWA is designed to help Microsoft enterprise customers ensure that web-based resources are accessible only by authorized users, whether working remotely or inside the firewall. It delivers a simplified and consistent user login experience and helps organizations comply with regulatory requirements. The use of Two-Factor Authentication (2FA) instead of just traditional static passwords to access OWA is a critical step for information security.

This document describes how to:

- Deploy 2FA in OWA, managed by the SAS solution.
- Deploy and configure OWA using the SAS agent.

Applicability

The information in this document applies to:

- **SafeNet Authentication Service - Cloud (SAS Cloud)** — The SafeNet’s cloud-based authentication service.
- **SafeNet Authentication Service - Service Provider Edition (SAS SPE)** — The on-premises, server version targeted at service providers interested in hosting SAS in their data center(s).
- **SafeNet Authentication Service - Private Cloud Edition (SAS PCE)** — The on-premises, server version targeted at organizations interested in hosting SAS in their private cloud environment.
## Environment

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network</strong></td>
<td>TCP 443</td>
</tr>
<tr>
<td><strong>Supported Architecture</strong></td>
<td>64-bit</td>
</tr>
<tr>
<td><strong>Supported Web Servers</strong></td>
<td>IIS 7.0</td>
</tr>
<tr>
<td></td>
<td>IIS 7.5</td>
</tr>
<tr>
<td></td>
<td>IIS 8.0</td>
</tr>
<tr>
<td><strong>Supported Exchange Server Versions</strong></td>
<td>Microsoft Exchange Server 2010</td>
</tr>
<tr>
<td></td>
<td>Microsoft Exchange Server 2013</td>
</tr>
<tr>
<td></td>
<td>Microsoft Exchange Server 2016</td>
</tr>
<tr>
<td><strong>Additional Software</strong></td>
<td>.NET 3.5</td>
</tr>
<tr>
<td><strong>Supported Web Browsers</strong></td>
<td>Internet Explorer (IE) 10 and 11</td>
</tr>
<tr>
<td>Note: For SAS OWA 2016 Agent, the supported web browser is Internet Explorer (IE) 11 (and onwards).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Firefox</td>
</tr>
<tr>
<td></td>
<td>Chrome</td>
</tr>
<tr>
<td><strong>Additional Web Browsers Requirements</strong></td>
<td>Cookies must be enabled</td>
</tr>
<tr>
<td></td>
<td>JavaScript must be enabled</td>
</tr>
<tr>
<td></td>
<td>ActiveX must be enabled</td>
</tr>
<tr>
<td><strong>Supported Authentication Methods</strong></td>
<td>All tokens and authentication methods supported by SAS.</td>
</tr>
<tr>
<td><strong>SAS releases</strong></td>
<td>SafeNet Authentication Service PCE/SPE 3.5.4 (and earlier)</td>
</tr>
<tr>
<td></td>
<td>SafeNet Authentication Service Cloud Edition</td>
</tr>
</tbody>
</table>
Authentication Modes

There are two modes of operation for the SAS OWA Agent. By default, **Split Authentication** mode is enabled. The authentication mode can be modified after installation by using the **SafeNet Microsoft Exchange OWA Manager**.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard Authentication Mode</strong></td>
<td>Standard Authentication Mode enables a single-stage login process. Domain and SAS credentials must be entered in the OWA login page to access web-based resources.</td>
</tr>
<tr>
<td><strong>Split Authentication Mode</strong></td>
<td>Split Authentication Mode enables a two-stage login process. In the first stage, users provide their domain credentials. In the second stage, users provide their SAS credentials. This mode allow administrators to control authentication dialogs, based on Microsoft groups, token type (such as GrIDsure), or IP-exclusion groups.</td>
</tr>
</tbody>
</table>

Setting Authentication Mode

Authentication mode is set in the SafeNet Microsoft Exchange OWA Manager, Authentication tab.

See **Authentication Methods Tab** on page 20.
Standard Authentication Mode - Hardware/Software

1. Open OWA in your browser.
2. For hardware or software token login, select **Hardware** radio button and click **Log On**.

3. Enter **Domain/User Name**, **Password** and **OTP** (One Time Password), and click **Log On**.
Standard Authentication Mode - GrIDsure/SMS Challenge

1. Open OWA in your browser.
2. Select **GrIDsure / SMS Challenge** radio button and click **Log On**.
3. Enter **Domain/User Name**, **Password**, and click **Log On**.
4. Do one of the following, and click **Log On**.

- Enter the GrIDsure OTP, derived from your grid pattern.
- Enter the OTP received in the SMS.

---

**Split Authentication Mode**

1. Open OWA in your browser.
2. Enter **Domain/User Name** and **Password**, and click **Log On**.
3. Enter OTP and click **Log On**.

4. If your system is configured to work with GrIDsure, enter GrIDsure OTP, derived from your grid pattern, and click **Log On**.

5. If your system is configured to send OTP via SMS, enter the Token Code received on your phone, and click **Log On**.
Challenge-Response

If your system is configured to work with Challenge Response, following login (in either Standard Authentication Mode or Split Authentication Mode), you will be prompted to respond to a challenge.

6. Send the challenge code, as displayed on the screen, to the designated recipient in your organization (typically System Administrator or Help Desk).

In return, you will receive a response code.

7. Enter the response code into the OTP field, and click Log On.

Prerequisites

- Ensure that TCP port 80 or 443 is open between the SAS OWA Agent and the SAS solution.
- Administrative rights to the Windows system are required during installation of the SAS OWA Agent.
- Download the Exchange Agent installation package. A link to the agents and other software can be found on the Snapshot tab in the References module for users of SAS.

Installing SAS Agent for OWA 2010

NOTE: Always work in Run as administrator mode when installing, uninstalling, upgrading, enabling, or disabling the SAS OWA Agent.
1. Log on to the Microsoft Exchange server.
2. Locate and run the SAS Agent for Exchange x64.exe installation package, following the prompts. The **Authentication Service Setup** window is displayed.

   ![Authentication Service Setup Window]
   
   - In the **Location** field, enter the hostname or IP address of the primary SAS server.
   - Select **Connect using SSL** if SAS is configured to accept incoming SSL connections.
   - If a failover server is available, select the associated checkbox and add the hostname or IP address of a failover SAS server.

3. Click **Next**. The **Exchange Server Selection** window is displayed.
4. Select the version of Microsoft Exchange Server, and click **Next**.

   ![Exchange Server Selection Window]
Upgrading SAS Agent for OWA 2010

**NOTES:**

- Automatic upgrade from 1.09 to 1.1 version is not supported. See [Installing SAS Agent for OWA 2010 Using Previous Configurations](#) on page 17.
- The upgrade can be performed only to and from the folder where the previous version of SAS OWA Agent was installed.
- Always work in **Run as administrator** mode when installing, uninstalling, upgrading, enabling, or disabling the SAS OWA Agent.
- Before upgrading, close the SafeNet Microsoft Exchange OWA Manager.

To upgrade SAS OWA Agent from 1.09 to 1.1 version, perform the following steps:

1. Back up the installation folder contents, including any changed templates, the INI file, and the Caption (localization) file.
2. Disable the SAS OWA Agent using the **SafeNet Microsoft Exchange OWA Manager**.
3. Close the **SafeNet Microsoft Exchange OWA Manager**.
4. Run the installation file, **SafeNet Agent for Exchange x64.exe** as an administrator. When prompted to upgrade, select **Yes**.
5. Open the **SafeNet Microsoft Exchange OWA Manager** and enable SAS OWA Agent.

**Installing SAS Agent for OWA 2010 Using Previous Configurations**

Automatic upgrade from 1.09 to 1.1 version is not supported.

The procedure requires export of the configurations from the previously installed version(s) followed by import of the configurations in the newly installed SAS OWA Agent 1.1.

**NOTES:**

- Always work in **Run as administrator** mode when installing, uninstalling, upgrading, enabling, or disabling the SAS OWA Agent.
- The Export/Import procedure can be performed only to and from the folder where the previous version of SAS OWA Agent was installed.

The SAS Agent for OWA 1.1 version supports import of configurations from SAS Agent for OWA 1.06 and earlier versions.
To install the SAS Agent for OWA 1.1 version using configurations from a previous version, perform the following steps:

1. In the previously installed SAS OWA Agent, export the configurations as follows:
   
   I. In the **SafeNet Microsoft Exchange OWA Manager** window, select **File > Export Current Configuration**.

   ![SafeNet Microsoft Exchange OWA Manager window](image)

   II. In the **Save As** dialog, click **Save** to save the configuration files.

2. Uninstall the previously installed SAS OWA Agent.

3. Manually delete the **Exchange** folder (located at **Program Files > SafeNet**).

4. To install the new SAS Agent for OWA 1.1, run the installation file, **SafeNet Agent for Exchange x64.exe** as an administrator.
5. In the newly installed SAS Agent, load the saved settings as follows:
   
   I. In the **SafeNet Microsoft Exchange OWA Manager** window, select **File > Load Saved Configuration**.

   ![SafeNet Microsoft Exchange OWA Manager window](image)

   II. In the **Open** window, select the saved configuration file (.bsidconfig) and click **Open**.

6. Enable SAS OWA Agent in the **SafeNet Microsoft Exchange OWA Manager** window.
NOTES:

- After installing **SAS Agent for OWA 1.1** version, the SSL server certificate check is disabled by default.
  
  To change the settings, go to **SafeNet Microsoft Exchange OWA Manager > Communications Tab > Authentication Server Settings**, and unselect **Disable SSL server certificate check**.

- After installing **SAS Agent for OWA 1.1** version, the **Split Authentication Mode** is selected by default.
  
  To change the settings, go to **SafeNet Microsoft Exchange OWA Manager > Authentication Methods** and select **Standard Authentication Mode**.

---

**SafeNet Microsoft Exchange OWA Manager**

The SafeNet Microsoft Exchange OWA Manager allows modification of various features available within the SAS OWA Agent.

**Policy Tab**

![Policy Tab](image)

The **Policy** tab deals primarily with enabling the OWA Agent and defining the website settings.
Authentication Processing Group

- **Enable Agent**: Turns the SAS ID Agent for OWA, On or Off.
  Default value: Disabled

Web Site Group

- **Web Site Name**: Allows selection of the Exchange Server website.
  Default value: Default Web Site

- **Protected Applications**: Specifies the OWA directory on the Exchange Server.
  Default value: /owa

Client IP Address Forwarding Group

If selected, the remote client IP address will be sent to the SAS solution. Otherwise, the web server’s IP address will be used.
Default value: Enabled

Authentication Methods Tab

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

- **Standard Authentication Mode**: As explained earlier, this mode enables a single-step login process. Microsoft and SAS credentials must be entered in a single login page.
  Default value: Disabled

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

  - **Hardware, Software, GrIDsure, and SMS Challenge Token Detection**: This is the default option. If selected, the following fields are displayed on the login page: **Username**, **Password**, **OTP**, **Hardware**, **GrIDsure/SMS Challenge**.

  - **Hardware and Software Token Detection**: If a software token is detected, the login page will display **Domain\Username**, **Password**, and **OTP** fields.

- **Split Authentication Mode**: As explained earlier, this mode enables a two-stage login process. In the first stage, users provide their domain credentials. In the second stage, users provide their SAS credentials.
  Default value: Enabled

  The Split Authentication Mode provides the following advantages over Standard Authentication Mode:

  - Microsoft group exclusions may be used to migrate users gradually from static passwords to a combination of static and one-time passwords.

  - Allow administrators to specify (via Microsoft Groups) users who have been provided with GrIDsure or SMS Challenge-response tokens. This allows for a seamless login experience as the agent displays exactly what is required from the user.

  - **GrIDsure Tab (Optional)**: Allows an administrator to specify a Microsoft group, which contains SAS 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 that contains SAS 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 Tab

The **Exceptions** tab allows specific Microsoft groups or network traffic to bypass SAS authentication. By default, all users are required to perform SAS authentication unless otherwise defined by exclusion.
SafeNet Authentication Service Agent for Outlook Web App 2010

IP Range Exclusions / Inclusions Group

It allows an administrator to define which network traffic requires SAS authentication.

Group Authentication Exceptions Group

Group authentication exceptions omit single or multiple domain groups from performing SAS authentication. Only one group filter option is valid at any given time; it cannot overlap with another group authentication exception.

Default value: Everyone must use SafeNet

The following group authentication exceptions are available:

- **Everyone must use SafeNet**: All users must perform SAS authentication.
- **Only selected groups will bypass SafeNet**: All users are required to perform SAS authentication, except the defined Microsoft Group(s).
• **Only selected groups must use SafeNet:** All users are not required to perform SAS authentication, except the defined Microsoft Group(s).

Adding a group authentication exception entry will display the following window:

![Select Groups Local / Domain](image)

The following provide the field descriptions:

• **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**. It allows searching Microsoft groups.

• **Highlight already selected groups in search results:** If a Microsoft Group is already configured in the exception, selecting this checkbox will make it appear as a highlighted entry.
Communications Tab
This tab deals primarily with the SAS connection options.

![Image of SafeNet Authentication Service Agent for Outlook Web App 2010](image)

Authentication Server Settings Group

- **Primary Server (IP:Port):** It is used to configure the IP address/hostname of the primary SAS server. Default: Port 80
  Alternatively, **Use SSL** checkbox can also be selected.
  Default TCP port for SSL requests: 443

- **Failover Server (Optional):** It is used to configure the IP address/hostname of the failover SAS server. Default: Port 80
  Alternatively, **Use SSL** checkbox can also be selected.
  Default TCP port for SSL requests: 443

- **Disable SSL server certificate check:** Select the checkbox to disable the SSL server certificate error check. The SSL certificate check is enabled by default. This supports backward compatibility for customers using the on-premises deployment of SAS, within a well-controlled network where self-signed certificates are used and cannot be properly validated by the SAS OWA Agent.

---

**NOTE:** We strongly recommend the use of SSL certificates.
• **Select Minimum SSL/TLS version**: Configure the agent communication to use TLS. When the TLS option is selected, the agent forces a secured TLS-based channel for processing authentication requests to the SAS. This is required as a consequence of the reported POODLE vulnerability in SSL.

For more details, click [here](#).

• **Attempt to return to primary Authentication Server every**: It sets the Primary Authentication server retry interval. This setting only takes effect when the agent is using the **Failover Server**.

• **Communication Timeout**: It sets the maximum timeout value for authentication requests sent to the SAS.

• **Agent Encryption Key File**: It is used to specify the location of the SAS Agent Key File.

---

**NOTE**: If the SAS Agent Key File is changed, close and reopen the SAS Exchange Agent Configuration Tool to apply changes.

---

**Authentication Test Group**

It allow administrators to test authentication between the agent and the SAS.

**Server Status Check Group**

It performs a test to verify a connection to the SAS.

**Logging Tab**
Logging Level Group

It allows administrators to adjust the logging level. For log levels 1, 2, and 3, only the initial connection between the agent and the server, and any failed connection attempts, are logged. Log level 5 sets the agent in debug mode. Default value: 3

Log File Location Group

It allows administrators to specify the location where log files will be saved. The log file is rotated on a daily basis. The default location is \\Program Files\\SafeNet\\SAS\\Exchange\\Log.

Localization Tab

The settings on this tab represent the prompts and information messages provided by the SAS OWA Agent. These can be modified as necessary to improve usability. The Messages.txt file can also be manually modified outside of the SafeNet Microsoft Exchange Manager. This file can be found in the \\Program Files\\SafeNet\\SAS\\Exchange\\LocalizedMessages folder.
Authentication Modes

There are two modes of operation for the SAS OWA Agent. By default, **Split Authentication** mode is enabled. The authentication mode can be modified after installation using the **SafeNet Microsoft Exchange OWA Manager**.

The modes of operation are:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard Authentication Mode</strong></td>
<td>Standard Authentication Mode enables a single stage login process. Microsoft domain and SAS credentials must be entered in the OWA login page.</td>
</tr>
<tr>
<td><strong>Split Authentication Mode</strong></td>
<td>Split Authentication Mode enables a two-stage login process. In the first stage, users provide their Microsoft credentials. In the second stage, users provide their SAS credentials. This mode allow 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>

**Setting Authentication Mode**

Authentication mode is set in the SafeNet Microsoft Exchange OWA Manager, Authentication Tab.

See **Authentication Methods Tab** on page 36.
Standard Authentication Mode - Hardware/Software

1. Open OWA in your browser.
2. Enter **Domain/User Name**, **Password** and **OTP**, and click **Sign in**.

![Outlook Web App](image)

Split Authentication Mode

1. Open OWA in your browser.
2. Enter **Domain/User Name** and **Password**, and click **Sign in**.

![Outlook Web App](image)
**GrIDsure**

3. If configured for GrIDsure, do the following:
   
   I. Click **Sign In** (leaving the OTP field empty).

   ![Sign In](image1)

   II. Enter the GrIDsure OTP, derived from your grid pattern, and click **Sign in**.

   ![Enter OTP](image2)
SMS Challenge

4. If your system is configured to send OTP via SMS, enter the Token Code received on your phone and click Sign in.

Challenge-Response

If configured to work with Challenge Response, following login (in either Standard Authentication Mode or Split Authentication Mode), you will be prompted to respond to a challenge.

5. Send the challenge code, as displayed on the screen, to the designated recipient in your organization (typically System Administrator or Help Desk).

In return, you will receive a response code.

6. Enter the response code into the OTP field and click Sign in.

Prerequisites

- Ensure that TCP port 80 or 443 is open between the SAS OWA Agent and the SAS solution.
- Administrative rights to the Windows system are required during installation of the SAS OWA Agent.
- Download the Exchange Agent installation package. A link to the agents and other software can be found on the Snapshot tab in the References module for users of SAS.
To install SAS OWA Agent, follow the steps:

1. Log on to the Microsoft Exchange server.
2. Locate and run the SAS Agent for Exchange x64.exe installation package following the prompts. The Authentication Service Setup window is displayed.

   • In the Location field, enter the hostname or IP address of the primary SAS server.
   • Select Connect using SSL if SAS is configured to accept incoming SSL connections.
   • If a failover server is available, select the associated checkbox and add the hostname or IP address of a failover SAS server.
3. Click Next. The Exchange Server Selection window is displayed.
4. Select the version of Microsoft Exchange Server, and click **Next**.

![Exchange Server Selection](image)

**Upgrading SAS Agent for OWA 2013**

**NOTES:**

- Automatic upgrade from **1.09** to **1.1** is not supported. See *Installing SAS Agent for OWA 2013 Using Previous Configurations* on page 33.
- The upgrade can be performed only to and from the folder where the previous version of SAS OWA Agent was installed.
- Always work in **Run as administrator** mode when installing, uninstalling, upgrading, enabling, or disabling the SAS OWA Agent.
- Before upgrading, close the **SafeNet Microsoft Exchange OWA Manager**.

**To upgrade SAS OWA Agent from **1.09** to **1.1** version, perform the following steps:**

1. Back up the installation folder contents, including any changed templates, the INI file, and the Caption (localization) file.
2. Disable the SAS OWA Agent using the **SafeNet Microsoft Exchange OWA Manager**.
3. Close the **SafeNet Microsoft Exchange OWA Manager**.
4. Run the installation file, **SafeNet Agent for Exchange x64.exe** as an administrator. When prompted to upgrade, select **Yes**.
5. Open the **SafeNet Microsoft Exchange OWA Manager** and enable SAS OWA Agent.
Installing SAS Agent for OWA 2013 Using Previous Configurations

Automatic upgrade from 1.09 to 1.1 version is not supported.

The procedure requires export of the configurations from the previously installed version(s) followed by import of the configurations in the newly installed SAS OWA Agent 1.1.

**NOTE:** Always work in Run as administrator mode when installing, uninstalling, upgrading, enabling, or disabling the SAS OWA Agent.

The Export/Import/ procedure can be performed only to and from the folder where the previous version of SAS OWA Agent was installed.

The SAS Agent for OWA 1.1 version supports import of configurations from SAS Agent for OWA 1.06 and earlier versions.

1. To install the SAS Agent for OWA 1.1 version using configurations from a previous version, perform the following steps: In the previously installed SAS OWA Agent, export the configurations as follows:
   
   **I.** In the SafeNet Microsoft Exchange OWA Manager window, select File > Export Current Configuration.

   ![SafeNet Microsoft Exchange OWA Manager](image)

   **II.** In the Save As dialog, click Save to save the configuration files.

2. Uninstall the previously installed SAS OWA Agent.

3. Manually delete the Exchange folder (located at Program Files > SafeNet).

4. To install the new SAS Agent for OWA 1.1, run the installation file SafeNet Agent for Exchange x64.exe as an administrator.
5. In the newly installed SAS Agent, load the saved settings as follows:
   I. In the **SafeNet Microsoft Exchange OWA Manager** window, select **File > Load Saved Configuration**.

   ![SafeNet Microsoft Exchange OWA Manager window](image)

   II. In the **Open** window, select the saved configuration file (.bsidconfig) and click **Open**.

6. Enable SAS OWA Agent in the **SafeNet Microsoft Exchange OWA Manager** window

---

**NOTES:**

- After installing **SAS Agent for OWA 1.1** version, the SSL server certificate check is disabled by default.
  To change the setting go to **SafeNet Microsoft Exchange OWA Manager > Communications Tab > Authentication Server Settings**, and unselect **Disable SSL server certificate check**.

- After installing **SAS Agent for OWA 1.1** version, the Split Authentication Mode is selected by default.
  To change the settings, go to **SafeNet Microsoft Exchange OWA Manager > Authentication Methods** and select **Standard Authentication Mode**.
SafeNet Microsoft Exchange OWA Manager

The SafeNet Microsoft Exchange OWA Manager allows modification of various features available within the SAS OWA Agent.

Policy Tab

The **Policy** tab deals primarily with enabling the OWA Agent and defining the website settings.

**Authentication Processing Group**

- **Enable Agent**: Turns the SAS OWA Agent On or Off.
  
  Default value: Disabled

**Web Site Group**

- **Web Site Name**: Allows selection of the Exchange Server website.
  
  Default value: Default Web Site

- **Protected Applications**: Specifies the OWA directory on the Exchange Server.
  
  Default value: /owa

**Client IP Address Forwarding Group**

If selected, the remote client IP address will be sent to the SAS solution. Otherwise, the web server’s IP Address will be used.

Default value: Enabled
Authentication Methods Tab

The Authentication Methods tab allows selection of the login authentication method and web page authentication layout as will be presented to the user.

![Authentication Methods Tab Image](image)

**Authentication Methods Group**

- **Standard Authentication Mode**: As explained earlier, this mode enables a single-step login process. Microsoft and SAS credentials must be entered into a single login page.
  Default value: Disabled
  
  The Standard Authentication Mode provides the option to select one of two login templates:
  
  - **Hardware, Software, GrI_dsure and SMS Challenge Token Detection**: This is the default option. Domain\Username, Password, and OTP fields will be displayed.
  - **Hardware and Software Token Detection**: Domain/Username, Password, and OTP fields will be displayed.

- **Split Authentication Mode**: As explained earlier, this mode enables a two-stage login process. In the first stage, users provide their Microsoft credentials. In the second stage, users provide their SAS credentials.
  Default value: Enabled
  
  The Split Authentication Mode provides the following advantages over Standard Authentication Mode:
  
  - Microsoft group exclusions may be used to migrate users gradually from static passwords to a combination of static and one-time passwords.
- Allow administrators to specify (via Microsoft Groups) users who have been provided with GrIDsure or SMS Challenge-response tokens. This allows for a seamless login experience as the agent displays exactly what is required from the user.

- **GrIDsure Tab (Optional):** Allows an administrator to specify a Microsoft group, which contains SAS 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 that contains SAS 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 Tab**

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

**IP Range Exceptions / Inclusions Group**

It allows an administrator to define which network traffic requires SAS authentication.

**Group Authentication Exceptions Group**

Group authentication exceptions omit single or multiple domain groups from performing SAS authentication. Only one group filter option is valid at any given time; it cannot overlap with another group authentication exception.

Default value: Everyone must use SafeNet
The following group authentication exceptions are available:

- **Everyone must use SafeNet**: All users must perform SAS authentication.

- **Only selected groups will bypass SafeNet**: All users are required to perform SAS authentication, except the defined Microsoft Group(s).

- **Only selected groups must use SafeNet**: All users are not required to perform SAS authentication, except the defined Microsoft Group(s).

Adding a group authentication exception entry will display the following window:

The following provide the field descriptions:

- **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**. It allows searching Microsoft groups.

- **Highlight already selected groups in search results**: If a Microsoft group is configured in the exception, selecting this checkbox will make it appear as a highlighted entry.
Communications Tab

This tab deals primarily with the SAS connection options.

Authentication Server Settings Group

- **Primary Server (IP:Port):** It is used to configure the IP address/hostname of the primary SAS server. Default: Port 80
  Alternatively, Use SSL checkbox can also be selected.
  Default TCP port for SSL requests: 443

- **Failover Server (Optional):** It is used to configure the IP address/hostname of the failover SAS server. Default: Port 80
  Alternatively, Use SSL checkbox can also be selected.
  Default TCP port for SSL requests: 443

- **Disable SSL server certificate check:** Select the checkbox to disable the SSL server certificate error check.
  The SSL certificate check is enabled by default. This option enables you to disable the SSL server certificate error check. This supports backward compatibility for customers using the on-premises deployment of SAS, within a well-controlled network where self-signed certificates are used and cannot be properly validated by the SAS OWA Agent.

  **NOTE:** We strongly recommend the use of SSL certificates.
• **Select Minimum SSL/TLS version**: Configure the agent communication to use TLS. When the TLS option is selected the agent forces a secured TLS-based channel for processing authentication requests to SAS. This is required as a consequence of the reported POODLE vulnerability in SSL. For more details, click [here](#).

• **Attempt to return to primary Authentication Server every**: It sets the Primary Authentication server retry interval. This setting only takes effect when the agent is using the Failover Server.

• **Communication Timeout**: It sets the maximum timeout value for authentication requests sent to the SAS.

• **Agent Encryption Key File**: It is used to specify the location of the SAS Agent Key File.

**NOTE**: If the SAS Agent Key File is changed, close and reopen the SAS Exchange Agent Configuration Tool to apply changes.

**Authentication Test Group**

It allow administrators to test authentication between the agent and the SAS.

**Server Status Check Group**

It performs a test to verify a connection to the SAS.

**Logging Tab**
Logging Level Group

It allows administrators to adjust the logging level. For log levels 1, 2 and 3, only the initial connection between the agent and the server, and any failed connection attempts, are logged. Log level 5 sets the agent in debug mode.

Default value: 3

Log File Location Group

It allows administrators to specify the location where log files will be saved. The log file is rotated on a daily basis. The default location is \Program Files\SafeNet\SAS\Exchange\Log.

Localization Tab

The settings on this tab represent the prompts and information messages provided by the SAS OWA Agent. These can be modified as necessary to improve usability. The Messages.txt file can also be manually modified outside of the SafeNet Microsoft Exchange Manager. This file can be found in the \Program Files\SafeNet\SAS\Exchange\LocalizedMessages folder.
Authentication Modes

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

The modes of operation are:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard Authentication Mode</strong></td>
<td>Standard Authentication Mode enables a single stage login process. Microsoft domain and SAS credentials must be entered in the OWA login page.</td>
</tr>
<tr>
<td><strong>Split Authentication Mode</strong></td>
<td>Split Authentication Mode enables a two-stage login process. In the first stage, users provide their Microsoft credentials. In the second stage, users provide their SAS credentials. This mode allow 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>

Setting Authentication Mode

Authentication mode is set in the SafeNet Microsoft Exchange OWA Manager, Authentication Tab.

See Authentication Methods Tab on page 51.
Standard Authentication Mode - Hardware/Software

1. Open OWA in your browser.
2. Enter **Domain/User Name**, **Password** and **OTP**, and click **Sign in**.

![Sign in](image)

Split Authentication Mode

1. Open OWA in your browser.
2. Enter **Domain/User Name** and **Password**, and click **Sign in**.

![Sign in](image)
GrIDsure

3. If configured for GrIDsure, do the following:
   
   I. Click **Sign In** (leaving the OTP field empty).

   ![Sign In](image1)

   II. Enter the GrIDsure OTP, derived from your grid pattern, and click **Sign in**.

   ![Sign in](image2)
**SMS Challenge**

4. If your system is configured to send OTP via SMS, enter the Token Code received on your phone and click **Sign in.**

![Image of Outlook with OTP field and Sign in button]

**Challenge-Response**

If configured to work with Challenge Response, following login (in either Standard Authentication Mode or Split Authentication Mode), you will be prompted to respond to a challenge.

5. Send the challenge code, as displayed on the screen, to the designated recipient in your organization (typically System Administrator or Help Desk).

![Image of Outlook with OTP field and Sign in button]

In return, you will receive a response code.

6. Enter the response code into the **OTP** field and click **Sign in.**

**Prerequisites**

- Ensure that TCP port 80 or 443 is open between the SAS OWA Agent and the SAS solution.
- Administrative rights to the Windows system are required during installation of the SAS OWA Agent.
- Download the Exchange installation package. A link to the agents and other software can be found on the **Snapshot** tab in the **References** module for users of SAS.
Installing SAS Agent for OWA 2016

NOTE: Always work in Run as administrator mode when installing, uninstalling, upgrading, enabling, or disabling the SAS OWA Agent.

To install SAS OWA Agent, follow the steps:

1. Log on to the Microsoft Exchange server.
2. Locate and run the SAS Agent for Exchange x64.exe installation package following the prompts. The Authentication Service Setup window is displayed.

   - In the Location field, enter the hostname or IP address of the primary SAS server.
   - Select Connect using SSL if SAS is configured to accept incoming SSL connections.
   - If a failover server is available, select the associated checkbox and add the hostname or IP address of a failover SAS server.
3. Click Next. The Exchange Server Selection window is displayed.
4. Select the version of Microsoft Exchange Server, and click **Next**.

![SafeNet Authentication Service Agent for Exchange - InstallShield](image)

**Installing SAS Agent for OWA 2016 Using Previous Configurations**

Automatic upgrade from **1.09** to **1.1** version is not supported.

The procedure requires export of the configurations from the previously installed version(s) followed by import of the configurations in the newly installed SAS OWA Agent 1.1.

**NOTE:** Always work in **Run as administrator** mode when installing, uninstalling, upgrading, enabling, or disabling the SAS OWA Agent.

The Export/Import/ procedure can be performed only to and from the folder where the previous version of SAS OWA Agent was installed.

The SAS Agent for OWA 1.1 version supports import of configurations from SAS Agent for OWA 1.09 and earlier versions.
1. To install the SAS Agent for OWA 1.1 version using configurations from a previous version, perform the following steps: In the previously installed SAS OWA Agent, export the configurations as follows:
   I. In the **SafeNet Microsoft Exchange OWA Manager** window, select **File > Export Current Configuration**.
   II. In the **Save As** dialog, click **Save** to save the configuration files.

2. Uninstall the previously installed SAS OWA Agent.
3. Manually delete the **Exchange** folder (located at **Program Files > SafeNet**).
4. To install the new SAS Agent for OWA 1.1, run the installation file **SafeNet Agent for Exchange x64.exe** as an administrator.
5. In the newly installed SAS Agent, load the saved settings as follows:
   
   I. In the SafeNet Microsoft Exchange OWA Manager window, select File > Load Saved Configuration.

   ![SafeNet Microsoft Exchange OWA Manager window](image)

   II. In the Open window, select the saved configuration file (.bsidconfig) and click Open.


7. Restart the IIS services manually.

---

**NOTES:**

- After installing SAS Agent for OWA 1.1 version, the SSL server certificate check is disabled by default.
  
  To change the setting go to SafeNet Microsoft Exchange OWA Manager > Communications Tab > Authentication Server Settings, and unselect Disable SSL server certificate check.

- After installing SAS Agent for OWA 1.1 version, the Split Authentication Mode is selected by default.
  
  To change the settings, go to SafeNet Microsoft Exchange OWA Manager > Authentication Methods and select Standard Authentication Mode.
SafeNet Microsoft Exchange OWA Manager

The SafeNet Microsoft Exchange OWA Manager allows modification of various features available within the SAS OWA Agent.

Policy Tab

![Policy Tab Image]

The **Policy** tab deals primarily with enabling the OWA Agent and defining the website settings.

Authentication Processing Group

- **Enable Agent**: Turns the SAS OWA Agent On or Off.
  Default value: Disabled

Web Site Group

- **Web Site Name**: Allows selection of the Exchange Server website.
  Default value: Default Web Site

- **Protected Applications**: Specifies the OWA directory on the Exchange Server.
  Default value: /owa
Client IP Address Forwarding Group

If selected, the remote client IP address will be sent to the SAS solution. Otherwise, the web server’s IP Address will be used.
Default value: Enabled

Authentication Methods Tab

The Authentication Methods tab allows selection of the login authentication method and web page authentication layout as will be presented to the user.

Authentication Methods Group

- **Standard Authentication Mode:** As explained earlier, this mode enables a single-step login process. Microsoft and SAS credentials must be entered into a single login page.
  Default value: Disabled

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

  - **Hardware, Software, GrIDsure and SMS Challenge Token Detection:** This is the default option. Domain\Username, Password, and OTP fields will be displayed.
  - **Hardware and Software Token Detection:** Domain/Username, Password, and OTP fields will be displayed.
• **Split Authentication Mode**: As explained earlier, this mode enables a two-stage login process. In the first stage, users provide their Microsoft credentials. In the second stage, users provide their SAS credentials.
  
  Default value: Enabled

  The Split Authentication Mode provides the following advantages over Standard Authentication Mode:

  • Microsoft group exclusions may be used to migrate users gradually from static passwords to a combination of static and one-time passwords.

  • Allow administrators to specify (via Microsoft Groups) users who have been provided with GrIdSure or SMS Challenge-response tokens. This allows for a seamless login experience as the agent displays exactly what is required from the user.

  • **GrIdSure Tab (Optional)**: Allows an administrator to specify a Microsoft group, which contains SAS 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 that contains SAS 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 Tab**

The **Exceptions** tab allows specific Microsoft groups or network traffic to bypass SAS authentication. By default, all users are required to perform SAS authentication unless otherwise defined by exclusion.
IP Range Exceptions / Inclusions Group

It allows an administrator to define which network traffic requires SAS authentication.

Group Authentication Exceptions Group

Group authentication exceptions omit single or multiple domain groups from performing SAS authentication. Only one group filter option is valid at any given time; it cannot overlap with another group authentication exception.

Default value: Everyone must use SafeNet

The following group authentication exceptions are available:

- **Everyone must use SafeNet**: All users must perform SAS authentication.
- **Only selected groups will bypass SafeNet**: All users are required to perform SAS authentication, except the defined Microsoft Group(s).
- **Only selected groups must use SafeNet**: All users are not required to perform SAS authentication, except the defined Microsoft Group(s).

Adding a group authentication exception entry will display the following window:

The following provide the field descriptions:

- **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**. It allows searching Microsoft groups.
- **Highlight already selected groups in search results**: If a Microsoft group is configured in the exception, selecting this checkbox will make it appear as a highlighted entry.

**Communications Tab**

This tab deals primarily with the SAS connection options.

**Authentication Server Settings Group**

- **Primary Server (IP:Port)**: It is used to configure the IP address/hostname of the primary SAS server.
  - Default: Port 80
  - Alternatively, **Use SSL** checkbox can also be selected.
  - Default TCP port for SSL requests: 443

- **Failover Server (Optional)**: It is used to configure the IP address/hostname of the failover SAS server.
  - Default: Port 80
  - Alternatively, **Use SSL** checkbox can also be selected.
  - Default TCP port for SSL requests: 443
• **Disable SSL server certificate check:** Select the checkbox to disable the SSL server certificate error check.

The SSL certificate check is enabled by default. This option enables you to disable the SSL server certificate error check. This supports backward compatibility for customers using the on-premises deployment of SAS, within a well-controlled network where self-signed certificates are used and cannot be properly validated by the SAS OWA Agent.

NOTE: We strongly recommend the use of SSL certificates.

• **Select Minimum SSL/TLS version:** Configure the agent communication to use TLS.

When the TLS option is selected the agent forces a secured TLS-based channel for processing authentication requests to SAS. This is required as a consequence of the reported POODLE vulnerability in SSL.

For more details, click here.

• **Attempt to return to primary Authentication Server every:** It sets the Primary Authentication server retry interval. This setting only takes effect when the agent is using the Failover Server.

• **Communication Timeout:** It sets the maximum timeout value for authentication requests sent to the SAS.

• **Agent Encryption Key File:** It is used to specify the location of the SAS Agent Key File.

NOTE: If the SAS Agent Key File is changed, close and reopen the SAS Exchange Agent Configuration Tool to apply changes.

---

**Authentication Test Group**

It allows administrators to test authentication between the agent and the SAS.

**Server Status Check Group**

It performs a test to verify a connection to the SAS.
Logging Tab

Logging Level Group

It allows administrators to adjust the logging level. For log levels, 1, 2, and 3, only the initial connection between the agent and the server, and any failed connection attempts, are logged. Log level 5 sets the agent in debug mode.

Default value: 3

Log File Location Group

It allows administrators to specify the location where log files will be saved. The log file is rotated on a daily basis.

The default location is `C:\Program Files\SafeNet\SAS\Exchange\Log`. 
Localization Tab

The settings on this tab represent the prompts and information messages provided by the SAS OWA Agent. These can be modified as necessary to improve usability. The `Messages.txt` file can also be manually modified outside of the SafeNet Microsoft Exchange Manager. This file can be found in the `Program Files\SafeNet\SAS\Exchange\LocalizedMessages` folder.