

THALES

gemalto<sup>★</sup>  
a Thales company

# SafeNet Agent for Microsoft Outlook Web App

Installation and Configuration Guide

All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in 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.

© 2020 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:** 007-000005-001, Rev. K

**Version:** 2.1.3

**Release Date:** September 2020

# Table of Contents

<b>1 Preface.....</b>	<b>5</b>
Customer Release Notes .....	5
Audience.....	5
Third-Party Software Acknowledgement.....	5
Support Contacts.....	5
Customer Support Portal .....	5
Telephone Support .....	6
Email Support .....	6
<b>2 Introduction .....</b>	<b>7</b>
Overview.....	7
Applicability.....	7
Environment .....	8
<b>3 SafeNet Agent for Outlook Web App 2010.....</b>	<b>10</b>
Authentication Modes.....	10
Setting Authentication Mode.....	10
Standard Authentication Mode - Hardware/Software .....	11
Standard Authentication Mode - GrIDSure/SMS Challenge .....	12
Split Authentication Mode .....	13
Prerequisites.....	15
Installing SafeNet Agent for OWA 2010.....	15
Upgrading SafeNet Agent for OWA 2010 .....	18
Migrating SafeNet Agent for OWA 2010 Using Previous Configurations .....	18
SafeNet Agent for Outlook Web App .....	21
Policy Tab .....	21
Authentication Methods Tab .....	23
Exceptions Tab .....	24
Communications Tab.....	27
Logging Tab.....	29
Localization Tab.....	30
<b>4 SafeNet Agent for Outlook Web App 2013.....</b>	<b>31</b>
Authentication Modes.....	31
Setting Authentication Mode.....	31
Standard Authentication Mode - Hardware/Software .....	32
Split Authentication Mode .....	32
Prerequisites.....	34
Installing SafeNet Agent for OWA 2013.....	35
Upgrading SafeNet Agent for OWA 2013 .....	38
Migrating SafeNet Agent for OWA 2013 Using Previous Configurations .....	39
SafeNet Agent for Outlook Web App .....	42
Policy Tab .....	42
Authentication Methods Tab .....	44
Exceptions Tab .....	45

---

Communications Tab .....	48
Logging Tab .....	50
Localization Tab .....	51
<b>5 SafeNet Agent for Outlook Web App 2016/2019 .....</b>	<b>52</b>
Authentication Modes .....	52
Setting Authentication Mode .....	52
Standard Authentication Mode - Hardware/Software .....	53
Split Authentication Mode .....	53
Prerequisites .....	55
Installing SafeNet Agent for OWA 2016/2019 .....	56
Upgrading SafeNet Agent for OWA 2016 .....	59
Migrating SafeNet Agent for OWA 2016 Using Previous Configurations .....	60
SafeNet Agent for Outlook Web App .....	63
Policy Tab .....	63
Authentication Methods Tab .....	65
Exceptions Tab .....	66
Communications Tab .....	69
Logging Tab .....	71
Localization Tab .....	72

# Preface

This document describes how to install and configure the SafeNet 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 SafeNet 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, refer to the documentation. If you cannot resolve the issue, contact your supplier or [Gemalto Customer Support](#).

Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

## Customer Support Portal

The Customer Support Portal, at <https://supportportal.gemalto.com>, is a 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 Gemalto Customer Support by telephone at +1 410-931-7520. 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).

# Introduction

## 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 SafeNet solution 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 SafeNet server 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 SafeNet 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 SafeNet 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 SafeNet solution.
- Deploy and configure using the SafeNet agent.

## Applicability

---

The information in this document applies to:

- **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.
- **SafeNet Trusted Access (earlier, SAS Cloud)** — The SafeNet's cloud-based authentication service.

## Environment

<b>Network</b>	<ul style="list-style-type: none"> <li>• TCP 443</li> <li>• TCP 80</li> </ul>
<b>Supported Architecture</b>	<ul style="list-style-type: none"> <li>• 64-bit</li> </ul>
<b>Supported Web Servers</b>	<ul style="list-style-type: none"> <li>• IIS 7.0</li> <li>• IIS 7.5</li> <li>• IIS 8.0</li> <li>• IIS 8.5</li> <li>• IIS 10</li> </ul>
<b>Supported Exchange Server Versions</b>	<ul style="list-style-type: none"> <li>• Microsoft Exchange Server 2010</li> <li>• Microsoft Exchange Server 2013</li> <li>• Microsoft Exchange Server 2016</li> <li>• Microsoft Exchange Server 2019</li> </ul>
<b>Operating System</b>	<ul style="list-style-type: none"> <li>• Windows Server 2008 R2</li> <li>• Windows Server 2012</li> <li>• Windows Server 2012 R2</li> <li>• Windows Server 2016</li> <li>• Windows Server 2019</li> </ul>
<b>Additional Software</b>	<ul style="list-style-type: none"> <li>• .NET 3.5 (for SafeNet Agent for Outlook Web App 2010)</li> <li>• .NET 4.5.2 (for SafeNet Agent for Outlook Web App 2013, SafeNet Agent for Outlook Web App 2016, and SafeNet Agent for Outlook Web App 2019)</li> </ul> <p><u>Note:</u> If .NET framework 4.5.2 (or above) is installed from the agent package, the Exchange Server will be restarted automatically.</p>
<b>Supported Web Browsers</b>	<ul style="list-style-type: none"> <li>• Internet Explorer (IE) 10 and 11</li> </ul> <p><u>Note:</u> Recommended browser for Microsoft Exchange Server 2013, Microsoft Exchange Server 2016, and Microsoft Exchange Server 2019 is Internet Explorer (IE) 11.</p> <ul style="list-style-type: none"> <li>• Firefox</li> <li>• Chrome</li> </ul>
<b>Additional Web Browsers Requirements</b>	<ul style="list-style-type: none"> <li>• Cookies must be enabled</li> <li>• JavaScript must be enabled</li> <li>• ActiveX must be enabled</li> </ul>



---

<b>Supported Authentication Methods</b>	All tokens and authentication methods supported by SafeNet server except Push OTP.
<b>SafeNet Authentication Service (SAS) releases</b>	<ul style="list-style-type: none"><li>• SAS PCE/SPE 3.9.1 (and later)</li><li>• SafeNet Trusted Access (earlier, SAS Cloud)</li></ul>

---

# SafeNet Agent for Outlook Web App 2010

## Authentication Modes

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

Mode	Description
<b>Standard Authentication Mode</b>	Standard Authentication Mode enables a single-stage login process. Domain and SafeNet credentials must be entered in the OWA login page to access web-based resources.
<b>Split Authentication Mode</b>	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 SafeNet credentials. This mode allow administrators to control authentication dialogs, based on Microsoft groups, token type (such as Gridsure), or IP-exclusion groups.

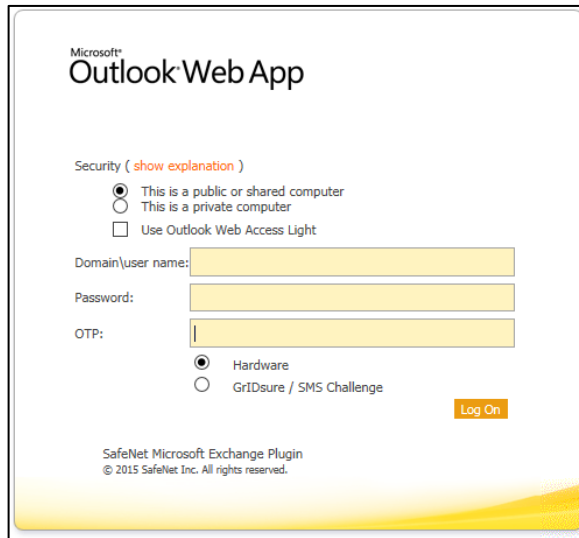
## Setting Authentication Mode

Authentication mode is set in the SafeNet Agent for Outlook Web App, Authentication tab.

See **Authentication Methods Tab**.

## 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**.



Microsoft®  
Outlook Web App

Security ( [show explanation](#) )

This is a public or shared computer  
 This is a private computer  
 Use Outlook Web Access Light

Domain\user name:

Password:

OTP:

Hardware  
 Gridsure / SMS Challenge

SafeNet Microsoft Exchange Plugin  
© 2015 SafeNet Inc. All rights reserved.

3. Enter **Domain/User Name**, **Password** and **OTP** (One Time Password), and click **Log On**.



Microsoft®  
Outlook Web App

Security ( [show explanation](#) )

This is a public or shared computer  
 This is a private computer  
 Use Outlook Web Access Light

Domain\user name:

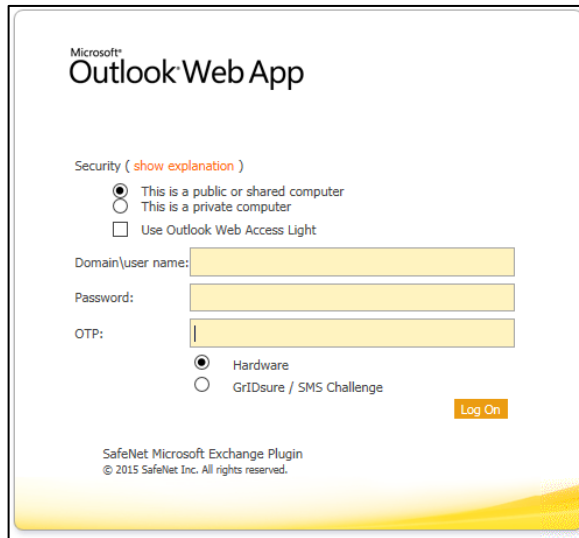
Password:

OTP:

SafeNet Microsoft Exchange Plugin  
© 2015 SafeNet Inc. All rights reserved.

## Standard Authentication Mode - GrIDSure/SMS Challenge

1. Open OWA in your browser.
2. Select **GrIDSure / SMS Challenge** radio button and click **Log On**.



Microsoft®  
Outlook Web App

Security ( [show explanation](#) )

This is a public or shared computer  
 This is a private computer  
 Use Outlook Web Access Light

Domain\user name:

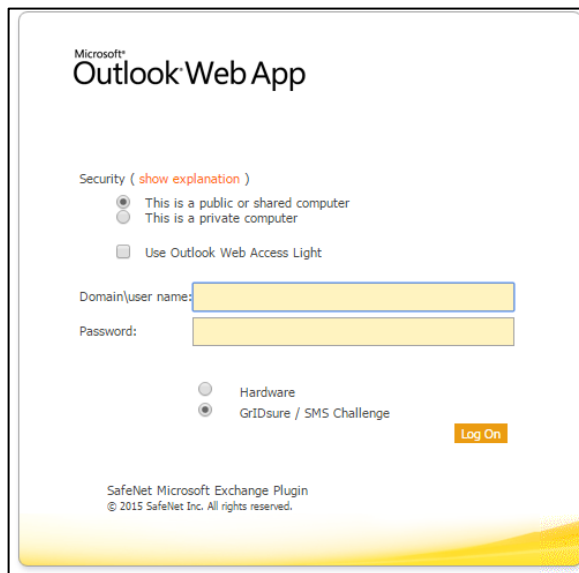
Password:

OTP:

Hardware  
 GrIDSure / SMS Challenge

SafeNet Microsoft Exchange Plugin  
© 2015 SafeNet Inc. All rights reserved.

3. Enter **Domain/User Name, Password,** and click **Log On**.



Microsoft®  
Outlook Web App

Security ( [show explanation](#) )

This is a public or shared computer  
 This is a private computer  
 Use Outlook Web Access Light

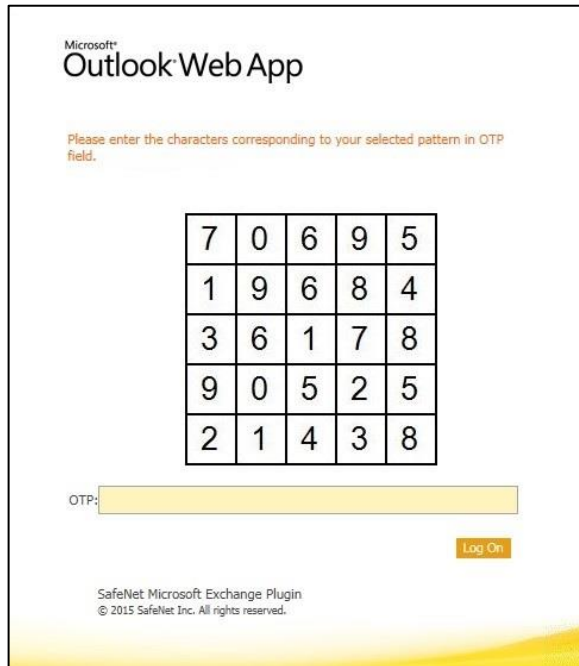
Domain\user name:

Password:

Hardware  
 GrIDSure / SMS Challenge

SafeNet Microsoft Exchange Plugin  
© 2015 SafeNet Inc. All rights reserved.

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.



Microsoft  
Outlook Web App

Please enter the characters corresponding to your selected pattern in OTP field.

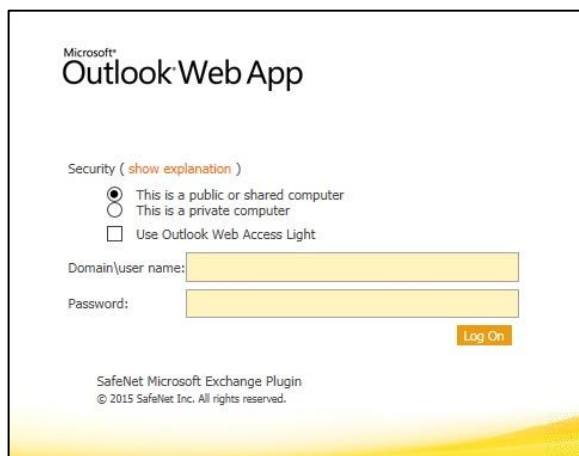
7	0	6	9	5
1	9	6	8	4
3	6	1	7	8
9	0	5	2	5
2	1	4	3	8

OTP:

SafeNet Microsoft Exchange Plugin  
© 2015 SafeNet Inc. All rights reserved.

## Split Authentication Mode

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



Microsoft  
Outlook Web App

Security ( [show explanation](#) )

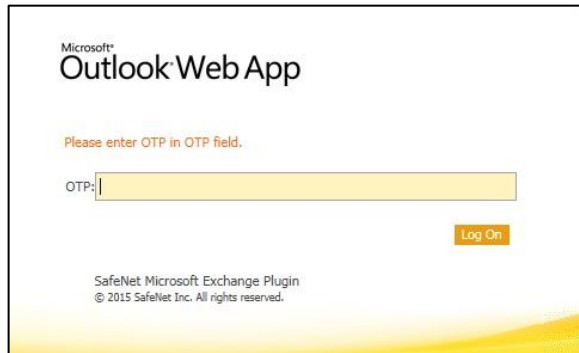
This is a public or shared computer  
 This is a private computer  
 Use Outlook Web Access Light

Domain\user name:

Password:

SafeNet Microsoft Exchange Plugin  
© 2015 SafeNet Inc. All rights reserved.

3. Enter OTP and click **Log On**.



Microsoft  
Outlook Web App

Please enter OTP in OTP field.

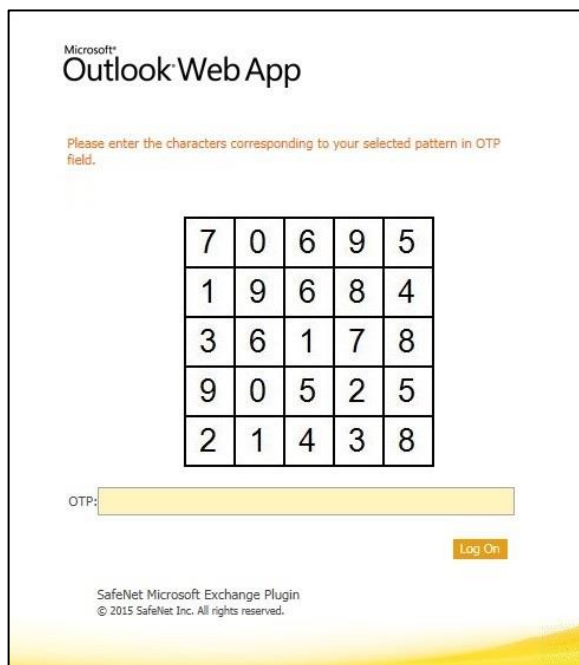
OTP:

Log On

SafeNet Microsoft Exchange Plugin  
© 2015 SafeNet Inc. All rights reserved.

## GrIDSure

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



Microsoft  
Outlook Web App

Please enter the characters corresponding to your selected pattern in OTP field.

7	0	6	9	5
1	9	6	8	4
3	6	1	7	8
9	0	5	2	5
2	1	4	3	8

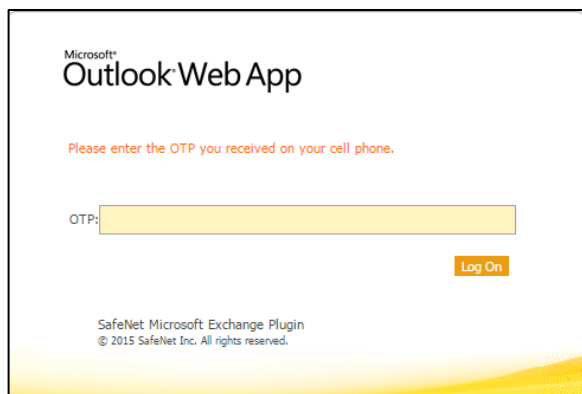
OTP:

Log On

SafeNet Microsoft Exchange Plugin  
© 2015 SafeNet Inc. All rights reserved.

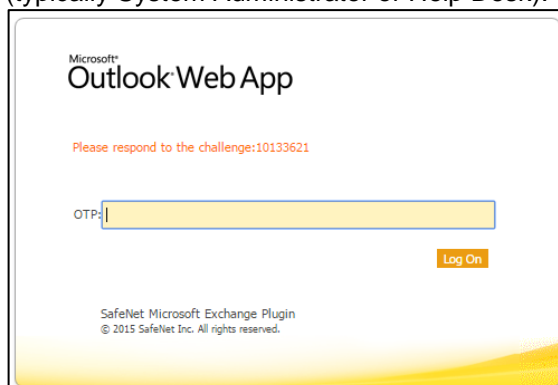
## SMS Challenge

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



## Challenge-Response

1. 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.
2. 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.

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

## Prerequisites

- Ensure that TCP port 80 or 443 is open on the Exchange Server, which would act as a gateway of communication between the SafeNet OWA Agent and the SafeNet solution.
- Administrative rights to the Windows system are required during installation of the SafeNet 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 SafeNet server.

## Installing SafeNet Agent for OWA 2010



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

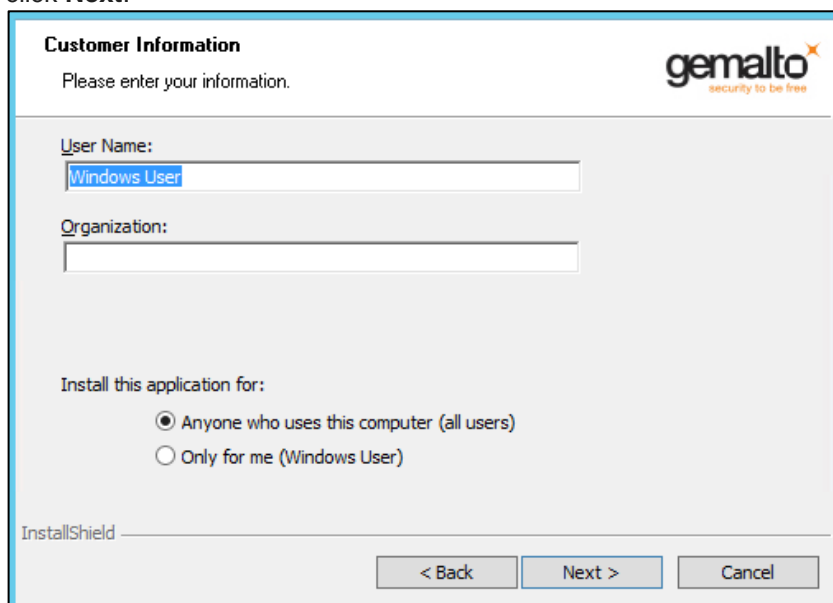
---

Always disable the agent first, and then uninstall, if required.

---

To install SafeNet OWA Agent, follow the steps:

1. Log on to the Microsoft Exchange server.
2. Locate and execute the following installation file:  
SafeNet Agent for Microsoft Outlook Web App 2010.exe
3. On the **Welcome to the InstallShield Wizard...** window, click **Next**.
4. On the **License Agreement** window, select **I accept the terms in the license agreement**, and click **Next**.
5. 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)**
- **Only for me (Windows User)**

- 
6. On the **Authentication Service Setup** window, enter the following details:
    - In the **Location** field, enter the hostname or IP address of the primary SafeNet server.
    - Select **Connect using SSL** if SafeNet server 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 SafeNet server.



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**.

To proceed, the InstallShield Wizard searches for, and selects the **Microsoft Exchange Server 2010** version in the background.

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.

## Upgrading SafeNet Agent for OWA 2010

---

Automatic upgrade to **2.1.3** version is not supported. For upgrade, the configurations from the older version must be saved, and then imported into the new installation. For migrating from one version to another, see [Migrating SafeNet Agent for OWA 2010 Using Previous Configurations](#) section below.

### Migrating SafeNet Agent for OWA 2010 Using Previous Configurations

The migration procedure requires export of the configurations from the previously installed version(s) followed by import of the configurations in the newly installed SafeNet OWA Agent 2.1.3.

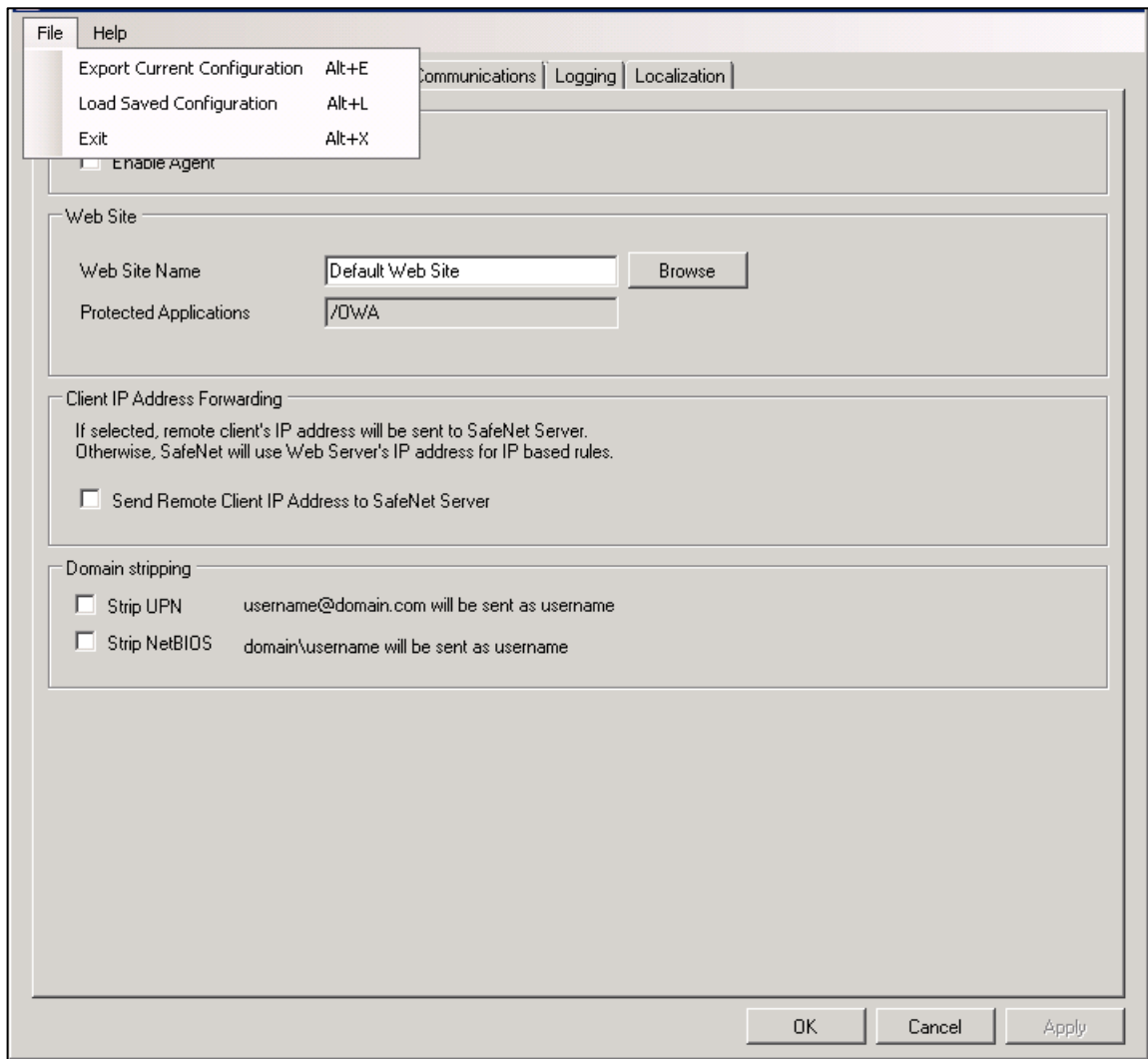
---

**NOTES:**

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

The SafeNet Agent for OWA 2.1.3 version supports import of configurations from SafeNet Agent for OWA **1.09** and later versions. To install the SafeNet Agent for OWA 2.1.3 version using configurations from a previous version, perform the following steps:

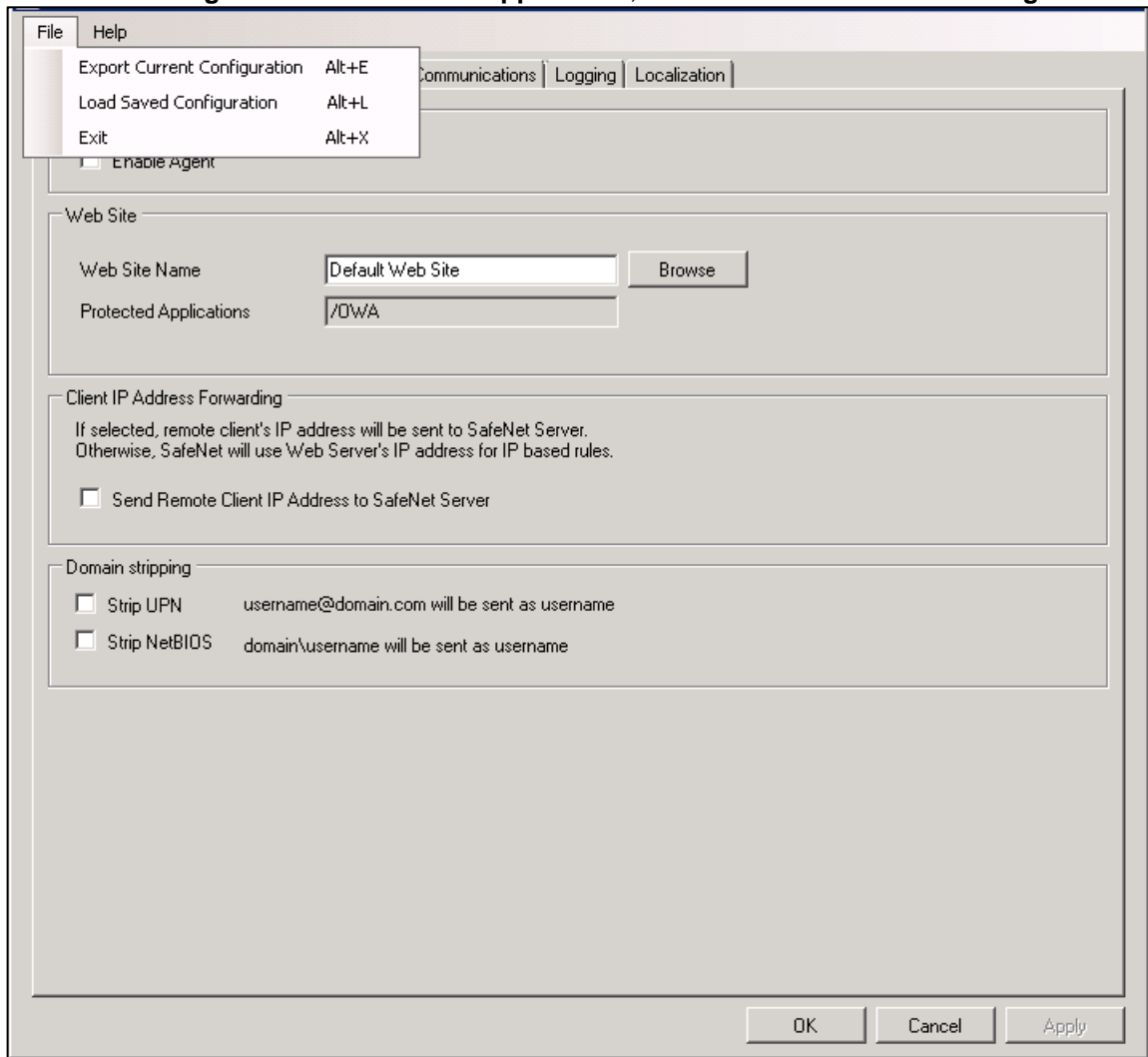
1. In the previously installed SafeNet OWA Agent, export the configurations as follows:
  - I. In the **SafeNet Agent for Outlook Web App** window, select **File > Export Current Configuration**.



- II. In the **Save As** dialog, click **Save** to save the configuration files.
2. Uninstall the previously installed SafeNet OWA Agent.
3. Manually delete the **Exchange** folder (located at **Program Files > SafeNet**).
4. To install the new SafeNet Agent for OWA, run the installation file as an administrator:  
**SafeNet Agent for Microsoft Outlook Web App 2010.exe**

5. In the newly installed SafeNet Agent, load the saved settings as follows:

- I. In the **SafeNet Agent for Outlook Web App** window, select **File > Load Saved Configuration**.



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

6. Click **OK**.



**NOTES:** After migrating to **SafeNet Agent for OWA 2.1.3** version, the **Split Authentication Mode** is selected, by default. If you require to change the settings, go to **SafeNet Agent for Outlook Web App > Authentication Methods** and select **Standard Authentication Mode**.

## SafeNet Agent for Outlook Web App

The SafeNet Agent for Outlook Web App allows modification of various features available within the SafeNet OWA Agent.

### Policy Tab

The screenshot shows the 'Policy' tab in the configuration window. The 'Authentication Processing' section has the 'Enable Agent' checkbox checked. The 'Web Site' section has 'Web Site Name' set to 'Default Web Site' and 'Protected Applications' set to '/OWA'. The 'Client IP Address Forwarding' section has the 'Send Remote Client IP Address to SafeNet Server' checkbox unchecked. The 'Domain stripping' section has both 'Strip UPN' and 'Strip NetBIOS' checkboxes checked.

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

### Authentication Processing Group

- **Enable Agent:** Turns the SafeNet 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 SafeNet solution. Otherwise, the web server's IP address will be used.

Default value: Enabled

## Domain Stripping

- Strip realm from UPN (`username@domain.com` will be sent as username): Select the checkbox if the SafeNet server username is required without the suffix `@domain`.
- Strip NetBIOS prefix (`domain\username` will be sent as username): Select the checkbox if the SafeNet server username is required without the prefix `\domain`.

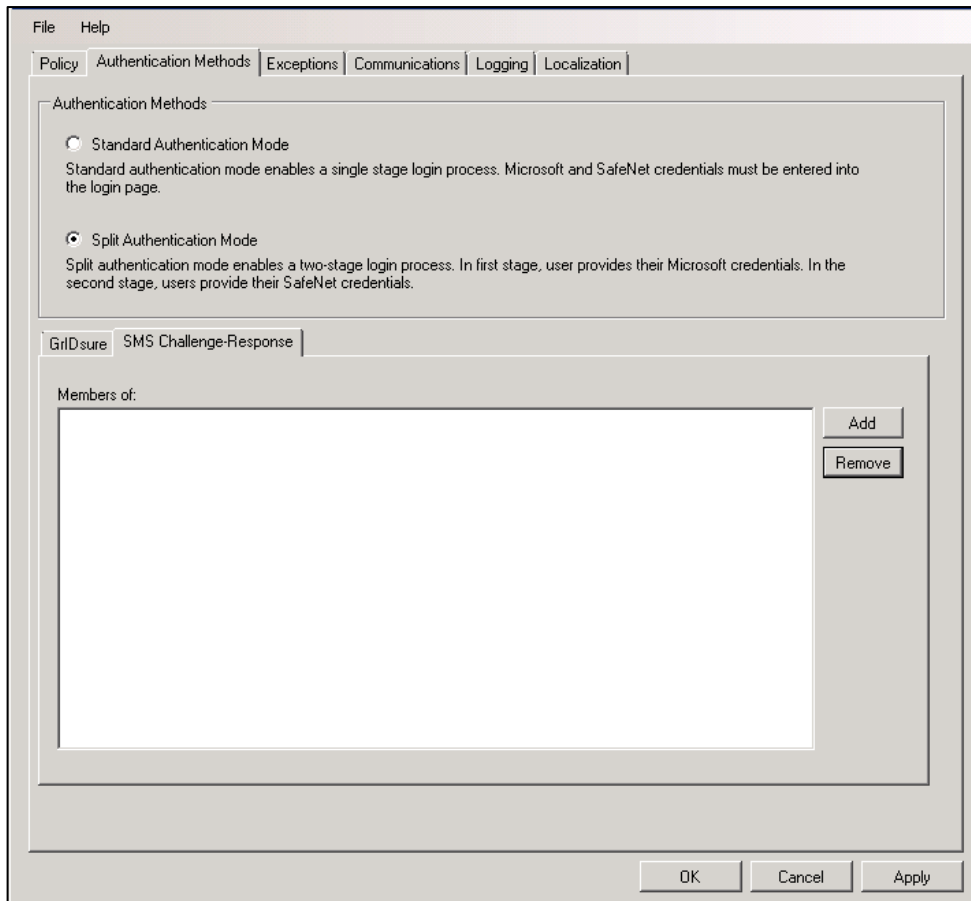


**NOTE:** The realm-stripping feature applies to SafeNet server usernames only.  
Active Directory usernames are not affected.

---

## 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 SafeNet 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:

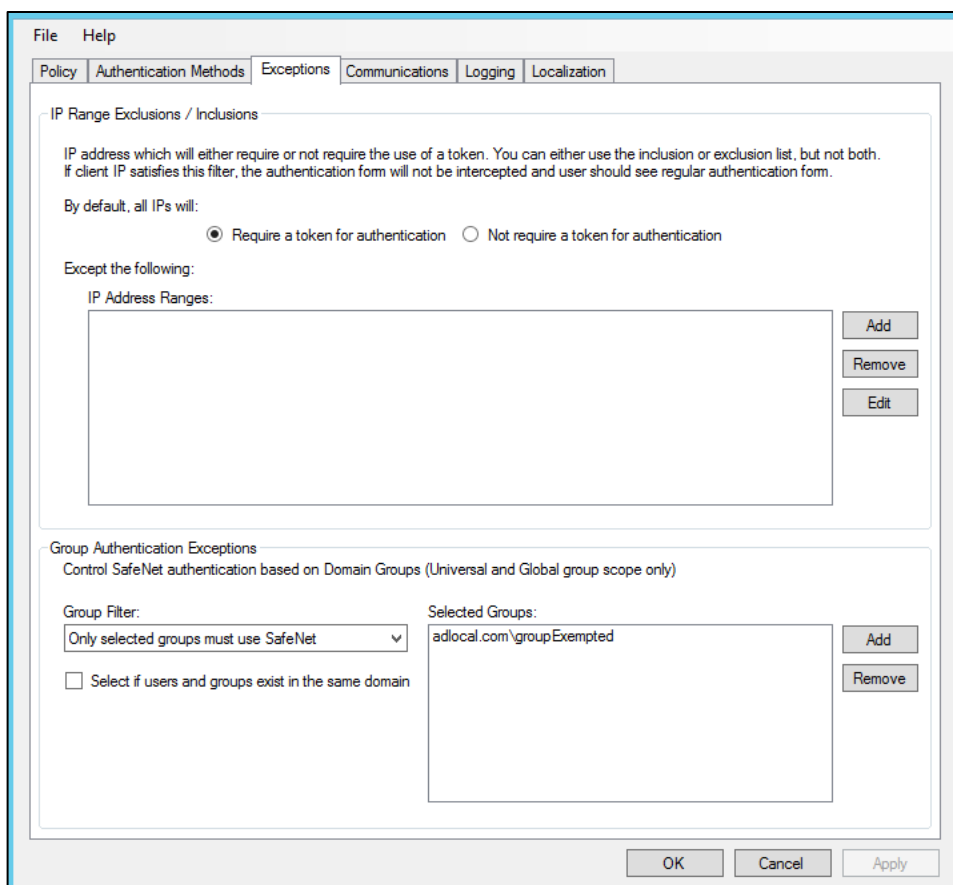
- **Hardware, Software, GridSure, and SMS Challenge Token Detection:** This is the default option. If selected, the following fields are displayed on the login page: **Username, Password, OTP, Hardware, and GridSure/SMS Challenge.**
- **Hardware and Software Token Detection:** If a software token is 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 SafeNet 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 SafeNet server 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 SafeNet server 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 SafeNet authentication. By default, all users are required to perform SafeNet authentication unless otherwise defined by exclusion.



## IP Range Exclusions / Inclusions Group

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



## Group Authentication Exceptions Group



**NOTE:** While adding Security Groups, the groups having the **Domain Local** scope will not be visible in the OWA Manager. Only the universal and global domain groups will be visible.

- **Group Filter** and **Selected Groups:** Group authentication exceptions omit single or multiple domain groups from performing SafeNet 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 SafeNet authentication.
- **Only selected groups will bypass SafeNet:** All users are required to perform SafeNet authentication, except the defined Microsoft Group(s).
- **Only selected groups must use SafeNet:** All users are not required to perform SafeNet authentication, except the defined Microsoft Group(s).

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

The screenshot shows a dialog box titled "Select Domain Groups". It contains the following elements:

- A dropdown menu labeled "From this location:" with "adlocal.com" selected.
- A text input field labeled "Enter the group names to select (examples):" with a "Check Names" button to its right.
- A checkbox labeled "Highlight already selected groups in search result".
- Buttons labeled "Show All" and "UnSelect All" to the right of the checkbox.
- Buttons labeled "Select All" and "UnSelect All" above the search result area.
- A large empty rectangular area for the search results.
- "OK" and "Cancel" buttons at the bottom.

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.
- **Select if users and groups exist in the same domain:** The checkbox ensures that the child domain is also effectively searched for users and groups. If selected, the group exclusions functionality will search and apply authentication exceptions even if both users and groups exist in the child domain. If the checkbox is cleared, exceptions will only be applied if both users and groups exist in the parent domain. Default value: Clear

## Communications Tab

This tab deals primarily with the SafeNet server connection options.

### Authentication Server Settings Group

- Primary Server (IP:Port):** It is used to configure the IP address/hostname of the primary SafeNet 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 SafeNet 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 SafeNet server, within a well-controlled network where self-signed certificates are used and cannot be properly validated by the SafeNet 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 SafeNet server. 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 SafeNet server.
  - **Agent Encryption Key File:** It is used to specify the location of the SafeNet Agent Key File.
- 



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

---

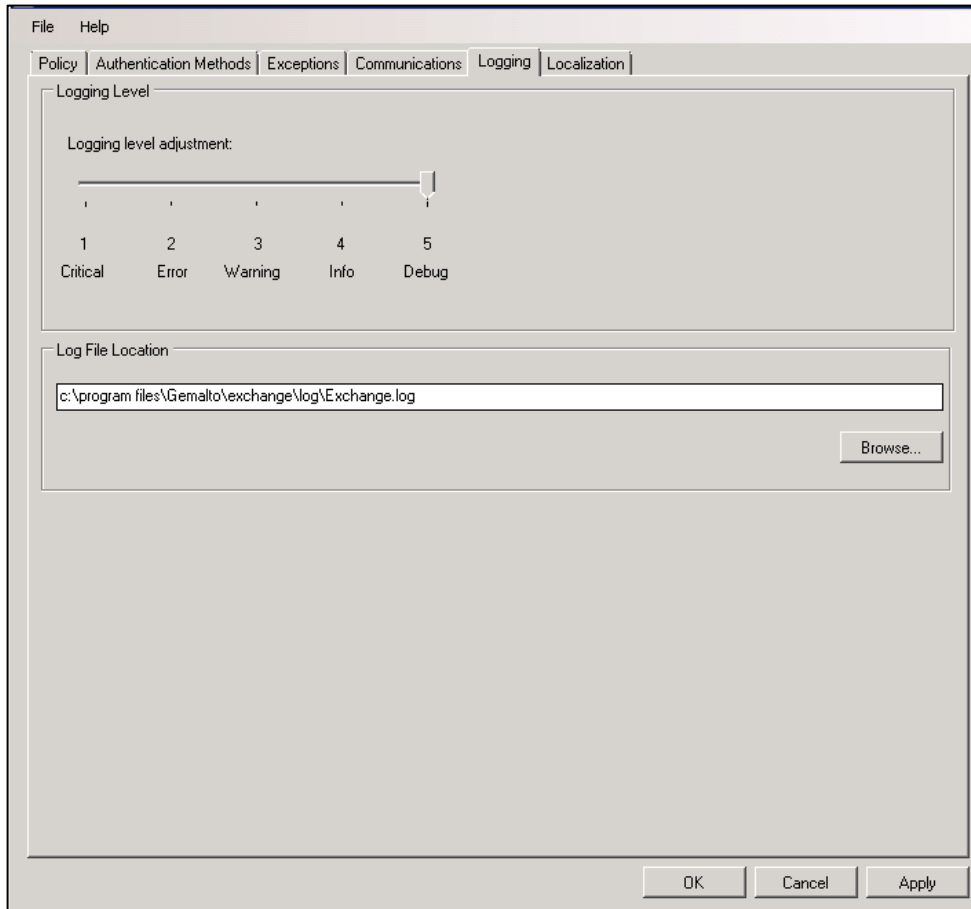
## Authentication Test Group

It allow administrators to test authentication between the agent and the SafeNet server.

## Server Status Check Group

It performs a test to verify a connection to the SafeNet server.

## Logging Tab



### Logging Level Group

It allow 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.

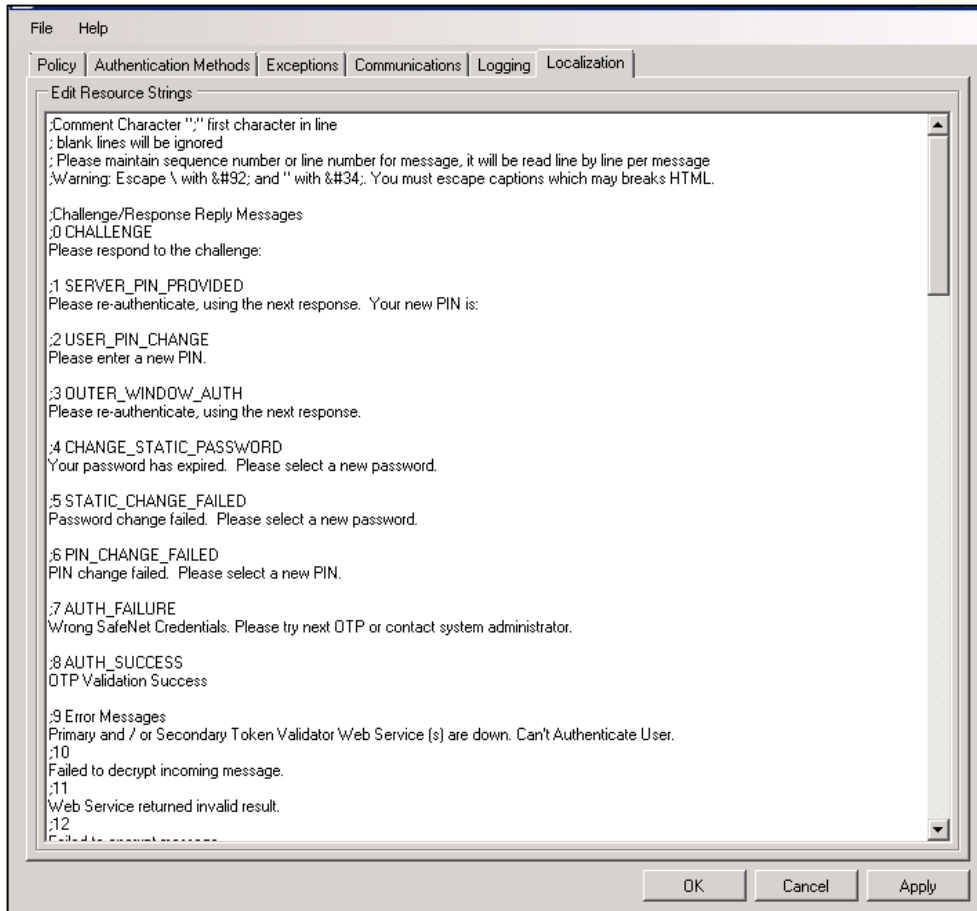
Default value: 5

### Log File Location Group

It allow 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\Gemalto\Exchange\Log`.

## Localization Tab



The settings on this tab represent the prompts and information messages provided by the SafeNet OWA Agent. These can be modified as necessary to improve usability. The **Messages.txt** file can be manually modified outside of the SafeNet Microsoft Exchange Manager. This file can be found at the following location:  
 Program Files\Gemalto\Exchange\LocalizedMessages

# SafeNet Agent for Outlook Web App 2013

## Authentication Modes

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

The modes of operation are:

Mode	Description
<b>Standard Authentication Mode</b>	Standard Authentication Mode enables a single stage login process. Microsoft domain and SafeNet credentials must be entered in the OWA login page.
<b>Split Authentication Mode</b>	Split Authentication Mode enables a two-stage login process. In the first stage, users provide their Microsoft credentials. In the second stage, users provide their SafeNet credentials. This mode 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.

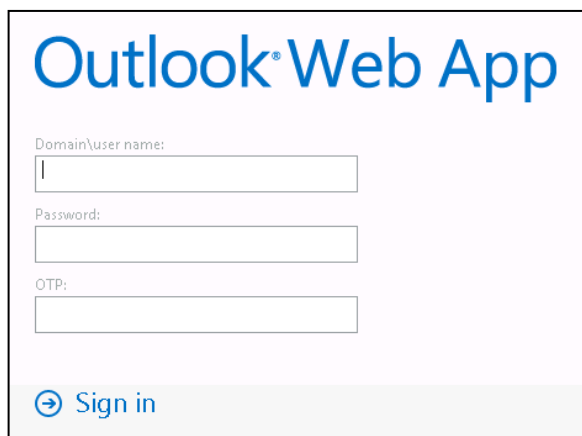
## Setting Authentication Mode

Authentication mode is set in the SafeNet Agent for Outlook Web App, Authentication Tab.

See **Authentication Methods Tab**.

## 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

Domain\user name:

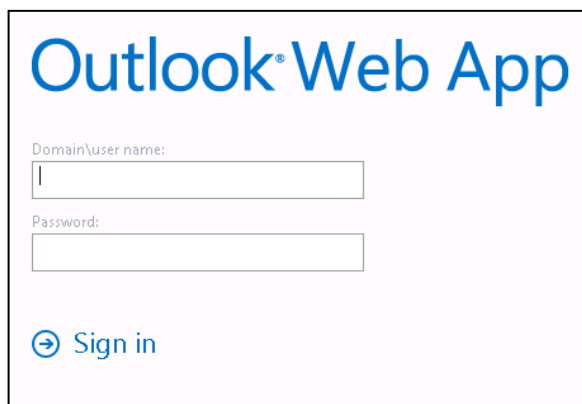
Password:

OTP:

 Sign in

## Split Authentication Mode


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



Outlook® Web App

Domain\user name:

Password:

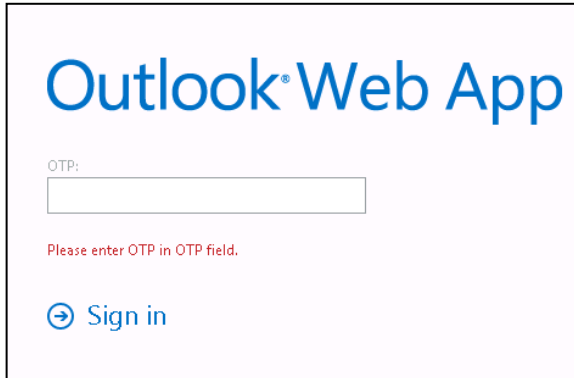
 Sign in



## GrIDSure

1. If configured for GrIDSure, do the following:

- I. Click **Sign In** (leaving the OTP field empty).



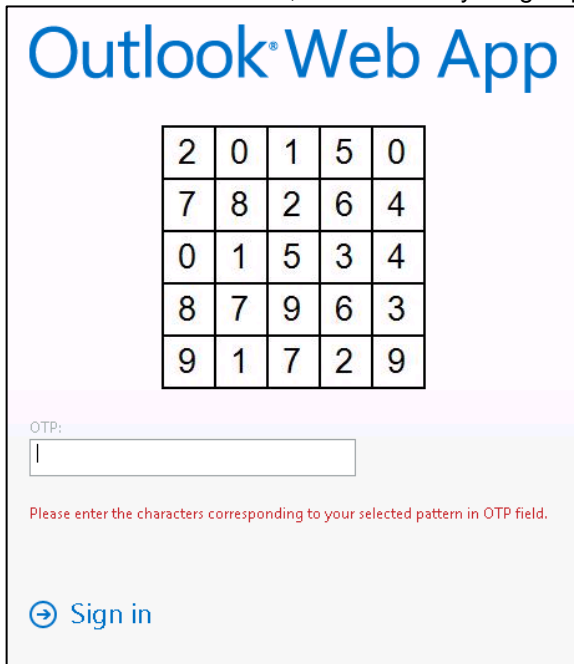
Outlook® Web App

OTP:

Please enter OTP in OTP field.

[➔ Sign in](#)

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



Outlook® Web App

2	0	1	5	0
7	8	2	6	4
0	1	5	3	4
8	7	9	6	3
9	1	7	2	9

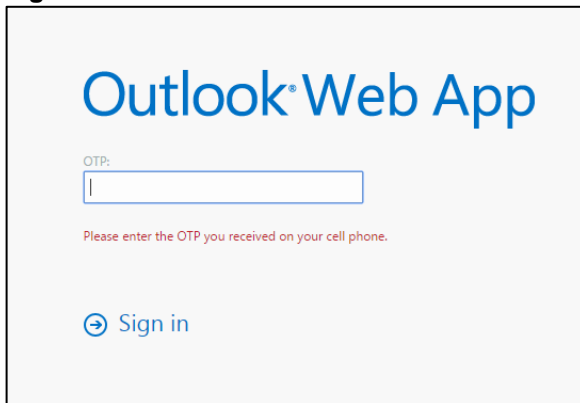
OTP:

Please enter the characters corresponding to your selected pattern in OTP field.

[➔ Sign in](#)

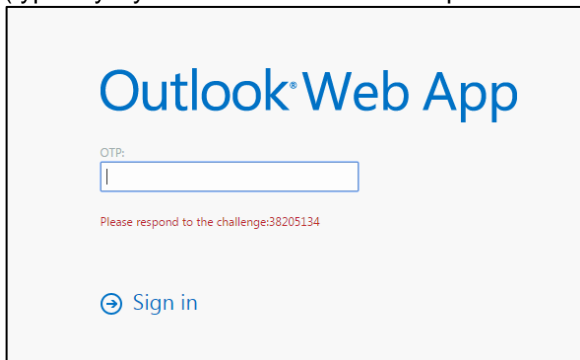
## SMS Challenge

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

A screenshot of the Outlook Web App login page. The title "Outlook Web App" is at the top in blue. Below it is an "OTP:" label and a text input field. Under the input field, a red message reads "Please enter the OTP you received on your cell phone." At the bottom left, there is a blue "Sign in" button with a right-pointing arrow icon.

## Challenge-Response

1. 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.
2. Send the challenge code, as displayed on the screen, to the designated recipient in your organization (typically System Administrator or Help Desk).

A screenshot of the Outlook Web App login page. The title "Outlook Web App" is at the top in blue. Below it is an "OTP:" label and a text input field. Under the input field, a red message reads "Please respond to the challenge:38205134". At the bottom left, there is a blue "Sign in" button with a right-pointing arrow icon.

In return, you will receive a response code.

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

## Prerequisites

- Ensure that TCP port 80 or 443 is open on the Exchange Server, which would act as a gateway of communication between the SafeNet OWA Agent and the SafeNet solution.
- Administrative rights to the Windows system are required during installation of the SafeNet 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 SafeNet server.

## Installing SafeNet Agent for OWA 2013

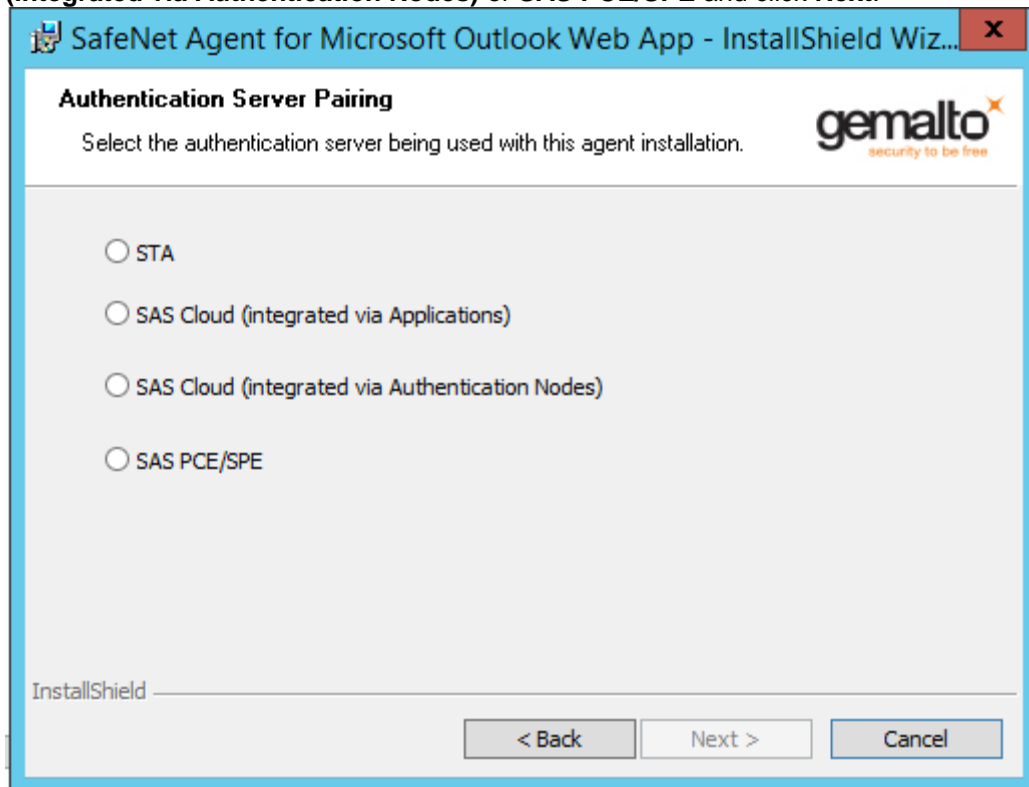


**NOTE:** Always work in **Run as administrator** mode when installing, uninstalling, enabling, or disabling the SafeNet OWA Agent.

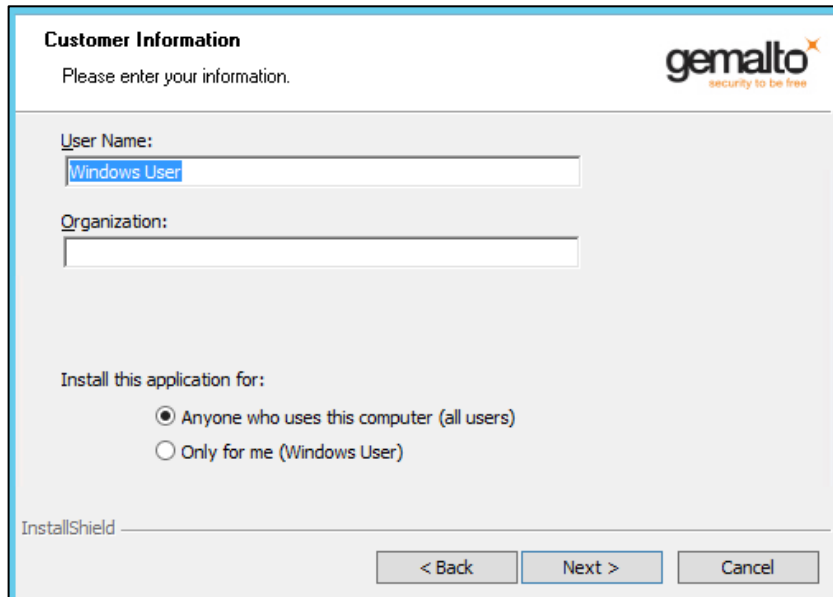
Always disable the agent first, and then uninstall, if required.

To install SafeNet OWA Agent, follow the steps:

1. Log on to the Microsoft Exchange server.
2. Locate and execute the following installation file:  
SafeNet Agent for Microsoft Outlook Web App 2013-2016.exe
3. On the **Welcome to the InstallShield Wizard...** window, click **Next**.
4. On the **License Agreement** window, select **I accept the terms in the license agreement**, and click **Next**.
5. On the **Authentication Server Pairing** window, select the Authentication Server type, **SAS Cloud (integrated via Authentication Nodes)** or **SAS PCE/SPE** 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:

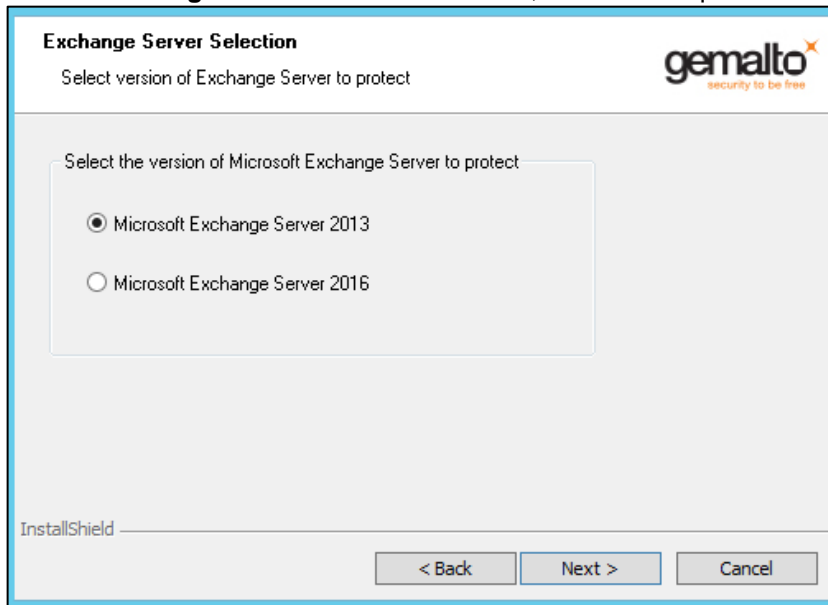
- **Anyone who uses this computer (all users)**
- **Only for me (Windows User)**

7. On the **Authentication Service Setup** window, enter the following details:
- In the **Location** field, enter the hostname or IP address of the primary SafeNet server.
  - Select **Connect using SSL** if SafeNet server 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 SafeNet server.

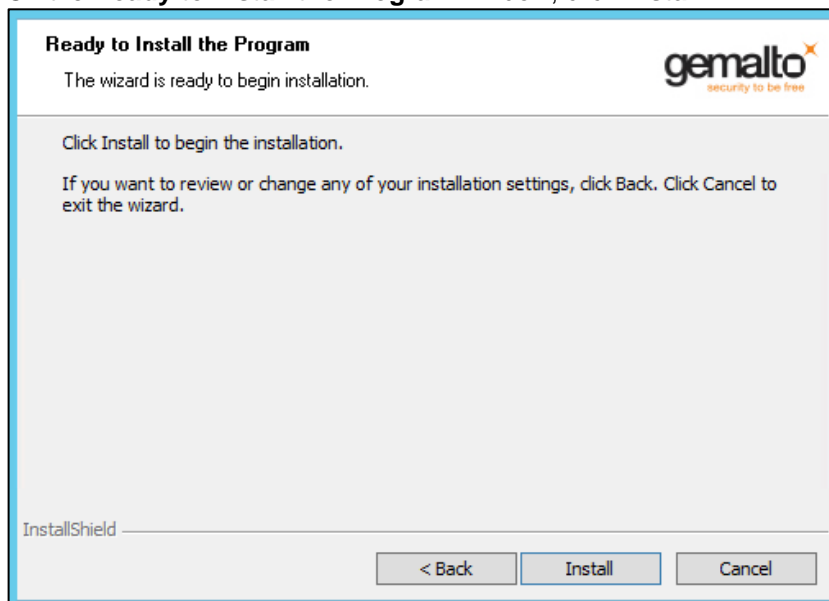
8. On the **Destination Folder** window, perform one of the following steps:
- To change the installation folder, click **Change** and navigate to the required folder, and then click **Next**.
  - To accept the default installation folder as displayed, click **Next**.

To proceed, the InstallShield Wizard searches for the applicable Exchange Server version in the background. If the Exchange Server is not found, it prompts for the following additional selection:

- I. On the **Exchange Server Selection** window, select the required Exchange Server version.



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



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

## Upgrading SafeNet Agent for OWA 2013

Automatic upgrade to **2.1.3** version is not supported. For upgrade, the configurations from the older version must be saved, and then imported into the new installation. For migrating from one version to another, see [Migrating SafeNet Agent for OWA 2013 Using Previous Configurations](#) section below.

## Migrating SafeNet Agent for OWA 2013 Using Previous Configurations

The migration procedure requires export of the configurations from the previously installed version(s) followed by import of the configurations in the newly installed SafeNet OWA Agent 2.1.3.

---



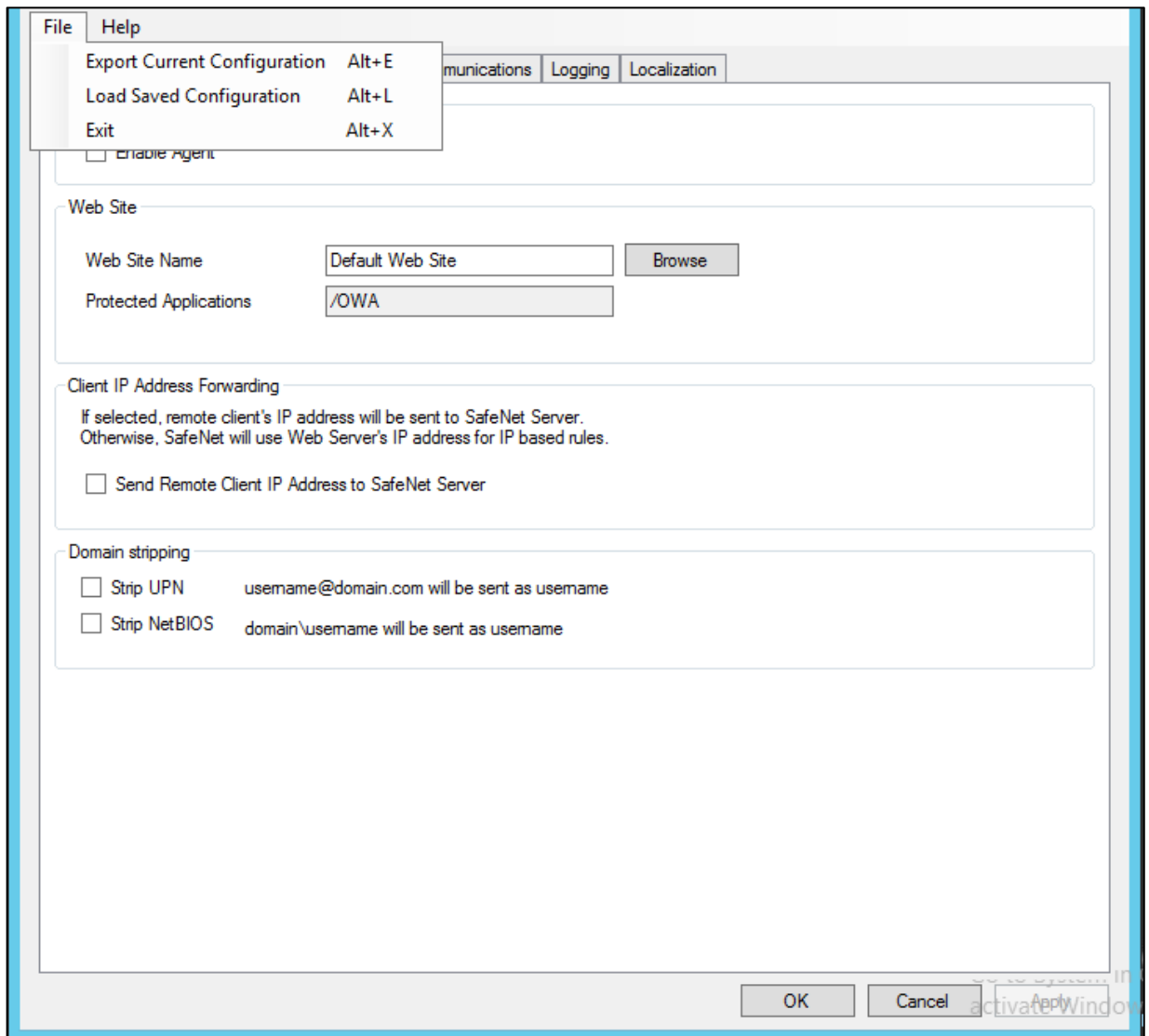
### NOTES:

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

The SafeNet Agent for OWA 2.1.3 version supports import of configurations from SafeNet Agent for OWA **1.09** and later versions. To install the SafeNet Agent for OWA 2.1.3 version using configurations from a previous version, perform the following steps:

1. In the previously installed SafeNet OWA Agent, export the configurations as follows:

- I. In the **SafeNet Agent for Outlook Web App** window, select **File > Export Current Configuration**.



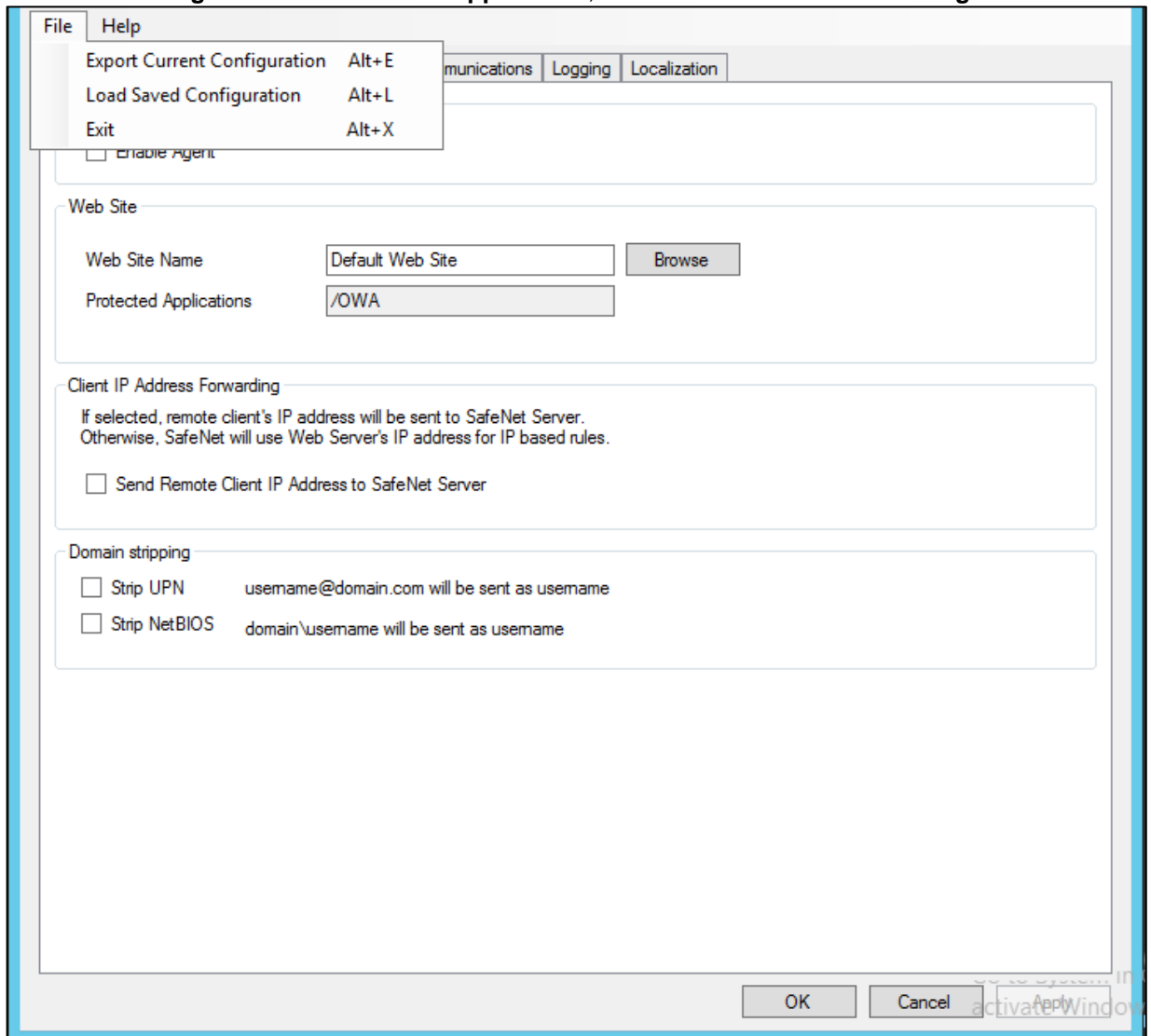
- II. In the **Save As** dialog, click **Save** to save the configuration files.

2. Uninstall the previously installed SafeNet OWA Agent.
3. Manually delete the **Exchange** folder (located at **Program Files > SafeNet**).
4. To install the new SafeNet Agent for OWA, run the installation file as an administrator: **SafeNet Agent for Microsoft Outlook Web App 2013-2016.exe**



5. In the newly installed SafeNet Agent, load the saved settings as follows:

- I. In the **SafeNet Agent for Outlook Web App** window, select **File > Load Saved Configuration**.



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

6. Click **OK**.



**NOTES:** After migrating to **SafeNet Agent for OWA 2.1.3** version, the **Split Authentication Mode** is selected, by default. If you require to change the settings, go to **SafeNet Agent for Outlook Web App > Authentication Methods** and select **Standard Authentication Mode**.

## SafeNet Agent for Outlook Web App

The SafeNet Agent for Outlook Web App allows modification of various features available within the SafeNet 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 SafeNet 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 SafeNet solution. Otherwise, the web server's IP Address will be used.

Default value: Enabled

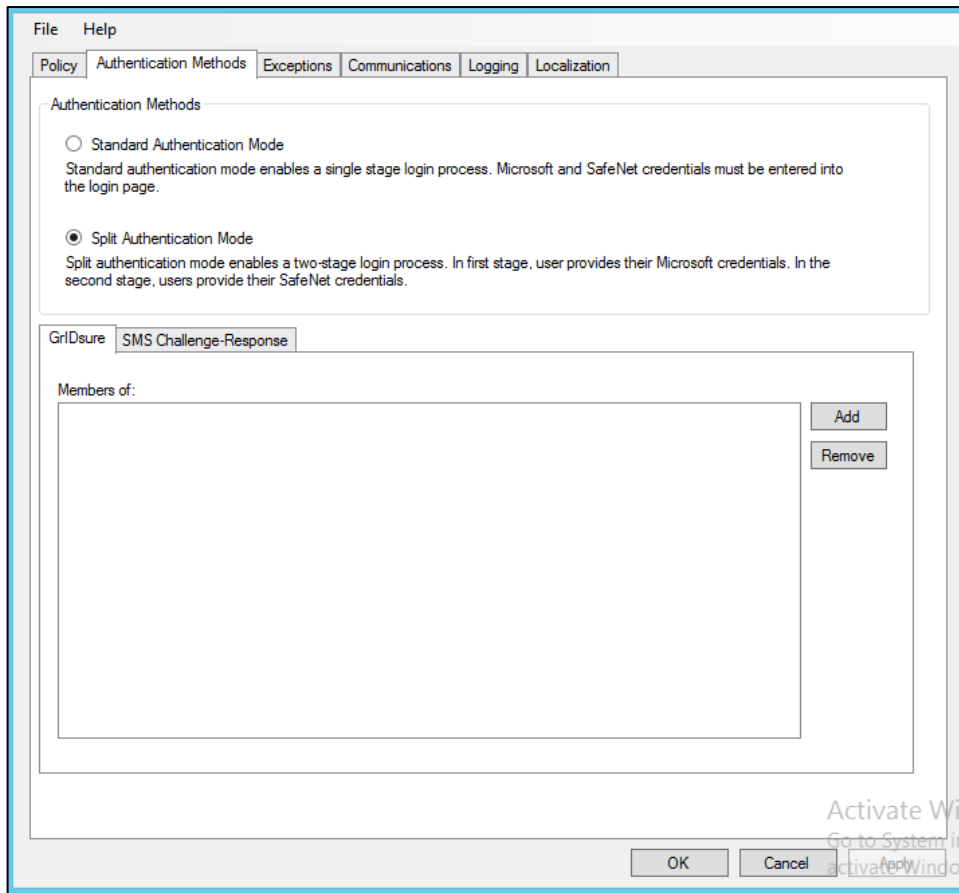
## Domain Stripping

- Strip realm from UPN (`username@domain.com` will be sent as username): Select the checkbox if the SafeNet server username is required without the suffix `@domain`.
- Strip NetBIOS prefix (`domain\username` will be sent as username): Select the checkbox if the SafeNet server username is required without the prefix `\domain`.

Note: The realm-stripping feature applies to SafeNet server usernames only. Active Directory usernames are not affected.

## 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 SafeNet 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. **DomainUsername**, **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 SafeNet 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 SafeNet server 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 SafeNet server 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 SafeNet authentication. By default, all users are required to perform SafeNet authentication unless otherwise defined by exclusion.

### IP Range Exceptions / Inclusions Group

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

## Group Authentication Exceptions Group



**NOTE:** While adding Security Groups, the groups having the **Domain Local** scope will not be visible in the OWA Manager. Only the universal and global domain groups will be visible.

- **Group Filter** and **Selected Groups:** Group authentication exceptions omit single or multiple domain groups from performing SafeNet 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 SafeNet authentication.
- **Only selected groups will bypass SafeNet:** All users are required to perform SafeNet authentication, except the defined Microsoft Group(s).
- **Only selected groups must use SafeNet:** All users are not required to perform SafeNet authentication, except the defined Microsoft Group(s). Adding a group authentication exception

entry will display the following window:

The following provides 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.
- **Select if users and groups exist in the same domain:** The checkbox ensures that the child domain is also effectively searched for users and groups. If selected, the group exclusions functionality will search and apply authentication exceptions even if both users and groups exist in the child domain. If the checkbox is cleared, exceptions will only be applied if both users and groups exist in the parent domain. Default value: Clear

## Communications Tab

This tab deals primarily with the SafeNet server connection options.

The screenshot shows the 'Communications' tab in the SafeNet Agent configuration window. The 'Authentication Server Settings' group includes:

- Primary Server (IP:Port):** 10.164.47.151. There is a checkbox for 'Use SSL (requires a valid certificate)' which is currently unchecked.
- Failover Server (optional):** An empty text box. There is a checkbox for 'Use SSL (requires a valid certificate)' which is currently unchecked.
- Disable SSL server certificate check:** An unchecked checkbox.
- Select minimum SSL/TLS version:** A dropdown menu set to 'TLS 1.0'.
- Attempt to return to primary Authentication Server every:** A spinner box set to '10' with the unit 'minute(s)'.
- Agent Encryption Key File:** A text box containing 'c:\program files\Gemalto\exchange\bsidKey\Agent.bsidkey' and a 'Browse...' button.

The 'Authentication Test' section has input fields for 'User Name:' and 'Passcode:', a 'Test' button, and a 'Result:' area.

The 'Server Status Check' section has a 'Test that the Authentication Server is online' label and a 'Test' button.

At the bottom of the window are 'OK', 'Cancel', and 'Apply' buttons. A watermark 'Activate Windows' is visible in the bottom right corner.

## Authentication Server Settings Group

- Primary Server (IP:Port):** It is used to configure the IP address/hostname of the primary SafeNet 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 SafeNet 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 SafeNet server, within a well-controlled network where self-signed certificates are used and cannot be properly validated by the SafeNet 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 SafeNet server. 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 SafeNet server.
  - **Agent Encryption Key File:** It is used to specify the location of the SafeNet Agent Key File.
- 



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

---

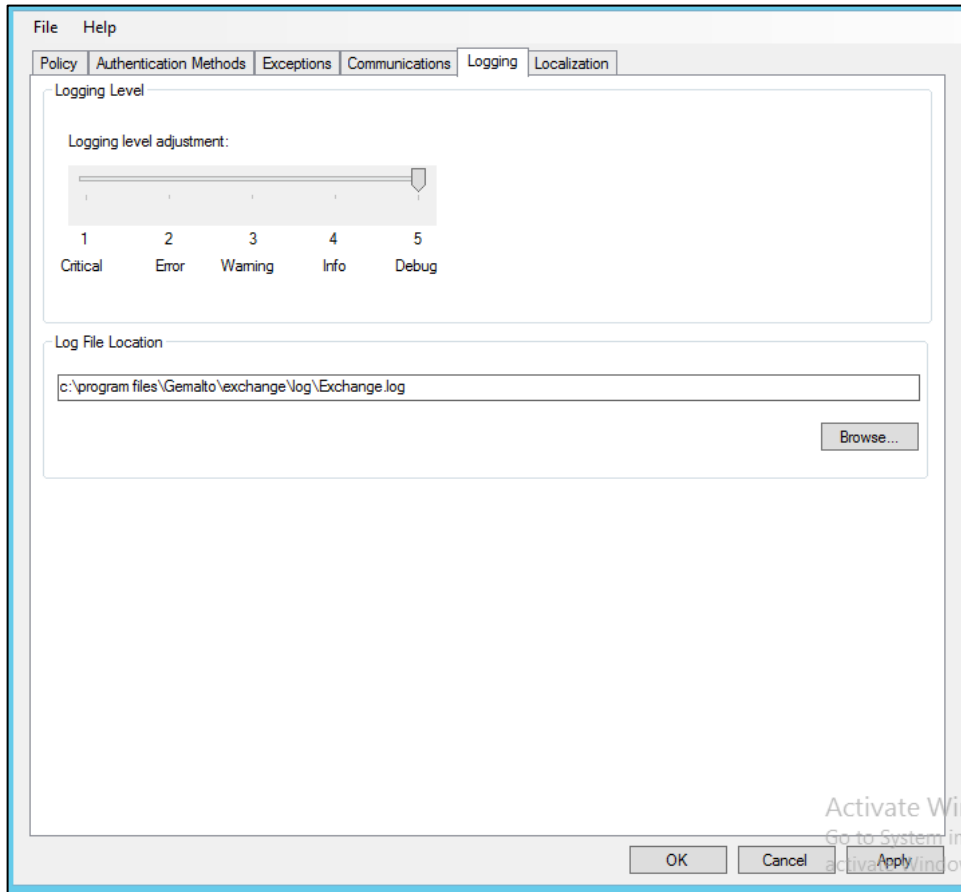
## Authentication Test Group

It allow administrators to test authentication between the agent and the SafeNet server.

## Server Status Check Group

It performs a test to verify a connection to the SafeNet server.

## Logging Tab



### Logging Level Group

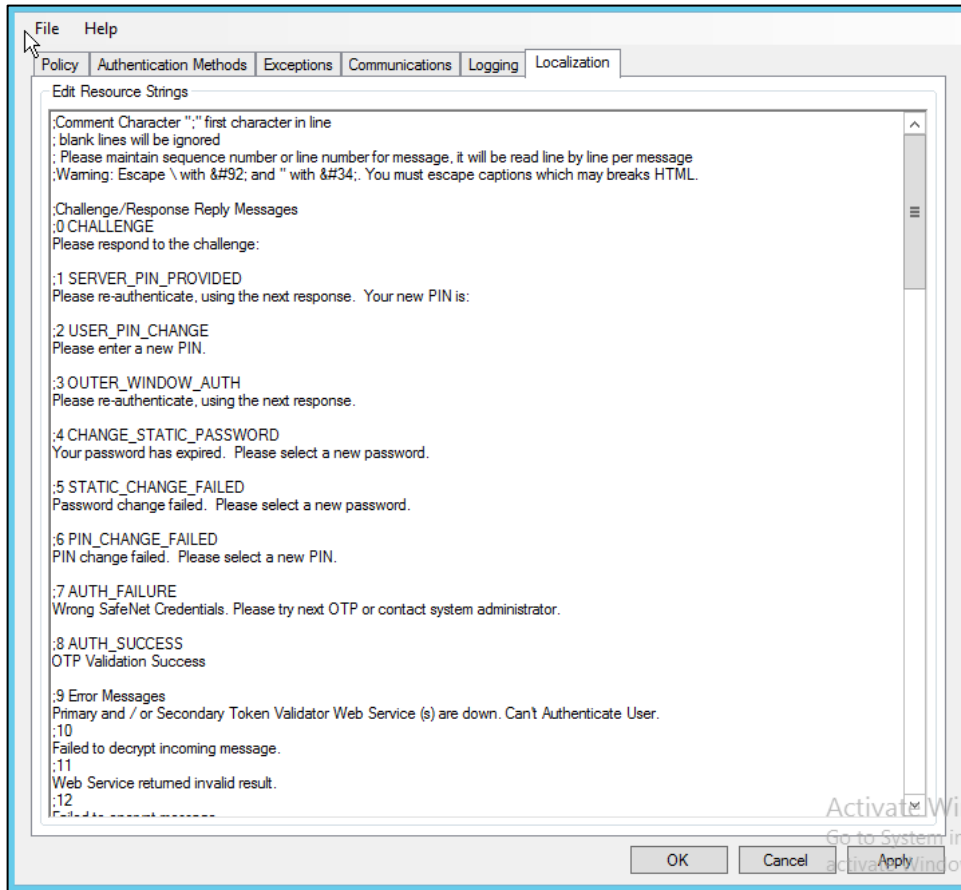
It allow administrators to adjust the logging level. For log levels, **1**, **2** and **3**, only the initial connection between the agent and the server, and any failed connection attempts, are logged. Log level **5** sets the agent in debug mode.

Default value: 5

### Log File Location Group

It allow 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\Gemalto\Exchange\Log`.

## Localization Tab



The settings on this tab represent the prompts and information messages provided by the SafeNet OWA Agent. These can be modified as necessary to improve usability. The **Messages.txt** file can be manually modified outside of the SafeNet Microsoft Exchange Manager. This file can be found at the following location:  
 Program Files\Gemalto\Exchange\LocalizedMessages

## 4

# SafeNet Agent for Outlook Web App 2016/2019

## Authentication Modes

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

The modes of operation are:

Mode	Description
<b>Standard Authentication Mode</b>	Standard Authentication Mode enables a single stage login process. Microsoft domain and SafeNet credentials must be entered in the OWA login page.
<b>Split Authentication Mode</b>	Split Authentication Mode enables a two-stage login process. In the first stage, users provide their Microsoft credentials. In the second stage, users provide their SafeNet credentials. This mode 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.

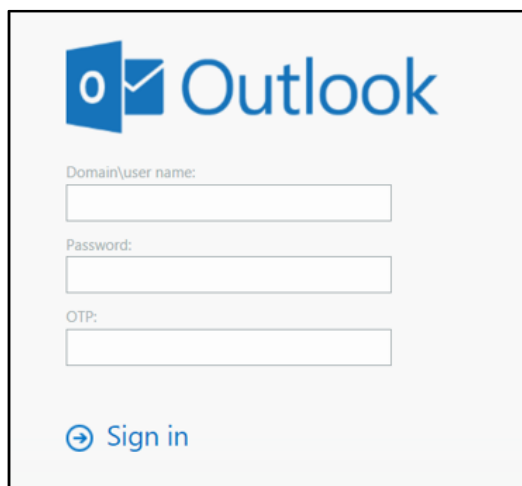
## Setting Authentication Mode

Authentication mode is set in the SafeNet Agent for Outlook Web App, Authentication Tab.

See **Authentication Methods Tab**.

## Standard Authentication Mode - Hardware/Software

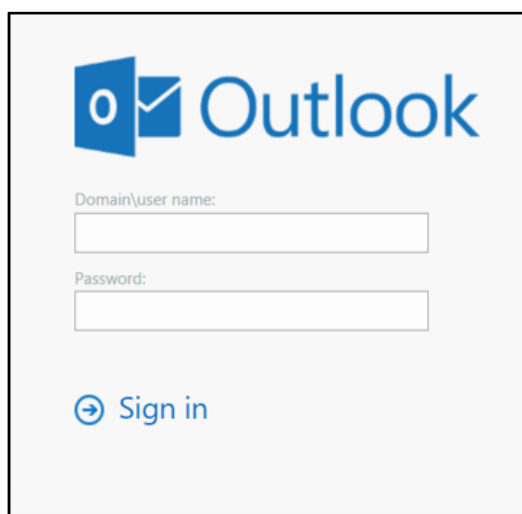
1. Open OWA in your browser.
2. Enter **Domain/User Name**, **Password** and **OTP**, and click **Sign in**.



The screenshot shows the Outlook login interface for Standard Authentication Mode - Hardware/Software. At the top left is the Outlook logo. Below it are three input fields: "Domain\user name:", "Password:", and "OTP:". At the bottom left is a blue "Sign in" button with a right-pointing arrow icon.

## Split Authentication Mode

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

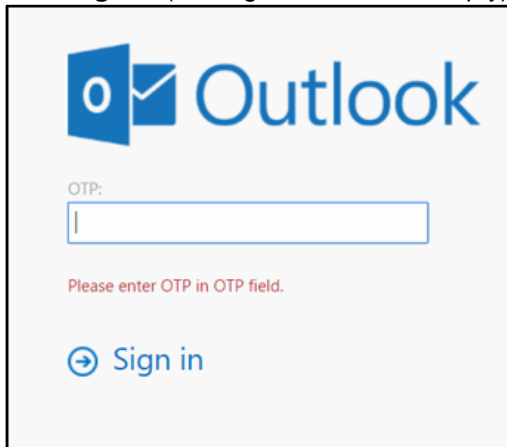


The screenshot shows the Outlook login interface for Split Authentication Mode. At the top left is the Outlook logo. Below it are two input fields: "Domain\user name:" and "Password:". At the bottom left is a blue "Sign in" button with a right-pointing arrow icon.

## GrIDSure

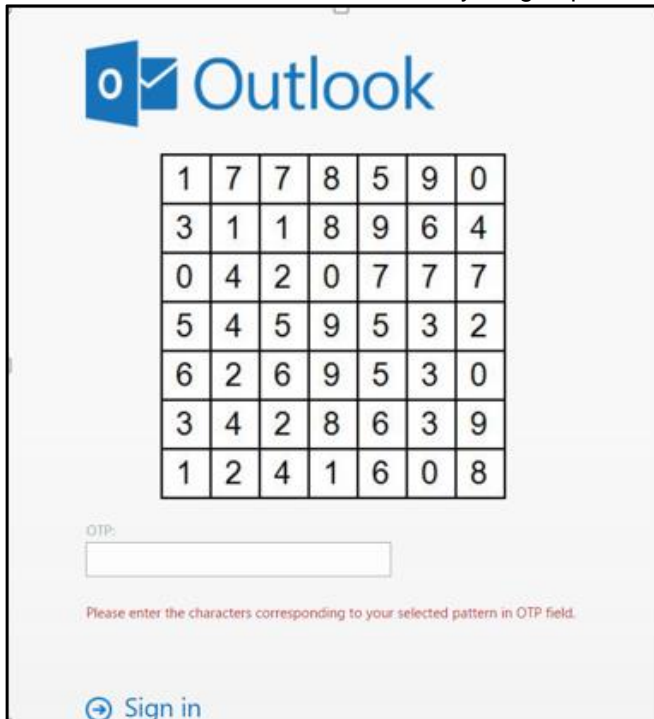
1. If configured for GrIDSure, do the following:

- I. Click **Sign In** (leaving the OTP field empty).



The screenshot shows the Outlook sign-in interface. At the top left is the Outlook logo. Below it is the text "OTP:" followed by an empty text input field. Underneath the input field is a red error message: "Please enter OTP in OTP field." At the bottom left is a blue "Sign in" button with a right-pointing arrow icon.

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



The screenshot shows the Outlook sign-in interface with a grid pattern. The grid is a 7x7 table of numbers:

1	7	7	8	5	9	0
3	1	1	8	9	6	4
0	4	2	0	7	7	7
5	4	5	9	5	3	2
6	2	6	9	5	3	0
3	4	2	8	6	3	9
1	2	4	1	6	0	8

Below the grid is the text "OTP:" followed by a text input field containing the characters "1778590". Underneath the input field is a red error message: "Please enter the characters corresponding to your selected pattern in OTP field." At the bottom left is a blue "Sign in" button with a right-pointing arrow icon.

## SMS Challenge

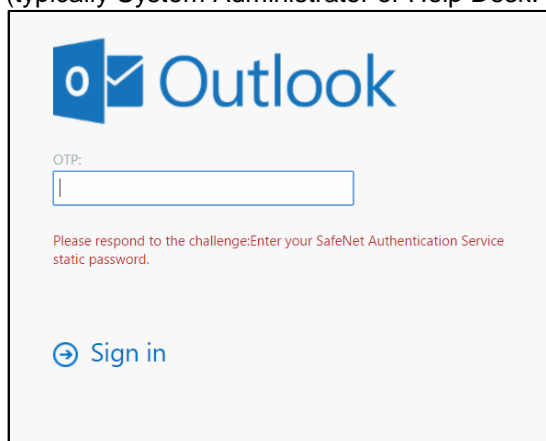
1. If your system is configured to send OTP via SMS, enter the Token Code received on your phone and click **Sign in**.



The screenshot shows the Outlook sign-in interface. At the top left is the Outlook logo. Below it is a text input field labeled "OTP:". Below the input field is a red instruction: "Please enter the OTP you received on your cell phone." At the bottom left is a blue "Sign in" button with a right-pointing arrow icon.

## Challenge-Response

1. 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.
2. Send the challenge code, as displayed on the screen, to the designated recipient in your organization (typically System Administrator or Help Desk).



The screenshot shows the Outlook sign-in interface. At the top left is the Outlook logo. Below it is a text input field labeled "OTP:". Below the input field is a red instruction: "Please respond to the challenge: Enter your SafeNet Authentication Service static password." At the bottom left is a blue "Sign in" button with a right-pointing arrow icon.

In return, you will receive a response code.

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

## Prerequisites

- Ensure that TCP port 80 or 443 is open on the Exchange Server, which would act as a gateway of communication between the SafeNet OWA Agent and the SafeNet solution.
- Administrative rights to the Windows system are required during installation of the SafeNet 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 SafeNet server.

## Installing SafeNet Agent for OWA 2016/2019

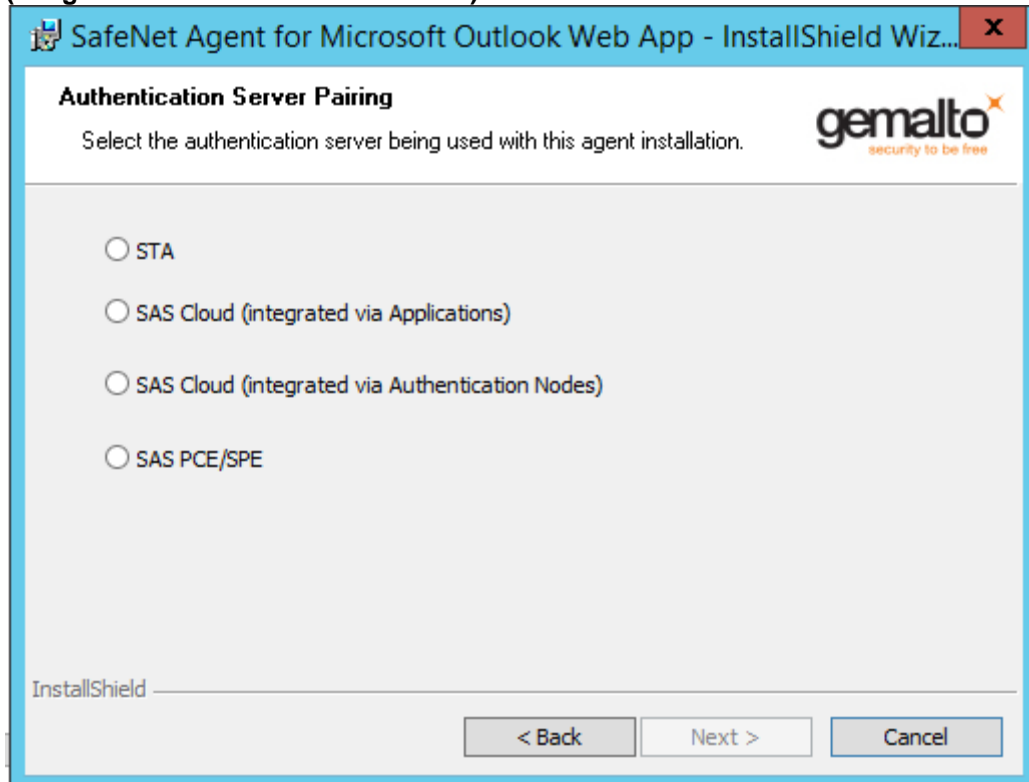


**NOTE:** Always work in **Run as administrator** mode when installing, uninstalling, enabling, or disabling the SafeNet OWA Agent.

Always disable the agent first, and then uninstall, if required.

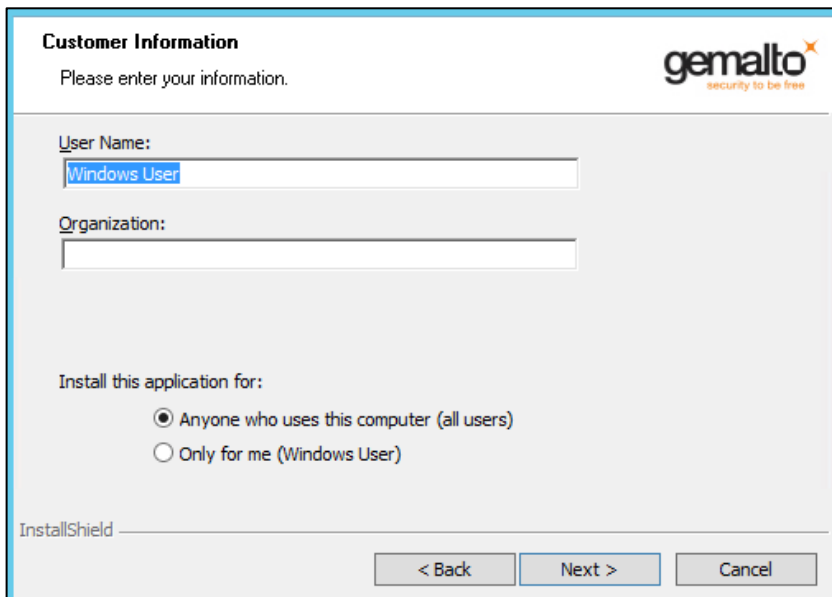
To install SafeNet OWA Agent, follow the steps:

1. Log on to the Microsoft Exchange server.
2. Locate and execute the following installation file:  
SafeNet Agent for Microsoft Outlook Web App 2013-2016.exe
3. On the **Welcome to the InstallShield Wizard...** window, click **Next**.
4. On the **License Agreement** window, select **I accept the terms in the license agreement**, and click **Next**.
5. On the **Authentication Server Pairing** window, select the Authentication Server type, **SAS Cloud (integrated via Authentication Nodes)** or **SAS PCE/SPE** 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)**
- **Only for me (Windows User)**

7. On the **Authentication Service Setup** window, enter the following details:
- In the **Location** field, enter the hostname or IP address of the primary SafeNet server.
  - Select **Connect using SSL** if SafeNet server 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 SafeNet server.

8. 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**.

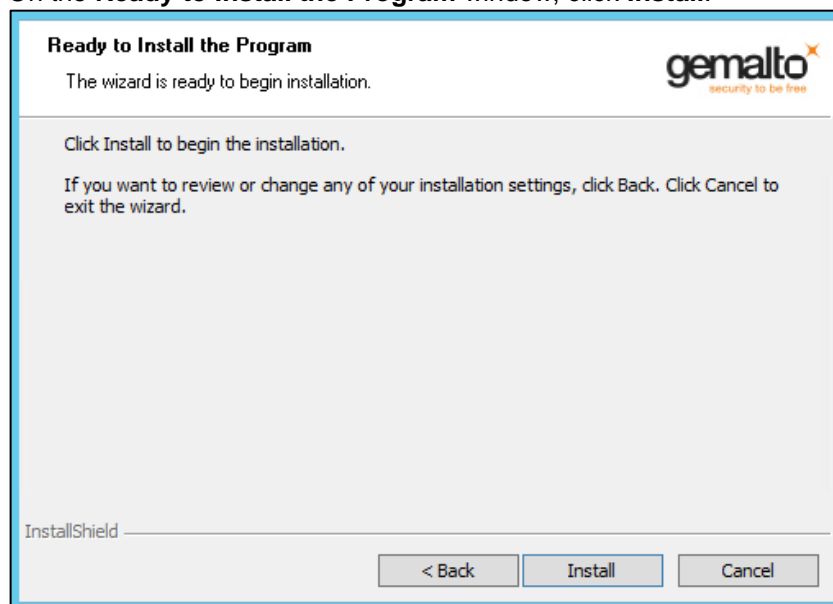
To proceed, the InstallShield Wizard searches for the applicable Exchange Server version in the background. If the Exchange Server is not found, it prompts for the following additional selection:

- I. On the **Exchange Server Selection** window, select the required Exchange Server version.



**NOTE:** Select *Microsoft Exchange Server 2016* for both Microsoft Exchange Server 2016 and Microsoft Exchange Server 2019.

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



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

## Upgrading SafeNet Agent for OWA 2016

Automatic upgrade to **2.1.3** version is not supported. For upgrade, the configurations from the older version must be saved, and then imported into the new installation. For migrating from one version to another, see [Migrating SafeNet Agent for OWA 2016 Using Previous Configurations](#) section below.

## Migrating SafeNet Agent for OWA 2016 Using Previous Configurations

The migration procedure requires export of the configurations from the previously installed version(s) followed by import of the configurations in the newly installed SafeNet OWA Agent 2.1.3.

---

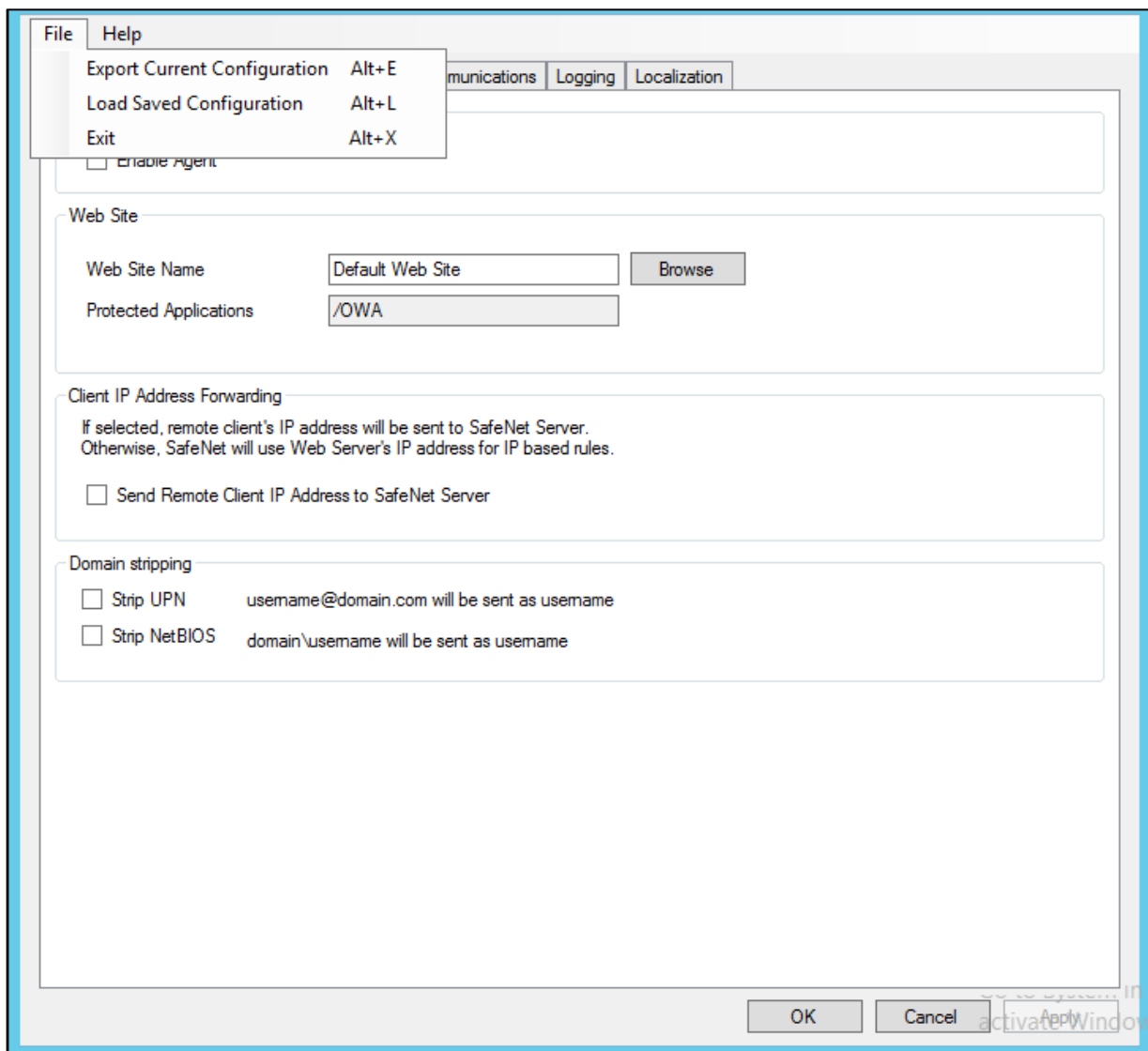


### NOTES:

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

The SafeNet Agent for OWA 2.1.3 version supports import of configurations from SafeNet Agent for OWA **1.09** and later versions. To install the SafeNet Agent for OWA 2.1.3 version using configurations from a previous version, perform the following steps:

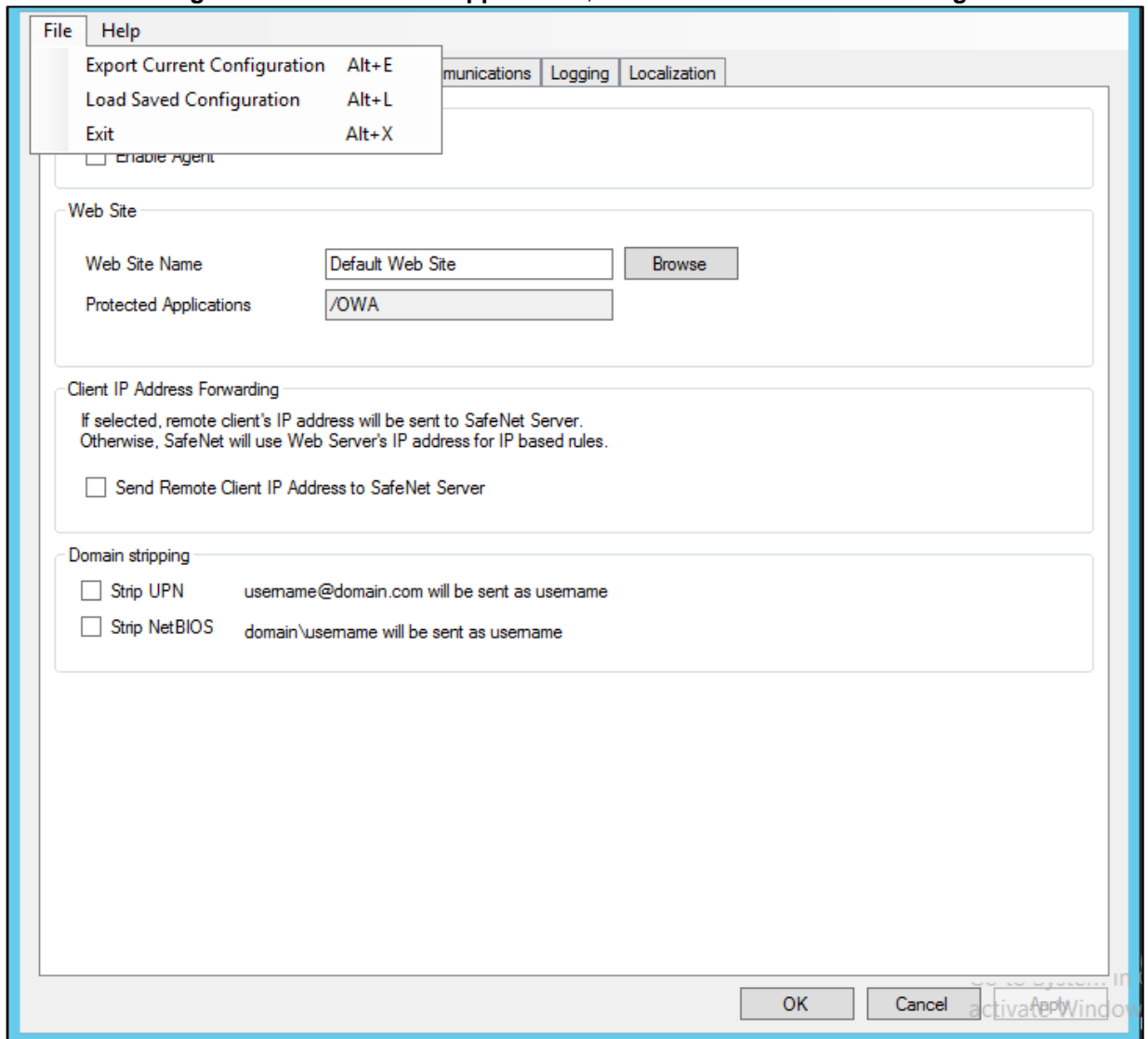
1. In the previously installed SafeNet OWA Agent, export the configurations as follows:
  - I. In the **SafeNet Agent for Outlook Web App** window, select **File > Export Current Configuration**.



- II. In the **Save As** dialog, click **Save** to save the configuration files.
2. Uninstall the previously installed SafeNet OWA Agent.
3. Manually delete the **Exchange** folder (located at **Program Files > SafeNet**).
4. To install the new SafeNet Agent for OWA, run the installation file, as an administrator: **SafeNet Agent for Microsoft Outlook Web App 2013-2016.exe**

5. In the newly installed SafeNet Agent, load the saved settings as follows:

- I. In the **SafeNet Agent for Outlook Web App** window, select **File > Load Saved Configuration**.



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

6. Click **OK**.



**NOTES:** After migrating to **SafeNet Agent for OWA 2.1.3** version, the **Split Authentication Mode** is selected, by default. If you require to change the settings, go to **SafeNet Agent for Outlook Web App > Authentication Methods** and select **Standard Authentication Mode**.

## SafeNet Agent for Outlook Web App

The SafeNet Agent for Outlook Web App allows modification of various features available within the SafeNet 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 SafeNet 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 SafeNet solution. Otherwise, the web server's IP Address will be used.

Default value: Enabled

## Domain Stripping

- Strip realm from UPN (`username@domain.com` will be sent as username): Select the checkbox if the SafeNet server username is required without the suffix `@domain`.
- Strip NetBIOS prefix (`domain\username` will be sent as username): Select the checkbox if the SafeNet server username is required without the prefix `\domain`.



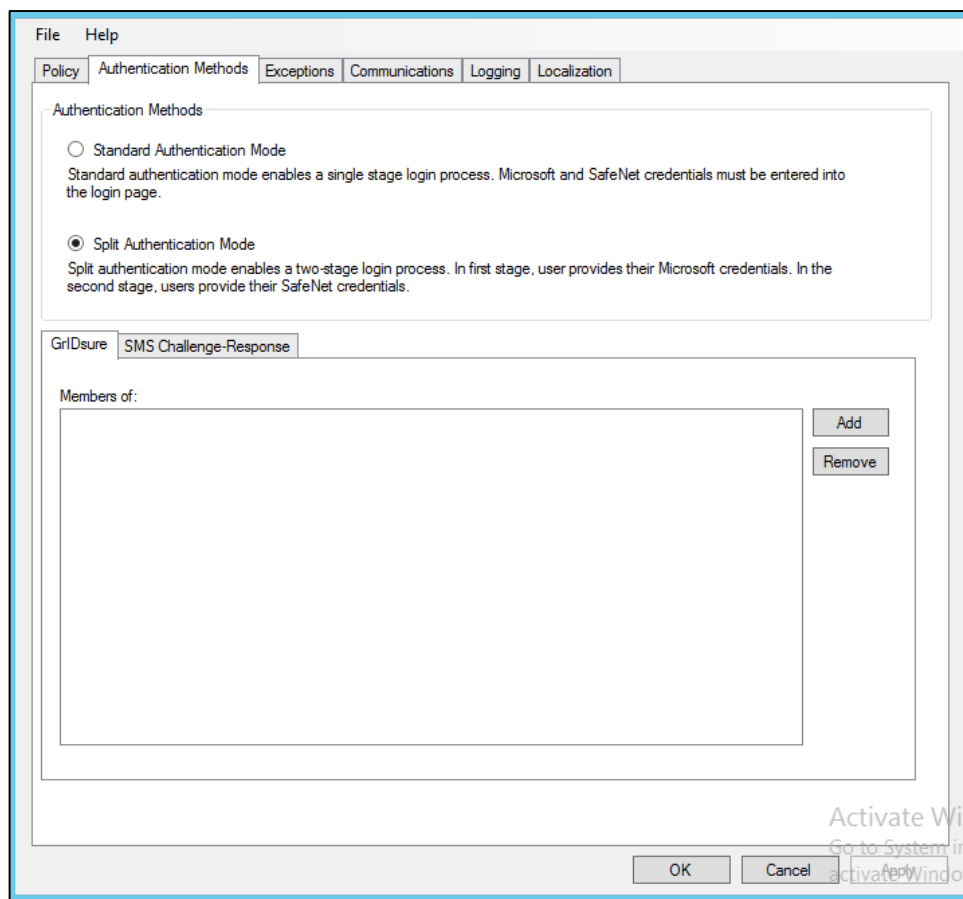
**NOTE:** The realm-stripping feature applies to SafeNet server usernames only.  
Active Directory usernames are not affected.

---



## 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 SafeNet 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 SafeNet 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 SafeNet server 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 SafeNet server 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 SafeNet authentication. By default, all users are required to perform SafeNet authentication unless otherwise defined by exclusion.

### IP Range Exceptions / Inclusions Group

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

## Group Authentication Exceptions Group



**NOTE:** While adding Security Groups, the groups having the **Domain Local** scope will not be visible in the OWA Manager. Only the universal and global domain groups will be visible.

- **Group Filter** and **Selected Groups:** Group authentication exceptions omit single or multiple domain groups from performing SafeNet 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 SafeNet authentication.
- **Only selected groups will bypass SafeNet:** All users are required to perform SafeNet authentication, except the defined Microsoft Group(s).
- **Only selected groups must use SafeNet:** All users are not required to perform SafeNet authentication, except the defined Microsoft Group(s). Adding a group authentication exception entry will display the following window:

The screenshot shows a dialog box titled "Select Domain Groups". It contains the following elements:

- A dropdown menu labeled "From this location:" with "adlocal.com" selected.
- A text input field labeled "Enter the group names to select (examples):" with a "Check Names" button to its right.
- A checkbox labeled "Highlight already selected groups in search result".
- Below the input field, there are "Select All" and "UnSelect All" buttons.
- At the bottom of the dialog are "OK" and "Cancel" buttons.

The following provides 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.
- **Select if users and groups exist in the same domain:** The checkbox ensures that the child domain is also effectively searched for users and groups. If selected, the group exclusions functionality will search and apply authentication exceptions even if both users and groups exist in the child domain. If the checkbox is cleared, exceptions will only be applied if both users and groups exist in the parent domain. Default value: Clear

## Communications Tab

This tab deals primarily with the SafeNet server connection options.

The screenshot shows the 'Communications' tab in the SafeNet Agent configuration window. The 'Authentication Server Settings' group contains the following options:

- Primary Server (IP:Port):** A text box containing '10.164.47.151'. To its right is a checkbox labeled 'Use SSL (requires a valid certificate)'.
- Failover Server (optional):** An empty text box. To its right is a checkbox labeled 'Use SSL (requires a valid certificate)'.
- Disable SSL server certificate check:** An unchecked checkbox.
- Select minimum SSL/TLS version:** A dropdown menu set to 'TLS 1.0'.
- Attempt to return to primary Authentication Server every:** A spinner box set to '10' with the label 'minute(s)'.
- Agent Encryption Key File:** A text box containing 'c:\program files\Gemalto\exchange\bsidKey\Agent.bsidgey' and a 'Browse...' button.

The 'Authentication Test' section includes:

- Test authentication from the agent to the Authentication Server:** A label with a 'Result:' column to its right.
- User Name:** An empty text box.
- Passcode:** An empty text box.
- Test:** A button.

The 'Server Status Check' section includes:

- Test that the Authentication Server is online:** A label with a 'Test' button.

At the bottom of the window are 'OK', 'Cancel', and 'Apply' buttons. A watermark 'Activate Windows' is visible in the bottom right corner.

## Authentication Server Settings Group

- Primary Server (IP:Port):** It is used to configure the IP address/hostname of the primary SafeNet 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 SafeNet 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 SafeNet server, within a well-controlled network where self-signed certificates are used and cannot be properly validated by the SafeNet 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 SafeNet server. 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 SafeNet server.
  - **Agent Encryption Key File:** It is used to specify the location of the SafeNet Agent Key File.
- 



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

---

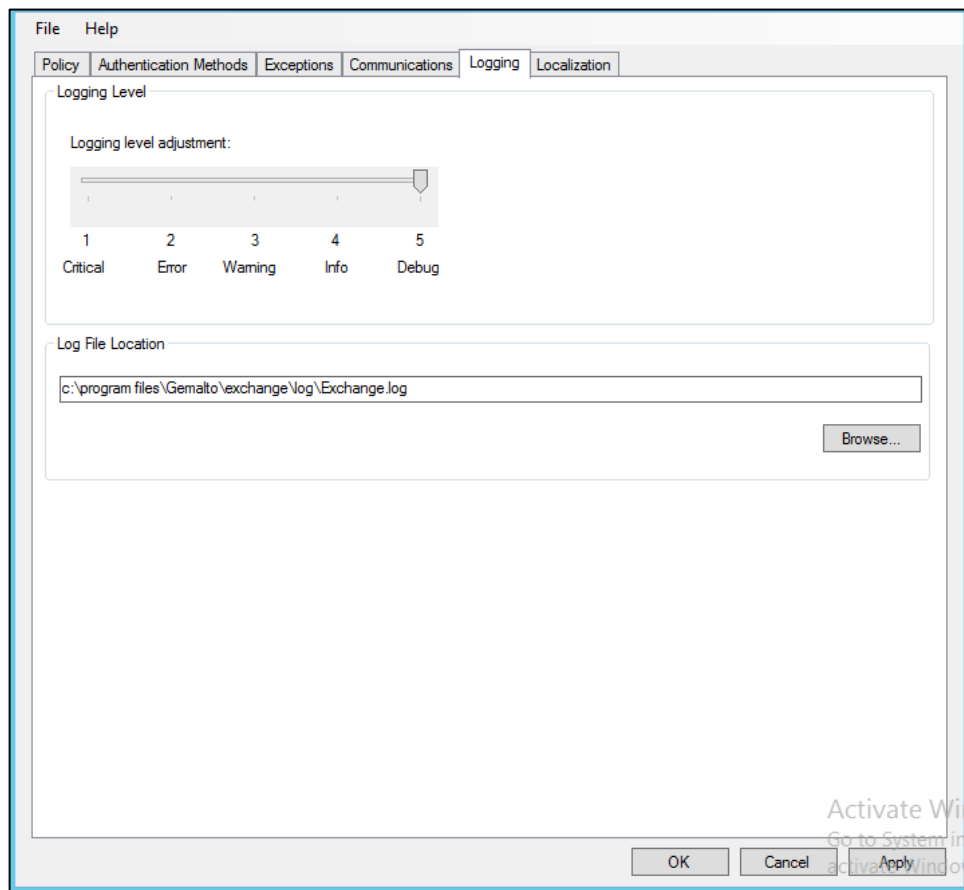
## Authentication Test Group

It allow administrators to test authentication between the agent and the SafeNet server.

## Server Status Check Group

It performs a test to verify a connection to the SafeNet server.

## Logging Tab



### Logging Level Group

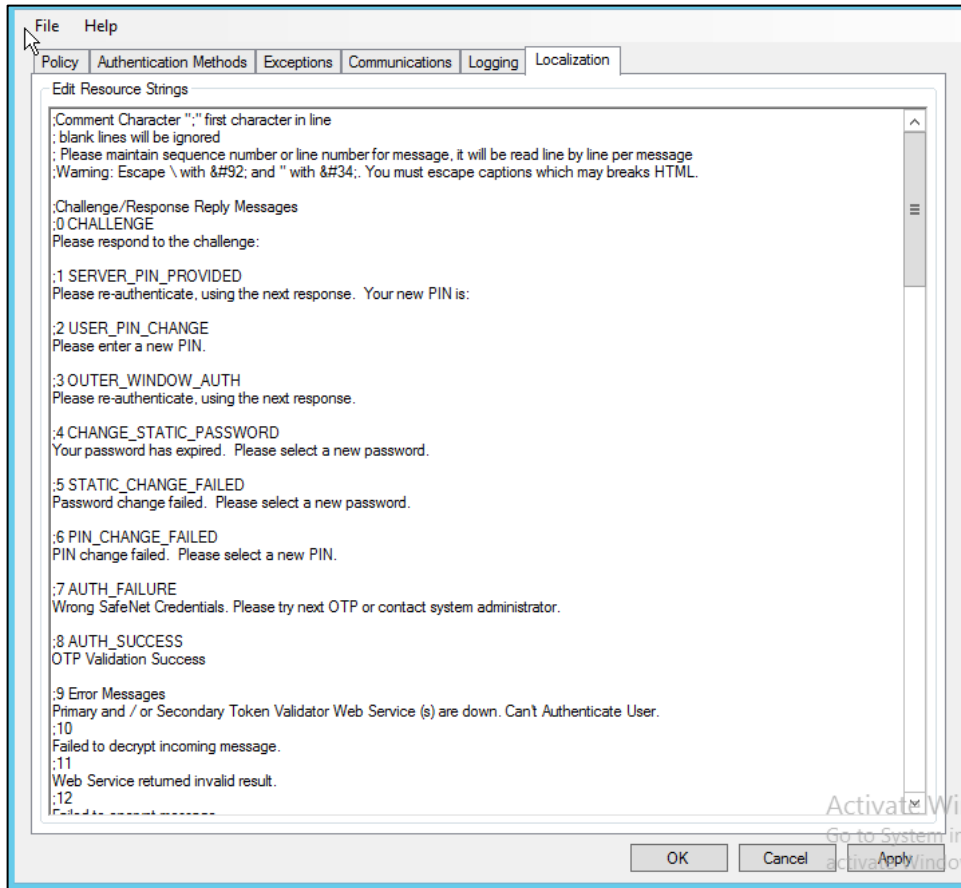
It allow administrators to adjust the logging level. For log levels, **1**, **2** and **3**, only the initial connection between the agent and the server, and any failed connection attempts, are logged. Log level **5** sets the agent in debug mode.

Default value: 5

### Log File Location Group

It allow 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\Gemalto\Exchange\Log`.

## Localization Tab



The settings on this tab represent the prompts and information messages provided by the SafeNet OWA Agent. These can be modified as necessary to improve usability. The **Messages.txt** file can be manually modified outside of the SafeNet Microsoft Exchange Manager. This file can be found at the following location:  
 Program Files\Gemalto\Exchange\LocalizedMessages