

SafeNet Agent for Microsoft Outlook Web App 2.1.5

INSTALLATION AND CONFIGURATION GUIDE



Document Information

Product Version	2.1.5
Document Part Number	007-000005-001, Rev. N
Release Date	July 2023

Trademarks, Copyrights, and Third-Party Software

© 2023 THALES. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and affiliates and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Disclaimer

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

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales and any of its subsidiaries and affiliates (collectively referred to herein after as "Thales") information.

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

> The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.

> This document shall not be posted on any publicly accessible network computer or broadcast in any media and no modification of any part of this document shall be made.

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

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

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

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

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any

application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

CONTENTS

PREFACE	7
Audience	7
Related Documents	7
Support Contacts	7
Customer Support Portal	7
Telephone Support	8
Email Support	8
CHAPTER 1: Overview	9
Applicability	9
System Requirements.....	9
CHAPTER 2: SafeNet Agent for Outlook Web App 2013	11
Authentication Modes.....	11
Setting Authentication Mode.....	11
Standard Authentication Mode - Hardware/Software	12
Split Authentication Mode	12
Prerequisites	14
Installing SafeNet Agent for OWA 2013.....	14
Upgrading SafeNet Agent for OWA 2013	18
Migrating SafeNet Agent for OWA 2013 Using Previous Configurations	18
SafeNet Agent for Outlook Web App	21
Policy Tab	21
Authentication Methods Tab.....	23
Exceptions Tab	24
Communications Tab.....	26
Logging Tab	28
Localization Tab.....	29
CHAPTER 3: SafeNet Agent for Outlook Web App 2016/2019	30
Authentication Modes.....	30
Setting Authentication Mode.....	30
Standard Authentication Mode - Hardware/Software	31
Split Authentication Mode	31
Prerequisites	33
Installing SafeNet Agent for OWA 2016/2019	34
Upgrading SafeNet Agent for OWA 2016/2019	37
Migrating SafeNet Agent for OWA 2016/2019 Using Previous Configurations	37
SafeNet Agent for Outlook Web App	40
Policy Tab	40
Authentication Methods Tab	42
Exceptions Tab	43
Communications Tab.....	45
Logging Tab.....	47

Localization Tab 48

PREFACE

This document describes how to install and configure the **SafeNet Agent for Microsoft Outlook Web App (OWA)**.

Audience

This document is intended for 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 Thales Group are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

Related Documents

The following documents contain related or additional information:

- > *SafeNet Agent for Microsoft Outlook Web App 2.1.5: Customer Release Notes*

Support Contacts

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

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

Customer Support Portal

The Customer Support Portal, at <https://supportportal.thalesgroup.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 Thales Group 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.DIS@thalesgroup.com.

CHAPTER 1: Overview

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. It 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 agent 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 2 FA 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 SafeNet server in their data center(s).
- > **SafeNet Authentication Service - Private Cloud Edition (SAS PCE)** — The on-premises, server version targeted at organizations interested in hosting SafeNet server in their private cloud environment.
- > **SafeNet Trusted Access (earlier, SAS Cloud)** — The SafeNet's cloud-based authentication service.

System Requirements

Network Port	<ul style="list-style-type: none"> > TCP 443 > TCP 80
Architecture	<ul style="list-style-type: none"> > 64-bit
Web Servers	<ul style="list-style-type: none"> > IIS 7.0 > IIS 7.5

	<ul style="list-style-type: none"> > IIS 8.0 > IIS 10
Exchange Servers	<ul style="list-style-type: none"> > Microsoft Exchange Server 2013 > Microsoft Exchange Server 2016 > Microsoft Exchange Server 2019
Operating Systems	<ul style="list-style-type: none"> > Windows Server 2012 > Windows Server 2012 R2 > Windows Server 2016 > Windows Server 2019 > Windows Server 2022
Additional Software	<ul style="list-style-type: none"> > .NET 4.5.2 (for SafeNet Agent for Outlook Web App 2013, 2016, and 2019) <p>NOTE: If .NET Framework 4.5.2 (or above) is installed from the agent package, the Exchange Server will restart automatically.</p>
Web Browsers	<ul style="list-style-type: none"> > Internet Explorer (IE) 10 and 11 <p>NOTE: 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"> > Mozilla Firefox > Google Chrome
Additional Web Browsers Requirements	<ul style="list-style-type: none"> > Cookies must be enabled > JavaScript must be enabled > ActiveX must be enabled
Authentication Methods	All tokens and authentication methods supported by the SafeNet server except Push OTP.
SafeNet Authentication Service (SAS) releases	<ul style="list-style-type: none"> > SAS PCE/SPE 3.9.1 (and later) > SafeNet Trusted Access (earlier, SAS Cloud)

CHAPTER 2: 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
Standard Authentication Mode	Standard Authentication Mode enables a single stage login process. Microsoft domain and SafeNet credentials must be entered in the OWA login page.
Split Authentication Mode	Split Authentication Mode enables a two-stage login process. In the first stage, users provide their Microsoft credentials. In the second stage, users provide their SafeNet credentials. This mode 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.

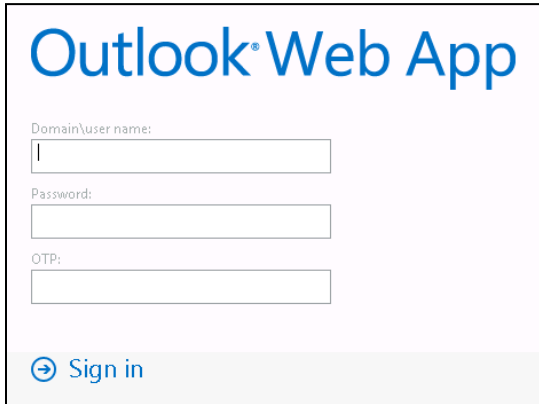
Setting Authentication Mode

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

See **Authentication Methods Tab**.

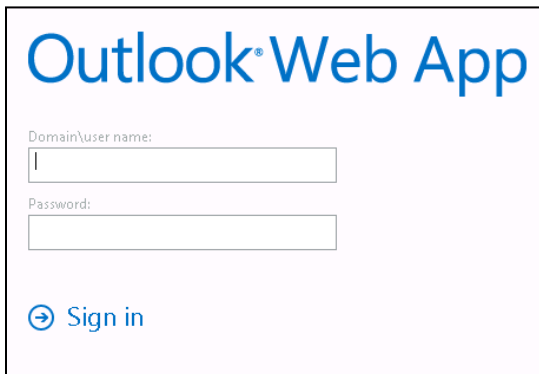
Standard Authentication Mode - Hardware/Software

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



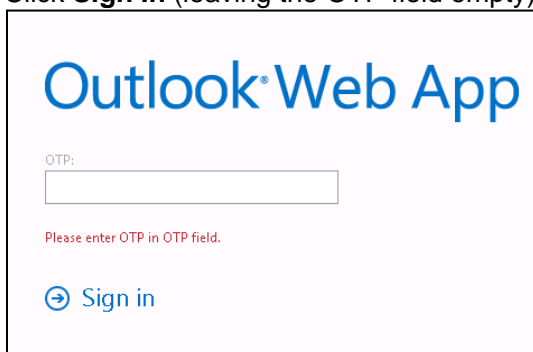
Split Authentication Mode

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

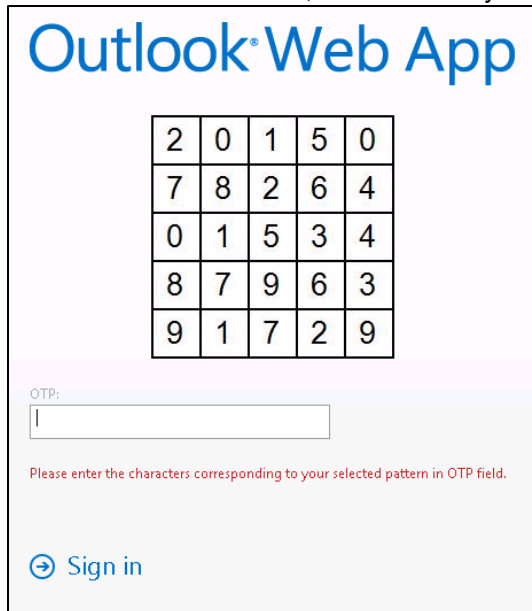


GrIDSure

1. If configured for GrIDSure, do the following:
 - a. Click **Sign In** (leaving the OTP field empty).



- b. 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

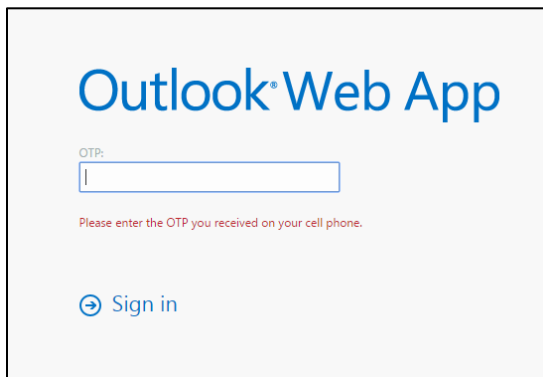
OTP:

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**.



Outlook® Web App

OTP:

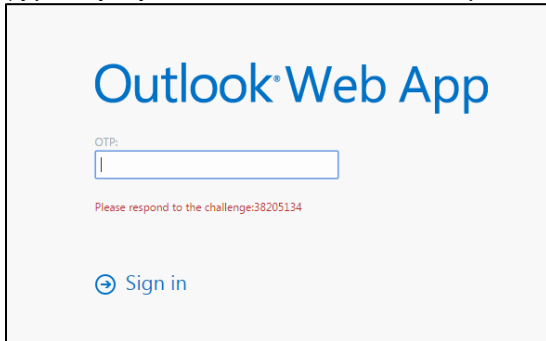
Please enter the OTP you received on your cell phone.

[→ Sign in](#)

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).



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 will 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.

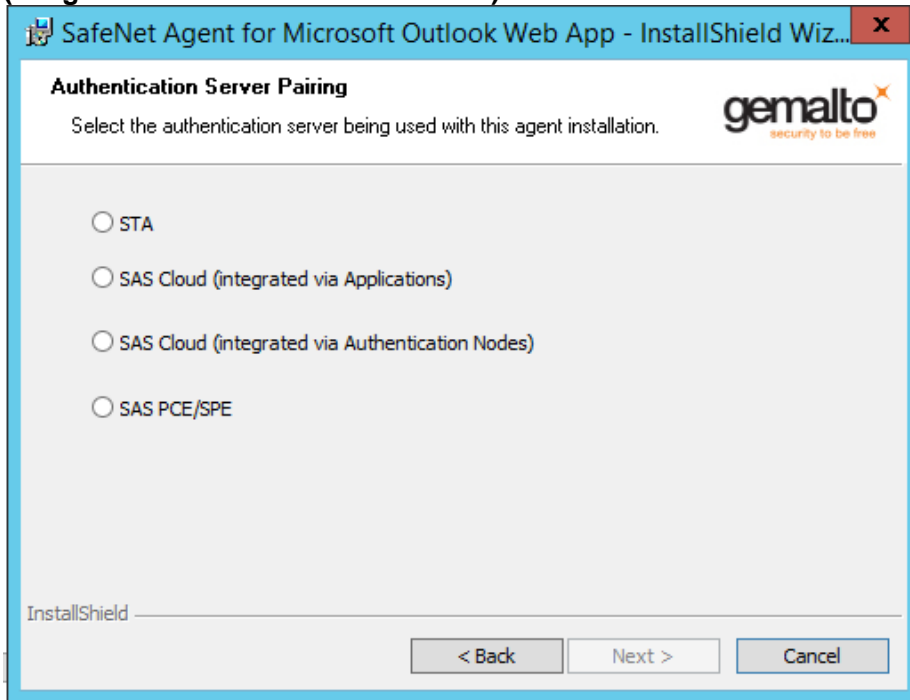
Installing SafeNet Agent for OWA 2013

IMPORTANT: Always work in **Run as administrator** mode when installing, configuring, upgrading, and uninstalling the agent.
Always disable the agent first, and then uninstall, if required.

To install **SafeNet** OWA Agent, perform the following steps:

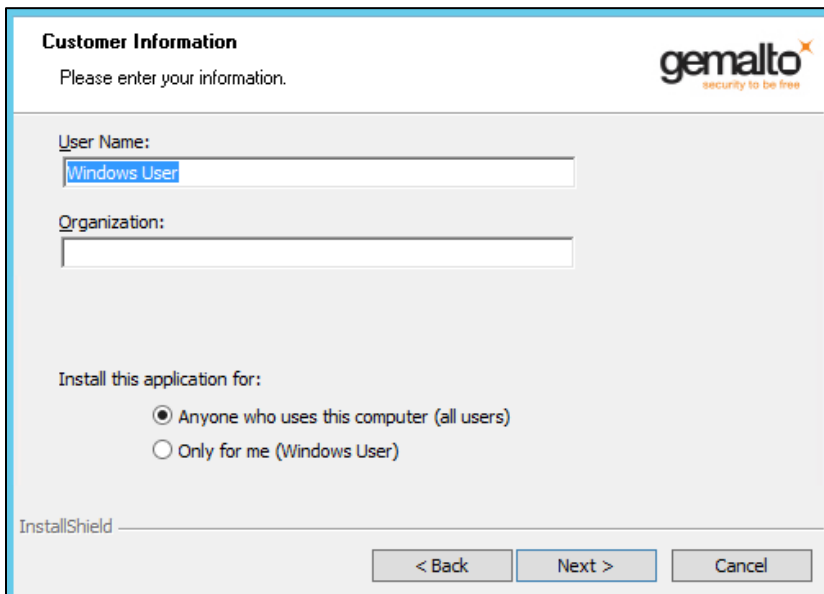
1. Login to the Microsoft Exchange server.
2. Locate and execute the following installation file:
SafeNet Agent for Microsoft Outlook Web App 2013-2016-2019.exe
3. On the **Welcome to the InstallShield Wizard for SafeNet Agent for Microsoft Outlook Web App** window, click **Next**.
4. On the **License Agreement** window, read the software license agreement and to proceed, 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**.



The screenshot shows the 'Authentication Server Pairing' window from the 'SafeNet Agent for Microsoft Outlook Web App - InstallShield Wiz...' wizard. The window title bar includes a close button (X). The main content area has the Gemalto logo (security to be free) in the top right. Below the title, it says 'Select the authentication server being used with this agent installation.' There are four radio button options: STA, SAS Cloud (integrated via Applications), SAS Cloud (integrated via Authentication Nodes), and SAS PCE/SPE. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'InstallShield' logo is visible in the bottom left corner.

6. On the **Customer Information** window, perform the following steps:
- In the **User Name** field, enter your user name.
 - In the **Organization** field, enter the name of your organization.
 - Click **Next**.



The screenshot shows the 'Customer Information' window from the 'SafeNet Agent for Microsoft Outlook Web App - InstallShield Wiz...' wizard. The window title bar includes a close button (X). The main content area has the Gemalto logo (security to be free) in the top right. Below the title, it says 'Please enter your information.' There are two text input fields: 'User Name:' with the text 'Windows User' and 'Organization:'. Below these fields, there is a section titled 'Install this application for:' with two radio button options: 'Anyone who uses this computer (all users)' (selected) and 'Only for me (Windows User)'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'InstallShield' logo is visible in the bottom left corner.

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, and click **Next**.
 - 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.

Authentication Service Setup
Provide connection information for the Authentication Server

Please enter the hostname or IP Address of your SafeNet Authentication Server.

Location:
localhost Connect using SSL (requires valid certificate)

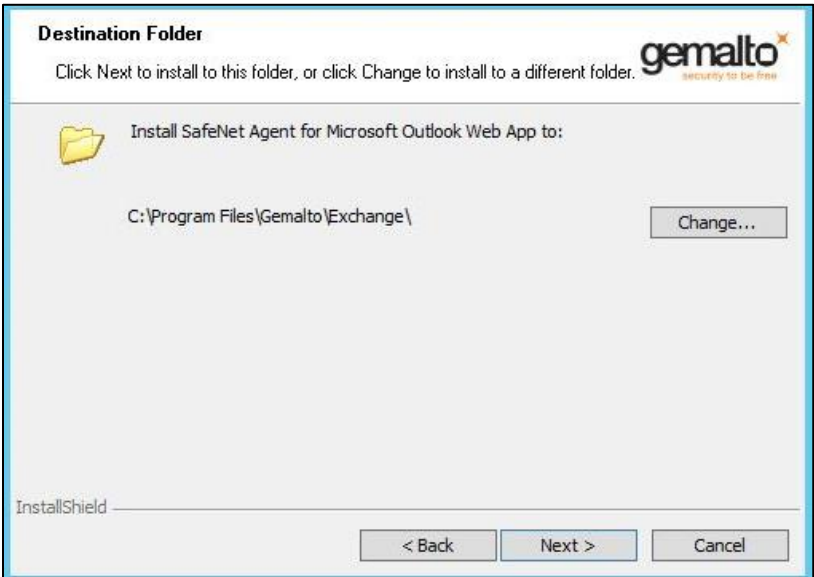
Specify failover SafeNet Authentication Server (optional)

Location:
localhost Connect using SSL (requires valid certificate)

InstallShield

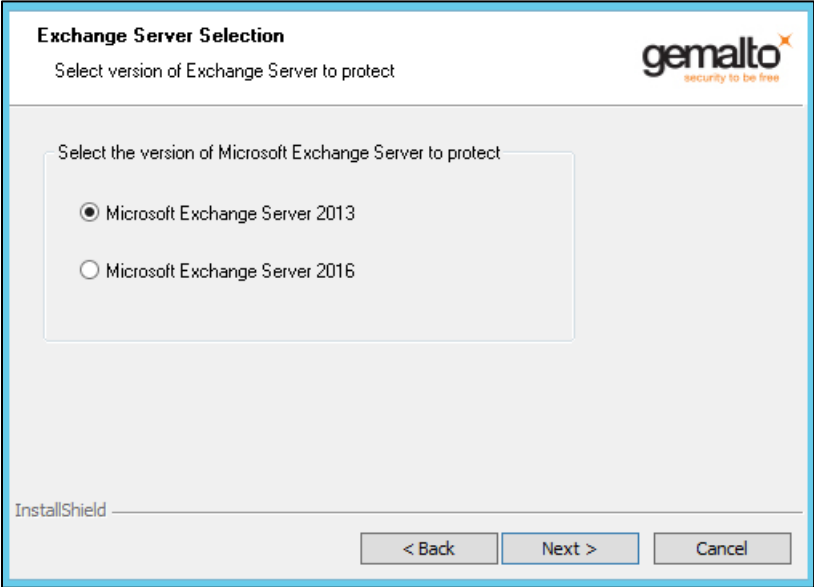
< Back Next > Cancel

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**.

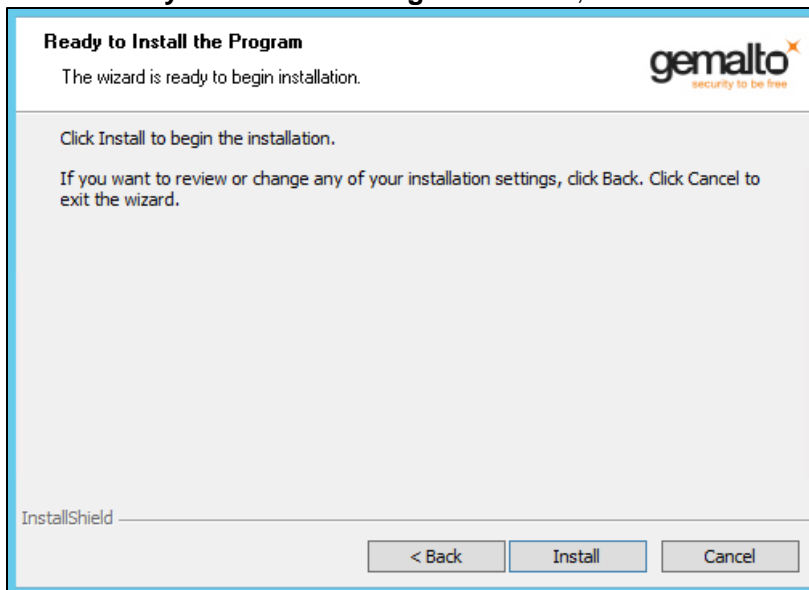


To proceed, the InstallShield Wizard searches for the applicable Exchange Server version in the background. If the Exchange Server is not found, it prompts for the following additional selection:

- a. 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

The SafeNet Agent for OWA 2.1.5 supports upgrade from 2.1.2 (and later). For upgrade, the configurations from the older version must be saved, and then imported into the new installation.

Direct upgrade from versions prior to 2.1.2 to the latest version of the agent is not supported. The earlier versions can be **migrated** to SafeNet Agent for OWA 2.1.5. For migrating from one version to another, see [Migrating SafeNet Agent for OWA 2013 Using Previous Configurations](#) section below.

NOTE: Disable the agent from the management console before proceeding with the upgrade.

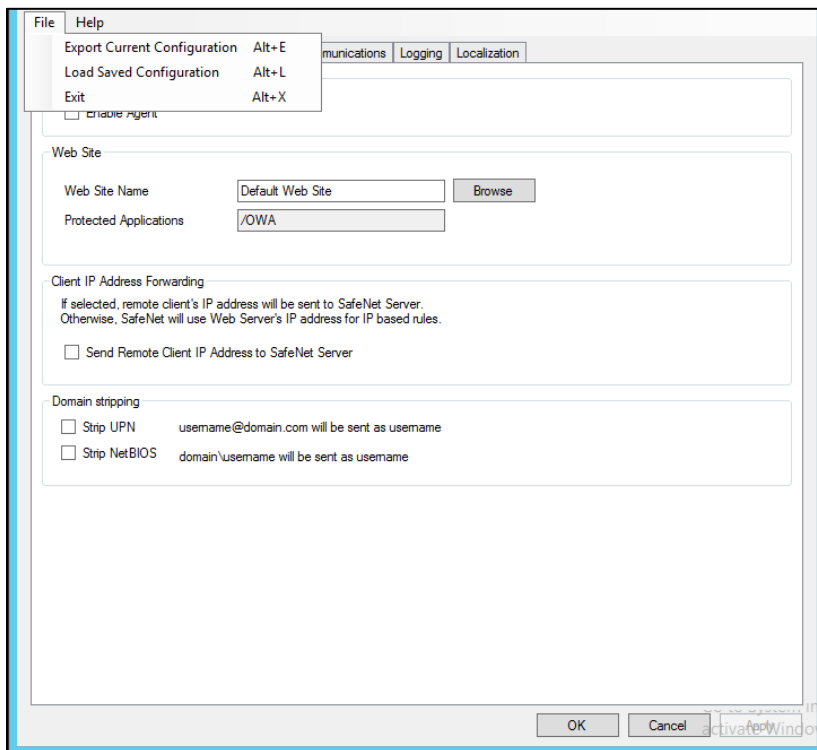
Migrating SafeNet Agent for OWA 2013 Using Previous Configurations

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 2.1.5.

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

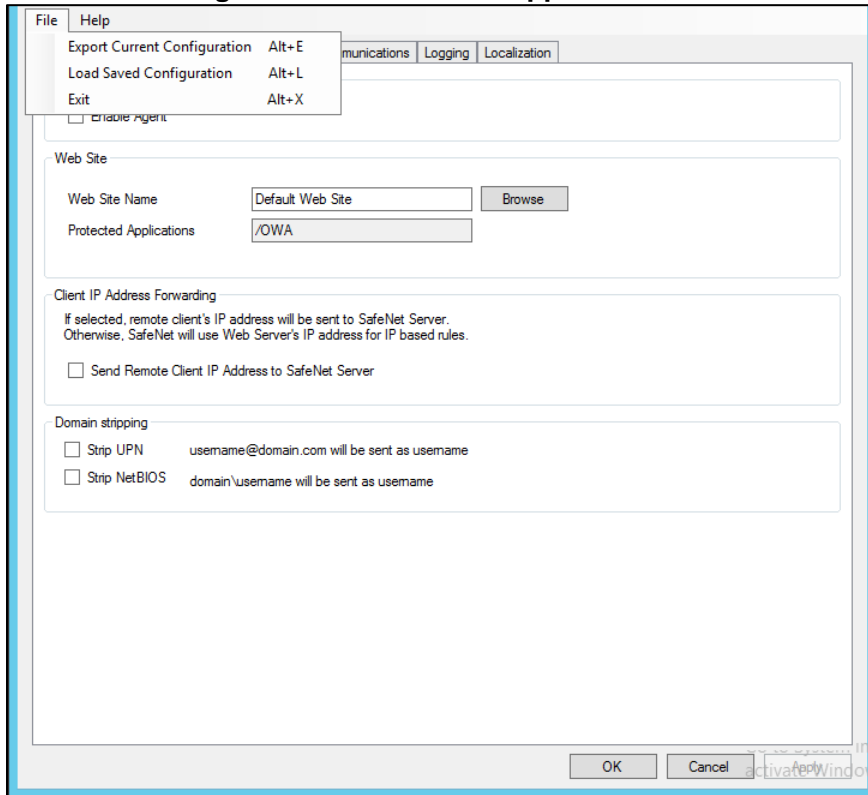
In the existing setup of the agent, perform the following steps:

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



- b.** 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 2013-2016-2019.exe

5. In the newly installed SafeNet Agent, load the saved settings as follows:
 - a. In the **SafeNet Agent for Outlook Web App** window, select **File > Load Saved Configuration**.



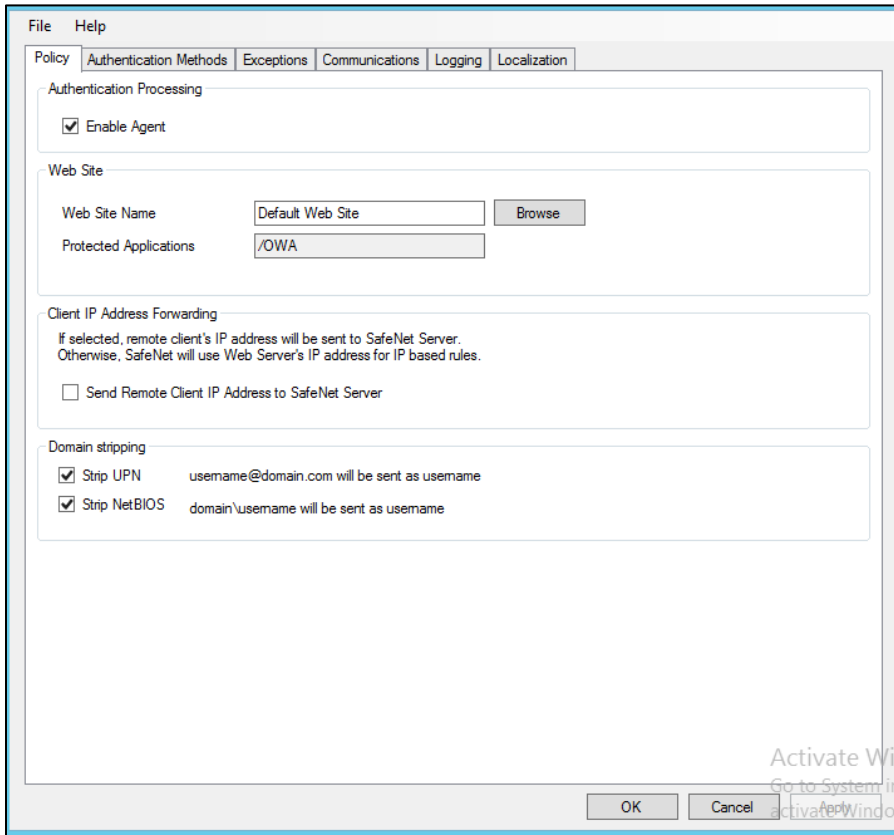
- b. In the **Open** window, select the saved configuration file (**.bsidconfig**) and click **Open**.
6. Click **OK**.

NOTES: After migrating to the latest 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 with enabling the OWA Agent and defining the website settings.

Authentication Processing Group

- > **Enable Agent:** Turns the SafeNet OWA agent **On** or **Off**.
Default: Disabled

Web Site Group

- > **Web Site Name:** Allows selection of the Exchange Server website.
Default: Default Web Site
- > **Protected Applications:** Specifies the OWA directory on the Exchange Server.
Default: /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: Enabled

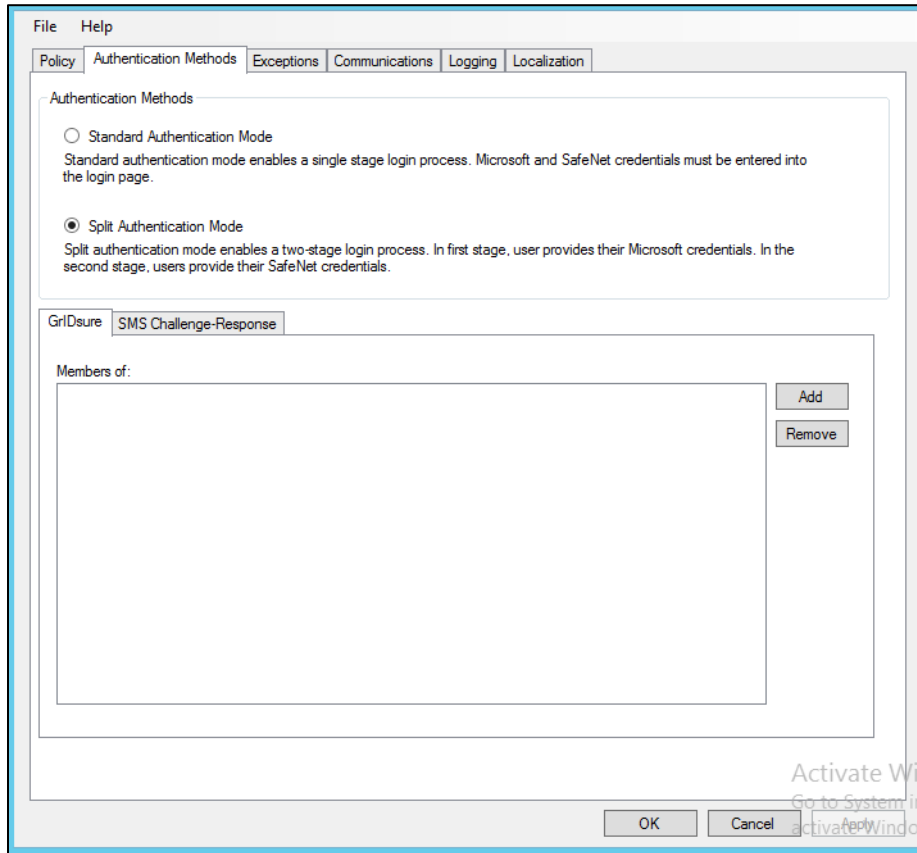
Domain Stripping

- **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: 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: 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: 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 with the various SafeNet server connection options.

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

- Primary Server (IP:Port): 10.164.47.151
- Use SSL (requires a valid certificate):
- Failover Server (optional): [Empty field]
- Use SSL (requires a valid certificate):
- Disable SSL server certificate check:
- Select minimum SSL/TLS version: TLS 1.0
- Attempt to return to primary Authentication Server every: 10 minute(s)
- Agent Encryption Key File: c:\program files\Gemalto\exchange\bsidKey\Agent.bsdkkey

The 'Authentication Test' section includes:

- Test authentication from the agent to the Authentication Server
- User Name: [Empty field]
- Passcode: [Empty field]
- Result: [Empty field]
- Test button

The 'Server Status Check' section includes:

- Test that the Authentication Server is online
- Test button

At the bottom, there are buttons for OK, Cancel, and Apply. 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.

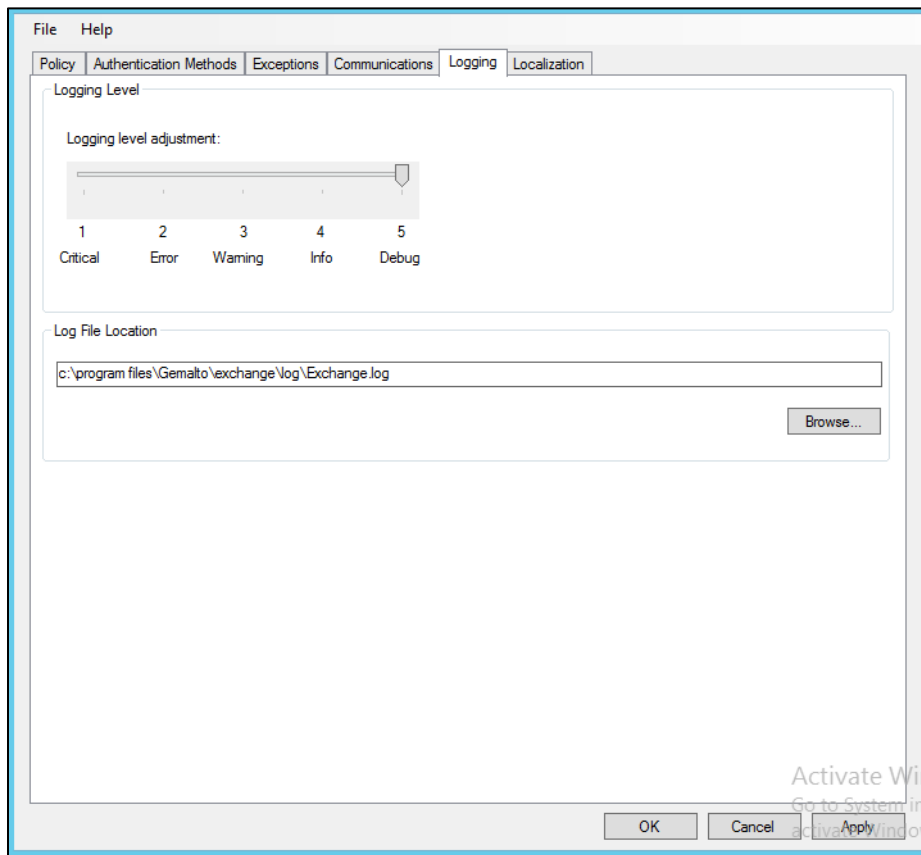
Authentication Test Group

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

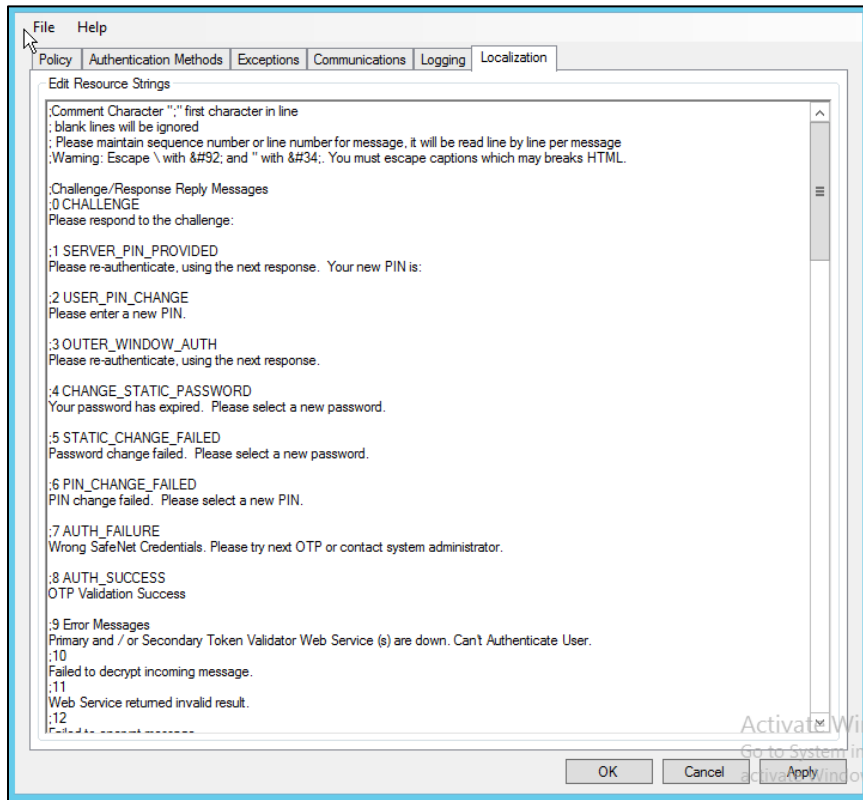
It allow administrators to adjust the logging level. For log levels **1**, **2** and **3**, only the initial connection between the agent and the server, and any failed connection attempts, are logged. Drag the pointer on the **Logging level adjustment** scale to the required level:

- 1 – Critical:** Very severe error events that might cause the application to terminate.
- 2 – Error:** Error events that prevent normal program execution, but might still allow the application to continue running.
- 3 – Warning:** Potentially harmful error events.
- 4 – Info:** Informational error events that highlight the progress of the application.
- 5 – Debug:** Detailed tracing error events that are useful to debug an application. (**Default**)

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\Gemalto\exchange\log\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

CHAPTER 3: 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
Standard Authentication Mode	Standard Authentication Mode enables a single-stage login process. Microsoft domain and SafeNet credentials must be entered in the OWA login page.
Split Authentication Mode	Split Authentication Mode enables a two-stage login process. In the first stage, users provide their Microsoft credentials. In the second stage, users provide their SafeNet credentials. This mode 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.

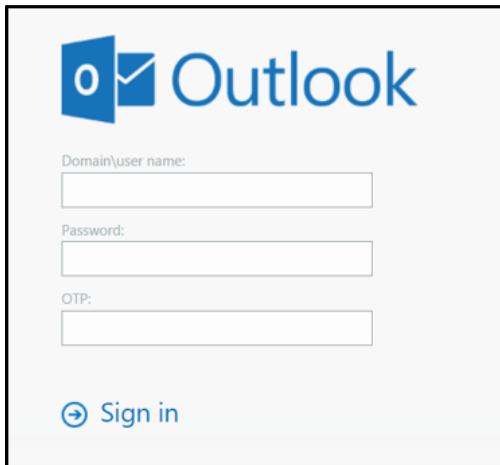
Setting Authentication Mode

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

See [Authentication Methods Tab](#).

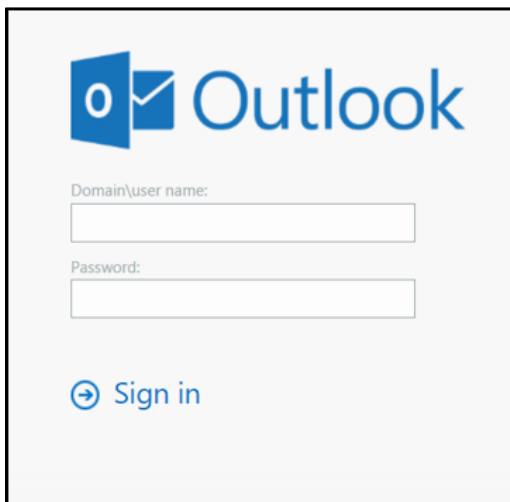
Standard Authentication Mode - Hardware/Software

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



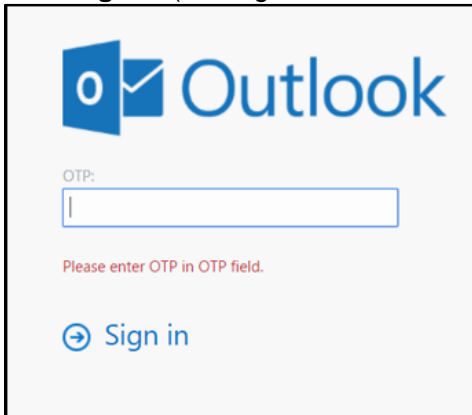
Split Authentication Mode

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



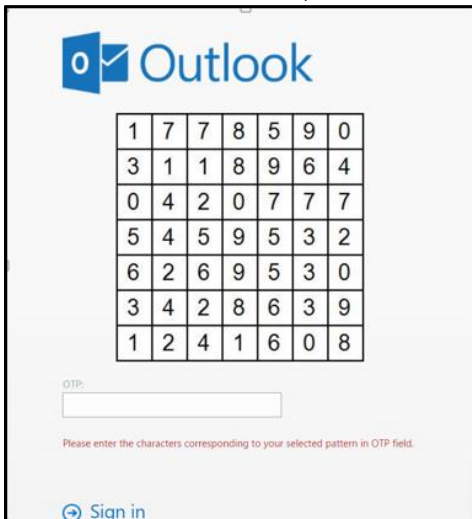
GrIDSure

1. If configured for GrIDSure, do the following:
 - a. Click **Sign In** (leaving the OTP field empty).



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

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



The screenshot shows the Outlook sign-in page with a 7x7 grid pattern. The grid contains the following 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 label "OTP:" followed by an empty text input field. Below the input field is the red text "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.

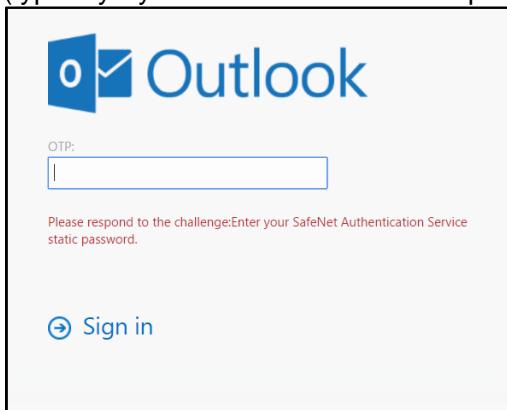
SMS Challenge

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



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).



In return, you will receive a response code.

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

Prerequisites

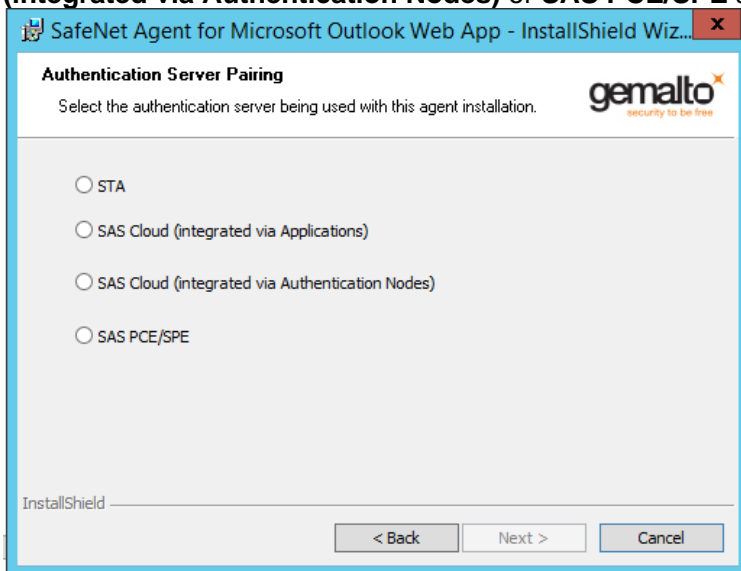
- > Ensure that TCP port 80 or 443 is open on the Exchange Server, which would act as a gateway of communication between the SafeNet OWA agent and the SafeNet solution.
- > Administrative rights to the Windows system are required during the installation of the SafeNet OWA agent.
- > Download the Exchange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

Installing SafeNet Agent for OWA 2016/2019

IMPORTANT: Always work in **Run as administrator** mode when installing, configuring, upgrading, and uninstalling the agent. Always disable the agent first, and then uninstall, if required.

To install the SafeNet OWA agent, follow the steps:

1. Log in to the Microsoft Exchange server.
2. Locate and execute the following installation file:
SafeNet Agent for Microsoft Outlook Web App 2013-2016-2019.exe
3. On the **Welcome to the InstallShield Wizard for SafeNet Agent for Microsoft Outlook Web App** window, click **Next**.
4. On the **License Agreement** window, read the software license agreement and to proceed, 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**.



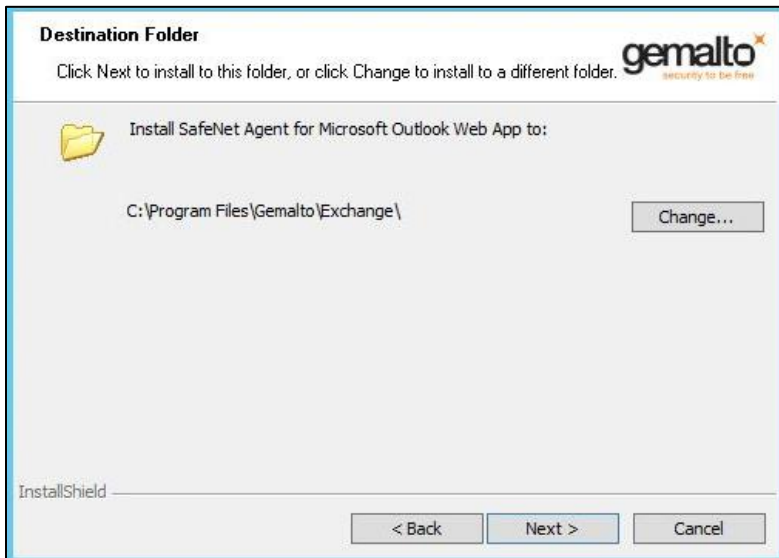
6. On the **Customer Information** window, perform the following steps:
 - a. In the **User Name** field, enter your user name.
 - b. In the **Organization** field, enter the name of your organization.
 - c. Click **Next**.

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)

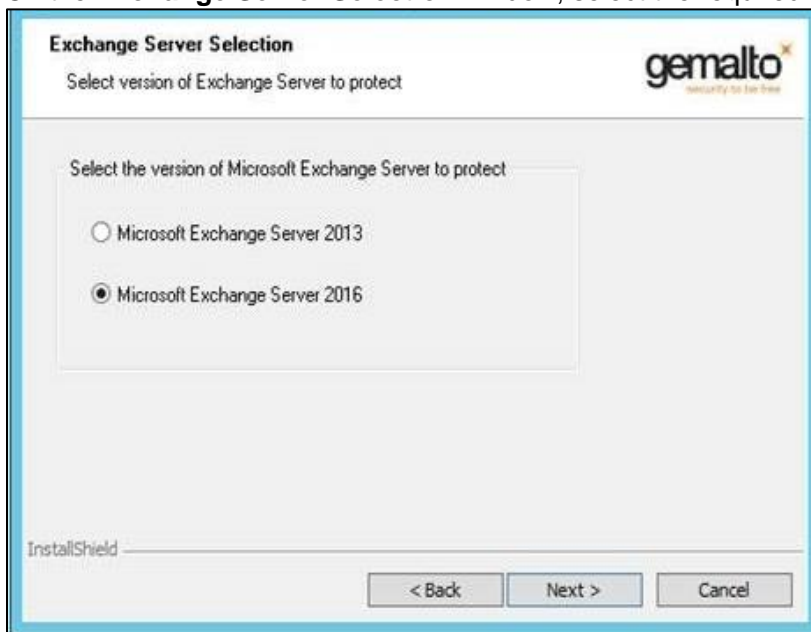
7. On the **Authentication Service Setup** window, enter the following details:
- In the **Location** field, enter the hostname or IP address of the primary SafeNet server.
 - Select **Connect using SSL** if SafeNet server is configured to accept incoming SSL connections.
 - If a failover server is available, 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**.



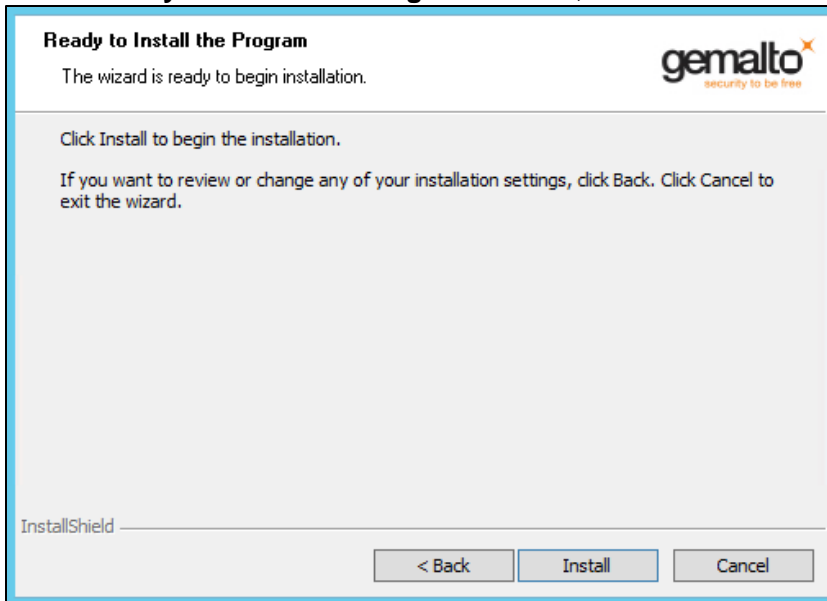
To proceed, the InstallShield Wizard searches for the applicable Exchange Server version in the background. If the Exchange Server is not found, it prompts for the following additional selection:

- a. 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 2016/2019

The SafeNet Agent for OWA 2.1.5 supports upgrade from 2.1.2 (and later). For upgrade, the configurations from the older version must be saved, and then imported into the new installation.

Direct upgrade from versions prior to 2.1.2 to the latest version of the agent is not supported. The earlier versions can be **migrated** to SafeNet Agent for OWA 2.1.5. For migrating from one version to another, see [Migrating SafeNet Agent for OWA 2016/2019 Using Previous Configurations](#) section below.

NOTE: Disable the agent from the management console before proceeding with the upgrade.

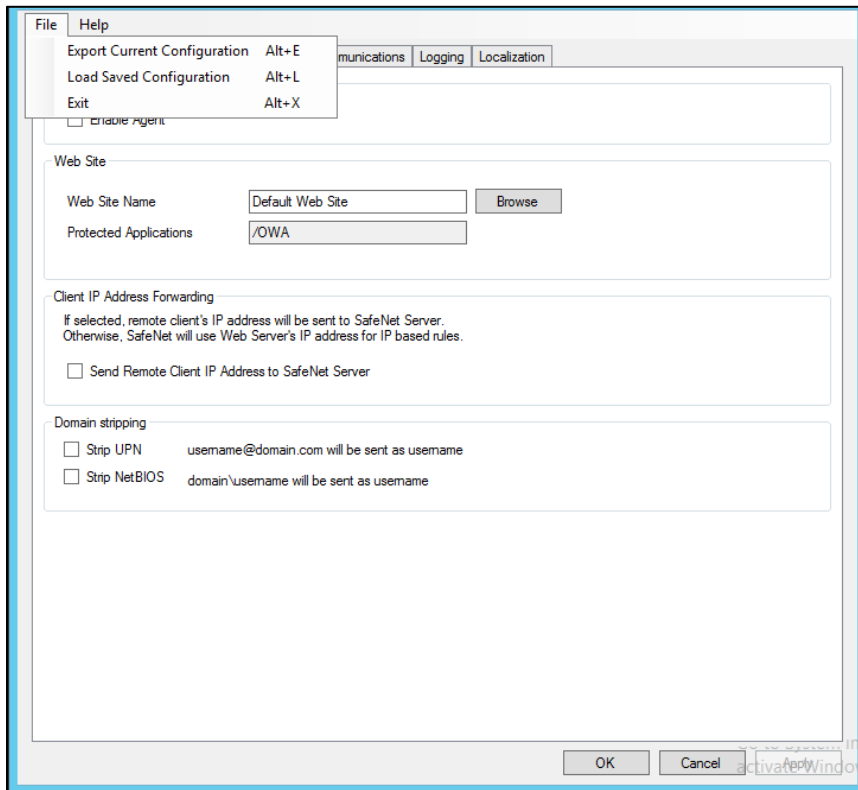
Migrating SafeNet Agent for OWA 2016/2019 Using Previous Configurations

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 2.1.5.

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

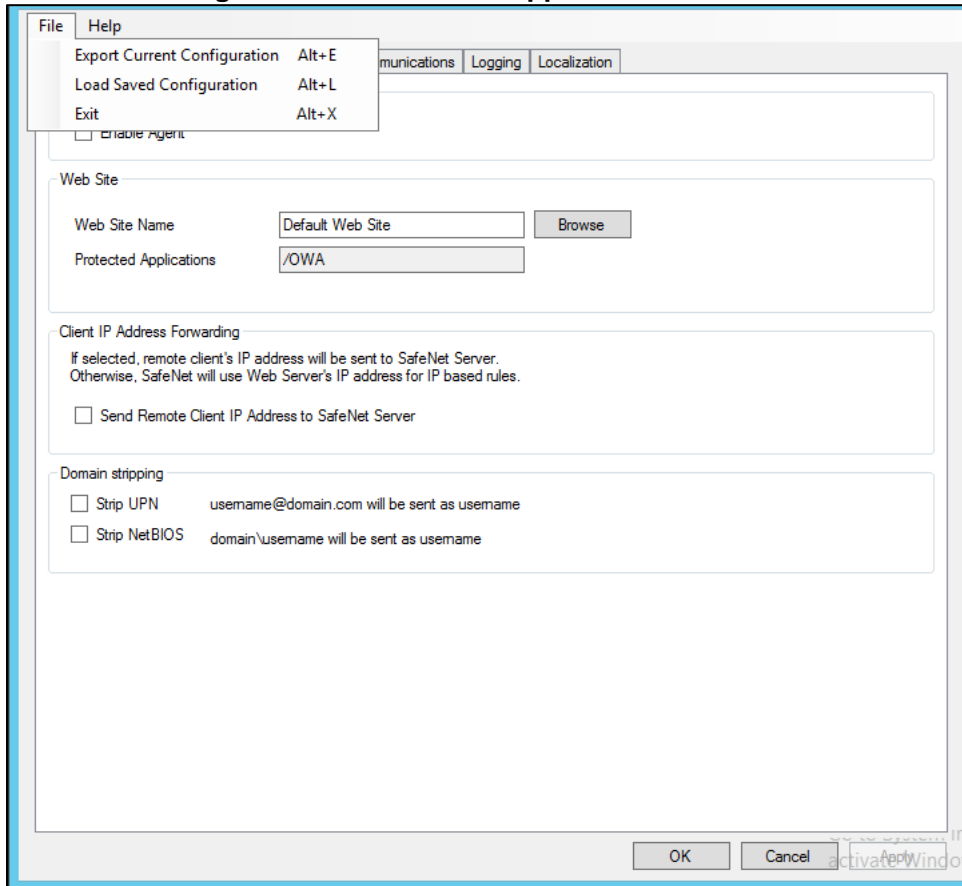
In the existing setup of the agent, perform the following steps:

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



- b. 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 2013-2016-2019.exe

5. In the newly installed agent, load the saved settings as follows:
 - a. In the **SafeNet Agent for Outlook Web App** window, select **File > Load Saved Configuration**.



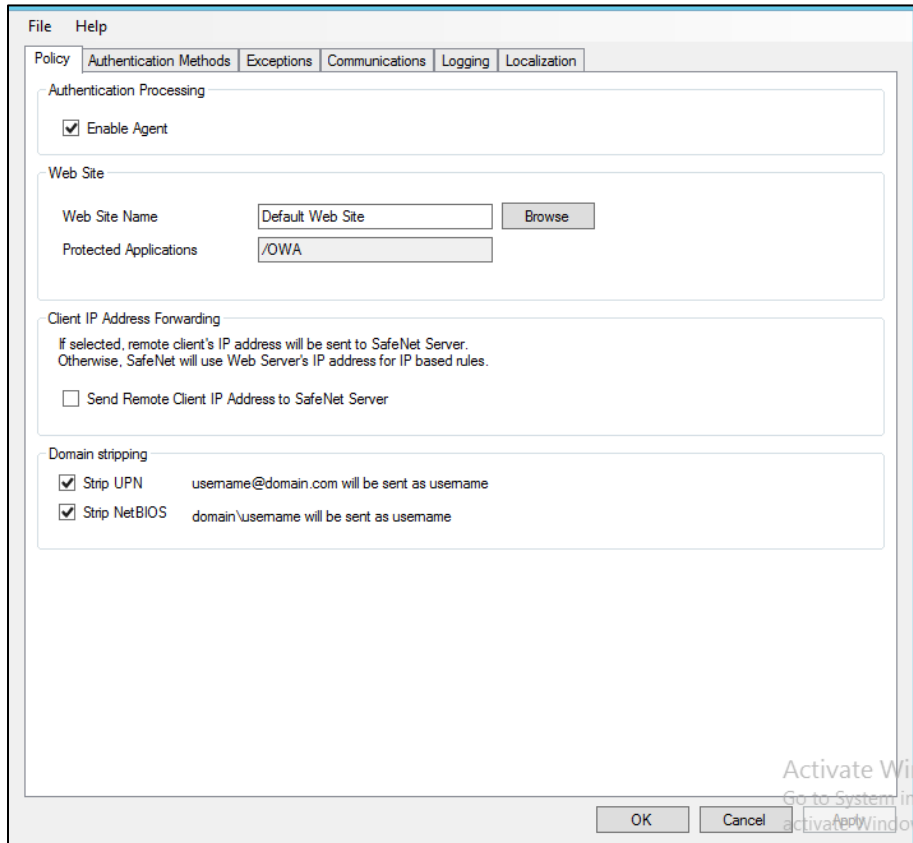
- b. In the **Open** window, select the saved configuration file (.bsidconfig) and click **Open**.
6. Click **OK**.

NOTE: After migrating to the latest 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 with enabling the OWA Agent and defining the website settings.

Authentication Processing Group

- > **Enable Agent:** Turns the SafeNet OWA agent **On** or **Off**.
Default: Disabled

Web Site Group

- > **Web Site Name:** Allows selection of the Exchange Server website.
Default: Default Web Site
- > **Protected Applications:** Specifies the OWA directory on the Exchange Server.
Default: /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: Enabled

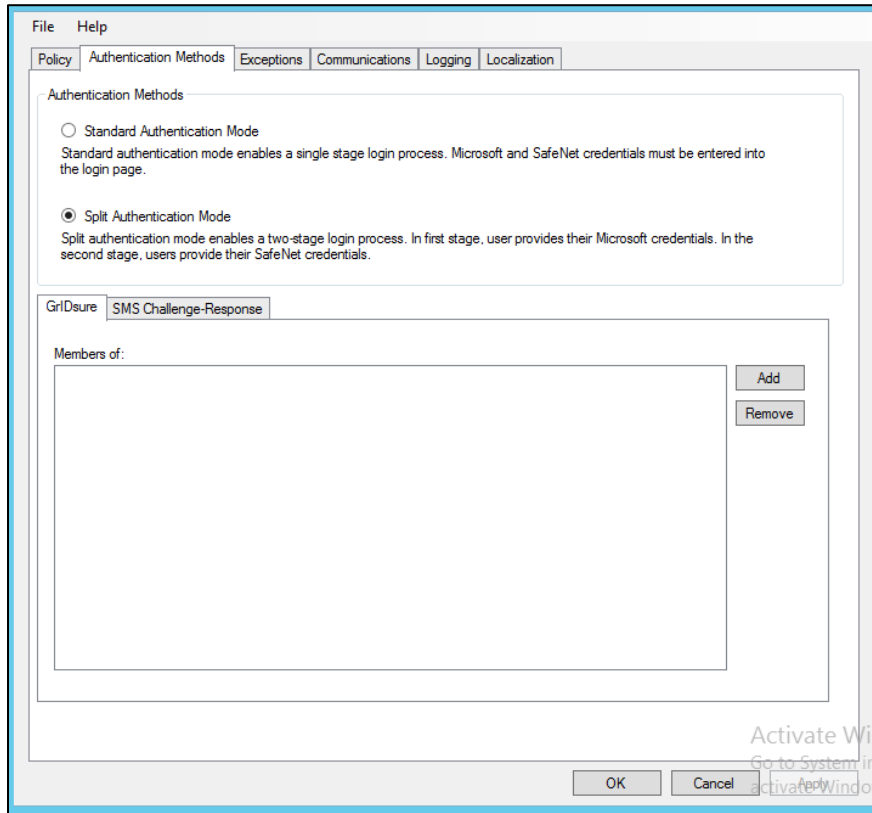
Domain Stripping

- **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: 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 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 with the various SafeNet server connection options.

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

- Primary Server (IP:Port): 10.164.47.151
- Failover Server (optional): (empty)
- Use SSL (requires a valid certificate): (unchecked)
- Disable SSL server certificate check: (unchecked)
- Select minimum SSL/TLS version: TLS 1.0
- Attempt to return to primary Authentication Server every: 10 minute(s)
- Agent Encryption Key File: c:\program files\Gemalto\exchange\bsidKey\Agent.bsidkey

 The 'Authentication Test' section has input fields for 'User Name' and 'Passcode', and a 'Test' button. The 'Server Status Check' section has a 'Test' button. At the bottom, there are 'OK', 'Cancel', and 'Apply' buttons.

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.

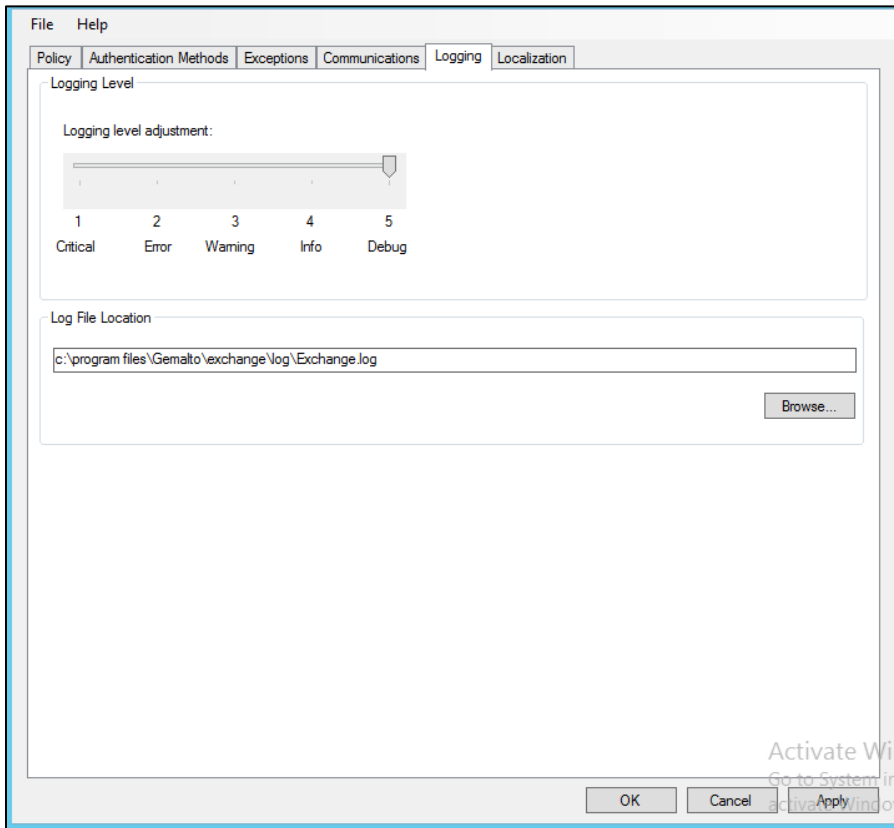
Authentication Test Group

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

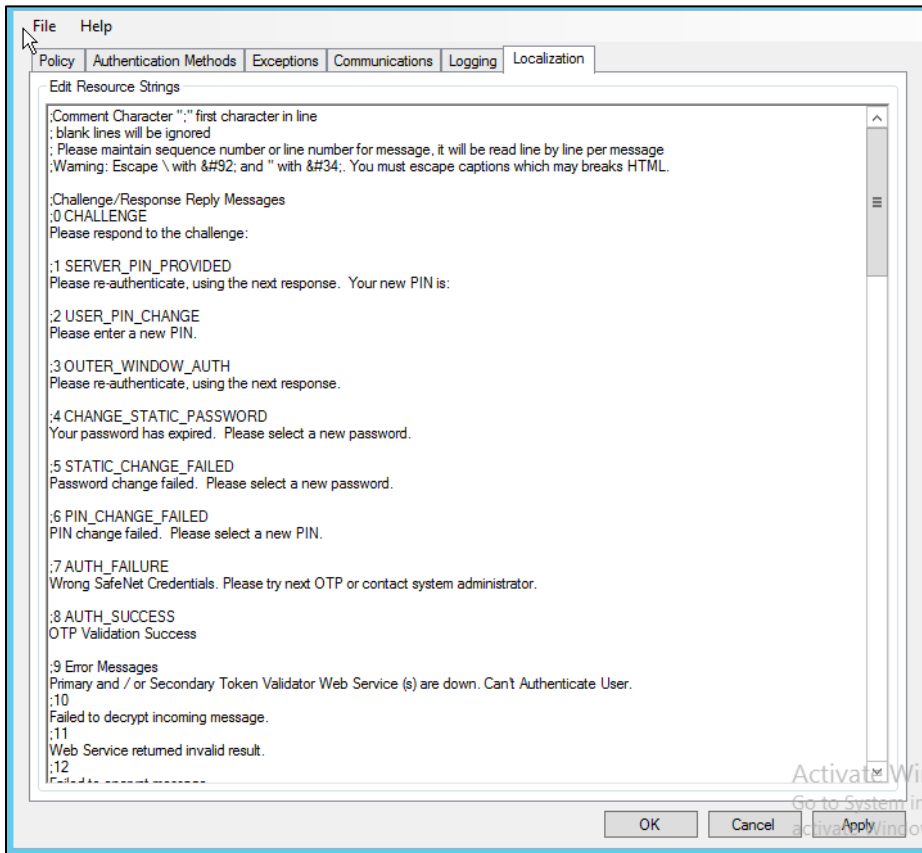
It allow administrators to adjust the logging level. For log levels **1**, **2** and **3**, only the initial connection between the agent and the server, and any failed connection attempts, are logged. Drag the pointer on the **Logging level adjustment** scale to the required level:

- 1 – Critical:** Very severe error events that might cause the application to terminate.
- 2 – Error:** Error events that prevent normal program execution, but might still allow the application to continue running.
- 3 – Warning:** Potentially harmful error events.
- 4 – Info:** Informational error events that highlight the progress of the application.
- 5 – Debug:** Detailed tracing error events that are useful to debug an application. **(Default)**

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\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