SafeNet Authentication Service

Configuration Guide

SAS Agent for Microsoft Outlook Web Access 1.06

SafeNet. THE DATA PROTECTION COMPANY

Document Information

Product Version	1.06
Document Part Number	007-012889-001, Rev. C
Release Date	4 February 2015

Trademarks

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Introduction

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Microsoft Outlook Web Access. 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 as such.

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)** - A cloud authentication service of SafeNet, Inc.
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)** - The software used to build a SafeNet authentication service.
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)** - A term used to describe the implementation of SAS-SPE/PCE.

Environment

Network	• TCP 443
Supported Architecture	• 64-bit
Supported Web Servers	• IIS 7.0 • IIS 7.5 • IIS 8.0
Supported Exchange Server Versions	• Microsoft Exchange Server 2007 • Microsoft Exchange Server 2010 • Microsoft Exchange Server 2013
Supported Web Browsers	• Internet Explorer 8, 9, 10, 11 • Firefox 3 and later • Chrome
Additional Web Browsers Requirements	• Cookies must be enabled • JavaScript must be enabled • ActiveX must be enabled
Supported Authentication Methods	All tokens and authentication methods supported by SafeNet Authentication Service.

SafeNet Authentication Service

SAS Agent for OWA 1.05 supports the following SafeNet Authentication Service releases:

- SafeNet Authentication Service PCE 3.2.1/3.3.2
- SafeNet Authentication Service Cloud

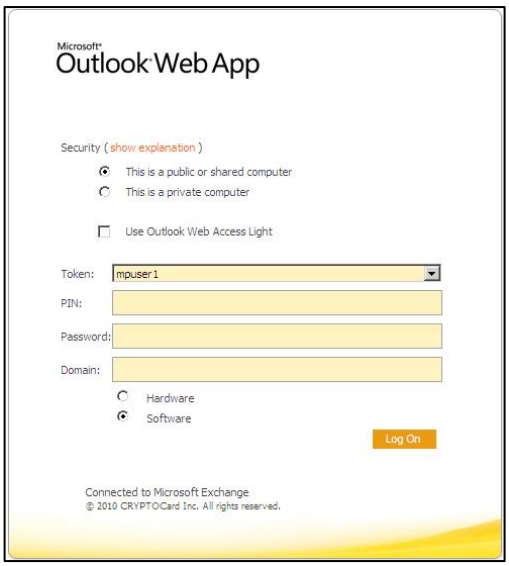
SAS Agent for Outlook Web Access 2007 and 2010

Authentication Modes

There are two modes of operation for the SAS Agent for Outlook Web Access. By default, **Split Authentication** mode is enabled. The authentication mode can be modified after installation using the SAS Exchange Agent Configuration Tool.

Mode	Description
Standard Authentication Mode	Standard Authentication Mode enables a single-stage login process. Microsoft and SafeNet Authentication Service credentials must be entered into the Outlook Web Access 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 SAS credentials. This mode allows administrators to control authentication dialogs based on Microsoft groups or token type (such as GrIDsure). This is the preferred mode when migrating from static to one-time passwords.

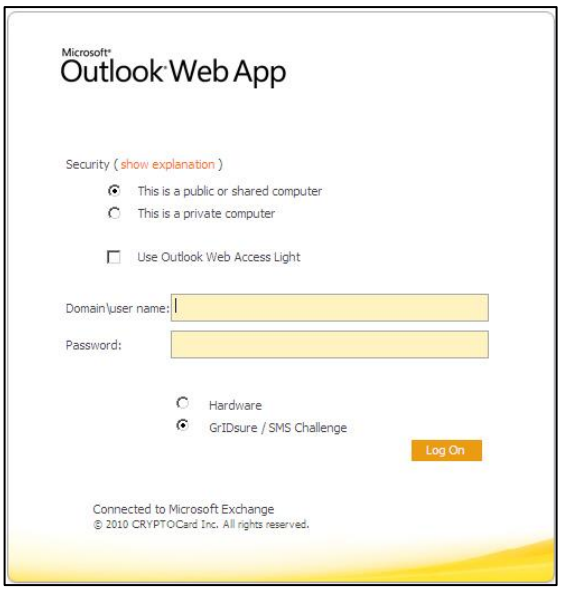
Standard Authentication Mode (Hardware and Software)

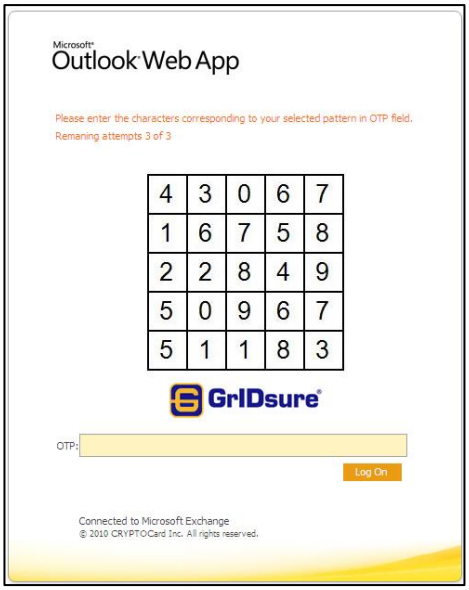


1. The user enters the Outlook Web Access URL into their web browser.
2. The SAS agent examines the incoming request against its **IP Range Exclusions/Inclusions** list to determine if SAS authentication can be ignored.

3. If IP address exclusion is detected, SAS credentials are not required. The user authenticates using Microsoft credentials.
4. If IP address exclusion is not detected, a SAS-enabled login page appears.
5. If a software token is detected, the Outlook Web Access login page will display **Token**, **PIN**, **Microsoft Password** and **Microsoft Domain** fields. An option to toggle between hardware and software token mode will be available.
6. If a software token is not detected, the Outlook Web Access login page will display **Microsoft Username**, **Microsoft Password**, and **OTP** fields.
7. The user enters their Microsoft and SAS credentials into the login page. If both sets of credentials are valid, the user is presented with their mailbox; otherwise, the attempt is rejected.

Standard Authentication Mode (GrIDsure/SMS)

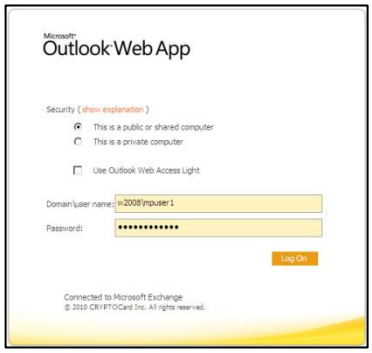


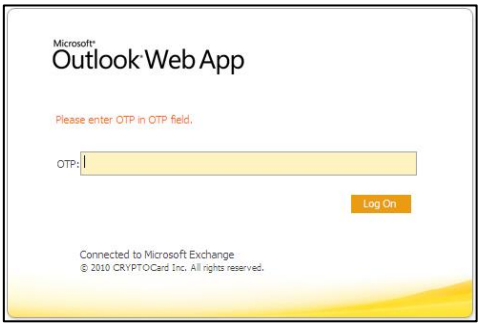


1. The user enters the Outlook Web Access URL into their web browser.
2. The SAS agent examines the incoming request against its **IP Range Exclusions/Inclusions** list to determine if SAS authentication can be ignored.
3. If IP address exclusion is detected, SAS credentials are not required. The user authenticates using Microsoft credentials.
4. If IP address exclusion is not detected, a SAS-enabled login page appears.
5. If a software token is detected, the Outlook Web Access login page will display **Token**, **PIN**, **Microsoft Password** and **Domain** fields. The option to toggle between hardware, software, and GrIDsure/SMS token mode will be available.
6. If a software token is not detected, the Outlook Web Access login page will display **Microsoft Username**, **Microsoft Password**, and **OTP** fields. The option to toggle between hardware and GrIDsure/SMS Challenge-response token mode will be available.

7. The user enters their Microsoft and SAS credentials into the login page. If both sets of credentials are valid, the user is presented with their mailbox; otherwise, the attempt is rejected.
8. In GrIDsure/SMS Challenge-response mode, the user enters their Microsoft credentials into the login page. If the Microsoft credentials are valid, the user is presented with a GrIDsure grid or provided with an OTP via SMS. If the SAS credentials entered are valid, the user is presented with their mailbox; otherwise, the attempt is rejected.

Split Authentication Mode





1. The user enters the Outlook Web Access URL into their web browser.
2. The SAS agent examines the incoming request against its **IP Range Exclusions/Inclusions** list to determine if SAS authentication can be ignored.
3. If IP address exclusion is detected, SAS credentials are not required. The user authenticates and logs into Outlook Web Access using their Microsoft credentials.
4. If IP address exclusion is not detected, the user is presented with **Microsoft Username** and **Microsoft Password** fields. If the Microsoft credentials are valid, the user is allowed to continue; otherwise, the attempt is rejected.
5. The SAS agent examines the Microsoft username against its **Group Authentication Exceptions** list to determine if SAS authentication can be ignored.
6. If a group authentication exception is detected, SAS credentials are not required. The user is presented with their mailbox.
7. If a group authentication exception is not detected, the SAS agent examines the Microsoft username against its GrIDsure and SMS authentication group list.
8. If a GrIDsure or SMS authentication group match is detected, the user is presented with their GrIDsure grid or provided with an OTP via SMS. If the SAS credentials are valid, the user is presented with their mailbox; otherwise, the attempt is rejected.
9. If a software token is detected, the Outlook Web Access login page will display a **PIN** field. The option to toggle between hardware and software mode will be available.
10. If a software token is not detected, the Outlook Web Access login page will display an **OTP** field.
11. The user enters their SAS credentials into the login page. If the credentials are valid, the user is presented with their mailbox; otherwise, the attempt is rejected.

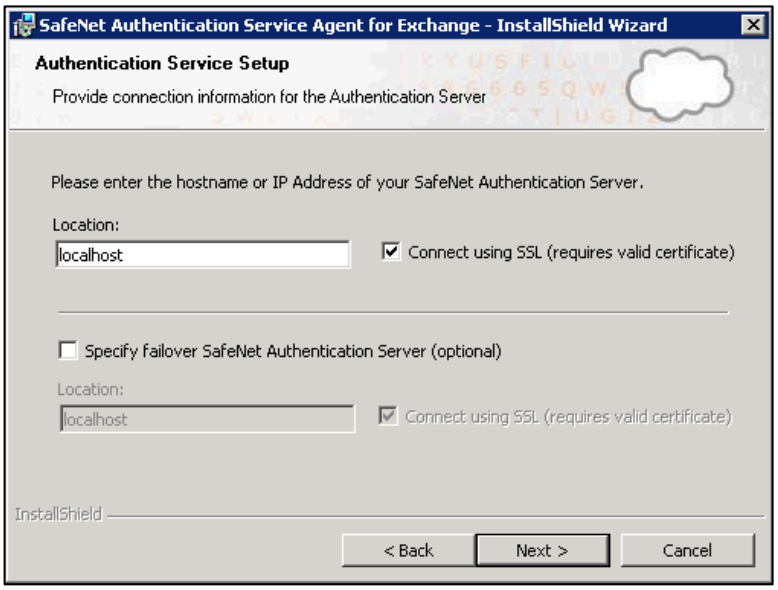
Prerequisites

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

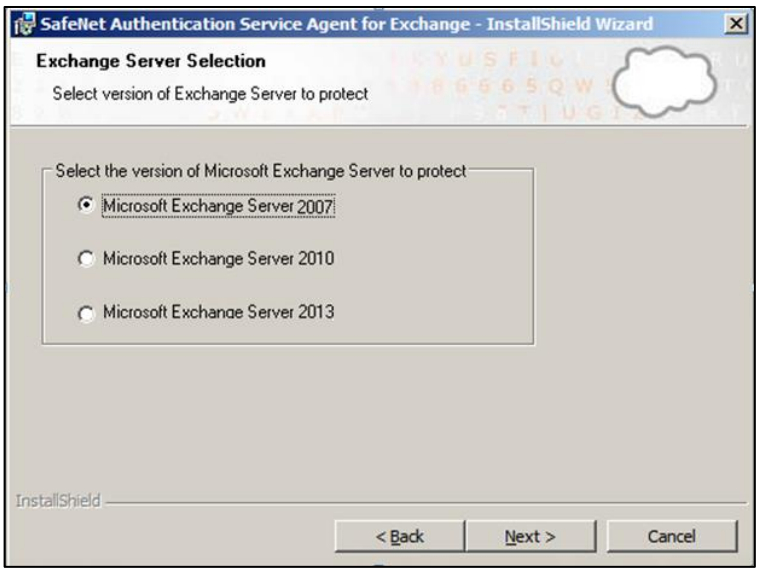
Installing the SAS Agent for Outlook Web Access (2007/2010)

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

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



   - In the **Location** field, enter the hostname or IP address of the primary SafeNet Authentication Service server.
   - Select **Connect using SSL** if SAS has been configured to accept incoming SSL connections.
   - If available, select the check box and add the hostname or IP address of a failover SafeNet Authentication Service server.
3. Click **Next**.
4. Select the version of Microsoft Exchange Server to protect, and then click **Next**.



Upgrading the SAS Agent for Outlook Web Access (2007/2010)

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

Upgrading from SAS Agent for OWA Version 1.05 to 1.06

Automatic upgrade from SAS Agent for OWA version 1.05 to version 1.06 is not supported. Uninstall the installed agent and install SAS Agent for OWA 1.06 as follows.

To upgrade from SAS Agent for OWA version 1.05 to 1.06:

1. Uninstall the currently installed SAS Agent for OWA
2. Delete manually all contents from the SAS Agent for OWA installation folder.
3. Delete manually all registry keys for SAS Agent for OWA.
4. Run the installation file SafeNet Agent for Exchange x64.exe as an administrator.
5. Enable the OWA Agent using the SAS Management Console.

Upgrading from SAS Agent for OWA Versions1.03 or 1.04 to 1.06

To upgrade from SAS Agent for OWA version 1.03 or 1.04 to 1.06:

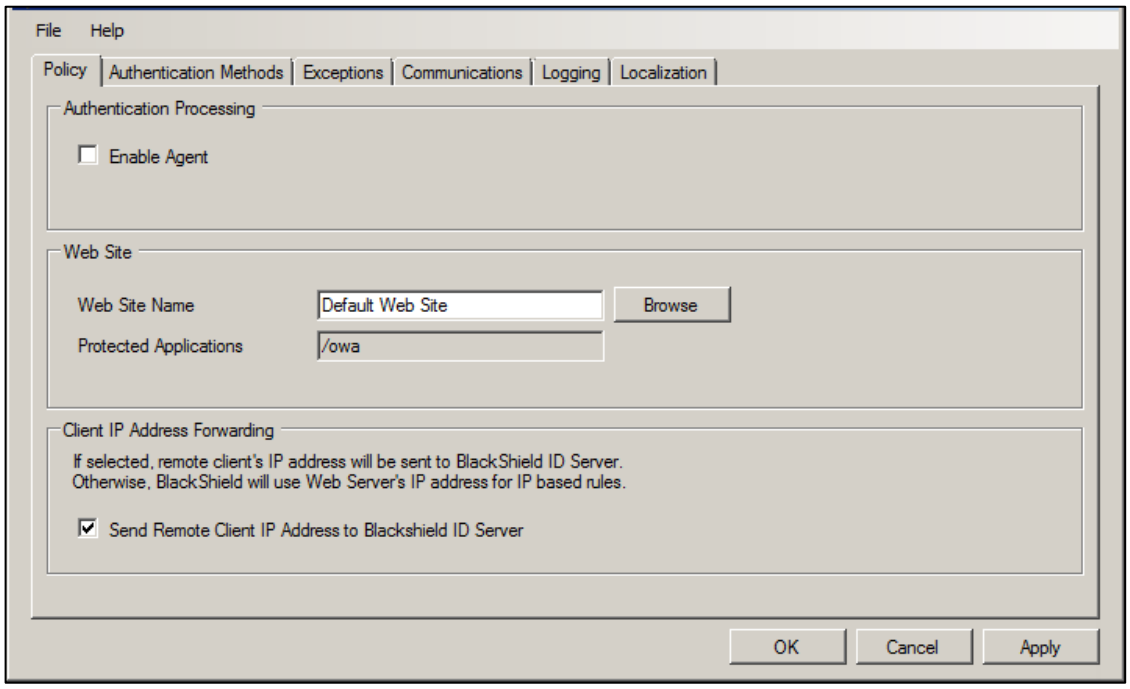
1. Back up the installation folder contents, including any changed templates, the INI file, and the Caption (localization) file.
2. Disable the OWA Agent using the SAS Management Console.
3. Run the installation file SafeNet Agent for Exchange x64.exe as an administrator and, when prompted, select Upgrade.
4. Enable the OWA Agent using the SAS Management Console.

NOTE: If the previously installed SAS Agent for OWA was installed in a location that was not the default, a window will be displayed during the upgrade process prompting you to enter the location of the previous SAS Agent for OWA.

SAS Exchange Agent Configuration Tool

The SAS Exchange agent configuration tool allows for the modification of various features available within the SAS Agent for Outlook Web Access.

Policy Tab



The **Policy** tab deals primarily with enabling the Outlook Web Access agent and defining the website settings.

Authentication Processing Group

- **Enable Agent:** Turns the SAS ID Agent for Outlook Web Access on or off. Default value: Disabled.

Web Site Group

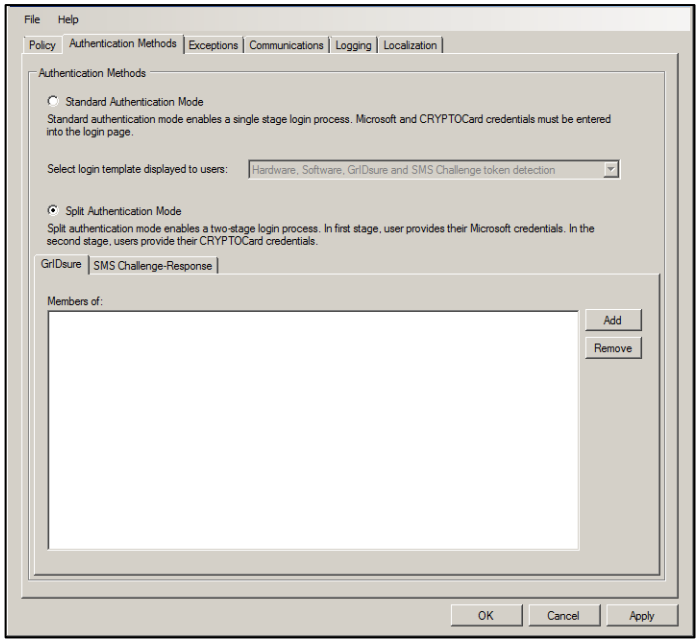
- **Web Site Name:** Allows the selection of the Exchange Server website. Default value: Default Web Site.
- **Protected Applications:** Specifies the Outlook Web Access directory on the Exchange Server. Default value: /owa.

Client IP Address Forwarding Group

If selected, the remote client IP address will be sent to the SafeNet Authentication Service. Otherwise, the web server's IP address will be used. Default value: Enabled.

Authentication Methods Tab

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



Authentication Methods Group

- **Standard Authentication Mode:** This mode enables a single-step login process. Microsoft and SafeNet Authentication Service credentials must be entered into a single login page. Default value: Disabled.

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

- **Hardware and Software Token Detection:** If a software token is detected, the login page will display **Token**, **PIN**, **Microsoft Password**, and **Microsoft Domain** fields; otherwise, **Microsoft Username**, **Microsoft Password**, and **OTP** fields will be displayed. The option to toggle between Hardware and Software token mode will be available if a software token is detected on the local workstation.
- **Hardware, Software, GrIDsure, and SMS Challenge Token Detection:** If a software token is detected, the login page will display **Token**, **PIN**, **Microsoft Password**, and **Microsoft Domain** fields. If required, a set of radio button options will allow the user to select a different token type. If no software token exists, the user will be presented with **Microsoft Username**, **Microsoft Password**, and **OTP** fields, along with an option to enable a GrIDsure\SMS Challenge login page.
- **Split Authentication Mode:** 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 Authentication Service credentials. Default value: Enabled.

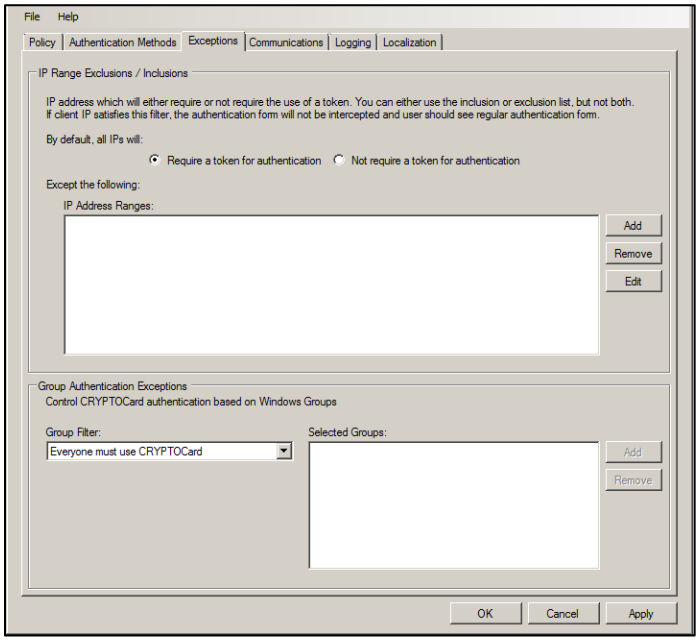
This mode provides the following advantages over Standard Authentication Mode:

- Microsoft group exclusions may be used to migrate users gradually from static passwords to a combination of static and one-time passwords.
- Allows 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 Authentication Service 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 Authentication Service users who have been assigned an SMS Challenge-response token. When the agent detects a user within the group, it will automatically provide them with a one-time password via SMS after they have provided valid Microsoft credentials.

Exceptions Tab

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



IP Range Exceptions/Inclusions Group

Allows an administrator to define which network traffic requires SafeNet Authentication Service authentication. By default, all networks are required to perform SafeNet Authentication Service authentication.

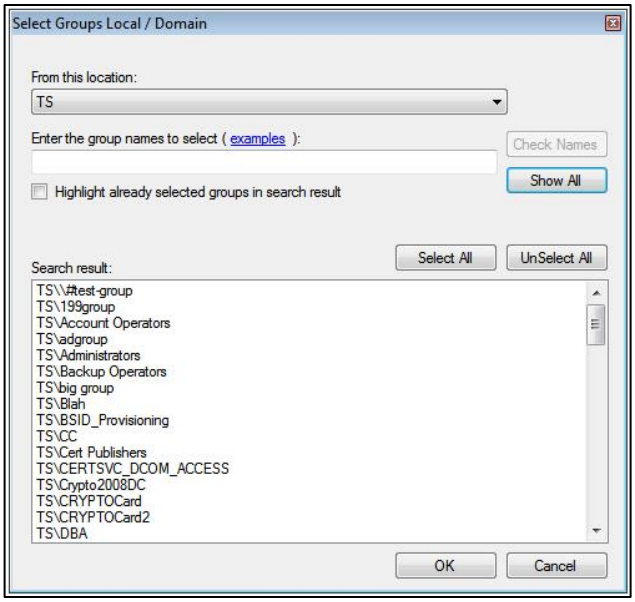
Group Authentication Exceptions Group

Group authentication exceptions omit single and/or multiple domain groups from performing SafeNet Authentication Service 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 Authentication Service.

The following group authentication exceptions are available:

- **Everyone must use SafeNet Authentication Service:** All users must perform SafeNet Authentication Service authentication.
- **Only selected groups will bypass SafeNet Authentication Service:** All users are required to perform SafeNet Authentication Service authentication except the Microsoft Group(s) defined.

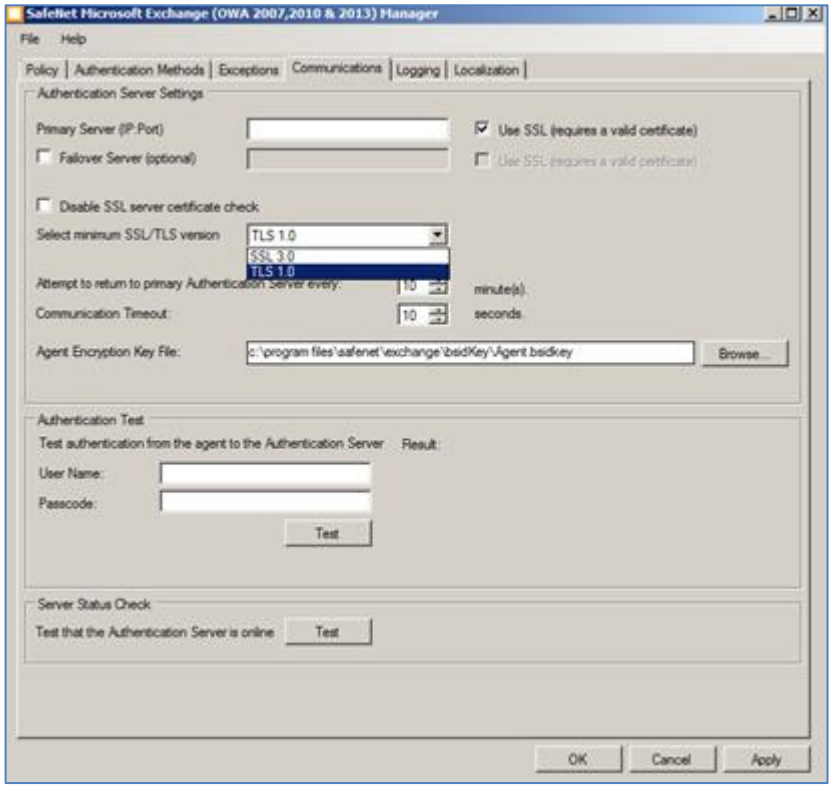
- **Only selected groups must use SafeNet Authentication Service:** All users are not required to perform SafeNet Authentication Service authentication except the Microsoft Group(s) defined. Adding a group authentication exception entry will display the following window:



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

Communications Tab

This tab deals primarily with the connection options for SafeNet Authentication Service.



Authentication Server Settings Group

- **Primary Server (IP:Port):** Used to configure the IP address/hostname of the primary SafeNet Authentication Service. Default is port 80. Alternatively, **Use SSL** can also be selected. Default TCP port for SSL requests is 443.
- **Failover Server (Optional):** Used to configure the IP address/hostname of the failover SafeNet Authentication Service. Default is port 80. Alternatively, **Use SSL** can also be selected. Default TCP port for SSL requests is 443.
- **Disable SSL server certificate check:** Select to disable the SSL server certificate error check.

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

NOTE: We strongly recommend the use of SSL certificates.

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

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

  For more details see: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566
- **Attempt to return to primary Authentication Server every:** Sets the Primary Authentication server retry interval. This setting only takes effect when the agent is using the **Failover Server** entry.
- **Communication Timeout:** Sets the maximum timeout value for authentication requests sent to SafeNet Authentication Service.
- **Agent Encryption Key File:** Used to specify the location of the SAS Agent Key File.

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

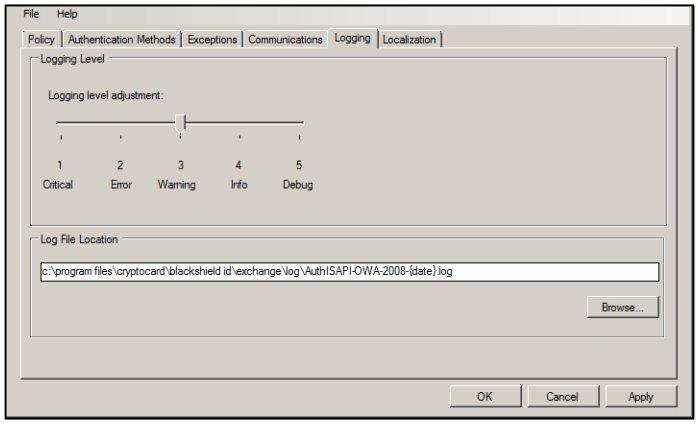
Authentication Test Group

Allows administrators to test authentication between the agent and SafeNet Authentication Service.

Server Status Check Group

Performs a communication test to verify a connection to SafeNet Authentication Service.

Logging Tab



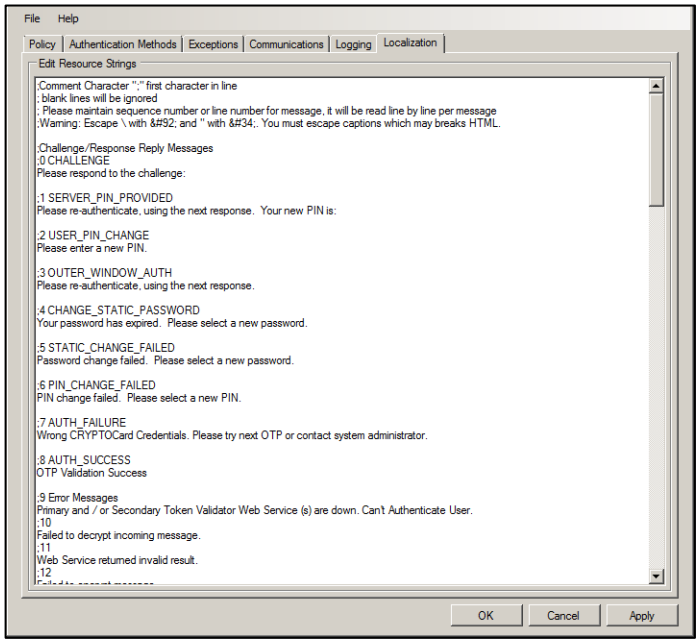
Logging Level Group

Adjusts 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 is 3.

Log File location Group

Specifies the location of the log files. The log file is rotated on a daily basis. The default location is: \Program Files\SafeNet\SAS \Exchange\Log.

Localization Tab



The settings on this tab represent the prompts and information messages provided by the SAS Agent for Outlook Web Access. These can be modified as necessary to improve usability. The **Messages.txt** file can also be manually modified outside of the configuration tool. This file can be found in the **\Program Files\SafeNet\SAS\Exchange\LocalizedMessages** folder.

SAS Agent for Outlook Web Access 2013

The SAS Agent for Outlook Web Access 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 instead of just traditional static passwords to access Outlook Web Access is a necessary critical step for information security.

Modes of Operation

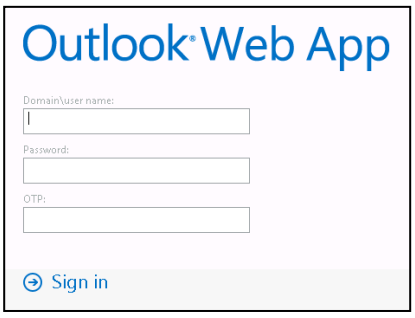
There are two modes of operation for the SAS Agent for Outlook Web Access. By default, Split Authentication mode is enabled. The authentication mode can be modified after installation using the SAS Exchange Agent Configuration Tool.

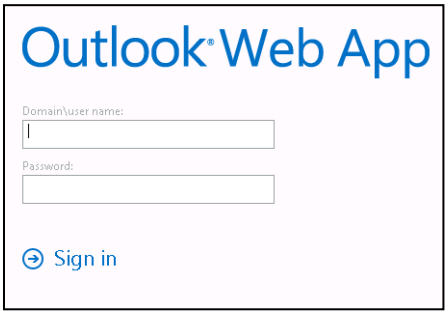
The modes of operation are:

Mode	Description
Standard Authentication Mode	Standard Authentication Mode enables a single stage login process. Microsoft and SafeNet Authentication Service credentials must be entered into the Outlook Web Access 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 SAS credentials. This mode allows administrators to control authentication dialogs based on Microsoft groups or token type (such as GrIDsure). This is the preferred mode when migrating from static to one-time passwords.

Standard Authentication Mode

1. The user enters the Outlook Web Access URL into their web browser.
2. The SAS agent examines the incoming request against its **IP Range Exclusions/Inclusions** list to determine if SafeNet Authentication Service authentication can be ignored.
3. If IP address exclusion is detected, SafeNet Authentication Service credentials are not required. The user authenticates using Microsoft credentials.
4. If IP address exclusion is not detected, a SafeNet Authentication Service enabled login page appears.





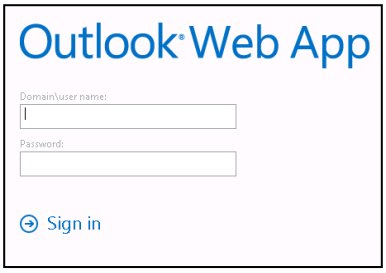
5. The user enters their Microsoft and SafeNet Authentication Service credentials into the login page. If both sets of credentials are valid, the user is presented with their mailbox; otherwise, the attempt is rejected.

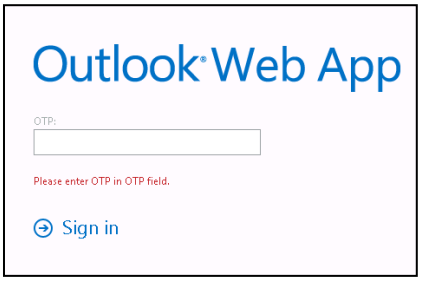
Standard Authentication Mode (GrIDsure\SMS)

1. The user enters the Outlook Web Access URL into their web browser.
2. The SAS agent examines the incoming request against its **IP Range Exclusions/Inclusions** list to determine if SafeNet Authentication Service authentication can be ignored.
3. If IP address exclusion is detected, SafeNet Authentication Service credentials are not required. The user authenticates using Microsoft credentials.
4. If IP address exclusion is not detected, a SafeNet Authentication Service enabled login page appears.
5. The user enters their Microsoft and SafeNet Authentication Service credentials into the login page. If both sets of credentials are valid, the user is presented with their mailbox; otherwise, the attempt is rejected.
6. In GrIDsure\SMS Challenge-response mode, the user enters their Microsoft credentials into the login page. If the Microsoft credentials are valid the user is presented with a GrIDsure grid or provided with an OTP via SMS. If the SafeNet Authentication Service credentials entered are valid, the user is presented with their mailbox; otherwise, the attempt is rejected.

Split Authentication Mode

1. The user enters the Outlook Web Access URL into their web browser.
2. The SAS agent examines the incoming request against its **IP Range Exclusions/Inclusions** list to determine if SafeNet Authentication Service authentication can be ignored.
3. If IP address exclusion is detected, SafeNet Authentication Service credentials are not required. The user authenticates and logs into Outlook Web Access using their Microsoft credentials.
4. If IP address exclusion is not detected, the user is presented with **Microsoft Username** and **Microsoft Password** fields. If the Microsoft credentials are valid, the user is allowed to continue; otherwise, the attempt is rejected.





5. The SAS agent examines the Microsoft username against its **Group Authentication Exceptions** list to determine if SafeNet Authentication Service authentication can be ignored.
6. If a group authentication exception is detected, SafeNet Authentication Service credentials are not required. The user is presented with their mailbox.
7. If a group authentication exception is not detected, the SAS agent examines the Microsoft username against its GrIDsure and SMS authentication group list.
8. If a GrIDsure or SMS authentication group match is detected, the user is presented with their GrIDsure grid or provided with an OTP via SMS. If the SafeNet Authentication Service credentials are valid, the user is presented with their mailbox; otherwise, the attempt is rejected.
9. If a software token is detected, the Outlook Web Access login page will display a **PIN** field. The option to toggle between hardware and software mode will be available.
10. If a software token is not detected, the Outlook Web Access login page will display an **OTP** field.
11. The user enters their SafeNet Authentication Service credentials into the login page. If the credentials are valid, the user is presented with their mailbox; otherwise, the attempt is rejected.

Preparation

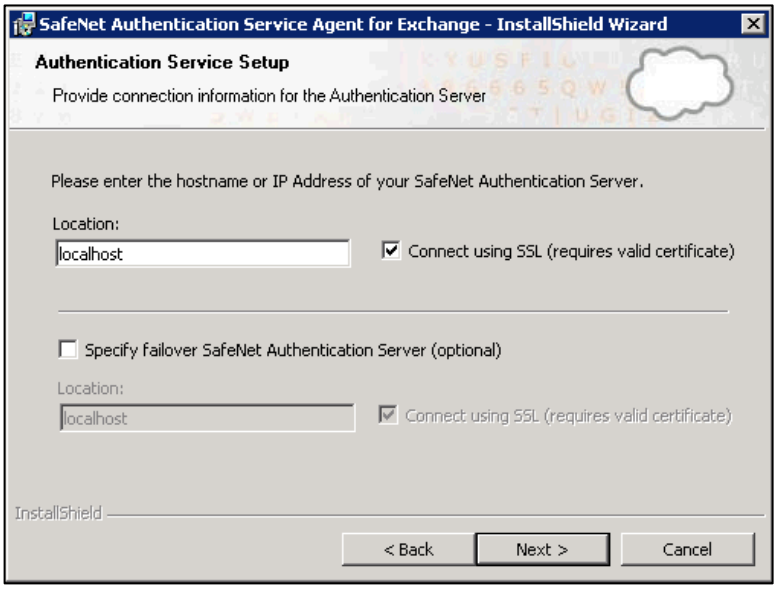
- Ensure that TCP port 80 or 443 is open between the SafeNet Authentication Service Agent for Outlook Web Access and the SafeNet Authentication Service.
- Administrative rights to the Windows system are required during installation of the SafeNet Authentication Service Outlook Web Access Agent.
- Download 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 Authentication Service (SAS).

Installing SAS Agent for Outlook Web Access (2013)

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

To install SAS Agent for Outlook Web Access:

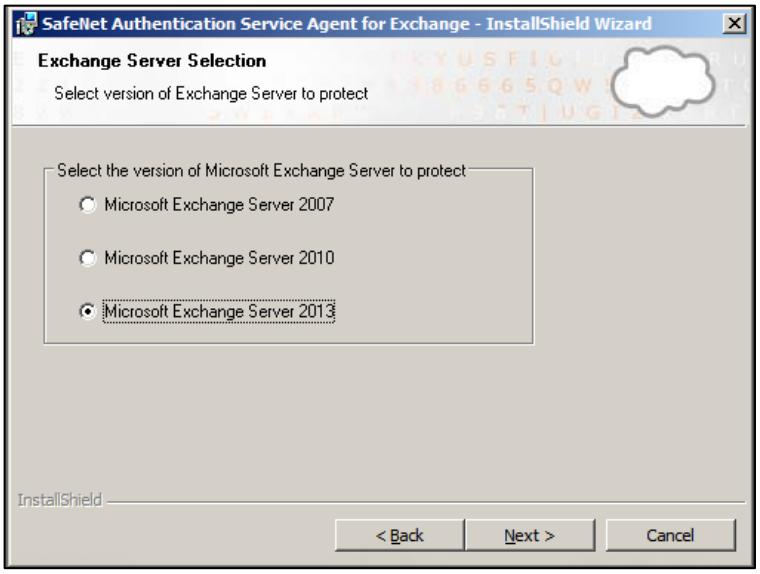
1. Log on to the Microsoft Exchange server.
2. Locate and run the SAS Agent for Exchange x64.exe installation package following the prompts. The **Authentication Service Setup** window opens.



- In the **Location** field, enter the hostname or IP address of the primary SafeNet Authentication Service.
- Select **Connect using SSL** if SAS has been configured to accept incoming SSL connections.
- If available, select the check box and add the hostname or IP address of a failover SafeNet Authentication Service.

3. Click **Next** to continue.

4. Select the version of Microsoft Exchange Server to protect.



5. Click **Next** to continue.

Upgrading the SAS Agent for Outlook Web Access (2013)

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

Upgrading from SAS Agent for OWA Version 1.05 to 1.06

Automatic upgrade from SAS Agent for OWA version 1.05 to version 1.06 is not supported. Uninstall the installed agent and install SAS Agent for OWA 1.06 as follows.

To upgrade from SAS Agent for OWA version 1.05 to 1.06:

1. Uninstall the currently installed SAS Agent for OWA
2. Delete manually all contents from the SAS Agent for OWA installation folder.
3. Delete manually all registry keys for SAS Agent for OWA.
4. Run the installation file SafeNet Agent for Exchange x64.exe as an administrator.
5. Enable the OWA Agent using the SAS Management Console.

Upgrading from SAS Agent for OWA Versions1.03 or 1.04 to 1.06

To upgrade from SAS Agent for OWA version 1.03 or 1.04 to 1.06:

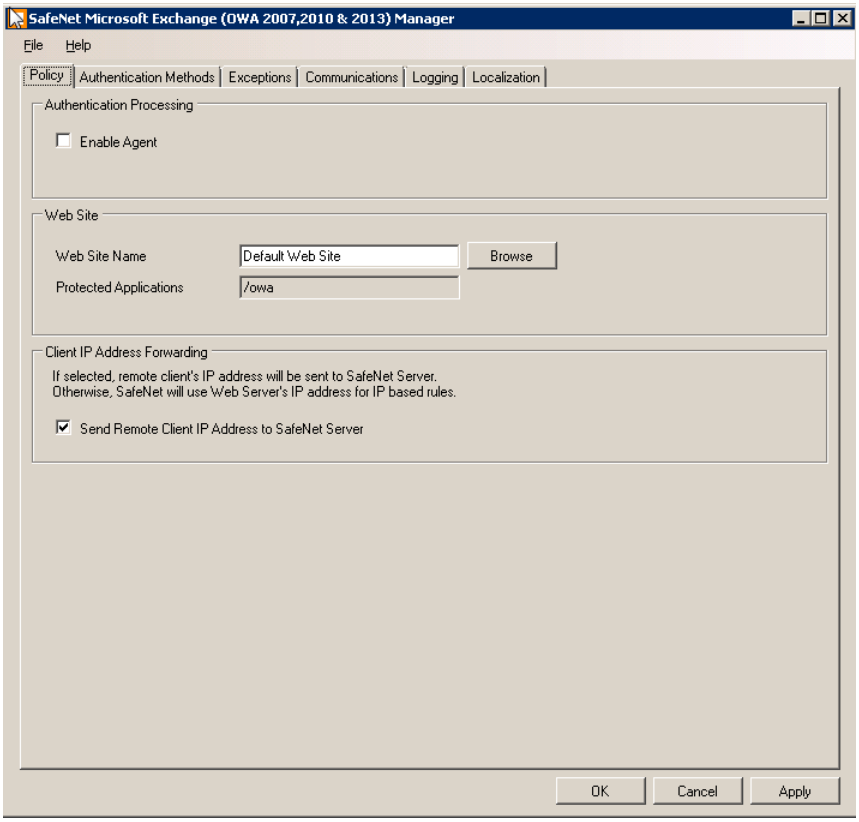
1. Back up the installation folder contents, including any changed templates, the INI file, and the Caption (localization) file.
2. Disable the OWA Agent using the SAS Management Console.
3. Run the installation file SafeNet Agent for Exchange x64.exe as an administrator and, when prompted, select Upgrade.
4. Enable the OWA Agent using the SAS Management Console.

NOTE: If the previously installed SAS Agent for OWA was installed in a location that was not the default, a window will be displayed during the upgrade process prompting you to enter the location of the previous SAS Agent for OWA.

SAS Exchange Agent Configuration Tool

The SAS Exchange agent configuration tool allows for the modification of various features available within the SAS Agent for Outlook Web Access.

Policy Tab



The **Policy** tab deals primarily with enabling the Outlook Web Access agent and defining the web site settings.

Authentication Processing Group

- **Enable Agent:** Turns the SAS Agent for Outlook Web Access on or off. Default value: Disabled.

Web Site Group

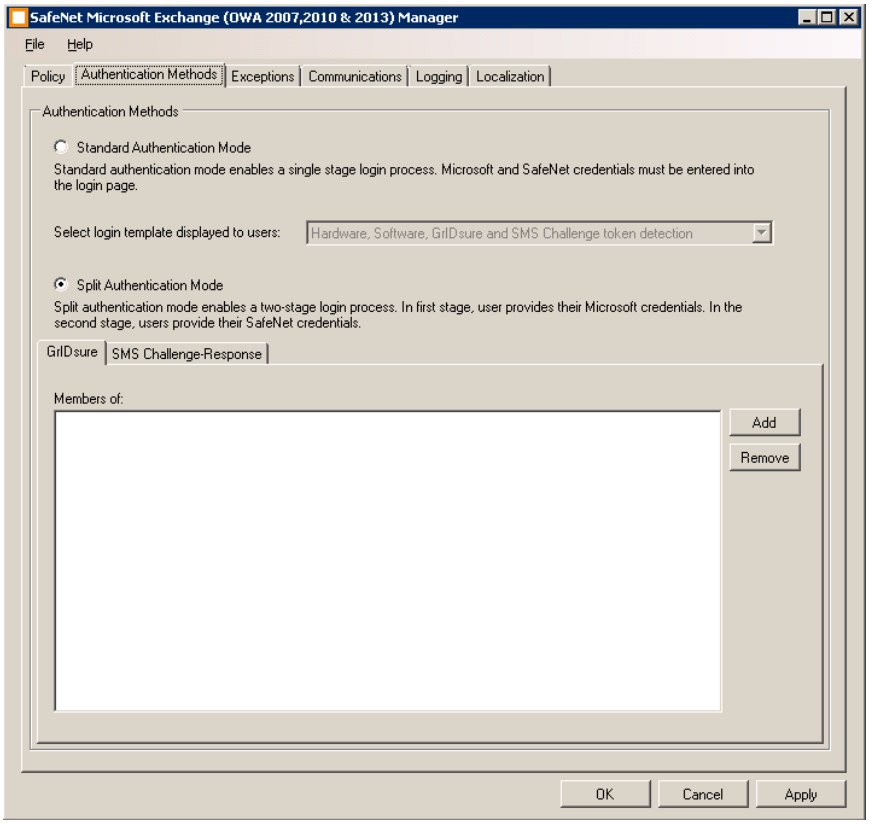
- **Web Site Name:** Allows the selection of the Exchange Server website. Default value: Default Web Site.
- **Protected Applications:** Specifies the Outlook Web Access directory on the Exchange Server. Default value: /owa.

Client IP Address Forwarding Group

If selected, the remote client IP address will be sent to the SafeNet Authentication Service; otherwise, the Web server's IP Address will be used. Default value: Enabled.

Authentication Methods Tab

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



Authentication Methods Group

- **Standard Authentication Mode:** Standard Authentication Mode enables a single-step login process. Microsoft and SafeNet Authentication Service credentials must be entered into a single login page. Default value: Disabled.

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

- **Hardware and Software Token Detection:** If a software token is detected, the login page will display **Token**, **PIN**, **Microsoft Password**, and **Microsoft Domain** fields; otherwise, **Microsoft Username**, **Microsoft Password**, and **OTP** fields will be displayed. The option to toggle between Hardware and Software token mode will be available if a software token is detected on the local workstation.
- **Hardware, Software, GrIDsure and SMS Challenge Token Detection:** If a software token is detected, the login page will display **Token**, **PIN**, **Microsoft Password**, and **Microsoft Domain** fields. If required, a set of radio button options will allow the user to select a different token type. If no software token

exists, the user will be presented with **Microsoft Username**, **Microsoft Password**, and **OTP** fields, along with an option to enable a GrIDsure\SMS Challenge login page.

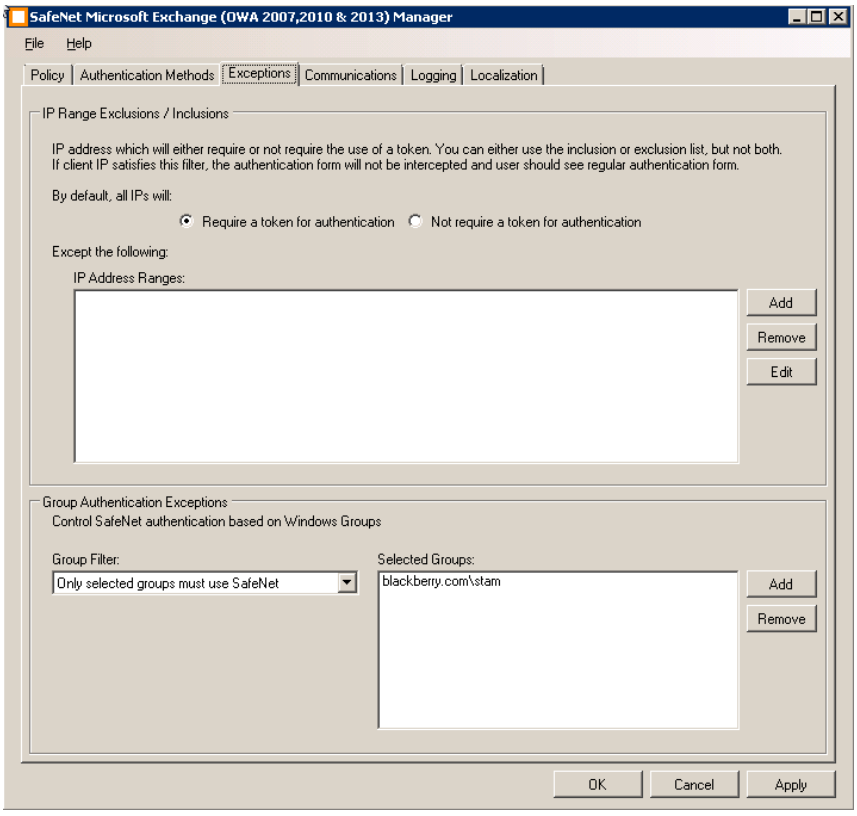
- **Split Authentication Mode:** Split Authentication Mode enables a two-stage login process. In the first stage, users provide their Microsoft credentials. In the second stage, users provide their SafeNet Authentication Service credentials. Default value: Enabled.

This mode provides the following advantages over Standard Authentication Mode:

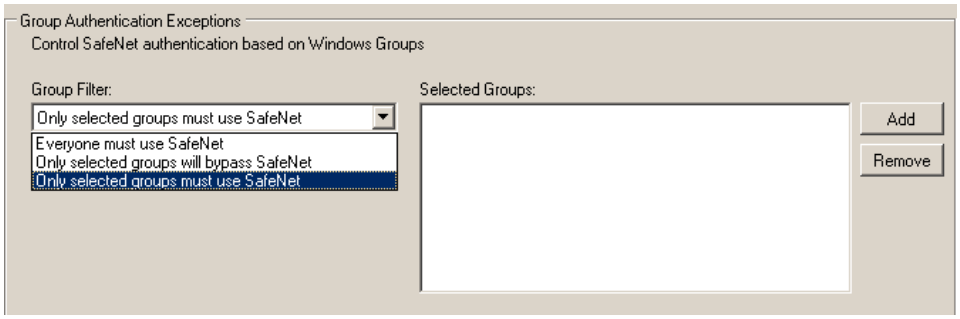
- Microsoft group exclusions may be used to migrate users gradually from static passwords to a combination of static and one-time passwords.
- Allows administrators to specify via Microsoft Groups, users who have been provided with GrIDsure or SMS Challenge-response tokens. This allows for a seamless 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 Authentication Service 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 Authentication Service users who have been assigned an SMS Challenge-response token. When the agent detects a user within the group, it will automatically provide them with a one-time password via SMS after they have provided valid Microsoft credentials.

Exceptions Tab

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

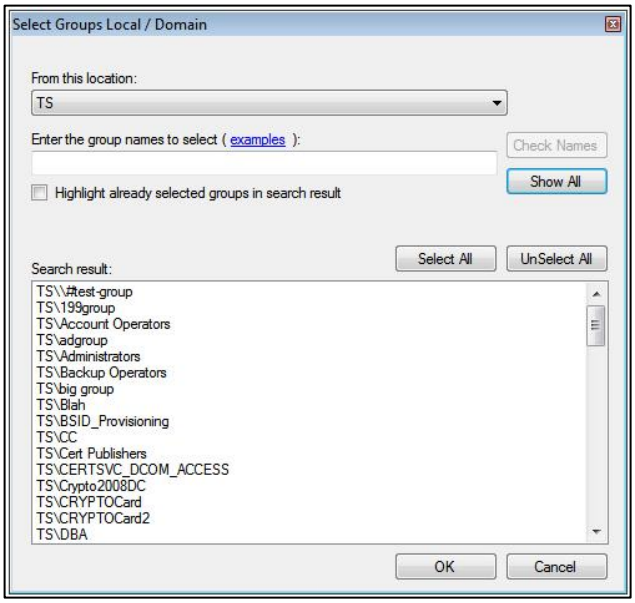


- **IP Range Exceptions/Inclusions Group:** Allows an administrator to define which network traffic requires SafeNet Authentication Service authentication. By default, all networks are required to perform SafeNet Authentication Service authentication.
- **Group Authentication Exceptions Group:** Group authentication exceptions omit single and/or multiple domain groups from performing SafeNet Authentication Service 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 Authentication Service.



The following group authentication exceptions are available:

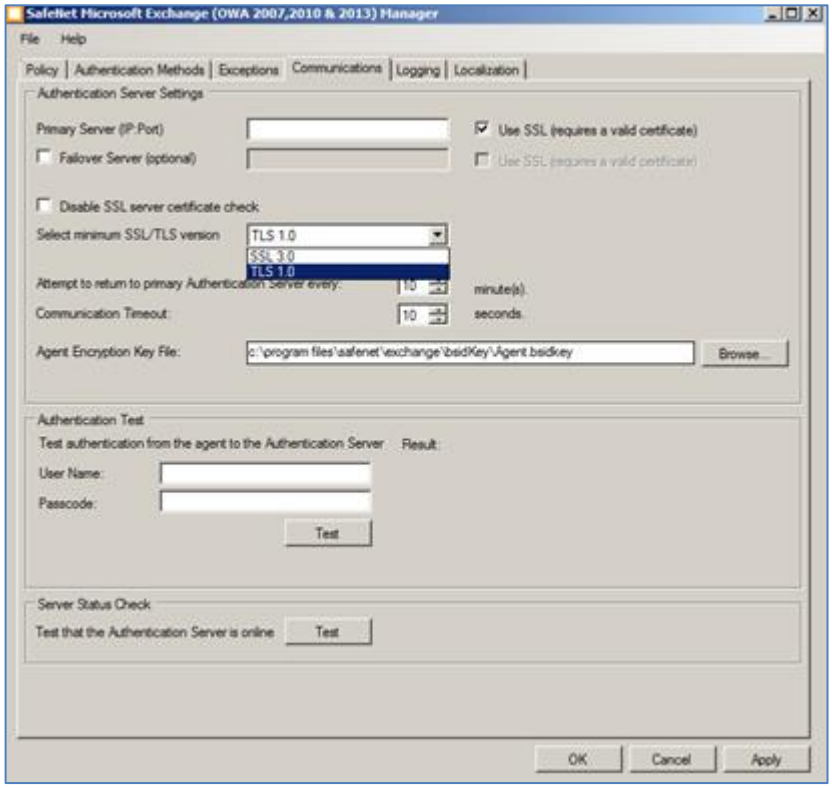
- **Everyone must use SafeNet Authentication Service:** All users must perform SafeNet Authentication Service authentication.
- **Only selected groups will bypass SafeNet Authentication Service:** All users are required to perform SafeNet Authentication Service authentication except the Microsoft Group(s) defined.
- **Only selected groups must use SafeNet Authentication Service:** All users are not required to perform SafeNet Authentication Service authentication except the Microsoft Group(s) defined. Adding a group authentication exception entry will display the following:



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

Communications Tab

This tab deals primarily with the connection options for SafeNet Authentication Service.



Authentication Server Settings Group

- **Primary Server (IP:Port):** Used to configure the IP address/hostname of the primary SafeNet Authentication Service. Default is port 80. Alternatively, **Use SSL** can also be selected. Default TCP port for SSL requests is 443.
- **Failover Server (Optional):** Used to configure the IP address/hostname of the failover SafeNet Authentication Service. Default is port 80. Alternatively, **Use SSL** can also be selected. Default TCP port for SSL requests is 443.
- **Disable SSL server certificate check:** Select to disable the SSL server certificate error check.

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

NOTE: We strongly recommend the use of SSL certificates.

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

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

  For more details see: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566
- **Attempt to return to primary Authentication Server every:** Sets the Primary Authentication server retry interval. This setting only takes effect when the agent is using the **Failover Server** entry.
- **Communication Timeout:** Sets the maximum timeout value for authentication requests sent to SafeNet Authentication Service.
- **Agent Encryption Key File:** Used to specify the location of the SAS Agent Key File.

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

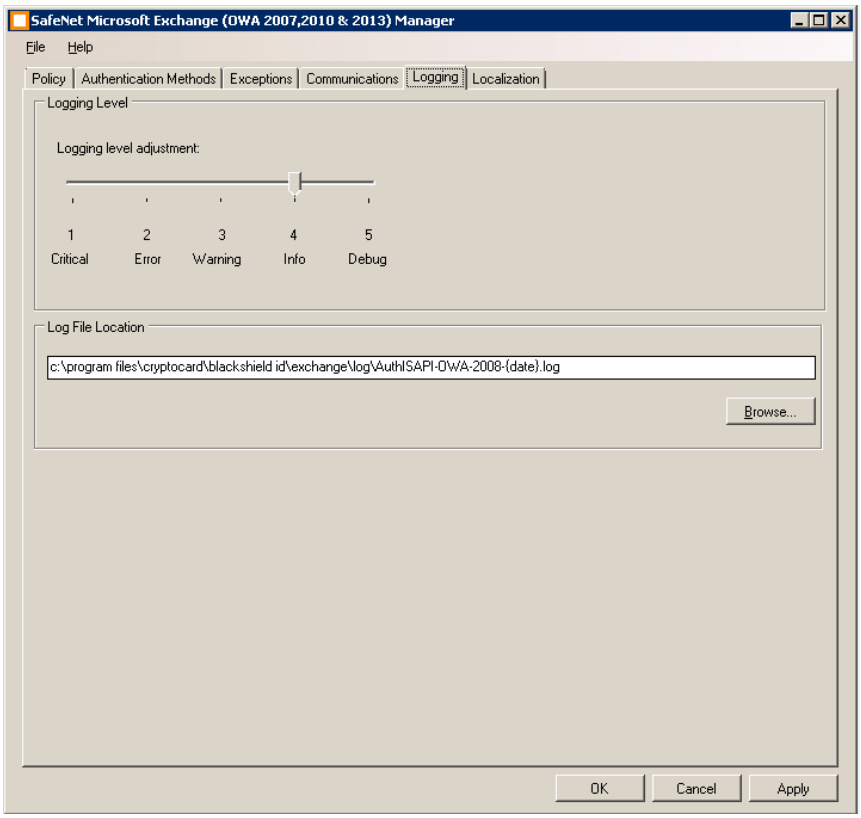
Authentication Test Group

Allows administrators to test authentication between the agent and SafeNet Authentication Service.

Server Status Check Group

Performs a communication test to verify a connection to SafeNet Authentication Service.

Logging Tab



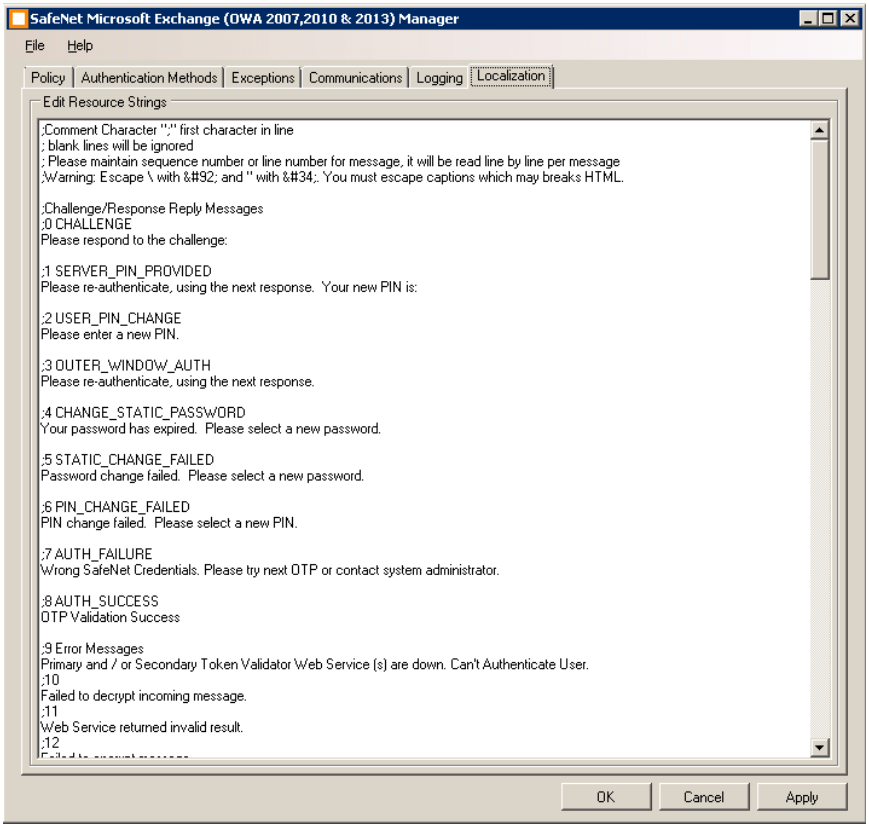
Logging Level Group

Adjusts 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 is 3.

Log File location Group

Specifies the location of the log files. The log file is rotated on a daily basis. The default location is **\Program Files\SafeNet\SAS\Exchange\Log**.

Localization Tab



The settings in this tab represent the prompts and information messages provided by the SAS Agent for Outlook Web Access. These can be modified as necessary to improve usability. The **Messages.txt** file can also be manually modified outside of the configuration tool. This file can be found in the **\Program Files\SafeNet\SAS\Exchange\LocalizedMessages** folder.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet 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 SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when phone support is available to you.

Table 1: Support Contacts

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	