SafeNet Authentication Service
Integration Guide

Using SafeNet Authentication Service as an Identity Provider for Microsoft Outlook Web App
All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

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

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

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

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

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

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

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

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

© 2016 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

**Document Part Number:** 007-012828-001, Rev. B

**Release Date:** June 2016
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 App.

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.

Description

SafeNet Authentication Service delivers a fully automated, versatile, and strong authentication-as-a-service solution.

With no infrastructure required, SafeNet Authentication Service provides smooth management processes and highly flexible security policies, token choice, and integration APIs.

Web Application Proxy is a role service of the Remote Access server role in Windows Server® 2012 R2. Web Application Proxy provides reverse proxy functionality for web applications inside your corporate network to allow users on any device to access your web applications from outside the corporate network. Web Application Proxy pre-authenticates access to web applications by using Active Directory Federation Services (AD FS), and also functions as an AD FS proxy.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Microsoft Outlook Web App using SafeNet pse-time password (OTP) authenticators managed by SafeNet Authentication Service.
- Configure SAML authentication in Microsoft Outlook Web App using SafeNet Authentication Service as an identity provider.

It is assumed that the Microsoft Outlook Web App environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Microsoft Outlook Web App can be configured to support multi-factor authentication in several modes. The SAML authentication will be used for the purpose of working with SafeNet Authentication Service.

Applicability

The information in this document applies to:

- SafeNet Authentication Service (SAS)—SafeNet’s cloud-based authentication service
- SafeNet Authentication Service – Service Provider Edition (SAS-SPE)—A server version that is used by Service providers to deploy instances of SafeNet Authentication Service
- SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)—A server version that is used to deploy the solution on-premises in the organization
Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Service** – SafeNet’s cloud-based authentication service
- **Microsoft Outlook Web App (Exchange 2013 SP1)** – on Server 2012 R2
- **AD FS 3.0** – on Server 2012 R2
- **Web Application Proxy** – on Server 2012 R2

Audience

This document is targeted to system administrators who are familiar with Microsoft Outlook Web App, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

SAS Authentication API Authentication using SafeNet Authentication Service Cloud

SAS Cloud provides a service for SafeNet Authentication Service (SAS) Authentication API that is already implemented in the SAS Cloud environment and can be used using the Gemalto SafeNet SAS AD FS Agent.

SAS Authentication API using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE

In addition to the pure cloud-based offering, SafeNet Authentication Service (SAS) comes with two on-premises versions:

- **SafeNet Authentication Service – Service Provider Edition (SPE)**—An on-premises version of SafeNet Authentication Service targeted at service providers interested in hosting SAS in their data center.
- **SafeNet Authentication Service – Private Cloud Edition (PCE)**—An on-premises version of SafeNet Authentication Service targeted at organizations interested in hosting SAS in their private cloud environment.
For both on-premises versions, SAS can be integrated with AD FS infrastructure, which uses a special on-premises agent called Gemalto SafeNet SAS AD FS Agent.

**SafeNet Authentication Service Authentication API Flow using SAS**

AD FS provides extensible multi-factor authentication through the concept of “additional authentication providers” that are invoked during secondary authentication. External providers can be registered in AD FS.

Once a provider is registered with AD FS, it is invoked from the AD FS authentication code via specific interfaces and methods that the provider implements and that AD FS calls. Because it provides a bridge between AD FS and an external authentication provider, the external authentication provider is also called an AD FS MFA “adapter”.

Gemalto SafeNet SAS AD FS Agent is an AD FS MFA adapter that provides users a way to authenticate through AD FS using SAS as a secondary authenticator.

The image below describes the dataflow of a multi-factor authentication transaction for Microsoft Outlook Web App.

1. A user attempts Sign in to Microsoft Outlook Web App. The user is redirected AD FS proxy server (WAP), then after successful authentication, is forwarded to SafeNet Authentication Service (SAS) for a secondary authentication (AD FS multi-factor authentication).
2. The user uses his or her SAS token for authenticating. SAS collects and evaluates the user’s credentials.
3. The SAS authentication reply is sent back to AD FS which returns a response to Microsoft Outlook Web App, accepting or rejecting the user’s authentication request.
4. The user is granted or denied access to Microsoft Outlook Web App.
Integration Checklist

To configure SAS as an Identity Provider of Microsoft Outlook Web (through AD FS 3.0) make sure you follow the following checklist:

1. Adding AD FS Authentication for Microsoft Outlook Web App
2. Configuring Gemalto SafeNet SAS AD FS Agent
3. Configuring AD FS 3.0 as Primary Authentication Method for Microsoft Outlook Web App (using WAP)
4. Configuring SafeNet Authentication Service

Adding AD FS Authentication for Microsoft Outlook Web App

In order to add AD FS authentication for Microsoft Outlook Web, perform the following steps:

1. Creating a Relying Party Trust for Outlook Web App and EAC
2. Adding AD FS Claim Rules for OWA and EAC
3. Verifying AD FS Authentication with Outlook Web App

Creating a Relying Party Trust for Outlook Web App and EAC

For all applications and services that are to be published through the Web Application Proxy, a relying party must be configured on the AD FS server. For deployments with multiple Active Directory sites that use separate namespaces, a relying party trust for Outlook Web App and EAC must be added for each namespace.

To create a relying party trust for Outlook Web App and EAC:

1. Open the Server Manager window, click Tools, and then select AD FS Management.

2. In the left pane, under AD FS, expand Trust Relationships, right-click Relying Party Trusts, and then click Add Relying Party Trust. The Add Relying Party Trust Wizard opens.
3. On the **Welcome** window, click **Start**.

4. On the **Select Data Source** window, click **Enter data about the relying party manually**, and then click **Next**.
5. On the **Specify Display Name** window, in the **Display Name** box, enter **Outlook Web App** or **OWA**. Under **Notes**, enter a description for this relying party trust (for example, **This is a trust for https://exchange.integ.com/owa**), and then click **Next**.
6. On the **Choose Profile** window, click **AD FS profile**, and then click **Next**.

![Choose Profile Window](image1)

7. On the **Configure Certificate** window, click **Next**.

![Configure Certificate Window](image2)

8. On the **Configure URL** window:
a. Select Enable support for the WS-Federation Passive protocol.

b. Under Relying party WS-Federation Passive protocol URL, enter your OWA URL (for example, https://iis.integ.com/owa), and then click Next.

9. On the Configure Identifiers window, specify one or more identifiers for this relying party. Click Add to add them to the list, and then click Next.

10. On the Configure Multi-factor Authentication Now? window, leave the default configuration (MFA will be configured later), and then click Next.
11. On the **Choose Issuance Authorization Rules** window, select **Permit all users to access this relying party**, and then click **Next**.

12. On the **Ready to Add Trust** window, review the settings, and then click **Next** to save your relying party trust information.
13. On the Finish window, verify that the option Open the Edit Claim Rules dialog for this relying party trust when the wizard closes is not selected, and then click Close.

14. Follow steps 1-13 again to create a relying party trust for EAC, with the following changes:
   - For the display name, enter EAC.
   - In the Description field, enter This is a trust for the Exchange Admin Center.
   - The Relying party WS-Federation Passive protocol URL is ECP’s URL (for example, https://exchange.integ.com/ecp).

15. The AD FS Relying Party Trusts tab now includes two new trusts - OWA and ECP.
Adding AD FS Claim Rules for OWA and EAC

In a claims-based identity model, the function of Active Directory Federation Services (AD FS) as a federation service is to issue a token that contains a set of claims. Claim rules govern the decisions with regards to claims that AD FS issues. Claim rules and all server configuration data are stored in the AD FS configuration database.

The following claim rules must be created:

- Active Directory user SID
- Active Directory group SID
- Active Directory UPN

To add the required claims:

1. Open the Server Manager, click Tools, and then click AD FS Management.

2. In the left pane, click AD FS, expand Trust Relationships, and then click Relying Party Trusts.
3. Right-click **Outlook Web App trust** and select **Edit Claim Rules** from the menu.

4. On the **Edit Claim Rules** window, click the **Issuance Transform Rules** tab, and then click **Add Rule** to start the Add Transform Claim Rule Wizard.
5. On the Select Rule Template window, under Claim rule template, select Send Claims Using a Custom Rule from the list, and then click Next.

![Select Rule Template Wizard](image)

6. On the Configure Rule window, in the Choose Rule Type step, under Claim rule name, enter the name for the claim rule. Use a descriptive name for the claim rule, for example, `ActiveDirectoryUserSID`. Under Custom rule, enter the following claim rule syntax language:

```plaintext
```
7. On the **Configure Rule** window, click **Finish**.

8. On the **Edit Claim Rules** window, click **Add Rule** on the **Issuance Transform Rules** tab to start the Add Transform Claim Rule Wizard.

9. On the **Select Rule Template** window, under **Claim rule template**, select **Send Claims Using a Custom Rule** from list, and then click **Next**.

10. On the **Configure Rule** window, under **Claim rule name**, enter the claim rule name. Use a descriptive name for the claim rule, for example, **ActiveDirectoryGroupSID**.
11. Under **Custom rule**, enter the following claim rule syntax language:

```plaintext
[c: [Type ==
  Issuer == "AD AUTHORITY"]
=> issue(store = "Active Directory", types =
  ["http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid"], query =
  ";tokenGroups(SID);{0}"
  param = c.Value);
```

12. On the **Configure Rule** window, click **Finish**.
13. In the **Edit Claim Rules** window, click **Add Rule** on the **Issuance Transform Rules** tab to start the Add Transform Claim Rule Wizard.

![Edit Claim Rules window](image)

14. On the **Select Rule Template** window, under **Claim rule template**, select **Send Claims Using a Custom Rule** from the list. Click **Next**.

![Select Rule Template window](image)

15. On the **Configure Rule** window, under **Claim rule name**, enter a descriptive name for the claim rule, for example, **ActiveDirectoryUPN**.
16. Under **Custom rule**, enter the following claim rule syntax language:

```c
[Type ==
Issuer == "AD AUTHORITY"]
=> issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
"{userPrincipalName;0}", param = c.Value);
```

17. Click **Finish**.

18. On the **Edit Claim Rules** window, click **Apply**, and then **OK**.
Verifying AD FS Authentication with Outlook Web App

To test the AD FS claims for Outlook Web App:

1. Open a browser and browse to the Outlook Web App (https://iis.integ.com/owa).

2. Enter a valid user name (domain\user) and password, and then click Sign in. The Outlook Web App opens.
To test the AD FS claims for Exchange Administrator Console (EAC):

3. Open a browser and browse to the EAC with Administrator account (https://iis.integ.com/ecp).

To test the AD FS claims for Exchange Administrator Console (EAC):

3. Open a browser and browse to the EAC with Administrator account (https://iis.integ.com/ecp).

4. Enter a valid user name (domain\user) and password, and then click Sign in. The Exchange admin center opens.
Configuring Gemalto SafeNet SAS AD FS Agent

1. Run the Gemalto SafeNet SAS AD FS agent.
2. On the Policy tab, verify that the Enable Agent check box is selected and Push Challenge option is checked.

![SAS MFA Plug-In Manager](image)

3. On the Communications tab, in the Primary Server box, enter the SAS server IP address or name (and port if non-causal is used). Also, ensure that Strip realm from UPN is checked.

   In case your SafeNet Authentication Service server is not installed on same machine as the AD and AD FS, encryption key file needs to be downloaded (as explained in Configuring the SafeNet Authentication Service Auth Node and Downloading the Encryption Key, page 34).

![SAS MFA Plug-In Manager](image)
4. Click Apply. Enabling the agent registers the SafeNet multi-factor authentication (MFA) adapter with AD FS and enables it at a global policy level.

5. You can verify your settings by testing authentication from the agent to the authentication server. To do so, under Authentication Test, enter your user name and passcode, and then click the Test button. The result of the test will be displayed in the Authentication Test Result field.

6. Click OK when finished.

**Configuring AD FS Authentication Policy**

1. On the AD FS Management Console, in the left pane, under AD FS, click Authentication Policies. Then, in the right pane, click Edit Global Primary Authentication.

2. On the Edit Global Authentication Policy window, on the Primary tab, ensure that Forms Authentication is selected for both Extranet and Intranet.
3. Click the **Multi-factor** tab, and then perform the following steps:
   a. Under **Users/Groups**, add the users and/or groups for which MFA will be required.
   b. Select **Extranet** and/or **Intranet**, according to your preferred configuration.
   c. Ensure that **SafeNet Multi Factor Authentication (SMFA)** is selected as an additional authentication method.
   d. Click **OK**.
Edit Global Authentication Policy

**Primary**

Configure multi-factor authentication (MFA) settings.

**Users/Groups**

MFA is required for the following users and groups:

- SAFENETDEMOS\Domain Users

**Devices**

MFA is required for the following devices:

- [ ] Unregistered devices
- [ ] Registered devices

**Locations**

MFA is required when accessing applications from the following locations:

- [x] Extranet
- [x] Intranet

Select additional authentication methods. You must select at least one of the following methods to enable MFA:

- [ ] Certificate Authentication
- [x] SafeNet Multi Factor Authentication (SMFA)

What is multi-factor authentication?
Configuring AD FS 3.0 as Primary Authentication Method for Microsoft Outlook Web App (using WAP)

In order to configure AD FS as a primary authentication method for Microsoft Outlook Web App, perform the following steps:

2. Configuring Exchange 2013 SP1 to use only AD FS authentication.
3. Enabling AD FS authentication on the OWA and ECP virtual directories.
4. Restarting the Internet Information Service (IIS).

Publishing the Outlook Web App and EAC using Web Application Proxy

After creating claims for Outlook Web App and EAC, the next step would be to publish both of these applications. Before doing so, verify that the OWA and EAC relying party trusts were created and ensure that you have a valid certificate on the Web Application Proxy server, which is suitable for Outlook Web App and EAC.

To publish Outlook Web App and EAC using Web Application Proxy:

2. In the Configuration pane, click Web Application Proxy, and then in the Tasks pane, click Publish.
3. On the **Welcome** window, click **Next**.

![Welcome window](image)

4. On the **Preauthentication** window, click **Active Directory Federation Services (AD FS)**, and then click **Next**.

![Preauthentication window](image)
5. On the **Relying Party** window, in the list of relying parties, select the relying party for the application that you want to publish (use the same relying party created in “Creating a Relying Party Trust for Outlook Web App and EAC”; for example, http://exchange.integ.com/owa), and then click **Next**.

![Relying Party window](image)

6. On the **Publishing Settings** window, complete the following fields, and then click **Next**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a friendly name for the application. This name is used only in the list of published applications in the <strong>Remote Access Management</strong> console. You can use OWA and EAC for the names.</td>
</tr>
<tr>
<td><strong>External URL</strong></td>
<td>Enter the external URL for this application; for example, <a href="http://exchange.integ.com/owa">http://exchange.integ.com/owa</a> for Outlook Web App and <a href="http://exchange.integ.com/ecd">http://exchange.integ.com/ecd</a> for EAC.</td>
</tr>
<tr>
<td><strong>External certificate</strong></td>
<td>Select a certificate whose subject name matches the host name of the external URL.</td>
</tr>
<tr>
<td><strong>Backend server URL</strong></td>
<td>Enter the URL of the back-end server. Note that this value is automatically entered when you enter the external URL, and you should change it only if the back-end server URL is different; for example, <a href="http://exchange.integ.com/owa">http://exchange.integ.com/owa</a> for Outlook Web App and <a href="http://exchange.integ.com/ecd">http://exchange.integ.com/ecd</a> for EAC.</td>
</tr>
</tbody>
</table>
7. On the **Confirmation** window, review the settings, and then click **Publish**. You can copy the Windows PowerShell command to set up additional published applications.

8. On the **Results** window, ensure the application was published successfully, and then click **Close**.

9. Follow steps 1-6 to publish the EAC. When publishing the EAC, change the following:
   - Name
   - External URL
   - External certificate
   - Back-end URL (https://exchange.integ.com/ecp)
10. From the Remote Access Management Console, both the OWA and EAC applications will be added to the table.

![Remote Access Management Console](image)

**Configuring Exchange 2013 SP1 to use Only AD FS Authentication**

When you are configuring AD FS to be used for claims-based authentication with Outlook Web App and EAC in Exchange 2013 SP1, you must enable AD FS for your Exchange organization.

Use the `Set-OrganizationConfig` cmdlet to configure AD FS settings for your organization:

- Set the AD FS issuer to `https://<ADFS machine>/adfs/ls`.
- Set the AD FS URIs to `https://<Exchange machine>/owa` and `https://<Exchange machine>/ecp`.
- Find the AD FS token-signing certificate thumbprint by using Windows PowerShell on the AD FS server and entering `Get-AD FS Certificate -Certificate Enter "Token-signing"`. Assign the token-signing certificate thumbprint. If the AD FS token-signing certificate has expired, the thumbprint from the new AD FS token-signing certificate must be updated by using the `Set-OrganizationConfig` cmdlet.

Using the Exchange Management Shell ( ), enter the following code.

```powershell
$uris = @("https://<Exchange machine name>/owa","https://<Exchange machine name>/ecp")
```
For example:

```bash
Set-OrganizationConfig -AdfsIssuer "https://dc.integ.com/adfs/ls/
-AdfsAudienceUris $urlis -AdfsSignCertificateThumbprints
"88970C64278A15D642934DC2961D9CCA5E28DA6B"
```

### Enabling AD FS Authentication on the OWA and ECP Virtual Directories

To enable AD FS authentication on the OWA and ECP virtual directories:

1. For the OWA and ECP virtual directories, enable AD FS authentication as the only authentication method and disable all other forms of authentication.

   **NOTE:** Configure the ECP virtual directory before you configure the OWA virtual directory.

2. Configure the ECP virtual directory by using the Exchange Management Shell. In the Shell window, enter the following code:

   ```bash
   ```

3. Configure the OWA virtual directory by using the Exchange Management Shell. In the Shell window, enter the following code:

   ```bash
   ```

### Restarting the Internet Information Service (IIS)

After completing all required steps, as well as making changes to Exchange virtual directories, Internet Information Services must be restarted. To do this, use one of the following methods:

- **Using Windows PowerShell:** Run the following command:

  ```bash
  Restart-Service W3SVC,WAS -noforce
  ```

- **Using the command line:** Click **Start > Run**, enter **IISReset /noforce**, and then click **OK**.

- **Using Internet Information Servers (IIS) Manager:** Click **Server Manager > IIS > Tools**, and then click **Internet Information Services (IIS) Manager**. On the **Internet Information Services (IIS) Manager** window, in the action pane under **Manage Server**, click **Restart**.
Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with Microsoft Outlook Web App using SAML authentication requires:

- Creating Users Stores in SafeNet Authentication Service, page 33
- Assigning an Authenticator in SafeNet Authentication Service, page 33
- Configuring the SafeNet Authentication Service Auth Node and Downloading the Encryption Key, page 34

Creating Users Stores in SafeNet Authentication Service

Before SafeNet Authentication Service can authenticate any user in your organization, you need to create a user store in SafeNet Authentication Service (SAS) that reflects the users that would need to use multi-factor authentication. User records are created in the SAS user store using one of the following methods:

- Manually, one user at a time, using the Create User shortcut
- Manually, by importing one or more user records via a flat file
- Automatically, by synchronizing with your Active Directory / LDAP server using the SAS Synchronization Agent

For additional details on importing users to SafeNet Authentication Service, refer to “Creating Users” in the SafeNet Authentication Service Subscriber Account Operator Guide:


All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.

Assigning an Authenticator in SafeNet Authentication Service

SafeNet Authentication Service (SAS) supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through Microsoft Outlook Web App.

The following authenticators are supported:

- eToken PASS
- RB-1 keypad token
- KT-4 token
- SafeNet GOLD
- SMS tokens
- MP-1 software token
- GrIDsure
- MobilePASS
Authenticators can be assigned to users in two ways:

- **Manual provisioning**—Assign an authenticator to users one at a time.
- **Provisioning rules**—The administrator can set provisioning rules in SAS so that the rules will be triggered when group memberships and other user attributes change. An authenticator will be assigned automatically to the user.

Refer to “Provisioning Rules” in the *SafeNet Authentication Service Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SAS user store.


**Configuring the SafeNet Authentication Service Auth Node and Downloading the Encryption Key**

In the event that the SafeNet Authentication Service server is not installed on the same machine as AD and AD FS, the following steps must be performed:

1. Log in to the SafeNet Authentication Service console as the account operator.
2. Click **Virtual Servers > Comms > Authentication Processing**.
3. Click the **Authentication Agent Settings** link, and then select **Download** to download the encryption key file. This file will be needed in step 4 of Configuring Gemalto SafeNet SAS AD FS Agent on page 23.

4. Click **Virtual Servers > Comms > Auth Nodes**.
5. Click the **Auth Nodes** link and select **Add**. Complete the **Auth Notes** tab as follows:

<table>
<thead>
<tr>
<th>Agent Description</th>
<th>Type a description for this node (for example, DC).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Type a host name.</td>
</tr>
</tbody>
</table>
### Low IP Address In Range
Type the low IP address.

### High IP Address In Range
Type the high IP address. (The low and high IP addresses may be the same since the node is referencing a single machine.)

### Exclude from PIN change requests
Do not select this check box.

---

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Nodes</td>
<td>Create and configure SafeNet Authentication Service Authentication Nodes</td>
</tr>
</tbody>
</table>

---

**Auth Nodes**

Using the RADIUS protocol over the Internet provides limited security of the traffic between the organization’s data center and the authentication service. For improved security and for alternatives to RADIUS traffic, refer to the recommendations included in the SafeNet Authentication Service Administrator Guide.

<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
<th>Host Name</th>
<th>IP Address</th>
<th>Auth</th>
<th>Sync/Reauthentication</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ADPS</td>
<td>64.94.215.91</td>
<td>64.94.215.91</td>
<td>Fails</td>
<td>Edit</td>
<td>Remove</td>
</tr>
<tr>
<td>2</td>
<td>WAP server</td>
<td>64.94.215.92</td>
<td>64.94.215.92</td>
<td>Fails</td>
<td>Edit</td>
<td>Remove</td>
</tr>
</tbody>
</table>
Running the Solution

After WAP is configured to use SafeNet Authentication Service as its identity provider (through AD FS), and SafeNet Authentication Service is configured to use AD FS as a SAML service provider, users can log in to Exchange 2013 SP1 through Outlook Web App using multi-factor authentication with SafeNet OTP authenticators.

**NOTE:** The AD FS server and the SAS server time should be NTP synchronized, as a difference in time of more than two (2) seconds will cause a failure.

1. Bob browses to https://<Exchange server name>/OWA.
2. He is redirected to his organization’s AD FS login window.

![Login window](image)
3. Bob enters his AD credentials.

4. After successful login, The SafeNet Authentication Service login window is displayed.

```
Welcome INTEG\Bob
For security reasons, we require additional information to verify your account.
```

5. Bob enters his SafeNet Authentication Service credentials and then clicks **Submit**.

6. After successful login, Bob is redirected to his organization’s Exchange server (OWA).
# Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

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