SafeNet Authentication Service
Integration Guide
Using SafeNet Authentication Service as an Identity Provider for Microsoft SharePoint
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: 007-013637-001, Rev. A
Release Date: November 2016
## Contents

Third-Party Software Acknowledgement ................................................................. 4
Description ................................................................................................................. 4
Applicability ................................................................................................................. 4
Environment .................................................................................................................. 4
Audience ....................................................................................................................... 5

SAS Authentication API Authentication using SafeNet Authentication Service Cloud ............ 5
SAS Authentication API using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE ................................................................. 5
SafeNet Authentication Service Authentication API Flow using SAS ............................... 5

Configuring Microsoft SharePoint ................................................................................ 6
  Configuring AD FS for a Relying Party ................................................................. 6
  Configuring the AD FS Claim Rule ......................................................................... 13
  Exporting the AD FS Token Signing Certificate ...................................................... 14
  Importing the Token Signing Certificate Using Windows PowerShell ...................... 14
  Defining a Unique Identifier for Claims Mapping using Windows PowerShell ............. 19
  Creating a New Authentication Provider in SharePoint ........................................... 19
  Associating a New Web Application with the AD FS Identity Provider ....................... 20
  Configuring Permissions to Access the Web Application .......................................... 24
  Sharing the Web Application with Users ............................................................... 28

Configuring Web Application Proxy with SharePoint ............................................... 30
Configuring Gemalto SafeNet SAS AD FS Agent ....................................................... 34
  Configuring AD FS Authentication Policy ............................................................. 35

Configuring SafeNet Authentication Service ............................................................. 37
  Creating Users Stores in SafeNet Authentication Service ......................................... 38
  Assigning an Authenticator in SafeNet Authentication Service ................................. 38
    Configuring the SafeNet Authentication Service Auth Node and Downloading the Encryption Key ................................. 39

Running the Solution ................................................................................................. 40
Support Contacts ....................................................................................................... 42
Third-Party Software Acknowledgement

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

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 (SAS) 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.

SharePoint is a web application that integrates with Microsoft Office. Organizations use SharePoint to create websites. You can use it as a secure place to store, organize, share, and access information from almost any device. All you need is a web browser, such as Internet Explorer, Chrome, or Firefox.

This document describes how to:

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

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

Microsoft SharePoint 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 SharePoint—Version 2013 SP1 and Version 2016
Audience

This document is targeted to system administrators who are familiar with Microsoft SharePoint, 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 SharePoint.

1. A user attempts to sign in to Microsoft SharePoint. The user is redirected to the 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 authentication. 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 SharePoint, accepting or rejecting the user’s authentication request.

4. The user is granted or denied access to Microsoft SharePoint.

Configuring Microsoft SharePoint

In order to configure a web-application or a website with AD FS authentication ensure that the SSL web-application or website and its certificate must be valid.

Configuring SharePoint to authenticate with AD FS requires:

- Configuring AD FS for a Relying Party, page 6
- Configuring the AD FS Claim Rule, page 13
- Exporting the AD FS Token Signing Certificate, page 14
- Importing the Token Signing Certificate Using Windows PowerShell, page 18
- Defining a Unique Identifier for Claims Mapping using Windows PowerShell, page 19
- Creating a New Authentication Provider in SharePoint, page 19
- Associating a New Web Application with the AD FS Identity Provider, page 20
- Configuring Permissions to Access the Web Application, page 24
- Sharing the Web Application with Users, page 28

Configuring AD FS for a Relying Party

The relying party defines how the AD FS recognizes the relying party application and issues claims to it.

1. Verify that the user account that is performing this procedure is a member of the Administrators group on the local computer.

2. On the AD FS server, open the Active Directory Federation Services (AD FS) Management console.
3. In the left pane, expand **Trust Relationships**, and then double-click **Relying Party Trusts**.

4. In the right pane, click **Add Relying Party Trust**.

5. On **Add Relying Party Trust Wizard**, click **Start**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
6. In the right pane, select the **Enter data about the relying party manually** option, and then click **Next**.

![Image of Add Relying Party Trust Wizard](image1.png)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

7. In the **Display name** field, enter a display name for the relying party, and then click **Next**.

![Image of Specify Display Name](image2.png)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
8. Ensure that the **AD FS Profile** option is selected, and then click **Next**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

9. Do not specify an encryption certificate. Click **Next**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
10. Select **Enable support for the WS-Federation Passive protocol**. In the **Relying party WS-Federation Passive protocol URL** field, enter `<name of the web application URL>/_trust/` (for example, https://app1.safenetdemos.com/_trust/), and then click **Next**.

   ![Configure URL](image1.png)

   *(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

11. In the **Relying party trust identifier** field, enter the name of the relying party trust identifier (for example, urn:sharepoint:SP2013), and then click **Add**.

   ![Configure Identifiers](image2.png)

   *(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
12. Click **Next**.

13. Select **I do not want to configure mult-factor authentication settings for this relying party trust at this time**, and then click **Next**.

![Add Relying Party Trust Wizard](image-url)

*The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.*
14. Click **Next**.

![Add Relying Party Trust Wizard](image1.jpg)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

15. Click **Close**. The Rules Editor Management console is displayed.

![Add Relying Party Trust Wizard](image2.jpg)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

Use the Rules Editor Management console and the next procedure to configure the mapping of claims from your chosen directory source to SharePoint 2013.
Configuring the AD FS Claim Rule

In this section, you will configure to send values of a Lightweight Directory Access Protocol (LDAP) attribute as claims and specify how the attributes will be mapped to the outgoing claim type.


2. On Add Transform Claim Rule Wizard, under Select Rule Template, in the right pane, in the Claim rule template field, select Send LDAP Attributes as Claims, and then click Next.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
3. Under Configure Rule, perform the following steps:
   a. In the Claim rule name field, enter a name for the claim rule.
   b. In the Attribute store field, select Active Directory.
   c. Under Mapping of LDAP attributes to outgoing claim type, perform the following steps:
      - In the first row, under LDAP Attribute, select E-Mail-Addresses, and then under Outgoing Claim Type, select E-Mail Address.
      - In the second row, under LDAP Attribute, select User-Principal-Name, and then Under Outgoing Claim Type, select UPN.

![Configure Rule](image.png)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

d. Click Finish, and then click OK.

**Exporting the AD FS Token Signing Certificate**

Export the token signing certificate of the AD FS server with which you want to establish a trust relationship, and then copy the certificate to a location that SharePoint 2013 can access.

1. On the AD FS server, open the Active Directory Federation Services (AD FS) Management console.
2. In the left pane, click **Service > Certificates**, and then in the middle pane, under **Token-signing**, double click on the primary token certificate

![Certificate Management Screen](image1.png)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

3. In the right pane, click **View Certificate**. The certificate is displayed.

![Certificate Information](image2.png)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
4. On the **Details** tab, click **Copy to File**.

![Certificate Export Wizard](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

5. On **Certificate Export Wizard**, under **Welcome to the Certificate Export Wizard**, click **Next**.

![Certificate Export Wizard](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
6. Under **Export File Format**, select the **DER encoded binary X.509 (.CER)** format, and then click **Next**.

7. Under **File to Export**, click **Browse** to search for and select the file (for example, C:\ADFS.cer) that you want to export, and then click **Next**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
8. Under **Completing the Certificate Export Wizard**, click **Finish**.

![Certificate Export Wizard](image)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

**Importing the Token Signing Certificate Using Windows PowerShell**

Import the token signing certificates to the trusted root authority list that resides on the SharePoint Server. This step must be repeated for every token signing certificate in the chain until the root certification authority is reached.

1. Verify that you have the following memberships:
   - `securityadmin` fixed server role on the SQL Server instance.
   - `db_owner` fixed database role on all databases that are to be updated.
   - Administrators group on the server on which you are running the Windows PowerShell cmdlets.
   - Add memberships that are required beyond the minimums above.

   An administrator can use the `Add-SPShellAdmin` cmdlet to grant permissions to use SharePoint 2013 Products cmdlets.

2. Start the SharePoint 2013 Management Shell. On the **Start** screen, click **SharePoint 2013 Management Shell**.

3. On the Windows PowerShell command prompt, use the following syntax to import the parent certificate of the token signing certificate (that is, the root authority certificate).

   ```powershell
   New-SPTrustedRootAuthority -Name "Token Signing Cert Parent" -Certificate $root
   ```
4. Use the following syntax to import the token signing certificate that was copied from the AD FS server.

```powershell
New-SPTrustedRootAuthority -Name "Token Signing Cert" -Certificate $cert
```

**Defining a Unique Identifier for Claims Mapping using Windows PowerShell**

1. On the Windows PowerShell command prompt, use the following syntax to create the email address claim mapping.

```powershell
$emailClaimMap = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress" -IncomingClaimTypeDisplayName "EmailAddress" -SameAsIncoming
```

2. Use the following syntax to create the UPN claim mapping.

```powershell
$upnClaimMap = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn" -IncomingClaimTypeDisplayName "UPN" -SameAsIncoming
```

3. Use the following syntax to create the role claim mapping.

```powershell
$roleClaimMap = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.microsoft.com/ws/2008/06/identity/claims/role" -IncomingClaimTypeDisplayName "Role" -SameAsIncoming
```

4. Use the following syntax to create the Primary SID claim mapping.

```powershell
$sidClaimMap = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid" -IncomingClaimTypeDisplayName "SID" -SameAsIncoming
```

**Creating a New Authentication Provider in SharePoint**

Create an SPTrustedIdentityTokenIssuer. On the Windows PowerShell command prompt, use the following syntax to create a new authentication provider. Use the same name that you have used for relying party trust identifier in AD FS (refer to “Configuring AD FS for a Relying Party” on page 6).

```powershell
$realm = "urn:sharepoint:<WebAppName>"
For Example - "urn:sharepoint:Sharepoint2013"

$signInURL = https://<YourADFSServerName>/adfs/ls
For Example - https://ADFS.SafeNetDemos.com/adfs/ls
```
Associating a New Web Application with the AD FS Identity Provider

In this section, configure a new web application to use AD FS sign-in.

1. Verify that the user account used to perform this procedure is a member of the Farm Administrators SharePoint group.

2. On the home page, in the left pane, under Central Administration, click Application Management.

```powershell
$ap = New-SPTrustedIdentityTokenIssuer -Name <ProviderName> -Description <ProviderDescription> -realm $realm -ImportTrustCertificate $cert -ClaimsMappings $emailClaimMap,$upnClaimMap,$roleClaimMap,$sidClaimMap -SignInUrl $signInURL -IdentifierClaim $emailClaimmap.InputClaimType

For Example - New-SPTrustedIdentityTokenIssuer -Name ADFS -Description “ADFS Authentication” -realm $realm -ImportTrustCertificate $cert -ClaimsMappings $emailClaimMap,$upnClaimMap,$roleClaimMap,$sidClaimMap -SignInUrl $signInURL -IdentifierClaim $emailClaimmap.InputClaimType
```
3. In the right pane, Under Application Management, under Web Applications, click Manage web applications.

4. Select the appropriate web application, and then click Extend.
5. On the **Extend Web application to Another IIS Web Site** window, select the **Create a new IIS web site** option, and then perform the following steps:

a. Complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the IIS web site.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Enter a port number (for example, <strong>443</strong>).</td>
</tr>
<tr>
<td><strong>Use Secure Socket Layer</strong></td>
<td>Select <strong>Yes</strong>.</td>
</tr>
</tbody>
</table>

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
b. Ensure that **Trusted Identity Provider** is selected and the ADFS identity provider is also selected.

**NOTE:** If you want only the AD FS authentication screen, ensure that **Enable Windows Authentication** is not selected. For first test, it should be left as default.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

c. In the **URL** field, modify the URL as per your preferred configuration, and then in the **Zone** field, select your zone (for example, **Extranet**).

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

d. Click **OK**.
Configuring Permissions to Access the Web Application

Configure the web application for permissions based on email addresses.

1. On the home page, in the left pane, under **Central Administration**, click **Application Management**.

2. In the right pane, under **Application Management**, under **Web Applications**, click **Manage web applications**.
3. Select the appropriate web application, and then click **User Policy**.

![SharePoint Central Administration](image1)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

4. On the **Policy for Web Application** window, click **Add Users**.

![Policy for Web Application](image2)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
5. On the **Add Users** window, in the **Zone** field, select your zone, and then click **Next**.

   (The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

6. Click the **Browse** icon in the lower-right corner of the **Users** box.

   (The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
7. On the **Select People and Groups** window, perform the following steps:
   a. In the **Find** field, enter the email address of a user account, and then click the **Search** icon.
   b. Under **All Search Results**, under the name of your AD FS identity provider, click **EmailAddress**.
   c. In the right pane, in the **Display Name** column, select the email address of the user.
   d. Click **Add**
   e. Click **OK**.

![Select People and Groups window](image)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

8. On the **Add Users** window, under **Permissions**, select the level of permissions as per your preferred configuration.

![Add Users window](image)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
9. Repeat steps 6 to 9 for additional email addresses of users with the same level of permissions.
10. Click Finish.
11. Click OK.

Sharing the Web Application with Users

1. Log in to the web application with as an administrator.
2. On the web application console, in the right pane, in the upper right corner, click the Site Settings () icon.

![Site Settings](image)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

3. On the Site Settings window, in the right pane, under Users and Permissions, click People and groups.

![People and groups](image)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
4. On **People and Groups > My SharePoint Members**, in the right pane, click **New > Add Users**.

![Image of SharePoint interface](image1.png)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

5. On the **Share ‘MySharePoint’** window, in the **Add people to the MySharePoint Members group** field, enter the user email address to search for the user’s UPN. After the user’s UPN is found, click **Share**.

![Image of SharePoint interface](image2.png)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

The user is added to the **People and Groups** list.

![Image of SharePoint interface](image3.png)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
Configuring Web Application Proxy with SharePoint

In order to configure WAP to work with SharePoint web application, we need to publish it through the Remote Access Management Console. Afterwards, the WAP will forward all requests to SharePoint to authenticate first by AD FS and only after successful authentication the user will login to SharePoint.


2. On the Publish New Application Wizard, on the Welcome window, click Next.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
3. On the **Preauthentication** window, select the **Active Directory Federation Services (AD FS)** option, and then click **Next**.

4. On the **Relying Party** window, under **Name**, select the relying party (for example, **SharePoint 2013**) configured in AD FS (refer to step 7 of “Configuring AD FS for a Relying Party” on page 6), and then click **Next**.
5. 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>Name</td>
<td>Enter a name for the web application (for example, <strong>SharePoint 2013</strong>).</td>
</tr>
<tr>
<td>External URL</td>
<td>Enter the web application URL.</td>
</tr>
<tr>
<td>External certificate</td>
<td>Select the public certificate as per your preferred configuration.</td>
</tr>
<tr>
<td>Backend server URL</td>
<td>Enter the web application internal URL (it may be same as the external URL).</td>
</tr>
</tbody>
</table>

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
6. On the **Confirmation** window, read the summary, and then click **Publish**.

![Publish New Application Wizard](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

7. A success message is displayed, click **Close**.

![Publish New Application Wizard](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
The Web Application is published in WAP and it will be available from the external network.

![Configuration screenshot](image1)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

## 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.
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 39).

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**.

### Configuring SafeNet Authentication Service

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

- Creating Users Stores in SafeNet Authentication Service, page 38
- Assigning an Authenticator in SafeNet Authentication Service, page 38
- Configuring the SafeNet Authentication Service Auth Node and Downloading the Encryption Key, page 39
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 SharePoint.

The following authenticators are supported:

- eToken PASS
- RB-1 keypad token
- KT-4 token
- SafeNet GOLD
- SMS tokens
- MP-1 software token
- GrlDsure
- 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 34.

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>
<tr>
<td>Low IP Address In Range</td>
<td>Type the low IP address.</td>
</tr>
<tr>
<td>High IP Address In Range</td>
<td>Type the high IP address. (The low and high IP addresses may be the same since the node is referencing a single machine.)</td>
</tr>
</tbody>
</table>
Exclude from PIN change requests

Do not select this check box.

Running the Solution

1. In a web browser, open the configured web application.
2. You will be redirected to your organization’s login page. Enter your organizational user name and password, and then click Sign in.
3. After successful login, the SafeNet Authentication Service (SAS) login page is displayed. Enter your SAS credentials (PIN+OTP), and then click Submit.

After successful authentication, you will be able to access the SharePoint Web Application.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
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>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>Gemalto</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland  21017 USA</td>
</tr>
<tr>
<td><strong>Phone</strong></td>
<td>United States</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td><strong>Technical Support</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td><strong>Customer Portal</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>