Microsoft Office 365 Using SAML Integration Guide

Revision A
Contacting SafeNet

We work closely with our reseller partners to offer the best worldwide technical support services. Your reseller is the first line of support when you have questions about products and services. However, if you require additional assistance you can contact the SafeNet technical support team help-desk which is available 24 hours a day, seven days a week:

<table>
<thead>
<tr>
<th>Country/Region</th>
<th>Telephone</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>+1-800-545-6608</td>
</tr>
<tr>
<td>International</td>
<td>+1-410-931-7520</td>
</tr>
</tbody>
</table>

For further assistance submit additional questions to the SafeNet technical support team at the following web page:

http://c3.safenet-inc.com/secure.asp

For assistance via email to SafeNet technical support send the request to the following address:

support@safenet-inc.com
# Table of Contents

About This Guide ........................................................................................................................................... 4

Intended Audience ......................................................................................................................................... 4
Additional Information ................................................................................................................................. 4
Software Requirements ............................................................................................................................... 4

Overview .......................................................................................................................................................... 5

Introduction .................................................................................................................................................... 5
SAML ............................................................................................................................................................... 5
Authentication Flow for this Solution ........................................................................................................ 6

AD FS Configuration ..................................................................................................................................... 7

Defining SAM as an Identity Provider in AD FS 2.0 ................................................................................... 7
Setting the Identity Provider’s Hash Algorithm ........................................................................................... 13
Configuring the Identity Provider’s Claim Rule ......................................................................................... 14
Configuring the Microsoft Office 365 Claim Rule .................................................................................... 16
Setting the FS Application Protocol ........................................................................................................ 18

SAM Portal Configuration .......................................................................................................................... 20

Running the Solution ................................................................................................................................. 23

Troubleshooting ........................................................................................................................................... 29
About This Guide

The goal of this document is to provide guidance for setting up and managing SafeNet’s authentication solutions in a Microsoft Office 365 environment using SAML 2.0.

In this document, Microsoft Office 365 is configured for Single Sign On (SSO) against an on-premise AD FS 2.0 service with reliance on SafeNet Authentication Manager for strong authentication.

Intended Audience

The guide is intended for Information Technology professionals responsible for the organization’s network security.

Additional Information

For a detailed explanation of SafeNet Authentication Manager (SAM) 8.0 SP4 and the other infrastructure components involved in this solution, or any other SafeNet products mentioned in this guide, refer to SafeNet’s product documentation.

For additional information on Microsoft or Office 365 software and hardware components mentioned in this guide, refer to the manufacturer’s documentation.

Software Requirements

For this scenario, the working environment must include the following software:

- *Microsoft Office 365* account
- *Microsoft Active Directory Federation Services (AD FS) 2.0*
- *SafeNet Authentication Manager 8.0 SP4 or later*
Overview

Introduction

This guide describes the process for enabling strong authentication using SafeNet Authentication Manager (SAM) with Microsoft Office 365. This document assumes that the Microsoft Office 365 with Microsoft Active Directory Federation Services (AD FS) 2.0 environment is already configured.

SAML

Security Assertion Markup Language (SAML) 2.0 is a standard for exchanging authentication and authorization data between security domains.

SAML 2.0 is an XML-based protocol that uses security tokens (information packets) containing assertions to pass information about a principal (usually an end-user) between an Identity Provider (IdP) and a web service. SAML 2.0 enables web-based scenarios including single sign-on (SSO) authentication.

The SafeNet Authentication Manager (SAM) authentication portal uses SAML 2.0 to communicate with Microsoft AD FS 2.0. AD FS 2.0 uses WS-security to communicate with Microsoft Office 365.
Authentication Flow for this Solution

The figure describes the following SAML scenario:

a. Sarah, a user, enters her logon credentials to Microsoft Office 365, and selects SafeNet Authentication Manager (SAM) as her Identity Provider for authentication.
b. AD FS passes authentication authority to the SAM authentication server.
c. The SAM authentication portal prompts Sarah for her SAM logon credentials.
d. SAM verifies Sarah’s credentials, and provides an accept/reject authentication assertion to Microsoft Office 365.
e. Sarah is logged on to Microsoft Office 365.
AD FS Configuration

Perform the following steps to configure AD FS for this solution:

- Defining SAM as an Identity Provider in AD FS 2.0; see page 7
- Setting the Identity Provider’s Hash Algorithm; see page 13
- Configuring the Identity Provider’s Claim Rule; see page 14
- Configuring the Microsoft Office 365 Claim Rule; see page 16
- Setting the FS Application Protocol; see page 18

Defining SAM as an Identity Provider in AD FS 2.0

Using the AD FS 2.0 management console, define SafeNet Authentication Manager as an Identity Provider by adding it to the Claims Provider Trusts list.

To define SAM as an Identity Provider in AD FS 2.0:

1. In the AD FS 2.0 management console, expand the tree in the left panel to **AD FS 2.0 > Trust Relationships**.

2. Right-click **Claims Provider Trusts**, and from the drop-down menu, select **Add Claims Provider Trust**.
The Add Claims Provider Trust Wizard opens to the Welcome window.

3. Click **Start**.

The Select Data Source window opens.

4. Select **Enter claims provider trust data manually**, and click **Next**.
The Specify Display Name window opens.

5. Enter a **Display name**, and click **Next**.
   In this example, the display name is **Portal**.

   The Choose Profile window opens.

6. Select **AD FS 2.0 profile**, and click **Next**.
The **Configure URL** window opens.

![Configure URL window](image)

7. Select **Enable support for the SAML 2.0 WebSSO protocol**.

8. Copy the following text to the **Claims provider WS-Federation Passive protocol URL** field, replacing `<SAM Server Name>` with the SAM server's domain name:

   ```
   https://<SAM Server Name>/samlcloud/default.aspx
   ```

   **Note**
   
   Ensure that the URL begins with **https**. This value will be used as the **SAM Issuer** value in step 7b on page 21 of **SAM Portal Configuration**.

9. Click **Next**.

   The **Configure Identifier** window opens, displaying the SAM portal URL that was entered in step 7.

![Configure Identifier window](image)

10. Click **Next**.
The Configure Certificates window opens.

11. Click Add to add the SAM portal certificate.

The Select a Token Signing Certificate window opens.

12. Browse to the location of the exported SafeNet portal certificate, and click Open.

Note
If the SafeNet portal certificate has not been exported, open the SAM Configuration Manager, go Action > Cloud Configuration, select the Info for Service Provider tab, and click Export Certificate.

See the SafeNet Authentication Manager 8.0 SP4 Administrator’s Guide for more information.
The certificate is added.

13. If the SAM server’s domain is different from the AD FS domain that is registered in Office 365, double-click the certificate icon, and install the certificate to the trusted root.

14. In the Configure Certificates window, click **Next**.

The **Ready to Add Trust** window opens.

15. Click **Next**, and click **Finish** to close the wizard.
In the AD FS 2.0 Management console, the new Identity Provider entry for SAM, named in step 5, is included in the Claims Provider Trusts list. In this example, the name assigned to the SAM Identity Provider is Portal.

Setting the Identity Provider’s Hash Algorithm

Define SHA-1 as the hash algorithm of the Identity Provider.

To set the hash algorithm:

1. In the AD FS 2.0 management console, expand the tree in the left panel to AD FS 2.0 > Trust Relationships, and select Claims Provider Trusts. The Claims Provider Trusts list is displayed in the middle panel.

2. Right-click the Identity Provider entry for SAM named in step 5 of Defining SAM as an Identity Provider in AD FS 2.0, and from the drop-down menu, select Properties. The Identity Provider’s Properties window opens.

3. Select the Advanced tab.

4. In the Secure hash algorithm drop-down menu, select SHA-1.
5. Click **Apply**, and click **OK**.

**Configuring the Identity Provider’s Claim Rule**

Configure a mapping rule for the Identity Provider.

**To configure the Identity Provider’s claim rule:**

1. In the *AD FS 2.0* management console, expand the tree in the left panel to *AD FS 2.0 > Trust Relationships*, and select *Claims Provider Trusts*.

   The *Claims Provider Trusts* list is displayed in the middle panel.

2. Right-click the Identity Provider entry for SAM named in step 5 of in *Defining SAM as an Identity Provider in AD FS 2.0*, and from the drop-down menu, select **Edit Claim Rules**.

   The Identity Provider’s *Edit Claim Rules* window opens.

3. Click **Add Rule**.
The Add Transform Claim Rule Wizard opens to the Select Rule Template window.

4. From the Claim rule template drop-down menu, select Transform an Incoming Claim, and click Next.

The Configure Rule window opens.

5. In the Claim rule name field, enter a name for the new rule.
   In this example, the rule name is Name ID to Windows account name.

6. Select the appropriate settings.
   In this example, we do the following:
   - In the Incoming claim type drop-down menu, select Name ID.
   - In the Incoming name ID format drop-down menu, select Unspecified.
   - In the Outgoing claim type drop-down menu, select Windows account name.
   - Select Pass through all claim values.

7. Click Finish.
A warning message may open confirming your intention to select **Pass through all claim values**.

8. Click **Yes** to close the warning message.

   In the *Edit Claim Rules* window, the rule named in step 5 is included in the *Rule Name* list. In this example, the rule name is *Name ID to Windows account name*.

---

**Configuring the Microsoft Office 365 Claim Rule**

Configure a custom rule for the Microsoft Office 365 Identity Platform.

**To configure a custom rule for the Microsoft Office 365 Identity Platform:**

1. In the *AD FS 2.0* Management console, expand the tree in the left panel to *AD FS 2.0 > Trust Relationships > Relying Party Trusts*.

   The *Relying Party Trusts* list is displayed in the middle panel.

2. In the middle panel, right-click **Microsoft Office 365 Identity Platform**, and from the drop-down menu, select **Edit Claim Rules**.
Microsoft Office 365’s *Edit Claim Rules* window opens, displaying two rules.

3. Select the first rule, and click **Edit Rule**.

   *The Edit Rule window opens.*

4. Do the following:
   - In the *Claim rule name* field, enter a name for the rule. In this example, the new rule name is *Custom Rule for Microsoft*.
   - In the *Custom Rule* box, delete the existing text, and then copy the following text, replacing `<AD FS Domain Name>` with the AD FS domain name that is registered in Office 365 for your installation.

```c
[Type ==
 ("http://schemas.xmlsoap.org/claims/UPN",
 "http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID")
 , query = "samAccountName=\{0\};userPrincipalName,objectGUID;<AD FS Domain Name>\{1\}", param = c.Value, param = c.Value);
```
Note
Ensure that the script is copied exactly as displayed above. Change only the `<AD FS Domain Name>` parameter.

5. Click **OK** to save the rule.

The new name of the rule is displayed.

6. Click **Apply**, and click **OK**.

Setting the FS Application Protocol

Ensure that the Federation Service’s Hypertext Transfer Protocol does not use SSL/TLS secure protocol.

To set the Federation Service’s application protocol:

1. In the *AD FS 2.0* management console, right-click **Service**, and from the drop-down menu, select **Edit Federation Service Properties**.

   The *Federation Service Properties* window opens.

2. In the *General* tab, change the protocol listed at the beginning of the *Federation Service identifier* field from **https** to **http**.
Note
You will need the information in this window for step 7 on page 21 in SAM Portal Configuration.
In this example, the Federation Service display name is dc.safenetdemos.com.

3. Click Apply, and click OK.
SAM Portal Configuration

SAM’s Token Policy Object (TPO) policies include Protected Application Settings. These settings are used by the SAM portals.

**Note**
See the SafeNet Authentication Manager 8.0 SP4 Administrator’s Guide for general portal configuration information.

**To configure the SAM portal for this solution:**

1. Open the Token Policy Object Editor for the appropriate group.  
   See the SafeNet Authentication Manager 8.0 SP4 Administrator’s Guide for more information.
   
   The Token Policy Object Editor window opens.

2. In the left pane, select **Protected Application Settings > User Authentication**.  
   Policies are displayed in the right pane.

3. In the right pane, double-click **Application Authentication Settings**.
   The Application Authentication Settings Properties window opens.
4. Select Define this policy setting, and select Enabled.

5. Click Definitions.

The Application Authentication Settings window opens.

6. In the left pane, select Application Authentication Settings > ADFS.

Policies are displayed in the right pane.

7. In the right pane, double-click the following policies, and enter the appropriate information:

   a. Application Issuer: Copy the Federation Service identifier value from the Federation Service Properties window, and then change the application protocol of the Application Issuer from http to https.

   Note
   The Federation Service identifier value is displayed in the General tab of the Federation Service Properties window.

   b. SAM Issuer: Copy the following text, replacing <SAM Server Name> with the SAM server’s domain name:

   https://<SAM Server Name>/samcloud/default.aspx

   Note
   This is the Claims provider WS-Federation Passive protocol URL value that was entered in step 8 on page 10 of Defining SAM as an Identity Provider in AD FS 2.0.
c. **Application’s login URL:** Copy the following text, replacing `<FS Name>` with the Federation Service’s display name:

```plaintext
https://<FS Name>/adfs/ls
```

In this example, the *Federation Service display name* is `dc.safenetdemos.com`.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>The <em>Federation Service display name</em> value is displayed in the <em>General</em> tab of the <em>Federation Service Properties</em> window.</td>
</tr>
</tbody>
</table>

d. **Audience URI:** Copy the value entered into **Application’s login URL**, in step 7c.

e. **User mapping:** Enter *AccountName*.

8. Ensure that at least one authentication type is enabled.

9. Click **OK** until all of the *TPO Editor* windows are closed.
Running the Solution

This section describes a typical user authentication scenario using the solution.

**How Sarah authenticates to Microsoft Office 365:**

1. Sarah opens a web browser and browses to *Microsoft Online Services*. The Microsoft Office 365 *sign in* window opens.
Sarah enters her account username including the domain name.

2. Sarah clicks the link that appears beneath the sign-in credentials: **Sign in at** <followed by the domain name>.

If more than one Identity Provider is available, Sarah is prompted to select one.
From the drop-down menu, Sarah selects the Identity Provider entry for SAM named in step 5 on page 9 of *Defining SAM as an Identity Provider in AD FS 2.0*. In this example, the name assigned to the SAM Identity Provider is *Portal*.

3. Sarah clicks **Continue to Sign In**.
   AD FS redirects the authentication request to the SAM Authentication Portal.
The Authentication Portal’s *User Identification* window opens.

4. Sarah enters her username, and clicks **OK**.
Sarah is prompted to enter the appropriate SAM credentials for the authentication method defined in the SAM TPO.

5. Sarah enters her SAM logon credentials, and clicks **Log on**.
A message is displayed informing Sarah that she has successfully logged on.
Sarah is authenticated to her Microsoft Office 365 account.
## Troubleshooting

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>An error message is displayed: “Your system configuration is incorrect. Contact your administrator.”</td>
<td>The <strong>Application Issuer</strong> in the TPO is incorrect.</td>
<td>Ensure that the correct <strong>Application Issuer</strong> is in the TPO setting.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See step 7a on page 21 of <strong>SAM Portal Configuration</strong>.</td>
</tr>
<tr>
<td>The SAM Authentication Portal does not open.</td>
<td>The URL entered is not correct.</td>
<td>Ensure that the user typed the correct URL.</td>
</tr>
<tr>
<td></td>
<td>The <strong>SAM Issuer</strong> in the TPO is incorrect.</td>
<td>Ensure that the correct <strong>SAM Issuer</strong> is in the TPO setting.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See step 7b on page 21 of <strong>SAM Portal Configuration</strong>.</td>
</tr>
<tr>
<td>After logon, an error message is displayed: “The page you requested could not be found”</td>
<td>The <strong>Application’s login URL</strong> in the TPO is incorrect.</td>
<td>Ensure that the correct <strong>Application’s login URL</strong> is in the TPO setting.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See step 7c on page 22 of <strong>SAM Portal Configuration</strong>.</td>
</tr>
<tr>
<td>After logon, an error message is displayed: “Schema validation failed for response. Audience must have TextContent”</td>
<td>The <strong>Audience URI</strong> in the TPO is not enabled or is empty.</td>
<td>Ensure that the correct <strong>Audience URI</strong> is in the TPO setting.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See step 7d on page 22 of <strong>SAM Portal Configuration</strong>.</td>
</tr>
<tr>
<td>Users cannot authenticate.</td>
<td>The <strong>User mapping</strong> in the TPO does not match the mapped value defined in the Microsoft Office 365 rule’s script.</td>
<td>Ensure that the rule’s script is exactly as instructed in step 4 on page 17 of <strong>Configuring the Microsoft Office 365 Claim Rule</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See step 7e on page 22 of <strong>SAM Portal Configuration</strong>.</td>
</tr>
<tr>
<td>Problem</td>
<td>Possible Cause</td>
<td>Solution</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-----------------------------------------------------</td>
<td>----------------------------------------------------------------</td>
</tr>
<tr>
<td>A log file must be created and sent to SafeNet technical support for debugging purposes.</td>
<td></td>
<td>To enable logging, run the following from the AD FS computer's command line: <code>wevtutil.exe sl “AD FS 2.0 Tracing/Debug” /l:5</code></td>
</tr>
<tr>
<td>Writing to a log file is no longer needed.</td>
<td></td>
<td>Disable logging from the Windows Event Viewer application.</td>
</tr>
</tbody>
</table>