SafeNet Authentication Manager
Integration Guide

Using SAM as an Identity Provider for Apache HTTP Server
## Contents

Third-Party Software Acknowledgement........................................................................................................................................4  
Description..................................................................................................................................................................................4  
Applicability..................................................................................................................................................................................4  
Environment..................................................................................................................................................................................4  
Audience.......................................................................................................................................................................................5  
SAML Authentication using SAM.......................................................................................................................................................5  
SAML Authentication Dataflow using SAM........................................................................................................................................5  
SAML Prerequisites.........................................................................................................................................................................5  
Configuring SafeNet Authentication Manager..............................................................................................................................6  
  Synchronizing User Stores to SafeNet Authentication Manager.................................................................................................6  
  Assigning a Token in SAM............................................................................................................................................................6  
  Configuring SAM as an Identity Provider.......................................................................................................................................7  
  Configuring SAM for SAML-based User Federation.....................................................................................................................9  
Configuring Apache HTTP Server....................................................................................................................................................12  
  Installing the Shibboleth Service Provider......................................................................................................................................12  
  Configuring the Shibboleth Service Provider..................................................................................................................................13  
Running the Solution.........................................................................................................................................................................14  
Support Contacts..............................................................................................................................................................................16
Third-Party Software Acknowledgement

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

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 Manager (SAM) is a versatile authentication solution that allows you to match the authentication method and form factor to your functional, security, and compliance requirements. Use this innovative management service to handle all authentication requests and to manage the token lifecycle.

Apache HTTP Server, also referred to as Apache, is the world’s most widely-used web server software. Apache is developed and maintained by an open community of developers under the auspices of the Apache Software Foundation. Most commonly used on a UNIX-like system, the software is available for a wide variety of operating systems, including UNIX, FreeBSD, Linux, Solaris, Novell NetWare, OS X, Microsoft Windows, OS/2, TPF, OpenVMS, and eComStation.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Apache HTTP Server using SafeNet tokens managed by SafeNet Authentication Manager.
- Configure SAML authentication in Apache HTTP Server using SafeNet Authentication Manager as an Identity Provider.

It is assumed that Apache HTTP Server environment is already configured and working prior to implementing multi-factor authentication using SafeNet Authentication Manager.

Apache HTTP Server 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 Manager.

Applicability

The information in this document applies to SafeNet Authentication Manager 8.2.

Environment

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

- **SafeNet Authentication Manager 8.2 HF 468**—A server version of SAM that is used to deploy the solution on-premises in an organization.
- **Apache HTTP Server**—version 2.2.15 on CentOS 6.3 (32-bit)
- **Shibboleth SP**—version 2.5.3 on CentOS 6.3 (32-bit)
Audience

This document is targeted to system administrators who are familiar with Apache HTTP Server and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Manager.

SAML Authentication using SAM

SAM provides a SAML authentication option that is already implemented in the SAM environment and can be used without any installation.

SAML Authentication Dataflow using SAM

SafeNet Authentication Manager communicates with a large number of Service Providers and cloud-based services solutions using the SAML protocol.

The image below describes the dataflow of a multi-factor authentication transaction for Apache HTTP Server.

1. A user attempts to log on to Apache HTTP Server. The user is redirected to SafeNet Authentication Manager (SAM). SAM collects and evaluates the user's credentials.
2. SAM returns a response to Apache HTTP Server, accepting or rejecting the user’s authentication request.

SAML Prerequisites

To enable SafeNet Authentication Manager to receive SAML authentication requests from Apache HTTP Server, ensure that end users can access websites hosted on Apache HTTP Server.
Configuring SafeNet Authentication Manager

The deployment of multi-factor authentication using SAM with the Apache HTTP Server using SAML authentication requires the following:

- Synchronizing User Stores to SafeNet Authentication Manager, page 6
- Assigning a Token in SAM, page 6
- Configuring SAM as an Identity Provider, page 7
- Configuring SAM for SAML-based User Federation, page 9

Synchronizing User Stores to SafeNet Authentication Manager

SAM manages and maintains token information in its data store, including the token status and the token assignment to users. For user information, SAM can be integrated with an external user store. During the design process, it is important to identify which user store the organization is using, such as Microsoft Active Directory.

If the organization is not using an external user store, SAM uses an internal (“stand-alone”) user store created and maintained by the SAM server.

SAM 8.2 supports the following external user stores:

- Novell eDirectory
- Microsoft ADAM/AD LDS
- OpenLDAP
- Microsoft SQL Server 2005 and 2008
- IBM Lotus Domino
- IBM Tivoli Directory Server

Assigning a Token in SAM

SAM supports a number of OTP authentication methods that can be used as a second authentication factor for users authenticating through Apache HTTP Server.

The following tokens are supported:

- eToken PASS
- SafeNet GOLD
- SafeNet eToken 3400
- SafeNet eToken 3500
- eToken NG-OTP
- MobilePASS
- SafeNet eToken Virtual products
- MobilePASS Messaging
- SafeNet Mobile Authentication (iOS)
Tokens can be assigned to users as follows:

- **SAM Management Center:** Management site used by SAM administrators and help desk for token enrollment and lifecycle management.
- **SAM Self-Service Center:** Self-service site used by end users for managing their tokens.
- **SAM Remote Service:** Self-service site used by employees not on the organization’s premises as a rescue website to manage cases where tokens are lost or passwords are forgotten.

For more information on SafeNet’s tokens and service portals, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

**Configuring SAM as an Identity Provider**

In order to use Apache HTTP Server as a Service Provider and SAM as an Identity Provider, the SAM has to be set as an Identity Provider.

1. From the Windows **Start** menu, click **All Programs > SafeNet > SafeNet Authentication Manager > Configuration Manager**.

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

2. On the **SafeNet Authentication Manager – Configuration Manager** window, from the menu bar, click **Action > Cloud Configuration**.
3. On the **Cloud Settings** window, click the **Info for Service Provider** tab. In the **Domain URL** field, enter the web address of the SAM portal server.

   The system fills in the rest of the fields according to the **Domain URL** entered.

4. To download the SAM metadata, click **Download Metadata**.

5. Save the metadata at the required location.

6. Click **OK**.
Configuring SAM for SAML-based User Federation

SafeNet Authentication Manager’s Token Policy Object (TPO) policies include **Application Authentication Settings** for SAML Service Providers. These settings are used by SAM’s portal to communicate with Service Providers.

For general portal configuration, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

**To download the Apache HTTP Server metadata:**

The Apache HTTP Server metadata can be downloaded only after configuring Apache HTTP Server. For configuration information, refer to "Configuring Apache HTTP Server", on page 12.

1. Browse to the following URL: https://<DNS or IP of Apache>/Shibboleth.sso/Metadata
2. Metadata is downloaded automatically. Save it with the .xml extension. (For example, Metadata.xml)

**To edit the Token Policy Object for SAM’s portal configuration:**

1. Open the Token Policy Object Editor for the appropriate group. Refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide* for more information.
2. On the **Token Policy Object Editor** window, in the left pane, expand **Protected Application Settings** and then click **User Authentication**.

   ![Token Policy Object Editor Version 3.0](image)

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

3. In the right pane, double-click **Application Authentication Settings**.
4. On the Application Authentication Settings Properties window, perform the following steps:
   a. Select Define this policy setting.
   b. Select Enabled.
   c. Click Definitions.

5. On the Application Authentication Settings window, in the left pane, right-click Application Authentication Settings and then click Create a new profile from metadata.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
6. Browse to the location where the Apache HTTP Server metadata was downloaded, select the metadata file, and then click **Open**.

7. On the **Import Metadata** window, click **OK**. The metadata is added in the left pane of the **Application Authentication Settings** window.

8. On the **Application Authentication Settings** window, in the left pane, rename the newly added metadata to a friendly name; for example, **Apache**.

9. In the left pane, click **Apache**.

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

<table>
<thead>
<tr>
<th><strong>SAM issuer</strong></th>
<th>Enter a unique SAM ID to be identified in SAML authentication. This ID should match the entityID of the SAM metadata file.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Audience URI</strong></td>
<td>Enter the Apache Entity ID, same as present in the <strong>Application Issuer</strong> policy.</td>
</tr>
<tr>
<td><strong>User mapping</strong></td>
<td>Select the field name in your user repository that identifies your Apache HTTP Server login name.</td>
</tr>
</tbody>
</table>
11. Enable the appropriate authentication methods for your organization. Refer to the SafeNet Authentication Manager Version 8.2 Administrator’s Guide for detailed information on authentication methods.

The following is an example of completed fields on the Application Authentication Settings window:

![Application Authentication Settings Window]

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

12. Click OK until all of the TPO Editor windows are closed.

Configuring Apache HTTP Server

Add SafeNet Authentication Manager as an Identity Provider for the Apache HTTP Server. To do so, perform the following procedures:

- Installing the Shibboleth Service Provider, page 12
- Configuring the Shibboleth Service Provider, page 13

Installing the Shibboleth Service Provider

Apache HTTP Server itself cannot act as a Service Provider for SAML. Therefore, you need to install the Shibboleth Service Provider.

1. Log in to Apache HTTP Server as a root user.
2. Run the following commands:
   ```
   cd /etc/yum.repos.d
   yum install -y shibboleth
   ```

   **NOTE:** It is not mandatory to install the Shibboleth Service Provider using the above method. It can be downloaded and installed from other sources as well. In the command, the path specified for repository is specific to CentOS 6.
Configuring the Shibboleth Service Provider

Configure the Shibboleth Service Provider and add SAM as an Identity Provider.

1. From the `/etc/httpd/conf.d` location, edit the `shib.conf` file as follows:
   
   ```
   LoadModule mod_shib /usr/lib/shibboleth/mod_shib_22.so
   UseCanonicalName On
   <IfModule mod_alias.c>
     <Location /shibboleth-sp>
       Allow from all
     </Location>
     Alias /shibboleth-sp/main.css /usr/share/shibboleth/main.css
   </IfModule>
   <Location /secure>
     AuthType shibboleth
     ShibRequestSetting requireSession 1
     require valid-user
   </Location>
   
   where, in the `<Location /secure>`, `secure` is the location of the web page (including the filename) on which SAML authentication is applied. For example, if `/var/www/html` is the location where the website is hosted, and you replaced `secure` with `my_secure/my_website.html`, the resultant path will be `/var/www/html/my_secure/my_website.html` on which SAML authentication will be applied. In this case, `my_website.html` is the name of the web page.

2. From the `/etc/selinux` location, edit the `config` file and set the following:

   ```
   SELINUX=permissive
   ```

3. Save and close the `config` file, and then run the following command:

   ```
   setenforce 0
   ```

   **NOTE:** It is mandatory to run SELINUX service in **permissive** mode as Shibboleth Service Provider does not work in **enforced** mode. Refer to the following link for more information:

   https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPSELinux

4. From the `/etc/shibboleth` location, edit the `shibboleth2.xml` file as follows:

   ```
   <ApplicationDefaults entityID="https://<DNS or IP of Apache>/shibboleth"
                      REMOTE_USER="eppn persistent-id targeted-id">
   
   <SSO entityID="SAM">
     SAML2 SAML1
   </SSO>
   ```

   where `SAM` is the entityID mentioned in the SAM metadata file.
• Uncomment the `MetadataProvider` element and update as shown below. The `SAM-Idp-Metadata.xml` file is the SAM metadata file present at `/etc/shibboleth`. To download the SAM metadata, refer to step 4 of “Configuring SAM as an Identity Provider” on page 7.

```xml
<MetadataProvider type="XML file="SAM-Idp-Metadata.xml" reloadInterval="7200"> ...
</MetadataProvider>
```

5. Save and close the `shibboleth2.xml` file.

6. Run the following commands to restart the Apache and Shibboleth services:

   ```bash
   service httpd restart
   service shibd restart
   ```

### Running the Solution

After successfully installing the Shibboleth Service Provider and configuring the Apache HTTP Server for SAML authentication, verify the integration solution.

For this integration, the SafeNet NG-OTP token is configured for authentication with the SAM solution.

1. In a web browser, open the website you have protected. You will be redirected to the SAM User Identification page.

2. In the **Username** field, enter your user name, and then click **OK**.

![User Identification]

Enter your username, select the computer's security level, and click 'OK'.

- **Username:**
- **Security:**
  - This is a public computer that is used by others
  - This is a private computer for authorized users only

*This Internet connection is not secure. Sensitive information may be intercepted by unauthorized persons. We recommend that this website be configured with an SSL server certificate.*
3. Generate an OTP using the SafeNet token. On the **OTP Authentication** window, enter the OTP in the **OTP Authentication Code** field, and then click **OK**.

If the credentials are valid, you will be redirected to the protected website.
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 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>SafeNet, Inc.</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 1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International 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 SafeNet Knowledge Base.</td>
</tr>
</tbody>
</table>