SafeNet Authentication Manager
Integration Guide

Using SAM as an Identity Provider for DenyAll Web Application Firewall
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 N.V. 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:** 007-013387-001, Rev. A

**Release Date:** January 2016
# Contents

Third-Party Software Acknowledgement ................................................................................. 4  
Description .......................................................................................................................... 4  
Applicability .......................................................................................................................... 4  
Environment .......................................................................................................................... 4  
Audience ............................................................................................................................... 4  
SAML Authentication using SAM ........................................................................................... 5  
Authentication Flow using SAM ............................................................................................. 5  
SAML Prerequisites ............................................................................................................... 5  
Configuring SafeNet Authentication Manager ......................................................................... 6  
  Synchronizing User Stores to SAM ....................................................................................... 6  
  Assigning Tokens in SAM .................................................................................................... 6  
  Configuring SAM as an Identity Provider ......................................................................... 7  
  Exporting the SAM Certificate ............................................................................................ 9  
  Configuring SAM for SAML-based User Federation ......................................................... 10  
Configuring DenyAll Web Application Firewall .................................................................... 13  
  Adding SAM as an Identity Provider in DenyAll Web Application Firewall ..................... 13  
  Adding SAML Authentication to a Workflow .................................................................... 19  
Running the Solution ............................................................................................................ 27  
Support Contacts .................................................................................................................. 28
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as DenyAll Web Application Firewall.

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.

To make the web access authentication easier while maintaining a high level of security, DenyAll offers the Web Application Firewall (WAF) solution, without any agent deployment on the application server. The DenyAll Web Application Firewall solution swerves and centralizes authentication at the network perimeter (on an application security gate).

This document describes how to:

- Deploy multi-factor authentication (MFA) options in DenyAll Web Application Firewall using SafeNet tokens managed by SafeNet Authentication Manager.
- Configure SAML authentication in DenyAll Web Application Firewall using SafeNet Authentication Manager as an identity provider.

It is assumed that the DenyAll Web Application Firewall environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager.

DenyAll Web Application Firewall 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**—A server version of SAM 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 Manager**—Version 8.2 (HF 710)
- **DenyAll Web Application Firewall**—Version 5.7.0

Audience

This document is targeted to system administrators who are familiar with DenyAll Web Application Firewall, 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.

Authentication Flow 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 DenyAll Web Application Firewall.

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

SAML Prerequisites

To enable SafeNet Authentication Manager to receive SAML authentication requests from DenyAll Web Application Firewall, ensure that the end users can authenticate from the DenyAll Web Application Firewall environment with a static password.
Configuring SafeNet Authentication Manager

Using SAM as an identity provider for DenyAll Web Application Firewall requires the following:

- Synchronizing User Stores to SAM, page 6
- Assigning Tokens in SAM, page 6
- Configuring SAM as an Identity Provider, page 7
- Exporting the SAM Certificate, page 9
- Configuring SAM for SAML-based User Federation, page 10

Synchronizing User Stores to SAM

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 Tokens in SAM

SAM supports a number of token methods that can be used as a second authentication factor for users authenticating through DenyAll Web Application Firewall.

The following tokens are supported:

- eToken PASS
- eToken NG-OTP
- SafeNet GOLD
- SMS tokens
- 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 helpdesk personnel 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

To use DenyAll Web Application Firewall as a service provider and SAM as an identity provider, SAM must be configured as an identity provider.

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

   ![Configuration Manager](image)

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

2. Click the **Action** tab, and then select **Cloud Configuration**.
3. On the **Info for Service Provider** tab, type the web address of the SAM portal server in the **Domain URL** field.

4. Click **OK**.
Exporting the SAM Certificate

SAM’s certificate is shared between SAM and DenyAll Web Application Firewall. The certificate will be used to sign the authentication requests.

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

2. Click the Action tab, and then select Cloud Configuration.
3. On the **Info for Service Provider** tab, perform the following steps:
   a. Click **Export Certificate** and save the certificate file. This certificate file will be imported into DenyAll Web Application Firewall later.
   b. Copy the values of the **Sign-in page URL**, **Sign-out page URL** and **Change password URL** fields, and save them in a text file. These URLs will be required while configuring DenyAll Web Application Firewall.

4. Click **OK**.

**Configuring SAM for SAML-based User Federation**

SAM’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 edit the TPO for SAM’s portal configuration:**

1. Open the **Token Policy Object Editor** for the appropriate group. See the *SafeNet Authentication Manager 8.2 Administrator’s Guide* for more information.
2. In the left pane, click **Protected Application Settings > User Authentication**.

   *(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**.

   ![Application Authentication Settings Properties](image)

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

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

   ![Application Authentication Settings](image)

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

6. In the left pane, right-click the new profile, and then rename it to a user-friendly name.
7. In the left pane, click the new profile.

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

<table>
<thead>
<tr>
<th>Application Issuer</th>
<th>Enter an issuer ID for DenyAll Web Application Firewall, same as you will enter in step 5 of “Adding SAML Authentication to a Workflow” on page 19.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAM issuer</td>
<td>Enter a unique SAM ID to be identified in SAML authentication.</td>
</tr>
<tr>
<td>Application’s login URL</td>
<td>Enter the ACS URL of DenyAll Web Application Firewall (for example, https://&lt;FQDN or IP address of the interface on which application is hosted&gt;/saml/acs).</td>
</tr>
<tr>
<td>User mapping</td>
<td>Select AccountName.</td>
</tr>
</tbody>
</table>


The following is an example of the completed policy settings in the Application Authentication Settings window:

10. Click OK until all of the Token Policy Object Editor windows are closed.
Configuring DenyAll Web Application Firewall

Configuring DenyAll Web Application Firewall with SAM for SAML authentication requires:

- Adding SAM as an Identity Provider in DenyAll Web Application Firewall, page 13
- Adding SAML Authentication to a Workflow, page 19

Adding SAM as an Identity Provider in DenyAll Web Application Firewall

1. Log in to https://my.bee-ware.net/ to download the SAML sample backup file.
2. Browse to the http://en.documentation.bee-ware.net/display/waf57/SAML URL.
3. Download the SAML_Pack_v1.5.4.backup file and then save it on your local drive.
4. Launch the DenyAll Web Application Firewall application.
5. On the Management i-Box Login window, in the Password field, enter your password, and then click Connect.

(The screen image above is from DenyAll® software. Trademarks are the property of their respective owners.)
6. On the Management i-Box main window, click the **Management** tab.

![Management i-Box main window](image1)

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

7. In the left pane, click **Backups**.

8. In the right pane, click **Upload**, select the **SAML_Pack_v1.5.4.backup** file you downloaded earlier (refer to step 3), then and click **OK**.

![Uploading SAML Pack](image2)

(The screen image above is from DenyAll® software. Trademarks are the property of their respective owners.)
9. The **SAML_Pack_v1.5.4.backup** file is uploaded and listed in the right pane. Select the row listing the file, and then click **Restore**.

![Screen Image](image1.png)

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

10. On the **Restore a backup** window, in the right pane, select the row containing the **Sample: SAMLv2 SP Binding HTTP Post** workflow, and then click **OK**.

![Screen Image](image2.png)

*(The screen image above is from DenyAll® software. Trademarks are the property of their respective owners.)*
11. A message is displayed. Click **OK**.

![Image of a message box](image)

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

12. On the Management i-Box main window, click the **Management** tab.

13. In the left pane, click **XML > XML Keystores**.

![Image of the management interface](image)

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

14. In the right pane, click **Add**.

15. On the **Add XML Keystore** window, in the **Name** field, enter a name for the XML keystore (for example, **SAM SAML**), and then click **OK**.

![Image of the add XML keystore window](image)

*(The screen image above is from DenyAll® software. Trademarks are the property of their respective owners.)*
16. On the Management i-Box main window, in the right pane, the newly created XML keystore is listed. Select the newly created XML keystore, and then click **Add**.

![XML keystore list](image1.png)

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

17. On the **Add XML Key** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the XML key (for example, <strong>IdP</strong>).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Certificate</strong></td>
<td>Click on the folder icon, select the SAM certificate that you downloaded earlier (refer to step 3 of “Exporting the SAM Certificate” on page 9). Convert the SAM certificate to the CRT file format before uploading it.</td>
</tr>
</tbody>
</table>

![Add XML Key window](image2.png)

*(The screen image above is from DenyAll® software. Trademarks are the property of their respective owners.)*
18. On the Management i-Box main window, click **Apply**.

![Management i-Box main window](image1.png)

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

19. On the **Apply configuration** window, click **Select all**, and then click **OK**.

![Apply configuration window](image2.png)

*(The screen image above is from DenyAll® software. Trademarks are the property of their respective owners.)*
20. On the **Apply result** window, click **OK**.

![Apply result](image)

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

**Adding SAML Authentication to a Workflow**

A workflow is a flow-processing diagram. It is assumed that a workflow is already configured on which you want to add SAML authentication.

---

**NOTE:** A default workflow is used for configuring SAML authentication in DenyAll Web Application Firewall. To download the backup of the workflow, a user must have an account on [https://my.bee-ware.net/](https://my.bee-ware.net/).

---

1. On the Management i-Box main window, click the **Policies** tab, and then click **Workflows**.

![Workflows](image)

*(The screen image above is from DenyAll® software. Trademarks are the property of their respective owners.)*
2. Double-click the **Sample: SAMLv2 SP Binding HTTP Post** workflow (the default workflow used in this integration).

3. In the right pane, on the **Tools** tab, click **Miscellaneous**, and then drag and drop the **SAML: Use UTC in Issuelnstant** tool to an appropriate location in the workflow.

4. In the workflow, double-click **SAML: Generate request**.
5. On the **Modify SAML: Generate request** window, change the values of the following fields appropriately, and then click **OK**.

<table>
<thead>
<tr>
<th><strong>Display name</strong></th>
<th>Enter a name you want to display for the block (for example, <strong>SafeNet</strong>).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Issuer</strong></td>
<td>Enter a name for the issuer (for example, <strong>DenyAll</strong>) same as entered in step 8 of “Configuring SAM for SAML-based User Federation” on page 10.</td>
</tr>
<tr>
<td><strong>IdP Recipient URL</strong></td>
<td>Enter the SAM login URL (for example, <code>http://&lt;FQDN/IP of SAM server&gt;/samcloud/default.aspx</code>).</td>
</tr>
</tbody>
</table>

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

6. On the Management i-Box main window, in the workflow, double-click **SAML: Send request to IdP**.

7. On the **Modify SAML: Send request to IdP** window, in the **Request Signing** field, select **No**, and then click **OK**.

(The screen image above is from DenyAll® software. Trademarks are the property of their respective owners.)
8. On the Management i-Box main window, in the workflow, double-click **SAML: Decode assertion**.

9. On the **Modify SAML: Decode assertion** window, change the values of the following fields appropriately, and then click **OK**.

<table>
<thead>
<tr>
<th>XML Keystore for signature validation and decryption</th>
<th>Select the XML keystore (for example, <strong>SAM SAML</strong>) that you created earlier in step 15 of “Adding SAM as an Identity Provider in DenyAll Web Application Firewall” on page 13.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NotBefore tolerance (s)</td>
<td>Enter 60.</td>
</tr>
<tr>
<td>NotAfter tolerance (s)</td>
<td>Enter 30.</td>
</tr>
</tbody>
</table>

10. On the Management i-Box main window, in the workflow, double-click **Redirect**.

11. On the **Modify Redirect** window, in the **The redirection URL** field, enter 

```
${url_of("","",http.request.host,http.request.ssl.enabled)}
```

, and then click **OK**.

(The screen image above is from DenyAll® software. Trademarks are the property of their respective owners.)
12. On the Management i-Box main window, click **Save**.

![Management i-Box main window](image)

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

13. On the **Confirmation requested** window, click **Yes**.

![Confirmation requested](image)

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

14. On the Management i-Box main window, click the **Applications** tab.

15. In the **Tunnel** column, double-click the application name (for example, **SafeNet Demo**) on which you want to apply the SAML workflow.

![Applications tab](image)

(The screen image above is from DenyAll® software. Trademarks are the property of their respective owners.)
16. On the Modify Tunnel window, on the General tab, change the values of the following fields appropriately.

<table>
<thead>
<tr>
<th>Policy type</th>
<th>Select Workflow.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workflow</td>
<td>Select the workflow that you modified earlier.</td>
</tr>
</tbody>
</table>

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

17. Click the Network tab.

18. Under Incoming, in the Port field, enter 443 (if not already populated).

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

19. Click the SSL tab.
20. Change the values of the following fields appropriately, and then click **OK**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL Cipher Profile</td>
<td>Select the SSL cipher profile.</td>
</tr>
<tr>
<td>Proxy certificate (Server)</td>
<td>Select the proxy server certificate.</td>
</tr>
</tbody>
</table>

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

21. On the Management i-Box main window, click **Apply**.

*(The screen image above is from DenyAll® software. Trademarks are the property of their respective owners.)*
22. On the **Apply configuration** window, click **Select all**, and then click **OK**.

![Apply Configuration Window](image)

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

23. On the **Apply result** window, click **OK**.

![Apply Result Window](image)

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

For this integration, the SafeNet eToken PASS is configured for authentication with the SAM solution.

1. Open the following URL in a web browser on which the SAML workflow is applied:
   https://<Incoming IP address of application>

2. On the SAM login window, in the Username field, enter your user name, and then click OK.

3. On the OTP Authentication window, in the OTP Authentication Code field, enter the OTP (generated using SafeNet eToken PASS), and then click OK.
If the credentials are valid, you are provided access to the web application hosted as reverse proxy on DenyAll Web Application Firewall.

**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, Inc.  
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. |