SafeNet Authentication Service
Integration Guide

Using SAS as an Identity Provider for DenyAll Web Application Firewall
Contents

Third-Party Software Acknowledgement .............................................................................................................................................. 4
Description .................................................................................................................................................................................................... 4
Applicability ..................................................................................................................................................................................................... 4
Environment ...................................................................................................................................................................................................... 4
Audience ........................................................................................................................................................................................................ 5
SAML Authentication using SAS Cloud .................................................................................................................................................. 5
SAML Authentication using SAS-SPE and SAS-PCE .................................................................................................................................. 5
SAML Authentication Flow using SAS .................................................................................................................................................. 6
SAML Prerequisites .................................................................................................................................................................................................. 6
Configuring DenyAll Web Application Firewall ......................................................................................................................................... 6
  Downloading the SafeNet Identity Provider Certificate .................................................................................................................. 6
  Adding SAS as an Identity Provider in DenyAll Web Application Firewall .................................................................................. 7
  Adding SAML Authentication to a Workflow ..................................................................................................................................... 13
Configuring SafeNet Authentication Service ........................................................................................................................................... 21
  Synchronizing Users Stores to SAS .................................................................................................................................................. 21
  Assigning an Authenticator in SAS ...................................................................................................................................................... 21
  Adding DenyAll Web Application Firewall as a Service Provider (SP) in SAS ........................................................................... 22
  Enable SAML Services in SAS ........................................................................................................................................................... 25
Running the Solution .................................................................................................................................................................................................. 29
Support Contacts ............................................................................................................................................................................................................... 30
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet 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 Service delivers a fully automated, versatile, and strong authentication-as-a-service solution.

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

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 one-time password (OTP) authenticators managed by SafeNet Authentication Service.
- Configure SAML authentication in DenyAll Web Application Firewall using SafeNet Authentication Service 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 Service.

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 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 (Cloud)**
- **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 Service.

**SAML Authentication using SAS Cloud**

SAS Cloud provides a service for SAML authentication that is already implemented in the SAS Cloud environment and can be used without any installation.

**SAML Authentication using SAS-SPE and SAS-PCE**

In addition to the pure cloud-based offering, SafeNet Authentication Service 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 the Shibboleth infrastructure, which uses a special on-premises agent called SafeNet Authentication Service Agent for Shibboleth.

For more information on how to install and configure the SafeNet Authentication Service Agent for Shibboleth, refer to the SafeNet Support Portal.
SAML Authentication Flow using SAS

SafeNet Authentication Service 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 Service (SAS). SAS collects and evaluates the user's credentials.
2. SAS returns a response to DenyAll Web Application Firewall, accepting or rejecting the user's authentication request.

SAML Prerequisites

To enable SafeNet Authentication Service 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 DenyAll Web Application Firewall

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

- Downloading the SafeNet Identity Provider Certificate, page 6
- Adding SAS as an Identity Provider in DenyAll Web Application Firewall, page 7
- Adding SAML Authentication to a Workflow, page 13

Downloading the SafeNet Identity Provider Certificate

Browse to the https://cloud.safenet-inc.com/console/cert/idp.crt URL. The SafeNet IDP certificate will automatically download. Save it locally on your machine.
Adding SAS 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.

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

(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 tab](image)

(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), and then click **OK**.

![Screen image of DenyAll® software](image1.png)

*(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 of DenyAll® software](image2.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**.

![Image of Restore a backup window]

*(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 information message]

*(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**.

![XML Keystores screenshot](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, **SAS SAML**), and then click **OK**.

![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.

![Image](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, IdP).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td>Click on the folder icon, select the SAS identity provider certificate you downloaded previously (refer to “Downloading the SafeNet Identity Provider Certificate” on page 6), and then click open.</td>
</tr>
</tbody>
</table>

![Image](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](image)

*(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](image)

*(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 window](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**.

![Management i-Box main window](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 IssueInstant** 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>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name</td>
<td>Enter a name you want to display for the block (for example, <strong>SafeNet</strong>).</td>
</tr>
<tr>
<td>Issuer</td>
<td>Enter a name for the issuer (for example, <strong>DenyAll</strong>).</td>
</tr>
<tr>
<td>IdP Recipient URL</td>
<td>Enter the SAS Identity Provider HTTP-POST login URL (for example, <strong><a href="https://idp1.cryptocard.com/idp/profile/SAML2/POST/SSO">https://idp1.cryptocard.com/idp/profile/SAML2/POST/SSO</a></strong>).</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>SAS SAML</strong>) that you created earlier in step 15 of “Adding SAS as an Identity Provider in DenyAll Web Application Firewall” on page 7.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NotBefore tolerance (s)</td>
<td>Enter <strong>60</strong>.</td>
</tr>
<tr>
<td>NotAfter tolerance (s)</td>
<td>Enter <strong>30</strong>.</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

\[
\text{${url_of("","",http.request.host,http.request.ssl.enabled)}},
\]

and then click **OK**.
12. On the Management i-Box main window, click **Save**.

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

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

(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.

(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><strong>Workflow</strong></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><strong>SSL Cipher Profile</strong></th>
<th>Select the SSL cypher profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Proxy certificate (Server)</strong></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](image1)

*(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](image2)

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

The deployment of multi-factor authentication using SAS with DenyAll Web Application Firewall using SAML authentication requires:

- Synchronizing Users Stores to SAS, page 21
- Assigning an Authenticator in SAS, page 21
- Adding DenyAll Web Application Firewall as a Service Provider (SP) in SAS, page 22
- Enable SAML Services in SAS, page 25

Synchronizing Users Stores to SAS

Before SAS can authenticate any user in your organization, you need to create a user store in 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 further 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 SAS

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

The following authenticators are supported:

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

- **Manual provisioning**—Assign an authenticator to users one by one.
- **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” 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.


**Adding DenyAll Web Application Firewall as a Service Provider (SP) in SAS**

Add a service provider entry in the SAS **SAML Service Providers** module to prepare it to receive SAML authentication requests from DenyAll Web Application Firewall. You will need the Issuer ID and assertion consumer URL location of DenyAll Web Application Firewall.

**To add DenyAll Web Application Firewall as a service provider in SAS:**

1. Log in to the SAS console with an Operator account.

   ![SAS Console](image)

2. Click the **COMMS** tab, and then click **SAML Service Providers**.

   ![SAML Service Providers](image)
3. In the **SAML Service Providers** module, click the **SAML 2.0 Settings** link.

4. Click **Add**.

5. In the **Add SAML 2.0 Settings** section, complete the following fields, and then click **Apply**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friendly Name</td>
<td>Enter the DenyAll Web Application Firewall name.</td>
</tr>
<tr>
<td>SAML 2.0 Metadata</td>
<td>Select <strong>Create New Metadata File</strong>.</td>
</tr>
<tr>
<td>Entity ID</td>
<td>Enter the Service Provider Issuer ID same as entered in step 5 of “Adding SAML Authentication to a Workflow” on page 13.</td>
</tr>
<tr>
<td>Location</td>
<td>Enter the Assertion Consumer URL (for example, <code>https://&lt;FQDN or IP address of the interface on which application is hosted&gt;/saml/acs</code>).</td>
</tr>
</tbody>
</table>

![Add SAML 2.0 Settings](image-url)
NOTE: The remaining options are used to customize the appearance of the logon page presented to the user. For more information on logon page customization, refer “Configure SAML Service” in the SAML Configuration Guide: http://www2.safenet-inc.com/sas/implementation-guides/sas-on-prem/SAS-QS-SAML.pdf

DenyAll Web Application Firewall is added as a service provider in the system.
Enable SAML Services in SAS

After DenyAll Web Application Firewall has been added to SAS as a service provider, the users should be granted permission to use this service provider with SAML authentication.

There are two methods to enable the user to use the service provider:

- Manually, one user at a time, using SAML Services module
- Automatically, by defining groups of users, using SAML Provisioning Rules

Using SAML Services Module

Manually enable a single user to authenticate against one or more configured SAML service providers.

1. Log in to the SAS console with an Operator account.

2. Click the ASSIGNMENT tab and then search for the required user.

3. Click the appropriate user in the User ID column.
4. Click **SAML Services**.

5. Click **Add**.

6. Under **Add SAML Service**, do the following:

   a. In the **Service** field, select the DenyAll Web Application Firewall service provider.

   b. In the **SAML Login ID** field, select the type of login ID (User ID, E-mail, or Custom) to be sent as a User ID to DenyAll Web Application Firewall in the response.

   c. Click **Add**.

The user can now authenticate to DenyAll Web Application Firewall using SAML authentication.
Using SAML Provisioning Rules

Use this module to enable groups of users to authenticate to SAML service providers.

1. Log in to the SAS console with an Operator account.

2. Click the POLICY tab, and then click Automation Policies.

3. Click the SAML Provisioning Rules link.
4. Click **New Rule**.

5. Configure the rule as follows, and then click **Add**:

<table>
<thead>
<tr>
<th><strong>Rule Name</strong></th>
<th>Enter a name for the rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User is in container</strong></td>
<td>Users affected by this rule must be in the selected container.</td>
</tr>
<tr>
<td><strong>Groups</strong></td>
<td>The Virtual Server groups box lists all groups. Click the user groups that will be affected by the rule, and then click the right arrow to move it to the Used by rule box.</td>
</tr>
<tr>
<td><strong>Parties</strong></td>
<td>The Relying Parties box lists all service providers. Click the service providers that the groups of users will authenticate to, and then click the right arrow to move it to Rule Parties box.</td>
</tr>
<tr>
<td><strong>SAML Login ID</strong></td>
<td>Select User ID. The User ID will be returned to the service provider in the SAML assertion.</td>
</tr>
</tbody>
</table>
### Running the Solution

For this integration, the SafeNet eToken PASS is configured for authentication with the SAS 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 SAS Login window, complete the following fields, and then click **Login**.

   | User Name | Enter your user name. |
   | Password  | Generate an OTP using the SafeNet eToken PASS token, and then enter that OTP in this field. |

   If the credentials are validated, 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>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>Gemalto, 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 Gemalto Knowledge Base.</td>
</tr>
</tbody>
</table>