SafeNet Authentication Service
Integration Guide

Using RADIUS Protocol 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.

© 2015 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:** 007-013281-001, Rev. A

**Release Date:** September 2015
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-Party Software Acknowledgement</td>
<td>4</td>
</tr>
<tr>
<td>Description</td>
<td>4</td>
</tr>
<tr>
<td>Applicability</td>
<td>4</td>
</tr>
<tr>
<td>Environment</td>
<td>4</td>
</tr>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS-based Authentication using SAS Cloud</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS-based Authentication using SAS-SPE and SAS-PCE</td>
<td>6</td>
</tr>
<tr>
<td>RADIUS Authentication Flow using SAS</td>
<td>6</td>
</tr>
<tr>
<td>RADIUS Prerequisites</td>
<td>7</td>
</tr>
<tr>
<td>Configuring SafeNet Authentication Service</td>
<td>7</td>
</tr>
<tr>
<td>Creating Users Stores in SAS</td>
<td>7</td>
</tr>
<tr>
<td>Assigning an Authenticator in SAS</td>
<td>8</td>
</tr>
<tr>
<td>Adding DenyAll Web Application Firewall as an Authentication Node in SAS</td>
<td>9</td>
</tr>
<tr>
<td>Checking the SAS RADIUS Server’s IP Address</td>
<td>11</td>
</tr>
<tr>
<td>Configuring DenyAll Web Application Firewall</td>
<td>12</td>
</tr>
<tr>
<td>Adding SAS as a RADIUS Server in DenyAll Web Application Firewall</td>
<td>12</td>
</tr>
<tr>
<td>Adding RADIUS Authentication to a Workflow</td>
<td>20</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>26</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>27</td>
</tr>
</tbody>
</table>
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.

DenyAll Web Application Firewall (WAF) combines ease of configuration with a proven ability to secure web apps, maintains a high level of security, and does not require agent deployment on the application server.

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 DenyAll Web Application Firewall to work with SafeNet Authentication Service in RADIUS mode.

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 RADIUS protocol 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.

RADIUS-based Authentication using SAS Cloud

SAS Cloud provides two RADIUS mode topologies:

- **SAS cloud hosted RADIUS service**—A RADIUS service that is already implemented in the SAS cloud environment and can be used without any installation or configuration requirements.

- **Local RADIUS hosted on-premises**—A RADIUS agent that is implemented in the existing customer’s RADIUS environment. The agent forwards the RADIUS authentication requests to the SAS cloud environment. The RADIUS agent can be implemented on a Microsoft NPS/IAS or FreeRADIUS server.

This document demonstrates the solution using the SAS cloud hosted RADIUS service.

For more information on how to install and configure SAS Agent for IAS/NPS, refer to: http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-Agents-IASNPS.pdf

For more details on how to install and configure FreeRADIUS, refer to the SafeNet Authentication Service FreeRADIUS Agent Configuration Guide.
RADIUS-based Authentication using SAS-SPE and SAS-PCE

For both on-premises versions, SAS can be integrated with the following solutions that serve as local RADIUS servers:

- **Microsoft Network Policy Server (MS-NPS) or the legacy Microsoft Internet Authentication Service (MS-IAS)**—SafeNet Authentication Service is integrated with the local RADIUS servers using a special on-premises agent called SAS Agent for Microsoft IAS and NPS.
  
  For more information on how to install and configure the SAS Agent for Microsoft IAS and NPS, refer to the following document:
  

- **FreeRADIUS**—The SAS FreeRADIUS Agent is a strong authentication agent that is able to communicate with SAS through the RADIUS protocol.
  
  For more information on how to install and configure the SAS FreeRADIUS Agent, refer to the SafeNet Support Portal.

RADIUS Authentication Flow using SAS

SafeNet Authentication Service communicates with a large number of VPN and access-gateway solutions using the RADIUS protocol.

The image below describes the data flow of a multi-factor authentication transaction for DenyAll Web Application Firewall.

1. A user attempts to log on to DenyAll Web Application Firewall using an OTP authenticator.
2. DenyAll Web Application Firewall sends a RADIUS request with the user’s credentials to SafeNet Authentication Service for validation.
3. The SAS authentication reply is sent back to the DenyAll Web Application Firewall.
4. The user is granted or denied access to the DenyAll Web Application Firewall based on the OTP value calculation results from SAS.
RADIUS Prerequisites

To enable SafeNet Authentication Service to receive RADIUS requests from DenyAll Web Application Firewall, ensure the following:

- End users can authenticate from the DenyAll Web Application Firewall environment with a static password before configuring the DenyAll Web Application Firewall to use RADIUS authentication.
- Ports 1812/1813 are open to and from DenyAll Web Application Firewall.
- A shared secret key has been selected. A shared secret key provides an added layer of security by supplying an indirect reference to a shared secret key. It is used by a mutual agreement between the RADIUS server and RADIUS client for encryption, decryption, and digital signatures.

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with DenyAll Web Application Firewall using RADIUS protocol requires the following:

- Creating Users Stores in SAS, page 7
- Assigning an Authenticator in SAS, page 8
- Adding DenyAll Web Application Firewall as an Authentication Node in SAS, page 9
- Checking the SAS RADIUS Server’s IP Address, page 11

Creating Users Stores in SAS

Before SAS can authenticate any user in your organization, you must 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 additional details on importing users to SafeNet Authentication Service, refer to “Creating Users” in the SafeNet Authentication Service Subscriber Account Operator Guide:


All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.
Assigning an Authenticator in SAS

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

The following authenticators are supported:

- eToken PASS
- RB-1 Keypad Token
- KT-4 Token
- SafeNet GOLD
- SMS Token
- MP-1 Software Token
- MobilePASS

Authenticators can be assigned to users in two ways:

- **Manual provisioning**—Assign an authenticator to users one at a time.
- **Provisioning rules**—The administrator can set provisioning rules in SAS so that the rules will be triggered when group memberships and other user attributes change. An authenticator will be assigned automatically to the user.

Refer to “Provisioning Rules” in the *SafeNet Authentication Service Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SAS user store.

Adding DenyAll Web Application Firewall as an Authentication Node in SAS

Add a RADIUS entry in the SAS Auth Nodes module to prepare it to receive RADIUS authentication requests from DenyAll Web Application Firewall. You will need the IP address of DenyAll Web Application Firewall and the shared secret to be used by both SAS and DenyAll Web Application Firewall.

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

2. Click the COMMS tab, and then select Auth Nodes.

3. In the Auth Nodes module, click the Auth Nodes link.
4. Under **Auth Nodes**, click **Add**.

5. In the **Add Auth Nodes** section, complete the following fields, and then click **Save**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Description</td>
<td>Enter a host description.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Enter the name of the host that will authenticate with SAS.</td>
</tr>
<tr>
<td>Low IP Address In Range</td>
<td>Enter the IP address of the host, or the lowest IP address in a range of</td>
</tr>
<tr>
<td></td>
<td>addresses that will authenticate with SAS.</td>
</tr>
<tr>
<td>Configure FreeRADIUS</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Synchronization</td>
<td></td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the shared secret key.</td>
</tr>
<tr>
<td>Confirm Shared Secret</td>
<td>Re-enter the shared secret key.</td>
</tr>
</tbody>
</table>

The authentication node is added to the system.
Checking the SAS RADIUS Server’s IP Address

Before adding SAS as a RADIUS server in DenyAll Web Application Firewall, check the IP address. The IP address will then be added to DenyAll Web Application Firewall as a RADIUS server at a later stage.

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

2. Click the COMMS tab, and then select Auth Nodes.

3. In the Auth Nodes module, click the Auth Nodes link. The SAS RADIUS server details are displayed.
Configuring DenyAll Web Application Firewall

The deployment of multi-factor authentication using SAS with DenyAll Web Application Firewall using RADIUS protocol requires the following:

- Adding SAS as a RADIUS Server in DenyAll Web Application Firewall, page 12
- Adding RADIUS Authentication to a Workflow, page 20

Adding SAS as a RADIUS Server in DenyAll Web Application Firewall

1. Launch the DenyAll WAF application.
2. In the Management i-Box Login window, enter your password, and then click Connect.

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

4. In the left pane of the console, select **WAM > Perimeter Gates > Authentication Servers**.

5. Click **Add**.
6. In the **Add Authentication Server** window, click the **General** tab.

![Add Authentication Server window]

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

7. In the **Type** menu, select **RADIUS**.

8. Click the blue circle adjacent to the **Datastore** menu.

![Add Authentication Server window with RADIUS selected]

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

![Add Authentication Server window]

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

10. In the **Add Datastore** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for the datastore (for example, SAS).</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Do not change this selection (<strong>RADIUS</strong>).</td>
</tr>
<tr>
<td><strong>RADIUS Servers IPs</strong></td>
<td>Enter the SAS Cloud RADIUS IP (for example, <strong>109.73.120.148</strong>).</td>
</tr>
</tbody>
</table>

![Add Datastore window]

*(The screen image above is from DenyAll®. Trademarks are the property of their respective owners.)*
11. In the **Add Authentication Server** window, on the **General** tab, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Enter a name for the Authentication Server (for example, <strong>SAS Cloud</strong>).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Do not change this selection (<strong>RADIUS</strong>).</td>
</tr>
<tr>
<td><strong>Datastore</strong></td>
<td>Select the datastore created in the previous step (for example, <strong>SAS</strong>).</td>
</tr>
<tr>
<td><strong>N.A.S</strong></td>
<td>Enter the IP address of the DenyAll interface that will be used to reach the SAS Server.</td>
</tr>
<tr>
<td><strong>Shared secret</strong></td>
<td>Enter the same shared secret that you entered in step 5 in “Adding DenyAll Web Application Firewall as an Authentication Node in SAS.”</td>
</tr>
</tbody>
</table>

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

12. In the left pane of the console, select **Gates Network Configurations**.
13. Click **Add**.

![DenyAll® Management Interface Screen](image)

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

14. In the **Add Gates Network Configuration** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Enter a configuration name (for example, <strong>RadiusAuth</strong>).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>i-Box</strong></td>
<td>Select the appropriate i-Box.</td>
</tr>
<tr>
<td><strong>IP</strong></td>
<td>Select the listening IP address of the WAM engine. This IP address can be one that is not contactable by the clients.</td>
</tr>
</tbody>
</table>

![Add Gates Network Configuration](image)

(The screen image above is from DenyAll*. Trademarks are the property of their respective owners.)
15. In the left pane of the console, select **Perimeter Gates**.

![Image of DenyAll console with Perimeter Gates selected.](image)

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

16. Click **Add**.

17. On the **Add Perimeter Gate** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for Perimeter Gate.</td>
</tr>
<tr>
<td><strong>IAM listeners</strong></td>
<td>Select the IAM listener that you created in step 14.</td>
</tr>
<tr>
<td><strong>IP</strong></td>
<td>Select the listening IP address of the WAM engine. This IP address can be one that is not contactable by the clients.</td>
</tr>
</tbody>
</table>

![Image of Add Perimeter Gate window.](image)

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

19. In the **Authentication method** menu, select **From**.

   ![Authentication tab](image1)

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

20. Click the **Authentication Backends** tab, complete the following fields, and then click **OK**.

   | Internal authentication server | Deselect this check box. |
   | Authentication server type     | Select **RADIUS**.       |
   | Authentication Server          | Select the authentication server that you created in step 11. |

   ![Authentication Backends tab](image2)

(The screen image above is from DenyAll®. Trademarks are the property of their respective owners.)
Adding RADIUS Authentication to a Workflow

In this section, we will add the RADIUS Authentication to an existing workflow. It is assumed that a workflow is already created.

A screenshot of the workflow used in this section is shown below.

(The screen image above is from DenyAll®. Trademarks are the property of their respective owners.)
1. Click the **Policies** tab, and then select **Workflows**.

![Diagram of DenyAll WAF Management Interface with Policies and Workflows selected]

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

2. Double-click the workflow to which you want to add RADIUS authentication.

3. In the right pane, select **Tools > Authentication**. Drag and drop the **WAM Perimeter Authentication** tool in the appropriate location in the workflow.

![Drag and drop WAM Perimeter Authentication tool]

*(The screen image above is from DenyAll®. Trademarks are the property of their respective owners.)*
4. Double-click **WAM Perimeter Authentication**.
5. Complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Name of this node</th>
<th>Enter a name for the node (for example <strong>Radius_Auth</strong>).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perimeter gate</td>
<td>Select the <strong>Perimeter gate</strong> that you created in step 17 in &quot;Adding SAS as a RADIUS Server in DenyAll Web Application Firewall.&quot;</td>
</tr>
<tr>
<td>Perimeter gate IP port</td>
<td>Select the <strong>Gates Network Configuration</strong> that you created in step 14 in &quot;Adding SAS as a RADIUS Server in DenyAll Web Application Firewall.&quot;</td>
</tr>
</tbody>
</table>

6. Click **Apply**.
7. In the **Save changes?** window, click **Save**.

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

![Apply Window](image)

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

9. In the **Apply result** window, click **OK**.

![Apply Result](image)

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

![Applications Tab](image)

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

11. Double-click the application to add to the RADIUS workflow that you created.

12. In the **Modify Tunnel** window, click the **General** tab.

13. Complete the following fields and then click **OK**.

<table>
<thead>
<tr>
<th><strong>Policy type</strong></th>
<th><strong>Select Workflow.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Workflow</strong></td>
<td>Select the workflow edited above.</td>
</tr>
</tbody>
</table>

![Modify Tunnel Window](image)

(The screen image above is from DenyAll®. Trademarks are the property of their respective owners.)
14. Click **Apply** in the upper-right corner.

15. In the **Apply** window, click **Select all**, and then click **OK**.

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

![Apply result window](image)

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

## Running the Solution

Test the final solution after successfully configuring DenyAll Web Application Firewall with SAS for RADIUS authentication. In this solution, the user is enrolled with an eToken PASS.

1. Enter the URL of the application on which the RADIUS workflow was applied. The **Authentication** window is displayed.

![Authentication window](image)

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

2. Enter your username in the **Login** field.
3. Generate an OTP, and then enter it in the **Password** field.
4. Click **Connection**.
5. After a successful authentication, you will be granted 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</td>
</tr>
<tr>
<td></td>
<td>manage incidents, get the latest software upgrades, and access the Gemalto Knowledge</td>
</tr>
<tr>
<td></td>
<td>Base.</td>
</tr>
</tbody>
</table>