SafeNet Authentication Manager
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:** 007-013301-001, Rev. A

**Release Date:** October 2015
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-Party Software Acknowledgement</td>
<td>5</td>
</tr>
<tr>
<td>Description</td>
<td>5</td>
</tr>
<tr>
<td>Applicability</td>
<td>5</td>
</tr>
<tr>
<td>Environment</td>
<td>5</td>
</tr>
<tr>
<td>Audience</td>
<td>6</td>
</tr>
<tr>
<td>RADIUS-based Authentication using SAM</td>
<td>6</td>
</tr>
<tr>
<td>RADIUS Authentication Flow using SAM</td>
<td>6</td>
</tr>
<tr>
<td>RADIUS Prerequisites</td>
<td>7</td>
</tr>
<tr>
<td>Configuring SafeNet Authentication Manager</td>
<td>7</td>
</tr>
<tr>
<td> Synchronizing Users Stores to SAM</td>
<td>7</td>
</tr>
<tr>
<td> Configuring SAM’s Connector for OTP Authentication</td>
<td>8</td>
</tr>
<tr>
<td> Assigning a Token in SAM</td>
<td>8</td>
</tr>
<tr>
<td> Adding DenyAll Web Application Firewall as a RADIUS Client in IAS/NPS</td>
<td>9</td>
</tr>
<tr>
<td> Configuring SAM’s OTP Plug-In for Microsoft RADIUS Client</td>
<td>10</td>
</tr>
<tr>
<td>Configuring DenyAll Web Application Firewall</td>
<td>11</td>
</tr>
<tr>
<td> Adding SAM as a RADIUS Server in DenyAll Web Application Firewall</td>
<td>11</td>
</tr>
<tr>
<td> Adding RADIUS Authentication to a Workflow</td>
<td>17</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>22</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>23</td>
</tr>
</tbody>
</table>
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 one-time password (OTP) tokens managed by SafeNet Authentication Manager.
- Configure DenyAll Web Application Firewall to work with SafeNet Authentication Manager 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 Manager and that the SafeNet Authentication Manager OTP plug-in for Microsoft RADIUS Client was installed as part of the simplified installation mode of SAM. For more information on the SafeNet Authentication Manager installation modes, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

DenyAll Web Application Firewall can be configured to support multi-factor authentication in several modes. RADIUS protocol 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 (Hotfix 493)
- 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.

**RADIUS-based Authentication using SAM**

SafeNet’s OTP architecture includes the SafeNet RADIUS server for back-end OTP authentication. This enables integration with any RADIUS-enabled gateway or application. The SafeNet RADIUS server accesses user information in the Active Directory infrastructure via SAM.

SAM’s OTP plug-in for Microsoft RADIUS Client works with Microsoft’s IAS or NPS, providing strong, authenticated remote access through the IAS or NPS RADIUS server.

When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet OTP plug-in for Microsoft RADIUS Client, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

**RADIUS Authentication Flow using SAM**

SafeNet Authentication Manager communicates with a large number of VPN and access-gateway solutions using the RADIUS 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 using an OTP token.
2. DenyAll Web Application Firewall sends a RADIUS request with the user’s credentials to SafeNet Authentication Manager for validation.
3. The SAM authentication reply is sent back to DenyAll Web Application Firewall.
4. The user is granted or denied access to DenyAll Web Application Firewall based on the OTP value calculation results from SAM.
RADIUS Prerequisites

To enable SafeNet Authentication Manager 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 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 Manager

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

- Synchronizing Users Stores to SAM, page 7
- Configuring SAM’s Connector for OTP Authentication, page 8
- Assigning a Token in SAM, page 8
- Adding DenyAll Web Application Firewall as a RADIUS Client in IAS/NPS, page 9
- Configuring SAM’s OTP Plug-In for Microsoft RADIUS Client, page 10

Synchronizing Users Stores to SAM

SAM manages and maintains OTP token information in its data store, including the token status, the OTP algorithm used to generate the OTP, 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
Configuring SAM’s Connector for OTP Authentication

SafeNet Authentication Manager is based on open standards architecture with configurable connectors. This supports integration with a wide range of security applications, including network logon, VPN, web access, one-time password authentication, secure email, and data encryption.

If you selected the **Simplified OTP-only** configuration, SafeNet Authentication Manager is automatically configured with a typical OTP configuration, providing a working SafeNet Authentication Manager OTP solution.

The **Simplified OTP-only** configuration is as follows:

- **Connectors**—SAM Connector for OTP Authentication is installed
- **SAM Back-end Service**—Activated on this server; scheduled to operate every 24 hours

In addition, the SAM default policy is set as follows:

- OTP support (required for OTP) is selected in the **Token Initialization** settings.
- The **SAM Connector for OTP Authentication** is set, by default, to enable enrollment of OTP tokens without requiring changes in the Token Policy Object (TPO) settings. For more information on how to install and configure the SafeNet Authentication Manager for simplified installation, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

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 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)
- SafeNet eToken 3400
- SafeNet eToken 3500

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*.
Adding DenyAll Web Application Firewall as a RADIUS Client in IAS/NPS

For Windows Server 2003, the Windows RADIUS service is Internet Authentication Service (IAS). The IAS is added as the RADIUS server in DenyAll Web Application Firewall.

For Windows Server 2008 and above, the Windows RADIUS service is the Microsoft Network Policy Server (NPS). The NPS server is added as the RADIUS server in DenyAll Web Application Firewall.

DenyAll Web Application Firewall must be added as a RADIUS client on the IAS/NPS server so that IAS/NPS will authorize DenyAll Web Application Firewall for authentication.

NOTE: It is assumed that IAS/NPS policies are already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager.

The details below refer to NPS, and are very similar to IAS.

1. Click **Start > Administrative Tools > Network Policy Server**.
2. From the NPS web console, in the left pane, expand **RADIUS Clients and Servers**, right-click **RADIUS Clients**, and then click **New**.

   ![Network Policy Server](image)

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

3. On the **New RADIUS Client** window, on the **Settings** tab, complete the following fields:

   | **Enable this RADIUS client** | Select this option. |
   | **Friendly name** | Enter a RADIUS client name. |
   | **Address (IP or FQDN)** | Enter the DenyAll Web Application Firewall IP address. |
   | **Manual/Generate** | Select **Manual**. |
   | **Shared secret** | Enter the shared secret for the RADIUS client. This entry must match the shared secret that was used when the RADIUS server was configured in DenyAll Web Application Firewall. |
   | **Confirm shared secret** | Re-enter the shared secret. |
4. Click OK. DenyAll Web Application Firewall is added as a RADIUS client in NPS.

**Configuring SAM’s OTP Plug-In for Microsoft RADIUS Client**

RADIUS protocol is used for authentication and authorization. The SafeNet OTP solution supports the Microsoft IAS service (used in Windows 2003) and Microsoft NPS service (used in Windows 2008 and later) as Windows services running a RADIUS server. These services may be extended by adding plug-ins for the authentication process.

SAM’s OTP plug-in for Microsoft RADIUS Client works with Microsoft’s IAS or NPS to provide strong, authenticated remote access through the IAS or NPS RADIUS server. When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet Authentication Manager OTP plug-in, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.
Configuring DenyAll Web Application Firewall

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

- Adding SAM as a RADIUS Server in DenyAll Web Application Firewall, page 11
- Adding RADIUS Authentication to a Workflow, page 17

Adding SAM as a RADIUS Server in DenyAll Web Application Firewall

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

3. On the Management i-Box main window, click the Policies tab.
4. In the left pane, click **WAM > Perimeter Gates > Authentication Servers**, and then in the right pane, click **Add**.

![DenyAll® software](image)

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

5. On the **Add Authentication Server** window, complete the following steps:

   a. On the **General** tab, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the authentication server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select <strong>RADIUS</strong>.</td>
</tr>
<tr>
<td>Datastore</td>
<td>Click the icon adjacent to this field, and then click <strong>Add &gt; Add</strong>.</td>
</tr>
</tbody>
</table>

![Add Authentication Server](image)

(The screen image above is from DenyAll® software. Trademarks are the property of their respective owners.)
b. On 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 data store.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Select <strong>RADIUS</strong>.</td>
</tr>
<tr>
<td><strong>RADIUS Servers IPs</strong></td>
<td>Enter IP address of the SAM RADIUS server.</td>
</tr>
</tbody>
</table>

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

c. On the **Add Authentication Server** window, on the **General** tab, complete the following fields, and then click **OK**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>N.A.S</strong></td>
<td>Enter the IP address of the DenyAll interface that will be used to reach SAM.</td>
</tr>
<tr>
<td><strong>Shared secret</strong></td>
<td>Enter the same shared secret that you entered in step 3 of “Adding DenyAll Web Application Firewall as a RADIUS Client in IAS/NPS” on page 9.</td>
</tr>
</tbody>
</table>

(The screen image above is from DenyAll® software. Trademarks are the property of their respective owners.)
6. On the **Policies** tab, in the left pane, click **WAM > Perimeter Gates > Gates Network Configurations**.

7. Click **Add**.

![Image](image.png)

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

8. On the **Add Gates Network Configuration** window, complete the following details, and then click **OK**.

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Enter a name for the gates network.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>i-Box</strong></td>
<td>Select an appropriate i-Box.</td>
</tr>
<tr>
<td><strong>IP</strong></td>
<td>Enter the listening IP address of the WAM engine. This IP address must not be contactable by the clients.</td>
</tr>
</tbody>
</table>

![Image](image.png)

*(The screen image above is from DenyAll® software. Trademarks are the property of their respective owners.)*
9. On the Policies tab, in the left pane, click **WAM > Perimeter Gates**.

10. Click **Add**.

11. On the **Add Perimeter Gate** window, on the **General** tab, complete the following details:

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the perimeter gate.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAM listeners</td>
<td>Select the IAM listener that you created in step 8 (for example, <strong>RadiusAuth</strong>).</td>
</tr>
</tbody>
</table>

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

13. In the Authentication method field, select Form.

![Image of Add Perimeter Gate](image1)

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

14. Click the Authentication Backends tab, complete the following fields, and then click OK:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal authentication server</td>
<td>Clear this option.</td>
</tr>
<tr>
<td>Authentication server type</td>
<td>Select RADIUS.</td>
</tr>
<tr>
<td>Authentication Server</td>
<td>Select the authentication server that you created in step 5.</td>
</tr>
</tbody>
</table>

![Image of Add Perimeter Gate](image2)

(In the screen image above is from DenyAll® software. Trademarks are the property of their respective owners.)
Adding RADIUS 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 RADIUS authentication.

The workflow used in this integration is shown below.

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

![Image of DenyAll® software]

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

2. Select the workflow on which you want to add RADIUS authentication, and then click Open.

![Another image of DenyAll® software]

(The screen image above is from DenyAll® software. Trademarks are the property of their respective owners.)
3. In the right pane, on the **Tools** tab, click **Authentication**, and then drag and drop the **WAM Perimeter Authentication** tool in the appropriate location in the workflow.

4. Double-click **WAM Perimeter Authentication** in the workflow.

5. On the **Modify WAM Perimeter Authentication** window, on the **General** tab, 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><strong>Perimeter gate</strong></td>
<td>Select the perimeter gate that you created earlier in step 11 of “Adding SAM as a RADIUS Server in DenyAll Web Application Firewall” on page 11.</td>
</tr>
<tr>
<td><strong>Perimeter gate IP port</strong></td>
<td>Select the Gates Network Configuration created earlier in step 8 of “Adding SAM as a RADIUS Server in DenyAll Web Application Firewall” on page 11.</td>
</tr>
</tbody>
</table>

(The screen image above is from DenyAll® software. Trademarks are the property of their respective owners.)
6. On your workflow window, click **Save**.

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

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

9. Complete the following fields, and then click **OK**.

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

(The screen image above is from DenyAll® software. Trademarks are the property of their respective owners.)
10. In the top right corner, click **Apply**.

![DenyAll Management Interface with Apply button highlighted](image1.png)

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

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

![DenyAll Apply Configuration Window](image2.png)

(The screen image above is from DenyAll® software. Trademarks are the property of their respective owners.)
12. 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. In a web browser, enter the URL on which reverse proxy web application is configured.
2. On the **Authentication** window, complete the following fields, and then click **Connection**:

<table>
<thead>
<tr>
<th>Login</th>
<th>Enter your user name.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password</strong></td>
<td>Generate an OTP using the SafeNet eToken PASS token, and then enter that OTP in this field.</td>
</tr>
</tbody>
</table>

![Authentication window](image)

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

If the credentials are validated, you are provided access to the web application hosted as reverse proxy on DenyAll Web Application Firewall.

![Reverse proxy web application](image)
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</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td><strong>Technical Support</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Customer Portal</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td></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>