SafeNet Authentication Service
Integration Guide

Using RADIUS Protocol for Enterprise Random Password Manager
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 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:** 007-013669-001, Rev. A

**Release Date:** December 2016
Contents

Third-Party Software Acknowledgement ........................................................................................................ 4
Description ....................................................................................................................................................... 4
Applicability ................................................................................................................................................... 4
Environment .................................................................................................................................................. 5
Audience ......................................................................................................................................................... 5
RADIUS-based Authentication using SafeNet Authentication Service Cloud ............................................... 5
RADIUS-based Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication
Service-PCE ................................................................................................................................................... 6
RADIUS Authentication Flow using SafeNet Authentication Service ............................................................. 6
RADIUS Prerequisites .................................................................................................................................... 7
Configuring SafeNet Authentication Service .................................................................................................. 7
  Creating Users Stores in SafeNet Authentication Service ....................................................................... 7
  Assigning an Authenticator in SafeNet Authentication Service................................................................. 8
  Adding Enterprise Random Password Manager as an Authentication Node in SafeNet Authentication Service.......................................................... 9
  Checking the SafeNet Authentication Service RADIUS Address .......................................................... 10
Configuring Enterprise Random Password Manager ................................................................................... 12
  Single Factor Authentication .................................................................................................................. 12
  Configuring for Two-factor Authentication .............................................................................................. 15
Running the Solution .................................................................................................................................... 19
  Single Factor Authentication .................................................................................................................. 19
  Two-factor Authentication ....................................................................................................................... 20
  GridSure Token ...................................................................................................................................... 21
Appendix: Customizing the LoginRadius Page ............................................................................................ 23
Support Contacts .......................................................................................................................................... 24
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Enterprise Random Password Manager.

Material from Enterprise Random Password Manager software is being used solely for the purpose of making instructions clear. Screen images and content obtained from Enterprise Random Password Manager will be acknowledged as such.

Description

SafeNet Authentication Service (SAS) 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.

Enterprise Random Password Manager (ERPM) from Lieberman Software is a proactive authentication and protection system designed to secure networks against cyber-attack. ERPM streamlines the management and monitoring of authentication and credentials, thereby reducing the chances that critical, confidential data may be compromised. Through ERPM, organizations can follow authentication and identity best practices without having to create involved safety procedures and protocols.

This document describes how to:

• Deploy multi-factor authentication (MFA) options in Enterprise Random Password Manager using SafeNet one-time password (OTP) authenticators managed by SafeNet Authentication Service.

• Configure Enterprise Random Password Manager to work with SafeNet Authentication Service in RADIUS mode.

It is assumed that the Enterprise Random Password Manager environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Enterprise Random Password Manager 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 – Private Cloud Edition (SAS-PCE)**
- **Enterprise Random Password Manager—Version 5.5.0**

Audience

This document is targeted to system administrators who are familiar with Enterprise Random Password Manager, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

**RADIUS-based Authentication using SafeNet Authentication Service Cloud**

SafeNet Authentication Service (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 details on how to install and configure FreeRADIUS, refer to the SafeNet Authentication Service FreeRADIUS Agent Configuration Guide.

### RADIUS-based Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE

For both on-premises versions, SafeNet Authentication Service (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 SafeNet Authentication Service

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 Enterprise Random Password Manager.

![RADIUS Authentication Flow Diagram](image)

1. A user attempts to log on to the web application of the Enterprise Random Password Manager (ERPM) using an OTP authenticator.
2. ERPM sends a RADIUS request with the user’s credentials to SafeNet Authentication Service (SAS) for validation.
3. The SAS authentication reply is sent back to ERPM.
4. The user is granted or denied access to the ERPM web application based on the OTP value calculation results from SAS.
RADIUS Prerequisites

To enable SafeNet Authentication Service (SAS) to receive RADIUS requests from Enterprise Random Password Manager, ensure the following:

- End users can authenticate from the Enterprise Random Password Manager environment with a static password before configuring ERPM to use RADIUS authentication.
- Ports 1812/1813 are open to and from Enterprise Random Password Manager.
- 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.
- User should be created with the explicit account of the ERPM

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with Enterprise Random Password Manager using RADIUS protocol requires the following:

- Creating Users Stores in SafeNet Authentication Service, page 7
- Assigning an Authenticator in SafeNet Authentication Service, page 8
- Adding Enterprise Random Password Manager as an Authentication Node in SafeNet Authentication Service, page 8
- Checking the SafeNet Authentication Service RADIUS Address, page 10

Creating Users Stores in SafeNet Authentication Service

Before SafeNet Authentication Service (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 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 SafeNet Authentication Service

SafeNet Authentication Service (SAS) supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through Enterprise Random Password Manager.

The following authenticators are supported:

- eToken PASS
- RB-1 Keypad Token
- KT-4 Token
- SafeNet Gold
- SMS Token
- MP-1 Software Token
- MobilePASS
- GrIDsure Authentication

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 Enterprise Random Password Manager as an Authentication Node in SafeNet Authentication Service

Add a RADIUS entry in the SafeNet Authentication Service (SAS) **Auth Nodes** module to prepare it to receive RADIUS authentication requests from Enterprise Random Password Manager. You will need the IP address of Enterprise Random Password Manager and the shared secret to be used by both SAS and Enterprise Random Password Manager.

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 addresses that will authenticate with SAS (in this case, a range of IP addresses is being used).</td>
</tr>
<tr>
<td>High IP Address In Range</td>
<td>Enter the highest IP address in a range of IP addresses that will authenticate with SAS (in this case, a range of IP addresses is being used).</td>
</tr>
<tr>
<td>Configure FreeRADIUS Synchronization</td>
<td>Select this option.</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 SafeNet Authentication Service RADIUS Address

Before adding SafeNet Authentication Service (SAS) as a RADIUS server in Enterprise Random Password Manager, check its IP address. The IP address will then be added to Enterprise Random Password Manager 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 Enterprise Random Password Manager

Configure Enterprise Random Password Manager (ERPM) for:

- Single factor authentication
- Two-factor authentication

Single Factor Authentication

Add an authentication server to configure ERPM for single factor authentication.

1. Double-click the ERPM icon to open the ERPM configuration tool.
2. In the ERPM configuration tool, on the Delegation tab, click Authentication Servers.

![Configuration tool image](image1)

3. On the Authentication Servers window, click on Add RADIUS.

   ![Configuring RADIUS](image2)

4. On the RADIUS Authentication Server Settings window, perform the following steps:
   a. Complete the following fields:
      
      | Field          | Description                                      |
      |----------------|--------------------------------------------------|
      | Authenticator ID | Enter a name for the RADIUS server (for example, SAS). |
      | Server Name     | Enter the domain name of the RADIUS Server (for example, rad1.safenet-inc.com). |
      | IP address      | Enter the IP address of the RADIUS server.         |
      | Port            | Enter 1812.                                       |
**Shared Secret**  
Enter the shared secret that you entered earlier in step 5 of “Adding Enterprise Random Password Manager as an Authentication Node in SafeNet Authentication Service” on page 9.

b. Select **Show as an Authentication Server Option in Web Interface**.

c. Click **OK**.

![RADIUS Authentication Server Settings](image)

(The screen image above is from Enterprise Random Password Manager™. Trademarks are the property of their respective owners.)

**NOTE**: Once the RADIUS server is configured, use the **Connection Verification** section to validate authentication to the RADIUS server.

5. On the **Authentication Servers** window, select the RADIUS server (for example, **SAS**) that you added earlier in step 4, and then click **OK**.

![Authentication Servers](image)

(The screen image above is from Enterprise Random Password Manager™. Trademarks are the property of their respective owners.)
6. On the **Delegation** tab, click **Delegation Identities**.

![Delegation Identities](image)

(The screen image above is from Enterprise Random Password Manager™. Trademarks are the property of their respective owners.)

7. On the **Delegation Identities** window, click **Add**.

![Add Delegation Identity](image)

(The screen image above is from Enterprise Random Password Manager™. Trademarks are the property of their respective owners.)

8. On the **Add Delegation Identity** window, under **Role Type**, perform the following steps:
   a. Select **RADIUS User**, and then enter the SAS username (for example, *alice*).
   b. In the **RADIUS Server** field, select the RADIUS server (for example, *SAS*) that you added earlier in step 4.
   c. Click **OK**.

![Add Delegation Identity](image)

(The screen image above is from Enterprise Random Password Manager™. Trademarks are the property of their respective owners.)
9. On the **Delegation Identities** window, the SAS user (for example, alice) is listed. Click **OK**.

![Delegation Identities window](image)

*(The screen image above is from Enterprise Random Password Manager™. Trademarks are the property of their respective owners.)*

**Configuring for Two-factor Authentication**

1. In the ERPM configuration tool, on the **Delegation** tab, click **External 2 Factor Configuration**.

![ERPM configuration tool](image)

*(The screen image above is from Enterprise Random Password Manager™. Trademarks are the property of their respective owners.)*
2. On the **Configure 2 Factor Authentication** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Authenticator Type</th>
<th>Select RADIUS.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticator Label</td>
<td>Enter a name for the authenticator label.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the RADIUS server (for example, SAS)</td>
</tr>
<tr>
<td>Port</td>
<td>Enter 1812.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the shared secret that you entered earlier in step 5 of “Adding Enterprise Random Password Manager as an Authentication Node in SafeNet Authentication Service” on page 9.</td>
</tr>
</tbody>
</table>

![Configure 2 Factor Authentication](image)

(The screen image above is from Enterprise Random Password Manager™. Trademarks are the property of their respective owners.)

**NOTE**: Once the RADIUS server is configured, use the **Test Authentication** section to validate authentication to the RADIUS server.

3. On the **Delegation** tab, click **Web Application Global Delegation Permissions**.

![Web Application Global Delegation Permissions](image)

(The screen image above is from Enterprise Random Password Manager™. Trademarks are the property of their respective owners.)
4. On the **Web Application Global Delegation Permissions** window, perform the following steps:
   a. Under **Delegation Identities**, select the explicit target identity (for example, **alice**).
   c. Click **OK**.

![Web Application Global Delegation Permissions](image1)

*(The screen image above is from Enterprise Random Password Manager™. Trademarks are the property of their respective owners.)*

5. In the left pane, click **Manage Web App**.

![Manage Web App](image2)

*(The screen image above is from Enterprise Random Password Manager™. Trademarks are the property of their respective owners.)*
6. On the Manage Web Application Instances window, select the web application instance, and then click Edit.

![Manage Web Application Instances](image1)

(The screen image above is from Enterprise Random Password Manager™. Trademarks are the property of their respective owners.)

7. On the pop-up window, click Yes.

![Enterprise Random Password Manager - Confirm S...](image2)

(The screen image above is from Enterprise Random Password Manager™. Trademarks are the property of their respective owners.)

8. On the Web Application Settings window, on the Multi-Factor Authentication (MFA) tab, select Enable external and internal MFA, and then click OK.

![Web Application Settings](image3)

(The screen image above is from Enterprise Random Password Manager™. Trademarks are the property of their respective owners.)
NOTE: For single factor authentication, select No MFA.

9. On the pop-up window, click OK, and then on the Manage Web Application Instances window, click Close.

![Manage Web Application Instances](image)

(The screen image above is from Enterprise Random Password Manager™. Trademarks are the property of their respective owners.)

10. Customize the LoginRadius file to access Enterprise Random Password Manager using the GrIDsure token. Refer to “Appendix: Customizing the LoginRadius Page” on page 23 on page.

Running the Solution

Single Factor Authentication

1. In a web browser, open a web application instance URL. For example:

   http://win-pjvi7jja8j0/PWCWeb/Login.asp

2. On the Enterprise Random Password Manager login window, complete the following fields, and then click Login.

<table>
<thead>
<tr>
<th>Username</th>
<th>Enter your SAS user name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Enter your password.</td>
</tr>
<tr>
<td>Authenticator</td>
<td>Select the RADIUS server (for example, SAS) that you configured earlier.</td>
</tr>
</tbody>
</table>

![Enterprise Random Password Manager](image)

(The screen image above is from Enterprise Random Password Manager™. Trademarks are the property of their respective owners.)
After successful authentication done by the RADIUS server (for example, SAS), the application web page is displayed.

(The screen image above is from Enterprise Random Password Manager™. Trademarks are the property of their respective owners.)

**Two-factor Authentication**

1. In a web browser, open a web application instance URL. For example:
   
   http://win-pjvi7ja8j0/PWCWeb/Login.asp

2. On the Enterprise Random Password Manager login window, complete the following fields, and then click **Login**.

<table>
<thead>
<tr>
<th>Username</th>
<th>Enter your explicit user name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Enter your password.</td>
</tr>
<tr>
<td>Authenticator</td>
<td>Select <strong>Explicit</strong>.</td>
</tr>
</tbody>
</table>

(The screen image above is from Enterprise Random Password Manager™. Trademarks are the property of their respective owners.)
3. After successful authentication, the RADIUS server login window is displayed. In the **Token Code** field, enter the SAS password, and then click **Login**.

![RADIUS Server Login Window](image1)

*(The screen image above is from Enterprise Random Password Manager™. Trademarks are the property of their respective owners.)*

After successful two-factor authentication, the application web page is displayed.

![Application Web Page](image2)

*(The screen image above is from Enterprise Random Password Manager™. Trademarks are the property of their respective owners.)*

**GridSure Token**

1. In a web browser, open a web application instance URL. For example:

   http://win-pjvi7jja8j0/PWCWeb/Login.asp
2. On the Enterprise Random Password Manager login window, complete the following fields, and then click Login.

<table>
<thead>
<tr>
<th>Username</th>
<th>Enter your explicit user name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Enter your password.</td>
</tr>
<tr>
<td>Authenticator</td>
<td>Select Explicit.</td>
</tr>
</tbody>
</table>

(The screen image above is from Enterprise Random Password Manager™. Trademarks are the property of their respective owners.)

3. After successful authentication, the RADIUS server login page is displayed. Click GetGrid.

(The screen image above is from Enterprise Random Password Manager™. Trademarks are the property of their respective owners.)

4. In the Token Code field, enter your preferred grid pattern, and then click Login.

(The screen image above is from Enterprise Random Password Manager™. Trademarks are the property of their respective owners.)
After successful two-factor authentication, the application web page is displayed.

(The screen image above is from Enterprise Random Password Manager™. Trademarks are the property of their respective owners.)

**Appendix: Customizing the LoginRadius Page**

1. Go to web server path (for example, `c:\inetpub\wwwroot\PWCWeb`).
2. Open the **LoginRadius** asp file.
3. In the file, search for the following content:
   ```html
   <button class="btn btn-default" onclick="javascript:history.go(-1); return false;" <%=AddToolTip("Back")%>>>Back</button>
   ```
4. Enter the following content below the content searched in step 3:
   ```html
   <button class="btn btn-default" onclick="showGrid();" <%=AddToolTip("GetGrid")%>>>GetGrid</button>
   ```
5. Search for the `<script type="text/javascript">` line and then enter the following content below the line:
   ```javascript
   //URL of the BlackShield ID Self Service page
   function showGrid()
   {
     var obj=document.getElementById('CommandForm');
     var uname=document.getElementById('Username');
     obj.innerHTML += '<br><br><img border="1" src="' + gridMakerURL + uname.value + '">';
     uname.readOnly=true;
     uname.style.backgroundColor='gray'
   }
   ```
6. Save the **LoginRadius** asp file.
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
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. |