SafeNet Authentication Service
Push OTP 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: 007-013674-001, 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 Authentication Flow using SafeNet Authentication Service ....................... 5
RADIUS Prerequisites ........................................................................................ 6
Push OTP Prerequisites ....................................................................................... 7
Configuring SafeNet Authentication Service .......................................................... 7
  Creating Users Stores in SafeNet Authentication Service .................................... 7
  Assigning an Authenticator in SafeNet Authentication Service ............................ 7
  Adding Enterprise Random Password Manager as an Authentication Node in SafeNet Authentication Service ................................................................. 8
  Checking the SafeNet Authentication Service RADIUS Address ....................... 10
  Enabling the Software Token Push OTP Setting ............................................... 11
  Enabling the Allowed Targets Policy .................................................................. 12
Configuring Enterprise Random Password Manager ............................................. 14
Running the Solution ............................................................................................ 17
  Simple Mode .................................................................................................... 17
  Hybrid Mode ................................................................................................... 19
Appendix: Customizing the LoginRadius Page ..................................................... 21
  Simple Mode .................................................................................................... 21
  Hybrid Mode ................................................................................................... 22
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 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.

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 Push one-time password (OTP) solution 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 Push OTP solution.

The primary objective of the Push OTP solution is to reduce the friction around two-factor authentication, and provide users with an improved two-factor authentication experience.

It’s likely that most users already own and always carry a device that can be used as a second factor of authentication. Using the mobile phone as an authenticator replaces the need for a user to carry any additional hardware. So, with Push OTP, a user can:

• Receive authentication requests in real-time via push notifications to his or her smart phone.

• Assess the validity of the request with the information displayed on the screen.

• Respond quickly with a one-tap response to approve or deny the authentication.

Applicability

The information in this document applies to:

• SafeNet Authentication Service (SAS)—SafeNet’s cloud-based authentication service

• MobilePASS+ application
**Environment**

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Service (SAS)**
- **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 the following RADIUS topology that supports Push OTP tokens:

*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.

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

**RADIUS Authentication Flow using SafeNet Authentication Service**

SafeNet Authentication Service (SAS) 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 Enterprise Random Password Manager.

1. A user attempts to log on to web application of the Enterprise Random Password Manager (ERPM) using a Push OTP authenticator.
2. ERPM sends a RADIUS request with the user's credentials to SafeNet Authentication Service (SAS) for validation.
3. SAS identifies the user or mobile device, and detects that the OTP field is empty. Then:
   - SAS will directly trigger a Push OTP authentication request.
   - The user receives a push notification on the configured mobile device to indicate that there is a login request pending.
   - The user taps on the notification to view the login request details, and can respond with a tap to approve or deny the request (approving will require providing the token's PIN code).
4. The SAS authentication reply is sent back to ERPM.
5. The user is granted or denied access to web application of the ERPM 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 the Enterprise Random Password Manager 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.
- On the client machine, set the RADIUS timeout value at least 60 seconds.
Push OTP Prerequisites

In order to use SafeNet Authentication Service (SAS) Push OTP you will need:

- SafeNet Authentication Service configured to enable Push OTP
- MobilePASS+ application

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service 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 7
- Adding Enterprise Random Password Manager as an Authentication Node in SafeNet Authentication Service, page 8
- Checking the SafeNet Authentication Service RADIUS Address, page 10
- Enabling the Software Token Push OTP Setting, page 11
- Enabling the Allowed Targets Policy, page 12

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:

- 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 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 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 click **Auth Nodes**.
3. In the **Auth Nodes** module, click the **Auth Nodes** link, and then click **Add**.

![Auth Nodes](image)

4. Under **Add Auth Nodes**, complete the following fields, and then click **Save**:

<table>
<thead>
<tr>
<th><strong>Auth Node Name</strong></th>
<th>Enter a host description.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Resource Name</strong></td>
<td>Enter a resource name which will identify in a push notification which authentication node it relates to.</td>
</tr>
<tr>
<td><strong>Low IP Address In Range</strong></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><strong>High IP Address In Range</strong></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><strong>Configure FreeRADIUS Synchronization</strong></td>
<td>Select this option.</td>
</tr>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter the shared secret key.</td>
</tr>
<tr>
<td><strong>Confirm Shared Secret</strong></td>
<td>Re-enter the shared secret key.</td>
</tr>
</tbody>
</table>
The authentication node is added to the system.

<table>
<thead>
<tr>
<th>Auth Nodes:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary RADIUS Server IP: 109.73.129.148:1812</td>
</tr>
<tr>
<td>Fallback RADIUS Server IP: 69.20.230.201:1812</td>
</tr>
<tr>
<td>Primary SafeNet Authentication Service Agent DNS: agent1.safenet-inc.com:443</td>
</tr>
<tr>
<td>Fallback SafeNet Authentication Service Agent DNS: agent2.safenet-inc.com:443</td>
</tr>
</tbody>
</table>

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 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 click Auth Nodes.
3. In the **Auth Nodes** module, click the **Auth Nodes** link. The SAS RADIUS server details are displayed.

---

### Enabling the Software Token Push OTP Setting

To use Push OTP authentication, the Software Token Push OTP setting must be enabled in the SafeNet Authentication Service (SAS) token policy.

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

![Policy Tab](image)

2. Click the **POLICY** tab, and then click **Token Policies**.

![Token Policies](image)
3. In the **Token Policies** module, click the **Software Token Push OTP Setting** link.

4. Select **Enable Push OTP communication with MobilePass+**, and then click **Apply**.

**Enabling the Allowed Targets Policy**

For Push OTP to be permitted during authentication the user must have a MobilePASS+ token enrolled and this policy must be enabled.

The settings to enable this policy will determine which OS targets are presented to users during the self-enrollment of MobilePASS tokens. You can restrict the targets on which MobilePASS+ or MobilePASS 8 tokens are allowed to be activated or enrolled.

1. Log in to the SafeNet Authentication Service (SAS) console with an Operator account.
2. Click the **POLICY** tab, and then click **Token Policies**.

![Policy tab screenshot](image)

3. In the **Token Policies** module, click the **Allowed Targets Settings** link.

![Token Policies module screenshot](image)

4. On the **MobilePASS** tab, select the desired targets to allow for each MobilePASS application for this virtual server, and then click **Apply**.

![MobilePASS tab screenshot](image)
Configuring Enterprise Random Password Manager

Configure two-factor authentication in Enterprise Random Password Manager (ERPM).

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

![Configuration Tool Screenshot](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.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the RADIUS server (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 the step 4 of “Adding Enterprise Random Password Manager as an Authentication Node in SafeNet Authentication Service” on page 8.</td>
</tr>
</tbody>
</table>

![Authentication Configuration](image)

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

![Delegation tab](image1)

*(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 target identity (for example, **alice**).
   b. Under **Global Identity Rules**, and select **Require Ext 2-Factor Auth**.
   c. Click **OK**.

![Delegation permissions](image2)

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

6. On the Manage Web Application Instances window, select the web application instance, and then click Edit.

7. On the pop-up window, click Yes.
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](image)

(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 in the Simple mode and Hybrid mode. Refer to “Appendix: Customizing the LoginRadius Page” on page 21.

Running the Solution

Simple Mode

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>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter your explicit user name.</td>
</tr>
<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 Login.

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

4. On the registered mobile device, tap APPROVE to accept the OTP request.
5. On the **TOKEN AUTHENTICATION** screen, enter the token PIN, and then tap **Continue** to send the approval with OTP to SAS.

![TOKEN AUTHENTICATION screen](image)

A success message is displayed on the mobile device.

![Success message](image)

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

![Application web page](image)

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

**Hybrid Mode**

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>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter your explicit user name.</td>
</tr>
<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. Select either Use my mobile to autosend passcode or Enter passcode manually, and then click Login.

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

**NOTE:** In this scenario, the Use mobile to autosend passcode option is selected.

4. On the mobile device, tap APPROVE to accept the OTP request.
5. On the **TOKEN AUTHENTICATION** screen, enter the token PIN, and then tap **Continue** to send the approval with OTP to SAS.

![TOKEN AUTHENTICATION screen](image)

A success message is displayed on the mobile device.

**Autosend passcode was successful.**

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

![Application web page](image)

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

**Appendix: Customizing the LoginRadius Page**

**Simple Mode**

1. Go to the web server path (for example, `c:\inetpub\wwwroot\PWCWeb`).
2. Open the **LoginRadius** asp file.
3. In the file, search for the following content:
   `<% OutputBootstrapPanelPasswordInput "", "", "Token Code", "RadiusPasscode", "", "Token Code", "", false %>`

4. Replace the content searched in Step 3 with the following content:
   `<%
   %>
   <tr>
   <td> <span id = "PassLabel" name = "PassLabel" style = "display:none;" langauge = "LOCALIZED_STRING"> Token Code </span> </td>
   <td>
   <input type = "password" class = "form-control input-sm" style = "width:100%;display:none;" placeHolder ="Token Code" name ="RadiusPasscode" id = "RadiusPasscode" value="p" />
   </td>
   </tr>`

5. Save the LoginRadius asp file.

**Hybrid Mode**

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:
   `<% OutputBootstrapPanelPasswordInput "", "", "Token Code", "RadiusPasscode", "", "Token Code", "", false %>`

4. Replace the content searched in step 3 with the following content:
   `<%
   %>
   <tr>
   <td> <span id = "PassLabel" name = "PassLabel" style = "display:none;" langauge = "LOCALIZED_STRING"> Token Code </span> </td>
   <td>
   <input type = "password" class = "form-control input-sm" style = "width:100%;display:none;" placeHolder ="Token Code" name ="RadiusPasscode" id = "RadiusPasscode" value="p" />
   </td>
   </tr>`
5. Search for the `<div class="panel-footer">` line, and then copy the following content below it:

```html
<div>
  <input type="radio" id="rdoPassword" name="rdoPassword" onClick='pushOTP(true);' checked > Use my mobile to autosend passcode
</div>

6. Search for the `<script type="text/javascript">` line and then copy the following content below it.

```javascript
function pushOTP(value)
{
  if(value != false)
  {
    document.getElementById("RadiusPasscode").value = "p";
    document.getElementById("RadiusPasscode").style.display = "none";
    document.getElementById("PassLabel").style.display = "none";
  }
  else
  {
    document.getElementById("RadiusPasscode").value = "";
    document.getElementById("RadiusPasscode").style.display = "block";
    document.getElementById("PassLabel").style.display = "block";
  }
}
```

7. 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>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>Gemalto</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>