SafeNet Authentication Service
Push OTP Integration Guide
Using RADIUS Protocol for Pulse Connect Secure
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:** 007-013338-001, Rev. B

**Release Date:** November 2015
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Pulse Connect Secure.

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.

The Pulse Connect Secure appliances meet the needs of companies of all sizes. The Junos Pulse Gateway MAG series appliances use SSL—the security protocol found in all standard web browsers. The use of SSL eliminates the need for pre-installed client software, changes to internal servers, and costly ongoing maintenance and desktop support. The SA Series also offers sophisticated partner/customer extranet features that enable controlled access to differentiated users and groups without requiring infrastructure changes, demilitarized zone (DMZ) deployments, or software agents.

This document describes how to:


- Configure Pulse Connect Secure to work with SafeNet Authentication Service in RADIUS mode.

It is assumed that the Pulse Connect Secure environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Pulse Connect Secure can be configured to support multi-factor authentication in several modes. The RADIUS protocol will be used for the purpose of working with the 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)**—Cloud version 3.5
- **Pulse Connect Secure Gateway**—Version 7.2R2

Audience

This document is targeted to system administrators who are familiar with Pulse Connect Secure, 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:

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

**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 dataflow of a multi-factor authentication transaction for Pulse Connect Secure.

1. A user attempts to log on to Pulse Connect Secure using a Push OTP authenticator.
2. Pulse Connect Secure sends a RADIUS request with the user’s credentials to SafeNet Authentication
   Service 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 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 Pulse Connect Secure.
5. The user is granted or denied access to Pulse Connect Secure based on the OTP value calculation results
   from SAS.
RADIUS Prerequisites

To enable SafeNet Authentication Service to receive RADIUS requests from Pulse Connect Secure, ensure the following:

- End users can authenticate from the Pulse Connect Secure environment with a static password before configuring the Pulse Connect Secure to use RADIUS authentication.
- Ports 1812/1813 are open to and from Pulse Connect Secure.
- 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

To use Push OTP, you will need:

- SAS configured to enable Push OTP
- MobilePASS which is supported on the following OS platforms:
  - MobilePASS+ (Push OTP support)
    - Android 4.x, 5.x
    - iOS 7+

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with Pulse Connect Secure using RADIUS protocol requires the following:

- Creating Users Stores in SAS, page 7
- Assigning an Authenticator in SAS, page 8
- Adding Pulse Connect Secure as an Authentication Node in SAS, page 9
- Checking the SAS RADIUS Server’s IP Address, page 11
- Enabling the Software Token Push OTP Setting, page 12
- Enabling the Allowed Targets Policy, page 13

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 who 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 Pulse Connect Secure.

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 Pulse Connect Secure 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 Pulse Connect Secure. You will need the IP address of Pulse Connect Secure and the shared secret to be used by both SAS and Pulse Connect Secure.

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>Auth Node Name</th>
<th>Enter a host description.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Name</td>
<td>Enter a resource name which will identify in a push notification which authentication node it relates to.</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.</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.</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 SAS RADIUS Server’s IP Address

Before adding SAS as a RADIUS server in Pulse Connect Secure, check its IP address. The IP address will then be added to Pulse Connect Secure 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.
Enabling the Software Token Push OTP Setting

To use Push OTP authentication, the setting must be enabled in the SAS token policy.

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

2. Click the POLICY tab, and then select Token Policies.

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 SAS console with an Operator account.

2. Click the POLICY tab, and then select Token Policies.
3. In the **Token Policies** module, click the **Allowed Targets Settings** link.

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

Configuring the Pulse Connect Secure to use SAS RADIUS authentication requires the following:

- Creating a RADIUS Authentication Server, page 15
- Configuring an Authentication Realm, page 18
- Configuring Push OTP Hybrid Mode, page 22

Creating a RADIUS Authentication Server

1. Open the Pulse Connect Secure admin console.

(The screen image above is from Pulse Secure®. Trademarks are the property of their respective owners.)
2. In the left pane, select **Authentication > Auth. Servers**.

![Authentication Servers](image1.png)

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

3. In the **New** menu, select **Radius Server**, and then click **New Server**.

![New Server](image2.png)

(The screen image above is from Pulse Secure®. Trademarks are the property of their respective owners.)
4. On the **Settings** tab, complete the following, and the click **Save Changes** at the bottom of the page:

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter the server name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAS-Identifier</td>
<td>Enter the name of the device.</td>
</tr>
<tr>
<td>Radius Server</td>
<td>Enter the IP address of the SAS RADIUS server.</td>
</tr>
<tr>
<td>Authentication Port</td>
<td>Enter the RADIUS authentication port number. The default is 1812.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the RADIUS shared secret.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Set the value to <strong>60</strong> seconds.</td>
</tr>
</tbody>
</table>

Do not change the other default values.

![Screen Image](image-url)

*(The screen image above is from Pulse Secure®. Trademarks are the property of their respective owners.)*
Configuring an Authentication Realm

After the RADIUS authentication server is created, assign it to a user authentication realm.

1. Open the Pulse Connect Secure admin console.
2. In the left pane, select Users > Users Realms.

3. In the Authentication Realm table, click Users.

(The screen image above is from Pulse Secure®. Trademarks are the property of their respective owners.)
4. On the **General** tab, select the **Additional authentication server** check box, and then complete the following fields:

<table>
<thead>
<tr>
<th>Authentication #2</th>
<th>Select the RADIUS authentication server that you created in the previous section (for example, SAS-RADIUS).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username is</td>
<td>Select predefined as: &lt;USER&gt;.</td>
</tr>
<tr>
<td>Password is</td>
<td>Select predefined as, and leave the letter <strong>p</strong>.</td>
</tr>
</tbody>
</table>

5. Click the **Role Mapping** tab, and then click **New Rule**.
6. In the **Role Mapping Rule** window, complete the following fields, and then click **Save Changes**:

<table>
<thead>
<tr>
<th>Rule based on</th>
<th>Select Username.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the rule.</td>
</tr>
<tr>
<td>Rule: If username...</td>
<td>Select a user or a list of users that need to authenticate to the realm.</td>
</tr>
<tr>
<td>...then assign these roles</td>
<td>Select a role from the <strong>Available Roles</strong> window, and then click <strong>Add</strong> to move it to the <strong>Selected Roles</strong> window. Repeat as needed to add more roles.</td>
</tr>
</tbody>
</table>

(The screen image above is from Pulse Secure®. Trademarks are the property of their respective owners.)
7. Go back to the User Authentication Realm you created and press on **Authentication Policy**

![Authentication Policy](image1.png)

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

8. Press on **Password**, and under **Options for primary authentication server**, select **Allow all users (passwords of any length)**

   Also under **Options for additional authentication server**, select **Allow all users (passwords of any length)**

   ![Password Options](image2.png)

   (The screen image above is from Pulse Secure®. Trademarks are the property of their respective owners.)
**Configuring Push OTP Hybrid Mode**

To configure Pulse Connect Secure to support Push OTP Hybrid mode, you will need to configure Pulse Connect Secure to support an additional authentication field, and then upload the login page package to replace the default login page.

1. Open the Pulse Connect Secure admin console.
2. In the left pane, select **Users > User Realms**.

![Image of Pulse Connect Secure admin console](https://www.pulsesecure.net/images/pulseconnectsecure.png)

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

3. In the **Authentication Realm** table, click the user realm you created in the previous section.
4. Under **Additional authentication server**, where Safenet Authentication Service is configured, under **Password is:** select the **Specified by user on sign-in page** radio button.
5. Next, upload the login page package to replace the default page. In the left pane, select Authentication > Signing In, and then click the Sign-in Pages tab.

6. Click Upload Custom Pages.

7. On the Upload Custom Sign-In Pages window, complete the following, and then click Upload Custom Pages:

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the custom sign-in page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Templates File</td>
<td>Click Choose File, and then select the following zip file: Sample.ZIP (can be downloaded from inquira DOW4052 - <a href="http://bel1web002:9876/Files/0e001351d8da40ee81b6bd2cd8ce64ea">http://bel1web002:9876/Files/0e001351d8da40ee81b6bd2cd8ce64ea</a>)</td>
</tr>
<tr>
<td>Skip validation checks during upload</td>
<td>Select this check box.</td>
</tr>
</tbody>
</table>
8. When the upload has finished, in the left pane, select **Authentication > Signing In.**

9. Press on your **Sign-in policy.**

10. In the **Sign-in page** menu, select the custom page you created, and then click **Save Changes.**
Running the Solution

After Pulse Connect Secure is configured to use RADIUS with SafeNet Authentication Service, users can log in to the Pulse Connect Secure portal.

Connecting to the Pulse Connect Secure Portal using Simple Mode

In the following scenario, the standard Pulse Connect Secure login page and OOB configuration are used.

1. Login to the Pulse Connect Secure console via the web browser.

2. Enter your LDAP credentials, and then click Sign In.
3. You will then receive a push notification on your mobile. Tap **Approve**.

![MobilePASS+](image)

4. On the **Token Authentication** screen, enter your PIN code, and then tap **Continue**.

![Token Authentication](image)

5. After a successful authentication, you will be logged in to the Pulse Connect Secure portal.

![Pulse Connect Secure](image)

*(The screen image above is from Pulse Secure®. Trademarks are the property of their respective owners.)*
Connecting to the Pulse Connect Secure Portal using Hybrid Mode

In the following scenario, the hybrid mode login screen is used, and you will have the option to choose between authentication using the Push OTP notification message, or manually typing a passcode.

1. Login to the Pulse Connect Secure console via the web browser.

2. Enter your LDAP credentials, and then choose one of the following:
   - **Use my mobile to autosend a passcode**—If you choose this option, a push notification will be sent to your mobile. Follow the steps as described in the previous scenario.
   - **Enter a passcode manually**—If you choose this option, you will need to manually enter a passcode.
     - Open the mobile app, and then tap on the token.
     - On the **Token Authentication** screen, enter your PIN code, and then tap **Continue**.
• You will receive a passcode.

3. In the Pulse Connect Secure console, in the **Additional password** field, enter the passcode, and then click **Sign In**.

![Pulse Connect Secure console](image)

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

4. After a successful authentication, you will be logged in to the Pulse Connect Secure portal.

![Pulse Connect Secure portal](image)

*(The screen image above is from Pulse Secure®. Trademarks are the property of their respective owners.)*
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>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>
<td></td>
</tr>
</tbody>
</table>