SafeNet Authentication Service
Integration Guide

Using RADIUS Protocol for Junos Pulse
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:** 007-012683-001, Rev. C

**Release Date:** November 2015
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-Party Software Acknowledgement</td>
<td>4</td>
</tr>
<tr>
<td>Description</td>
<td>4</td>
</tr>
<tr>
<td>Applicability</td>
<td>4</td>
</tr>
<tr>
<td>Environment</td>
<td>4</td>
</tr>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS-based Authentication using SAS Cloud</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS-based Authentication using SAS-SPE and SAS-PCE</td>
<td>6</td>
</tr>
<tr>
<td>RADIUS Authentication Flow using SAS</td>
<td>6</td>
</tr>
<tr>
<td>RADIUS Prerequisites</td>
<td>7</td>
</tr>
<tr>
<td>Configuring SafeNet Authentication Service</td>
<td>7</td>
</tr>
<tr>
<td>Creating Users Stores in SAS</td>
<td>7</td>
</tr>
<tr>
<td>Assigning an Authenticator in SAS</td>
<td>8</td>
</tr>
<tr>
<td>Adding Junos Pulse as an Authentication Node in SAS</td>
<td>9</td>
</tr>
<tr>
<td>Checking the SAS RADIUS Address</td>
<td>11</td>
</tr>
<tr>
<td>Configuring Junos Pulse</td>
<td>12</td>
</tr>
<tr>
<td>Configuring Junos Pulse Login Pages to Support GrID Authentication</td>
<td>15</td>
</tr>
<tr>
<td>Configuring Sign-In Page to support GrID Authentication</td>
<td>16</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>19</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>21</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 Junos Pulse.

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.

Junos Pulse enables dynamic SSL VPN connectivity, network access control (NAC), mobile security, and collaboration, through a simple end-user interface. It simplifies and optimizes connectivity to end users at the same time it check their device type and security state, location, identity, and adherence to corporate access control policies.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Junos Pulse using SafeNet one-time (OTP) authenticators managed by SafeNet Authentication Service.
- Configure Junos Pulse to work with SafeNet Authentication Service in RADIUS mode.

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

Junos Pulse 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)**—only when using this version. For Cloud not necessary to fill in version number.
- **Junos Pulse**
Audience

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

RADIUS-based Authentication using SAS Cloud

SAS Cloud provides two RADIUS mode topologies:

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

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

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

For more information on how to install and configure SAS Agent for IAS/NPS, refer to: http://www2.gemalto.com/cryptocard/implementation-guides/Microsoft/Blackshield Agent Implementation Guide for Microsoft IAS, NPS.pdf

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

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

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

- **FreeRADIUS**—The SAS FreeRADIUS Agent is a strong authentication agent that is able to communicate with SAS through the RADIUS protocol.

  For more information on how to install and configure the SAS FreeRADIUS Agent, refer to the SafeNet Support Portal.

RADIUS Authentication Flow using SAS

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

The image below describes the data flow of a multi-factor authentication transaction for Junos Pulse.

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

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

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

Configuring SafeNet Authentication Service

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

- Creating Users Stores in SAS, page 7
- Assigning an Authenticator in SAS, page 8
- Adding Junos Pulse as an Authentication Node in SAS, page 8
- Checking the SAS RADIUS Address, page 11

Creating Users Stores in SAS

Before 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 SAS

SAS supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through Junos Pulse.

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

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.

![Auth Nodes module image]

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.</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.

![SAS RADIUS Address](image1)

**Checking the SAS RADIUS Address**

Before adding SAS as a RADIUS server in Junos Pulse, check its IP address. The IP address will then be added to Junos Pulse as a RADIUS server at a later stage.

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

![COMMS Tab](image2)

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.

![Auth Nodes screenshot]

**Configuring Junos Pulse**

1. Connect to Junos Pulse webmin.
2. On the left pane, under **Authentication**, press **Auth. Servers**

![Junos Pulse screenshot]

(The screen image above is from Juniper Networks®. Trademarks are the property of their respective owners.)
3. Open the drop down box, select **Radius server** and then click the **New Server** button

4. Enter the relevant info:

   **Name** – a name for the rule
   **NAS-Identifier** – Name of the device
   **Radius Server** – FQDN or IP of the NPS
   **Shared Secret** – The shared secret that was configured in the NPS

5. Press **Save Changes**
6. Assign the Radius policy you created to the user authentication realm as additional authentication server under **User Realms -> Authentication Realm**

![Image of Junos Pulse configuration interface](image)

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

7. Press **Save Changes**.
Configuring Junos Pulse Login Pages to Support GrID Authentication

In order to use GrID authentication, it is necessary to update the following files:

1. Edit the file gridsure.js

2. Search for the string "<URL of the BlackShield ID Self Service page>"

3. Replace the string with the Safenet SAS self service URL + ?getChallengeImage=true&userName=

   (i.e. https://grid.safenet-inc.com/blackshieldss/O/1MAGXLUGLK/index.aspx?getChallengeImage=true&userName=)

4. Save the page
Configuring Sign-In Page to support GrID Authentication

In order to add support of Safenet SAS GrID authentication to the Junos Pulse, one need to update the Junos Pulse login page.

We will update 3 login pages that support several devices:

- LoginPage.html – Default login page
- LoginPage-ipad.html – iPad login page
- LoginPage-mobile.webkit.html – Default mobile login page
- gridsure.js – contains several js functions that supports the GrID authentication

The following steps describe the process of updating the Junos Pulse sign in pages to support GrID authentication:

1. Login the Junos Pulse webmin and on the left pane select: Authentication -> Signing In

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

2. Select Sign-In Pages

(The screen image above is from Juniper Networks®. Trademarks are the property of their respective owners.)
3. Press **Upload Custom Pages**

4. On the right pane select **Sample**

5. The file sample.zip will be downloaded. Extract the file to a temporary folder.

6. Download the Gridsure customization package (DOW3564 in InQuira) extract the file to another temporary folder, and then copy the following files into the sample.zip extracted temporary folder (replace the existing files):
   a. LoginPage.html
   b. LoginPage-ipad.thtml
   c. LoginPage-mobile-webkit.thtml
   d. gridsure.js

7. Compress the files in the folder to a new zip file

8. Under Name enter a name for the sign in method

9. Under Template Files, press Choose file

10. A file explorer window will be open. Select the new zip file you created and press Upload Custom Pages button
Now we will assign the new Sign-in pages to the Users realm:

1. On the left pane press Authentication -> Signing In
   Under users URL press on /*

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

2. In the Sign In Page drop down box, select the log-in policy name you created in step 7, page 17 and press Save Changes.

   (The screen image above is from Juniper Networks®. Trademarks are the property of their respective owners.)
Running the Solution

In the following solution we will demonstrate the Junos Pulse Safenet SAS GrID authentication on iPad.

1. Login to the Junos Pulse URL

![Login Screen](image1)

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

2. Enter the username, LDAP password and press Get GrID

![Password Entry Screen](image2)

*(The screen image above is from Juniper Networks®. Trademarks are the property of their respective owners.)*
3. The GrID matrix will appear. In the Additional password text box enter your GrID pattern and press on the Sign In button. Upon successful authentication, you will be redirected to the default ssl page

(The screen image above is from Juniper Networks®. 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><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>