SafeNet Authentication Service
Integration Guide

Using RADIUS Protocol for Juniper MAG2600 Junos Pulse Gateway
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:** 007-013192-001, 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 Juniper MAG2600 Junos Pulse Gateway.

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 Juniper MAG2600 Junos Pulse Gateway provides SSL/VPN, network access control (NAC) with Unified Access Control (UAC), or guest access capabilities to SMBs and small and medium enterprises.

Junos Pulse software 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 checks 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 Juniper MAG2600 Junos Pulse Gateway using SafeNet one-time (OTP) authenticators managed by SafeNet Authentication Service.
- Configure Juniper MAG2600 Junos Pulse Gateway to work with SafeNet Authentication Service in RADIUS mode.

It is assumed that the Juniper MAG2600 Junos Pulse Gateway environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Juniper MAG2600 Junos Pulse Gateway 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.
- **Juniper MAG2600 Junos Pulse Gateway**
- **Juniper Junos Pulse**—Version 3.0

Audience

This document is targeted to system administrators who are familiar with Juniper MAG2600 Junos Pulse Gateway, 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.

![Diagram of SAS cloud hosted RADIUS service](image)

- **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.

![Diagram of Local RADIUS hosted on-premises](image)

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:
http://www2.gemalto.com/cryptocard/implementation-guides/Microsoft/Blackshield Agent Implementation
Guide for Microsoft IAS, NPS.pdf

- **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 Juniper MAG2600
Junos Pulse Gateway.

1. A user attempts to log on to Juniper MAG2600 Junos Pulse Gateway using an OTP authenticator.
2. Juniper MAG2600 Junos Pulse Gateway 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 Juniper MAG2600 Junos Pulse Gateway.
4. The user is granted or denied access to the Juniper MAG2600 Junos Pulse Gateway based on the OTP
value calculation results from SAS.
RADIUS Prerequisites

To enable SafeNet Authentication Service to receive RADIUS requests from Juniper MAG2600 Junos Pulse Gateway, ensure the following:

- End users can authenticate from the Juniper MAG2600 Junos Pulse Gateway environment with a static password before configuring the Juniper MAG2600 Junos Pulse Gateway to use RADIUS authentication.
- Ports 1812/1813 are open to and from Juniper MAG2600 Junos Pulse Gateway.
- 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 Juniper MAG2600 Junos Pulse Gateway using RADIUS protocol requires the following:

- Creating Users Stores in SAS, page 7
- Assigning an Authenticator in SAS, page 8
- Adding Juniper MAG2600 Junos Pulse Gateway 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 Juniper MAG2600 Junos Pulse Gateway.

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 Juniper MAG2600 Junos Pulse Gateway 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 Juniper MAG2600 Junos Pulse Gateway. You will need the IP address of Juniper MAG2600 Junos Pulse Gateway and the shared secret to be used by both SAS and Juniper MAG2600 Junos Pulse Gateway.

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**:

   - **Agent Description**: Enter a host description.
   - **Host Name**: Enter the name of the host that will authenticate with SAS.
   - **Low IP Address In Range**: Enter the IP address of the host or the lowest IP address in a range of addresses that will authenticate with SAS.
   - **High IP Address In Range**: Enter the highest IP address in a range of IP addresses that will authenticate with SAS.
   - **Configure FreeRADIUS Synchronization**: Select this option.
   - **Shared Secret**: Enter the shared secret key.
   - **Confirm Shared Secret**: Re-enter the shared secret key.

   The authentication node is added to the system.
Checking the SAS RADIUS Address

Before adding SAS as a RADIUS server in Juniper MAG2600 Junos Pulse Gateway, check its IP address. The IP address will then be added to Juniper MAG2600 Junos Pulse Gateway 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 Juniper MAG2600 Junos Pulse Gateway

Configuring Juniper MAG2600 Junos Pulse Gateway requires the following:

- Adding a RADIUS Authentication Server, page 12
- Attaching an Authentication Server to the User Realm, page 14

Adding a RADIUS Authentication Server

The authentication server that you create in this section will be configured with RADIUS support.

1. Open the Juniper administrator console.
2. Click Authentication, and then click Auth. Servers. The Authentication Servers window is displayed
3. In the New menu, select Radius Server, and then click New Server.
4. Complete the following fields, and then click **Save Changes**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for this server.</td>
</tr>
<tr>
<td><strong>Radius Server</strong></td>
<td>Enter the SAS RADIUS IP address.</td>
</tr>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter the shared secret configured in SAS.</td>
</tr>
</tbody>
</table>

Do not change any default values.

(The screen image above is from Juniper Networks®. Trademarks are the property of their respective owners.)
Attaching an Authentication Server to the User Realm

To use SAS RADIUS authentication, attach the authentication server policy that you created in the previous section to the user realm.

1. Log in to the Juniper administrator console.
2. Click User, and then click User Realms.

3. Under Authentication Realms, click the user realm to edit.
4. Click the General tab.

5. Under Servers, click the Authentication menu, and then select the authentication server that you created in the previous section.
6. Click Save Changes.
Running the Solution

Verify the integration solution after you have successfully configured the Juniper MAG2600 Junos Pulse Gateway for SAS authentication.

1. From the Windows Start menu, select All Programs > Juniper Networks > Junos Pulse > Junos Pulse.
2. In the Junos Pulse client interface, click Connections.
3. In the right pane, select the connection (for example, SAS), and then click Connect.

4. Enter the user credentials in the User Name and Password fields, and then click Connect.
After successful authentication, the user can access the company’s internal network through the VPN.

Configuring Juniper MAG2600 Junos Pulse Gateway Login Pages to Support grID Authentication

Configuring Juniper MAG2600 Junos Pulse Gateway for grIDsure authentication requires the following:

- Updating the grIDsure.js File, page 16
- Configuring the Juniper Login Pages, page 17
- Assigning the grIDsure Sign-in Pages to the User Realm, page 19

Updating the grIDsure.js File

1. Open Notepad or any other text editor, and edit the grIDsure.js file as follows:
   a. Search for the string, `<URL of the BlackShield ID Self Service page>`,
   b. Replace the string with the SafeNet SAS GrIDsure URL, `+ ?getChallengedImage=true&userName=`

   For example:

2. Save the changes to the grIDsure.js file.
Configuring the Juniper Login Pages

To support GrIDsure authentication, the following Juniper login pages must be updated:

- `loginPage.html`—default login page
- `loginPage-ipad.thtml`—iPad login page
- `loginPage-mobile-webkit.thtml`—default mobile login page
- `gridsure.js`—contains several js functions that support the GrID authentication

1. Log in to the Juniper administrator console.
2. Select **Authentication > Signing In**.

   ![Screen Image](image1)

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

3. Click the **Sign-in Pages** tab.

   ![Screen Image](image2)

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

5. In the far-right pane, under **Sample Template Files**, select **Sample**. The file **sample.zip** will be downloaded.

6. Extract the **sample.zip** file and copy the following files into the extracted folder (replace the existing files):
   - `loginPage.html`
   - `loginPage-ipad.html`
   - `loginPage-mobile-webkit.html`
   - `gridsure.js`

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

8. On the **Upload Custom Sign-In Pages** window, under **Sign-in Pages**, complete the following:

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the sign-in method.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template Files</td>
<td>• Select <strong>Choose file</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Select the new zip file you created, and then click <strong>Upload Custom Pages</strong>.</td>
</tr>
</tbody>
</table>
Assigning the GrIDsure Sign-in Pages to the User Realm

1. Log in to the Juniper administrator console.
2. Select **Authentication > Signing In**.
3. Under **User URLs**, click /*.
4. In the **Sign-in Page** menu, select the login policy name that you created in step 8 in “Configuring the Juniper Login Pages” on page 17, and then click **Save Changes**.

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

Verify the integration solution after you have successfully configured the Juniper MAG2600 Junos Pulse Gateway for SAS authentication with GrIdsure. The following example illustrates authenticating with a GrIdsure token to the Juniper MAG2600 Junos Pulse Gateway on an iPad®.

1. Browse to the Junos Pulse URL.
2. Enter your **username** and LDAP **password**, and then tap **Get GrID**. The challenge grid is displayed.

   ![Challenge Grid Example](image)

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

3. In the **Additional password** field, enter the characters from the grid that correspond to your PIP (personal identification pattern), and then tap **Sign In**.

After successful authentication, you will be redirected to the default SSL page.

![SSL Page Example](image)

*(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></td>
</tr>
<tr>
<td>United States</td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td>International</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>