SafeNet Authentication Service (SAS)
Migration Guide

RADIUS Migration Using Microsoft NPS/IAS Agent
All information herein is either public information or is the property of and owned solely by Gemalto 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:** 007-012697-001, Rev. E  
**Release Date:** June 2016
Introduction

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Microsoft® NPS/IAS Agent.

Material from the 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.

NPS/IAS Agent in Migration Mode

Using NPS/IAS Agent to migrate from a third-party OTP solution to a SafeNet Authentication Service (SAS) cloud or on-premises solution is easy and straight forward.
The SAS NPS/IAS Agent is configured between the RADIUS client and the original third-party OTP solution. When an authentication request is received, it is first checked against SAS and, if an error occurs, the request is forwarded to the third-party OTP. This ensures a smooth and easy migration to SAS.

### Advantages and Considerations of SAS Solution

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Easy to set up, and acts as a “wedge” between SAS and other RADIUS server</td>
<td>Need to manage two separate systems for tokens (same as RADIUS tokens)</td>
</tr>
<tr>
<td>No heavy configuration in SAS for user/token association for current third-party token</td>
<td>Need to reconfigure remote access device to send to SAS once all users have been moved</td>
</tr>
<tr>
<td>Only deploy new tokens as needed</td>
<td>You will see “Failed or invalid user” messages in the SAS dashboard for non-existing users or authentications with a third-party token</td>
</tr>
<tr>
<td></td>
<td>SAS token can be locked if previous tokens are used for a long period of time</td>
</tr>
</tbody>
</table>

### Configure NPS/IAS Remote RADIUS Server Group

1. Open the Network Policy Server (NPS) console.
2. In the left pane, right-click **Remote RADIUS Server Groups**, then click **New**.
   a. In the **Group name** box, type a name for the new RADIUS server group, then click **Add**.
   b. In the **Add RADIUS Server** dialog box, under **RADIUS Server**, enter your previous OTP solution as a RADIUS server.
   c. Click **OK** to save.
   d. Ensure that you add this NPS server as a RADIUS client on the previous OTP solution.
3. In the left pane, under **Policies**, right-click **Connection Request Policies**, then click **New**.
   a. In the **Policy Name** box, type a name for the new policy.
   b. Create a policy that forwards connection requests to the newly created remote RADIUS server group for authentication.
   c. Click **OK** to save.
4. In the left pane, under **Policies**, right-click **Network Policies**, then click **New**.
   a. In the **Policy Name** box, type a friendly name for the new policy.
   b. Complete the remaining fields as appropriate.
   c. Click **OK** to save.
   d. Right-click the new policy, then click **Edit**.
   e. Click the **Constraints** tab and select the **Unencrypted authentication (PAP, SPAP)** check box.
   f. Click **OK** to save.
5. On the NPS server, add your local machine and your VPN appliance as RADIUS clients.

(The screen image above is from Microsoft® software. Trademarks are property of their respective owners.)
6. Use a RADIUS client tool, such as NTRadPing, to authenticate against the local NPS. NPS should forward the request to your previous OTP solution.

(The screen image above is from Microsoft® software. Trademarks are property of their respective owners.)
Install and Configure NPS/IAS Agent

1. Install NPS Agent and configure against your SAS cloud or on-premises solution.

2. Add the NPS Agent as an Auth Node on your SAS virtual server.

3. Browse to **COMMS > Auth Nodes > Add** and supply your NPS Agent details. Ensure that the **Configure FreeRadius Synchronization** check box is not selected.
4. Perform an authentication test using an existing SAS user. Upon successful authentication, the following message will be displayed:

![Authentication Succeeded](image)

Test the Solution

To test the SAS solution, the following steps must be performed:

- **Authenticate against the NPS agent with a SAS user**—Authentication in NTRadPing should succeed and the corresponding entry will appear in the SAS dashboard.

![NTRadPing Test Utility](image)

*(The screen image above is from Master Soft software. Trademarks are property of their respective owners.)*

![Authentication Activity](image)
Authenticate with a user that only exists in the third-party OTP solution—Authentication should succeed against the third-party solution, but you will receive an "Invalid user account" message in the SAS console.
- **Authenticate with a user that also exists in SAS but has no token assigned yet**—Authentication should succeed against the third-party OTP solution, but you will receive a "User does not have a token assigned" message in the SAS console.

!(The screen image above is from Master Soft software. Trademarks are property of their respective owners.)!
• Provision a token to your migrated user—Both the old and new token should work.

**NOTE:** Although both tokens will work, the user will probably lock his SAS token, as the third-party token and the SAS token are not in sync. You should inform your users that they should no longer use their previous token if they were provided with a SAS token.
SafeNet Authentication Service (SAS): Migration Guide
RADIUS Migration Using Microsoft NPS/IAS Agent
Document PN: 007-012697-001, Rev. E

(The screen image above is from Master Soft software. Trademarks are 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>Address</td>
<td>Gemalto 4690 Millennium Drive Belcamp, Maryland 21017 USA</td>
</tr>
<tr>
<td>Phone</td>
<td>United States 1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International 1-410-931-7520</td>
</tr>
<tr>
<td>Technical Support</td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td>Customer Portal</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>