SafeNet Authentication Service
Migration Guide

RADIUS Migration Using Microsoft NPS/IAS Agent
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012697-001, Rev. A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>April 2014</td>
</tr>
</tbody>
</table>

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail</td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017, USA</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:TechPubs@safenet-inc.com">TechPubs@safenet-inc.com</a></td>
</tr>
</tbody>
</table>
Contents

Introduction .................................................................................................................................................. 4
Third-Party Software Acknowledgement .................................................................................................. 4
NPS/IAS Agent in Migration Mode ........................................................................................................... 4
Configure NPS/IAS Remote RADIUS Server Group ............................................................................. 5
Install and Configure NPS/IAS Agent ....................................................................................................... 10
Test the Solution ....................................................................................................................................... 11
Support Contacts ...................................................................................................................................... 16
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 straightforward.
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

### Advantages
- Easy to set up, and acts as a “wedge” between SAS and other RADIUS server
- No heavy configuration in SAS for user/token association for current third-party token
- Only deploy new tokens as needed

### Considerations
- Need to manage two separate systems for tokens (same as RADIUS tokens)
- Need to reconfigure remote access device to send to SAS once all users have been moved
- You will see “Failed or invalid user” messages in the SAS dashboard for non-existing users or authentications with a third-party token
- SAS token can be locked if previous tokens are used for a long period of time

## 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.
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 Successful](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.)*
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.

(The screen image above is from Master Soft software. Trademarks are property of their respective owners.)
• **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.
(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 SafeNet Customer Support. SafeNet 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 SafeNet 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>SafeNet, 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 SafeNet Knowledge Base.</td>
</tr>
</tbody>
</table>