SafeNet Authentication Service
Integration Guide

Using RADIUS Protocol for AIX pam_radius
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.

© 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: 007-013638-001, Rev. A
Release Date: October 2016
Contents

Third-Party Software Acknowledgement ........................................................................................................ 4
Description .......................................................................................................................................................... 4
Applicability ...................................................................................................................................................... 4
Environment ..................................................................................................................................................... 4
Audience ............................................................................................................................................................ 5
RADIUS-based Authentication using SafeNet Authentication Service Cloud ..................................................... 5
RADIUS-based Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE .................................................................................................................................................. 6
RADIUS Authentication Flow using SafeNet Authentication Service ............................................................... 6
RADIUS Prerequisites ........................................................................................................................................ 7
Pam_auth Prerequisites ..................................................................................................................................... 7
Configuring SafeNet Authentication Service .................................................................................................... 8
    Creating Users Stores in SafeNet Authentication Service ............................................................................. 8
    Assigning an Authenticator in SafeNet Authentication Service ................................................................. 8
    Adding AIX as an Authentication Node in SafeNet Authentication Service ................................................. 9
    Checking the SafeNet Authentication Service RADIUS Address ............................................................. 11
Configuring AIX pam_radius ............................................................................................................................ 12
Running the Solution ....................................................................................................................................... 16
Support Contacts .............................................................................................................................................. 18
Third-Party Software Acknowledgement

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

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 (SAS) 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.

AIX pam_radius is the PAM to RADIUS authentication module. It allows machine to become a RADIUS client for authentication and password change requests.

This document describes how to:

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

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

AIX pam_radius 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)**—Version 3.4.316.26039
- **pam_radius**—Version 1.40 on AIX 6.1
Audience

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

RADIUS-based Authentication using SafeNet Authentication Service Cloud

SafeNet Authentication Service (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-based Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE

For both on-premises versions, SafeNet Authentication Service (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 SafeNet Authentication Service

SafeNet Authentication Service (SAS) 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 AIX.

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

To enable SafeNet Authentication Service (SAS) to receive RADIUS requests from AIX pam_radius, ensure the following:

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

Pam_auth Prerequisites

To enable radius authentication we need to install and configure pam_radius on AIX. Following are the dependencies for pam_radius:

1. Gcc
2. gcc-c++
3. gcc-cpp
4. gettext
5. gmp
6. gmp-devel
7. info
8. libcommon
9. libcommon-devel
10. libgcc
11. libmpc
12. libisgsegv
13. libisgsegv-devel
14. libstdc++
15. libstdc++-devel
16. lzlib
17. lzlib-devel
18. m4
19. mpfr
20. mpfr-devel
21. zlib
22. zlib-devel
Download the above prerequisites in /tmp directory then go to /tmp directory using “cd /tmp” command and by `rpm` command, install above packages (we will be needing root user permissions for this). Following is example:

```
$ cd /tmp
$ rpm -Uvh gcc-4.8.3-1.aix7.1.ppc.rpm gcc-c++-4.8.3-1.aix7.1.ppc.rpm gettext-0.10.40-0.aix5.2.ppc.rpm gmp-6.0.0a-1.aix5.1.ppc.rpm gmp-devel-6.0.0a-1.aix5.1.ppc.rpm info-5.1-2.aix5.1.ppc.rpm libcommon-0.97.3-1.aix5.1.ppc.rpm libcommon-devel-0.97.3-1.aix5.1.ppc.rpm libgcc-4.8.3-1.aix7.1.ppc.rpm libmpc-1.0.3-1.aix5.1.ppc.rpm libstdc++-4.8.3-1.aix7.1.ppc.rpm m4-1.4.17-1.aix5.1.ppc.rpm gcc-c++-4.8.3-1.aix7.1.ppc.rpm libsigsegv-2.10-1.aix5.2.ppc.rpm libsigsegv-devel-2.10-1.aix5.2.ppc.rpm lzlib-1.6-1.aix5.1.ppc.rpm lzlib-devel-1.6-1.aix5.1.ppc.rpm mpfr-3.1.3-1.aix5.1.ppc.rpm mpfr-devel-3.1.3-1.aix5.1.ppc.rpm zlib-1.2.4-2.aix5.1.ppc.rpm zlib-devel-1.2.4-2.aix5.1.ppc.rpm
```

### Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with AIX using RADIUS protocol requires the following:

- Creating Users Stores in SafeNet Authentication Service, page 8
- Assigning an Authenticator in SafeNet Authentication Service, page 8
- Adding AIX as an Authentication Node in SafeNet Authentication Service, page 9
- Checking the SafeNet Authentication Service RADIUS Address, page 11

### Creating Users Stores in SafeNet Authentication Service

Before SafeNet Authentication Service (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 SafeNet Authentication Service

SafeNet Authentication Service (SAS) supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through AIX pam_radius.

The following authenticators are supported:

- eToken PASS
- RB-1 Keypad Token
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 AIX as an Authentication Node in SafeNet Authentication Service

Add a RADIUS entry in the SafeNet Authentication Service (SAS) **Auth Nodes** module to prepare it to receive RADIUS authentication requests from AIX pam_radius. You will need the IP address of AIX pam_radius and the shared secret to be used by both SAS and AIX pam_radius.

1. Log in to the SAS console with an Operator account.
2. Click the **COMMS** tab, and then select **Auth Nodes**.

![Auth Nodes](image1)

3. In the **Auth Nodes** module, click the **Auth Nodes** link.

![Auth Nodes](image2)

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><strong>Agent Description</strong></td>
<td>Enter a host description.</td>
</tr>
<tr>
<td><strong>Host Name</strong></td>
<td>Enter the name of the host that will authenticate with SAS.</td>
</tr>
<tr>
<td><strong>Low IP Address In Range</strong></td>
<td>Enter the IP address of the host or the lowest IP address in a range of addresses that will authenticate with SAS. Here host IP used is 10.164.44.108</td>
</tr>
<tr>
<td><strong>Configure FreeRADIUS</strong></td>
<td>Select this option.</td>
</tr>
<tr>
<td><strong>Synchronization</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter the shared secret key.</td>
</tr>
<tr>
<td><strong>Confirm Shared Secret</strong></td>
<td>Re-enter the shared secret key.</td>
</tr>
</tbody>
</table>
The authentication node is added to the system.

Checking the SafeNet Authentication Service RADIUS Address

Before adding SafeNet Authentication Service (SAS) as a RADIUS server in AIX pam_radius, check its IP address. The IP address will then be added to AIX pam_radius 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**.

![Auth Nodes module](image1)

3. In the **Auth Nodes** module, click the **Auth Nodes** link. The SAS RADIUS server details are displayed.

![Auth Nodes Details](image2)

### Configuring AIX pam_radius

1. Perform the following steps to download AIX pam_radius:
   a. In a web browser, open the following link to download Pamradius 1.4.0 rpm:
      
   b. Select `pam_radius-1.4.0.tar.gz` from the given list of files. The file size is 175K.
   c. Download and transfer the software from your windows machine to the AIX machine using winscp. If you use any other suitable software, it is recommended that you transfer your software to `/tmp` or `/root` path.
   d. Log in as the root user before you proceed for configuration.
2. Perform the following steps to compile **pam_radius 1.4.0**:
   a. Go to the folder where you have downloaded **pam_radius-1.4.0.tar.gz**.
   b. Run the following commands to untar the file.

   ```bash
   gunzip pam_radius-1.4.0.tar.gz
tar xvf pam_radius-1.4.0.tar
   ```

   (The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

   c. Perform the following steps to modify the **pam_radius-1.4.0/src/pam_radius_auth.h** file.

   ```bash
   cd pam_radius-1.4.0
   vi src/pam_radius_auth.h
   ```
• On line 80, add “# define __sun”, just before #ifndef CONST
There are two underscores before sun and there is a space between define and underscores.

After modification, the code will be changed to:

```c
/**************************************************************************
* Platform specific defines
**************************************************************************/
#define __sun
#ifndef CONST
  if defined(__sun) || defined(__linux__) || defined(__FreeBSD__) || defined(__APPLE__)
/*
```

• Save the file.

d. Run the following commands to configure and compile.

```bash
bash-4.3# ./configure
```

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

```bash
bash-4.3# make
```

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
15
3. After the compilation is complete, copy the `pam_radius_auth.so` file to `/usr/lib/security/
   cp pam_radius_auth.so /usr/lib/security/
4. Run the following commands to configuring the RADIUS server in `pam_radius`:
   mkdir /etc/raddb
   cp pam_radius_auth.conf /etc/raddb/server
   chown root /etc/raddb
   chmod go-rwx /etc/raddb
   chmod go-rwx /etc/raddb/server
5. Add the RADIUS server hostname or IP Address in `/etc/raddb/server` in following format:
   radius_server <secret code> <timemout>
6. Enable SSH for pam_radius authentication using PAM. Add the following lines at the end of `/etc/pam.conf` to enable ssh to use pam_radius:

   ```
   #SSHD
   sshd auth required /usr/lib/security/pam_radius_auth.so
   sshd account required /usr/lib/security/pam_aix
   sshd password required /usr/lib/security/pam_aix
   sshd session required /usr/lib/security/pam_aix
   ```

7. Modify the `/etc/security/login.cfg` file. Change "auth_type = STD_AUTH" to "auth_type = PAM_AUTH".

8. Update the following parameter in `/etc/ssh/sshd_config`:

   ```
   PasswordAuthentication no
   PermitEmptyPasswords no
   UsePrivilegeSeparation no
   ChallengeResponseAuthentication yes
   UsePAM yes
   ```

9. Run the following command to restart the sshd service:

   ```
   stopsrc -s sshd ; startsrc -s sshd
   ```

### Running the Solution

For this integration, the Mobile Pass token in the challenge response mode is configured for authentication with the SAS solution. Before running the solution, ensure that the SSH service is running on the client machine.

1. Login to the client machine, and then enter `ssh tom@127.0.0.1`.

2. In the **Password**, enter any one number, and then press `<Enter>`. You will receive a challenge code.

   ```
   bash-4.3# ssh tom@127.0.0.1
   Password:
   Please respond to the challenge: 31872116
   ```

   *(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)*

3. On the registered mobile device, on the **Token Authentication** screen, enter the challenge code, and then tap **Generate Passcode**. A passcode will be generated.
4. Enter the passcode after the challenge code on AIX. You will receive a welcome message as shown below.

```
Last unsuccessful login: Wed Sep  9 15:47:44 CDT 2015 on ssh
Last login: Wed Sep  9 15:52:37 CDT 2015 on /dev/pts/1

*******************************************************************************
* *
* Welcome to AIX Version 6.1!
* *
* Please see the README file in /usr/lpp/bos for information pertinent to *
* this release of the AIX Operating System.
* *
*******************************************************************************
```

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

5. Run users command to check users. It shows the current users who are logged in to the system.

```
$ users
root  tom
$   
```

(The screen image above is from F5 Networks® software. 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</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>