Third-Party Software Acknowledgement

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

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.

Oracle Solaris 10 is a standard UNIX operating system with excellent performance, system management, and network functions. Oracle Solaris sets the standard in UNIX operating systems with leading performance, breadth of applications, system management and networking functionality. Oracle Solaris 10 also provides new standards in business performance, efficiency, availability and security, from new functions such as Solaris Containers, Predictive Self-healing, and Dynamic Trace. Oracle Solaris 10 is the successor OS of Oracle Solaris 9.

This document describes how to:

• Deploy multifactor authentication (MFA) options in Oracle Solaris using SafeNet one-time password (OTP) authenticators managed by SafeNet Authentication Service.

• Configure Oracle Solaris to work with SafeNet Authentication Service in RADIUS mode.

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

Oracle Solaris 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 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 is used in this document is based on the following software versions:

• SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)

• Oracle Solaris – Version 10
**Audience**

This document is targeted to system administrators who are familiar with Oracle Solaris, 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 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 Gemalto Support Portal.

## RADIUS Authentication Flow using SafeNet Authentication Service

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 Oracle Solaris.

1. A user attempts to log on to Oracle Solaris using an OTP authenticator.
2. Oracle Solaris 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 Oracle Solaris.
4. The user is granted or denied access to Oracle Solaris based on the OTP value calculation results from SAS.

## RADIUS Prerequisites

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

- End users can authenticate from the Oracle Solaris environment with a static password before configuring Oracle Solaris to use RADIUS authentication.
- Ports 1812/1813 are open to and from Oracle Solaris.
- 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.
- Download the PAM RADIUS v1.4.1 installation file (for example, pam_radius-master.zip) from the following URL:
  https://github.com/FreeRADIUS/pam_radius
NOTE: The URL is a third-party website and can be changed at any time in future.

The URL is a third-party website and can be changed at any time in future.

- The PAM RADIUS v1.4.1 file must be unzipped to a directory on the Solaris machine. Ensure that the read and write permissions are given on that directory.
- The user name in Solaris and the user ID in SAS must be identical.

Configuring SafeNet Authentication Service

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

- Creating Users Stores in SafeNet Authentication Service, page 7
- Assigning an Authenticator in SafeNet Authentication Service, page 7
- Adding Oracle Solaris as an Authentication Node in SafeNet Authentication Service, page 8

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 Oracle Solaris.

The following authenticators are supported:

- eToken PASS
- RB-1 Keypad Token
- KT-4 Token
- SafeNet Gold
- SMS Token
- MP-1 Software Token
- MobilePASS
- MobilePASS+

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

1. Log in to the SAS console with an Operator account.
2. Click the COMMS tab and click Auth Nodes.

![Auth Nodes](image1)

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

![Auth Nodes](image2)

**NOTE:** Before adding SafeNet Authentication Service (SAS) as a RADIUS server in Oracle Solaris, check its IP address (Primary RADIUS Server IP). The IP address will then be added to Oracle Solaris as a RADIUS server at a later stage.

4. Under Auth Nodes, click Add.
5. Under **Add Auth Nodes**, complete the following fields, and 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>High 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.</td>
</tr>
<tr>
<td><strong>Configure FreeRADIUS Synchronization</strong></td>
<td>Select this option.</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.

**Configuring Oracle Solaris**

Oracle Solaris can be configured to use RADIUS for user authentication by using the `pam_radius` module. Configuring Oracle Solaris requires:

- Installing `pam_radius`, page 11
Installing pam_radius

Perform the following steps to install pam_radius:

1. Log in to the Solaris machine as the root user.
2. Go to the directory where you unzipped the `pam_radius-master.zip` file.
3. Perform the following steps to modify the `pam_radius-master/src/ pam_radius_auth.h` file.
   a. Run the following command to open the `pam_radius_auth.h` file:
      ```
vim pam_radius-master/src/ pam_radius_auth.h
      ```
   b. In the file, on line 80, add `# define __sun, just before #ifndef CONST`.  
      For example:
      ```
      /*************************************************************************
      * Platform specific defines
      *************************************************************************/
      #define __sun
      ifndef CONST
      # if defined(__sun) || defined(__linux__) || defined(__FreeBSD__) || defined(__APPLE__)
      /*
      * On older versions of Solaris, you may have to change this to:
      ***************************************************************************/
      ```
      
      **NOTE:** In `# define __sun, there are two underscores before sun and there is one space between define and the underscores).**

4. Run the following command to open the `Makefile` file available under the `pam_radius-master` directory:
   ```
vim pam_radius-master/Makefile
   ```
5. In the `Makefile` file, comment the line 17:
   ```
   CFLAGS += -Wall -fPIC
   ```
6. Run the following command to configure PAM:
   ```
   ./configure
   ```
7. Perform the following steps to compile the PAM module for your system:
   a. Run the following command:
      ```
      make
      ```
      **NOTE:** If the make command path is not added, you can add it by running the following command:
      ```
      PATH=$PATH:/usr/ccs/bin:/usr/sfw/bin
      ```
   b. Run the following command:
      ```
      cc -G pam_radius_auth.o md5.o -lpam -o pam_radius_auth.so
      ```
8. After the compilation is complete, run the following command to copy the `pam_radius_auth.so` file to the `/usr/lib/security/ pam_radius_auth.so.1` directory:
Configuring the RADIUS Server

Perform the following steps to configure the RADIUS server in PAM:

1. Verify that the `/etc/raddb` directory exists on the Solaris machine. If the directory does not exist, run the following command to create it:
   ```bash
   mkdir /etc/raddb
   ```

2. Run the following command to copy the `pam_radius_auth.conf` file to the `/etc/raddb/` directory:
   ```bash
   cp pam_radius_auth.conf /etc/raddb/server
   ```

3. Run the following commands to change the permissions on the file copied in the previous step:
   ```bash
   chown root /etc/raddb
   chmod go-rwx /etc/raddb
   chmod go-rwx /etc/raddb/server
   ```

4. Run the following command to add the RADIUS server hostname or IP Address in the `/etc/raddb/server` directory in the following format:
   ```bash
   radius_server    <secret code>       <timeout>
   ```

5. RADIUS can be enabled in SSH by changing the SSH_config file. To perform this operation, run the following commands to update the following parameters in the `/etc/ssh/sshd_config` directory:
   ```bash
   PasswordAuthentication no
   PermitEmptyPasswords no
   UsePrivilegeSeparation no
   ```

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.
2. On the command prompt, run the following command:
   ```bash
   ssh <username>@127.0.0.1
   ```
   Where `<username>` is the username of the Solaris user.

   ```bash
   bash-3.2# ssh alice@127.0.0.1
   ```

3. Enter your system password and the SAS password.

   ```bash
   bash-3.2# ssh alice@127.0.0.1
   Password: 
   ```
4. On the configured mobile device, open the mobile pass application, choose the MobilePASS token, and enter the PIN. A passcode will be generated on the token.

![Image of the MobilePASS application](image)

5. Enter the passcode.

6. After successful authentication, you will be logged in to the system.

```
bash-3.2$ ssh alice@127.0.0.1
Password:
Password: Login@ idle JCPU FCPU what
Last login: Wed Jul 27 12:42:54 2016 from localhost
Could not chdir to home directory /home/alice: No such file or directory
Oracle Corporation SunOS 5.10 Generic Patch January 2005
```

7. Run the following command to check users, which are already logged in to the system.

```
bash-3.2$ w
12:51pm up 1 day(s), 1:31, 2 users, load average: 0.00, 0.00, 0.00
User       tty     login@ idle JCPU FCPU what
root       pts/1  12:34pm      ssh alice@127.0.0.1
alice      pts/2  12:43pm
bash-3.2$ w
```
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://supportportal.gemalto.com">https://supportportal.gemalto.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>