SafeNet Authentication Service
Integration Guide

Using RADIUS Protocol for Imprivata OneSign
Third-Party Software Acknowledgement

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

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.

Imprivata OneSign is an easy, smart, and affordable appliance for securing networks, applications and building/IT access. Packaged as an affordable, easy-to-implement appliance, OneSign uses patent-pending technology to enable SSO without modifying applications. Companies benefit through centralized password administration, lower help-desk costs, increased productivity, and complete compliance.

This document describes how to:

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

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

Imprivata OneSign 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)
- Imprivata OneSign
**Audience**

This document is targeted to system administrators who are familiar with Imprivata OneSign, 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.

![Diagram of RADIUS Protocol](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 RADIUS Protocol](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/sas-downloads/docs/007-012390-002_SAS_Agent_for_NPS_1.30_ConfigurationGuide_RevD.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 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 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 Imprivata OneSign.

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

**RADIUS Prerequisites**

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

- End users can authenticate from the Imprivata OneSign environment with a static password before configuring the Imprivata OneSign to use RADIUS authentication.
- Ports 1812/1813 are open to and from Imprivata OneSign.
- 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 SafeNet Authentication Service (SAS) with Imprivata OneSign 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 Imprivata OneSign as an Authentication Node in SafeNet Authentication Service, page 8
- Checking the SafeNet Authentication Service RADIUS Address, page 10

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 Imprivata OneSign.

The following authenticators are supported:

- eToken PASS
- RB-1 Keypad Token
- KT-4 Token
- SafeNet Gold
- SMS Token
- MP-1 Software Token
- 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 Imprivata OneSign 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 Imprivata OneSign. You will need the IP address of Imprivata OneSign and the shared secret to be used by both SAS and Imprivata OneSign.

1. Log in to the SAS console with an Operator account.

2. Click the **COMMS** tab and then select **Auth Nodes**.

![Image of SAS console with Auth Nodes selected](image-url)
3. In the **Auth Nodes** module, click the **Auth Nodes** link.

![Auth Nodes module](image)

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>Agent Description</td>
<td>Enter a host description.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Enter the name of the host that will authenticate with SAS.</td>
</tr>
<tr>
<td>Low IP Address In Range</td>
<td>Enter the IP address of the host or the lowest IP address in a range of</td>
</tr>
<tr>
<td></td>
<td>addresses that will authenticate with SAS (in this case, a range of IP</td>
</tr>
<tr>
<td></td>
<td>addresses is being used).</td>
</tr>
<tr>
<td>High IP Address In Range</td>
<td>Enter the highest IP address in a range of IP addresses that will</td>
</tr>
<tr>
<td></td>
<td>authenticate with SAS (in this case, a range of IP addresses is being</td>
</tr>
<tr>
<td></td>
<td>used).</td>
</tr>
<tr>
<td>Configure FreeRADIUS</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Synchronization</td>
<td></td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the shared secret key.</td>
</tr>
<tr>
<td>Confirm Shared Secret</td>
<td>Re-enter the shared secret key.</td>
</tr>
</tbody>
</table>

![Add Auth Node](image)

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 Imprivata OneSign, check its IP address. The IP address will then be added to Imprivata OneSign 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 Imprivata OneSign

1. Log in to the Imprivata admin console.
2. On the Imprivata admin console, click Devices > Configure external OTP tokens.

(Imprivata admin console screenshot)

3. On the Configure external OTP tokens window, perform the following steps:
   a. Under Server configuration, in the Host : Port field, enter the IP address and port number of the server.
   b. In the Encryption key field, enter the shared secret.
   c. Under Enrolling users, select the Enroll users automatically option.
   d. Click Save.

(Configure external OTP tokens window screenshot)

(The screen image above is from Imprivata. Trademarks are the property of their respective owners.)
Running the Solution

1. Connect to the terminal server.
2. You will be redirected to the Imprivata login window. On the login window, perform the following steps:
   a. Under **Choose how to authenticate with OneSign**, select **ID Token**.
   b. In the **User Name** field, enter your user name.
   c. In the **Passcode** field, enter the SafeNet MobilePASS+ passcode.
   d. Click **OK**.

(The screen image above is from Imprivata. Trademarks are the property of their respective owners.)

After successful authentication, you will be able access the terminal server.

(The screen image above is from Imprivata. Trademarks are the property of their respective owners.)
Appendix: User Activity Report

The User Activity report gives information about all the activities of a user on the server for a specified period.

1. On the Imprivata admin console, click **Reports > Add new report**.

![Add new report window](image1)

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

The **Add new report** window is displayed.

![Add new report window](image2)

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

2. On the **Add new report** window, scroll down, and then click **User Activity**.

![User Activity window](image3)

*(The screen image above is from Imprivata. Trademarks are the property of their respective owners.)*
3. On the **Add report: Platform - User Activity** window, perform the following steps:
   a. In the **User** field, enter the user name,
   b. Select the user domain.
   c. Scroll down and then click **Run**.

   ![Add report: Platform - User Activity](image)

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

   The User Activity report is displayed.

   ![User Activity report](image)

   *(The screen image above is from Imprivata. 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>
</table>
   | **Address**            | Gemalto
   |                         | 4690 Millennium Drive
   |                         | Belcamp, Maryland  21017 USA                            |
   | **Phone**              | United States                                           |
   |                         | 1-800-545-6608                                           |
   |                         | International                                            |
   |                         | 1-410-931-7520                                           |
   | **Technical Support**  | https://serviceportal.safenet-inc.com                   |
   | **Customer Portal**    | 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. |