SafeNet Authentication Service
Integration Guide

Using RADIUS Protocol for Application Request Routing (ARR)
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-Party Software Acknowledgement</td>
<td>4</td>
</tr>
<tr>
<td>Description</td>
<td>4</td>
</tr>
<tr>
<td>Applicability</td>
<td>4</td>
</tr>
<tr>
<td>Environment</td>
<td>5</td>
</tr>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS-based Authentication using SafeNet Authentication Service Cloud</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS-based Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE</td>
<td>6</td>
</tr>
<tr>
<td>RADIUS Authentication Flow using SafeNet Authentication Service</td>
<td>6</td>
</tr>
<tr>
<td>RADIUS Prerequisites</td>
<td>7</td>
</tr>
<tr>
<td>Configuring SafeNet Authentication Service</td>
<td>8</td>
</tr>
<tr>
<td>Creating Users Stores in SafeNet Authentication Service</td>
<td>8</td>
</tr>
<tr>
<td>Assigning an Authenticator in SafeNet Authentication Service</td>
<td>8</td>
</tr>
<tr>
<td>Adding ARR as an Authentication Node in SafeNet Authentication Service</td>
<td>9</td>
</tr>
<tr>
<td>Configuring ARR</td>
<td>11</td>
</tr>
<tr>
<td>Creating Rule for the Web Application</td>
<td>13</td>
</tr>
<tr>
<td>Configuring Rules for Response Rewriting</td>
<td>13</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>19</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>21</td>
</tr>
<tr>
<td>Customer Support Portal</td>
<td>21</td>
</tr>
<tr>
<td>Telephone Support</td>
<td>21</td>
</tr>
</tbody>
</table>
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Application Request Routing (ARR).

Material from ARR software is being used solely for the purpose of making instructions clear. Screen images and content obtained from ARR 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.

Application Request Routing (ARR) is an extension to Internet Information Server (IIS), which enables an IIS server to function as a load balancer.

With ARR, an IIS server can be configured to route incoming requests to one of multiple web servers using one of the several routing algorithms. By load balancing requests, high availability of web servers can be achieved without incurring the typically-high costs of dedicated load balancing products.

ARR requires the URL Rewrite extension to function, and uses it for routing requests. ARR can be configured to redirect traffic based on server variables, URLs, cookies and more, and performs full layer 7 load balancing. ARR's functionality can be described as a load balancing and reverse proxy.

This document describes how to:

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

It is assumed that the ARR environment is already configured with IIS, URL rewrite and web application working prior to implementing multi-factor authentication using SafeNet Authentication Service.

ARR 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)**
- **ARR – Version 3**
- **IIS – Version 7**
- **IIS agent -- Version 1.05**
- **URL rewrite – Version 2.0**

Audience

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

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.

  ![SAS Cloud Hosted RADIUS Service Diagram]

- **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.

  ![Local RADIUS Hosted on-premises Diagram]
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 Gemalto 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 ARR.

1. A user attempts to access a website hosted on the IIS server using an OTP authenticator.
2. IIS agent 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 IIS.
4. The IIS-ARR will rewrite the Published URL with internal web application URL and the user is presented with the application.

**RADIUS Prerequisites**

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

- The ARR environment is already configured with IIS. The URL rewrite and web application functionalities must be working before implementing the multi-factor authentication using SAS.
- Active directory should be installed and configured on the IIS server.
- The IIS agent should be installed and configured. To know about the IIS agent configuration, open the following link:
  http://www2.gemalto.com/sas-downloads/docs/007-012393-002_SAS_IIS_Agent_1.05_Configuration_Guide_RevD.pdf
- Ports 1812/1813 are open to and from ARR.
- 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.
NOTE: For this integration the sample web application access URL is:
http://example.com/webmail/default.aspx

- Created webmail folder in inetpub and copied default.aspx page in webmail folder.
- The web application can be accessed locally by using the following URL with port number:
  - http://localhost:8081/ or http://example.com:8081

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with ARR 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 ARR as an Authentication Node in SafeNet Authentication Service, page 9

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 ARR.

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

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

![Auth Nodes module](image)

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

![Auth Nodes table](image)

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

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 addresses that will authenticate with SAS (in this case, a range of IP 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 authenticate with SAS (in this case, a range of IP addresses is being used).</td>
</tr>
<tr>
<td>Configure FreeRADIUS Synchronization</td>
<td>Select this option.</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>

The authentication node is added to the system.

**Configuring ARR**

When a request is made to the web application (for example, [http://example.com/webmail/default.aspx](http://example.com/webmail/default.aspx)), ARR forwards these requests to an internal server using the [http://example.com:8081](http://example.com:8081) URL.

Configuring ARR to use the RADIUS protocol as a secondary authentication method requires:

- Enabling the Reverse Proxy Functionality, page 12
- Creating Rule for the Web Application, page 13
- Configuring Rules for Response Rewriting, page 13
Enabling the Reverse Proxy Functionality

Perform the following steps to enable the Reverse Proxy functionality:

1. On the IIS server machine, open IIS Manager.

2. In the left pane, click the server node name (for example, ARR-COM) and in the middle pane, under IIS, double-click on the Application Request Routing Cache icon.

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

3. In the right pane, under Proxy, click Server Proxy Settings.

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

4. In the middle pane, under Use this feature to configure proxy settings for Application Request Routing, select Enable proxy.

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

5. In the right pane, under Actions, click Apply.
Creating Rule for the Web Application

If the requested URL path starts with `webmail`, the rewrite rule forwards the request to the `http://localhost:8081/` URL.

1. On the IIS server machine, open the `web.config` file located at the `%SystemDrive%\inetpub\wwwroot\` location.
2. In the `web.config` file, locate the following line:
   
   ```xml
   /configuration/system.webServer
   ```

   After the `/configuration/system.webServer` line, add the following code:

   ```xml
   <rewrite>
   <rules>
     <rule name="Reverse Proxy to webmail" stopProcessing="true">
       <match url="^webmail/(.*)" />
       <action type="Rewrite" url="http://localhost:8081/{R:1}" />
     </rule>
   </rules>
   </rewrite>
   ```

3. Save the file.

Configuring Rules for Response Rewriting

Perform the following steps to configure rules for Response Rewriting:

1. Go to IIS Manager.
2. In the left pane, expand the server node name (for example, `ARR-COM`), and then click Sites > Default Web Site.

![IIS Manager Screenshot](image-url)

*(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)*
3. In the middle pane, under **IIS**, double-click on the **URL Rewrite** icon.

![URL Rewrite icon in IIS](image)

4. In the right pane, under **Actions**, click **Add Rule(s)**.

![Add Rule(s) window](image)

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

5. On the **Add Rule(s)** window, under **Outbound rules**, click **Blank rule**, and then click **OK**.

![Add Rule(s) window](image)

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
6. On the **Edit Outbound Rule** window, perform the following steps:
   a. In the **Name** field, enter a name for the rule (for example, *Add application prefix*).
   b. In the **Precondition** field, select `<Create New Pre-condition...>`.

   ![Edit Outbound Rule](image)

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

7. On the **Add Pre-condition** window, perform the following steps:
   a. In the **Name** field, enter *IsHTML*.
   b. In the **Using** field, select *Regular Expressions*.
   c. Click **Add**.

   ![Add Pre-condition](image)

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

8. On the **Add Condition** window, perform the following steps:
   a. In the **Condition input** field, enter the following expression:

   ```
   {RESPONSE_CONTENT_TYPE}
   ```

   b. In the **Check if input string** field, select *Matches the pattern*.
   c. In the **Pattern** field, enter `^text/html`. 
d. Click **OK**.

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

9. On the **Add Pre-condition** window, click **OK**.

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

10. In the middle pane, under **Edit Outbound Rule**, in the **Matching scope** field, select **Response**.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
11. In the **Match the content within** field, select A **(href attribute)**.

![Edit Outbound Rule](image)

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

12. Scroll down, in the **Pattern** field, enter the following string:

   ^/(.\*)

![Edit Outbound Rule](image)

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

13. Click **Conditions**.
14. Under **Conditions**, click **Add**.

![Add Condition window](image)

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

15. On the **Add condition** window, perform the following steps:

   a. In the **Condition input** field, enter the following:

       ```text
       {URL}
       ```

   b. In the **Check if input string** field, select **Matches the Pattern**.

   c. In the **Pattern** field, enter the following string:

       ```text
       ^/(webmail)/.*
       ```

   d. Click **OK**.

![Add Condition window](image)

*(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)*
16. In the middle pane, under **Action**, perform the following steps:
   
a. In the **Action Type** field, select **Rewrite**
   
b. In the **Value** field, enter the following string:

   ```
   /{C:1}/[{R:1}]
   ```

17. In the right pane, click **Apply**.

**Running the Solution**

For this integration, the eToken PASS token is used as the enrolled OTP token.

1. In a web browser, open a web application URL.
   
   For example, [http://example.com/webmail/default.aspx](http://example.com/webmail/default.aspx)

2. On the SafeNet Authentication Service login page, enter your domain/user name and the generated OTP and then click **Log On**.
3. After successful authentication, you will be able to view the required web page.
Support Contacts

If you encounter a problem while installing, registering, or operating this product, refer to 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.

Customer Support Portal

The Customer Support Portal, at https://supportportal.gemalto.com, is a where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

NOTE: You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the REGISTER link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Customer Support by telephone. Calls to Customer Support are handled on a priority basis.

<table>
<thead>
<tr>
<th>Region</th>
<th>Telephone number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>+1-410-931-7520</td>
</tr>
<tr>
<td>Australia</td>
<td>1800.020.183</td>
</tr>
<tr>
<td>China</td>
<td>North: 10800-713-1971  South: 10800-1301-932</td>
</tr>
<tr>
<td>France</td>
<td>0800-912-857</td>
</tr>
<tr>
<td>Germany</td>
<td>0800-181-6374</td>
</tr>
<tr>
<td>India</td>
<td>000.800.100.4290</td>
</tr>
<tr>
<td>Israel</td>
<td>180-931-5798</td>
</tr>
<tr>
<td>Italy</td>
<td>800-786-421</td>
</tr>
<tr>
<td>Japan</td>
<td>0066 3382 1699</td>
</tr>
<tr>
<td>Korea</td>
<td>+82 2 3429 1055</td>
</tr>
<tr>
<td>Region</td>
<td>Telephone number</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>(Subject to change. An up-to-date list is maintained on the Customer Support Portal)</td>
</tr>
<tr>
<td>Netherlands</td>
<td>0800.022.2996</td>
</tr>
<tr>
<td>New Zealand</td>
<td>0800.440.359</td>
</tr>
<tr>
<td>Portugal</td>
<td>800.863.499</td>
</tr>
<tr>
<td>Singapore</td>
<td>800.1302.029</td>
</tr>
<tr>
<td>Spain</td>
<td>900.938.717</td>
</tr>
<tr>
<td>Sweden</td>
<td>020.791.028</td>
</tr>
<tr>
<td>Switzerland</td>
<td>0800.564.849</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>0800.056.3158</td>
</tr>
<tr>
<td>United States</td>
<td>(800) 545-6608</td>
</tr>
</tbody>
</table>