SafeNet Authentication Service
Integration Guide

Using RADIUS Protocol for CryptoAuditor
Contents

Third-Party Software Acknowledgement ........................................................................................................ 4
Description .......................................................................................................................................................... 4
Applicability .................................................................................................................................................. 4
Environment .................................................................................................................................................. 5
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
Configuring SafeNet Authentication Service ................................................................................................. 7
  Creating Users Stores in SafeNet Authentication Service ...................................................................... 7
  Assigning an Authenticator in SafeNet Authentication Service ............................................................. 8
  Adding CryptoAuditor as an Authentication Node in SafeNet Authentication Service ....................... 9
Configuring CryptoAuditor ............................................................................................................................ 11
  Configuring External RADIUS Authentication Server ....................................................................... 11
  Creating a Rule to Connect the Destination Server with SSH ............................................................. 13
  Creating a Rule to Connect the Destination Server with RDP .............................................................. 19
Running the Solution .................................................................................................................................... 24
  Authentication for SSH Session ............................................................................................................. 24
  Authentication for RDP Session ............................................................................................................. 25
Support Contacts ........................................................................................................................................ 27
Third-Party Software Acknowledgement

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

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

CryptoAuditor from SSH Communications Security Corporation reduces the security risks when organizations use SSH or RDP for remote system access.

CryptoAuditor monitors, controls, and audits encrypted administrator sessions, 3rd party access, and file transfers.

CryptoAuditor allows you to see, control, and record what happens inside encrypted privileged sessions to your corporate resources. CryptoAuditor monitors and controls encrypted secure connections, and enforces your corporate security policy also on privileged users.

This document describes how to:

• Deploy multi-factor authentication (MFA) options in CryptoAuditor using SafeNet one-time password (OTP) authenticators managed by SafeNet Authentication Service.

• Configure CryptoAuditor to work with SafeNet Authentication Service in the RADIUS mode.

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

CryptoAuditor 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)**
- **CryptoAuditor**—Version 2.2.1.25

Audience

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

- **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 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 CryptoAuditor.

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

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

- End users can authenticate from the CryptoAuditor environment with a static password before configuring the CryptoAuditor to use RADIUS authentication.
- Ports 1812/1813 are open to and from CryptoAuditor.
- 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 CryptoAuditor using RADIUS protocol requires the following:

- Creating Users Stores in SafeNet Authentication Service, page 7
- Assigning an Authenticator in SafeNet Authentication Service, page 8
- Adding CryptoAuditor 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 CryptoAuditor.

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

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** task.

![Auth Nodes](image)

**NOTE:** Before adding SafeNet Authentication Service (SAS) as a RADIUS server in CryptoAuditor, check its IP address (“Primary RADIUS Server IP”). The IP address will then be added to CryptoAuditor 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>

![Add Auth Node](image)
The authentication node is added to the system.

### Configuring CryptoAuditor

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

- Configuring External RADIUS Authentication Server, page 11
- Creating a Rule to Connect the Destination Server with SSH, page 13
- Creating a Rule to Connect the Destination Server with RDP, page 19

#### Configuring External RADIUS Authentication Server

1. In a web browser, open the following URL:

   https://<CryptoAuditor IP address>/accounts/login

2. On the CryptoAuditor login window, enter your administrator **Username** and **Password**, and then click **LOGIN**.

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

3. On the CryptoAuditor administrator dashboard, click the **Settings** tab.

   *(The screen image above is from CryptoAuditor. Trademarks are the property of their respective owners.)*
4. In the left pane, click **External Authentication**.

![CryptAuditor Screen](image1.png)

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

5. In the right pane, under **Manage external authentication backends**, click **+Add RADIUS server**.

![CryptAuditor Screen](image2.png)

*(The screen image above is from CryptoAuditor. Trademarks are the property of their respective owners.)*
6. Complete the following fields, and then click **SAVE**.

<table>
<thead>
<tr>
<th><strong>Address</strong></th>
<th>Enter the <strong>Primary RADIUS Server IP</strong> address that is available in the <strong>Auth Nodes</strong> module of your SAS server. Refer to step 3 of “Adding CryptoAuditor as an Authentication Node in SafeNet Authentication Service” on page 9.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Shared secret</strong></td>
<td>Enter the <strong>Shared Secret</strong> that you entered earlier in step 5 of “Adding CryptoAuditor as an Authentication Node in SafeNet Authentication Service” on page 9.</td>
</tr>
<tr>
<td><strong>Shared secret</strong></td>
<td>Re-enter the shared secret.</td>
</tr>
</tbody>
</table>

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

### Creating a Rule to Connect the Destination Server with SSH

Perform the following steps to create a rule to connect the destination server with SSH:

1. On the CryptoAuditor administrator dashboard, click the **Policy** tab.

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

2. In the right pane, under **Rules**, click **+Add rule**.

   (The screen image above is from CryptoAuditor. Trademarks are the property of their respective owners.)
3. In the **Name** field, enter a name for the rule (for example, **SSH**).

4. In the **Connecting with** field, select **ssh**.

5. In the **To port** field, select **Via Bastion listener**.

6. In the **Bastion listener** field, select **SSH: default: 0.0.0.0:22**, and then click **Continue**.
7. Under **Authentication**, complete the following fields:

<table>
<thead>
<tr>
<th>Client-to-Hound authentication</th>
<th>Select Authenticate against a RADIUS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radius server</td>
<td>Select the RADIUS server IP address (given along with the port number) that you added in step 6 of “Configuring External RADIUS Authentication Server” on page 11.</td>
</tr>
<tr>
<td>Hound-to-target authentication</td>
<td>Select Mapped user credentials.</td>
</tr>
</tbody>
</table>

8. Under **Destination**, complete the following fields, and then click **Continue**.

<table>
<thead>
<tr>
<th>Destination selection</th>
<th>Select Fixed address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed destination address</td>
<td>Enter the IP address of the destination server for SSH.</td>
</tr>
<tr>
<td>Fixed destination port</td>
<td>Enter the port number of the destination server for SSH.</td>
</tr>
</tbody>
</table>

(The screen image above is from CryptoAuditor. Trademarks are the property of their respective owners.)
9. Click **Save**.

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

10. In the left pane, click **User Mappings**.

(The screen image above is from CryptoAuditor. Trademarks are the property of their respective owners.)
11. In the right pane, under **USER MAPPINGS**, click **ADD NEW USER MAPPING**.

![Image](image1.png)

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

12. Under **GATEWAY USER**, complete the following fields:

<table>
<thead>
<tr>
<th>USER NAME</th>
<th>Enter the SAS username (for example, alice).</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER PROVIDER</td>
<td>Select the RADIUS server IP address (given along with the port number) that you added in step 6 of “Configuring External RADIUS Authentication Server” on page 11.</td>
</tr>
</tbody>
</table>

![Image](image2.png)

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

13. Under **TARGET**, complete the following fields:

<table>
<thead>
<tr>
<th>ADDRESS</th>
<th>Enter the IP address of the destination server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>PORT</td>
<td>Enter the SSH port number (for example, 22).</td>
</tr>
<tr>
<td>PROTOCOL</td>
<td>Select SSH.</td>
</tr>
</tbody>
</table>

![Image](image3.png)

(The screen image above is from CryptoAuditor. Trademarks are the property of their respective owners.)
14. Under **AUTHENTICATION**, complete the following fields, and then click **SAVE**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>USER NAME</strong></td>
<td>Enter the username of the destination server (for example, <code>nsroot</code>).</td>
</tr>
<tr>
<td><strong>PASSWORD</strong></td>
<td>Enter the password of the destination server.</td>
</tr>
<tr>
<td><strong>VERIFY PASSWORD</strong></td>
<td>Re-enter the password of the destination server.</td>
</tr>
</tbody>
</table>

15. Click the **Pending changes** tab.

16. On the **Pending changes** window, click **Apply**.
Creating a Rule to Connect the Destination Server with RDP

Perform the following steps to create a rule to connect the destination server with RDP:

1. On the CryptoAuditor administrator dashboard, in the left pane, click **Rules**.

   ![CryptoAuditor Dashboard](image)

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

2. In the right pane, under **Rules**, click **+Add rule**.

   ![Add Rule](image)

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

3. In the **Name** field, enter a name for the rule (for example, **RDP**).

4. In the **Connecting with** field, select **rdp**.

   ![Rule Configuration](image)

   *(The screen image above is from CryptoAuditor. Trademarks are the property of their respective owners.)*
5. In the **To port** field, select **Via Bastion listener**.

![Image of CryptoAuditor](image1.png)

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

6. In the **Bastion listener** field, select **RDP: default: 0.0.0.0:3389**, and then click **Continue**.

![Image of CryptoAuditor](image2.png)

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

7. Under **Authentication**, complete the following fields:

<table>
<thead>
<tr>
<th>Client-to-Hound authentication</th>
<th>Select <strong>Authenticate against a RADIUS server</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radius server</td>
<td>Select the RADIUS server IP address (given along with the port number) that you added in step 6 of “Configuring External RADIUS Authentication Server” on page 11.</td>
</tr>
<tr>
<td>Hound-to-target authentication</td>
<td>Select <strong>Mapped user credentials</strong>.</td>
</tr>
</tbody>
</table>

![Image of CryptoAuditor](image3.png)

(The screen image above is from CryptoAuditor. Trademarks are the property of their respective owners.)
8. Under **Destination**, complete the following fields, and then click **Continue**.

<table>
<thead>
<tr>
<th>Destination selection</th>
<th>Select <strong>Fixed address</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed destination address</td>
<td>Enter the IP address of the destination server for RDP.</td>
</tr>
<tr>
<td>Fixed destination port</td>
<td>Enter the port number of the destination server for RDP.</td>
</tr>
</tbody>
</table>

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

9. Click **Save**.

(The screen image above is from CryptoAuditor. Trademarks are the property of their respective owners.)
10. In the left pane, click **User Mappings**.

11. In the right pane, click **ADD NEW USER MAPPING**.

12. Under **GATEWAY USER**, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER NAME</td>
<td>Enter the SAS username (for example, <em>alice</em>).</td>
</tr>
<tr>
<td>USER PROVIDER</td>
<td>Select the RADIUS server IP address (given along with the port number) that you added in step 6 of “Configuring External RADIUS Authentication Server” on page 11.</td>
</tr>
</tbody>
</table>

13. Under **TARGET**, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADDRESS</td>
<td>Enter the IP address of the destination server.</td>
</tr>
<tr>
<td>PORT</td>
<td>Enter the RDP port number (for example, <strong>3389</strong>).</td>
</tr>
<tr>
<td>PROTOCOL</td>
<td>Select <strong>RDP</strong>.</td>
</tr>
</tbody>
</table>
14. Under **AUTHENTICATION**, complete the following fields, and then click **SAVE**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER NAME</td>
<td>Enter the username of the destination server (for example, Administrator).</td>
</tr>
<tr>
<td>PASSWORD</td>
<td>Enter the password of the destination server.</td>
</tr>
<tr>
<td>VERIFY PASSWORD</td>
<td>Re-enter the password of the destination server.</td>
</tr>
</tbody>
</table>

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

15. Click the **Pending changes** tab.

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

16. On the **Pending changes** window, click **Apply**.

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

For this integration, PASSWORD token is configured for authentication with the SAS solution.

Authentication for SSH Session

Perform the following steps to access the SSH destination server using the CryptoAuditor IP address:

1. Open the Putty application.
2. On the Putty Configuration window, in the right pane, perform the following steps:
   a. In the Host Name (or IP address) field, enter the IP address of the CryptoAuditor.
   b. Under Connection type, select the SSH option.
3. On the SSH console, enter the SAS username (for example, alice), and then press the Enter key.
4. Enter the user password that is provisioned as the token code in SAS and then press the Enter key.
After successful authentication done by the RADIUS server, the SSH session of the destination server is opened.

Authentication for RDP Session

Perform the following steps to access the RDP destination server using the CryptoAuditor IP address:

1. Open the Remote Desktop Connection application.
2. On the Remote Desktop Connection application console, in the Computer field, enter the IP address of CryptoAuditor, and then click the Show Options icon.
3. Perform the following steps:
   a. In the User name field, enter the SAS username (for example, alice)
   b. Select the Allow me to save credentials check box.
   c. Click Connect.
4. On the **Windows Security** window, enter the user password that is provisioned as the token code in SAS, and then click **OK**.

![Windows Security](image)

After successful authentication done by the RADIUS server, the RDP session of the destination server is opened.

![RDP Session](image)
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></td>
</tr>
<tr>
<td><strong>Customer Portal</strong></td>
<td><a href="https://supportportal.gemalto.com">https://supportportal.gemalto.com</a></td>
</tr>
<tr>
<td></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>