SafeNet Authentication Service
Integration Guide

SAS Using RADIUS Protocol with Palo Alto GlobalProtect
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Palo Alto GlobalProtect.

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 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.

The Palo Alto GlobalProtect is a platform that safely enables applications, users, and content in your enterprise branch offices. Dedicated computing resources for the functional areas of networking, security, content inspection, and management ensure predictable firewall performance.

This document describes how to:

- Configure Palo Alto GlobalProtect to work with SafeNet Authentication Service in RADIUS mode.

This document assumes that the Palo Alto GlobalProtect environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Palo Alto GlobalProtect 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

Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Service** – a cloud version of SAS
- **Palo Alto PA-200**
- **Palo Alto GlobalProtect** firmware version 2.0.3-5

Audience

This document is targeted to system administrators who are familiar with Palo Alto GlobalProtect and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.
RADIUS-based Authentication using SAS Cloud

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.

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 SAS FreeRADIUS Agent Configuration Guide.

This document demonstrates the solution using the SAS cloud hosted RADIUS service.
RADIUS-based Authentication using SAS-SPE and SAS-PCE

In addition to the pure cloud-based offering, SafeNet Authentication Service comes with two on-premises versions:

- **SafeNet Authentication Service – Service Provider Edition (SPE)** – An on-premises version of SafeNet Authentication Service targeted at service providers interested in hosting SAS in their data center.
- **SafeNet Authentication Service – Private Cloud Edition (PCE)** – An on-premises version of SafeNet Authentication Service targeted at organizations interested in hosting SAS in their private cloud environment.

For both on-premises versions, 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 SAS**

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 Palo Alto GlobalProtect.

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

To enable SafeNet Authentication Service to receive RADIUS requests from Palo Alto GlobalProtect, ensure the following:

- End users can authenticate through from the Palo Alto GlobalProtect environment with a static password before configuring the Palo Alto GlobalProtect to use RADIUS authentication.
- Ports 1812/1813 are open to and from Palo Alto GlobalProtect.
- 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 signature purposes.

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with Palo Alto GlobalProtect using RADIUS protocol requires:

- Synchronizing Users Stores to SAS
- Authenticator Assignment in SAS
- Adding Palo Alto GlobalProtect as an Authentication Node in SAS
- Checking the SAS RADIUS IP address

Synchronizing Users Stores to SafeNet Authentication Service

Before 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 further details on importing users to SafeNet Authentication Service, refer to the SafeNet Authentication Service Subscriber Account Operator Guide (Chapter 2 > Assignment tab > Creating users):


All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.
Authenticator Assignment in SAS

SAS supports a number of authentication methods that can be used as second authentication factor for users who are authenticating through Palo Alto GlobalProtect.

The following authenticators are supported:

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

Authenticators can be assigned to users in two ways:

- **Manually provision** – Assign an authenticator to users one by one.
- **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 the *SafeNet Authentication Service - Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SafeNet Authentication Service User Store.

(Chapter 2 > Assignment Tab > Token Module > Provision - Manually provision; Chapter 2 > Policy Tab > Automation Policies Module > Provisioning Rules - Provisioning rules).

Adding Palo Alto GlobalProtect as an Authentication Node in SAS

Add a RADIUS entry in the SAS Authentication Nodes module to prepare it to receive RADIUS authentication requests from Palo Alto GlobalProtect. You will need the IP address of Palo Alto GlobalProtect and the shared secret to be used by both SAS and Palo Alto GlobalProtect.

To add an Authentication Node in SAS:

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

2. Click the COMMS tab, and then select the Auth Nodes module.

3. In the Auth Nodes module, click the Auth Nodes link.
4. 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.</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.</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 entered above to confirm it.</td>
</tr>
</tbody>
</table>

![Add Auth Nodes section](image-url)
The Auth Node is added to the system.

Checking the SAS RADIUS Address

Before adding SafeNet Authentication Service as a RADIUS server in Palo Alto GlobalProtect, check the IP address of the SAS RADIUS server. The IP address will then be added to Palo Alto GlobalProtect as a RADIUS server at a later stage.

To check the IP address of the SAS RADIUS server:

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

![COMMS tab](image)

3. Click the **Auth Nodes** link.

![Auth Nodes link](image)

The SAS RADIUS server details are displayed.
Configuring Sharing & Realms

Since in Palo Alto, when using RADIUS authentication, the user is being sent with its domain name (i.e. example.com\user_name), there is a need to add a rule under Sharing & Realms to trim the domain name.

In order to trim the domain name:

1. Log in to the SAS console with

2. Select Virtual Servers -> Comms -> Auth Nodes

![Auth Nodes](image)

3. Press on the Edit link in the Palo Alto instance you have added

![Edit Auth Node](image)
4. Press the Sharing & Realms tab

5. Press on the Enable Realms checkbox. Make sure that the Strip Realm from UserID is also checked. In the Delimiter Character text box enter \\", The Delimiter instance should be First and the Realm First checkbox also need to be checked.

6. On the Available Accounts select the relevant account and press on the right arrow to add it to the Share Auth Node With section
7. Double click on the account you have added to Share Auth Node With. The account name will be added to the Selected Account and Realm Identifier text boxes

8. Change the Realm Identifier to the domain name that needs to be trimmed and press Add

9. Press Save
Support for Palo Alto RADIUS Attributes

Palo Alto Networks supports RADIUS authentication with VSA (Vendor Specific Attributes).

SAS can be configured to return several; specific Roles and User Group information in the RADIUS response.

To configure SAS return specific Palo Alto RADIUS attributes:

Under Virtual Server > Assignment > User > RADIUS Attributes, SAS now allows the selection of vendor-specific RADIUS attributes for Palo Alto, as shown below.
Configuring Palo Alto GlobalProtect

This section covers the following:

- Configuring RADIUS Authentication
- Configuring Authentication Profile
- Configuring Global Protect Gateway

Configuring RADIUS Authentication

In the following section the SAS RADIUS server will be configured as the RADIUS server in Palo Alto.

**To configure RADIUS authentication in Palo Alto GlobalProtect:**

1. Connect to the **Palo Alto GlobalProtect webmin**.
2. Click the **Device** tab at the top of the screen.
3. In the left pane, click **Server Profile > RADIUS**.

(The screen image above is from Palo Alto Networks – GlobalProtect. Trademarks are the property of their respective owners.)
4. In the right pane, click on **Add** at the bottom of the screen.

5. On the **RADIUS Server Profile** window, enter the following:

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a profile name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Enter the network domain</td>
</tr>
<tr>
<td>Servers</td>
<td>Add a server. Provide the Name, IP Address and Shared Secret key, of the SAS RADIUS server. Enter Port 1812</td>
</tr>
</tbody>
</table>

6. Click **OK**.
Configuring an Authentication Profile

This section explains how to create a RADIUS authentication profile for the users. The authentication profile enables the administrator to set an authentication method for a user, a group of users or for all users.

1. Connect to the **Palo Alto GlobalProtect webmin**.
2. Click the **Device** tab, and then on the left pane, click **Authentication Profile**.

   ![Screen Image](image)

   *(The screen image above is from Palo Alto Networks – GlobalProtect. Trademarks are the property of their respective owners.)*

3. In the right pane, click on **Add** at the bottom of the screen.
4. On the **Authentication Profile** window, enter the following:

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a profile name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow List</td>
<td>Add and select the users that will use this profile</td>
</tr>
<tr>
<td>Authentication</td>
<td>Select <strong>RADIUS</strong></td>
</tr>
<tr>
<td>Server Profile</td>
<td>Select the server profile created in the previous section</td>
</tr>
</tbody>
</table>

   ![Authentication Profile Window](image)

   *(The screen image above is from Palo Alto Networks – GlobalProtect. Trademarks are the property of their respective owners.)*

5. Click on **OK** button.
Configuring Global Protect Gateway

This section explains how to configure the gateway to use SAS RADIUS authentication.

1. Connect to the **Palo Alto GlobalProtect webmin**.
2. Click the **Network** tab.

![Network Tab](image1)

(The screen image above is from Palo Alto Networks – GlobalProtect. Trademarks are the property of their respective owners.)

3. On the left pane, click **GlobalProtect -> Gateways**.

![Gateways Tab](image2)

(The screen image above is from Palo Alto Networks – GlobalProtect. Trademarks are the property of their respective owners.)

4. Click on the gateway you created previously (it is assumed that you have a portal configured with username/password authentication).

   Click the **General** tab. Under **Authentication** section, in the **Authentication Profile** field, select the authentication profile you created in the "
5. Configuring an Authentication Profile procedure.

6. Click OK button and then Commit button to save the changes.
Running the Solution

This section explains how to authenticate to Palo Alto GlobalProtect using the GlobalProtect client and a SafeNet OTP authenticator.

1. A user opens the GlobalProtect client, and then clicks File → Connect.

   ![Image of the GlobalProtect client](image1)

   *(The screen image above is from Palo Alto Networks – GlobalProtect software. Trademarks are the property of their respective owners.)*

2. The user enters his LDAP credentials in the GlobalProtect Portal Authentication window and clicks the Apply button.

   ![Image of the GlobalProtect Portal Authentication](image2)

   *(The screen image above is from Palo Alto Networks – GlobalProtect software. Trademarks are the property of their respective owners.)*
3. After a successful authentication, the user enters his username in the username field and generates an OTP using his OTP authenticator. The user fills his OTP value in the Password field.

![Image](image1.png)

(The screen image above is from Palo Alto Networks – GlobalProtect software. Trademarks are the property of their respective owners.)

4. The user clicks OK. The user is now connected to the VPN.

![Image](image2.png)
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 SafeNet Customer Support. SafeNet 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 SafeNet 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>Address</td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017 USA</td>
</tr>
<tr>
<td>Phone</td>
<td>United States 1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International 1-410-931-7520</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 SafeNet Knowledge Base.</td>
</tr>
</tbody>
</table>