SafeNet Authentication Manager

Integration Guide

SAM using RADIUS Protocol with Palo Alto GlobalProtect
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012719-001, Rev A.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>October 2014</td>
</tr>
</tbody>
</table>

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail</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>Email</td>
<td><a href="mailto:TechPubs@safenet-inc.com">TechPubs@safenet-inc.com</a></td>
</tr>
</tbody>
</table>
## Contents

- Third-Party Software Acknowledgement ................................................................. 4
- Description ................................................................................................................. 4
- Applicability ................................................................................................................ 4
- Environment .................................................................................................................. 4
- Audience ....................................................................................................................... 5
- RADIUS-based Authentication using SAM ................................................................. 5
- RADIUS Authentication Flow using SAM ................................................................. 5
- RADIUS Prerequisites .................................................................................................. 6
- Configuring SafeNet Authentication Manager ............................................................ 6
  - Synchronizing Users Stores to SafeNet Authentication Manager .............................. 6
  - Configuring SAM’s Connector for OTP Authentication ........................................... 7
  - Token Assignment in SAM .......................................................................................... 8
  - Adding Palo Alto GlobalProtect as a RADIUS Client in IAS/NPS .......................... 8
  - SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration ........................... 10
- Configuring Third Party Product ................................................................................ 11
  - Configuring an Authentication Profile ...................................................................... Error! Bookmark not defined.
  - Configuring Global Protect Gateway ...................................................................... Error! Bookmark not defined.
- Running the Solution .................................................................................................. Error! Bookmark not defined.
- Support Contacts ........................................................................................................ Error! Bookmark not defined.
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 Palo Alto GlobalProtect software is being used solely for the purpose of making instructions clear. Screen images and content obtained from Palo Alto GlobalProtect will be acknowledged as such.

Description

SafeNet Authentication Manager (SAM) is a versatile authentication solution that allows you to match the authentication method and form factor to your functional, security, and compliance requirements. Use this innovative management service to handle all authentication requests and to manage the token lifecycle.

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 Manager in RADIUS mode.

It is assumed that the Palo Alto GlobalProtect environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager and that the SafeNet Authentication Manager OTP plug-in for Microsoft RADIUS Client was installed as part of the simplified installation mode of SAM. For more information on SafeNet Authentication Manager installation modes, refer to SafeNet Authentication Manager 8.2 Administrator’s Guide.

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 Manager.

Applicability

The information in this document applies to:

- **SafeNet Authentication Manager** - A server version of SAM 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 Manager 8.2 HF 539** - A server version of SAM that is used to deploy the solution on-premises in the organization.
- **Palo Alto GlobalProtect – version 6.0.3**
**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 Manager.

**RADIUS-based Authentication using SAM**

SafeNet’s OTP architecture includes the SafeNet RADIUS server for back-end OTP authentication. This enables integration with any RADIUS-enabled gateway or application. The SafeNet RADIUS server accesses user information in the Active Directory infrastructure via SafeNet Authentication Manager (SAM).

SAM’s OTP plug-in for Microsoft RADIUS Client works with Microsoft’s IAS or NPS, providing strong authenticated remote access through the IAS or NPS RADIUS server.

When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet OTP plug-in for Microsoft RADIUS Client, refer to *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

**RADIUS Authentication Flow using SAM**

SafeNet Authentication Manager communicates with a large number of VPN and access-gateway solutions using the RADIUS protocol.

The image below describes the dataflow of a multi-factor authentication transaction for Palo Alto GlobalProtect.

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

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

- End users can authenticate from the Palo Alto GlobalProtect environment with a static password before configuring 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 the RADIUS client for encryption, decryption, and digital signature purposes.

Configuring SafeNet Authentication Manager

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

- Synchronizing Users Stores to SafeNet Authentication Manager, page 6
- Configuring SAM’s Connector for OTP Authentication, page 7
• Token Assignment in SAM, page 8
• Adding Palo Alto GlobalProtect as a RADIUS Client in IAS/NPS, page 8
• SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration, page 10

Synchronizing Users Stores to SafeNet Authentication Manager

SAM manages and maintains OTP token information in its data store, including the token status, the OTP algorithm used to generate the OTP, and the token assignment to users. For user information, SAM can be integrated with an external user store. During the design process, it is important to identify which user store the organization is using, such as Microsoft Active Directory.

If the organization is not using an external user store, SAM uses an internal (“stand-alone”) user store created and maintained by the SAM server.

SAM 8.2 supports the following external user stores:

• Microsoft Active Directory – 2003, 2008, and 2008 R2
• Novell eDirectory
• Microsoft ADAM/AD LDS
• OpenLDAP
• Microsoft SQL Server 2005 and 2008
• IBM Lotus Domino
• IBM Tivoli Directory Server

Configuring SAM’s Connector for OTP Authentication

SafeNet Authentication Manager is based on open standards architecture with configurable connectors. This supports integration with a wide range of security applications including network logon, VPN, web access, one-time password authentication, secure email, and data encryption.

If you selected Simplified OTP-only configuration, SafeNet Authentication Manager is automatically configured with a typical OTP configuration, providing a working SafeNet Authentication Manager OTP solution.

The Simplified OTP-only configuration is as follows:

• Connectors - SAM Connector for OTP Authentication is installed
• SAM Backend Service - Activated on this server; scheduled to operate every 24 hours

In addition, the SAM default policy is set as follows:

• OTP support (required for OTP) is selected in the Token Initialization settings.

The SAM Connector for OTP Authentication is set, by default, to enable enrollment of OTP tokens without requiring changes in the TPO settings. For more information on how to install and configure the SafeNet Authentication Manager for simplified installation, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.
Token Assignment in SAM

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

The following tokens are supported:

- eToken PASS
- eToken NG-OTP
- SafeNet GOLD
- SMS tokens
- MobilePASS
- SafeNet eToken Virtual products
- MobilePASS Messaging
- SafeNet Mobile Authentication (iOS)
- SafeNet eToken 3400
- SafeNet eToken 3500

Tokens can be assigned to users as follows:

- **SAM Management Center**: Management site used by SAM administrators and help desk for token enrollment and lifecycle management.
- **SAM Self Service Center**: Self-service site used by end users for managing their tokens.
- **SAM Remote Service**: Self-service site used by employees not on the organization's premises as a rescue website to manage cases where tokens are lost or passwords are forgotten.

For more information on SafeNet's tokens and service portals, refer to the *SafeNet Authentication Manager 8.2 Administrator's Guide*.

Adding Palo Alto GlobalProtect as a RADIUS Client in IAS/NPS

For Windows Server 2003, the Windows RADIUS service is Internet Authentication Service (IAS). The IAS is added as the RADIUS server in Palo Alto GlobalProtect.

For Windows Server 2008 and above, the Windows RADIUS service is the Microsoft Network Policy Server (NPS). The NPS server is added as the RADIUS server in Palo Alto GlobalProtect.

Palo Alto GlobalProtect must be added as a RADIUS client on the IAS/NPS server so that IAS/NPS will authorize Palo Alto GlobalProtect for authentication.

**NOTE:** This document assumes that IAS/NPS policies are already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager.

The details below refer to NPS, and are very similar to IAS.
To add a RADIUS client:

2. From the NPS web console, in the left pane, expand RADIUS Clients and Servers, right-click RADIUS Clients and then click New.

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

3. On the New RADIUS Client window, complete the following fields on the Settings tab:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable this RADIUS client</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Friendly name</td>
<td>Enter a RADIUS client name.</td>
</tr>
<tr>
<td>Address (IP or DNS)</td>
<td>Enter the IP address or DNS of Palo Alto GlobalProtect.</td>
</tr>
<tr>
<td>Shared secret</td>
<td>Enter the shared secret for the RADIUS client. The value must be the same</td>
</tr>
<tr>
<td></td>
<td>when configuring the RADIUS server in Palo Alto GlobalProtect.</td>
</tr>
<tr>
<td>Confirm shared secret</td>
<td>Re-enter the shared secret to confirm it.</td>
</tr>
</tbody>
</table>
4. Click OK.

Palo Alto GlobalProtect is added as a RADIUS client in NPS.

**SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration**

RADIUS protocol is used for authentication and authorization. The SafeNet OTP solution supports the Microsoft IAS service (used in Windows 2003) and Microsoft NPS service (used in Windows 2008 and later) are Windows services running a RADIUS server. These services may be extended by adding plug-ins for the authentication process.

SAM’s OTP plug-in for Microsoft RADIUS Client works with Microsoft’s IAS or NPS to provide strong, authenticated remote access through the IAS or NPS RADIUS Server. When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet Authentication Manager OTP plug-in, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.
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 SAM 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.
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 IAS/NPS server. Enter Port 1812</td>
</tr>
</tbody>
</table>

![RADIUS Server Profile](image)

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

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

This section explains how to create a RADIUS authentication profile for the users. This profile can be assigned to user/s or group/s.

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

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 RADIUS</td>
</tr>
<tr>
<td>Server Profile</td>
<td>Select the server profile created in the previous section</td>
</tr>
</tbody>
</table>

5. Click on OK button.
Configuring Global Protect Gateway

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

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

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

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 will demonstrate 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**.

![GlobalProtect client screenshot](image1.png)

*(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.

![GlobalProtect portal authentication screenshot](image2.png)

*(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.

4. The user clicks OK. The user is now connected to the VPN.
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><strong>Address</strong></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><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://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.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 SafeNet Knowledge Base.</td>
</tr>
</tbody>
</table>