SafeNet Authentication Manager
Integration Guide

Using RADIUS Protocol for CyberArk Privileged Account Security Suite
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012984-001, Rev. A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>April 2015</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

<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>4</td>
</tr>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS-based Authentication using SAM</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS Authentication Flow using SAM</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS Prerequisites</td>
<td>6</td>
</tr>
<tr>
<td>Configuring SafeNet Authentication Manager</td>
<td>6</td>
</tr>
<tr>
<td>Synchronizing Users Stores to SAM</td>
<td>6</td>
</tr>
<tr>
<td>Configuring SAM’s Connector for OTP Authentication</td>
<td>7</td>
</tr>
<tr>
<td>Assigning a Token in SAM</td>
<td>7</td>
</tr>
<tr>
<td>Adding CyberArk Privileged Account Security Suite as a RADIUS Client in IAS/NPS</td>
<td>8</td>
</tr>
<tr>
<td>SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration</td>
<td>10</td>
</tr>
<tr>
<td>Configuring CyberArk Privileged Account Security Suite</td>
<td>10</td>
</tr>
<tr>
<td>Configuring a RADIUS Shared Secret</td>
<td>10</td>
</tr>
<tr>
<td>Configuring a RADIUS Server on the Vault</td>
<td>11</td>
</tr>
<tr>
<td>Adding RADIUS Authentication to the Privileged Account Security Portal</td>
<td>12</td>
</tr>
<tr>
<td>Configuring a User for RADIUS Authentication</td>
<td>14</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>16</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>17</td>
</tr>
</tbody>
</table>
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as CyberArk Privileged Account Security Suite.

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 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.

CyberArk Enterprise Password Vault®, part of the CyberArk Privileged Account Security Solution, enables organizations to secure, manage and track the use of privileged credentials, whether on-premise or in the cloud, across operating systems, databases, applications, hypervisors, network devices and more.

This document describes how to:
- Configure CyberArk Privileged Account Security Suite to work with SafeNet Authentication Manager in RADIUS mode.

It is assumed that the CyberArk Privileged Account Security Suite 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.

CyberArk Privileged Account Security Suite 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**—Version 8.2 (HF 493)
- **CyberArk Privileged Account Security Suite**—Version 9.0.1
Audience

This document is targeted to system administrators who are familiar with CyberArk Privileged Account Security Suite, 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 the 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 CyberArk Privileged Account Security Suite.

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

To enable SafeNet Authentication Manager to receive RADIUS requests from CyberArk Privileged Account Security Suite, ensure the following:

- End users can authenticate from the CyberArk Privileged Account Security Suite environment with a static password before configuring CyberArk Privileged Account Security Suite to use RADIUS authentication.
- Ports 1812/1813 are open to and from CyberArk Privileged Account Security Suite.
- 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 signatures.

Configuring SafeNet Authentication Manager

The deployment of multi-factor authentication using SAM with CyberArk Privileged Account Security Suite using the RADIUS protocol requires the following:

- Synchronizing Users Stores to SAM, page 7
- Configuring SAM’s Connector for OTP Authentication, page 7
- Assigning a Token in SAM, page 8
- Adding CyberArk Privileged Account Security Suite as a RADIUS Client in IAS/NPS, page
Synchronizing Users Stores to SAM

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:
- 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 the 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 Back-end 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 (Token Policy Object) 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.

Assigning a Token in SAM

SAM supports a number of OTP authentication methods that can be used as a second authentication factor for users authenticating through CyberArk Privileged Account Security Suite.

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 personnel 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 CyberArk Privileged Account Security Suite 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 CyberArk Privileged Account Security Suite.

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 CyberArk Privileged Account Security Suite.

CyberArk Privileged Account Security Suite must be added as a RADIUS client on the IAS/NPS server so that IAS/NPS will authorize CyberArk Privileged Account Security Suite 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.

---

1. Click **Start > Administrative Tools > Network Policy Server**.
2. From the NPS web console, expand **RADIUS Clients and Servers**, right-click **RADIUS Clients** and then click **New**.

![Network Policy Server](image)

(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><strong>Enable this RADIUS client</strong></td>
<td>Select this option.</td>
</tr>
<tr>
<td><strong>Friendly name</strong></td>
<td>Enter a name for the RADIUS client.</td>
</tr>
<tr>
<td><strong>Address (IP or DNS)</strong></td>
<td>Enter the CyberArk Privileged Account Security Suite IP address or DNS.</td>
</tr>
<tr>
<td><strong>Manual/Generate</strong></td>
<td>Select <strong>Manual</strong>.</td>
</tr>
<tr>
<td><strong>Shared secret</strong></td>
<td>Enter the shared secret for the RADIUS client. This entry must match the shared secret that was used when the RADIUS server was configured in CyberArk Privileged Account Security Suite.</td>
</tr>
<tr>
<td><strong>Confirm shared secret</strong></td>
<td>Re-enter the shared secret.</td>
</tr>
</tbody>
</table>

![New RADIUS Client settings](image)

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

4. Click **OK**. CyberArk Privileged Account Security Suite 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) as 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 CyberArk Privileged Account Security Suite

Configuring CyberArk Privileged Account Security Suite to use RADIUS authentication requires the following:

- Configuring a RADIUS Shared Secret, page 10
• Configuring a RADIUS Server on the Vault, page 11
• Adding RADIUS Authentication to the Privileged Account Security Portal, page 12
• Configuring a User for RADIUS Authentication, page 14

For additional information on configuring RADIUS authentication, please refer to the “RADIUS Authentication” section in the CyberArk Privileged Account Security Installation Guide.

Configuring a RADIUS Shared Secret

1. Create a certificate for the vault (if needed).
2. On the RADIUS server, run CAVaultManager to create an encrypted RADIUS shared secret file. Refer to the following example:

   CAVaultManager SecureSecretFiles /SecretType Radius /Secret VaultSecret /SecuredFileName c:\RadiusSecret.dat
Configuring a RADIUS Server on the Vault

1. On the vault server, open **Server Central Administration**.

2. Click ⭕ to shut down the PrivateVault server.

3. Navigate to `C:\Program Files (x86)\PrivateArk\Server`.

4. Locate and open `DBParm.ini`, and add the `RadiusServerInfo` key under the `[MAIN]` section:
   ```plaintext
   RadiusServersInfo=RADIUS_Server_IP;RADIUS_Port;vaulthostname;radiusauth.dat
   ```

   Values are defined below.

<table>
<thead>
<tr>
<th><strong>RADIUS_Server_IP</strong></th>
<th>The IP of the RADIUS server</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RADIUS_Port</strong></td>
<td>Port number of the RADIUS</td>
</tr>
<tr>
<td><strong>vaulthostname</strong></td>
<td>The name of the RADIUS client</td>
</tr>
<tr>
<td><strong>radiusauth.dat</strong></td>
<td>The shared secret file, created in the previous section</td>
</tr>
</tbody>
</table>

   (The screen image above is from CyberArk®. Trademarks are the property of their respective owners.)
5. Open Server Central Administration and click \( \text{Start} \) to start the PrivateVault server.

**Adding RADIUS Authentication to the Privileged Account Security Portal**

1. Log in to the Privileged Account Security portal as **administrator**.

![Privileged Account Security Portal](image)

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

2. Click the **ADMINISTRATION** tab, and then select **Options**.

![Administration Options](image)

*(The screen image above is from CyberArk®. Trademarks are the property of their respective owners.)*
3. Expand **Authentication Methods**, and then select **radius**.

![Image of Authentication Methods settings with radius selected](image)

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

4. On the **Properties** window, complete the following fields, click **Apply**, and then click **Save**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DisplayName</strong></td>
<td>Enter a name for the policy. This name will be displayed on the Privileged Account Security portal login page.</td>
</tr>
<tr>
<td><strong>UseRadius</strong></td>
<td>Select <strong>Yes</strong>.</td>
</tr>
</tbody>
</table>

5. On the Privileged Account Security portal login page, verify that the new authentication policy has been added (for example, **Safenet SAM**).

![Image of CyberArk Privileged Account Security](image)

*(The screen image above is from CyberArk®. Trademarks are the property of their respective owners.)*
Configuring a User for RADIUS Authentication

1. Open the PrivateArk console and log in to the vault.

![PrivateArk Console](image1.png)

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

2. Select **Tools > Administrative Tools > Users and Groups**.

![Users and Groups](image2.png)

(The screen image above is from CyberArk®. Trademarks are the property of their respective owners.)
3. Select the user and click **Update**.

   ![User and Groups on Server Demo Vault](image1)

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

4. Click the **Authentication** tab.

5. Select **RADIUS Authentication** from the **Authentication method** menu.

   ![Update User](image2)

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

6. Click **OK**, and then click **Close**.
Running the Solution

Verify the integration solution after you have successfully configured CyberArk Privileged Account Security Suite for SAM authentication.

For this integration, the MobilePASS token is configured for authentication with the SAM solution.

1. On the Privileged Account Security Portal login page, select the RADIUS authentication method (for example, Safenet SAM).

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

2. Type the username and the OTP, and then click Sign in.

(The screen image above is from CyberArk®. Trademarks are the property of their respective owners.)
After successful authentication, the user is logged in.

(Screenshot image above is from CyberArk®. 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 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>
</table>
| Address              | SafeNet, Inc.  
4690 Millennium Drive  
Belcamp, Maryland 21017 USA |
| Phone                | United States 1-800-545-6608  
International 1-410-931-7520 |
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. |