SafeNet Authentication Service
Integration Guide

Using RADIUS Protocol for ManageEngine Password Manager Pro
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-013242-001, Rev. A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>July 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

Third-Party Software Acknowledgement........................................................................................................4
Description..........................................................................................................................................................4
Applicability......................................................................................................................................................4
Environment.....................................................................................................................................................4
Audience.........................................................................................................................................................5
RADIUS-based Authentication using SAS Cloud.............................................................................................5
RADIUS-based Authentication using SAS-SPE and SAS-PCE.................................................................6
RADIUS Authentication Flow using SAS ..................................................................................................6
Prerequisites...................................................................................................................................................7
Configuring SafeNet Authentication Service.................................................................................................7
  Synchronizing Users Stores to SAS ................................................................................................................7
  Assigning an Authenticator in SAS ..............................................................................................................8
  Adding ManageEngine Password Manager Pro as an Authentication Node in SAS ..........................8
  Checking the SAS RADIUS Server’s IP Address ..................................................................................10
Configuring ManageEngine Password Manager Pro ..................................................................................12
Running the Solution......................................................................................................................................16
Support Contacts...........................................................................................................................................17
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as ManageEngine Password Manager Pro.

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.

ManageEngine Password Manager Pro is a secure vault for storing and managing shared, sensitive information such as passwords, documents, and digital identities of enterprises. It can integrate with your Active Directory systems to ease password management.

This document describes how to:

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

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

ManageEngine Password Manager Pro 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 (SAS)**—SafeNet’s cloud-based authentication service
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—Version 3.3
- **ManageEngine Password Manager Pro**—Version 7.5.0
Audience

This document is targeted to system administrators who are familiar with ManageEngine Password Manager Pro, 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.

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: http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-Agent-IASNPS.pdf

For more details on how to install and configure FreeRADIUS, refer to the **SAS FreeRADIUS Agent Configuration Guide.**
RADIUS-based Authentication using SAS-SPE and SAS-PCE

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: http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-Agents-IASNPS.pdf

- **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 dataflow of a multi-factor authentication transaction for ManageEngine Password Manager Pro.

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

To enable SafeNet Authentication Service to receive RADIUS requests from ManageEngine Password Manager Pro, ensure the following:

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

- Synchronizing Users Stores to SAS, page 7
- Assigning an Authenticator in SAS, page 8
- Adding ManageEngine Password Manager Pro as an Authentication Node in SAS, page 8
- Checking the SAS RADIUS Server’s IP Address, page 10

Synchronizing Users Stores to SAS

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.
Assigning an Authenticator in SAS

SAS supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through ManageEngine Password Manager Pro.

The following authenticators are supported:

- eToken PASS
- RB-1 Keypad Token
- SafeNet GOLD
- SMS Token
- MP-1 Software Token

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 ManageEngine Password Manager Pro as an Authentication Node in SAS

Add a RADIUS entry in the SAS **Auth Nodes** module to prepare it to receive RADIUS authentication requests from ManageEngine Password Manager Pro. You will need the IP address of ManageEngine Password Manager Pro and the shared secret to be used by both SAS and ManageEngine Password Manager Pro.

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

![Auth Nodes](image1)

3. Under **Auth Nodes**, click the **Auth Nodes** link.

![Auth Nodes](image2)

4. Under **Auth Nodes**, click **Add**.

![Auth Nodes](image3)

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 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.</td>
</tr>
</tbody>
</table>
The authentication node is added to the system.

Checking the SAS RADIUS Server’s IP Address

Before adding SAS as a RADIUS server in ManageEngine Password Manager Pro, check the IP address of the SAS RADIUS server. The IP address will then be added to ManageEngine Password Manager Pro 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 click **Auth Nodes**.

![COMMS tab and Auth Nodes](image)

3. Under **Auth Nodes**, click the **Auth Nodes** link.

The SAS RADIUS server details are displayed.

![Auth Nodes](image)
Configuring ManageEngine Password Manager Pro

Configure ManageEngine Password Manager Pro to use a RADIUS server for user authentication. The Password Manager Pro service must be started before configuring it.

1. In a web browser, open the Manage Engine Password Manager Pro application.
2. On the login window, enter the administrator user name and password, and then click Login.

3. On the Password Manager Pro home page, click Admin.

4. Under the General section, click General Settings.
5. On the **General Settings** window, in the left pane, click **User Management**.

![General Settings](image)

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

6. In the right pane, clear the **Allow 'Local Authentication' when 'AD/LDAP/RADIUS/Smart Card/SAML Single Sign On authentication is enabled** check box.

7. If the following message is displayed, click **OK**.

![Message from webpage](image)

*Please make sure you have at least one user with the 'Administrator' role, among the users imported from AD/LDAP/RADIUS*

8. Click **Save**.

9. On the Password Manager Pro home page, click **Admin**.

10. Under the **Users** section, click **RADIUS**.

![Password Manager Pro](image)

*(The screen image above is from ManageEngine™. Trademarks are the property of their respective owners.)*
11. Under Configure RADIUS Server, click Configure.

12. On the Configure RADIUS Server window, complete the following fields, and then click Save.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name / IP Address</td>
<td>Enter the IP address of the RADIUS server.</td>
</tr>
<tr>
<td>Server Authentication Port</td>
<td>Enter the port number through which the RADIUS server communicates.</td>
</tr>
<tr>
<td>Server Protocol</td>
<td>Select either PAP or MSCHAP2.</td>
</tr>
<tr>
<td>Authentication Retries</td>
<td>Select the number of tries for authentication, or keep the default selection.</td>
</tr>
<tr>
<td>Server Secret</td>
<td>Select Specify Server Secret manually, and then enter the server secret text.</td>
</tr>
</tbody>
</table>

(The screen image above is from ManageEngine™. Trademarks are the property of their respective owners.)
13. Under **Enable RADIUS Authentication**, click **Enable**.

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

The **Current Status** is changed to **Enabled**.

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

For this integration, the SafeNet e-Token PASS is configured for authentication with the SAS solution.

1. Ensure that the ManageEngine Password Manager Pro service is started.
2. In a web browser, open the **Manage Engine Password Manager Pro** application.
3. On the login window, complete the following fields, and then click **Login**.

<table>
<thead>
<tr>
<th>User Name</th>
<th>Enter your user name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Generate an OTP using the SafeNet eToken PASS token, and then enter the OTP in this field.</td>
</tr>
<tr>
<td>Log on to</td>
<td>Select <strong>RADIUS</strong>.</td>
</tr>
</tbody>
</table>

![Login Screen](image)

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

If the credentials are validated, the user will be successfully logged in.

![Logged In Screen](image)

*(The screen image above is from ManageEngine™. 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>
<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</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>Technical Support</td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td>Customer Portal</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>