SafeNet Authentication Manager
Integration Guide

Using SAM as an Identity Provider for ManageEngine Password Manager Pro
All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2015 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

**Document Part Number:** 007-013244-001, Rev. A
**Release Date:** September 2015
# Contents

Third-Party Software Acknowledgement ................................................................................. 4  
Description .......................................................................................................................... 4  
Applicability ......................................................................................................................... 4  
Environment .......................................................................................................................... 4  
Audience .................................................................................................................................. 4  
SAML Authentication using SAM .......................................................................................... 5  
Authentication Flow using SAM ............................................................................................. 5  
SAML Prerequisites ............................................................................................................... 5  
Configuring SafeNet Authentication Manager ...................................................................... 6  
  Synchronizing User Stores to SAM ..................................................................................... 6  
  Assigning Tokens in SAM .................................................................................................... 6  
  Configuring SAM as an Identity Provider .......................................................................... 7  
  Exporting the SAM’s Certificate and Downloading the SAM’s Metadata ......................... 9  
  Configuring SAM for SAML-based User Federation .......................................................... 11  
Configuring ManageEngine Password Manager Pro ............................................................. 13  
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 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.

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) tokens managed by SafeNet Authentication Manager.
- Configure SAML authentication in ManageEngine Password Manager Pro using SafeNet Authentication Manager as an identity provider.

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 Manager.

ManageEngine Password Manager Pro can be configured to support multi-factor authentication in several modes. The SAML authentication 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 (Hotfix 710)
- **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 Manager.
SAML Authentication using SAM

SAM provides a SAML authentication option that is already implemented in the SAM environment and can be used without any installation.

Authentication Flow using SAM

SafeNet Authentication Manager communicates with a large number of service providers and cloud-based service solutions using the SAML 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. The user is redirected to SafeNet Authentication Manager (SAM). SAM collects and evaluates the user’s credentials.
2. SAM returns a response to ManageEngine Password Manager Pro, accepting or rejecting the user’s authentication request.

SAML Prerequisites

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

- End users can authenticate from the ManageEngine Password Manager Pro environment with a static password.
- The user in SAM and ManageEngine Password Manager Pro must have the same username.
Configuring SafeNet Authentication Manager

Using SAM as an identity provider for ManageEngine Password Manager Pro requires the following:

- Synchronizing User Stores to SAM, page 6
- Assigning Tokens in SAM, page 6
- Configuring SAM as an Identity Provider, page 7
- Exporting the SAM’s Certificate and Downloading the SAM’s Metadata, page 9
- Configuring SAM for SAML-based User Federation, page 11

Synchronizing User Stores to SAM

SAM manages and maintains tokens information in its data store, including the tokens status 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

Assigning Tokens in SAM

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

The following tokens are supported:

- eToken PASS
- SafeNet GOLD
- SafeNet eToken 3400
- SafeNet eToken 3500
- eToken NG-OTP
- MobilePASS
- SafeNet eToken Virtual products
- MobilePASS Messaging
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*.

### Configuring SAM as an Identity Provider

To use ManageEngine Password Manager Pro as a service provider and SAM as an identity provider, SAM must be configured as an Identity Provider.

1. From the Windows **Start** menu, click **Programs > SafeNet > SafeNet Authentication Manager > Configuration Manager**.

*(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)*
2. Click the **Action** tab, and then select **Cloud Configuration**.

3. On the **Info for Service Provider** tab, type the web address of the SAM portal server in the **Domain URL** field.

   The remaining fields are generated according to the Domain URL that was entered.

4. Click **OK**.
Exporting the SAM’s Certificate and Downloading the SAM’s Metadata

SAM’s certificate and metadata are shared between SAM and ManageEngine Password Manager Pro. The certificate will be used to sign the authentication requests.

1. From Windows Start menu, click Programs > SafeNet > SafeNet Authentication Manager > Configuration Manager.

2. Click the Action tab, and then select Cloud Configuration.
3. On the **Info for Service Provider** tab, click **Export Certificate**, and save the SAM’s certificate file.

![](image)

4. Click **Download Metadata**, and save the metadata file (for example, **SAM-IDP-Metadata.xml**).

![](image)

5. Click **OK**.
Configuring SAM for SAML-based User Federation

SAM's Token Policy Object (TPO) policies include application authentication settings for SAML service providers. These settings are used by SAM's portal to communicate with service providers.

For general portal configuration, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

To edit the Token Policy Object for SAM's portal configuration:

1. Open the Token Policy Object Editor for the appropriate group. See the SafeNet Authentication Manager 8.2 Administrator’s Guide for more information.

2. In the left pane, click Protected Application Settings > User Authentication.

3. In the right pane, double-click Application Authentication Settings.

4. Select Define this policy setting, select Enabled, and then click Definitions.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
5. In the left pane, right-click **Application Authentication Settings**, select **Create a new profile**, and then specify the details for a new profile and save it.

![Image of Application Authentication Settings](image)

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

6. In the left pane, right-click the new profile, and then rename it to a user-friendly name (for example, **Manage Engine-Password Manager Pro**).

7. In the left pane, click the new profile.

8. In the right pane, double-click on the following policies, and then enter the appropriate information:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application Issuer</strong></td>
<td>Enter the Entity ID of ManageEngine Password Manager Pro (for example, 182e240fd2f3491c97f528b0888af0c0).</td>
</tr>
<tr>
<td><strong>SAM issuer</strong></td>
<td>Enter a unique SAM ID to be identified in SAML authentication. This entity ID should match the entity ID of the SAM metadata file.</td>
</tr>
<tr>
<td><strong>Application’s login URL</strong></td>
<td>Enter the ManageEngine Password Manager Pro Consumer Assertion URL. The format of the URL is https://&lt;pmp-server&gt;:7272/saml2.</td>
</tr>
<tr>
<td><strong>Audience URI</strong></td>
<td>Enter the ManageEngine Password Manager Pro entity ID. It should match the entity ID in the <strong>Application Issuer</strong> field.</td>
</tr>
<tr>
<td><strong>User mapping</strong></td>
<td>Select <strong>AccountName</strong>.</td>
</tr>
<tr>
<td><strong>OTP authentication</strong></td>
<td>Enable this policy.</td>
</tr>
</tbody>
</table>

The following is an example of the completed policy fields in the Application Authentication Settings window:

![Application Authentication Settings](image1)

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

10. Click OK until all of the Token Policy Object Editor windows are closed.

**Configuring ManageEngine Password Manager Pro**

Before you begin, make sure the Password Manager Pro service is started, and then configure ManageEngine Password Manager Pro and add SAM as an identity provider.

1. In a web browser, open the ManageEngine Password Manager Pro application.
2. On the login window, enter the administrator User Name and Password, and then click Log In.

![Login Window](image2)

(The screen image above is from ManageEngine™. Trademarks are the property of their respective owners.)
3. On the Password Manager Pro Home page, click Admin.

![Password Manager Pro Home page with Admin highlighted](image)

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

4. Under the Users section, click SAML Single Sign On.

![Password Manager Pro Users section with SAML Single Sign On highlighted](image)

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

5. Under Configure Identity Provider Details, click Browse, select the SAM metadata file (for example, SAM-IDP-Metadata.xml), and then click Upload.

![Configuration for Single Sign-On using SAML](image)

(The screen image above is from ManageEngine™. Trademarks are the property of their respective owners.)
6. Under **Import IdPs Certificate**, click **Browse**, select the SAM certificate file, and then click **Save**.

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

7. Under **Enable / Disable SAML Single Sign On**, 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 SAM solution.

1. Open the following URL in a web browser: `https://<pmp-server>:7272/saml2`
   where `pmp-server` is the fully-qualified name or IP address of the machine running the ManageEngine Password Manager Pro server.

2. You are redirected to the SAM login page. In the **Username** field, enter your user name, and then click **OK**.

3. The **OTP Authentication** page is displayed. Generate a one-time password using the SafeNet token, enter it in the **OTP Authentication Code** field, and then click **OK**.
After successful authentication, you are redirected to your ManageEngine Password Manager Pro account.

(Thescreen 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 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, 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 Gemalto Knowledge Base.</td>
</tr>
</tbody>
</table>