SafeNet Authentication Client

Integration Guide

Using SAC CBA for Manage Engine-Password Manager Pro

gemalto
security to be free

Document Part Number: 007-013283-001, Rev. A

Release Date: September 2015

Contents

Third-Party Software Acknowledgement 4
Description 4
Applicability 5
Environment 5
Audience 5
CBA Flow using SAC 6
Prerequisites 6
Supported Tokens in SAC 7
    Certificate-based USB Tokens 7
    Smart Cards 7
    Certificate-based Hybrid USB Tokens 7
    Software Tokens 7
Configuring Manage Engine-Password Manager Pro 8
Running the Solution 10
Support Contacts 11

Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Manage Engine-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

Customers today are looking to desktop virtualization to transform static desktops into dynamic mobile workspaces that can be centrally and securely managed from the data center, and accessed across a wide range of devices and locations. Deploying desktop virtualization without strong authentication is like putting your sensitive data in a vault (the data center) and leaving the key (user password) under the door mat. A robust user authentication solution is required to screen access and provide proof-positive assurance that only authorized users are allowed access.

SafeNet Authentication Client (SAC) is a public key infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities. SafeNet's certificate-based tokens provide secure remote access, as well as other advanced functions, in a single token, including digital signing, password management, network logon, and combined physical/logical access.

The tokens come in different form factors, including USB tokens, smart cards, and software tokens. All of these form factors are interfaced using a single middleware client, SafeNet Authentication Client (SAC). The SAC generic integration with CAPI, CNG, and PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications, offering secure web access, secure network logon, PC and data security, and secure email. PKI keys and certificates can be created, stored, and used securely with the hardware or software tokens.

SafeNet Authentication Manager (SAM) provides your organization with a comprehensive platform to manage all of your authentication requirements, across the enterprise and the cloud, in a single, integrated system. SAM enables management of the complete user authentication life cycle. SAM links tokens with users, organizational rules, and security applications to allow streamlined handling of your organization's authentication infrastructure with a flexible, extensible, and scalable management platform.

SAM is a comprehensive token management system. It is an out-of-the-box solution for Public Certificate Authorities (CA) and enterprises to ease the administration of SafeNet's hardware or software tokens devices. SAM is designed and developed based on the best practices of managing PKI devices in common PKI implementations. It offers robust yet easy to customize frameworks that meets different organizations' PKI devices management workflows and policies. Using SAM to manage tokens is not mandatory, but it is recommended for enterprise organizations.

For more information, refer to the *SafeNet Authentication Manager Administrator Guide*.

Manage Engine-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 the management of all your passwords.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to Manage Engine-Password Manager Pro using SafeNet tokens.

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

Manage Engine-Password Manager Pro can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with SafeNet products.

Applicability

The information in this document applies to:

- **SafeNet Authentication Client (SAC)—**SafeNet Authentication Client is the middleware that manages SafeNet's tokens.
- **Manage Engine-Password Manager Pro**

Environment

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

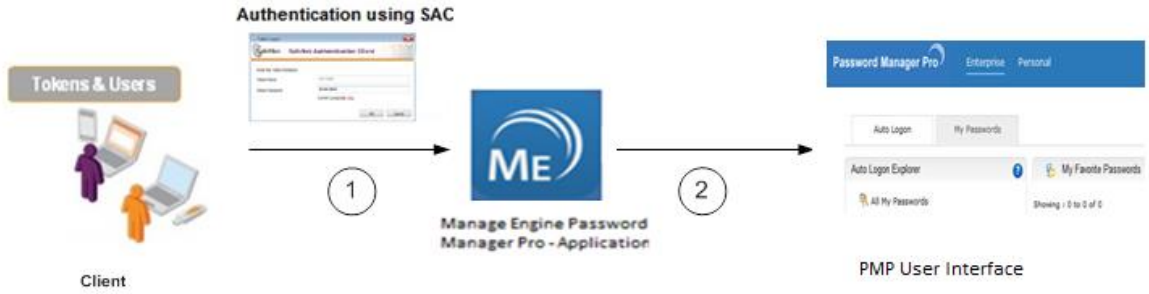
- **SafeNet Authentication Client (SAC)—**Version 9.0
- **Manage Engine-Password Manager Pro—**Version 7.5.0

Audience

This document is targeted to system administrators who are familiar with Manage Engine-Password Manager Pro, and are interested in adding certificate-based authentication capabilities using SafeNet tokens.

CBA Flow using SAC

The diagram below illustrates the flow of certificate-based authentication.



1. A user attempts to connect to the PMP application. The user inserts the SafeNet token on which his certificate resides, and, when prompted, enters the token password.
2. After successful authentication, the user is provided access to the PMP user interface.

Prerequisites

This section describes the prerequisites that must be installed and configured before implementing certificate-based authentication for Manage Engine-Password Manager Pro using SafeNet tokens:

- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. Note that any CA can be used. However, in this guide, integration is demonstrated using Microsoft CA.
- If SAM is used to manage the tokens, TPO (Token Policy Object) should be configured with a Microsoft CA connector. For additional details, refer to the “Connector for Microsoft CA” section in the *SafeNet Authentication Manager Administrator’s Guide*.
- Users must have a SafeNet token enrolled with an appropriate certificate.
- SafeNet Authentication Client (SAC 9.0) should be installed on all client machines.

Supported Tokens in SAC

SAC supports a number of tokens that can be used as second authentication factor for users who authenticate to Manage Engine-Password Manager Pro.

SafeNet Authentication Client 9.0 (GA) supports the following tokens:

Certificate-based USB Tokens

- SafeNet eToken PRO Java 72K
- SafeNet eToken PRO Anywhere
- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID and VSR

Smart Cards

- SafeNet eToken PRO Smartcard 72K
- SafeNet eToken 4100

Certificate-based Hybrid USB Tokens

- SafeNet eToken 7300
- SafeNet eToken 7300-HID
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)

Software Tokens

- SafeNet eToken Virtual
- SafeNet eToken Rescue

Configuring Manage Engine-Password Manager Pro

In this section, you will configure Password Manager Pro to work with certificate-based authentication.

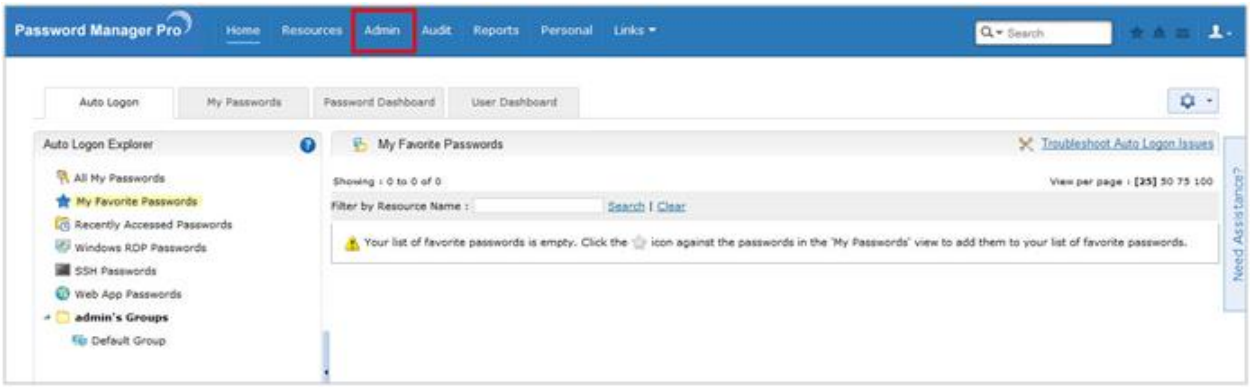
1. From the Windows **Start** menu, select **All Programs > Manage Engine Password Manager Pro**.
2. Click **Start Service**.

> **NOTE:** If a message is displayed which indicates that the PMP server cannot be started because an instance of the service is already running, please ignore the message.

3. In the Windows taskbar, right-click the PMP icon  , and then click **PMP Web Console**.
4. The PMP application will open in a web browser. Enter your admin **User Name** and **Password**, and then click **Login**.

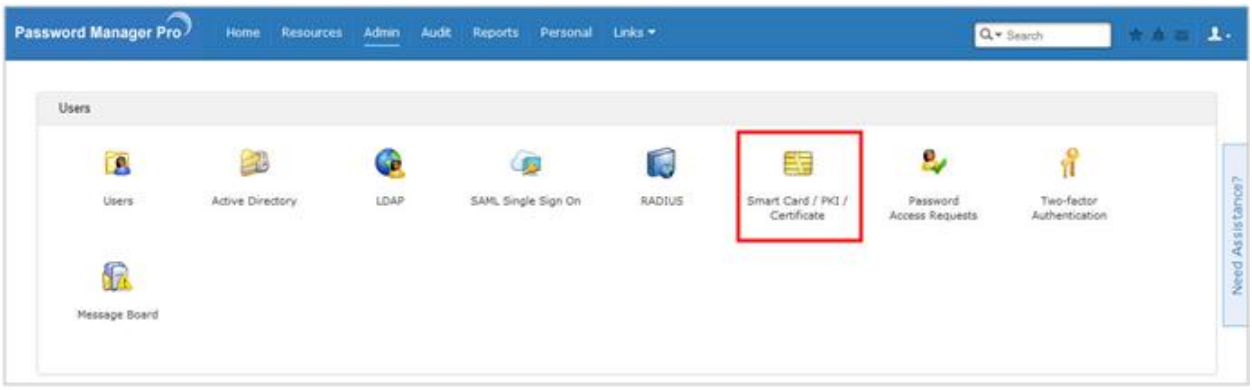
(The screen image above is from Password Manager Pro®. Trademarks are the property of their respective owners.)

5. Click the **Admin** tab.



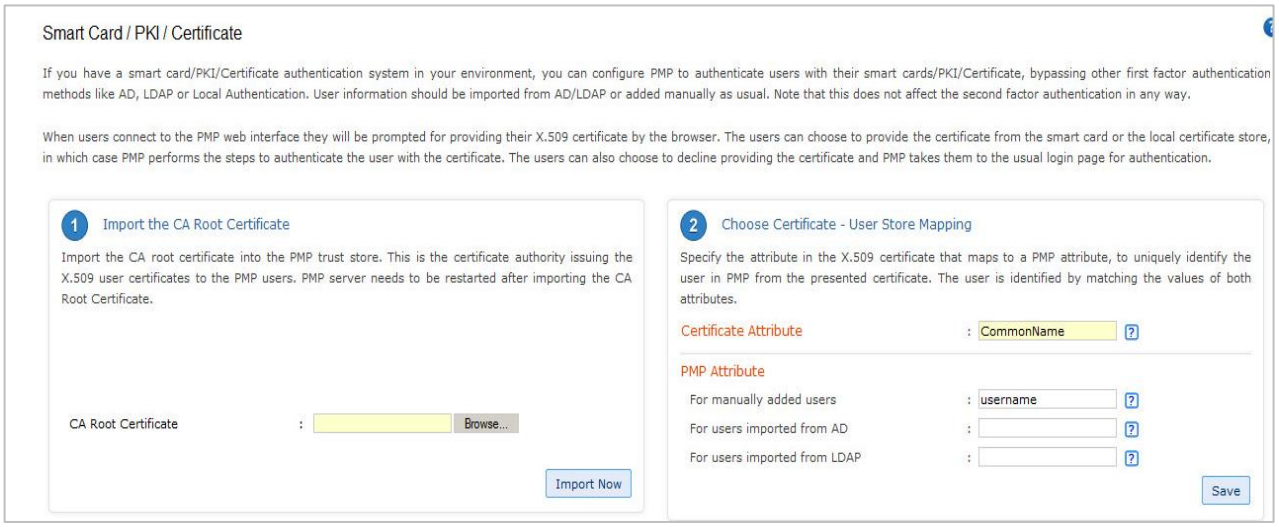
(The screen image above is from Password Manager Pro®. Trademarks are the property of their respective owners.)

6. Click **Smart Card/PKI/Certificate**.



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

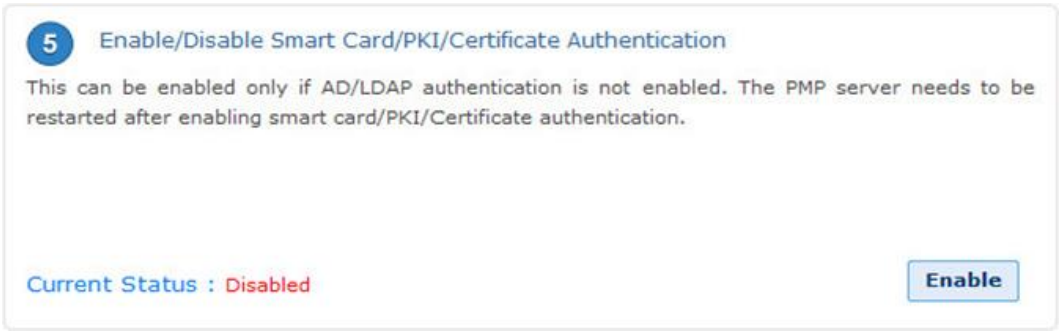
7. In the **Import the CA Root Certificate** section, browse to the CA root certificate, and then click **Import now**.



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

8. Restart the PMP server.
9. In the Windows taskbar, right-click the PMP icon  , and then click **Stop PMP Service**. When the PMP service is stopped, the PMP icon will turn red: 
10. Right-click the PMP icon  again, and then and click **Start PMP Service**. When the PMP service is started, the PMP icon will turn blue: 
11. In the **Choose Certificate-User Store Mapping** section, in the **Certificate Attribute** field, enter **CommonName**, and then click **Save**.

12. In the **Enable/Disable Smart Card/PKI/Certificate Authentication** section, click **Enable**.



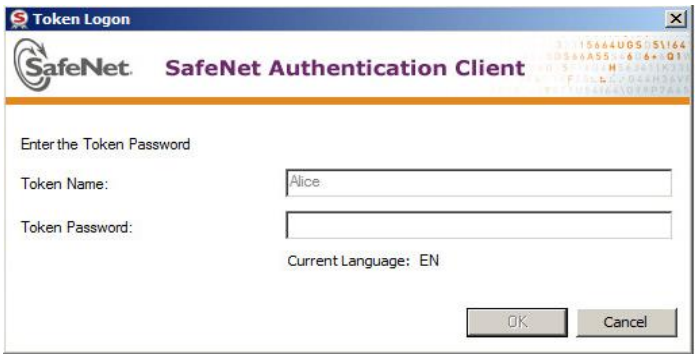
(The screen image above is from Password Manager Pro®. Trademarks are the property of their respective owners.)

13. Restart the PMP server.

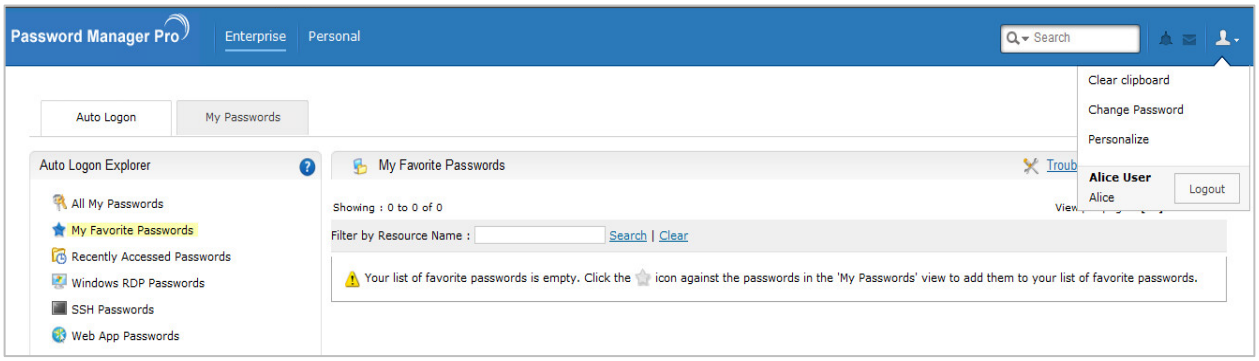
Running the Solution

Check the final running solution of Manage Engine-Password Manager Pro with SafeNet Authentication Client.

1. Open the web browser from the client machine and type the **Manage Engine-Password Manager Pro** URL.
2. The **SafeNet Authentication Client** login window is displayed. Enter the **Token Password**, and then click **OK**.



After a successful authentication, you are granted access to the Password Manager Pro dashboard.



(The screen image above is from Password Manager Pro®. 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.

Contact Method	Contact Information	
Address	Gemalto, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com 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.	