SafeNet Authentication Client

Integration Guide

Using SafeNet Authentication Client CBA for Evidian ESSO

gemalto
security to be free

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.

Document Part Number: 007-013818-001, Rev. A

Release Date: May 2017

Contents

Third-Party Software Acknowledgement

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

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 datacenter, 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 datacenter), 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*.

The number of passwords required from users never stops growing. It becomes necessary to simplify access to your information system, but also to increase security by reducing the risk of losing or sharing passwords.

Evidian Enterprise SSO replaces user passwords with a single authentication such as a password, biometrics, a smartcard or a radio badge. Access is immediate, whether the applications are internal or external to the company.

The result for users is simplified access to their applications – they automatically comply with the security policy. And by removing tiresome administration tasks, Evidian Enterprise SSO simplifies information system management.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to Evidian ESSO using Gemalto tokens and smart cards.

It is assumed that the Evidian ESSO environment is already configured and working with static passwords prior to implementing Gemalto multi-factor authentication.

Evidian ESSO can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with Gemalto products.

Applicability

The information in this document applies to:

- **SafeNet Authentication Client (SAC) Typical installation mode**— SafeNet Authentication Client is public key infrastructure (PKI) middleware that manages Gemalto's tokens and smart cards.
- **SafeNet Authentication Client (SAC) IDGo800 Compatible mode**— IDGo800 Minidriver based package, uses Microsoft Smart Card Base Cryptographic Provider to manage Gemalto IDPrime MD smart cards.
- **Enterprise SSO 9**

For more details about different SAC installation modes, refer to the Customization section in the *SafeNet Authentication Client Administrator Guide.*

Environment

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

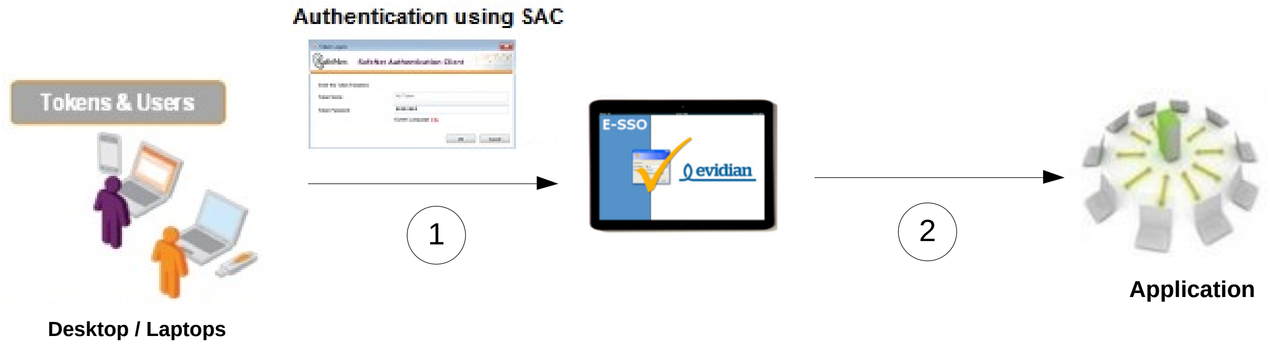
- **SafeNet Authentication Client (SAC)**— *version 10.2*
- **Evidian ESSO**

Audience

This document is intended for system administrators who are familiar with Evidian ESSO, and are interested in adding certificate-based authentication capabilities using Gemalto tokens and smart cards.

CBA Flow using SafeNet Authentication Client

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



1. A user attempts to login to an application using the Evidian ESSO client application. The user inserts the Gemalto token/smart card on which his certificate resides, and, when prompted, enters the token/smart card password.
2. After successful authentication, the user is authenticated to the application.

Prerequisites

This following prerequisites must be installed and configured before implementing certificate-based authentication for Evidian ESSO using Gemalto tokens and smart cards:

- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. In general, any CA can be used. However, in this guide, integration is demonstrated using Microsoft CA.
- If SAM is used to manage the tokens, Token Policy Object (TPO) must be configured with the MS CA Connector. For further details, refer to the section "Connector for Microsoft CA" in the *SafeNet Authentication Manager Administrator's Guide*.
- Users must have a Gemalto token/smart card with an appropriate certificate enrolled on it.
- SafeNet Authentication Client 10.2 should be installed on all client machines.

Supported Tokens in SafeNet Authentication Client

SafeNet Authentication Client (SAC) supports a number of devices that can be used as a second authentication factor for users who authenticate to Evidian ESSO.

SafeNet Authentication Client 10.2 (GA) supports the following tokens:

Certificate-based USB tokens

- SafeNet eToken 5110 GA
- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 CC

Smart Cards

- Gemalto IDPrime MD 830
- Gemalto IDPrime MD 840

For a full list of all supported devices, refer to the *SafeNet Authentication Client Customer Release Notes*.

Configuring Evidian ESSO

In this section we will describe how to configure CBA with Evidian ESSO.

NOTES: This document assumes that Evidian ESSO is installed and configured with windows and password authentication.

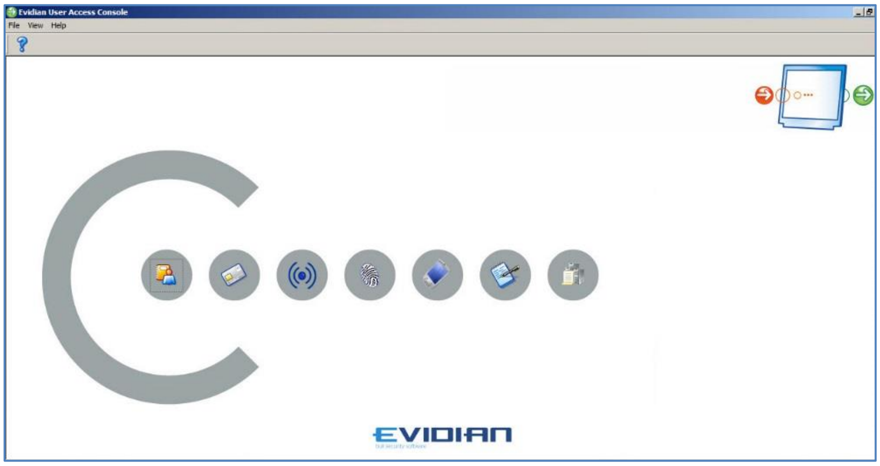
In this guide we'll demonstrate a demo app that was written to show the ESSO ability, to authenticate an application.

Updating Token/Smart Card Support on the Server

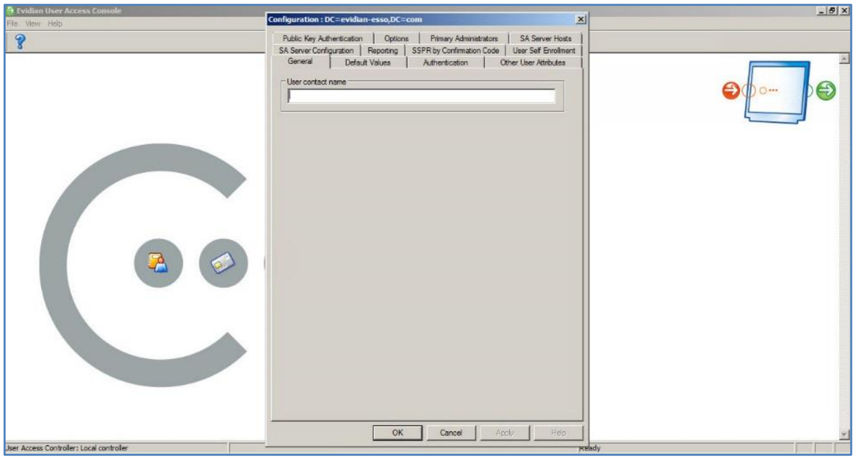
To update token support, download the configuration file (**TokenManagerStructure.xml**) from here: KB0015671

To enable Evidian to support Gemalto's smart cards and tokens, perform the following update:

1. Open the **Evidian User Access Console.**



2. Select **File > Configuration.**



3. Select the **Authentication** tab.

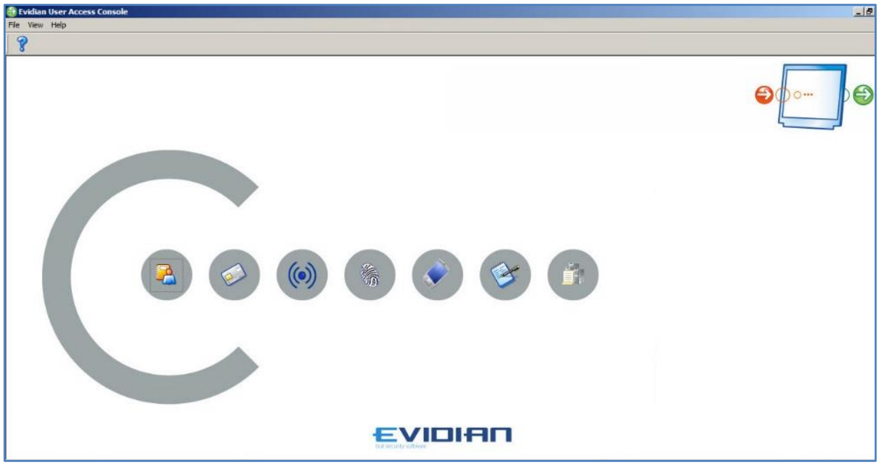
4. Under **Authentication token description file**, click **Select** and import the **TokenManagerStructure.xml** file.

5. Click **OK**
6. Restart the server**.**

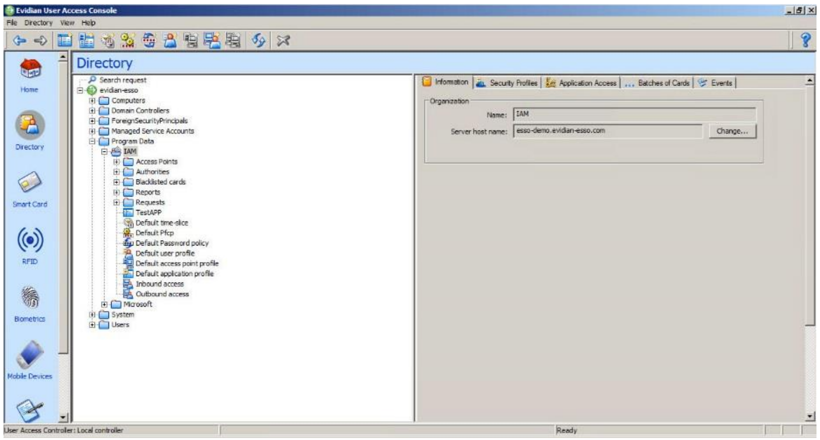
Configuring the Server

In this section, we will configure the Evidian server for CBA through the Evidian User Access Console.

1. Open the **Evidian User Access Console.**



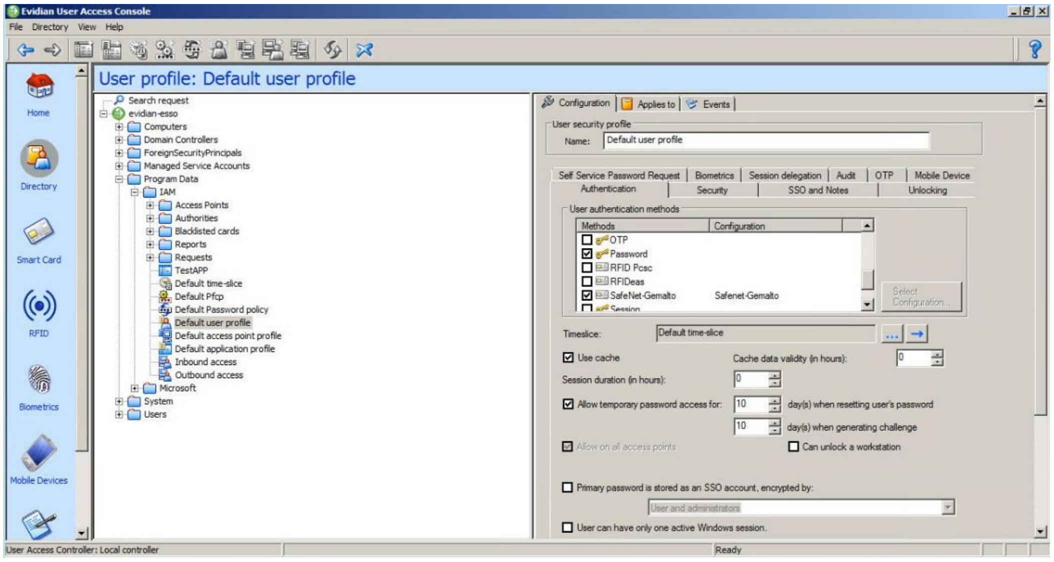
2. Select **Accounts and access rights management**. The Evidian User Access Console opens.



Name: IAM

Server host name: esso-demo.evidian-esso.com

3. In the left pane, under **Directory**, select **Program Data > IAM > Default user profile.**



User profile: Default user profile

- Search request
- evidian-esso
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Managed Service Accounts
  - Program Data
    - IAM
      - Access Points
      - Authorities
      - Blacklisted cards
      - Reports
      - Requests
      - TestAPP
      - Default time-slice
      - Default Pfcp
      - Default Password policy
      - Default user profile
      - Default access point profile
      - Default application profile
      - Inbound access
      - Outbound access
    - Microsoft
  - System
  - Users

User security profile — Name: Default user profile

User authentication methods

Methods	Configuration
□ OTP	
☑ Password	
□ RFID Pcsc	
□ RFIDeas	
☑ SafeNet-Gemalto	Safenet-Gemalto
□ Session	

Timeslice: Default time-slice

☑ Use cache — Cache data validity (in hours): 0

Session duration (in hours): 0

☑ Allow temporary password access for: 10 day(s) when resetting user's password

10 day(s) when generating challenge

☑ Allow on all access points — □ Can unlock a workstation

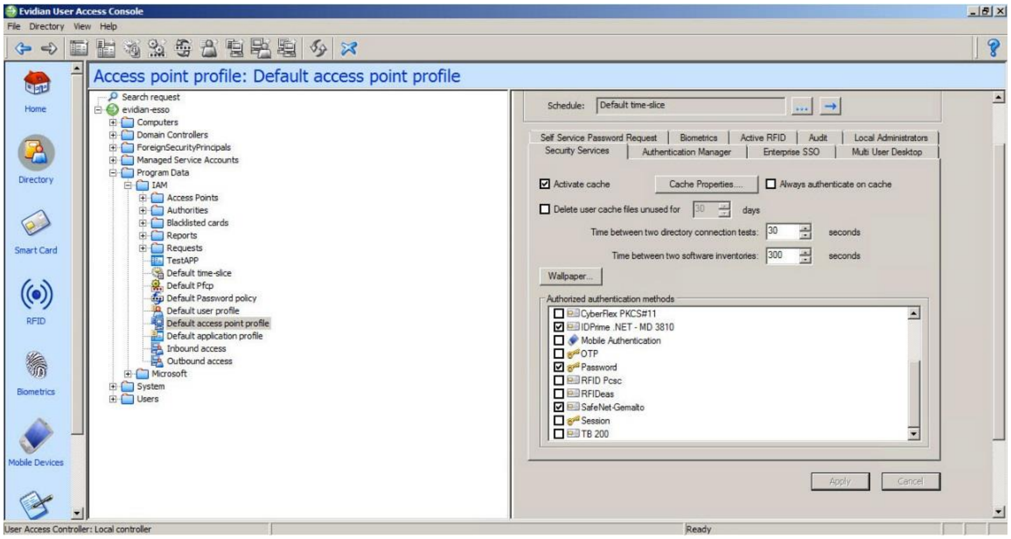
□ Primary password is stored as an SSO account, encrypted by: User and administrators

□ User can have only one active Windows session.

4. On the right pane, select the **Configuration** tab. Under the **Authentication** sub tab, select the relevant token/smart card support (**SafeNet-Gemalto** for the tokens and **IDPrime** for the Gemalto smart cards).

5. Click **Apply**.

6. On the left pane, select **Default access point profile.**



Access point profile: Default access point profile

- Search request
- evidian-esso
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Managed Service Accounts
  - Program Data
    - IAM
      - Access Points
      - Authorities
      - Blacklisted cards
      - Reports
      - Requests
      - TestAPP
      - Default time-slice
      - Default Pfcp
      - Default Password policy
      - Default user profile
      - Default access point profile
      - Default application profile
      - Inbound access
      - Outbound access
    - Microsoft
  - System
  - Users

Schedule: Default time-slice

☑ Activate cache — □ Always authenticate on cache

□ Delete user cache files unused for 30 days

Time between two directory connection tests: 30 seconds

Time between two software inventories: 300 seconds

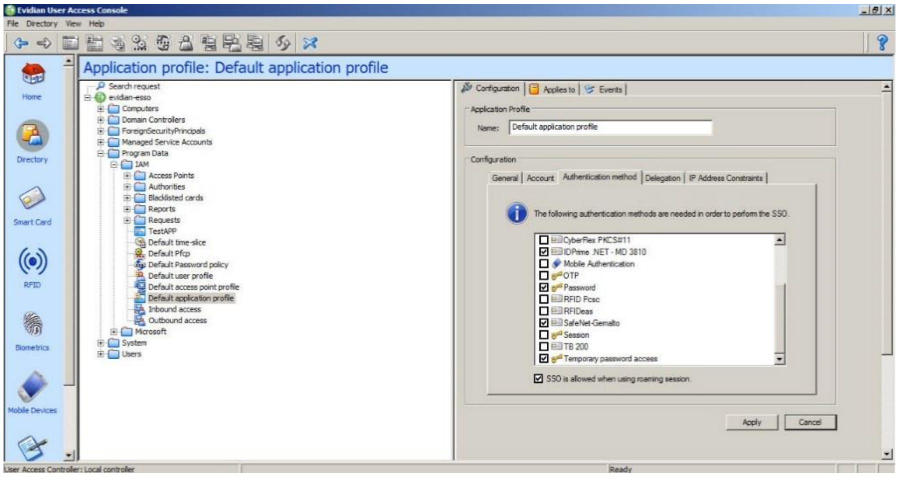
Authorized authentication methods

- □ CyberFlex PKCS#11
- ☑ IDPrime .NET - MD 3810
- □ Mobile Authentication
- □ OTP
- ☑ Password
- □ RFID Pcsc
- □ RFIDeas
- ☑ SafeNet-Gemalto
- □ Session
- □ TB 200

7. In the right pane, in the **Security Sevices** tab under **Authorized authentication methods,** select the relevant method **(SafeNet-Gemalto** for token support of **IDPrime for Gemalto** smart cards)

8. Click **Apply.**

9. On the left pane, select **Default application profile.**



Application profile: Default application profile

Application Profile

Name: Default application profile

Configuration

The following authentication methods are needed in order to perform the SSO.

- □ CyberFlex PKCS#11
- ☑ IDPrime .NET - MD 3810
- □ Mobile Authentication
- □ OTP
- ☑ Password
- □ RFID Pcsc
- □ RFIDeas
- ☑ SafeNet-Gemalto
- □ Session
- □ TB 200
- ☑ Temporary password access

☑ SSO is allowed when using roaming session.

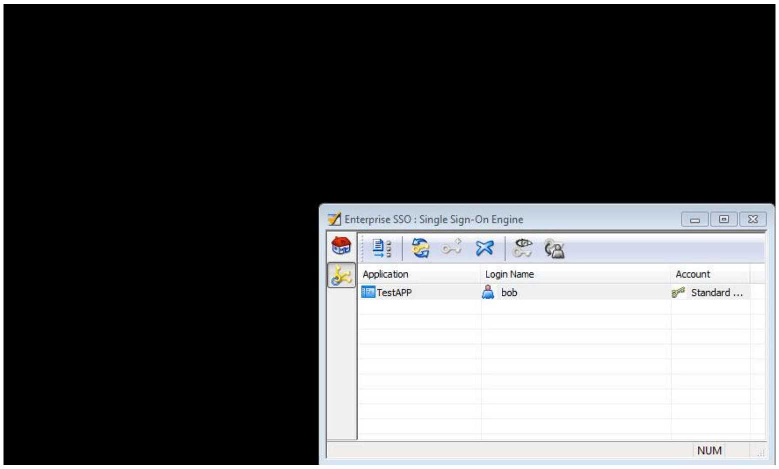
10. In the right pane, in the **Configuration** tab under **Configuration,** select the relevant method (**SafeNet-Gemalto** for token support of **IDPrime for Gemalto** smart cards)

11. Click **Apply.**

Running the Solution

In this section, we will demonstrate the authentication to Evidian ESSO 9 with Gemalto token/smart card using the SafeNet Authentication Client. In this section we will use a demo app to demonstrate the ESSO authentication with the user Bob.

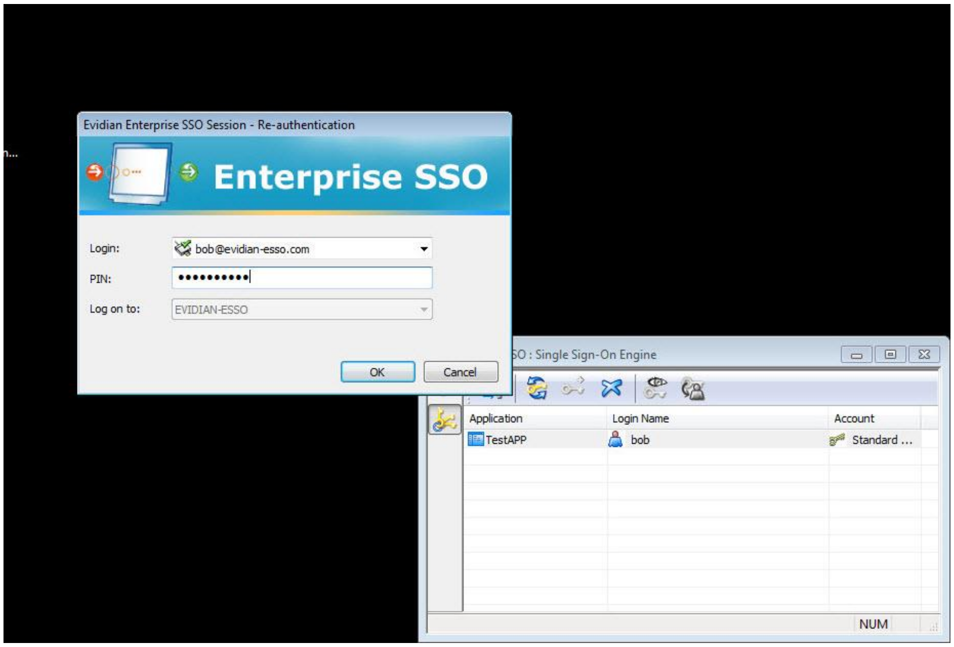
1. Login to the client and open the Evidian ESSO software.



Application	Login Name	Account
TestAPP	bob	Standard ...

2. Double click on the TestApp demo application. The ESSO authentication window opens.

3. In the **Login** field, select the smart card/token, enter the PIN code and click **OK**.


Evidian Enterprise SSO Session - Re-authentication
Enterprise SSO
OK
Cancel
SO : Single Sign-On Engine
NUM

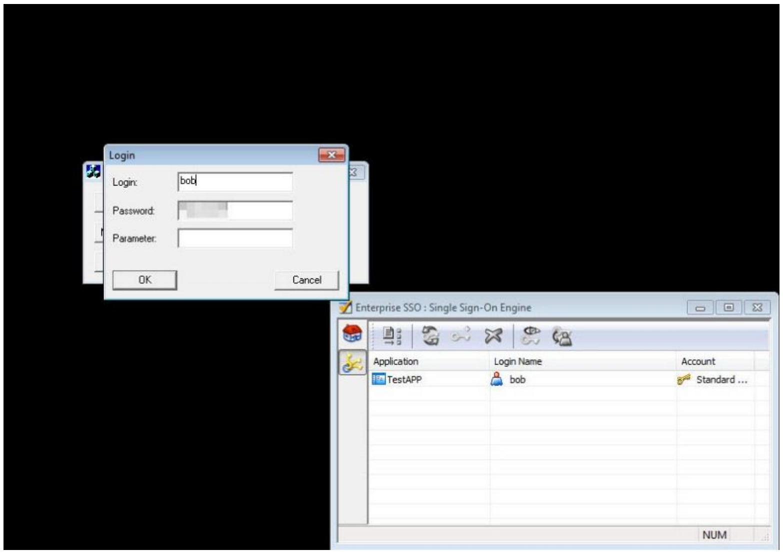
Login: bob@evidian-esso.com

PIN: ••••••••••

Log on to: EVIDIAN-ESSO

Application	Login Name	Account
TestAPP	bob	Standard ...

After successful authentication, the application is executed and the user is not required to re-authenticate.



Login: bob

Password:

Parameter:

Application	Login Name	Account
TestAPP	bob	Standard ...

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
Customer Support Portal	https://supportportal.gemalto.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.
Technical Support contact email	technical.support@gemalto.com