

# SafeNet Authentication Client Compatibility Guide

Using SAC CBA for OpenTrust 5.0.0

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.

© 2018 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.

**Release Date:** November 2018

**Product Number:** 007-013815-001 Rev B

# Contents

Applicability .....	4
Environment.....	4
Tested Tokens .....	4
Using eToken only .....	5
Using IDPrime only .....	7
Using both eToken and IDPrime.....	9
Configuring the SAC Registry.....	12
Registry on Windows 32-bit.....	12
Registry on Windows X64 (set both registries X32 and X64) .....	13
Validated Use Cases with SAC .....	14
Results .....	14
Support Contacts.....	15

# Applicability

---

The information in this document applies to:

- **SafeNet Authentication Client (SAC) - SAC 10.6**

# Environment

---

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

- **SafeNet Authentication Client (SAC 10.6)**
- **OpenTrust CMS client 5.0.0**
- **OpenTrust server**

# Tested Tokens

---

SAC supports a number of tokens and smart cards that can be used as a second authentication factor for users who authenticate to OpenTrust.

Below is the list of tokens and smart cards tested with OpenTrust.

The smart cards were tested using the Gemalto CT40 smart card reader.

## Certificate-based USB tokens

- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 GA
- SafeNet eToken 5110 CC
- SafeNet eToken 5300

## Smart Cards

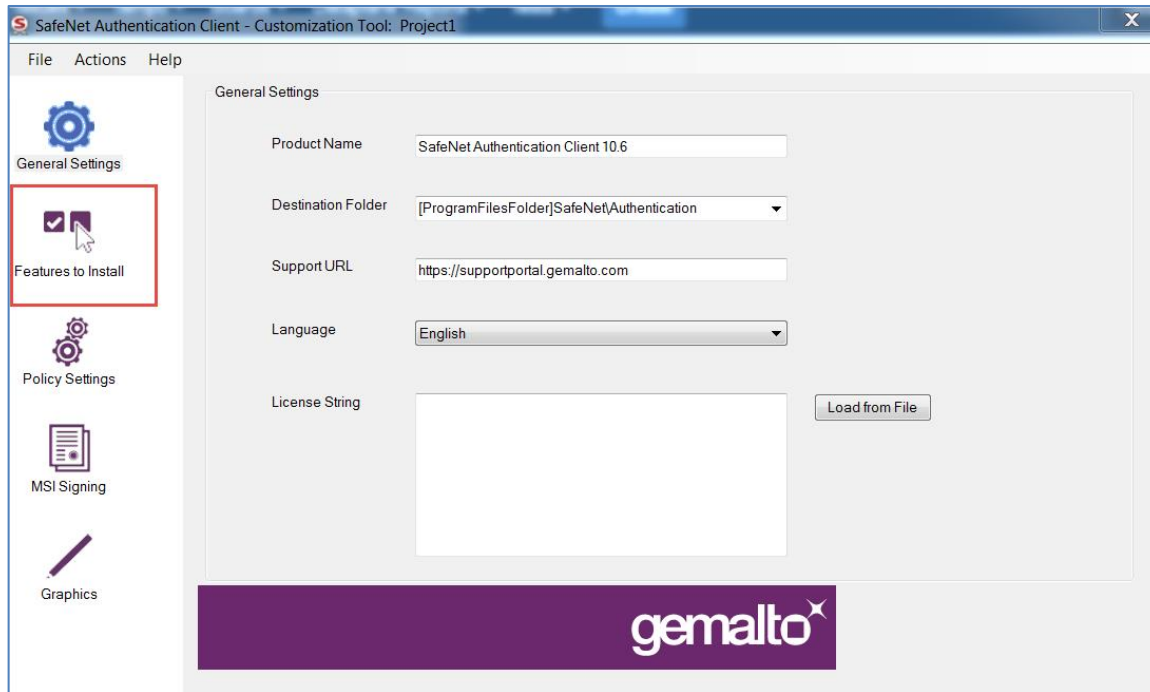
- IDprime MD 840 Rev B
- IDprime MD 830 Rev B
- IDprime MD 830
- IDprime MD 840
- IDprime MD 940

# Using eToken only

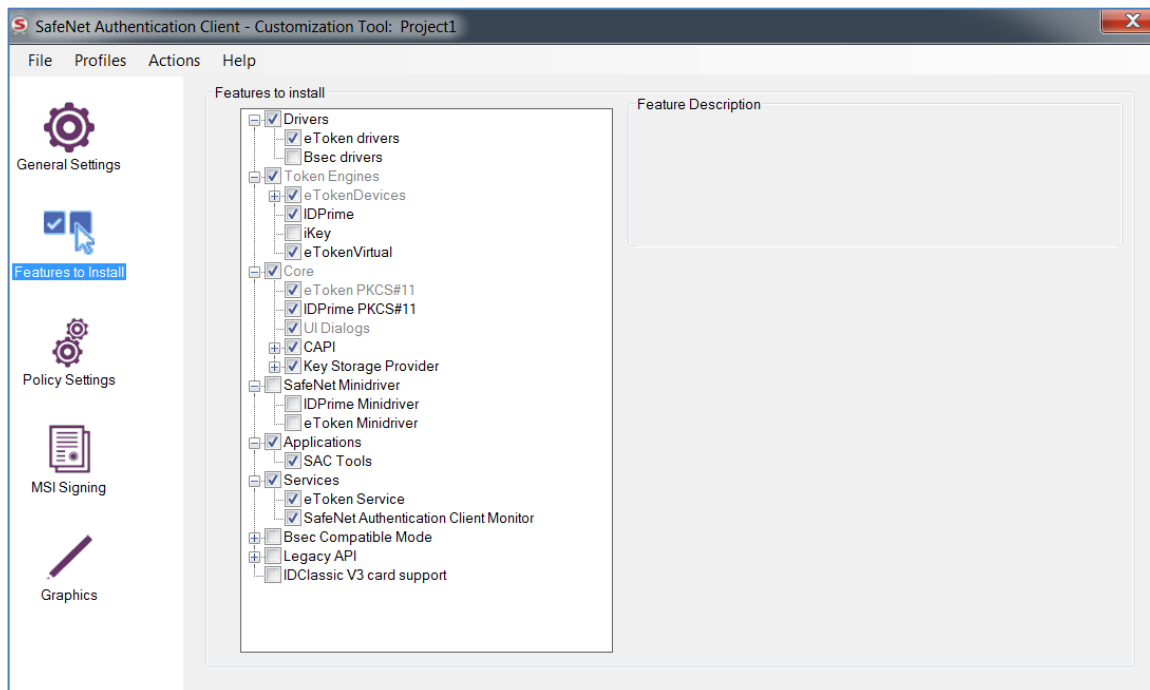
The SAC 10.6 installation package must be generated using the **SAC Customization Tool**

**To use eToken devices:**

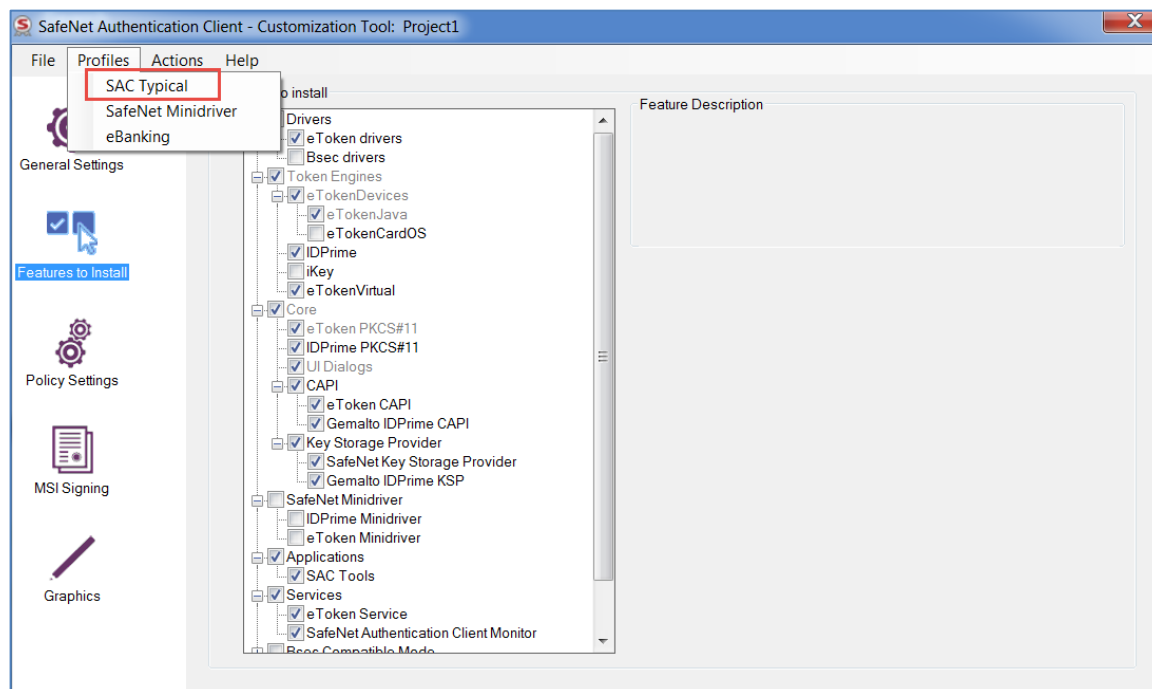
1. Open **Safenet Authentication Client – Customization Tool**.



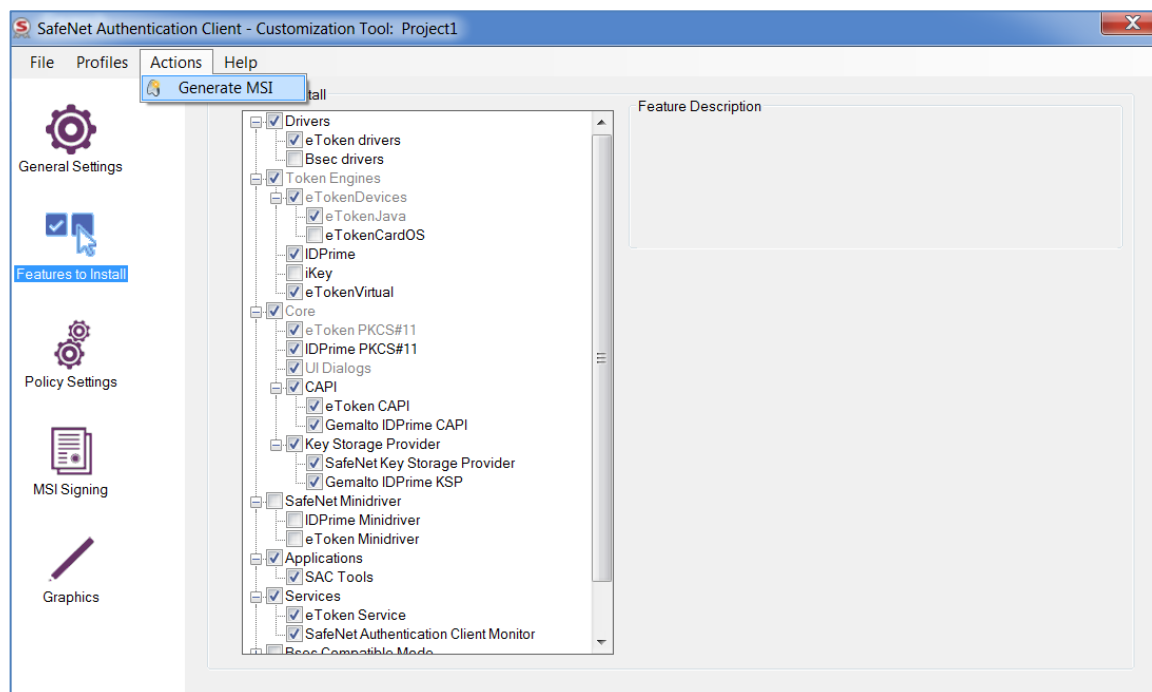
2. On the left pane, click **Features to Install**.



3. On the top menu select **Profiles -> SAC Typical**.



4. To create the installation executable, on the top menu select **Actions > Generate MSI**.

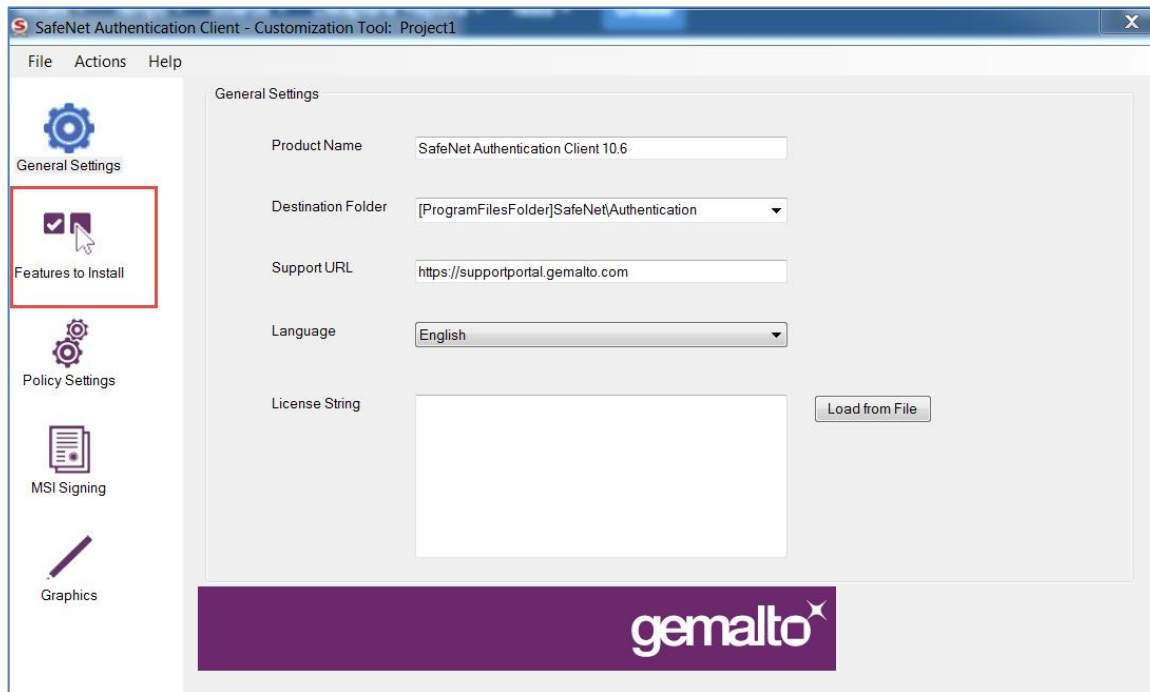


# Using IDPrime only

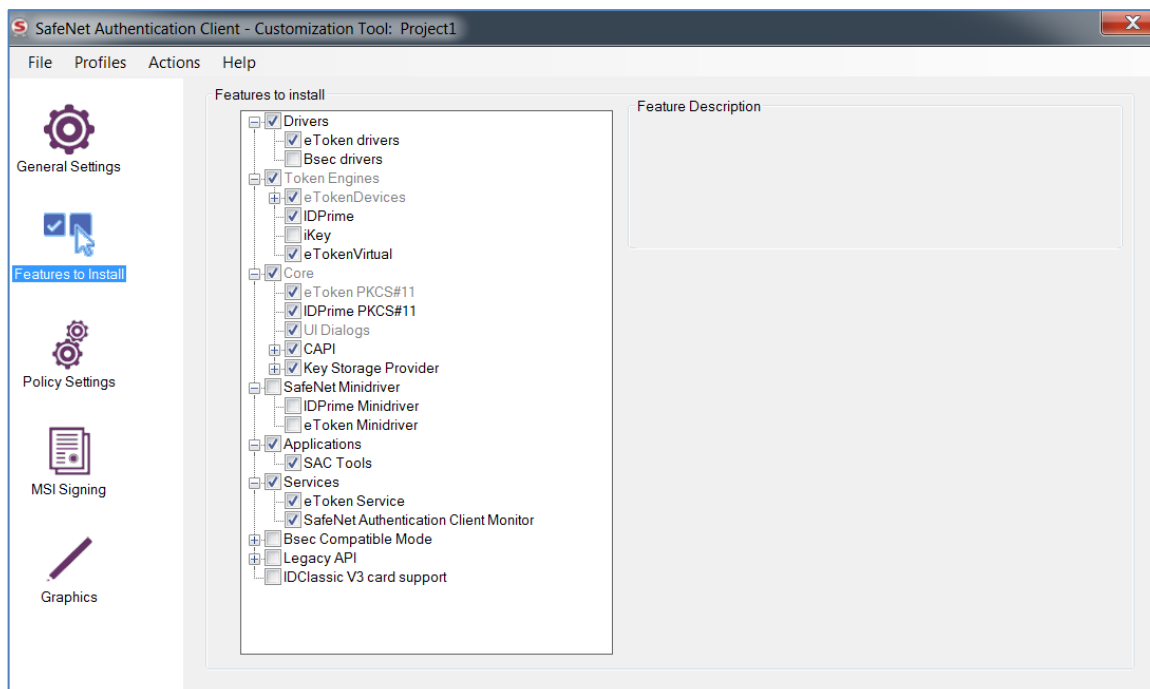
When using only IDPrime cards, the installation must be created using the **Safenet Minidriver** profile, in the **Safenet Authentication Client Customization Tool**.

To use IDPrime:

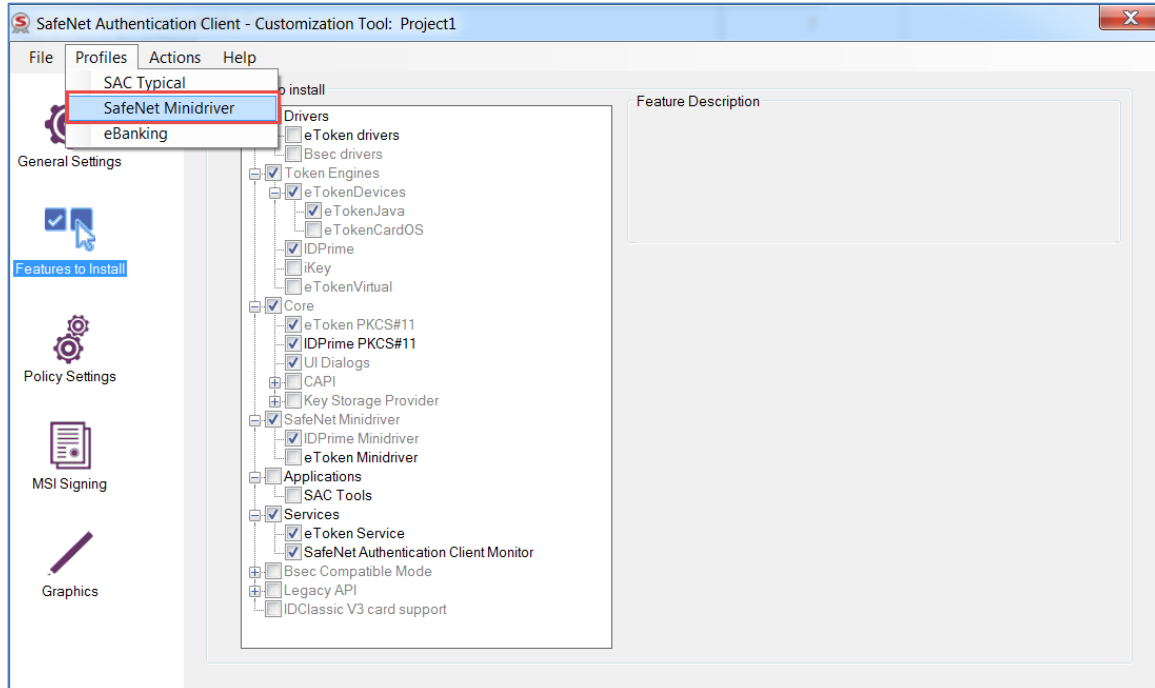
1. Open the **Safenet Authentication Client – Customization Tool**.



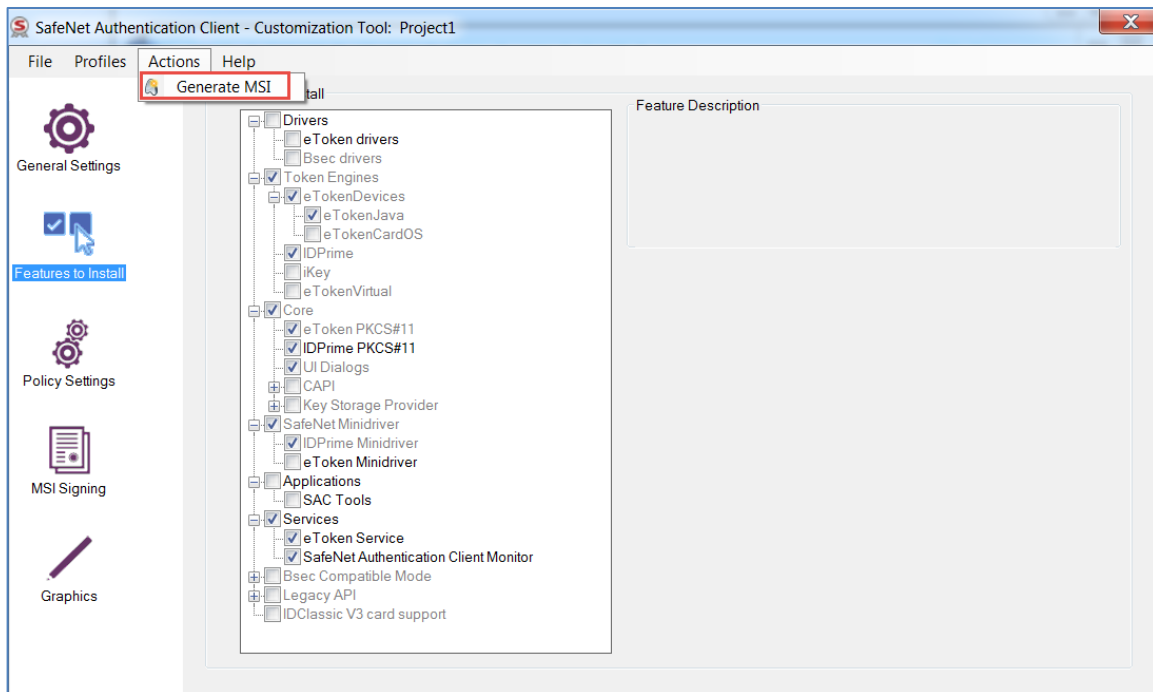
2. On the left pane, select **Features to Install**.



3. On the top menu select **Profiles > SafeNet Minidriver**.



4. To create the installation executable, on the top menu select **Actions > Generate MSI**.



**NOTE:** To display the SAC user interface, select **Applications > SAC Tools**.

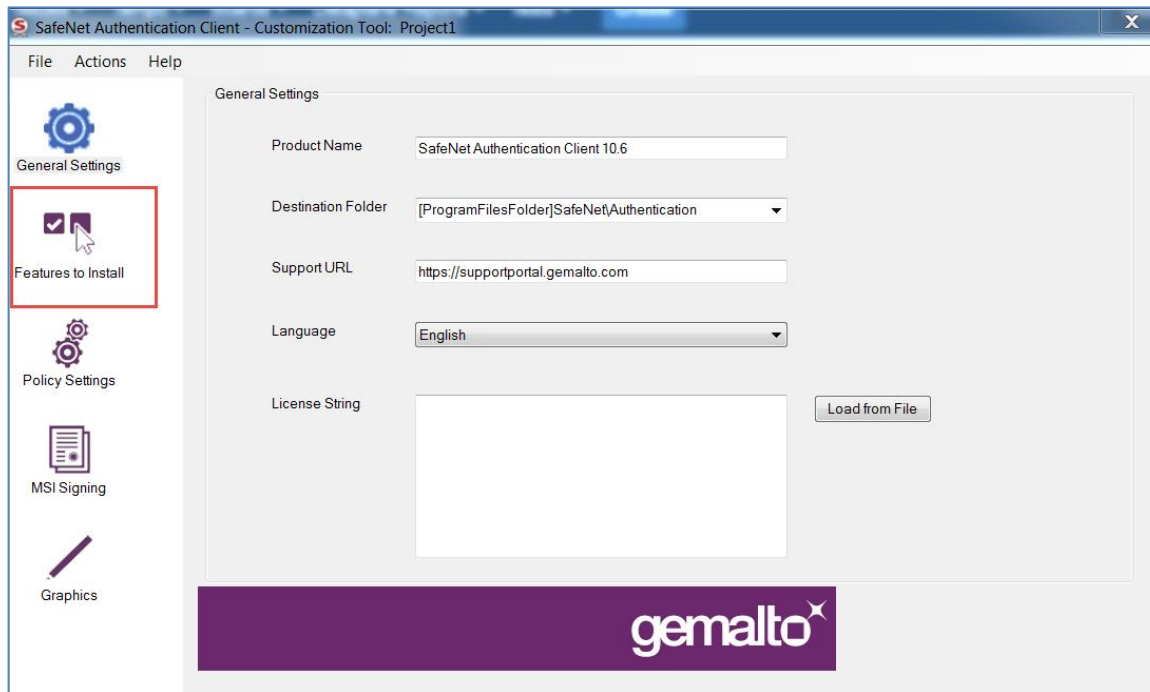


# Using both eToken and IDPrime

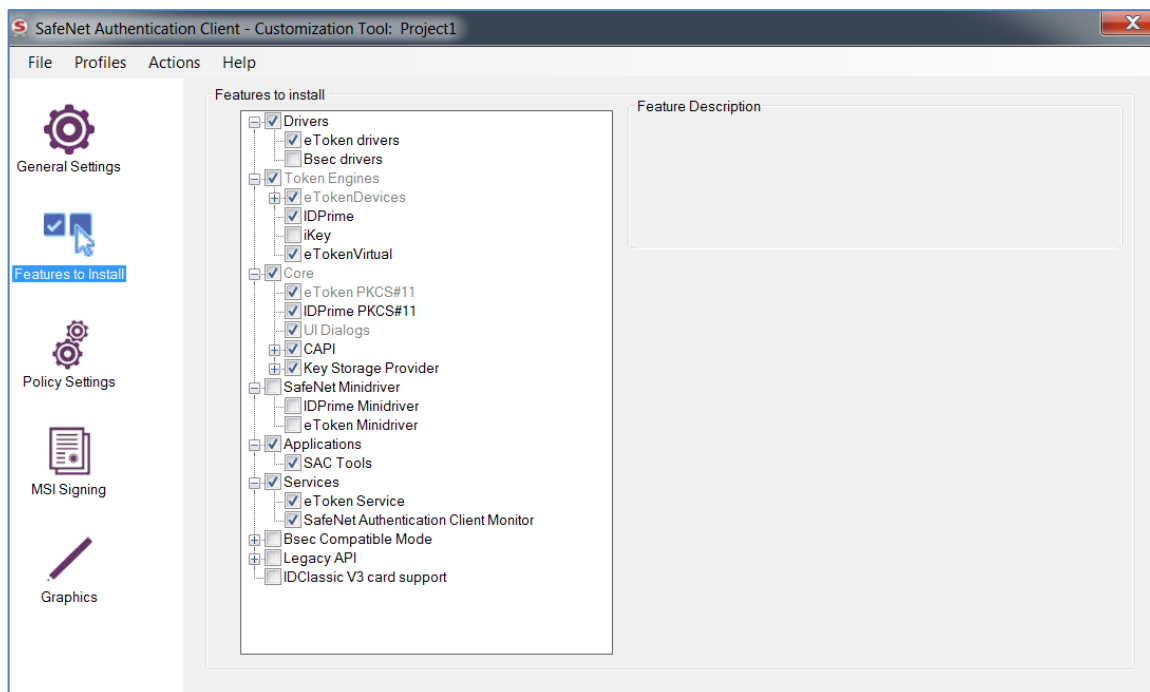
When using both IDPrime cards and eToken devices, the installation must be created using the **Safenet Minidriver** profile, in the **Safenet Authentication Client Customization Tool**.

To use both eToken and IDPrime:

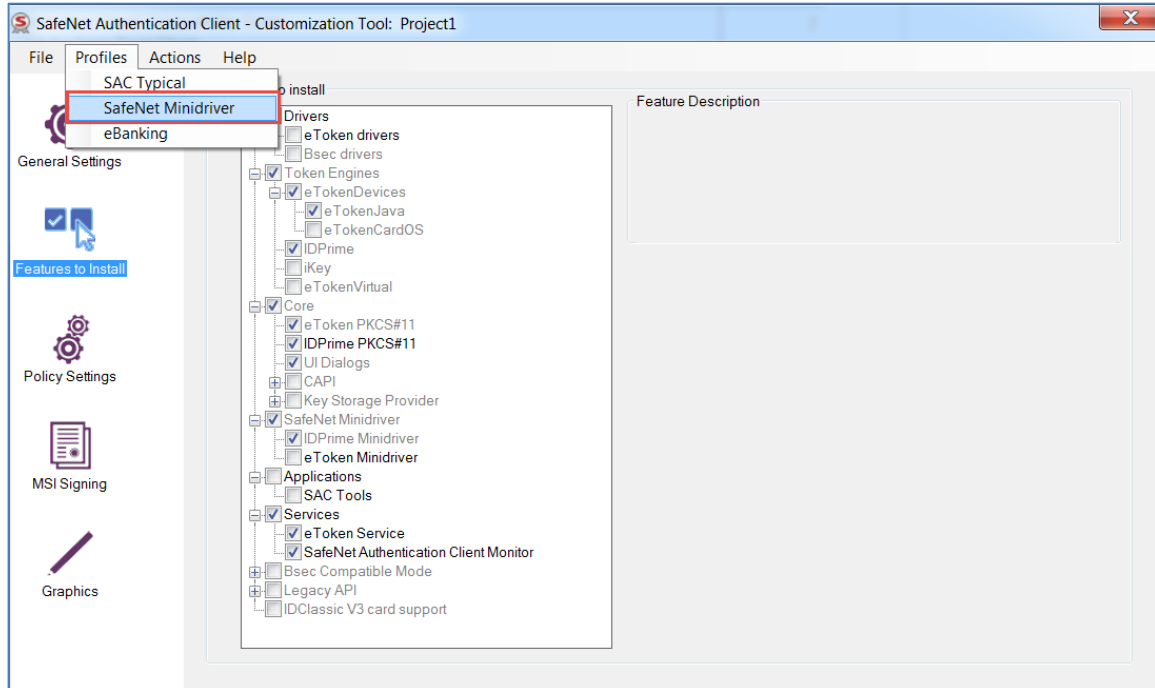
1. Open the **Safenet Authentication Client – Customization Tool**.



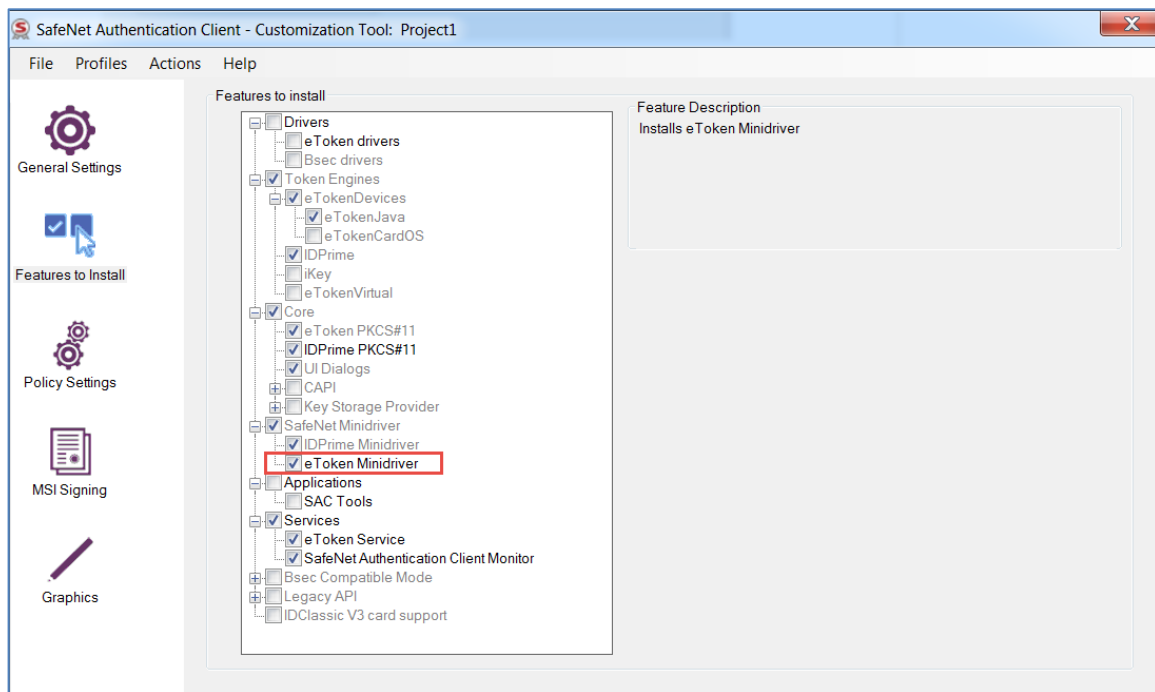
2. On the left pane, select **Features to Install**.



3. On the top menu select **Profiles > SafeNet Minidriver**.



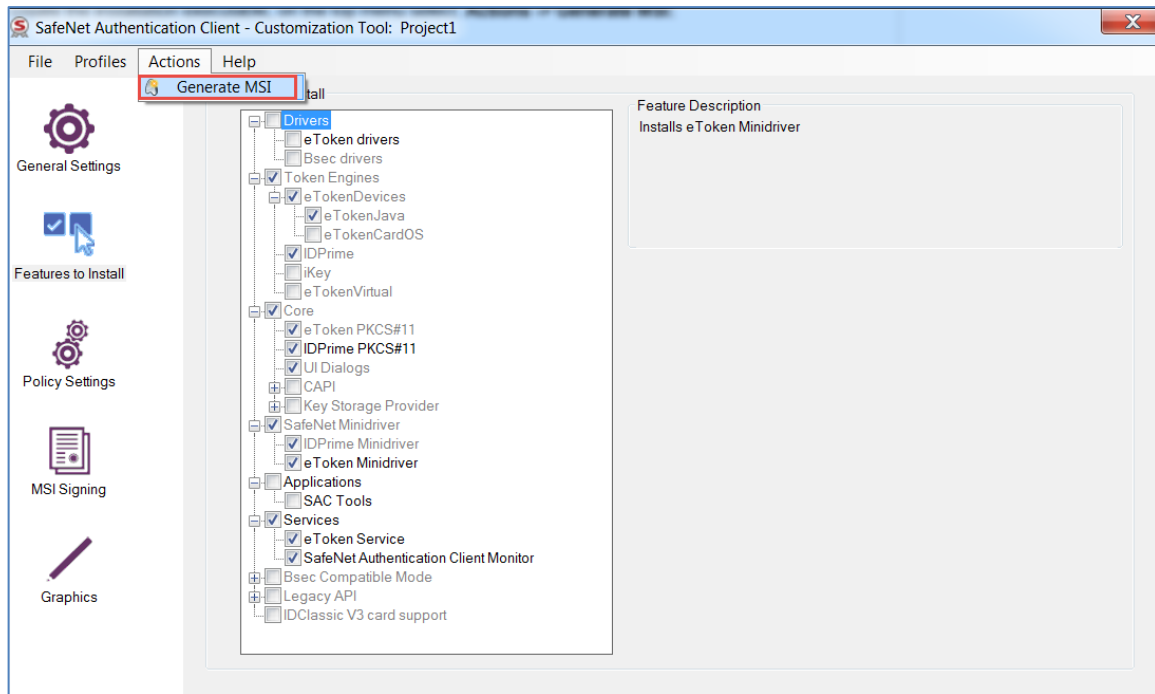
4. To support eToken, select **SafeNet Minidriver > eToken Minidriver**.





**NOTE:** To display the SAC user interface, select **Applications > SAC Tools**.

5. To create the installation executable, on the top menu select **Actions -> Generate MSI**.



# Configuring the SAC Registry

Following to the installation of the SAC MSI, the ApiMode configuration must be added to the SAC Registry.

## Registry on Windows 32-bit

Create the General key under the following root:

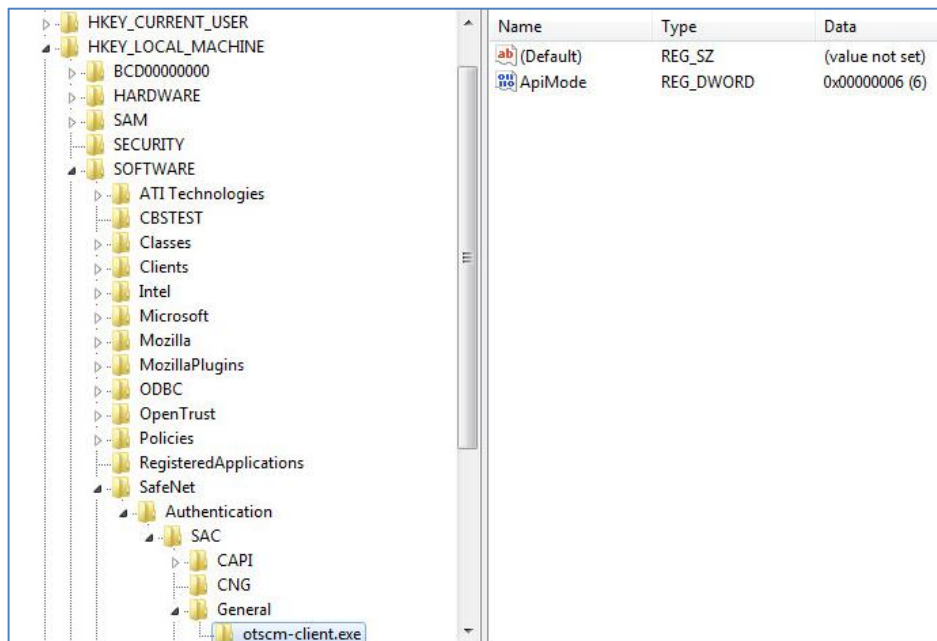
**HKEY\_LOCAL\_MACHINE\SOFTWARE\SafeNet\Authentication\SAC**

Create the otscm-client.exe key under the following root:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\SafeNet\Authentication\SAC\General**

Create the entry "ApiMode" of type "REG\_DWORD", with the value 6:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\SafeNet\Authentication\SAC\General\otscm-client.exe**



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

## Registry on Windows X64 (set both registries X32 and X64)

Create the General Key under the following root:

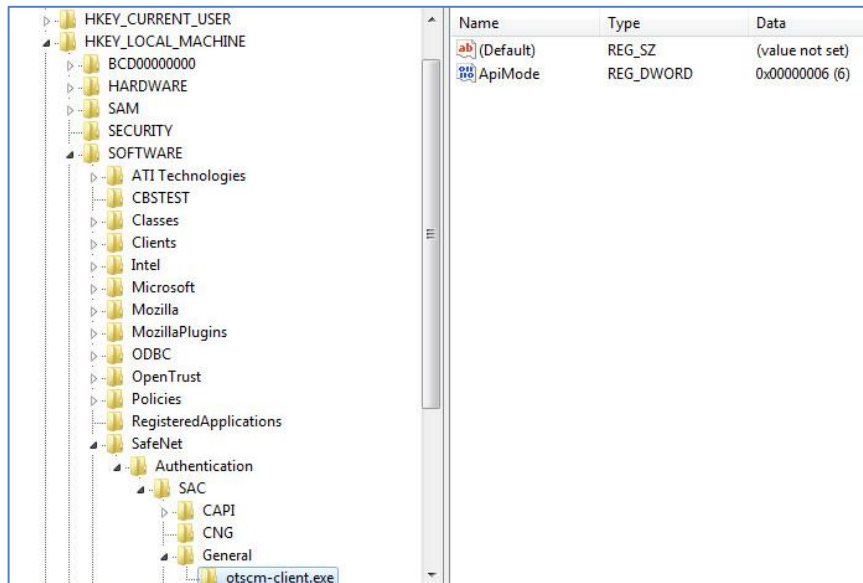
**HKEY\_LOCAL\_MACHINE\SOFTWARE\SafeNet\Authentication\SAC**

Create the otscm-client.exe key under the following root:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\SafeNet\Authentication\SAC\General**

Create the entry "ApiMode" of type "REG\_DWORD", with the value 6:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\SafeNet\Authentication\SAC\General\otscm-client.exe**



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

Create the General Key under the following root:

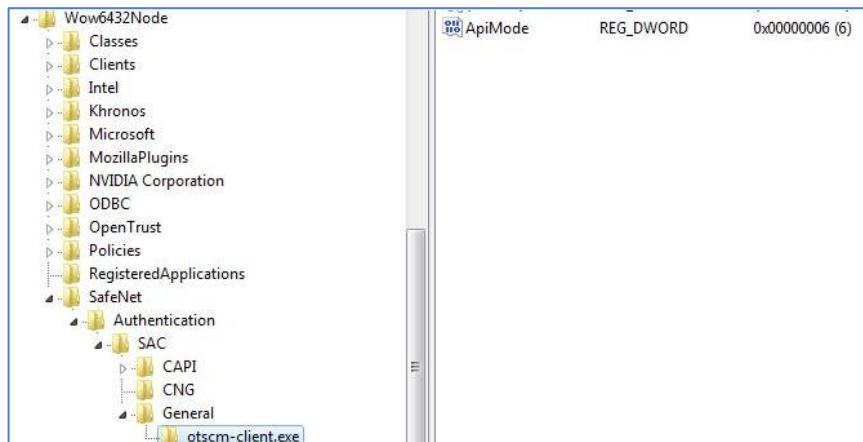
**HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\SafeNet\Authentication\SAC**

Create the otscm-client.exe key under the following root:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\SafeNet\Authentication\SAC\General**

Create the entry "ApiMode" of type "REG\_DWORD", with the value of 6:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\SafeNet\Authentication\SAC\General\otscm-client.exe**



## Validated Use Cases with SAC

---

- Self-enrollment with card initialization
- Self-unlock
- User PIN change
- SSL authentication
- Authoritative offline unblock - SAC Tools Generate the Challenge , Paste on Server Side and Get the Response > Paste in SAC Tools and Perform Unblock (Not Supported on MD 840 / 940 /5110 CC)

Two tokens connected

- Operator - eToken (5110 GA) connected always
- Target User - smart card/Token Changed Smart Card Connected with CT40 reader
- Badge office enrollment full test
- Badge Unlock option

## Results

---

The following devices passed the above tests using SAC on win7x64 / x32:

- IDPrime 840
- IDPrime 840 B
- IDPrime 830 B
- IDPrime 830
- IDPrime 940
- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 GA
- SafeNet eToken 5110 CC
- SafeNet eToken 5300



**NOTE:** When minidriver support is not available in OpenTrust the following functionalities are not supported:

- Challenge/response admin authentication
  - OpenTrust's Self-Care Web Portal
-

## 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	<a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a> 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.	