SafeNet Authentication Client
Compatibility Guide

Using SAC CBA for OpenTrust 5.0.0
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicability</td>
<td>4</td>
</tr>
<tr>
<td>Environment</td>
<td>4</td>
</tr>
<tr>
<td>Tested Tokens</td>
<td>4</td>
</tr>
<tr>
<td>Using eToken only</td>
<td>5</td>
</tr>
<tr>
<td>Using IDPrime only</td>
<td>7</td>
</tr>
<tr>
<td>Using both eToken and IDPrime</td>
<td>9</td>
</tr>
<tr>
<td>Configuring the SAC Registry</td>
<td>12</td>
</tr>
<tr>
<td>Registry on Windows 32-bit</td>
<td>12</td>
</tr>
<tr>
<td>Registry on Windows X64 (set both registries X32 and X64)</td>
<td>13</td>
</tr>
<tr>
<td>Validated Use Cases with SAC</td>
<td>14</td>
</tr>
<tr>
<td>Results</td>
<td>14</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>15</td>
</tr>
</tbody>
</table>
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\otsxml-client.exe
```

-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\otsxml-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.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</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>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</td>
</tr>
<tr>
<td></td>
<td>manage incidents, get the latest software upgrades, and access the Gemalto Knowledge</td>
</tr>
<tr>
<td></td>
<td>Base.</td>
</tr>
</tbody>
</table>