SafeNet Authentication Client (Windows)

Version 10.7 (GA)

Administrator Guide

gemalto
security to be free

All information herein is either public information or is the property of and owned solely by Gemalto 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 publicly accessible 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.

G**emalto 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 e functioning could result in damage to persons or property, denial of service or loss of privacy.

Product Version: 10.7 (GA)

Document Number: 007-013560-005, Rev. C

Release Date: April 2019

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

Additional Documentation

The following publications are available:

- 007-013561-005 SafeNet Authentication Client 10.7 Windows (GA) User Guide Rev C
- 007-013559-007 SafeNet Authentication Client 10.7 Windows (GA) Release Notes (RN) Rev C

Table of Contents

Introduction

SafeNet Authentication Client (SAC) is a middleware client that manages Gemalto's extensive SafeNet portfolio of certificate-based authenticators, including eToken, IDPrime smart cards, iKey smart card, USB and software-based devices.

With full backward compatibility and incorporating features from previous middleware versions, SafeNet Authentication Client ensures complete support for all currently deployed eToken and iKey devices, as well as IDPrime MD and .NET smart cards.

Overview

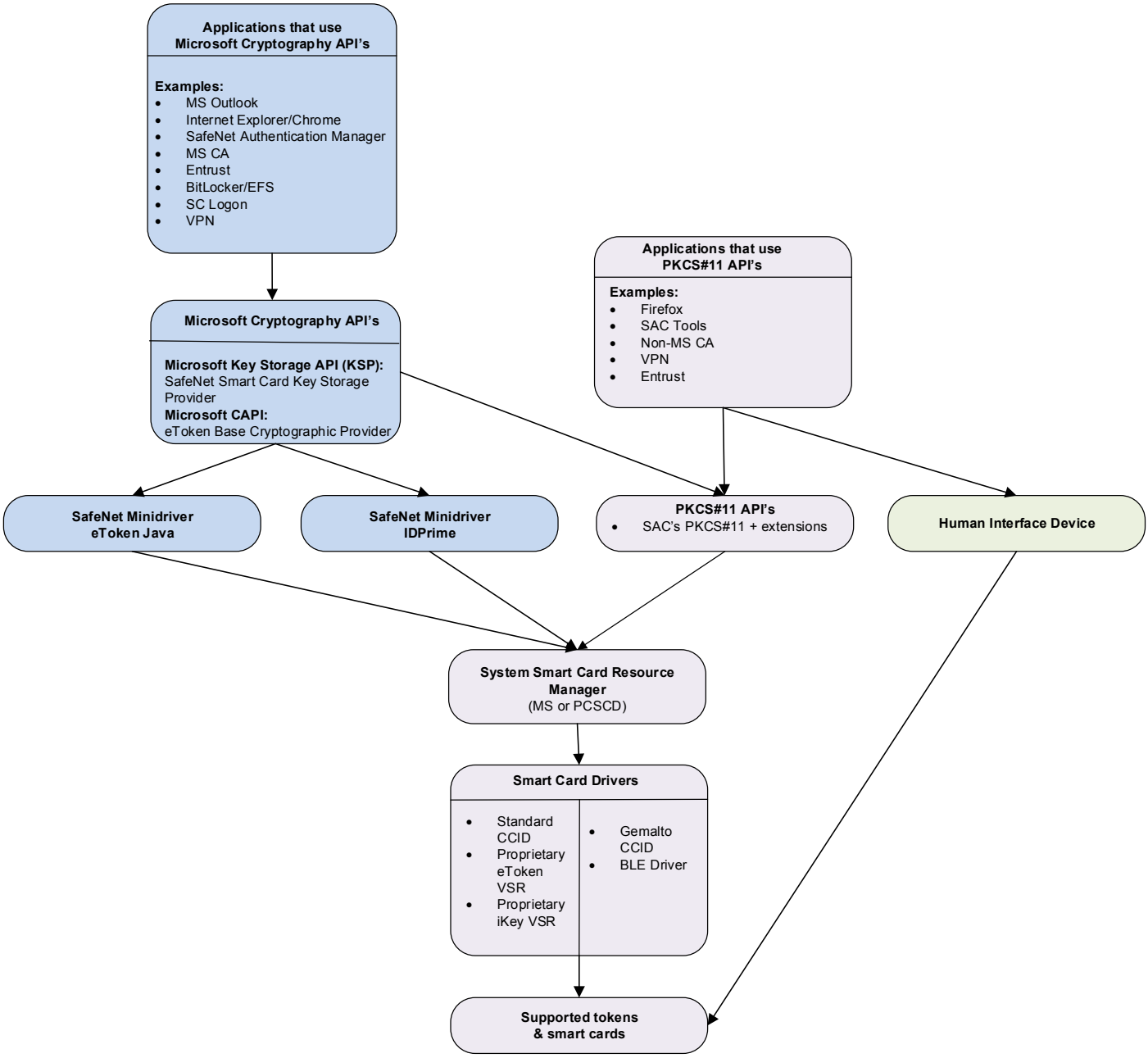
SafeNet Authentication Client is Public Key Infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities. It utilizes a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an internet transaction.

SafeNet Authentication Client enables the implementation of strong two-factor authentication using standard certificates as well as encryption and digital signing of data. 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 from within hardware or software.

SafeNet Authentication Client can be deployed and updated using any standard software distribution system, such as Windows Group Policy Objects (GPO) or Microsoft System Management Server (SMS).

The SafeNet Authentication Client Tools application and the SafeNet Authentication Client tray icon application are installed with SafeNet Authentication Client, providing easy-to-use configuration tools for users and administrators.

SafeNet Authentication Client API Flow



License Activation

SafeNet Authentication Client is installed by default as non-licensed.

NOTE:
SafeNet Minidriver is part of the SafeNet Authentication Client Customization Tool minidriver profile. It is also available as a stand-alone solution.
See "SafeNet Minidriver Profile" on page 23

To activate the license perform the following steps:

1. Obtain a valid SAC License Key from SafeNet Customer Service.
2. Activate the license using one of the following procedures:
   - Manual Activation

   See the *Licensing* chapter in the *SafeNet Authentication Client 10.4 (GA) User Guide*.

   - Command Line Activation

   See "PROP_LICENSE_FILE Property" on page 55 (Command Line column) and *Installing the MSI file via the Command Line* on page 51.

   Group Policy Object Editor

   See "License Settings" on page 81 (ADM File Setting column) and *Setting SafeNet Authentication Client Properties* on page 68.

   - SafeNet Authentication Client Customization Tool

   You can specify the license key when creating a customized MSI Installation file.

   See *Using the SafeNet Authentication Client Customization Tool*, step 3, on page 31.

NOTE:
SafeNet Authentication Client retrieves the license file (SACLicense.lic) automatically, if the license file is located in the following default path Windows: **\ProgramData\SafeNet\SAC**

IDPrime MD Common Criteria Profile

The IDPrime MD Applet 4.0 is Common Criteria certified on Common Criteria based smartcards and token. See the *SafeNet Authentication Client Release Notes* for a list of supported smartcards and tokens. These devices can have certain parameters customized in the factory with different values to the default profile.

NOTE:
The IDPrime MD 840/ 3840 cards or eToken 5110 CC do not support modifying the retry counter on the Admin Key.
The recommended workaround is to set the profiles with a PUK instead of the Admin Key.
To ensure maximum security, when using friendly mode, set the password with at least 16 random printable characters.

The following parameters can be customized:

- Number and type of key containers
- Support of RSA 4,096-bit key containers.
- PINs (#1, #3 and #4 only)
- Try Limit
- Unblock PIN (PIN#1 only)
- PIN validity period
- Secure messaging in contactless mode

Number and Type of Key Containers

NOTE:
The following are the default settings. For other options consult your Gemalto representative.

By default, the IDPrime MD Applet 4.0 is pre-personalized with:

- 2 X 2,048-bit CC Sign Only RSA Keys
- 2 X 1,024-bit Standard Sign and Decrypt RSA Keys
- 8 X 2,048-bit Standard Sign and Decrypt RSA Keys
- 2 X 256-bit Standard Sign and Decrypt EC Keys

By default, the IDPrime Applet 4.4.2 is pre-personalized with:

- 2 X 2048-bit CC Sign Only RSA Keys
- 2 X 4096-bit CC Sign Only RSA Keys
- 2 X 256-bit CC Sign Only ELC Keys

NOTE:
The Key Generation method for CC key containers is either OBKG or Key import.

API Adjustments

The table below provides a high-level description of the adjustments that can be made to the Standard and Extended PKCS#11 API to work with IDPrime MD CC devices. For more detailed information, see the code samples.

Standard PKCS#11 API	Extended PKCS#11 API
The `C_InitToken` function must receive the current Security Officer (SO) Password	The `C_InitToken` function must receive the current Security Officer (SO) Password
When the `C_InitToken` function is called, you can enable linked mode on the IDPrime MD CC device by using the following registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SafeNet\Authentication\SAC\Init - LinkMode (DWORD)` The registry key must be set to 1 and the device must be in the factory initialized state (Admin key = 48 zeros, PUK = 6 zeros) To revert a device back to unlinked mode after it was initialized in linked mode, use the PKCS#11 Extended API, or by using SAC Tools initialization process.	To initialize the IDPrime MD CC device, the `ETCKA_CC` attribute must be set to `CK_TRUE`. To initialize a device in linked mode, set the `ETCKA_IDP_CC_LINK` attribute to `1`. To pass the current Digital Signature PUK value, use the `ETCKA_IDP_CURRENT_PUK` attribute. To revert a device back to unlinked mode after it was initialized in linked mode, set the `ETCKA_IDP_CC_LINK` attribute to `0` and use the `ETCKA_PUK` attribute to set the new Digital Signature PUK value.

If a device is not configured to use linked mode, the `C_InitToken` function ignores the Digital Signature PUK and Digital Signature PIN.	If a device is not configured to use linked mode, use the `ETCKA_PUK` attribute to set the new Digital Signature PUK value.
After the device has been initialized in linked mode, the `C_InitPIN` function initializes the Digital Signature PIN and the User PIN. Both PIN's are set to the same value. The `C_SetPIN` function used with the `CKU_SO` flag changes both the Administrator PIN and Digital Signature PUK to a new value. See the SafeNet Authentication Client User Guide for details on Friendly Admin Password. The C_SetPIN function used with the CKU_USER flag changes both the User PIN and Digital Signature PIN to a new value.	If the device is initialized to use linked mode, the `C_InitPIN` function and `C_SetPIN` function behaves the same as described in the Standard PKCS#11 section.

Differences between PIN Policy SSO, Session PIN, PIN Caching and Single Logon

The table below describes the PIN caching options available on IDPrime MD and .Net devices.

Feature	Description	Configuration Level
PIN Policy SSO (Only on IDPrime MD 830B and .NET devices) **Note:** -PIN Policy SSO is available for legacy purposes and is limited to customers already using this feature. It is recommended that you use the SAC Single Logon feature instead.	• Works only via the SafeNet Minidriver as a standalone installation • A cold reset or disconnecting the card will require the user PIN to be re-entered. • The PIN is entered once and thereafter the card behaves as if it's in 'No PIN' mode.	PIN Policy is configured at card level. It is configurable by factory settings or by using the Minidriver Manager.
Session PIN	• Session PIN is a mechanism defined by Microsoft Windows Smart Card Minidriver Specification (here) • It is managed automatically by Microsoft Base CSP and CNG	IDPrime MD and .Net cards are compliant with Session PIN via the SafeNet Minidriver For IDPrime MD cards, Session PIN is supported only for User PIN. For .NET cards, Session PIN is supported for all PIN Roles.
PIN Caching	• PIN Caching is a Minidriver specific Microsoft feature (here) and is applicable only for Minidriver use cases (Microsoft Base CSP and CNG)	Pin Caching Mode is a PIN property configurable through Minidriver Manager or via SAC Tools. There are 4 modes that can be applied (See the PIN Cache Mode table below) PIN Cache Normal is the default configuration for IDPrime MD devices.

Single Logon **Note:** As of SAC 10.6, the Single Logon feature is also supported for SafeNet Minidriver (10.2 and above) users when installed with SAC Service via the SAC Customization Tool (SafeNet Minidriver profile). For more information see the chapter: *Customization* on page 21.	• The Single Logon feature is a software based solution driven by SAC and is not connected to PIN Policy SSO or to PIN Caching. • Single Logon can be configured per process both SafeNet CSP/KSP & PKCS#11. For more details, see the Single Logon property under *General Settings* on page 72 • When Single Sign On (on the card) is present, the behavior is overridden by the Single Logon (configured in software).	Single Logon is configurable via SAC Tools, SafeNet Authentication Client Customization Tool or via GPO.

PIN Caching Modes

PIN Caching Modes are available on IDPrime MD and .Net devices.

Cache Mode	Description
PinCacheNormal (Default)	The PIN is cached by the Base CSP per process per logon ID. The entire PIN cache structure is encrypted in memory to keep it protected.
PinCacheTimed	The PIN is invalidated after an indicated period of time (value is given in seconds). This was implemented by recording the time stamp when the PIN is added to the cache and then verifying this time stamp versus the time when the PIN is accessed. This means that the PIN potentially lives in the cache longer than the specified time stamp, but is not used after it has expired. The PIN is encrypted in memory to keep it protected.
PinCacheNone	When the PIN cannot be cached, Base CSP never adds the PIN to the cache. When the Base CSP/KSP is called with `CryptSetProvParam` to set a PIN, the PIN is submitted to the card for verification but not cached. This means that any subsequent operations must occur before the Base CSP transaction time-out expires.
PinCacheAlwaysPrompt	Unlike PinCacheNone, when this cache mode is set, the Base CSP transaction time-out is not applicable. The PIN is collected from the user and then submitted to the card for verification before each call that requires authentication. Calls to `CryptSetProvParam` and `NcryptSetProperty` for setting the PIN return `ERROR_SUCCESS` without verifying and caching the PIN. This implies that calls from applications that use silent contexts will fail if the call requires authentication.

NOTE:

Microsoft: Windows logon may not work properly if a PIN is not cached. This behavior is by design. Therefore, careful consideration should be given when setting a PIN cache mode to any value other than `PinCacheNormal`.

Security Recommendations

Ensuring a Secured SAC Environment

This section provides short guidelines on how to maintain a safe PC computer environment. The information is based on the security recommendations defined by Microsoft.

Windows Malware Prevention

Up-to-date security software is the best way to help protect your computer from a malware attack. Microsoft provides security software that is regularly updated to protect against the latest threats. More details are to be found here:

https://www.microsoft.com/en-us/security/portal/mmWinodpc/shared/prevention.aspx

Enable Automatic Windows Updates

Automatic Windows updates ensure that you are running software with the latest security enhancements. When new updates are available, Windows sends you a notification. Accept the updates with a click and they download and install automatically.

Anti-Virus Software

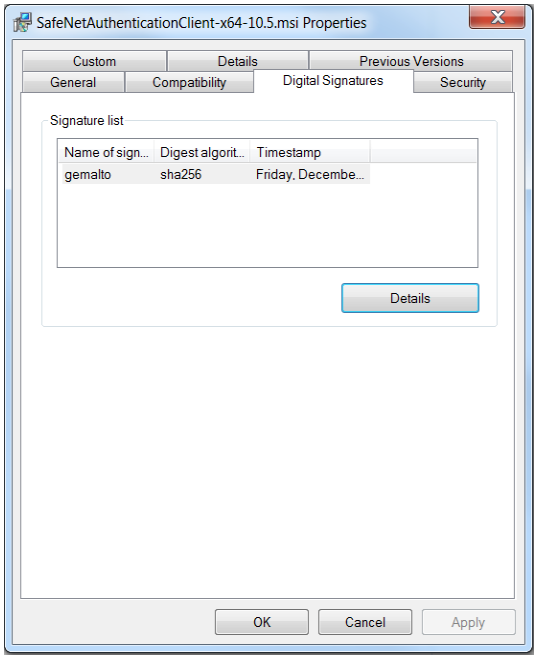
Make sure to choose an effective Anti-Virus/Malware software to protect your client machines. It is essential to keep the Anti-Virus/Malware software updated.

Install the SAC Package Only from the Official Gemalto Site

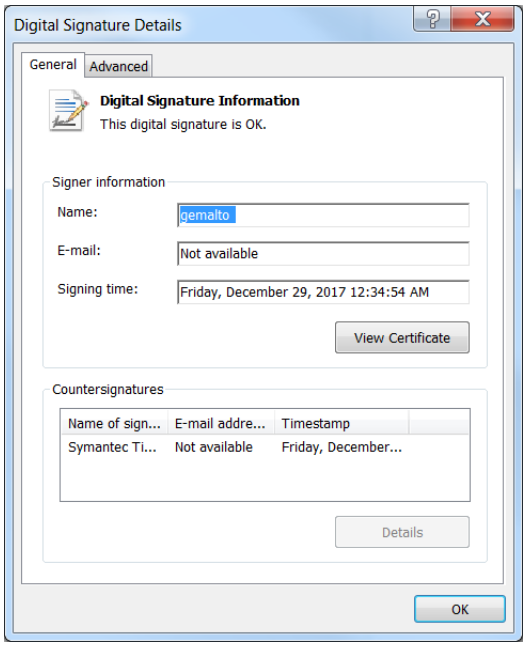
https://serviceportal.safenet-inc.com/eservice_ENU/start.swe?SWECmd=Start&SWEHo=serviceportal.safenet-inc.com

To ensure that the Gemalto certificate is being utilized:

1. After downloading the package (MSI/EXE), right click on the file and select **Properties**
2. In the **Properties** window, click the **Digital Signatures** tab and verify that the Gemalto signature is listed.



3. Select the Gemalto signature and click **Details**.
4. In the **Digital Signature Details** window, **General** tab, verify that the text **The Digital Signature is OK** is displayed.



Malware Awareness

Malware authors use several common tricks to install their malicious software on your PC. Understanding the most common ways they do this can help you stay protected.

- **Email** – Malware often arrives on your PC in an email attachment. You should never open an attachment from someone you don't know or if an email looks suspicious. Instant messages and requests for file transfers can also spread malware.
- **Websites** – Never open links to webpages that you don't recognize or that are sent from people you don't know. Malicious websites can install malware on your PC when you visit them.
- **Use caution** – If you view a website that doesn't look quite right, or unexpected things happen when you visit, close your browser, download the latest updates for your security software and run a quick scan on your PC.
- **Pirated software** – Malware is often bundled together with pirated software. When you install the pirated software you may also install malware.
- **Social engineering** – Malware authors often try and trick you into doing what they want. This can be clicking or opening a file because it looks legitimate, paying money to unlock your PC or visiting a malicious webpage. These deceptive appeals are known as social engineering.
- **Passwords** – Attackers may try to guess your Windows account or other passwords. This is why you should always use a password that can't be guessed easily. A strong password has at least eight characters and includes letters, numbers, and symbols.
- **Removable drives** – Some types of malware, such as worms, can spread by copying themselves to any USB flash drives or other removable drives that are connected to your computer. Always be careful when sharing removable drives, and make sure you scan them.

Limit User Privileges

Many malware threats need full access to your computer to run properly. Windows 10, Windows 8.1, Windows 7, and Windows Vista use User Account Control (UAC) to limit what a program can do without your permission.

This means you will be notified if any software or application tries to make any changes to your system. It can also help stop malware and unwanted software from installing themselves or changing the way your computer works.

Windows 10 Elevated Security

In Windows 10 and Windows Server 2016 you should use Credential Guard to enhance security.

See more details at:

https://technet.microsoft.com/en-us/itpro/windows/keep-secure/credential-guard

Additional Environment Recommendations

The following actions will help keep your information as safe as possible:

- Enable Windows Defender
- Control access to your computer by locking your screen after a period of inactivity.
- Set up secure file sharing.
- Make sure you're running only those sharing services that you really need.
- Use a local account - This provides greater security than, for example, a Microsoft account which, if hacked, it will enable remote logon to your applications.
- Enable secure boot and UEFI, instead of legacy BIOS.
- Disable Flash and Java. These frequently report security vulnerabilities.
- Encrypt hard drive. This will protect your data if your computer accessed directly.

NOTE:
SAC 10.7 is compliant with Windows 10 Microsoft Credential Guard and Windows 8.1 Local Security Authority (LSA) with code integrity enabled.

SAC Configuration Recommendations

The following recommendations will help you maintain a secured SAC environment as well as keep your information as safe as possible:

- **Common SAC configuration:** The preferred mechanism to use when deploying SAC configuration policies through the company domain computers, is to use the domain GPO with SAC ADM and ADMX files. For more information, refer to Chapter 7: SafeNet Authentication Client Settings (page 63).
- **Common UI restrictions:** System administrators can hide/disable an unwanted UI option/s and configure the non overridable UI parameters. For more information, refer to Chapter 8: SafeNet Authentication Client Tools UI Initialization Settings (page 85), Chapter 8: SafeNet Authentication Client Tools UI Settings (page 89) and Chapter 8: SafeNet Authentication Client Tools UI Access Control List (page 109).
- **User/Administrator smart card password protection:** To avoid password leakage, we recommend the following:
  - **Use PIN Pad readers -** user passwords do not pass through a computers memory when using a PIN Pad reader.
  - **Use devices configured to support secured messaging -** secured messaging protects the transfer of data between the middleware and the device.
- **Protect the device from unauthorized usage:**
  - Ensure the device is disconnected when not in use.
  - Enable the CAPI Password Timeout option - this requires re-authenticating (See Chapter 8: CAPI Settings (page 96))
  - Using the Single Logon option is less secured and is therefore not recommended (See the Single Logon registry key in Chapter 8: General Settings (page 72))
- **Configure restrictive password policies:**
  - Change the default administrator password. For more information, see the SafeNet Authentication Client User Guide - Chapter 4 - Token Management.
  - For devices running the eToken applet, change the default Initialization Key (this protects devices from unwanted initialization). For more information, see the SafeNet Authentication Client User Guide.

- If the device was enrolled by an administrator (on behalf of a user), use the 'Token password must be changed on first logon' option. For more information, see the SafeNet Authentication Client User Guide.
- For supported devices use the on-board password quality settings (use the 'Enforce password quality settings' option). For more information, see the SafeNet Authentication Client User Guide.
- The recommended password strength is:
  - User PIN should include at least 8 characters of different types.
  - Admin PIN should include at least 16 characters of different character types.
  - The Friendly Admin Password should include at least 16 characters of different types (See the SafeNet Authentication Client User Guide for more details on the Friendly Admin Password)
  - Digital Signature PUK, when using a friendly name, this should include at least 16 characters of different types.
  - For devices running the IDPrime applet, the 3DES random key may be used instead of the administrator password.
  - Use the password validity period combined with password history options.

For more information on how to configure password policy settings, refer to 'Chapter 8: Token Password Quality Settings (page 103), the **Token Initialization** chapter in the SafeNet Authentication Client User Guide and the **Password Recommendations** section in the SafeNet Authentication Client Release Notes.

NOTE:
Character types include upper case, lower case, numbers, and special characters.

- **Configure restrictive cryptographic policies:**

  To allow organizations to enforce restrictive cryptographic policies when using SafeNet / Gemalto security devices (smart cards and USB tokens), the following policies were updated:

  - Deprecated Cryptographic Algorithms and Features Policy
  - Key Management Policy

  The motivation behind these policy updates:

  Legacy cryptographic schemes can cause organizations to fail current compliance requirements or expose cryptographic weakness associated with deprecated algorithms and mechanisms.
  Changes have been made to the default SAC configuration to disallow the usage of cryptographic algorithms, or protocols, that are now considered to be weak.

  Default settings were updated to eliminate revealing sensitive data:

  - The creation, generation and usage of exportable symmetric keys are blocked.
  - The unwrapping and wrapping of asymmetric/symmetric private keys is blocked.
  - Preventing legacy algorithms from being used by adding a key wrapping policy that enforces the usage of only GCM and CCM modes of operation for symmetric encryption, and PKCS#1 v2.1 padding for RSA encryption.
    GCM or CCM modes are used for wrap/unwrap operations using the session wrapping key. All other modes are blocked.

- Legacy and obsolete algorithms are blocked - these cryptographic algorithms conform to the National Institute of Standards and Technology (NIST), preventing third-party applications from using legacy or obsolete algorithms..

NOTE:
Once a restrictive policy has been set, the use of SafeNet Authentication Client with the above algorithms will be blocked. This might have implications on the way in which the third-party's applications currently work. Administrators must make sure that the third-party applications used by the organization are configured accordingly and do no use one of the algorithms listed above, as they will be blocked.

For more information, refer to Chapter 8: Security Settings (page 113).

- **Create symmetric key objects using PKCS#11:**

  As part of SafeNet Authentication Client security enhancement campaign, the following was performed:

  - Protected memory was used when working with the private cache between PKCS#11 API calls. Private cache is unlocked to retrieve data and then locked immediately after retrieving the data to ensure that there is no sensitive data in the private cache. This ensures that the key cannot be revealed in plain text.
  - Sensitive data is securely zeroed prior to freeing up the memory.
  - AES and Generic symmetric key files were created with Secured Messaging (SM) protection so that the Microsoft smart card transport layer does not contain any APDU data with plain symmetric key material.
  - For Secure Messaging (SM) to support the AES/3DES and Generic symmetric keys, the keys must be created on an eToken Java device that is initialized in FIPS/CC mode. Applying SM to symmetric keys changes the object format on the smart card, resulting in the keys not being backward compatible.
  - Keys that are created with previous SAC versions or on eToken Java devices which are formatted in non-FIPS/CC mode will not be protected by SM.

  AES/3DES keys that are created using the `CKA_SENSITIVE = TRUE` and `CKA_EXTRACTABLE = FALSE` attributes are backward compatible (BS Object keys).

NOTE:
As of SAC 10.5, the creation, generation and usage of exportable symmetric keys were blocked. For more information, refer to Chapter 8: Security Settings (page 113).

Customization

The SafeNet Authentication Client (SAC) installation features and the graphic user interface provided by Gemalto can be customized for your installation.

NOTE:
- .Net Framework 3.5 or higher is required on all operating systems when running the SafeNet Authentication Client Customization Tool.
- For backward compatibility with Gemalto IDGo 800 PKCS#11 and Minidriver deployments, refer to the section: Installing the SafeNet Authentication Client Customization Tool below.

Customization Overview

You can customize the following SafeNet Authentication Client 10.7 (GA) features:

- Product name, which appears in the installation wizard, the *Add/Remove* program, and the *About* window
- Destination folder
- URL of the support link in the *Add/Remove* program
- License string
- SafeNet Authentication Client and SafeNet Minidriver features to be installed
- Policy settings
- MSI Signing settings
- Window banners

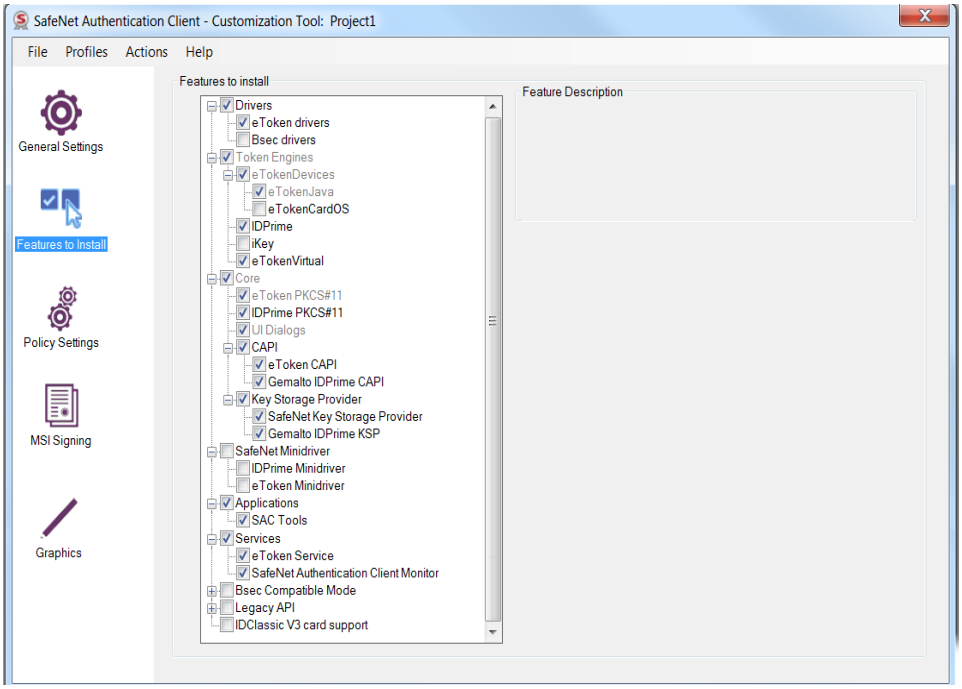
SAC Customization Tool Profiles

SafeNet Authentication Client Customization Tool has three predefined installation profiles. By selecting these profiles, there's no need to configure and install individual elements.

The following predefined installation profiles are available:

SAC Typical Profile

Installs the most common application features available when installing SafeNet Authentication Client using the installation wizard. Selecting SAC Typical will not install support for Bsec, CardOS and iKey.



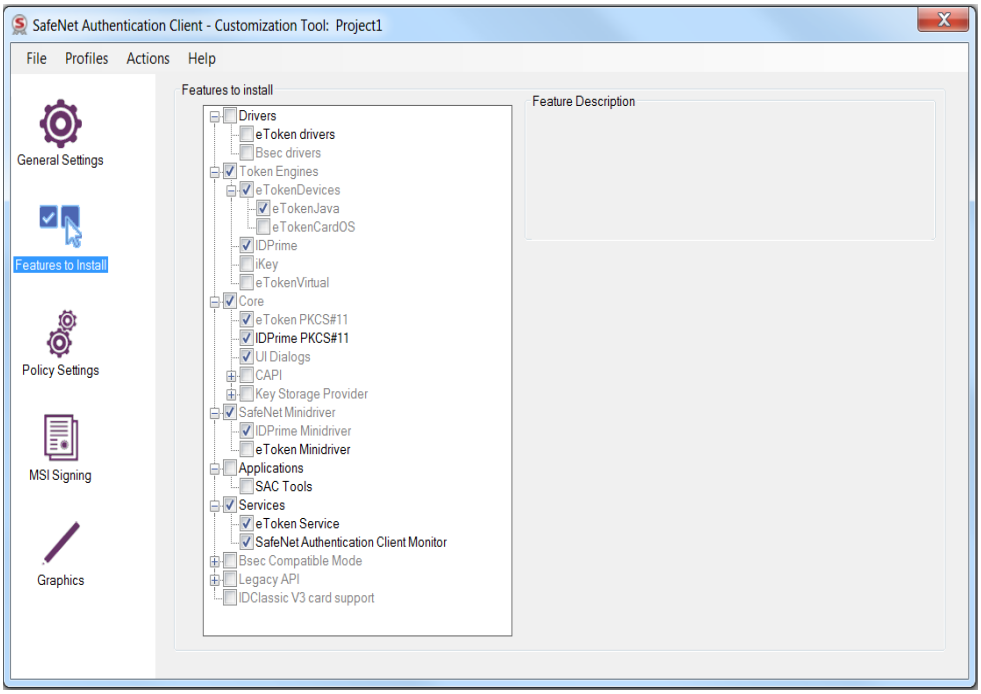
SafeNet Minidriver Profile

Mainly for Gemalto customers who want to work only with SafeNet Minidriver together with SAC services. Only the relevant SafeNet Minidriver components have been made available in this profile, all other components that are not relevant to this profile have been grayed out.

Selecting SafeNet Minidriver profile installs core Middleware services, such as eToken Service and SafeNet Authentication Client Monitor that allow managing public device data for better Minidriver performance, as well as support for Single Logon.

The SafeNet Minidriver profile allows editing (selecting/clearing) the following components:

- eToken Minidriver
- Applications (SAC Tools)
- Services (eToken Services and SafeNet Authentication Client Monitor)
- Core (IDPrime PKCS#11)
- eToken Drivers



The SafeNet Minidriver feature may be used by Gemalto customers that require IDGo 800 PKCS#11 and have a dependency on the location of the IDGo 800 PKCS#11 dll file. Selecting the SafeNet Minidriver Profile enables Gemalto customers with existing applications that depend on it to seamlessly migrate to SAC without breaking the compatibility of these applications.

Configuring SafeNet Minidriver profile for Backward Compatibility

SAC 10.7 Customization Tool enables you to generate an .msi file, which contains SafeNet Minidriver 10.2 as well as PKCS#11 proxy. This customized installation is fully compatible with the legacy IDGo 800.

When selecting the SafeNet Minidriver profile, the following dll files are installed under C:\Program Files (x86)\Gemalto\IDGo 800 PKCS#11:

Dll File	Description
IDPrimePKCS11.dll	x32 PKCS#11 library stub for Gemalto IDPrime cards.
IDPrimePKCS1164.dll	x64 PKCS#11 library stub for Gemalto IDPrime cards.
axaltocm.dll	Installed in the System32 folder.
axaltocm.dll	Installed in the SysWOW64 folder.

eBanking Profile

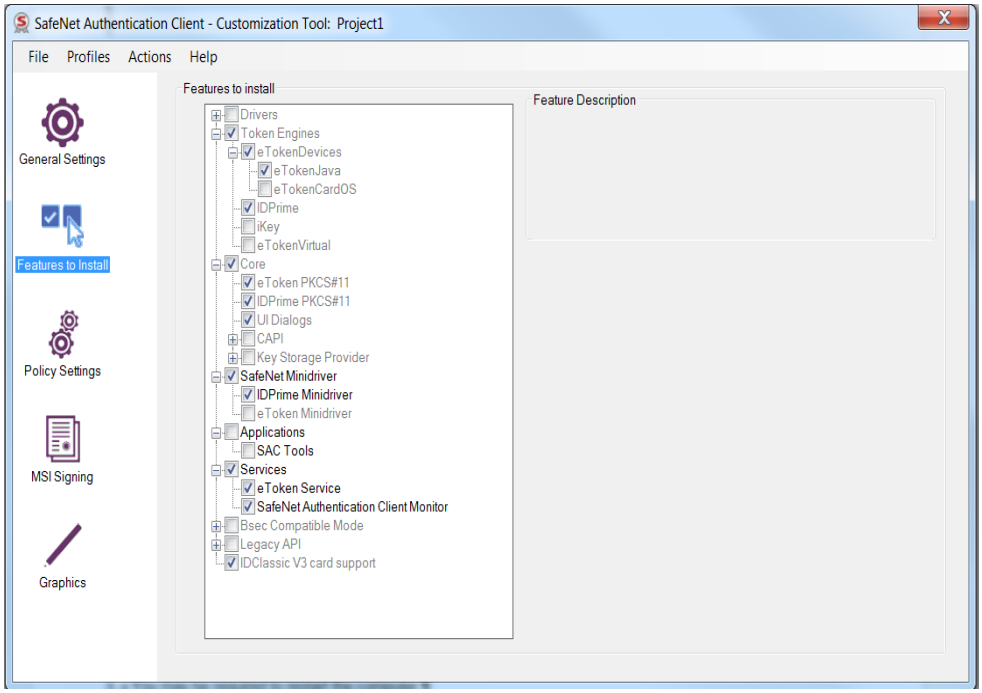
NOTE:
For more details, see *IDClassic 340 (V3) Card Support on SafeNet Authentication Client Solution Guide*

Mainly for legacy Classic Client users (who use IDClassic V3 cards) migrating to SafeNet Authentication Client and for IDPrime card user who want to install IDPrime Minidriver. Customers working in the eBanking profile (IDClassic V3 users) and want to migrate to IDPrime cards, can continue working with Classic Client's Toolbox, until fully migrated to SAC.

Only the relevant eBanking components have been made available in this profile (for example: The IDClassic V3 card support component cannot be deselected from the eBanking profile), all other components that are not relevant to this profile have been grayed out.

The eBanking profile allows editing (selecting/clearing) the following components:

- SafeNet Minidriver (IDPrime Minidriver is selected by default)
- Applications (SAC Tools)
- Services (eToken Services and SafeNet Authentication Client Monitor)



NOTE:
The eBanking profile also installs V3 cards supported using PKCS#11 and IDPrime MD cards supported via PKCS11 and Minidriver.

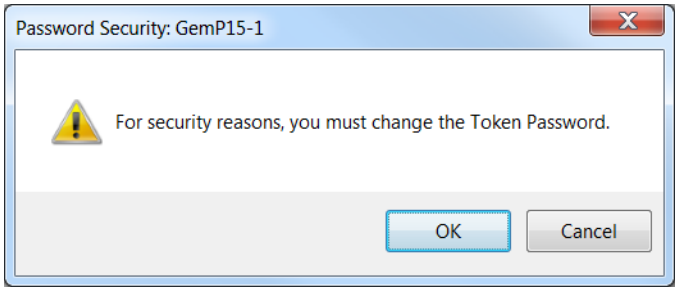
Must Change Password at First logon

If the Token password must be changed on first logon option is enabled, the user will be prompted to set a new password when connecting the device or next logging on.

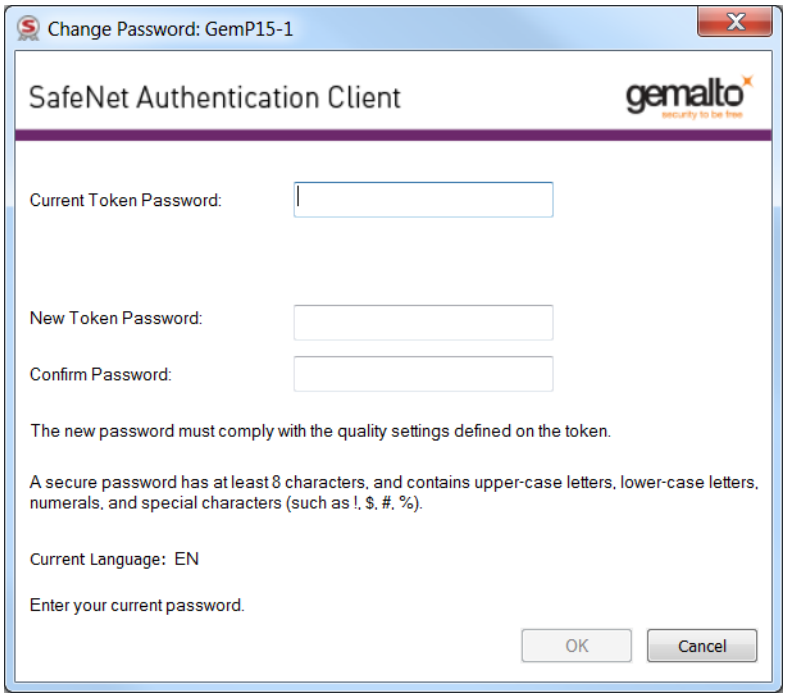
To change the password at first logon:

1. Connect the device.

   The **Password Security** window opens.



2. Click **OK**.



3. Enter the current token password in the **Current Token Password** field.
4. Enter the new token password in the **New Token Password** and **Confirm Password** fields.

> **NOTE**:
> The new password must meet the Password Quality requirements configured in the Settings window.

5. Click **OK**.

   Your password has been changed.

PIN Policy on IDClassic 340 (V3) Cards

IDClassic 340 (V3) cards are first initialized (factory settings) using a 6 digit password (PIN Minimum Length = 6) and the cards PIN Policy contains only the Minimum and Maximum PIN lengths. The minimum and maximum PIN lengths on the card together with the settings in SafeNet Authentication Client make up the IDClassic 340 (V3) card's PIN Policy.

NOTE: The default PIN minimum length in SafeNet Authentication Client is 8 therefore, the next password must have at least 8 digits.

Installing the SafeNet Authentication Client Customization Tool

Before installing SafeNet Authentication Client, install the *SafeNet Authentication Client Customization Tool*.

NOTE:
Only users that have Domain Admin Credentials may use the Customization Tool to create MSI files.

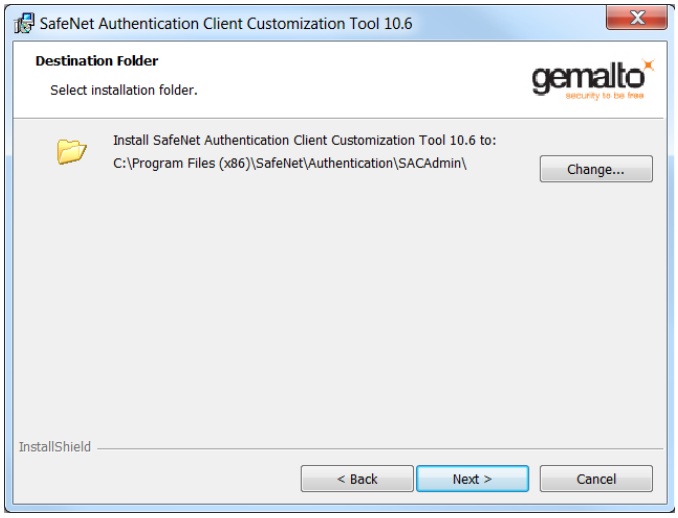
To install the SafeNet Authentication Client Customization Tool:

1. Double-click **SACCustomizationPackage-10.7.msi**.
   The *SafeNet Authentication Client Customization Package Installation Wizard* opens.

2. Click **Next**.
   The *License Agreement* is displayed.

3. Read the license agreement, and select the option, **I accept the license agreement**.
4. Click **Next**.

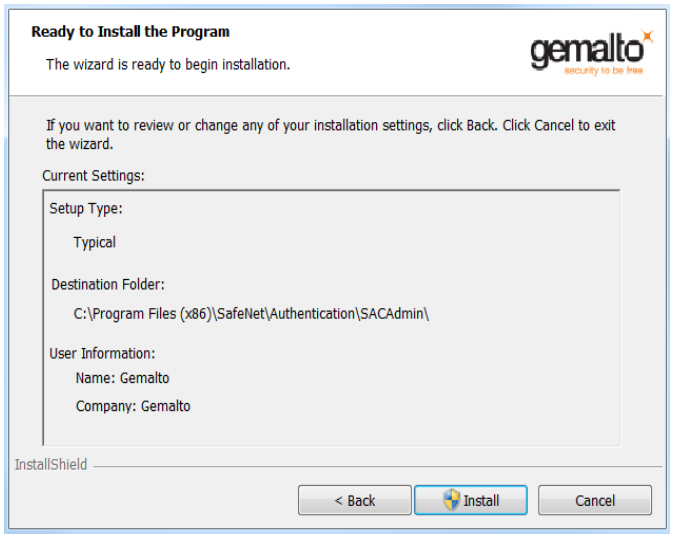
The *Destination Folder* window opens, displaying the default installation folder.



5. You can click **Browse** to select a different destination folder, or install the Customization Tool's SACAdmin folder into the default folder:
`C:\Program Files\SafeNet\Authentication\`

NOTE:
If an application from the SafeNet Authentication line of products, or an eToken legacy product, is already installed, we recommend that the destination folder not be changed.

The R*eady to Install the Program* window opens.



6. Click **Install** to start the installation.

When the installation is complete, the *SafeNet Authentication Client Customization Package has been successfully installed* window opens.

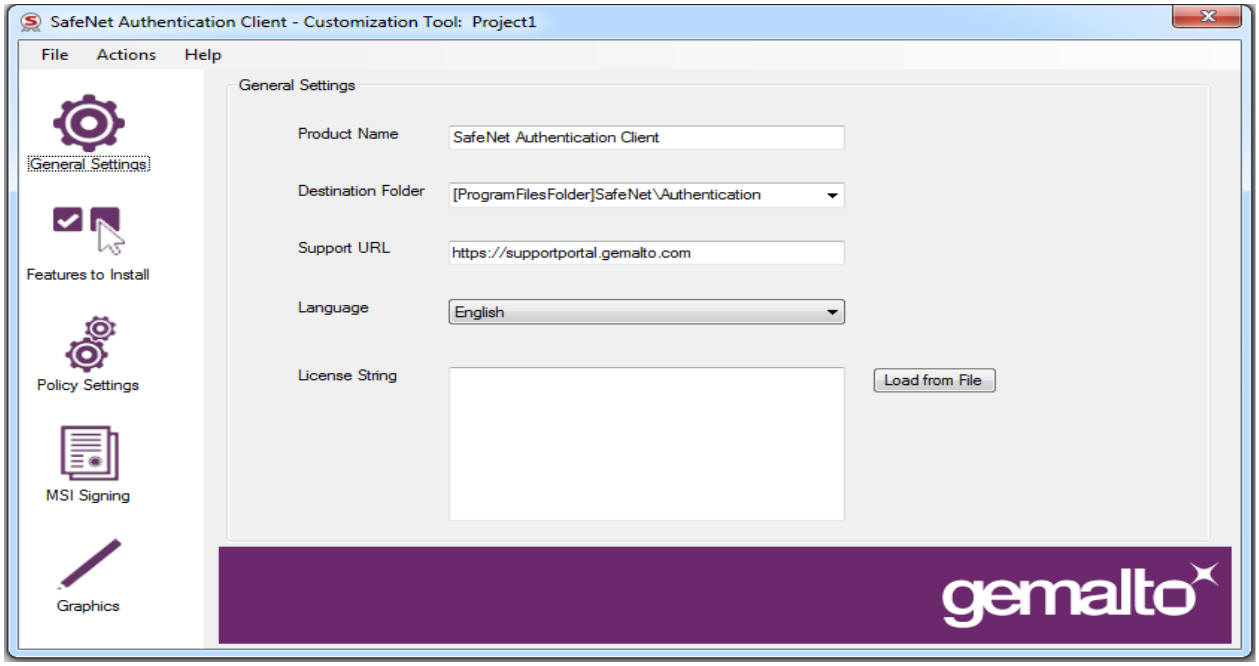
7. Click **Finish** to exit the wizard.

Using the SafeNet Authentication Client Customization Tool

After installing the SafeNet Authentication Client Customization Package, customize the appropriate features.

To use the Customization Tool:

1. From the Windows *Start* menu, select **Programs > SafeNet > SACAdmin > SAC Customization Tool**.
   The *SafeNet Authentication Client Customization Tool* opens to the *General Settings* tab.



2. To open a project you already saved, select **File > Open**, and browse to the xml file of an existing project.

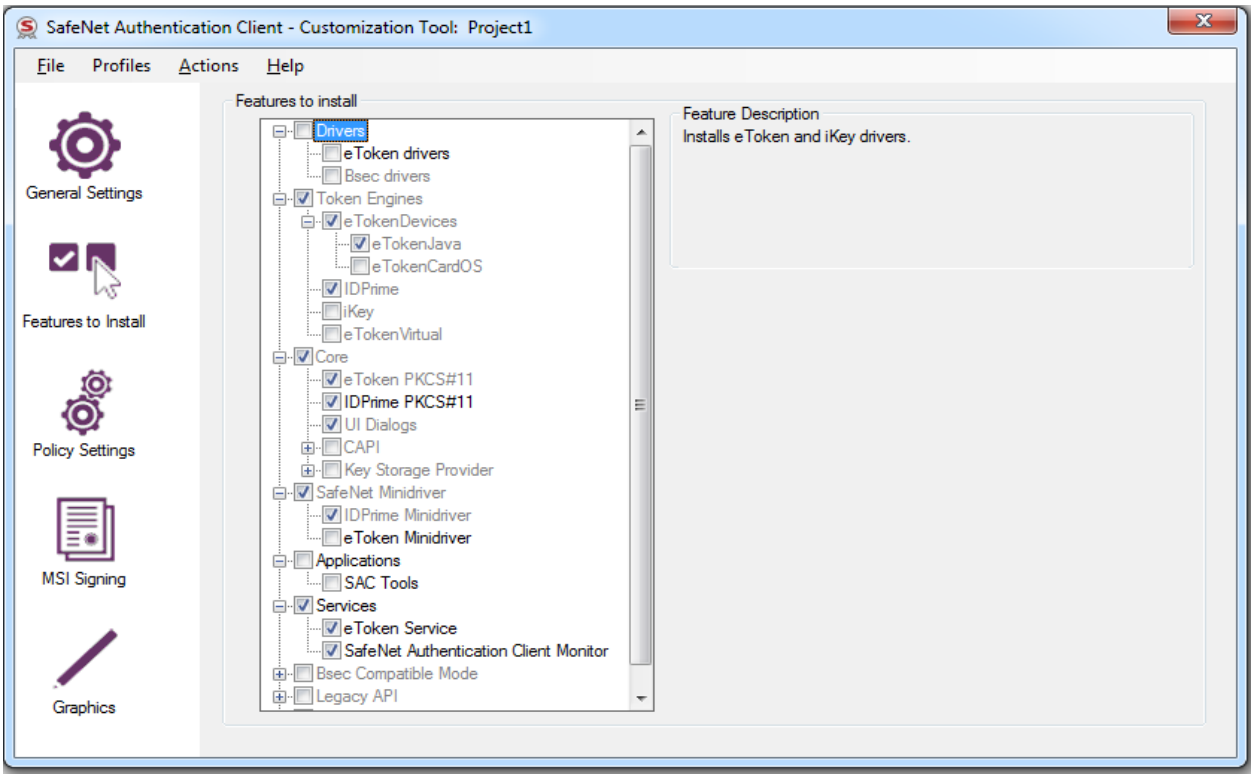
> **NOTE**:
> Due to the changes implemented in the SAC 10.7 Customization Tool, opening an xml file saved with earlier versions of SAC is not supported.

3. You can replace the following items:
   - **Product Name:** enter the relevant product name (the default value is SafeNet Authentication Client 10.7).
   - **Destination Folder:** the path to be used by the SafeNet Authentication Client Customization Tool when no other SafeNet product has been installed on the client computer
   - **Support URL:** the URL to be displayed in the Windows *Add/Remove Programs* support link (the default value is http://www.safenet-inc.com/authentication).
   - **Language:** select the language in which SafeNet Authentication Client will be installed.

> **NOTE**:
> If a language other than English is selected, the language option is disabled (grayed out) during the installation process. SAC is installed in the language chosen here.

   - **License String:** either copy and paste a license into the box, or click **Load from File**, and browse to the .lic file containing the SafeNet Authentication Client license.
4. In the left column, select the **Features to Install** tab.

   The *Features to Install* window opens with the default SAC installation features selected.

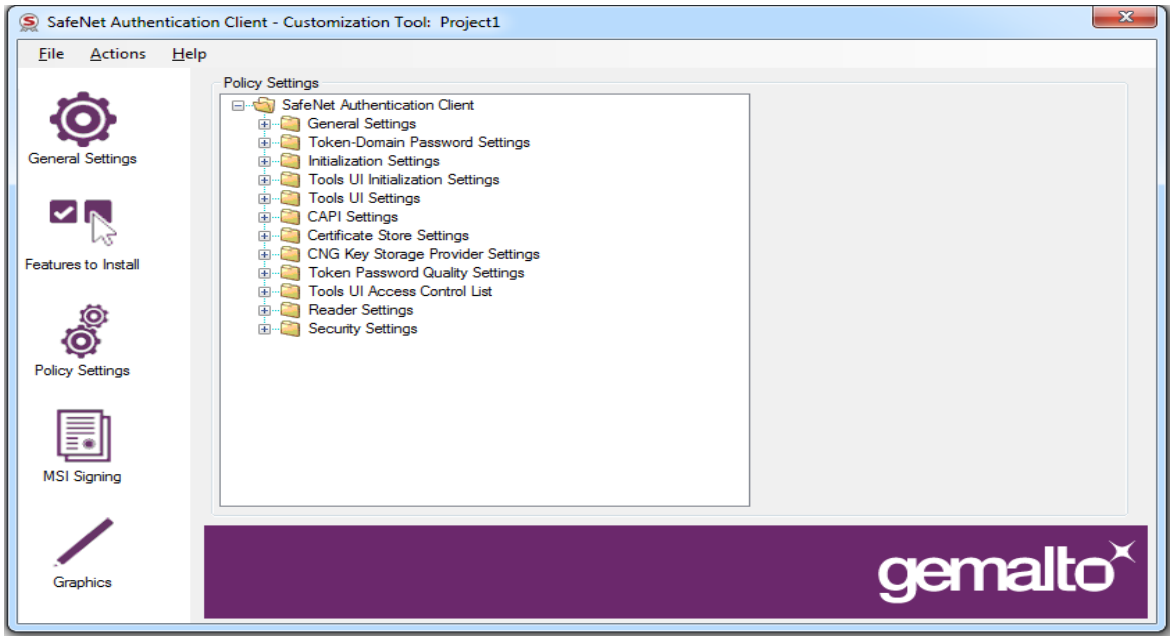


5. The features may be customized by changing the editable check-boxes.

> **NOTE**:
> - When using eToken Devices it is recommended to check the eToken CAPI and SafeNet Key Storage Provider check-boxes.
> - In order to work with SafeNet Network Logon the eToken SAPI check-box must be checked.

6. In the left column, select the **Policy Settings** tab.

   The *Policy Settings* window opens.

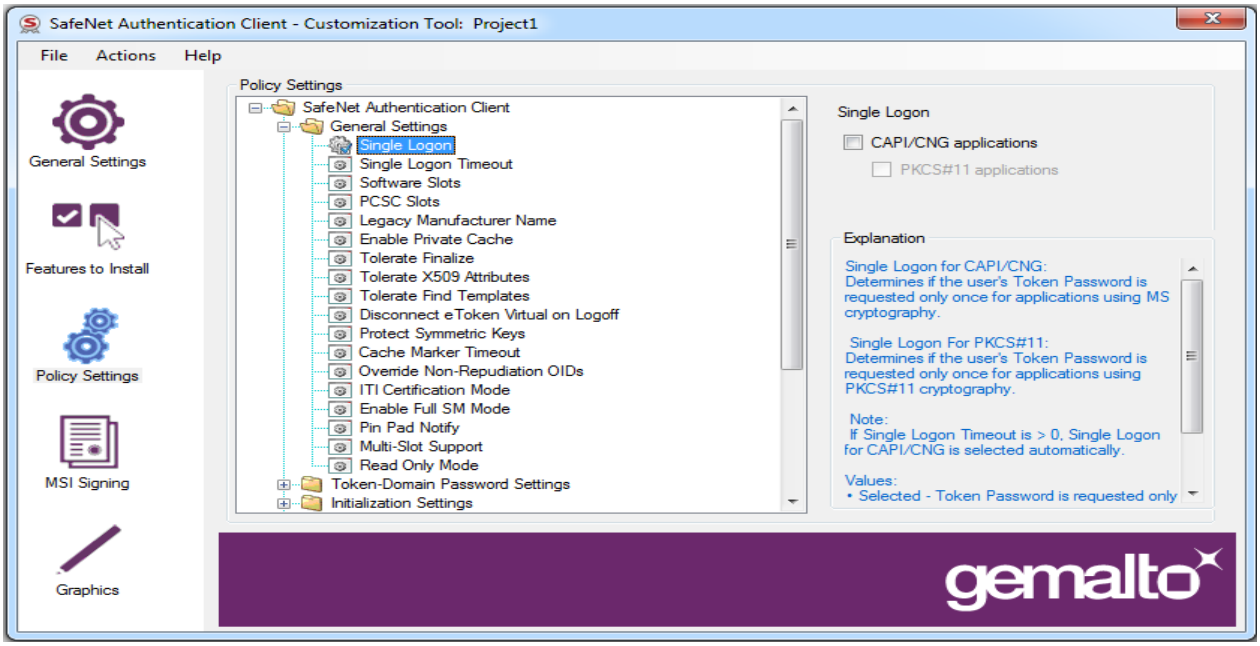


7. You can override the application's default values by changing the configuration properties to be written to the registry keys. These new values are saved in `HKEY_LOCAL_MACHINE/SOFTWARE/Policies/SafeNet/Authentication/SAC`.

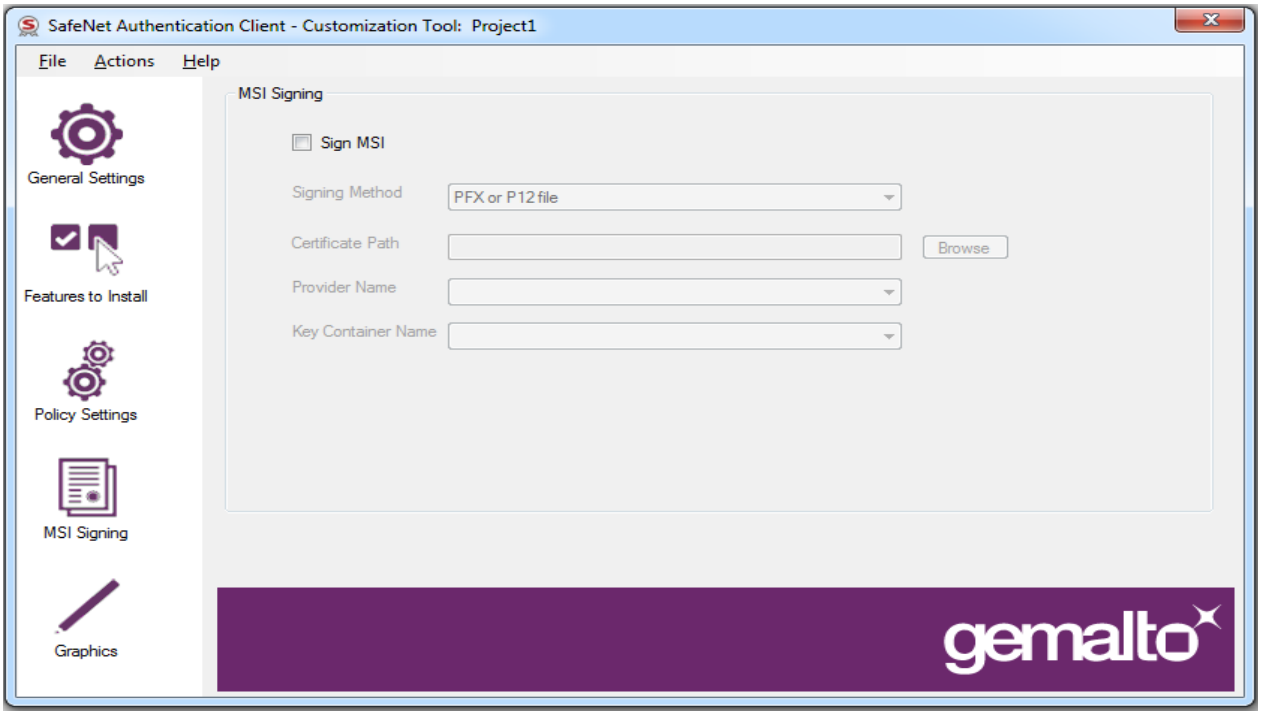
   For more information, see Chapter 8: *Configuration Properties*, on page 68.

For each setting to be changed, expand the appropriate node, select the setting, and change its value.

NOTE:
Not all policy settings are supported by IDPrime MD cards. For more details see Chapter 8: "Configuration Properties" on page 68.



8. In the left column, select the **MSI Signing** tab.
   The *MSI Signing* window opens.

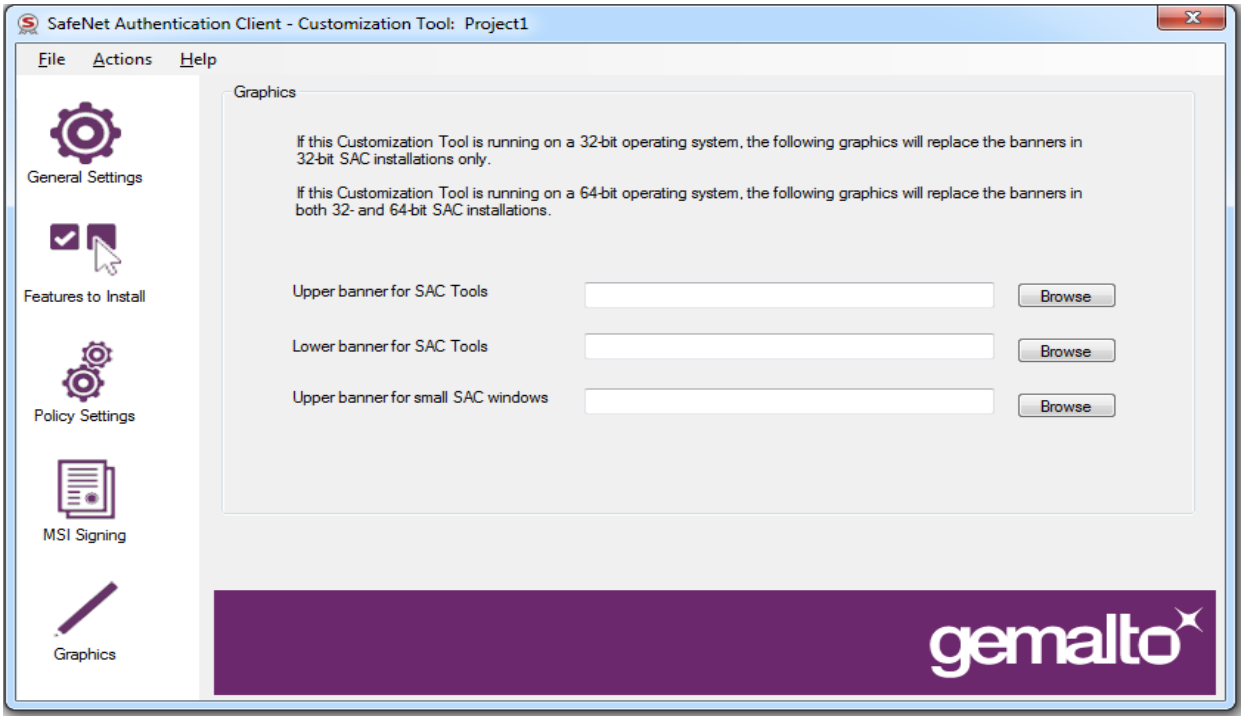


9. To sign the installation file, select **Sign MSI**, and complete the enabled fields. These may include:
   - Signing Method (P12, Smartcard or HSM)
   - Certificate Path
   - Provider Name
   - Key Container Name

> **NOTE**:
> - Ensure that a Code Signing certificate is used when using the MSI signing feature.
> - .msi files are now signed using the SHA 2 algorithm.

10. In the left column, select the **Graphics** tab.

The *Graphics* window opens.



NOTE:
When installing only IDGo 800 Minidriver, the Graphics feature is not applicable.

The following graphics can be replaced:

- Upper Banner for SAC Tools - (File name: SACTopLogo.png, Properties: Dimensions - 764X142 pixels, Bit Depth - 24)
- Lower Banner for SAC Tools - (File name: SACBottomLogo.png, Properties: Dimensions - 764X76 pixels, Bit Depth - 24)
- Upper banner for small SAC windows - (File name: SACLogo.png, Properties: Dimensions - 506X65 pixels, Bit Depth - 32)

NOTE:
All banner formats must be in PNG format.

11. To change a banner, click **Browse**, and select the graphic file required.
12. To save the customized settings, select **File > Save As**, and enter a name for the project.

NOTE:
- The customized settings are saved as an xml file.
- By default, project folders are saved in the following location: My Documents\SafeNet\Authentication\SAC\[ProfileName]

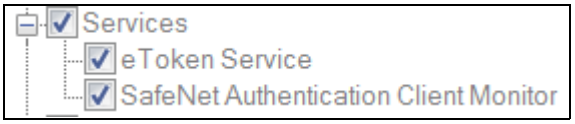
Features to Install

This section covers a few SafeNet Authentication Client Customization Tool installation features.

For more details on what binary files are installed and their location, see Chapter 5: “SafeNet Authentication Client Binary Files” on page 43.

Services

Installs SafeNet Authentication Client Monitor (Tray icon). All check-boxes are selected and shaded.

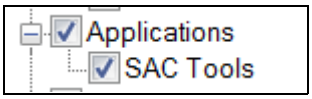


If the above options are selected, the following files are installed:

- SACSRV.exe
- SACMonitor.exe

Applications

Installs the SAC Tools application (Middleware).



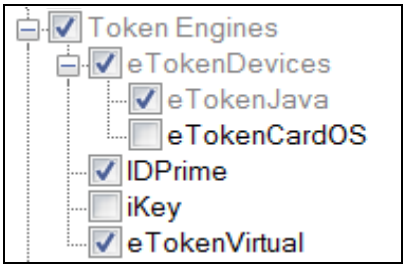
If the above options are selected, the following files are installed:

- SACTools.exe
- SACMonitor.exe

eToken Engines

Installs token engines to support Java and CardOS devices. When selecting the SAC Typical profile, the following check-boxes are selected and shaded:

- Token Engines
- eTokenDevices
- eTokenJava



If the above options are selected, the following files are installed:

- cardosTokenEngine.dll - CardOS token engine
- IDPrimeTokenEngine.dll - IDPrime token/card engine
- iKeytokenEngine.dll - iKey token engine
- etvTokenEngine.dll - SafeNet Virtual Token engine

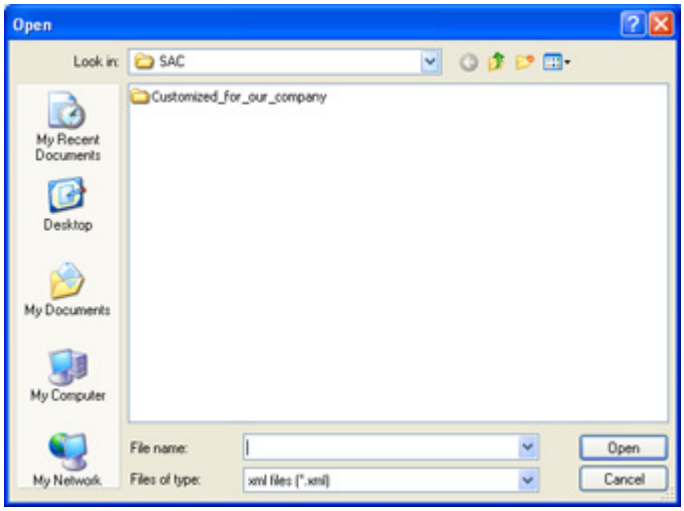
Generating a Customized MSI Installation File

After the appropriate features are customized, generate an installation file.

NOTE:
Generating an MSI file can be performed with administrator privileges only.

To generate a customized installation file:

1. Open the *SAC Customization Tool*.
   See "Using the SafeNet Authentication Client Customization Tool" on page 30.
2. Select **File > Open**.



3. Browse to the `xml` file in the folder of an existing project, and click **Open**.

NOTE:
- By default, project folders are saved in the following location:
  My Documents\SafeNet\Authentication\SAC
- SAC 10.7 does not support legacy GA configuration profiles.

   The saved project opens.
4. Select **Actions > Generate MSI**.
   An information window is displayed, informing you that the MSI installation files have been generated.

5. Click **OK** to close the window.

   The project folder contains two customized MSI files:

   - A file named `<Project Name>-x32-10.7.msi` for 32-bit installations
   - A file named `<Project Name>-x64-10.7.msi` for 64-bit installations

Installing the Customized Application

After the .msi installation file is generated, use it to install the application with its customized properties and features.

To install the customized application:

1. Log on as an administrator.
2. Close all applications.
3. Browse to the folder of the customized project saved in *Features to Install* on page 36.

   NOTE:
   By default, project folders are saved in the following location:
   My Documents\SafeNet\Authentication\SAC

4. Double-click the appropriate msi file:
   - `<Project Name>-x32-10.7.msi` (for 32-bit installations)
   - `<Project Name>-x64-10.7.msi` (for 64-bit installations)

   where `<Project Name>` is the name of the customized project.

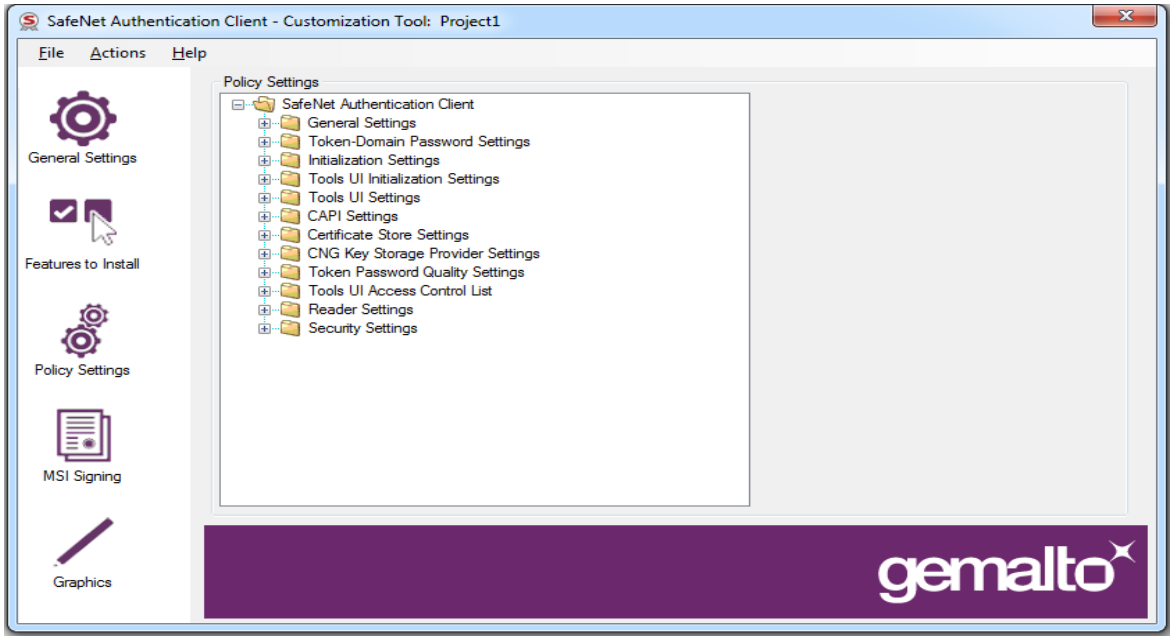
   The *Installation Wizard* runs.
5. Follow the wizard until the installation is complete, and a confirmation message is displayed.
6. Click **Finish** to complete the installation.

Changing the Password Minimum Length Permanently

Follow the procedures bellow to set the Password Minimum Length property as a permanent value.

To change the Password Minimum Length permanently:

1. Open the *SAC Customization Tool*.
   See "Using the SafeNet Authentication Client Customization Tool" on page 30.
2. In the left column, select the **Policy Settings** tab.
   The *Policy Settings* window opens.



3. Expand the **Token Password Policy Settings** node select the **Password - Minimum Length** setting and set the required value.
4. Expand the **Tools UI Access Control List** node select the **PIN Quality** setting and uncheck the **Minimum length (characters)** parameter. This disables the **Minimum length (characters)** parameter under **Token Settings > PIN Quality** in SAC Tools as well as in the SAC Tools Initialization process.

Upgrade

It is recommended that eToken PKI Client, BSec, and earlier versions of SafeNet Authentication Client be upgraded to the latest version on each computer that uses a SafeNet eToken, iKey token, or SafeNet smartcard. Local administrator rights are required to upgrade SafeNet Authentication Client.

NOTE:
- You must restart your computer when the upgrade procedure completes. When upgrading via the command line using the /qn parameter, your computer is restarted automatically.
- When upgrading from previous versions of SAC, it is recommended that you save feature settings from the previous versions. If not, then uninstall and install SAC 10.7 with the new feature list.

Upgrading Using the SafeNet Authentication Client .msi File

To upgrade from earlier versions of SafeNet Authentication Client using the msi file:

- On a 32-bit system, run **SafeNetAuthenticationClient-x32-10.7.msi**.
- On a 64-bit system, run **SafeNetAuthenticationClient-x64-10.7.msi**.

NOTE:
Ensure that all SafeNet Authentication Client applications are closed before upgrading, installing, or uninstalling SafeNet Authentication Client.

To upgrade SAC 10.5 (installed on Windows x32 OS via the Customization Tool) with SafeNet Minidriver, SAC 10.5 must be uninstalled before installing SAC 10.7.

Upgrading from Versions Earlier than SAC 9.0

Legacy versions of SafeNet Authentication Client, earlier than 9.0 must be uninstalled before installing SafeNet Authentication Client 10.4 (GA).

Upgrading from SafeNet Authentication Client 9.0

You can upgrade from SafeNet Authentication Client 9.0 to 10.7 using the **MSI** file wizard installation, or by using the command line installation. See Installing the MSI file via the Command Line on page 51.

While running the wizard, be sure to select **Use the existing configuration settings** parameter on the installation wizard **Interface Language** window. This will save the configuration settings that were detected from the previous version.

Installation

Follow the installation procedures below to install SafeNet Authentication Client. Local administrator rights are required to install or uninstall SafeNet Authentication Client.

NOTE:

- When using an MSI file to install on Windows 7, do not run the installation from the *Desktop* folder. To ensure a successful installation, run the installation from another location on your computer.
- Systems later than Windows 7 and Window 2008 R2, the total number of readers is limited to 10 from among: iKey readers, eToken readers, third-party readers, and reader emulations.
- **Firefox Settings:** Before installing SAC, Firefox must be installed on the computer and opened at least once to make the registration available. To verify that registration in Firefox was performed correctly, after installing SAC, open Firefox and go to **Options > Privacy and Security > Certificates > Security Devices**. The eToken module should be displayed with eTPKCS11.dll configured.

To customize the user interface and the features to be installed, see Chapter 3: *Customization*, on page 21.

NOTE: •

- When installing SafeNet Authentication Client on a machine with IDGo 800 Minidriver installed, the IDGo 800 Minidriver must be uninstalled before installing SAC 10.7. If IDGo 800 PKCS#11 is installed, remove it before installing SAC.

Installation Files

The software package provided includes files for installing or upgrading to SafeNet Authentication Client 10.7.

The following installation and documentation files are provided:

File	Environment	Description
Windows		
SafeNetAuthenticationClient-x32-10.7.msi	32-bit	Installs SafeNet Authentication Client 10.7, and upgrades from earlier versions of SafeNet Authentication Client.
SafeNetAuthenticationClient-x64-10.7.msi	64-bit	
SACCustomizationPackage-10.7.msi	32-bit 64-bit	Installs SafeNet Authentication Client 10.7 Customization Package. Use to customize SafeNet Authentication Client installation with non-default settings. If a previous version of the Customization package exists, uninstall the previous version, and then install the new version.
Documentation Files		
007-013559-007_SafeNet Authentication Client_ 10.7_Windows_GA_RN_Revision D		SafeNet Authentication Client 10.7 Release Notes for Windows. Read before installation for last minute updates that may affect installation; contains important information such as resolved and known issues and troubleshooting.
007-013561-005_ SafeNet Authentication Client 10.7_Windows_User Guide_Revision C		SafeNet Authentication Client 10.7 User Guide for Windows. Provides detailed information for the user and system administrator regarding the use of SafeNet Authentication Client.
007-013560-005_SafeNet Authentication Client 10.7_Windows_ Administrator Guide_Revision C		SafeNet Authentication Client 10.4 (GA) Administrator Guide for Windows (this document). Provides detailed information for the system administrator regarding the installation, configuration, maintenance, and management of SafeNet Authentication Client.

SafeNet Authentication Client Binary Files

After installing SafeNet Authentication Client, all binary data (compiled programs, images, media and compressed files) is saved in: **C:\Program Files\SafeNet\Authentication\SAC.**

The following folders and files exist under **C:\Program Files\SafeNet\Authentication\SAC:**

Folder/File	Folder Contents (.exe, .dll, .reg, .iso files)	Description
Install	• pki_defaults.reg	Default registry file. Double click the pki_defaults.reg file to change SAC configuration back to the default configuration.
LogoImages	• SACBottomLogo.png • SACLogo.png • SACTopLogo.png	Contains SAC Logo image files. These files may be customized using the SafeNet Authentication Client Customization Tool.
x32	• Language support packages (e.g. cs-CZ, fr-CA, etc.)	These folders contain Windows x32-bit and x64-bit related DLL's and packages. **Note:** For x64-bit installations, both directories (x32 and x64) are created. All x64-bit binaries are located in the x64 folder and x32-bit binaries are located in the x32 folder. All .exe files (applications) are located in the x64 folder only. If a custom installation is performed using the SAC Customization Tool, additional .exe files will be shown in either the x32 or x64 folders.
x64	• cardosTokenEngine.dll- installs the CardOS token engine. This file is the main SAC dll file, which contains the majority of SAC codes and the eToken java engine (required for all devices). • eTokenHID.dll - this file supports HID devices (only required for devices that are in HID mode). • etvTokenEngine.dll - installs the SafeNet Virtual Token engine. • IDPrimeTokenEngine.dlll - installs the DPrime token/card engine. • iKeyTokenEngine.dll - installs the iKey token engine. • ManageReaders.exe - this application manages reader settings (uses eTCoreInst.dll). • RegistereTokenVirtual.exe - this application manages the registration of SafeNet Virtual Tokens. • SACLog.dll - manages all application logs and DLL's (The 'Enable logging' options must be selected). • SACMonitor.exe - Installs the SafeNet Authentication Client application. • SACSRV.exe - Installs SafeNet Authentication Client services • SACTools.exe - Installs SACUI.dll	
App-RTE	SafeNet Authentication Client icon	
SACHelp	SafeNet Authentication Client User Guide	This file opens when clicking the Help icon in SAC Tools.

System32 and SysWOW64 Folders

All SafeNet Authentication Client DLL files that exist in the System32 folder are compiled as x64-bit.

All SafeNet Authentication Client DLL files in the SysWOW64 folder are compiled as x32-bit.

The following binaries are installed in both the System32 and SysWOW64 folders:

Dll File	Description
eTPKCS11.dll	Installs the PKCS#11 wrapper that supports both eToken and IDPrime cards.
eTCAPI.dll	Installs and supports CAPI security interface.
eTCoreInst.dll	A custom dll that installs eToken drivers and adds Smart Card reader device nodes.
SNSCKSP.dll	Supports CNG KSP security interface.
eTOKCSP.dll	Supports CAPI CSP security interface.

NOTE:

- For 64-bit installations, both the C:\Windows\System32 folder and C:\Windows\SysWOW64 folder are created and all the 64-bit binaries are located in the System32 folder and all 32-bit binaries are located in the SysWOW64 folder.
- For 32-bit installations: Only the C:\Windows\System32 folder is created and only the 32-bit binaries are located in this folder.
- There is an option available that allows checking SAC binary signatures via the SafeNet Authentication Client User Interface (About Window). For more information, refer to the SafeNet Authentication Client User Guide.

IDClassic (V3) Binary Files on SafeNet Authentication Client

After installing legacy Classic Client side-by-side with SafeNet Authentication Client 10.7, all binary data (compiled programs, images, media and compressed files) are saved in:

`C:\Program Files\Gemalto\Classic Client\BIN\gck2014.dll`

`C:\Program Files\Gemalto\IDGo 800\PKCS#11\IDPrimePKCS11.dll`

`C:\Program Files\SafeNet\Authentication\SAC\x32\ClassicClientPKCS11.dll`

The absolute path (x32 or x64) for loaded PKCS11 modules are listed in the `RouterLibs` registry key under:
`HKEY_LOCAL_MACHINE\SOFTWARE\Gemplus\Cryptography\Pkcs11\Multiplexer`

or under:
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Gemplus\Cryptography\Pkcs11\Multiplexer` for x32 applications on x64 platforms.

- **On x64 platforms:**
  The following dll path: `C:\Program Files\Gemalto\Classic Client\BIN\gck2015x.dll`
  is replaced with:
  `C:\Program Files\SafeNet\Authentication\SAC\x64\ClassicClientPKCS11.dll`
  and the path to the IDPrime PKCS11 module:
  `C:\Program Files (x86)\Gemalto\IDGo 800 PKCS#11\IDPrimePKCS1164.dll`
  was added to support IDPrime cards in the future.

- **On x32 platforms:**
  The following dll path: `C:\Program Files(x86)\Gemalto\Classic Client\BIN\gck2015x.dll` is replaced with:
  `C:\Program Files\SafeNet\Authentication\SAC\x32\ClassicClientPKCS11.dll`
  and the path to the ID Prime PKCS11 module:
  `C:\Program Files (x86)\Gemalto\IDGo 800 PKCS#11\IDPrimePKCS11.dll`
  was added to support IDPrime cards in the future.

NOTE:
For the side-by-side solution to run properly, Classic Client must be installed before the eBanking .msi file is generated using the Customization Tool.
See "eBanking Profile" on page 25

The files listed in the table below are included in the SAC installation:

Folder Contents (.exe, .dll, .reg, .iso files)	Supported Cards	Description
ClassicClientPKCS11.dll	IDClassic 340 (V3)	(Restricted - read only functionality) This is the new implementation that replaces the GCK2015X software module functionality in SAC to support the IDClassic V3 card.
IDPrimePKCS1164.dll IDPrimePKCS11.dll	IDPrime MD	(Full functionality)See "eBanking Profile" on page 25 This is the new implementation that replaces the GCK2015X software module functionality in SAC to support the IDClassic V3 card. This solution enables working with IDPrime cards via the legacy GCLIB interface.

The files listed in the table below are not included in the SAC installation:

Folder Contents (.exe, .dll, .reg, .iso files)	Supported Cards	Description
GCK2014X.dll	legacy Classic Client - IDClassic (V1)	A simple upgrade of the former GemSafe GCLIB Libraries v4.2.x. Allows backward compatibility of Classic Client with cards that use the Classic V1 Applet and also old GPK cards.
GCK2015X.dll	Legacy Classic Client - IDClassic (V2)	(Full functionality) This is the legacy PKCS#11 standard implementation, redesigned to support in particular PKCS#15-compliant smart card mapping. This component is used by the GCLIB.dll to address cards with V2, V3 and IAS ECC Applet. Note: This dll will not be used after the customized eBanking msi installation has been installed.

Installation Configurations

SafeNet Authentication Client can be installed with the following configurations:

Configuration	Description	Installation Steps
Typical SafeNet Authentication Client Installation	Typical - installs the most common application features.	• Install SafeNet Authentication Client. When using the installation wizard, select the **Typical Configuration** option.
Custom SafeNet Authentication Client Installation	Custom - installs only the application features you select.	• Install SafeNet Authentication Client using the installation wizard, and select the **Custom** option.

Installing SafeNet Authentication Client on Windows (MSI)

Use the *SafeNet Authentication Client Installation Wizard* to install the application with its default properties and features.

The components that can be set using the wizard are:

- **Language**: the language in which the SafeNet Authentication Client user interface is displayed
- **Destination folder**: the installation library for this and all future SafeNet authentication product applications
- **Typical:** installs the most common application features.
- **Custom**: installs only the application features you select.

> **NOTE**:
> Ensure that SafeNet Authentication Client applications are closed before upgrading, installing, or uninstalling SafeNet Authentication Client.

To install via the installation wizard:

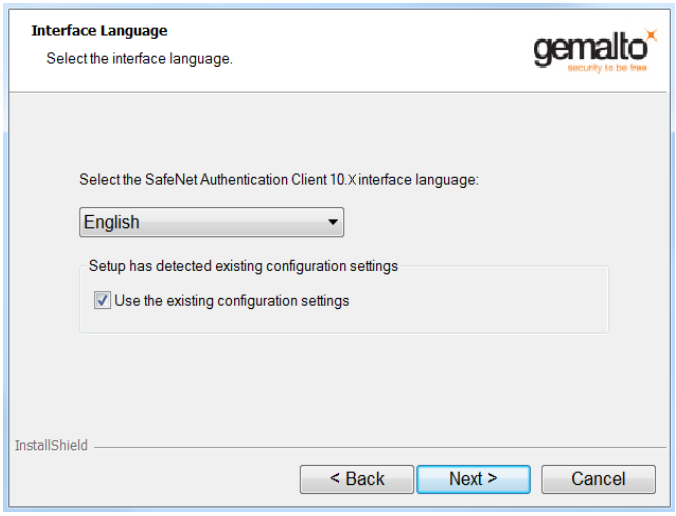
1. Log on as an administrator.
2. Close all applications.
3. Double-click the appropriate file:
   - `SafeNetAuthenticationClient-x32-10.7.msi` (32-bit)
   - `SafeNetAuthenticationClient-x64-10.7.msi` (64-bit)

The **SafeNet Authentication Client Installation Wizard** opens.

4. Click **Next**.

   The Interface Language window is displayed.

> **NOTE**:
> If configuration settings have been saved from a previous SafeNet Authentication Client installation, an option is displayed to use the existing settings.



5. From the dropdown list, select the language in which the SafeNet Authentication Client screens will appear.
6. If configuration settings are detected from a previous version, you can select **Use the existing configuration settings**.

7. Click **Next**.

   The *End-User License Agreement* is displayed.

8. Read the license agreement, and select the option, **I accept the license agreement**.
9. Click **Next**.

   The *Destination Folder* window opens, displaying the default installation folder.

10. You can click **Change** to select a different destination folder, or install the *SAC* application into the default folder:

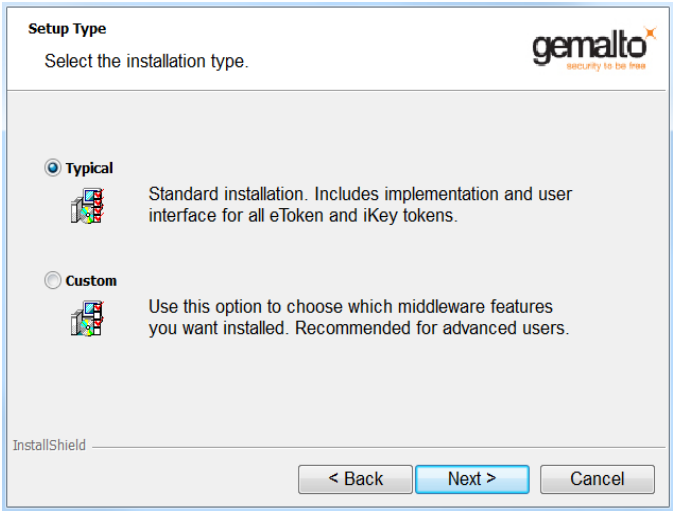
    `C:\Program Files\SafeNet\Authentication\`

> **NOTE**:
> If an application from the SafeNet Authentication line of products, or an eToken legacy product, is already installed, we recommend that the destination folder not be changed.

This folder will be used as the installation library for all future SafeNet Authentication applications.

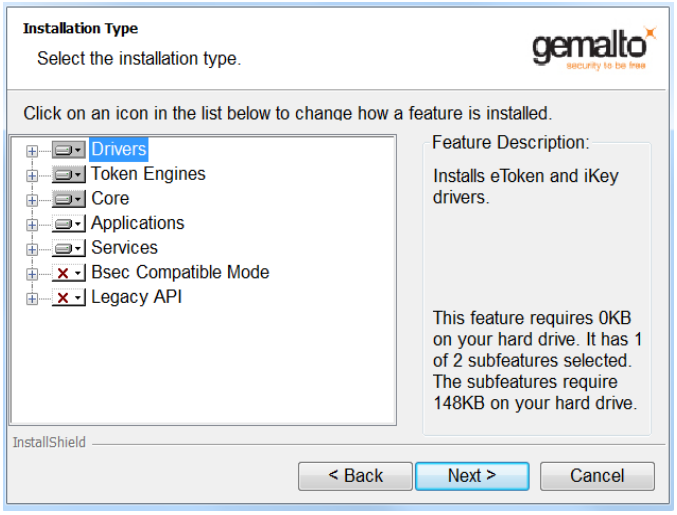
11. Click **Next**.

    The *Setup Type* window opens.



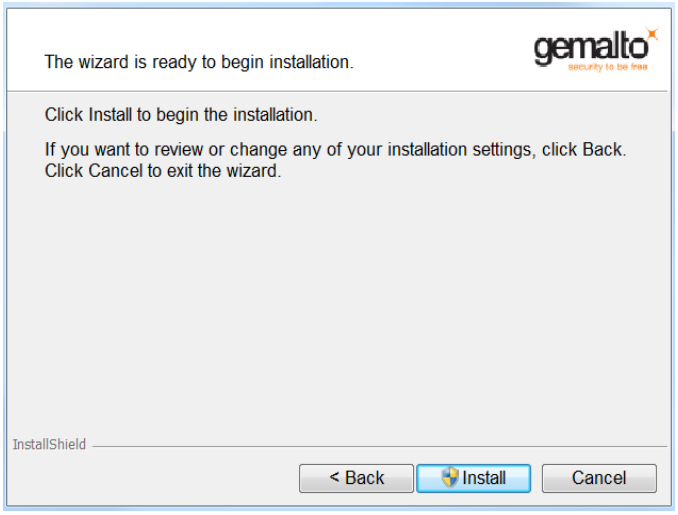
12. Select one of the following:
    - **Typical**: installs the most common application features (recommended)
    - **Custom**: installs only the application features you select.
13. If you select **Custom**, click **Next**.

    The *Custom Installation Type* window opens.



14. Use this window to enable or disable specific features. Some features cannot be disabled, as they are mandatory for the installation.

15. If you select **Typical**, click **Next**, and then click **Install** to proceed with the installation.
    The installation proceeds.



When the installation is complete, a confirmation message is displayed.

16. Click **Finish** to complete the installation.

Installing the MSI file via the Command Line

Command line installation gives the administrator full control of installation properties and features.

The SafeNet Authentication Client command line installation uses the standard Windows Installer `msiexec` syntax:

- for 32-bit systems:
  `msiexec /i SafeNetAuthenticationClient-x32-10.7.msi`
- for 64-bit systems:
  `msiexec /i SafeNetAuthenticationClient-x64-10.7.msi`

> **NOTE**:
> Ensure that SafeNet Authentication Client applications are closed before upgrading, installing, or uninstalling SafeNet Authentication Client.

To install via the command line:

1. Log on as an administrator.
2. Close all applications.
3. To open the *Command Prompt* window, do one of the following, depending on your operating system:
   - From the Windows taskbar, select **Start > Programs > Accessories > Command Prompt**.
   - Right-click **Command Prompt**, select **Run as**, and set the user to administrator.
4. Type the `msiexec` command with the appropriate parameters, properties and feature settings, as described in this chapter.

Installing in Silent Mode

Installing via the command line enables the administrator to define a silent mode installation in addition to optional property settings.

To run the installation in silent mode with no user interface, add **`/qn`** to the end of the `msiexec` command:

```
msiexec /i [msi file] /qn
```

> **NOTE**:
> To display a basic installation user interface, use the /qb parameter.

Setting Application Properties via the Command Line

During a command line installation, the administrator can override the application's default values by including specific properties, and assigning each a value. These new values are saved in `HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC`.
For more information, see Chapter 8: *Application Properties Hierarchy*, on page 68.

Properties can be set during installation only, and not during repair.

To set properties during installation, use the following command format:

- For 32-bit systems:
  ```
  msiexec /i SafeNetAuthenticationClient-x32-10.4 (GA).msi PROPERTY=VALUE
  PROPERTY=VALUE /qb
  ```
- For 64-bit systems:
  ```
  msiexec /i SafeNetAuthenticationClient-x64-10.4 (GA).msi PROPERTY=VALUE
  PROPERTY=VALUE /qb
  ```

where

- `PROPERTY` is the name of a configurable property, often identified by the prefix PROP_
- `VALUE` is the value assigned to the property

See the *Command Line Installation Properties* tableon page 52 for the list of properties that can be set during installation.

Some properties are stored as registry values and can be set or modified after installation. These properties are described in the *General Settings* section on page 72.

Some properties can be set during a command line installation only, and cannot be modified afterwards. These properties are described in the *Installation-Only Properties* sectionon page 53.

> **Example:** To install the Spanish version of SafeNet Authentication Client in a 32-bit system, with the SAC Tools *Advanced* Mode setting disabled, all registry keys to be cleared automatically upon uninstall, and all other properties assigned their default values, type the following command:
>
> ```
> msiexec /i SafeNetAuthenticationClient-x32-10.4 (GA).msi
> ET_LANG_NAME=Spanish
> PROP_ADVANCED_VIEW=0
> PROP_CLEAR_REG=1 /qb
> ```

Command Line Installation Properties

Property	Description
READER_COUNT	on page 54
PROP_FAKEREADER	on page 55
READERS	on page 55
PROP_LICENSE_FILE	on page 55
PROP_REG_FILE	on page 56

Deprecated Command Line Installation Properties

Property	Description
ET_LANG_NAME	on page 53
KSP_ENABLED	on page 54
PROP_ADVANCED_VIEW	on page 85
PROP_CLEAR_REG	on page 54
PROP_EXPLORER_DEFENROL	on page 98
PROP_PCSCSLOTS	on page 74
PROP_PQ_HISTORYSIZE	on page 104
PROP_PQ_MAXAGE	on page 103
PROP_PQ_MINAGE	on page 104
PROP_PQ_MINLEN	on page 103
PROP_PQ_MIXCHARS	on page 105
PROP_PQ_WARNPERIOD	on page 104
PROP_PROPAGATECACER	on page 99
PROP_PROPAGATEUSERCER	on page 99
PROP_SINGLELOGON	on page 72
PROP_SINGLELOGONTO	on page 73
PROP_SOFTWARESLOTS	on page 73
PROP_UPD_INFPATH	on page 56
TARGETDIR	on page 56

Installation-Only Properties

The following properties, unless stated otherwise, can be set during command line installation only, and cannot be modified afterwards:

ET_LANG_NAME Property

Property Name	ET_LANG_NAME
Description	Determines the language in which the GUI is displayed
Value	Chinese / Czech / English / French (Canada) / French / German / Hungarian / Italian / Japanese / Korean / Lithuanian / Polish / Portuguese / Romanian / Russian / Spanish / Thai / Traditional Chinese / Vietnamese / Turkish **Note:** Values that consist of two words (*Traditional Chinese* and *French (Canada)*), must be enclosed in double quotes.
Default	English

KSP_ENABLED Property

NOTE:
This feature can also be set using SafeNet Authentication Client Tools, Property Settings (ADM), or registry key.

Property Name	KSP_ENABLED
Description	Determines if KSP is installed
Value	0 - KSP is not installed 1 - KSP is installed and used as the default cryptographic provider on Windows Vista or higher 2 - KSP is installed but the certificate's provider details stored on the token are used. These are the details displayed when the certificate is selected in SAC Tools.
Default	2

PROP_CLEAR_REG Property

Property Name	PROP_CLEAR_REG
Description	Determines if all registry settings are automatically cleared upon uninstall
Value	1 (True) - Registry settings are cleared upon uninstall 0 (False)- Registry settings are not cleared upon uninstall
Default	0 (False)

READER_COUNT Property

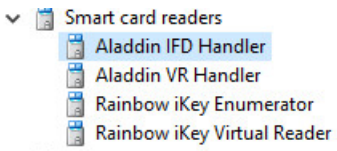
NOTE:
This feature can also be set using SafeNet Authentication Client Tools.

Property Name	READER_COUNT
Description	Determines the number of virtual readers for physical eToken devices only. This determines the number of eToken devices that can be connected concurrently. **Note:** On Windows Vista 64-bit and on systems later than Windows 7 and Window 2008 R2, the total number of readers is limited to 10 from among: iKey readers, eToken readers, third-party readers, and reader emulations.
Value	0 - No virtual readers installed 1 - 16 - Number of virtual readers installed
Default	2

PROP_FAKEREADER Property

Property Name	PROP_FAKEREADER
Description	Determines if the emulation of a smartcard reader is installed, enabling SafeNet Virtual Tokens to be used with applications requiring a smartcard reader, such as smartcard logon and VPN. **Note:** On Windows Vista 64-bit and on systems later than Windows 7 and Window 2008 R2, the total number of readers is limited to 10 from among: iKey readers, eToken readers, third-party readers, and reader emulations.
Value	1 (True) - Emulation of a smartcard reader is installed 0 (False)- Emulation of a smartcard reader is not installed 128 - No virtual readers
Default	1 (True)

READERS Property

Property Name	READERS
Description	Determines the number of virtual readers for physical iKey devices only. This determines the number of iKey devices that can be connected concurrently. **Note:** On Windows Vista 64-bit and on systems later than Windows 7 and Window 2008 R2, the total number of readers is limited to 10 from among: iKey readers, eToken readers, third-party readers, and reader emulations. **For example:** Following command line is enough if you want to change readers counters properties (and any additional properties): C:\Windows\system32>msiexec /i "c:\temp\SafeNetAuthenticationClient-x32-10.7.msi" READER_COUNT=1 READERS=1 /qb 
Value	0 - No virtual readers are installed 1 - 16 - Number of virtual readers installed
Default	2

PROP_LICENSE_FILE Property

Property Name	PROP_LICENSE_FILE
Description	Defines the location of the SAC license file
Value	The path to a file containing the SafeNet Authentication Client license **Note:** The full path must be used.
Default	none

PROP_REG_FILE Property

Property Name	PROP_REG_FILE
Description	Defines the BSec settings .reg file, created manually, that is imported to the computer's registry folder during the installation The default registry folder is HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC
Value	The path to a saved registry file **Note:** The full path must be used.
Default	none

NOTE:
While other command line installation properties set values only in HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC, values set in the PROP_REG_FILE file are appended to the sub folders of the registry location.

PROP_UPD_INFPATH Property

Property Name	PROP_UPD_INFPATH
Description	Determines the update driver search path on install/uninstall
Value	The update driver search path on install/uninstall
Default	none

TARGETDIR Property

Property Name	TARGETDIR
Description	Determines which installation folder to use as the installation library for this and all future SafeNet Authentication application installations. Use only if there are no other SafeNet Authentication or legacy eToken applications installed.
Value	The path to the installation library
Default	None - the application is installed in the default SafeNet Authentication installation folder

NOTE:
Include the TARGETDIR property only if there are no other SafeNet Authentication applications or legacy eToken applications installed on the computer.

Configuring Installation Features via the Command Line

To exclude specific features from the SafeNet Authentication Client installation, use the `ADDDEFAULT` parameter to install only those features required. The excluded features can be added afterwards to the installed application.

To install only specific features, use the following command format:

```
msiexec /i SafeNetAuthenticationClient-x32-10.4 (GA).msi ADDDEFAULT=F1,F2…Fn
INSTALLLEVEL=n PROP_IKEYREADERCOUNT=n /qb
```

where

- `SafeNetAuthenticationClient-x32-10.7` is the 32-bit SafeNet Authentication Client installation file. For 64-bit systems, use `SafeNetAuthenticationClient-x64-10.7.msi`.
- `ADDDEFAULT` indicates that only the following features are included in the installation, or added to the installed application.
- `Fx` is the name of each feature to be included.
- `INSTALLLEVEL` indicates the installation level, where `n` is:
  - 3: standard installation (default)

NOTE:
The number of iKey readers can be set from the command line only.

SafeNet Authentication Client Command Line Feature Names

Feature Parent Name	Command Line Feature Name	Description
DriverFeature	eTokenDrivers	Installs etoken drivers.
	BsecDrivers	Installs iKey drivers.
CoreFeature	CAPI: eTokenCAPI IDPrimeCAPI	Installs the standard CAPI implementation for eToken, iKey and Gemalto IDPrime devices. Installs the standard CAPI implementation for eToken and iKey devices. Installs the standard CAPI implementation for Gemalto IDPrime devices.
	eTokenPKCS11	Installs the standard PKCS#11 API implementation for eToken and iKey devices. **Note:** This feature is mandatory.
	UIDialogs	Installs support for CAPI password dialogs. **Note:** This feature is mandatory.
	KSP: CNG IDPrimeKSP	Registers SafeNet Key Storage Provider. Registers eToken and iKey devices for SafeNet Key Storage Provider (KSP). Registers Gemalto IDPrime devices for SafeNet Key Storage Provider (KSP).
Applications	SACTools	Installs the SAC Tools application for managing devices.
Services	SACService	Installs eToken Service for the support of eToken and iKey devices. **Note:** This feature is mandatory.
	SACMonitor	Installs SafeNet Authentication Client Monitor (Tray icon). **Note:** This feature is mandatory.
LegacyAPI	eTokenSAPI	Installs proprietary supplementary API.
TokenEngines	eTokenDevices: eTokenJava eTokenCardOS	Support for JAVA and CardOS devices. Support for Java devices. Support for CardOS devices. **Note:** the eToken Java feature is mandatory.
	iKey	Installs iKey token support.
	eTokenVirtual	Support for SafeNet Virtual Tokens.
	IDPrime	Support for IDPrime devices.

Feature Parent Name	Command Line Feature Name	Description
IDGoCompatibleMode	IDGoMinidriver	Installs legacy IDGo 800 Minidriver.
	IDGoPKCS11	Support for legacy IDGo 800 PKCS#11 applications.

NOTE:
To enable SafeNet token support without installing SafeNet Authentication Client Tools, use the SafeNet Authentication Client command line installation with eTokenDrivers and/or BsecDrivers only.

Installing All Features - Example

To install SafeNet Authentication Client on a 32-bit system with all features, type the following command:

```
msiexec /i SafeNetAuthenticationClient-x32-10.4 (GA).msi
```

ADDDEFAULT=eTokenDrivers,BsecDrivers,eTokenCAPI,eTokenPKCS11,UIDialogs,KSP,SACTools,SACService,SACMonitor,BsecCAPI,BsecPKCS11,eTokenSAPI,eTokenJava,eTokenCardOS,iKey,eTokenVirtual,IDPrime,IDPrimeCAPI,IDPrimeKSP /qb

Installing All Features Except KSP Support - Example

To install SafeNet Authentication Client on a 32-bit system with all features except support for KSP, type the following command:

```
msiexec /i SafeNetAuthenticationClient-x32-10.4 (GA).msi KSP_Enabled=0 /qb
```

Installing Specific Readers - Example

To install SafeNet Authentication Client on a 64-bit system with five eToken readers, three iKey readers, two SafeNet Virtual Token readers, and no smartcard reader emulation, type the following command:

msiexec /i `SafeNetAuthenticationClient-x64-10.4 (GA).msi PROP_PCSCSLOTS=10 PROP_ETOKENREADERCOUNT=5 PROP_IKEYREADERCOUNT=3 PROP_SOFTWARESLOTS=2 PROP_FAKEREADER=0 /qb`

Installing without eToken Drivers - Example

To install SafeNet Authentication Client without support for eToken devices on a 32-bit system, type the following command:

```
msiexec /i SafeNetAuthenticationClient-x32-10.4 (GA).msi ADDDEFAULT=

BsecDrivers,eTokenSAPI,eTokenPKCS11,IDPrime,IDPrimePKCS11,IDPrimeCAPI,eTokenCAPI,UIDialogs,SACMonitor,SACService,SACTools /qb
```

Any of the optional features in this example can be excluded.

Installing without SAC Tools - Example

To install SafeNet Authentication Client on a 32-bit system, with many standard features, but without the SafeNet Authentication Client Tools application, type the following command:

```
msiexec /i SafeNetAuthenticationClient-x32-10.4 (GA).msi ADDDEFAULT=
eTokenDrivers,BsecDrivers,eTokenSAPI,eTokenPKCS11,IDPrime,IDPrimePKCS11,IDPrimeCAPI,e
TokenCAPI,KSP,UIDialogs,SACMonitor,SACService /qb
```

To add the SafeNet Authentication Client Tools application to SafeNet Authentication Client on a 32-bit system after installation, type the following command:

```
msiexec /i SafeNetAuthenticationClient-x32-10.4 (GA).msi ADDDEFAULT=SACTools /qb
```

Removing Features via the Command Line

Installed features can be removed from the SafeNet Authentication Client installation. To remove features, use the following format:

```
msiexec /x SafeNetAuthenticationClient-x32-10.4 (GA).msi REMOVE=F1,F2…,Fn /qb
```

where

- `SafeNetAuthenticationClient-x32-10.4 (GA).msi` is the 32-bit SafeNet Authentication Client installation file. For 64-bit systems, use `SafeNetAuthenticationClient-x64-10.4 (GA).msi`
- `REMOVE` indicates that the following features are to be removed
- `F`x is the name of each feature to be removed

NOTE:
Only optional features can be removed. Mandatory fields cannot be removed.

Example: To remove the SafeNet Authentication Client Tools application after it was installed with SafeNet Authentication Client on a 32-bit system, type the following command:

```
msiexec /x SafeNetAuthenticationClient-x32-10.4 (GA).msi
REMOVE=SACTools /qb
```

Uninstall

After SafeNet Authentication Client 10.7 has been installed, it can be uninstalled. Local administrator rights are required to uninstall SafeNet Authentication Client. When SafeNet Authentication Client is uninstalled, user configuration and policy files may be deleted.

Uninstall Overview

If a device remains connected while SafeNet Authentication Client is being uninstalled, you will be prompted to remove the device before uninstalling the driver.

Use the Windows Control Panel *Add and Remove Programs* feature to uninstall the driver.

To remove SafeNet Authentication Client, use one of the following methods:

- *Uninstalling via Add or Remove Programs* on page 61
- *Uninstalling via the Command Line* on page 62

NOTE:
- If a DLL is in use by another application, a *Files in Use* message is displayed. Click **Ignore** to continue the uninstall, and when the uninstall completes, restart the computer.
- If the PROP_CLEAR_REG property was enabled when SafeNet Authentication Client was installed, all machine and user registry settings are automatically cleared during the uninstall.

Uninstalling via Add or Remove Programs

To uninstall via *Add or Remove Programs*:

1. From the Windows taskbar, select **Start > Settings > Control Panel.**
2. Double-click **Add or Remove Programs**.
3. Select **SafeNet Authentication Client 10.7** and click **Remove**.
4. Follow the instructions to remove the application.

   If the PROP_CLEAR_REG property was not enabled during installation, a *Save settings* window is displayed.
5. Click **Yes** to save the machine and user registry settings, or **No** to delete them.

   The uninstall process proceeds.

Uninstalling via the Command Line

If the PROP_CLEAR_REG property is not enabled, the registry settings are retained during uninstall via the command line.

To uninstall via the command line:

1. Log on as an administrator.
2. Close all applications.
3. From the Windows taskbar, select **Start > Programs > Accessories > Command Prompt**.
   Right-click **Command Prompt**, and select **Run as Administrator**.
4. Type the appropriate command line utility:
   `msiexec /x SafeNetAuthenticationClient-x32-10.7.msi` (for 32-bit installations)
   `msiexec /x SafeNetAuthenticationClient-x32-10.7.msi` (for 64-bit installations)
   To uninstall in silent mode, add `/qn` to the end of the command.
5. When the uninstall completes, restart the computer.

SafeNet Authentication Client Settings

SafeNet Authentication Client settings are policy settings that are stored in a Windows Administrative Template (ADM or ADMX) file, and can be edited using Windows tools. When edited on the server, the settings can be propagated to client computers.

SafeNet Authentication Client Settings Overview

Administrative Template files are used to display registry-based SafeNet Authentication Client policy settings for editing by the administrator.

Sample Administrative Template files are provided by SafeNet in the SafeNet Authentication Client software package.

Sample Administrative Template files provided by SafeNet:

Sample File	Configuration
SAC_[Major_Minor].adm	SafeNet Authentication Client settings
SAC_[Major_Minor].admx	SafeNet Authentication Client settings
SAC_[Major_Minor].adml	File of English strings

Use the Active Directory *Group Policy Object Editor (GPO)* to configure the Administrative Template ADM and ADMX files.

When configured on a client, SafeNet Authentication Client settings apply to the local computer only.

When configured on a server, SafeNet Authentication Client settings can be set to be propagated to the entire domain, or to apply to the domain controllers only.

The sample Administrative Template files provided by SafeNet are configured to write registry settings to:
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SafeNet\Authentication\SAC`

The values in this folder have a higher priority than values in any other registry folder. See "Application Properties Hierarchy" on page 68 for an explanation of the registry folders.

To write settings to a different registry folder, modify the Administrative Template file.

NOTE: •

- When setting the Microsoft GPO parameter **ForceReadingAllCertificates** to 'Enabled' or 'Not Configured', all smart card logon certificates are visible on the operating system log on screen.
- When setting the Microsoft GPO parameter **ForceReadingAllCertificates** to 'Disabled', only the default smart card logon certificates is visible on the operating system log on screen.

Adding SafeNet Authentication Client Settings

Add the Administrative Templates snap-in to enable you to modify the SafeNet Authentication Client settings.

To add the Administrative Templates to a client computer, see *Adding an ADM file to a Client Computer* on page 65.

Configuring SAC Password Prompt Settings

You can configure SAC logon settings to request a password prompt on every cryptographic operation performed.

To activate the password prompt request whenever a cryptographic API (CAPI) operation is required, ensure either one of the following parameters exist:

- Ensure the certificate you are using includes a **Non Repudiation OID** (generated via Entrust). See "General Settings" on page 72 for more details on the Non Repudiation OIDs setting.
- Ensure the certificate you are using includes an **Identity OID**. See "IdenTrust Settings" on page 118 for more details on the Identity OIDs setting.
- Open **SAC tools>Advanced View>Token Settings>Advanced Tab**, and set the **RSA key secondary authentication** parameter to **Token authentication on application request**.
- **Logout Mode** setting is **True**.

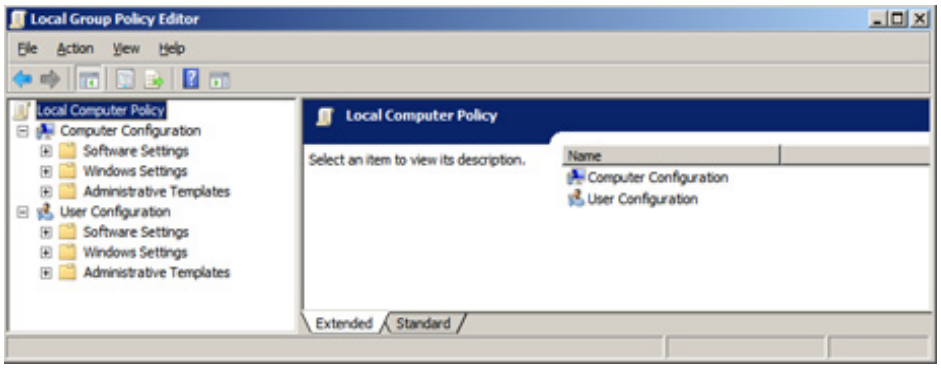
Adding an ADM file to a Client Computer

You can add ADM files to Windows 7, 8, 8.1, and 10. When configured on a client, SafeNet Authentication Client settings apply to the local computer only.

To add SafeNet Authentication Client settings:

1. From the Windows taskbar, select **Start > Run**.
2. In the *Run* dialog box, enter **gpedit.msc**, and click **OK**.

   The *Local Group Policy Editor* opens.



3. Under the **Computer Configuration** node, right-click **Administrative Templates**, and select **Add/Remove Templates.**

   The *Add/Remove Templates* window opens.

4. Click **Add**, and browse to the appropriate ADM file.

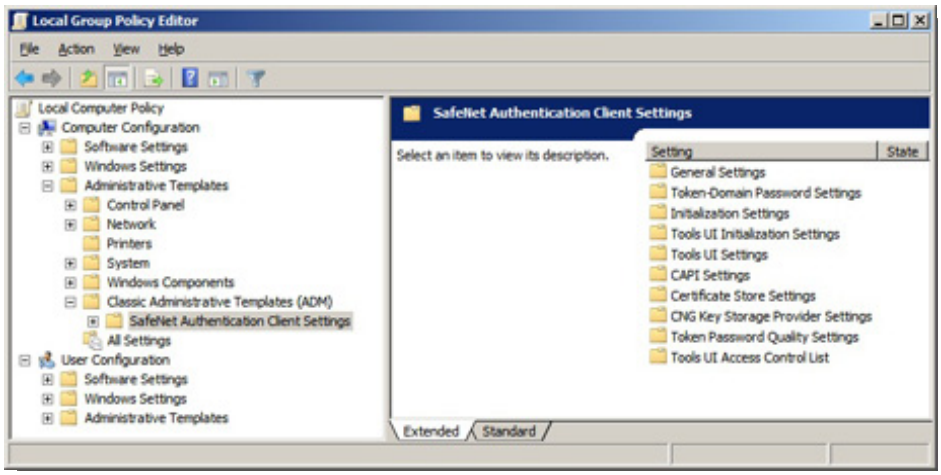
   Sample files are included in the SafeNet Authentication Client software package provided by SafeNet.

5. Select the file, and click **Open.**

   The selected template file is displayed in the *Add/Remove Templates* window.

6. Click **Close.**

   In the *Local Group Policy Editor* window, the *Settings* node is added under **Administrative Templates > Classic Administrative Templates (ADM)**.



Editing SafeNet Authentication Client Settings

Each SafeNet Authentication Client *Settings* folder contains settings that can be configured to have priority over the SafeNet Authentication Client application defaults.

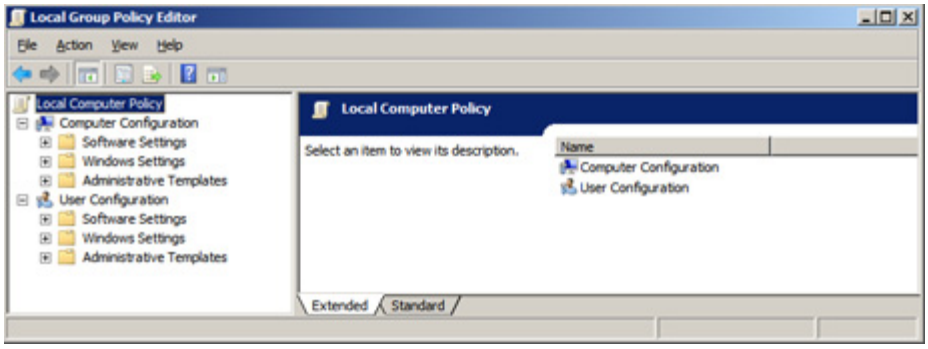
When you edit the settings, values in the registry key are changed. For more information, see *Configuration Properties* on page 68.

Editing Settings on a Client Computer

To edit SafeNet Authentication Client settings:

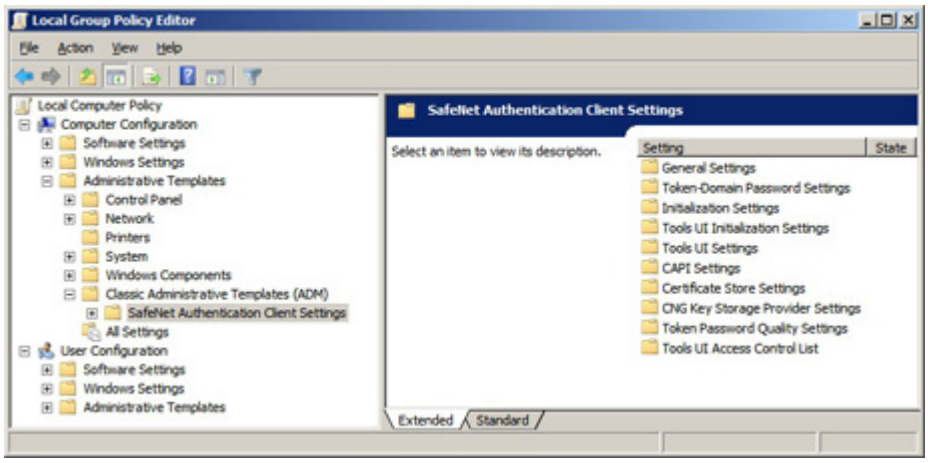
1. From the Windows taskbar, select **Start > Run**.
2. In the *Run* dialog box, enter **gpedit.msc**, and click **OK**.

   The *Local Group Policy Editor* opens.



3. In the left pane, navigate to **Computer Configuration > Administrative Templates > Classic Administrative Templates**.
4. Select one of the **SafeNet Authentication Client Settings** nodes.

   The settings are displayed in the right pane.



Deploying SafeNet Authentication Client Settings

After editing the SafeNet Authentication Client settings on the server, update the registry settings on the server and on all client computers on which SafeNet Authentication Client is installed.

To apply SafeNet Authentication Client settings:

1. From the Windows taskbar, select **Start > Run**.
2. In the *Run* dialog box, enter **gpupdate**, and click **OK**.

   The registry values on the server are updated to the *SafeNet Authentication Client Settings* values.
3. On each client computer's Windows taskbar, select **Start > Run**.
4. In the *Run* dialog box, enter **gpupdate**, and click **OK**.

   The registry values are copied from the server to the client computer.

Configuration Properties

SafeNet Authentication Client properties are stored on the computer as registry key values which can be added and changed to determine SafeNet Authentication Client behavior. Depending on where a registry key value is written, it will apply globally, or be limited to a specific user or application.

Setting SafeNet Authentication Client Properties

Depending on the property, registry key values can be set using at least one of the following methods:

- Define the property during command line installation of SafeNet Authentication Client (but not during repair). See "Installing the MSI file via the Command Line" on page 51.
  The property name, and not the registry value name, is needed when setting the value during command line installation.
- Set a value using the SafeNet Authentication Client Tools application.
  See the *SafeNet Authentication Client User's Guide*.
  Neither the registry value name nor the property name is needed.

NOTE:
Values set using the SafeNet Authentication Client Tools application are saved on a per user basis in HKEY_CURRENT_USER, and not in HKEY_LOCAL_MACHINE.

- Set a value using the Administrator Templates (ADM/ADMX) policy settings.
  See Chapter 7: *SafeNet Authentication Client Settings*, on page 63.
  The registry value name, and not the property name, is needed when setting the value.
- Manually edit the registry setting.
  See *Setting Registry Keys Manually* on page 70.
  The registry value name, and not the property name, is needed when setting the value.

NOTE:
- All properties can be manually set and edited.
- It is recommended to set the policies using the Administrator Templates (ADM/ADMX) policy settings. This option allows spreading policies in a controlled manner and ensures that end users are not able to override any policies. For more information, refer to the section below: Application Properties Hierarchy.

Application Properties Hierarchy

Each property can be defined in up to four registry key folders. For each property, the setting found in the highest level of the hierarchy determines the application's behavior.

If a property is set in a folder which requires administrator permissions, that setting overrides any other settings for that property.

Hierarchy List

SafeNet Authentication Client uses the following hierarchy to determine the application's behavior:

1. `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SafeNet\Authentication\SAC`
   Requires administrator permissions.
2. `HKEY_CURRENT_USER\SOFTWARE\Policies\SafeNet\Authentication\SAC`
   Requires administrator permissions.
3. `HKEY_CURRENT_USER\SOFTWARE\SafeNet\Authentication\SAC`
   Does not require administrator permissions.
4. `HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC`
   Requires administrator permissions.
5. SafeNet Authentication Client default value

Hierarchy Implications

The applications properties hierarchy has the following implications:

- When you use the sample Administrative Template (ADM/ADMX) files supplied by SafeNet to edit *SafeNet Authentication Client Settings*, the edited properties are written to: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SafeNet\Authentication\SAC`.
  These values override values set by any other method.
- When you set properties using *SafeNet Authentication Client Tools*, the edited properties are written to: `HKEY_CURRENT_USER\SOFTWARE\SafeNet\Authentication\SAC`.
  These values override values set during command line installation. Since Tools settings apply "per user" only after the user is authenticated, the user must first log on to Windows before these settings take effect.
- When you set properties during command line installation, the properties (except for `PROP_REG_FILE`) are written to: `HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC`.
- When you set properties manually, write them to their appropriate registry keys in any of the registry folders listed in the *Hierarchy List* on page 69. Unless the properties must override other settings, we recommend writing them to: `HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC`.

Setting Registry Keys Manually

To set a registry key value:

1. From the Windows taskbar, select **Start > Run**.
2. In the *Run* dialog box, enter **regedit**, and click **OK**.

   The *Registry Editor* opens, displaying the registry folders tree in the left pane.
3. Expand the tree, and select the folder of the required registry key.

   Unless the properties must override other settings, we recommend writing them to: HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC.
4. If a property's folder does not exist in the Registry Editor tree, create it.

   The names and settings of the values in the registry key are displayed in the right pane.

   The registry value name, and not the property name, is used when setting the value manually.
5. To rename or delete a value, or to modify its data, right-click its Name.
6. Registry settings that are not displayed in the right pane can be added.

   To add a value to the registry key, or to add a new registry key in the tree, right-click the white space in the right pane.

Defining a Per Process Property

You can set properties to be limited to specific applications. To do this, open the registry key in which the property belongs, create a registry folder within it, and assign the new folder the full name of the process. Then define the appropriate settings within the process's folder.

In the following example, the Single Logon feature is defined for the Internet Explorer process only. It will not apply to any other process.

To define a per process property, such as Single Logon for IE only:

1. From the Windows taskbar, select **Start > Run**.
2. In the *Run* dialog box, enter **regedit**, and click **OK**.

   The *Registry Editor* opens, displaying the registry folders tree in the left pane.
3. Expand the appropriate registry tree.
   In this example, the tree is `HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC\`
4. Ensure that a folder exists in which the property belongs.
   In this example, the property must be written to the *General* folder.
   If the *General* folder does not exist, right-click **SAC**, select **New > Key**, and assign it the name **General**.
5. Right-click the folder in which the property belongs.
   In this example, right-click the *General* folder.
6. If a new registry key is required, select **New > Key**, and assign it the name of the process.
   In this example, **IEXPLORE.EXE**.

To define a per process property, such as Password Timeout for a certain CAPI process:

1. From the Windows taskbar, select **Start > Run**.

2. In the *Run* dialog box, enter **regedit**, and click **OK**.

   The *Registry Editor* opens, displaying the registry folders tree in the left pane.

3. Expand the appropriate registry tree.
   In this example, the tree is
   `HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC\CAPI\[Process Name e.g. AcroRd32.exe]`

NOTE:
The example below explains how to integrate between two registry processes.

The Single Logon feature can be defined for both the Internet Explorer process as well as for the Adobe Password Timeout process. To perform this, define the following configurations:

[HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC\CAPI\AcroRd32.exe]
"PasswordTimeout"=dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC\General\IEXPLORE.EXE]
"Singlelogon"=dword:00000001

AcroRd32.exe can be replaced by any other CAPI process.

General Settings

The following settings are written to the appropriate folder's `SafeNet\Authentication\SAC\General` registry key.

Description	ADM File Setting	Registry Value	Command Line
Single Logon Determines if the user's Token Password is requested only once for applications using MS cryptography (CAPI, eToken Base Cryptographic Provider, SafeNet Smart Card Key Storage Provider and PKCS#11). **Note:** • Can be set in SafeNet Authentication Client Tools, but since Tools settings apply "per user" only after the user is authenticated, the user must first log on to Windows, and only the next Token Password entry will be saved. • Single Logon For PKCS#11: Determines if the user's Token Password is requested only once for applications using PKCS#11 cryptography. • To force Single Logon to start from Windows Logon, define this setting in HKEY_LOCAL_MACHINE • PKCS11 is also supported for SAC login windows only. This can be achieved only when the PKCS11 function C_Login is configured with PIN=Null. • SingleLogon is not supported when using PIN Pad readers. • As of SAC 10.6, the Single Logon feature is also supported for SafeNet Minidriver (10.2 and above) users when installed with SAC Service via the SAC Customization Tool (SafeNet Minidriver profile). For more information see the chapter: *Customization* on page 21.	**Setting name:** Single Logon **Values:** **0** - Token Password is requested as needed **1** - Token Password is requested only once for applications using MS cryptography. **2** - Token Password is requested only once for applications using MS and PKCS#11 cryptography **Default**: **0**	**Registry Value Name:** SingleLogon **Values:** **0** - Token Password is requested as needed **1** - Token Password is requested only once for applications using MS cryptography. **2** - Token Password is requested only once for applications using MS and PKCS#11 cryptography **Default: 0**	**Property name:** PROP_SINGLELOGON

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
Single Logon Timeout Determines the timeout, in seconds, of a single logon. **Note:** • Applies only when Single Logon is **True**. • Applies to all connected tokens and affects all applications using these tokens. • If the Single Logon Timeout value is > 0, Single Logon for CAPI/CNG is selected automatically.	Single Logon Timeout is set in the Single Logon setting. (See “Single Logon” entry above.)	**Registry Value Name:** SingleLogonTimeout **Value**: >=0 (Seconds) **Default**: 0 (no timeout)	**Property name:** PROP_SINGLELOGONTO
Software Slots Defines the number of virtual readers for SafeNet Virtual Tokens. **Note:** Can be modified in ‘Reader Settings’ in SafeNet Authentication Client Tools also. On Windows Vista 64-bit and on systems later than Windows 7 and Window 2008 R2, the total number of readers is limited to 10 from among: iKey readers, eToken readers, third-party readers, and reader emulations.	**Setting name:** Software Slots **Values**: >=0 (0 = SafeNet Virtual Token is disabled; only physical tokens are enabled) **Default**: 2	**Registry Value Name:** SoftwareSlots **Values**: >=0 (0 = SafeNet Virtual Token is disabled; only physical tokens are enabled) **Default**: 2	**Property name:** PROP_SOFTWARESLOTS

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
PCSC Slots Defines the total number of PC/SC slots for all USB tokens and smartcards. Included in this total: • the number of allocated readers for third-party providers • the number of allocated iKey readers, which is defined during installation and cannot be changed • the number of allocated readers for other SafeNet physical tokens, which can be modified in 'Reader Settings' in SafeNet Authentication Client Tools **Note:** .No more than 10 physical tokens can be connected to Windows 64-bit systems.	**Setting name:** PCSC Slots **Values**: >=0 (0 = Physical tokens are disabled; only SafeNet Virtual Tokens are enabled) **Default**: 8	**Registry Value Name:** PcscSlots **Values**: >=0 (0 = Physical tokens are disabled; only SafeNet Virtual Token is enabled) **Default**: 8	**Property name:** PROP_PCSCSLOTS
Legacy Manufacturer Name Determines if 'Aladdin Knowledge Systems Ltd.' is written as the manufacturer name in token and token slot descriptions. Use for legacy compatibility only.	**Setting name:** Legacy Manufacturer Name Values: **Selected** - The legacy manufacturer name is written **Not selected** - The new manufacturer name is written **Default**: Not selected	**Registry Value Name:** LegacyManufacturerName Values: **1** - The legacy manufacturer name is written **0** - The new manufacturer name is written **Default**: 0	Cannot be set by command line installation.
Enable Private Cache Determines if SafeNet Authentication Client allows the token's private data to be cached. Applies only to tokens that were initialized with the private data cache setting. The private data is cached in per process memory. **Note:** Can be set in SafeNet Authentication Client Tools	**Setting name:** Enable Private Cache Values: **Selected** - Private data caching is enabled **Not selected** - Private data caching is disabled **Default**: Selected	**Registry Value Name:** EnablePrvCache **Values**: **1 (True)** - Private data caching is enabled **0 (False)** - Private data caching is disabled **Default**:1 (True)	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
Tolerate Finalize Determines if C_Finalize can be called by DllMain **Note:** Define this property per process Select this setting when using Novell Modular Authentication Service (NMAS) applications only	**Setting name:** Tolerate Finalize Values: **Selected** - C_Finalize can be called by DllMain **Not selected** - C_Finalize cannot be called by DllMain **Default**: Not selected	**Registry Value Name:** TolerantFinalize **Values**: **1 (True)** - C_Finalize can be called by DllMain **0 (False)** - C_Finalize cannot be called by DllMain **Default**: 0 (False)	Cannot be set by command line installation
Tolerate X509 Attributes Determines if CKA_SERIAL_NUMBER, CKA_SUBJECT, and CKA_ISSUER attributes can differ from those in CKA_VALUE during certificate creation **Note:** Enable TolerantX509Attributes when using certificates created in a non- DER encoded binary x.509 format. In some versions of eToken PKI Client, this setting was not selected by default.	**Setting name:** Tolerate X509 Attributes Values: **Selected** - The attributes can differ **Not selected**- Check that the values match **Default**: Not selected	**Registry Value Name:** TolerantX509Attributes **Values**: **1 (True)** - The attributes can differ **0 (False**) - Check that the values match **Default**: 0 (False)	Cannot be set by command line installation
Tolerate Find Templates Determines if PKCS#11 tolerates a Find function with an invalid template, returning an empty list instead of an error.	**Setting name:** Tolerate Find Templates Values: **Selected** - A Find function with an invalid template is tolerated and returns an empty list **Not Selected** - A Find function with an invalid template is not tolerated and returns an error **Default**: Not selected	**Registry Value Name:** TolerantFindObjects **Values**: **1 (True)** - A Find function with an invalid template is tolerated and returns an empty list **0 (False)** - A Find function with an invalid template is not tolerated and returns an error **Default**: 0 (False)	Cannot be set by command line installation

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
Disconnect eToken Virtual Token on Logoff Determines if eToken Virtual tokens are disconnected when the user logs off.	**Setting name:** Disconnect SafeNet Virtual Token on Logoff Values: **Selected** - Disconnect eToken Virtual when logging off **Not selected** - Do not disconnect eToken Virtual Token when logging off **Default**: Not selected	**Registry Value Name:** EtvLogoffUnplug **Values**: **1 (True)** - Disconnect eToken Virtual when logging off **0 (False)** - Do not disconnect eToken Virtual when logging off **Default**: 0 (False)	Cannot be set by command line installation.
Protect Symmetric Keys Determines if symmetric keys are protected **Note:** If selected, even non-sensitive symmetric keys cannot be extracted	**Setting name:** Protect Symmetric Keys **Values**: **Selected** - Symmetric keys cannot be extracted **Not selected** - Symmetric keys can be extracted **Default**: Not selected	**Registry Value Name:** SensitiveSecret **Values**: **1** - Symmetric keys cannot be extracted **0** - Symmetric keys can be extracted **Default**: 0	Cannot be set by command line installation.
Cache Marker Timeout Determines if SAC Service periodically inspects the cache markers of connected tokens for an indication that token content has changed **Note:** If tokens were initialized as "eToken PKI Client 3.65 compatible" in SafeNet Authentication Client 8.0 and later, set this value to 0 to improve performance.	**Setting name:** Cache Marker Timeout **Values**: **Selected** - Connected tokens' cache markers are periodically inspected **Not selected** - Connected tokens' cache markers are never inspected **Default**: Not Selected	**Registry Value Name:** CacheMarkerTimeout **Values**: **1** - Connected tokens' cache markers are periodically inspected **0** - Connected tokens' cache markers are never inspected **Default**: 0	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
Override Non-Repudiation OIDs Overrides SAC's list of standard certificate OIDs that require a high level of security **Note:** Users must log on to their tokens whenever signing with a certificate defined as non-repudiation. To avoid having to authenticate every time a cryptographic operation is required for certificates containing Entrust certificate OID details, remove the default registration key value.	**Setting name:** Override Non-Repudiation OIDs **Value**: 1.3.6.1.5.5.7.1.3 To add additional OID values of non-repudiation certificates, enter after the existing value separated by commas **Default**: No override	**Registry Value Name:** NonRepudiationOID **Value**: 1.3.6.1.5.5.7.1.3 To add additional OID values of non-repudiation certificates, enter after the existing value separated by commas **Default**: No override	Cannot be set by command line installation.
ITI Certification Mode Enables ITI Certification, which requires the following: • Administrator and User Passwords must be changed at first logon. • If Initialization is performed without changing the Administrator and User Passwords at first logon, the Administrator Password is required for the initialization process. Note: When the ITI Certification Mode property is enabled, the Enable Administrator Password Quality Check property will be disabled.	Not supported	**Registry Value Name:** MustChangeAdmin **Values**: **0**- None **1** - ITI certification mode **2** - Special administrator PIN policy **Default**: 0	Cannot be set by command line installation.
No Pin Pad Determines whether or not the PIN Pad reader is used as a regular smart card reader. SAC UI will require entering user credentials.	Not supported	**Registry Value Name:** NoPinPad **Values:** **0** - Disabled **1** - Enabled **Default:** 0 (Disabled)	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
Full SM Mode Enables/disables the full Security Messaging (SM) mode for IDPrime MD FIPS L2 devices. **Note:** SAC cache must be reset after changing the FullSMMode property. This configuration is for applet 4.3.5 L2 cards only.	Not supported	**Registry Value Name:** FullSMMode **Values:** **0 (False)** - Disabled **1 (True)** - FIPS L2 only **Default:** 0 (Disabled)	Cannot be set by command line installation.
PIN Pad Notify Determines if the Pin Pad notification is displayed as balloon or in a window.	**PIN Pad Notify** Values: Show window Show balloon No notification Default: Show window	**Registry Value Name:** PinPadNotify Values: 0 - Show window 1 - Show balloon 2 - No notification -Default: 0 (Show window)	Cannot be set by command line installation.
Touch Sense Notify Determines if the Touch Sense notification is displayed as balloon or in a window.	**Touch Sense Notify** **Values**: Show window Show balloon No notification **Default**: Show balloon	**Registry Value Name:** TSNotify **Values:** 0 - Show window 1 - Show balloon 2 - No notification **Default**: 1 (Show balloon)	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
Multi-Slot Support Determines if SafeNet Authentication Client is backward compatible with Gemalto PKCS#11 Common Criteria devices (IDPrime MD 840, IDPrime MD 3840 and eToken 5110 CC). The Multi-Slot feature affects only SAC customized in compatible mode via IDPrimePKCS11.dll (i.e. The IDGo 800 PKCS#11) option is selected in the Customization Tool. See Chapter 3: "Installing the SafeNet Authentication Client Customization Tool" on page 28. For more information on Multi-Slots, see the PKCS#11 Digital Signature PIN Authentication section of the SafeNet Authentication Client User Guide. **Note:** Linked Mode is not compatible with the Multi-Slot feature.		**Value Name:** MultiSlotSupport **Values**: **Selected** - Activates this feature **Not Selected** - Normal operation **Default**: Not Selected	Cannot be set by command line installation.
Read Only Mode Prevents deletion of certificates from the Token. **Note:** When a user deletes certificates on a Firefox browser and this property is set to 'Selected', Firefox displays these certificates as deleted when in fact they are not.	Not supported	**Registry Value Name:** ReadOnlyMode **Values:** **0 - Disabled** - any user with the right permission can delete the certificates and their associated keys. **1 - Enabled** - certificates and their associated keys cannot be deleted. **Default**: **0**	Cannot be set by command line installation.
Enable Log Events Enables event viewer messages.	**Setting name:** Enable Log Events **Values:** Selected Not Selected	**Registry Value Name:** EnableLogEvents **Values:** **0 -** Selected **1 -** Not Selected **Default**: 1 (not selected)	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
HID Slots Defines the total number of HID slots for all HID USB tokens.	**Setting name:** HID Slots **Values:**=0, =2, >=0 0 - 5200 token works in VSR mode. 2 = 5200 HID token works in HID mode (2 slots). **Default**: 0	**Registry Value Name:** HIDSlots **Values**: =0, =2, >=0 **Default**: 0	**Property name:** PROP_HIDSLOTS
Ignore Silent Mode Determines if the *Token Logon* window is displayed even when the application calls the CSP/KSP in silent mode.	Not supported	**Registry Value Name:** IgnoreSilentMode **Values**: **1 (True)** - Display the *Token Logon* window even in silent mode **0 (False)** - Respect silent mode **Note:** Set to True when the SafeNet RSA KSP must use SHA-2 to enroll a CA private key to a token **Default**: 0 (False)	Cannot be set by command line installation.
TempDir Determines the path to a folder containing the SafeNet Authentication Client internal services folder (eToken.cache, eToken.HID, eToken.Log, eToken.Lock).	Not supported	**Registry Value Name:** TempDir **Value**: Enter a folder name e.g. C:\windows\temp **Default**: Windows: C:\windows\temp Note: This property is not supported on Linux and Mac	
Unlock Authorization Activates authorization protection for SAC Tools Unlock feature	Not supported	**Registry Value Name:** UnlockAuthorization **Value:** **0** - Do not activate authorization protection **1** - Activate authorization protection **Default**: 0	

Token-Domain Password Settings

The following settings are written to the appropriate folder's `SafeNet\Authentication\SAC\SyncPin` registry key.

Description	ADM File Setting	Registry Value	Command Line
Synchronize with Domain Password Determines if synchronization is enabled between the eToken password and the domain password. **Note**: If the "Smart card is required for interactive logon" flag is enabled in AD, it blocks the option to change the domain password. So changing the token's password via SAC will also fail.	**Setting name:** Synchronize with Domain Password **Values**: Name of the domain (written without a suffix) whose password is synchronized with the Token Password **None** - Password synchronization is not enabled **Default**: None	**Registry Value Name:** Domain **Values**: Name of the domain (written without a suffix) whose password is synchronized with the Token Password **None** - Password synchronization is not enabled **Default**: None	Cannot be set by command line installation.

License Settings

The following settings are written to the appropriate folder's `SafeNet\Authentication\SAC\License` registry key.

Description	ADM File Setting	Registry Value	Command Line
SAC License String Defines the license string issued by SafeNet for product registration	**Setting name:** SAC License String **Values**: License string provided by SafeNet **Default**: None	**Registry Value Name:** License **Values**: License string provided by SafeNet **Default**: None	**Name of related property:** PROP_LICENSE_FILE contains the path to the license string, but not the string itself. See "PROP_LICENSE_FILE" on page 55.

Initialization Settings

The following settings are written to the appropriate folder's `SafeNet\Authentication\SAC\INIT` registry key.

NOTE:
- None of the settings in this section are relevant to IDPrime MD cards, except for the LinkMode setting.
- Properties relevant to end of life tokens and cards can be found in previous versions of the Administrator Guide.

Description	ADM File Setting	Registry Value	Command Line
Maximum Token Password Retries Defines the default number of consecutive failed logon attempts that lock the token.	**Setting Name:** Maximum Token Password Retries **Values**: 1-15 **Default**: 15	**Registry Value Name:** UserMaxRetry **Values**: 1-15 **Default**: 15	Cannot be set by command line installation.
Maximum Administrator Password Retries Defines the default number of consecutive failed administrator logon attempts that lock the token.	**Setting name:** Maximum Administrator Password Retries **Values**: 1-15 **Default**: 15	**Registry Value Name:** AdminMaxRetry **Values**: 1-15 **Default**: 15	Cannot be set by command line installation.
Force SO object on Token	**Setting Name:** Force SO object on Token **Values:** **Selected** - Token is initialized with SO object **Not selected** - Token is initialized without SO object **Default:** Selected	**Registry Value Name:** ForceAdmin **Values**: **1(True)** - Token is initialized with SO object **0 (False)** - Token is initialized without SO object **Default:** 1 (True)	Cannot be set by command line installation
Force User object on Token	**Setting Name:** Force User object on Token **Values:** **Selected** – Token is initialized with User object **Not selected** - Token is initialized without User object **Default:** Selected	**Registry Value Name:** ForceUser **Values:** **1(True) -** Token is initialized with User object **0(False)** - Token is initialized without User object **Default:** 1(True)	Cannot be set by command line installation

Description	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
Default Token Name Defines the default Token Name written to tokens during initialization.	**Setting Name**: Default Token Name **Value**: String **Default**: My Token	**Registry Value Name:** DefaultLabel **Value**: String **Default**: My Token	Cannot be set by command line installation.
API: Keep Token Settings When initializing the token using the SDK, determines if the token is automatically re-initialized with its current settings. **Note:** If selected, this setting overrides all other initialization settings.	**Setting Name:** API: Keep Token Settings Values: **Selected** - Use current token settings **Not selected** - Override current token settings **Default:** Not selected	**Registry Value Name:** KeepTokenInit Values: **1 (True) -** Use current token settings **0 (False) -** Override current token settings **Default**: 0 (False)	Cannot be set by command line installation.
API: Private Data Caching If using an independent API for initialization, and if 'Enable Private Cache' is selected, determines the token's private data cache default behavior.	**Setting Name:** API: Private Data Caching Values: **0 -** Always (fastest); private data is cached when used by an application while the user is logged on to the token, and erased when the token is disconnected. **1 -** While user is logged on; private data is cached when used by an application while the user is logged on to the token, and erased when the user logs off or the token is disconnected. **2 -** Never; private data is not cached. **Default:** 0 (Always)	**Registry Value Name:** PrvCachingMode Values: **0 -** Always 1 - While user is logged on **2 -** Never **Default:** 0 (Always)	Cannot be set by command line installation.
Enable Private Data Caching Modification Determines if the token's Private Data Caching mode can be modified after initialization.	**Setting Name:** Enable Private Data Caching Modification Values: **Selected** -Can be modified **Not selected** -Cannot be modified **Default:** Not selected	**Registry Value Name:** PrvCachingModify Values: **1 (True) -** Can be modified **0 (False) -** Cannot be modified **Default**: 0 (False)	Cannot be set by command line installation.

Description	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
Private Data Caching Mode If 'Enable Private Data Caching Modification' is selected, determines who has rights to modify the token's Private Data Caching mode.	**Setting Name:** Private Data Caching Mode Values: **Admin** -Only the administrator has rights **User** -Only the user has rights **Default:** Admin	**Registry Value Name:** PrvCachingOwner Values: **0** - Admin **1** - User **Default**: 0 (Admin)	Cannot be set by command line installation.
API: RSA Secondary Authentication Mode If using an independent API for initialization, determines the default behavior for protecting RSA private keys on the token.	**Setting Name:** API: RSA Secondary Authentication Mode Values: **Never** -New RSA private keys are not protected with an additional password. **Prompt on application request -**If the key generation application requires key passwords to be created for strong private key protection, new RSA private keys must be protected with an additional password. If the key generation application does not require strong private key protection, new RSA private keys are not protected with an additional password. **Always prompt user -** A prompt appears asking if a new RSA private key is to be protected with an additional password. Always - New RSA private keys must be protected with an additional password. Token authentication on application request - If the key generation application requires key passwords to be created for strong private key protection, new RSA private keys are protected with the Token Password. **Default:** Never	**Registry Value Name:** 2ndAuthMode Values: **0** - Never **1** - Prompt on application request **2 -** Always prompt user 3- Always 4 - Token authentication on application request **Default**: **0** -(Never)	Cannot be set by command line installation.

Description	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
Enable RSA Secondary Authentication Modified Determines if the token's RSA secondary authentication can be modified after initialization.	**Setting Name:** Enable RSA Secondary Authentication Modified Values: **Selected** -Can be modified **Not selected** -Cannot be modified **Default:** Not selected	**Registry Value Name:** 2ndAuthModify Values: **1 (True) -** Can modify **0 (False) -** Cannot modify **Default**: 0 (False)	Cannot be set by command line installation.
Use the same token and administrator passwords for digital signature operations. **Notes:** If LinkMode set to zero or not defined, the SAC Tools UI will not show the Link Mode option. Linked Mode is not compatible with the Multi-Slots feature.	**Setting Name:** IDPrime Common Criteria Linked Mode Values: **Selected** -PUK is derived from the Administrator password and Digital Signature PIN is derived from the Token password **Not selected** -Common Criteria PIN's are not managed **Default:** Not selected	**Registry Value Name:** LinkMode Values: **1 (True) -** Linked **0 (False) -** Unlinked **Default**: 0 (False)	Cannot be set by command line installation.

SafeNet Authentication Client Tools UI Initialization Settings

The following settings are written to the appropriate folder's `SafeNet\Authentication\SAC\AccessControl` registry key.

Description	ADM File Setting	Registry Value	Command Line
Enable Advanced View Button Determines if the Advanced View icon is enabled in SAC Tools	**Setting Name:** Enable Advanced View Button **Values**: **Selected** - Enabled **Not selected** -Disabled **Default**: Selected	**Registry Value Name:** AdvancedView **Values**: **1** - Selected **0** - Not selected **Default**: 1	PROP_ADVANCED_VIEW

The following settings are written to the appropriate folder's `SafeNet\Authentication\SAC\InitApp` registry key.

Description	ADM File Setting	Registry Value	Command Line
Default Token Password Defines the default Token Password	**Setting Name:** Default Token Password **Value**: String **Default**: 1234567890	**Registry Value Name:** DefaultUserPassword **Values**: String **Default**: 1234567890	Cannot be set by command line installation.
Enable Change Password on First Logon Determines if the “Token Password must be changed on first logon” option can be changed by the user in the Token Initialization window. **Note:** This option is selected by default. If the option is de-selected, it can be selected again only by setting the registry key.	**Setting Name:** Enable Change Password on First Logon **Values**: **Selected** - Enabled **Not selected** -Disabled **Default**: Selected	**Registry Value Name:** MustChangePasswordEnabled **Values**: **1** - Selected **0** - Not selected **Default**: 1	Cannot be set by command line installation.
Change Password on First Logon Determines if the *Token Password must be changed on first logon* option is selected by default in the Token Initialization window. **Note:** This option is not supported by iKey.	**Setting Name:** Change Password on First Logon **Values**: Selected Not selected **Default**: Selected	**Registry Value Name:** MustChangePassword **Value**: **1** - Selected **0** - Not selected **Default**: 1	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
Private Data Caching If *Enable Private Cache* is selected, determines the token's private data cache default behavior. **Note:** Can be set in SafeNet Authentication Client Tools. This option is not supported by IDPrime MD cards.	**Setting Name:** Private Data Caching **Values**: **Always -** (fastest) private data is cached when used by an application while the user is logged on to the token, and erased only when the token is disconnected **While user is logged on -** private data is cached when used by an application while the user is logged on to the token, and erased when the user logs off or the token is disconnected **Never** - private data is not cached **Default**: Always	**Registry Value Name:** PrivateDataCaching **Values**: **0 -** (fastest) private data is cached when used by an application while the user is logged on to the token, and erased only when the token is disconnected **1 -** private data is cached when used by an application while the user is logged on to the token, and erased when the user logs off or the token is disconnected **2** - private data is not cached **Default**: 0	Cannot be set by command line installation.
RSA Secondary Authentication Mode Defines the default behavior for protecting RSA private keys on the token **Note:** Can be set in SafeNet Authentication Client Tools. This option is not supported by IDPrime MD cards.	**Setting Name:** RSA Secondary Authentication Mode Values: **Never** - New RSA private keys are not protected with an additional password. **Prompt user on application request** - If the key generation application requires key passwords to be created for strong private key protection, new RSA private keys must be protected with an additional password. If the key generation application does not require strong private key protection, new RSA private keys are not protected with an additional password. **Always prompt user** - A prompt appears asking if a new RSA private key is to be protected with an additional password. **Always** - New RSA private keys must be protected with an additional password.	**Registry Value Name:** RSASecondaryAuthentication Mode Values: **0** - Never **1** - Prompt user on application request **2** - Always prompt user **3** - Always **4** - Token authentication on application request **Default**: **0**	Cannot be set by command line installation

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
RSA Secondary Authentication Mode (continued). **Note:** This option is not supported by IDPrime MD cards.	**Token authentication on application request** - If the key generation application requires key passwords to be created for strong private key protection, new RSA private keys are protected with the Token Password. If the key generation application does not require strong private key protection, new RSA private keys are not protected with any password. **Default**: Never		
Reuse Current Token Name Determines if the token's current Token Name is displayed as the default Token Name when the token is re initialized.	**Setting Name:** Reuse Current Token Name **Values**: **Selected** -The current Token Name is displayed **Not selected** -The current Token Name is ignored **Default**: Not Selected	**Registry Value Name:** ReadLabelFromToken **Values**: **1** -The current Token Name is displayed **0** -The current Token Name is ignored **Default**: 1	Cannot be set by command line installation.

SafeNet Authentication Client Tools UI Settings

The following settings are written to the appropriate folder's `SafeNet\Authentication\SAC\UI` registry key.

Description	ADM File Setting	Registry Value	Command Line
Use Default Password Determines if the *Change Password on First Logon* process assumes the current Token Password is the default (defined in the Default Token Password), and does not prompt the user to supply it.	**Setting Name**: Use Default Password **Values**: **Selected** - The default Token Password is automatically entered in the password field **Not selected** -The default Token Password is not automatically entered in the password field **Default**: Not selected	**Registry Value Name**: UseDefaultPassword **Values**: **1 (True)** - The default Token Password is automatically entered in the password field **0 (False)** -The default Token Password is not automatically entered in the password field **Default**: o (False)	Cannot be set by command line installation.
Password Term Defines the term used for the token's user password. **Note:** If a language other than English is used, ensure that the Password Terms are translated.	**Setting Name:** Password Term **Values**: Password PIN Passcode Passphrase **Default**: Password	**Registry Value Name**: PasswordTerm **Values** (String): Password PIN Passcode Passphrase **Default**: Password	Cannot be set by command line installation.
Decimal Serial Number Determines if the Token Information window displays the token serial number in hexadecimal or in decimal format.	**Setting Name:** Decimal Serial Number **Values**: **Selected** -Displays the serial number in decimal format **Not selected** -Displays the serial number in hexadecimal format **Default**: Not selected	**Registry Value Name:** ShowDecimalSerial **Values**: **1 (True)** -Displays the serial number in decimal format **0 (False)** -Displays the serial number in hexadecimal format **Default**: 0	Cannot be set by command line installation.F
Enable Tray Icon Determines if the application tray icon is displayed when SafeNet Authentication Client is started.	**Setting Name:** Enable Tray Icon **Values**: Never show Always show **Default**: Always show	**Registry Value Name**: ShowInTray **Values**: **0** - Never Show **1 -** Always Show **Default**: Always show	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
Enable Connection Notification Determines if a notification balloon is displayed when a token is connected or disconnected.	**Setting Name:** Enable Connection Notification Values: **Selected** - Displayed **Not selected**- Not displayed **Default**: Not selected	**Registry Value Name**: ShowBalloonEvents **Values**: **0** - Not Displayed **1 -** Displayed **Default**: 0	Cannot be set by command line installation.
iKey LED On Determines when the connected iKey LED is on. **Note:** When working with applications related to Citrix, set this value to 0.	**Setting Name:** iKey LED On Values: **Selected** - The iKey LED is always on when SAC Tray Icon is running **Not selected** -The iKey LED is on when the token has open connections only **Default**: Selected	**Registry Value Name:** IKeyLEDOn **Values**: **1** - The iKey LED is always on when SAC Tray Icon is running **0** -The iKey LED is on when the token has open connections only **Default**:1	Cannot be set by command line installation.
Enable Logging Control Determines if the *Enable Loggin*g /*Disable Logging* button is enabled in the Client Settings Advanced tab	**Setting Name:** Enable Logging Control **Values**: **Selected** -Enabled **Not selected** -Disabled **Default**: Selected	**Registry Value Name:** AllowLogsControl **Values**: **1** -Enabled **0** -Disabled **Default**: 1	Cannot be set by command line installation.
Home URL Overwrites the SafeNet home URL in SafeNet Authentication Client Tools	**Setting Name:** Home URL **Values**: Valid URL **Default**: SafeNet's home URL	**Registry Value Name:** HomeUrl **Values** (String): Valid URL **Default**: SafeNet's home URL	Cannot be set by command line installation.
eToken Anywhere Determines if eToken Anywhere features are supported	**Setting Name:** eToken Anywhere **Values**: **Selected** -Supported **Not selected** -Not supported **Default**: Selected	**Registry Value Name:** AnywhereExtendedMode **Values**: **1** -Supported **0** -Not supported **Default**: 1	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
Enable Certificate Expiration Warning Determines if a warning message is displayed when certificates on the token are about to expire.	**Setting Name:** Enable Certificate Expiration Warning **Values**: **Selected** - A message is displayed **Not selected** - A message is not displayed **Default**: Not Selected	**Registry Value Name:** CertificateExpiryAlert **Values**: **1 (True)** - Notify the user **0 (False**) - Do not notify the user **Default**: 1 (True)	Cannot be set by command line installation.
Ignore Archived Certificates Determines if archived certificates are ignored, and no warning message is displayed for certificates that are about to expire.	**Setting Name:** Ignore Archived Certificates **Values**: **Selected** -Archived certificates are ignored **Not selected**- A warning message is displayed if the token contains expired archived certificates. **Default**: Selected	**Registry Value Name:** IgnoreArchivedCertificates **Values:** **1** - Archived certificates are ignored **0** - A warning message is displayed if the token contains archived certificates. **Default**: 1	Cannot be set by command line installation.
Ignore Expired Certificates Determines if expired certificates are ignored, and no warning message is displayed for expired certificates.	**Setting Name:** Ignore Expired Certificates **Values**: **Selected** -Expired certificates are ignored **Not selected**- A warning message is displayed if the token contains expired certificates **Default**: Not selected	**Registry Value Name:** IgnoreExpiredCertificates Values: **1** - Expired certificates are ignored **0** - A warning message is displayed if the token contains expired certificates **Default**: 0	Cannot be set by command line installation.
Certificate Expiration Verification Frequency Defines the minimum interval, in days, between certificate expiration date verifications.	**Setting Name:** Certificate Expiration Verification Frequency **Values**: > 0 **Default**: 14 days	**Registry Value Name:** UpdateAlertMinInterval **Values**: > 0 **Default**: 14 days	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
Certificate Expiration Warning Period Defines the number of days before a certificate's expiration date during which a warning message is displayed.	**Setting Name:** Certificate Expiration Warning Period **Values**: > =0 (0 = No warning) **Default**: 30 days	**Registry Value Name:** ExpiryAlertPeriodStart **Values**: > =0 (0 = No warning) **Default**: 30 days	Cannot be set by command line installation.
Warning Message Title Defines the title to display in certificate expiration warning messages	**Setting Name:** Warning Message Title **Values**: String **Default**: SafeNet Authentication Client	**Registry Value Name:** AlertTitle **Values**: String **Default**: SafeNet Authentication Client	Cannot be set by command line installation.
Certificate Will Expire Warning Message Defines the warning message to display in a balloon during a certificate's "Certificate Expiration Warning Period."	**Setting Name:** Certificate Will Expire Warning Message **Values**: The message can include the following keywords **$EXPIRY_DATE** - the certificate expiration date **$EXPIRE_IN_DAYS** - the number of days until expiration **Default**: A certificate on your token expires in $EXPIRE_IN_DAYS days.	**Registry Value Name:** FutureAlertMessage **Values**: String **Default**: A certificate on your token expires in $EXPIRE_IN_DAYS days.	Cannot be set by command line installation.
Expiry Date Format Defines the format of the certificate's expiry date (**$EXPIRY_DATE)** displayed in a balloon	**Setting Name:** Expiry Date Format **Values**: Set the year/month/day in the required order. **Default**: Y/m/d	**Registry Value Name:** EXPIRY_DATE_FORMAT **Values**: Set the year/month/day in the required order using the following format: %Y/%m/%d **Default**: %Y/%m/%d	Cannot be set by command line installation.
Certificate Expired Warning Message Defines the warning message to display in a balloon if a certificate's expiration date has passed.	**Setting Name:** Certificate Expired Warning Message **Values**: String **Default**: Update your token now.	**Registry Value Name:** PastAlertMessage **Values**: String **Default**: Update your token now.	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
Warning Message Click Action Defines what happens when the user clicks the message balloon.	**Setting Name:** Warning Message Click Action **Values**: • No action • Show detailed message • Open website **Default**: No action	**Registry Value Name:** AlertMessageClickAction **Values**: **0 -** No action **1 -** Show detailed message **2 -** Open website **Default**: 0	Cannot be set by command line installation.
Detailed Message If “Show detailed message” is selected in “Warning Message Click Action” setting, defines the detailed message to display.	**Setting Name:** Detailed Message **Values**: String No default	**Registry Value Name:** ActionDetailedMessage **Values**: String No default	Cannot be set by command line installation.
Website URL If “Open website” is selected in the “Warning Message Click Action” setting, defines the URL to display	**Setting Name:** Website URL **Values**: Website address **No default**	**Registry Value Name:** ActionWebSiteURL **Values** (string): Website address **No default**	Cannot be set by command line installation.
Enable Password Expiration Notification Determines if a pop-up message is displayed in the system when the Token Password is about to expire.	**Setting Name:** Enable Password Expiration Notification **Values**: **Selected** - A message is displayed **Not selected** - A message is not displayed **Default**: Selected	**Registry Value Name:** NotifyPasswordExpiration **Values**: **1 (True)**- A message is displayed **0 (False)** - A message is not displayed **Default**: 1 (True)	Cannot be set by command line installation.
Display Virtual Keyboard Determines if SafeNet’s keystroke-secure Virtual Keyboard replaces standard keyboard entry of password fields in the following windows: • Token Logon • Change Password **Note:** The virtual keyboard supports English characters only.	**Setting Name:** Display Virtual Keyboard **Values**: **Selected** - Enabled **Not selected** -Disabled **Default**: Disabled	**Registry Value Name:** VirtualKeyboardOn **Values**: **1 (True)**- Virtual keyboard on **0 (False)** - Virtual keyboard off **Default**: 0 (False)	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
Password Policy Instructions If not empty, defines a string that replaces the default password policy description displayed in the *Unlock* and *Change Password* windows.	**Setting Name:** Modify Password Policy Description **Values**: If key does not exist, the default value is used: "A secure %REPLACE_PASSWORD_TERM% has at least 8 characters, and contains upper-case letters, lower-case letters, numerals, and special characters (such as !, $, #, %)." If key exists, the value in the key is displayed.	**Registry Value Name:** PasswordPolicyInstructions **Values**: String	Cannot be set by command line installation.
Define Initialization Mode Select this option if you want the 'Initialization Options' window (first window displayed when initializing a device) to be ignored.	**Setting Name:** Define Initialization Mode **Values**: 0 - Display the 'Initialization Options' window 1 - The 'Preserve the token settings and policies' option in the Initialization options window will be selected. (Set Preserve Mode) 2 - The 'Configure all initialization settings and policies' option in the Initialization options window will be selected. (Set Configure Mode) **Default**: Display the 'Initialization Options' window	**Registry Value Name:** DefInitMode **Values**: 0 - Display the 'Initialization Options' window 1 - Set Preserve Mode 2 - Set Configure Mode **Default**: 0	Cannot be set by command line installation.
Import Certificate Chain Determines if the certificate chain is imported to the token	**Setting Name:** Import Certificate Chain **Values**: • Do not import • Import • User selects import behavior **Default**: Do not import	**Registry Value Name:** ImportCertChain **Values**: **0 -** Do not import certificate chain **1** - Import certificate chain **2**- User selects import behavior **Default**: 0	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
Prevent Must Change Password dialog popup Determines if the tray icon will display a popup message to prompt the user to change the user password for tokens that are not initialized.	**Setting Name:** Prevent Must Change Password dialog popup **Values**: **Selected** - Must Change Password pop-up message will not be displayed **Not selected** -Must Change Password pop-up message will be displayed **Default**: Not selected	**Registry Value Name:** DenyMustChangePopup **Values**: **0 -** Must Change Password pop-up message will not be displayed **1** - Must Change Password pop-up message will be displayed **Default**: 0	Cannot be set by command line installation.

CAPI Settings

The following settings are written to the appropriate folder's `SafeNet\Authentication\SAC\CAPI` registry key.

NOTE:
These settings also apply to the Key Storage Provider (KSP).

Description	ADM File Setting	Registry Value	Command Line
Password Timeout Defines the number of minutes the CAPI-required password is valid following the last logon activity **Note:** • For iKey tokens - per token and per process. In addition to this registry key, an unrelated *Password Timeout* value is written to every iKey token during manufacture. The shorter of these two *Password Timeout* values - the one on the token and the one in this registry key during initialization - is applied. • For Java, CardOS, SafeNet Virtual Token - no token/process specificity. The attribute is taken from this registry key.	**Setting Name:** Password Timeout **Values**: >=0 (0= No timeout) **Default**: 0	**Registry Value Name:** PasswordTimeout **Values**: >=0 (0= No timeout) **Default**: 0	Cannot be set by command line installation.
Logout Mode Determines if the user is prompted to enter a password for each operation requiring the user to be logged on.	**Setting Name:** Logout Mode **Values**: **Selected** - A password prompt is displayed for each operation **Not selected** - The user remains logged on after the first logon **Default**: Not Selected	**Registry Value Name:** LogoutMode **Values**: **1 (True)** - A password prompt is displayed for each operation **0 (False)**- The user remains logged on after the first logon **Default**: 0	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
ASCII Password Determines if non-ASCII characters are supported in Token Passwords, enabling a string containing non-ASCII characters to be used as a smart card logon password.	**Setting Name:** ASCII Password **Values**: **Selected** - Non ASCII character are supported **Not selected** -Only ASCII characters are supported **Default**: Not selected	**Registry Value Name:** AsciiPassword **Values**: **1 (True)** - Non ASCII character are supported **0 (False)**- Non ASCII characters are not supported **Default**: 0(False)	Cannot be set by command line installation.
Overwrite Default Certificate Determines if the default certificate selection can be reset after being explicitly set in legacy eToken PKI Client 3.65	**Setting Name:** Overwrite Default Certificate **Values**: **Selected** -Default certificate can be reset **Not selected -** Default certificate cannot be reset **Default**: Not selected	**Registry Value Name:** OverwriteDefaultCertificate **Values**: **1** - Default certificate can be reset **0 -** Default certificate cannot be reset **Default**: 0	Cannot be set by command line installation.
Sign Padding On-Board Determines if sign padding is performed on-board supported devices for added security. Sign padding is supported by Java tokens. **Note:** To use this feature, SafeNet Authentication Client 8.1 or later must be installed.	**Setting Name:** Sign Padding On-Board **Values**: • Not supported - Sign padding is always performed on the host computer • Supported (backwardly compatible) - Sign padding is performed on-board supported devices when running SafeNet Authentication Client 8.1 or later; Sign padding is performed on the host computer when running SafeNet Authentication Client versions earlier than 8.1 • Required - Sign padding is always performed on-board supported devices; Not backwardly compatible with SafeNet Authentication Client versions earlier than 8.1 **Default**: Not supported	**Registry Value Name:** SignPaddingOnBoard **Values**: **0 -** Not supported: Sign padding is always performed on the host computer **1** - Supported: Sign padding is performed on-board supported devices when running SafeNet Authentication Client 8.1 or later; Sign padding is performed on the host computer when running SafeNet Authentication Client versions earlier than 8.1 **2**- Required: Sign padding is always performed on-board supported devices; Not backwardly compatible with SafeNet Authentication Client versions earlier than 8.1 **Default**: 0	Cannot be set by command line installation.

Internet Explorer Settings

The following settings are written to the appropriate folder's `SafeNet\Authentication\SAC\CAPI\IEXPLORE.EXE` registry key. They apply when using Internet Explorer only. The values are set per process on a per machine basis.

Description	ADM File Setting	Registry Value	Command Line
No Default Key Container Determines if the latest Default Key Container certificate on the user's token is ignored when a new certificate is enrolled on the token. This feature relates to the scrdenrl.dll ActiveX control used by the Microsoft CA web site and the SafeNet Authentication Client. **Note:** If the "Enrollment on Behalf" certificate used for enrollment is stored on an administrator token and not on a computer, this value must be 0.	**Setting Name:** No Default Key Container **Values**: **Selected** - The latest Default Key Container certificate on the user's token is ignored when a new certificate is enrolled on the token **Not selected** - The latest Default Key Container certificate on the user's token is deleted when a new certificate is enrolled on the token **Default**: Selected, for the IEXPLORE.EXE process only	**Registry Value Name:** NoDefaultKeyContainer **Values**: **1 (True)**- The latest Default Key Container certificate on the user's token is ignored when a new certificate is enrolled on the token **0 (False)** - The latest Default Key Container certificate on the user's token is deleted when a new certificate is enrolled on the token **Default**: 1 (True), for the IEXPLORE.EXE process only	PROP_EXPLORER_DEFENROL
Default Enrollment Type Determines if the administrator token's latest Enrollment Agent certificate must be the certificate used to enroll a new certificate on the user's token. This feature applies when "Enrollment on Behalf" uses a certificate on an administrator token and not on a computer. **Note:** To enable the token containing the "Enrollment on Behalf" certificate to contain Smartcard Logon certificates also, this value must be 1.	This feature cannot be set in the GPO Editor or MMC	**Registry Value Name:** DefEnrollType **Values**: **1 (True**) - The administrator token's latest Enrollment Agent certificate is used, even if the token's Default Key Container contains a different type of certificate, such as Smartcard Logon **0 (False)** - Regardless of its certificate type, the administrator token's Default Key Container certificate is used **Default**: 0 (False), for the IEXPLORE.EXE process only	Cannot be set by command line installation, so must be added manually

Certificate Store Settings

Microsoft Certificate Propagation Service

Windows Vista and later include the Microsoft Certificate Propagation Service. This duplicates some of the features of the SafeNet Authentication Client propagation functionality. To avoid a lack of synchronization between these different propagation processes, we strongly recommend closing the Microsoft Certificate Propagation Service and using only SafeNet Authentication Client for certificate propagation.

The following settings are written to the appropriate folder's `SafeNet\Authentication\SAC\CertStore` registry key.

Description	ADM File Setting	Registry Value	Command Line
Propagate User Certificates Determines if all user certificates on the token are exported to the user store. **Note:** Can be set in SafeNet Authentication Client Tools.	**Setting Name:** Propagate User Certificates **Values**: **Selected** -User certificates are exported **Not selected** - User certificates are not exported **Default**: Selected	**Registry Value Name:** PropagateUserCertificates **Values**: **1 (True)** - User certificates are exported **0 (False)** - User certificates are not exported **Default**: 1 (True)	PROP_PROPAGATEUSERCER
Propagate CA Certificates Determines if all CA certificates on the token are exported to the Trusted CA store. **Note:** Can be set in SafeNet Authentication Client Tools.	**Setting Name:** Propagate CA Certificates **Values**: **Selected** - CA certificates are exported **Not selected** - CA certificates are not exported **Default**: Selected	**Registry Value Name:** PropagateCACertificates **Values**: **1 (True)**- CA certificates are exported **0 (False)**- CA certificates are not exported **Default**: 1 (True)	PROP_PROPAGATECACER
Synchronize Store Determines if store synchronization is enabled. The synchronize store is part of the SAC Monitor application. It synchronizes between the contents of the token and the SAC application. For example, if so configured, when the token is connected the token certificate is propagated to the certificate store, and removed when the token is disconnected.	**Setting Name:** Synchronize Store **Values**: **Selected** -Enabled **Not selected** -Disabled **Default**: Selected	**Registry Value Name:** SynchronizeStore **Values**: **1 (True)**-Enabled **0 (False)** -Disabled **Default**: 1 (True)	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
Add New Certificates to Token When a certificate with exportable keys is added to the user store, determines if an option is displayed to import that certificate to the selected token.	**Setting Name:** Add New Certificates to Token **Values**: **Selected** - An option is displayed to import the new certificate **Not selected** - An option is not displayed to import the new certificate **Default**: Selected	**Registry Value Name:** AddToTokenOnNewCertInStore **Values**: **1 (True)** - An option is displayed to import the new certificate **0 (False)** - An option is not displayed to import the new certificate **Default**: 1 (True)	Cannot be set by command line installation.
Remove User Certificates upon Token Disconnect When a token is disconnected, determines if the user certificates that were exported from it are removed from the user store.	**Setting Name:** Remove User Certificates upon Token Disconnect **Values**: **Selected** - User certificates are removed from the user store **Not selected** - User certificates are not removed from the user store **Default**: Selected	**Registry Value Name:** RemoveUserCertsOnTokenRemove **Values**: **1 (True)** - User certificates are removed from the user store **0 (False)** - User certificates are not removed from the user store **Default**: 1 (True)	Cannot be set by command line installation.
Remove Certificates from Store upon Token Disconnect When an exported certificate is removed from the token, determines if that certificate is removed from the user store.	**Setting Name:** Remove Certificates upon Removal from Token **Values**: **Selected** - The certificate is removed from the user store **Not selected** - The certificate is not removed from the user store **Default**: Selected	**Registry Value Name:** RemoveFromStoreOnRemoveFromToken **Values**: **1 (True)** - The certificate is removed from the user store **0 (False)** - The certificate is not removed from the user store **Default**: 1 (True)	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
Remove Certificates from Token upon Removal from Store When an exported certificate is removed from the user store, determines if an option is displayed to remove that certificate from the token.	**Setting Name:** Remove Certificates from Token upon Removal from Store **Values**: Never - an option is not displayed to remove the certificate Always - an option is displayed to remove the certificate **Template dependent** - an option is displayed to remove only those certificates whose templates are listed in "Certificate Templates to Remove from Token" setting. **Default**: Never	**Registry Value Name:** RemoveFromTokenOnRemoveFromStore **Values**: **0** - Never; an option is not displayed to remove the certificate **1** - Always; an option is displayed to remove the certificate **2** - An option is displayed to remove only those certificates whose templates are listed in the registry setting RemoveFromStoreOnRemoveFromToken Templates. **Default**: 0	Cannot be set by command line installation.
Certificate Templates to Remove from Token Lists templates of the certificates that can be removed from a token when the exported certificates are removed from the user store.	**Setting Name:** Certificate Templates to Remove from Token **Values**: Template names, separated by commas **Default**: None Applies only when the *Remove Certificates from Token upon Removal from Store* setting is set to **Template dependent**.	**Registry Value Name:** RemoveFromTokenOnRemoveFromStoreTemplates **Values**: Template names, separated by commas **Default**: None Applies only when the registry setting RemoveFromTokenOnRemoveFromStore is set to **2.**	Cannot be set by command line installation.
Certificate Removal Period When an exported certificate is removed from the user store, defines the number of days to attempt to remove that certificate from a token that is not connected Relevant only when the setting *Remove Certificates from Token upon Removal from Store (RemoveFromTokenOnRemoveFromStore)* is set to **Always** or **Template dependent**.	**Setting Name:** Certificate Removal Period **Values**: >=0 **Default**: 7	**Registry Value Name:** CertsToRemoveStorePeriod **Values**: >=0 **Default**: 7	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
Delete Original Key After Copy When a key and its certificate are copied from the certificate store to a token, determines if the private key is deleted from the source CSP.	**Setting Name:** Delete Original Key After Copy **Values**: **Selected** - Key is deleted from the CSP **Not selected** - Key is retained in the CSP **Default**: Selected	**Registry Value Name:** DeleteOriginalKeyAfterCopy **Values**: **1 (True)** - Key is deleted from the CSP **0 (False)** - Key is retained in the CSP **Default**: 1 (True)	Cannot be set by command line installation.
Calculates the Certificate Friendly Name if it does not exist.	**Setting Name:** Calculate Certificate Friendly Name **Values**: **Selected** - Calculate friendly name using other certificate attributes **Not selected** - Does not calculate friendly name **Default**: Not Selected	**Registry Value Name:** CalculateCertFriendlyName **Values**: **1 (True)** - Calculate Friendly Name **0 (False)** - Do not calculate Friendly Name **Default**: 0 (False) **Note:** If the Value=1, and the friendly name is manually set, the calculated friendly name will be applied.	Cannot be set by command line installation.

CNG Key Storage Provider Settings

The following settings are written to the appropriate folder's `SafeNet\Authentication\SAC\CNG` registry key.

NOTE:
These settings apply to the Key Storage Provider (KSP) only.

Description	Settings in GPO Editor or MMC	Registry Key	Command Line
Cryptographic Provider Determines which cryptographic provider to use for certificate propagation. **Note:** Can be set in SafeNet Authentication Client Tools. **Note:** After changing the cryptographic provider setting, reconnect the token to ensure that the properties are updated to the token. **Note:** This setting is not relevant to IDPrime MD cards.	**Setting Name:** Cryptographic Provider **Values**: 0 = CSP 1 = KSP (if supported by the OS) 2 = The Provider that enrolled the certificate (This information is stored on the token) **Default**: 2	**Registry Value Name:** KspPropagationMode **Values**: 0 = CSP 1 = KSP (if supported by the OS) 2 = The Provider that enrolled the certificate (This information is stored on the token) **Default**: 2	KSP_ENABLED Enables you to prevent KSP from being installed. See "KSP_ENABLED" on page 54.

Token Password Quality Settings

The following settings are written to the appropriate folder's `SafeNet\Authentication\SAC\PQ` registry key.

NOTE:
These settings are relevant for smartcards or tokens based on eToken Applet (for example, eToken 5110 GA and eToken 5110 FIPS)

Description	Settings in GPO Editor or MMC	Registry Key	Command Line
Password - Minimum Length Defines the minimum password length. **Note:** Can be set in SafeNet Authentication Client Tools. For more information on how to configure the 'Password Minimum Length' property as permanent See "Changing the Password Minimum Length Permanently" on page 39	**Setting Name:** Password -Minimum Length **Values**: >=4 **Default**: 8	**Registry Key Name:** pqMinLen **Values**: >=4 **Default**: 8	PROP_PQ_MINLEN
Password - Maximum Length Defines the maximum password length. **Note:** Can be set in SafeNet Authentication Client Tools.	**Setting Name:** Password -Maximum Length **Values**: Cannot be less than the Password Minimum Length **Default**: 16	**Registry Key Name:** pqMaxLen **Values**: Cannot be less than the Password Minimum Length **Default**: 16	Cannot be set by command line installation.
Password - Maximum Usage Period Defines the maximum number of days a password is valid. **Note:** Can be set in SafeNet Authentication Client Tools. **Note:** This parameter is 'Day Sensitive' i.e. the system counts the day's and not the hour in which the user made the change.	**Setting Name:** Password - Maximum Usage Period **Values**: >=0 (0 =No expiration) **Default**: 0	**Registry Key Name:** pqMaxAge **Values**: >=0 (0 =No expiration) **Default**: 0	PROP_PQ_MAXAGE

Description (Cont.)	Settings in GPO Editor or MMC (Cont.)	Registry Key (Cont.)	Command Line (Cont.)
Password - Minimum Usage Period Defines the minimum number of days between password changes. **Note:** Can be set in SafeNet Authentication Client Tools. **Note:** Does not apply to iKey devices.	**Setting Name:** Password - Minimum Usage Period **Values**: >=0 (0 = No minimum) **Default**: 0	**Registry Key Name:** pqMinAge **Values**: >=0 (0 = No minimum) **Default**: 0	PROP_PQ_MINAGE
Password - Expiration Warning Period Defines the number of days before expiration during which a warning is displayed. **Note:** Can be set in SafeNet Authentication Client Tools.	**Setting Name:** Password - Expiration Warning Period **Values**: >=0 (0 = No warning) **Default**: 0	**Registry Key Name:** pqWarnPeriod **Values**: >=0 (0 = No warning) **Default**: 0	PROP_PQ_WARNPERIOD
Password - History Size Defines the number of recent passwords that must not be repeated. **Note:** Can be set in SafeNet Authentication Client Tools.	**Setting Name:** Password - History Size **Values**: >= 0 (0 = No minimum) **Default**: 10	**Registry Key Name:** pqHistorySize **Values**: >= 0 (0 = No minimum) **Default**: 10 (iKey device history is limited to 6)	PROP_PQ_HISTORYSIZE
Password - Maximum Consecutive Repetitions Defines the maximum number of consecutive times a character can be used in a password. **Note:** Can be set in SafeNet Authentication Client Tools. **Note:** Does not apply to iKey devices.	**Setting Name:** Password - Maximum Consecutive Repetitions **Values**: 0 - 16 (0 = No maximum) **Default**: 3	**Registry Key Name:** pqMaxRepeated **Values**: 0 - 16 (0 = No maximum) **Default**: 3	Cannot be set by command line installation.

Description (Cont.)	Settings in GPO Editor or MMC (Cont.)	Registry Key (Cont.)	Command Line (Cont.)
Password - Complexity Determines if there is a minimum number of character types that must be included in a new Token Password The character types are: upper-case letters, lower-case letters, numerals, and special characters. **Note:** Can be set in SafeNet Authentication Client Tools.	**Setting Name:** Password - Complexity **Values**: **Standard complexity** - A minimum of 2 or 3 types must be included, as defined in the *Password- Minimum Mixed Character Type*s setting **Manual complexity** - The rule for each character type is defined in the character type's *Include* setting **Default**: Standard complexity	**Registry Key Name:** pqMixChars **Values**: **1** - A minimum of 2 or 3 types must be included, as defined in the *Password- Minimum Mixed Character Type*s setting **0** -The rule for each character type is defined in the character type's *Include* setting **Default**: 1	PROP_PQ_MIXCHARS
Password - Minimum Mixed Character Types Defines the minimum number of character types that must be included in a new Token Password. The character types are: upper-case letters, lower-case letters, numerals, and special characters. **Note:** • Applies only when the *Password - Complex*ity setting is set to **Standard complexity.** • Can be set in SafeNet Authentication Client Tools.	**Setting Name:** Password - Minimum Mixed Character Types **Values**: At least 3 character types At least 2 character types **Default**: At least 3 character types	**Registry Key Name:** pqMixLevel **Values**: **0 -** At least 3 character types **1** - At least 2 character types **Default**:0	Cannot be set by command line installation
Password - Include Numerals Determines if the password can include numerals. **Note:** • Applies only when the *Password - Complex*ity setting is set to **Manual complexity.** • Can be set in SafeNet Authentication Client Tools.	**Setting Name:** Password - Include Numerals **Values**: Permitted Forbidden Mandatory **Default**: Permitted **Note:** *Forbidden* is not supported by iKey devices.	**Registry Key Name:** pqNumbers **Values**: 0 -Permitted 1 - Forbidden 2 - Mandatory **Default**: 0	Cannot be set by command line installation

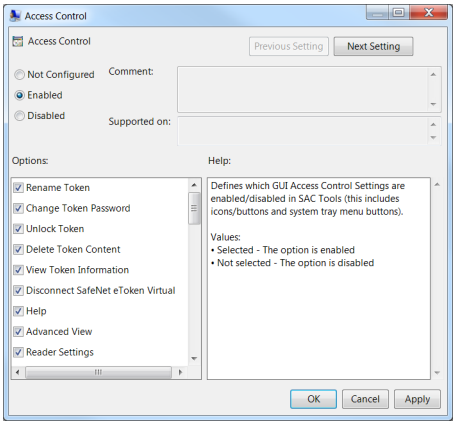
Description (Cont.)	Settings in GPO Editor or MMC (Cont.)	Registry Key (Cont.)	Command Line (Cont.)
Password - Include Upper-Case Determines if the password can include upper-case letters. **Note:** • Applies only when the *Password - Complexity* setting is set to **Manual complexity.** • Can be set in SafeNet Authentication Client Tools.	**Setting Name:** Password - Include Upper-Case **Values**: Permitted Forbidden Mandatory **Default**: Permitted	**Registry Key Name:** pqUpperCase **Values**: 0 - Permitted 1 - Forbidden 2 - Mandatory **Default**: 0	Cannot be set by command line installation.
Password - Include Lower-Case Determines if the password can include lower-case letters. **Note:** • Applies only when the *Password - Complexity* setting is set to **Manual complexity.** • Can be set in SafeNet Authentication Client Tools.	**Setting Name:** Password - Include Lower - Case **Values**: Permitted Forbidden Mandatory **Default**: Permitted	**Registry Key Name:** pqLowerCase **Values**: 0 - Permitted 1 - Forbidden 2 - Mandatory **Default**: 0	Cannot be set by command line installation.
Password - Include Special Characters Determines if the password can include special characters, such as @,!, &. **Note:** • Applies only when the *Password - Complexity* setting is set to **Manual complexity.** • Can be set in SafeNet Authentication Client Tools.	**Setting Name:** Password - Include Special Characters **Values**: Permitted Forbidden Mandatory **Default**: Permitted	**Registry Key Name:** pqSpecial **Values**: 0 - Permitted 1 - Forbidden 2 - Mandatory **Default**: 0	Cannot be set by command line installation.

Description (Cont.)	Settings in GPO Editor or MMC (Cont.)	Registry Key (Cont.)	Command Line (Cont.)
Password Quality Check on Initialization Determines if the password quality settings are checked and enforced when a token is initialized **Note:** We recommend that this policy not be set when tokens are enrolled using SafeNet Authentication Manager.	**Setting Name:** Password Quality Check on Initialization **Values**: **Selected** -The password quality is enforced **Not selected** - The password quality is not enforced **Default**: Not selected	**Registry Key Name:** pqCheckInit **Values**: **1 (True)** -The password quality is enforced **0 (False)** - The password quality is not enforced **Default**: 0	Cannot be set by command line installation.
Password Quality Owner Defines the owner of the password quality settings on a re initialized token, and defines the default of the *Password Quality Modifiable* setting.	**Setting Name:** Password Quality Owner **Values**: Administrator User **Default**: Administrator, for tokens with an Administrator Password. User, for tokens without an Administrator Password.	**Registry Key Name:** pqOwner **Values**: **0** - Administrator **1** - User **Default**: 0, for tokens with an Administrator Password. 1, for tokens without an Administrator Password.	Cannot be set by command line installation.
Enable Password Quality Modification Determines if the password quality settings on a newly initialized token can be modified by the owner. See the *Password Quality Owner* setting. To configure the 'Password Minimum Length' property as permanent during or after the initialization process, See "Changing the Password Minimum Length Permanently" on page 39	**Setting Name:** Enable Password Quality Modification. **Values**: **Selected** - The password quality can be modified by the owner **Not selected** - The password quality cannot be modified by the owner **Default**: Selected, for administrator-owned tokens Not selected, for user owned tokens.	**Registry Key Name:** pqModifiable **Values**: **1 (True)**- The password quality can be modified by the owner **0 (False)** - The password quality cannot be modified by the owner **Default**: 1 (True), for administrator-owned tokens 0 (False), for user owned tokens.	Cannot be set by command line installation.

Description (Cont.)	Settings in GPO Editor or MMC (Cont.)	Registry Key (Cont.)	Command Line (Cont.)
Enable Administrator Password Quality Check Determines if the Administrator Password Quality Check is enabled. When enabled, this property enforces an administrator (SO) password (on eToken and IDPrime devices) that has at least 3 different character types and a minimum length of 8 characters. The character types are: upper-case letters, lower-case letters, numerals, and special characters. **Note:** For backward compatibility on IDPrime devices, the Administrator Key can be used with 48 hexadecimal characters via the UI and/or 24 binary bytes via the API call. When disabled, the old behavior is as follows: **eToken:** minimum of 4 characters and no minimum character type enforcement **IDPrime:** minimum of 8 characters and no minimum character type enforcement, or the administrator key can be used. **Note:** When the ITI Certification mode property is enabled, the Enable Administrator Password Quality Check property will be disabled	**Setting Name:** Enable Administrator Password Quality Check **Values**: **Selected** - Administrator Password Quality is enforced **Not Selected** - Administrator Password Quality is disabled **Default**: Selected	**Registry Key Name:** pqAdminPQ **Values**: **1 (Enabled)** - Administrator Password Quality is enforced **0 (Disabled)** - Administrator Password Quality is disabled **Default**: Enabled	Cannot be set by command line installation.

SafeNet Authentication Client Tools UI Access Control List

The *Access Control Properties* window contains a list of settings that determine which features are enabled in the SafeNet Authentication Client Tools and Tray Menu.



The following settings are written to the appropriate folder's `SafeNet\Authentication\SAC\AccessControl` registry key.

Access Control Feature	ADM File Setting	Registry Key	Command Line
All access control features listed below	**Values**: **Selected** - The feature is enabled **Not selected** - The feature is disabled. **Default**: Selected, except where indicated in the table	**Values**: **1 (True)** - The feature is enabled. **0 (False)** - The feature is disabled. **Default**: 1(True), except where indicated in the table	Cannot be set by command line installation.

In the following table, the *Access Control Feature* column displays the name in the *Access Control Properties* window.

NOTE:
All access control features are enabled by default, except where indicated in the table.

Access Control Feature	Registry Value Name	Description
Crypto Notification Timeout	CryptoNotficationTimeout	Enables/Disables the notification: "The process may take a while..." Enter the time in seconds after which the notification is displayed. for example, the value 30 means the notification is delayed by 30 seconds. **Note:** By default the value is 0 (meaning this feature is disabled).

Access Control Feature (Cont.)	Registry Value Name (Cont.)	Description (Cont.)
Rename Token	RenameToken	Enables/Disables the *Rename Token* feature in SafeNet Authentication Client Tools.
Change Token Password	ChangePassword	Enables/Disables the *Change Token Password* feature in SafeNet Authentication Client Tools.
Unlock Token	UnlockEtoken	Enables/Disables the *Unlock Token* feature in SafeNet Authentication Client Tools.
Delete Token Content	ClearEToken	Enables/Disables the *Delete Token Content* feature in SafeNet Authentication Client Tools.
View Token Information	ViewTokenInfo	Enables/Disables the *View Token Information* feature in SafeNet Authentication Client Tools.
Disconnect SafeNet Virtual Token	DisconnectVirtual	Enables/Disables the *Disconnect* SafeNet Virtual Token feature in SafeNet Authentication Client Tools.
Help	ShowHelp	Determines if the user can open the *Help* file in SafeNet Authentication Client Tools.
Advanced View	OpenAdvancedView	Determines if the user can open the Advanced View in SafeNet Authentication Client Tools.
Reader Settings	ManageReaders	Enables/Disables the *Reader Settings* feature in SafeNet Authentication Client Tools.
Connect SafeNet Virtual Token	AddeTokenVirtual	Enables/Disables the *Connect* SafeNet Virtual Token feature in SafeNet Authentication Client Tools.
Initialize Token	InitializeEToken	Enables/Disables the *Initialize Token* feature in SafeNet Authentication Client Tools.
Import Certificate	ImportCertificate	Enables/Disables the *Import Certificate* feature in SafeNet Authentication Client Tools.
Reset Default Certificate Selection	ClearDefaultCert	Enables/Disables the *Reset Default Certificate Selection* feature in SafeNet Authentication Client Tools.
Delete Certificate	DeleteCertificate	Enables/Disables the *Delete Certificate* feature in SafeNet Authentication ClientTools.
Export Certificate	ExportCertificate	Enables/Disables the *Export Certificate* feature in SafeNet Authentication Client Tools.
Set Certificate as Default	SetCertificateAsDefault	Enables/Disables the *Set Certificate as Default* feature in SafeNet Authentication Client Tools.
Log On as Administrator	LoginAsAdministrator	Enables/Disables the *Log On as Administrator* feature in SafeNet Authentication Client Tools.
Change Administrator Password	ChangeAdministratorPassword	Enables/Disables the *Change Administrator Password* feature in SafeNet Authentication Client Tools.
Set Token Password	SetUserPassword	Enables/Disables the *Set Token Password* feature in SafeNet Authentication Client Tools.
Token Password Retries	AllowChangeUserMaxRetry	Enables/Disables the *Logon retries before token is locked* feature (for the Token Password) in SafeNet Authentication Client Tools.

Access Control Feature (Cont.)	Registry Value Name (Cont.)	Description (Cont.)
Administrator Password Retries	AllowChangeAdminMaxRetry	Enables/Disables the *Logon retries before token is locked* feature (for the Administrator Password) in SafeNet Authentication Client Tools.
Advanced Initialization Settings	OpenAdvancedModeOfInitialize	Enables/Disables the *Advanced* button in the *Token Initialization* window in SafeNet Authentication Client Tools.
System Tray - Unlock Token	TrayIconUnlockEtoken	Enables/Disables the *Unlock Token* feature in the SafeNet Authentication Client Tray Menu
System Tray - Generate OTP	GenerateOTP	Enables/Disables the *Generate OTP* feature in the SafeNet Authentication Client Tray Menu
System Tray - Delete Token Content	TrayIconClearEToken	Enables/Disables the *Delete Token Content* feature in the SafeNet Authentication Client Tray Menu. **Note:** By default, this feature is **Disabled**
System Tray -Change Token Password	TrayIconChangePassword	Enables/Disables the *Change Token Password* feature in the SafeNet Authentication Client Tray Menu.
System Tray -Synchronize Domain-Token Passwords	SyncDomainAndTokenPass	Enables/Disables the *Synchronize Domain Token Passwords* feature in the SafeNet Authentication Client Tray Menu.
System Tray - Tools	OpeneTokenProperties	Enables/Disables the *Tools* menu item (open SafeNet Authentication Client Tools) in the SafeNet Authentication Client Tray Menu.
System Tray - About	About	Enables/Disables the *About* menu item in the SafeNet Authentication Client Tray Menu.
Enable Change IdenTrust Identity	IdentrusChangePassword	Enables/Disables the *Change IdenTrust PIN* feature in SafeNet Authentication Client Tools.
Enable Unblock IdenTrust Passcode	IdentrusUnlock	Enables/Disables the *Unlock IdenTrust* feature in SafeNet Authentication Client Tools.
Delete Data Object	DeleteDataObject	Enables/Disables the *Delete Data Object* feature in SafeNet Authentication Client Tools.
Allow One Factor	AllowOneFactor	Enables/Disables the *Allow One Factor* feature in the *Advanced Token Initialization Settings* window in SafeNet Authentication Client Tools.
Verisign Serial Number **Note:** This property cannot be set in the Access Control Properties window. It must be set in the registry key.	VerisignSerialNumber	Enables/Disables the *Verisign Serial number* feature in SafeNet Authentication Client Tools.

Access Control Feature (Cont.)	Registry Value Name (Cont.)	Description (Cont.)
PIN Type	PinType	Defines which GUI PIN Properties are enabled/disabled in SAC Tools 'Advanced' PIN Properties tab and the 'Initialization' window.
PIN Purpose	PinPurpose	
Cache Type	PinCacheType	
Cache Timeout	PinCacheInfo	
PIN Flags	PinFlags	
Ext. PIN Flags	PinFlagsEx	
Validity period (days)	PinValidity	
Expiration warning period (days)	PinWarning	
Minimum length (characters)	PinMinLen	Defines which GUI PIN Quality parameters are enabled/disabled in SAC Tools 'Advanced' tab and the 'Initialization' window.
Maximum length (characters)	PinMaxLen	
History size	PinHistory	
Number of different characters that can be repeated at least once	PinNumDiffCharRepeat	
Maximum number a characters can appear	PinMaxNumCharAppear	
Maximum number of characters in a sequence	PinMaxNumCharSequence	
Maximum number a character can be repeated in adjacent positions	PinMaxNumCharRepeatPos	
Numeric	PinNumber	
Alpha Upper	PinUpper	
Alpha Lower	PinLower	
Non alpha	PinSpecial	
Alpha	PinAlphabetic	
Non Ascii	PinNonAlphabetic	
Minimum usage period (days)	PinMinUse	
Maximum usage period (days)	PinMaxUse	
Must meet complexity requirements	PinComplexity	
Maximum consecutive repetitions	PinMaxRepeat	

Security Settings

The following settings are written to the appropriate folder's `SafeNet\Authentication\SAC\Crypto` registry key.

Description	ADM File Setting	Registry Value	Command Line
Deprecated Cryptographic Algorithms and Features The default list of deprecated cryptographic algorithms and features may be enhanced in order to comply with NIST requirements in future versions. It is up to the customer to check that it will be compatible with third-party applications.	**Setting Name:** Deprecated Cryptographic Algorithms and Features **Values**: **None** - All SAC cryptographic algorithms and features are supported. This was the default value for SAC versions below 10.5. Setting this value will cause SAC to be compatible with SAC 10.5 and below. It is strongly recommended to read *SAC Configuration Recommendations* on page 18 before applying legacy values. **Obsolete** - A list of restricted and deprecated cryptographic algorithms and features. The following are deprecated: MD5, RC2, RC4, DES, 2DES, GenericSecret<112, RSA-RAW, RSA<2048, ECC<224, ECB, Sign-SHA1 Alternatively, you can create your own list of deprecated algorithms and features manually (See the description below). **Default**: Obsolete	**Value Name:** Disable-Crypto **Values:** (String) **None** - All SAC cryptographic algorithms and features are supported. This was the default value for SAC versions below 10.5. Setting this value will cause SAC to be compatible with SAC 10.5 and below. It is strongly recommended to read *SAC Configuration Recommendations* on page 18 before applying legacy values. **Obsolete** - A list of restricted and deprecated cryptographic algorithms and features. The following are deprecated: MD5, RC2, RC4, DES, 2DES, GenericSecret<112, RSA-RAW, RSA<2048, ECC<224, ECB, Sign-SHA1 Alternatively, you can create your own list of deprecated algorithms and features manually (See the description below). **Default**: Obsolete	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)

The following can be disabled:

Algorithms: RSA, ECC, DES, 2DES, 3DES, AES, RC2, RC4, GenericSecret
Hash types: MD5, SHA1, SHA2
Padding types: RAW, PKCS1, OAEP, PSS
Cipher modes: ECB, CBC, CTR, CCM
Mechanisms: MAC, HMAC, ECDSA, ECDH
Operations: Encrypt, Decrypt, Sign, Verify, Generate, Derive, Wrap, Unwrap, Digest, Create (keys only)
Weak key size: RSA<2048
Object types: HWEF – elementary file (EF) objects (used by eToken devices for storing exportable symmetric keys and symmetric keys without on-board implementation)
HWALL – all types of objects implemented on token (Base Security Object (BSO) and EF),
ETV – eToken Virtual

The following is an example list of restricted and deprecated cryptographic algorithms and features:
Encrypt-DES-ECB, Sign-3DES-MAC, DES-CTR, HMAC-MD5, HMAC-SHA1, HMAC-SHA2, DES-CBC, Unwrap-DES-ECB, RSA-PKCS1-MD5, Verify-RSAPSS-SHA2, AES-CTR, AES-MAC,
Decrypt-RC2, Wrap-ECB.

To allow a cryptographic algorithm or feature, remove it from the list.
For example, if the administrator wants to allow usage of RSA<2048, it must be removed from the list.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
Key Management Defines key creation, export, unwrap, and off-board crypto policies. SAC default behavior may be updated in future versions in order to comply with NIST requirements. It is up to the customer to check that it will be compatible with third-party applications.	Setting Name: Key Management **Values**: (String) **Compatible** - enables the use of features that are deprecated in the Optimized and Strict configurations below. This was the default value for SAC versions below 10.5. Setting this value will cause SAC to be compatible with SAC 10.5 and below. It is strongly recommended to read *SAC Configuration Recommendations* on page 18 before applying legacy values. **Optimized:** Disable the generation or creation of exportable keys. Disable the exporting of keys, regardless of how they were generated. Disable any usage of symmetric keys off-board including unwrap. Disable the unwrap-PKCS1.5 and unwrap-AES-CBC on hardware tokens (session enable). **Strict:** Disable the generation or creation of exportable keys. Disable the exporting of keys, regardless of how they were generated. Disable any usage of symmetric keys off-board including unwrap. Disable all unwrap-PKCS1.5 and unwrap-AES-CBC operations. **Default**: Optimized	Registry Value Name: Key-Management-Security **Values**: (String) **Compatible** - enables the use of features that are deprecated in the Optimized and Strict configurations below. This was the default value for SAC versions below 10.5. Setting this value will cause SAC to be compatible with SAC 10.5 and below. It is strongly recommended to read *SAC Configuration Recommendations* on page 18 before applying legacy values. **Optimized:** Disable the generation or creation of exportable keys. Disable the exporting of keys, regardless of how they were generated. Disable any usage of symmetric keys off-board including unwrap. Disable the unwrap-PKCS1.5 and unwrap-AES-CBC on hardware tokens (session enable). **Strict:** Disable the generation or creation of exportable keys. Disable the exporting of keys, regardless of how they were generated. Disable any usage of symmetric keys off-board including unwrap. Disable all unwrap-PKCS1.5 and unwrap-AES-CBC operations. **Default**: Optimized	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
DotNetOBKGType Enables the generation of the RSA keypairs using BCrypt API on the local computer instead of On Board Key Generation. If the value of this key is set to 0 or is absent (default installation), then the RSA keypairs on IDPrime.NET cards are generated using the standard On Board Key Generation mechanism. If this key is created and set to 1, the Minidriver creates the RSA keypairs using the BCrypt API on the local computer and keys are imported into the IDPrime.NET smart card.	Not Supported	**Setting Name:** DotNetOBKGType **Values**: **0** = Generate on board (key pair) **1 (and above)** = Key pair generation is done by software (that is: disable on board key generation) **Default**: 0	Cannot be set by command line installation.
HashOffboard Determines the hash behavior used by the combined mechanisms CKM_SHA1_RSA_PKCS (eToken 5110 GA) and CKM_SHA256_RSA_PKCS (eToken 5110 GA and eToken 5110 FIPS)	Not Supported	**Setting Name:** HashOffboard **Values:** 1(True) - Run hash off-board 0(False) - Run hash on-board Set to True when required to run hash off-board **Default:** 0(False)	Cannot be set by command line installation.

Log Settings

The following settings are written to the appropriate folder's

`SafeNet\Authentication\SAC\Log` registry key.

These settings may be defined using:

HKEY_LOCAL_MACHINE or HKEY_CURRENT_USERettings may be defined using:

Description	ADM File Setting	Registry Value	Command Line
Enabled Determines if the SafeNet Authentication Client Log feature is enabled.	Not supported	**Registry Value Name:** Enabled **Value**: 1 - Enabled 0 - Disabled **Default**: 0 (Disabled)	
Days Defines the number of days log files will be saved from the time the log feature was enabled.	Not supported	Registry Value Name: Days **Value**: Enter the number of days (numerical). **Default**: 1 day	
MaxFileSize Defines the maximum size of an individual log file. Once the maximum fil size is reached, SAC removes older log records to allow saving newer log information.	Not supported	**Registry Value Name:** MaxFileSize **Value**: Enter a value in Bytes. **Default**: 2000000 (Bytes) (Approximately 2MB)	
TotalMaxSizeMB Defines the total size of all the log files when in debug mode. (Megabytes).	Not supported	**Registry Value Name:** TotalMaxSizeMB **Value**: Enter a value in Megabytes. **Default**: 0 (Unlimited)	
ManageTimeInterval Defines how often the TotalMaxSize parameter is checked to ensure the total maximum size has not been exceeded.	Not supported	**Registry Value Name:** ManageTimeInterval **Value**: Enter a value in minutes (numerical). **Default**: 60 minutes	

IdenTrust Settings

Description	ADM File Setting	Registry Value	Command Line
Override IdenTrust OIDs Overrides SAC's list of IdenTrust OIDs **Note:** Users must log on to their tokens whenever signing with a certificate defined as IdenTrust. To avoid having to authenticate every time a cryptographic operation is required for certificates containing IdenTrust OID, and Entrust details, remove the OID value from the registration key value.	**Setting name:** Override IdenTrust OIDs **Value**:The following settings are written to the appropriate folder's `SafeNet\Authentication\SAC\Identrust` registry key. Empty **Default**: No override	**Registry Value Name:** IdentrusIdentity **Value**: Empty **Default**: No override	Cannot be set by command line installation.