THALES

SafeNet Authentication Client

WINDOWS ADMINISTRATOR GUIDE

Document Information

Product Version	10.8 (R6) GA
Document Number	007-013560-005
Release Date	October 2021

Revision History

Revision	Date	Reason
Rev. H	October 2021	Updated for 10.8 (R6) GA release

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.

Thales Group 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 Thales Group be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales Group products. Thales Group disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service, or loss of privacy.

CONTENTS

PREFACE: About this Document

This document describes the operational and administrative tasks you can perform to maintain the functionality and efficiency of your SafeNet Authentication Client.

This section also identifies the audience, explains how to best use the written material, and discusses the documentation conventions used. They are:

For information regarding the document status and revision history, refer to "Document Information" on page 2.

Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure. This includes SafeNet Authentication Client users and administrators.

All products manufactured and distributed by Thales Group are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

It is assumed that the users of this document are proficient with security concepts.

Document Conventions

This section describes the conventions used in this document.

Command Syntax and Typeface Conventions

This document uses the following conventions for command syntax descriptions, and to highlight elements of the user interface.

Format	Convention
bold	The bold attribute is used to indicate the following: > Command-line commands and options that you enter verbatim (Type **dir /p**.) > Button names (Click **Save As**.) > Check box and radio button names (Select the **Print Duplex** check box.) > Dialog box titles (On the **Protect Document** dialog box, click **Yes**.) > Field names (**User Name**: Enter the name of the user.) > Menu names (On the **File** menu, click **Save**.) (Click **Menu** > **Go To** > **Folders**.) > User input (In the **Date** box, type **April 1**.)
italics	In type, the italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[**optional**] [<optional>]	Represent optional **keywords** or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.
{**a**|**b**|**c**} {<a>|<b>|<c>}	Represent required alternate **keywords** or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.
[**a**|**b**|**c**] [<a>|<b>|<c>]	Represent optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.

Notifications and Alerts

Notifications and alerts are used to highlight important information or alert you to the potential for data loss or personal injury.

Tips

Tips are used to highlight information that helps to complete a task more efficiently.

> **TIP** This is some information that will allow you to complete your task more efficiently.

Notes

Notes are used to highlight important or helpful information.

> **NOTE** Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss.

> **CAUTION!** Exercise caution. Contains important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury.

> ****WARNING** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.**

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Thales Group Customer Support.

Thales Group 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 Thales Group and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone

The support portal also lists telephone numbers for voice contact (Contact Us).

CHAPTER 1: Introduction

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

With full backward compatibility and incorporating features from previous middleware versions, SACensures complete support for all currently deployed eToken devices, as well as IDPrime and .NET smart cards.

Overview

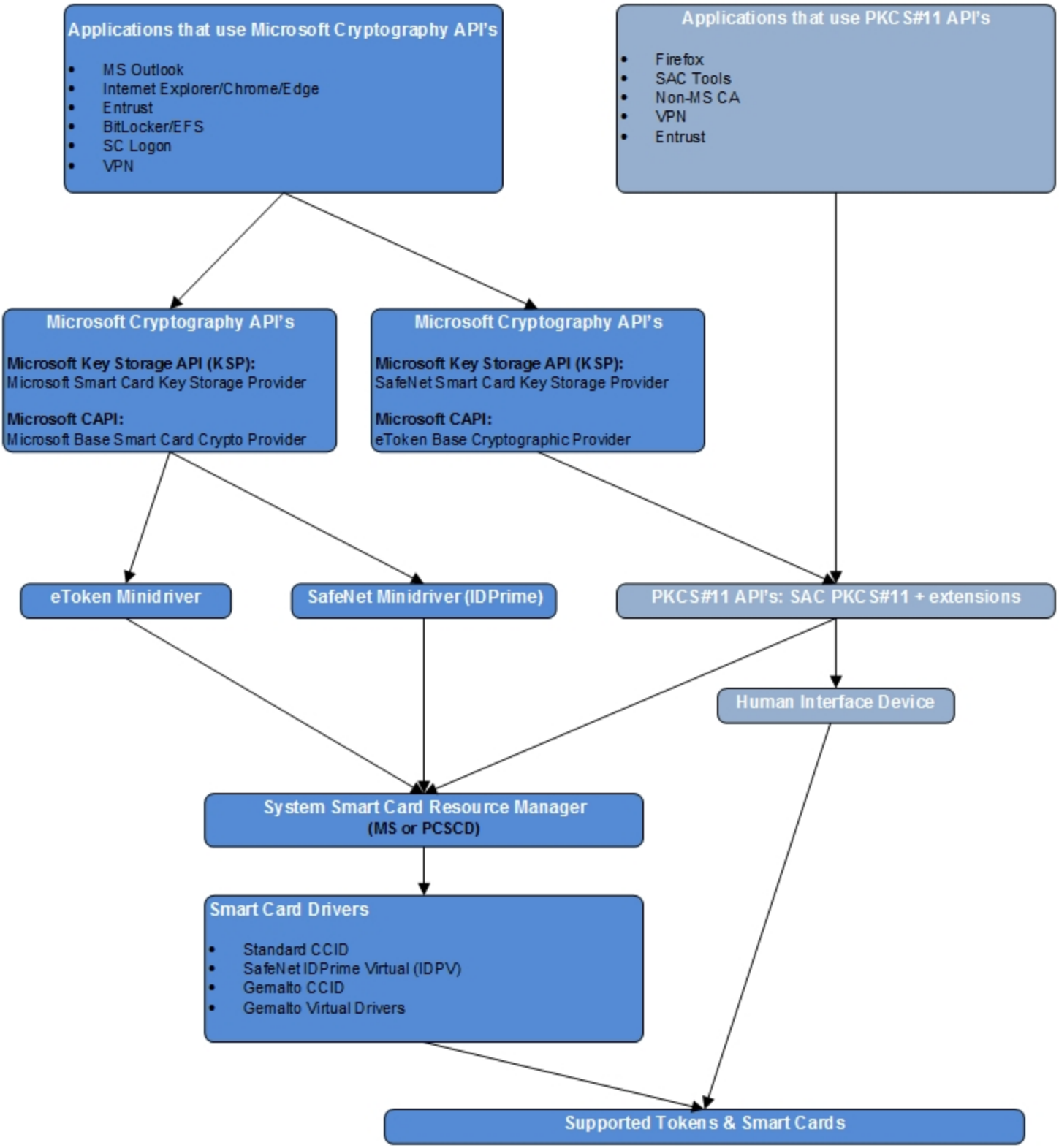
SAC is Public Key Infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities. It utilizes a system of digital certificates, Certificate Authorities, and other registration authorities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

SAC 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.

SAC 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.

API Flow



Password Quality Information

SAC supports password quality settings for Administrator Passwords (also known as Security Officer (SO) passwords) and Initialization Keys that are implemented by SafeNet Authentication Client software. The setting is the same for all devices and cannot be modified. Though, it can be switched off for backward compatibility.

Additionally, IDPrime supports the insertion of the Administrator Key directly (without derivation), in which case the password policy is not validated. The Administrator Key derivation method is proprietary and may vary depending on the device.

The Administrator Password quality and Initialization Key quality must include three out of the following four rules:

- English uppercase letters (ASCII 0x41...0x5A)
- English lowercase letters (ASCII 0x61...0x7A)
- Numeric (ASCII 0x30...0x39)
- Special characters (ASCII 0x20...0x2F + 0x3A...0x40 + 0x5B...0x60 + 0x7B...0x7F)

For backward compatibility, the Administrator Password quality check can be switched off through the SAC `pqAdminPQ` property.

Initialization Key password quality check cannot be switched off.

> **NOTE**
>
> The Password quality is in use only when the Administrator Password and Initialization Keys are used in a 'Friendly' (textual) format. For more information, refer to the Friendly Admin Password section in *SafeNet Authentication Client User Guide*.
>
> eToken 5110 FIPS and eToken 5110 devices support only 'Friendly Admin' passwords.
>
> If a customer does not want to be compliant with these PIN Quality policies, use hexadecimal keys (also through SAC UI and SAC API). Friendly Admin PIN length can be 24 binary or 48 hexadecimal. The Initialization Key length can be 32 binary or 64 hexadecimal. In this case, the keys are used as-is (without derivation) and PIN Quality will not be checked.

SAC supports password quality settings for the User PIN. The implementation of these settings may differ on various devices. User PIN policies can be created or modified during a device's initialization process or during the device's life cycle after Administrator (SO) authentication

Depending on the device model (for example: IDPrime or eToken devices) and initialization mode that was set (for example: the device was initialized without password policies), password quality policies can be enforced by the device or by the middleware software (SAC).

Device Type	Where the policy is stored:	Policy is enforced by:
eToken 5110 GA eToken 5110 FIPS	Depends on how the device was formatted: On board SAC configuration	Middleware

Device Type	Where the policy is stored:	Policy is enforced by:
IDPrime MD 840/3840 SafeNet IDPrime 940/3940 eToken 5110 CC	On board	Middleware (except for the PIN length, which is validated on board)
IDPrime MD 830/3811 SafeNet IDPrime 930/3930 eToken 5300	On board	On board

NOTE Each device (IDPrime / eToken) has a different policy setting. For more information, refer to the Token Settings chapter in *SafeNet Authentication Client User Guide*.

The SAC Client Settings policy is currently used only on eToken 5110 GA and 5110 FIPS. This policy is used in the following cases:

- The device was initialized without on board policies
- The default values used during the device initialization flow

PIN Retry Counter

Setting the Administrator/User PIN Retry Counter may vary depending on your device type:

Administrator PIN Retry Counter

- **Gemalto IDPrime MD 840 -** The Administrator PIN retry counter cannot be modified on this device.
- **SafeNet IDPrime 940/3940 -** The Administrator PIN retry counter is supported. The parameter is configured during factory settings and therefore cannot be modified.
- **Gemalto IDPrime MD 830 B / SafeNet IDPrime 930/3930 -** The Administrator PIN retry counter is supported. The parameter can be modified using SAC.

User PIN Retry Counter

SafeNet eToken 5110 FIPS or SafeNet eToken 5110 - Due to an eToken applet limitation, the User PIN Retry counter cannot be set on these smart cards, unless they are initialized.

PIN History Settings

Implementation differences exist in SAC as to how devices run IDPrime and eToken applets:

- Devices that run eToken applets - old password hashes are remembered
- Devices that run IDPrime applets - old and new password hashes are remembered

To reach the same behavior, set the History Size for IDPrime devices to '+1'.

NOTE The Pin History feature is not supported on IDPrime Common Criteria devices.

Collecting SAC Logs and MS TraceLogging

Collecting SAC logs allow administrators and technical-support personnel to diagnose the source of many problems that may have occurred while working with SafeNet Authentication Client. This information is used for debugging purposes.

SAC logs can be collected through either one of the following methods:

- SAC GUI (SAC Tools)
- SAC Registry
- MS Event Viewer

To enable SAC logs through SAC GUI (SAC Tools)

Perform the following steps:

1. Open **SafeNet Authentication Client Tools** > **Advanced View**.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced tab**.
4. Click **Enable Logging**.
5. The button changes to: Disable Logging. (For more information, refer to Client Settings > Enable Logging in *SafeNet Authentication Client User Guide*.
6. Restart the application that requires the debug log to be created.

To enable SAC logs through the registry

Perform the following steps:

1. Create the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC\Log
"Enabled"=dword:00000001
"maxfilesize"=dword:0c800000
"days"=dword:0000016d
```

2. To collect all events, reboot the machine (Ensure the reboot is performed prior to collecting logs).

> **NOTE** SAC Log files are created in the following directory `%WinDir%\Temp\eToken.log`.

For more details, refer to the following sections:

- **Enable Logging Control** "SafeNet Authentication Client Tools UI Settings" on page 99
- **Enable Log Events** "SafeNet Authentication Client Tools UI Settings" on page 99"Log Settings" on page 146
- **Enable Log Settings** "Log Settings" on page 146

> **NOTE** To read SAC logs, use the Log Viewer that is part of the SafeNet Authentication Client Developer's Guide (SDK).

To trace SAC events through the MS Event Viewer

Create the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC\General
"EnableLogEvents"=dword:00000001
```

SAC Monitor Propagation

When installing SAC together with SACMonitor (tray icon process), SAC Monitor is responsible for the propagation of certificates . This functionality can be disabled using specific SAC properties (refer to "Certificate Store Settings" on page 113).

Windows 'Certificate propagation' service also executes certificate propagation. This functionality is disabled by stopping Windows 'Certificate propagation' service and selecting disable the service from the *Properties* option.

> **TIP** It is recommended to use only one of these methods on the same machine as using both may cause overlapping of the propagation functionality.

SACMonitor and MS Certificate Store

SACMonitor periodically checks the personal certificate store status and performs either one of the following:

- **Adding a Certificate -** When a new certificate is added to the personal certificates store, the new certificate is stored on the connected device.

  This behavior can be disabled using specific SAC properties. Refer to the **Add New Certificates to Token** property in "Certificate Store Settings" on page 113

- **Removing a Certificate -** When the certificate is removed from the Personal Certificates Store, the certificate is removed from the connected device.

  This behavior can be disabled using specific SAC properties. Refer to the **Remove Certificates from Token upon Removal from Store** property in "Certificate Store Settings" on page 113

- **Updating a Certificate -** When a certificate's properties (such as Archived or FriendlyName) are updated in the personal certificates Store by any 3rd-Party application, the exact same update is executed to the properties of the same certificate on the connected device.

  This behavior can be disabled using specific SAC properties. Refer to the **Synchronize Store** property in "Certificate Store Settings" on page 113

When a device is connected:

All personal certificates stored on the device are propagated to the personal certificates store. This behavior can be disabled using specific SAC properties. Refer to the **Propagate User Certificates** property in "Certificate Store Settings" on page 113.

CA certificates can also be copied from the device to the store by defining specific SAC properties. Refer to the **Propagate CA Certificates** property in "Certificate Store Settings" on page 113

When a device is disconnected:

All certificates that were stored on the device are removed from the personal certificates store. This behavior can be disabled using specific SAC properties. Refer to the **Remove User Certificates upon Token Disconnect** property in "Certificate Store Settings" on page 113

Propagating Archived certificates and FriendlyName:

3rd-Party tools and utilities can be used to display certificate data in the personal certificates store, including certificate properties, such as archived certificates and FriendlyName.

SAC does not set these properties as it updates the personal certificate store with the certificate properties stored on the device. This is based on the values that are updated when a new certificate is enrolled.

CHAPTER 2: SingleLogon & Single Sign On (SSO)

Both the SingleLogon and Single Sign On (SSO) features are used to prevent users from inserting device passwords/PIN every time a cryptographic operation is required. SingleLogon is the preferred method to use, while SSO is supported for backward compatibility purposes. Both SingleLogon and SSO are supported only on Windows Operating Systems.

The SSO mode is defined on a smart card per PIN and is supported when SafeNet Minidriver is installed on it's own (i.e. without SACSrv). For details on whether or not the device supports SSO, refer to the device specifications.

SingleLogon mode configuration is per machine, it supports all APIs and requires SACSrv to run (i.e. cannot run on a machine that has only SafeNet Minidriver installed).

SingleLogon

SingleLogon is a SafeNet Authentication Client (SAC) feature that determines if the user's Token Password is requested only once for applications that use MS Cryptography (CAPI/CNG/Minidriver) and PKCS#11 Cryptography.

- SingleLogon is not supported when using PIN Pad readers.
- To activate SingleLogon to start from Windows Logon, define the SingleLogon setting in: HKEY_LOCAL_MACHINE.
- If the setting is defined in: HKEY_CURRENT_USER, the SingleLogon feature will be activated only after the you log into the device again.
- If the SingleLogon setting is defined through SAC Tools, it is set in: HKEY_CURRENT_USER. This means that SingleLogon is not active from Windows Logon.
- SingleLogon has 3 configuration modes: 0=SingleLogon is off 1=SingleLogon for MS Cryptography (excluding Minidriver) 2=SingleLogon for all SAC applications (CAPI/CNG/Minidriver/PKCS#11).
- Even though SingleLogon is configured to support MS Cryptography (value=1) the PKCS#11 application can us this functionality if C_Login is called with PIN=NULL (this is non-standard behavior).
- The SingleLogon feature is also supported when configured through the SAC Customization Tool. For more information, refer to "Customization" on page 25.

> **NOTE** To disable the SingleLogon option in SAC Tools (i.e. the option is made unavailable), set the following in the registry:
> `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SafeNet\Authentication\SAC\GENERAL DWORD: SingleLogon value=0`

SingleLogon and SSO Behavior Differences

Below table displays the behavioral differences between SingleLogon and SSO.

MD / PKCS#11	SSO	SingleLogon Minidriver	SingleLogon PKCS#11
CardAuthenticate / C_Login	Logon to card	Logon to card + save PIN to SingleLogon	Logon to card + save PIN to SingleLogon
CardDeauthenticate / C_Logout	skip	Logout from card	Logout from card + clean the SingleLogon saved PIN
CardGetProperty ("Authenticated State") / C_ GetSessionInfo	card in login	Get password from SingleLogon, login and report "in login" state	Get password from SingleLogon, login and report "in login" state

SSO Deactivation Option

Windows operating systems come with a power saving mode by default. This feature sends the **Power Off** command (63 00 00 …) to the reader after about 20-30 seconds after any transaction to the smart card is completed.

When this command is sent to the reader, the reader essentially powers off the card, which triggers the SSO to be deactivated. As a workaround, you can configure the registry key to change the delay period, so that the OS sends the command after a longer period of inactivity.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\calais\
"CardDisconnectPowerDownDelay"= dword:xxh
```

Type: `REG_DWORD`

Value: `xx` is the delay period in seconds.

To modify the registry key, use the registry editor (from Start > Run, type regedit).

Differences between PIN Policy SSO, Session PIN,PIN Caching and SingleLogon

Below table describes the PIN caching options available on IDPrime 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 users already using this feature. It is recommended that you use the SAC SingleLogon feature instead.	> Works only through 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 and .Net cards are compliant with Session PIN through the SafeNet Minidriver . For IDPrime 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 through SAC Tools. There are 4 modes that can be applied (Refer to "PIN Caching Modes" on the next page) PIN Cache Normal is the default configuration for IDPrime devices.

Feature	Description	Configuration Level
SingleLogon **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 through the SAC Customization Tool (SafeNet Minidriver profile). For more information refer to"Customization" on page 25.	> The SingleLogon feature is a software based solution driven by SAC and is not connected to PIN Policy SSO or to PIN Caching. > SingleLogon can be configured per process both SafeNet CSP/KSP & PKCS#11. For more details, refer to the SingleLogon section under"General Settings" on page 71 > When Single Sign On (on the card) is present, the behavior is overridden by the SingleLogon (configured in software).	SingleLogon is configurable through SAC Tools, SafeNet Authentication Client Customization Tool or through GPO.

PIN Caching Modes

PIN Caching Modes are available on IDPrime 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.

Cache Mode	Description
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`.

CHAPTER 3: Common Criteria

The IDPrime Applets 4.0, 4.2, 4.4 are Common Criteria certified on Common Criteria based smart cards and tokens. These devices can have certain parameters customized in the factory with values that differ from the default profile. For a detailed list of supported cards, refer to *SafeNet Authentication Client Release Notes*

> **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

The following are the default settings. For other options consult your Thales representative.

By default, the IDPrime 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 EC Keys
- 8 X 2048-bit CC Sign and Decrypt RSA Keys

- 2 X 1024-bit CC Sign and Decrypt RSA Keys
- 2 X 4096-bit CC Sign and Decrypt RSA Keys
- 2 X 1024-bit CC Sign and Decrypt EC Keys

> **NOTE** The Key Generation method for Common Criteria key containers is either OBKG or Key import.

Common Criteria API Adjustments

Below table provides a high-level description of the adjustments that can be made to the Standard and Extended PKCS#11 API to work with IDPrime Common Criteria devices. For more detailed information, refer to 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 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 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.

Standard PKCS#11 API	Extended PKCS#11 API
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. For details on Friendly Admin Password, refer to *SafeNet Authentication Client User Guide* . > 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.

CHAPTER 4: Customization

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

> **NOTE** .Net Framework 3.5 is required on all operating systems when running the SafeNet Authentication Client Customization Tool.

Overview

You can customize the following SAC 10.8 (R6) 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
- SafeNet Authentication Client and SafeNet Minidriver features to be installed
- Policy settings
- MSI Signing settings
- Window banners

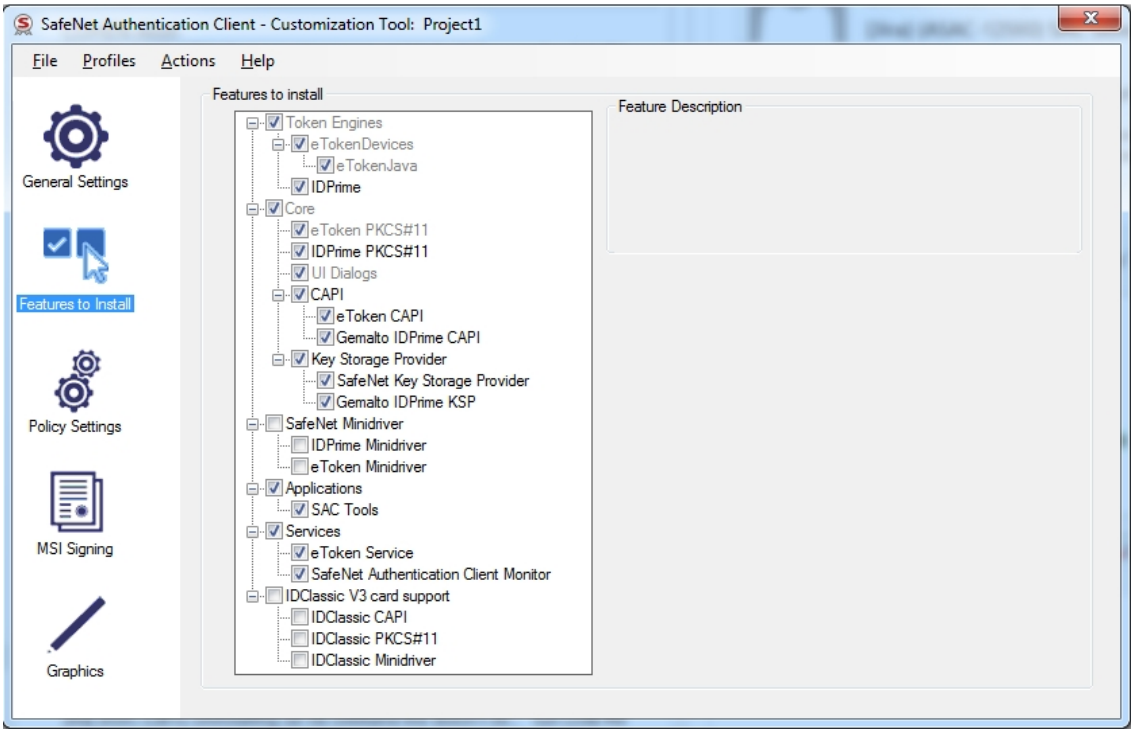
SAC Customization Tool Profiles

SAC Customization Tool has two 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 SAC using the installation wizard.



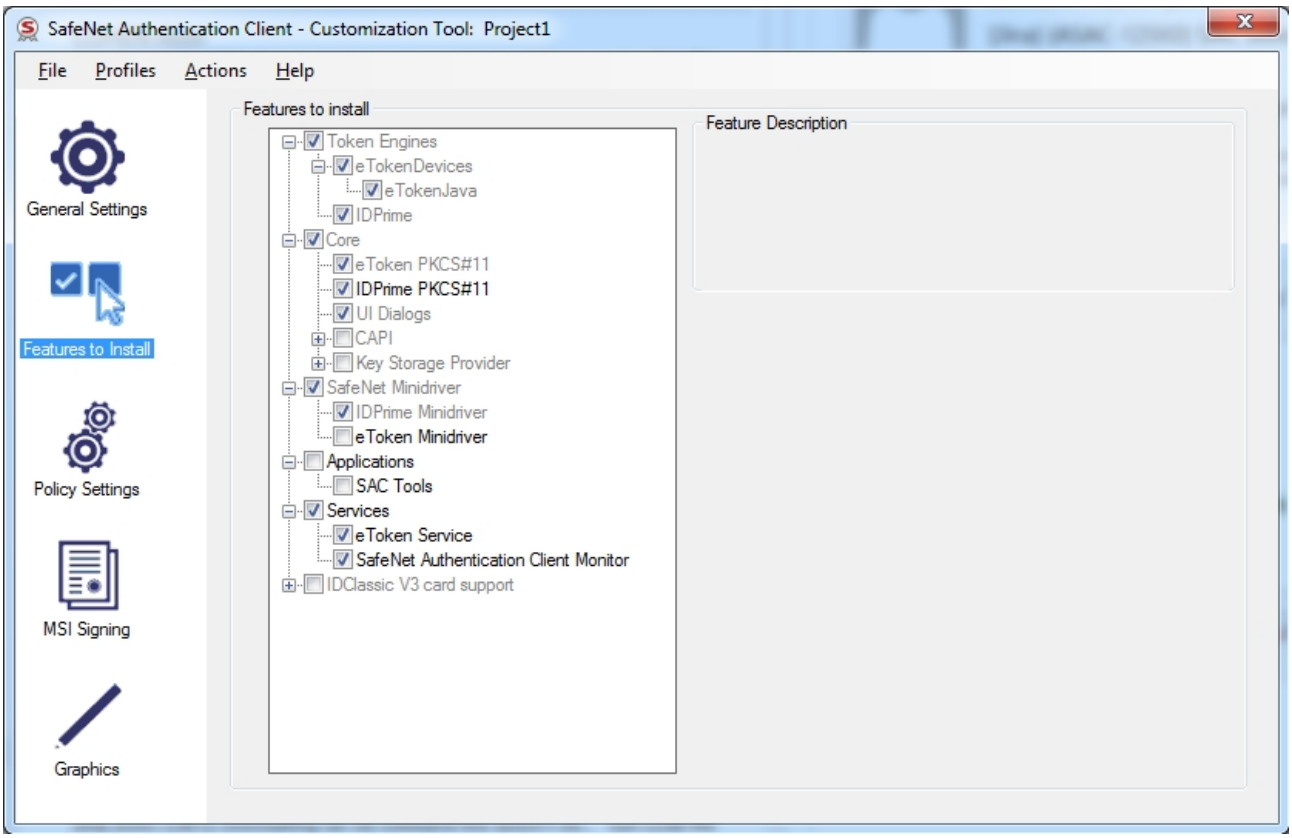
SafeNet Minidriver Profile

Mainly for Thales 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



Configuring SafeNet Minidriver profile for Backward Compatibility

SAC 10.8 (R6) GA Customization Tool enables you to generate an .msi file, which contains SafeNet Minidriver 10.8 (R6) GA as well as PKCS#11 proxy. When selecting the SafeNet Minidriver profile, the following dll files are installed under:

Dll File	Description	Path
IDPrimePKCS11.dll	x32 PKCS#11 library stub for Gemalto IDPrime cards.	`C:\Program Files\SafeNet\Authentication\SAC\x32` and `C:\Program Files\Gemalto\IDGo 800 PKCS#11` **NOTE** The path with the Gemalto folder is for backward compatibility purposes.
IDPrimePKCS1164.dll	x64 PKCS#11 library stub for Gemalto IDPrime cards.	`C:\Program Files\SafeNet\Authentication\SAC\x64` and `C:\Program Files (x86)\Gemalto\IDGo 800 PKCS#11` **NOTE** The path with the Gemalto folder is for backward compatibility purposes.
axaltocm.dll	A wrapper of the SafenetMD.dll (for backward compatibility). For 64 bit system.	`C:\Program Files\SafeNet\Authentication\SafeNet Minidriver and C:\Windows\SysWOW64`
axaltocm.dll	A wrapper of the SafenetMD.dll (for backward compatibility). For 32 bit system.	`C:\Program Files\SafeNet\Authentication\SafeNet Minidriver and C:\Windows\System32`

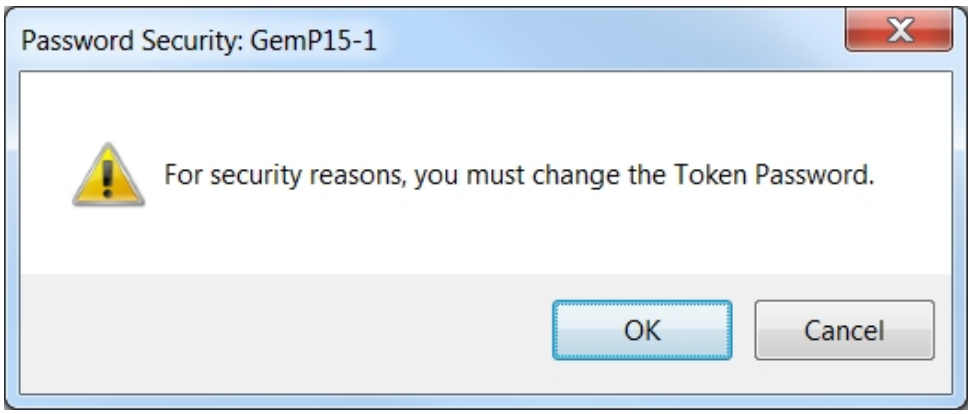
Must Change Password at First Logon

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

Perform the following steps to change the password at first logon:

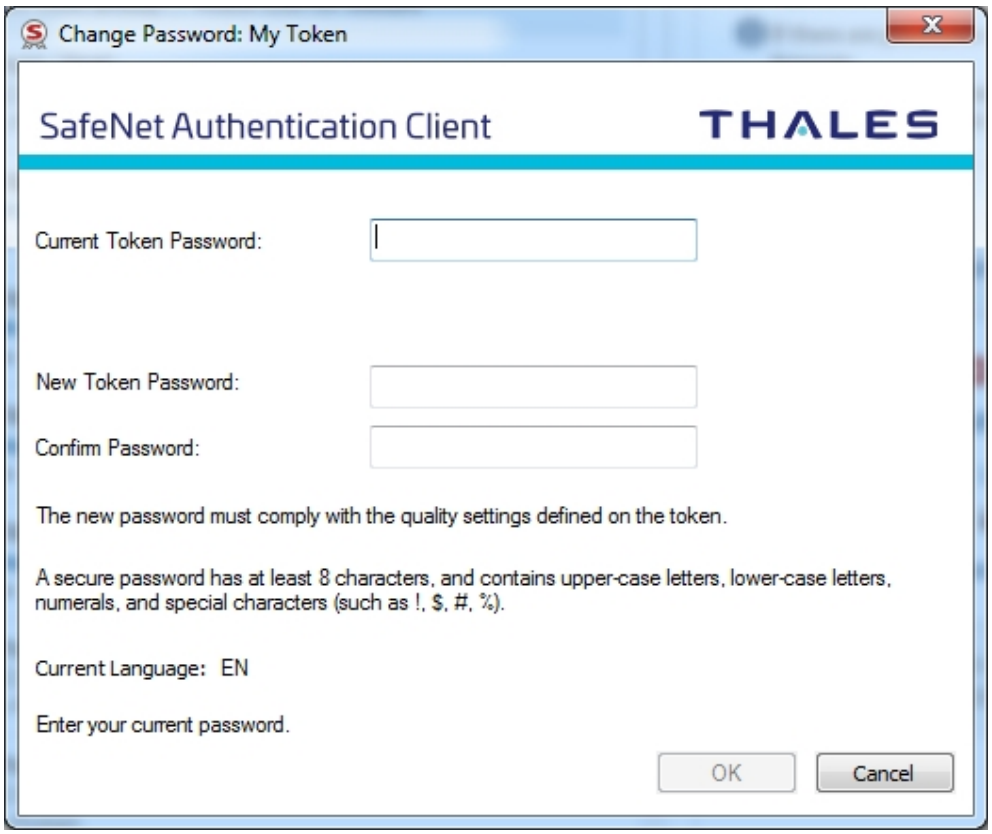
1. Connect the device.

   The **Password Security** window is displayed.



2. Click **OK**.

   The **Change Password** window is displayed.



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 SAC make up the IDClassic 340 (V3) card's PIN Policy.

> **NOTE** The default PIN minimum length in SAC is 8 therefore, the next password must have at least 8 digits.

Installing the SAC Customization Tool

Before installing SAC, install the SAC Customization Tool.

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

Perform the following steps to install the SAC Customization Tool:

1. Double-click **SACCustomizationPackage-10.8-R6**.

   The **SafeNet Authentication Client Customization Package Installation Wizard** is displayed.
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 is displayed, showing the default installation folder.
5. You can click **Browse** to select a different destination folder, or install the Customization Tool's SACAdmin 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 **Ready to Install the Program** window is displayed.
6. Click **Install** to start the installation.

   When the installation is complete, the **SafeNet Authentication Client Customization Package has been successfully installed** window is displayed.
7. Click **Finish** to exit the wizard.

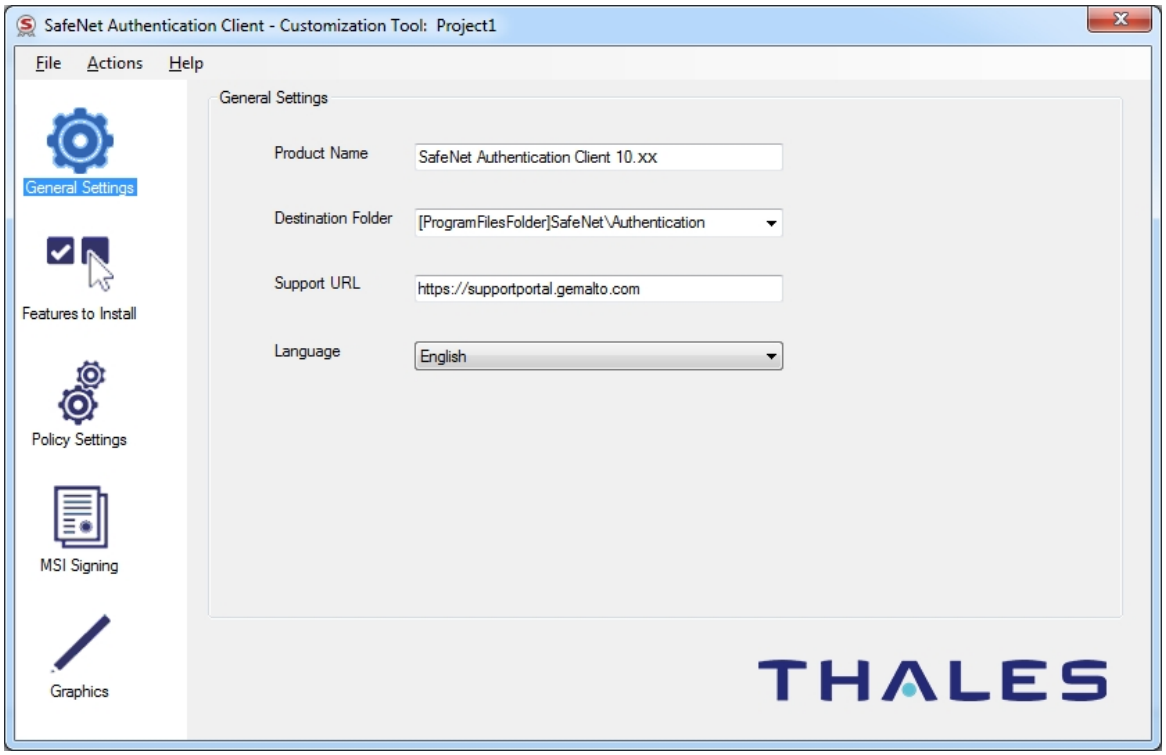
Using the SAC Customization Tool

After installing the SAC Customization Package, customize the appropriate features.

Perform the following steps 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.

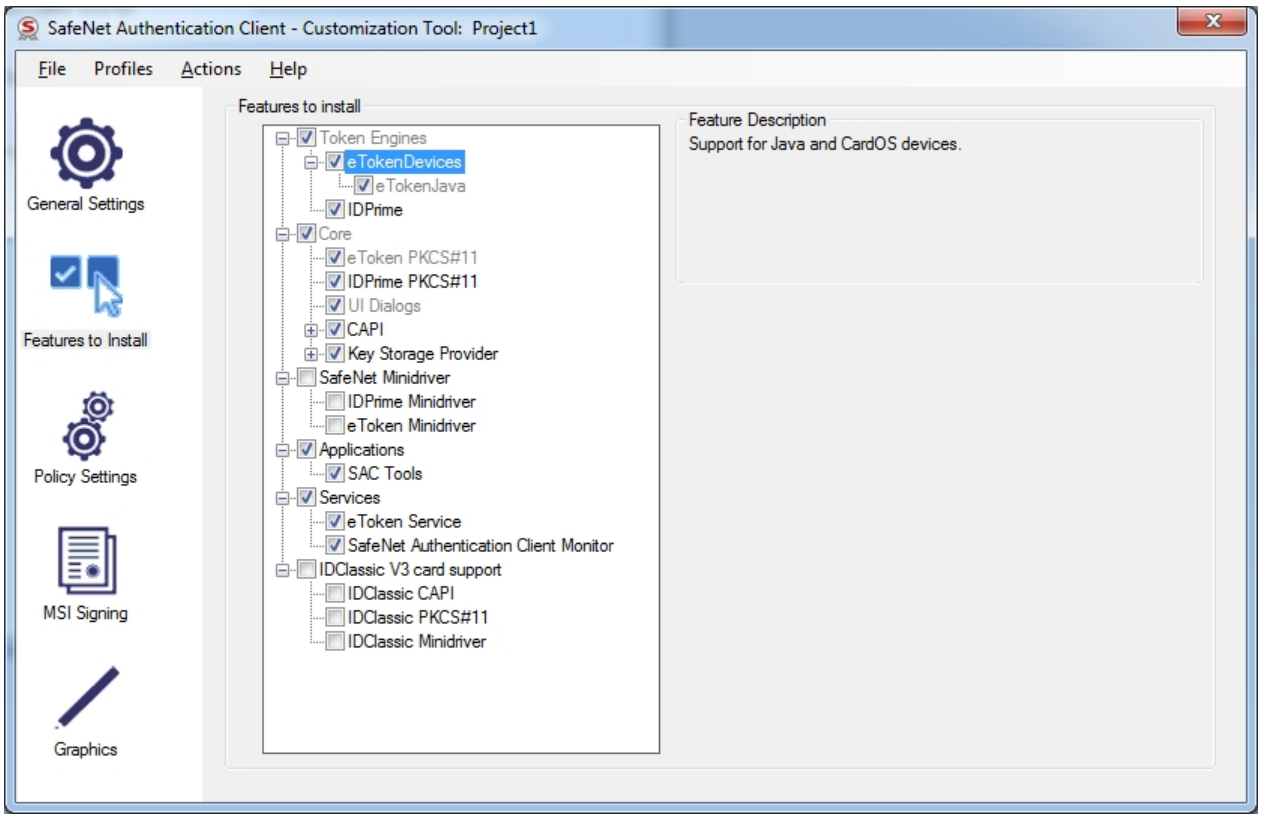
   > **NOTE** Due to the changes implemented in the SAC 10.8 Customization Tool, opening an `xml` file saved with earlier versions of SAC is not supported.

3. You can replace the following items:
   - **Product Name:** Enter the relevant product name (the default value is SafeNet Authentication Client 10.8).
   - **Destination Folder:** Enter the path to be used by the SAC Customization Tool when no other SafeNet product has been installed on the client computer
   - **Support URL:** Enter 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 SAC to 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.

In the left column, select the **Features to Install** tab.

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

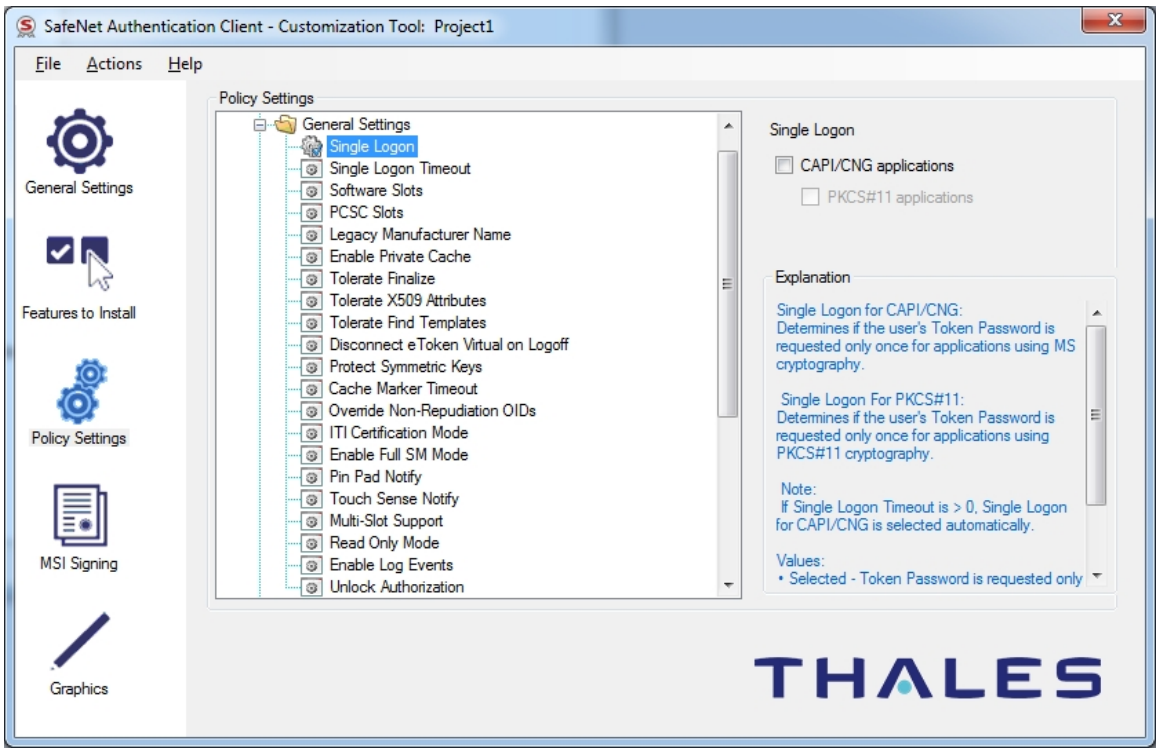


4. The features may be customized by changing the editable check-boxes.

> **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.

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

   The **Policy Settings** window is displayed.



6. 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`.

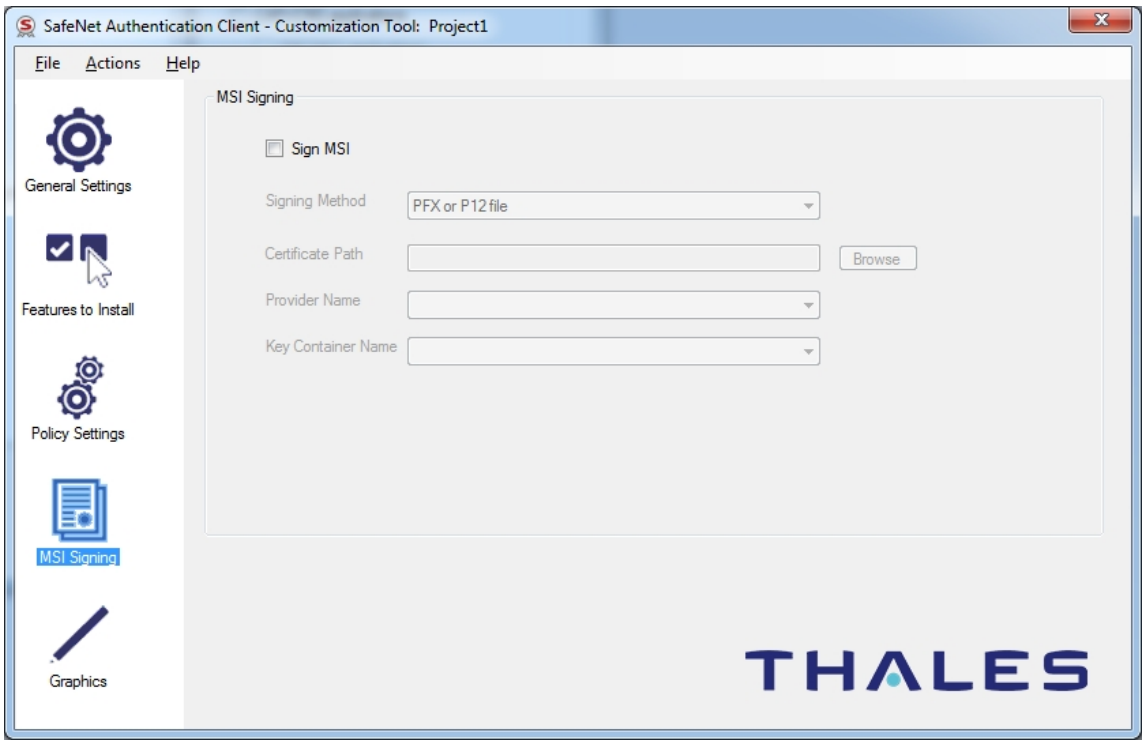
   For more information, refer to "Configuration Properties" on page 68.

   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 cards. For more details, refer to "Configuration Properties" on page 68.

7. In the left column, select the **MSI Signing** tab.

   The **MSI Signing** window is displayed.



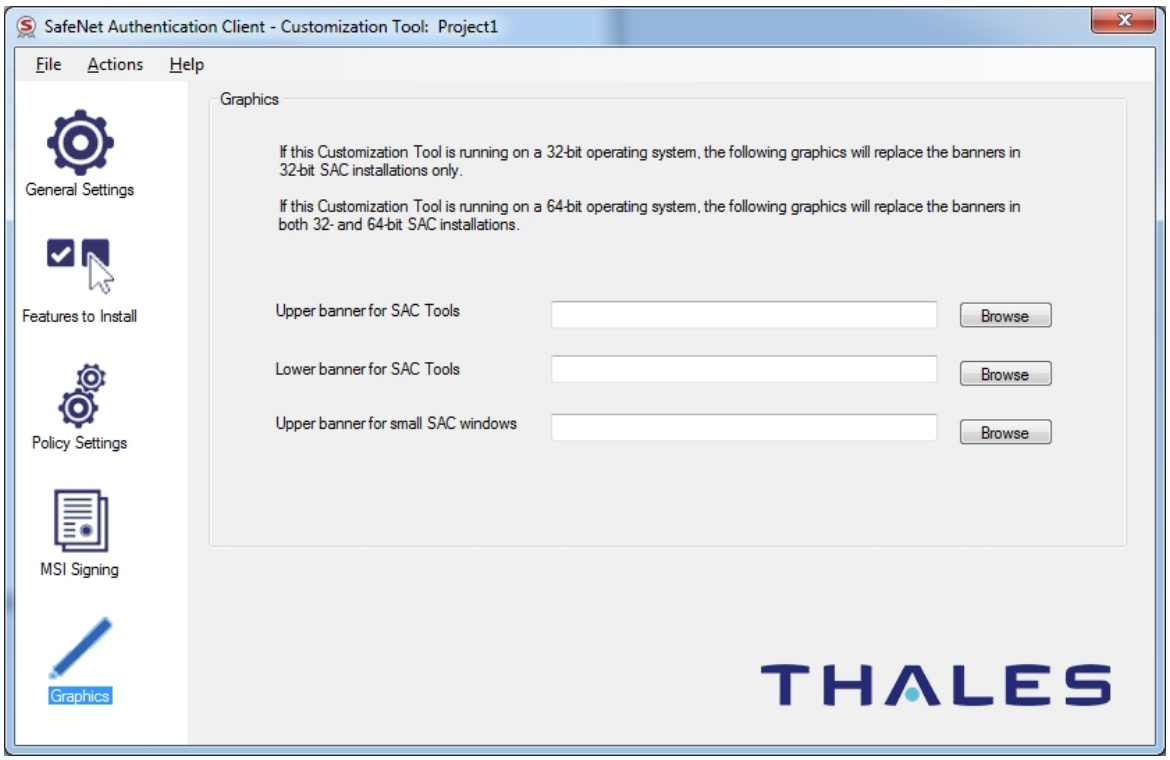
To sign the installation file, select Sign MSI, and complete the enabled fields. These may include:

- Signing Method (P12, smart card 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 signed using the SHA 2 algorithm.

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

   The **Graphics** window is displayed.



> **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.

9. To change a banner, click **Browse**, and select the graphic file required.
10. 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]`

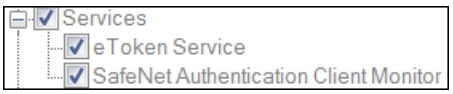
Features to Install

This section covers a few SAC Customization Tool installation features.

For more details on what binary files are installed and their location, refer to "SafeNet Authentication Client Binary Files" on page 44.

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).

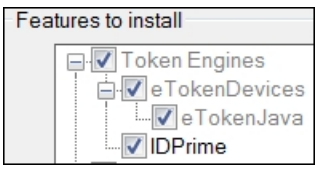
If the above options are selected, the following files are installed:

- `SACTools.exe`
- `SACMonitor.exe`

Token Engines

Installs token engines to support Java 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:

- `IDPrimeTokenEngine.dll` - IDPrime token/card engine

Generating a Customized MSI Installation File

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

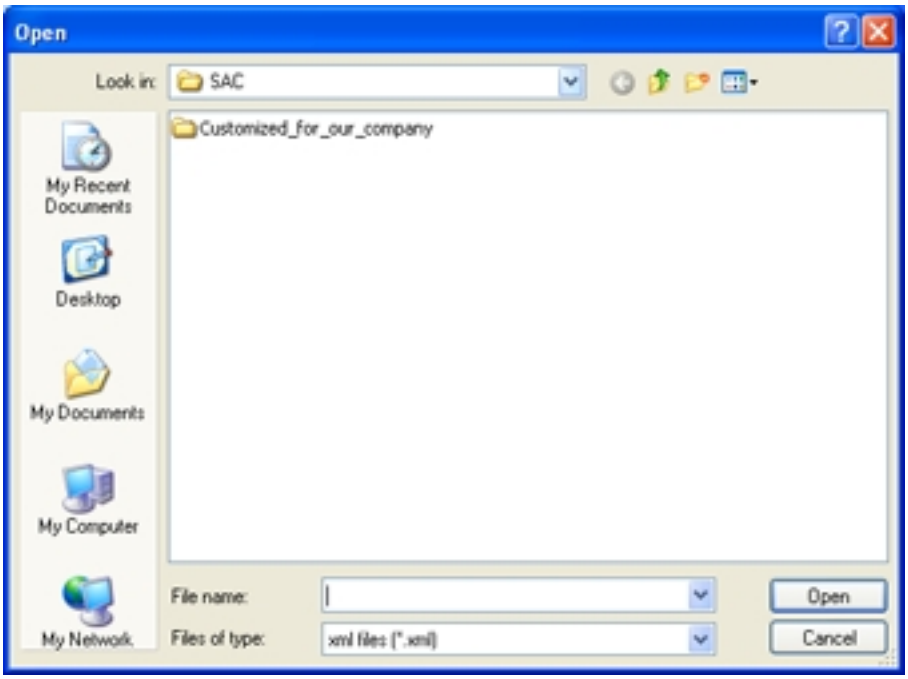
> **NOTE** Generating an MSI file can be performed with administrator privileges only.

Perform the following steps to generate a customized installation file:

1. Open the **SAC Customization Tool**.

   Refer to "Using the SAC Customization Tool" on page 31.

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 10.8 (R6) GA 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>-x32-10.8-R6.msi` for 32-bit installations
   - A file named `<Project Name>-x64-10.8-R6.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.

Perform the following steps 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 38.

   > **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>-x32-10.8-R6.msi` (for 32-bit installations)
   - `<Project Name>-x64-10.8-R6.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

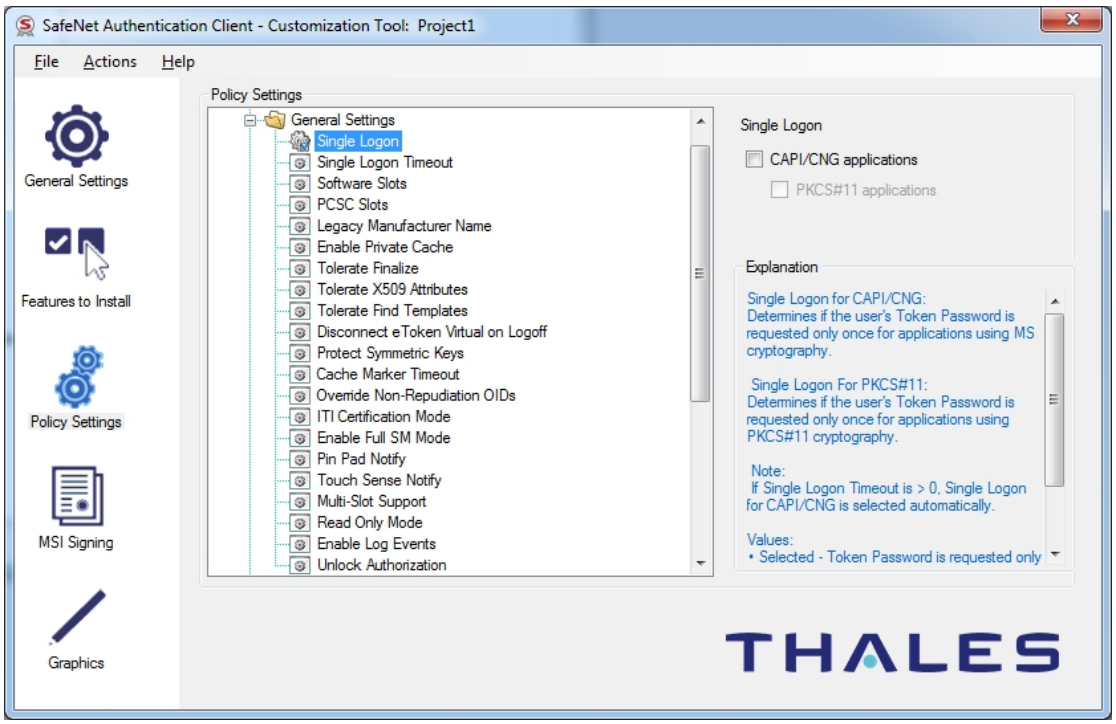
Follow the procedures below to set the Password Minimum Length property as a permanent value.

Perform the following steps to change the password minimum length permanently:

1. Open the SAC Customization Tool.

   Refer to "Using the SAC Customization Tool" on page 31.
2. In the left column, select the **Policy Settings** tab.

   The **Policy Settings** window is displayed.



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.

Customized ICC Public Key

It is defined as a public key for IDPrime cards with a customized ICC Public key for Mutual Authentication. If enabled the communication between cards that have Customized ICC Public Key for Mutual Authentication and the terminal (SafeNet Authentication Client) is protected. Otherwise, SAC can communicate with cards that have a default ICC Public key for Mutual Authentication.

SAC has a built in, default public key that allows a secure communication channel between SAC and any IDPrime device that also has the same default ICC Public key.

To allow SAC to recognize and use the customized device, a customized SAC installation must be generated using the SAC Customization Tool (See below), ensuring that a Customized ICC Public Key is uploaded. There is change in behavior because now if Customized ICC Public Key is specified then Mutual Authentication works only with cards containing this key.

Connecting a device that has a Customized ICC Public Key into a terminal where standard SAC is installed (i.e. not installed through the SAC Customization Tool), displays the associated smart card with an exclamation mark as it is not recognized:

Enabling the Customized ICC Public Key Feature

Create a new SAC msi installation using the SAC Customization Tool with the Customized ICC Public Key feature enabled.

Perform the following steps to generate a customized SAC installation with the customized ICC public key feature:

1. Open the SAC Customization Tool.

   Refer to "Using the SAC Customization Tool" on page 31.

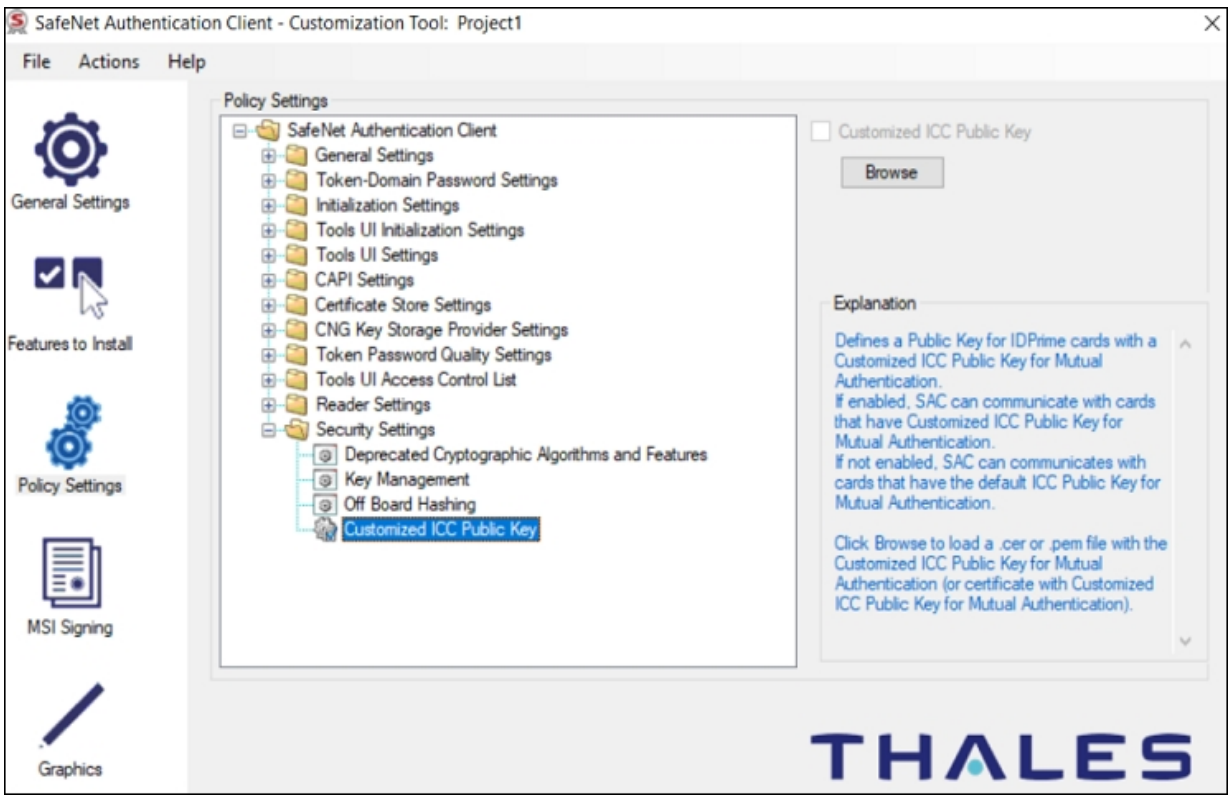
2. In the left column, select the **Policy Settings** tab.

   The **Policy Settings** window is displayed.

3. Expand the **Security Settings** node, and click **Customized ICC Public Key**.

4. Click **Browse** to load a **.cer** or **.pem** file that contains the Customized ICC Public Key for Mutual Authentication (or certificate with Customized ICC Public Key for Mutual Authentication).

> **NOTE** Ensure the uploaded .pem or .cer file includes the correct OID header. For example: 1.2.840.10045.3.1.7 (prime256v1(7)).



The Customized ICC Public Key check-box is selected and a new customized SAC installation is ready to be generated.

CHAPTER 5: Upgrade

It is recommended to upgrade earlier versions of SafeNet Authentication Client (SAC) to the latest version on each computer that uses SafeNet eToken, or SafeNet/Gemalto IDPrime devices. Local administrator rights are required to upgrade SAC.

> **NOTE**
> You must restart your computer when the upgrade procedure completes. When upgrading through 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 10.8 (R6) GA with the new feature list.

Upgrading Using the SAC .msi File

Use the following to upgrade from earlier versions of SAC using the msi file:

- On a 32-bit system, run `SafeNetAuthenticationClient-x32-10.8-R6.msi`.
- On a 64-bit system, run `SafeNetAuthenticationClient-x64-10.8-R6.msi`.

> **NOTE**
> Ensure that all SAC applications are closed before upgrading, installing, or uninstalling SafeNet Authentication Client.
>
> To upgrade SAC 10.8 (installed on Windows x32 OS through the Customization Tool) with SafeNet Minidriver, SAC 10.8 must be uninstalled before installing SAC 10.8 (R6) GA.

Upgrading from Versions Earlier than SAC 9.0

Legacy versions of SAC, earlier than 9.0 must be uninstalled before installing SAC 10.8 (R6) GA.

Upgrading from SafeNet Authentication Client 9.0

You can upgrade from SAC 9.0 to 10.8 (R6) GA using the MSI file wizard installation, or by using the command line installation. Refer to "Installing the MSI file through the Command Line" on page 55.

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

CHAPTER 6: Installation

Follow the installation procedures below to install SafeNet Authentication Client (SAC). 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: eToken readers and third-party readers.
>
> **Firefox Settings:** Before installing SAC, Firefox must be installed on the computer and opened at least once to make the registration available. To verify if the registration in Firefox is 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, refer to "Customization" on page 25.

Installation Files

The software package provided includes files for installing or upgrading to SAC 10.8 (R6) GA. The following installation and documentation files are provided:

File	Environ-ment	Description
Installation Files:		
SafeNetAuthenticationClient-x32-10.8-R6.msi	32-bit	Installs SafeNet Authentication Client 10.8 (R6) GA, and upgrades from earlier versions of SafeNet Authentication Client
SafeNetAuthenticationClient-x64-10.8-R6.msi	64-bit	
SACCustomizationPackage-10.8-R6.msi	32-bit 64-bit	Installs SafeNet Authentication Client 10.8 (R6) GA 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.

File	Environ-ment	Description
Documentation Files:		
007-013559-007-SafeNet Authentication Client_ 10.8 (R6) GA_Windows_Release Notes_Rev. H		SafeNet Authentication Client 10.8 (R6) GA 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 10.8 (R6) GA_Windows_User Guide_Rev. H		SafeNet Authentication Client 10.8 (R6) GA 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 10.8 (R6) GA_Windows_ Administrator Guide_ Rev. H		SafeNet Authentication Client 10.8 (R6) 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 SAC, 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	Includes third-party application files that are compiled with x32-bit.	
x64	> **eTokenHID.dll -** this file supports HID devices (only required for devices that are in HID mode). > **IDPrimeTokenEngine.dlll -** installs the DPrime token/card engine. > **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 > **Language support packages** (e.g. cs-CZ, fr-CA, etc.)	These folders contain Windows x32-bit and x64-bit related DLL's and packages. > 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 is shown in either x32 or x64 folders.
App-RTE	SafeNet Authentication Client icon	
SACHelp	SafeNet Authentication Client User Guide	This PDF file opens when clicking the Help icon in SAC Tools.

System32 and SysWOW64 Folders

All SAC DLL files that exist in the `System32` folder are compiled as x64-bit.

All SAC 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
`eToken.dll`	Installs SAC core files.
`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.

NOTE
For 64-bit installations - Both the `C:\Windows\System32` folder and `C:\Windows\SysWOW64` folders 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 through the SafeNet Authentication Client User Interface (About Window). For more information, refer to *SafeNet Authentication Client User Guide*.

IDPrime PKCS#11 Binary Files

IDPrime PKCS11 DLL files are located in the following folders:

> **SAC Folder:**

`C:\Program Files\SafeNet\Authentication\SAC\x32`

Or

`C:\Program Files\SafeNet\Authentication\SAC\x64` (This location is for applications that obtain SAC binaries dynamically).

> **Gemalto Folder:**

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

Or

`C:\Program Files (x86)\Gemalto\IDGo 800 PKCS#11` (This location is for backward compatiblity purposes).

DII File	Description
`IDPrimePKCS11.dll`	x32 PKCS#11 library stub for Gemalto IDPrime cards.
`IDPrimePKCS1164.dll`	x64 PKCS#11 library stub for Gemalto IDPrime cards.

IDClassic (V3) Binary Files in SAC

After installing legacy Classic Client side-by-side with SAC 10.8 (R6) GA, 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\SafeNet\Authentication\SAC\x32\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\SafeNet\Authentication\SAC\x64\IDPrimePKCS1164.dll`

is 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`

`C:\Program Files\SafeNet\Authentication\SAC\x32\IDPrimePKCS11.dll`

is added to support IDPrime cards in the future

Below table lists the files 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	These dlls provide compatibility with legacy IDGo800 middleware, especially with regards to multi-slot support feature. For details, refer to "Configuration Properties" on page 68.

Installation Configurations

SAC can be installed with either one of 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.
Minidriver Profile	Minidriver Profile - Installs cryptographic interfaces (PKCS#11 and Microsoft Minidriver) for supported devices.	Install SafeNet Minidriver. When using the installation wizard, select the **Minidriver Profile** 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 SAC 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 SAC 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 SAC applications are closed before upgrading, installing, or uninstalling SAC.

Perform the following steps to install SAC through the installation wizard:

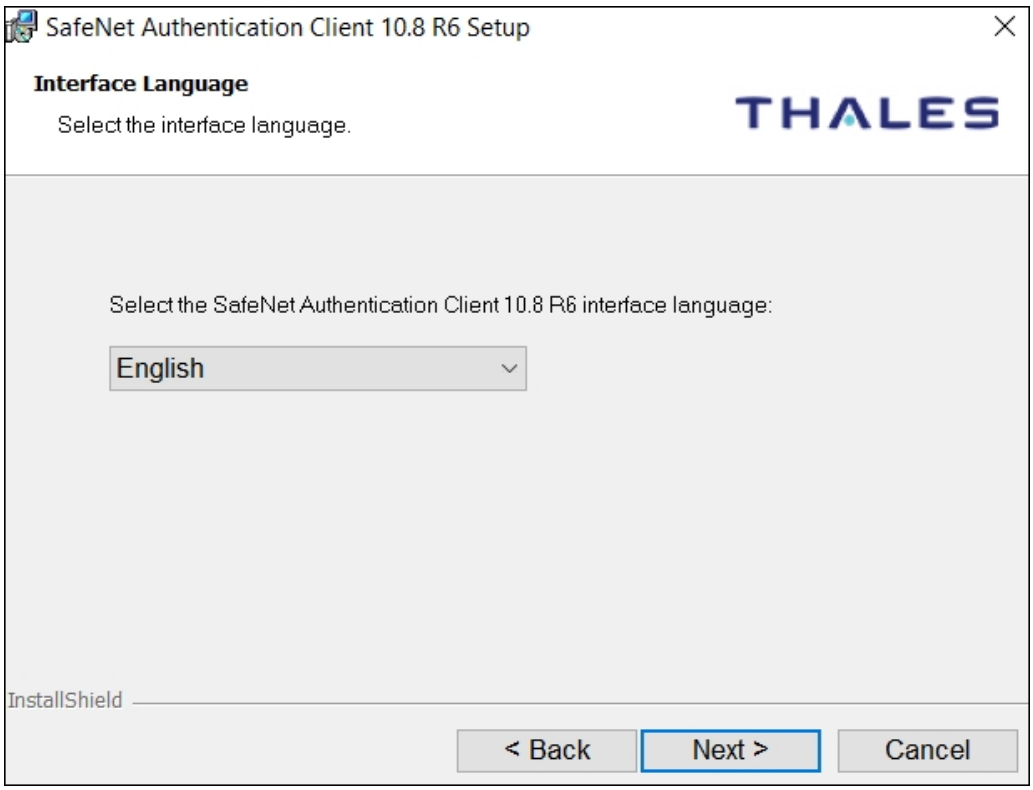
1. Log on as an administrator.
2. Close all applications.
3. Double-click the appropriate file:
   - `SafeNetAuthenticationClient-x32-10.8-R6.msi` (32-bit)
   - `SafeNetAuthenticationClient-x64-10.8-R6.msi` (64-bit)

   The **SafeNet Authentication Client Installation Wizard** is displayed.

4. Click **Next**.

The **Interface Language** window is displayed.

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

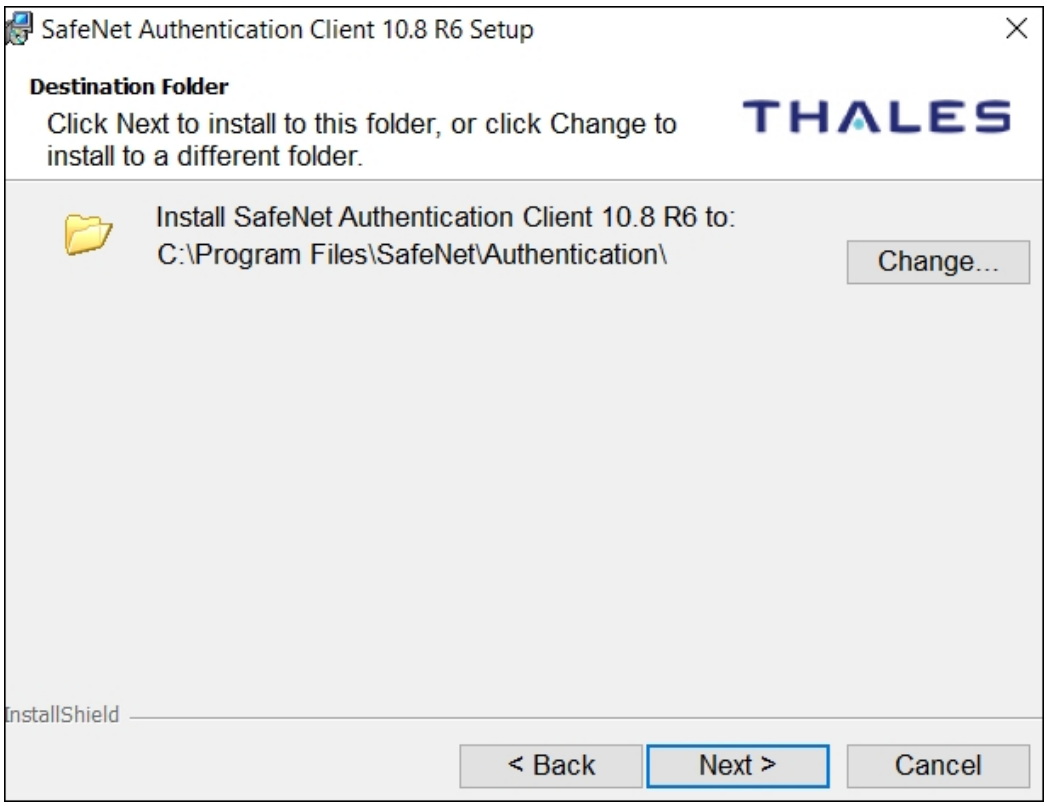


5. From the drop-down list, select the language in which you want the SAC screens to appear.
6. If configuration settings are detected from a previous version, you can select **Use the existing configuration settings**.
7. Click **Next**.

   The **End-User License Agreement** is displayed.

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

   The **Destination Folder** window is displayed, showing the default installation folder.



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

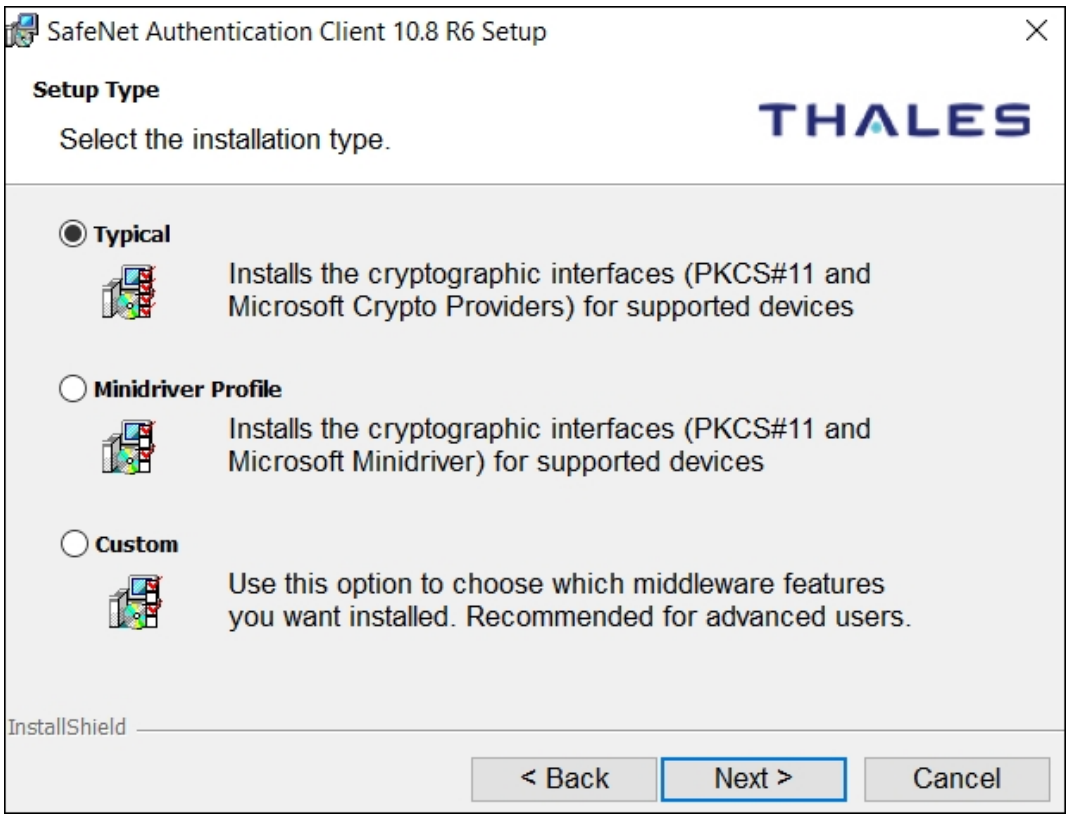
    `C:\Program Files\SafeNet\Authentication\`

    > **NOTE** If an application from the SafeNet Authentication line of products, or an eToken legacy product, is already installed, it is recommended to not change the the destination folder.

    This folder isused as the installation library for all future SAC applications.

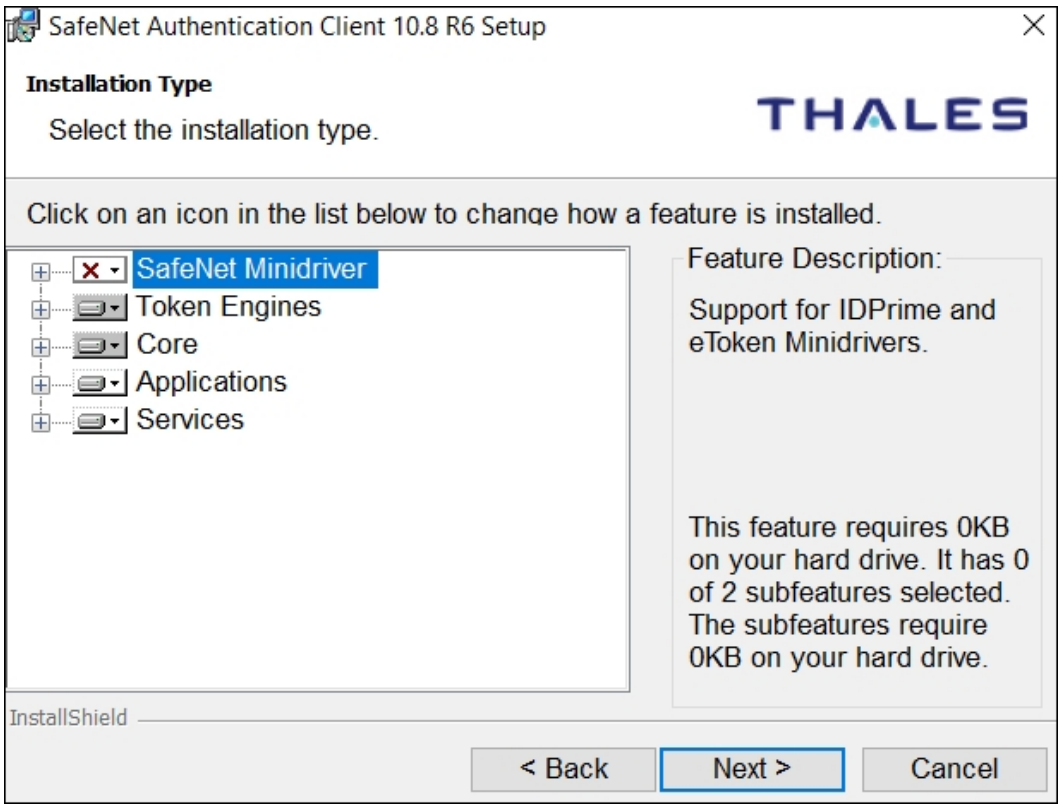
11. Click **Next**.

    The **Setup Type** window is displayed.



12. Select one of the following:
    - **Typical:** Installs the most common application features (recommended)
    - **Minidriver Profile:** Installs cryptographic interfaces (PKCS#11 and Microsoft Minidriver) for supported devices
    - **Custom:** Installs only the application features you select.
13. If you select **Custom**, click **Next**.

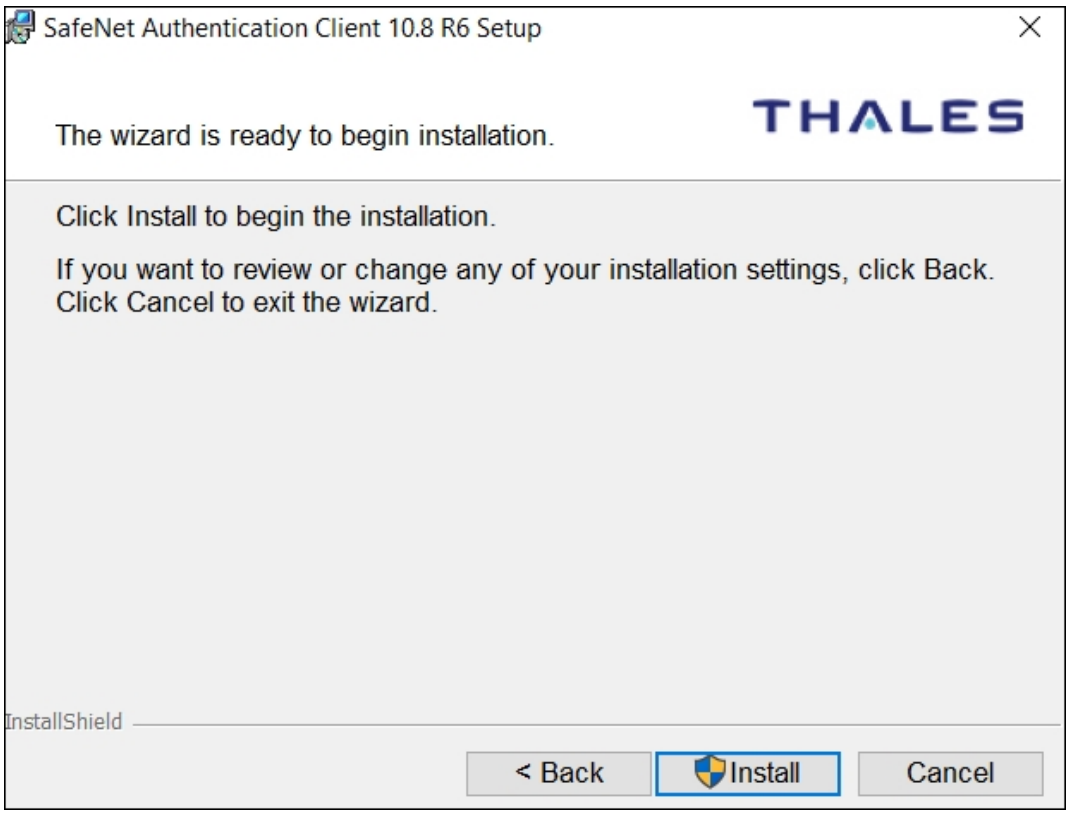
    The **Installation Type** window is displayed.



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

14. 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.

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

Installing the MSI file through the Command Line

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

The SAC command line installation uses the standard Windows Installer `msiexec` syntax:

> **for 32-bit systems:**

```
msiexec /i SafeNetAuthenticationClient-x32-10.8-R6.msi
```

> **for 64-bit systems:**

```
msiexec /i SafeNetAuthenticationClient-x64-10.8-R6.msi
```

> **NOTE** Ensure that all SAC applications are closed before upgrading, installing, or uninstalling it.

Perform the following steps to install SAC through 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 through 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 through 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, refer to "Application Properties Hierarchy" on page 69.

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-x32-10.8-R6.msi PROPERTY=VALUE
PROPERTY=VALUE /qb
```

> **For 64-bit systems:**

```
msiexec /i SafeNetAuthenticationClient-x64-10.8-R6 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

Some properties are stored as registry values and can be set or modified after installation. Refer to "General Settings" on page 71.

Some properties can be set during a command line installation only, and cannot be modified afterwards. Refer to "Installation-Only Properties" below.

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-x32-10.8-R6 msi
ET_LANG_NAME=Spanish
PROP_ADVANCED_VIEW=0
/qb
```

Command Line Installation Properties

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 / Slovenian / Slovakian 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

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 through the Command Line

To exclude specific features from the SAC 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-x32-10.8-R6 msi ADDDEFAULT=F1,F2…Fn
INSTALLLEVEL=n /qb
```

where:

- `SafeNetAuthenticationClient-x32-10.8-R6` is the 32-bit SAC installation file. For 64-bit systems, use `SafeNetAuthenticationClient-x64-10.8-R6.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)

SafeNet Authentication Client Command Line Feature Names

Feature Parent Name	Command Line Feature Name	Description
CoreFeature	**CAPI:**	Installs the standard CAPI implementation for eToken and Gemalto IDPrime devices.
	eTokenCAPI	Installs the standard CAPI implementation for eToken devices. Installs the standard
	IDPrimeCAPI	CAPI implementation for Gemalto IDPrime devices.
	eTokenPKCS11	Installs the standard PKCS#11 API implementation for eToken devices. **NOTE** This feature is mandatory.
	UIDialogs	Installs support for CAPI password dialogs. **NOTE** This feature is mandatory.
	KSP:	Registers SafeNet Key Storage Provider.
	CNG	Registers eToken devices for SafeNet Key Storage Provider (KSP).
	IDPrimeKSP	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 devices. **NOTE** This feature is mandatory.
	SACMonitor	Installs SafeNet Authentication Client Monitor (Tray icon). **NOTE** This feature is mandatory.

Feature Parent Name	Command Line Feature Name	Description
TokenEngines	**eTokenDevices:** eTokenJava	Support for JAVA devices. Support for Java devices. **NOTE** the eToken Java feature is mandatory.
	IDPrime	Support for IDPrime devices.

Installing All Features - Example

To install SACon a 32-bit system with all features, type the following command:

```
msiexec /i SafeNetAuthenticationClient-x32-10.8-R6 msi
ADDDEFAULT=eTokenCAPI,eTokenPKCS11,UIDialogs,KSP,SACTools,SACService,SACMonitor,eTokenJava,IDPrime,IDPrimeCAPI,IDPrimeKSP /qb
```

Installing All Features Except KSP Support - Example

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

```
msiexec /i SafeNetAuthenticationClient-x32-10.8-R6 msi KSP_Enabled=0 /qb
```

Installing without SAC Tools - Example

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

```
msiexec /i SafeNetAuthenticationClient-x32-10.8-R6 msi ADDDEFAULT=
eTokenDrivers,eTokenPKCS11,IDPrime,IDPrimePKCS11,IDPrimeCAPI,eTokenCAPI,KSP,UIDialogs,SACMonitor,SACService /qb
```

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

```
msiexec /i SafeNetAuthenticationClient-x32-10.8-R6.msi ADDDEFAULT=SACTools /qb
```

Removing Features through the Command Line

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

```
msiexec /x SafeNetAuthenticationClient-x32-10.8-R6.msi REMOVE=F1,F2…,Fn /qb
```

where:

`SafeNetAuthenticationClient-x32-10.8-R6.msi` is the 32-bit SAC installation file.

For 64-bit systems, use `SafeNetAuthenticationClient-x64-10.8-R6.msi`

`REMOVE` indicates that the following features are to be removed.

`Fx` 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 SAC application after it is installed with SAC on a 32-bit system, type the following command:

```
msiexec /x SafeNetAuthenticationClient-x32-10.8-R6 msi REMOVE=SACTools /qb
```

Disabling Reboot Reminder through the Command Line

A restart message during the SAC installation can be disabled. Flag values `NEVERREBOOT=0|1` are used in the following format:

```
msiexec /x SafeNetAuthenticationClient-x32-10.8-R6 NEVERREBOOT=1|0
```

Where:

`SafeNetAuthenticationClient-x32-10.8-R6` is the 32-bit SafeNet Authentication Client installation installer name.

`NEVERREBOOT` is the flag with values:

- `0`: Enables reminder
- `1`: Disables reminder

Example:

To disable the restart message reminder at the time of SAC installation type the following command:

```
msiexec /x SafeNetAuthenticationClient-x32-10.8-R6 NEVERREBOOT=1
```

CHAPTER 7: Uninstall

After SafeNet Authentication Client (SAC) 10.8 (R6) GA has been installed, it can be uninstalled.

Local administrator rights are required to uninstall SAC. When it is uninstalled, user configuration and policy files may be deleted.

Overview

If a device remains connected while SAC is being uninstalled, you are 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 SAC, use one of the following methods:

- Uninstalling through Add or Remove Programs
- Uninstalling through the Command Line

> **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.

Uninstalling through Add or Remove Programs

Perform the following steps to uninstall SAC through ADD or Remove programs:

1. Log on as an administrator.
2. Close all applications.
3. From the Windows taskbar, select **Start** > **Settings** > **Control Panel**.
4. Double-click **Add or Remove Programs**.
5. Select **SafeNet Authentication Client 10.8-R6**, and click **Remove**.
6. Follow the instructions to remove the application.

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

   The uninstall process proceeds.

Uninstalling through the Command Line

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

Perform the following steps to uninstall SAC through CLI:

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-x32-10.8-R6.msi` (for 32-bit installations)

   `msiexec /x SafeNetAuthenticationClient-x32-10.8-R6.msi` (for 64-bit installations)

   To uninstall in silent mode, add `/qn` to the end of the command.
5. When the uninstall completes, restart your computer.

CHAPTER 8: Client Settings

SafeNet Authentication Client (SAC) 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.

Overview

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

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

Sample Administrative Template files provided by SafeNet are:

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, SAC settings apply to the local computer only.

When configured on a server, SAC 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. Refer to "Application Properties Hierarchy" on page 69 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 SAC Settings

Add the Administrative Templates snap-in to enable you to modify the SAC settings.

To add the Administrative Templates to a client computer, refer to "Adding an ADM file to a Client Computer" below.

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).
  For details on the Non-Repudiation OIDs setting, refer to "General Settings" on page 71 .
- Ensure the certificate you are using includes an **Identity OID**.
  For details on the Identity OIDs setting, refer to "IdenTrust Settings" on page 147 .
- 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**.

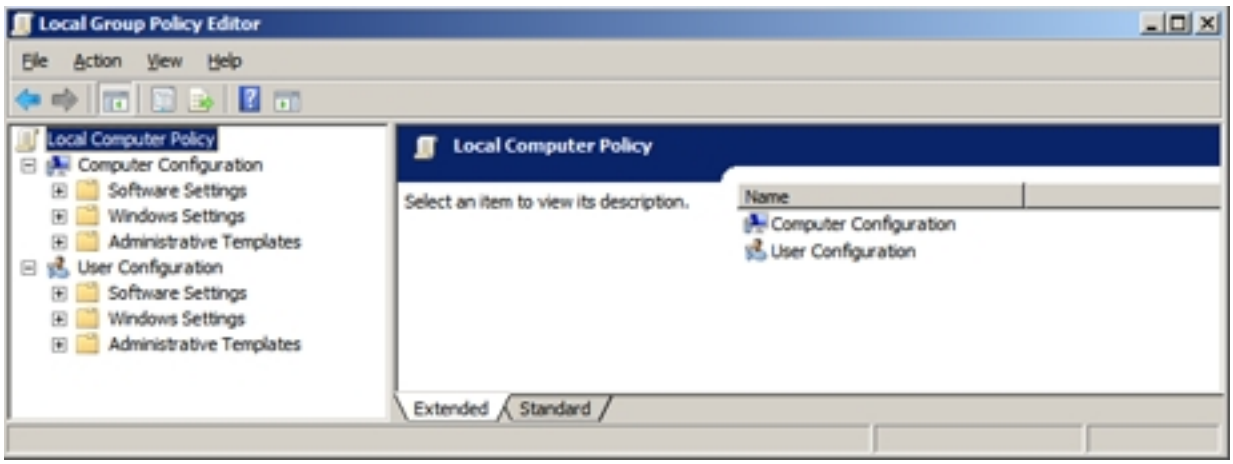
Adding an ADM file to a Client Computer

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

Perform the following steps to add SAC 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 is displayed.

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

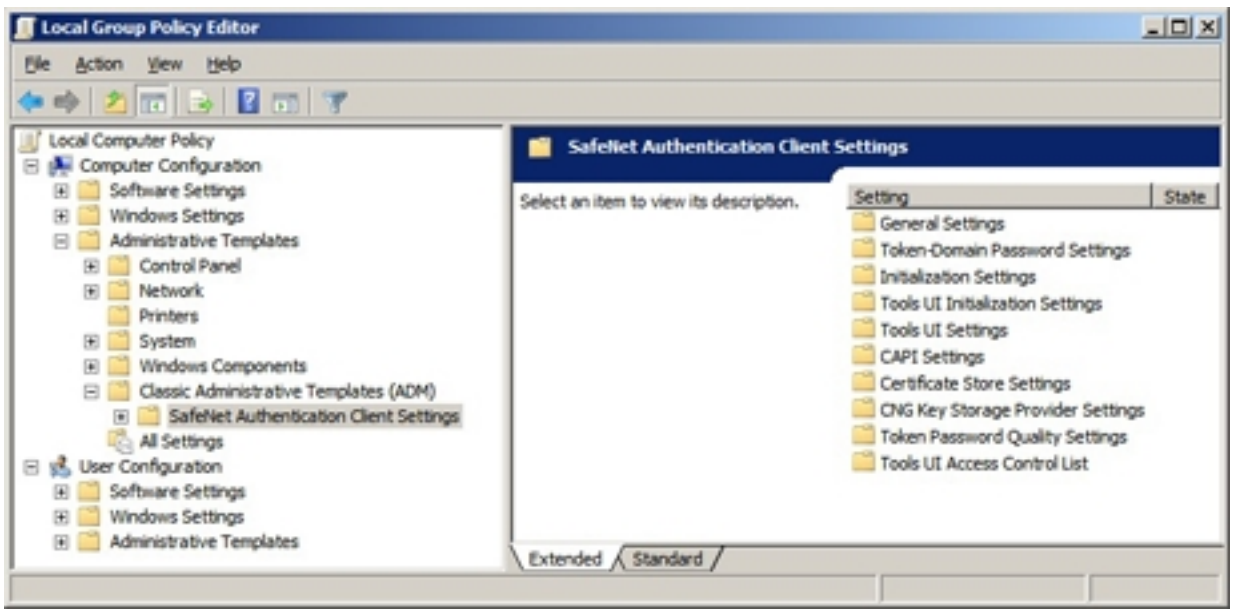
   Sample files are included in the SafeNet Authentication Client software package provided.

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 in **Administrative Templates > Classic Administrative Templates (ADM)**.



Editing SAC Settings

Each SAC Settings folder contains settings that can be configured to have priority over the SAC application defaults.

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

Perform the following steps to edit SAC 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 SAC Settings

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

Perform the following steps to apply SAC 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.

CHAPTER 9: Configuration Properties

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

Setting SAC 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 SAC (but not during repair). Refer to "Installing the MSI file through the Command Line" on page 55.

  The property name, and not the registry value name, is needed when setting the value during command line installation.

> Set a value using the SAC Tools application.

  Refer to *SafeNet Authentication Client User Guide*.

  Neither the registry value name nor the property name is needed.

  NOTE Values set using the SAC 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.

  Refer to "Client Settings" on page 64.

  The registry value name, and not the property name, is needed when setting the value.

> Manually edit the registry setting.

  Refer to "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 set manually 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 section below: "Application Properties Hierarchy" on the next page

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

SAC 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. SAC 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 SAC 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 SAC 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 above. Unless the properties must override other settings, it is recommended to write them to: `HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC`.

Setting Registry Keys Manually

Perform the following steps 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** is displayed, showing 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, it is recommended to write 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 is not applicable to any other process.

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

Perform the following steps:

1. From the Windows taskbar, select **Start** > **Run**.
2. In the **Run** dialog box, enter `regedit`, and click **OK**.
   The **Registry Editor** is displyed, showing 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

Perform the following steps:

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

   The **Registry Editor** is displayed, showing 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 **General** section in the `SafeNet\Authentication\SAC\General` registry key.

Description	ADM File Setting	Registry Value	Comm. Line
SingleLogon Determines if the user's Token Password is requested only once for applications using MS Cryptography (CAPI/CNG/Minidriver) and PKCS#11 Cryptography. For more details, refer to "SingleLogon & Single Sign On (SSO)" on page 17	**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	ADM File Setting	Registry Value	Comm. Line
SingleLogon Timeout Determines the timeout, in seconds, of a single logon. > 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. For more details, refer to "SingleLogon & Single Sign On (SSO)" on page 17	SingleLogon Timeout is set in the SingleLogon setting. (Refer to the "SingleLogon" entry above.)	**Registry Value Name:** SingleLogonTimeout **Value:** >=0 (Seconds) **Default:** 0 (no timeout)	**Property name:** `PROP_SINGLELOGONTO`
PCSC Slots Defines the total number of PC/SC slots for all USB tokens and smart cards. Included in this total: > the number of allocated readers for third-party providers . **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) **Default:** 8	**Registry Value Name:** PcscSlots **Values:** >=0 (0 = Physical tokens are disabled) **Default:** 8	**Property name:** `PROP_PCSCSLOTS`

Description	ADM File Setting	Registry Value	Comm. Line
Enable Private Cache Determines if SAC allows the token's private data to be cached. Applies only to tokens that are initialized with the private data cache setting. The private data is cached in per process memory. **NOTE** Can be set in SAC 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)	N/A
Retry Counter Cached Determines in which cache the retry counter is saved. If stored in the public cache, the API (SAC) performance increases, but it does not support transitioning of the device between computers. If stored in the private cache, performance is more accurate, even though it decreases.	Not supported	**Registry Value Name:** RetryCountCached **Values:** > **1 (True) -** The retry counter is stored in the public cache. Cache is updated on login operations. > **0 (False) -** The retry counter is stored in the private cache. Cache is updated on each transaction. **Default:** 1 (True)	N/A

Description	ADM File Setting	Registry Value	Comm. Line
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)	N/A
Tolerate X509 Attributes Determines if `CKA_SERIAL_NUMBER`, `CKA_SUBJECT`, and `CKA_ISSUER` attributes can differ from those in `CKA_VALUE` during certificate creation.	**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)	N/A

Description	ADM File Setting	Registry Value	Comm. Line
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)	N/A
Protect Symmetric Keys Determines if symmetric keys are protected. 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	N/A

Description	ADM File Setting	Registry Value	Comm. Line
Cache Marker Timeout Determines if SAC Service periodically inspects the cache markers of connected tokens for an indication that token content has changed. This property is used for Remote sessions or when crossing between machines.	**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	N/A
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 them 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 them after the existing value separated by commas **Default:** No override	N/A

Description	ADM File Setting	Registry Value	Comm. Line
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 is be disabled.	Not supported	**Registry Value Name:** MustChangeAdmin **Values:** > **0-** None > **1 -** ITI certification mode > **2 -** Special administrator PIN policy **Default:** 0	N/A
No Pin Pad Determines whether or not the PIN Pad reader is used as a regular smart card reader. SAC Tools UI requires entering user credentials.	Not supported	**Registry Value Name:** NoPinPad **Values:** > **0 -** Disabled > **1 -** Enabled **Default:** 0 (Disabled)	N/A

Description	ADM File Setting	Registry Value	Comm. Line
Enable Logon SSO Determines whether or not the SSO is enabled for Windows logon.	Not supported	**Registry Value Name:** EnableLogonSSO **Values:** > **0 -** Disabled > **1 -** Enabled **Default:** 0 (Disabled)	N/A
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)	N/A
PIN Pad Notify Determines if the Pin Pad notification is displayed as a balloon or in a window.	**Setting name:** 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)	N/A

Description	ADM File Setting	Registry Value	Comm. Line
Multi-Slot Support Determines if SafeNet Authentication Client is backward compatible with the following Gemalto PKCS#11 Common Criteria devices: IDPrime MD 840, IDPrime MD 3840 and eToken 5110 CC as well as supports compatibility with IDPrime MD 940 and 3940 devices. The Multi-Slot feature affects only SAC customized in compatible mode via the IDPrimePKCS11.dll (i.e. The IDGo 800 PKCS#11) option is selected in the Customization Tool. Refer to "Installing the SAC Customization Tool" on page 30. For more information on Multi-Slots, refer to 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.	Not supported	**Value Name:** MultiSlotSupport **Values:** > **Selected -** Activates this feature > **Not Selected -** Normal operation **Default:** Not Selected	N/A

Description	ADM File Setting	Registry Value	Comm. Line
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	N/A
Enable Log Events Enables event viewer messages.	**Setting name:** Enable Log Events **Values:** > Selected > Not Selected	**Registry Value Name:** EnableLogEvents **Values:** > 0 - Not Selected > 1 - Selected **Default:** 0 - (not selected)	N/A
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`

Description	ADM File Setting	Registry Value	Comm. Line
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 Set to True when the SafeNet RSA KSP must use SHA-2 to enroll a CA private key to a token **Default:** 0 (False)	N/A
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	N/A
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	N/A

Description	ADM File Setting	Registry Value	Comm. Line
Bipass Firefox Pin Dialog Bypasses Firefox Pin dialog.	**Setting name:** Bipass Firefox Pin Dialog **Values:** > **Selected** - Firefox does not display its PIN Dialog for eToken and IDPrime cards. SAC PIN Dialog is displayed when actual authentication occurs. > **Not Selected**- Firefox displays its PIN Dialog for eToken and IDPrime cards. **Default:** Not Selected	**Registry Value Name:** BypassFirefoxPinDialog **Values:** > **1** - Firefox does not displays its PIN Dialog for eToken and IDPrime cards. SAC PIN Dialog is displayed when actual authentication occurs. > **0** - Firefox displays its PIN Dialog for eToken and IDPrime cards. **Default:** 0	N/A
Force New Key A Determines the deletion of either User or Admin keys associated with the role different from the user.	Not supported	**Registry Value Name:** ForceNewKeyA **Value:** > **0-** Keys can be deleted by either User or Admin > **1-** Keys associated with a Role different from user can be deleted only by the Admin **Default:** 0	N/A

Description	ADM File Setting	Registry Value	Comm. Line
Disable Cache File Info Disables cache file info.	Not supported	**Registry Value Name:**DisableCacheFileInfo **Value:** > **0**- SAC caches file information > **1**- SAC does not cache file information and query it when needed **Default:** 0	N/A
Skip CMap File Check Skips CMap file check.	Not supported	**Registry Value Name:**SkipCMapFileCheck **Value:** > **0** - SAC checks if the disk cache contains an entry named "cmapfileFixedValue" > **1**- SAC does not check if CMap file stored in the card is corrupted or not **Default:** 0	N/A

Token-Domain Password Settings

The following settings are written to the **SyncPin** section in the `SafeNet\Authentication\SAC\SyncPin` registry key.

> **NOTE** This setting works only if the installation contains SAC UI (referred to as SAC Tools in the SAC Customization Tool).

Description	ADM File	Setting Registry Value	Comm. 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 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	N/A

Initialization Settings

> **NOTE** The following new registry settings are applicable to IDPrime Cards only:
> - In **Init Key** folder: `ForceInitExternalPinPolicy` and `ForceDefaultInitKey`
> - In **InitApp Key** folder: `HideInitCreateAdmin` and `HideInitPinPolicy`

The following settings are written to the **Init** section in the `SafeNet\Authentication\SAC\Init` registry key.

> **NOTE** None of the settings in this section are relevant to IDPrime cards, except for the *LinkMode* and *UserMaxRetry* settings.
>
> 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	Comm. Line
Always Use Default Initialization Key Defines the use of default initialization key during token initialization. **NOTE** If Selected, the following windows on the SAC Tools UI are skipped while Initializing IDPrime FIPS Devices (with initialization key): - Administrator Logon - Initializing Key Settings	**Setting Name:** Always Use Default Initialization Key **Values:** > **Selected:** Token is initialized with the default initialization key > **Not selected:** Token is initialized with the initialization key entered by the user **Default:** > Not selected	**Registry Value Name:** ForceDefaultInitKey **Values:** > **1:** Token is initialized with the default initialization key > **0:** Token is initialized with the initialization key entered by the user **Default:** > 0	N/A

Description	ADM File	Setting Registry Value	Comm. Line
Use PIN Quality Parameters From Policy Defines if the PIN Quality parameters in the SAC Client Settings are used during initialization. **NOTE** If Selected, user cannot modify the Pin Policy of the card manually through *Initialize Token* setting. Also, all the fields in the *PIN Quality* and *Advanced* tabs on the SAC Tools are disabled.	**Setting Name:** Use PIN Quality Parameters From Policy **Values:** > **Selected:** Token is initialized with PIN Quality parameters stored in SAC Client Settings > **Not selected:** Token is initialized with PIN Quality parameters stored on the card or entered by the user **Default:** > Not selected	**Registry Value Name:** ForceInitExternalPinPolicy **Values:** > **1:** Token is initialized with PIN Quality parameters stored in SAC Client Settings > **0:** Token is initialized with PIN Quality parameters stored on the card or entered by the user **Default:** > 0	N/A
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	N/A
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	N/A

Description	ADM File	Setting Registry Value	Comm. Line
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)	N/A
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)	N/A
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	N/A

Description	ADM File	Setting Registry Value	Comm. Line
API: Keep Token Settings When initializing the token using the SDK, this setting 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)	N/A
API: Private Data Caching If using an independent API for initialization, and if 'Enable Private Cache' is selected, this setting 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)	N/A

Description	ADM File	Setting Registry Value	Comm. Line
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)	N/A
Private Data Caching Mode If 'Enable Private Data Caching Modification' is selected, this setting 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)	N/A

Description	ADM File	Setting Registry Value	Comm. Line
API: RSA Secondary Authentication Mode If using an independent API for initialization, this setting 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)	N/A

Description	ADM File	Setting Registry Value	Comm. Line
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)	N/A

Description	ADM File	Setting Registry Value	Comm. Line
Use the same token and administrator passwords for digital signature operations.	**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)	N/A

Description	ADM File	Setting Registry Value	Comm. Line
NOTE If `LinkMode` is 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. When using a Common Criteria smart card (SafeNet IDPrime 940 or Gemalto IDPrime MD 840), if the Admin PIN is set to default, the unlock button will be disabled until changed. For example: When using a SafeNet IDPrime 940 or Gemalto IDPrime MD 840 card in linked mode, the Unlock Token button (in SAC Tools) will be disabled until the default Admin PIN is changed.			

SafeNet Authentication Client Tools UI Initialization Settings

The following settings are written to the **AccessControl** section in the `SafeNet\Authentication\SAC\AccessControl` registry key.

Description	ADM File	Setting Registry Value	Comm. 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	**Property name:** `PROP_ADVANCED_VIEW`

The following settings are written to the **InitApp** section in the `SafeNet\Authentication\SAC\InitApp` registry key.

Description	ADM File	Setting Registry Value	Comm. Line
Hide Create Administrator Password Fields Defines if Create Administrator Password fields are hidden/ visible in the Password Settings window.	**Setting Name:** Hide Create Administrator Password Fields **Values:** > **Selected:** Create Administrator Password fields are hidden > **Not selected:** Create Administrator Password fields are visible **Default:** > Not selected	**Registry Value Name:** HideInitCreateAdmin **Values:** > **1:** Create Administrator Password fields are hidden > **0:** Create Administrator Password fields are visible **Default:** > 0	N/A

Description	ADM File	Setting Registry Value	Comm. Line
Hide PinPolicy Button Defines if the Pin Policy button is hidden/ visible in the Password Settings window.	**Setting Name:** Hide PinPolicy Button **Values:** > **Selected:** PIN Policy button is hidden > **Not selected:** PIN Policy button is visible **Default:** > Not selected	**Registry Value Name:** HideInitPinPolicy **Values:** > **1:** PIN Policy button is hidden > **0:** PIN Policy button is visible **Default:** > 0	N/A
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	N/A
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:** MustChangePassword Enabled **Values:** > **1 -** Selected > **0 -** Not selected **Default:** 1	N/A

Description	ADM File	Setting Registry Value	Comm. Line
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.	**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	N/A
Private Data Caching If Enable Private Cache is selected,this setting determines the token's private data cache default behavior. Can be set in SafeNet Authentication Client Tools. This option is not supported by IDPrime 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	N/A

Description	ADM File	Setting Registry Value	Comm. Line
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 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. > **Token authentication on application request -** If the key generation application requires key	**Registry Value Name:** RSASecondaryAuthenticationMode **Values**: > **0 -** Never > **1 -** Prompt user on application request > **2 -** Always prompt user > **3 -** Always > **4 -** Token authentication on application request **Default:** 0	N/A

Description	ADM File	Setting Registry Value	Comm. Line
	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	N/A

SafeNet Authentication Client Tools UI Settings

The following settings are written to the **UI** section in the `SafeNet\Authentication\SAC\UI` registry key.

Description	ADM File	Setting Registry Value	Comm.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)	N/A
Password Term Defines the term used for the token's user password. 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	N/A
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	N/A

Description	ADM File	Setting Registry Value	Comm.Line
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	N/A
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	N/A
Enable Logging Control Determines if the Enable Logging /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	N/A
Home URL Overwrites the Thales home URL in SafeNet Authentication Client Tools.	**Setting Name:** Home URL **Values:** Valid URL **Default:** Thales' (CPL) home URL https://cpl.thalesgroup.com/	**Registry Value Name:** HomeUrl **Values (String):** Valid URL **Default:** Thales' (CPL) home URL	N/A

Description	ADM File	Setting Registry Value	Comm.Line
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)	N/A
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	N/A
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	N/A

Description	ADM File	Setting Registry Value	Comm.Line
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	N/A
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	N/A
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	N/A

Description	ADM File	Setting Registry Value	Comm.Line
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.	N/A
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	N/A
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.	N/A

Description	ADM File	Setting Registry Value	Comm.Line
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	N/A
Detailed Message If “Show detailed message” is selected in the “Warning Message Click Action” setting, this setting defines the detailed message to display.	**Setting Name:** Detailed Message **Values:** String **No default**	**Registry Value Name:** ActionDetailedMessage **Values:** String **No default**	N/A
Website URL If “Open website” is selected in the “Warning Message Click Action” setting, this 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	N/A
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)	N/A

Description	ADM File	Setting Registry Value	Comm.Line
Display Virtual Keyboard Determines if Thales' keystroke-secure Virtual Keyboard replaces standard keyboard entry of password fields in the following windows: > Token Logon > Change Password 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)	N/A
Password Policy Instructions If not empty, this setting 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	N/A

Description	ADM File	Setting Registry Value	Comm.Line
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	N/A
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	N/A

Description	ADM File	Setting Registry Value	Comm.Line
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	N/A

CAPI Settings

The following settings are written to the **CAPI** section in the `SafeNet\Authentication\SAC\CAPI` registry key.

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

Description	ADM File Setting	Registry Value	Comm. Line
Password Timeout Defines the number of minutes the CAPI-required password is valid following the last logon activity.	**Setting Name:** Password Timeout **Values:** >=0 (0= No timeout) **Default:** 0	**Registry Value Name:** PasswordTimeout **Values:** >=0 (0= No timeout) **Default:** 0	N/A

Description	ADM File Setting	Registry Value	Comm. Line
Logout Mode Determines if the user is prompted to enter a password for each operation requiring the user to be logged on. **NOTE** If selected, this setting takes precedence over *Password Timeout* setting in the SAC Tools.	**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	N/A
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)	N/A

Description	ADM File Setting	Registry Value	Comm. Line
Overwrite Default Certificate Determines if the default certificate selection can be reset .	**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	N/A

Description	ADM File Setting	Registry Value	Comm. Line
Sign Padding On-Board Determines if sign padding is performed on-board supported devices for added security. Sign padding is supported by Java tokens. 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	N/A

Internet Explorer Settings

The following settings are written to the **IEXPLORE.EXE** section in the `SafeNet\Authentication\SAC\CAPI\IEXPLORE.EXE` registry key. These are applied while using Internet Explorer only. The values are set per process on a per machine basis.

Description	ADM Fil 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 SafeNet Authentication Client. 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`

Description	ADM Fil Setting	Registry Value	Command Line
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. To enable the token containing the "Enrollment on Behalf" certificate to contain smart card 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 smart card 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	N/A

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 SAC propagation functionality. To avoid a lack of synchronization between these different propagation processes, it is strongly recommended closing the Microsoft Certificate Propagation Service and using only SAC for certificate propagation.

The following settings are written to the **CertStore** section in the `SafeNet\Authentication\SAC\CertStore` registry key.

Description	ADM File Setting	Registry Value	Comm. Line
Propagate User Certificates Determines if all user certificates on the token are exported to the user store. 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. 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

Description	ADM File Setting	Registry Value	Comm. Line
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)	N/A
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)	N/A

Description	ADM File Setting	Registry Value	Comm. Line
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:** RemoveUserCertsOn TokenRemove **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)	N/A

Description	ADM File Setting	Registry Value	Comm. Line
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)	N/A

Description	ADM File Setting	Registry Value	Comm. Line
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	**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	N/A

Description	ADM File Setting	Registry Value	Comm. Line
	from Token" setting. **Default:** Never		
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**.	N/A

Description	ADM File Setting	Registry Value	Comm. Line
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	N/A
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)	N/A

Description	ADM File Setting	Registry Value	Comm. Line
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.	N/A

CNG Key Storage Provider Settings

The following settings are written to the **CNG** section in the `SafeNet\Authentication\SAC\CNG registry key`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 SAC Tools. -After changing the cryptographic provider setting, reconnect the token to ensure that the properties are updated to the token. This setting is not relevant to IDPrime 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. Refer to "KSP_ENABLED Property" on page 56.

Token Password Quality Settings

The following settings are written to the **PQ** section in the `SafeNet\Authentication\SAC\PQ` registry key.

Description	GPO Editor/MMC Settings	Registry Key	Comm. Line
Password - Include Non ASCII Characters Determines if the password can be included for non-ASCII characters. **NOTE** Applicable for IDPrime cards only.	**Setting Name:** Password - Include Non ASCII Characters **Values:** > 0: Permitted > 1: Forbidden > 2: Mandatory **Default:** Permitted	**Registry Key Name:** pqNonAscii **Values:** > 0: Permitted > 1: Forbidden > 2: Mandatory **Default:** 0	N/A
Password - Number Of Different Repeating Characters Determines the number of different characters that can be repeated at least once.	**Setting Name:**Password - Number Of Different Repeating Characters **Values:** >= 0 (0 = No check) **Default:** 0	**Registry Key Name:** pqNumDiffCharRepeat **Values:** >= 0 (0 = No check) **Default:** 0	N/A
Password - Maximum Number A Character Can Appear Determines the maximum number a character can appear.	**Setting Name:**Password - Maximum Number A Character Can Appear **Values:** >= 0 (0 = No check) **Default:** 0	**Registry Key Name:** pqMaxNumCharAppear **Values:** >= 0 (0 = No check) **Default:** 0	N/A

Description	GPO Editor/MMC Settings	Registry Key	Comm. Line
Password - Maximum Number Of Characters In A Sequence Determines the maximum number of characters in a sequence. For example: If the value is set to 4, the sequence 1,2,3,4,a,5 is allowed but 1,2,3,4,5,a is not allowed.	**Setting Name:**Password - Maximum Number Of Characters In A Sequence **Values:** >= 0 (0 = No check) **Default:** 0	**Registry Key Name:** pqMaxNumCharSequence: **Values:** >= 0 (0 = No check) **Default:** 0	N/A
Password - Maximum Adjacent Repetitions Of A Character Determines the maximum number a character can be repeated in adjacent positions. **NOTE** If pqMaxNumCharRepeatPos = 0, then the value of pqMaxRepeated is applicable.	**Setting Name:**Password - Maximum Adjacent Repetitions Of A Character **Values:** >= 0 (0 = No check) **Default:** 0	**Registry Key Name:** pqMaxNumCharRepeatPos **Values:** >= 0 (0 = No check) **Default:** 0	N/A
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, refer to "Changing the Password Minimum Length Permanently" on page 38	**Setting Name:** Password - Minimum Length **Values:** >=4 **Default:** 8	**Registry Key Name:** pqMinLen **Values:** >=4 **Default:** 8	`PROP_PQ_MINLEN`

Description	GPO Editor/MMC Settings	Registry Key	Comm. Line
Password - Maximum Length Defines the maximum password length. **NOTE** - Can be set in SAC Tools. - Devices that have an eToken applet (such as: eToken 5110, 5110 FIPS or IDCore 830B) the max pin length property is not saved on the device. This property has only a UI meaning (i.e.no security meaning). -The value of the proprietary PKCS#11 attribute `ETCKA_PIN_MAX_LEN` on these devices is always read from SAC's `pqMaxLen` property. - If the `pqMaxLen` property is not explicitly defined in the registry, it receives the default value (20).	**Setting Name:** Password - Maximum Length **Values:** Cannot be less than the Password Minimum Length **Default:** 20	**Registry Key Name:** pqMaxLen Values: Cannot be less than the Password Minimum Length **Default:** 20	N/A
Password - Maximum Usage Period Defines the maximum number of days a password is valid. **NOTE** - Can be set in SAC Tools. -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	GPO Editor/MMC Settings	Registry Key	Comm. Line
Password - Minimum Usage Period Defines the minimum number of days between password changes. **NOTE** Can be set in SAC Tools.	**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 SAC 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 SAC Tools. **NOTE** Maximum value of History size for IDPrime devices is 10.	**Setting Name:** Password - History Size **Values:** >= 0 (0 = No minimum) **Default:** 10	**Registry Key Name:** pqHistorySize **Values:** >= 0 (0 = No minimum) **Default:** 10	PROP_PQ_HISTORYSIZE

Description	GPO Editor/MMC Settings	Registry Key	Comm. Line
Password - Maximum Consecutive Repetitions Defines the maximum number of consecutive times a character can be used in a password. **NOTE** Can be set in SAC Tools. **NOTE** If pqMaxNumCharRepeatPos = 0, then the value of pqMaxRepeated is applicable.	**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	N/A

Description	GPO Editor/MMC Settings	Registry Key	Comm. Line
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 SAC 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 Types 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 Types setting > **0 -**The rule for each character type is defined in the character type's Include setting **Default:** 1	`PROP_PQ_MIXCHARS`

Description	GPO Editor/MMC Settings	Registry Key	Comm. Line
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 - Complexity setting is set to Standard complexity. - Can be set in SAC 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	N/A
Password - Include Numerals Determines if the password can include numerals. **NOTE** - Applies only when the Password - Complexity setting is set to Manual complexity. - Can be set in SAC Tools.	**Setting Name:** Password - Include Numerals **Values:** > Permitted > Forbidden > Mandatory **Default:** Permitted	**Registry Key Name:** pqNumbers **Values:** > **0 -** Permitted > **1 -** Forbidden > **2 -** Mandatory **Default:** 0	N/A
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 SAC 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	N/A

Description	GPO Editor/MMC Settings	Registry Key	Comm. Line
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 SAC 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	N/A
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 SAC 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	N/A

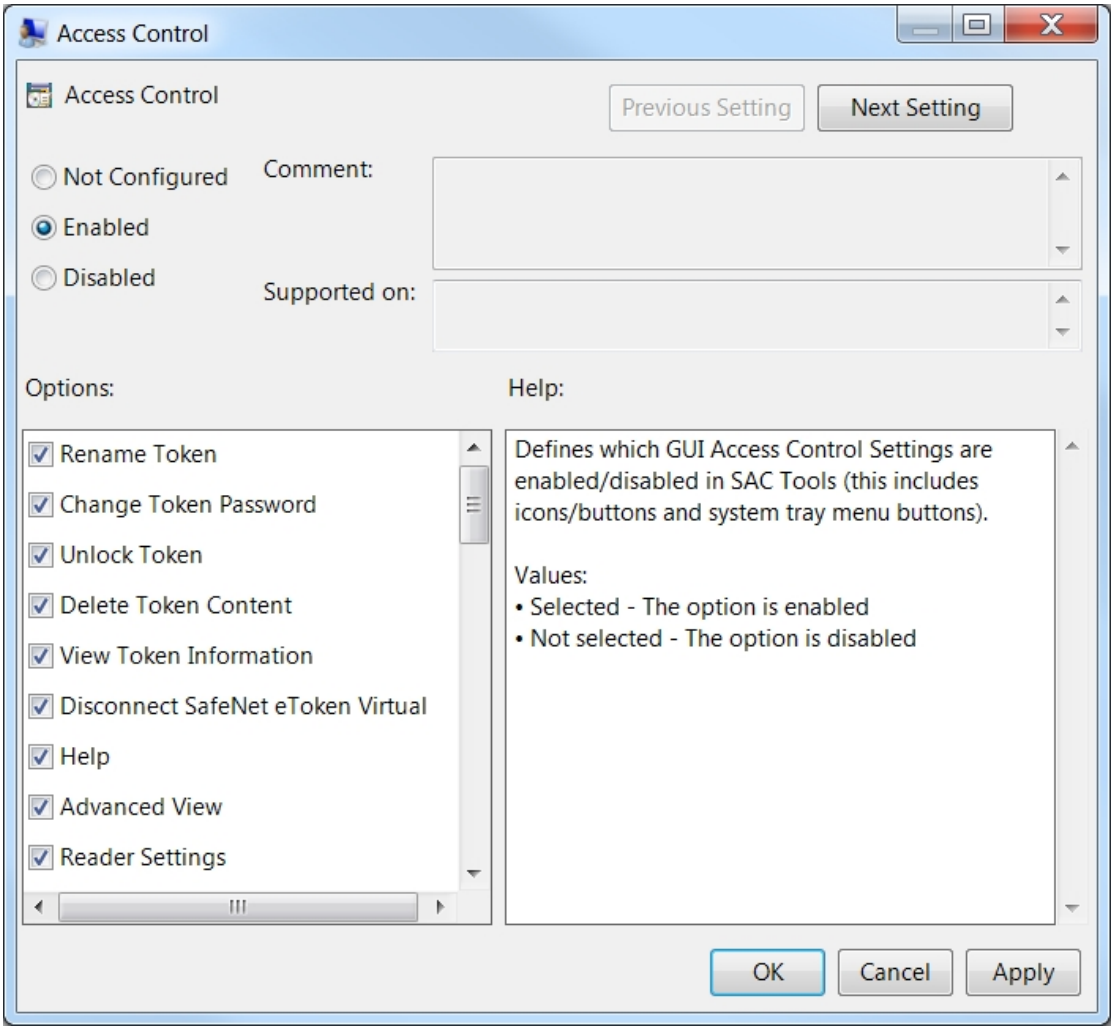
Description	GPO Editor/MMC Settings	Registry Key	Comm. Line
Password Quality Check on Initialization Determines if the password quality settings are checked and enforced when a token is initialized. **TIP** It is recommended that this policy not be set when tokens are enrolled using SafeNet Authentication 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	N/A
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.	N/A

Description	GPO Editor/MMC Settings	Registry Key	Comm. Line
Enable Password Quality Modification Determines if the password quality settings on a newly initialized token can be modified by the owner. Refer to the `Password Quality Owner` setting under"Token Password Quality Settings" on page 123. To configure the 'Password Minimum Length' property as permanent during or after the initialization process, refer to "Changing the Password Minimum Length Permanently" on page 38	**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.	N/A

Description	GPO Editor/MMC Settings	Registry Key	Comm. Line
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: Uppercase letters, Lowercase 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	N/A

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 SAC Tools and Tray Menu.



The following settings are written to the **AccessControl** section in the `SafeNet\Authentication\SAC\AccessControl` registry key.

Access Control Feature	ADM File Setting	Registry Key	Comm. 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	N/A

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).
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.

Access Control Feature	Registry Value Name	Description
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.
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.
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.

Access Control Feature	Registry Value Name	Description
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.
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. **NOTE** If disabled, IDPrime CC card cannot be initialized.
System Tray - Unlock Token	TrayIconUnlockEtoken	Enables/Disables the Unlock Token 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.

Access Control Feature	Registry Value Name	Description
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	Registry Value Name	Description
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	

Access Control Feature	Registry Value Name	Description
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 **Crypto** section in the `SafeNet\Authentication\SAC\Crypto` registry key.

Description	ADM File Setting	Registry Value	Comm. 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 21 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 (Refer to 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 21 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 (Refer to the description below). **Default:** Obsolete	N/A

Description	ADM File Setting	Registry Value	Comm. Line
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), **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	ADM File Setting	Registry Value	Comm. Line
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 151 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	**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 151 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	N/A

Description	ADM File Setting	Registry Value	Comm. Line
	unwrap-PKCS1.5 and unwrap-AES-CBC operations. **Default:** Optimized	unwrap-PKCS1.5 and unwrap-AES-CBC operations. **Default:** Optimized	
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	N/A
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)	N/A

Description	ADM File Setting	Registry Value	Comm. Line
Customized ICC Public Key Determines the public key for IDPrime cards with a customized ICC Public Key for mutual authentication. For more details, refer to "Customized ICC Public Key" on page 39.	Not Supported	**Registry Value Name:** SMKeys **Values:** > **Enabled-** SAC can communicate with cards that have Customized ICC Public Key for Mutual Authentication > **Disabled-** SAC can communicate with cards that have default ICC Public Key for Mutual Authentication **Default:** Disabled	N/A

Log Settings

The following settings are written to the **Log** section in the `SafeNet\Authentication\SAC\Log` registry key.

These settings may be defined using:

`HKEY_LOCAL_MACHINE or HKEY_CURRENT_USER`

Description	ADM File Setting	Registry Value
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)

Description	ADM File Setting	Registry Value
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 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	N/A

CHAPTER 10: 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://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/prevent-malware-infection

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

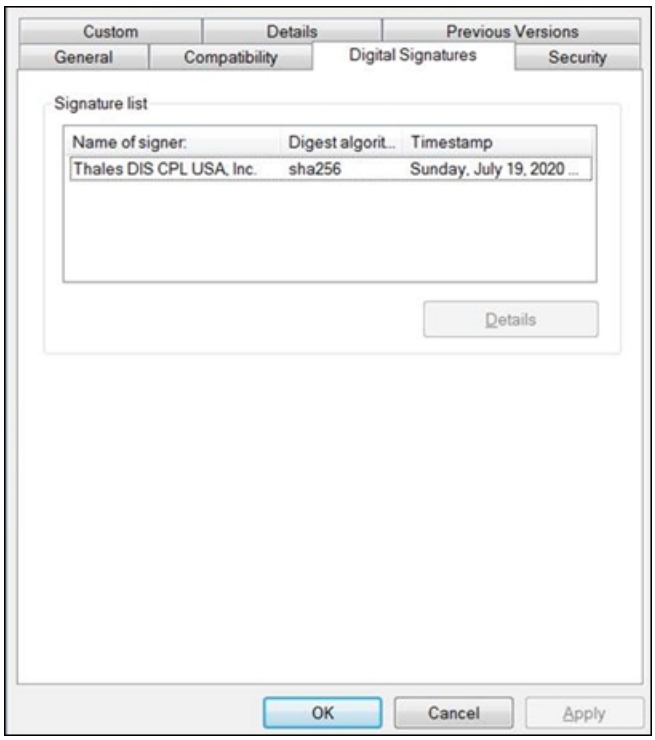
Make sure to choose an effective Anti-Virus/Malware software to protect your client machines. It is essential to keep the Anti-Virus/Malware software updated.

Install the SAC Package Only from the Official Thales Site

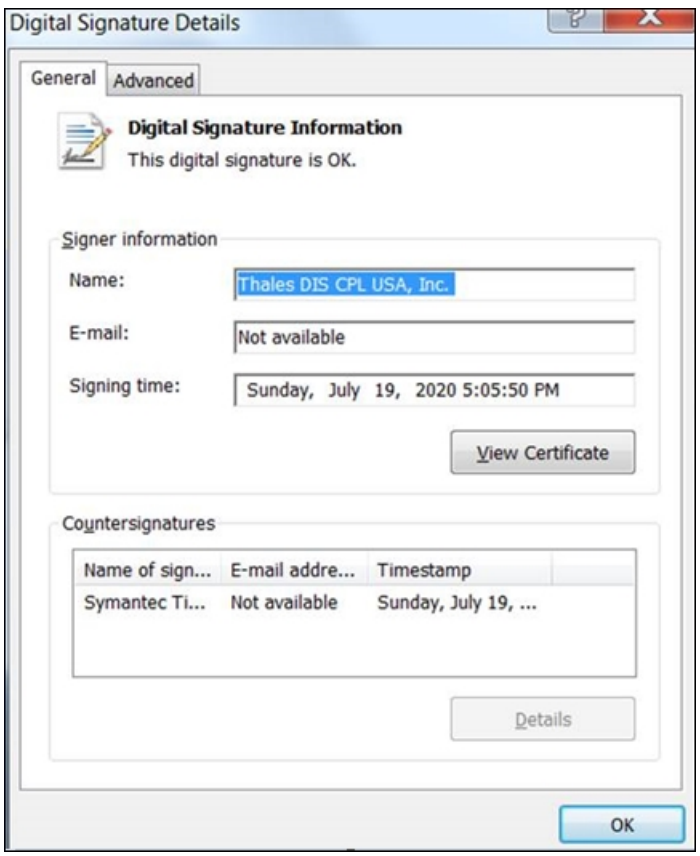
https://gemalto.service-now.com/csm/?id=kb_article&sys_id=e49d34944f69b680873b69d18110c7b2

Perform the following steps to ensure that the Thales 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 Thales signature is listed.



3. Select the **Thales** 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.

For more details, refer to:

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 10.8 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 "Client Settings" on page 64.
- **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 "SafeNet Authentication Client Tools UI Initialization Settings" on page 95, "SafeNet Authentication Client Tools UI Settings" on page 99 and "SafeNet Authentication Client Tools UI Access Control List" on page 134.
- **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 (Refer to "CAPI Settings" on page 108).
  - Using the Single Logon option is less secured and is therefore not recommended (See the SingleLogon registry key under "General Settings" on page 71)
- **Configure restrictive password policies:**
  - Change the default administrator password.
  - 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. As per 3DES algorithm for 24 binary or 48 hexadecimal values (entered as Admin PIN) every LSB bit is ignored, which means if user enters any random number as the LSB, it is ignored and more number of Admin PIN are possible.

    NOTE It is recommended to not use 24 binary or 48 hexadecimal values for Admin PIN.

  - Use the password validity period combined with password history options.

For more information on how to configure password policy settings, refer to "Token Password Quality Settings" on page 123, 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 / Thales 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 "Security Settings" on page 140.

> **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 "Security Settings" on page 140.