SafeNet Authentication Client (Windows)

Version 10.2

Administrator Guide

gemalto
security to be free

Product Version: 10.2 (GA)

Document Number: 007-013560-002, Rev. A

Release Date: December 2016

Support Contacts

We work closely with our reseller partners to offer the best worldwide technical support services. Your reseller is the first line of support when you have questions about products and services. However, if you require additional assistance you can contact us directly at:

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017, USA
Phone US International	 +1-800-545-6608 +1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.

Additional Documentation

The following publications are available:

- 007-013561-002 SafeNet Authentication Client 10.2 (GA) User Guide
- 007-013559-003 SafeNet Authentication Client 10.2 (GA) Customer Release Notes (CRN)

Table of Contents

1 Introduction 7
Overview 7
SafeNet Authentication Client Main Features 8
What's New 9
Supported Tokens and Smart Cards 9
Certificate-based USB Tokens 9
Certificate-based Hybrid USB Tokens 9
Software Tokens 9
Smart Cards 10
End-of-Sale Tokens/Smart Cards 10
End-of-Life Tokens/Smart Cards 10
External Smart Card Readers 11
Supported Localizations 12
SafeNet Authentication Client API Flow 13
License Activation 13
IDPrime MD Applet 4.0 14
Number and Type of Key Containers 15
API Adjustments 15

2 System Requirements 16
Supported Browsers 16
Supported Platforms 16
Hardware and Screen Resolution Requirements 17
Compatibility with Gemalto Applications 17
Compatibility with Third-Party Applications 18

3 Customization 19
Customization Overview 19
Compatibility with IDGo 800 Minidriver and PKCS#11 20
Configuring IDGo 800 Minidriver Only 20
Configuring IDGo 800 PKCS#11 for Backward Compatibility 21
Installing IDGo 800 Minidriver and SafeNet Authentication Client eToken Features 22
Installing the SafeNet Authentication Client Customization Tool 23
Using the SafeNet Authentication Client Customization Tool 25
Features to Install 31
Services 31
Applications 31
eToken Engines 31
Generating a Customized MSI Installation File 32
Installing the Customized Application 33

4 Upgrade . . . 34
Upgrading Using the SafeNet Authentication Client .exe or .msi Files . . . 34
Upgrading from Versions Earlier than SAC 9.0 . . . 35
Upgrading from SafeNet Authentication Client 9.0 . . . 35
5 Installation . . . 36
Installation Files . . . 37
SafeNet Authentication Client Binary Files . . . 38
System32 and SysWOW64 Folders . . . 39
Installation Configurations . . . 39
Installing SafeNet Authentication Client on Windows (MSI) . . . 39
Installing the MSI file via the Command Line . . . 44
Installation-Only Properties . . . 46
Installing All Features - Example . . . 52
Removing Features via the Command Line . . . 53
Installing SafeNet Authentication Client on Windows (Simplified Installation) . . . 53
Command Line Parameters via the Simplified Installation . . . 54
Configuring Root Certificate Storage for Win Server 2008 R2 . . . 54
6 Uninstall . . . 55
Uninstall Overview . . . 55
Uninstalling via Add or Remove Programs . . . 55
Uninstalling via the Command Line . . . 56
7 SafeNet Authentication Client Settings . . . 57
SafeNet Authentication Client Settings Overview . . . 57
Adding SafeNet Authentication Client Settings . . . 58
Configuring SAC Password Prompt Settings . . . 58
Adding an ADM file to Windows Server 2008 / R2 . . . 58
Adding an ADMX file to Windows Server 2008 / R2 . . . 60
Adding an ADM file to a Client Computer . . . 61
Editing SafeNet Authentication Client Settings . . . 62
Editing Settings in Windows Server 2008 / R2 . . . 62
Editing Settings on a Client Computer . . . 63
Deploying SafeNet Authentication Client Settings . . . 64
8 Configuration Properties . . . 65
Setting SafeNet Authentication Client Properties . . . 65
Application Properties Hierarchy . . . 66
Hierarchy List . . . 66
Hierarchy Implications . . . 66
Setting Registry Keys Manually . . . 67
Defining a Per Process Property . . . 67

General Settings 69
Token-Domain Password Settings 74
License Settings 75
Initialization Settings 75
SafeNet Authentication Client Tools UI Initialization Settings 80
SafeNet Authentication Client Tools UI Settings 85
CAPI Settings 91
    Internet Explorer Settings 93
Certificate Store Settings 94
CNG Key Storage Provider Settings 97
Token Password Quality Settings 98
SafeNet Authentication Client Tools UI Access Control List 103
Security Settings 106
SafeNet Authentication Client Security Enhancements 107
    Enforcing Restrictive Cryptographic Policies 107
Log Settings 108
IdenTrust Settings 109

Introduction

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

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

In this chapter:

- Overview
- SafeNet Authentication Client Main Features
- What's New
- Supported Tokens and Smart Cards
- Supported Localizations
- SafeNet Authentication Client API Flow
- License Activation
- IDPrime MD Applet 4.0
- Number and Type of Key Containers
- API Adjustments

Overview

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

SafeNet Authentication Client enables the implementation of strong two-factor authentication using standard certificates as well as encryption and digital signing of data. Generic integration with CAPI, CNG, and PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications offering secure web access, secure network logon, PC and data security, and secure email. PKI keys and certificates can be created, stored, and used securely from within hardware or software.

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

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

SafeNet Authentication Client Main Features

SafeNet Authentication Client 10.2 introduces the support for PIN Pad readers as well as Gemalto IDPrime MD 3811 cards.

IDPrime MD cards are Minidriver enabled PKI smart cards. Administrators and users can use and manage IDPrime MD smart cards seamlessly via the standard PKCS#11 with any Microsoft CSP/KSP interface and without the need for any additional middleware. They offer secure IT Security and ID access and are compatible with the NFC standard.

For more details on the list of Gemalto IDPrime cards supported, See "Supported Tokens and Smart Cards" on page 9.

NOTE:
The term Token is used throughout the document and is applicable to both Smart Cards and Tokens.

SafeNet Authentication Client includes the following features[1]:

- Token usage, including:
  - Digitally signing sensitive data
  - Remote data access
  - Use of SafeNet Virtual Token
  - Management of certificates on the token
- Token management operations, including:
  - Token initialization
  - Initializing Common Criteria Certified devices
  - Token Password changes
  - Token unlock
  - Configuration of token settings and Token Password quality
  - Token renaming
  - Logging
- SafeNet Authentication Client settings configuration
- SafeNet Authentication Client Customization Tool

NOTE:
SafeNet Authentication Client offers full backward compatibility for eToken PKI Client or SafeNet Borderless Security Client (BSec). Future versions of SafeNet Authentication Client may not support BSec compatibility.

1.- Some of the features listed under “SafeNet Authentication Client Main Features” may not be supported on certain IDPrime MD smart cards. For more details refer to the relevant section in this document.

What's New

SafeNet Authentication Client 10.2 (GA) offers the following new features:

- **Support for PIN Pad - See "External Smart Card Readers" on page 11** for a list of supported PIN Pad readers.
- **Support for Gemalto IDPrime MD 3811 (applet 4.1.3)**

Supported Tokens and Smart Cards

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

Certificate-based USB Tokens

- SafeNet eToken 5110
- SafeNet eToken 5110 CC
- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 FIPS HID
- SafeNet eToken 5110 HID

Certificate-based Hybrid USB Tokens

- SafeNet eToken 7300
- SafeNet eToken 7300-HID

Software Tokens

- SafeNet Virtual Token
- SafeNet Rescue Token

Smart Cards

- Gemalto IDPrime MD 840
- Gemalto IDPrime MD 840 B
- Gemalto IDPrime MD 3840
- Gemalto IDPrime MD 3840 B
- Gemalto IDPrime MD 830-FIPS
- Gemalto IDPrime MD 830-ICP
- Gemalto IDPrime MD 830 B
- Gemalto IDPrime MD 3810
- Gemalto IDPrime MD 3811
- Gemalto IDPrime .NET (only SAC PKCS#11 and IDGo 800 Minidriver interfaces).

NOTE:
For more information on IDPrime MD Smart Cards, see the IDPrime MD Configuration Guide.

End-of-Sale Tokens/Smart Cards

- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID
- SafeNet eToken 4100
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)

NOTE:
SafeNet HID tokens are not compatible with Smart Card Logon and CAPI based VPN applications).

End-of-Life Tokens/Smart Cards

- SafeNet eToken PRO 32K v4.2B
- SafeNet eToken PRO 64K v4.2B
- SafeNet eToken Pro SC 32K v4.2B
- SafeNet eToken Pro SC 64K v4.2B
- SafeNet eToken 7100 (SafeNet eToken NG-Flash)
- SafeNet iKey: 2032, 2032u, 2032i (Windows and Mac only)
- SafeNet smart cards: SC330, SC330u, SC330i
- SafeNet eToken 5000 (iKey 4000)
- SafeNet eToken 4000 (SC400)
- SafeNet eToken PRO Java 72K
- SafeNet eToken PRO Anywhere
- SafeNet eToken PRO Smartcard 72K

External Smart Card Readers

SafeNet Authentication Client 10.2 supports the following smart card readers:

- Gemalto IDBridge K30
- Gemalto IDBridge K50
- Gemalto IDBridge CT30
- Gemalto IDBridge CT40
- Gemalto IDBridge CL 3000 (ex Prox-DU)
- SCR 3310 v2 Reader
- Athena AESDrive IIIe USB v2 and v3
- Advanced Card System ACR 1281U
- Athena Keyboard
- Omnikey 3121
- Dell Broadcom
- Unotron

Mobile PKI Bluetooth Readers:

- SafeNet Reader CT1100
- SafeNet Reader K1100

> **NOTE**:
> SC Reader drivers must be compatible with the extended APDU format in order to be used with RSA-2048 (relevant to SafeNet eToken 4100).

Secure PIN Pad Readers:

SafeNet Authentication Client 10.2 supports the following PIN pad readers:

- Gemalto IDBridge CT700
- Gemalto IDBridge CT710
- Ezio Shield Pro
- Ezio Bluetooth Reader
- Ezio BLE

Tablets

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

- Lenovo ThinkPad Tablet running Windows 8.
- Microsoft Surface Pro 4 running Windows 8.1 and Windows 10.

Supported Localizations

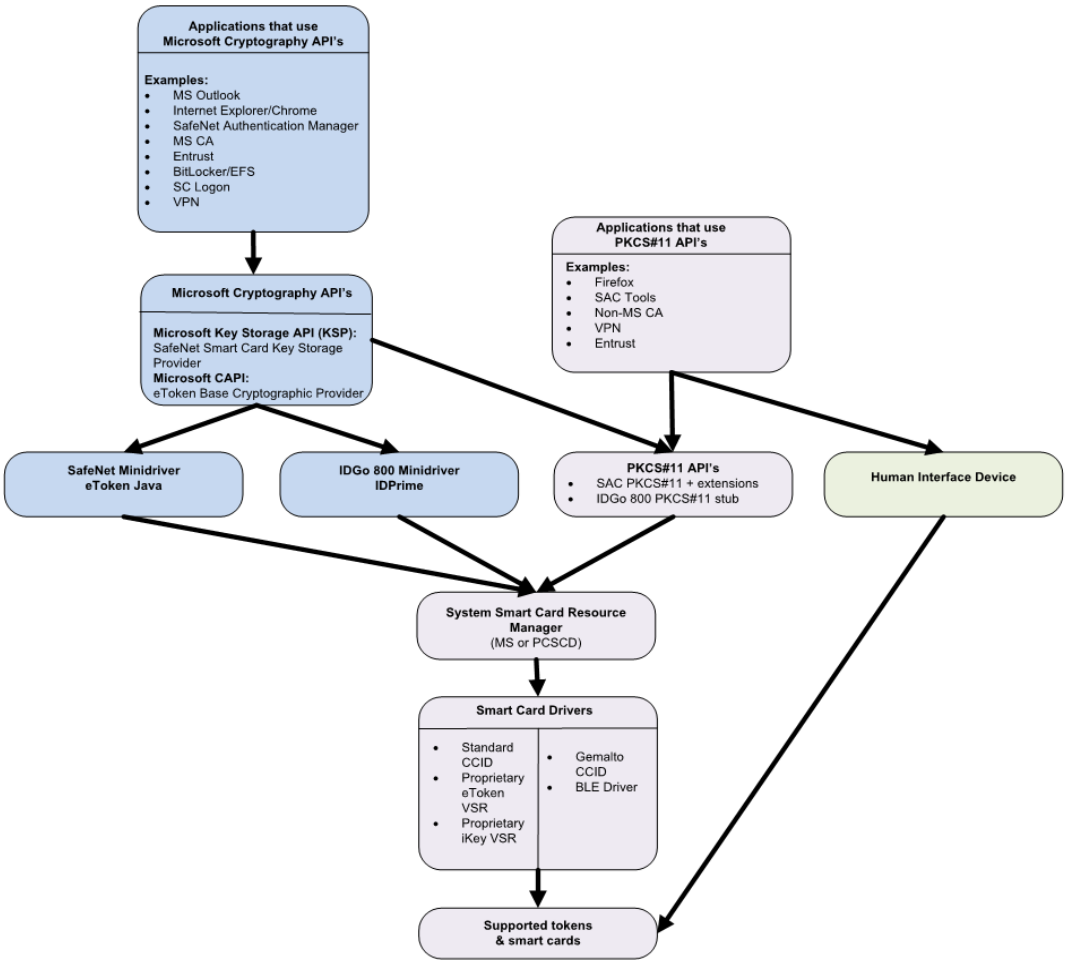
SafeNet Authentication Client 10.2 (GA) supports the following languages:

• Chinese (Simplified and Traditional)	• Italian	• Romanian
• Czech	• Japanese	• Russian
• English	• Korean	• Spanish
• French (Canadian and European)	• Lithuanian	• Thai
• German	• Polish	• Vietnamese
• Hungarian	• Portuguese (Brazilian)	• Turkish

NOTE:

- When using IDPrime MD, .Net cards and eToken 5110 CC, the user PIN and Admin Pin can be in English only.
- IDPrime features are available in English localization only (e.g. Iinitializing Common Criteria devices and PIN Pad functionality).

SafeNet Authentication Client API Flow



License Activation

SafeNet Authentication Client 10.2 (GA) is installed by default as non-licensed.

NOTE:
IDGo 800 Minidriver is part of the SafeNet Authentication Client 10.2 Customization Tool package. The usage and installation of the IDGo 800 Minidriver as a standalone component does not require licensing.

To activate the license perform the following steps:

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

     See the *Licensing* chapter in the *SafeNet Authentication Client 10.2 (GA) User Guide*.
   - Command Line Activation

     See "PROP_LICENSE_FILE Property" on page 48 (Command Line column) and *Installing the MSI file via the Command Line* on page 44.

   Group Policy Object Editor

   See "License Settings" on page 75 (ADM File Setting column) and *Setting SafeNet Authentication Client Properties* on page 65.
   - SafeNet Authentication Client Customization Tool

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

     See *Using the SafeNet Authentication Client Customization Tool*, step 3, on page 26.

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

IDPrime MD Applet 4.0

The IDPrime MD Applet 4.0 is Common Criteria certified on IDPrime MD 840 and 3840. These cards can have certain parameters customized in the factory with different values to the standard default profile.

The following parameters can be customized:

- Number and type of key containers
- Support of RSA 4,096-bit key containers (import operation only) - Note: The card needs to be configured by the SAC supported key length.
- Change PIN at first use Secure messaging in contactless mode
- PINs (#1, #3 and #4 only)
- Try Limit
- Unblock PIN (PIN#1 only)
- Policy values
- Properties
- PIN validity period
- Secure messaging in contactless mode

Number and Type of Key Containers

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

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

API Adjustments

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

Standard PKCS#11 API	Extended PKCS#11 API
The `C_InitToken` function must receive the current Security Officer (SO) Password	The `C_InitToken` function must receive the current Security Officer (SO) Password
When the `C_InitToken` function is called, you can enable linked mode on the IDPrime MD CC device by using the following registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SafeNet\Authentication\SAC\Init - LinkMode (DWORD)` The registry key must be set to 1 and the device must be in the factory initialized state (Admin key = 48 zeros, PUK = 6 zeros) To revert a device back to unlinked mode after it was initialized in linked mode, use the PKCS#11 Extended API, or by using SAC Tools initialization process.	To initialize the IDPrime MD CC device, the `ETCKA_CC` attribute must be set to `CK_TRUE`. To initialize a device in linked mode, set the `ETCKA_IDP_CC_LINK` attribute to `1`. To pass the current Digital Signature PUK value, use the `ETCKA_IDP_CURRENT_PUK` attribute. To revert a device back to unlinked mode after it was initialized in linked mode, set the `ETCKA_IDP_CC_LINK` attribute to `0` and use the `ETCKA_PUK` attribute to set the new Digital Signature PUK value.
If a device is not configured to use linked mode, the `C_InitToken` function ignores the Digital Signature PUK and Digital Signature PIN.	If a device is not configured to use linked mode, use the `ETCKA_PUK` attribute to set the new Digital Signature PUK value.
After the device has been initialized in linked mode, the `C_InitPIN` function initializes the Digital Signature PIN and the User PIN. Both PIN's are set to the same value. The `C_SetPIN` function used with the `CKU_SO` flag changes both the Administrator PIN and Digital Signature PUK to a new value. See the SafeNet Authentication Client User Guide for details on Friendly Admin Password. The C_SetPIN function used with the CKU_USER flag changes both the User PIN and Digital Signature PIN to a new value.	If the device is initialized to use linked mode, the `C_InitPIN` function and `C_SetPIN` function behaves the same as described in the Standard PKCS#11 section.

System Requirements

Before installing SafeNet Authentication Client, ensure that your system meets the minimum requirements.

In this chapter:

- Supported Browsers
- Supported Platforms
- Hardware and Screen Resolution Requirements
- Compatibility with Gemalto Applications
- Compatibility with Third-Party Applications

Supported Browsers

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

- Firefox (up to and including version 50)
- Internet Explorer (up to and including version 11 and Metro)
- Microsoft Edge 38.14393.0.0 and 25.10586.672.0 (does not support certificate enrollment)
- Chrome version 54, for authentication only (does not support certificate enrollment)

Supported Platforms

SafeNet Authentication Client 10.2 (GA) supports the following operating systems:

- Windows Server 2008 R2 SP1 (32-bit, 64-bit)
- Windows Server 2008 SP2 (32-bit, 64-bit)
- Windows Server 2012 and 2012 R2 (64-bit)
- Windows Server 2016 (64-bit)
- Windows Vista SP2 (32-bit, 64-bit)
- Windows 7 SP1 (32-bit, 64-bit)
- Windows 8 (32-bit, 64-bit)
- Windows 8.1 (32-bit, 64-bit)
- Windows 10 (32-bit, 64-bit)

NOTE:
In Windows 8.1 environments, SafeNet eToken 7300 devices earlier than version 9.0.35 can be used only when SafeNet Authentication Client is installed.

Hardware and Screen Resolution Requirements

Required hardware:

- USB port, for physical token devices
- Recommended display resolution (for SafeNet Authentication Client Tools) 1024 x 768 pixels and higher.

Compatibility with Gemalto Applications

IDPrime MD cards can be used with the following products:

- IDGo 800 Credential Provider (V1.2.4)
- IDGo 800 User Tool for Windows (V1.1.30)
- IDGo 800 Cert Tool (V1.0.5)
- IDGo 800 Minidriver (V1.2.8) (dll - v8.5.0.5)

NOTE:
SafeNet Authentication Client provider is installed by default.

To work with these products, install IDGo 800 Minidriver by generating an .msi file using the SAC Customization Tool. See "Generating a Customized MSI Installation File" on page 32.

SafeNet Authentication Client can be used with the following products:

- SafeNet Network Logon 8.3
- SafeNet Authentication Manager 8.2.158.749 (Gemalto IDPrime MD 840 / 3840 are not supported on this version of SAM).

Compatibility with Third-Party Applications

The majority of third-party applications listed below have been validated and tested with SafeNet Authentication Client 10.2 (GA).

For more information see the Solution Marketplace section in the Service Portal:

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

https://kb.safenet-inc.com/kb/link.jsp?id=GUD253

Solution Type	Vendor	Product Version
Remote Access VPN	Check Point	Client E-80 (Security Gateway)
	Microsoft	Windows Server 2008 SP2 and later
	Cisco	NAM
		AnyConnect
	Palo Alto	PA- 200 GW Appliance
	Juniper	Juniper MAG 2600 GW Appliance
Virtual Desktop Infrastructure (VDI)	Citrix	XenApp/XenDesktop 7.11
	Microsoft	Remote Desktop
Identity Access Management (IAM) Identity Management (IDP)	VMware View	Horizon 6.0
	IBM	ISAM for Web 9.0 (eToken only)
	Intercede	MyID (eToken only)
	Microsoft	FIM 2010 R2
	IDnomic	OpenTrust CMS 4.9.1
Pre Boot Authentication (PBA)	Sophos	SafeGuard Easy (eToken only)
	Microsoft	BitLocker (RSA only)
Certificate Authority (CA)	Entrust	SMA 8.1 (eToken only)
	Check Point (Local CA)	For All Check Point platforms
	Microsoft (Local CA)	For All Windows platforms
Local Access	Microsoft	All supported OS
	Evidian	ESSO (eToken only)
Digital Signatures	Entrust	ESP 9.2 (eToken only)
	Adobe	Reader XI and DC
	Microsoft	Outlook 2010 and 2013
	Mozilla	Thunderbird 45

Customization

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

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

In this chapter:

- Customization Overview
- Compatibility with IDGo 800 Minidriver and PKCS#11
- Features to Install
- Using the SafeNet Authentication Client Customization Tool
- Features to Install
- Installing the Customized Application

Customization Overview

You can customize the following SafeNet Authentication Client 10.1 (GA) features:

- Product name, which appears in the installation wizard, the *Add/Remove* program, and the *About* window
- Destination folder
- URL of the support link in the *Add/Remove* program
- License string
- SafeNet Authentication Client and IDGo 800 features to be installed
- Policy settings
- MSI Signing settings
- Window banners

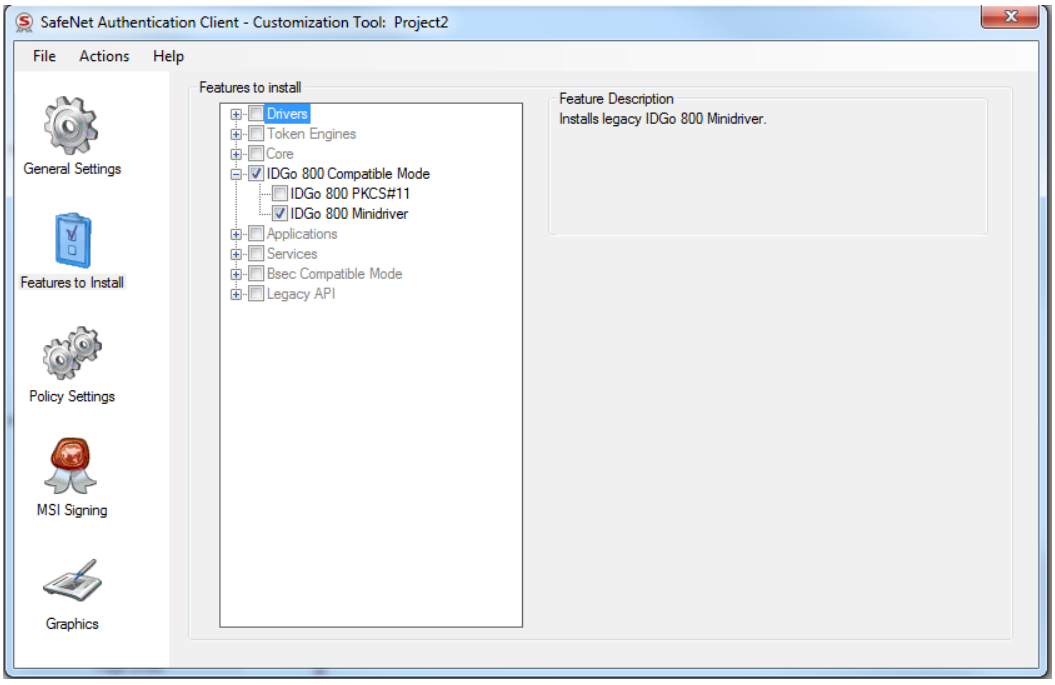
Compatibility with IDGo 800 Minidriver and PKCS#11

SAC 10.2 Customization Tool enables you to generate an .msi file, which contains IDGo 800 Minidriver and IDGo 800 PKCS#11 proxy.

For details on the compatibility of IDGo 800 with SAC and different use cases, see the SafeNet Authentication Client 10.1 Planning Guide.

Configuring IDGo 800 Minidriver Only

Selecting the IDGo 800 Minidriver check-box in the ***Features to install*** list will generate an .msi file that contains only the Gemalto IDGo 800 Minidriver. This option disables all other features in the list, except for the IDGo 800 PKCS#11 check-box.



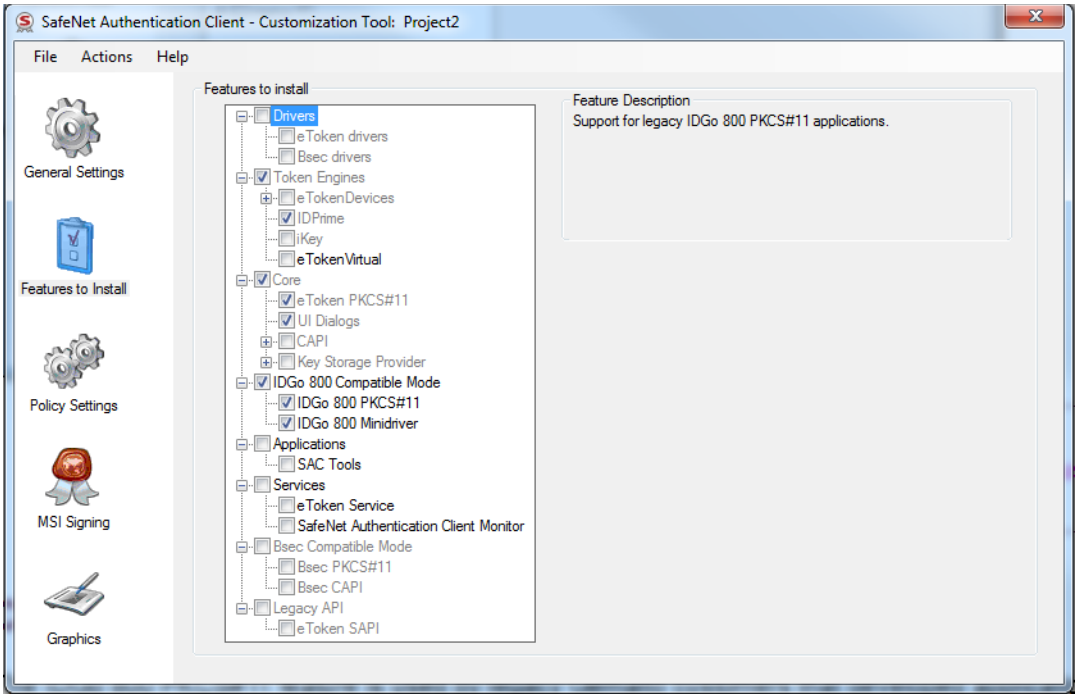
When selecting the IDGo 800 Minidriver check-box, the following IDGo 800 Minidriver binary files are installed:

Dll File	Description
axaltocm.dll	Installed in the System32 folder.
axaltocm.dll	Installed in the SysWOW64 folder.

Configuring IDGo 800 PKCS#11 for Backward Compatibility

The IDGo 800 PKCS#11 feature is used by Gemalto customers that have existing applications that use IDGo 800 PKCS#11 and have a dependency on the location of IDGo 800 PKCS#11 dll file. Selecting the IDGo 800 PKCS#11 check-box in addition to the IDGo 800 Minidriver check-box enables other features in the list, such as SAC Tools and SAC Monitor.

Selecting the IDGo 800 PKCS#11 together with SAC features enables Gemalto customers with existing applications that depend on it to seamlessly migrate to SAC without breaking compatibility of these applications.



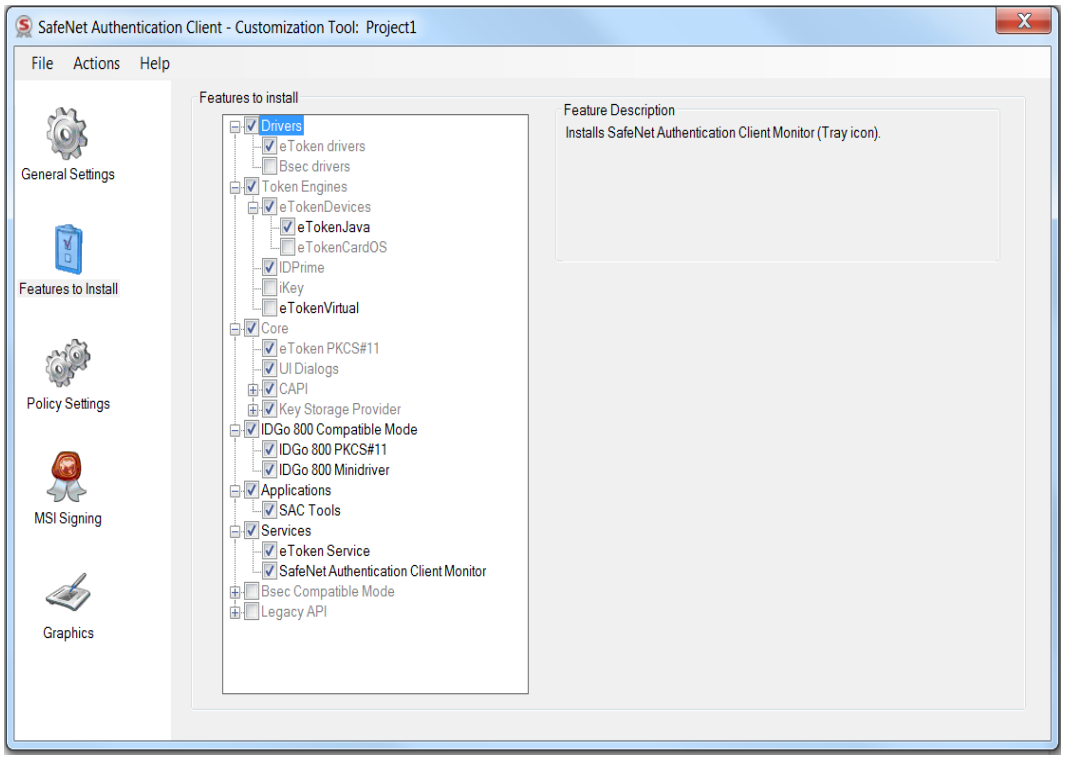
When selecting the IDGo 800 Compatible Mode check-boxes, the following dll files are installed under C:\Program Files (x86)\Gemalto\IDGo 800 PKCS#11:

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

Installing IDGo 800 Minidriver and SafeNet Authentication Client eToken Features

To work with both IDGo 800 Minidriver and SafeNet Authentication Client eToken, select the options as displayed in the image below.

Working in this mode ensures that the certificates on IDPrime devices will use Microsoft Smart Card CSP and the certificates on eToken devices will use SafeNet CSP.



Installing the SafeNet Authentication Client Customization Tool

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

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

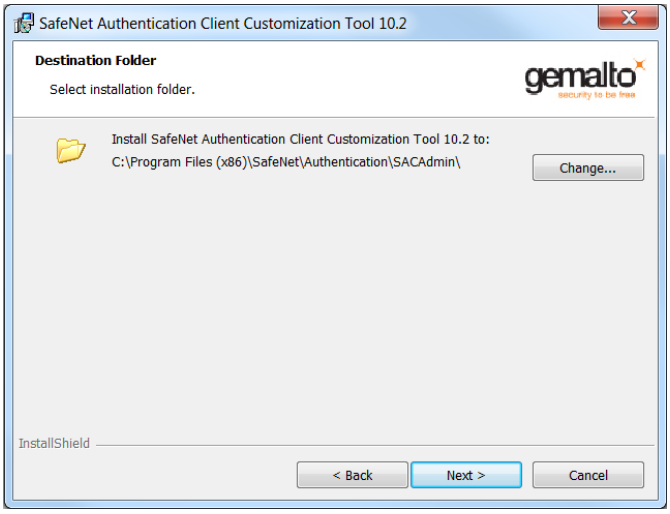
To install the SafeNet Authentication Client Customization Tool:

1. Double-click **SACCustomizationPackage-10.2.msi**.
   The *SafeNet Authentication Client Customization Package Installation Wizard* opens.

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

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

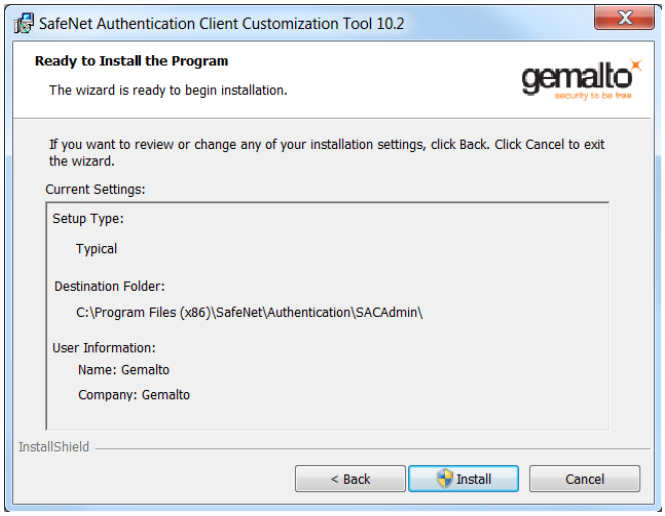
The *Destination Folder* window opens, displaying the default installation folder.



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

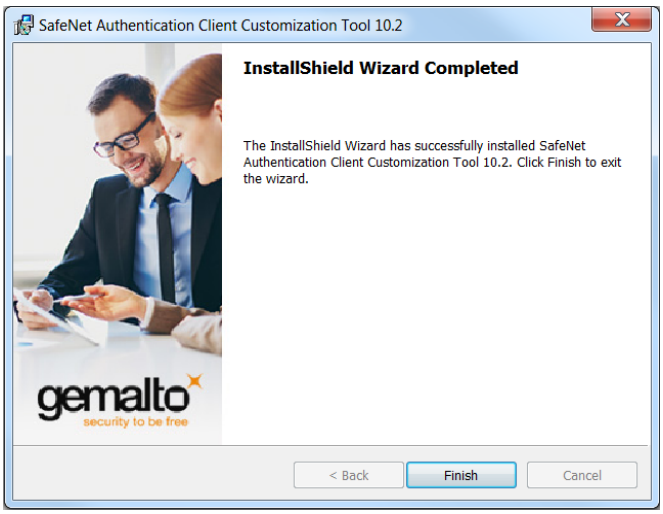
> **NOTE**:
> If an application from the SafeNet Authentication line of products, or an eToken legacy product, is already installed, we recommend that the destination folder not be changed.

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



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

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



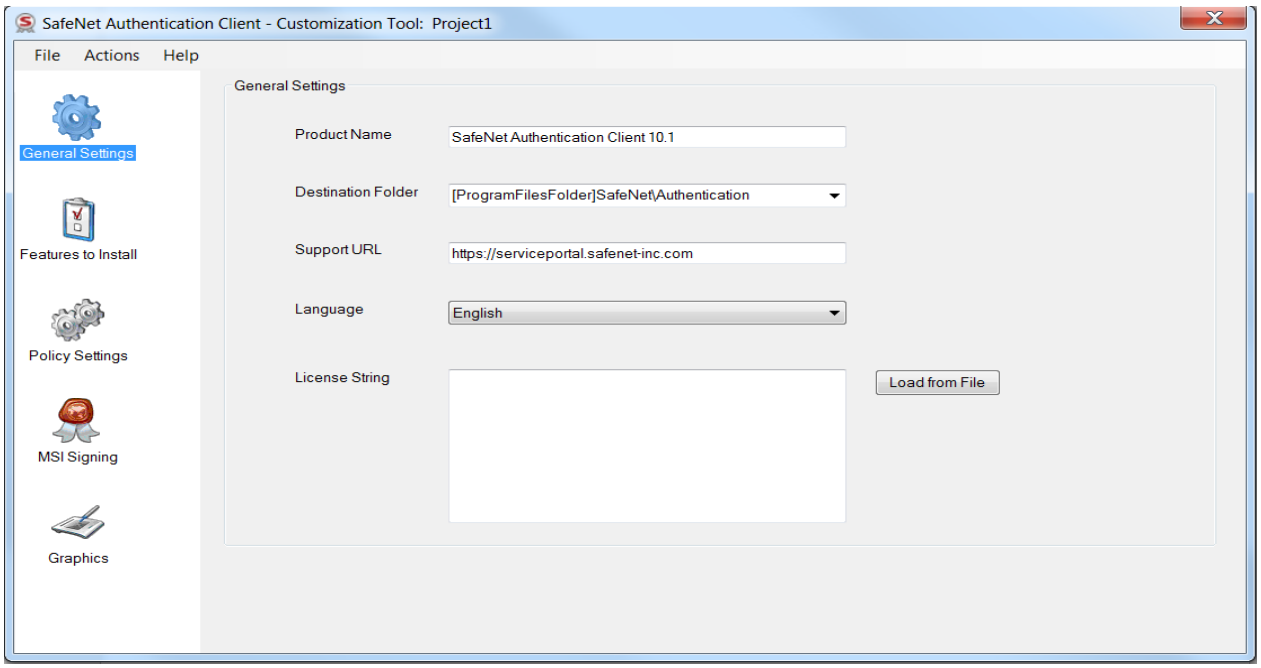
7. Click **Finish** to exit the wizard.

Using the SafeNet Authentication Client Customization Tool

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

To use the Customization Tool:

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



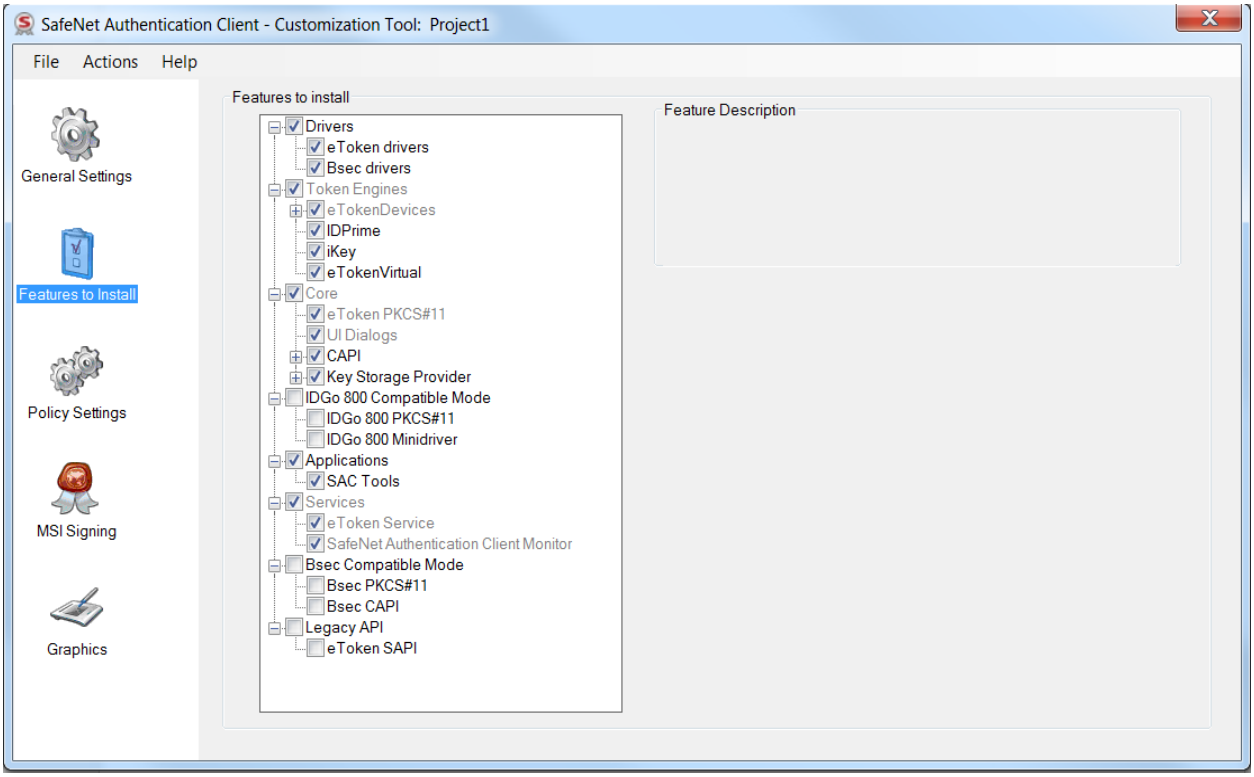
2. To open a project you already saved, select **File > Open**, and browse to the xml file of an existing project.

3. You can replace the following items:
   - **Product Name:** enter the relevant product name (the default value is SafeNet Authentication Client 10.2).
   - **Destination Folder:** the path to be used by the SafeNet Authentication Client Customization Tool when no other SafeNet product has been installed on the client computer
   - **Support URL:** the URL to be displayed in the Windows *Add/Remove Programs* support link (the default value is http://www.safenet-inc.com/authentication).
   - **Language:** select the language in which SafeNet Authentication Client will be installed.

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

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

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

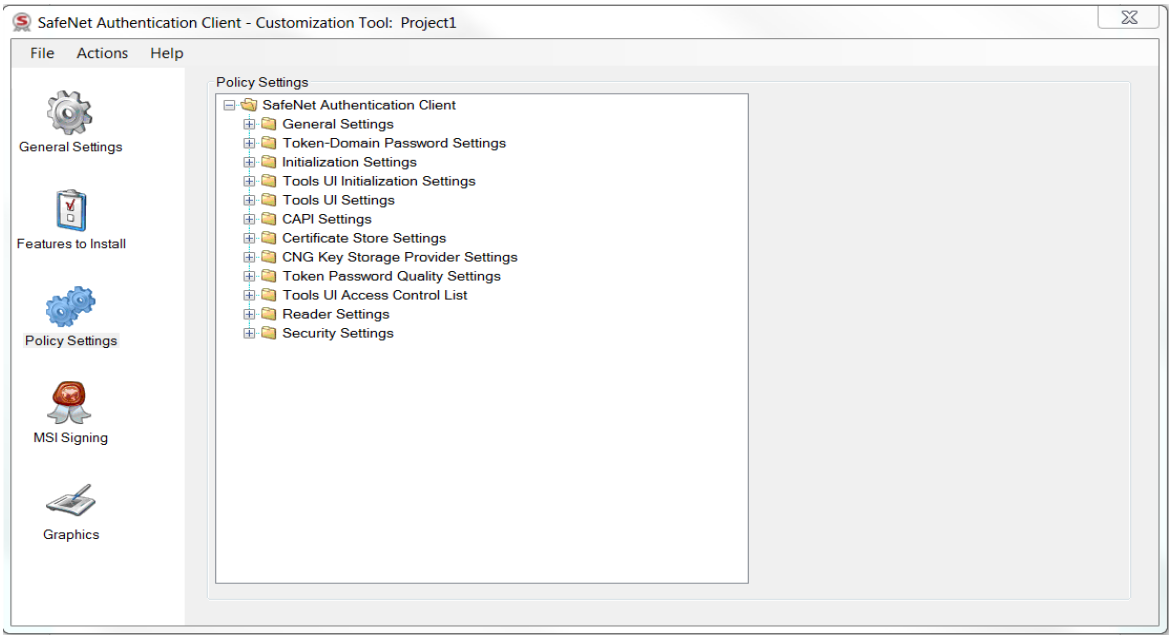


5. The features may be customized by changing the editable check-boxes.

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

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

   The *Policy Settings* window opens.



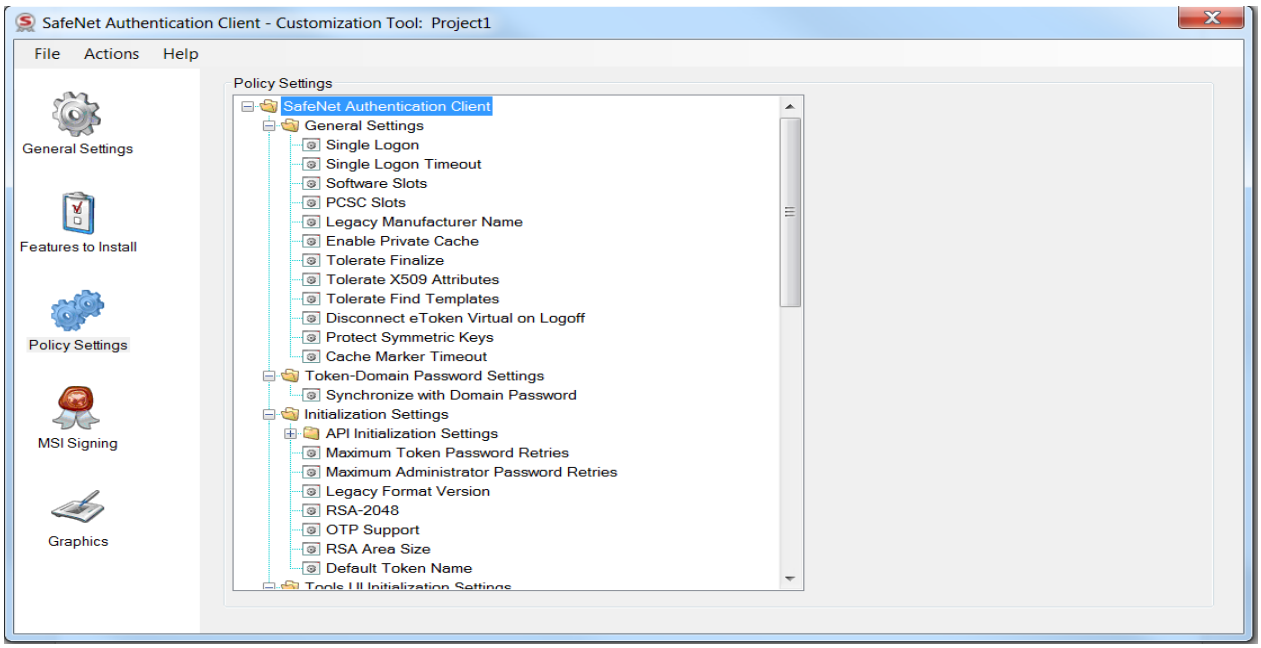
NOTE:
When installing only IDGo 800 Minidriver, the Policy Settings feature are not applicable.

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

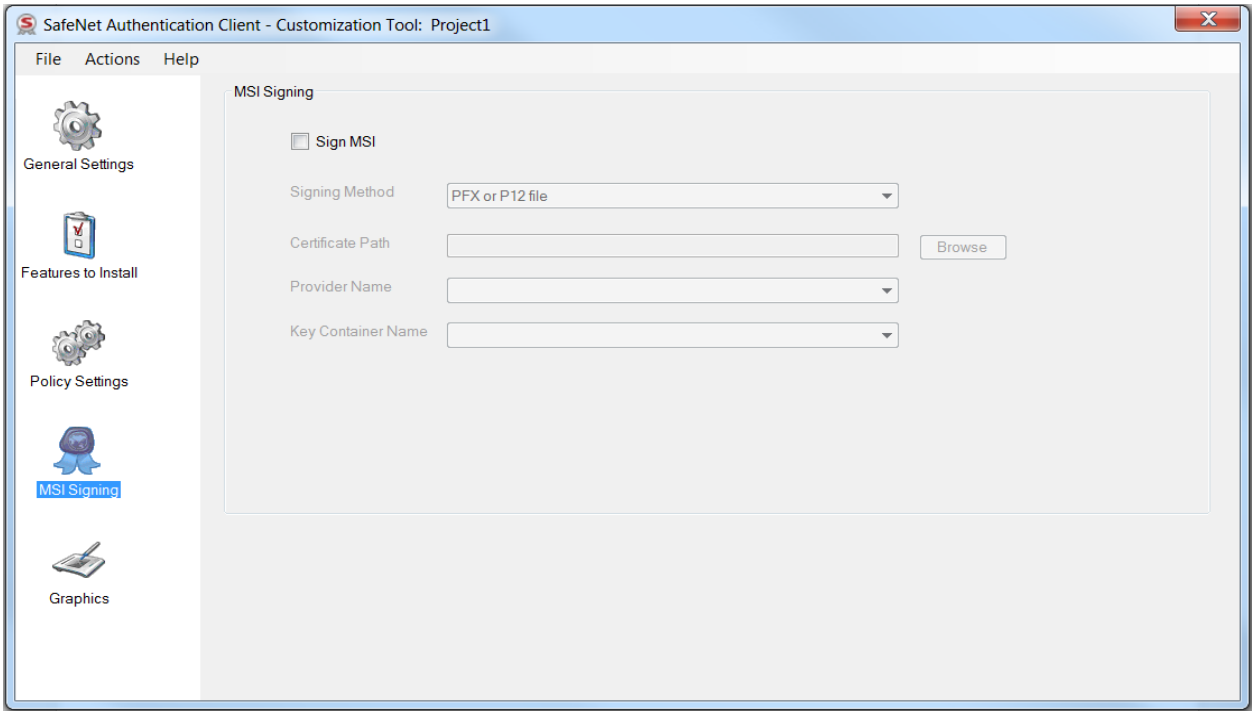
   For more information, see Chapter 8: *Configuration Properties*, on page 65.

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

NOTE:
Not all policy settings are supported by IDPrime MD cards. For more details see Chapter 8: "Configuration Properties" on page 65.



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

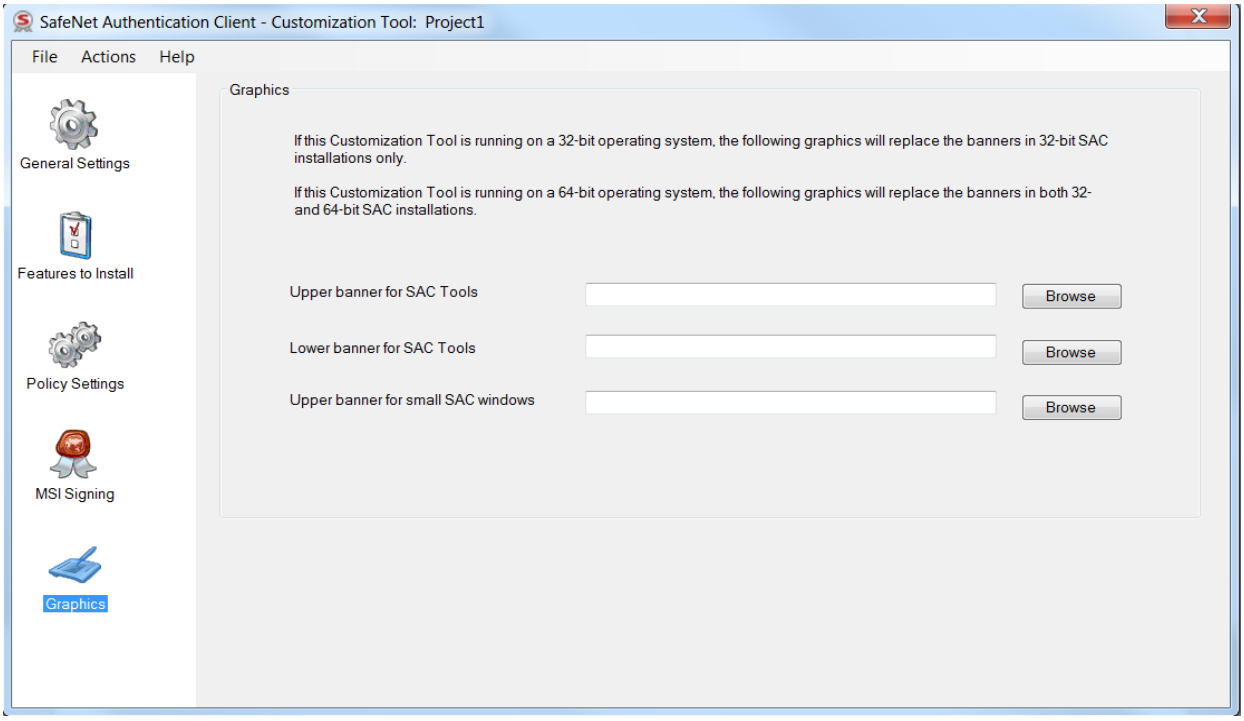


9. To sign the installation file, select **Sign MSI**, and complete the enabled fields. These may include:
   - Signing Method (P12, Smartcard or HSM)
   - Certificate Path
   - Provider Name
   - Key Container Name

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

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

The *Graphics* window opens.



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

The following graphics can be replaced:

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

NOTE:
All banner formats must be in PNG format.

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

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

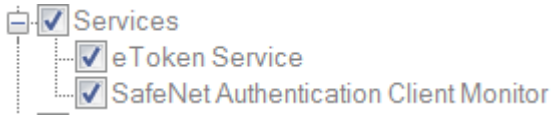
Features to Install

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

For more details on what binary files are installed and their location, see Chapter 5: “SafeNet Authentication Client Binary Files” on page 38.

Services

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

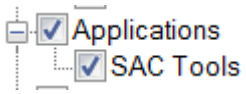


If the above options are selected, the following files are installed:

- SACSRV.exe
- SACMonitor.exe

Applications

Installs the SAC Tools application (Middleware).



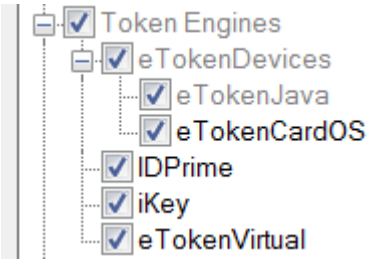
If the above options are selected, the following files are installed:

- SACTools.exe
- SACMonitor.exe

eToken Engines

Installs token engines to support Java and CardOS devices. The following check-boxes are selected and shaded:

- Token Engines
- eTokenDevices
- eTokenJava



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

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

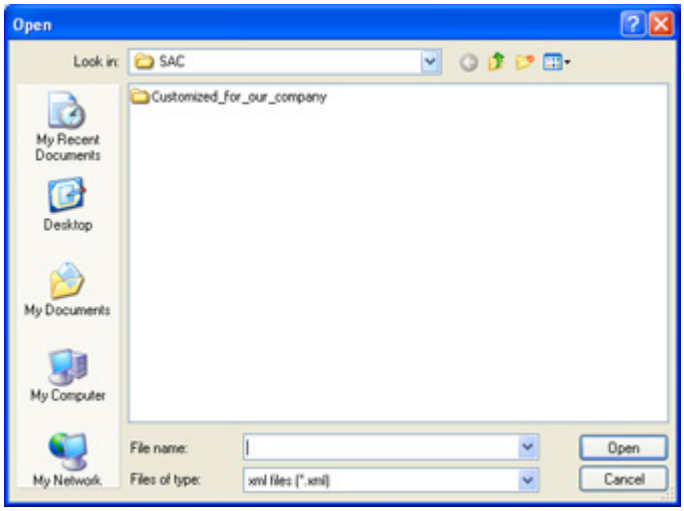
Generating a Customized MSI Installation File

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

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

To generate a customized installation file:

1. Open the *SAC Customization Tool*.
   See "Using the SafeNet Authentication Client Customization Tool" on page 25.
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 10.2 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 now contains two customized MSI files:

- A file named `<Project Name>-x32-10.2.msi` for 32-bit installations

- A file named `<Project Name>-x64-10.2.msi` for 64-bit installations

Installing the Customized Application

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

To install the customized application:

1. Log on as an administrator.
2. Close all applications.
3. Browse to the folder of the customized project saved in *Features to Install* on page 31.

   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>-x32-10.2.msi` (for 32-bit installations)
   - `<Project Name>-x64-10.2.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.

Upgrade

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

NOTE:
- You must restart your computer when the upgrade procedure completes. When upgrading via the command line using the /qn parameter, your computer is restarted automatically.
- When upgrading from previous versions of SAC, it is recommended that you save feature settings from the previous versions. If not, then uninstall and install SAC 10.2 with the new feature list.

In this chapter:

- Upgrading Using the SafeNet Authentication Client .exe or .msi Files
- Upgrading from Versions Earlier than SAC 9.0
- Upgrading from SafeNet Authentication Client 9.0

Upgrading Using the SafeNet Authentication Client .exe or .msi Files

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

The **SafeNetAuthenticationClient-x32-x64-10.2 (GA).exe** simplified installer file upgrades previous versions of SafeNet Authentication Client on 32-bit and 64-bit environments. The simplest way to upgrade to SafeNet Authentication Client 10.2 (GA) is to use an .exe simplified installer file.

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

- On a 32-bit system, run **SafeNetAuthenticationClient-x32-10.2.msi**.
- On a 64-bit system, run **SafeNetAuthenticationClient-x64-10.2.msi**.

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

Upgrading from Versions Earlier than SAC 9.0

Legacy versions of SafeNet Authentication Client, earlier than 9.0 must be uninstalled before installing SafeNet Authentication Client 10.2 (GA).

Upgrading from SafeNet Authentication Client 9.0

You can upgrade from SafeNet Authentication Client 9.0 to 10.2 using the **MSI** file wizard installation, or by using the command line installation. See Installing the MSI file via the Command Line on page 44.

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

Installation

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

NOTE:
- When using an MSI file to install on Windows 7, do not run the installation from the *Desktop* folder. To ensure a successful installation, run the installation from another location on your computer.
- Systems later than Windows 7 and Window 2008 R2, the total number of readers is limited to 10 from among: iKey readers, eToken readers, third-party readers, and reader emulations.

Firefox Settings:
- After installing SAC 10.2, ensure that the Gemalto PKCS#11 module does not exits in the Firefox security settings.

To customize the user interface and the features to be installed, see Chapter 3: *Customization*, on page 19.

In this chapter:

- Installation Files
- SafeNet Authentication Client Binary Files
- Installation Configurations
- Installing SafeNet Authentication Client on Windows (MSI)
- Installing the MSI file via the Command Line
- Installing SafeNet Authentication Client on Windows (Simplified Installation)

NOTE:
- When installing SafeNet Authentication Client on a computer with IDGo 800 Minidriver, IDGo 800 Minidriver must be uninstalled before installing SAC 10.2.
- If IDGo 800 PKCS#11 is installed, be sure to remove it before installing SAC 10.2.

Installation Files

The software package provided by SafeNet includes files for installing or upgrading to SafeNet Authentication Client 10.2 (GA).

The following installation and documentation files are provided:

File	Environment	Description	Use
Windows			
SafeNetAuthenticationClient-x32-x64-10.2.exe	32-bit 64-bit	Installs SafeNet Authentication Client 10.2, and upgrades from earlier versions (8.3 or 9.0) of SafeNet Authentication Client.	Use to install SafeNet Authentication Client 10.2 (GA), and to upgrade from: SafeNet Authentication Client 8.3 or 9.0.
SafeNetAuthenticationClient-x32-10.2.msi	32-bit	Installs SafeNet Authentication Client 10.2, and upgrades from version 8.3 or 9.0 of SafeNet Authentication Client.	Use to install SafeNet Authentication Client 10.2 (GA) and upgrades from version 8.3 or 9.0of SafeNet Authentication Client.
SafeNetAuthenticationClient-x64-10.2.msi	64-bit		
SACCustomizationPackage-10.2.msi	32-bit 64-bit	Installs SafeNet Authentication Client 10.2 (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.
Documentation Files			
007-013559-003_SafeNet Authentication Client_ 10.2_Windows_GA_CRN_Revision A		SafeNet Authentication Client 10.2 (GA) Customer 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.
007-013561-002_SafeNet Authentication Client_10.2_GA_User_Guide_Revision A		SafeNet Authentication Client 10.2 (GA) User Guide for Windows	Provides detailed information for the user and system administrator regarding the use of SafeNet Authentication Client.
007-013560-002_SafeNet Authentication Client_10.2_GA_Administrator_Guide_Revision A		SafeNet Authentication Client 10.2 (GA) Administrator Guide for Windows (this document)	Provides detailed information for the system administrator regarding the installation, configuration, maintenance, and management of SafeNet Authentication Client.

SafeNet Authentication Client Binary Files

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

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

Folder/File	Folder Contents (.exe, .dll, .reg, .iso files)	Description
Install	• pki_defaults.reg	Default registry file. Double click the pki_defaults.reg file to change SAC configuration back to the default configuration.
ISO	• Default.iso	Default ISO for eToken 7300 devices.
LogoImages	• SACBottomLogo.png • SACLogo.png • SACTopLogo.png	Contains SAC Logo image files. These files may be customized using the SafeNet Authentication Client Customization Tool.
x32	• Language support packages (e.g. cs-CZ, fr-CA, etc.) •	These folders contain Windows x32-bit and x64-bit related DLL's and packages. **Note:** For x64-bit installations, both directories (x32 and x64) are created. All x64-bit binaries are located in the x64 folder and x32-bit binaries are located in the x32 folder. All .exe files (applications) are located in the x64 folder only. If a custom installation is performed using the SAC Customization Tool, additional .exe files will be shown in either the x32 or x64 folders.
x64	• cardosTokenEngine.dll- installs the CardOS token engine. This file is the main SAC dll file, which contains the majority of SAC codes and the eToken java engine (required for all devices). • eTokenHID.dll - this file supports HID devices (only required for devices that are in HID mode). • etvTokenEngine.dll - installs the SafeNet Virtual Token engine. • IDPrimeTokenEngine.dlll - installs the DPrime token/card engine. • iKeyTokenEngine.dll - installs the iKey token engine. • ManageReaders.exe - this application manages reader settings (uses eTCoreInst.dll). • RegistereTokenVirtual.exe - this application manages the registration of SafeNet Virtual Tokens. • SACLog.dll - manages all application logs and DLL's (The 'Enable logging' options must be selected). • SACMonitor.exe - Installs the SafeNet Authentication Client application. • SACSRV.exe - Installs SafeNet Authentication Client services • SACTools.exe - Installs SACUI.dll	
App-RTE	SafeNet Authentication Client icon	
SACHelp	SafeNet Authentication Client User Guide	This file opens when clicking the Help icon in SAC Tools.

System32 and SysWOW64 Folders

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

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

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

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

NOTE:
- For 64-bit installations, both the C:\Windows\System32 folder and C:\Windows\SysWOW64 folder are created and all the 64-bit binaries are located in the System32 folder and all 32-bit binaries are located in the SysWOW64 folder.
- For 32-bit installations, only the C:\Windows\System32 folder is created and only the 32-bit binaries are located in this folder.

Installation Configurations

SafeNet Authentication Client can be installed with the following configurations:

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

Installing SafeNet Authentication Client on Windows (MSI)

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

The components that can be set using the wizard are:

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

- **Custom**: installs only the application features you select.

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

To install via the installation wizard:

1. Log on as an administrator.
2. Close all applications.
3. Double-click the appropriate file:
   - `SafeNetAuthenticationClient-x32-10.2.msi` (32-bit)
   - `SafeNetAuthenticationClient-x64-10.2.msi` (64-bit)

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

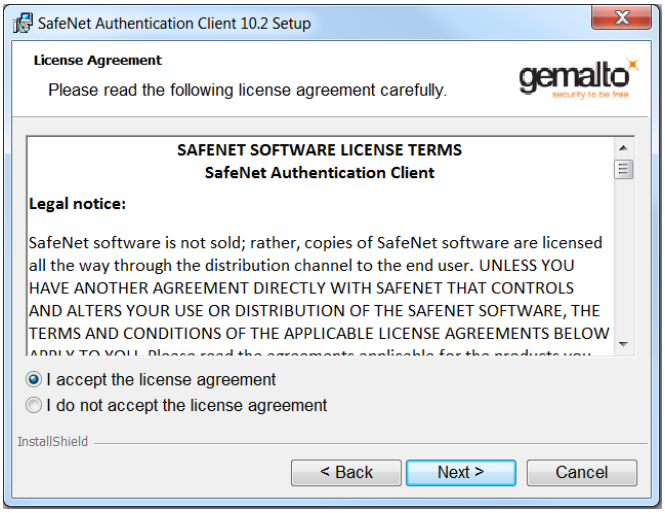
4. Click **Next**.

The Interface Language window is displayed.

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

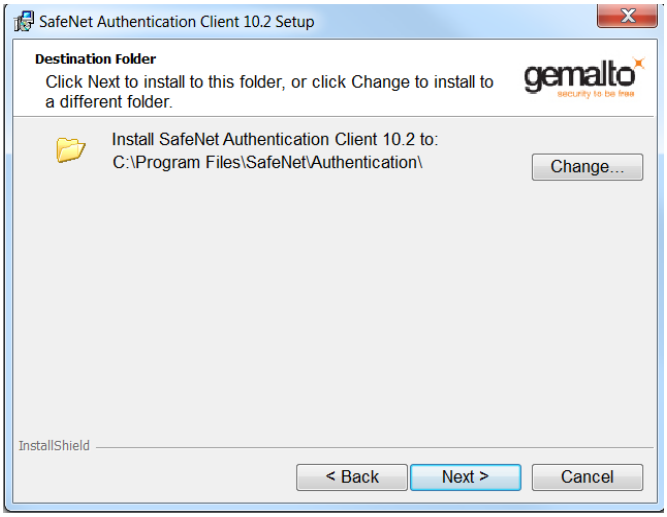
5. From the dropdown list, select the language in which the SafeNet Authentication Client screens will appear.
6. If configuration settings are detected from a previous version, you can select **Use the existing configuration settings**.
7. Click **Next**.

   The *End-User License Agreement* is displayed.



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

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



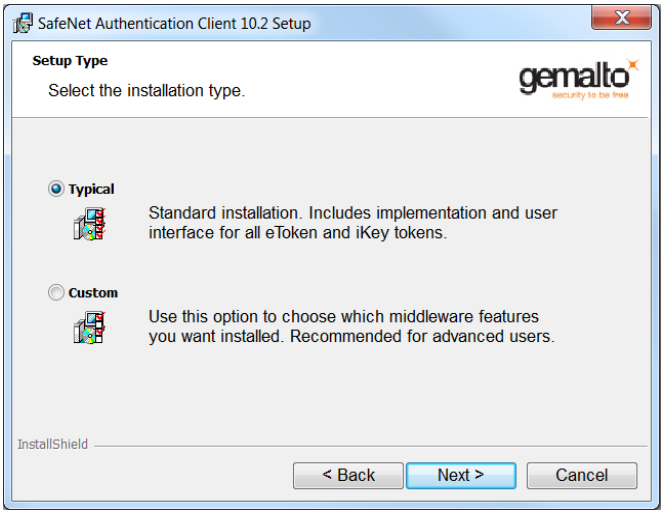
10. You can click **Change** to select a different destination folder, or install the *SAC* application into the default folder:
`C:\Program Files\SafeNet\Authentication\`

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

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

11. Click **Next**.

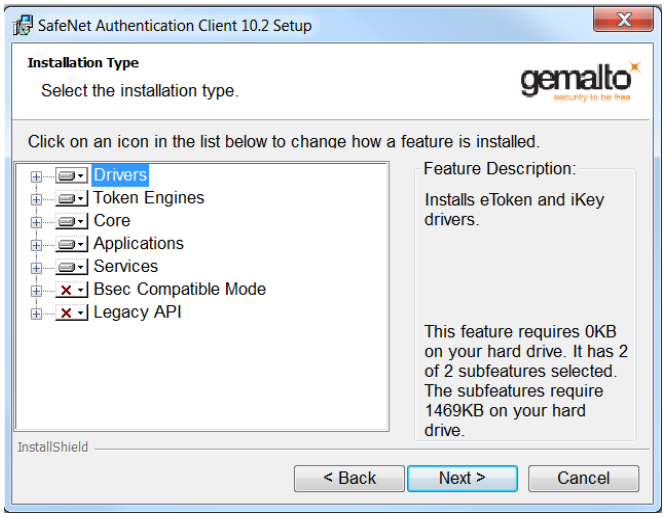
The *Setup Type* window opens.



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

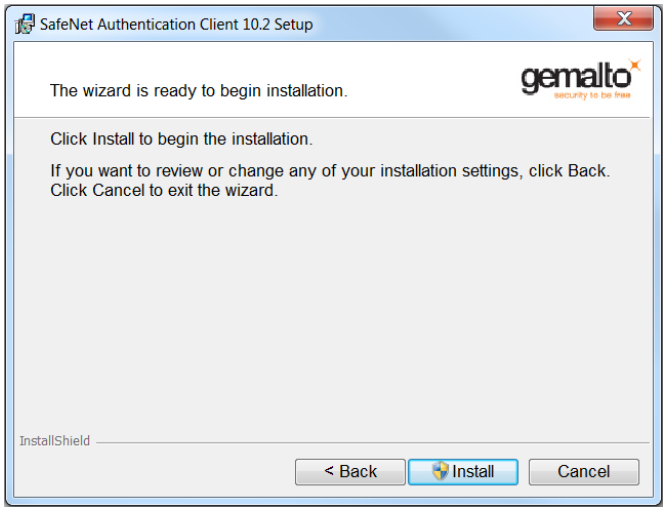
13. If you select **Custom**, click Next.

    The *Custom Installation Type* window opens.



14. Use this window to enable or disable specific features. Some features cannot be disabled, as they are mandatory for the installation.
15. If you select **Typical**, click **Next**, and then click **Install** to proceed with the installation.

    The installation proceeds.



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

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

Installing the MSI file via the Command Line

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

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

- for 32-bit systems:
  `msiexec /i SafeNetAuthenticationClient-x32-10.2.msi`
- for 64-bit systems:
  `msiexec /i SafeNetAuthenticationClient-x64-10.2.msi`

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

To install via the command line:

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

Installing in Silent Mode

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

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

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

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

Setting Application Properties via the Command Line

During a command line installation, the administrator can override the application's default values by including specific properties, and assigning each a value. These new values are saved in `HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC`.
For more information, see Chapter 8: *Application Properties Hierarchy*, on page 66.

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-x32-10.2 (GA).msi PROPERTY=VALUE
  PROPERTY=VALUE /qb
  ```
- For 64-bit systems:
  ```
  msiexec /i SafeNetAuthenticationClient-x64-10.2 (GA).msi PROPERTY=VALUE
  PROPERTY=VALUE /qb
  ```

where

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

See the *Command Line Installation Properties* tableon page 46 for the list of properties that can be set during installation.

Some properties are stored as registry values and can be set or modified after installation. These properties are described in the *General Settings* section on page 69.

Some properties can be set during a command line installation only, and cannot be modified afterwards. These properties are described in the *Installation-Only Properties* sectionon page 46.

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-x32-10.2 (GA).msi
ET_LANG_NAME=Spanish
PROP_ADVANCED_VIEW=0
PROP_CLEAR_REG=1 /qb
```

Command Line Installation Properties

Property	Description
PROP_ETOKENREADERCOUNT	on page 48
PROP_FAKEREADER	on page 48
PROP_IKEYREADERCOUNT	on page 48
PROP_LICENSE_FILE	on page 48
PROP_REG_FILE	on page 49

Deprecated Command Line Installation Properties

Property	Description
ET_LANG_NAME	on page 47
KSP_ENABLED	on page 47
PROP_ADVANCED_VIEW	on page 80
PROP_CLEAR_REG	on page 48
PROP_EXPLORER_DEFENROL	on page 93
PROP_PCSCSLOTS	on page 70
PROP_PQ_HISTORYSIZE	on page 99
PROP_PQ_MAXAGE	on page 98
PROP_PQ_MINAGE	on page 98
PROP_PQ_MINLEN	on page 98
PROP_PQ_MIXCHARS	on page 99
PROP_PQ_WARNPERIOD	on page 99
PROP_PROPAGATECACER	on page 94
PROP_PROPAGATEUSERCER	on page 94
PROP_SINGLELOGON	on page 69
PROP_SINGLELOGONTO	on page 69
PROP_SOFTWARESLOTS	on page 70
PROP_UPD_INFPATH	on page 49
TARGETDIR	on page 49

Installation-Only Properties

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

ET_LANG_NAME Property

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

KSP_ENABLED Property

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

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

PROP_CLEAR_REG Property

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

PROP_ETOKENREADERCOUNT Property

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

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

PROP_FAKEREADER Property

Property Name	PROP_FAKEREADER
Description	Determines if the emulation of a smartcard reader is installed, enabling SafeNet Virtual Tokens to be used with applications requiring a smartcard reader, such as smartcard logon and VPN. **Note:** On Windows Vista 64-bit and on systems later than Windows 7 and Window 2008 R2, the total number of readers is limited to 10 from among: iKey readers, eToken readers, third-party readers, and reader emulations.
Value	1 (True) - Emulation of a smartcard reader is installed 0 (False)- Emulation of a smartcard reader is not installed
Default	1 (True)

PROP_IKEYREADERCOUNT Property

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

PROP_LICENSE_FILE Property

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

PROP_REG_FILE Property

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

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

PROP_UPD_INFPATH Property

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

TARGETDIR Property

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

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

Configuring Installation Features via the Command Line

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

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

```
msiexec /i SafeNetAuthenticationClient-x32-10.2 (GA).msi ADDDEFAULT=F1,F2…Fn
INSTALLLEVEL=n PROP_IKEYREADERCOUNT=n /qb
```

where

- `SafeNetAuthenticationClient-x32-10.2` is the 32-bit SafeNet Authentication Client installation file. For 64-bit systems, use `SafeNetAuthenticationClient-x64-10.2 (GA).msi`.
- `ADDDEFAULT` indicates that only the following features are included in the installation, or added to the installed application.
- `Fx` is the name of each feature to be included.
- `INSTALLLEVEL` indicates the installation level, where `n` is:
  - 3: standard installation (default)

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

SafeNet Authentication Client Command Line Feature Names

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

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

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

Installing All Features - Example

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

```
msiexec /i SafeNetAuthenticationClient-x32-10.2 (GA).msi
```

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

Installing All Features Except KSP Support - Example

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

```
msiexec /i SafeNetAuthenticationClient-x32-10.2 (GA).msi KSP_Enabled=0 /qb
```

Installing Specific Readers - Example

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

msiexec /i `SafeNetAuthenticationClient-x64-10.2 (GA).msi PROP_PCSCSLOTS=10 PROP_ETOKENREADERCOUNT=5 PROP_IKEYREADERCOUNT=3 PROP_SOFTWARESLOTS=2 PROP_FAKEREADER=0 /qb`

Installing without eToken Drivers - Example

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

```
msiexec /i SafeNetAuthenticationClient-x32-10.2 (GA).msi ADDDEFAULT=
BsecDrivers,eTokenSAPI,eTokenPKCS11,IDPrime,IDPrimePKCS11,IDPrimeCAPI,eTokenCAPI,UIDialogs,SACMonitor,SACService,SACTools /qb
```

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

Installing without SAC Tools - Example

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

```
msiexec /i SafeNetAuthenticationClient-x32-10.2 (GA).msi ADDDEFAULT=
eTokenDrivers,BsecDrivers,eTokenSAPI,eTokenPKCS11,IDPrime,IDPrimePKCS11,IDPrimeCAPI,e
TokenCAPI,KSP,UIDialogs,SACMonitor,SACService /qb
```

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

```
msiexec /i SafeNetAuthenticationClient-x32-10.2 (GA).msi ADDDEFAULT=SACTools /qb
```

Removing Features via the Command Line

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

```
msiexec /x SafeNetAuthenticationClient-x32-10.2 (GA).msi REMOVE=F1,F2…,Fn /qb
```

where

- `SafeNetAuthenticationClient-x32-10.2 (GA).msi` is the 32-bit SafeNet Authentication Client installation file. For 64-bit systems, use `SafeNetAuthenticationClient-x64-10.2 (GA).msi`
- `REMOVE` indicates that the following features are to be removed
- `F`x is the name of each feature to be removed

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

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

```
msiexec /x SafeNetAuthenticationClient-x32-10.2 (GA).msi
REMOVE=SACTools /qb
```

Installing SafeNet Authentication Client on Windows (Simplified Installation)

The simplest way to install SafeNet Authentication Client 10.2 (GA) is to use the SafeNetAuthenticationClient-x32-x64-10.2.exe simplified installation file.

NOTE:
This installer file does not support Customization Tool changes.

The SafeNetAuthenticationClient-x32-x64-10.2.exe simplified installation file uninstalls older SAC versions, and then installs SafeNet Authentication Client 10.2 properly on 32-bit and 64-bit environments in each of the following situations:

- No middleware is yet installed (Installation only)

To run the installer on 32-bit and 64-bit systems:

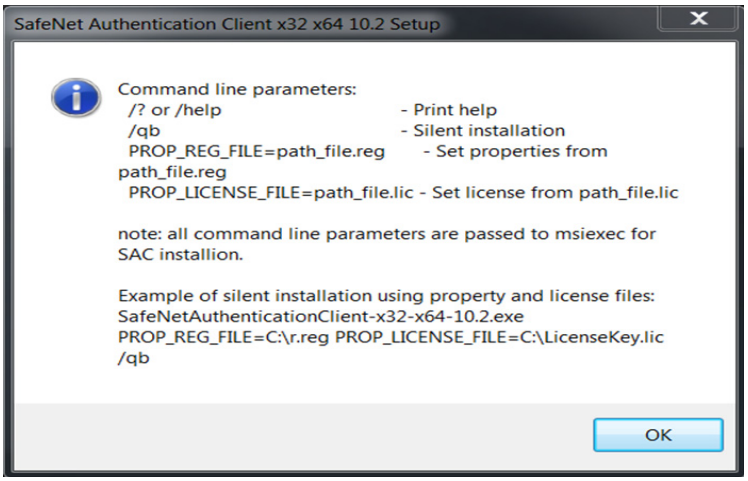
- Double-click the **SafeNetAuthenticationClient-x32-x64-10.2 (GA).exe** file.

Command Line Parameters via the Simplified Installation

All the command line parameters that are described in the section: “Installing the MSI file via the Command Line” on page 44, can also be entered when installing the simplified installation.

From the command line, enter: `SafeNetAuthenticationClient-x32-x64-10.2.exe /h`

The help window opens.



Configuring Root Certificate Storage for Win Server 2008 R2

In most environments, no special configuration is required to store a root certificate on a token. In a Windows Server 2008 R2 environment, the Active Directory Certificate Service registry value, *CertSvc*, must be manually configured to enable a root certificate to be stored on a token. If it is not configured properly, the following message is displayed when an attempt is made to store a root certificate on a token: “Could not load or verify the current CA certificate. The system cannot find the file specified.”

To configure the registry to store a root certificate on a token in Windows Server 2008 R2:

1. In the Windows *Registry Editor*, create a registry value named `RequiredPrivileges`, in the Multi-String Value format, in the following location:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc`

   For more information about creating and editing registry keys, see *Setting Registry Keys Manually*on page 67.

2. In the *Registry Editor* right column, right-click *RequiredPrivileges*, select **Modify**, and add the following lines to the value data:

   `SeTcbPrivilege`

   `SeIncreaseQuotaPrivilege`

   `SeAssignPrimaryTokenPrivilege`

CertSvc is now configured to open the *Token Logon* window whenever access is required to the private key.

Uninstall

After SafeNet Authentication Client 10.2 has been installed, it can be uninstalled. Local administrator rights are required to uninstall SafeNet Authentication Client. When SafeNet Authentication Client is uninstalled, user configuration and policy files may be deleted.

In this chapter:

- Uninstall Overview
- Uninstalling via Add or Remove Programs
- Uninstalling via the Command Line

Uninstall Overview

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

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

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

- *Uninstalling via Add or Remove Programs* on page 55
- *Uninstalling via the Command Line* on page 56

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

Uninstalling via Add or Remove Programs

To uninstall via *Add or Remove Programs*:

1. From the Windows taskbar, select **Start > Settings > Control Panel.**
2. Double-click **Add or Remove Programs**.
3. Select **SafeNet Authentication Client 10.2**, and click **Remove**.
4. Follow the instructions to remove the application.

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

   The uninstall process proceeds.

Uninstalling via the Command Line

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

To uninstall via the command line:

1. Log on as an administrator.
2. Close all applications.
3. From the Windows taskbar, select **Start > Programs > Accessories > Command Prompt**.
   Right-click **Command Prompt**, and select **Run as Administrator**.
4. Type the appropriate command line utility:
   `msiexec /x SafeNetAuthenticationClient-x32-10.2.msi` (for 32-bit installations)
   `msiexec /x SafeNetAuthenticationClient-x32-10.2.msi` (for 64-bit installations)
   To uninstall in silent mode, add `/qn` to the end of the command.
5. When the uninstall completes, restart the computer.

SafeNet Authentication Client Settings

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

In this chapter:

- SafeNet Authentication Client Settings Overview
- Adding SafeNet Authentication Client Settings
- Editing SafeNet Authentication Client Settings
- Deploying SafeNet Authentication Client Settings

SafeNet Authentication Client Settings Overview

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

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

Sample Administrative Template files provided by SafeNet:

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

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

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

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

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

The values in this folder have a higher priority than values in any other registry folder. See "Application Properties Hierarchy" on page 66 for an explanation of the registry folders.

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

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

Adding SafeNet Authentication Client Settings

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

- To add the Administrative Templates to Windows Server 2008 SP1 or Windows Server 2008 R2 SP1, do one of the following:
  - Add a standard ADM Administrative Template file. See "Adding an ADM file to Windows Server 2008 / R2" on page 58.
  - Add an XML-based ADMX Administrative Template file. See "Adding an ADMX file to Windows Server 2008 / R2" on page 60.
- To add the Administrative Templates to a client computer, see *Adding an ADM file to a Client Computer* on page 61.

Configuring SAC Password Prompt Settings

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

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

- Ensure the certificate you are using includes a **Non Repudiation OID** (generated via Entrust). See "General Settings" on page 69 for more details on the Non Repudiation OIDs setting.
- Ensure the certificate you are using includes an **Identity OID**. See "IdenTrust Settings" on page 109 for more details on the Identity OIDs setting.
- Open **SAC tools>Advanced View>Token Settings>Advanced Tab**, and set the **RSA key secondary authentication** parameter to **Token authentication on application request**.
- **Logout Mode** setting is **True**.

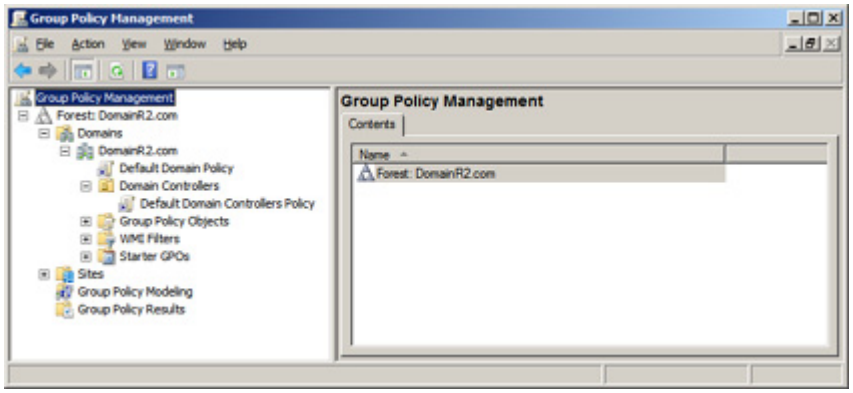
Adding an ADM file to Windows Server 2008 / R2

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

To add SafeNet Authentication Client settings:

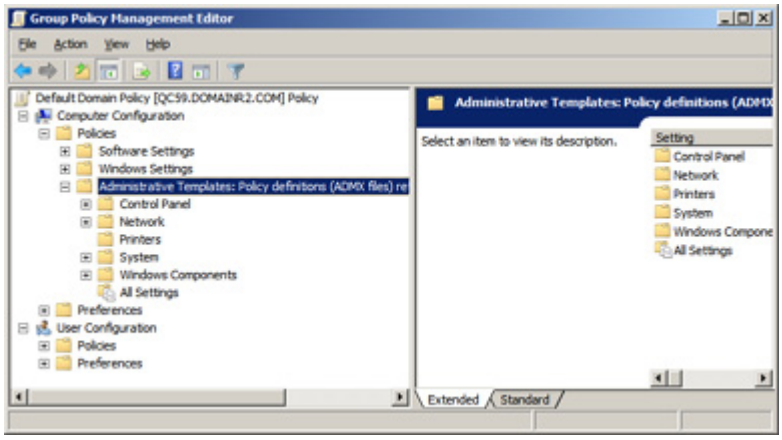
1. From the Windows taskbar, select **Start > Run**.
2. In the *Run* dialog box, enter **gpmc.msc**, and click **OK**.

The *Group Policy Management* window opens.



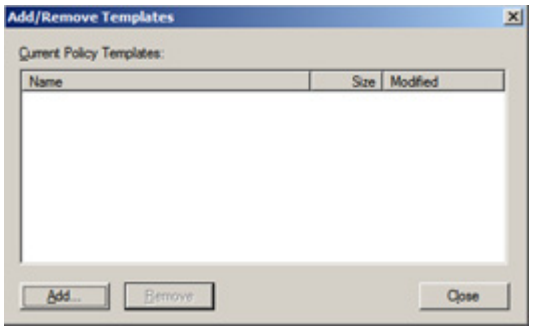
3. Do one of the following:
   - To propagate the settings to all clients in the domain, right-click **Default Domain Policy** under the domain node.
   - To apply the settings to the local machine and any other domain controllers in this domain, right-click **Default Domain Controllers Policy** under the domain node.
4. From the dropdown menu, select **Edit**.

   The *Group Policy Management Editor* opens.



5. Under **Computer Configuration > Policies**, right-click **Administrative Templates: Policy definitions (ADMX files)**, and select **Add/Remove Templates.**

   The *Add/Remove Templates* window opens.



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

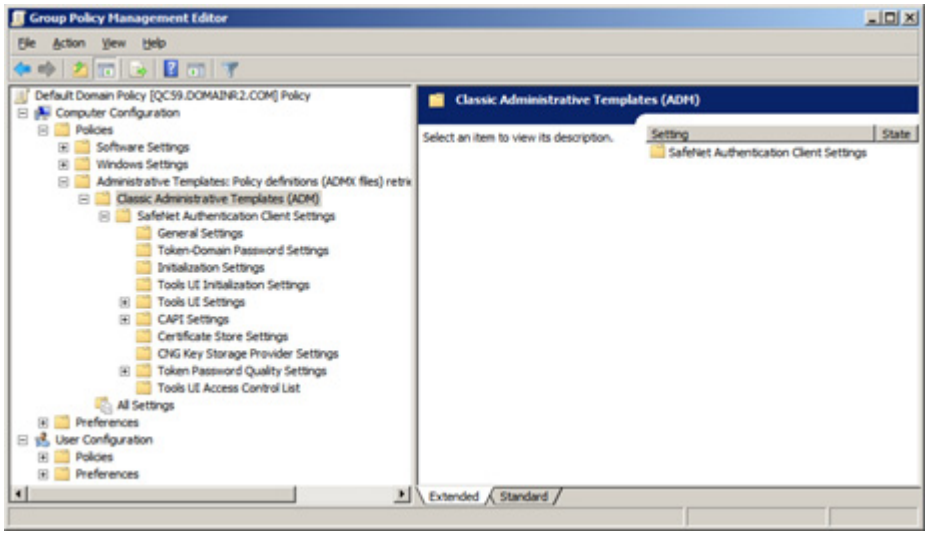
   Sample files are included in the SafeNet Authentication Client software package provided by SafeNet**.**

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

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

8. Click **Close.**

   In the *Group Policy Management Editor* window, the *Settings* node is added under **Administrative Templates: Policy definitions (ADMX files)**.



Adding an ADMX file to Windows Server 2008 / R2

When using an ADMX file, you can decide in which language to display the settings. The sample ADMX folder provided by SafeNet includes English language `adml` files.

To add SafeNet Authentication Client settings:

1. Copy the file `SAC_10_2.admx` that is included in the SafeNet Authentication Client software package provided by SafeNet to the following location:
   `C:\Windows\PolicyDefinitions`
2. Copy the appropriate `adml` language file (`SAC_10_2.adml`) to a language folder in the following location:
   `C:\Windows\PolicyDefinitions\`

> **NOTE**:
> The English language file provided by SafeNet should be written to:
> C:\Windows\PolicyDefinitions\en-US

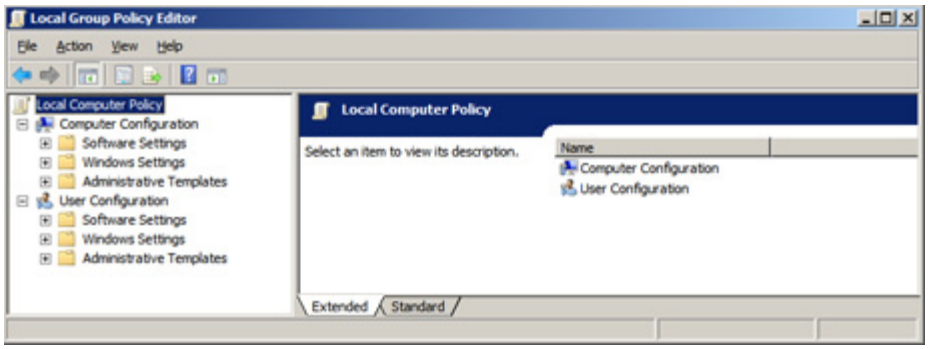
Adding an ADM file to a Client Computer

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

To add SafeNet Authentication Client settings:

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

   The *Local Group Policy Editor* opens.



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

   The *Add/Remove Templates* window opens.

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

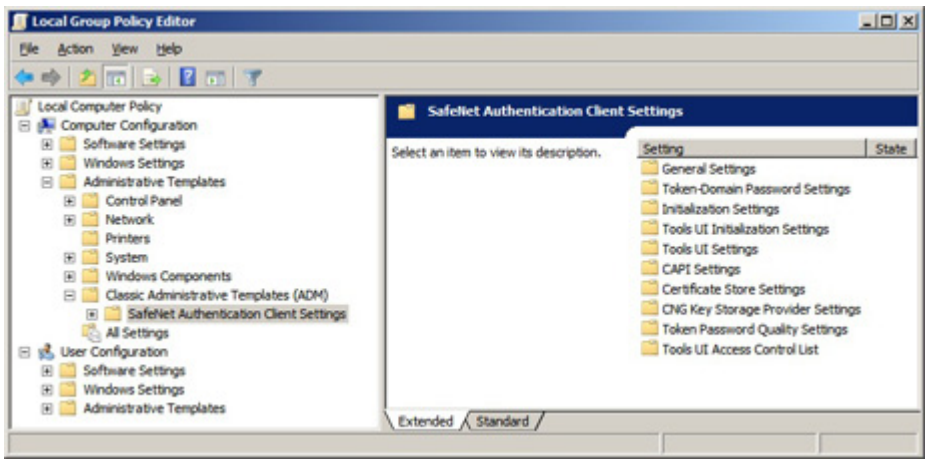
   Sample files are included in the SafeNet Authentication Client software package provided by SafeNet.

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

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

6. Click **Close.**

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



Editing SafeNet Authentication Client Settings

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

When you edit the settings, values in the registry key are changed. For more information, see *Configuration Properties* on page 65.

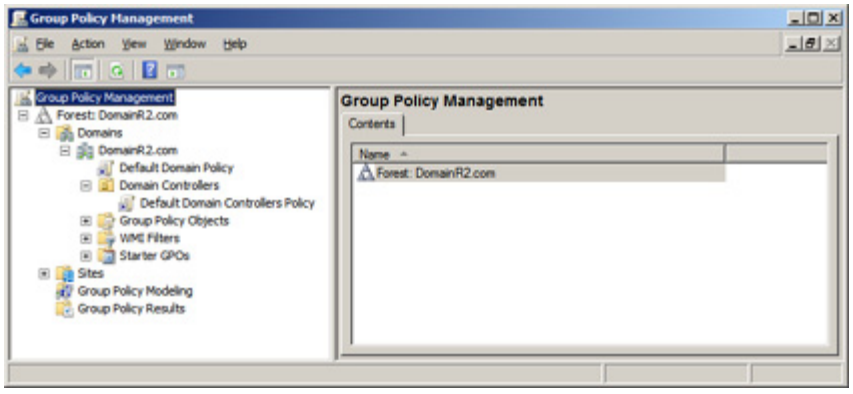
- To edit the policy settings on Windows Server 2008 or Windows Server 2008 R2, see *Editing Settings in Windows Server 2008 / R2* on page 62.
- To edit the policy settings on a client computer, see *Editing Settings on a Client Computer* on page 63.

Editing Settings in Windows Server 2008 / R2

To edit SafeNet Authentication Client settings:

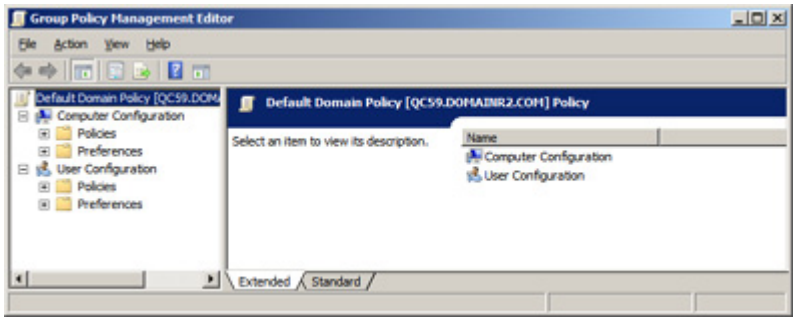
1. From the Windows taskbar, select **Start > Run**.
2. In the *Run* dialog box, enter **gpmc.msc**, and click **OK**.

   The *Group Policy Management* window opens.



3. Do one of the following:
   - To propagate the settings to all clients in the domain, right-click **Default Domain Policy** under the domain node.
   - To apply the settings to the local machine and any other domain controllers in this domain, right-click **Default Domain Controllers Policy** under the domain node.
4. From the dropdown menu, select **Edit**.

   The *Group Policy Management Editor* opens.



5. In the left pane, expand **Computer Configuration > Policies > Administrative Templates: Policy definitions (ADMX files)**.
6. Select one of the **SafeNet Authentication Client Settings** nodes.

   The settings are displayed in the right pane.
7. Select the settings folder to edit.

   The settings are displayed in the right pane.
8. Double-click the setting to edit.
9. Select the Explain tab for an explanation of the setting and its values.
10. In the Setting tab, select one of the following:
    - **Not Configured**

      No change is made to the registry for this setting
    - **Enabled**

      The registry is changed to indicate that the policy applies to users or computers that are subject to this GPO.
    - **Disabled**

      The registry is changed to indicate that the policy does not apply to users or computers that are subject to this GPO.
11. If **Enabled** is selected, complete the values in the box.
12. Click **Previous Setting** or **Next Setting** to progress through the settings in the same folder, or click **OK** to return to the list of settings.

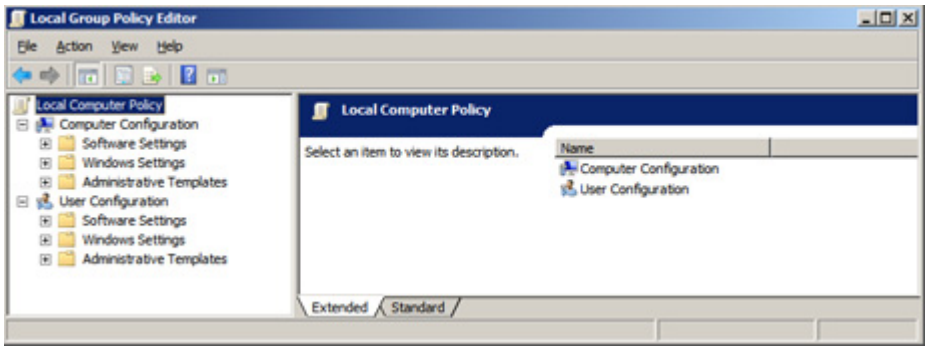
    The registry is updated.

Editing Settings on a Client Computer

To edit SafeNet Authentication Client settings:

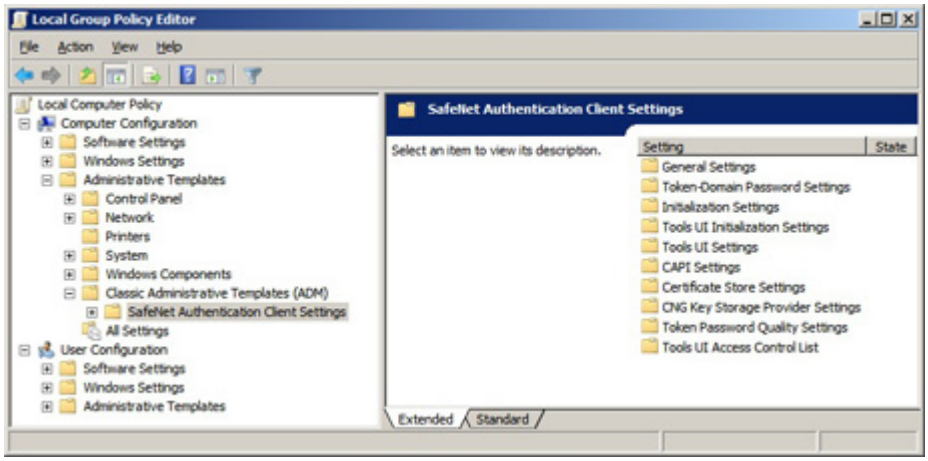
1. From the Windows taskbar, select **Start > Run**.
2. In the *Run* dialog box, enter **gpedit.msc**, and click **OK**.

   The *Local Group Policy Editor* opens.



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

The settings are displayed in the right pane.



5. Continue from *Editing Settings in Windows Server 2008 / R2* - Step 8 above.

Deploying SafeNet Authentication Client Settings

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

To apply SafeNet Authentication Client settings:

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

Configuration Properties

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

In this chapter:

- Setting SafeNet Authentication Client Properties
- Application Properties Hierarchy
- Setting Registry Keys Manually
- Defining a Per Process Property
- General Settings
- Token-Domain Password Settings
- License Settings
- Initialization Settings
- SafeNet Authentication Client Tools UI Initialization Settings
- SafeNet Authentication Client Tools UI Settings
- CAPI Settings
- Certificate Store Settings
- CNG Key Storage Provider Settings
- Token Password Quality Settings
- SafeNet Authentication Client Tools UI Access Control List
- Security Settings
- SafeNet Authentication Client Security Enhancements
- Log Settings
- IdenTrust Settings

Setting SafeNet Authentication Client Properties

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

- Define the property during command line installation of SafeNet Authentication Client (but not during repair). See "Installing the MSI file via the Command Line" on page 44.
  The property name, and not the registry value name, is needed when setting the value during command line installation.
- Set a value using the SafeNet Authentication Client Tools application.
  See the *SafeNet Authentication Client User's Guide*.
  Neither the registry value name nor the property name is needed.

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

- Set a value using the Administrator Templates (ADM/ADMX) policy settings.
  See Chapter 7: *SafeNet Authentication Client Settings*, on page 57.
  The registry value name, and not the property name, is needed when setting the value.
- Manually edit the registry setting.
  See *Setting Registry Keys Manually* on page 67.
  The registry value name, and not the property name, is needed when setting the value.

NOTE:
All properties can be manually set and edited.

Application Properties Hierarchy

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

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

Hierarchy List

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

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

Hierarchy Implications

The applications properties hierarchy has the following implications:

- When you use the sample Administrative Template (ADM/ADMX) files supplied by SafeNet to edit *SafeNet Authentication Client Settings*, the edited properties are written to: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SafeNet\Authentication\SAC`.

  These values override values set by any other method.

- When you set properties using *SafeNet Authentication Client Tools*, the edited properties are written to: `HKEY_CURRENT_USER\SOFTWARE\SafeNet\Authentication\SAC`.

  These values override values set during command line installation. Since Tools settings apply "per user" only after the user is authenticated, the user must first log on to Windows before these settings take effect.

- When you set properties during command line installation, the properties (except for `PROP_REG_FILE`) are written to: `HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC`.

- When you set properties manually, write them to their appropriate registry keys in any of the registry folders listed in the *Hierarchy List* on page 66. Unless the properties must override other settings, we recommend writing them to: `HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC`.

Setting Registry Keys Manually

To set a registry key value:

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

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

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

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

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

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

Defining a Per Process Property

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

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

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

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

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

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

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

   The *Registry Editor* opens, displaying the registry folders tree in the left pane.
3. Expand the appropriate registry tree.
   In this example, the tree is
   `HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC\CAPI\[Process Name e.g. AcroRd32.exe]`

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

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

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

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

General Settings

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

Description	ADM File Setting	Registry Value	Command Line
Single Logon Determines if the user's Token Password is requested only once for applications using MS cryptography. **Note:** • Does not apply to applications that do not use MS cryptography. • Can be set in SafeNet Authentication Client Tools, but since Tools settings apply "per user" only after the user is authenticated, the user must first log on to Windows, and only the next Token Password entry will be saved. • To force Single Logon to start from Windows Logon, define this setting in HKEY_LOCAL_MACHINE • This property is not relevant to IDPrime MD cards.	**Setting name:** Single Logon **Selected** - Token Password is requested only once **Not Selected**- Token Password is requested as needed **Default:** Not selected **Values**: Single Logon Timeout >= 0 (0 = no timeout) **Default**: 0	Registry Value Name: SingleLogon Values: **1 (True)** - Token Password is requested only once **0 (False)** - Token Password is requested as needed **Default:** 0 (False)	Property name: PROP_SINGLELOGON
Single Logon Timeout Determines the timeout, in seconds, of a single logon. **Note:** • Applies only when Single Logon is **True**. • Applies to all connected tokens and affects all applications using these tokens. • This property is not relevant to IDPrime MD cards.	Single Logon Timeout is set in the Single Logon setting. (See "Single Logon" entry above.)	**Registry Value Name:** SingleLogonTimeout **Value**: >=0 (Seconds) **Default**: 0 (no timeout)	Property name: PROP_SINGLELOGONTO

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Software Slots Defines the number of virtual readers for SafeNet Virtual Tokens. **Note:** Can be modified in 'Reader Settings' in SafeNet Authentication Client Tools also. On Windows Vista 64-bit and on systems later than Windows 7 and Window 2008 R2, the total number of readers is limited to 10 from among: iKey readers, eToken readers, third-party readers, and reader emulations.	**Setting name:** Software Slots **Values**: >=0 (0 = SafeNet Virtual Token is disabled; only physical tokens are enabled) **Default**: 2	**Registry Value Name:** SoftwareSlots **Values**: >=0 (0 = SafeNet Virtual Token is disabled; only physical tokens are enabled) **Default**: 2	Property name: PROP_SOFTWARESLOTS
PCSC Slots Defines the total number of PC/SC slots for all USB tokens and smartcards. Included in this total: • the number of allocated readers for third-party providers • the number of allocated iKey readers, which is defined during installation and cannot be changed • the number of allocated readers for other SafeNet physical tokens, which can be modified in 'Reader Settings' in SafeNet Authentication Client Tools **Note:** On Windows Vista 64-bit and on systems later than Windows 7 and Window 2008 R2, the total number of readers, consisting of this value and any enabled reader emulations, is limited to 10.	**Setting name:** PCSC Slots **Values**: >=0 (0 = Physical tokens are disabled; only SafeNet Virtual Tokens are enabled) **Default**: 8	**Registry Value Name:** PcscSlots **Values**: >=0 (0 = Physical tokens are disabled; only SafeNet Virtual Token is enabled) **Default**: 8	Property name: PROP_PCSCSLOTS
HID Slots Defines the total number of HID slots for all HID USB tokens.	**Setting name:** HID Slots **Values:**=0, =4, >=0 0 - 5200 token works in VSR mode. 4 = 5200 HID token works in HID mode (4 slots). **Default**: 4	**Registry Value Name:** HIDSlots **Values**: =0, =4, >=0 **Default**: 4 slots	Property name: PROP_HIDSLOTS

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Legacy Manufacturer Name Determines if 'Aladdin Knowledge Systems Ltd.' is written as the manufacturer name in token and token slot descriptions Use for legacy compatibility only	**Setting name:** Legacy Manufacturer Name Values: **Selected** - The legacy manufacturer name is written **Not selected** - The new manufacturer name is written **Default**: Not selected	**Registry Value Name:** LegacyManufacturerName Values: **1** - The legacy manufacturer name is written **0** - The new manufacturer name is written **Default**: 0	Cannot be set by command line installation.
Enable Private Cache Determines if SafeNet Authentication Client allows the token's private data to be cached. Applies only to tokens that were initialized with the private data cache setting. The private data is cached in per process memory. **Note:** Can be set in SafeNet Authentication Client Tools	**Setting name:** Enable Private Cache Values: **Selected** - Private data caching is enabled **Not selected** - Private data caching is disabled **Default**: Selected	**Registry Value Name:** EnablePrvCache **Values**: **1 (True)** - Private data caching is enabled **0 (False)** - Private data caching is disabled **Default**:1 (True)	Cannot be set by command line installation.
Tolerate Finalize Determines if C_Finalize can be called by DllMain **Note:** Define this property per process Select this setting when using Novell Modular Authentication Service (NMAS) applications only	**Setting name:** Tolerate Finalize Values: **Selected** - C_Finalize can be called by DllMain **Not selected** - C_Finalize cannot be called by DllMain **Default**: Not selected	**Registry Value Name:** TolerantFinalize **Values**: **1 (True)** - C_Finalize can be called by DllMain **0 (False)** - C_Finalize cannot be called by DllMain **Default**: 0 (False)	Cannot be set by command line installation
Tolerate X509 Attributes Determines if CKA_SERIAL_NUMBER, CKA_SUBJECT, and CKA_ISSUER attributes can differ from those in CKA_VALUE during certificate creation **Note:** Enable TolerantX509Attributes when using certificates created in a non- DER encoded binary x.509 format. In some versions of PKI Client, this setting was not selected by default.	**Setting name:** Tolerate X509 Attributes Values: **Selected** - The attributes can differ **Not selected**- Check that the values match **Default**: Not selected	**Registry Value Name:** TolerantX509Attributes **Values**: **1 (True)** - The attributes can differ **0 (False**) - Check that the values match **Default**: 0 (False)	Cannot be set by command line installation

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

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
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**: Empty **Default**: No override	**Registry Value Name:** NonRepudiationOID **Value**: Empty **Default**: No override	Cannot be set by command line installation.
Ignore Silent Mode Determines if the *Token Logon* window is displayed even when the application calls the CSP/KSP in silent mode.	This feature cannot be set in the GPO Editor or MMC	**Registry Value Name:** IgnoreSilentMode **Values**: **1 (True)** - Display the *Token Logon* window even in silent mode **0 (False)** - Respect silent mode **Note:** Set to True when the SafeNet RSA KSP must use SHA-2 to enroll a CA private key to a token **Default**: 0 (False)	Cannot be set by command line installation.

Token-Domain Password Settings

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

Description	ADM File Setting	Registry Value	Command Line
Synchronize with Domain Password Determines if synchronization is enabled between the eToken password and the domain password.	**Setting name:** Synchronize with Domain Password **Values**: Name of the domain (written without a suffix) whose password is synchronized with the Token Password **None** - Password synchronization is not enabled **Default**: None	**Registry Value Name:** Domain **Values**: Name of the domain (written without a suffix) whose password is synchronized with the Token Password **None** - Password synchronization is not enabled **Default**: None	Cannot be set by command line installation.

License Settings

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

Description	ADM File Setting	Registry Value	Command Line
SAC License String Defines the license string issued by SafeNet for product registration	**Setting name:** SAC License String **Values**: License string provided by SafeNet **Default**: None	**Registry Value Name:** License **Values**: License string provided by SafeNet **Default**: None	Name of related property: PROP_LICENSE_FILE contains the path to the license string, but not the string itself. See "PROP_LICENSE_FILE" on page 48.

Initialization Settings

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

NOTE:
All setting in this section are not relevant to IDPrime MD cards, except for the LinkMode setting.

Description	ADM File Setting	Registry Value	Command Line
Maximum Token Password Retries Defines the default number of consecutive failed logon attempts that lock the token.	Setting Name: Maximum Token Password Retries **Values**: 1-15 **Default**: 15	**Registry Value Name:** UserMaxRetry **Values**: 1-15 **Default**: 15	Cannot be set by command line installation.
Maximum Administrator Password Retries Defines the default number of consecutive failed administrator logon attempts that lock the token.	**Setting name:** Maximum Administrator Password Retries **Values**: 1-15 **Default**: 15	**Registry Value Name:** AdminMaxRetry **Values**: 1-15 **Default**: 15	Cannot be set by command line installation.
Legacy Format Version Defines the default token format.	Setting Name: Legacy Format Version **Values**: **0 -** Tokens are formatted as backwardly compatible to eToken PKI Client 3.65 (CardOS tokens only) **4** - Tokens are not formatted as backwardly compatible, and password quality settings can be saved on the token (CardOS tokens only) **5** - Format includes new RSA behavior that is not controlled by key size; each key is created in a separate directory (CardOS 4.20B FIPS or Java Card-based tokens only) **Default**: 4, for CardOS tokens 5, for 4.20B FIPS and Java Card -based tokens	**Registry Value Name:** Legacy-Format-Version **Values**: **0 -** Tokens are formatted as backwardly compatible to eToken PKI Client 3.65 (CardOS tokens only) **4** - Tokens are not formatted as backwardly compatible, and password quality settings can be saved on the token (CardOS tokens only) **5** - Format includes new RSA behavior that is not controlled by key size; each key is created in a separate directory (CardOS 4.20B FIPS or Java Card-based tokens only) **Default**: 4, for CardOS tokens 5, for 4.20B FIPS and Java Card -based tokens	Cannot be set by command line installation

Description	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
RSA-2048 Determines if the token support 2048-bit RSA keys by default. **Note:** Can be set in SafeNet Authentication Client Tools.	**Setting Name:** RSA-2048 Values: **Selected** - 2048-bit RSA keys are supported **Not selected** - 2048-bit RSA keys are not supported **Default:** Not selected	**Registry Value Name:** RSA-2048 **Values**: **1(True)** - 2048-bit RSA keys are supported **0 (False)** - 2048-bit RSA keys are not supported **Default:** 0 (False)	Cannot be set by command line installation
OTP Support Determines if the token supports OTP generation by default. This setting enables HMAC-SHA1 support, required by OTP tokens. **Note:** Can be set in SafeNet Authentication Client Tools.	**Setting Name:** OTP Support Values: **Selected** - OTP generation is supported **Not selected** - OTP generation is not supported **Default**: Selected, for OTP tokens. Not selected, for other tokens	**Registry Value Name:** HMAC-SHA1 Values: **1 (True)** - OTP generation is supported **0 (False)** - OTP generation is not supported **Default**: 1 (True), for OTP tokens. 0 (False), for other tokens	Cannot be set by command line installation
RSA Area Size For CardOS-based tokens, defines the default size, in bytes, of the area to reserve for RSA keys. • The size of the area allocated on the token is determined during token initialization, and cannot be modified without initializing the token. • RSA-Area-Size is not relevant when Legacy-Format-Version is set to 5. **Note:** Can be set in SafeNet Authentication Client Tools.	**Setting Name:** RSA Area Size Values: >=0 (0 =RSA keys cannot be created on a token) **Default:** depends on the token size: • For 16 K tokens, enough bytes for three 1024-bit keys • For 32 K tokens, enough bytes for five 1024-bit keys • For larger tokens, enough bytes for seven 1024-bit keys	**Registry Value Name:** RSA-Area-Size **Default:** depends on the token size: • For 16 K tokens, enough bytes for three 1024-bit keys • For 32 K tokens, enough bytes for five 1024-bit keys • For larger tokens, enough bytes for seven 1024-bit keys	Cannot be set by command line installation.
Default Token Name Defines the default Token Name written to tokens during initialization.	**Setting Name**: Default Token Name **Value**: String **Default**: My Token	Registry Value Name: DefaultLabel **Value**: String **Default**: My Token	Cannot be set by command line installation.

Description	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
API: Keep Token Settings When initializing the token using the SDK, determines if the token is automatically re-initialized with its current settings. **Note:** If selected, this setting overrides all other initialization settings.	Setting Name: API: Keep Token Settings Values: **Selected** - Use current token settings **Not selected** - Override current token settings **Default:** Not selected	Registry Value Name: KeepTokenInit Values: **1 (True) -** Use current token settings **0 (False) -** Override current token settings **Default**: 0 (False)	Cannot be set by command line installation.
Automatic Certification When initializing the token using the SDK. If the token has FIPS or Common Criteria certification, the token is automatically initialized with the original certification.	Setting Name: Automatic Certification Values: **Selected** - initialize the token with the original certification **Not selected** - initialize the token without the certification **Default:** initialize the token without the certification.	Registry Value Name: Certification **Values**: **1(True)** - initialize the token with the original certification. **0 (False)** - initialize the token without the certification **Default:** 1 (True) **Note:** Previous to SAC 8.2, the default setting was 0 (False). As CardOS 4.2 does not support both FIPS and RSA-2048, failure to take this into account this may lead to token initialization failure when using PKCS#11. To prevent this, ensure that the default is set to False, or else ensure that the application provides both the required FIPS and RSA-2048 settings.	Cannot be set by command line installation.

Description	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
API: Private Data Caching If using an independent API for initialization, and if 'Enable Private Cache' is selected, determines the token's private data cache default behavior.	Setting Name: API: Private Data Caching Values: **0 -** Always (fastest); private data is cached when used by an application while the user is logged on to the token, and erased when the token is disconnected. **1 -** While user is logged on; private data is cached when used by an application while the user is logged on to the token, and erased when the user logs off or the token is disconnected. **2 -** Never; private data is not cached. **Default:** 0 (Always)	Registry Value Name: PrvCachingMode Values: **0 -** Always 1 - While user is logged on **2 -** Never **Default:** 0 (Always)	Cannot be set by command line installation.
Enable Private Data Caching Modification Determines if the token's Private Data Caching mode can be modified after initialization.	Setting Name: Enable Private Data Caching Modification Values: **Selected** -Can be modified **Not selected** -Cannot be modified **Default:** Not selected	Registry Value Name: PrvCachingModify Values: **1 (True) -** Can be modified **0 (False) -** Cannot be modified **Default**: 0 (False)	Cannot be set by command line installation.
Private Data Caching Mode If 'Enable Private Data Caching Modification' is selected, determines who has rights to modify the token's Private Data Caching mode.	Setting Name: Private Data Caching Mode Values: **Admin** -Only the administrator has rights **User** -Only the user has rights **Default:** Admin	Registry Value Name: PrvCachingOwner Values: **0** - Admin **1** - User **Default**: 0 (Admin)	Cannot be set by command line installation.

Description	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
API: RSA Secondary Authentication Mode If using an independent API for initialization, determines the default behavior for protecting RSA private keys on the token.	Setting Name: API: RSA Secondary Authentication Mode Values: **Never** -New RSA private keys are not protected with an additional password. **Prompt on application request -**If the key generation application requires key passwords to be created for strong private key protection, new RSA private keys must be protected with an additional password. If the key generation application does not require strong private key protection, new RSA private keys are not protected with an additional password.	Registry Value Name: 2ndAuthMode Values: **0** - Never **1** - Prompt on application request **2 -** Always prompt user 3- Always 4 - Token authentication on application request **Default**: **0** -(Never)	Cannot be set by command line installation.
	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		
Enable RSA Secondary Authentication Modified Determines if the token's RSA secondary authentication can be modified after initialization.	Setting Name: Enable RSA Secondary Authentication Modified Values: **Selected** -Can be modified **Not selected** -Cannot be modified **Default:** Not selected	Registry Value Name: 2ndAuthModify Values: **1 (True) -** Can modify **0 (False) -** Cannot modify **Default**: 0 (False)	Cannot be set by command line installation.

Description	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
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)	Cannot be set by command line installation.

SafeNet Authentication Client Tools UI Initialization Settings

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

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

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

Description	ADM File Setting	Registry Value	Command Line
Default Token Password Defines the default Token Password	**Setting Name:** Default Token Password **Value**: String **Default**: 1234567890	**Registry Value Name:** DefaultUserPassword **Values**: String **Default**: 1234567890	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Enable Change Password on First Logon Determines if the "Token Password must be changed on first logon" option can be changed by the user in the Token Initialization window. **Note:** This option is selected by default. If the option is de-selected, it can be selected again only by setting the registry key.	**Setting Name:** Enable Change Password on First Logon **Values**: **Selected** - Enabled **Not selected** -Disabled **Default**: Selected	**Registry Value Name:** MustChangePasswordEnabled **Values**: **1** - Selected **0** - Not selected **Default**: 1	Cannot be set by command line installation.
Change Password on First Logon Determines if the *Token Password must be changed on first logon* option is selected by default in the Token Initialization window. **Note:** This option is not supported by iKey.	**Setting Name:** Change Password on First Logon **Values**: Selected Not selected **Default**: Selected	**Registry Value Name:** MustChangePassword **Value**: **1** - Selected **0** - Not selected **Default**: 1	Cannot be set by command line installation.
Private Data Caching If *Enable Private Cache* is selected, determines the token's private data cache default behavior. **Note:** Can be set in SafeNet Authentication Client Tools. This option is not supported by IDPrime MD cards.	**Setting Name:** Private Data Caching **Values**: **Always -** (fastest) private data is cached when used by an application while the user is logged on to the token, and erased only when the token is disconnected **While user is logged on -** private data is cached when used by an application while the user is logged on to the token, and erased when the user logs off or the token is disconnected **Never** - private data is not cached **Default**: Always	**Registry Value Name:** PrivateDataCaching **Values**: **0 -** (fastest) private data is cached when used by an application while the user is logged on to the token, and erased only when the token is disconnected **1 -** private data is cached when used by an application while the user is logged on to the token, and erased when the user logs off or the token is disconnected **2** - private data is not cached **Default**: 0	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command 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 MD cards.	**Setting Name:** RSA Secondary Authentication Mode Values: **Never** - New RSA private keys are not protected with an additional password. **Prompt user on application request** - If the key generation application requires key passwords to be created for strong private key protection, new RSA private keys must be protected with an additional password. If the key generation application does not require strong private key protection, new RSA private keys are not protected with an additional password. **Always prompt user** - A prompt appears asking if a new RSA private key is to be protected with an additional password. **Always** - New RSA private keys must be protected with an additional password.	**Registry Value Name:** RSASecondaryAuthentication Mode Values: **0** - Never **1** - Prompt user on application request **2** - Always prompt user **3** - Always **4** - Token authentication on application request **Default**: **0**	Cannot be set by command line installation
RSA Secondary Authentication Mode (continued). **Note:** This option is not supported by IDPrime MD cards.	**Token authentication on application request** - If the key generation application requires key passwords to be created for strong private key protection, new RSA private keys are protected with the Token Password. If the key generation application does not require strong private key protection, new RSA private keys are not protected with any password. **Default**: Never		
Reuse Current Token Name Determines if the token's current Token Name is displayed as the default Token Name when the token is re initialized.	**Setting Name:** Reuse Current Token Name **Values**: **Selected** -The current Token Name is displayed **Not selected** -The current Token Name is ignored **Default**: Not Selected	**Registry Value Name:** ReadLabelFromToken **Values**: **1** -The current Token Name is displayed **0** -The current Token Name is ignored **Default**: 1	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Maximum number of 1024-bit RSA keys Defines the amount of space to reserve on the token for Common Criteria certificates that use 1024 -bit RSA keys. **Note:** This option is not supported by IDPrime MD cards.	**Setting Name:** Maximum number of 1024-bit RSA keys **Values**: 0-16 certificates **Default**: 0	**Registry Value Name:** NumOfCertificatesWith1024Keys_help **Values**: 0-16 certificates **Default**: 0	Cannot be set by command line installation.
Maximum number of 2048-bit RSA keys Defines the amount of space to reserve on the token for Common Criteria certificates that use 2048-bit RSA keys. **Note:** This option is not supported by IDPrime MD cards.	**Setting Name:** Maximum number of 2048-bit RSA keys **Values**: 1-16 certificates (For example, 1 = One 2048 -bit RSA key certificate can be written) **Default**: 4	**Registry Value Name:** NumOfCertificatesWith2048Keys_help **Values**: 1-16 certificates **Default**: 4	Cannot be set by command line installation.
Default Common Criteria Import PIN Defines the default Common Criteria Import PIN. **Note:** This option is not supported by IDPrime MD cards.	This feature cannot be set in the GPO Editor or MMC	**Registry Value Name:** DefaultCommonCriteriaImportPIN **Values**: String **Default**: 1234567890	

SafeNet Authentication Client Tools UI Settings

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

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

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

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Enable Certificate Expiration Warning Determines if a warning message is displayed when certificates on the token are about to expire.	**Setting Name:** Enable Certificate Expiration Warning **Values**: **Selected** - A message is displayed **Not selected** - A message is not displayed **Default**: Not Selected	**Registry Value Name:** CertificateExpiryAlert **Values**: **1 (True)** - Notify the user **0 (False**) - Do not notify the user **Default**: 1 (True)	Cannot be set by command line installation.
Ignore Expired Certificates Determines if expired certificates are ignored, and no warning message is displayed for expired certificates	**Setting Name:** Ignore Expired Certificates **Values**: **Selected** -Expired certificates are ignored **Not selected**- A warning message is displayed if the token contains expired certificates **Default**: Not selected	**Registry Value Name:** IgnoreExpiredCertificates Values: **1** - Expired certificates are ignored **0** - A warning message is displayed if the token contains expired certificates **Default**: 0	Cannot be set by command line installation.
Certificate Expiration Verification Frequency Defines the minimum interval, in days, between certificate expiration date verifications	**Setting Name:** Certificate Expiration Verification Frequency **Values**: > 0 **Default**: 14 days	**Registry Value Name:** UpdateAlertMinInterval **Values**: > 0 **Default**: 14 days	Cannot be set by command line installation.
Certificate Expiration Warning Period Defines the number of days before a certificate's expiration date during which a warning message is displayed.	**Setting Name:** Certificate Expiration Warning Period **Values**: > =0 (0 = No warning) **Default**: 30 days	**Registry Value Name:** ExpiryAlertPeriodStart **Values**: > =0 (0 = No warning) **Default**: 30 days	Cannot be set by command line installation.
Warning Message Title Defines the title to display in certificate expiration warning messages	**Setting Name:** Warning Message Title **Values**: String **Default**: SafeNet Authentication Client	**Registry Value Name:** AlertTitle **Values**: String **Default**: SafeNet Authentication Client	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command 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.	Cannot be set by command line installation.
Certificate Expired Warning Message Defines the warning message to display in a balloon if a certificate's expiration date has passed.	**Setting Name:** Certificate Expired Warning Message **Values**: String **Default**: Update your token now.	**Registry Value Name:** PastAlertMessage **Values**: String **Default**: Update your token now.	Cannot be set by command line installation.
Warning Message Click Action Defines what happens when the user clicks the message balloon.	**Setting Name:** Warning Message Click Action **Values**: • No action • Show detailed message • Open website **Default**: No action	**Registry Value Name:** AlertMessageClickAction **Values**: **0 -** No action **1 -** Show detailed message **2 -** Open website **Default**: 0	Cannot be set by command line installation.
Detailed Message If "Show detailed message" is selected in "Warning Message Click Action" setting, defines the detailed message to display.	**Setting Name:** Detailed Message **Values**: String No default	**Registry Value Name:** ActionDetailedMessage **Values**: String No default	Cannot be set by command line installation.
Website URL If "Open website" is selected in the "Warning Message Click Action" setting, defines the URL to display	**Setting Name:** Website URL **Values**: Website address **No default**	**Registry Value Name:** ActionWebSiteURL **Values** (string): Website address **No default**	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Enable Password Expiration Notification Determines if a pop-up message is displayed in the system when the Token Password is about to expire.	**Setting Name:** Enable Password Expiration Notification **Values**: **Selected** - A message is displayed **Not selected** - A message is not displayed **Default**: Selected	**Registry Value Name:** NotifyPasswordExpiration **Values**: **1 (True)**- A message is displayed **0 (False)** - A message is not displayed **Default**: 1 (True)	Cannot be set by command line installation.
Display Virtual Keyboard Determines if SafeNet's keystroke-secure Virtual Keyboard replaces standard keyboard entry of password fields in the following windows: • Token Logon • Change Password **Note:** The virtual keyboard supports English characters only.	**Setting Name:** Display Virtual Keyboard **Values**: **Selected** - Enabled **Not selected** -Disabled **Default**: Disabled	**Registry Value Name:** VirtualKeyboardOn **Values**: **1 (True)**- Virtual keyboard on **0 (False)** - Virtual keyboard off **Default**: 0 (False)	Cannot be set by command line installation.
Password Policy Instructions If not empty, defines a string that replaces the default password policy description displayed in the *Unlock* and *Change Password* windows.	**Setting Name:** Modify Password Policy Description **Values**: If key does not exist, the default value is used: "A secure %REPLACE_PASSWORD_TERM% has at least 8 characters, and contains upper-case letters, lower-case letters, numerals, and special characters (such as !, $, #, %)." If key exists, the value in the key is displayed.	**Registry Value Name:** PasswordPolicyInstructions **Values**: String	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command 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	Cannot be set by command line installation.
Import Certificate Chain Determines if the certificate chain is imported to the token	**Setting Name:** Import Certificate Chain **Values**: • Do not import • Import • User selects import behavior **Default**: Do not import	**Registry Value Name:** ImportCertChain **Values**: **0 -** Do not import certificate chain **1** - Import certificate chain **2**- User selects import behavior **Default**: 0	Cannot be set by command line installation.

CAPI Settings

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

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

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

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

Internet Explorer Settings

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

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

Certificate Store Settings

Microsoft Certificate Propagation Service

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

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

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

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

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

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

CNG Key Storage Provider Settings

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

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

Description	Settings in GPO Editor or MMC	Registry Key	Command Line
Cryptographic Provider Determines which cryptographic provider to use for certificate propagation. **Note:** Can be set in SafeNet Authentication Client Tools. **Note:** After changing the cryptographic provider setting, reconnect the token to ensure that the properties are updated to the token. **Note:** This setting is not relevant to IDPrime MD cards.	**Setting Name:** Cryptographic Provider **Values**: 0 = CSP 1 = KSP (if supported by the OS) 2 = The Provider that enrolled the certificate (This information is stored on the token) **Default**: 2	**Registry Value Name:** KspPropagationMode **Values**: 0 = CSP 1 = KSP (if supported by the OS) 2 = The Provider that enrolled the certificate (This information is stored on the token) **Default**: 2	KSP_ENABLED Enables you to prevent KSP from being installed. See "KSP_ENABLED" on page 47.

Token Password Quality Settings

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

NOTE:
These settings are not relevant to IDPrime MD cards, as the password quality settings reside on the card itself.

Description	Settings in GPO Editor or MMC	Registry Key	Command Line
Password - Minimum Length Defines the minimum password length. **Note:** Can be set in SafeNet Authentication Client Tools.	**Setting Name:** Password -Minimum Length **Values**: >=4 **Default**: 6	**Registry Key Name:** pqMinLen **Values**: >=4 **Default**: 6	PROP_PQ_MINLEN
Password - Maximum Length Defines the maximum password length. **Note:** Can be set in SafeNet Authentication Client Tools.	**Setting Name:** Password -Maximum Length **Values**: Cannot be less than the Password Minimum Length **Default**: 16	**Registry Key Name:** pqMaxLen **Values**: Cannot be less than the Password Minimum Length **Default**: 16	Cannot be set by command line installation.
Password - Maximum Usage Period Defines the maximum number of days a password is valid. **Note:** Can be set in SafeNet Authentication Client Tools. **Note:** This parameter is 'Day Sensitive' i.e. the system counts the day's and not the hour in which the user made the change.	**Setting Name:** Password - Maximum Usage Period **Values**: >=0 (0 =No expiration) **Default**: 0	**Registry Key Name:** pqMaxAge **Values**: >=0 (0 =No expiration) **Default**: 0	PROP_PQ_MAXAGE
Password - Minimum Usage Period Defines the minimum number of days between password changes. **Note:** Can be set in SafeNet Authentication Client Tools. **Note:** Does not apply to iKey devices.	**Setting Name:** Password - Minimum Usage Period **Values**: >=0 (0 = No minimum) **Default**: 0	**Registry Key Name:** pqMinAge **Values**: >=0 (0 = No minimum) **Default**: 0	PROP_PQ_MINAGE

Description (Cont.)	Settings in GPO Editor or MMC (Cont.)	Registry Key (Cont.)	Command Line (Cont.)
Password - Expiration Warning Period Defines the number of days before expiration during which a warning is displayed. **Note:** Can be set in SafeNet Authentication Client Tools.	**Setting Name:** Password - Expiration Warning Period **Values**: >=0 (0 = No warning) **Default**: 0	**Registry Key Name:** pqWarnPeriod **Values**: >=0 (0 = No warning) **Default**: 0	PROP_PQ_WARNPERIOD
Password - History Size Defines the number of recent passwords that must not be repeated. **Note:** Can be set in SafeNet Authentication Client Tools.	**Setting Name:** Password - History Size **Values**: >= 0 (0 = No minimum) **Default**: 10	**Registry Key Name:** pqHistorySize **Values**: >= 0 (0 = No minimum) **Default**: 10 (iKey device history is limited to 6)	PROP_PQ_HISTORYSIZE
Password - Maximum Consecutive Repetitions Defines the maximum number of consecutive times a character can be used in a password. **Note:** Can be set in SafeNet Authentication Client Tools. **Note:** Does not apply to iKey devices.	**Setting Name:** Password - Maximum Consecutive Repetitions **Values**: 0 - 16 (0 = No maximum) **Default**: 3	**Registry Key Name:** pqMaxRepeated **Values**: 0 - 16 (0 = No maximum) **Default**: 3	Cannot be set by command line installation.
Password - Complexity Determines if there is a minimum number of character types that must be included in a new Token Password The character types are: upper-case letters, lower-case letters, numerals, and special characters. **Note:** Can be set in SafeNet Authentication Client Tools.	**Setting Name:** Password - Complexity **Values**: **Standard complexity** - A minimum of 2 or 3 types must be included, as defined in the *Password- Minimum Mixed Character Type*s setting **Manual complexity** - The rule for each character type is defined in the character type's *Include* setting **Default**: Standard complexity	**Registry Key Name:** pqMixChars **Values**: **1** - A minimum of 2 or 3 types must be included, as defined in the *Password- Minimum Mixed Character Type*s setting **0** -The rule for each character type is defined in the character type's *Include* setting **Default**: 1	PROP_PQ_MIXCHARS

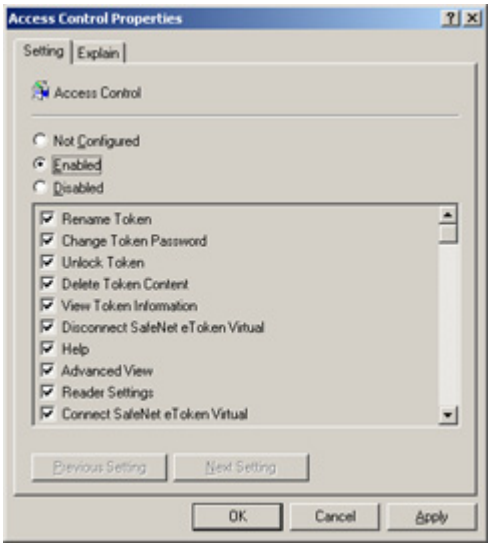
Description (Cont.)	Settings in GPO Editor or MMC (Cont.)	Registry Key (Cont.)	Command Line (Cont.)
Password - Minimum Mixed Character Types Defines the minimum number of character types that must be included in a new Token Password. The character types are: upper-case letters, lower-case letters, numerals,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

Description (Cont.)	Settings in GPO Editor or MMC (Cont.)	Registry Key (Cont.)	Command Line (Cont.)
Password - Include Lower-Case Determines if the password can include lower-case letters. **Note:** • Applies only when the *Password - Complexity* setting is set to **Manual complexity.** • Can be set in SafeNet Authentication Client Tools.	**Setting Name:** Password - Include Lower - Case **Values**: Permitted Forbidden Mandatory **Default**: Permitted	**Registry Key Name:** pqLowerCase **Values**: 0 - Permitted 1 - Forbidden 2 - Mandatory **Default**: 0	Cannot be set by command line installation.
Password - Include Special Characters Determines if the password can include special characters, such as @,!, &. **Note:** • Applies only when the *Password - Complexity* setting is set to **Manual complexity.** • Can be set in SafeNet Authentication Client Tools.	**Setting Name:** Password - Include Special Characters **Values**: Permitted Forbidden Mandatory **Default**: Permitted	**Registry Key Name:** pqSpecial **Values**: 0 - Permitted 1 - Forbidden 2 - Mandatory **Default**: 0	Cannot be set by command line installation.
Password Quality Check on Initialization Determines if the password quality settings are checked and enforced when a token is initialized **Note:** We recommend that this policy not be set when tokens are enrolled using SafeNet Authentication Manager.	**Setting Name:** Password Quality Check on Initialization **Values**: **Selected** -The password quality is enforced **Not selected** - The password quality is not enforced **Default**: Not selected	**Registry Key Name:** pqCheckInit **Values**: **1 (True)** -The password quality is enforced **0 (False)** - The password quality is not enforced **Default**: 0	Cannot be set by command line installation.

Description (Cont.)	Settings in GPO Editor or MMC (Cont.)	Registry Key (Cont.)	Command Line (Cont.)
Password Quality Owner Defines the owner of the password quality settings on a re initialized token, and defines the default of the *Password Quality Modifiable* setting.	**Setting Name:** Password Quality Owner **Values**: Administrator User **Default**: Administrator, for tokens with an Administrator Password. User, for tokens without an Administrator Password.	**Registry Key Name:** pqOwner **Values**: **0** - Administrator **1** - User **Default**: 0, for tokens with an Administrator Password. 1, for tokens without an Administrator Password.	Cannot be set by command line installation.
Enable Password Quality Modification Determines if the password quality settings on a newly initialized token can be modified by the owner. See the *Password Quality Owner* setting.	**Setting Name:** Enable Password Quality Modification. **Values**: **Selected** - The password quality can be modified by the owner **Not selected** - The password quality cannot be modified by the owner **Default**: Selected, for administrator-owned tokens Not selected, for user owned tokens.	**Registry Key Name:** pqModifiable **Values**: **1 (True)**- The password quality can be modified by the owner **0 (False)** - The password quality cannot be modified by the owner **Default**: 1 (True), for administrator-owned tokens 0 (False), for user owned tokens.	Cannot be set by command line installation.

SafeNet Authentication Client Tools UI Access Control List

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



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

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

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

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

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

Access Control Feature	Registry Value Name (Cont.)	Description (Cont.)
Advanced Initialization Settings	OpenAdvancedModeOfInitialize	Enables/Disables the *Advanced* button in the *Token Initialization* window in SafeNet Authentication Client Tools.
Change Initialization Key during Initialization	ChangeInitializationKeyDuringInitialize	Enables/Disables the *Change Initialization key* button in the *Advanced Token Initialization Settings* window in SafeNet Authentication Client Tools
Common Criteria Settings	CommonCriteriaPasswordSetting	Enables/Disables the Common Criteria option in the Certification combo box.
System Tray - Unlock Token	TrayIconUnlockEtoken	Enables/Disables the *Unlock Token* feature in the SafeNet Authentication Client Tray Menu
System Tray - Generate OTP	GenerateOTP	Enables/Disables the *Generate OTP* feature in the SafeNet Authentication Client Tray Menu
System Tray - Delete Token Content	TrayIconClearEToken	Enables/Disables the *Delete Token Content* feature in the SafeNet Authentication Client Tray Menu. **Note:** By default, this feature is **Disabled**
System Tray -Change Token Password	TrayIconChangePassword	Enables/Disables the *Change Token Password* feature in the SafeNet Authentication Client Tray Menu.
System Tray - Select Token	SwitcheToken	Enables/Disables the *Select Token* feature in the SafeNet Authentication Client Tray Menu.
System Tray -Synchronize Domain-Token Passwords	SyncDomainAndTokenPass	Enables/Disables the *Synchronize Domain Token Passwords* feature in the SafeNet Authentication Client Tray Menu.
System Tray - Tools	OpeneTokenProperties	Enables/Disables the *Tools* menu item (open SafeNet Authentication Client Tools) in the SafeNet Authentication Client Tray Menu.
System Tray - About	About	Enables/Disables the *About* menu item in the SafeNet Authentication Client Tray Menu.
Enable Change IdenTrust Identity	IdentrusChangePassword	Enables/Disables the *Change IdenTrust PIN* feature in SafeNet Authentication Client Tools.
Enable Unblock IdenTrust Passcode	IdentrusUnlock	Enables/Disables the *Unlock IdenTrust* feature in SafeNet Authentication Client Tools.
Delete Data Object	DeleteDataObject	Enables/Disables the *Delete Data Object* feature in SafeNet Authentication Client Tools.
Allow One Factor	AllowOneFactor	Enables/Disables the *Allow One Factor* feature in the *Advanced Token Initialization Settings* window in SafeNet Authentication Client Tools.
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.

Security Settings

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

Description	ADM File Setting	Registry Value	Command Line
Key Management Defines key creation, export, unwrap, and off-board crypto policies.	Setting Name: Key Management **Values**: **Compatible –** maintain a non restrictive policy that is compatible with previous releases of SAC, and allows the use of exportable keys and legacy unwrap operations. **Optimized -** Applies a restrictive policy that prevents generation and use of exportable keys, and blocks legacy unwrap operations. **Default**: Legacy	Registry Value Name: Key-Management-Security **Values**: (String) Compatible - has no effect, current behavior is kept Optimized - do not generate exportable keys, do not allow keys to be exported, regardless of how they were generated, do not allow Unwrap-PKCS1.5 or Unwrap-AES-CBC **Default**: Compatible	Cannot be set by command line installation.
Unsupported Cryptographic Algorithms and Features The following list of cryptographic algorithms will not be supported by SAC: MD5, RC2, RSA<1024, DES, GenericSecret<80, RC4<80, ECC<160, ECB, RSA-RAW.	Setting Name: Unsupported Cryptographic Algorithms and Features **Values**: **None –** All SAC cryptographic algorithms and features are supported. **Obsolete algorithms –** SAC blocks the use of: MD5, RC2, RSA<1024, DES, GenericSecret<80, RC4<80, ECC<160, ECB, RSA-RAW. **Default**: None	**Registry Value Name:** Disable-Crypto **Values**: (String) None Obsolete **Default**: None	Cannot be set by command line installation.

SafeNet Authentication Client Security Enhancements

Enforcing Restrictive Cryptographic Policies

To allow organizations to enforce restrictive cryptographic policies when using SafeNet smart card and USB tokens, the following enhancements were introduced:

- Key Management Policy
- Cryptographic Algorithms Policy

The motivation behind these enhancements:

- Legacy cryptographic schemes can cause organizations to fail current compliance requirements or expose cryptographic weakness associated with obsolete algorithms and mechanisms.

  The following enhancements were made to SafeNet Authentication Client to allow organizations to block the use of such schemes, according to organizational policies.

  - Enabling symmetric keys wrapping with other symmetric keys using GCM and CCM modes of operation.
  - 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.
- SafeNet introduced a new mechanism that allows administrators to prevent the use of legacy or obsolete algorithms by third-party applications. These cryptographic algorithms conform to the National Institute of Standards and Technology (NIST), preventing third-party applications from using legacy or obsolete algorithms.

  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.

NOTE:
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.

Creating Symmetric Key Objects using PKCS#11

As part of SafeNet Authentication Client security enhancement campaign, the following was performed in SAC 10.2:

1. 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.
2. Sensitive data is securely zeroed prior to freeing up the memory.
3. 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 in SAC 10.2, 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).

Log Settings

The following settings are written to the appropriate folder's

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

These settings may be defined using:
HKEY_LOCAL_MACHINE or HKEY_CURRENT_USER

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

The following settings are written to the appropriate folder's

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

These settings may be defined using:

HKEY_LOCAL_MACHINE or HKEY_CURRENT_USER

TempDir Determines the path to a file containing the SafeNet Authentication Client log files.	Not supported	**Registry Value Name:** TempDir **Value**: Enter a folder name e.g. C:\temp **Default**: Windows: C:\windows\temp Linux & Mac: /tmp	

IdenTrust Settings

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

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