SafeNet Authentication Client (Windows)

Version 8.3 Revision B

Administrator's Guide

All attempts have been made to make the information in this document complete and accurate.

SafeNet, Inc. is not responsible for any direct or indirect damages or loss of business resulting from inaccuracies or omissions. The specifications contained in this document are subject to change without notice.

SafeNet and SafeNet Authentication Manager are either registered with the U.S. Patent and Trademark Office or are trademarks of SafeNet, Inc., and its subsidiaries and affiliates, in the United States and other countries. All other trademarks referenced in this Manual are trademarks of their respective owners.

SafeNet Hardware and/or Software products described in this document may be protected by one or more U.S. Patents, foreign patents, or pending patent applications.

Please contact SafeNet Support for details of FCC Compliance, CE Compliance, and UL Notification.

Document Name: SafeNet Authentication Client 8.3 Administrator's Guide

Document Part Number: 007-012450-001, Revision B

Date of publication: January 2014

Last update: Monday, January 27, 2014 11:26 am

Support

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:

Telephone

You can call our help-desk 24 hours a day, seven days a week:
USA: 1-800-545-6608
International: +1-410-931-7520

Email

You can send a question to the technical support team at the following email address:
support@safenet-inc.com

Website

You can submit a question through the SafeNet Support portal:
https://serviceportal.safenet-inc.com

Additional Documentation

The following SafeNet publications are available:

- SafeNet Authentication Client 8.3 User's Guide
- SafeNet Authentication Client 8.3 Customer Release Notes

Table of Contents

1 Introduction

SafeNet Authentication Client (SAC) enables token operations and the implementation of token PKI-based solutions.

In this chapter:

- Overview
- SafeNet Authentication Client Main Features
- What's New
- Supported Tokens
- Supported Localizations
- SafeNet Authentication Client Architecture
- License Activation

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 tokens.

Cryptography API: Next Generation (CNG)

CNG is the long-term replacement for the CryptoAPI. CNG is designed to be extensible at many levels, and it is cryptography-agnostic in behavior.
CNG includes support for Suite B algorithms, enabling the selection of SHA-2 algorithms for tokens used with SafeNet Authentication Client.
CNG currently supports the storage of asymmetric private keys by using the Microsoft software *Key Storage Provider (KSP)* that is installed by default with Windows Server 2008 and Windows Vista.

Key Storage Provider (KSP)

KSP is a software library that implements the standard CNG key storage provider plug-in interfaces and is registered with the CNG system. This enables applications to choose different mechanisms for key storage, such as software, smartcards, or hardware security.

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 incorporates features that were supported by previous releases of eToken PKI Client and SafeNet Borderless Security (BSec). It provides a unified middleware client for a variety of SafeNet smartcards, SafeNet iKey tokens, and SafeNet eToken devices.

SafeNet Authentication Client offers full backward compatibility so that customers who have been using eToken PKI Client or SafeNet Borderless Security Client (BSec) can continue to use deployed eToken and iKey devices.

NOTE
Future versions of SafeNet Authentication Client may not support BSec-compatibility.

SafeNet Authentication Client includes the following features:

- Token usage, including:
  - Digitally signing sensitive data
  - Remote data access
  - SafeNet eToken Virtual use
  - Management of certificates on the token

- Token management operations, including:
  - Token initialization
  - 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

What's New

SafeNet Authentication Client 8.3 offers the following new features:

- Windows 8.1 support
- Each SafeNet eToken 7300 (HID and non-HID) device initialized using SafeNet Authentication Client 8.3 can be used on both Windows and MAC computers even where SafeNet Authentication Client is not installed
- Each SafeNet eToken 5200/5205 HID device can be used on both Windows and MAC computers even where SafeNet Authentication Client is not installed
- New common SafeNet Authentication Client tray icons and tray menu user interface for both eTokens and iKey tokens
- eToken 7300 CD-ROM update (supported via SDK)

NOTE
There is no 8.3 release of the BSec Utility package. Continue to use *BSec Compatibility Utilities Package 8.2*.
Future versions of SafeNet Authentication Client may not support BSec-compatibility.

Supported Tokens

SafeNet Authentication Client 8.3 supports the following tokens:

- SafeNet eToken PRO
- SafeNet eToken PRO Anywhere
- SafeNet eToken PRO Smartcard
- SafeNet eToken 7300 (standard and HID)
- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID
- SafeNet eToken 4100
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)
- SafeNet eToken 7100 (SafeNet eToken NG-Flash)
- SafeNet eToken NG-Flash Anywhere
- SafeNet eToken Virtual Family
- SafeNet iKey: 2032, 2032u, 2032i
- SafeNet Smartcard: SC330, SC330u, SC330i
- SafeNet Smartcard SC400
- SafeNet iKey 4000

Supported Localizations

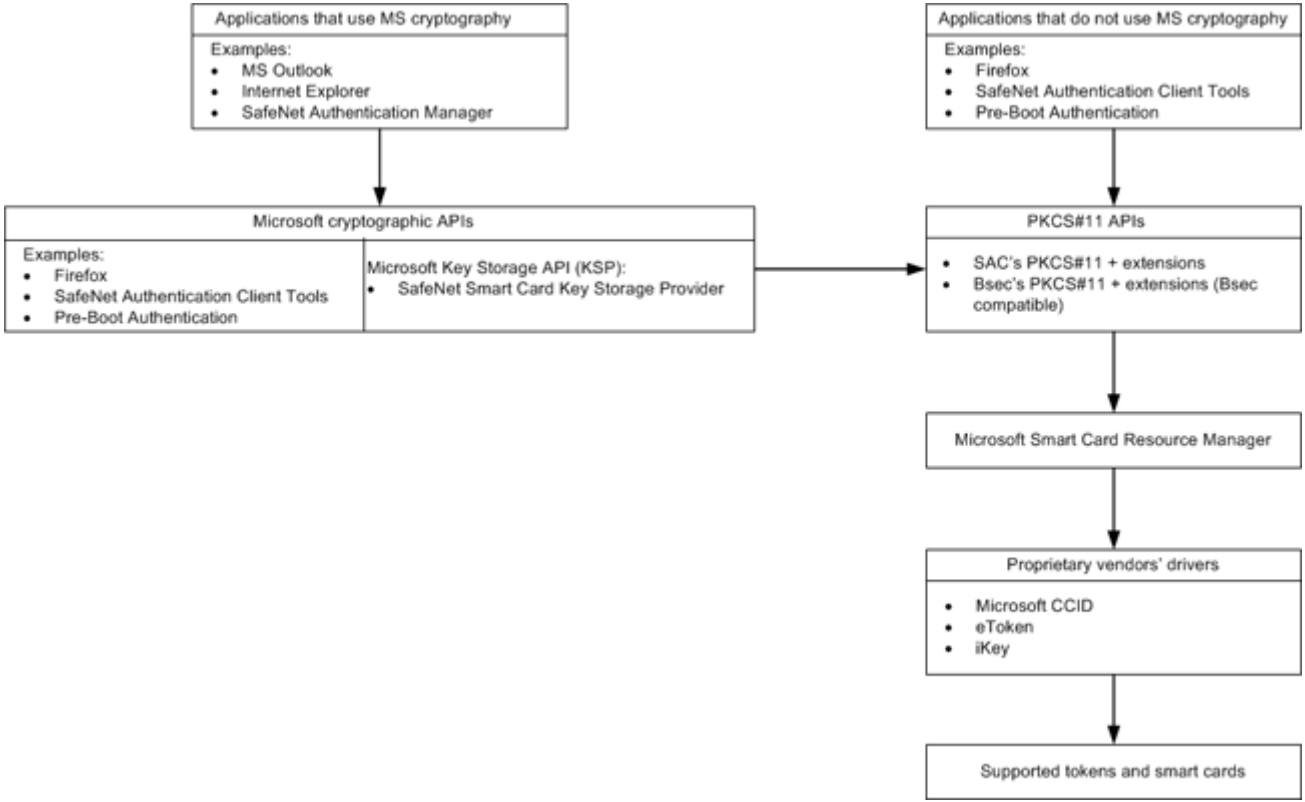
NOTE
Localizations are not supported in the BSec Utility applications.

SafeNet Authentication Client 8.3 supports the following languages:

- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- English
- French (Canadian)
- French (European)
- German
- Hungarian
- Italian
- Japanese
- Korean
- Lithuanian
- Polish
- Portuguese (Brazilian)

- Romanian
- Russian
- Spanish
- Thai
- Vietnamese

SafeNet Authentication Client Architecture



License Activation

By default, SafeNet Authentication Client 8.3 is installed as licensed for evaluation only.

To install a non-evaluation license:

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 8.3 User's Guide*.
   - **Command Line Activation**

     See *License Settings* on page 173 (Command Line column) and *Installing via the Command Line* on page 83.
   - **Group Policy Object Editor**

     See *License Settings* on page 173 (ADM File Setting column) and *Setting SafeNet Authentication Client Properties* on page 157.
   - **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 43.

2 System Requirements

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

In this chapter:

Supported Browsers

SafeNet Authentication Client 8.3 supports the following browsers:

- Firefox 5 and later
- Internet Explorer 7, 8, 9, 10, 11, Metro
- Chrome version 14 and later, for authentication only (Does not support enrollment)

Supported Platforms

SafeNet Authentication Client 8.3 supports the following operating systems:

- Windows XP SP3 (32-bit, 64-bit)
- Windows Server 2003 SP3 (32-bit, 64-bit)
- Windows Server 2003 R2 (32-bit, 64-bit)
- Windows Vista SP2 (32-bit, 64-bit)
- Windows Server 2008 SP2 (32-bit)
- Windows Server 2008 R2 SP1 (64-bit)
- Windows Server 2012 (64-bit)
- Windows Server 2012 R2 (64-bit)
- Windows 7 SP1 (32-bit, 64-bit)
- Windows 8 (32-bit, 64-bit)
- Windows 8.1 (32-bit, 64-bit)

NOTE

- To use a KSP cryptographic provider, Windows Vista or higher is required.
- 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.

The following Mac operating systems support SafeNet eToken 7300 devices initialized using SafeNet Authentication Client 8.3, and SafeNet eToken 5200/5205 HID devices:

- Mac OS X 10.8 (Mountain Lion)
- Mac OS X 10.7.3 and 10.7.4 (Lion)

Hardware and Screen Resolution Requirements

Required hardware:

- USB port, for physical token devices

Recommended screen resolution:

- 1024 x 768 pixels and higher, for SafeNet Authentication Client Tools

Compatibility with SafeNet Applications

SafeNet Authentication Client 8.3 works with the following SafeNet products:

eToken Devices

- SafeNet Network Logon 8.0
- SafeNet Authentication Manager 8.0 and later
- eToken Minidriver 5.1 (Java cards only)

Compatibility with Third-Party Applications

SafeNet Authentication Client 8.3 works with the following products:

- Juniper Secure Access
- RDP Windows Logon
- Entrust ESP 9.0 and later (Entrust EDS and ESP applicable to iKey 2032i, SC330i, iKey 4000)
- Citrix XenApp 5.0, XenApp 6.0, XenApp 6.5
- Cisco AnyConnect, Cisco ASA, Cisco VPN Client
- IdenTrust
- MS Office 2007, 2010
- Adobe Acrobat 9, X
- VMware Workstation
- Certificate Authorities:
  - Microsoft CA 2003 / R2
  - Microsoft CA 2008 / R2
  - VeriSign CA
  - Entrust Authority Security Manager 8.1
- Microsoft FIM/ILM

- VPNs:
  - Microsoft VPN
  - Cisco VPN
  - Check Point VPN
- MyID (Intercede) - for iKey devices only

3 Installation Files and Administrator Tasks

The software package provided by SafeNet includes files for installing or upgrading to SafeNet Authentication Client 8.3.

In this chapter:

Installation Files

The following installation, migration, and documentation files are provided:

File	Environment	Description	Use
SafeNetAuthenticationClient-x32-x64-8.3.exe	32-bit 64-bit	Installs SafeNet Authentication Client 8.3, and upgrades from earlier versions of SafeNet Authentication Client and eToken PKI Client	Use to install SafeNet Authentication Client 8.3, and to upgrade from: ♦ SafeNet Authentication Client 8.0 and later ♦ eToken PKI Client 5.1 SP1
SafeNetAuthenticationClient-x32-8.3.msi	32-bit		
SafeNetAuthenticationClient-x64-8.3.msi	64-bit		
SafeNetAuthenticationClient-eToken-x32-8.3.msi	32-bit	Installs SafeNet Authentication Client 8.3 for eToken devices only (without BSec components), and upgrades from earlier versions of SafeNet Authentication Client and eToken PKI Client for eToken devices only	Use to install SafeNet Authentication Client 8.3 for eToken devices only (without BSec components), and to upgrade from: ♦ SafeNet Authentication Client 8.0 and later ♦ eToken PKI Client 5.1 SP1 for eToken devices only
SafeNetAuthenticationClient-eToken-x64-8.3.msi	64-bit		

File	Environment	Description	Use
SACCustomizationPackage-8.3.exe	32-bit 64-bit	Installs SafeNet Authentication Client 8.3 Customization Package, and upgrades from SafeNet Authentication Client 8.1 and later Customization Packages	Use to customize SafeNet Authentication Client installation with non-default settings
SafeNetAuthenticationClientPackage-8.3.exe	32-bit	Upgrades to SafeNet Authentication Client 8.3 from BSec	Use to upgrade from BSec 7.2.0 and later
PolicyMigrationTool.exe	32-bit	Migrates policy configurations and registry key settings from BSec to SafeNet Authentication Client	Use to import existing settings from a BSec installation earlier than 7.2.0 following upgrade to SafeNet Authentication Client
SAC_CRN_8_3_Rev_A.pdf		SafeNet Authentication Client 8.3 Customer Release Notes	Read before installation for last minute updates that may affect installation; contains important information such as resolved and known issues and troubleshooting
SAC_User_Guide_8_3_Rev_A.pdf		SafeNet Authentication Client 8.3 User's Guide	Provides detailed information for the user and system administrator regarding the use of SafeNet Authentication Client

File	Environment	Description	Use
SAC_Admin_Guide_8_3_Rev_A.pdf		SafeNet Authentication Client 8.3 Administrator's Guide (this document)	Provides detailed information for the system administrator regarding the installation, configuration, maintenance, and management of SafeNet Authentication Client

NOTE

SafeNetAuthenticationClient-BSecUtilities-8.2.msi, which installs legacy BSec Utilities that can be used with BSec-compatible SafeNet Authentication Client versions 8.2 and 8.3, is not packaged with SafeNet Authentication Client 8.3. It is provided in the SafeNet Authentication Client 8.2 installation folder.

Checklist of Administrator Tasks

If upgrading from eToken PKI Client or BSec, determine if the registry keys are to be cleared before installing SafeNet Authentication Client.

- For upgrading from eToken PKI Client, see *Upgrading from eToken PKI Client* on page 62.
- For upgrading from BSec, see *Upgrading from SafeNet Borderless Security (BSec)* on page 64.

Customize the SafeNet Authentication Client default installation features, if required, to create a customized SafeNet Authentication Client 8.3 installation.

- See *Customization* on page 34.

If a previous version of SafeNet Authentication Client is already installed:

- For upgrading using the installer file, see *Simplified Upgrade* on page 59.
- For upgrading using the msi file, see *Upgrading Using MSI* on page 61.

If not upgrading, install SafeNet Authentication Client on each computer on which a token is to be used.

- For installing via the installation wizard, see *Installing via the Wizard* on page 75.
- For installing via the command line, see *Installing via the Command Line* on page 83.

Customize the SafeNet Authentication Client settings, if required, and update all client computers.

See *SafeNet Authentication Client Settings* on page 119.

Initialize and manage tokens.

- See the *Token Initialization* and *Token Management* chapters in the SafeNet Authentication Client User's Guide.

4 Customization

The SAC installation features and the graphic user interface provided by SafeNet can be customized for your installation.

NOTE
.Net Framework 2.0 or higher is required on all operating system when running the SafeNet Authentication Client Customization Tool.

In this chapter:

- Customization Overview
- Installing the SafeNet Authentication Client Customization Tool
- Using the SafeNet Authentication Client Customization Tool
- Generating a Customized MSI Installation File
- Installing the Customized Application

Customization Overview

You can customize the following SafeNet Authentication Client 8.3 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 features to be installed
- Policy settings
- MSI Signing settings
- Window banners

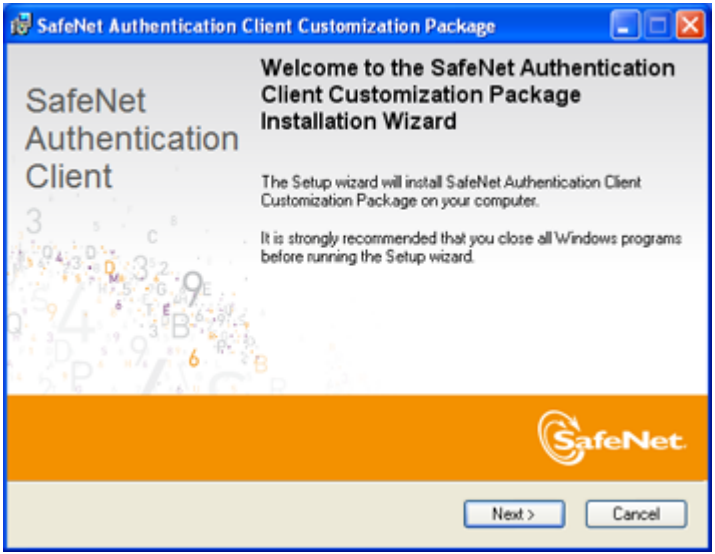
Installing the SafeNet Authentication Client Customization Tool

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

To install the SafeNet Authentication Client Customization Tool:

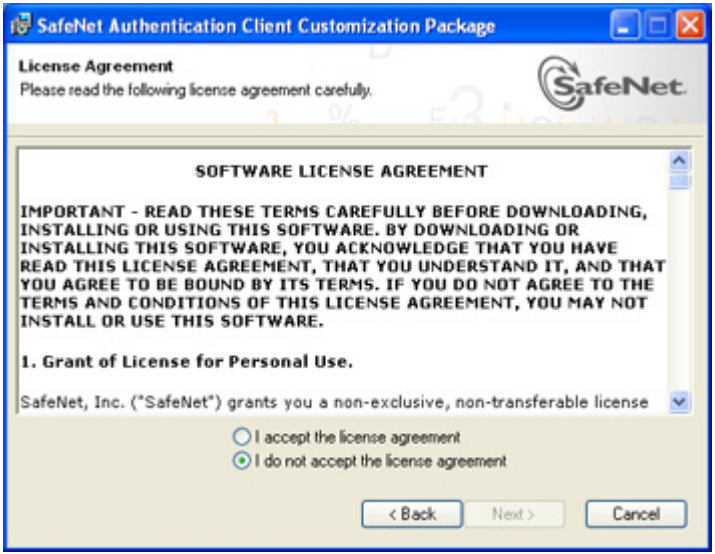
1 Double-click **SACCustomizationPackage-8.3.exe**.

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



2 Click **Next**.

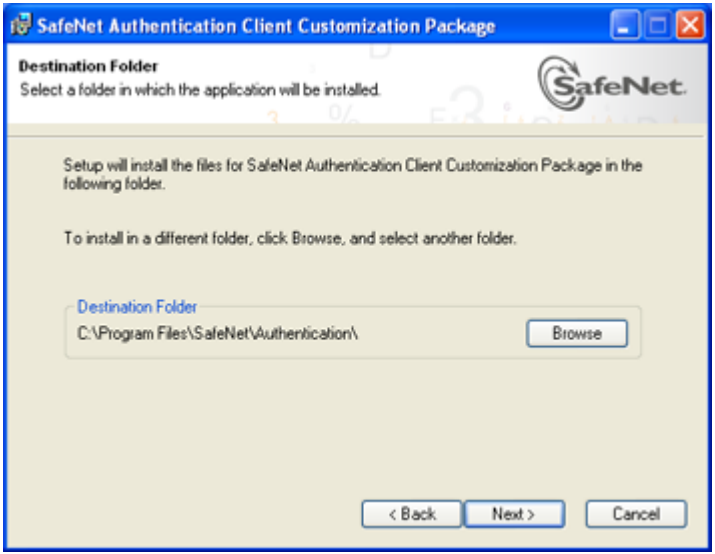
The *License Agreement* is displayed.



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:

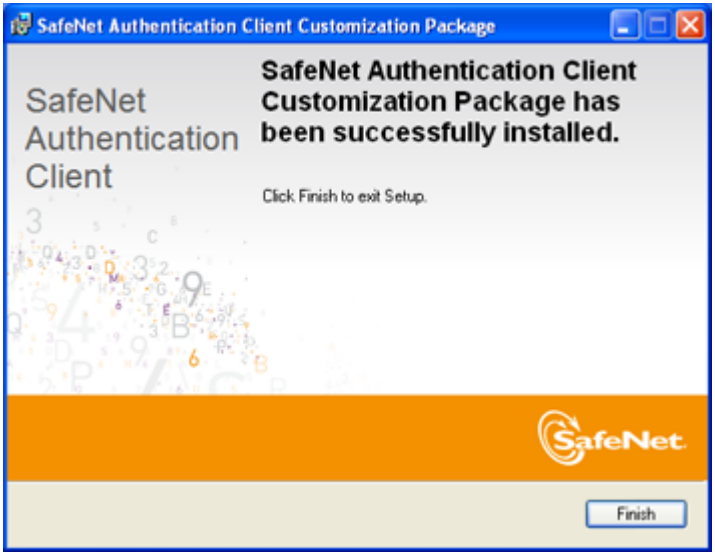
`C:\Program Files\SafeNet\Authentication\`

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.

6 Click **Next** 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.

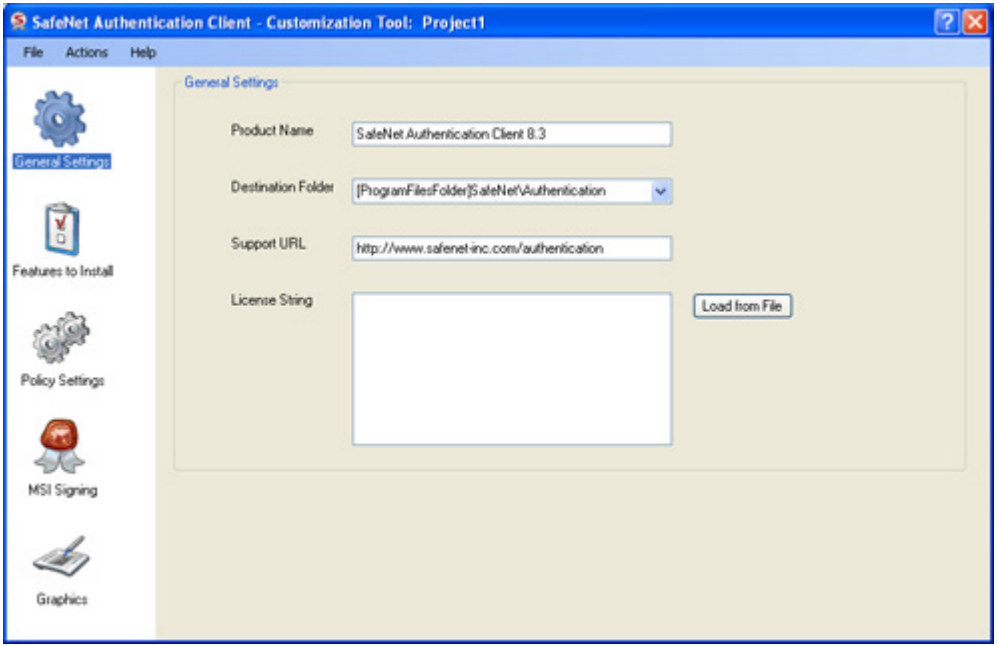
Using the SafeNet Authentication Client Customization Tool

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.



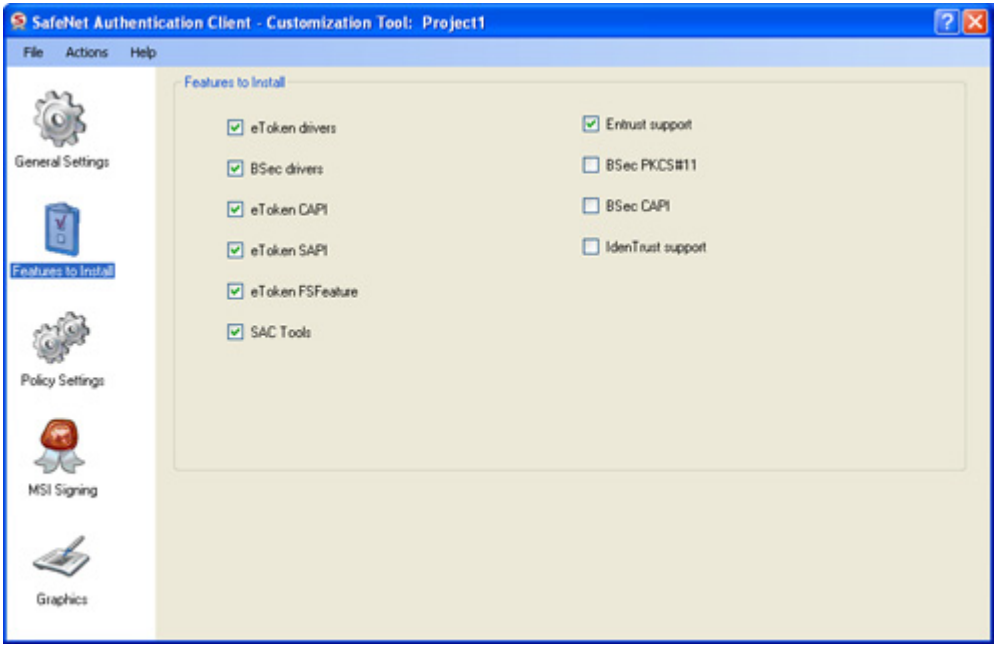
2 To open a project you already saved, select **File > Open**, and browse to the xml file of an existing project.

3 You can replace the following items:

- Destination folder path to be used by the SafeNet Authentication Client Customization Tool when no other SafeNet product has been installed on the client computer
- URL to be displayed in the Windows *Add/Remove Programs* support link
- License string to be installed: either paste to 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.



5 You can select which features will be installed when the SafeNet Authentication Client Customization Tool is run:

- eToken Drivers
- BSec Drivers
- eToken CAPI

NOTE
Ensure that *eToken CAPI* is selected.

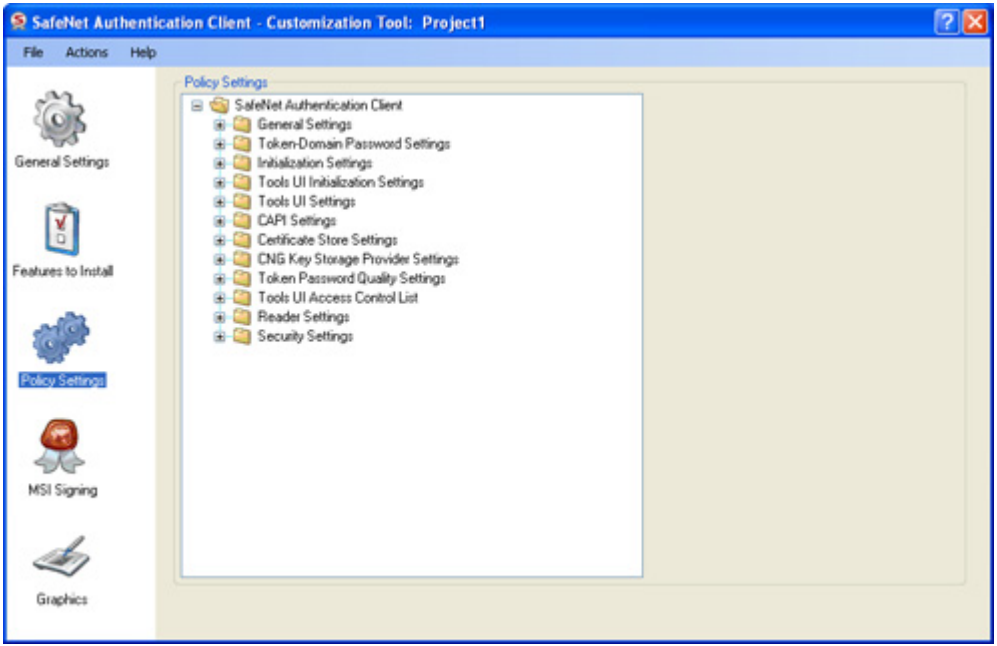
- eToken SAPI
- eToken FSFeature
- SAC Tools
- Entrust support
- BSec PKCS#11
- BSec CAPI
- IdenTrust support

NOTE
If *IdenTrust support* is selected, ensure that *BSec PKCS#11* is selected also.

For more information, see Chapter 6: *Command Line Installation Features*, on page 102.

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

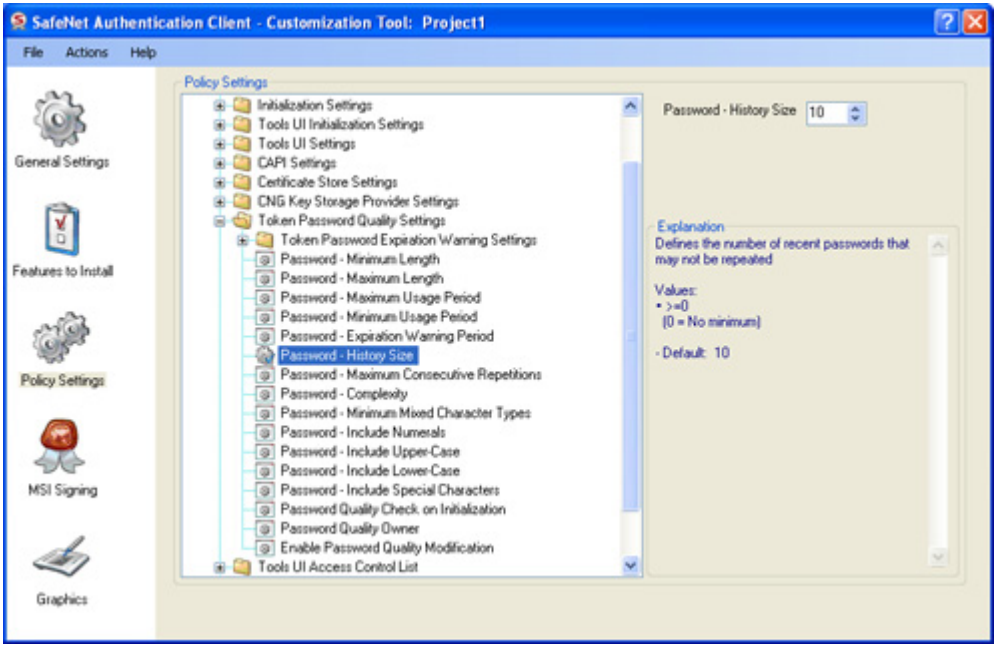
The *Policy Settings* window opens.



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

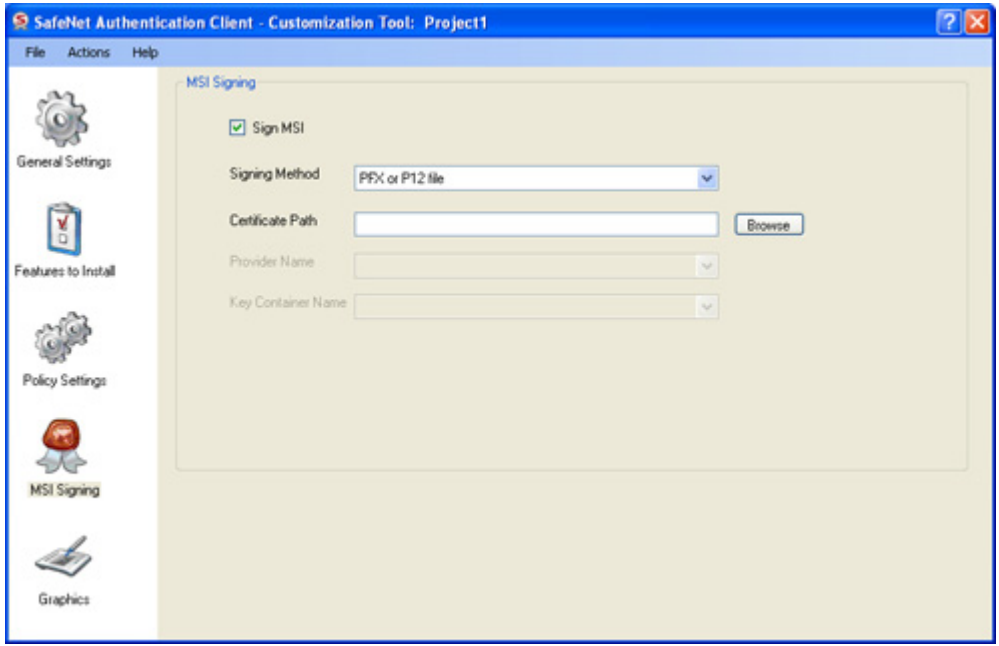
For more information, see Chapter 9: *Configuration Properties*, on page 155.

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



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

The *MSI Signing* window opens.


SafeNet Authentication Client - Customization Tool: Project1
File
Actions
Help
General Settings
Features to Install
Policy Settings
MSI Signing
Graphics
MSI Signing
Sign MSI
Signing Method
PFX or P12 file
Certificate Path
Browse
Provider Name
Key Container Name

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

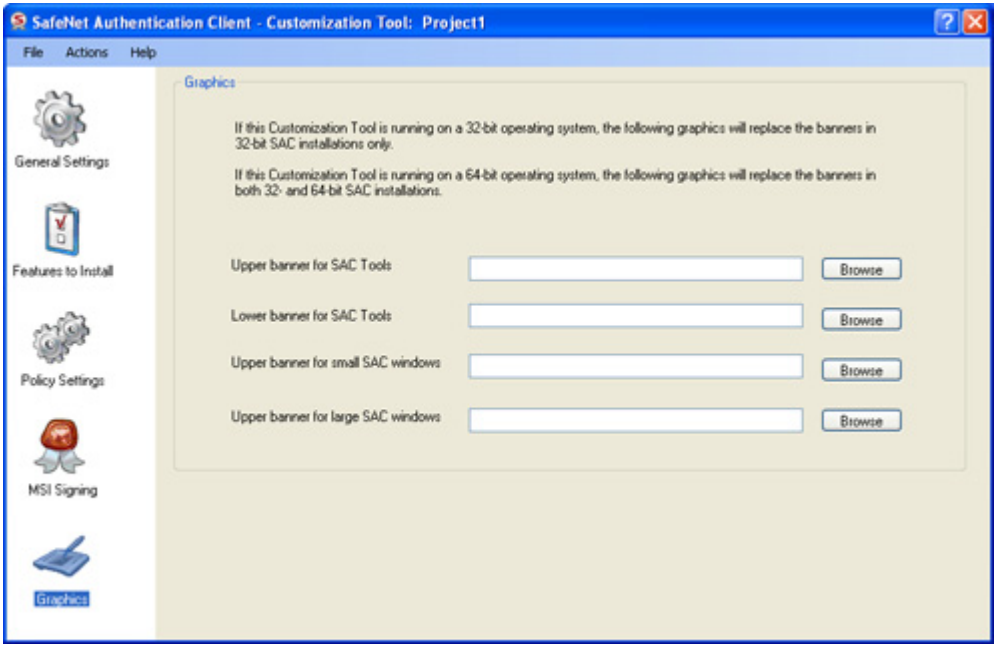
- Signing Method (P12, Smartcard or HSM)
- Certificate Path

> **NOTE**
> Ensure that a Code Signing certificate is used when using the MSI signing feature.

- Provider Name
- Key Container Name

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

The *Graphics* window opens.


SafeNet Authentication Client - Customization Tool: Project1
File
Actions
Help
General Settings
Features to Install
Policy Settings
MSI Signing
Graphics
Graphics
If this Customization Tool is running on a 32-bit operating system, the following graphics will replace the banners in 32-bit SAC installations only.
If this Customization Tool is running on a 64-bit operating system, the following graphics will replace the banners in both 32- and 64-bit SAC installations.
Upper banner for SAC Tools
Browse
Lower banner for SAC Tools
Browse
Upper banner for small SAC windows
Browse
Upper banner for large SAC windows
Browse

The following graphics can be replaced:

- Upper Banner for SAC Tools - (Properties: Dimensions - 764X142 pixels, Horizontal/Vertical Resolution - 96/96 dpi, Bit Depth - 24, Frame Count - 1)
- Lower Banner for SAC Tools - (Properties: Dimensions - 764X76 pixels, Horizontal/Vertical Resolution - 72/72 dpi, Bit Depth - 24, Frame Count - 1)
- Upper Banner for small SAC windows - (Properties: Dimensions - 506X65 pixels, Horizontal/Vertical Resolution - 96/96 dpi, Bit Depth - 32, Frame Count - 1)

> **NOTE**
> In SafeNet Authentication Client 8.3 GA, banners for SAC windows cannot be customized.

- Upper Banner for large SAC windows - (Properties: Dimensions - 760X65 pixels, Horizontal/Vertical Resolution - 96/96 dpi, Bit Depth - 32, Frame Count - 1)

> **NOTE**
> In SafeNet Authentication Client 8.3 GA, banners for SAC windows cannot be customized.

> **NOTE**
> The file format for the upper and lower banner of SAC Tools must be in JPG format, and the upper banners for small and large SAC windows 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

Generating a Customized MSI Installation File

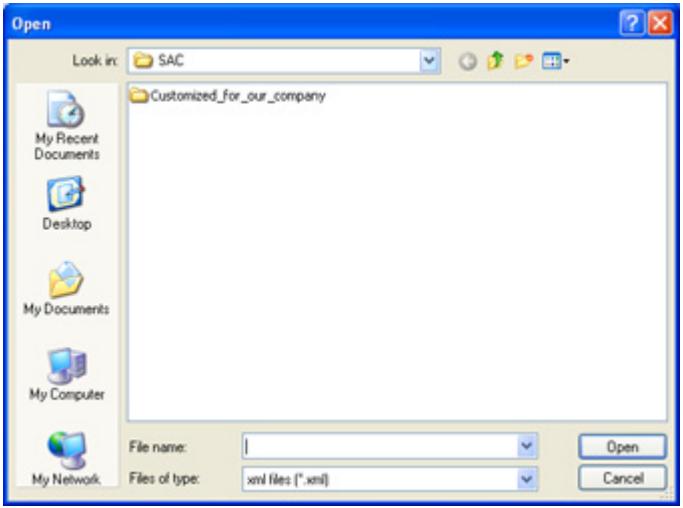
After the appropriate features are customized, generate an installation file.

To generate a customized installation file:

1. Open the *SAC Customization Tool*.

   See *Using the SafeNet Authentication Client Customization Tool* on page 41.

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

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>-x32-8.3.msi` for 32-bit installations
- A file named `<Project Name>-x64-8.3.msi` for 64-bit installations

Installing the Customized Application

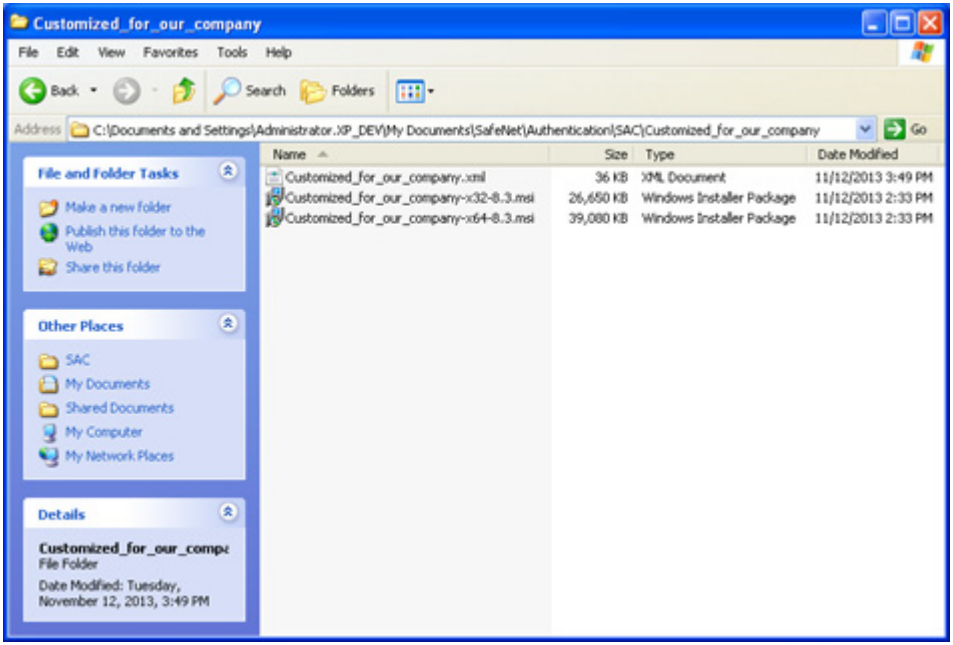
After the .msi installation file is generated, use it to install the application with its customized properties and features.

NOTE
Ensure that all legacy eToken Properties or SafeNet Authentication Client Tools applications are closed before upgrading, installing, or uninstalling SafeNet Authentication Client.

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 *Generating a Customized MSI Installation File* on page 53.

   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>-x32-8.3.msi` (for 32-bit installations)
- `<Project Name>-x64-8.3.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.

5 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.

In this chapter:

Simplified Upgrade

The simplest way to upgrade to SafeNet Authentication Client 8.3 is to use an .exe installer file. These files do not support customization.

An .exe installer file installs SafeNet Authentication Client 8.3 properly on 32-bit and 64-bit environments in each of the following situations:

- No middleware is yet installed
- SafeNet Authentication Client 8.0 or later is installed, with or without BSec compatibility
- eToken PKI Client 5.1 SP1 is installed
- BSec 7.2.0 or later is installed

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

eToken PKI Client 5.1 SP1, BSec 7.2.0 or later, and earlier versions of SafeNet Authentication Client, are automatically upgraded during the SafeNet Authentication Client 8.3 installation.

To run the installer:

- To upgrade from an earlier version of SafeNet Authentication Client or from eToken PKI Client 5.1 SP1 on a 32-bit or 64-bit system, run **SafeNetAuthenticationClient-x32-x64-8.3.exe**.
- To upgrade from BSec 7.2.0 or later on a 32-bit system, run **SafeNetAuthenticationClientPackage-8.3.exe**.

After the installer file is run, SafeNet Authentication Client 8.3 is installed. No other installation or upgrade file need be run.

Upgrading Using MSI

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

- On a 32-bit system, run **SafeNetAuthenticationClient-x32-8.3.msi**.
- On a 64-bit system, run **SafeNetAuthenticationClient-x64-8.3.msi**.

See *Installing via the Wizard* on page 75.

Upgrading from eToken PKI Client

Computer and user registry settings from legacy installations are not cleared when SafeNet Authentication Client is installed.

To manage the registry settings from eToken PKI Client installations not earlier than 4.55:

1. Install SafeNet Authentication Client 8.3 using the wizard. See *Installing via the Wizard* on page 75.

   If computer and user registry settings from the earlier installation are detected, a **Use the existing configuration settings** option appears on the *Select interface language* window. See step 6 of Installing via the Wizard on page 77.

2. Do one of the following:

   - To maintain the registry settings from the earlier installation, select the **Use the existing configuration settings** option.
   - To clear the registry settings from the earlier installation, clear the **Use the existing configuration settings** option.

3. Continue the installation.

Upgrading from Versions Earlier than eToken PKI Client 5.1 SP1

Legacy versions of eToken PKI Client earlier than 5.1 SP1 must be uninstalled before installing SafeNet Authentication Client 8.3.

Upgrading from SafeNet Borderless Security (BSec)

You can upgrade from BSec to SafeNet Authentication Client 8.3 using automatic or manual upgrade.

You must use manual upgrade in the following situations:

- Command line configuration is required
- A BSec version earlier than 7.2.0 is installed

Automatic Upgrade

The automatic upgrade process runs an internal Policy Migration Tool to retain your current BSec settings, uninstalls BSec, and installs SafeNet Authentication Client with the saved BSec settings.

Automatic upgrade is supported for BSec 7.2.0 and later. For earlier versions of BSec, use the manual upgrade process.

> **NOTE**
> Automatic upgrade does not support command line configuration.

To upgrade from BSec 7.2.0 and later to SafeNet Authentication Client 8.3:

- Run **SafeNetAuthenticationClientPackage-8.3.exe**.

Manual Upgrade of BSec Policies and Registry Settings

When upgrading manually from BSec to SafeNet Authentication Client 8.3, first run the *Policy Migration Tool* to migrate BSec settings from the BSec Client or from the BSec policies created by the AMC on the management station. A SafeNet Authentication Client registry file is created that replicates the BSec configuration, enabling the user to use SafeNet Authentication Client with the legacy BSec configuration.

To upgrade and manually migrate policies and registry settings:

1. Locate the `PolicyMigrationTool.exe` file in installation package's `Tools` folder.
2. Copy the `PolicyMigrationTool.exe` file to the AMC management station, or to the folder in which you want the new registry file of BSec policies to be written.
3. From the command line, run
   `PolicyMigrationTool.exe [Mod [Options]]`
   For a description of the `Mod` and `Options` parameters, see *Policy Migration Tool Parameters* on page 67.

   If no command line parameters are included:

   - The BSec policies are written to a migration file named `PolicyMigrationTool.reg` in the folder from which the `PolicyMigrationTool.exe` was run.
   - The policies are set to be imported from that file to:
     `HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC`.
4. Uninstall BSec.

5 Install SafeNet Authentication Client, optionally importing the migration file created in step 3 on page 65 to the appropriate registry keys.

For example, if the *Policy Migration Tool* was run from the `C:\` folder, and migration file was saved using the default file name, run the following command:

```
msiexec /i SafeNetAuthenticationClient-x32-8.3.msi
PROP_REG_FILE="C:\PolicyMigrationTool.reg" /qb
```

6 If you did not include the `PROP_REG_FILE` property during the installation in step 5, import the migration file to the appropriate registry keys by double-clicking the file created in step 3 on page 65.

7 Configure SafeNet Authentication Client as required. (See *SafeNet Authentication Client Settings* on page 119.)

Ensure that the migration file of registry keys has been imported. The registry values are appended to the subfolders of the registry location defined when the *Policy Migration Tool* was run in step 3 on page 65. To determine the registry location, see *Policy Migration Tool Parameters* on page 67.

Policy Migration Tool Parameters

If no command line parameters are included when running `PolicyMigrationTool.exe`:

- The BSec policies are written to a migration file named `PolicyMigrationTool.reg` in the folder from which the `PolicyMigrationTool.exe` was run.
- The policies are set to be imported from the migration file to: `HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC`.

Parameter	Description
none	The Policy Migration Tool reads the BSec client database files whose location is defined in the registry key HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\BSecClient\InstallLocation and creates a .reg file named PolicyMigrationTool.reg in the folder from which the Policy Migration Tool was run. When the .reg file is included in the PROP_REG_FILE property during SafeNet Authentication Client installation, or when the file is double-clicked, its registry keys are imported to: HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC.
AMC -i [policy client name]	Same as option "none", but the name of the appropriate BSec policy client configuration is defined in the parameter. If no policy client name is defined and there are multiple configurations, the application displays the configuration names and prompts for a selection.
-u	Same as option "none", but the .reg file's registry keys are set to be imported to: HKEY_CURRENT_USER\SOFTWARE\SafeNet\Authentication\SAC, and not to the HKEY_LOCAL_MACHINE registry.

Parameter	Description
-p	Same as option "none", but the registry keys are set to be imported to the registry's *Policies* section. ♦ If option "-u" is present, this is: HKEY_CURRENT_USER\SOFTWARE\Policies\SafeNet\Authentication\SAC ♦ If option "-u" is not present, this is: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SafeNet\Authentication\SAC
-o [output file path and name]	Same as option "none", but the name and path of the new .reg file is defined in the parameter.

Client Installation Examples

- PolicyMigrationTool.exe -p -u -o c:\MyBSecConfiguration.reg

  Reads the client installation, and creates a file named: `c:\MyBSecConfiguration.reg`

  The file is set to import the registry keys to:

  `HKEY_CURRENT_USER\SOFTWARE\Policies\SafeNet\Authentication\SAC`

- PolicyMigrationTool.exe AMC -i My_AMC_Configuration

  Reads the `My_AMC_Configuration` package, and creates a `PolicyMigrationTool.reg` file in the folder from which the Policy Migration Tool was run.

  The file is set to import the registry keys to:
  `HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC`

6 Installation

SafeNet Authentication Client must be installed on each computer on which a SafeNet eToken, iKey token, or SafeNet smartcard is to be used. 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.
- 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.

To customize the user interface and the features to be installed, see Chapter 4: *Customization*, on page 34.

In this chapter:

- Installing a Customized Application
- Installing via the Wizard
- Installing via the Command Line
- Installing the BSec Utility Package
- Configuring Root Certificate Storage for Windows Server 2008 R2

Installation Configurations

SafeNet Authentication Client can be installed with the following configurations:

Configuration	Description	Installation Steps
Standard SafeNet Authentication Client Installation	Standard SafeNet Authentication Client features and user interface. Support for eToken and iKey tokens.	♦ Install SafeNet Authentication Client. When using the installation wizard, select the **Standard Configuration** option.
BSec API Compatible	Same as Standard SafeNet Authentication Client Installation with the addition of compatibility with third-party applications using the BSec API.	♦ Install SafeNet Authentication Client using the installation wizard, and select the **BSec-Compatible** option.

Upgrading

If SafeNet Authentication Client, eToken PKI Client, or BSec is already installed, see Chapter 5: *Upgrade*, on page 58.

Simplified Installation

The simplest way to install SafeNet Authentication Client 8.3 is to use the .exe installer file. This installer file does not support customization.

The .exe installer file installs SafeNet Authentication Client 8.3 properly on both 32-bit and 64-bit systems in all of the following situations:

- No middleware is yet installed
- Any version of SafeNet Authentication Client earlier than 8.3 is installed, with or without BSec compatibility
- eToken PKI Client 5.1 SP1 is installed

NOTE
Ensure that all legacy *eToken Properties* or *SafeNet Authentication Client Tools* applications are closed before upgrading, installing, or uninstalling SafeNet Authentication Client.

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

- Run **SafeNetAuthenticationClient-x32-x64-8.3.exe**.

After the installer file is run, SafeNet Authentication Client 8.3 is installed. No other installation or upgrade file need be run.

Installing a Customized Application

SafeNet Authentication Client can be installed with customized properties and features.

See Chapter 4: *Customization*, on page 34.

Installing via the Wizard

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

The properties that can be set using the wizard are:

- **Interface language**: the language in which the SafeNet Authentication Client user interface is displayed
- **BSec-compatibility**: support for third-party applications developed with the BSec SDK
- **Destination folder**: the installation library for this and all future SafeNet authentication product applications

  If an application from the SafeNet Authentication product line or an eToken legacy product was previously installed on the computer, do not change the destination folder.

NOTE
Ensure that all legacy *eToken Properties* and *SafeNet Authentication Client Tools* 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:

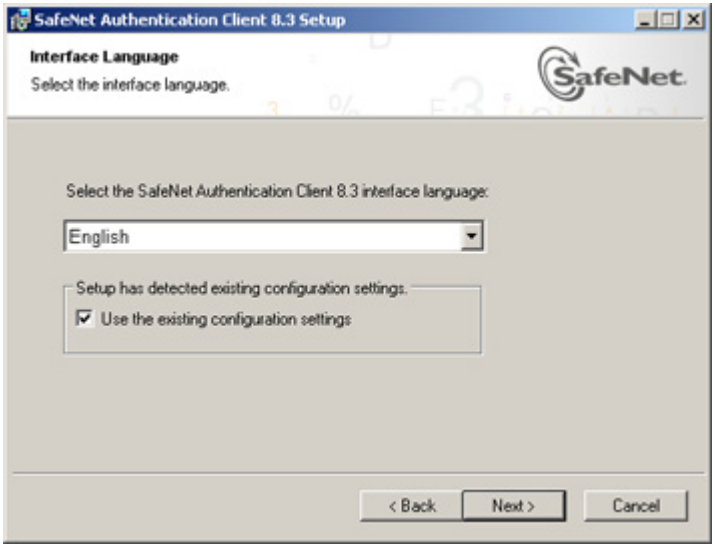
- `SafeNetAuthenticationClient-x32-8.3.msi` (32-bit)
- `SafeNetAuthenticationClient-x64-8.3.msi` (64-bit)

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**.

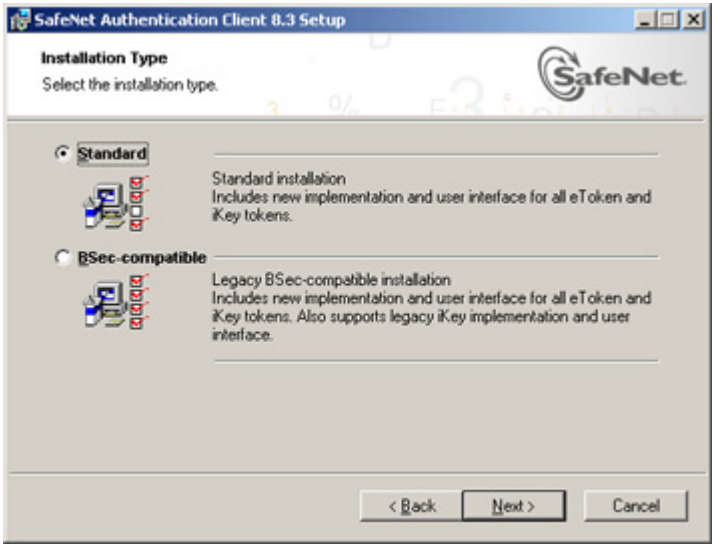
7 Click **Next**.

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 *Installation Type* window opens.



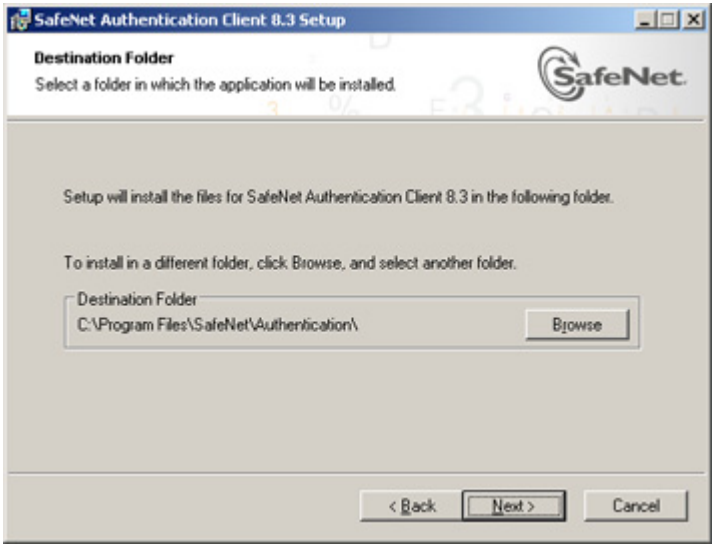
10 Select one of the following:

- **Standard**: supports all eToken and iKey tokens
- **BSec-compatible**: supports all eTokens and iKey tokens, and supports third-party applications developed with the BSec SDK

> **TIP**
> Future versions of SafeNet Authentication Client may not support BSec-compatibility.

11 Click **Next**.

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



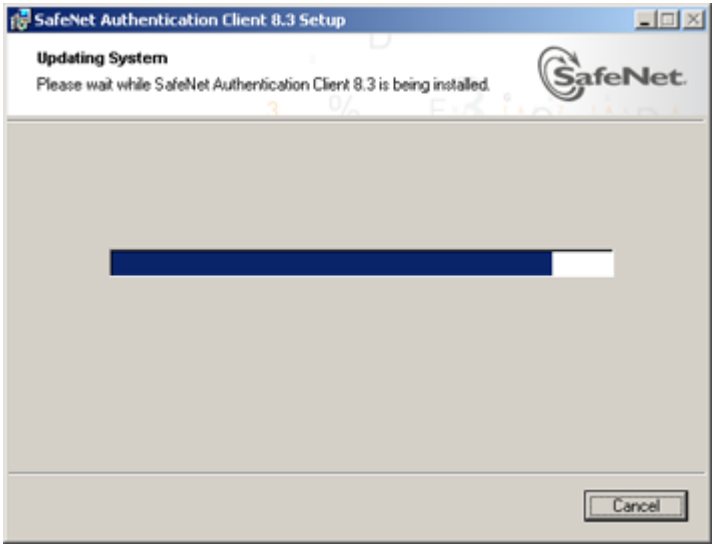
12 You can click **Browse** to select a different destination folder, or install the *SAC* application into the default folder:
`C:\Program Files\SafeNet\Authentication\`

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.

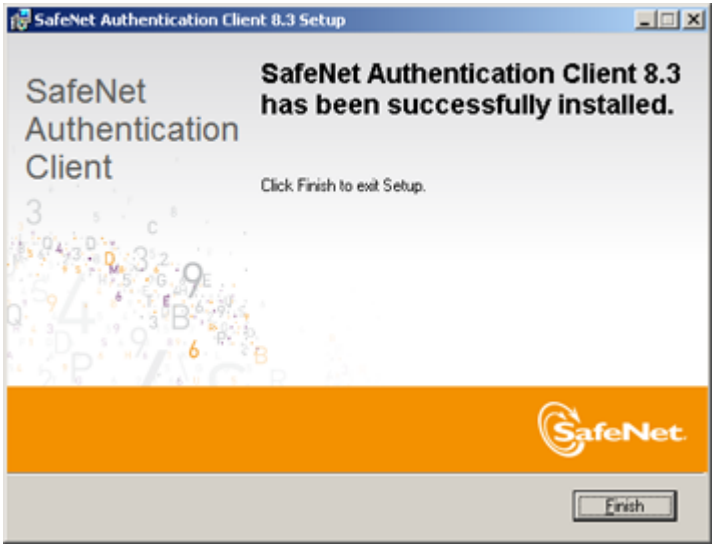
This folder will be used as the installation library for all future SafeNet Authentication applications.

13 Click **Next**.

The installation proceeds.



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



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

Installing 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-x32-8.3.msi`
- for 64-bit systems:
  `msiexec /i SafeNetAuthenticationClient-x64-8.3.msi`

NOTE
Ensure that all legacy eToken Properties or SafeNet Authentication Client Tools 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.
- Open the *Apps* screen, and then swipe or scroll to the right to locate the *Windows System* section heading. Under *Windows System*, right click **Command Prompt**, and select **Run as administrator**.

4 Type the `msiexec` command with the appropriate parameters, properties, and feature settings, as described in this chapter.

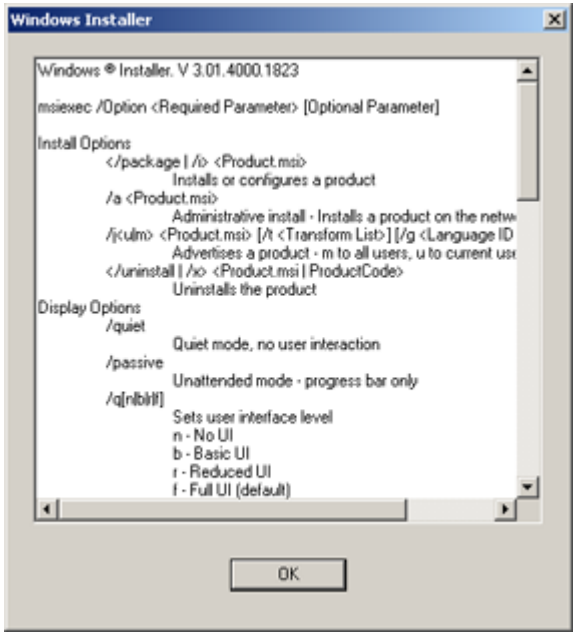
Viewing Command Line Parameters

To view optional parameters for the msiexec command:

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

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

The *Windows Installer* opens, displaying the available parameters and their explanations.



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:

- For 32-bit systems:
  `msiexec /i SafeNetAuthenticationClient-x32-8.3.msi /qn`
- For 64-bit systems:
  `msiexec /i SafeNetAuthenticationClient-x64-8.3.msi /qn`

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

Setting Application Properties via the Command Line

During 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 9: *Application Properties Hierarchy*, on page 158.

NOTE
The *PROP_REG_FILE* property, described on page 94, can be written to a different registry location. Its location is determined by the parameters set when the Policy Migration Tool runs.

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-x32-8.3.msi PROPERTY=VALUE PROPERTY=VALUE /qb
  ```
- For 64-bit systems:
  ```
  msiexec /i SafeNetAuthenticationClient-x64-8.3.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* table on page 88 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 163.

Some properties can be set during command line installation only, and cannot be modified afterward. These properties are described in the *Installation-Only Properties* section on page 90.

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-x32-8.3.msi
ET_LANG_NAME=Spanish
PROP_ADVANCED_VIEW=0
PROP_CLEAR_REG=1 /qb
```

Command Line Installation Properties

Property	Description
ET_LANG_NAME	on page 90
KSP_ENABLED	on page 90
PROP_ADVANCED_VIEW	on page 185
PROP_CLEAR_REG	on page 92
PROP_ETOKENREADERCOUNT	on page 92
PROP_EXPLORER_DEFENROL	on page 207
PROP_FAKEREADER	on page 92

Property	Description
PROP_IKEYREADERCOUNT	on page 93
PROP_LICENSE_FILE	on page 93
PROP_PCSCSLOTS	on page 165
PROP_PQ_HISTORYSIZE	on page 220
PROP_PQ_MAXAGE	on page 219
PROP_PQ_MINAGE	on page 219
PROP_PQ_MINLEN	on page 218
PROP_PQ_MIXCHARS	on page 222
PROP_PQ_WARNPERIOD	on page 220
PROP_PROPAGATECACER	on page 210
PROP_PROPAGATEUSERCER	on page 209
PROP_REG_FILE	on page 94
PROP_SINGLELOGON	on page 163
PROP_SINGLELOGONTO	on page 164
PROP_SOFTWARESLOTS	on page 164
PROP_UPD_INFPATH	on page 95
TARGETDIR	on page 95

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 **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 eToken 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 by the Policy Migration Tool, that is imported to the computer's registry folder during the installation The default registry folder is HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC See *Manual Upgrade of BSec Policies and Registry Settings* on page 65.
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 subfolders of the registry location defined when the *Policy Migration Tool* was run.

See *Manual Upgrade of BSec Policies and Registry Settings* on page 65.

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-x32-8.3.msi ADDDEFAULT=F1,F2…Fn INSTALLLEVEL=n
PROP_IKEYREADERCOUNT=n /qb
```

where

- SafeNetAuthenticationClient-x32-8.3 is the 32-bit SafeNet Authentication Client installation file. For 64-bit systems, use SafeNetAuthenticationClient-x64-8.3.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)
  - 5: BSec-compatible installation
- PROP_IKEYREADERCOUNT=n indicates the number of virtual iKey readers that are installed. (Default is 2.)

See the table *SafeNet Authentication Client Features to Add or Remove* on page 102 for the list of features that can be included during installation.

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

Installing All Features - Example

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

```
msiexec /i SafeNetAuthenticationClient-x32-8.3.msi /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-x32-8.3.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 eToken Virtual readers, and no smartcard reader emulation, type the following command:

```
msiexec /i SafeNetAuthenticationClient-x64-8.3.msi PROP_PCSCSLOTS=10
PROP_ETOKENREADERCOUNT=5 PROP_IKEYREADERCOUNT=3 PROP_SOFTWARESLOTS=2
PROP_FAKEREADER=0 /qb
```

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.

Installing without iKey Drivers - Example

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

```
msiexec /i SafeNetAuthenticationClient-x32-8.3.msi ADDDEFAULT=

eTokenDrivers,etFSFeature,eTokenSAPI,eTokenPKCS11,eTokenCAPI,KSP,SACUI,SACMonitor,SAC
Service,SACTools/qb
```

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

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-x32-8.3.msi ADDDEFAULT=
BsecDrivers,etFSFeature,eTokenSAPI,eTokenPKCS11,eTokenCAPI,SACUI,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-x32-8.3.msi ADDDEFAULT=
eTokenDrivers,BsecDrivers,etFSFeature,eTokenSAPI,eTokenPKCS11,eTokenCAPI,KSP,SACUI,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-x32-8.3.msi ADDDEFAULT=SACTools /qb
```

Installing with BSec-Compatible Configuration - Example

To install SafeNet Authentication Client with CAPI and PKCS#11 for both eToken and BSec on a 32-bit system, type the following command:

```
msiexec /i SafeNetAuthenticationClient-x32-8.3.msi INSTALLLEVEL=5 /qb
```

Where:

`INSTALLLEVEL=5` indicates that the installation is BSec-compatible.

The standard interface is installed by default. For the BSec user interface, configure the BSec UI Compatible setting. (See *Configuring Root Certificate Storage for Windows Server 2008 R2* on page 112.)

To install the BSec Utility applications (SafeNet CIP Utility, SafeNet Token Utility, and SafeNet Token Manager Utility) use `SafeNetAuthenticationClient-BSecUtilities-8.2.msi`

NOTE

SafeNetAuthenticationClient-BSecUtilities-8.2.msi, which installs legacy BSec Utilities that can be used with BSec-compatible SafeNet Authentication Client versions 8.2 and 8.3, is not packaged with SafeNet Authentication Client 8.3. It is provided in the SafeNet Authentication Client 8.2 installation folder.

Future versions of SafeNet Authentication Client may not support BSec-compatibility.

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-x32-8.3.msi REMOVE=F1,F2…,Fn /qb
```

where

- `SafeNetAuthenticationClient-x32-8.3.msi` is the 32-bit SafeNet Authentication Client installation file. For 64-bit systems, use `SafeNetAuthenticationClient-x64-8.3.msi`
- `REMOVE` indicates that the following features are to be removed
- `Fx` is the name of each feature to be removed

See the table: *SafeNet Authentication Client Features to Add or Remove* on page 102 for the list of features.

NOTE
Only optional features can 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-x32-8.3.msi
REMOVE=SACTools /qb
```

Command Line Installation Features

SafeNet Authentication Client Features to Add or Remove

Feature Parent	Feature	Installs	Comment
DriverFeature	eTokenDrivers	eToken drivers	Required for eToken and iKey physical devices.
	BsecDrivers	iKey token drivers	
CoreFeature	etFSFeature	Proprietary file system API	Required. Installs functionality for full operation of SafeNet Authentication Client. Can be installed without DriverFeature (to work with SafeNet eToken Virtual or other readers).
	eTokenSAPI	Proprietary supplementary API	
	eTokenPKCS11	Standard PKCS#11 implementation API for eToken and iKey tokens	
	eTokenCAPI	Standard CAPI implementation for eToken and iKey tokens; requires the eTokenPKCS11 feature to be included	
	KSP	Support for the Smart Card KSP provider; requires the eTokenCAPI feature to be included	
	BsecCAPI	Support for legacy iKey CAPI applications	
	BsecPKCS#11	Support for legacy iKey PKCS#11 applications	

SafeNet Authentication Client Features to Add or Remove (Cont.)

Feature Parent	Feature	Installs	Comment
SACUI (Use both SACUI and SACTools in command line)	SACTools	User interface applications	Optional, but required for SafeNet Authentication Client Tools and SafeNet Authentication Client tray icon application features.
Services	SACMonitor	SafeNet Authentication Client tray icon application (Monitor) for eToken and iKey token support	Required.
	SACService	SACService for eToken and iKey token support	
Extensions	Identrust	IdenTrust support	Optional. Installs IdenTrust software required for iKey device support.
	Entrust	SafeNet Authentication Client PKCS#11 provider to the Entrust configuration	Optional. Applicable to Entrust ESP Clients only.

SafeNet Authentication Client Features to Add or Remove (Cont.)

Feature Parent	Feature	Installs	Comment
UI_BSEC	x32 SafeNet Common Utilities	SafeNet Common Utilities	BSec-compatible features. UI_BSEC features are installed via SafeNetAuthenticationClient-BSecUtilities-8.2.msi
	SafeNetTokenManagerUtility	SafeNet Token Manager Utility application for iKey token support	
	SafeNetTokenUtilities	SafeNet Token Utilities application for iKey token support	
	SafeNetCIPUtilities	SafeNet CIP Utilities application for iKey token support	

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 the BSec Utility Package

If required, BSec-compatibility can be installed. See *Installation Configurations* on page 71.

There is no new release of the BSec Utility package for version 8.3. Continue to use *BSec Compatibility Utilities Package 8.2*.

The BSec Utilities package includes the following components:

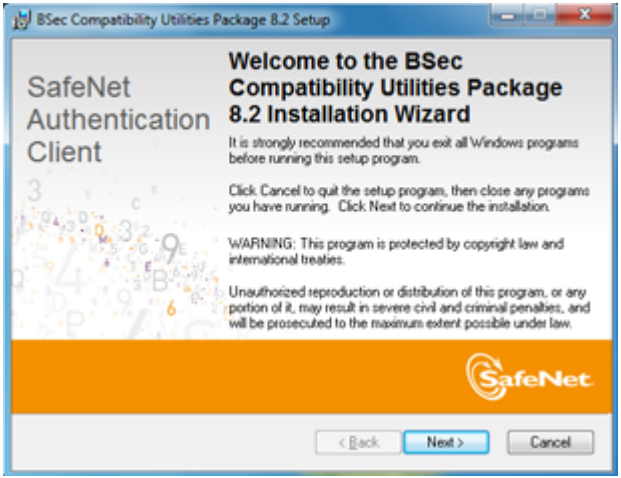
- SafeNet CIP Utilities
- SafeNet Token Utilities
- SafeNet Token Manager Utility

To install the BSec Utilities package:

> **NOTE**
> SafeNetAuthenticationClient-BSecUtilities-8.2.msi, which installs legacy BSec Utilities that can be used with BSec-compatible SafeNet Authentication Client versions 8.2 and 8.3, is not packaged with SafeNet Authentication Client 8.3. It is provided in the SafeNet Authentication Client 8.2 installation folder.
> Future versions of SafeNet Authentication Client may not support BSec-compatibility.

1. Install SafeNet Authentication Client with the BSec-compatible configuration. See *Installation Configurations* on page 71.
2. In the software package provided by SafeNet, double-click `SafeNetAuthenticationClient-BSecUtilities-8.2.msi`.

The *BSec Compatibility Utilities Package Setup Installation Wizard* opens.

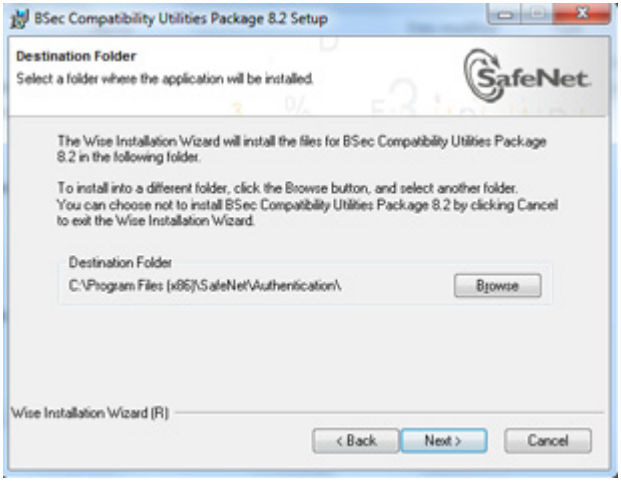


3 Click **Next**.

The *End-User License Agreement* window opens.

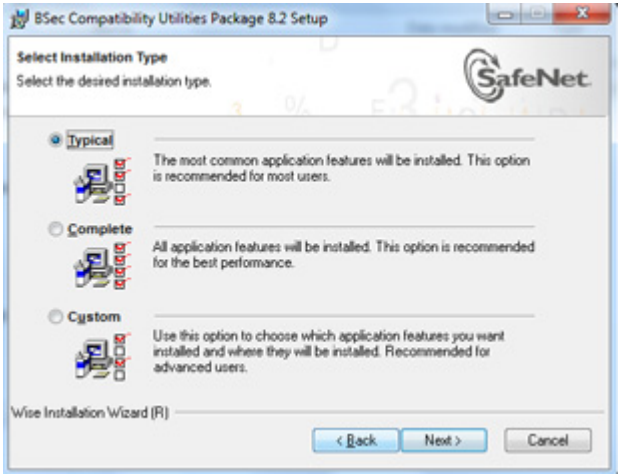
4 Select **I accept the license agreement** and click **Next**.

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



5 Click **Next**.

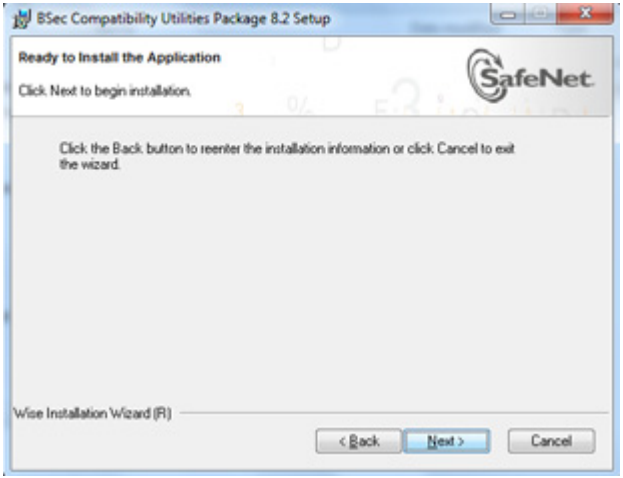
The *Select Installation Type* window opens.



6 Select the required installation type and click **Next**:

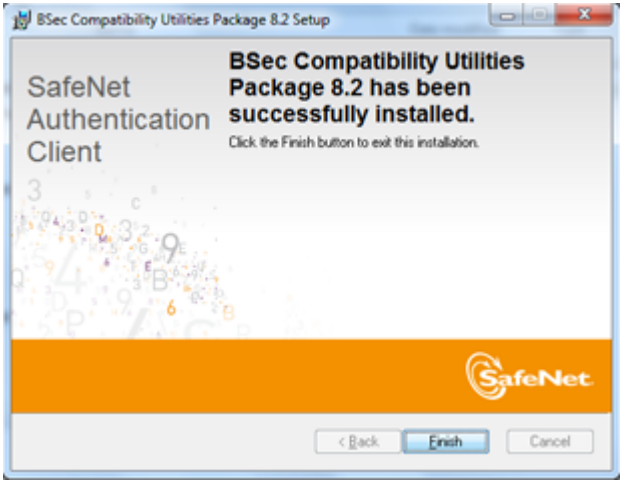
- **Typical -** installs *SafeNet Token Manager Utility* only
- **Complete** - installs all components
- **Custom** - select which components to install

The *Ready to Install the Application* window opens.



7 Click **Next** to start the installation.

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



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

Configuring Root Certificate Storage for Windows 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`

   NOTE
   For more information about creating and editing registry keys, see *Setting Registry Keys Manually* on page 160.

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.

7 Uninstall

After SafeNet Authentication Client 8.3 has been installed, it can be uninstalled. Local administrator rights are required to uninstall SafeNet Authentication Client.

In this chapter:

Uninstall Overview

If iKey tokens remain connected while SafeNet Authentication Client is being uninstalled, you will be prompted to remove the iKey tokens before uninstalling the SafeNet iKey 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 116
- *Uninstalling via the Command Line* on page 117

NOTE
Ensure that all legacy eToken Properties and SafeNet Authentication Client Tools applications are closed before upgrading, installing, or uninstalling SafeNet Authentication Client.

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.

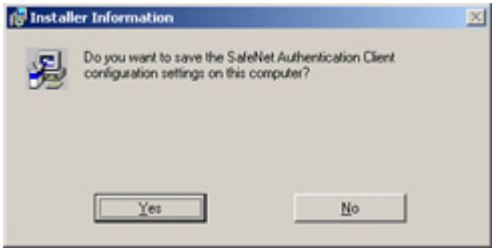
NOTE
If a DLL is in use by another application, a *Files in Use* message is displayed. Click **Ignore** to continue the uninstall, and when the uninstall completes, restart the computer.

Uninstalling 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 8.3**, 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**.

   When running on Windows Vista, right-click **Command Prompt**, and select **Run as**. Set the user to administrator.
4. Type the appropriate command line utility:

   `msiexec /x SafeNetAuthenticationClient-x32-8.3.msi` (for 32-bit installations)

   `msiexec /x SafeNetAuthenticationClient-x32-8.3.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.

Clearing Legacy Registry Settings

If the registry settings set by an eToken PKI Client or SafeNet Authentication Client installation were not cleared during the uninstall, you can clear them manually.

To clear all registry settings set by eToken PKI Client or SafeNet Authentication Client:

1. Install SafeNet Authentication Client 8.3 using the wizard. See *Installing via the Wizard* on page 75.
2. If computer and user registry settings from the earlier installation are detected, a **Use the existing configuration settings** option appears on the *Select interface language* window. See step 6 of *Installing via the Wizard* on page 77.
3. Clear the **Use the existing configuration settings** option, and continue the installation.
4. Uninstall SafeNet Authentication Client 8.3.

8 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

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.

*S*ample Administrative Template files provided by SafeNet:

Sample File	Configuration
SAC_8_3.adm	SafeNet Authentication Client settings
SAC_8_3.admx	SafeNet Authentication Client settings
SAC_8_3.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, such as Windows XP or Vista, 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 158 for an explanation of the registry folders.

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

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 2003 or Windows Server 2003 R2, see *Adding an ADM file to Windows Server 2003 / R2* on page 122.
- 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 129.
  - Add an XML-based ADMX Administrative Template file. See *Adding an ADMX file to Windows Server 2008 / R2* on page 135.
- To add the Administrative Templates to a client computer, see *Adding an ADM file to a Client Computer* on page 136.

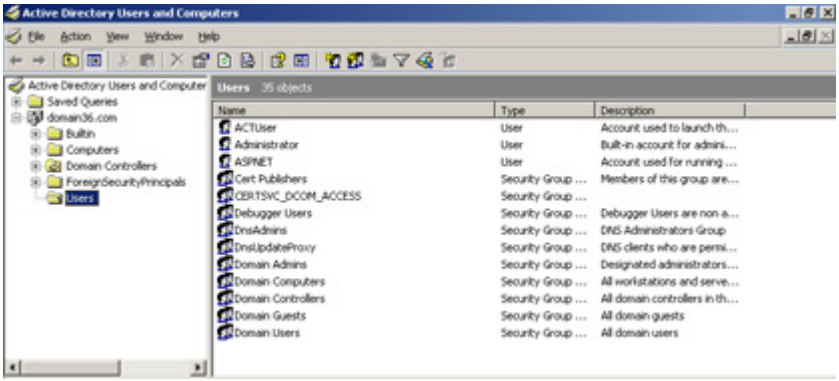
Adding an ADM file to Windows Server 2003 / R2

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:

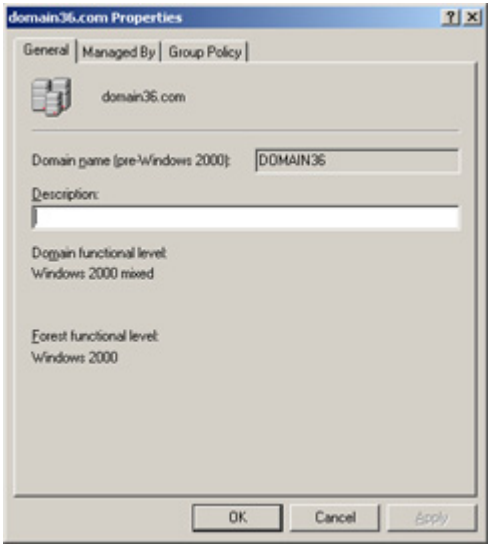
1 From the Windows taskbar, select **Start > Programs > Administrative Tools > Active Directory Users and Computers.**

The *Active Directory Users and Computers* window opens.

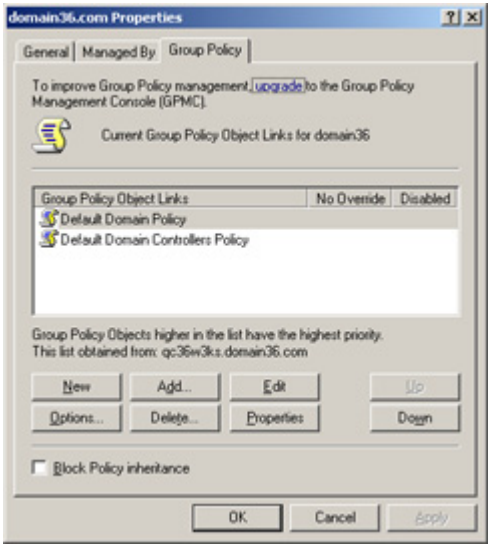


2 In the left pane, right-click the domain node, and select **Properties.**

The *Properties* window opens.



3 Select the *Group Policy* tab.

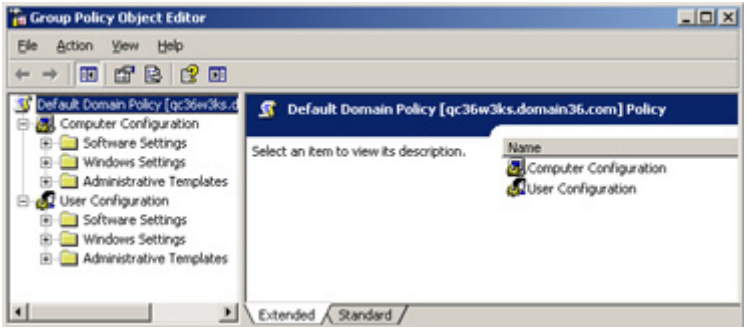


4 Do one of the following:

- To propagate the settings to all clients in the domain, select **Default Domain Policy**.
- To apply the settings to the local machine and any other domain controllers in this domain, select **Default Domain Controllers Policy**.

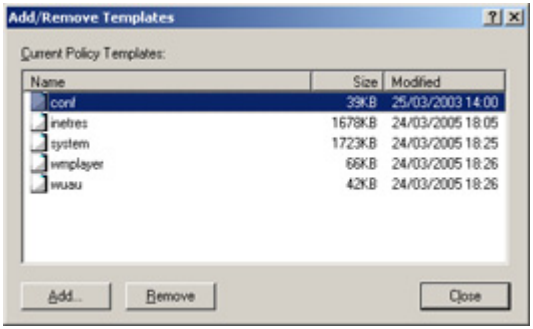
5 Click **Edit**.

The *Group Policy Object Editor* opens.



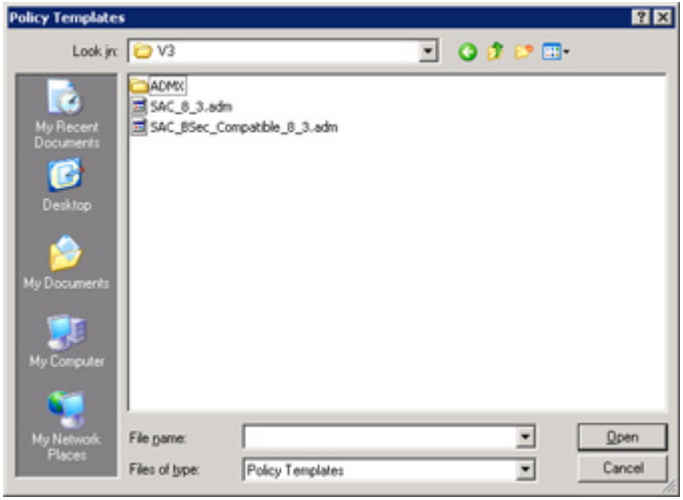
6 Under the **Computer Configuration** node, right-click **Administrative Templates**, and select **Add/Remove Templates.**

The *Add/Remove Templates* window opens.



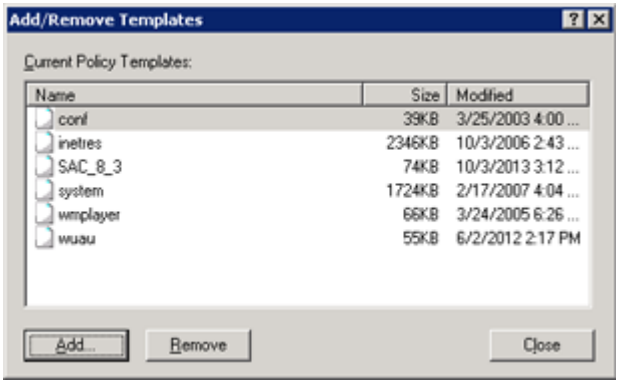
7 Click **Add**, and browse to the appropriate ADM file.

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



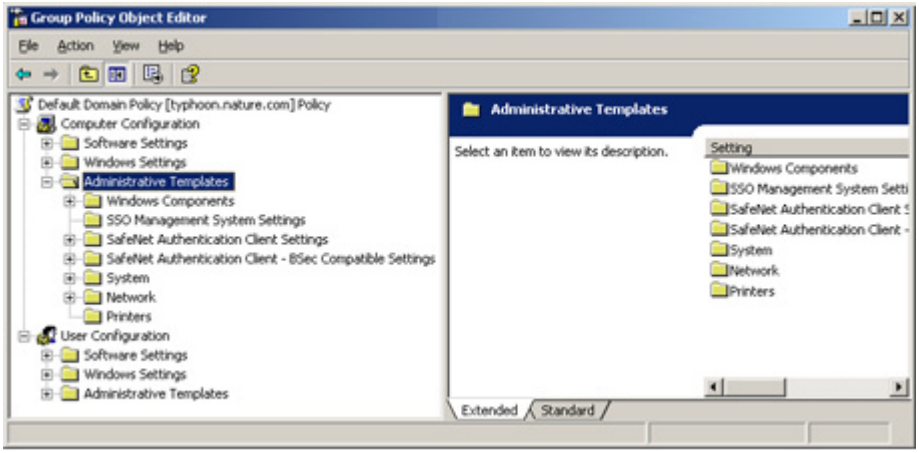
8 Select the file, and click **Open.**

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



9 Click **Close.**

In the *Group Policy Object Editor* window, the *Settings* node is added under **Administrative Templates**.



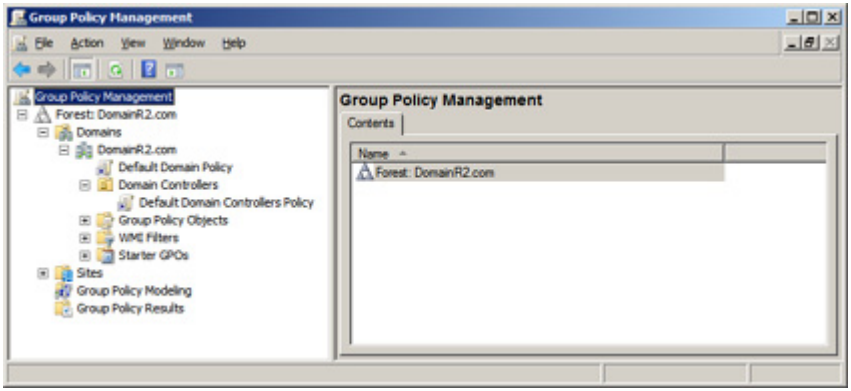
Adding an ADM file to Windows Server 2008 / R2

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.

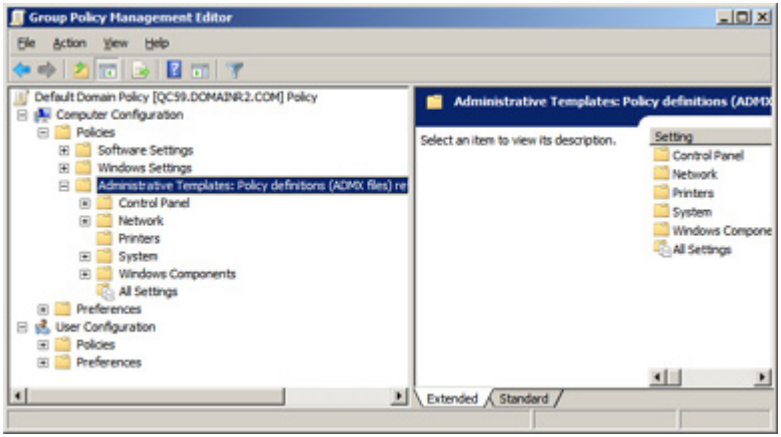


3 Do one of the following:

- 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.

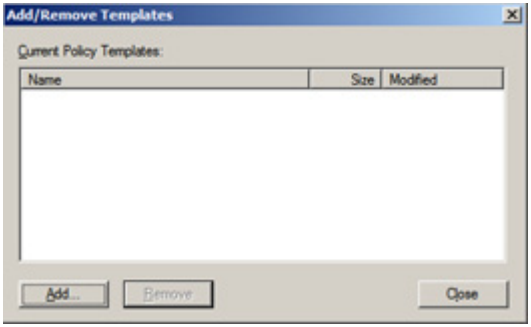
4 From the dropdown menu, select **Edit**.

The *Group Policy Management Editor* opens.



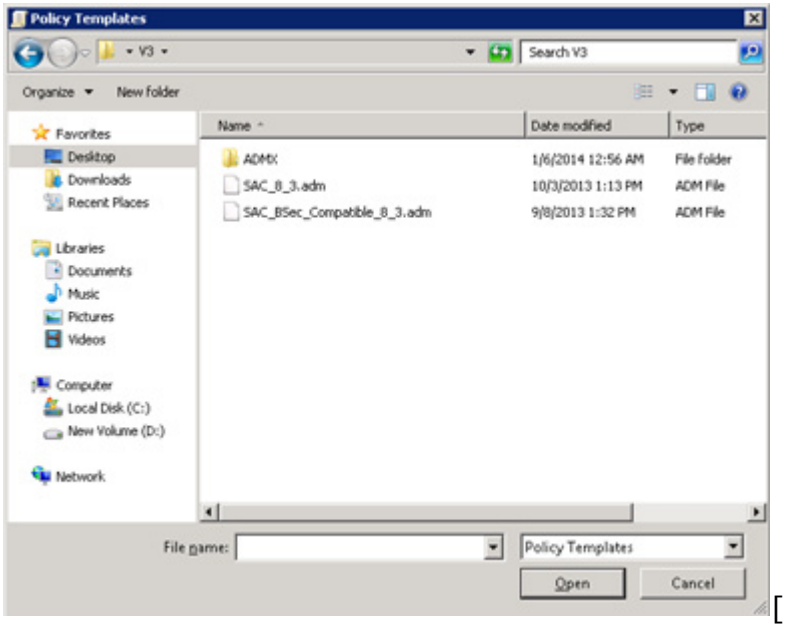
5 Under **Computer Configuration > Policies**, right-click **Administrative Templates: Policy definitions (ADMX files)**, and select **Add/Remove Templates.**

The *Add/Remove Templates* window opens.



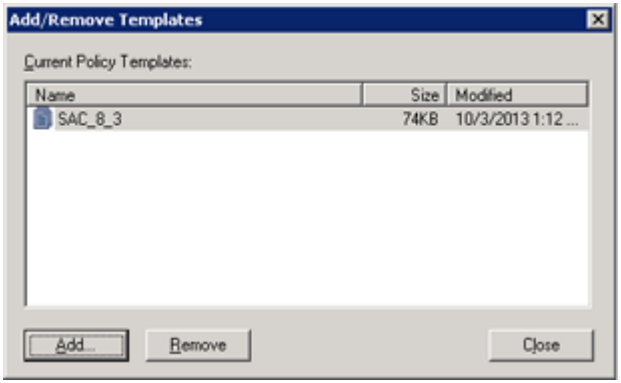
6 Click **Add**, and browse to the appropriate ADM file.

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



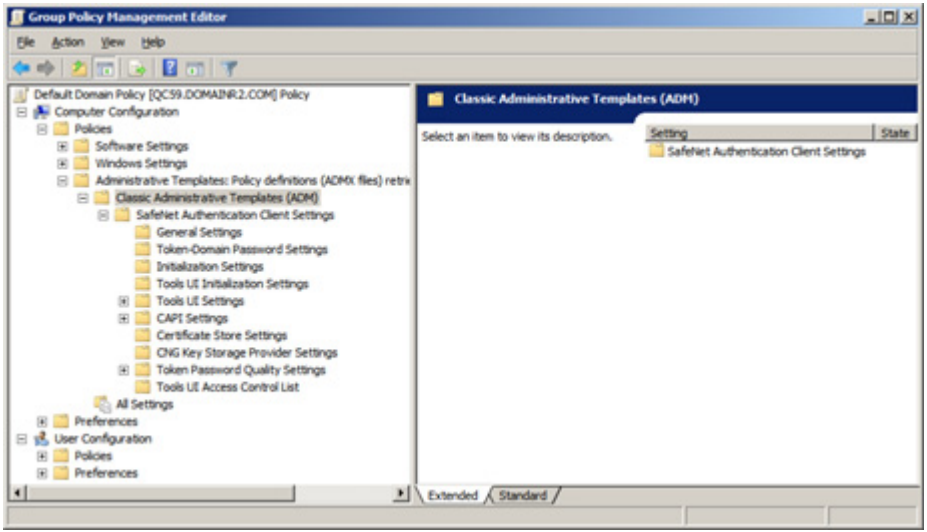
7 Select the file, and click **Open.**

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_8_3.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_8_3.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

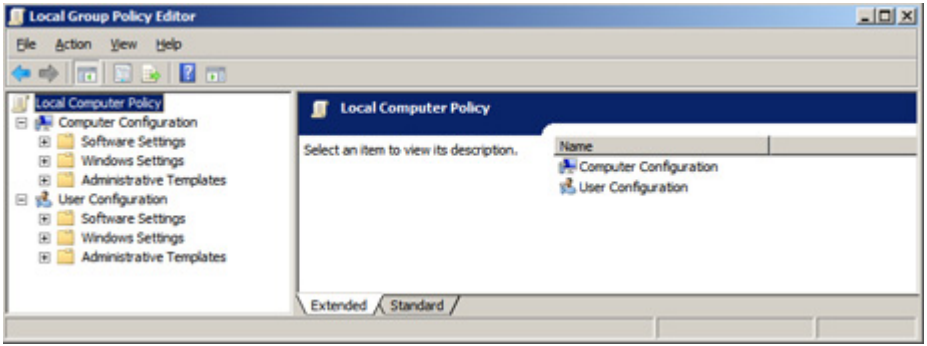
Adding an ADM file to a Client Computer

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

To add SafeNet Authentication Client settings:

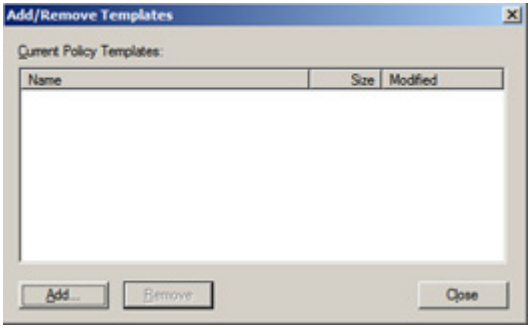
1. From the Windows taskbar, select **Start > Run**.
2. In the *Run* dialog box, enter **gpedit.msc**, and click **OK**.

   The *Local Group Policy Editor* opens.



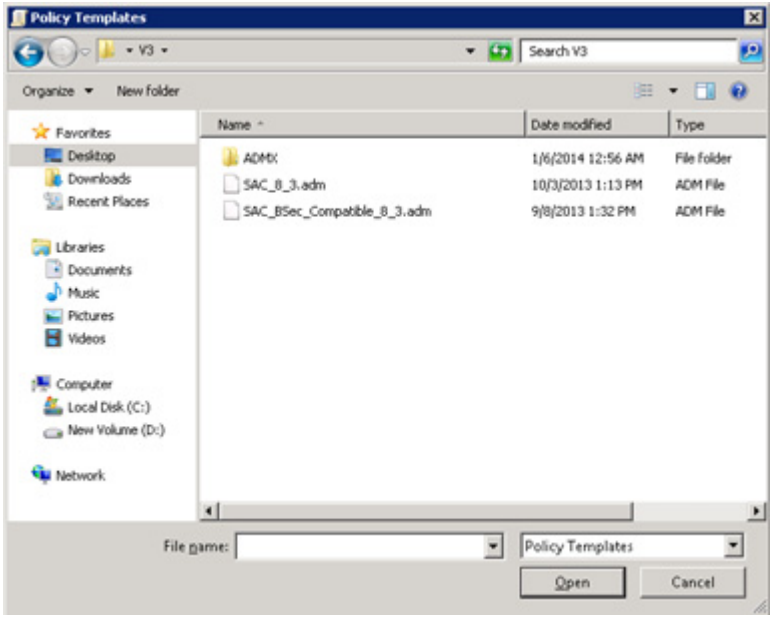
3 Under the **Computer Configuration** node, right-click **Administrative Templates**, and select **Add/Remove Templates.**

The *Add/Remove Templates* window opens.



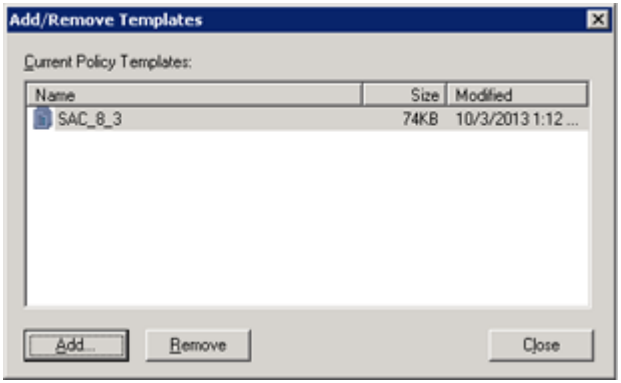
4 Click **Add**, and browse to the appropriate ADM file.

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



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

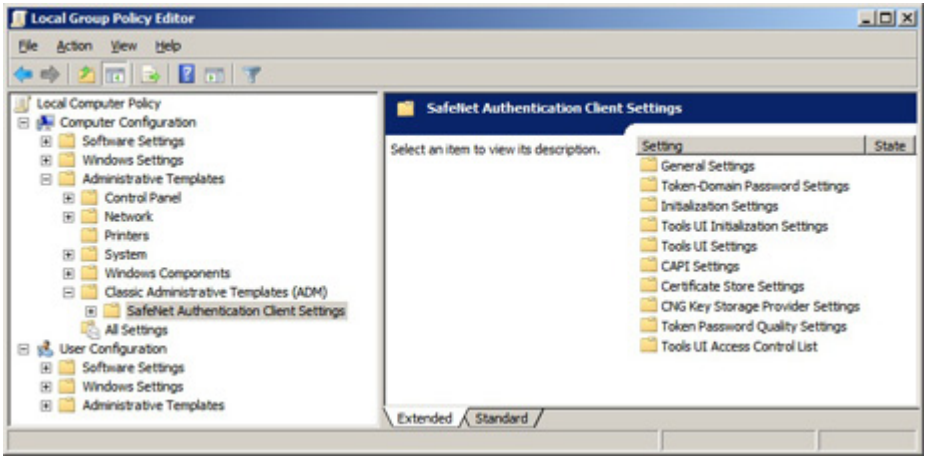
The selected template file is displayed in the *Add/Remove Templates* window.



6 Click **Close.**

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

> **NOTE**
> In Windows XP, the Settings node is added under Administrative Templates.


Local Group Policy Editor
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
Control Panel
Network
Printers
System
Windows Components
Classic Administrative Templates (ADM)
SafeNet Authentication Client Settings
All Settings
User Configuration
Software Settings
Windows Settings
Administrative Templates
SafeNet Authentication Client Settings
Select an item to view its description.
Setting
State
General Settings
Token-Domain Password Settings
Initialization Settings
Tools UI Initialization Settings
Tools UI Settings
CAPI Settings
Certificate Store Settings
CNG Key Storage Provider Settings
Token Password Quality Settings
Tools UI Access Control List
Extended
Standard

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 155.

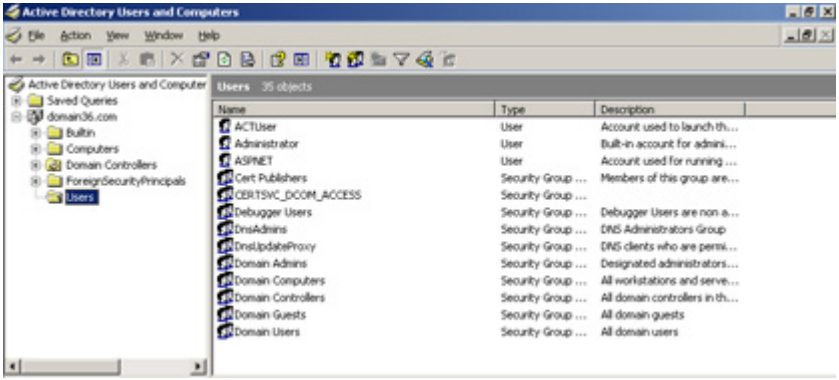
- To edit the policy settings on Windows Server 2003 or Windows Server 2003 R2, see *Editing Settings in Windows Server 2003 / R2* on page 141.
- To edit the policy settings on Windows Server 2008 or Windows Server 2008 R2, see *Editing Settings in Windows Server 2008 / R2* on page 150.
- To edit the policy settings on a client computer, see *Editing Settings on a Client Computer* on page 152.

Editing Settings in Windows Server 2003 / R2

To edit SafeNet Authentication Client settings:

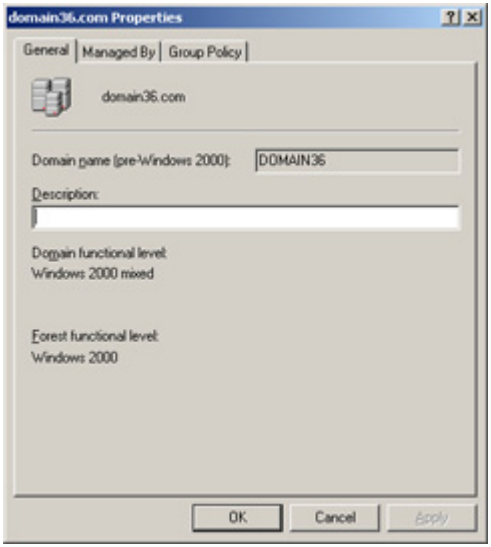
1 From the Windows taskbar, select **Start > Programs > Administrative Tools > Active Directory Users and Computers.**

The *Active Directory Users and Computers* window opens.

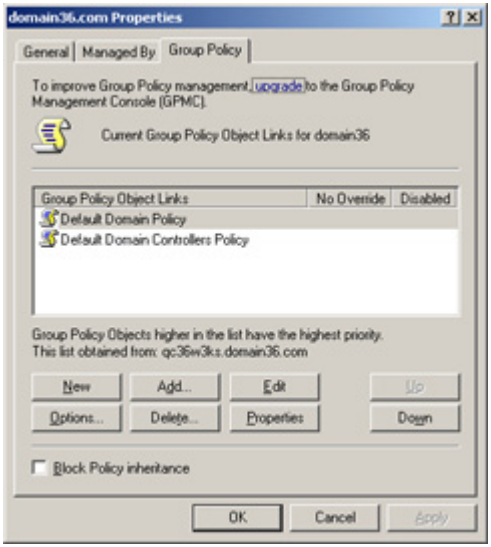


2 In the left pane, right-click the domain node, and select **Properties.**

The *Properties* window opens.



3 Select the *Group Policy* tab.

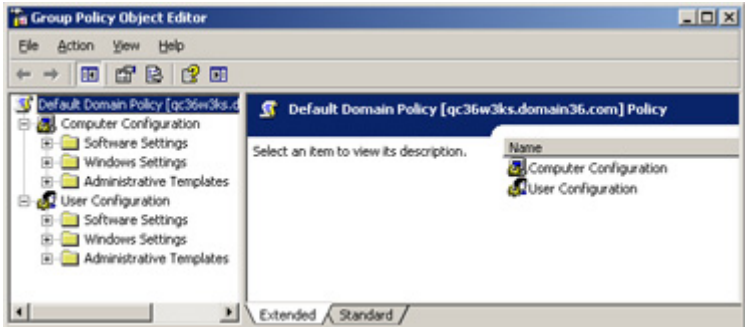


4 Do one of the following:

- To propagate the settings to all clients in the domain, select **Default Domain Policy**.
- To apply the settings to the local machine and any other domain controllers in this domain, select **Default Domain Controllers Policy**.

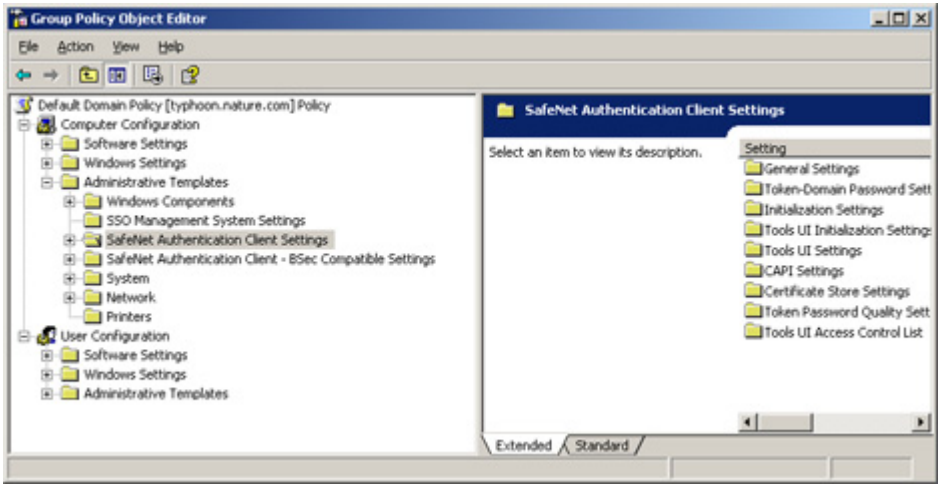
5 Click **Edit**.

The *Group Policy Object Editor* opens.



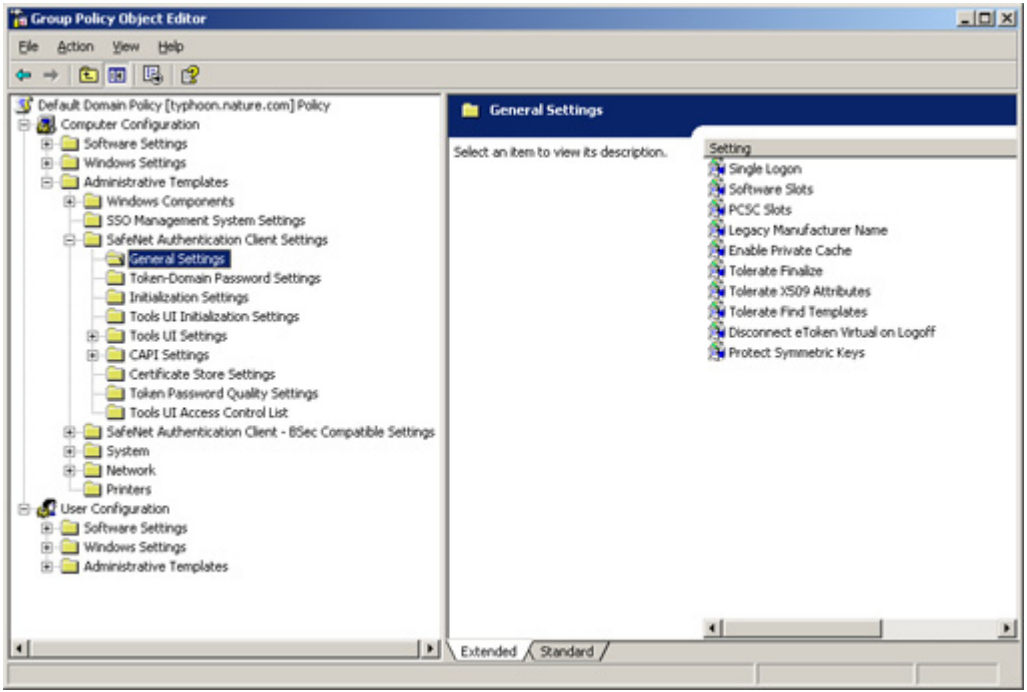
6 In the left pane, navigate to **Computer Configuration > Administrative Templates**, and select one of the **SafeNet Authentication Client Settings** nodes.

7 The *Settings* folders are displayed in the right pane.



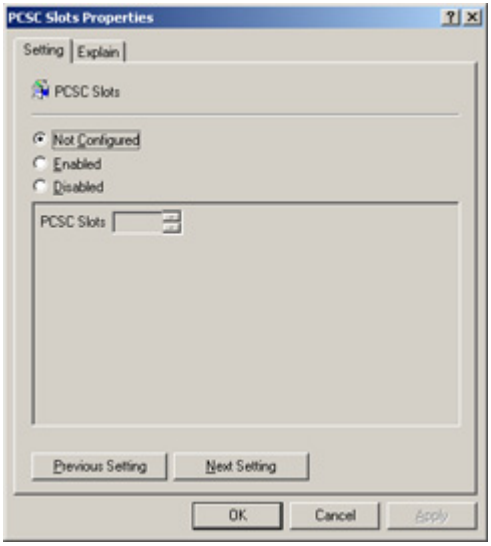
8 Select the settings folder to edit.

The settings are displayed in the right pane.



9 Double-click the setting to edit.

In this example, the *PCSC Slots* setting is selected.



10 Select the *Explain* tab for an explanation of the setting and its values.

For more information on each setting, see Chapter 9: *Configuration Properties*, on page 155.

11 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.

> **NOTE**
> For more information on these options, see Microsoft documentation.

12 If **Enabled** is selected, complete the values in the box.

13 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.

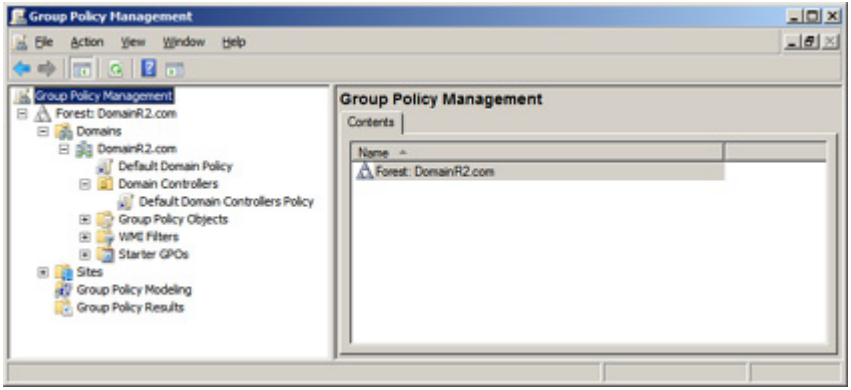
The registry is updated.

Editing Settings 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.

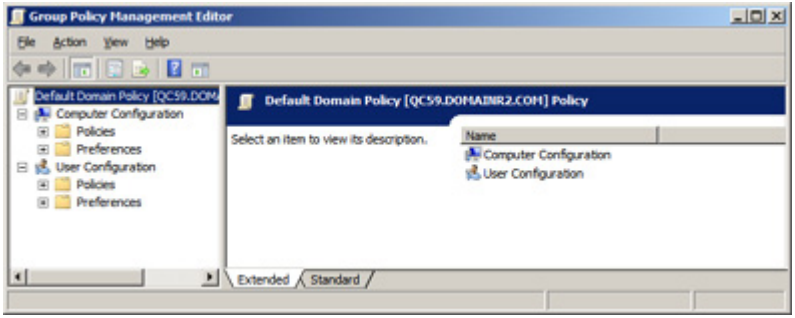


3 Do one of the following:

- 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.

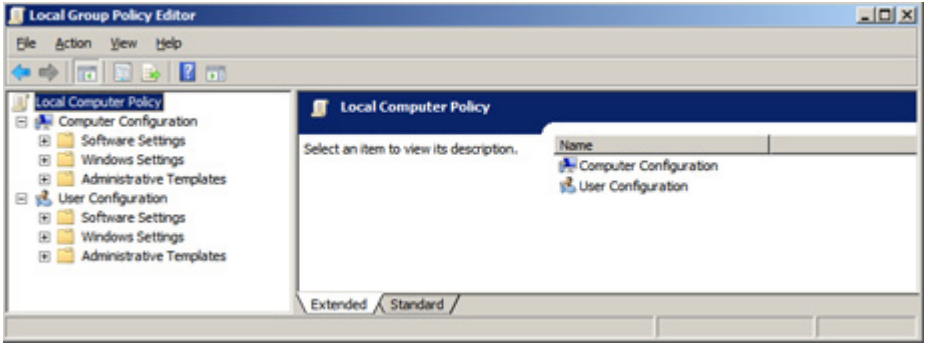
7 Continue from *Editing Settings in Windows Server 2003 / R2* step 8, on page 146.

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.

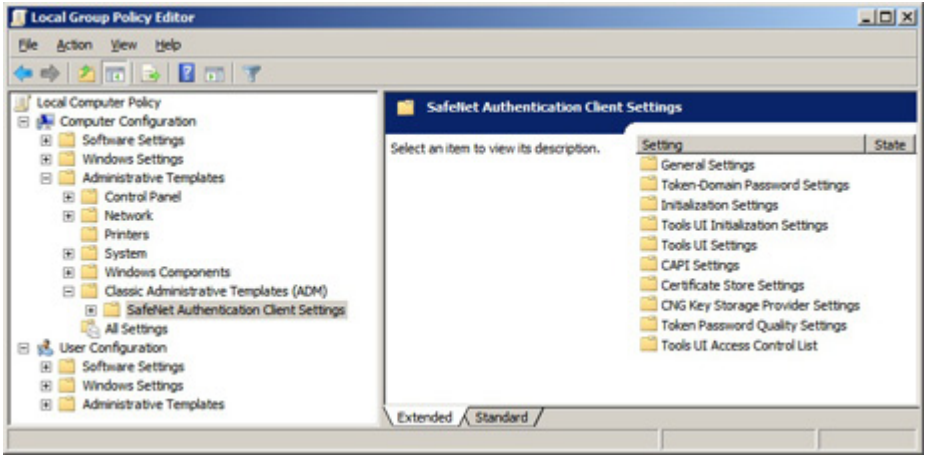


3. In the left pane, navigate to **Computer Configuration > Administrative Templates > Classic Administrative Templates**.

   NOTE
   In Windows XP, navigate to 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 2003 / R2* step 8, on page 146.

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.

9 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:

- 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
- SafeNet Authentication Client - BSec-Compatible Settings
- Security Settings
- SafeNet Authentication Client Security Enhancements
- 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 via the Command Line* on page 83.
  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 8: *SafeNet Authentication Client Settings*, on page 119.
  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 160.
  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_CURRENT_USER\SOFTWARE\SafeNet\Authentication\SAC`
   Does not require administrator permissions.
4. `HKEY_LOCAL_MACHINE\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 <Emphasis>Hierarchy List on page 158. 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**.

7 Right-click the key in which the value belongs, and select the type of value to be assigned.
In this example, select **New > DWORD value**.

8 Assign the appropriate setting name and value to the new key.
In this example, assign it the name **SingleLogon**, and to enable the feature, set the DWORD value to **1**.

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	**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

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
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.	Single Logon Timeout is set in the Single Logon setting. (See "Single Logon" entry above.)	**Registry Value Name:** SingleLogonTimeout **Value**: >=0 **Default**: 0 (no timeout)	Property name: PROP_SINGLELOGONTO
Software Slots Defines the number of virtual readers for SafeNet eToken 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 eToken Virtual is disabled; only physical tokens are enabled) **Default**: 2	**Registry Value Name:** SoftwareSlots **Values**: >=0 (0 = SafeNet eToken Virtual is disabled; only physical tokens are enabled) **Default**: 2	Property name: PROP_SOFTWARESLOTS

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
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 eToken Virtual is enabled) **Default**: 8	**Registry Value Name:** PcscSlots **Values**: >=0 (0 = Physical tokens are disabled; only SafeNet eToken Virtual is enabled) **Default**: 8	Property name: PROP_PCSCSLOTS

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.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Tolerate Finalize Determines if C_Finalize can be called by DllMain **Note:** Define this property per process Select this setting when using Novell Modular Authentication Service (NMAS) applications only	**Setting name:** Tolerate Finalize Values: **Selected** - C_Finalize can be called by DllMain **Not selected** - C_Finalize cannot be called by DllMain **Default**: Not selected	**Registry Value Name:** TolerantFinalize **Values**: **1 (True)** - C_Finalize can be called by DllMain **0 (False)** - C_Finalize cannot be called by DllMain **Default**: 0 (False)	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 eToken Virtual on Logoff Determines if SafeNet eToken Virtual tokens are disconnected when the user logs off.	**Setting name:** Disconnect eToken Virtual on Logoff Values: **Selected** - Disconnect eToken Virtual when logging off **Not selected** - Do not disconnect eToken Virtual when logging off **Default**: Not selected	**Registry Value Name:** EtvLogoffUnplug **Values**: **1 (True)** - Disconnect eToken Virtual when logging off **0 (False)** - Do not disconnect eToken Virtual when logging off **Default**: 0 (False)	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
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 IdenTrust OID details, remove the OID value from the registration key value.	**Setting name:** Override Non-Repudiation OIDs **Value**: All OID values of non-repudiation certificates, separated by commas **Default**: No override	**Registry Value Name:** NonRepudiationOID **Value**: All OID values of non-repudiation certificates, separated by commas **Default**: No override	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
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 93.

Initialization Settings

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

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**: 0-15 (0 = no retries) **Default**: 15	**Registry Value Name:** UserMaxRetry **Values**: 0-15 (0 = no retries) **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**: 0-15 (0 = no retries) **Default**: 15	**Registry Value Name:** AdminMaxRetry **Values**: 0-15 (0 = no retries) **Default**: 15	Cannot be set by command line installation.

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

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

Description	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
Default Token Name Defines the default Token Name written to tokens during initialization.	**Setting Name**: Default Token Name **Value**: String **Default**: My Token	**Registry Value Name:** DefaultLabel **Value**: String **Default**: My Token	Cannot be set by command line installation.
API: Keep Token Settings When initializing the token using the SDK, determines if the token is automatically re-initialized with its current settings. **Note:** If selected, this setting overrides all other initialization settings.	**Setting Name:** API: Keep Token Settings Values: **Selected** - Use current token settings **Not selected** - Override current token settings **Default:** Not selected	**Registry Value Name:** KeepTokenInit Values: **1 (True) -** Use current token settings **0 (False) -** Override current token settings **Default**: 0 (False)	Cannot be set by command line installation.

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

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

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

Description	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line (Cont.)
Enable RSA Secondary Authentication Modified Determines if the token's RSA secondary authentication can be modified after initialization.	**Setting Name:** Enable RSA Secondary Authentication Modified Values: **Selected** -Can be modified **Not selected** -Cannot be modified **Default:** Not selected	**Registry Value Name:** 2ndAuthModify Values: **1 (True) -** Can modify **0 (False) -** Cannot modify **Default**: 0 (False)	Cannot be set by command line installation.

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.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
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.	**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.	**Setting Name:** RSA Secondary Authentication Mode Values: **Never** - New RSA private keys are not protected with an additional password. **Prompt user on application request** - If the key generation application requires key passwords to be created for strong private key protection, new RSA private keys must be protected with an additional password. If the key generation application does not require strong private key protection, new RSA private keys are not protected with an additional password. **Always prompt user** - A prompt appears asking if a new RSA private key is to be protected with an additional password. **Always** - New RSA private keys must be protected with an additional password.	**Registry Value Name:** RSASecondaryAuthentication Mode Values: **0** - Never **1** - Prompt user on application request **2** - Always prompt user **3** - Always **4** - Token authentication on application request **Default**: **0**	Cannot be set by command line installation

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
RSA Secondary Authentication Mode (continued)	**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**: 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.	**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.	**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	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.

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

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Enable Tray Icon Determines if the application tray icon is displayed when SafeNet Authentication Client is started.	**Setting Name:** Enable Tray Icon **Values**: Never show Always show **Default**: Always show	**Registry Value Name**: ShowInTray **Values**: **0** - Never Show **1 -** Always Show **Default**: Always show	Cannot be set by command line installation.
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.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
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:** IKeyLEDOn **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 Loggin*g */Disable Logging* button is enabled in the Client Settings Advanced tab	**Setting Name:** Enable Logging Control **Values**: **Selected** -Enabled **Not selected** -Disabled **Default**: Selected	**Registry Value Name:** AllowLogsControl **Values**: **1** -Enabled **0** -Disabled **Default**: 1	Cannot be set by command line installation.
Home URL Overwrites the SafeNet home URL in SafeNet Authentication Client Tools	**Setting Name:** Home URL **Values**: Valid URL **Default**: SafeNet's home URL	**Registry Value Name:** HomeUrl **Values** (String): Valid URL **Default**: SafeNet's home URL	Cannot be set by command line installation.

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

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Ignore Expired Certificates Determines if expired certificates are ignored, and no warning message is displayed for expired certificates	**Setting Name:** Ignore Expired Certificates **Values**: **Selected** -Expired certificates are ignored **Not selected**- A warning message is displayed if the token contains expired certificates **Default**: Not selected	**Registry Value Name:** IgnoreExpiredCertificates Values: **1** - Expired certificates are ignored **0** - A warning message is displayed if the token contains expired certificates **Default**: 0	Cannot be set by command line installation.
Certificate Expiration Verification Frequency Defines the minimum interval, in days, between certificate expiration date verifications	**Setting Name:** Certificate Expiration Verification Frequency **Values**: > 0 **Default**: 14 days	**Registry Value Name:** UpdateAlertMinInterval **Values**: > 0 **Default**: 14 days	Cannot be set by command line installation.

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

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Warning Message Click Action Defines what happens when the user clicks the message balloon.	**Setting Name:** Warning Message Click Action **Values**: n No action n Show detailed message n 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.

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

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

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

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, eToken Virtual tokens - 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.

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

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

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Sign Padding On-Board Determines if sign padding is performed on-board supported devices for added security. Sign padding is supported by Java tokens. **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 Manager. **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

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Default Enrollment Type Determines if the administrator token's latest Enrollment Agent certificate must be the certificate used to enroll a new certificate on the user's token. This feature applies when "Enrollment on Behalf" uses a certificate on an administrator token and not on a computer. **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

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

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Remove Certificates from Store upon Token Disconnect When an exported certificate is removed from the token, determines if that certificate is removed from the user store.	**Setting Name:** Remove Certificates upon Removal from Token **Values**: **Selected** - The certificate is removed from the user store **Not selected** - The certificate is not removed from the user store **Default**: Selected	**Registry Value Name:** RemoveFromStoreOnRemoveFromToken **Values**: **1 (True)** - The certificate is removed from the user store **0 (False)** - The certificate is not removed from the user store **Default**: 1 (True)	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.

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

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Certificate Removal Period When an exported certificate is removed from the user store, defines the number of days to attempt to remove that certificate from a token that is not connected Relevant only when the setting *Remove Certificates from Token upon Removal from Store (RemoveFromTokenOnRemoveFromStore)* is set to **Always** or **Template dependent**.	**Setting Name:** Certificate Removal Period **Values**: >=0 **Default**: 7	**Registry Value Name:** CertsToRemoveStorePeriod **Values**: >=0 **Default**: 7	Cannot be set by command line installation.
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.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Import CA Certificates Chain When SAC Tools imports a user certificate from a P12/PFX file, determines if the CA chain is also imported to the token.	**Setting Name:** Import CA Certificates Chain **Values**: **Selected** - CA chain is imported to the token **Not selected** - CA chain is not imported **Default**: Selected	**Registry Value Name:** ImportUserCertCAChain **Values**: **1 (True)** - CA chain is imported to the token **0 (False)** - CA chain is not imported **Default**: 1 (True)	Cannot be set by command line installation.

CNG Key Storage Provider Settings

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

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

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.	**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 91.

Token Password Quality Settings

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

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.

Description (Cont.)	Settings in GPO Editor or MMC (Cont.)	Registry Key (Cont.)	Command Line (Cont.)
Password - Maximum Usage Period Defines the maximum number of days a password is valid. **Note:** Can be set in SafeNet Authentication Client Tools.	**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

Description (Cont.)	Settings in GPO Editor or MMC (Cont.)	Registry Key (Cont.)	Command Line (Cont.)
Password - Maximum Consecutive Repetitions Defines the maximum number of consecutive times a character can be used in a password. **Note:** Can be set in SafeNet Authentication Client Tools. **Note:** Does not apply to iKey devices.	**Setting Name:** Password - Maximum Consecutive Repetitions **Values**: 0 - 16 (0 = No maximum) **Default**: 3	**Registry Key Name:** pqMaxRepeated **Values**: 0 - 16 (0 = No maximum) **Default**: 3	Cannot be set by command line installation.

Description (Cont.)	Settings in GPO Editor or MMC (Cont.)	Registry Key (Cont.)	Command Line (Cont.)
Password - Complexity Determines if there is a minimum number of character types that must be included in a new Token Password The character types are: upper-case letters, lower-case letters, numerals, and special characters. **Note:** Can be set in SafeNet Authentication Client Tools.	**Setting Name:** Password - Complexity **Values**: **Standard complexity** - A minimum of 2 or 3 types must be included, as defined in the *Password- Minimum Mixed Character Type*s setting **Manual complexity** - The rule for each character type is defined in the character type's *Include* setting **Default**: Standard complexity	**Registry Key Name:** pqMixChars **Values**: **1** - A minimum of 2 or 3 types must be included, as defined in the *Password- Minimum Mixed Character Type*s setting **0** -The rule for each character type is defined in the character type's *Include* setting **Default**: 1	PROP_PQ_MIXCHARS

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

Description (Cont.)	Settings in GPO Editor or MMC (Cont.)	Registry Key (Cont.)	Command Line (Cont.)
Password - Include Numerals Determines if the password can include numerals. **Note:** ♦ Applies only when the *Password - Complexity* setting is set to **Manual complexity.** ♦ Can be set in SafeNet Authentication Client Tools.	**Setting Name:** Password - Include Numerals **Values**: Permitted Forbidden Mandatory **Default**: Permitted **Note:** *Forbidden* is not supported by iKey devices.	**Registry Key Name:** pqNumbers **Values**: 0 -Permitted 1 - Forbidden 2 - Mandatory **Default**: 0	Cannot be set by command line installation

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

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.

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

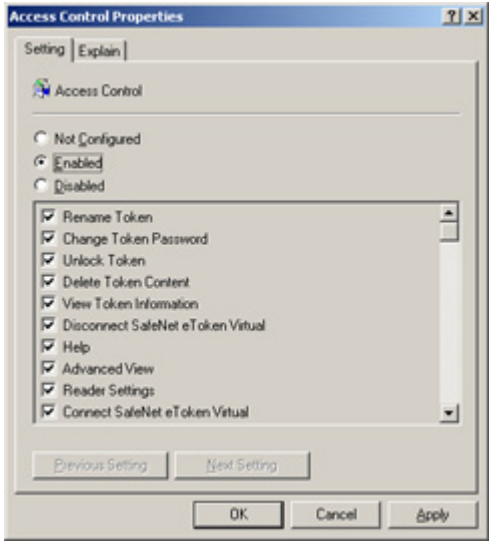
Description (Cont.)	Settings in GPO Editor or MMC (Cont.)	Registry Key (Cont.)	Command Line (Cont.)
Password Quality Check on Initialization Determines if the password quality settings are checked and enforced when a token is initialized **Note:** We recommend that this policy not be set when tokens are enrolled using TMS or 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.

Description (Cont.)	Settings in GPO Editor or MMC (Cont.)	Registry Key (Cont.)	Command Line (Cont.)
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.

Access Control Feature (Cont.)	Registry Value Name (Cont.)	Description (Cont.)
Change Token Password	ChangePassword	Enables/Disables the *Change Token Password* feature in SafeNet Authentication Client Tools.
Unlock Token	UnlockEtoken	Enables/Disables the *Unlock Token* feature in SafeNet Authentication Client Tools.
Delete Token Content	ClearEToken	Enables/Disables the *Delete Token Content* feature in SafeNet Authentication Client Tools.
View Token Information	ViewTokenInfo	Enables/Disables the *View Token Information* feature in SafeNet Authentication Client Tools.
Disconnect SafeNet eToken Virtual	DisconnectVirtual	Enables/Disables the *Disconnect SafeNet eToken Virtual* 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 eToken Virtual	AddeTokenVirtual	Enables/Disables the *Connect SafeNet eToken Virtual* feature in SafeNet Authentication Client Tools.
Initialize Token	InitializeEToken	Enables/Disables the *Initialize Token* feature in SafeNet Authentication Client Tools.

Access Control Feature (Cont.)	Registry Value Name (Cont.)	Description (Cont.)
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.

Access Control Feature (Cont.)	Registry Value Name (Cont.)	Description (Cont.)
Token Password Retries	AllowChangeUserMaxRetry	Enables/Disables the *Logon retries before token is locked* feature (for the Token Password) in SafeNet Authentication Client Tools.
Administrator Password Retries	AllowChangeAdminMaxRetry	Enables/Disables the *Logon retries before token is locked* feature (for the Administrator Password) in SafeNet Authentication Client Tools.
Advanced Initialization Settings	OpenAdvancedModeOfInitialize	Enables/Disables the *Advanced* button in the *Token Initialization* window in SafeNet Authentication Client Tools.
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**

Access Control Feature (Cont.)	Registry Value Name (Cont.)	Description (Cont.)
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.

Access Control Feature (Cont.)	Registry Value Name (Cont.)	Description (Cont.)
Note: This property cannot be set in the Access Control Properties window. It must be set in the registry key.	VerisignClearEToken	Enables/Disables the *Verisign Clear Token* feature 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.

SafeNet Authentication Client - BSec-Compatible Settings

The settings in this section are relevant for SafeNet Authentication Client BSec-compatible configuration.

PKI Enrollment - Token Manager Utility (TMU) Settings

Description	ADM File Setting	Registry Value	Command Line
Enable Token Enrollment Determines if the token enrollment option is enabled in the Token Manager Utility.	**Setting Name:** Enable Token Enrollment **Values**: **Selected** -Enabled **Not selected** -Disabled **Default**: Selected	**Registry Value Name:** EnrollEnabled **Values**: **1 (True)** - Enabled **0 (False)** - Disabled **Default**: 1	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Enroll Token Containing Data Determines how to proceed when data is detected on the token during token enrollment.	**Setting Name:** Enroll Token Containing Data **Values**: Always Initialize the token Prompt user for action Redirect to enrollment update **Default**: Always Initialize the token	**Registry Value Name:** PKIEnrollCheck **Values**: **1** - Continue initializing the token **2** - Redirect to enrollment update **3** - Prompt user for action **Default**: 1	Cannot be set by command line installation.
Enable Enrollment Update Determines if the option to update after enrollment is enabled in the Token Manager Utility.	**Setting Name:** Enable Enrollment Update **Values**: **Selected** -Enabled **Not selected** -Disabled **Default**: Selected	**Registry Value Name:** PKIEnrollUpdateEnabled **Values**: **1 (True)** - Enabled **0 (False)** - Disabled **Default**: 1	Cannot be set by command line installation.
Enable P12 Import Determines if the option to import a PKC12 file is enabled in the Token Manager Utility.	**Setting Name:** Enable P12 Import **Values**: **Selected** -Enabled **Not selected** -Disabled **Default**: Selected	**Registry Value Name:** PKIEnrollP12Enabled **Values**: **1 (True)** - Enabled **0 (False)** - Disabled **Default**: 1	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Enable PKI Certificate Enrollment Determines if the certificate enrollment option is enabled in the Token Manager Utility. **Note:** Certificates can be enrolled to a token only if appropriate values are defined in the following settings: ♦ Enrollment Certificate Key Size ♦ Enrollment CA Name ♦ Enrollment CA Certificate Template	**Setting Name:** Enable PKI Certificate Enrollment **Values**: **Selected** - Enabled **Not selected** - Disabled **Default**: Selected	**Registry Value Name:** PKIEnrollEnabled **Values**: **1 (True)** - Enabled **0 (False)** - Disabled **Default**: 1	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Enrollment Certificate Key Size Defines the size of the enrollment certificate key.	**Setting Name:** Enrollment Certificate Key Size **Values**: **1** - 512 bits **2** - 768 bits **3** - 1024 bits **4** - 1280 bits **5** - 1536 bits **6** - 1792 bits **7** - 2048 bits **Default**: 3 (1024 bit)	**Registry Value Name:** EnrollmentCertificateKeySize **Values**: **1** - 512 bits **2** - 768 bits **3** - 1024 bits **4** - 1280 bits **5** - 1536 bits **6** - 1792 bits **7** - 2048 bits **Default**: 3 (1024 bit)	Cannot be set by command line installation.
Enrollment CA Name Defines the distinguished name of the Certificate Authority for certificate enrollment.	**Setting Name:** Enrollment CA Name **Values**: String **Default**: None	**Registry Value Name:** EnrollmentCAName **Values**: String **Default**: None	Cannot be set by command line installation.
Enrollment CA Certificate Template Defines the CA certificate template for certificate enrollment	**Setting Name:** Enrollment CA Certificate Template **Values**: String **Default**: SmartcardUser	**Registry Value Name:** EnrollmentCertificateTemplate **Values**: String **Default**: SmartcardUser	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Enable PKI Certificate Reenrollment Determines if the certificate re-enrollment option is enabled in the Token Manager Utility.	**Setting Name:** Enable PKI Certificate Reenrollment **Values**: **Selected** - Enabled **Not selected** - Disabled **Default**: Selected	**Registry Value Name:** PKIReEnrollEnabled **Values**: **1 (True)** - Enabled **0 (False)** - Disabled **Default**: 1	Cannot be set by command line installation.

CIP Utilities and Token Utilities Settings

Description	ADM File Setting	Registry Value	Command Line
Enable Login Determines if the Login option is enabled.	**Setting Name:** Enable Login **Values**: **Selected** - Enabled **Not selected** - Disabled **Default**: Selected	**Registry Value Name:** Adminlogin **Values**: **1 (True)** - Enabled **0 (False)** - Disabled **Default**: 1	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Enable Change Password Determines if the Change Password option is enabled.	**Setting Name:** Enable Change Password **Values**: **Selected** - Enabled **Not selected** - Disabled **Default**: Selected	**Registry Value Name:** AdminchangePassPhrase **Values**: **1 (True)** - Enabled **0 (False)** - Disabled **Default**: 1	Cannot be set by command line installation.
Enable Initialize Token Determines if the Initialize Token option is enabled.	**Setting Name:** Enable Initialize Token **Values**: **Selected** - Enabled **Not selected** - Disabled **Default**: Selected	**Registry Value Name:** AdmininitializeToken **Values**: **1 (True)** - Enabled **0 (False)** - Disabled **Default**: 1	Cannot be set by command line installation.
Enable Test Token Determines if the Test Token option is enabled.	**Setting Name:** Enable Test Token **Values**: **Selected** - Enabled **Not selected** - Disabled **Default**: Selected	**Registry Value Name:** AdmintestToken **Values**: **1 (True)** - Enabled **0 (False)** - Disabled **Default**: 1	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Enable Change Inactivity Timer Determines if the Change Inactivity Timer option is enabled.	**Setting Name:** Enable Change Inactivity Timer **Values**: **Selected** - Enabled **Not selected** - Disabled **Default**: Selected	**Registry Value Name:** AdmineditInactivityTimer **Values**: **1 (True)** - Enabled **0 (False)** - Disabled **Default**: 1	Cannot be set by command line installation.
Enable Detailed Display Determines if the Detailed Display option is enabled.	**Setting Name:** Enable Detailed Display **Values**: **Selected** - Enabled **Not selected** - Disabled **Default**: Selected	**Registry Value Name:** AdmindisplayObjects **Values**: **1 (True)** - Enabled **0 (False)** - Disabled **Default**: 1	Cannot be set by command line installation.
Enable Delete from Token Determines if the Delete from Token option is enabled	**Setting Name:** Enable Delete from Token **Values**: **Selected** - Enabled **Not selected** - Disabled **Default**: Selected	**Registry Value Name:** AdmindeleteObjects **Values**: **1 (True)** - Enabled **0 (False)** - Disabled **Default**: 1	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Enable Export to File Determines if the Export to File option is enabled.	**Setting Name:** Enable Export to File **Values**: **Selected** - Enabled **Not selected** - Disabled **Default**: Selected	**Registry Value Name:** AdminsaveObjectsToFile **Values**: **1 (True)** - Enabled **0 (False)** - Disabled **Default**: 1	Cannot be set by command line installation.
Enable Edit Object Determines if the Edit Object option is enabled.	**Setting Name:** Enable Edit Object **Values**: **Selected** - Enabled **Not selected** - Disabled **Default**: Selected	**Registry Value Name**: AdmineditObjectAttributes **Values**: **1 (True)** - Enabled **0 (False)** - Disabled **Default**: 1	Cannot be set by command line installation.
Enable Set Default Container Determines if the Set to Default Container option is enabled.	**Setting Name:** Enable Set Default Container **Values**: **Selected** - Enabled **Not selected** - Disabled **Default**: Selected	**Registry Value Name:** Adminsetdefaultcontainer **Values**: **1 (True)** - Enabled **0 (False)** - Disabled **Default**: 1	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Enable Import P12 Determines if the Import PKCS# 12 File option is enabled.	**Setting Name:** Enable Import P12 **Values**: **Selected** - Enabled **Not selected** - Disabled **Default**: Selected	**Registry Value Name:** AdminimportP12 **Values**: **1 (True)** - Enabled **0 (False)** - Disabled **Default**: 1	Cannot be set by command line installation.
Enable Change Label Determines if the Change Label option is enabled.	**Setting Name:** Enable Change Label **Values**: **Selected** - Enabled **Not selected** - Disabled **Default**: Selected	**Registry Value Name:** AdminRFU9 **Values**: **1 (True)** - Enabled **0 (False)** - Disabled **Default**: 1	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Hide Unblocking Password Determines if the unblocking password characters are displayed as asterisks as they are typed.	**Setting Name:** Hide Unblocking Password **Values**: **Selected** - Password characters are displayed as asterisks **Not selected** – The actual password characters are displayed **Default**: Selected	**Registry Value Name:** AdminRFU8 **Values**: **1 (True)** - Enabled **0 (False)** - Disabled **Default**: 1	Cannot be set by command line installation.

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.

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

To allow organizations to enforce restrictive cryptographic policies when using SafeNet smartcard 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. By following NIST recommendations, the following algorithms have been excluded and are considered as weak:

Algorithms: RSA, ECC, AES, DES, 3DES, RC2, RC4, SHA2, SHA1, MD5, HMAC, GenericSecret.

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.

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 details, remove the OID value from the registration key value.	**Setting name:** Override IdenTrust OIDs **Value**: All OID values of non-repudiation certificates, separated by commas **Default**: No override	**Registry Value Name:** IdentrusIdentity **Value**: All OID values of non-repudiation certificates, separated by commas **Default**: No override	Cannot be set by command line installation.