SafeNet Authentication Client (Windows-Linux-Mac)

Version 9.0 (GA)

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: SAC 9.0 (GA) Administrator's Guide

Document Part Number: 007-012830-001, Revision B

Date of publication: February 2015

Last update: Sunday, February 08, 2015 9:02 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 9.0 (GA) User's Guide
- SafeNet Authentication Client 9.0 (GA) Customer Release Notes (CRN)

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 on Windows, Linux and Mac

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.

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 9.0 (GA) offers the following new features:

- **eToken 7300 Flash usage procedures are now supported on Windows, Linux and Mac** - Usage operations (performed via all operating systems) include:
  - Log On to Flash/Log Off from Flash
  - CD-ROM update
  - Firmware update (Windows only)
- **eToken 7300 unified bundle is now supported on Mac operating system**
- **New Linux operating systems are now supported New and enhanced UI across all platforms** - Previous versions of SAC supported the QT cross-platform framework. SAC 9.0 now supports an innovative technology that maintains the unique look and feel of each underlying (native) platform (Windows, Linux, and Mac).
- **Additional custom installation options (Windows only)** - The installation of SAC 9.0 enables selecting specific customized features to be installed. For example, BSec compatability mode is now available through the custom installation options. (Windows only)
- **Installation file size reduced** - The Windows, and Linux installation file size has been reduced significantly.
- **Mac Yosemite support** – SAC 9.0 now supports the MAC Yosemite operating system.

- **SAC (Mac) custom installation file**- This is a separate custom installation file, which enables administrators to distribute the SAC license and configuration installation file (SafeNet Authentication Client Customization 9.0.mpkg) to the organization. For details on how the administrator creates this file, see Preparing SAC (Mac) Custom Installation on page 114

Supported Tokens

SafeNet Authentication Client 9.0 (GA) supports the following tokens for Windows, Linux and Mac:

Certificate based USB tokens

- SafeNet eToken PRO Java 72K
- SafeNet eToken PRO Anywhere
- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID

Smart cards

- SafeNet eToken PRO Smartcard 72K
- SafeNet eToken 4100

Certificate based hybrid USB tokens

- SafeNet eToken 7300
- SafeNet eToken 7300-HID
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)

Software tokens

- SafeNet eToken Virtual
- SafeNet eToken Rescue

End-of-Sale tokens/smart cards

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

NOTE
SafeNet Authentication Client 9.0 (Linux) supports only Smart Card manageability for SafeNet eToken 7300. Storage management functionality such as Partitioning, Initialization, Image burning, etc. will only be available in SAC 8.2 and later, on Windows.

External Smart Card Readers

SafeNet Authentication Client 9.0 supports the following smart card readers:

- SCR 3310 v2 Reader
- Athena AESDrive IIIe USB v2 and v3

- ACR
- Athena Keyboard
- GemPC CCID
- Omnikey 3121
- Dell Broadcom
- Unotron

NOTE

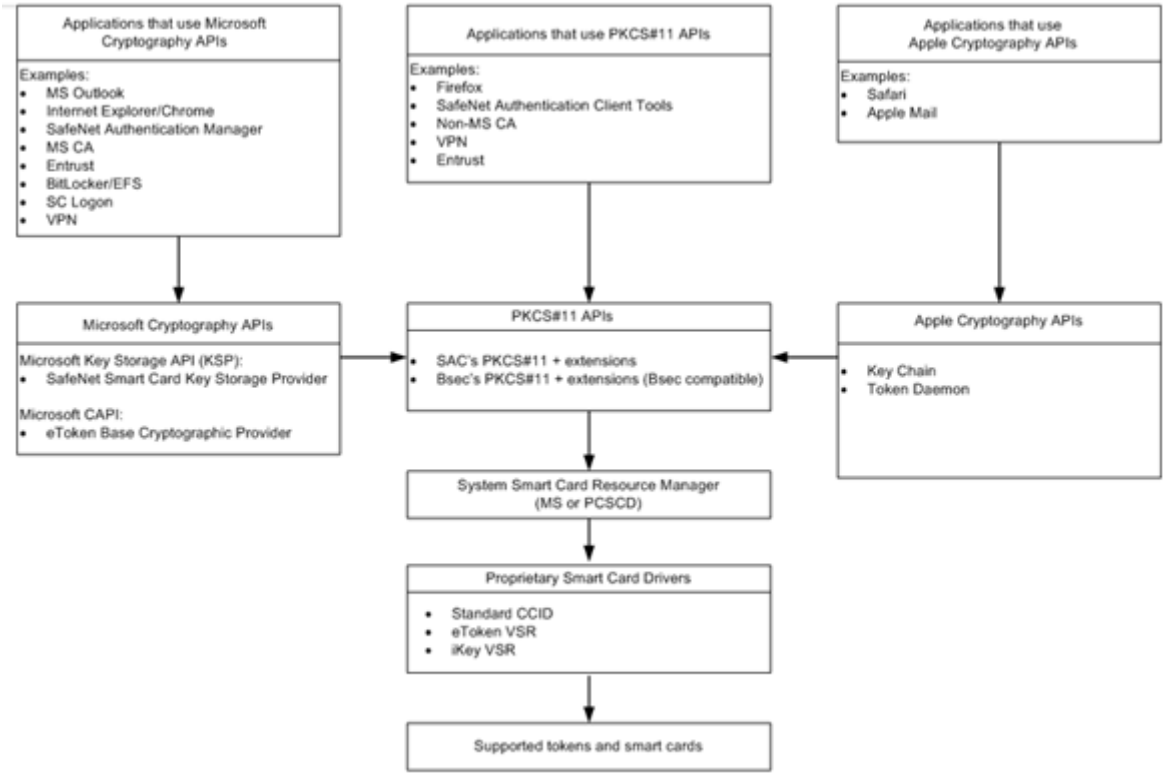
- Reader drivers must be compatible with the extended APDU format in order to be used with RSA-2048.
- The latest CCID Driver must be installed when using Athena v3.

Supported Localizations

SafeNet Authentication Client 9.0 supports the following languages:

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

SafeNet Authentication Client Architecture



License Activation on Windows, Linux, and Mac

By default, SafeNet Authentication Client 9.0 is installed by default as non-licensed.

To activate the license perform the following steps:

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

   - **Manual Activation**

     See the *Licensing* chapter in the *SafeNet Authentication Client 9.0 (GA) User's Guide*.

   - **Command Line Activation**

     See *PROP_LICENSE_FILE Property* on page 94 (Command Line column) and *Installing the MSI file via the Command Line* on page 84.

   - **Group Policy Object Editor**

     See *License Settings* on page 200 (ADM File Setting column) and *Setting SafeNet Authentication Client Properties* on page 183.

   - **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 46.

NOTE

SafeNet Authentication Client retrieves the license file (SACLicense.lic) automatically, if the license file is located in the following default path:

- Windows: **\ProgramData\SafeNet\SAC**
- Linux (per user): **/home/<user name>**
- Linux (per machine): **/etc/**
- Mac (per user): **/home/<user name>**
- Mac (per machine): **/Users/Shared/SafeNet/SAC**

2 System Requirements

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

In this chapter:

- Supported Browsers
- Supported Platforms
- Hardware and Screen Resolution Requirements (Windows, Linux, and Mac)
- Compatibility with SafeNet Applications
- Compatibility with Third-Party Applications
- Supported SHA 2 Algorithms
- Supported Algorithms for Onboard Hashing
- PCSC-Lite

Supported Browsers

SafeNet Authentication Client 9.0 (Windows) supports the following browsers:

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

SafeNet Authentication Client 9.0 (Linux) supports the following browsers:

- Firefox

SafeNet Authentication Client 9.0 (Mac) supports the following browsers:

- Firefox
- Safari
- Chrome

Supported Platforms

SafeNet Authentication Client 9.0 (Windows) supports the following operating systems:

- Windows Vista SP2 (32-bit, 64-bit)
- Windows Server 2008 R2 SP1 (32-bit, 64-bit)
- Windows Server 2008 SP2 (32-bit, 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
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.

SafeNet Authentication Client 9.0 (Linux) supports the following operating systems:

- Red Hat 6.6 (32-bit and 64-bit), 7.0 (64-bit)
- Ubuntu 13.10, 14.04 (32-bit and 64-bit)
- Debian 7.7 (32-bit and 64-bit)
- SUSE Enterprise Desktop 11.3 (32-bit and 64-bit), 12.0 (64-bit)

- CentOS 6.6 (32-bit and 64-bit), 7.0 (64-bit)
- Fedora 20 (32-bit and 64-bit)

SafeNet Authentication Client 9.0 (Mac) supports the following operating systems:

- Mac OS X 10.9 (Mavericks)
- Mac OS X 10.10 (Yosemite)

Hardware and Screen Resolution Requirements (Windows, Linux, and Mac)

Required hardware:

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

Compatibility with SafeNet Applications

SafeNet Authentication Client 9.0 (Windows) works with the following SafeNet products:

- SafeNet Network Logon 8.2 and above
- SafeNet Authentication Manager 8.2 and above
- eToken Minidriver 5.1 (Java cards only)

Compatibility with Third-Party Applications

SafeNet Authentication Client 9.0 works with the following products:

Solution Type	Vendor	Product Version
Remote Access VPN	Check Point	NGX R75, R77
	Cisco	ACS 5.4, NAM, ASA 5500, AnyConnect
	Citrix	Netscaler 10.1
	Juniper	Juniper SA 700
	Nortell	Avaya VPN Client 10.04
Virtual Desktop Infrastructure (VDI)	Citrix	XenApp 6.5, XenDesktop 7.5
	Microsoft	Remote Desktop
	VMware View	Horizon 5.2
Identity Access Management (IAM) Identity Management (IDM)	CA	Siteminder 12.1
	IBM	ISAM for Web 7.0
	Intercede	MyID
	Microsoft	FIM 2010 R2

Solution Type	Vendor	Product Version
Pre Boot Authentication (PBA)	Symantec	PGP Desktop 10.3
	WinMagic	SecureDoc
	Sophos	SafeGuard Easy
	Becrypt	Disk Protect 5.2
	Microsoft	BitLocker
	McAfee	Endpoint 7 x
Certificate Authority (CA)	Entrust	Authority 8.1
	CheckPoint (Local CA)	For all CheckPoint platforms
	Microsoft (Local CA)	For all Windows platforms
	Verisign	MPKI 8.x

Solution Type	Vendor	Product Version
Local Access	Putty	CAC
	Microsoft	All OS
	Cisco	ISR 8200
	OpenSSH	f-secure
	Tectia	SSH Client 6.2
	Evidian	ESSO
	Linux	PAM
Digital Signatures	Entrust	ESP 9.2
	Adobe	Reader X, XI
	Microsoft	Outlook 2013
	IBM	Lotus Notes 9.0
	Mozilla	Thunderbird 1.29

SafeNet Authentication Client 9.0 (GA) Linux supports 3rd party applications that communicate over PKCS#11.

NOTE
If the PKCS#11 security provider is not added automatically, it must be added manually. See *Loading the Token PKCS#11 Security Module* on page 136.

Supported SHA 2 Algorithms

- SHA256
- SHA384
- SHA512

Supported Algorithms for Onboard Hashing

- SHA1
- SHA256

PCSC-Lite

SafeNet Authentication Client (Mac) 9.0 uses the default PCSC-Lite that is installed with Mac OS X. SafeNet Authentication Client 9.0 installs a plug-in and driver for PCSC-Lite, during the normal installation process.

PCSC-Lite is managed by the Mac OS X Security Manager. When a device is inserted, the service runs automatically.

The SafeNet Authentication Client (Mac) 9.0 installation runs after reboot even if a token device is not inserted. This is required to support SafeNet eToken Virtual on a flash device.

3 Customization

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

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

In this chapter:

Customization Overview

You can customize the following SafeNet Authentication Client 9.0 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

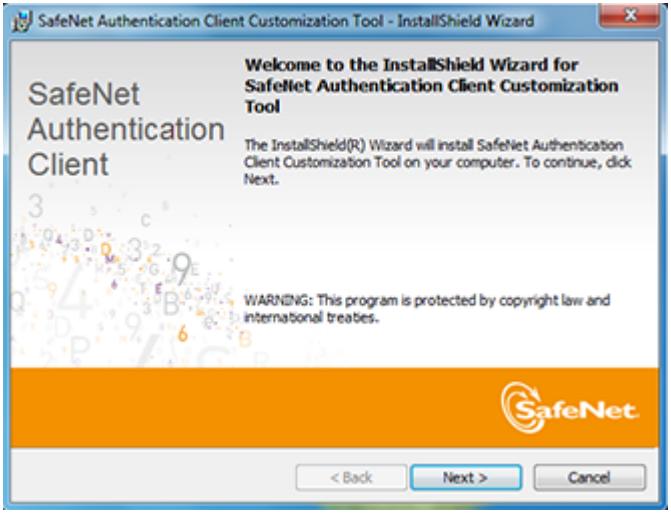
Installing the SafeNet Authentication Client Customization Tool

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

To install the SafeNet Authentication Client Customization Tool:

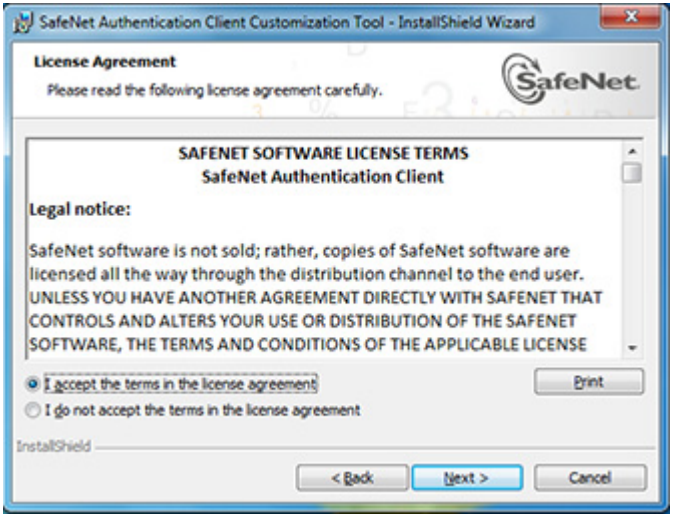
1 Double-click **SACCustomizationPackage-9.0-x32.msi**.

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



2 Click **Next**.

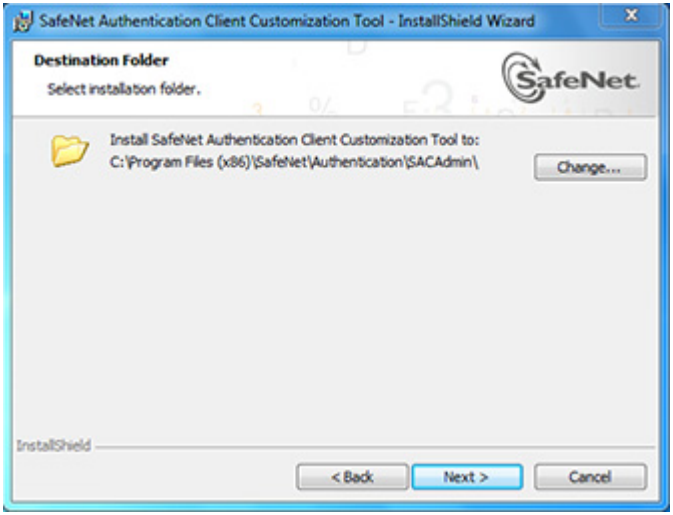
The *License Agreement* is displayed.



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

4 Click **Next**.

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

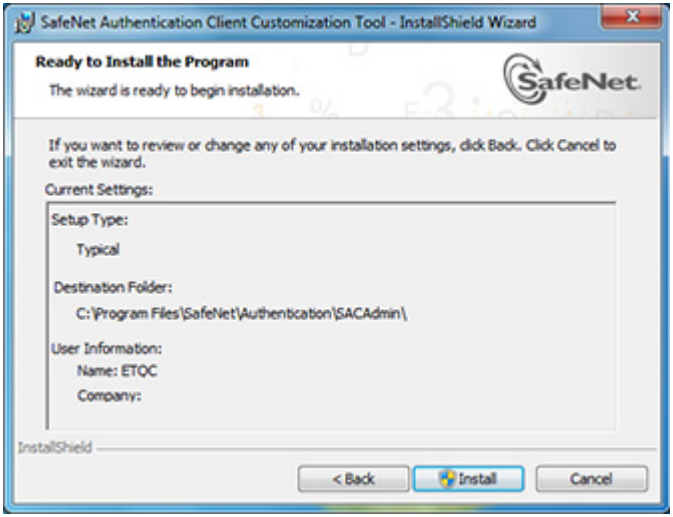


5 You can click **Browse** to select a different destination folder, or install the Customization Tool's SACAdmin folder into the default folder:

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

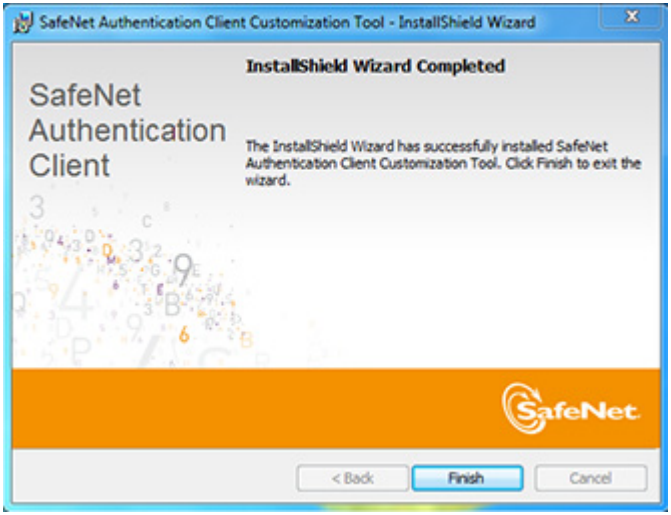
> **NOTE**
> If an application from the SafeNet Authentication line of products, or an eToken legacy product, is already installed, we recommend that the destination folder not be changed.

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



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

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



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

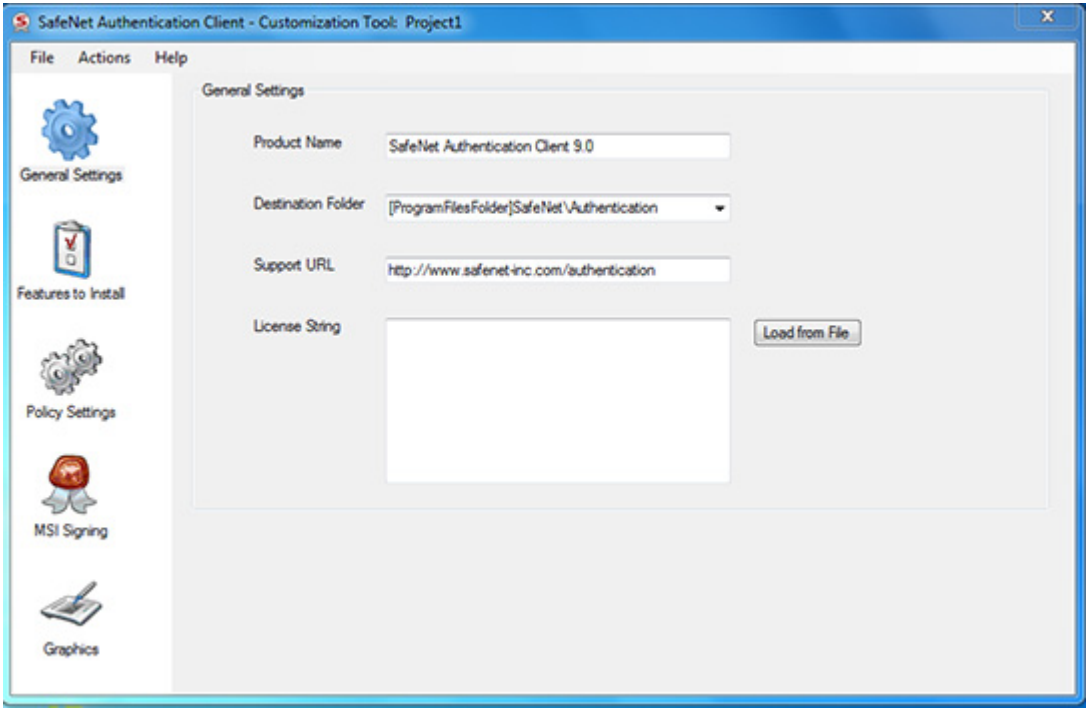
Using the SafeNet Authentication Client Customization Tool

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

To use the Customization Tool:

1 From the Windows *Start* menu, select **Programs > SafeNet > SACAdmin > SAC Customization Tool**.

The *SafeNet Authentication Client Customization Tool* opens to the *General Settings* tab.



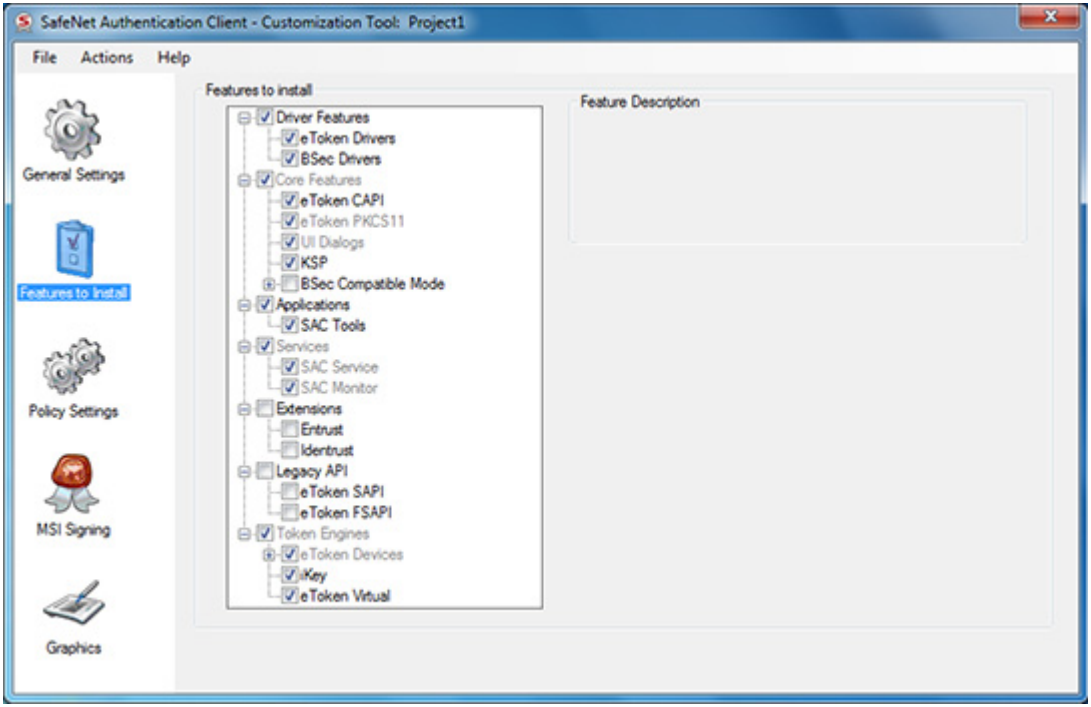
2 To open a project you already saved, select **File > Open**, and browse to the xml file of an existing project.

3 You can replace the following items:

- 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.


SafeNet Authentication Client - Customization Tool: Project1
File
Actions
Help
General Settings
Features to install
Policy Settings
MSI Signing
Graphics
Features to install
Driver Features
eToken Drivers
BSec Drivers
Core Features
eToken CAPI
eToken PKCS11
UI Dialogs
KSP
BSec Compatible Mode
Applications
SAC Tools
Services
SAC Service
SAC Monitor
Extensions
Entrust
Identrust
Legacy API
eToken SAPI
eToken FSAPI
Token Engines
eToken Devices
iKey
eToken Virtual
Feature Description

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.

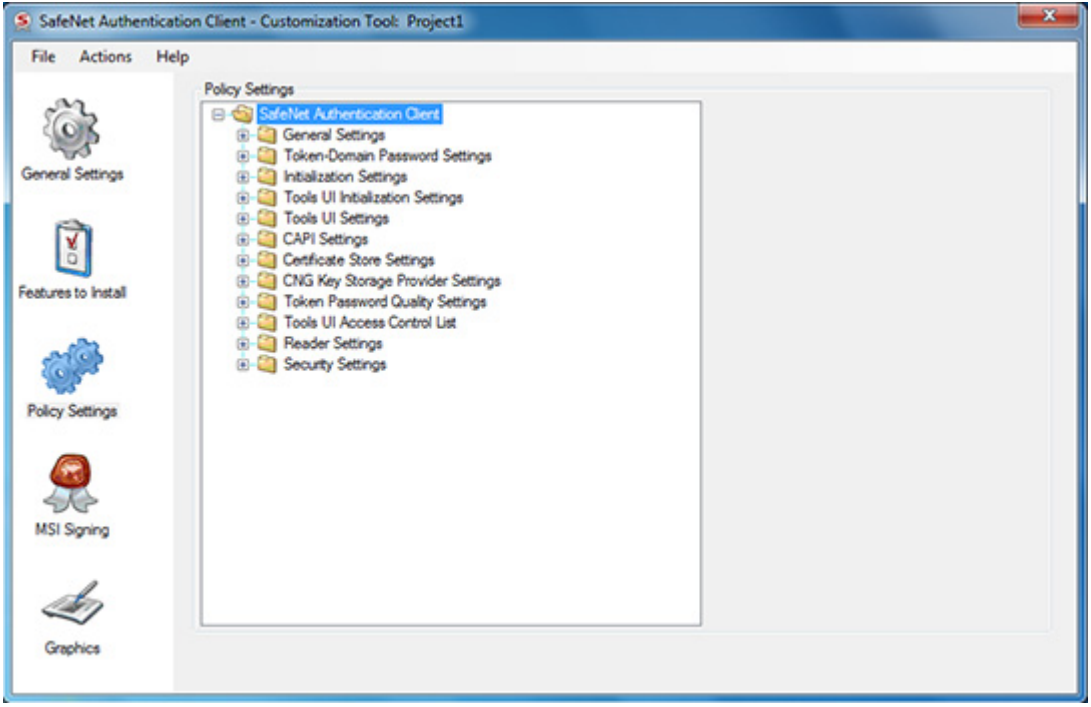
- eToken SAPI
- eToken FSFeature
- SAC Tools
- Entrust support
- BSec PKCS#11
- BSec CAPI
- IdenTrust support

NOTE
- If IdenTrust support is selected, ensure that BSec PKCS#11 is selected also.
- In order to work with SafeNet Network Logon eToken SAPI must be installed.

For more information, see Chapter 5: *Installing SafeNet Authentication Client on Windows (Simplified Installation)*, on page 105.

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

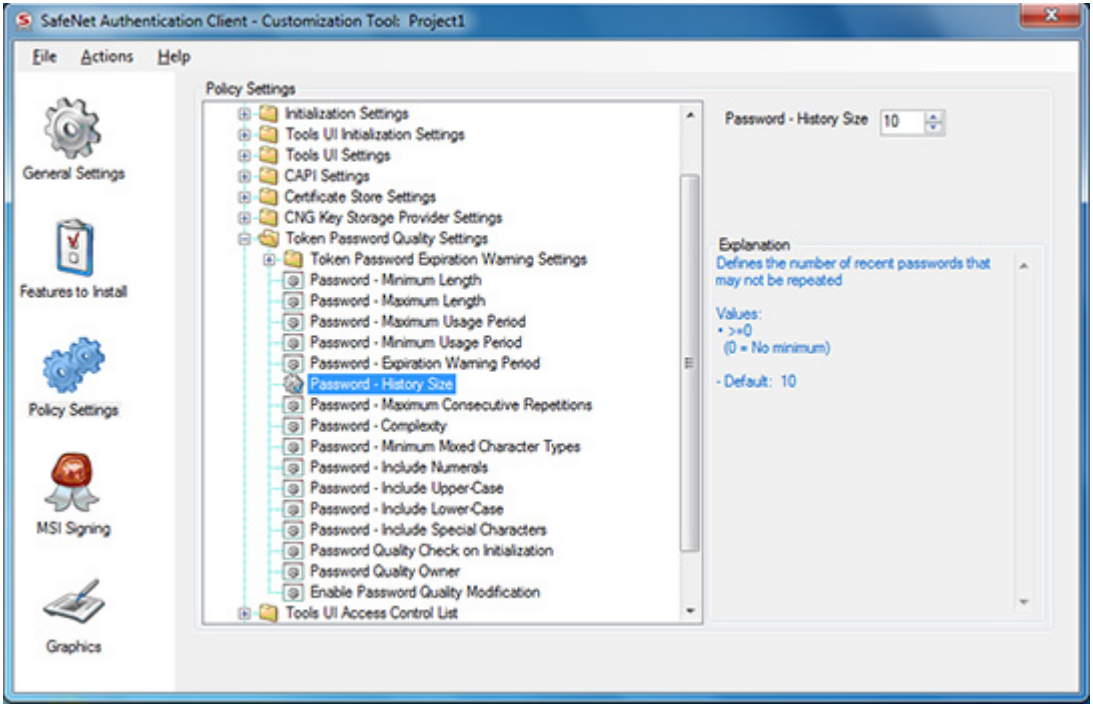
The *Policy Settings* window opens.



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

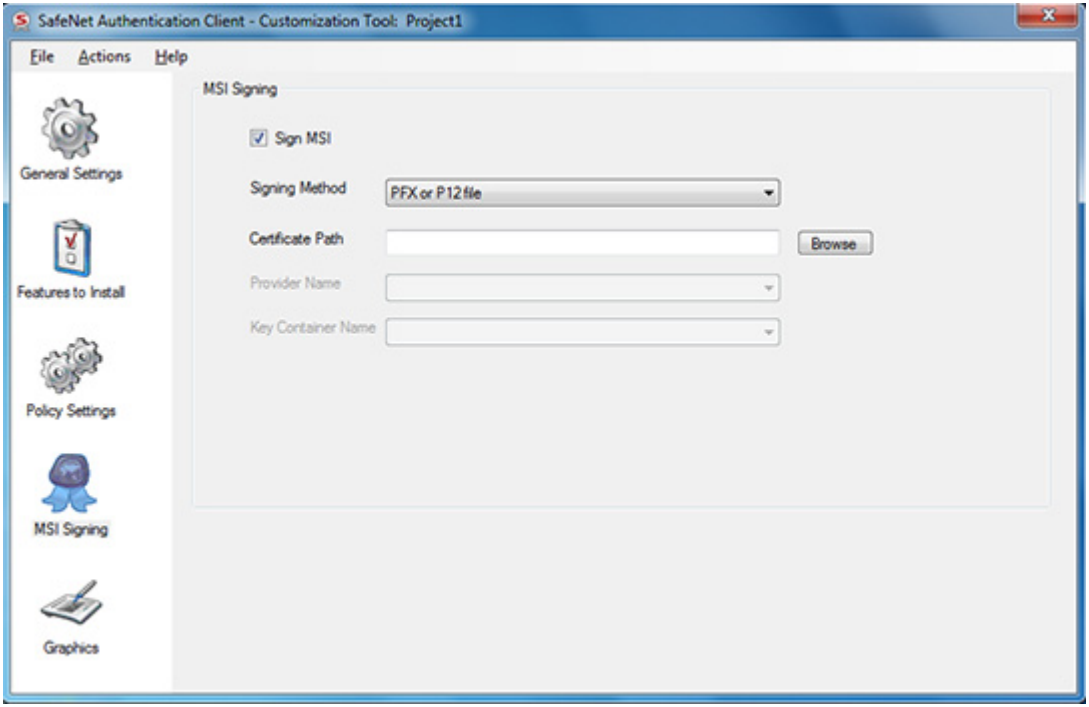
For more information, see Chapter 8: *Configuration Properties*, on page 180.

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:

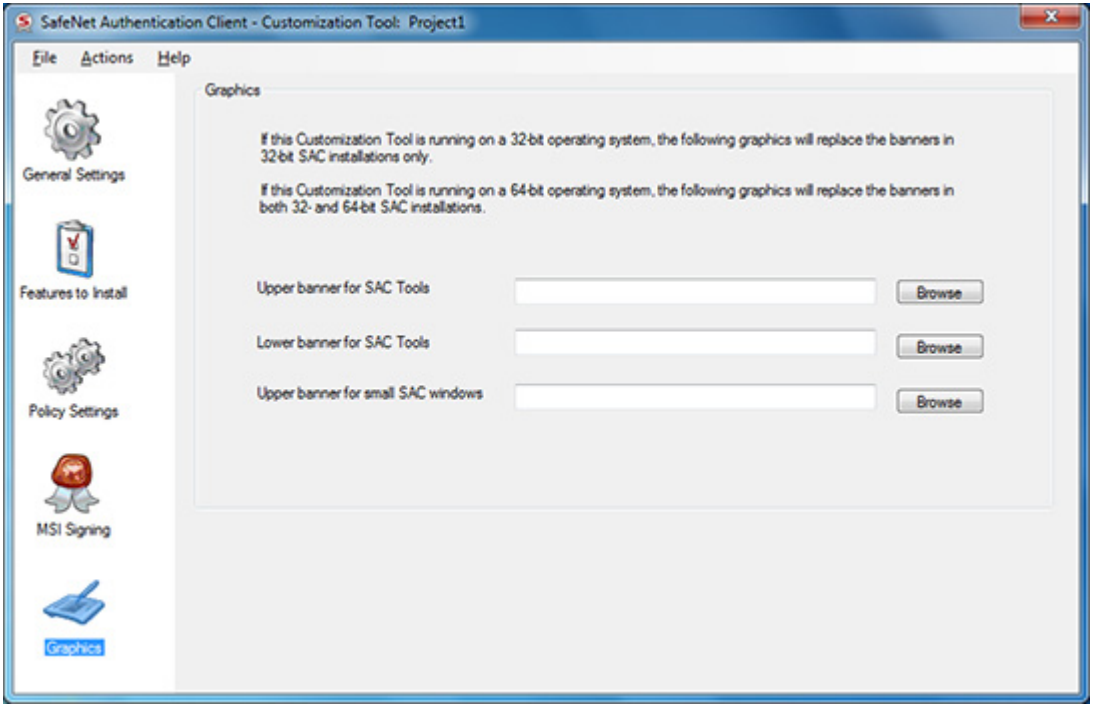
- Signing Method (P12, Smartcard or HSM)
- Certificate Path

> **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

The following graphics can be replaced:

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

NOTE

- All banner formats must be in PNG format.
- The customized settings are saved as an xml file.
- By default, project folders are saved in the following location: My Documents\SafeNet\Authentication\SAC\[ProfileName]

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.

Generating a Customized MSI Installation File

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

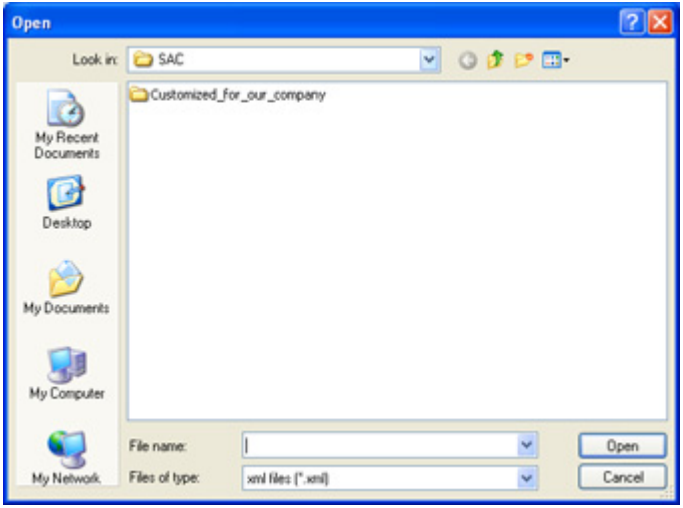
> **NOTE**
> Generating an MSI file can be performed with administrator privileges only.

To generate a customized installation file:

1. Open the *SAC Customization Tool*.

   See *Using the SafeNet Authentication Client Customization Tool* on page 44.

2. Select **File > Open**.



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

NOTE

- By default, project folders are saved in the following location: My Documents\SafeNet\Authentication\SAC
- SAC 9.0 does not support legacy GA configuration profiles.

The saved project opens.

4 Select **Actions > Generate MSI**.

An information window is displayed, informing you that the MSI installation files have been generated.

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

The project folder now contains two customized MSI files:

- A file named `<Project Name>-x32-9.0.msi` for 32-bit installations
- A file named `<Project Name>-x64-9.0.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 56.

   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>-x32-9.0.msi` (for 32-bit installations)
   - `<Project Name>-x64-9.0.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.

4 Upgrade

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

NOTE

- You must restart your computer when the upgrade procedure completes. When upgrading via the command line using the /qn parameter, your computer is restarted automatically.
- When upgrading from previous versions of SAC, it is recommended that you save feature settings from the previous versions. If not, then uninstall and install SAC 9.0 with the new feature list.

In this chapter:

Upgrading Using the SafeNet Authentication Client MSI File

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

- On a 32-bit system, run **SafeNetAuthenticationClient-x32-9.0.msi**.
- On a 64-bit system, run **SafeNetAuthenticationClient-x64-9.0.msi**.

See *Installing SafeNet Authentication Client on Windows (MSI)* on page 76.

Upgrading from Versions Earlier than SAC 8.3

Legacy versions of SafeNet Authentication Client, earlier than 8.3 must be uninstalled before installing SafeNet Authentication Client 9.0.

Upgrading from SafeNet Authentication Client 8.3

You can upgrade from SafeNet Authentication Client 8.3 to 9.0 using the **MSI** file wizard installation, or by using the command line installation. See Installing the MSI file via the Command Line on page 84.

While running the wizard, be sure to select **Use the existing configuration settings** parameter on the installation wizard **Interface Language** window. This will save the configuration settings that were detected from SAC 8.3. See Chapter 5 Installing SafeNet Authentication Client on Windows (MSI).

Upgrading using the Simplified Installer File

The simplest way to upgrade to SafeNet Authentication Client 9.0 is to use an .exe simplified installer file. These files do not support Custom changes.

If eToken PKI Client 5.1 SP1 or BSec 7.2 are installed, you are required to uninstall manually prior to SafeNet Authentication Client 9.0 Installation.

The **SafeNetAuthenticationClient-x32-x64-9.0.exe** simplified installer file uninstalls or upgrades previous versions of SafeNet Authentication Client, and then installs SafeNet Authentication Client 9.0 properly on 32-bit and 64-bit environments in each of the following situations:

- No middleware is yet installed (installation only).
- SafeNet Authentication Client 8.3 is installed (an upgrade will be performed).
- Versions earlier than SAC 8.3 are installed (an uninstall will be performed).

If you have a version earlier that SAC 8.0, then upgrade to a newer version, or uninstall manually before running the SAC 9.0 installation.

The simplified installation file automatically uninstalls and then installs SAC 9.0 from the following versions of SafeNet Authentication Client:

- SAC 8.0
- SAC 8.0 SP1, SP2
- SAC 8.1, SP1, SP2
- SAC 8.2

The simplified installation automatically upgrades from SAC 8.3 to SAC 9.0.

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

Upgrading SafeNet Authentication Client on a Mac

After upgrading from SAC 8.2 SP2 to SAC 9.0 on a Mac (Mavericks) you must restart the machine in order for the token to be recognized.

5 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.
- 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 3: *Customization*, on page 36.

In this chapter:

- Installation Files

Windows:

- Installation Configurations

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

Mac OS X:

- Installing SafeNet Authentication Client on a Mac OS X
- Installing SAC from the Mac Terminal
- Preparing SAC (Mac) Custom Installation
- Installing the Firefox Security Module (Mac)
- Installing the Thunderbird Security Module
- Configuring Acrobat Security Settings

Linux:

- Installing SAC on Linux Standard Package
- Installing a 32-bit Compatibility Package on a 64-bit OS
- Installing the Core Package
- Installing the Firefox Security Module (Linux)
- Loading the Token PKCS#11 Security Module

Installation Files

The software package provided by SafeNet includes files for installing or upgrading to SafeNet Authentication Client 9.0.

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

File	Environment	Description	Use
Windows			
SafeNetAuthenticationClient-x32-x64-9.0.exe	32-bit 64-bit	Installs SafeNet Authentication Client 9_0, and upgrades from earlier versions (8.0, 8.1, 8.2) of SafeNet Authentication Client.	Use to install SafeNet Authentication Client 9.0, and to upgrade from: ♦ SafeNet Authentication Client 8.0, 8.1, 8.2.
SafeNetAuthenticationClient-x32-9.0.msi	32-bit	Installs SafeNet Authentication Client 9.0, and upgrades from version 8.3 of SafeNet Authentication Client.	Use to install SafeNet Authentication Client 9.0 and upgrades from version 8.3 of SafeNet Authentication Client.
SafeNetAuthenticationClient-x64-9.0.msi	64-bit		

File	Environment	Description	Use
SACCustomizationPackage-9.0.msi	32-bit 64-bit	Installs SafeNet Authentication Client 9.0 Customization Package.	Use to customize SafeNet Authentication Client installation with non-default settings. If a previous version of the Customization package exists, uninstall the previous version, and then install the new version.
Linux			
SafenetAuthenticationClient-9.0.n-0.i386.rpm	32-bit	Installs: SafeNet Authentication Client on 32 bit platform.	Use to install SafeNet Authentication Client on 32 bit platform.
SafenetAuthenticationClient-9.0.n-0.x86_64.rpm	64-bit	Installs: SafeNet Authentication Client on 64 bit platform.	Use to install SafeNet Authentication Client on 64 bit platform.
SAC-32-CompatibilityPack-9.0.n-0.x86_64.rpm	64-bit	Installs: SafeNet Authentication Client 32 bit Compatibility package on 64 bit platform	The 32-bit compatibility package has been introduced to support 32-bit applications on 64-bit platforms. This package installs only PKCS#11 32-bit components to support 32-bit applications on a 64-bit platforms.

File	Environment	Description	Use
RPM-GPG-KEY-SafenetAuthenticationClient	32-bit 64-bit	This file is the public signature (GnuPG) for SafeNet rpm files.	Relevant only for RPM. The signature confirms that the package was signed by an authorized party and also confirms the integrity and origin of your file. Use this file to verify the signature of the RPM files before installing them to ensure that they have not been altered from the original source of the packages.
SafenetAuthenticationClient-9.0.n-0_i386.deb	32-bit	Installs: SafeNet Authentication Client on 32 bit platform	Use to install SafeNet Authentication Client on 32 bit platform.
SafenetAuthenticationClient-9.0.n-0_amd64.deb	64-bit	Installs: SafeNet Authentication Client on 64 bit platform	Use to install SafeNet Authentication Client on 64 bit platform.
SAC-32-CompatibilityPack-9.0.n-0_amd64.deb	64-bit	Installs: SafeNet Authentication Client 32 bit Compatibility package on 64 bit platform	The 32-bit compatibility package has been introduced to support 32-bit applications on 64-bit platforms. This package installs only PKCS#11 32-bit components to support 32-bit applications on a 64-bit platforms.

File	Environment	Description	Use
SafenetAuthenticationClient-core-9.0.n-0.i386.rpm	32-bit	Installs: SafeNet Authentication Client core on 32 bit platform	Installs eToken core library and IFD Handler
SafenetAuthenticationClient-core-9.0.n-0.x86_64.rpm	64-bit	Installs: SafeNet Authentication Client core on 64 bit platform	Installs eToken core library and IFD Handler.
SafenetAuthenticationClient-core-9.0.n-0_i386.deb	32-bit	Installs: SafeNet Authentication Client core on 32 bit platform	Installs eToken core library and IFD Handler.
SafenetAuthenticationClient-core-9.0.n-0_amd64.deb	64-bit	Installs: SafeNet Authentication Client core on 64 bit platform	Installs eToken core library and IFD Handler.
Mac			
SafeNetAuthenticationClient.9.0.xx.dmg.		Installs: SafeNet Authentication Client	Installs: SafeNet Authentication Client

File	Environment	Description	Use
SafeNet Authentication Client Customization 9.0.mpkg	Mac only	This is a separate customer specific installation, used to install the SAC license and configuration file. For details on how to create this file, see Preparing SAC (Mac) Custom Installation on page 113	This file is created and customized by the administrator, as part of the Sac (Mac) custom license and configuration installation script.
Documentation Files for Windows, Linux and Mac			
007-012829-001_SAC_CRN_9_0_GA_WLM_Revision_A.pdf		SafeNet Authentication Client 9.0 Customer Release Notes for Windows, Linux, and Mac.	Read before installation for last minute updates that may affect installation; contains important information such as resolved and known issues and troubleshooting (Windows, Linux, and Mac).
007-012831-001_SAC_9_0_GA_User_Guide_WLM_Revision A		SafeNet Authentication Client 9.0 User's Guide for Windows, Linux, and Mac	Provides detailed information for the user and system administrator regarding the use of SafeNet Authentication Client (Windows, Linux, and Mac).

File	Environment	Description	Use
007-012830-001_SAC_Admin_Guide_Windows_WLM_Revision A		SafeNet Authentication Client 9.0 Administrator's Guide for Windows, Linux, and Mac (this document)	Provides detailed information for the system administrator regarding the installation, configuration, maintenance, and management of SafeNet Authentication Client (Windows, Linux, and Mac).

Installation Configurations

SafeNet Authentication Client can be installed with the following configurations:

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

Installing SafeNet Authentication Client on Windows (MSI)

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

The components that can be set using the wizard are:

- **Language**: the language in which the SafeNet Authentication Client user interface is displayed
- **Destination folder**: the installation library for this and all future SafeNet authentication product applications

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

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

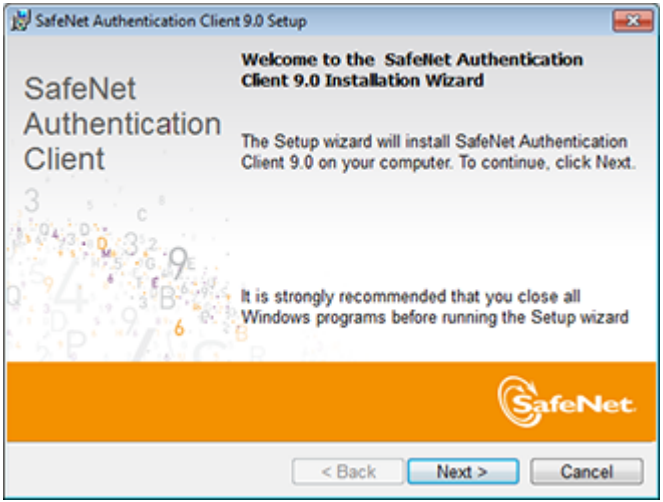
To install via the installation wizard:

1. Log on as an administrator.
2. Close all applications.

3 Double-click the appropriate file:

- `SafeNetAuthenticationClient-x32-9.0.msi` (32-bit)
- `SafeNetAuthenticationClient-x64-9.0.msi` (64-bit)

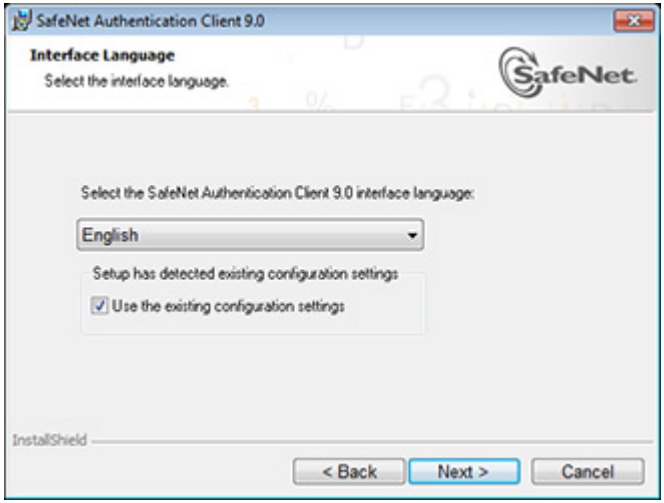
The **SafeNet Authentication Client Installation Wizard** opens.



4 Click **Next**.

The Interface Language window is displayed.

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



5 From the dropdown list, select the language in which the SafeNet Authentication Client screens will appear.

6 If configuration settings are detected from a previous version, you can select **Use the existing configuration settings**.

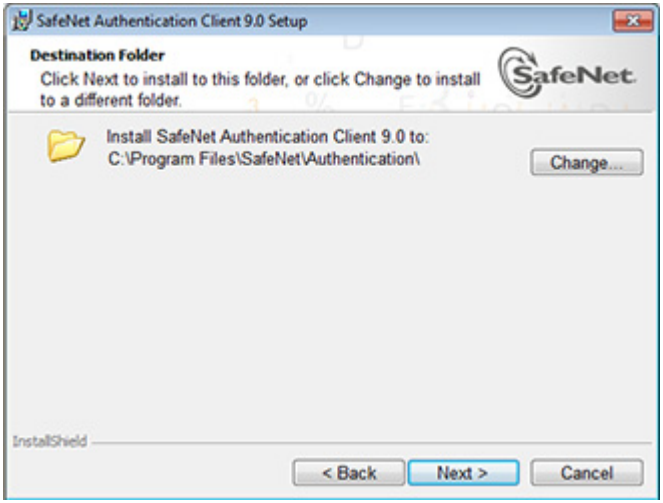
7 Click **Next**.

The *End-User License Agreement* is displayed.

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

9 Click **Next**.

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



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

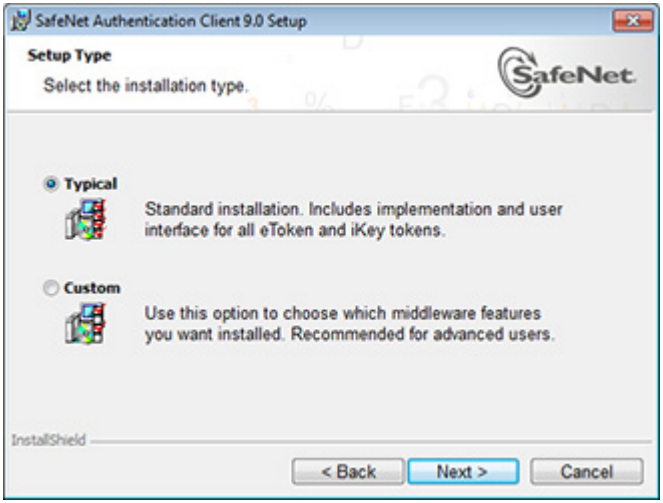
`C:\Program Files\SafeNet\Authentication\`

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

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

11 Click **Next**.

The *Setup Type* window opens.

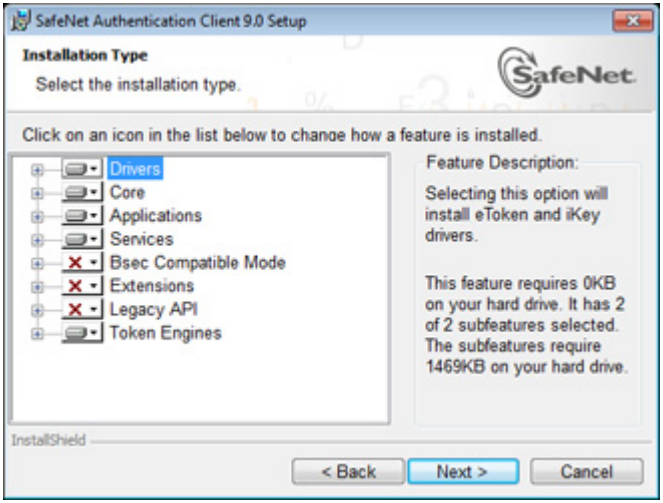


12 Select one of the following:

- **Typical**: installs the most common application features (recommended)
- **Custom**: installs only the application features you select.

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

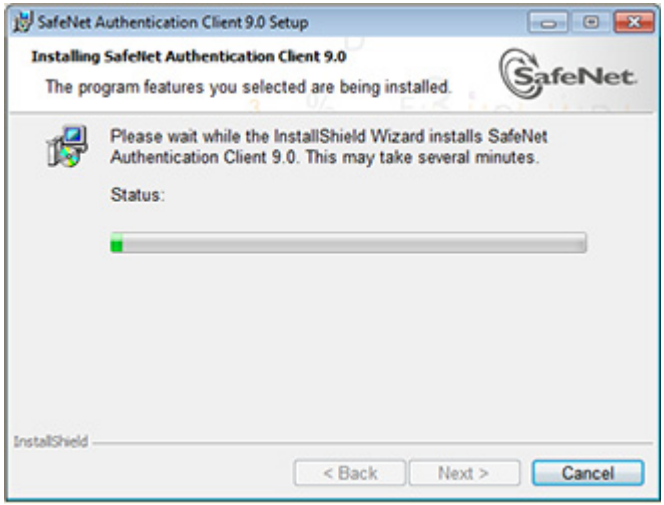
The *Custom Installation Type* window opens.



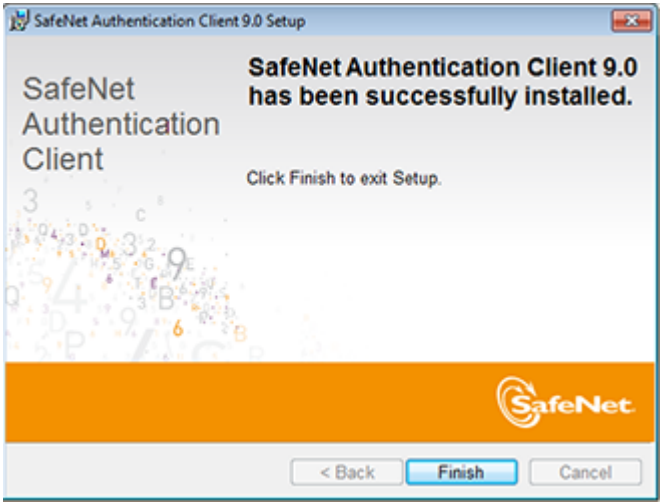
14 Use this window to enable or disable specific features. Some features cannot be disabled, as they are mandatory for the installation. For details on the specific installation features, see *Installing SafeNet Authentication Client on Windows (Simplified Installation)* on page 105

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

The installation proceeds.



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



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

Installing the MSI file via the Command Line

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

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

- for 32-bit systems:
  `msiexec /i SafeNetAuthenticationClient-x32-9.0.msi`
- for 64-bit systems:
  `msiexec /i SafeNetAuthenticationClient-x64-9.0.msi`

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

To install via the command line:

1. Log on as an administrator.
2. Close all applications.
3. To open the *Command Prompt* window, do one of the following, depending on your operating system:
   - From the Windows taskbar, select **Start > Programs > Accessories > Command Prompt**.
   - Right-click **Command Prompt**, select **Run as**, and set the user to administrator.
   - 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.

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-x32-9.0.msi /qn`
- For 64-bit systems:
  `msiexec /i SafeNetAuthenticationClient-x64-9.0.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 8: *Application Properties Hierarchy*, on page 184.

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-x32-9.0.msi PROPERTY=VALUE PROPERTY=VALUE /qb
  ```
- For 64-bit systems:
  ```
  msiexec /i SafeNetAuthenticationClient-x64-9.0.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 189.

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-x32-9.0.msi
ET_LANG_NAME=Spanish
PROP_ADVANCED_VIEW=0
PROP_CLEAR_REG=1 /qb
```

Command Line Installation Properties

Property	Description
PROP_ETOKENREADERCOUNT	on page 92
PROP_FAKEREADER	on page 93
PROP_IKEYREADERCOUNT	on page 93
PROP_LICENSE_FILE	on page 94
PROP_REG_FILE	on page 94

Deprecated Command Line Installation Properties

Property	Description
ET_LANG_NAME	on page 90
KSP_ENABLED	on page 91
PROP_ADVANCED_VIEW	on page 212
PROP_CLEAR_REG	on page 92
PROP_EXPLORER_DEFENROL	on page 234
PROP_PCSCSLOTS	on page 191
PROP_PQ_HISTORYSIZE	on page 247
PROP_PQ_MAXAGE	on page 246
PROP_PQ_MINAGE	on page 246
PROP_PQ_MINLEN	on page 245
PROP_PQ_MIXCHARS	on page 249
PROP_PQ_WARNPERIOD	on page 247
PROP_PROPAGATECACER	on page 237
PROP_PROPAGATEUSERCER	on page 236
PROP_SINGLELOGON	on page 189

Property	Description
PROP_SINGLELOGONTO	on page 190
PROP_SOFTWARESLOTS	on page 190
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 manually, that is imported to the computer's registry folder during the installation The default registry folder is HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC
Value	The path to a saved registry file **Note:** The full path must be used.
Default	none

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

PROP_UPD_INFPATH Property

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

TARGETDIR Property

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

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

Configuring Installation Features via the Command Line

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

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

```
msiexec /i SafeNetAuthenticationClient-x32-9.0.msi ADDDEFAULT=F1,F2…Fn INSTALLLEVEL=n
PROP_IKEYREADERCOUNT=n /qb
```

where

- SafeNetAuthenticationClient-x32-9.0 is the 32-bit SafeNet Authentication Client installation file. For 64-bit systems, use SafeNetAuthenticationClient-x64-9.0.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

See the table *SafeNet Authentication Client Features to Add or Remove* on page 110 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.

SafeNet Authentication Client Command Line Feature Names

Feature Parent Name	Command Line Feature Name	Description
DriverFeature	eTokenDrivers	Installs etoken and iKey drivers.
	BsecDrivers	
CoreFeature	eTokenCAPI	Installs a standard CAPI implementation for eToken and iKey devices.
	eTokenPKCS11	Installs a standard PKCS#11 API implementation for eToken and iKey devices. **Note:** This feature is mandatory.
	UIDialogs	Installs support for CAPI password dialogs. **Note:** This feature is mandatory.
	KSP	Registers SafeNet Key Storage Provider.
Applications	SACTools	Installs the SAC Tools application for eToken and iKey token support.

Feature Parent Name	Command Line Feature Name	Description
Services **Note:** This feature is mandatory.	SACService	Installs eToken Service for eToken and iKey token support. **Note:** This feature is mandatory.
	SACMonitor	Installs SafeNet Authentication Client Monitor for eToken and iKey token support. **Note:** This feature is mandatory.
BsecCompatibleMode **Note:** This feature is disabled in SAC 9.0 installation	BsecCAPI	Installs support for legacy iKey CAPI applications.
	BsecPKCS11	Installs support for legacy iKey PKCS#11 applications.
Extensions **Note:** This feature is disabled in SAC 9.0 installation	Identrust	Installs Identrust support. **Note:** To use this feature, you must enable the 'Bsec Compatible Mode' feature.
	Entrust	Installs legacy Entrust support.
LegacyAPI **Note:** This feature is disabled in SAC 9.0 installation	eTokenSAPI	Installs proprietary supplementary API.
	etFSFeature	Installs Proprietary File System API.

Feature Parent Name	Command Line Feature Name	Description
TokenEngines	eTokenDevices: eTokenJava eTokenCardOS	Installs eToken JAVA and CardOS support. **Note:** the eToken Java feature is mandatory.
	iKey	Installs iKey token support.
	eTokenVirtual	Installs eToken Virtual 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 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-x32-9.0.msi

ADDEFAULT=eTokenDrivers,BsecDrivers,eTokenCAPI,eTokenPKCS11,UIDialogs,KSP,SACTools,SACService,SACMonitor,BsecCAPI,BsecPKCS11,Identrust,Entrust,eTokenSAPI,etFSFeature,eTokenJava,eTokenCardOS,iKey,eTokenVirtual /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-x32-9.0.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-x64-9.0.msi PROP_PCSCSLOTS=10
PROP_ETOKENREADERCOUNT=5 PROP_IKEYREADERCOUNT=3 PROP_SOFTWARESLOTS=2
PROP_FAKEREADER=0 /qb
```

NOTE

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-x32-9.0.msi ADDDEFAULT=
```

```
eTokenDrivers,etFSFeature,eTokenSAPI,eTokenPKCS11,eTokenCAPI,KSP,UIDialogs,SACMonitor
,SACService,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 (only iKey device) on a 32-bit system, type the following command:

```
msiexec /i SafeNetAuthenticationClient-x32-9.0.msi ADDDEFAULT=

BsecDrivers,etFSFeature,eTokenSAPI,eTokenPKCS11,eTokenCAPI,UIDialogs,SACMonitor,SACSe
rvice,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-x32-9.0.msi ADDDEFAULT=
eTokenDrivers,BsecDrivers,etFSFeature,eTokenSAPI,eTokenPKCS11,eTokenCAPI,KSP,UIDialog
s,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-x32-9.0.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-x32-9.0.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 *Installing SafeNet Authentication Client on Windows (Simplified Installation)* on page 105.)

NOTE

SafeNetAuthenticationClient-BSecUtilities-8.2.msi, which installs legacy BSec Utilities that can be used with BSec-compatible mode in SafeNet Authentication Client versions 9.0, is not packaged with SafeNet Authentication Client 9.0. 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-x32-9.0.msi REMOVE=F1,F2…,Fn /qb
```

where

- `SafeNetAuthenticationClient-x32-9.0.msi` is the 32-bit SafeNet Authentication Client installation file. For 64-bit systems, use `SafeNetAuthenticationClient-x64-9.0.msi`
- `REMOVE` indicates that the following features are to be removed
- `F`x is the name of each feature to be removed

See the table: *SafeNet Authentication Client Features to Add or Remove* on page 110 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-x32-9.0.msi
REMOVE=SACTools /qb
```

Installing SafeNet Authentication Client on Windows (Simplified Installation)

The simplest way to install SafeNet Authentication Client 9.0 is to use the SafeNetAuthenticationClient-x32-x64-9.0.exe simplified installation file.

NOTE
This installer file does not support Customization Tool changes.

The SafeNetAuthenticationClient-x32-x64-9.0.exe simplified installation file uninstalls older SAC versions, and then installs SafeNet Authentication Client 9.0 properly on 32-bit and 64-bit environments in each of the following situations:

- No middleware is yet installed (Installation only)
- For details on how to upgrade, see *Chapter 4 Upgrading Using the SafeNet Authentication Client MSI File on page 62*

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

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

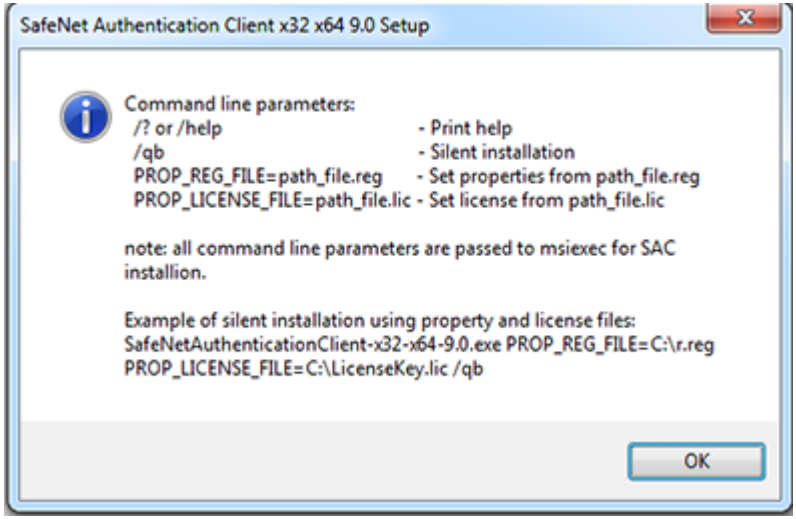
- Double-click the **SafeNetAuthenticationClient-x32-x64-9.0.exe** file.

Command Line Parameters via the Simplified Installation

All the command line parameters that are described in the section: *Installing the MSI file via the Command Line* on page 84, can also be entered when installing the simplified installation.

From the command line, enter: `SafeNetAuthenticationClient-x32-x64-9.0.exe /h`

The help window opens.



Configuring Root Certificate Storage for Win Server 2008 R2

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

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

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

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc`

   For more information about creating and editing registry keys, see *Setting Registry Keys Manually* on page 186.

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.

Installing SafeNet Authentication Client on a Mac OS X

The installation packaging for SafeNet Authentication Client 9.0 (Mac) is PackageMaker.

The installation package is `SafeNetAuthenticationClient.9.0.x.0.dmg`.

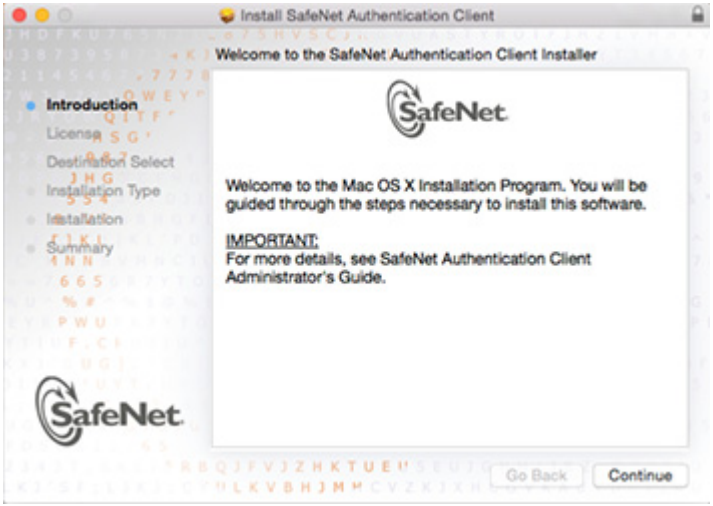
To install with the installer:

1 Double click the `SafeNetAuthenticationClient.9.0.x.0.dmg` file.

A new disk image file is created in the Finder window, including an mpkg installation file and an uninstall application.

2 To start the installation, double click **SafeNet Authentication Client 9.0.mpkg**.

The *Welcome to the SafeNet Authentication Client Installer* window opens.



3 Click **Continue**.

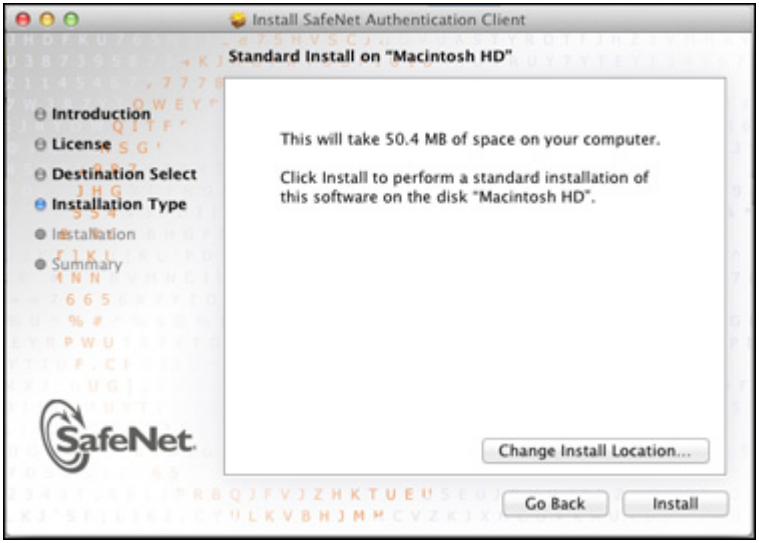
The *Software License Agreement* window opens.

4 Click **Continue**.

The agreement window opens.

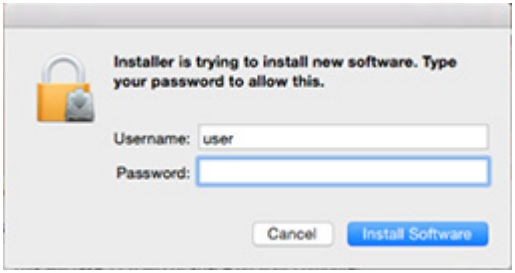
5 Click **Agree** to accept the software license agreement.

The *Standard Install on Macintosh HD* window opens.



6 Click **Install**.

The *Authenticate* window opens.



7 Enter *Name* and *Password* and click **OK**.

NOTE Administrator permissions are required to install SafeNet Authentication Client.

SafeNet Authentication Client installs.

The *Installation completed successfully* screen opens.

8 Click **Restart**.

Mac OS X restarts.

9 Log in again to Mac OS X.

Installing SAC from the Mac Terminal

To install from the Mac terminal:

1. Extract the *SafeNet Authentication Client 9.0.mpkg* file from the dmg file.
2. At the location in the terminal in which you extracted the file run `sudo installer -pkg ./SafeNet\Authentication\Client\ 9.0.mpkg/ -target /`
3. Enter your root password when prompted.

   SafeNet Authentication Client 9.0 is installed.
4. Following installation, restart Mac OS X.

Preparing SAC (Mac) Custom Installation

The custom installation script creates an additional customized installation file (**SafeNet Authentication Client Customization 9.0.mpkg**) with specific license and configuration properties and values.

> **NOTE**
> Before installing the **SafeNet Authentication Client Customization 9.0.mpkg** file, you must install SAC 9.0.

To create a custom installation:

1. Copy the **Custom Installation** (packaged with the Mac installation) folder to your Mac PC.
2. Select the **Custom Installation\CustomerConfiguration** folder, and update the contents of the **eToken.conf** file with the relevant organization properties, and the **SacLicense.lic** file with the organization's license.
3. From the Mac terminal enter the command:

   ```
   cd [Custom Installation path]\CustomInstallScript.
   ```

4. Run the script:

   ```
   ./createSacCustomInstallation
   ```

   The file **SafeNet Authentication Client Customization 9.0.mpkg** is created in the **Custom Installation\output** folder.

5 The **SafeNet Authentication Client Customization 9.0.mpkg** file can now be distributed to all users in the organization as an additional SAC 9.0 installation.

Running SafeNet Authentication Client Customization 9.0.mpkg

By running the **SafeNet Authentication Client Customization 9.0.mpkg** file the following is implemented:

- The **/etc/eToken.conf** file (created by the Mac SAC 9.0 installation) is replaced by the **eToken.conf** file, located in the **Custom Installation\CustomerConfiguration** folder.
- The **SacLicense.lic** file, located in the **Custom Installation\CustomerConfiguration** folder is copied to the **/Users/Shared/SafeNet/SAC** folder.

Installing the Firefox Security Module (Mac)

When SafeNet Authentication Client is installed, it does not install the security module in Firefox. This must be done manually.

To install the security module in Firefox

1. Open **FireFoxPreferences > Advanced >Certificates.**
2. On the *Encryption* tab click **Security Devices**.

   The *Device Manager* window opens.
3. Click **Load**.

   The *Load PKCS#11 Device* window opens.
4. In the *Module Filename* field enter the following string:
   `/usr/local/lib/libeTPkcs11.dylib`

   The *Confirm* window opens.
5. Click **OK**.

   The new security module is installed.

Installing the Thunderbird Security Module

When SafeNet Authentication Client is installed, it does not install the security module in Thunderbird. This must be done manually.

To install the security module in Thunderbird

1. Select **Thunderbird > Preferences > Advanced**.
2. On the *Security* tab click **Security Devices**.

   The *Device Manager* window opens.
3. Click **Load**.

   The *Load PKCS#11 Device* window opens.
4. In the *Module Filename* field enter the following string:
   /usr/local/lib/libeTPkcs11.dylib

   The *Confirm* window opens.
5. Click **OK**.

   The new security module is installed.

Configuring Acrobat Security Settings

Adobe Acrobat can be configured to protect PDF documents using a .CER certificate.

NOTE The following instructions refer to Adobe Acrobat X. Different versions may use a different procedure. See Adobe documentation for more details.

To set Adobe Acrobat security settings:

1. Select the **Tools** tab.
2. Select **Edit > Protection > Security Settings.**

   The *Security Settings* window opens.
3. Select **PKCS#11 Modules and Tokens**.
4. If a PKCS#11 Module is not attached, click **Attach Module,** browse to the required PKCS#11 module and click **Open**.
5. Close the Security Settings window and select **Sign & Certify >More Sign & Certify > Manage Trusted Identities**.

   The *Manage Trusted Identities* window opens.
6. Click **Add Contacts**.

   The *Choose Contact to Import* window opens.

7 Click **Browse**.

The *Locate Certificate File* wind opens.

8 Browse to the required root CA certificate (.cer) and click **Open**.

You are returned to the *Choose Contact to Import* window. The user associated with the certificate is displayed in the *Contact* box.

9 Select the contact.

The certificate is displayed in the *Certificates* box.

10 Select the certificate and click **Trust**.

The *Import Trust Settings* window opens.

11 Select the required trust settings and click **OK**.

You are returned to the *Choose Contacts to Import* window.

The *Import Completed* window confirms the import.

12 Click **OK** to close the *Import Completed* window.

NOTE To verify the security settings:

1. Select **Tools > Sign & Certify > More Sign & Certify > Manage Trusted Identities**.
   The *Manage Trusted Identities* window opens.
2. Select the contact and click **Details**.
   The *Edit Contact* window opens.
3. Select the contact and click **Show Certificate...**
   The *Certificate Viewer* Window opens.
4. Select the **Trust** tab.
   - Trusted settings for the certificate are marked with a green check-mark.
   - Non-trusted settings are marked with a red cross.

Installing SAC on Linux Standard Package

Installing on Red Hat Enterprise, SUSE, CentOS, or Fedora

The installation package for SafeNet Authentication Client on RedHat, SUSE, CentOS, or Fedora is the RPM Package. RPM is an installation file that can install, uninstall, and update software packages.

NOTES:

For the PKCS11 module to be installed automatically on a Firefox browser during the SAC installation, make sure the **nss-tools** package is installed prior to installing SAC.

- On SUSE, Fedora, Centos or Red Hat operating systems, in cases where the nns-tool package is not installed, install it as a privileged user by running the following command: **yum install nss-tools**.

SafeNet Authentication Client .rpm packages include:

- **.rpm Package Name:**
  - 32-bit

    SafenetAuthenticationClient-9.0.n-0.i386.rpm
  - 64-bit

    SafenetAuthenticationClient-9.0.n-0.x86_64.rpm
- **where:**

  n is the build number

To install from the package installer:

1. Double-click the relevant `.rpm` file.

   The package installer opens.

2. Click Install Package.

   A password prompt appears.

3. Enter the Super User or root password. The installation process runs.

To install from the terminal:

1. On the terminal, log on as a root user.
2. Run the following:

   ```
   rpm --import RPM-GPG-KEY-SafenetAuthenticationClient
   ```

3. Run one of the following:

   - On a 32-bit OS:

     ```
     rpm -hi SafenetAuthenticationClient-9.0.n-0.i386.rpm
     ```

   - On a 64-bit OS:

     ```
     rpm -hi SafenetAuthenticationClient-9.0.n-0.x86_64.rpm
     ```

   - where:

     -hi is the parameter for installation

     n is the version number

Installing on Ubuntu

NOTES:

- When installing from the user interface with a user that is not an administrator, the following message is displayed: 'The package is of bad quality'. Click **Ignore and Install** and continue with the installation.
- For the PKCS11 module to be installed automatically on a Firefox browser during the SAC installation, make sure the **nss-tools** package is installed prior to installing SAC.
  - On Ubuntu 14.04, install it by running the following command: **sudo apt-get install libnss3-tools**

The installation packaging for SafeNet Authentication Client running on Ubuntu is the Debian software package (.deb).

The following is the SafeNet Authentication Client .deb package:

- **.deb Package Name:**
  - 32-bit

    SafenetAuthenticationClient-9.0.n-0_i386.deb
  - 64-bit

    SafenetAuthenticationClient-9.0.n-0_amd64.deb
- **where:**

  n is the build number

To install from the package installer:

1 Double-click the relevant `.deb` file.

The package installer opens.

2 Click Install Package.

A password prompt appears.

3 Enter the Super User or root password.

The installation process runs.

4 To run SafeNet Authentication Client Tools, go to **Applications > SafeNet > SafeNet Authentication Client > SafeNet Authentication Client Tools.**

NOTES:
To enable the tray icon menu in the notification area, log out and log back in for the icon to appear.

To install from the terminal:

1 Enter the following:

- On a 32-bit OS:

```
sudu dpkg -i SafenetAuthenticationClient-9.0.n-0_i386.deb
```

- On a 64-bit OS:

```
sudu dpkg -i SafenetAuthenticationClient-9.0.n-0_amd64.deb
```

- where:

n is the version number

A password prompt appears.

2. Enter the password.

   The installation process runs.

3. If the installation fails due to a lack of dependencies, enter the following:

   ```
   sudo apt-get install -f
   ```

   The dependencies are installed and the installation continues.

4. To run the SafeNet Authentication Client Quick Menu, go to: **Applications > SafeNet > SafeNet Authentication Client > SafeNet Authentication Client Tools**.

NOTES:
Ensure you log out and log back in to see the tray icon menu.

Installing a 32-bit Compatibility Package on a 64-bit OS

The 32-bit Compatibility Package enables 32-bit applications to work with SAC on 64-bit systems.

The standard SAC 9.0(Linux) 64-bit version must be installed on the computer before the 32-bit Compatibility Package is installed.

Installing on Red Hat Enterprise, SUSE, CentoS or Fedora

SafeNet Authentication Compatibility .rpm packages include:

- **.rpm Package Name:**
  SAC-32-CompatibilityPack-9.0.n-0.x86_64.rpm
- **where:**
  n is the build number

To install from the package installer:

1. Double-click the `.rpm` file.
   The package installer opens.
2. Click Install Package.
   A password prompt appears.

3 Enter the Super User or root password.

The installation process runs.

To install from the terminal:

1 On the terminal, log on as a root user.

2 Run the following:

```
rpm --import RPM-GPG-KEY-SafenetAuthenticationClient
```

3 Run one of the following:

- On a 64-bit OS:

  ```
  rpm -hi SAC-32-CompatibilityPack-9.0.n-0.x86_64.rpm
  ```

- where:

  -hi is the parameter for installation

  n is the version number

Installing on Ubuntu and Debian

SafeNet Authentication Compatibility .deb packages include:

- **.deb Package Name:**

  SAC-32-CompatibilityPack-9.0.n-0_amd64.deb

- **where:**

  n is the build number

To install from the package installer:

1. Double-click the .deb file.

   The package installer opens.

2. Click Install Package.

   A password prompt appears.

3. Enter the Super User or root password.

   The installation process runs.

To install from the terminal:

1. Enter the following:

   ```
   sudu dpkg -i SAC-32-CompatibilityPack-9.0.n-0_amd64.deb
   ```

   - where: n is the version number

   A password prompt appears.

2. Enter the password.

   The installation process runs.

3. If the installation fails due to a lack of dependencies, enter the following:

```
sudo apt-get install -f
```

The dependencies are installed and the installation continues.

Installing on Red Hat Enterprise, SUSE, CentOS or Fedora

The installation package for SafeNet Authentication Client running on RedHat, SUSE, CentOS, or Fedora is the RPM Package Manager. RPM is a command line package management system that can install, uninstall, and update software packages.

SafeNet Authentication Client .rpm packages include:

- **.rpm Package Name:**
  - 32-bit

    SafenetAuthenticationClient-core-9.0.n-0.i386.rpm
  - 64-bit

    SafenetAuthenticationClient-core-9.0.n-0.x86_64.rpm
- **where:**

  n is the build number

To install from the package installer:

1. Double-click the relevant `.rpm` file.

   The package installer opens.

2 Click Install Package.

A password prompt appears.

3 Enter the Super User or root password.

The installation process runs.

To install from the terminal:

1 On the terminal, log on as a root user.

2 Run the following:.

```
rpm --import RPM-GPG-KEY-SafenetAuthenticationClient
```

3 Run one of the following:

- On a 32-bit OS:

  ```
  rpm -hi SafenetAuthenticationClient-core-9.0.n-0.i386.rpm
  ```

- On a 64-bit OS:

  ```
  rpm -hi SafenetAuthenticationClient-core-9.0.n-0.x86_64.rpm
  ```

- where:

  -hi is the parameter for installation

  n is the version number

Installing on Ubuntu and Debian

NOTE:

- When installing from the user interface with a user that is not an administrator, the following message is displayed: 'The package is of bad quality'. Click **Ignore and Install** and continue with the installation.
- After installing SAC on Ubuntu, log off, and then log back on in order for the SAC monitor to run, and to display the tray icon.

The installation packaging for SafeNet Authentication Client running on Ubuntu is the Debian software package (.deb).

The following is the SafeNet Authentication Client .deb package:

- **.deb Package Name:**
  - 32-bit

    SafenetAuthenticationClient-core-9.0.n-0_i386.deb
  - 64-bit

    SafenetAuthenticationClient-core-9.0.n-0_amd64.deb
- **where:**

  n is the build number

To install from the package installer:

Double-click the relevant `.deb` file.

The package installer opens.

1. Click Install Package.

   A password prompt appears.

2. Enter the Super User or root password.

   The installation process runs.

To install from the terminal:

1. Enter the following:

   - On a 32-bit OS:

     ```
     sudu dpkg -i SafenetAuthenticationClient-core-9.0.n-0_i386.deb
     ```

   - On a 64-bit OS:

     ```
     sudu dpkg -i SafenetAuthenticationClient-core-9.0.n-0_amd64.deb
     ```

   - where: n is the version number

   A password prompt appears.

2. Enter the password. The installation process runs.
3. If the installation fails due to a lack of dependencies, enter the following:

   ```
   sudo apt-get install -f
   ```

   The dependencies are installed and the installation continues.

Installing the Firefox Security Module (Linux)

When SafeNet Authentication Client is installed, it may not install the security module in Firefox. In cases where it is not installed, then install it manually.

To install the security module in Firefox

1. Select **Settings > Advanced**.
2. On the *Encryption* tab click **Security Devices**.

   The *Device Manager* window opens.
3. Click **Load**.

   The *Load PKCS#11 Device* window opens.
4. In the *Module Filename* field enter the following string:
   `/usr/lib/libeTPkcs11.so`

   The *Confirm* window opens.
5. Click **OK**. The new security module is installed.

Linux External Dependencies

Red Had Enterprise, SUSE, CentOS or Fedora

- PCSC (Smart Card Resource manager): libpcsclite1

Ubuntu

- PCSC (Smart Card Resource manager): libpcsclite1

Loading the Token PKCS#11 Security Module

To run SafeNet Authentication Client, the token PKCS#11 security module (libeTPkcs11.so) must be loaded. When working with Thunderbird, load the token PKCS#11 security module manually.

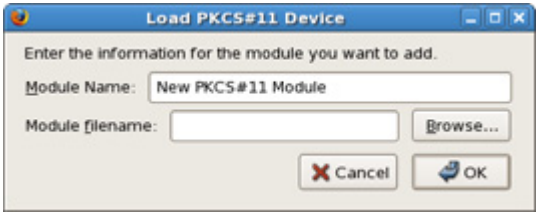
NOTE
Ensure that there is only one loaded security module having a path with the value: `libeTPkcs11.so`.

To ensure that the Token PKCS#11 module is loaded:

1. Do one of the following:
   - When working with Firefox, go to **Edit > Preferences > Advanced > Certificates > Security Devices**.
   - When working with Thunderbird, go to **Edit > Preferences > Advanced > Certificates > Security Devices**.

   The *Device Manager* window opens
2. If **eToken** is not listed in the *Security Modules and Devices* column, click **Load**.

   The *Load PKCS#11 Device* dialog box opens.



3 Do the following:

- Replace the contents of the *Module Name* field with **eToken**.
- In the *Module filename* field, enter the following:

  `/usr/lib/libeTPkcs11.so`

NOTE
The *Module fields* are case sensitive.

4 Click **OK**.

The *Confirm* window opens.

5 Click **OK**.

The *Alert* window opens.

6 Click **OK**.

Token is listed in the *Security Modules and Devices* column of the *Device Manager* window.

Click **OK** to exit the *Device Manager*.

6 Uninstall

After SafeNet Authentication Client 9.0 has been installed, it can be uninstalled. Local administrator rights are required to uninstall SafeNet Authentication Client. When SafeNet Authentication Client is uninstalled, user configuration and policy files are deleted.

In this chapter:

Uninstall Overview (Windows)

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 141
- *Uninstalling via the Command Line* on page 142

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 9.0**, 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-x32-9.0.msi` (for 32-bit installations)

   `msiexec /x SafeNetAuthenticationClient-x32-9.0.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 9.0 using the wizard. See *Installing SafeNet Authentication Client on Windows (MSI)* on page 76.
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 SafeNet Authentication Client on Windows (MSI)* on page 78.
3. Clear the **Use the existing configuration settings** option, and continue the installation.
4. Uninstall SafeNet Authentication Client 9.0.

Uninstalling Standard Package (Linux)

Uninstalling on Red Had Enterprise, SUSE, CentOS, Fedora, or Debian

To uninstall:

- Enter the following:

```
rpm -e SafenetAuthenticationClient
```

where `-e` is the parameter for uninstall

Uninstalling on Ubuntu

To uninstall:

- In the console, enter the following:

```
sudo dpkg --purge safenetauthenticationclient
```

where `--purge` is the parameter for uninstall.

Uninstalling 32-bit Compatibility Package on 64-bit OS

Uninstalling on Red Hat Enterprise, SUSE, CentOS, Fedora, or Debian

To uninstall:

- Enter the following:

  ```
  SAC-32-CompatibilityPack-9.0.38-0.x86_64.rpm
  ```

  where `-e` is the parameter for uninstall

Uninstalling on Ubuntu

To uninstall:

- In the console, enter the following:

  ```
  SAC-32-CompatibilityPack-9.0.38-0_amd64.deb
  ```

where `--purge` is the parameter for uninstall

Uninstalling Core Package

Uninstalling on Red Had Enterprise, SUSE, CentOS, or Fedora

To uninstall:

- Enter the following:

  `SafenetAuthenticationClient-core-9.0.38-0.i386.rpm`

  where `-e` is the parameter for uninstall

Uninstalling on Ubuntu

To uninstall:

- In the console, enter the following:

  `SafenetAuthenticationClient-core-9.0.38-0_i386.deb`

  where `--purge` is the parameter for uninstall

Uninstalling - MAC

Before uninstalling SafeNet Authentication Client (Mac) 9.0, make sure that SafeNet Authentication Client Tools is closed.

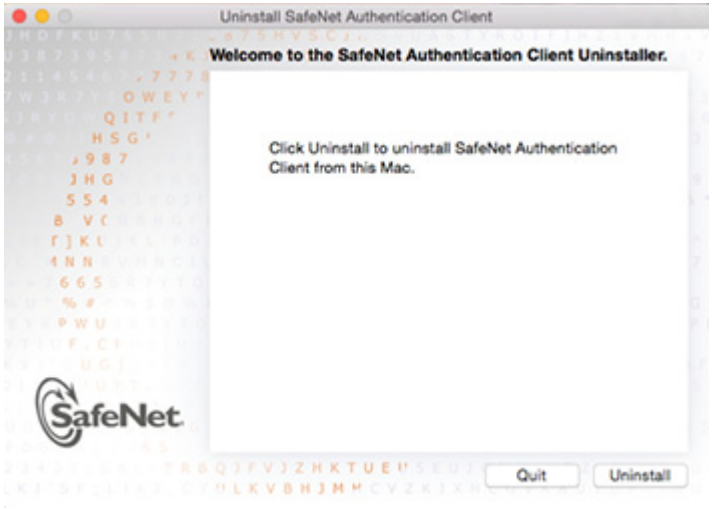
To uninstall SafeNet Authentication Client (Mac) 9.0

1 Double click *SafeNetAuthenticationClient.9.0.x.0.dmg* file.

A new disk image file is created in the Finder window, including an mpkg installation file and an uninstall application.

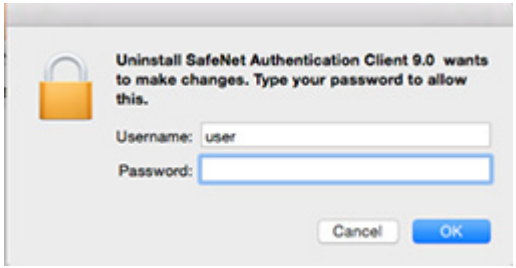
2 Click **Uninstall SafeNet Authentication Client (Mac) 9.0**.

The *Welcome to the SafeNet Authentication Client Uninstaller* window opens



3 Click **Uninstall**.

The *Authenticate* window opens



4 Enter **Name and Password** and click **OK**.

> **NOTE** You require Administrator permissions to uninstall SafeNet Authentication Client (Mac) 9.0.

SafeNet Authentication Client uninstalls and the *Uninstallation completed successfully* window opens

5 Click **Quit**.

7 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.

Sample Administrative Template files provided by SafeNet:

Sample File	Configuration
SAC_9_0.adm	SafeNet Authentication Client settings
SAC_9_0.admx	SafeNet Authentication Client settings
SAC_9_0.adml	File of English strings

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

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

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

The sample Administrative Template files provided by SafeNet are configured to write registry settings to:

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SafeNet\Authentication\SAC`

The values in this folder have a higher priority than values in any other registry folder. See *Application Properties Hierarchy* on page 184 for an explanation of the registry folders.

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

NOTE

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

Adding SafeNet Authentication Client Settings

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

- To add the Administrative Templates to Windows Server 2008 SP1 or Windows Server 2008 R2 SP1, do one of the following:
  - Add a standard ADM Administrative Template file. See *Adding an ADM file to Windows Server 2008 / R2* on page 154.
  - Add an XML-based ADMX Administrative Template file. See *Adding an ADMX file to Windows Server 2008 / R2* on page 160.
- To add the Administrative Templates to a client computer, see *Adding an ADM file to a Client Computer* on page 161.

Configuring SAC Password prompt Settings

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

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

- Ensure the certificate you are using includes a **Non Repudiation OID**.
- Ensure the certificate you are using includes an **Identity OID**.

- Open SAC tools>Advanced View>Token Settings>Advanced Tab, and set the **RSA key secondary authentication** parameter to **Token authentication on application request**.
- **Logout Mode** setting is **True**.

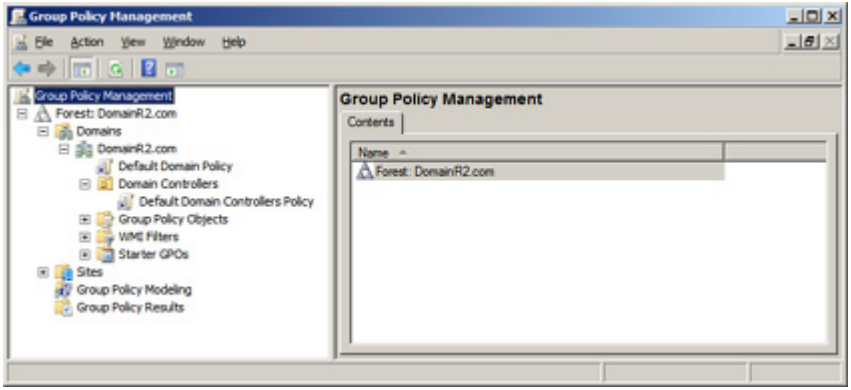
Adding an ADM file to Windows Server 2008 / R2

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

To add SafeNet Authentication Client settings:

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

   The *Group Policy Management* window opens.

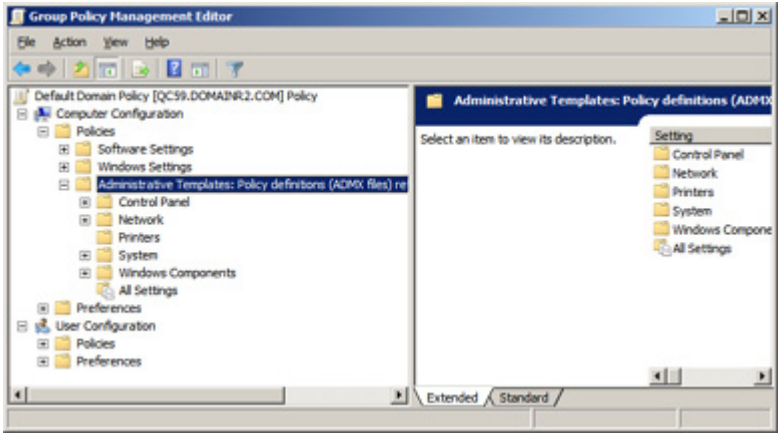


3 Do one of the following:

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

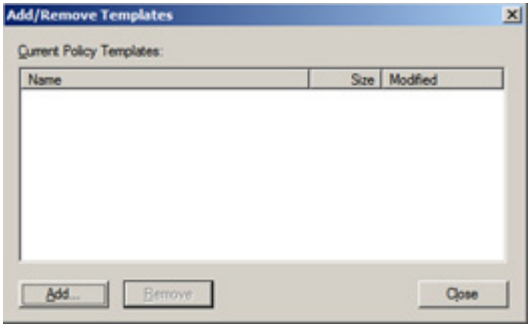
4 From the dropdown menu, select **Edit**.

The *Group Policy Management Editor* opens.



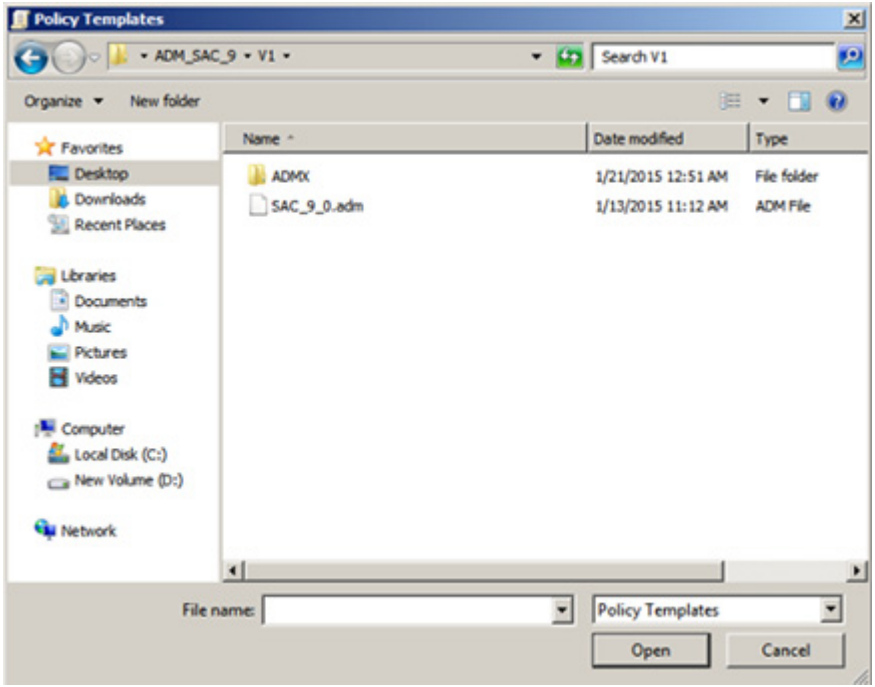
5 Under **Computer Configuration > Policies**, right-click **Administrative Templates: Policy definitions (ADMX files)**, and select **Add/Remove Templates.**

The *Add/Remove Templates* window opens.



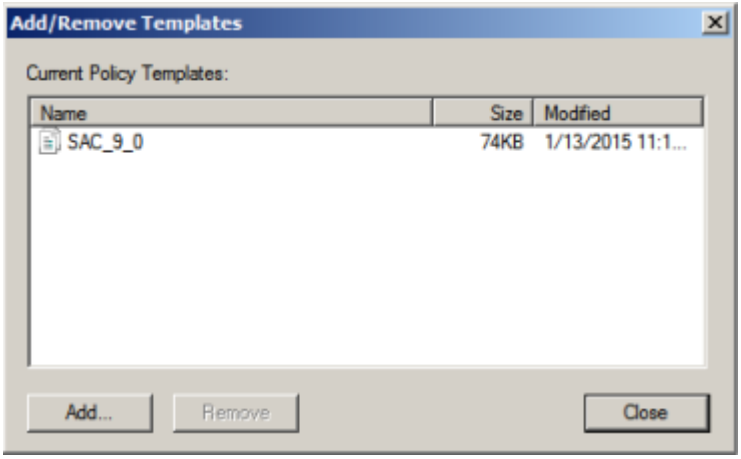
6 Click **Add**, and browse to the appropriate ADM file.

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



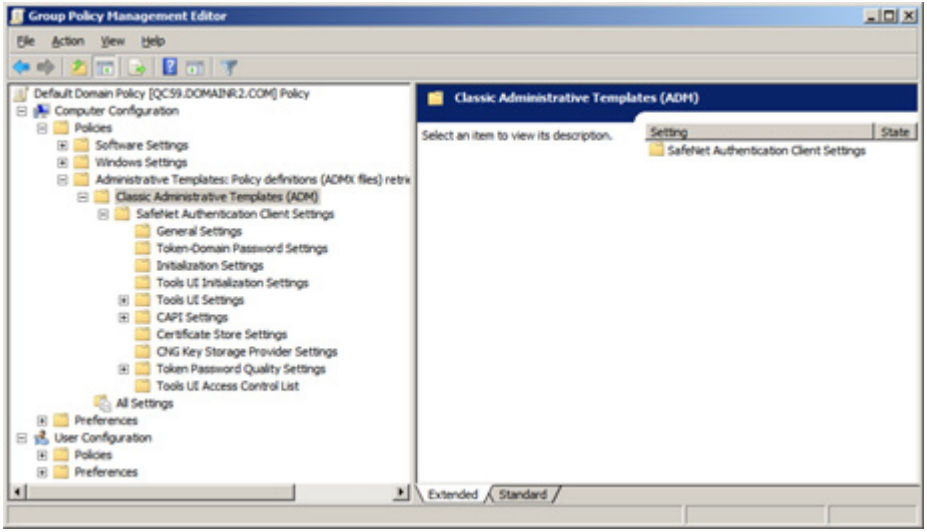
7 Select the file, and click **Open.**

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



8 Click **Close.**

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



Adding an ADMX file to Windows Server 2008 / R2

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

To add SafeNet Authentication Client settings:

1. Copy the file `SAC_9_0.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_9_0.adml`) to a language folder in the following location:
   `C:\Windows\PolicyDefinitions\`

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

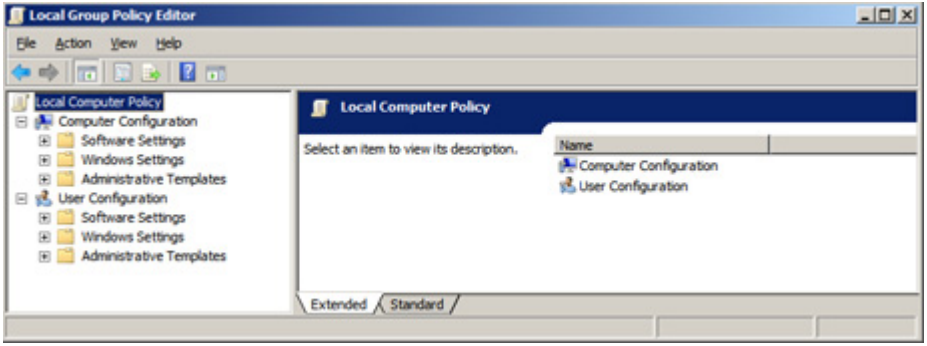
Adding an ADM file to a Client Computer

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

To add SafeNet Authentication Client settings:

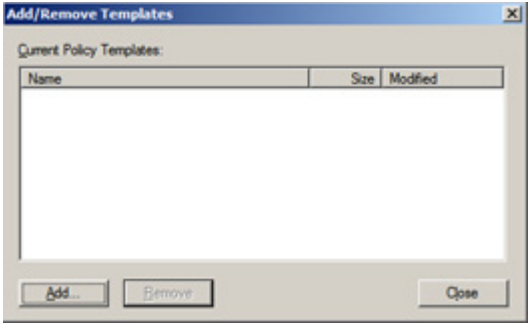
1. From the Windows taskbar, select **Start > Run**.
2. In the *Run* dialog box, enter **gpedit.msc**, and click **OK**.

   The *Local Group Policy Editor* opens.



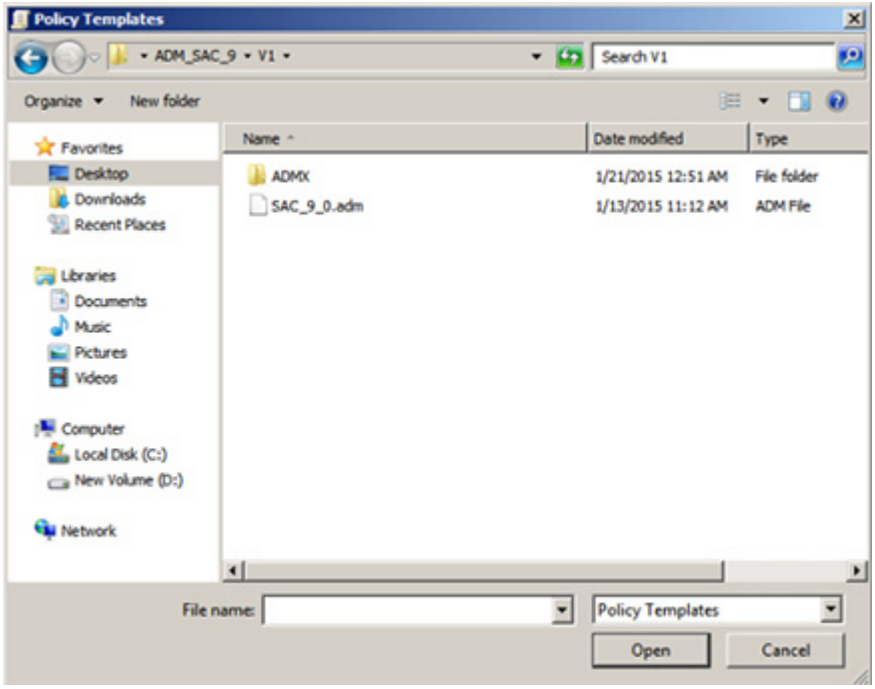
3 Under the **Computer Configuration** node, right-click **Administrative Templates**, and select **Add/Remove Templates.**

The *Add/Remove Templates* window opens.



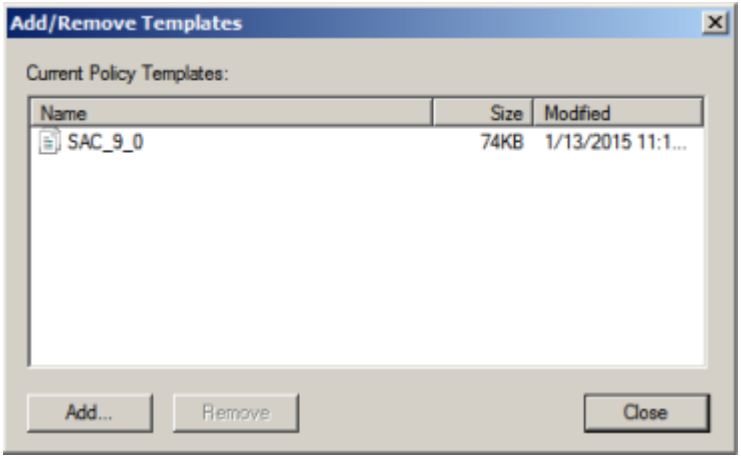
4 Click **Add**, and browse to the appropriate ADM file.

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



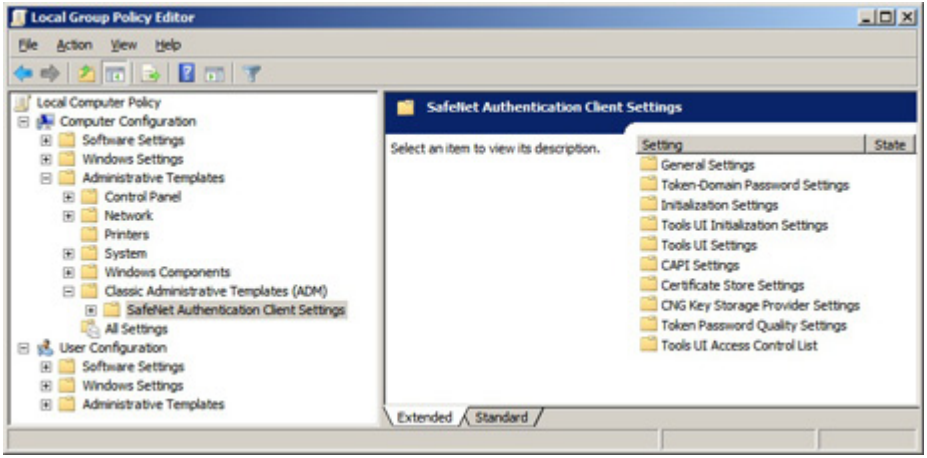
5 Select the file, and click **Open.**

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)**.


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 180.

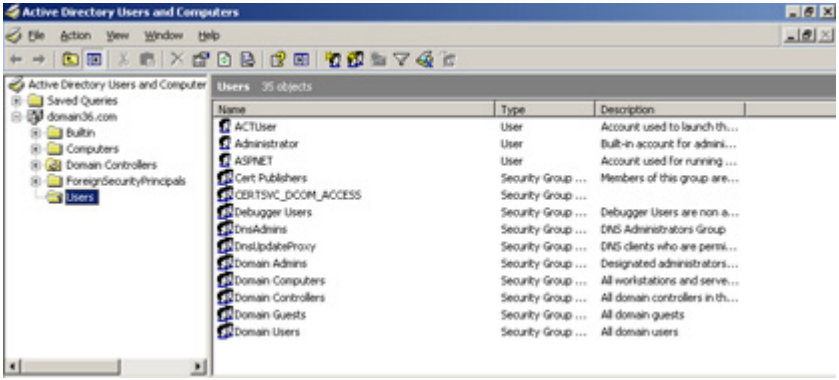
- To edit the policy settings on Windows Server 2003 or Windows Server 2003 R2, see *Editing Settings in Windows Server 2003 / R2* on page 166.
- To edit the policy settings on Windows Server 2008 or Windows Server 2008 R2, see *Editing Settings in Windows Server 2008 / R2* on page 175.
- To edit the policy settings on a client computer, see *Editing Settings on a Client Computer* on page 177.

Editing Settings in Windows Server 2003 / R2

To edit SafeNet Authentication Client settings:

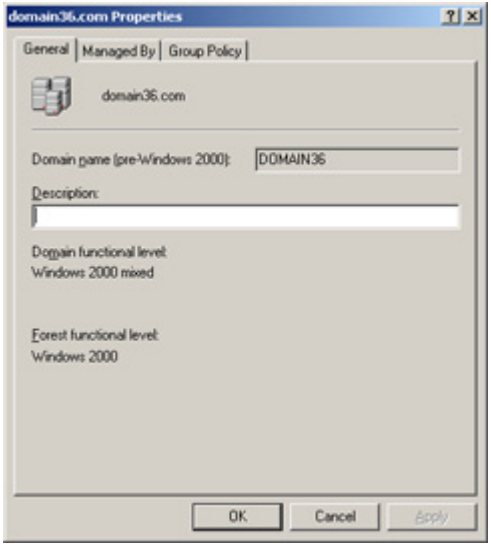
1 From the Windows taskbar, select **Start > Programs > Administrative Tools > Active Directory Users and Computers.**

The *Active Directory Users and Computers* window opens.

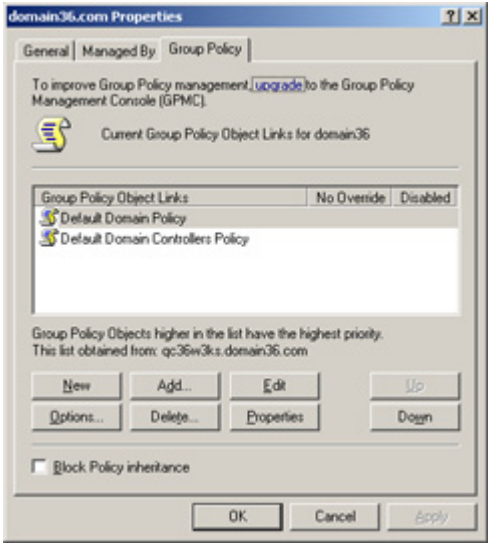


2 In the left pane, right-click the domain node, and select **Properties.**

The *Properties* window opens.



3 Select the *Group Policy* tab.

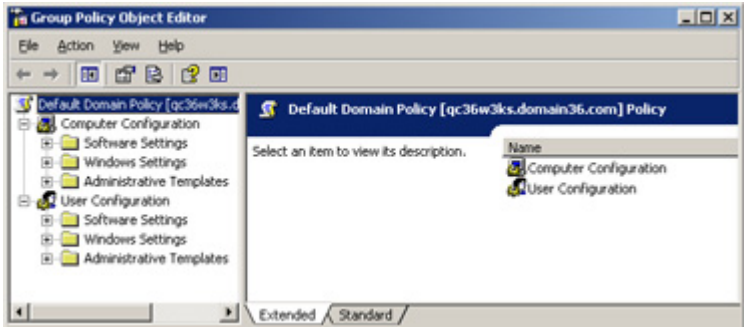


4 Do one of the following:

- 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**.

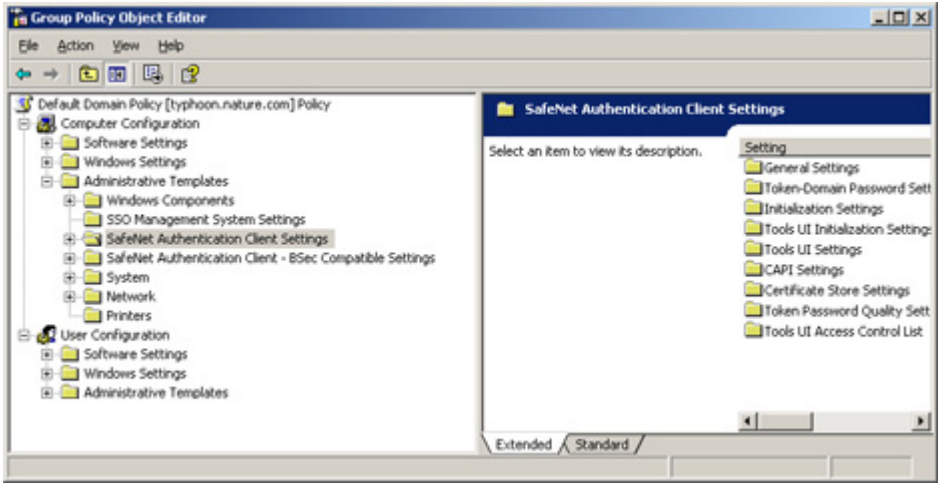
5 Click **Edit**.

The *Group Policy Object Editor* opens.



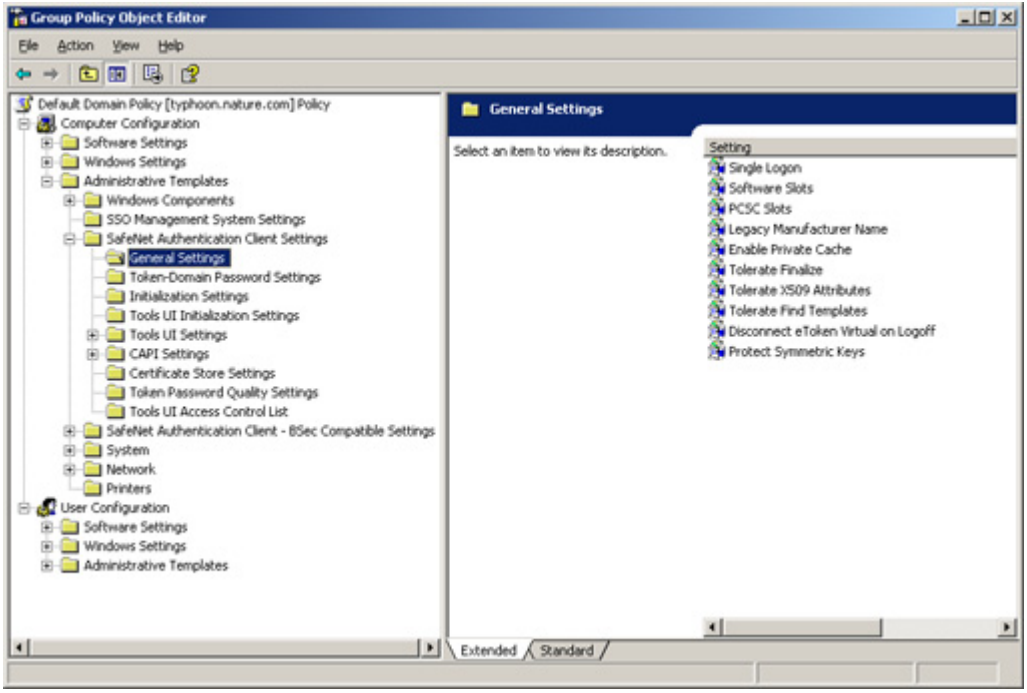
6 In the left pane, navigate to **Computer Configuration > Administrative Templates**, and select one of the **SafeNet Authentication Client Settings** nodes.

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



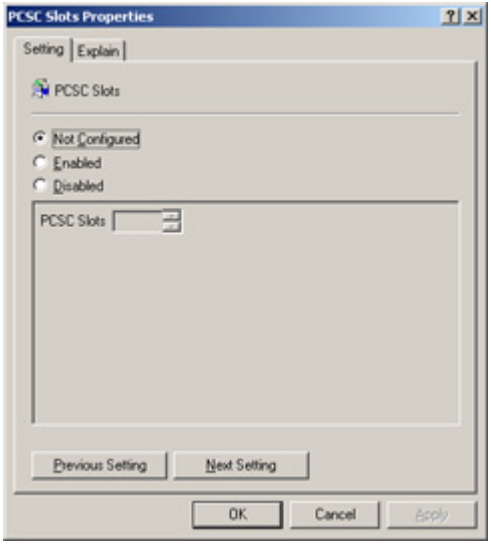
8 Select the settings folder to edit.

The settings are displayed in the right pane.



9 Double-click the setting to edit.

In this example, the *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 8: *Configuration Properties*, on page 180.

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.

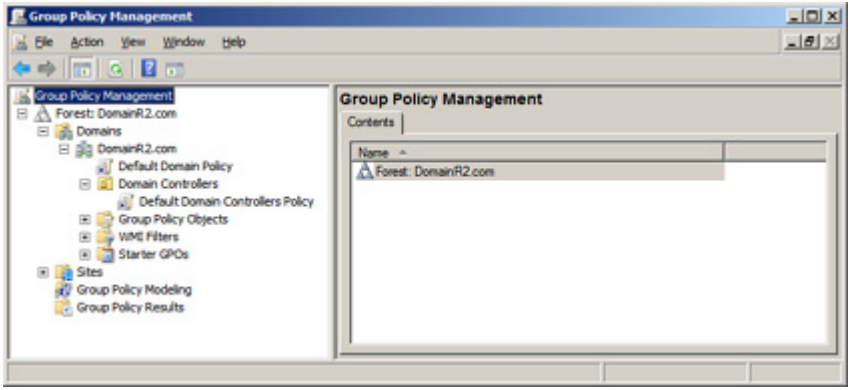
The registry is updated.

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.

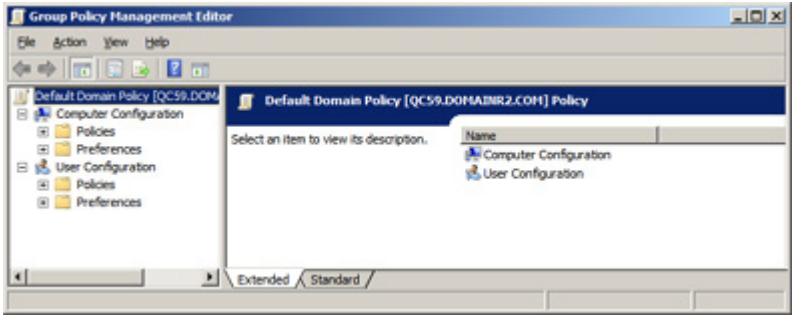


3 Do one of the following:

- 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.

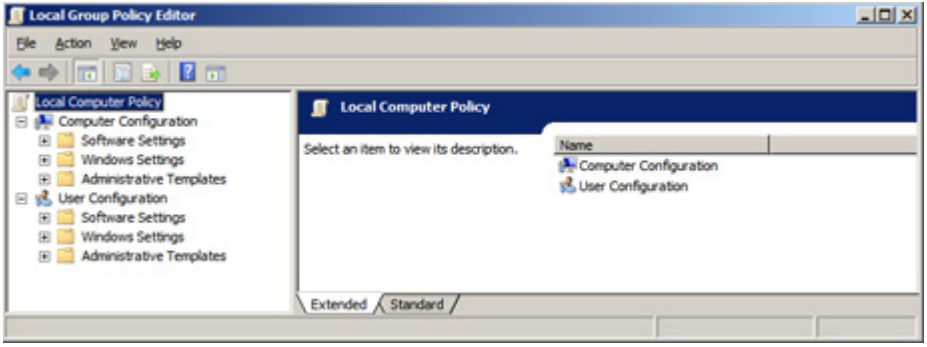
7 Continue from *Editing Settings in Windows Server 2003 / R2* step 8, on page 171.

Editing Settings on a Client Computer

To edit SafeNet Authentication Client settings:

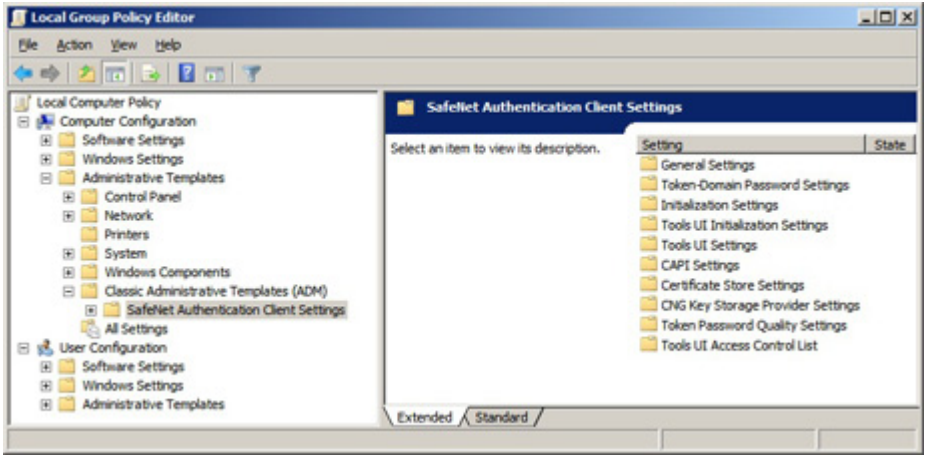
1. From the Windows taskbar, select **Start > Run**.
2. In the *Run* dialog box, enter **gpedit.msc**, and click **OK**.

   The *Local Group Policy Editor* opens.



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

   The settings are displayed in the right pane.



5 Continue from *Editing Settings in Windows Server 2003 / R2* step 8, on page 171.

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.

8 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
- Log Settings
- IdenTrust Settings

Mac:

This chapter provides administrator guidelines for setting configuration keys.

- Configuration Files
- eToken.conf Configuration Keys
- Apple Key Chain

This chapter describes how to set configurable keys.

NOTE
The Logging button is displayed only if the user has permissions to write to the eToken.conf file. Super Users are able to write to the eToken.conf file. Any other users must obtain permissions.

In this chapter:

Setting SafeNet Authentication Client Properties

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

- Define the property during command line installation of SafeNet Authentication Client (but not during repair). See *Installing the MSI file via the Command Line* on page 84.
  The property name, and not the registry value name, is needed when setting the value during command line installation.
- Set a value using the SafeNet Authentication Client Tools application.
  See the *SafeNet Authentication Client User's Guide*.
  Neither the registry value name nor the property name is needed.

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

- Set a value using the Administrator Templates (ADM/ADMX) policy settings.
  See Chapter 7: *SafeNet Authentication Client Settings*, on page 150.
  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 186.
  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`
   Requires administrator permissions.
5. SafeNet Authentication Client default value

Hierarchy Implications

The applications properties hierarchy has the following implications:

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

  These values override values set by any other method.

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

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

- When you set properties during command line installation, the properties (except for `PROP_REG_FILE`) are written to: `HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC`.
- When you set properties manually, write them to their appropriate registry keys in any of the registry folders listed in the Hierarchy List on page 184. 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
HID Slots Defines the total number of HID slots for all HID USB tokens.	**Setting name:** HID Slots **Values:**=0, =4, >=0 0 - 5200 token works in VSR mode. 4 = 5200 HID token works in HID mode (4 slots). **Default**: 4	**Registry Value Name:** HIDSlots **Values**: =0, =4, >=0 **Default**: 4 slots	Property name: PROP_HIDSLOTS
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.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Enable Private Cache Determines if SafeNet Authentication Client allows the token's private data to be cached Applies only to tokens that were initialized with the private data cache setting. The private data is cached in per process memory. **Note:** Can be set in SafeNet Authentication Client Tools	**Setting name:** Enable Private Cache Values: **Selected** - Private data caching is enabled **Not selected** - Private data caching is disabled **Default**: Selected	**Registry Value Name:** EnablePrvCache **Values**: **1 (True)** - Private data caching is enabled **0 (False)** - Private data caching is disabled **Default**:1 (True)	Cannot be set by command line installation.
Tolerate Finalize Determines if C_Finalize can be called by DllMain **Note:** Define this property per process Select this setting when using Novell Modular Authentication Service (NMAS) applications only	**Setting name:** Tolerate Finalize Values: **Selected** - C_Finalize can be called by DllMain **Not selected** - C_Finalize cannot be called by DllMain **Default**: Not selected	**Registry Value Name:** TolerantFinalize **Values**: **1 (True)** - C_Finalize can be called by DllMain **0 (False)** - C_Finalize cannot be called by DllMain **Default**: 0 (False)	Cannot be set by command line installation

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
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, and Entrust details, remove the OID value from the registration key value.	**Setting name:** Override Non-Repudiation OIDs **Value**: Empty **Default**: No override	**Registry Value Name:** NonRepudiationOID **Value**: Empty **Default**: No override	Cannot be set by command line installation.

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 94.

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**: 1-15 **Default**: 15	**Registry Value Name:** UserMaxRetry **Values**: 1-15 **Default**: 15	Cannot be set by command line installation.
Maximum Administrator Password Retries Defines the default number of consecutive failed administrator logon attempts that lock the token.	**Setting name:** Maximum Administrator Password Retries **Values**: 1-15 **Default**: 15	**Registry Value Name:** AdminMaxRetry **Values**: 1-15 **Default**: 15	Cannot be set by command line installation.

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**: Not Selected	**Registry Value Name:** ReadLabelFromToken **Values**: **1** -The current Token Name is displayed **0** -The current Token Name is ignored **Default**: 1	Cannot be set by command line installation.

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
Maximum number of 1024-bit RSA keys Defines the amount of space to reserve on the token for Common Criteria certificates that use 1024 -bit RSA keys.	**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**: Not Selected	**Registry Value Name:** CertificateExpiryAlert **Values**: **1 (True)** - Notify the user **0 (False**) - Do not notify the user **Default**: 1 (True)	Cannot be set by command line installation.

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. **Note:** This parameter is 'Day Sensitive' i.e. the system counts the day's and not the hour in which the user made the change.	**Setting Name:** Password - Maximum Usage Period **Values**: >=0 (0 =No expiration) **Default**: 0	**Registry Key Name:** pqMaxAge **Values**: >=0 (0 =No expiration) **Default**: 0	PROP_PQ_MAXAGE
Password - Minimum Usage Period Defines the minimum number of days between password changes. **Note:** Can be set in SafeNet Authentication Client Tools. **Note:** Does not apply to iKey devices.	**Setting Name:** Password - Minimum Usage Period **Values**: >=0 (0 = No minimum) **Default**: 0	**Registry Key Name:** pqMinAge **Values**: >=0 (0 = No minimum) **Default**: 0	PROP_PQ_MINAGE

Description (Cont.)	Settings in GPO Editor or MMC (Cont.)	Registry Key (Cont.)	Command Line (Cont.)
Password - Expiration Warning Period Defines the number of days before expiration during which a warning is displayed. **Note:** Can be set in SafeNet Authentication Client Tools.	**Setting Name:** Password - Expiration Warning Period **Values**: >=0 (0 = No warning) **Default**: 0	**Registry Key Name:** pqWarnPeriod **Values**: >=0 (0 = No warning) **Default**: 0	PROP_PQ_WARNPERIOD
Password - History Size Defines the number of recent passwords that must not be repeated. **Note:** Can be set in SafeNet Authentication Client Tools.	**Setting Name:** Password - History Size **Values**: >= 0 (0 = No minimum) **Default**: 10	**Registry Key Name:** pqHistorySize **Values**: >= 0 (0 = No minimum) **Default**: 10 (iKey device history is limited to 6)	PROP_PQ_HISTORYSIZE

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.

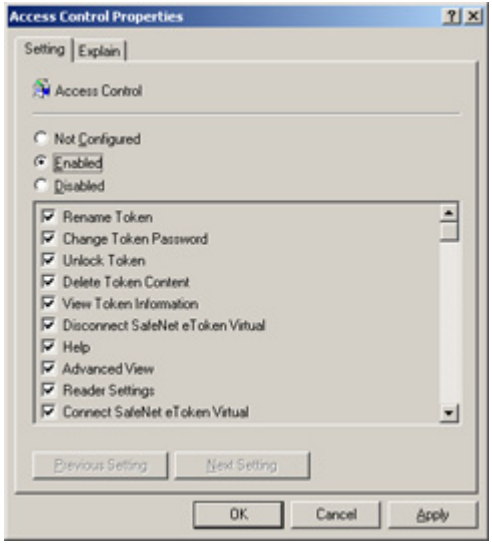
Description (Cont.)	Settings in GPO Editor or MMC (Cont.)	Registry Key (Cont.)	Command Line (Cont.)
Password Quality Check on Initialization Determines if the password quality settings are checked and enforced when a token is initialized **Note:** We recommend that this policy not be set when tokens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

Log Settings

The following settings are written to the appropriate folder's

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

These settings may be defined using:
HKEY_LOCAL_MACHINE or HKEY_CURRENT_USER

Description	ADM File Setting	Registry Value	Command Line
Enabled Determines if the SafeNet Authentication Client Log feature is enabled.	Not supported	**Registry Value Name:** Enabled **Value**: 1 - Enabled 0 - Disabled **Default**: 0 (Disabled)	
Days Defines the number of days log files will be saved from the time the log feature was enabled.	Not supported	**Registry Value Name:** Days **Value**: Enter the number of days (numerical). **Default**: 1 day	

Description (Cont.)	ADM File Setting (Cont.)	Registry Value (Cont.)	Command Line
MaxFileSize Defines the maximum size of an individual log file. Once the maximum fil size is reached, SAC removes older log records to allow saving newer log information.	Not supported	**Registry Value Name:** MaxFileSize **Value**: Enter a value in Bytes. **Default**: 2000000 (Bytes) (Approximately 2MB)	
TotalMaxSizeMB Defines the total size of all the log files when in debug mode. (Megabytes).	Not supported	**Registry Value Name:** TotalMaxSizeMB **Value**: Enter a value in Megabytes. **Default**: 0 (Unlimited)	
ManageTimeInterval Defines how often the TotalMaxSize parameter is checked to ensure the total maximum size has not been exceeded.	Not supported	**Registry Value Name:** ManageTimeInterval **Value**: Enter a value in minutes (numerical). **Default**: 60 minutes	

The following settings are written to the appropriate folder's

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

These settings may be defined using:

HKEY_LOCAL_MACHINE or HKEY_CURRENT_USER

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

IdenTrust Settings

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

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

Configuration Files (Mac)

SafeNet Authentication Client installs two configuration files:

- `/etc/eToken.conf`
  Requires administrator permissions `(-rw-rw-r--)`
- `/etc/eToken.common.conf`
  Does not require administrator permissions `(-rw-rw-rw-)`

Owner: root\admin

NOTE eToken.common.conf contains settings for SafeNet eToken Virtual use only.

Configuration Files Hierarchy

To enable hierarchical priorities, up to three different versions of the `eToken.conf` configuration file can be created. For each key, the setting found in the file with highest priority determines the application's behavior.

This design simulates the SafeNet Authentication Client (Windows) registry logic.

Windows Registry	Mac Installer	File Name	Priority	File Permissions
LM/Policies	Not provided	/etc/eToken.policy.conf	1(High)	Root
CU	Automatically created by GUI	~/.eToken.conf (located in user's home directory)	2	User
LM	Provided	/etc/eToken.conf	3	Root
LM	Provided	/etc/eToken.common.conf for eToken Virtual connections		All

NOTE /etc/eToken.policy.conf can be created manually by the system administrator.

Automatic Save of Configuration Files

When SafeNet Authentication Client is uninstalled, the configuration files are saved to:

```
/etc/eToken.conf.saved
/etc/eToken.common.conf.saved
```

The saved files can then be used to copy the settings to a new installation.

eToken.conf Configuration Keys

All keys that are not related to SafeNet eToken Virtual are located in `/etc/eToken.conf`.

All SafeNet eToken Virtual keys are located in `/etc/eToken.common.conf`.

General

Key Name	Description	Value	Default
PcscSlots	Number of PC/SC slots	1-16	3
SoftwareSlots	Number of software slots	1-10	2
ClientlessHID	eToken NG Flash 5.3 Anywhere	VID_0529&PID_3004	Not available

NOTE On a Mac OS X, the number of slots is determined by the `PcscSlots` and `SoftwareSlots` configuration keys described here. The *Reader Settings* window in SafeNet Authentication Client (Mac) Tools displays the number of slots that have been configured, but does not allow the user to change the settings.

InitApp

Key Name	Description	Values	Default
FIPS	FIPS Support 0 = disabled 1= enabled	0 = disabled 1= enabled	0

PQ

Key Name	Description	Value	Default
pqMinAge	Total number of days required before a password change 0 = none	>=0	0
pqMinLen	Minimum password length	>=4	6
pqMixChars	Mixed characters required 0 = disabled 1= enabled	0/1	1
pqWarnPeriod	Total number of days before expiration to display warning 0 = no warning	>=0	0

UI

Key Name	Description	Value	Default
LanguageId	UI Language (supports English only)	EN	EN
linguist	Path to Linguist application		
ExpiryAlertPeriodStart	Defines the number of days before a certificate's expiration date during which a warning message is displayed	>=0 (0 = No warning)	30
FutureAlertMessage	Defines the warning message to display in a balloon during a certificate's 'Certificate Expiration Warning Period' The message can include the following keywords: 1. $EXPIRY_DATE – the certificate's expiration date 2. $EXPIRE_IN_DAYS – the number of days until expiration	Message or empty	A certificate on your token expires in $EXPIRE_IN_DAYS days.'

Key Name (Cont.)	Description (Cont.)	Value (Cont.)	Default (Cont.)
PastAlertMessage	Defines the warning message to display in a balloon if a certificate's expiration date has passed	Message or empty	'Update your token now.'
IgnoreExpiredCertificates	Determines if expired certificates are ignored, and no warning message is displayed for expired certificates	♦ Selected - Expired certificates are ignored ♦ Not selected - A warning message is displayed if the token contains expired certificates	Not selected
AlertTitle	Defines the title to display in certificate expiration warning messages	Message or empty	'SafeNet Authentication Client'
ActionDetailedMessage	If 'Show detailed message' is selected in the 'Warning Message Click Action' setting, defines the detailed message to display	Message or empty	None
ActionWebSiteURL	If 'Open website' is selected in the 'Warning Message Click Action' setting, defines the URL to display	Message or empty	None

Key Name (Cont.)	Description (Cont.)	Value (Cont.)	Default (Cont.)
UpdateAlertMinInterval	Defines the minimum interval, in days, between certificate expiration date verifications	>0	14 days
AlertMessageClickAction	Defines what happens when the user clicks the message balloon	0 = No action 1 = Show detailed message 2 = Open website	0
ShowInTray	Determines if the Tools tray icon is displayed when SafeNet Authentication Client is launched	♦ Never show ♦ Always show	Always show
ShowBalloonEvents	Determines if a notification balloon is displayed when a token is connected or disconnected	Selected = Displayed Not selected = Not displayed	Selected
CertificateExpiryAlert	Determines if a warning message is displayed when certificates on the token are about to expire	0 = Not selected - A message is not displayed 1 = Selected - A message is displayed	0

Apple Key Chain

Apple Keychain is Apple Computer's password management system in Mac OS X. Keychain Access is a Mac OS X application that allows the user to access the Apple Keychain and configure its contents.

SafeNet Authentication Client (Mac) provides a plug-in to support integration with Mac OS X Keychain Access. The plug-in is installed during SafeNet Authentication Client (Mac) installation.

Features Supported by Keychain Access

The SafeNet Authentication Client (Mac) Keychain Access integration supports the following features:

- Upload of certificates from the token to Keychain Access.
- Encryption and Decryption - by uploading certificates from a token to Keychain, they become available for applications, such as Mail, that can use the certificates to encrypt and decrypt mail messages.

Keychain Access Limitations

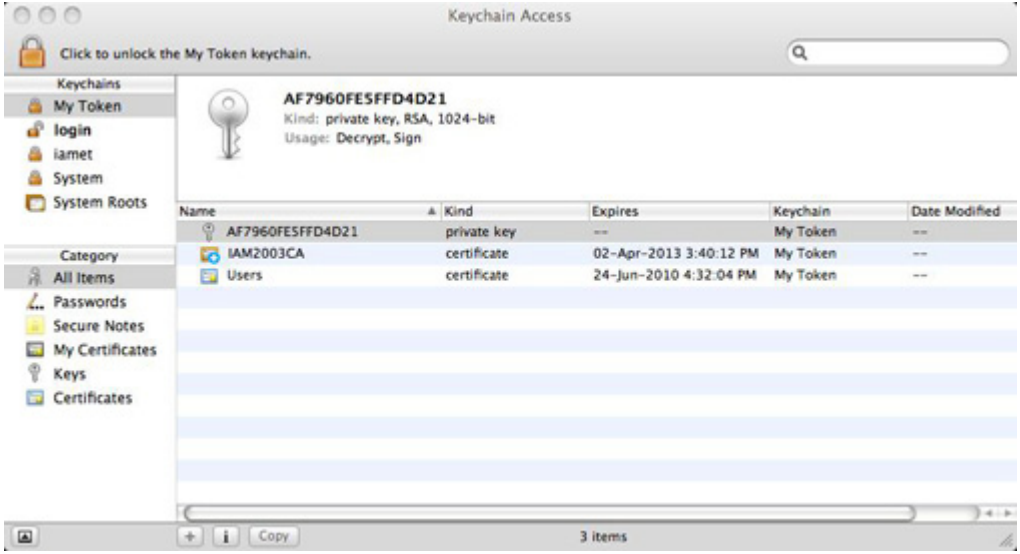
The following limitations apply when working with Keychain Access and SafeNet tokens.

- Keychain cannot be used to create new certificates. It can only upload certificates already located on the token.
- Change token password is not supported (however, it can be changed using SafeNet Authentication Client).
- Smartcards are not supported.
- It is not possible to import a certificate from a file to a token (however, certificates can be imported using SafeNet Authentication Client (Mac) Tools).
- The Keychain does not support RSA key generation to a token.

Displaying Token in Keychain Access

When you launch Keychain Access, you see a list of all the items in your Keychain, including information about each item's name, kind, creation date, and modification date.

When you insert a token, the device is displayed in the *Keychains* list.



To display token contents:

- In the *Keychains* list on the left of the window, select token, then select an item from the *Category* list.

  The details are displayed in the right section of the screen.

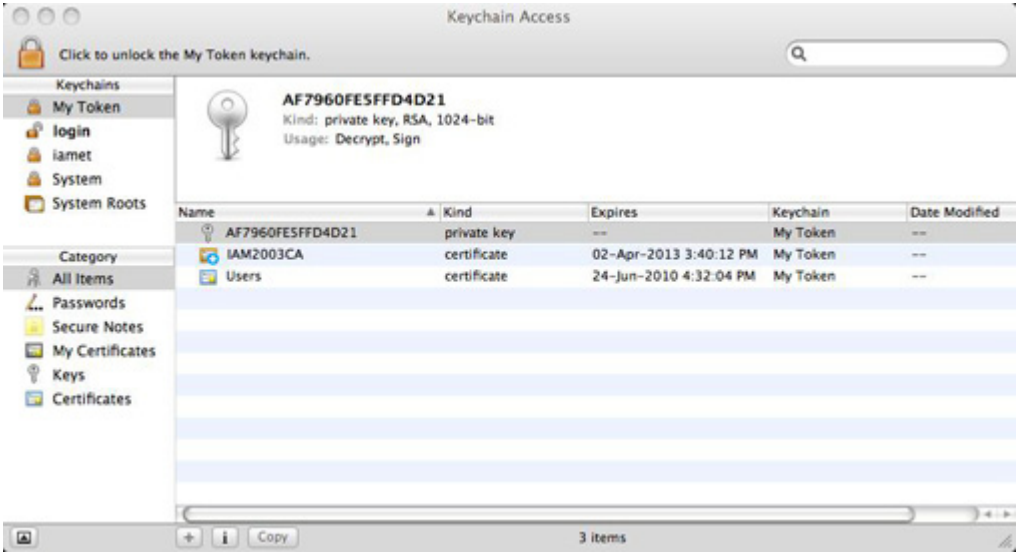
> **TIP** For details about performing additional functions with Keychain Access, refer to Mac OS X documentation.

Configuring Mac Keychain to Work with SSL and Secure Mail (S/MIME)

Mac Keychain must be configured to enable Safari to work with an SSL Connection and to enable encryption and decryption of emails.

To enable Mac Keychain to work with SSL and Secure Mail (S/MIME):

1 Open the *Keychain Access* window.



2 Double click on the root CA.

The window with the certificate details opens

3 Click on **Trust** to expand the section.

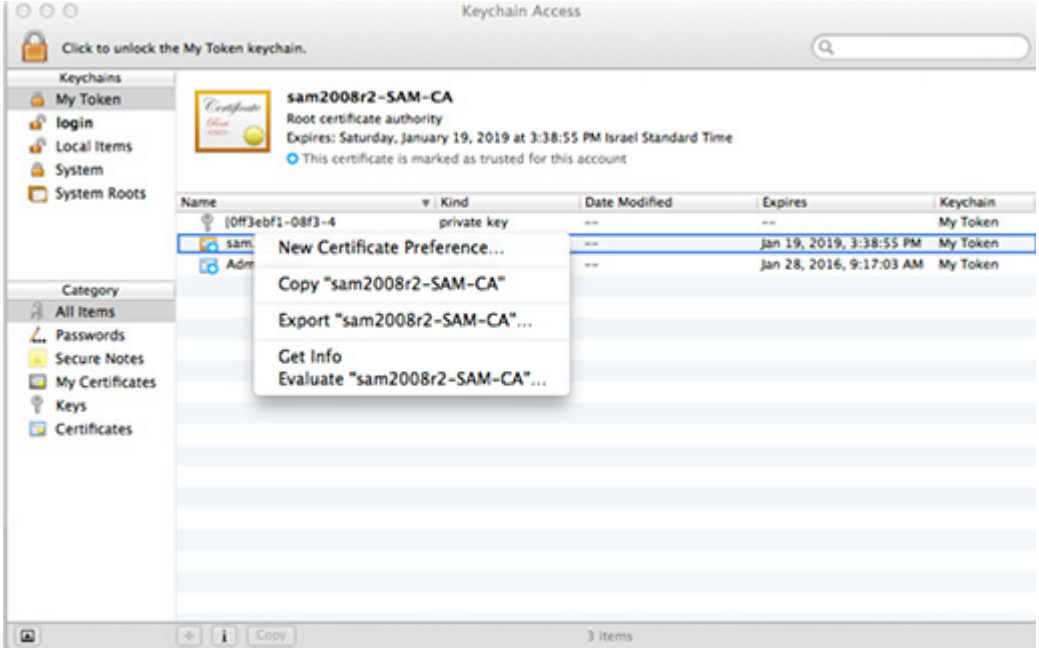
4 Set *Secure Socket Layer (SSL)* and/or *Secure Mail (S/MIME)* to **Always Trust**

5 Close the window.

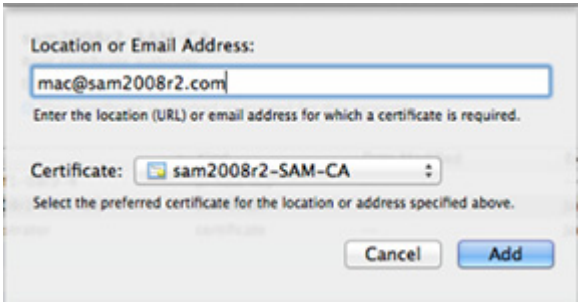
You are returned to the Keychain Access window.

The root CA certificate is now trusted for SSL and S/MIME operations.

6 Right click on the Users Certificate and select **New Certificate Preferences**.



The *Location or Email Address* window opens.



7 In the Certificate field, select the required certificate.

8 Do one of the following and click **Add**:

- For S/MIME, enter the email address of your mail account
- For SSL, enter the URL of your secured site.

The item is added to the *login* Keychain.

NOTE You must configure SSL for each required secured website.

If you configured Secure email (S/MIME), you will now be prompted to enter the token password when signing and sending an email or when decrypting an encrypted email.

If you configured SSL for your secured sites, when logging on with Safari you will be prompted for the token password.

Configuration Files (Linux)

SafeNet Authentication Client installs two configuration files

- eToken.conf: requires administrator permissions

  NOTE
  To enable the Enable Logging function in **Sac Tools>Advanced>Client Settings**, eToken.conf must have write permissions.

eToken.common.conf: does not require administrator permissions

NOTE
`eToken.common.conf` contains settings for SafeNet eToken Virtual use only.

Configuration Files Hierarchy

To enable hierarchical priorities, up to three different versions of the eToken.conf configuration file can be created. For each key, the setting found in the file with the highest priority determines the application's behavior. This design simulates the SafeNet Authentication Client (Windows) registry logic.

Windows Registry	Linux Installer	Linux File Name	Priority	File Permissions
LM/Policies	Not provided	/etc/eToken.policy.conf	1(High)	Root
CU	Automatically created by GUI	~/.eToken.conf(located in user's home directory)	2	User
LM	Provided	/etc/eToken.conf	3	Root
LM	Provided	/etc/eToken.common.conf for SafeNet eToken Virtual connections		All

NOTE
/etc/eToken.policy.conf can be created manually by the system administrator.

eToken.conf Configuration Keys

`eToken.conf` contains all keys not relating to SafeNet eToken Virtual. All SafeNet eToken Virtual keys are located in eToken.common.conf.

The configuration changes are effective only after SafeNet daemons and applications are restarted or after rebooting the machine.

The Key names must be placed in brackets and the Keys names and RegKey names and arguments are names are case sensitive.

The following is an example of the required syntax:

```
[UI]
LanguageId=en-US
linguist=/usr/share/eToken/languages/
Plugin32=/usr/lib/eToken/plugins/
LogoImages=/usr/share/eToken/LogoImages/
[GENERAL]
PcscSlots=4
SoftwareSlots=2
[LOG]
enabled=1
```