

# SafeNet Authentication Client (Linux)

**Version 8.3 Revision A**

**Administrator's Guide**



Copyright © 2013 SafeNet, Inc. All rights reserved.

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.

Date of publication: March 2013

Last update: Thursday, March 28, 2013 5:52 pm

## 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](mailto:support@safenet-inc.com)

### Website

You can submit a question through the SafeNet Support portal: <http://c3.safenet-inc.com/secure.asp>

## Additional Documentation

The following SafeNet publications are available:

- SafeNet Authentication Client 8.3 (Linux) Administrator's Guide (this document)
- SafeNet Authentication Client 8.3 (Linux) User's Guide
- SafeNet Authentication Client 8.3 (Linux) Customer Release Notes

# Table of Contents

Chapter 1: Introduction . . . . .	7
Overview. . . . .	8
SafeNet Authentication Client Main Features. . . . .	9
Supported Tokens . . . . .	11
Supported Localizations . . . . .	12
What's New . . . . .	13
SafeNet Authentication Client Architecture . . . . .	15
License Activation . . . . .	16
Chapter 2: System Requirements . . . . .	17
System Requirements. . . . .	18
Compatibility with Third Party Tools and Applications. . . . .	19
Chapter 3: Installation Files and External Dependencies . . . . .	20
Installation Files. . . . .	21
External Dependencies . . . . .	24
Red Hat Enterprise, SUSE, CentOS, or Fedora. . . . .	24
Ubuntu . . . . .	24

Chapter 4: Installation . . . . .	25
Installing Standard Package . . . . .	26
Installing on Red Hat Enterprise, SUSE, CentOS, or Fedora . . . . .	26
Installing on Ubuntu . . . . .	28
Installing 32-bit Compatibility Package on 64-bit OS . . . . .	31
Installing on Red Hat Enterprise, SUSE, CentOS, or Fedora . . . . .	31
Installing on Ubuntu . . . . .	32
Installing Core Package . . . . .	34
Installing on Red Hat Enterprise, SUSE, CentOS, or Fedora . . . . .	34
Installing on Ubuntu . . . . .	36
Upgrading . . . . .	39
Loading the Token PKCS#11 Security Module . . . . .	40
Chapter 5: Uninstall . . . . .	43
Uninstalling Standard Package. . . . .	44
Uninstalling on Red Hat Enterprise, SUSE, CentOS, or Fedora . . . . .	44
Uninstalling on Ubuntu . . . . .	44
Uninstalling 32-bit Compatibility Package on 64-bit OS. . . . .	45
Uninstalling on Red Hat Enterprise, SUSE, CentOS, or Fedora . . . . .	45
Uninstalling on Ubuntu . . . . .	45
Uninstalling Core Package. . . . .	46
Uninstalling on Red Hat Enterprise, SUSE, CentOS, or Fedora . . . . .	46
Uninstalling on Ubuntu . . . . .	46

Chapter 6: Configurable Settings . . . . .	47
Configuration Files . . . . .	48
Configuration Files Hierarchy . . . . .	49
eToken.conf Configuration Keys . . . . .	50
GENERAL . . . . .	51
INITAPP . . . . .	55
PQ . . . . .	59
UI . . . . .	68
INIT . . . . .	74
eToken.common.conf Configuration Keys . . . . .	77
ACCESSCONTROL . . . . .	77

# 1

# Introduction

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

## **In this chapter:**

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

# Overview

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

SafeNet Authentication Client provides 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 . It provides a unified middleware client for a variety of SafeNet smartcards, and SafeNet eToken devices.

Full backward compatibility means that customers who have been using eToken PKI Client can continue to use deployed eToken devices.

## **SafeNet Authentication Client includes the following features:**

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

- Token management operations, such as:
  - ◆ Token initialization
  - ◆ Token Password changes
  - ◆ Token unlock
  - ◆ Configuration of token settings and Token Password quality
  - ◆ Token renaming
  - ◆ Logging
- SafeNet Authentication Client settings configuration

# Supported Tokens

SafeNet Authentication Client 8.3 (Linux) supports the following tokens:

- SafeNet eToken 7300
- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 4100
- SafeNet eToken PRO
- SafeNet eToken PRO Anywhere (SC Operations only)
- SafeNet eToken PRO Smartcard
- SafeNet eToken NG-OTP
- SafeNet eToken NG-Flash
- SafeNet eToken NG-Flash Anywhere (Not protected Flash and SC operations only)
- SafeNet eToken Virtual Family

## NOTE

SafeNet Authentication Client 8.3 (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 for Windows and up.

# Supported Localizations

SafeNet Authentication Client 8.3 (Linux) supports the following languages:

- English

# What's New

SafeNet Authentication Client 8.3 (Linux) offers the following new features:

- Alignment with SafeNet's new branding.
- Supports selection of multiple tokens from the tray menu.
- Support for Elliptic Curve Cryptography (ECC)- a PKI encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys.

The following Elliptic Curves are supported:

- ◆ ECC\_CURVE\_P256 "1.2.840.10045.3.1.7"
- ◆ ECC\_CURVE\_P384 "1.3.132.0.34"

## NOTE

- ◆ eToken Virtual does not support Elliptic Curve Cryptography.
- ◆ SafeNet Authentication Client (Linux) supports many new configuration settings. For more details, see Chapter 7: (page 68).
- ◆ SafeNet Authentication Client (Linux) supports an updated list of Operating Systems. See Chapter 2: System Requirements (page 18).

- Support for Common Criteria (CC) certified devices and CC digital signatures.
- A new 32-bit compatibility package has been introduced to support 32-bit applications on 64-bit platforms. The user now has the choice of installing a 32-bit compatibility package to support 32-bit application on a 64-bit machine.

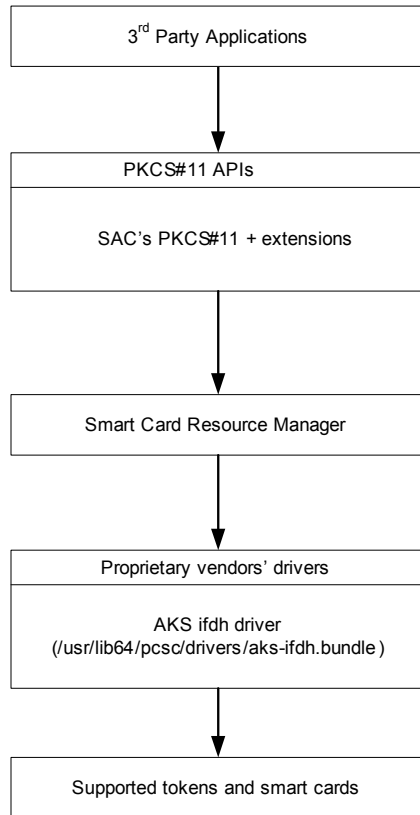
- Support the usage of 7300 tokens.

**NOTE**

eToken 7300 manageability functions (i.e. partitioning, initializing, image burn, etc.) will only be available with SafeNet Authentication Client for Windows version 8.2 onwards.

- Support for CAPI certificates (generated on MS platforms) used by OpenSSL and OpenSSH has been added.
- Support for new operating systems (See *System Requirements* on page 18)
- Additional configuration settings via the configuration file (See *Configurable Settings* on page 47)
- License keys are supported, and required (see *SafeNet Authentication Client 8.3 (Linux) User's Guide* for details)

# SafeNet Authentication Client Architecture



# License Activation

SafeNet Authentication Client 8.3 (Linux) is installed by default as non-licensed.

## To activate the licence perform the following steps:

- 1 Obtain a valid SafeNet License key from SafeNet Customer Service.
- 2 Activate the license using one of the following procedures
  - ◆ **Manual Activation** (For more information, see the *Licensing* chapter in the *SafeNet Authentication Client 8.3 (Linux) User's Guide*).
  - ◆ SafeNet Authentication Client retrieves the license file automatically, if the license file is located in the default path: `/home/<user name>`, and the license file is named `SACLicense.lic`



# 2

## System Requirements

Before installing SAC, ensure that your system meets the minimum requirements.

### **In this chapter:**

- System Requirements
- Compatibility with Third Party Tools and Applications

# System Requirements

Supported Operating Systems	◆ Red Hat 5.7 (32-bit and 64-bit) ◆ Red Hat 5.8 (32-bit and 64-bit) ◆ Red Hat 6.1 (32-bit and 64-bit) ◆ Red Hat 6.3 (32-bit and 64-bit)
	◆ Ubuntu 12.04 (32-bit and 64-bit) ◆ Ubuntu 12.10 (32-bit and 64-bit)
	Debian 6.0 (32-bit and 64-bit)
	SUSE Server 11 (32-bit and 64-bit)
	CentOS 6.3 (32-bit and 64-bit)
	◆ Fedora 17 (32-bit and 64-bit) ◆ Fedora 18 (32-bit and 64-bit)
Supported Browsers	Firefox 18
	Thunderbird 17

# Compatibility with Third Party Tools and Applications

SafeNet Authentication Client 8.3 (Linux) supports 3rd party applications that communicate over PKCS#11.

## NOTE

To make sure Firefox is automatically updated with the PKCS#11 security provider the ModUtil application which is part of the NSS package is required. 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 40.

## The following products are supported:

- openssh
- openssl
- pam-pkcs11
- pkcs11-tool
- openvpn
- Adobe Reader 9.5.x

# 3

## Installation Files and External Dependencies

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

### In this chapter:

- Installation Files
- External Dependencies

# Installation Files

The following installation and documentation files are provided:

File	Description	Environment	Use
SafenetAuthenticationClient-8.3.n-0.i386.rpm	Installs: SafeNet Authentication Client on 32 bit platform	32-bit	
SafenetAuthenticationClient-8.3.n-0.x86_64.rpm	Installs: SafeNet Authentication Client on 64 bit platform	64-bit	
SAC-32-CompatibilityPack-8.3.n-0.x86_64.rpm	Installs: SafeNet Authentication Client 32 bit Compatibility package on 64 bit platform	64-bit	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.
SafenetAuthenticationClient-8.3.n-0_i386.deb	Installs: SafeNet Authentication Client on 32 bit platform	32-bit	
SafenetAuthenticationClient-8.3.n-0_amd64.deb	Installs: SafeNet Authentication Client on 64 bit platform	64-bit	

File	Description	Environment	Use
SAC-32-CompatibilityPack-8.3.n-0_amd64.deb	Installs: SafeNet Authentication Client 32 bit Compatibility package on 64 bit platform	64-bit	
SafenetAuthenticationClient-core-8.3.n-0.i386.rpm	Installs: SafeNet Authentication Client core on 32 bit platform	32-bit	Installs eToken core library and IFD Handler.
SafenetAuthenticationClient-core-8.3.n-0.x86_64.rpm	Installs: SafeNet Authentication Client core on 64 bit platform	64-bit	Installs eToken core library and IFD Handler.
SafenetAuthenticationClient-core-8.3.n-0_i386.deb	Installs: SafeNet Authentication Client core on 32 bit platform	32-bit	Installs eToken core library and IFD Handler.
SafenetAuthenticationClient-core-8.3.n-0_amd64.deb	Installs: SafeNet Authentication Client core on 64 bit platform	64-bit	Installs eToken core library and IFD Handler.

File	Description	Environment	Use
SAC_8_3_Linux_CRN_Rev_A.pdf	Customer Release Notes		Read before installation, for last minute updates that may affect installation. Contains important information including troubleshooting, resolved and known issues.
SAC_8_3_Linux_User_Guide_Rev_A.pdf	8.3 User's Guide		Provides detailed information for the user and system administrator regarding the use of SafeNet Authentication Client
SAC_8_3_Linux_Admin_Guide_Rev_A.pdf	8.3 Administrator's Guide (this document)		Provides detailed information for the system administrator regarding the installation, configuration, maintenance, and management of SafeNet Authentication Client

# External Dependencies

## Red Hat Enterprise, SUSE, CentOS, or Fedora

- HAL packages: libhal1, hal-info, libhal-storage1
- PCSC (Smart Card Resource manager): libpcsclite1
- QT lib: libqt4-core, libqt4-gui (not required for core installation package)

### NOTE

To install QT on Red Hat 5.8, run the following command: `yum install qt4` (not required for core installation package).

## Ubuntu

- Autodepend



# 4

## Installation

SafeNet Authentication Client must be installed on each computer on which a SafeNet eToken, or SafeNet smartcard is to be used. Local administrator rights are required to install or uninstall SafeNet Authentication Client.

To customize the user interface and the features to be installed, see Chapter 6: , on page 25.

### In this chapter:

- Installing Standard Package
- Installing 32-bit Compatibility Package on 64-bit OS
- Installing Core Package
- Upgrading
- Loading the Token PKCS#11 Security Module

# Installing Standard Package

## 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-8.3.n-0.i386.rpm

- ◆ 64-bit

- SafenetAuthenticationClient-8.3.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-8.3.n-0.i386.rpm
```

- ◆ On a 64-bit OS:

```
rpm -hi SafenetAuthenticationClient-8.3.n-0.x86_64.rpm
```

- ◆ where:

-hi is the parameter for installation

n is the version number

# Installing on Ubuntu

**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.

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-8.3.n-0\_i386.deb
- ◆ 64-bit  
SafenetAuthenticationClient-8.3.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**.

**NOTE**

To enable the tray icon menu in the notification area, run the following command per user:

```
/usr/share/eToken/systray-whitelist.sh add SACMonitor
```

Ensure you log out and log back in for the changes to take effect.

**To install from the terminal:**

- 1 Enter the following:

- ◆ On a 32-bit OS:

```
sudo dpkg -i SafenetAuthenticationClient-8.3.n-0_i386.deb
```

- ◆ On a 64-bit OS:

```
sudo dpkg -i SafenetAuthenticationClient-8.3.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.**

**NOTE**

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

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

## Installing on Red Hat Enterprise, SUSE, CentoS, or Fedora

SafeNet Authentication Compatibility .rpm packages include:

- **.rpm Package Name:**  
SAC-32-CompatibilityPack-8.3.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-8.3.n-0.x86_64.rpm
```

◆ where:

-hi is the parameter for installation

n is the version number

## Installing on Ubuntu

SafeNet Authentication Compatibility .deb packages include:

■ **.deb Package Name:**

SAC-32-CompatibilityPack-8.3.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:  

```
sudo dpkg -i SAC-32-CompatibilityPack-8.3.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 Core Package

## 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-8.3.n-0.i386.rpm

- ◆ 64-bit

- SafenetAuthenticationClient-core-8.3.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-8.3.n-0.i386.rpm
```

- ◆ On a 64-bit OS:

```
rpm -hi SafenetAuthenticationClient-core-8.3.n-0.x86_64.rpm
```

- ◆ where:

-hi is the parameter for installation

n is the version number

# Installing on Ubuntu

**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.

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-8.3.n-0\_i386.deb

◆ 64-bit

SafenetAuthenticationClient-core-8.3.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.

**To install from the terminal:**

**1** Enter the following:

◆ On a 32-bit OS:

```
sudo dpkg -i SafenetAuthenticationClient-core-8.3.n-0_i386.deb
```

◆ On a 64-bit OS:

```
sudo dpkg -i SafenetAuthenticationClient-core-8.3.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.

# Upgrading

SafeNet Authentication Client 8.3 (Linux) does not support upgrading from previous SAC versions.

# 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 Firefox, the token PKCS#11 security module may have been loaded automatically during the SafeNet Authentication Client installation. 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 > Encryption > 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/lib/libTPkcs11.so`

**NOTE**

The *Module fields* are case sensitive.



**4** Click **OK**.

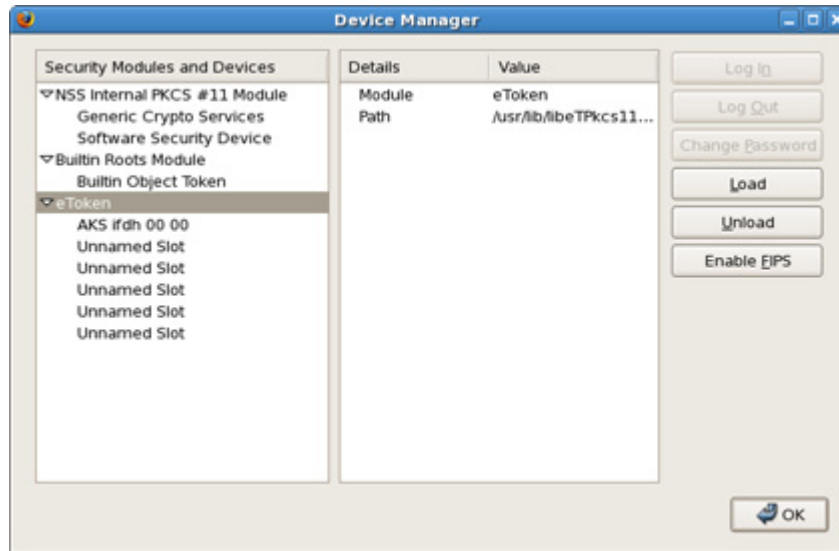
The *Confirm* window opens.

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*.

# 5

## Uninstall

After SafeNet Authentication Client has been installed, it may 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:**

- Uninstalling Standard Package
- Uninstalling 32-bit Compatibility Package on 64-bit OS
- Uninstalling Core Package

# Uninstalling Standard Package

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

### 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, or Fedora

### To uninstall:

- Enter the following:

```
rpm -e SAC-32-CompatibilityPack
```

where `-e` is the parameter for uninstall.

## Uninstalling on Ubuntu

### To uninstall:

- In the console, enter the following:

```
sudo dpkg --purge SAC-32CompatibilityPack
```

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

# Uninstalling Core Package

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

### To uninstall:

- Enter the following:

```
rpm -e SafenetAuthenticationClient-core
```

where `-e` is the parameter for uninstall.

## Uninstalling on Ubuntu

### To uninstall:

- In the console, enter the following:

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

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

# 6

## Configurable Settings

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:

- Configuration Files
- Configuration Files Hierarchy
- eToken.conf Configuration Keys

# Configuration Files

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
```

## GENERAL

Syntax example (case sensitive):

[GENERAL]

SoftwareSlots=2

Description	Settings Value
<p>Software Slots</p> <p>Defines the number of virtual readers for SafeNet eToken Virtual tokens.</p> <p><b>Note:</b> Can be modified in 'Reader Settings' in SafeNet Authentication Client Tools also.</p>	<p><b>Settings Value Name:</b> SoftwareSlots</p> <p><b>Values:</b> &gt;=0 (0 = SafeNet eToken Virtual is disabled; only physical tokens are enabled).</p> <p><b>Default:</b> 2</p>
<p>PCSC Slots</p> <p>Defines the total number of PC/SC slots for all USB tokens and smartcards. Included in this total:</p> <ul style="list-style-type: none"><li>◆ the maximum number of drivers for non-SafeNet tokens</li><li>◆ the maximum number of iKey drivers, which is defined during installation and cannot be changed</li><li>◆ the maximum number of drivers for other SafeNet physical tokens, which can be modified in 'Reader Settings' in SafeNet Authentication Client Tools only</li></ul>	<p><b>Settings Value Name:</b> PCSCSlots</p> <p><b>Values:</b> &gt;=0 (0 = Physical tokens are disabled; only SafeNet eToken Virtual is enabled).</p> <p><b>Default:</b> 4</p>

Description	Settings Value
<p>Legacy Manufacturer Name</p> <p>Determines if 'Aladdin Knowledge Systems Ltd.' is written as the manufacturer name in token and token slot descriptions. Use for legacy compatibility only.</p>	<p><b>Settings Value Name:</b> LegacyManufacturerName</p> <p><b>Values:</b>  <b>0</b> - The legacy manufacturer name is written  <b>1</b> - The new manufacturer name is written</p> <p><b>Default:</b> 0</p>
<p>Enable Private Cache</p> <p>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.</p> <p><b>Note:</b> Can be set in SafeNet Authentication Client Tools.</p>	<p><b>Settings Value Name:</b> EnablePrvCache</p> <p><b>Values:</b>  <b>0</b> - (False) - Private data caching is disabled  <b>1</b> - (True) - Private data caching is enabled</p> <p><b>Default:</b> 1 (True).</p>
<p>Tolerate Finalize</p> <p>Determines if C_Finalize can be called by DllMain</p> <p><b>Note:</b> Define this property per process. Select this setting when using Novell Modular Authentication Service (NMAS) applications only.</p>	<p><b>Settings Value Name:</b> TolerantFinalize</p> <p><b>Values:</b>  <b>0</b> - (False) - C_Finalize cannot be called by DllMain  <b>1</b> - (True) - C_Finalize can be called by DllMain</p> <p><b>Default:</b> 0 (False)</p>

Description	Settings Value
<p>Tolerate X509 Attributes</p> <p>Determines if CKA_SERIAL_NUMBER, CKA_SUBJECT, and CKA_ISSUER attributes can differ from those in CKA_VALUE during certificate creation.</p> <p><b>Note:</b> 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.</p>	<p><b>Settings Value Name:</b> TolerantX509Attributes</p> <p><b>Values:</b>  <b>0</b> - (False) - Check that the values match  <b>1</b> - (True) - The attributes can differ  <b>Default:</b> 0 (False)</p>
<p>Tolerate Find Templates</p> <p>Determines if PKCS#11 tolerates a Find function with an invalid template, returning an empty list instead of an error.</p>	<p><b>Settings Value Name:</b> TolerantFindObjects</p> <p><b>Values:</b>  <b>0</b> - (False) - A Find function with an invalid template is not tolerated and returns an error  <b>1</b> - (True) - A Find function with an invalid template is tolerated and returns an empty list  <b>Default:</b> 0 (False)</p>
<p>Protect Symmetric Keys</p> <p>Determines if symmetric keys are protected</p> <p><b>Note:</b> If selected, even non-sensitive symmetric keys cannot be extracted</p>	<p><b>Settings Value Name:</b> SensitiveSecret</p> <p><b>Values:</b>  <b>0</b> - Symmetric keys can be extracted  <b>1</b> - Symmetric keys cannot be extracted  <b>Default:</b> 0 (False)</p>

Description	Settings Value
<p>Cache Marker Timeout</p> <p>Determines if SAC Service periodically inspects the cache markers of connected tokens for an indication that token content has changed</p> <p><b>Note:</b> 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.</p>	<p><b>Settings Value Name:</b> CacheMarkerTimeout</p> <p><b>Values:</b>  <b>0</b> - Connected tokens' cache markers are never inspected  <b>1</b> - Connected tokens' cache markers are periodically inspected  <b>Default:</b> 1</p>
<p>Override Non-Repudiation OIDs</p> <p>Overrides SAC's list of standard certificate OIDs that require a high level of security</p> <p><b>Note:</b> 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, remove the default registration key value.</p>	<p><b>Settings Value Name:</b> NonRepudiationOID</p> <p><b>Values:</b>  All OID values of non-repudiation certificates, separated by commas  <b>Default:</b> No override</p>

## INITAPP

Syntax example (case sensitive):

[INITAPP]

AdvancedView=1

Description	Settings Value
FIPS  FIPS Support	<b>Settings Value Name:</b> FIPS <b>Values:</b> <b>0</b> - disabled <b>1</b> - enabled  <b>Default:</b> 0

Description	Settings Value
<p>Legacy Format Version</p> <p>Defines the default token format.</p>	<p><b>Settings Value Name:</b> Legacy-Format-Version</p> <p><b>Values:</b></p> <p><b>0</b> - Tokens are formatted as backwardly compatible to eToken PKI Client 3.65 (CardOS tokens only)</p> <p><b>4</b> - Tokens are not formatted as backwardly compatible, and password quality settings can be saved on the token (CardOS tokens only)</p> <p><b>5</b> - 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).</p> <p><b>Default:</b> 4, for CardOS tokens5, for 4.20B FIPS and Java Card -based tokens</p>
<p>Default Token Name</p> <p>Defines the default Token Name written to tokens during initialization.</p>	<p><b>Settings Value Name:</b> DefaultLabel</p> <p><b>Values:</b></p> <p>String</p> <p><b>Default:</b> My Token</p>



Description	Settings Value
<p>API: Keep Token Settings</p> <p>When initializing the token using the SDK, determines if the token is automatically re-initialized with its current settings.</p> <p><b>Note:</b> If selected, this setting overrides all other initialization settings.</p>	<p><b>Settings Value Name:</b> KeepTokenInit</p> <p><b>Values:</b></p> <p><b>0</b> - (False) - Override current token settings</p> <p><b>1</b> - (True) - Use current token settings</p> <p><b>Default:</b> 0 (False)</p>
<p>Automatic Certification</p> <p>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.</p>	<p><b>Settings Value Name:</b> Certification</p> <p><b>Values:</b></p> <p><b>0</b> - (False) - initialize the token without the original certification</p> <p><b>1</b> - (True) - initialize the token with the original certification.</p> <p><b>Default:</b> 0 (False)</p>
<p>API: Private Data Caching</p> <p>If using an independent API for initialization, and if 'Enable Private Cache' is selected, determines the token's private data cache default behavior.</p>	<p><b>Settings Value Name:</b> PrvCachingMode</p> <p><b>Values:</b></p> <p><b>0</b> - Always</p> <p><b>1</b> - While user is logged on</p> <p><b>2</b> - Never</p> <p><b>Default:</b> 0 (Always)</p>

Description	Settings Value
<p>Enable Private Data Caching Modification</p> <p>Determines if the token's Private Data Caching mode can be modified after initialization.</p>	<p><b>Settings Value Name:</b> PrvCachingMode</p> <p><b>Values:</b></p> <ul style="list-style-type: none"> <li><b>0</b> - Always</li> <li><b>1</b> - While user is logged on</li> <li><b>2</b> - Never</li> </ul> <p><b>Default:</b> 0 (Always)</p>
<p>Private Data Caching Mode</p> <p>If 'Enable Private Data Caching Modification' is selected, determines who has rights to modify the token's Private Data Caching mode.</p>	<p><b>Settings Value Name:</b> PrvCachingOwner</p> <p><b>Values:</b></p> <ul style="list-style-type: none"> <li><b>0</b> - Admin</li> <li><b>1</b> - User</li> </ul> <p><b>Default:</b> 0 (Admin)</p>

## PQ

Syntax example (case sensitive):

[PQ]

pqModifiable=1

Description	Settings Value
<p>pqModifiable</p> <p>Password quality can be changed after initialization</p>	<p><b>Settings Value Name:</b> pqModifiable</p> <p><b>Values:</b> <b>0</b> - cannot be changed <b>1</b> - can be changed</p> <p><b>Default:</b> 1</p>
<p>pqHistorySize</p> <p>Number of recent passwords that cannot be repeated.</p>	<p><b>Settings Value Name:</b> pqHistorySize</p> <p><b>Values:</b> <b>&gt;=0</b></p> <p><b>Default:</b> 0</p>

Description	Settings Value
<p>pqMaxAge</p> <p>Total number of days a password is valid 0 = no expiration</p>	<p><b>Settings Value Name:</b> pqMaxAge</p> <p><b>Values:</b>  <b>0</b> - no expiration  <b>Default:</b> 0</p>
<p>pqMinAge</p> <p>Total number of days required before a password change 0 = none</p>	<p><b>Settings Value Name:</b> pqMinAge</p> <p><b>Values:</b>  <b>0</b> - none  <b>Default:</b> 6</p>
<p>pqMinLen</p> <p>Minimum password length.</p>	<p><b>Settings Value Name:</b> pqMinLen</p> <p><b>Values:</b>  &gt;=4  <b>Default:</b> 1</p>
<p>pqMixChars</p> <p>Mixed characters required 0 = disabled 1 = enabled</p>	<p><b>Settings Value Name:</b> pqMixChars</p> <p><b>Values:</b>  <b>0</b> - disabled  <b>1</b> - enabled  <b>Default:</b> 0</p>

Description	Settings Value
<p>pqWarnPeriod</p> <p>Total number of days before expiration to display warning. 0 = no warning</p>	<p><b>Settings Value Name:</b> pqWarnPeriod</p> <p><b>Values:</b> <b>0</b> - no warning <b>Default:</b> 0</p>
<p>Password - Minimum Length</p> <p>Defines the minimum password length. <b>Note:</b> Can be set in SafeNet Authentication Client Tools.</p>	<p><b>Settings Value Name:</b> pqMinLen</p> <p><b>Values:</b> &gt;=4 <b>Default:</b> 6</p>
<p>Password - Maximum Length</p> <p>Defines the maximum password length. <b>Note:</b> Can be set in SafeNet Authentication Client Tools.</p>	<p><b>Settings Value Name:</b> pqMaxLen</p> <p><b>Values:</b> Cannot be less than the Password Minimum Length <b>Default:</b> 16</p>
<p>Password - Maximum Usage Period</p> <p>Defines the maximum number of days a password is valid. <b>Note:</b> Can be set in SafeNet Authentication Client Tools.</p>	<p><b>Settings Value Name:</b> pqMaxAge</p> <p><b>Values:</b> &gt;=0 (0 =No expiration) <b>Default:</b> 0</p>

Description	Settings Value
<p>Password - Minimum Usage Period</p> <p>Defines the minimum number of days between password changes.</p> <p><b>Note:</b> Can be set in SafeNet Authentication Client Tools.</p> <p><b>Note:</b> Does not apply to iKey devices.</p>	<p><b>Settings Value Name:</b> pqMinAge</p> <p><b>Values:</b>  &gt;=0  (0 = No minimum)</p> <p><b>Default:</b> 0</p>
<p>Password - Expiration Warning Period</p> <p>Defines the number of days before expiration during which a warning is displayed.</p> <p><b>Note:</b> Can be set in SafeNet Authentication Client Tools.</p>	<p><b>Registry Value Name:</b> pqWarnPeriod</p> <p><b>Values:</b>  &gt;=0  (0 = No warning)</p> <p><b>Default:</b> 0</p>
<p>Password - History Size</p> <p>Defines the number of recent passwords that may not be repeated.</p> <p><b>Note:</b> Can be set in SafeNet Authentication Client Tools.</p>	<p><b>Registry Value Name:</b> pqHistorySize</p> <p><b>Values:</b>  &gt;= 0  (0 = No minimum)</p> <p><b>Default:</b> 10  (iKey device history is limited to 6)</p>

Description	Settings Value
<p>Password - Maximum Consecutive Repetitions</p> <p>Defines the maximum number of consecutive times a character can be used in a password.</p> <p><b>Note:</b> Can be set in SafeNet Authentication Client Tools.</p> <p><b>Note:</b> Does not apply to iKey devices.</p>	<p><b>Registry Value Name:</b> pqMaxRepeated</p> <p><b>Values:</b> 0 - 16 (0 = No maximum)</p> <p><b>Default:</b> 3</p>
<p>Password - Complexity</p> <p>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.</p> <p><b>Note:</b> Can be set in SafeNet Authentication Client Tools.</p>	<p><b>Registry Value Name:</b> pqMixChars</p> <p><b>Values:</b> <b>1</b> - A minimum of 2 or 3 types must be included, as defined in the <i>Password- Minimum Mixed Character Types</i> setting <b>0</b> -The rule for each character type is defined in the character type's <i>Include</i> setting</p> <p><b>Default:</b> 1</p>

Description	Settings Value
<p>Password - Minimum Mixed Character Types</p> <p>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.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>◆ Applies only when the <i>Password - Complexity</i> setting is set to <b>Standard complexity</b>.</li> <li>◆ Can be set in SafeNet Authentication Client Tools.</li> </ul>	<p><b>Registry Value Name:</b> pqMixLevel</p> <p><b>Values:</b></p> <p><b>0</b> - At least 3 character types  <b>1</b> - At least 2 character types</p> <p><b>Default:</b>0</p>
<p>Password - Include Numerals</p> <p>Determines if the password may include numerals.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>◆ Applies only when the <i>Password - Complexity</i> setting is set to <b>Manual complexity</b>.</li> <li>◆ Can be set in SafeNet Authentication Client Tools.</li> </ul>	<p><b>Registry Value Name:</b> pqNumbers</p> <p><b>Values:</b></p> <p>0 -Permitted  1 - Forbidden  2 - Mandatory</p> <p><b>Default:</b> 0</p>



Description	Settings Value
<p>Password - Include Upper-Case</p> <p>Determines if the password may include upper-case letters.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>◆ Applies only when the <i>Password - Complexity</i> setting is set to <b>Manual complexity</b>.</li> <li>◆ Can be set in SafeNet Authentication Client Tools.</li> </ul>	<p><b>Registry Value Name:</b> pqUpperCase</p> <p><b>Values:</b></p> <ul style="list-style-type: none"> <li>0 - Permitted</li> <li>1 - Forbidden</li> <li>2 - Mandatory</li> </ul> <p><b>Default:</b> 0</p>
<p>Password - Include Lower-Case</p> <p>Determines if the password may include lower-case letters.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>◆ Applies only when the <i>Password - Complexity</i> setting is set to <b>Manual complexity</b>.</li> <li>◆ Can be set in SafeNet Authentication Client Tools.</li> </ul>	<p><b>Registry Value Name:</b> pqLowerCase</p> <p><b>Values:</b></p> <ul style="list-style-type: none"> <li>0 - Permitted</li> <li>1 - Forbidden</li> <li>2 - Mandatory</li> </ul> <p><b>Default:</b> 0</p>
<p>Password - Include Special Characters</p> <p>Determines if the password may include special characters, such as @,!, &amp;.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>◆ Applies only when the <i>Password - Complexity</i> setting is set to <b>Manual complexity</b>.</li> <li>◆ Can be set in SafeNet Authentication Client Tools.</li> </ul>	<p><b>Registry Value Name:</b> pqSpecial</p> <p><b>Values:</b></p> <ul style="list-style-type: none"> <li>0 - Permitted</li> <li>1 - Forbidden</li> <li>2 - Mandatory</li> </ul> <p><b>Default:</b> 0</p>

Description	Settings Value
<p>Password Quality Check on Initialization</p> <p>Determines if the password quality settings are checked and enforced when a token is initialized</p> <p><b>Note:</b> We recommend that this policy not be set when tokens are enrolled using TMS or SafeNet Authentication Manager.</p>	<p><b>Registry Value Name:</b> pqCheckInit</p> <p><b>Values:</b>  <b>1 (True)</b> -The password quality is enforced  <b>0 (False)</b> - The password quality is not enforced</p> <p><b>Default:</b> 0</p>
<p>Password Quality Owner</p> <p>Defines the owner of the password quality settings on a re initialized token, and defines the default of the <i>Password Quality Modifiable</i> setting.</p>	<p><b>Registry Value Name:</b> pqOwner</p> <p><b>Values:</b>  <b>0</b> - Administrator  <b>1</b> - User</p> <p><b>Default:</b>  0, for tokens with an Administrator Password.  1, for tokens without an Administrator Password.</p>

Description	Settings Value
<p>Enable Password Quality Modification</p> <p>Determines if the password quality settings on a newly initialized token can be modified by the owner.</p> <p>See the <i>Password Quality Owner</i> setting.</p>	<p><b>Registry Value Name:</b> pqModifiable</p> <p><b>Values:</b>  <b>1 (True)</b>- The password quality can be modified by the owner  <b>0 (False)</b> - The password quality cannot be modified by the owner</p> <p><b>Default:</b>  1 (True), for administrator-owned tokens  0 (False), for user owned tokens.</p>

## UI

Syntax example (case sensitive):

[UI]

LanguageId=en-US

Description	Settings Value
LanguageId  UI Language (supports English only)	<b>Settings Value Name:</b> LanguageId  <b>Values:</b> <b>ENG</b> <b>Default:</b> en-US
Enable Advanced View Button  Determines if the Advanced View icon is enabled in SAC Tools	<b>Settings Value Name:</b> AdvancedView  <b>Values:</b> <b>1</b> - Selected <b>0</b> - Not selected  <b>Default:</b> 1

Description	Settings Value
<p>Use Default Password</p> <p>Determines if the <i>Change Password on First Logon</i> process assumes the current Token Password is the default (defined in the Default Token Password), and does not prompt the user to supply it.</p>	<p><b>Settings Value Name:</b> UseDefaultPassword</p> <p><b>Values:</b>  <b>1 (True)</b> - The default Token Password is automatically entered in the password field  <b>0 (False)</b> -The default Token Password is not automatically entered in the password field</p> <p><b>Default:</b> 0 (False)</p>
<p>Password Term</p> <p>Defines the term used for the token's user password.</p>	<p><b>Settings Value Name:</b> PasswordTerm</p> <p><b>Values (String):</b>  Password  PIN  Passcode  Passphrase</p> <p><b>Default:</b> Password</p>

Description	Settings Value
<p>Decimal Serial Number</p> <p>Determines if the Token Information window displays the token serial number in hexadecimal or in decimal format.</p>	<p><b>Settings Value Name:</b> ShowDecimalSerial</p> <p><b>Values:</b>  <b>1 (True)</b> -Displays the serial number in decimal format  <b>0 (False)</b> -Displays the serial number in hexadecimal format</p> <p><b>Default:</b> 0</p>
<p>Enable Connection Notification</p> <p>Determines if a notification balloon is displayed when a token is connected or disconnected.</p>	<p><b>Settings Value Name:</b> ShowBalloonEvents</p> <p><b>Values:</b>  <b>0</b> - Not Displayed  <b>1</b> - Displayed</p> <p><b>Default:</b> 0</p>
<p>Enable Logging Control</p> <p>Determines if the <i>Enable Logging / Disable Logging</i> button is enabled in the Client Settings Advanced tab</p>	<p><b>Settings Value Name:</b> AllowLogsControl</p> <p><b>Values:</b>  <b>1</b> -Enabled  <b>0</b> -Disabled</p> <p><b>Default:</b> 1</p>

Description	Settings Value
<p>Home URL</p> <p>Overwrites the SafeNet home URL in SafeNet Authentication Client Tools</p>	<p><b>Settings Value Name:</b> HomeUrl</p> <p><b>Values (String):</b> Valid URL</p> <p><b>Default:</b> SafeNet's home URL</p>
<p>Enable Certificate Expiration Warning</p> <p>Determines if a warning message is displayed when certificates on the token are about to expire.</p>	<p><b>Settings Value Name:</b> CertificateExpiryAlert</p> <p><b>Values:</b>  <b>1 (True)</b> - Notify the user  <b>0 (False)</b> - Do not notify the user</p> <p><b>Default:</b> 1 (True)</p>
<p>Ignore Expired Certificates</p> <p>Determines if expired certificates are ignored, and no warning message is displayed for expired certificates</p>	<p><b>Settings Value Name:</b> IgnoreExpiredCertificates</p> <p><b>Values:</b>  <b>1</b> - Expired certificates are ignored  <b>0</b> - A warning message is displayed if the token contains expired certificates</p> <p><b>Default:</b> 0</p>

Description	Settings Value
<p>Certificate Expiration Verification Frequency</p> <p>Defines the minimum interval, in days, between certificate expiration date verifications</p>	<p><b>Settings Value Name:</b> UpdateAlertMinInterval</p> <p><b>Values:</b> &gt; 0</p> <p><b>Default:</b> 14 days</p>
<p>Certificate Expiration Warning Period</p> <p>Defines the number of days before a certificate's expiration date during which a warning message is displayed.</p>	<p><b>Settings Value Name:</b> ExpiryAlertPeriodStart</p> <p><b>Values:</b> &gt; =0 (0 = No warning)</p> <p><b>Default:</b> 30 days</p>
<p>Warning Message Title</p> <p>Defines the title to display in certificate expiration warning messages</p>	<p><b>Settings Value Name:</b> AlertTitle</p> <p><b>Values:</b> String</p> <p><b>Default:</b> SafeNet Authentication Client</p>



Description	Settings Value
<p>Certificate Will Expire Warning Message</p> <p>Defines the warning message to display in a balloon during a certificate's "Certificate Expiration Warning Period."</p>	<p><b>Settings Value Name:</b> FutureAlertMessage</p> <p><b>Values:</b> String</p> <p><b>Default:</b> A certificate on your token expires in \$EXPIRE_IN_DAYS days.</p>
<p>Certificate Expired Warning Message</p> <p>Defines the warning message to display in a balloon if a certificate's expiration date has passed.</p>	<p><b>Settings Value Name:</b> PastAlertMessage</p> <p><b>Values:</b> String</p> <p><b>Default:</b> Update your token now.</p>
<p>Enable Password Expiration Notification</p> <p>Determines if a pop-up message is displayed in the system when the Token Password is about to expire.</p>	<p><b>Settings Value Name:</b> NotifyPasswordExpiration</p> <p><b>Values:</b>  <b>1 (True)</b>- A message is displayed  <b>0 (False)</b> - A message is not displayed</p> <p><b>Default:</b> 1 (True)</p>
<p>Password Policy Instructions</p> <p>If not empty, defines a string that replaces the default password policy description displayed in the Unlock and Change Password windows.</p>	<p><b>Registry Value Name:</b> PasswordPolicyInstructions</p> <p><b>Values:</b> String</p>

## INIT

Syntax example (case sensitive):

[INIT]

DefaultUserPassword=1234567890

Description	Settings Value
PrivateDataCaching	Can be configured in SafeNet Authentication Client Tools
HMAC-SHA1	Can be configured in SafeNet Authentication Client Tools
Default Token Password  Defines the default Token Password	<b>Settings Value Name:</b> DefaultUserPassword  <b>Values:</b> String  <b>Default:</b> 1234567890
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.  <b>Note:</b> This option is selected by default.	<b>Settings Value Name:</b> MustChangePasswordEnabled  <b>Values:</b> <b>1</b> - Selected <b>0</b> - Not selected  <b>Default:</b> 1

Description	Settings Value
<p>Change Password on First Logon</p> <p>Determines if the <i>Token Password must be changed on first logon</i> option is selected by default in the Token Initialization window.</p>	<p><b>Settings Value Name:</b> MustChangePassword</p> <p><b>Value:</b>  <b>1</b> - Selected  <b>0</b> - Not selected</p> <p><b>Default:</b> 1</p>
<p>Private Data Caching</p> <p>If <i>Enable Private Cache</i> is selected, determines the token's private data cache default behavior.</p> <p><b>Note:</b> Can be set in SafeNet Authentication Client Tools.</p>	<p><b>Settings Value Name:</b> PrivateDataCaching</p> <p><b>Values:</b>  <b>0</b> - (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  <b>1</b> - 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  <b>2</b> - private data is not cached</p> <p><b>Default:</b> 0</p>

Description	Settings Value
<p>Reuse Current Token Name</p> <p>Determines if the token's current Token Name is displayed as the default Token Name when the token is re initialized.</p>	<p><b>Settings Value Name:</b> ReadLabelFromToken</p> <p><b>Values:</b>  <b>1</b> -The current Token Name is displayed  <b>0</b> -The current Token Name is ignored</p> <p><b>Default:</b> 1</p>
<p>Default Common Criteria Import PIN</p> <p>Defines the default Common Criteria Import PIN</p>	<p><b>Default:</b> 1234567890</p>
<p>Maximum Token Password Retries</p> <p>Defines the default number of consecutive failed logon attempts that lock the token.</p>	<p><b>Settings Value Name:</b> UserMaxRetry</p> <p><b>Values:</b> 0-15 (0 = no retries)</p> <p><b>Default:</b> 15</p>
<p>Maximum Administrator Password Retries</p> <p>Defines the default number of consecutive failed administrator logon attempts that lock the token.</p>	<p><b>Settings Value Name:</b> AdminMaxRetry</p> <p><b>Values:</b> 0-15 (0 = no retries)</p> <p><b>Default:</b> 15</p>

## eToken.common.conf Configuration Keys

eToken.common.conf contains SafeNet eToken Virtual keys.

Can be configured in SafeNet Authentication Client Tools

Description	Settings Value
FileName(slot0)  File name with full path	

## ACCESSCONTROL

Syntax example (case sensitive):

[ACCESSCONTROL]

RenameToken=1

Description	Settings Value
All access control features listed below	<b>Values:</b>  <b>1 (True)</b> - The feature is enabled. <b>0 (False)</b> - The feature is disabled.  <b>Default:</b> 1(True), except where indicated in the table

Description	Settings Value
Rename Token Enables/Disables the Rename Token feature in SafeNet Authentication Client Tools.	RenameToken
Change Token Password Enables/Disables the <i>Change Token Password</i> feature in SafeNet Authentication Client Tools.	ChangePassword
Unlock Token Enables/Disables the <i>Unlock Token</i> feature in SafeNet Authentication Client Tools.	UnlockEtoken
Delete Token Content Enables/Disables the <i>Delete Token Content</i> feature in SafeNet Authentication Client Tools.	ClearEToken
View Token Information Enables/Disables the <i>View Token Information</i> feature in SafeNet Authentication Client Tools.	ViewTokenInfo
Disconnect SafeNet eToken Virtual Enables/Disables the <i>Disconnect SafeNet eToken Virtual</i> feature in SafeNet Authentication Client Tools.	DisconnectVirtual

Description	Settings Value
<p>Help</p> <p>Determines if the user can open the <i>Help</i> file in SafeNet Authentication Client Tools.</p>	ShowHelp
<p>Advanced View</p> <p>Determines if the user can open the Advanced View in SafeNet Authentication Client Tools.</p>	OpenAdvancedView
<p>Reader Settings</p> <p>Enables/Disables the <i>Reader Settings</i> feature in SafeNet Authentication Client Tools.</p>	ManageReaders
<p>Connect SafeNet eToken Virtual</p> <p>Enables/Disables the <i>Connect SafeNet eToken Virtual</i> feature in SafeNet Authentication Client Tools.</p>	AddeTokenVirtual
<p>Initialize Token</p> <p>Enables/Disables the <i>Initialize Token</i> feature in SafeNet Authentication Client Tools.</p>	InitializeEToken
<p>Import Certificate</p> <p>Enables/Disables the <i>Import Certificate</i> feature in SafeNet Authentication Client Tools.</p>	ImportCertificate

Description	Settings Value
Reset Default Certificate Selection  Enables/Disables the <i>Reset Default Certificate Selection</i> feature in SafeNet Authentication Client Tools.	ClearDefaultCert
Delete Certificate  Enables/Disables the <i>Delete Certificate</i> feature in SafeNet Authentication Client Tools.	DeleteCertificate
Export Certificate  Enables/Disables the <i>Export Certificate</i> feature in SafeNet Authentication Client Tools.	ExportCertificate
Copy Certificate Data to Clipboard  Enables/Disables the <i>Copy Certificate Data to Clipboard</i> feature in SafeNet Authentication Client Tools.	CopyCertificateData
Log On as Administrator  Enables/Disables the <i>Log On as Administrator</i> feature in SafeNet Authentication Client Tools.	LoginAsAdministrator
Change Administrator Password  Enables/Disables the <i>Change Administrator Password</i> feature in SafeNet Authentication Client Tools.	ChangeAdministratorPassword



Description	Settings Value
<p>Set Token Password</p> <p>Enables/Disables the <i>Set Token Password</i> feature in SafeNet Authentication Client Tools.</p>	SetUserPassword
<p>Token Password Retries</p> <p>Enables/Disables the <i>Logon retries before token is locked</i> feature (for the Token Password) in SafeNet Authentication Client Tools.</p>	AllowChangeUserMaxRetry
<p>Administrator Password Retries</p> <p>Enables/Disables the <i>Logon retries before token is locked</i> feature (for the Administrator Password) in SafeNet Authentication Client Tools.</p>	AllowChangeAdminMaxRetry
<p>Advanced Initialization Settings</p> <p>Enables/Disables the <i>Advanced</i> button in the <i>Token Initialization</i> window in SafeNet Authentication Client Tools.</p>	OpenAdvancedModeOfInitialize
<p>Change Initialization Key during Initialization</p> <p>Enables/Disables the <i>Change Initialization key</i> button in the <i>Advanced Token Initialization Settings</i> window in SafeNet Authentication Client Tools</p>	ChangeInitializationKeyDuringInitialize

Description	Settings Value
<p>Common Criteria Settings</p> <p>Enables\Disables the Common Criteria option in the Certification combo box.</p>	CommonCriteriaPasswordSetting
<p>System Tray - Delete Token Content</p> <p>Enables/Disables the <i>Delete Token Content</i> feature in the SafeNet Authentication Client Tray Menu.</p> <p><b>Note:</b> By default, this feature is <b>Disabled</b></p>	TrayIconClearEToken
<p>System Tray -Change Token Password</p> <p>Enables/Disables the <i>Change Token Password</i> feature in the SafeNet Authentication Client Tray Menu.</p>	TrayIconChangePassword
<p>System Tray - Tools</p> <p>Enables/Disables the <i>Tools</i> menu item (open SafeNet Authentication Client Tools) in the SafeNet Authentication Client Tray Menu.</p>	OpeneTokenProperties
<p>System Tray - About</p> <p>Enables/Disables the <i>About</i> menu item in the SafeNet Authentication Client Tray Menu.</p>	About

Description	Settings Value
<p>System Tray - Unlock token</p> <p>Enables/Disables the unlock Token feature in SafeNet Authentication Client Tools.</p>	<p>TrayIconUnlockEToken</p>