SafeNet Authentication Client (Linux)

Administrator's Guide
Version 8.0 Revision A

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:

http://c3.safenet-inc.com/secure.asp

Additional Documentation

We recommend reading the following SafeNet Token publication:

- SafeNet Authentication Client (Linux) 8.0 User's Guide
- SafeNet Authentication Client (Linux) 8.0 ReadMe

`Table of Contents

Chapter 1

Introduction

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

Note:
This document refers to SafeNet Authentication Client 8.0.
For details of supported platforms in SafeNet Authentication Client 8.0, see *System Requirements* on page 3.

In this chapter:

Overview

Public Key Infrastructure (PKI) is a framework for creating a secure method for exchanging information based on public key cryptography, providing for trusted third-party vetting of, and vouching for, user identities. It is an arrangement that consists of 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's Authentication Client enables integration with various security applications. It enables token security applications and third party applications to communicate with the token. These include PKI solutions using PKCS#11 or proprietary token applications.

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 PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications offering secure web access, PC and data security, secure email, and more. PKI keys and certificates can be created, stored, and used securely from within token hardware or software devices.

SafeNet Authentication Client can be deployed and updated using any standard software distribution system.

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

New Features

The following features were introduced in SafeNet Authentication Client (for Linux) 8.0:

- Support for eToken NG Flash 5.3/Support for eToken NG Flash 5.3 Anywhere (in PKI mode only).
- Support for upgrade from previous version.

Chapter 2

System Requirements

Supported Operating Systems (SafeNet Authentication Client (Linux) 8.0)	Red Hat Enterprise 5.4 (32-bit and 64-bit) on 2.6 kernel
	CentOS 5.4 (32-bit and 64-bit) on 2.6 kernel
	SUSE Linux Enterprise 11 (32-bit) on 2.6 kernel
	Fedora 12 (32-bit)
	Ubuntu 10.04 (32-bit and 64-bit) on 2.6 kernel
Supported Browser	Firefox 3.6
Supported Mail Client	Thunderbird 2.0
Document Signing	Open Office 3.2

Supported Token Devices	eToken PRO
	eToken NG-OTP
	eToken NG-FLASH 5.3
	eToken NG-FLASH Anywhere (PKI mode only)
	eToken PRO Smartcard
	eToken PRO Anywhere (PKI mode only)
	SafeNet eToken Virtual
Required Hardware	USB port (for physical Token devices)
Recommended Screen Resolution	1024 x 768 pixels or higher (for SafeNet Authentication Client Tools)

Chapter 3

Installation

This chapter describes the installation options for SafeNet Authentication Client.

In this chapter:

Pre-Installation

Upgrading

If an earlier version of SafeNet Authentication Client is installed, it automatically detects the earlier version and removes before installing the latest SafeNet Authentication Client version.

Pre-Installation for 32-bit Operating Systems

The built-in PCSC-Lite service for 32-bit operating systems must be installed before running the SafeNet Authentication Client installation.

The following table lists the built-in PCSC-Lite service versions for 32-bit operating systems.

Operating System	Default PCSC-Lite Service Version
CentOS 5.4 32-bit on 2.6 kernel	pcsc-lite 1.4.4 (libusb)
CentOS 5.4 64-bit on 2.6 kernel	pcsc-lite 1.4.4 (libhal)
Red Hat Enterprise 5.4 32-bit on 2.6 kernel	pcsc-lite-1.4.4 (libusb)
Red Hat Enterprise 5.4 64-bit on 2.6 kernel	pcsc-lite-1.4.4 (libhal)
SUSE Linux Enterprise 11 32-bit on 2.6 kernel	pcsc-lite-1.4.1 (libhal)
Fedora 12 32-bit	pcsc-lite-1.5.2 (libhal)
Ubuntu 10.04 32-bit on 2.6 kernel	pcsc-lite - 1.5.3 (libusb, installed using apt-get
Ubuntu 10.04 64-bit on 2.6 kernel	pcsc-lite - 1.5.3 (libusb, installed using apt-get

Note:
There are few known issues with PCSC-Lite 1.5, such as:

- Token selection option is not available.
- Token insertion/removal is reflected in SAC Tools only after refreshing the window.
- Application hangs while connecting SafeNet eToken Virtual or on clicking SAC Monitor tray icon.
- Delete Token Content and Change Token Password disappear from SAC Monitor tray icon while trying to connect/disconnect SafeNet eToken Virtual.
- Incorrect state of token is shown in SAC Tools

It is recommended to use PCSC-Lite 1.4.x with `libusb` support.

Note:
The SafeNet Authentication Client driver requires the PCSC-Lite service to be compiled and installed with `libusb` support. Ensure that `pcscd` is compiled with `libusb` support, and not with `libhal` support.

Pre-Installation for Ubuntu

Before installing SafeNet Authentication Client on Ubuntu:

- Ensure that you have Super User permissions.
- If the built-in PSCS-Lite service is compiled with `libhal` support, uninstall the service, and install it with `libusb` support.

  Note:
  The SafeNet Authentication Client driver requires the PSCS-Lite service to be compiled and installed with `libusb` support.

Pre-Installation for 64-bit Operating Systems

The built-in PCSC-Lite service for 64-bit operating systems is not appropriate for SafeNet Authentication Client. Before installing SafeNet Authentication Client, the built-in PCSC-Lite service must be uninstalled, and PCSC-Lite 1.4.102 or later must be installed with `libusb` support.

Getting the PCSC-Lite Packages

The PCSC-Lite packages can be downloaded from the following website:

http://pcsclite.alioth.debian.org/

For 64 bit OS, we need to install the 64-bit and 32 bit libraries of pcsclite as well.

The following is the option of configure script to build PCSC-Lite for 32 bit.

For Ubuntu:

```
./configure –prefix=/usr –libdir=/usr/lib32
–localstatedir=/var –sysconfdir=/etc –enable-libusb
–disable-libhal CFLAGS=”-m32”
```

For RHEL, CentOS and Fedora:

```
./configure –prefix=/usr –libdir=/usr/lib
–localstatedir=/var –sysconfdir=/etc –enable-libusb
–disable-libhal CFLAGS=”-m32”
```

```
Now the following option will configure the PCSC-Lite
configuration script for 64 bit.
```

```
./configure –prefix=/usr –libdir=/usr/lib64
–localstatedir=/var –sysconfdir=/etc –enabledaemon
–enable-libusb –disable-libhal --enable-
usbdropdir=/usr/lib64/pcsc/drivers
```

The `pcsc-lite` and the `pcsc-lite-libs(i386, x64)` packages are required. For development, the `pcsc-lite-devel` package is also required.

Replacing PCSC-Lite

Remove the unsupported version of PCSC-Lite, and install a supported version.

To replace the 64-bit version of PCSC-Lite with the appropriate version:

1. Uninstall PCSC-Lite:
   - `yum remove pcsc-lite pcsc-lite-devel.i386 pcsc-lite-devel.x86_64 pcsc-lite-libs.i386 pcsc-lite-libs.x86_64`
2. Install the RPM packages:
   - `rpm -ivh <name>-pcsc-lite-1.4.102-1.x86_64.rpm <name>-pcsc-lite-libs-1.4.102-1.i386.rpm <name>-pcsc-lite-libs-1.4.102-1.x86_64.rpm`

   where `<name>` is the prefix of your PSCS-Lite filename
3. Start pcscd:
   - `/etc/init.d/pcscd start`

Installing SafeNet Authentication Client

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.

The SafeNet Authentication Client RPM packages:

- RPM Package Name: `SafenetAuthenticationClient-8.0.n-0.i386.rpm`
- RPM Installation Script Name: `signed-install_SafenetAuthenticationClient-8.0.n-0.i386.rpm`

where `n` is the build number

To install with authentication on RedHat, SUSE, or CentOS:

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-8.0.n-0.i386.rpm
     ```
   - On a 64-bit OS:
     ```
     rpm -hi SafeNetAuthenticationClient-8.0.n-
     0.x86_64.rpm
     ```

   where:
   - `-hi` is the parameter for installation
   - `n` is the build number

To install with a script on RedHat, SUSE, or CentOS:

1. Log on as a root user.
2. Run one of the following installation scripts:
   - On a 32-bit OS:
     ```
     ./signed-install_SafeNetAuthenticationClient-8.0.n-
     0.i386.rpm.sh
     ```
   - On a 64-bit OS:
     ```
     ./signed-install_SafeNetAuthenticationClient-8.0.n-
     0.x86_64.rpm.sh
     ```

Note:
When installing with a script, ensure that the following are all in the same folder:

- the key
- the script
- the RPM package

To install on Fedora:

1. Log on as a non-root user.
2. Double-click the RPM file:
   `SafeNetAuthenticationClient-8.0.n-0.i386.rpm`
   where `n` is the build number.

A root password prompt appears.

3. Enter the root password.

Installing on Ubuntu

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:
  `SafeNetAuthenticationClient-8.0.n-0_i386.deb`
  where `n` is the build number

To install from the package installer:

1. Double-click the required .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 the SafeNet Authentication Client Quick Menu, go to **Applications > SafeNet > SafeNet Authentication Client > SafeNet Authentication Client Tools**.

To install from the terminal:

1. Enter the following:
   ```
   sudo dpkg -i SafeNetAuthenticationClient-8.0.n-0_i386.deb
   ```
   where `n` is the build 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**.

Uninstalling SafeNet Authentication Client

When SafeNet Authentication Client is uninstalled, user configuration and policy files are deleted. For information regarding the files, see Chapter 4 *Configurable Settings* on page 17.

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 for uninstallation:
  `sudo dpkg --purge safenetauthenticationclient`
  where `--purge` is the parameter for uninstall.

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.

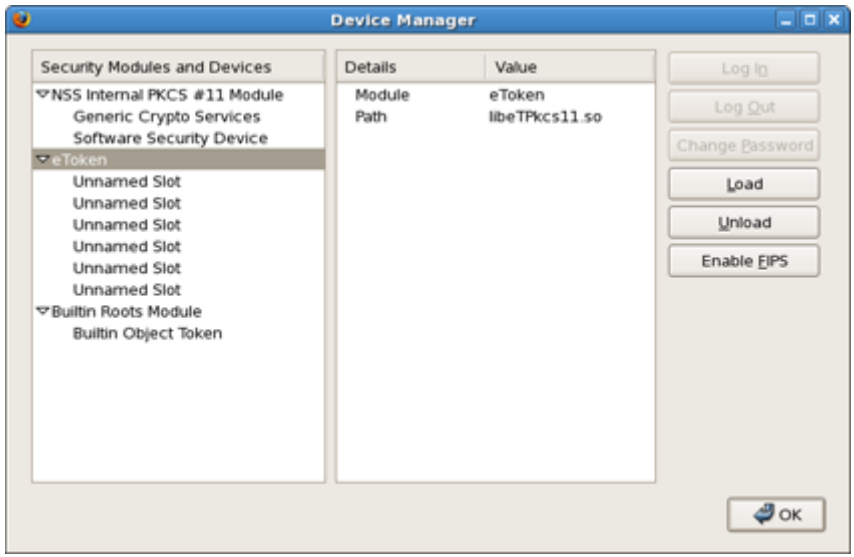
When working with Thunderbird, load the token PKCS#11 security module manually.

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:

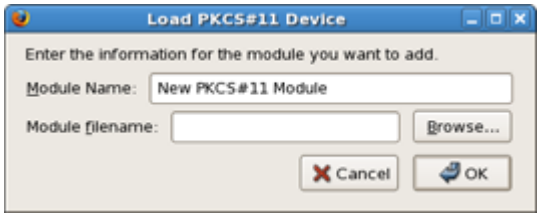
1. Do one of the following:
   - When working with Firefox, go to **Edit > Preferences > Advanced > Encryption > Security Devices.**
   - When working with Thunderbird, go to **Edit > Preferences > Advanced > Certificates > Security Devices.**

   The *Device Manager* dialog box opens.



2. If **Token** is listed in the *Security Modules and Devices* column, click **OK** to exit the *Device Manager*.
3. If **Token** is not listed in the *Security Modules and Devices* column, click **Load**.

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

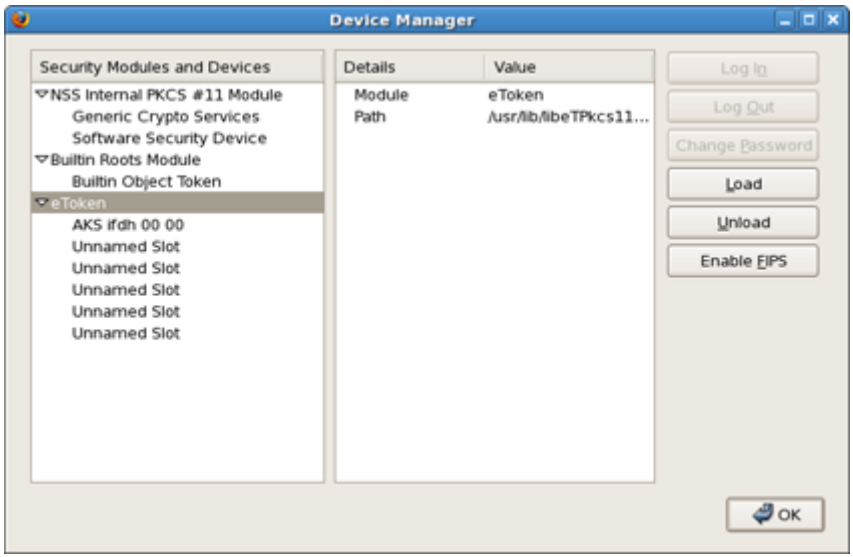


4. Do the following:
   - Replace the contents of the *Module Name* field with **Token**.
   - In the *Module filename* field, enter the following: **/usr/lib/libeTPkcs11.so**

Note:
The *Module* fields are case sensitive.

5. Click **OK.**
   The *Confirm* dialog box opens.
6. Click **OK.**
   The *Alert* dialog box opens.
7. Click **OK.**

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



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

Chapter 4

Configurable Settings

This chapter provides administrator guidelines for setting configuration keys.

In this chapter:

Configuration Files

SafeNet Authentication Client installs two configuration files:

- `eToken.conf`: requires administrator 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 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 Authentication Client daemons and applications are restarted or only after rebooting the machine.

General

Key Name	Description	DWord Value	Default
PcscSlots	Number of PC/SC slots	1-16	4 **Note:** to use more than 4 slots concurrently, enter the required number
SoftwareSlots	Number of software slots	1-10	2

CertStore

Key Name	Description	DWord Value	Default
PropagateCACertificates	Export all CA certificates on the token to the Trusted CA location 0 = disabled 1= enabled	0/1	1

InitApp

Key Name	Description	DWord Value	Default
FIPS	FIPS Support 0 = disabled 1= enabled	0/1	0
AdvancedView	*Advanced* button in SafeNet Authentication Client Tools application 0 = disabled 1= enabled	0/1	1
ShowInTray	The Quick Functions menu is displayed on the desktop. 0 = not displayed 1 = displayed 2= displayed when token is inserted (does not disappear when token is disconnected)	0/1/2	1

PQ

Key Name	Description	DWord Value	Default
pqModifiable	Password quality can be changed after initialization 0 = cannot be changed 1 = can be changed	0/1	1
pqHistorySize	Number of recent passwords that cannot be repeated	>=0	10
pqMaxAge	Total number of days a password is valid 0 = no expiration	>=0	0
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	DWord Value	Default
LanguageId	UI Language (supports English only)	EN	EN
linguist	Path to Linguist application		

Init

Key Name	Description	DWord Value	Default
RSASecondaryAuthenicationMode	Can be configured in SafeNet Authentication Client Tools		
PrivateDataCaching	Can be configured in SafeNet Authentication Client Tools		
RSA-2048	Can be configured in SafeNet Authentication Client Tools		
HMAC-SHA1	Can be configured in SafeNet Authentication Client Tools		

eToken.common.conf Configuration Keys

`eToken.common.conf` contains SafeNet eToken Virtual keys.

Key Name	Description	DWord Value	Default
FileName(slot0)	File name with full path		