

SafeNet Authentication Client

Version 10.x



All information herein is either public information or is the property of and owned solely by Gemalto and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any publicly accessible network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and noninfringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure e functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2010-18 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Product Version: 10.5 (GA)

Document Number: 007-013560-005, Rev. A

Release Date: March, 2018

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this

service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information
Customer Support Portal	https://supportportal.gemalto.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.
Technical Support contact email	technical.support@gemalto.com

Additional Documentation

The following publications are available:

- 007-013561-005 SafeNet Authentication Client 10.5 Windows (GA) User Guide
- 007-013559-007 SafeNet Authentication Client 10.5 Windows (GA) Release Notes (RN) Rev B

Introduction

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

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

Overview

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

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

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

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

Compatibility Information

Browsers

SafeNet Authentication Client 10.5 (GA) Windows supports the following browsers:

- Firefox 59
- Internet Explorer 11.15.16299.0
- Chrome version 65
- Microsoft Edge 42.17112.1.0

Operating Systems

SafeNet Authentication Client 10.5 (GA) Windows supports the following operating systems:

- Windows Server 2008 R2 SP1 (32-bit, 64-bit)
- Windows Server 2008 SP2 (32-bit, 64-bit)
- Windows Server 2012 and 2012 R2 (64-bit)
- Windows Server 2016 (64-bit)
- Windows 7 SP1 (32-bit, 64-bit)
- Windows 8 (32-bit, 64-bit)
- Windows 8.1 (32-bit, 64-bit)
- Windows 10 (32-bit, 64-bit) Fall Creators Update (1709)
- OSX 10.11 El Capitan
- OSX 10.12 Sierra
- Red Hat 7.3, 6.9
- CentOS 7.3, 6.9
- SUSE 12.2
- Debian 9.0
- Fedora 26
- Ubuntu 16.04 and 17.04

Windows 10 Elevated Security

In Windows 10 and Windows Server 2016 you should use Credential Guard to enhance security.

See more details at:

<https://technet.microsoft.com/en-us/itpro/windows/keep-secure/credential-guard>

Additional Environment Recommendations

The following actions will help keep your information as safe as possible:

- Enable Windows Defender
- Control access to your computer by locking your screen after a period of inactivity.
- Set up secure file sharing.
- Make sure you're running only those sharing services that you really need.
- Use a local account - This provides greater security than, for example, a Microsoft account which, if hacked, it will enable remote logon to your applications.
- Enable secure boot and UEFI, instead of legacy BIOS.
- Disable Flash and Java. These frequently report security vulnerabilities.
- Encrypt hard drive. This will protect your data if your computer accessed directly.



NOTE:

SAC 10.5 is compliant with Windows 10 Microsoft Credential Guard and Windows 8.1 Local Security Authority (LSA) with code integrity enabled.

Installation

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

**NOTE:**

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

Firefox Settings:

- After installing SAC 10.5, ensure that the Gemalto PKCS#11 module does not exit in the Firefox security settings.
-

Installation Files

The software package provided by SafeNet includes files for installing or upgrading to SafeNet Authentication Client 10.5.

The following installation and documentation files are provided:

File	Environment	Description
Windows		
SafeNetAuthenticationClient-x32-10.5.msi	32-bit	Installs SafeNet Authentication Client 10.5, and upgrades from earlier versions of SafeNet Authentication Client.
SafeNetAuthenticationClient-x64-10.5.msi	64-bit	
SACCustomizationPackage-10.5.msi	32-bit 64-bit	Installs SafeNet Authentication Client 10.5 Customization Package. Use to customize SafeNet Authentication Client installation with non-default settings. If a previous version of the Customization package exists, uninstall the previous version, and then install the new version.
Documentation Files		
007-013559-007_SafeNet Authentication Client_10.5_Windows_GA_RN_Revision B		SafeNet Authentication Client 10.5 Release Notes for Windows. Read before installation for last minute updates that may affect installation; contains important information such as resolved and known issues and troubleshooting.
007-013561-005_SafeNet Authentication Client 10.5_Windows_User Guide_Revision A		SafeNet Authentication Client 10.5 User Guide for Windows. Provides detailed information for the user and system administrator regarding the use of SafeNet Authentication Client.
007-013560-005_SafeNet Authentication Client 10.5_Windows_Administrator Guide_Revision A		SafeNet Authentication Client 10.5 Administrator Guide for Windows (this document). Provides detailed information for the system administrator regarding the installation, configuration, maintenance, and management of SafeNet Authentication Client.

System32 and SysWOW64 Folders

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

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

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

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

- For 64-bit installations, both the C:\Windows\System32 folder and C:\Windows\SysWOW64 folder are created and all the 64-bit binaries are located in the System32 folder and all 32-bit binaries are located in the SysWOW64 folder.
- For 32-bit installations: Only the C:\Windows\System32 folder is created and only the 32-bit binaries are located in this folder.
- There is an option available that allows checking SAC binary signatures via the SafeNet Authentication Client User Interface (About Window). For more information, refer to the SafeNet Authentication Client User Guide.

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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Install SafeNet Authentication Client using the installation wizard, and select the Custom option.

Installing SafeNet Authentication Client on Windows (MSI)

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

The components that can be set using the wizard are:

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



NOTE:

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

To install via the installation wizard:

1. Log on as an administrator.
2. Close all applications.
3. Double-click the appropriate file:
 - `SafeNetAuthenticationClient-x32-10.5.msi` (32-bit)
 - `SafeNetAuthenticationClient-x64-10.5.msi` (64-bit) The **SafeNet**

Authentication Client Installation Wizard opens.



4. Click **Next**.

The Interface Language window is displayed.



NOTE:

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



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

The *End-User License Agreement* is displayed.



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

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



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

C:\Program Files\SafeNet\Authentication\



NOTE:

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

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

11. Click **Next**.

The *Setup Type* window opens.

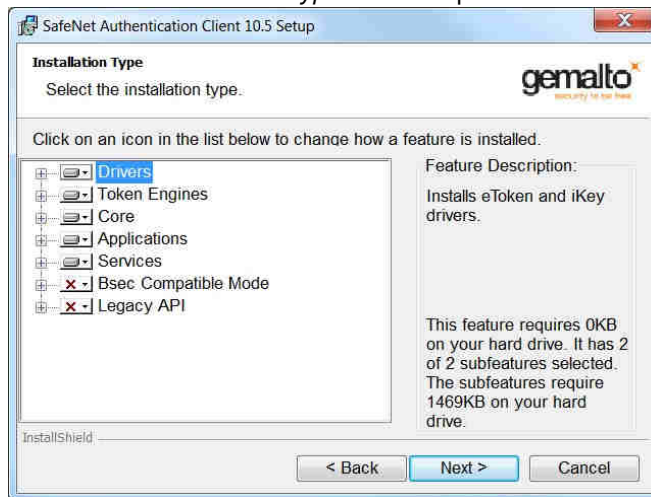


12. Select one of the following:

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

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

The *Custom Installation Type* window opens.



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

The installation proceeds.



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



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

Uninstall

After SafeNet Authentication Client 10.5 has been installed, it can be uninstalled. Local administrator rights are required to uninstall SafeNet Authentication Client. When SafeNet Authentication Client is uninstalled, user configuration and policy files may be deleted.

Uninstall Overview

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

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

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

- *Uninstalling via Add or Remove Programs* on page 54
- *Uninstalling via the Command Line* on page 55



NOTE:

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

Uninstalling via Add or Remove Programs

To uninstall via *Add or Remove Programs*:

1. From the Windows taskbar, select **Start > Settings > Control Panel**.
2. Double-click **Add or Remove Programs**.
3. Select **SafeNet Authentication Client 10.5** and click **Remove**.
4. Follow the instructions to remove the application.

If the PROP_CLEAR_REG property was not enabled during installation, a *Save settings* window is displayed.

5. Click **Yes** to save the machine and user registry settings, or **No** to delete them.
The uninstall process proceeds.

Uninstalling via the Command Line

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

To uninstall via the command line:

1. Log on as an administrator.
2. Close all applications.
3. From the Windows taskbar, select **Start > Programs > Accessories > Command Prompt**. Right-click **Command Prompt**, and select **Run as Administrator**.
4. Type the appropriate command line utility:
`msiexec /x SafeNetAuthenticationClient-x32-10.5.msi` (for 32-bit installations)
`msiexec /x SafeNetAuthenticationClient-x32-10.5.msi` (for 64-bit installations)
To uninstall in silent mode, add `/qn` to the end of the command.

When the uninstall completes, restart the computer.

Installing SafeNet Authentication Client on Mac OS X

The installation package is SafeNetAuthenticationClient.10.1.x.0.dmg.

To install with the installer:

1. Double click the **SafeNetAuthenticationClient.10.1.x.0.dmg** file.
A new disk image file is created in the Finder window, including an pkg installation file and an uninstall application.

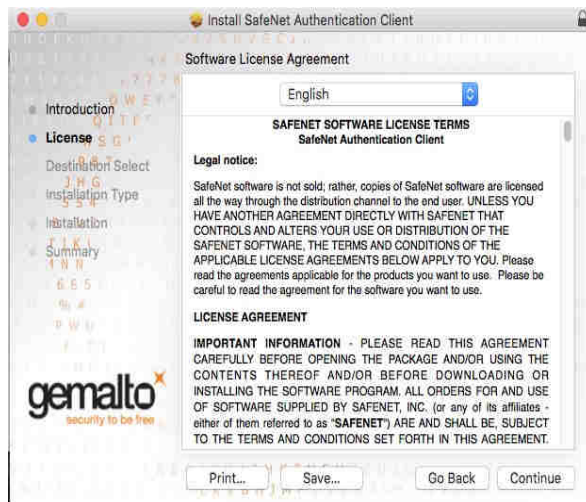


2. To start the installation, double click **SafeNet Authentication Client 10.1.pkg**.

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

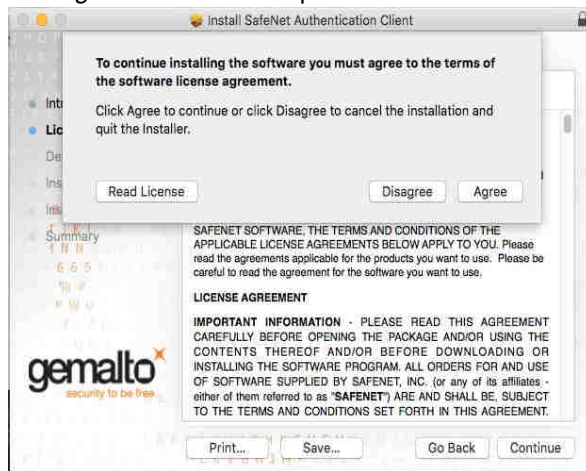


3. Click **Continue**.
Software License Agreement window opens.



4. Click **Continue**.

The *Agreement* window opens.



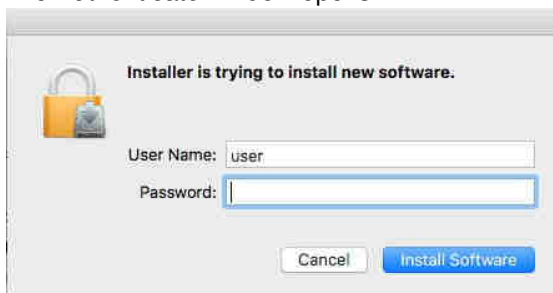
5. Click **Agree** to accept the software license agreement.

Standard Install window opens.



6. Click **Install**.

The *Authenticate* window opens.



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

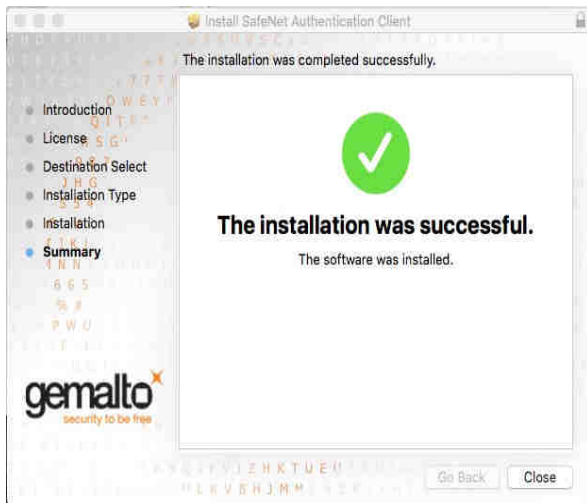


NOTE:

Administrator permissions are required to install SafeNet Authentication Client.

SafeNet Authentication Client is installed.

Installation completed successfully screen opens.



8. Click **Close** and then perform a **Restart** (recommended).
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 10.1.pkg 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\ 10.1.pkg/ -target /`
3. Enter your root password when prompted.
SafeNet Authentication Client 10.1 is installed.
4. It is recommended to Restart Mac OS X.

Uninstall

After SafeNet Authentication Client 10.1 Mac has been installed, it can be uninstalled. Local administrator rights are required to uninstall SafeNet Authentication Client. When SafeNet Authentication Client is uninstalled, user configuration and policy files may be deleted.

Uninstalling - Mac

Before uninstalling SafeNet Authentication Client 10.1 Mac, make sure that SafeNet Authentication Client Tools is closed.

To uninstall SafeNet Authentication Client 10.1 Mac:

1. Double click **SafeNetAuthenticationClient.10.1.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) 10.1**.

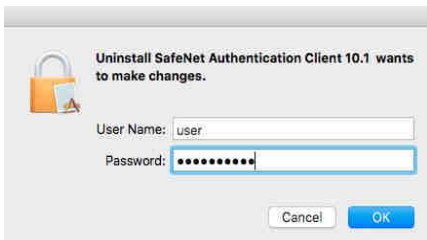
The **Welcome to the SafeNet Authentication Client Uninstaller** window opens.



3. Click **Uninstall**.

The *Authenticate* window opens.

4 – Uninstall



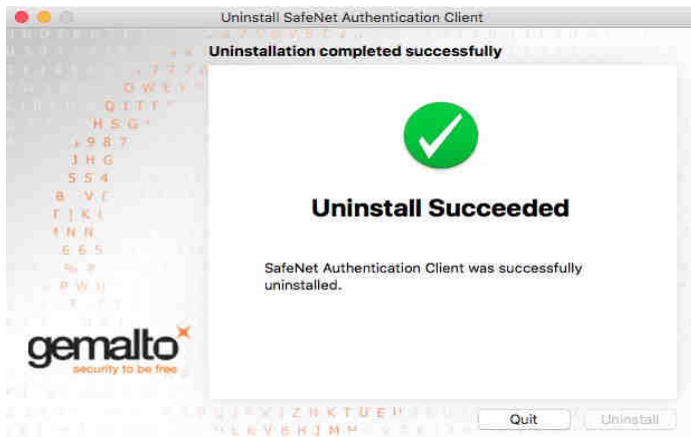
4. Enter a **Name and Password** and click **OK**.



NOTE:

You require Administrator permissions to uninstall SafeNet Authentication Client Mac 10.1.

The *Uninstallation completed successfully* window opens.



5. Click **Quit**.

Installing SAC on Linux Standard Package

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

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 and Red Hat operating systems, in cases where the nss-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-10.0.xx-0.i386.rpm`
- 64-bit - `SafenetAuthenticationClient-10.0.xx-0.x86_64.rpm`

where: xx 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 -Uvh SafenetAuthenticationClient-10.0.xx-0.i386.rpm`
 - On a 64-bit OS: `rpm -Uvh SafenetAuthenticationClient-10.0.xx-0.x86_64.rpm`

where: -hi is the parameter for installation and x is the version number.

Installing on Ubuntu and Debian

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

**NOTE:**

For the PKCS#11 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.

The following is the SafeNet Authentication Client .deb package:

- .deb Package Name:
 - 32-bit: SafenetAuthenticationClient-10.0.xx-0_i386.deb
 - 64-bit: SafenetAuthenticationClient-10.0.xx-0_amd64.deb
- where: xx 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, 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: `sudo dpkg -i SafenetAuthenticationClient-10.0.xx-0_i386.deb`

- On a 64-bit OS: `sudo dpkg -i SafenetAuthenticationClient-10.0.xx-0_amd64.deb` where: `xx` 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.**

**NOTE:**

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

Installing the Core Package

Installing on Red Hat Enterprise, SUSE, CentOS and Fedora

The installation package for SafeNet Authentication Client running on RedHat and CentOS 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-10.0.xx-0.i386.rpm`
- **64-bit:** `SafenetAuthenticationClient-core-10.0.xx-0.x86_64.rpm`

where: `x` 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-10.0.xx-0.i386.rpm`
 - **On a 64-bit OS:** `rpm -hi SafenetAuthenticationClient-core-10.0.xx-0.x86_64.rpm`

where: `-hi` is the parameter for installation and `x` 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-10.0.xx-0_i386.deb`
- 64-bit: `SafenetAuthenticationClient-core-10.0.xx-0_amd64.deb` **where:** `xx` 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-10.0.xx-0_i386.deb`

- On a 64-bit OS: `sudo dpkg -i SafenetAuthenticationClient-core-10.0.xx-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.

Linux External Dependencies

Red Had Enterprise, SUSE, CentOS and Fedora

- PCSC (Smart Card Resource manager): `libpcsclite1`

Ubuntu

- PCSC (Smart Card Resource manager): `libpcsclite1`

Installing the Firefox Security Module on Linux

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 **Firefox Preferences > 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:
On 32-bit: `/usr/lib/libeTPkcs11.so`
On 64-bit: `/usr/lib64/libeTPkcs11.so`



NOTE:

- To work with CC devices in unlinked mode, enter the following string for Multi-Slot support:
for 32-bit: `/usr/lib/libIDPrimePKCS11.so`
for 64-bit: `/usr/lib64/libIDPrimePKCS11.so`
- For information on how to work with Multi-Slots, see the PKCS#11 Digital Signature PIN Authentication section of the SafeNet Authentication Client User Guide.

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: On 32-bit: `/usr/lib/libeTPkcs11.so` On 64-bit: `/usr/lib64/libeTPkcs11.so`



NOTE:

- To work with CC devices in unlinked mode, enter the following string for Multi-Slot support:
for 32-bit: `/usr/lib/libIDPrimePKCS11.so`
for 64-bit: `/usr/lib64/libIDPrimePKCS11.so`
- For information on how to work with Multi-Slots, see the PKCS#11 Digital Signature PIN Authentication section of the SafeNet Authentication Client User Guide.

The *Confirm* window opens.

5. Click **OK**.

The new security module is installed.

Uninstall

After SafeNet Authentication Client 10.0 Linux has been installed, it can be uninstalled. Local administrator rights are required to uninstall SafeNet Authentication Client. When SafeNet Authentication Client is uninstalled, user configuration and policy files may be deleted.

Uninstalling Linux Standard Package

Before uninstalling SafeNet Authentication Client 10.0 Linux, make sure that SafeNet Authentication Client Tools is closed.

Uninstalling on Red Hat Enterprise, SUSE, CentOS and Fedora

To uninstall:

- Enter the following:

```
rpm -e SafenetAuthenticationClient-10.0.xx-0.i386.rpm
```

Where `-e` is the parameter for uninstalling.

Uninstalling on Ubuntu and Debian

To uninstall:

- In the console, enter the following:

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

Where `--purge` is the parameter for uninstalling.

Uninstalling the Core Package

Uninstalling on Red Hat Enterprise, SUSE, CentOS and Fedora

To uninstall:

- Enter the following:

```
rpm -e SafenetAuthenticationClient-core-10.0.xx-0.i386.rpm
```

Where `-e` is the parameter for uninstalling.

Uninstalling on Ubuntu or Debian

To uninstall:

- In the console, enter the following:
`SafenetAuthenticationClient-core-10.0.xx-0_i386.deb`

Where `--purge` is the parameter for uninstalling.