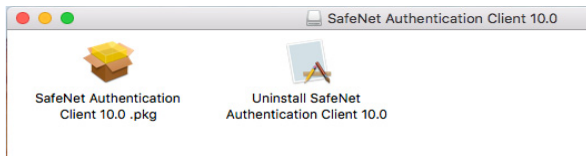


## Installing SafeNet Authentication Client on Mac OS X

The installation package is `SafeNetAuthenticationClient.10.0.x.0.dmg`.

### To install with the installer:

1. Double click the **SafeNetAuthenticationClient.10.0.x.0.dmg** file.  
A new disk image file is created in the Finder window, including an pkg installation file and an uninstall application.

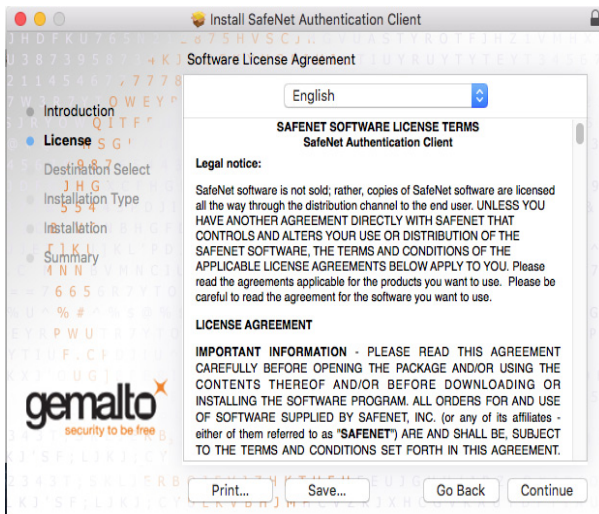


2. To start the installation, double click **SafeNet Authentication Client 10.0.pkg**.  
The *Welcome to the SafeNet Authentication Client Installer* window opens.



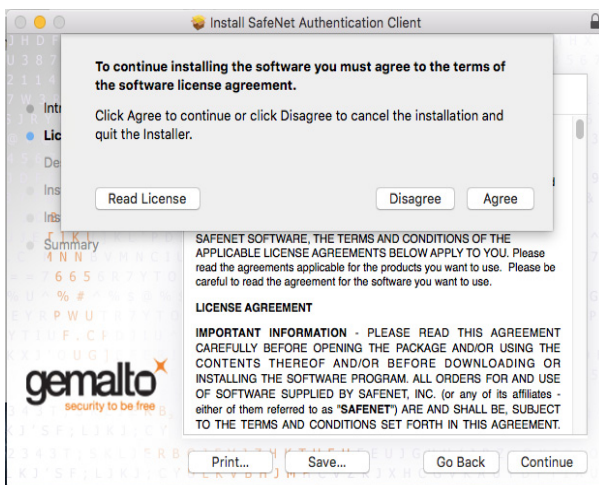
3. Click **Continue**.

The *Software License Agreement* window opens.



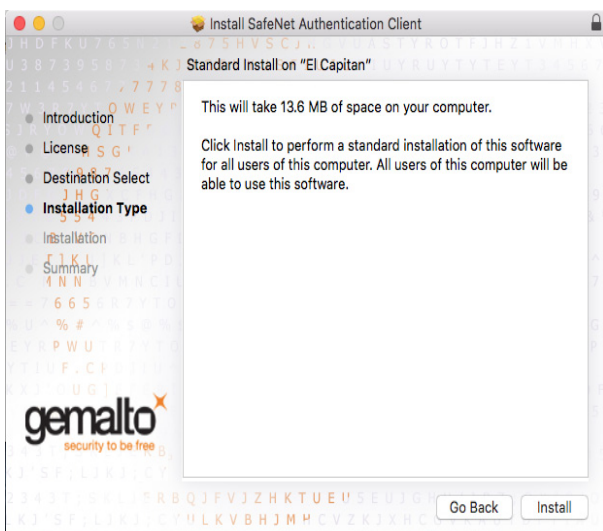
4. Click **Continue**.

The *Agreement* window opens.



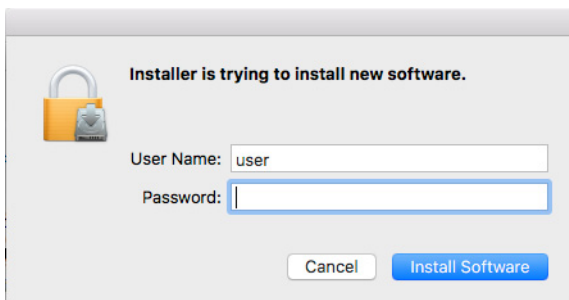
5. Click **Agree** to accept the software license agreement.

The *Standard Install* window opens.



6. Click **Install**.

The *Authenticate* window opens.



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

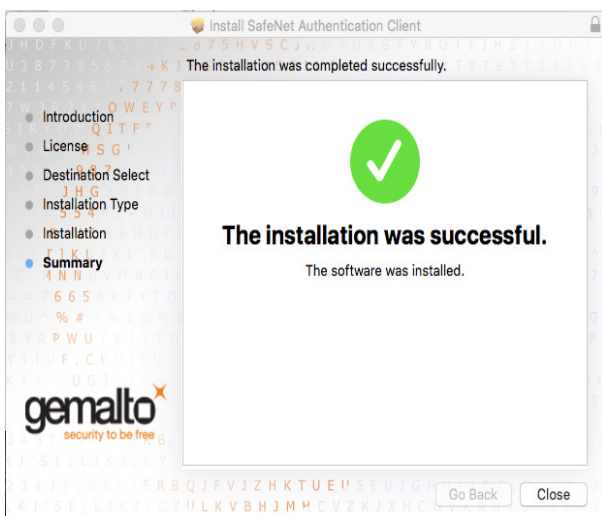


**NOTE:**

Administrator permissions are required to install SafeNet Authentication Client.

SafeNet Authentication Client is installed.

The *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 10.0.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\ 10.0.pkg/ -target /`
3. Enter your root password when prompted.  
SafeNet Authentication Client 10.0 is installed.
4. It is recommended to Restart Mac OS X.

---

## Preparing SAC Mac Custom Installation

---

The custom installation script creates an additional customized installation file (SafeNet Authentication Client Customization 10.0.mpkg) with specific license and configuration properties and values.

**NOTE:**

Before installing the SafeNet Authentication Client Customization 10.0.mpkg file, you must install SAC 10.0.

---

**To create a custom installation:**

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

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

4. Run the script:

```
./createSacCustomInstallation
```

The file **SafeNet Authentication Client Customization 10.0.mpkg** is created in the **Custom Installation\output** folder.

5. The SafeNet Authentication Client Customization 10.0.mpkg file can now be distributed to all users in the organization as an additional SAC 10.0 installation.

---

## Running SafeNet Authentication Client Customization 10.0.mpkg

---

By running the SafeNet Authentication Client Customization 10.0.mpkg file the following is implemented:

- The **/etc/eToken.conf** file (created by the Mac SAC 10.0 installation) is replaced by the eToken.conf file, located in the **Custom Installation\CustomerConfiguration** folder.
- The **SacLicense.lic** file, located in the **Custom Installation\CustomerConfiguration** folder is copied to the **/Users/Shared/SafeNet/SAC** folder.

---

## Installing the Firefox Security Module on Mac

---

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

### To install the security module in Firefox

1. Open **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:

```
/usr/local/lib/libeTPkcs11.dylib
```



---

**NOTE:**

- To work with CC devices in unlinked mode, enter the following string for Multi-Slot support:  
**/usr/local/lib/libidprimepkcs11.0.dylib**
  - 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:

```
/usr/local/lib/libeTPkcs11.dylib
```



#### NOTE:

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.

## Configuring Acrobat Security Settings

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

### To set Adobe Acrobat security settings:

1. Open Adobe Acrobat and select **Preferences > Signatures > Identities & Trusted Certificates > More**.  
The *Digital ID and Trusted Certificate Settings* window opens.
2. From the left panel, click **Digital IDs > PKCS#11 Modules and Tokens**.
3. If a PKCS#11 Module is not attached, click **Attach Module**, browse to **SAC PKCS11 lib/usr/local/lib/libeTPkcs11.dylib** and click **Open**.

The *connected token and certificate appear under PKCS#11 Modules and Tokens*.



#### NOTE:

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.

### To verify the security settings:

1. Select **Tools > Sign & Certify > More Sign & Certify > Manage Trusted Identities**.  
The *Manage Trusted Identities* window opens.
2. Select the contact and click **Details**.

The *Edit Contact* window opens.

3. Select the contact and click **Show Certificate**.

The *Certificate Viewer* Window opens.

4. Select the **Trust** tab.

- Trusted settings for the certificate are marked with a green check-mark.
- Non-trusted settings are marked with a red cross.

## Loading the Token PKCS#11 Security Module

To use SafeNet Authentication Client the PKCS#11 security module must be loaded.



### NOTE:

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

## New Locations of PKCS#11 Security Module and Tokend

El Capitan introduced a new security feature called “System Integrity Protection” (see <https://support.apple.com/en-us/HT204899>).

This means that the SAC PKCS11 library is installed in a different location for El Capitan (this is not relevant to earlier Mac versions):

SAC PKCS#11 library files are installed in `/usr/local/lib/` instead of `/usr/lib/`. This new location must be updated in applications using the SAC PKCS#11 module, such as Mozilla Firefox, Thunderbird or Adobe Reader.

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

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

The *Device Manager* window opens

2. If eToken is not listed in the Security Modules and Devices column, click **Load**.

The *Load PKCS#11 Device* window opens.

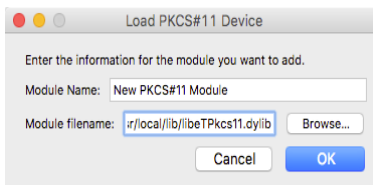




3. Do the following:
  - Replace the contents of the Module Name field with eToken.
  - In the Module filename field, enter the following:  
`/usr/lib/libeTPkcs11.dylib`

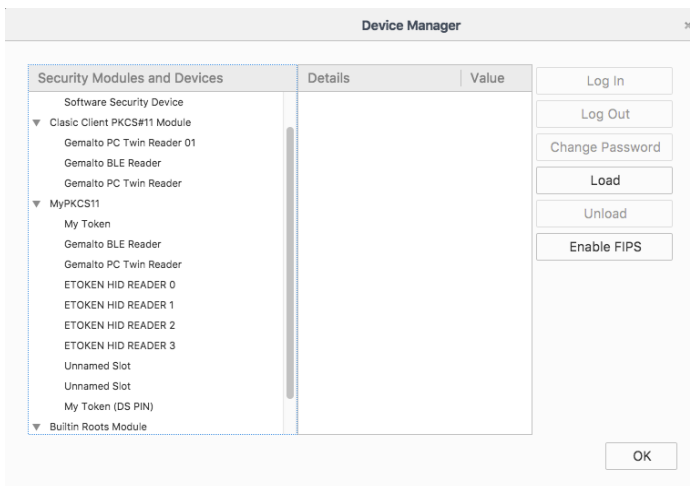
**NOTE:**

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.



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

## Upgrading SafeNet Authentication Client on a Mac

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

After upgrading from SAC 9.1 to SAC 10.0 on a Mac, it is recommended that you restart the machine in order for the device to be recognized.

# Uninstall

After SafeNet Authentication Client 10.0 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.

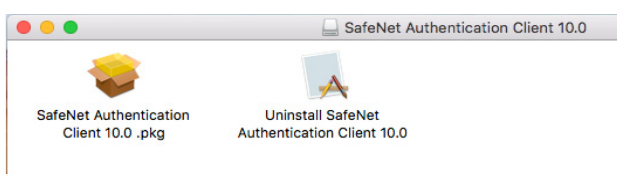
## Uninstalling - Mac

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

### To uninstall SafeNet Authentication Client 10.0 Mac:

1. Double click **SafeNetAuthenticationClient.10.0.x.0.dmg** file.

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



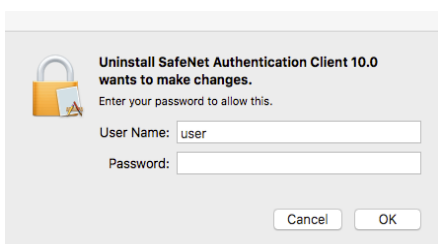
2. Click **Uninstall SafeNet Authentication Client (Mac) 10.0**.

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



3. Click **Uninstall**.

The *Authenticate* window opens.



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

**NOTE:**

You require Administrator permissions to uninstall SafeNet Authentication Client Mac 10.0.

5. Click **Quit**.