

SafeNet Authentication Client

MAC CUSTOMER RELEASE NOTES

Version: 10.0 – Mac (GA)
Build 26
Issue Date: March 2017
Document Number: 007-013724-001

Contents

Product Description	2
Release Description.....	2
New Features and Enhancements.....	2
Advisory Notes.....	3
Licensing.....	3
Default Password.....	3
Password Recommendations	3
Compatibility Information	4
Browsers.....	4
Operating Systems	4
Tokens	4
Certificate-based USB Tokens	4
Certificate-based Hybrid USB Tokens.....	4
Software Tokens	4
Smart Cards	5
End-of-Sale Tokens/Smart Cards	5
End-of-Life Tokens/Smart Cards.....	5
External Smart Card Readers	6
Localizations	6
Compatibility with Third-Party Applications.....	6
Installation.....	7
Resolved Issues (Mac)	7
Known Issues (Mac)	7
Known Issues – Deprecated Devices	9
Product Documentation	10
Support Contacts	10

Product Description

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.

Release Description

SafeNet Authentication Client 10.0 Mac introduces full IDPrime support including Multi-Slot support and Password Quality modifications for IDPrime MD cards.

IDPrime MD cards are PKI smart cards. Administrators and users can use and manage IDPrime MD smart cards seamlessly via the standard PKCS#11 interface and without the need for any additional middleware. They offer secure IT Security and ID access and are compatible with the NFC standard.

New Features and Enhancements

SafeNet Authentication Client 10.0 Mac offers the following new features:

- **Rebranding:** SAC Mac UI and documentation have Gemalto branding.
- **Support for the following IDPrime cards:**
 - IDPrime MD 830-FIPS
 - IDPrime MD 830-ICP
 - IDPrime MD 830 B
 - IDPrime MD 3810 Dual Interface Card
 - IDPrime MD 3810 MIFARE 1K (Contact and Contactless mode)
 - IDPrime MD 3811
- **Support for IDPrime .NET cards**
- **Support for the following IDPrime MD Common Criteria cards:**
 - IDPrime MD 840
 - IDPrime MD 840 B
 - IDPrime MD 3840– Dual Interface Card
- **Support for SafeNet eToken 5110 Common Criteria**
- **Support for SafeNet eToken 5110 FIPS**
- **Support for unlocking IDPrime MD card range**
- **Friendly Admin Password** - short user friendly passwords are now supported (on IDPrime MD and eToken 5110 CC devices) instead of using 48 hexadecimal digits. For more details, see the SafeNet Authentication Client 10.1 User Guide.
- **Support for Common Criteria PKCS#11 Multi-Slot** – for Common Criteria devices in unlinked mode. For information on how to work with Multi-Slots, see the PKCS#11 Digital Signature PIN section in the SafeNet Authentication Client User Guide.
- **PIN Quality modifications for IDPrime MD cards.**
- **Bug fixes** – this release includes bug fixes from previous SAC Mac versions.

Advisory Notes

- The Tokend security module can be used only to perform “read-only” operations, i.e. it cannot update the card.
- Some contactless readers are not fully compliant with PC/SC v2.0. They do not work properly with the most recent smartcards e.g. the Advanced Card System ACR 122 reader is not compatible with IDPrime MD 3811 and with the DESFire EV1, due to a gap in the PC/SC v2.0 standard.
- SAC 10.0 Mac enables you to manually disable certain cryptographic algorithms. Any cryptographic algorithms in this list will be blocked. See the Disable-Crypto feature in the SafeNet Authentication Client 10.0 Mac Administrator Guide.

Licensing

The use of this product is subject to the terms and conditions as stated in the End User License Agreement. A valid license must be obtained from the SafeNet License Center: <https://lc.cis-app.com/>.

Default Password

SafeNet eToken devices are supplied with the following default token password: 1234567890.

IDPrime cards are supplied with the following default token password: “0000” (4 digits). The administrator password must be entered using 48 hexadecimal zeros (24 binary zeros).

For IDPrime MD 840/3840/eToken 5110 CC devices:

- The default Digital Signature PIN is “000000” (6 digits)
- The default Digital Signature PUK is “000000” (6 digits)

Password Recommendations

We strongly recommend changing all device passwords upon receipt of a token/smart card according to the following:

- User PIN should include at least 8 characters of different types.
- Admin PIN should include at least 16 characters of different types.
- Digital Signature PUK, when using a friendly name, should include at least 16 characters of different types.



NOTE: Character types include upper case, lower case, numbers, and special characters.

Compatibility Information

Browsers

SafeNet Authentication Client 10.0 Mac supports the following browsers:

- Safari 10.1
- Firefox (up to and including version 52)
- Chrome version 57, for authentication only (does not support certificate enrollment)

Operating Systems

SafeNet Authentication Client 10.2 Windows supports the following operating systems:

- OSX 10.11 El Capitan
- OSX 10.12 Sierra

Tokens

SafeNet Authentication Client 10.0 Mac supports the following tokens:

Certificate-based USB Tokens

- SafeNet eToken 5110
- SafeNet eToken 5110 CC
- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 FIPS HID
- SafeNet eToken 5110 HID

Certificate-based Hybrid USB Tokens

- SafeNet eToken 7300
- SafeNet eToken 7300-HID

Software Tokens

- SafeNet Virtual Token
- SafeNet Rescue Token

Smart Cards

- Gemalto IDPrime MD 840
- Gemalto IDPrime MD 840 B
- Gemalto IDPrime MD 3840
- Gemalto IDPrime MD 3840 B
- Gemalto IDPrime MD 830-FIPS
- Gemalto IDPrime MD 830-ICP
- Gemalto IDPrime MD 830 B
- Gemalto IDPrime MD 3810
- Gemalto IDPrime MD 3811
- Gemalto IDPrime .NET (only SAC PKCS#11 and IDGo 800 Minidriver interfaces)



NOTE: For more information on IDPrime MD Smart Cards, see the IDPrime MD Configuration Guide.

End-of-Sale Tokens/Smart Cards

- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID
- SafeNet eToken 4100
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)

End-of-Life Tokens/Smart Cards

- SafeNet eToken PRO 32K v4.2B
- SafeNet eToken PRO 64K v4.2B
- SafeNet eToken Pro SC 32K v4.2B
- SafeNet eToken Pro SC 64K v4.2B
- SafeNet eToken 7100 (SafeNet eToken NG-Flash)
- SafeNet iKey: 2032, 2032u, 2032i (Windows and Mac only)
- SafeNet smart cards: SC330, SC330u, SC330i
- SafeNet eToken 5000 (iKey 4000)
- SafeNet eToken 4000 (SC400)
- SafeNet eToken PRO Java 72K
- SafeNet eToken PRO Anywhere
- SafeNet eToken PRO Smartcard 72K

External Smart Card Readers

SafeNet Authentication Client 10.0 Mac supports the following smart card readers:

- Gemalto IDBridge K30
- Gemalto IDBridge K50
- Gemalto IDBridge CT30
- Gemalto IDBridge CT40
- Gemalto IDBridge CL 3000 (ex Prox-DU)
- SCR 3310 v2 Reader
- Athena AESDrive IIIe USB v2 and v3
- Advanced Card System ACR 1281U
- Athena Keyboard
- Omnikey 3121
- Dell Broadcom (This reader is found only in laptops)
- Unotron



NOTE: SC Reader drivers must be compatible with the extended APDU format in order to be used with RSA-2048.

Mobile PKI Bluetooth Readers:

- SafeNet Reader CT1100
- SafeNet Reader K1100

Localizations

SafeNet Authentication Client 10.0 Mac supports only English.

Compatibility with Third-Party Applications

Most of the third-party applications listed below have been validated and tested with SafeNet Authentication Client 10.0 Mac (GA).

Solution Type	Vendor	Product Version
Virtual Desktop Infrastructure (VDI)	Citrix	XenApp/XenDesktop 7.11
VPN	Checkpoint	E80.61
Digital Signatures	Adobe	Reader XI and DC
	Microsoft	Outlook 2016
	Mozilla	Thunderbird 45
Smart Card Logon	Centrify	5.1.3.482

Installation

SafeNet Authentication Client must be installed on each computer on which IDPrime MD cards, as well as SafeNet Tokens or Smart Cards are to be used. Local administrator rights are required to install or uninstall SafeNet Authentication Client.

Resolved Issues (Mac)

Issue	Synopsis
ASAC-3865	SAC installation failed when using a Software Deployment Tool on El Capitan OS.
ASAC-1315	When working with SafeNet smart cards and iKey 4000 using SAC Tools, the amount of unblocking code retries remaining could not be changed , unless the token or smart card were locked. (i.e. there was no way of determining how many unblocking code retries remained).

Known Issues (Mac)

Issue	Synopsis
ASAC-4974	Summary: When you are logged in as a user and changes are made to the Password Quality settings, the enter Administrator password window is displayed, but the changed settings are not saved. Workaround: The user must log out before making Password Quality modifications.
ASAC-4394	Summary: When 2 iKey devices are connected simultaneously, the machine cannot detect an iKey device until a reboot is done. If there are 2 iKeys connected only one is recognized in SAC Tools. Workaround: Define the following in eToken.conf: [GENERAL] PcscSlots=1
ASAC-4270	Summary: After upgrading SAC Mac, the previous SAC version is displayed in the SAC monitor About window. Workaround: Perform a restart.
ASAC-2849	Summary: Enrolling a certificate on Mac via CheckPoint VPN E80.61 failed. Workaround: Use an enrolled certificate when connecting to VPN via CheckPoint.
ASAC-2834 ASAC-1853	Summary: When connecting an eToken 7300 for the first time, to a Mac version 10.9 and 10.0 system, the eToken 7300 was recognized in CCID debug mode. The device was unrecognized when the eToken 7300 was removed and then re-connect for the second time. Workaround: If SAC is installed, use the VSR driver. If SAC is not installed, use HID support.

Issue	Synopsis
ASAC-2299	<p>Summary: eToken Virtual devices that are locked to flash, and were enrolled on SafeNet Authenticaion Manager using a USB 3 port, cannot function on a USB 2 port, and visa versa.</p> <p>Workaround: If the eToken Virtual was enrolled on a USB 3 port, then use the token on a USB 3 port only. If the eToken Virtual was enrolled on a USB 2 port, then use the token on a USB 2 port only.</p>
ASAC-2298	<p>Summary: Connection problems occur when eToken Virtual devices are locked to flash and enrolled on a VMware environment.</p> <p>Workaround: When using an eToken Virtual device that is locked to flash, make sure the device is enrolled on a regular environment and not VMware.</p>
ASAC-2296	<p>Summary: eToken Virtual (on a Mac) is not recognized in the Keychain application, causing Safari , the default mail application and outlook not to work.</p> <p>See apple bug report: 19613234.</p> <p>Workaround: None.</p>
ASAC-2235	<p>Summary: After installing SAC, the PKCS11 module was not inserted automatically into Firefox's browser.</p> <p>Workaround: Insert the module manually.</p>
ASAC-2233	<p>Summary: After opening the KeyChain application and selecting the 'Lock all Keychains' parameter, it is not possible to log on to the token in Keychain, and SSL in Safari cannot be established.</p> <p>Workaround: Disconnect the token, and then re-connect it.</p>
ASAC-2227	<p>Summary: When two tokens are connected, one of the token's settings are not accessible in SAC Tools.</p> <p>Workaround: Work with one connected token at a time.</p>
ASAC-2223	<p>Summary: Occasionally, when an eToken is disconnected, and then a different token is connected, the first token is still shown in SAC Tools. This is due to a Mac OS X issue.</p> <p>Workaround: Restart the machine.</p>
ASAC-2191	<p>Summary: When working with a 5100 token that is recognized via the CCID driver, the token might not be recognized or the system may not respond when the machine returns from sleep mode.</p> <p>Workaround: Re-insert the token.</p>
ASAC-2079	<p>Summary: Some Keychain related functions do not work on Yosemite when using iKey 2032 and 4000.</p> <p>Workaround: Disconnect and then connect the token.</p>
ASAC-1470	<p>Summary: After updating the FW on an eToken 7300, the FW version might not be updated under Token information in SAC Tools.</p> <p>Workaround:</p>
ASAC-1053	<p>Summary: When re-decrypting an email using Microsoft Outlook on Mac, the decrypt process fails.</p> <p>Workaround: Perform the following:</p> <ol style="list-style-type: none"> 1. Disconnect the token, and close Outlook. Connect the token, and reopen Outlook.

Issue	Synopsis
ASAC-1035	<p>Summary: When connecting a CCID Smart Card reader, to a Mac system, the iKey 4000 device is unrecognized.</p> <p>Workaround: Perform one of the following:</p> <ol style="list-style-type: none"> 1. Disconnect the Smart Card reader, and reboot the system. 2. Install the latest Omnikey Smart Card reader driver. ifdokccid_mac_universal-3.1.0.2.bundle. <p>Disable the Mac OS X GENERIC Smart Card reader driver by removing it.</p>

Known Issues – Deprecated Devices

Issue	Synopsis
ASAC-1315	<p>Summary: When working with SafeNet smart cards and iKey 4000 using SAC Tools, the amount of unblocking codes retries remaining cannot be changed , unless the token or smart card are locked. (i.e. there is no way of determining how many unblocking code retries remain).</p> <p>Workaround: None. This is by design.</p>

Product Documentation

The following product documentation is associated with this release:

- 007-013726-001_SafeNet Authentication Client 10.0_Mac_Administrator Guide_Revision A
- 007-013725-001_SafeNet Authentication Client 10.0_Mac_User Guide_Revision A

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

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