SafeNet Authentication Client 10.9 (GA)

MAC RELEASE NOTES

Issue Date: December 2024

Build: 2499
Document Part Number: 007-0013724-005 Rev. A

Contents

Product Description

SafeNet Authentication Client (SAC) 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 10.9 (GA) Mac includes new features and bug fixes from previous SAC versions.

New Features and Enhancements

This release offers the following:

> Support for macOS 15 Sequoia.

> Support for IDPrime PIV cards and tokens, which includes reading the PIN Policy, Unlocking a token, Reinitialization of Admin key, reading logical Serial Number (for SafeNet Fusion S2 NFC PIV only), and token ID features.

> Support for SafeNet eToken Fusion S2 NFC PIV, and SafeNet IDPrime 3940C.

For details, refer to "Tokens" on page 5.

> External PIN PAD reader support for IDPrime 940 SIS.

> Reintroduced *Enforce FIPS* settings in SAC, which enables the ability to initialize eToken 5110+ with or without FIPS.

> Improvements done in SAC Tools related to SafeNet IDPrime 940 SIS.

> Security improvements, for example: TLS 1.3.

> Fixes from previous release. Refer to "Resolved Issues" on page 15.

Advisory Notes

Before deploying this release, note the following high-level requirements and limitations:

> **TokenD deprecated-** Due to Apple’s decision (starting from macOS 10.15.1 and above) to no longer support TokenD. Customers should either start using Crypto Token Kit (CTK) instead of TokenD, or continue using earlier versions of macOS (10.15.0 or below), which still supports TokenD.

> SAC 10.8 onwards supports Crypto Token Kit (CTK) framework only. When CTK is enabled:

- Tokens and certificates under keychain GUI: Not Displayed
- Sign only certificate usage: Applicable

> **Notarization-** This release is notarized. For more details, refer to https://developer.apple.com/documentation/xcode/notarizing_macos_software_before_distribution
As of January 2020, macOS Catalina notarized software is mandatory. SAC 10.9 (GA) is notarized and verified using the following command line: `xcrun stapler validate myapp.app`.

For more information, refer to https://help.apple.com/xcode/mac/current/#/dev88332a81e?sub=dev68b6e38a3

> **AKS drivers deprecated-** SAC 10.8 onwards removes the support for AKS drivers.

> **RSA 1024 key size deprecated-** SAC 10.8 onwards removes the support for RSA 1024 key size signing with SHA-1.

If you need it, use the `Disable-Crypto` setting mentioned in *SafeNet Authentication Client Administrator Guide*

> SafeNet IDPrime 930/3930:

- SafeNet IDPrime 930 has different profiles. A non-managed profile has no Administrator PIN and therefore, cannot be used in Managed environments (CMS).
- After deleting a key from a SafeNet IDPrime 930/3930 device, the available memory size may be reduced.

  For more information, refer to *IDPrime 930/3930 Card Configuration Guide*.

> eToken 5110 FIPS:

- Due to an eToken applet limitation, the User PIN Retry counter cannot be set on SafeNet eToken 5110 FIPS or SafeNet eToken 5110, unless they are initialized.

> SafeNet IDPrime 930 L3 cards:

- SHA-1 (160-bit) and RSA 1024-bit are not allowed in FIPS L3 cards. Also, sign operation with hash algorithms SHA-1 and more legacy hash algorithms (like MD5) are not supported. The hash mechanism available to use with sign operation is the SHA-2 mechanism with the following supported lengths: 224*, 256, 384, and 512 bits while 224 bits is not supported by SAC.
- PKCS#1 padding does not allow decrypt on IDPrime 930\3930 FIPS L3 cards.
- Cards (such as IDPrime 930 FIPS L3) that are based on FIPS L3 version 2018 onward, do not allow signing of data using NO_HASH algorithm.
- For IDPrime 930 FIPS L3 cards, the input of CKM_RSA_PKCS mechanism is in the form of OID+DIGEST.

  Where: OID includes one of the following hash functions- SHA256/ SHA384/ SHA512 and DIGEST is the hash value of the hash function indicated by the OID.

> **NOTE** The *RAW RSA* (AKA CKM_RSA_X_509) mechanism for both Sign and Decrypt operations is blocked in all IDPrime devices (including old IDPrime MD devices).

> Access Control setting enables /disables SAC UI buttons only and does not control any security restrictions or SAC functionality. The integration of SAC libraries with any third party applications is supported but should be used diligently by the third party applications.

> Install the CCID driver version 1.5.2 to work with the following tokens:

- SafeNet eToken 5110+ FIPS
- SafeNet eToken 5300 C
- SafeNet eToken Fusion
- SafeNet eToken Fusion S2 NFC PIV
- SafeNet eToken Fusion FIPS

Licensing

From SAC 10.8 release onwards, no license is required for SAC on Mac.

Localizations

This release supports only English.

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 zeros in hexadecimal (24 zeros in binary).

For IDPrime MD 940/3940/840/3840/eToken 5110 CC devices:

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

For IDPrime PIV cards devices:

- The default Admin Password is “01020304050607080102030405060708”
- The default PUK is “12345678"
- The default User PIN is “123456"

Password Recommendations

We strongly recommend changing all device passwords upon receipt of a token/smart card as follows:

> **NOTE** These recommendations are not applicable for IDPrime PIV cards and tokens, and IDPrime 940 SIS.

- User PIN should include at least 8 characters of different types.
- Admin PIN should include at least 16 characters of different types.
- Friendly Admin Password should include at least 16 characters of different types.

  For more details on the Friendly Admin Password, refer to *SafeNet Authentication Client User Guide*.
- Digital Signature PUK, when using a friendly name, should include at least 16 characters of different types.
- For devices running the IDPrime applet, the 3DES random key may be used instead of the administrator password. As per 3DES algorithm for 24 zeros in binary or 48 zeros in hexadecimal values (entered as Admin PIN) every LSB bit is ignored, which means if user enters any random number as the LSB, it will be ignored and more number of Admin PIN are possible.

> **NOTE** It is recommended to not use 24 zeros in binary or 48 zeros in hexadecimal values for Admin PIN.

- Use the password validity period combined with password history options.

> **NOTE** Character types include upper case, lower case, numbers, and special characters. For more information, refer to the ‘Security Recommendations’ chapter in *SafeNet Authentication Client Administrator Guide*.

Initialization Key Recommendations

Thales strongly recommends changing the Initialization Key using the *SAC Initialization* process.

For more details on Initialization Key settings, refer to *SafeNet Authentication Client User Guide*.

Compatibility Information

Browsers

Following browsers are supported:

- Firefox (version 133.0.3) (TLS 1.3 supported)
- Safari 18.1.1 (TLS 1.3 supported)
- Chrome version 131.0.6778.140, for authentication only (does not support certificate enrollment) (TLS 1.3 supported)

Operating Systems

Following operating systems are supported:

- macOS 15 (Sequoia)
- macOS 14 (Sonoma)
- macOS 13.3.1 (a) (Ventura)

Tokens

Following tokens are supported:

Certificate-based USB Tokens

- SafeNet eToken 5300 USB A
- SafeNet eToken 5300 USB A TS
- SafeNet eToken 5300-C
- SafeNet eToken 5300-C TS
- SafeNet eToken 5110
- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110+
- SafeNet eToken 5110+ FIPS
- SafeNet eToken 5110 CC
- SafeNet eToken 5110 CC (940)

- SafeNet eToken 5110+ CC (940B)
- SafeNet eToken 5110+ CC (940C)
- SafeNet eToken Fusion
- SafeNet eToken Fusion CC
- SafeNet eToken Fusion S2 NFC PIV

Smart Cards

- SafeNet IDPrime MD 830nc
- SafeNet IDPrime 930
- SafeNet IDPrime 930nc
- SafeNet IDPrime 3930
- SafeNet IDPrime 930 FIDO
- SafeNet IDPrime 3930 FIDO
- SafeNet IDPrime 940
- SafeNet IDPrime 940B
- SafeNet IDPrime 940C
- SafeNet IDPrime 3940
- SafeNet IDPrime 3940C
- SafeNet IDPrime 940B FIDO
- SafeNet IDPrime 3940 FIDO
- SafeNet IDPrime 940 SIS
- SafeNet IDPrime PIV 3.0
- SafeNet IDPrime PIV 4.0

> **NOTE**
> \- If the Admin PIN is locked on a SafeNet IDPrime 940 or 3940 smart card, the card is left in an unusable state.
> \- If the SafeNet IDPrime 3940 smart card is set with the type B contactless protocol, it is supported by the following readers only:
> \- Gemalto IDBridge CL 3000 (ex Prox-DU)
> \- Advanced Card System ACR 1281U

> **NOTE** Although the majority of contactless cards mentioned in this release notes are compliant with ISO 14443, it is recommended to test these cards on all customer laptop models before placing an order.
>
> For more information on IDPrime MD Smart Cards, refer to *IDPrime MD Configuration Guide*.

> **NOTE** SafeNet IDPrime 3940 and 3930 type B smart cards can be used in contactless mode using the readers in Smart Card Readers supported in Contact and Contactless modes.

External Smart Card Readers

- Omnikey 5422 (contact and contactless)
- Omnikey 5022 (Contactless only)
- Omnikey 3121
- Identiv uTrust 4701 F
- Gemalto IDBridge CT30
- Gemalto IDBridge CT40

> **NOTE**
> - It is recommended to use Vendor drivers for the above SC Readers.
> - SC Reader drivers must be compatible with the extended APDU format in order to be used with RSA-2048

Device Features Supported by SAC

Below table specifies the various features that are supported by SafeNet Authentication Client:

Features:	**Device:**					
	Gemalto IDPrime MD 840/3840/3840 B/ 8840/SafeNet eToken 5110 CC	**SafeNet IDPrime 940**	**Gemalto IDPrime MD 830-FIPS/830-ICP/830B/3810/3810 MIFARE 1K/3811/SafeNet eToken 5300**	**SafeNet IDPrime 930/3930**	**SafeNet eToken 5110-FIPS**	**SafeNet IDPrime PIV cards and tokens**
Number of key containers	14 – default **Note 1**	20 – default **Note 1**	15	32	Dynamic **Note 5**	23 (20 Retired, PIV Authentication, Digital Signature and Key Management) **Note 8**

Features:	Device:					
RSA Key sizes	2048-bit - default 3072-bit 4096-bit **Note 2 & 7**	2048-bit - default 3072-bit 4096-bit - default **Note 2**	2048-bit **Note 3**	2048-bit 3072-bit 4096-bit **Note 3**	2048-bit **Note 3**	For IDPrime PIV 3.0 : > 1024-bit > 1280-bit > 1536-bit > 2048-bit For IDPrime PIV 4.0/eToken Fusion S2 NFC PIV: > 2048-bit > 3072-bit > 4096-bit
RSA Padding	PKCS#1 v1.5, PSS, OAEP	PKCS#1 v1.5, PSS, OAEP	PKCS#1 v1.5, PSS, OAEP	PKCS#1 v1.5, PSS, OAEP **Note 4**	RAW, PKCS#1 v1.5, PSS, OAEP **Note 3 & 6**	PKCS#1 v1.5, PSS, OAEP
ECC Key sizes	256-bit - default 384-bit 521-bit **Note 2**	256-bit - default 384-bit 521-bit **Note 2**	256-bit 384-bit 521-bit	256-bit 384-bit 521-bit	256-bit 384-bit	256-bit - default 384-bit
Hash	SHA-1 160-bit SHA-2 256-bit, 384-bit, 512-bit	SHA-1 160-bit SHA-2 256-bit, 384-bit, 512-bit	SHA-1 160-bit SHA-2 256-bit, 384-bit, 512-bit **Note 3**	SHA-1 160-bit SHA-2 256-bit, 384-bit, 512-bit **Note 3**	SHA-1 160-bit SHA-2 256-bit, 384-bit, 512-bit **Note 3**	SHA-1 160-bit SHA-2 256-bit, 384-bit, 512-bit MD5
Activation PIN	N/A	Available	N/A	Available	N/A	N/A

Features:	Device:					
Re-init feature	N/A	N/A	N/A	Available	Available	Available and can be used via sample code in SDK. For details, refer to *SafeNet Authentication Client DeveloperGuide*.
SKI	N/A	N/A	Available	Available	N/A	N/A
Non-managed profile	N/A	N/A	N/A	Available	Available	N/A

NOTE
1. The default number of containers and default container capabilities can be customized during the PERSO process.
2. The supported key sizes depend on the PERSO container customizations.
3. SHA-1 (160-bit) and RSA 1024-bit are not allowed in FIPS L3 cards.
4. PKCS#1 padding does not allow decrypt on IDPrime 930\3930 FIPS L3 cards.
5. Keys can be created as long as free memory is available.
6. Raw RSA is not available on FIPS devices. The RAW RSA (AKA CKM_RSA_X_509) mechanism for both Sign and Decrypt operations is blocked in all IDPrime devices (including old IDPrime MD devices).
7: RSA 3072 and 4096-bit only key import available (no OBKG).
8. IDPrime PIV 3.0 cards support import and generation of keys in all the containers while IDPrime PIV cards and tokens support import of keys to all the containers and key generation in three containers only, which are PIV Authentication, Key Management, and Digital Signature.

NOTE For IDPrime PIV cards and tokens, the minimum RSA key size supported is 2048 and the maximum supported key size is 4096. While for IDPrime PIV 3.0 cards, the minimum and maximum key size supported are 1024 and 2048 respectively.

PIN Pad Readers

Following PIN Pad readers are supported:

Supported Reader Name	Firmware Version	IDPrime MD 830-FIPS IDPrime MD 830 B (L2) IDPrime MD 840 IDPrime MD 840 B SafeNet IDPrime 940/3940	IDPrime MD 830 B - FIPS L3
Ezio Shield Pro	GTO K6.14.00	SM Protected operations are not supported*,**	Not supported
Ezio Shield Pro	UKP K6.14.05	SM Protected operations are not supported	Not supported
Ezio Bluetooth Reader	GTO O7.04.05	Fully Supported**	Not supported
Ezio Bluetooth Reader	PKI P1.01.10	Fully Supported**	Not supported
Ezio Bluetooth Reader	PKI SWYS	Fully Supported**	Not supported
Gemalto IDBridge CT710	CT7xBarclays JA S1141693 18L13 05	Fully Supported**	Not supported
Gemalto IDBridge CT700	SWP113162F	Fully Supported**	Not supported

* Secure Messaging (SM) protected operations includes import key pair, generate key pair and change administrator key.

** Cards configured with PIN/s protected by SM are not supported by any PIN Pad reader.

> **NOTE** EZIO PKI cards (applet version 4.3.6) that have the ‘Enforce PIN Pad firewall’ feature enabled and are compatible with PIN Pad readers must have the FW version in the table above (or higher).
> Transparent readers (For the full list of transparent readers, refer to "Product Description" on page 2).

PIN Pad readers have different firewalls and therefore, different functional behavior. It is recommended that the reader specification document is reviewed before using the PIN Pad reader.

> **NOTE** The Secure PIN Pad readers listed above are subject to limitations. Certain readers may not fully support all Smart cards. For details of supported Smart card and PIN Pad reader combinations, refer to the *SafeNet Authentication Client Administrator Guide*.

Compatibility with Third-Party and Native Applications

Following third-party applications have been validated and tested with this release:

Solution Type	Vendor	Product Version
VPN	Pulse Secure	9.1 R2**
	Cisco AnyConnect	4.8.00175**
	Check Point	E80.61**
Access Management	Centrify	5.5.1**
Virtual Desktop Infrastructure (VDI)	*Citrix	XenApp/XenDesktop 7.18**
	VMware Horizon Client	5.1.0*
Digital Signatures	Adobe	Acrobat Reader 2024.005.20320
	Apple	Mail app 16.0
	Mozilla	Thunderbird 115.10.1
	SETCCE proXSign	2.1.4.31**

* Citrix receiver app 12.9.1 for Mac is not supported on Catalina. Instead, there is a new app called Citrix Software app v19.12.0.23 that is supported on MacOS Catalina

** Validated with SAC on Mac 10.2

Installation

SafeNet Authentication Client must be installed on each computer on which IDPrime 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.

Upgrade

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

After upgrading from SAC 10.8 R2 to SAC 10.9 (GA) on a Mac, it is recommended that you restart the machine in order to recognize the device.

Resolved and Known Issues

Issue Severity and Classification

This section lists the issues that have been resolved and known to exist in this release. The following table defines the severity of the issues listed in this section.

Severity	Classification	Definition
C	Critical	No reasonable workaround exists
H	High	Reasonable workaround exists
M	Medium	Medium-level priority problems
L	Low	Low-level priority problems

Resolved Issues

Issue	Severity	Synopsis
ASAC-19560	H	Unable to use the User certificates on Mac for SafeNet eToken 5110.
ASAC-17281	H	Signing is stuck in an endless loop after entering correct PIN on Mac while using SafeNet IDPrime 940 card.
ASAC-16432	M	In case of IDPrime CC cards, the following tokenFlags gives incorrect information for the `GetTokenFlags` command: > `CKF_SO_PIN_COUNT_LOW` > `CKF_SO_PIN_FINAL_TRY` > `CKF_SO_PIN_LOCKED`. (Customer ID: CS1477498)
ASAC-19313	H	Unable to configure the Maximum usage period (days) and Expiration warning period (days) parameters present in the Client Settings over the Token Settings of the IDPrime cards in the SAC Tools. (Customer ID: CS1552243 ; CS1577753)
ASAC-18193	M	Error in documentation regarding certificate expiry alert. (Customer ID: CS1519652)

Known Issues

Issue	Severity	Synopsis
ASAC-20126	M	**Summary:** The Generate Key operation fails in case of RSA keys on the SafeNet eToken Fusion S2 NFC PIV. **Workaround:** None
ASAC-20641	M	**Summary:** Unable to load the library `libeToken.dylib` in the Thunderbird browser on Mac. **Workaround:** Use Apple native mail.
ASAC-20462	M	**Summary:** The Gemalto IDBridge CT710 Pin Pad reader is not working for TLS operations on Chrome browser and while performing Adobe signing on MAC. **Workaround:** None
ASAC-4974	L	**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-15109	L	**Summary:** Free space is constant in SAC Tools for the legacy SafeNet eToken 5110 while importing or deleting the certificates. **Workaround:** None
ASAC-14152	L	**Summary:** Negative free space is updated in the SAC Tools if large objects are added to the card. **Workaround:** None
ASAC-16217	L	**Summary:** After inserting SafeNet IDPrime 940 SIS, the *Unlock Token* icon is not visible in the Advanced view for all other tokens. **Workaround:**Close and reopen the SAC Tools.
ASAC-15929	M	**Summary:** Kerberos login fails, after at least ONE use of CC certificate for signature **Workaround:** Disconnect the token/card and reconnect it again.
ASAC-11163	H	**Summary:** After locking the Administrator Key (due to an incorrect password being entered too many times), the IDPrime 940/3940 smart card switches to a locked state and as a result the device cannot be used (device is unrecognized). **Workaround:** None – this is a smart card design feature.
ASAC-8338	M	**Summary:** TLS and Web Signer operations could not be performed when logging in with an IDClassic 340 (V3) password length that's less than 8 on a CT710 or SWAT PIN Pad reader. **Workaround:** Define the PQMinLen = 6 in SAC PQ default settings.
ASAC-2849	M	**Summary:** Enrolling a certificate on Mac via Check Point VPN E80.61 failed. **Workaround:** Use an enrolled certificate when connecting to VPN via Check Point.

Issue	Severity	Synopsis
ASAC-2235	M	**Summary:** After installing SAC, the PKCS11 module was not inserted automatically into Firefox’s browser. **Workaround:** Insert the module manually.
ASAC-2227	M	**Summary:** When two tokens are connected, one of the token’s settings are not accessible in SAC Tools. **Workaround:** Work with one connected token at a time.
ASAC-11099	M	**Summary:** Using the salt length in the PSS parameter that is not equal to the hash length of the appropriate PSS mechanism, causes the C_Verify() command to fail with the CKR_ SIGNATURE_INVALID return value. Effected environment: All IDPrime based devices and any of the following mechanisms: CKM_SHA1_RSA_PKCS_PSS, CKM_SHA256_RSA_PKCS_PSS, CKM_SHA384_RSA_PKCS_PSS and CKM_ SHA512_RSA_PKCS_PSS. **Workaround:** On IDPrime based devices, use the PSS parameters with the salt length equal to the hash length.
ASAC-9288	M	**Summary:** By default, the retry counter cache causes the following problem in SAC: when switching the card between different machines, the true retry counter is not shown until it is changed on the current machine and the cache is updated. **Workaround:** Add the property RetryCountCached=0 under the [General] section in the file `/etc/eToken.conf.`
ASAC-8267	M	**Summary:** A Digital Signature PIN operation fails if the Digital Signature PIN (Role#3) and Digital Signature PUK (Role#4) have different PINPad configurations (PIN Type and Extended PIN Flags) **Workaround:** Ensure that the Digital Signature PIN (Role#3) and Digital Signature PUK (Role#4) have the same PINPad configuration.
ASAC-7969	M	**Summary:** Using the eToken Pro (no hash on-board functionality) and eToken 5110 FIPS (both hash and sign functionalities on-board) device when there are two or more threads running two PKCS#11 sessions in the same application, the signing operation fails. **Workaround:** Peform either one of the following: > Update the application to use the hash off-board mechanism and then perform the RSA operation with the token. > Update the application to synchronize between threads - make the `C_SignInit - C_ SignUpdate - C_SignFinal` a solid block. > If there is no option to update the application, enable the hash offboard property: *HashOffboard* in SAC. This allows SAC PKCS#11 to perform the hash off-board instead of the token.
ASAC-7932	M	**Summary:** Changing the PIN on Firefox using the CT710 PIN Pad does not work. **Workaround:** Change the PIN using SAC Tools or SAC tray icon.

Issue	Severity	Synopsis
ASAC-6214	M	**Summary:** VMView client may not work properly with SAC when using a smart card certificate. **Workaround:** Install SAC before installing the VMView Client.
ASAC-5815	M	**Summary:** When working with a token or a PIN pad reader on a VM Workstation, the token might be unrecognized when selecting the "Shared" device in VM > Removable Devices menu. **Workaround:** Connect the device that is not under the "Shared" devices list in order to work with the eToken/reader device.
ASAC-5343	M	**Summary:** When using a PIN Pad reader with the Smart Card initialized with the ‘Must change password’ flag enabled, and the password is changed on the same machine, the user may encounter an issue and receive an "Incorrect password" message. The issue will not occur if the card is initialized on one machine and the password is changed on another. **Workaround:** Delete the cache folder (/var/tmp/eToken.cache) after initialization and before changing the password.
ASAC-2653	M	**Summary:** When working with a token on VM Workstation, the token might be unrecognized when selecting the "Shared" device in VM > Removable Devices menu. **Workaround:** Connect the device that is not under the "Shared" devices list in order to work with the eToken device.
ASAC-4497	M	**Summary:** When Configuring the Maximum Password Usage value to a value other than zero (0), the password will expire a day later than was defined. For example: set it to 166 days, SAC will show 167 days. **Workaround:** None.
ASAC-4141	M	**Summary:** During the unblock operation, no other application can access the device until the unblock operation is finished or canceled. **Workaround:** None.
ASAC-4024	M	**Summary:** When unlocking a Common Criteria device (that’s in linked mode) via SAC Tools and an incorrect Challenge Response is sent, a general error message is received. **Workaround:** None.
ASAC-11149	M	**Summary:** VPN fails using IDPrime 930 L3 (with KSP SHA2 certificate) cards. **Workaround:** None.
ASAC-5306	M	**Summary:** When trying to log onto a locked device, two messages are shown instead of one. **Workaround:** Close both windows.

Issue	Severity	Synopsis
ASAC-4116	M	**Summary:** When entering an incorrect Digital Signature PIN while enrolling a CC Certificate onto a CC device in unlinked mode, the enrollment process fails. **Workaround:** Retry enrolling the certificate with the correct Digital Signature PIN.
ASAC-13343	L	**Summary:** SAC binaries and packages need to be signed from Thales Apple Certificate. **Workaround:** None -no impact on SAC functionality.
ASAC-4974	L	**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.

Known Limitations

Below is the list of known limitations that exist in this release:

- Thales PKI PIN Pad (Thales Shield M4 Reader) and Gemalto SWYS Pin Pad readers are not working with Mac.
- When multiple cards/tokens are present in a reader, the behavior of CTK is unpredictable.
- When P12 file has more certificates than available in the containers, "The Key container missing" message is shown.
- MacOS Kerberos SSO Extension selects wrong certificate automatically.
- Smart Card login with CryptoTokenKit (CTK) does not support PIN Pad readers. (Apple Bug ID: 34655464)
- When working with multiple PIN’s on a card (using Safari and Chrome), the login dialog displays a general PIN prompt instead of specifying the type of PIN to be entered. This is a Crypto Token Kit (CTK) framework limitation present on High Sierra and Mojave. Apple Bug ID: 34620675).
- The PIN Validity period cannot be set on IDPrime 830 Rev A cards. It is not supported by SAC if not configured already in production.
- After connecting and using an IDPrime 3811 device (on a contactless reader) the smart card was not recognized (loss of identification).
- The profile whereby a PUK replaces the Admin Key does not support initializing a device.
- IDPrime MD 840 and eToken 5110 CC do not support history size of Password Quality.
- IDPrime MD 830B (applet 4.3.5) FIPS L3 does not support RSA 1024, ECC signing with SHA1 algorithms, as per FIPS/NIST regulations.
- As of SAC 10.2, Symmetric keys created using PKCS#11 without the attributes: CKA_ SENSITIVE = TRUE and CKA_EXTRACTABLE = FALSE, on an eToken Java device initialized in FIPS/CC mode will face backward compatibility issues on previous SAC versions.
- SafeNet eToken 5110 FIPS does not support RSA 1024 and SHA1 on board, as per FIPS/NIST regulations.
- IDPrime smart cards cannot sign plain data longer than 36 bytes for RSA or ECC keys.
- On IDPrime MD cards, only CA private certificate objects are supported.
- The following PIN pad limitations exist:

- IDPrime MD 840 and IDPrime MD 3840 cards ignore the “Token password must be changed on first logon” parameter when working with the PIN pad reader.
- Performing a “Change PIN” operation via PKCS#11 (C_SetPIN) requires the PIN to be entered again at the end of the process.
- Single Sign On is not supported with PIN Pad readers.

Product Documentation

The following product documentation is associated with this release:

- SafeNet Authentication Client User Guide
- SafeNet Authentication Client Administrator Guide

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 refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Thales Customer Support.

Thales 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 Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone

The support portal also lists telephone numbers for voice contact (Contact Us).

Email Support

You can also contact technical support by email at technical.support.DIS@thalesgroup.com.