

# SafeNet Authentication Client 10.9

## (GA)

### LINUX RELEASE NOTES

**Issue Date:** December 2024

**Build:** RPM 4723 / DEB 4723

**Document Part Number:** 007-013841-005 Rev. A

#### Contents

|   |           |
|---|-----------|
| <b>Product Description</b>                  | <b>2</b>  |
| Release Description                         | 2         |
| New Features and Enhancements               | 2         |
| Advisory Notes                              | 2         |
| Licensing                                   | 3         |
| Localization                                | 3         |
| Default Password                            | 4         |
| Password Recommendations                    | 5         |
| Initialization Key Recommendation           | 5         |
| Compatibility Information                   | 5         |
| Browsers                                    | 5         |
| Operating Systems                           | 6         |
| Tokens                                      | 6         |
| Software Tokens                             | 6         |
| Device Features Supported by SAC            | 9         |
| Compatibility with Third-Party Applications | 11        |
| Installation                                | 12        |
| Upgrade                                     | 12        |
| <b>Resolved and Known Issues</b>            | <b>13</b> |
| Issue Severity and Classification           | 13        |
| Resolved Issues                             | 13        |
| Known Issues                                | 14        |
| Known Limitations                           | 18        |
| <b>Product Documentation</b>                | <b>20</b> |
| <b>Support Contacts</b>                     | <b>21</b> |

# 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) Linux includes new features and bug fixes from previous SAC versions.

## New Features and Enhancements

This release offers the following:

- > Support for Debian 12.8 OS.
- > 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 6](#).
- > Improvement done in the conversion of unmanaged card to managed card.
- > External PIN PAD reader support for IDPrime SIS 840, IDPrime 940 SIS and IDClassic 410 cards.
- > Reintroduced *Enforce FIPS* settings in SAC, which enables the ability to initialize eToken 5110+ with or without FIPS.
- > Security improvements.
- > Fixes from previous release. Refer to "Resolved Issues" on page 15.

## Advisory Notes

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

- > Legacy End-of-Life devices (eToken Virtual (ETV) and CardOS) are no longer supported with SAC 10.9 (GA) Linux.
- > SAC 10.9 (GA) Linux is compatible with all current Linux distributions, including OpenSSL 1.0 or above.
- > If the Security-Enhanced Linux (SELinux) is enabled, the policy module must be updated to enable smart card logon.
- > Support and deliverable for 32-bit OS have been removed from SAC 10.9 (GA) onwards.
- > In Ubuntu 22.04, the token driver stops working after the machine is rebooted. To fix this issue, execute the following command, and then reboot the machine:

```
sudo systemctl enable pcsd.socket
```

- > 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.
- > Install the CCID driver version 1.5.1 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
- > 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.
- > SAC does not support RSA 1024 key size signing with SHA-1. If you need it, use the Disable-Crypto setting mentioned in the *SafeNet Authentication Client Administrator Guide*.
- > 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.

## Licensing

---

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

## Localization

---

This release support the following languages:

- > Bulgarian
- > Chinese (Simplified)
- > Chinese (Traditional)
- > Croatian
- > Czech
- > English
- > French (Canadian)

- > French (European)
- > German
- > Hungarian
- > Italian
- > Japanese
- > Korean
- > Lithuanian
- > Polish
- > Portuguese (Brazilian)
- > Romanian
- > Russian
- > Serbian
- > Slovakian
- > Slovenian
- > Spanish
- > Swedish
- > Thai
- > Turkish
- > Vietnamese

**NOTE**

- The user PIN and Admin PIN can be in English only, while using IDPrime MD, eToken 5300, and eToken 5110 CC.
- IDPrime features are available only in English localization, such as Initializing Common Criteria devices and PIN Pad functionality.
- IDPrime PIV cards and tokens support English language only.

## 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 and tokens:**

- > 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, IDPrime SIS 840, IDPrime 940 SIS, and IDClassic 410 cards.

- > 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 'Security Recommendations' chapter in *SafeNet Authentication Client Administrator Guide*.

## Initialization Key Recommendation

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
- > Chrome

**NOTE** Thales recommends that you download the browser versions mentioned in ["Compatibility with Third-Party Applications" on page 11](#).

## Operating Systems

Following operating systems are supported:

- > Red Hat 8.10 and 9.4
- > CentOS 9
- > Fedora 41
- > Debian 12.8
- > Ubuntu 22.04 and 24.04.1

## Tokens

Following tokens are supported:

### Certificate-based USB Tokens

- > SafeNet eToken 5300 USB A
- > SafeNet eToken 5300 USB A TS
- > SafeNet eToken 5300-C TS
- > SafeNet eToken 5110 CC (940)
- > SafeNet eToken 5110+ CC (940C)
- > SafeNet eToken Fusion CC
- > SafeNet eToken 5110+
- > SafeNet eToken Fusion
- > SafeNet eToken Fusion S2 NFC PIV
- > SafeNet eToken Fusion FIPS
- > SafeNet eToken 5110
- > SafeNet eToken 5110 CC
- > SafeNet eToken 5110 FIPS
- > SafeNet eToken 5300 C
- > SafeNet eToken 5110+ FIPS
- > SafeNet eToken 5110+ CC (940B)

## Software Tokens

- > SafeNet IDPrime Virtual Smart Card

## Smart Cards

- > SafeNet IDPrime PIV 3.0
- > SafeNet IDPrime PIV 4.0
- > SafeNet IDPrime MD 830nc
- > SafeNet IDPrime SIS 840
- > SafeNet IDPrime 940 SIS
- > SafeNet IDClassic 410
- > 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 930
- > SafeNet IDPrime 3930
- > SafeNet IDPrime 930nc
- > SafeNet IDPrime 3930 FIDO
- > SafeNet IDPrime 930 FIDO

### 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** 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.

**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 the *IDPrime MD Configuration Guide*.

## Smart Cards and Tokens that Support Common Criteria

- > Gemalto IDPrime MD 840
- > Gemalto IDPrime MD 840 B

- > Gemalto IDPrime MD 3840
- > Gemalto IDPrime MD 3840 B
- > Gemalto IDPrime MD 8840 Micro SD Card
- > Gemalto IDPrime MD 940
- > SafeNet eToken Fusion
- > SafeNet eToken Fusion CC
- > SafeNet eToken 5110 CC
- > SafeNet eToken 5110 CC (940)
- > SafeNet eToken 5110+CC (940C)
- > SafeNet eToken 5110+ CC (940B)
- > SafeNet IDPrime 940
- > Safenet IDPrime 940B
- > Safenet IDPrime 940C
- > SafeNet IDPrime 3940
- > SafeNet IDPrime 3940C
- > SafeNet IDPrime 940B FIDO

### External Smart Card Readers

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

**NOTE** It is recommended to use Vendor drivers for the above SC Readers.

### Secure PIN Pad Readers

- > Gemalto IDBridge CT700
- > Gemalto IDBridge CT710
- > Gemalto SWYS
- > Thales PKI PIN Pad (Thales Shield M4 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*. PIN Pad readers do not support SafeNet IDClassic 410 and SafeNet IDPrime SIS 840 cards.

## Device Features Supported by SAC

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

| Features                 | Devices   |  |  |  |                                       |  |
|--------------------------|---|--|--|--|---------------------------------------|--|
|                          | Gemalto IDPrime MD 840/3840/3840 B/ 8840/SafeNet eToken 5110 CC                 | SafeNet IDPrime 940  | Gemalto IDPrime MD 830- FIPS/830- ICP/830B/3810/381 0 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<br><b>Note 1</b>   | 20 – default<br><b>Note 1</b>                                      | 15   | 32   | Dynamic<br><b>Note 5</b>              | 23 (20 Retired, PIV Authentication, Digital Signature and Key Management)<br><b>Note 8</b>   |
| RSA Key sizes            | 2048-bit - default<br>3072-bit 4096-bit<br>4096-bit<br><b>Note 2 and Note 7</b> | 2048-bit - default<br>3072-bit 4096-bit - default<br><b>Note 2</b> | 1024-bit<br>2048-bit<br><b>Note 3</b>  | 2048-bit<br>3072-bit 4096-bit<br><b>Note 3</b> | 1024-bit<br>2048-bit<br><b>Note 3</b> | For IDPrime PIV 3.0 :<br>> 1024-bit<br>> 1280-bit<br>> 1536-bit<br>> 2048-bit<br><br>For IDPrime PIV 4.0/eToken Fusion S2 NFC PIV:<br>> 2048-bit<br>> 3072-bit<br>> 4096-bit |

| Features            | Devices   |   |  |   |   |   |
|---------------------|---|---|--|---|---|---|
| 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<br><br><b>Note 4</b>                           | RAW, PKCS#1 v1.5, PSS, OAEP<br><br><b>Note 3 and Note 6</b>           | PKCS#1 v1.5, PSS, OAEP  |
| ECC Key sizes       | 256-bit - default<br>384-bit 521-bit<br><br><b>Note 2</b> | 256-bit - default<br>384-bit 521-bit<br><br><b>Note 2</b> | 256-bit 384-bit 521-bit  | 256-bit<br>384-bit 521-bit  | 256-bit<br>384-bit  | 256-bit - default<br>384-bit  |
| Hash                | SHA-1 160-bit<br>SHA-2 256-bit, 384-bit, 512-bit          | SHA-1 160-bit<br>SHA-2 256-bit, 384-bit, 512-bit          | SHA-1 160-bit SHA-2 256-bit, 384-bit, 512-bit<br><br><b>Note 3</b> | SHA-1 160-bit<br>SHA-2 256-bit, 384-bit, 512-bit<br><br><b>Note 3</b> | SHA-1 160-bit<br>SHA-2 256-bit, 384-bit, 512-bit<br><br><b>Note 3</b> | SHA-1 160-bit<br>SHA-2 256-bit, 384-bit, 512-bit<br>MD5   |
| Activation PIN      | N/A   | Available   | N/A  | Available   | N/A   | N/A   |
| 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 <i>SafeNet Authentication Client DeveloperGuide</i> . |
| 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 is 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-bit 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.

## Compatibility with Third-Party Applications

Following third-party applications are supported:

| Solution Type                        | Vendor      | Product Version  |         |
|--------------------------------------|-------------|--|---------|
| Virtual Desktop Infrastructure (VDI) | Citrix      | Virtual Apps and Desktops 7.2206 (Formerly XenDesktop) |         |
| VMware View                          | Horizon 7.8 | VMware View*   |         |
| Digital Signatures                   | Mozilla     | Thunderbird on OS                                      | Version |
|                                      |             | Ubuntu 22.04/CentOS 9                                  | 128.3.1 |
|                                      |             | RHEL 9.4/Ubuntu 24.04.1/Fedora 41                      | 128.4   |
|                                      |             | RHEL 8.10  | 128.4.0 |

| Solution Type | Vendor  | Product Version             |                |
|---------------|---------|-----------------------------|----------------|
|               |         | Firefox on OS               | Version        |
| Browsers      | Mozilla | Ubuntu--22.04, 24.04.1      | 115.9.1        |
|               |         | RHEL 9.4/CentOS 9/Fedora 41 | 133.0          |
|               |         | RHEL 8.10                   | 102.4.0esr     |
|               |         |                             |                |
|               | Google  | Chrome on OS                | Version        |
|               |         | Ubuntu-22.04, 24.04.1       | 130.0.6723.116 |
|               |         | RHEL 9.4/CentOS 9/Fedora 41 | 130.0.6723.116 |
|               |         | RHEL 8.10                   | 131.0.6778.85  |

\* Validated on SAC on Linux 10.7

## 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 (LA) to SAC 10.9 (GA), it is recommended to restart the system.

# 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-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.<br><br>(Customer ID: CS1552243 ; CS1577753) |
| ASAC-18193 | M        | Error in documentation regarding certificate expiry alert.<br><br>(Customer ID: CS1519652)  |
| 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 .<br><br>(Customer ID: CS1477498)                          |

## Known Issues

| Issue       | Severity | Synopsis   |
|-------------|----------|--|
| ASA C-20115 | M        | <b>Summary:</b> The "Finish" button is enabled at times in the <i>Initialize Token - IDPrime PIV PUK</i> window when the PUK is entered less than the minimum length.<br><b>Workaround:</b> None |
| ASA C-20126 | M        | <b>Summary:</b> The Generate Key operation fails in case of RSA keys on the SafeNet eToken Fusion S2 NFC PIV.<br><b>Workaround:</b> None   |
| ASA C-13003 | M        | <b>Summary:</b> On Red Hat 8.1, the TLS operations fails on the first attempt while using RSA 2048 for Sign Only certificate via PKCS#11.<br><b>Workaround:</b> None                             |
| ASA C-15190 | M        | <b>Summary:</b> Token name is missing from the notification pop up of <i>Change Digital Signature PUK</i> and <i>Change Digital Signature PIN</i> operations.<br><b>Workaround:</b> None         |
| ASA C-15319 | L        | <b>Summary:</b> Free space is constant in SAC Tools for the legacy SafeNet eToken 5110.<br><b>Workaround:</b> None   |
| ASA C-15318 | M        | <b>Summary:</b> The <i>Card type</i> shows unknown in SAC Tools for the legacy SafeNet eToken 5110.<br><b>Workaround:</b> None   |
| ASA C-20340 | L        | <b>Summary:</b> An unclear text is displayed in the <i>Initialize Token -Password Settings</i> window on Fedora 41.<br><b>Workaround:</b> None   |
| ASA C-20137 | L        | <b>Summary:</b> In SAC Tools, the alignment of "Advanced" window in the <i>Token's Settings</i> is not proper.<br><b>Workaround:</b> None  |

| Issue       | Severity | Synopsis   |
|-------------|----------|--|
| ASA C-18707 | M        | <p><b>Summary:</b> An incorrect message is displayed when the PIN Pad reader timeouts while performing <i>Change Administrator Password</i> operation.</p> <p><b>Workaround:</b> None</p>  |
| ASA C-20138 | M        | <p><b>Summary:</b> If multiple readers are connected to the system, a pop-up appears after the Save Configuration Setting during uninstallation.</p> <p><b>Workaround:</b> Remove extra reader from the system.</p>  |
| ASA C-20288 | M        | <p><b>Summary:</b> IDPrime PIV card/token is getting disconnected after performing TLS.</p> <p><b>Workaround:</b> Close and reopen the SAC Tools.</p>  |
| ASA C-20140 | L        | <p><b>Summary:</b> Getting two set of IDPrime PIV registries in the registry editor under Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards, when a standard SAC msi is installed in the Custom mode.</p> <p><b>Workaround:</b> None</p> |
| ASA C-20141 | L        | <p><b>Summary:</b> An incorrect warning message is displayed while importing a certificate in the Card Authentication container of the IDPrime PIV cards and tokens.</p> <p><b>Workaround:</b> None</p>  |
| ASA C-19637 | M        | <p><b>Summary:</b> Unable to detect SafeNet IDClassic 410 card on Gemalto SWYS and Thales PKI PIN Pad (Thales Shield M4 Reader) PIN Pad readers.</p> <p><b>Workaround:</b> None</p>  |
| ASA C-17930 | M        | <p><b>Summary:</b> The <i>Set Token Password</i> and <i>Set Digital Signature PIN</i> options failing on IDPrime SIS 840 and IDClassic 410 cards when working on IDBridge CT700 PIN Pad reader with SAC Tools.</p> <p><b>Workaround:</b> None</p>                    |
| ASA C-14425 | L        | <p><b>Summary:</b> Mozilla Thunderbird stops working if a smart card is swapped while performing the send email operation.</p> <p><b>Workaround:</b> Relaunch Thunderbird and perform the operation with a valid smart card.</p>                                     |

| Issue                    | Severity | Synopsis   |
|--------------------------|----------|--|
| ASA C-9244               | H        | <p><b>Summary:</b> When the <i>Must change password</i> flag is set and the password is changed using a Pin Pad reader through the SAC Monitor, the balloon notification appears for only a second.</p> <p><b>Workaround:</b> To disable the balloon notification, add the property <i>PinPadNotify=2</i> under the <i>General</i> section of the configuration file <code>/etc/eToken.conf</code>.</p>  |
| ASA C-9288<br>ASA C-9281 | M        | <p><b>Summary:</b> By default, the retry counter is cached causing 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.</p> <p><b>Workaround:</b> Add the property <i>RetryCountCached=0</i> under the <i>General</i> section of the configuration file <code>/etc/eToken.conf</code>.</p>   |
| ASA C-9108<br>ASA C-6191 | H<br>M   | <p><b>Summary:</b> Sign operations using IDPrime MD smart cards with PKCS#1 v1.5 padding with hash mechanisms SHA256, SHA384 and SHA512 require input data to be prefix with the hash object identifier (OID). The use of SHA1 does not require this prefix.</p> <p><b>Workaround:</b> Ensure the following OID's are prefixed to the hash of data to be signed:</p> <pre>SHA_256_HEADER [] = {0x30,0x31,0x30,0x0D,0x06,0x09,0x60,0x86,0x48,0x01,0x65,0x03,0x04,0x 02,0x01,0x05,0x00,0x04,0x20}; SHA_384_HEADER [] = {0x30,0x41,0x30,0x0D,0x06,0x09,0x60,0x86,0x48,0x01,0x65,0x03,0x04,0x 02,0x02,0x05,0x00,0x04,0x30}; SHA_512_HEADER [] = {0x30,0x51,0x30,0x0D,0x06,0x09,0x60,0x86,0x48,0x01,0x65,0x03,0x04,0x 02,0x03,0x05,0x00,0x04,0x40};</pre> |
| ASA C-1109<br>9          | M        | <p><b>Summary:</b> Using the salt length in the PSS parameter that is not equal to the hash length of the appropriate PSS mechanism, causes the <code>C_Verify()</code> command to fail with the <code>CKR_SIGNATURE_INVALID</code> return value. Effected environment: All IDPrime based devices and any of the following mechanisms: <code>CKM_SHA1_RSA_PKCS_PSS</code>, <code>CKM_SHA256_RSA_PKCS_PSS</code>, <code>CKM_SHA384_RSA_PKCS_PSS</code> and <code>CKM_SHA512_RSA_PKCS_PSS</code>.</p> <p><b>Workaround:</b> On IDPrime based devices, use the PSS parameters with the salt length equal to the hash length.</p>  |
| ASA C-8267               | M        | <p><b>Summary:</b> 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)</p> <p><b>Workaround:</b> Ensure that the Digital Signature PIN (Role#3) and Digital Signature PUK (Role#4) have the same PINPad configuration.</p>   |



| Issue      | Severity | Synopsis  |
|------------|----------|---|
| ASA C-7969 | M        | <p><b>Summary:</b> 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.</p> <p><b>Workaround:</b> Perform either one of the following:</p> <ul style="list-style-type: none"> <li>&gt; Update the application to use the hash off-board mechanism and then perform the RSA operation with the token.</li> <li>&gt; Update the application to synchronize between threads - make the <code>C_SignInit - C_SignUpdate - C_SignFinal</code> a solid block.</li> <li>&gt; If there is no option to update the application, enable the hash offboard property: <i>HashOffboard</i> in SAC. This allows SAC PKCS#11 to perform the hash off-board instead of the token.</li> </ul> |
| ASA C-7932 | M        | <p><b>Summary:</b> Changing the PIN on Firefox using the CT710 PIN Pad does not work.</p> <p><b>Workaround:</b> Change the PIN using SAC Tools or SAC tray icon.</p>  |
| ASA C-6214 | M        | <p><b>Summary:</b> VMView client may not work properly with SAC when using a smart card certificate.</p> <p><b>Workaround:</b> Install SAC before installing the VMView Client.</p>   |
| ASA C-5815 | M        | <p><b>Summary:</b> 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 &gt; Removable Devices menu.</p> <p><b>Workaround:</b> Connect the device that is not under the "Shared" devices list in order to work with the eToken/reader device.</p>  |
| ASA C-5343 | M        | <p><b>Summary:</b> 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.</p> <p><b>Workaround:</b> Delete the cache folder (C:\Windows\Temp\Token.cache) after initialization and before changing the password.</p>  |
| ASA C-2653 | M        | <p><b>Summary:</b> When working with a token on VM Workstation, the token might be unrecognized when selecting the "Shared" device in VM &gt; Removable Devices menu.</p> <p><b>Workaround:</b> Connect the device that is not under the "Shared" devices list in order to work with the eToken device.</p>   |
| ASA C-4497 | M        | <p><b>Summary:</b> 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.</p> <p><b>Workaround:</b> None.</p>  |

| Issue      | Severity | Synopsis  |
|------------|----------|---|
| ASA C-4141 | M        | <b>Summary:</b> During the unblock operation, no other application can access the device until the unblock operation is finished or canceled.<br><b>Workaround:</b> None.   |
| ASA C-4024 | M        | <b>Summary:</b> 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.<br><b>Workaround:</b> None.   |
| ASA C-5306 | M        | <b>Summary:</b> When trying to log onto a locked device, two messages are shown instead of one.<br><b>Workaround:</b> Close both windows.   |
| ASA C-4116 | M        | <b>Summary:</b> When entering an incorrect Digital Signature PIN while enrolling a CC Certificate onto a CC device in unlinked mode, the enrollment process fails.<br><b>Workaround:</b> Retry enrolling the certificate with the correct Digital Signature PIN.                                |
| ASA C-4974 | L        | <b>Summary:</b> 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.<br><b>Workaround:</b> The user must log out before making Password Quality modifications. |

## Known Limitations

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

- > When working in a VDI environment, you need to configure the `CacheMarkerTimeout` property on the host machine under the *General* section: `CacheMarkerTimeout=1`  
For more details, refer to *SafeNet Authentication Client Administrator Guide*.
- > When performing the TLS operation on Chrome browser, the login is required using both keyboard and PIN Pad reader. On the login pop-up, a correct or incorrect PIN can be entered but should not be left blank via keyboard. Later on, a correct PIN is required by using PIN Pad reader to proceed further.
- > The appropriate messages are not displayed on the Thales PKI PIN Pad (Thales Shield M4 Reader) while performing change PIN operations.
- > All screens in the SAC Tools display the "Current Language: EN" in Swedish and Bulgarian languages MSI.
- > 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 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).
- > 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.
- > 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.
- > 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.
- > Free space is not updating in SAC Tool for SIS Card's : 840 and 410.
- > Interoperability - Imported p12 file using NetID pkcs11 , is not visible in Find all objects when we use sac pkcs11.

# 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](mailto:technical.support.DIS@thalesgroup.com).