

# SafeNet Authentication Client 10.9 R1 (GA)

## LINUX RELEASE NOTES

**Issue Date:** December 2025

**Build:** RPM 6747 / DEB 6747

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

---

### 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	7
Device Features Supported by SAC	9
Compatibility with Third-Party Applications	12
Installation	13
Upgrade	13
<b>Resolved and Known Issues</b>	<b>14</b>
Issue Severity and Classification	14
Resolved Issues	14
Known Issues	15
Known Limitations	18
<b>Product Documentation</b>	<b>19</b>
<b>Support Contacts</b>	<b>20</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 R1 (GA) Linux includes new features, enhancements, and bug fixes from previous SAC versions.

## New Features and Enhancements

---

This release offers the following:

- > Introduced support for key generation on 9E container, making a total of 24 active containers ( 3 exchange + 1 sign only + 20 retired).
- > Support for contactless mode for IDPrime PIV cards and tokens, and IDPrime tokens.
- > NFC support for PIV and IDPrime tokens.
- > Support for IDPrime 930C/3930C new devices .
- > Enhancements in PKCS#11 for device information.
- > 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 R1 (GA) Linux.
- > SAC 10.9 R1 (GA) Linux is compatible with all current Linux distributions, including OpenSSL 3.0.
- > 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 R1 (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 930/3930:
  - 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*.
- > 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 latest CCID driver to work with the supported devices.
- > 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

**For SafeNet eToken devices:**

- > The default token password is "1234567890"

**For IDPrime cards:**

- > The default token password is "0000" (4 zeros)
- > The default administrator password is 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”
- > The default Opacity Pairing code is “12345678” (required for contactless mode only)

## 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.
- > The *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 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 12.](#)

## Operating Systems

Following operating systems are supported:

- > Red Hat 9.6 and 10
- > CentOS 9 and 10
- > Fedora 43
- > Debian 12 and 13
- > Ubuntu 22, 24.04.3 LTS, and 25

## 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+
- > SafeNet eToken 5110 FIPS
- > SafeNet eToken 5110+ FIPS
- > SafeNet eToken 5110+ FIPS L2 India
- > SafeNet eToken 5110+ FIPS L3 India
- > SafeNet eToken 5110 CC
- > SafeNet eToken 5110 CC (940)
- > SafeNet eToken 5110+ CC (940B)
- > SafeNet eToken 5110+ CC (940C)
- > SafeNet eToken Fusion CC
- > SafeNet eToken Fusion NFC PIV USB A and USB C
- > SafeNet eToken Fusion NFC PIV Enterprise USB A and USB C
- > SafeNet eToken Fusion FIPS
- > SafeNet eToken Fusion NFC FIPS
- > SafeNet eToken Fusion BIO USB-C

## 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 930C
- > SafeNet IDPrime 3930C
- > 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

- > SafeNet eToken Fusion CC
- > SafeNet eToken Fusion
- > SafeNet IDPrime 940B FIDO
- > SafeNet eToken 5110 CC (940)
- > SafeNet eToken 5110+ CC (940B)
- > SafeNet eToken 5110+ CC (940C)
- > SafeNet IDPrime 940B
- > SafeNet IDPrime 940C
- > SafeNet IDPrime 940
- > SafeNet IDPrime 3940
- > SafeNet IDPrime 3940C
- > Gemalto IDPrime MD 840
- > Gemalto IDPrime MD 840 B
- > Gemalto IDPrime MD 3840
- > Gemalto IDPrime MD 3840 B
- > SafeNet eToken 5110 CC

### External Smart Card Readers

- > Gemalto IDBridge CT30
- > Gemalto IDBridge CT40
- > HID Omnikey 5422 (contact and contactless)
- > HID Omnikey 5022 (contactless only)
- > HID OMNIKEY 5427 G2 (Contactless only)
- > HID OMNIKEY 3021
- > HID Omnikey 3121
- > Identiv uTrust 4701 F
- > Gemalto IDBridge K30\*
- > Gemalto IDBridge K50\*
- > Gemalto IDBridge CT30
- > Gemalto IDBridge CT40



- > Cherry KC 1000 Smartcard
- > Fujitsu KB SCR/eSIG
- > HP Business Slim Smartcard Keyboard (TPC-C001K) - Chicony HP Skylab Smartcard Reader
- > HP USB SmartCard CCID-keyboard (KUS1206) - Chicony HP Smartcard Keyboard
- > Dell Readers built in Latitude-serien (same reader in 5x10 och 5x20-models)
- > Dell Readers built in Latitude 5x30-model

**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/3810/3810 MIFARE 1K/3811/SafeNet eToken 5300	SafeNet IDPrime 930/3930	SafeNet eToken 5110-FIPS	SafeNet IDPrime PIV cards and tokens

Features	Devices					
Number of key containers	14 – default <b>Note 1</b>	20 – default <b>Note 1</b>	15	32	Dynamic <b>Note 5</b>	24 (20 Retired, 1 PIV Authentication, 1 Digital Signature, 1 Key Management, and 1 Card Authenticator)  <b>Note 8</b>
RSA Key sizes	2048-bit - default 3072-bit 4096-bit 4096-bit <b>Note 2 and Note 7</b>	2048-bit - default 3072-bit 4096-bit - default <b>Note 2</b>	1024-bit 2048-bit <b>Note 3</b>	2048-bit 3072-bit 4096-bit <b>Note 3</b>	1024-bit 2048-bit <b>Note 3</b>	For IDPrime PIV 3.0 : <ul style="list-style-type: none"> <li>&gt; 1024-bit</li> <li>&gt; 1280-bit</li> <li>&gt; 1536-bit</li> <li>&gt; 2048-bit</li> </ul> For IDPrime PIV 4.0/eToken Fusion NFC PIV /Enterprise: <ul style="list-style-type: none"> <li>&gt; 2048-bit</li> <li>&gt; 3072-bit</li> <li>&gt; 4096-bit</li> </ul>
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 <b>Note 4</b>	RAW, PKCS#1 v1.5, PSS, OAEP <b>Note 3 and Note 6</b>	PKCS#1 v1.5, PSS, OAEP
ECC Key sizes	256-bit - default 384-bit 521-bit <b>Note 2</b>	256-bit - default 384-bit 521-bit <b>Note 2</b>	256-bit 384-bit 521-bit	256-bit 384-bit 521-bit	256-bit 384-bit	256-bit - default 384-bit

Features	Devices					
Hash	SHA-1 160-bit SHA-2 256-bit, 384-bit, 512-b	SHA-1 160-bit SHA-2 256-bit, 384-bit, 512-bit	SHA-1 160-bit SHA- 2 256-bit, 384-bit, 512-bit <b>Note 3</b>	SHA-1 160-bit SHA-2 256-bit, 384-bit, 512-bit  <b>Note 3</b>	SHA-1 160-bit SHA-2 256-bit, 384-bit, 512-bit  <b>Note 3</b>	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
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 DeveloperGuid e</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 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-bit and 4096-bit only key import available (no OBKG).
8. The Card Authentication container (9E) is now enabled for key generation as well as the import of keys and certificates. This container (9E) is not supported for symmetric keys as it is exclusively designated for use in physical access mode..

**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 25	140.5.0esr
		Ubuntu 24.04	140.3.1esr
		CentOS 9/RHEL 9.6	140.5.0
		CentOS 10 /Fedora 43/RHEL 10/Debian 13	145.0

Solution Type	Vendor	Product Version	
Browsers	Mozilla	Firefox on OS	Version
		Ubuntu 25	143.0.4
		Ubuntu 24.04	141.0
		CentOS 10	140.4.0esr
		Fedora 43	143.0.3
		RHEL 9.6/CentOS 9	140.5.0esr
		RHEL 10	128.8.0esr
		Debian 13	141.0
	Google	Chrome on OS	Version
		Ubuntu-25/RHEL9.6, 10/CentOS 9, 10/Fedora 43/ Debian 13	143.0.7499.40
		Ubuntu 24.04	142.0.7444.175

\* 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 10.9 (GA) to SAC 10.9 R1 (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-21431	H	When attempting to retrieve the SafeNet eToken Fusion NFC PIV card (loaded with 2 or 3 or 5 certificates) information using the <code>certutil -scinfo</code> command with SAC 10.9 R2 (6003), the operation fails with the error: "Smart card cannot perform the requested operation."  (Customer ID: CS2211484)
ASAC-20284	H	The PIN policy is not enforced on the user PIN for the Common Criteria (CC) cards and tokens while <i>Unlocking a Token by the Challenge-Response</i> method. To know about the registry setting, refer to the Configuration Properties chapter in <i>SafeNet Authentication Client Administrator Guide</i> .  (Customer ID: CS1579561, CS1589826, CS2145735)
ASAC-15985	H	SAC is unable to identify and distinguish the IDPrime products using PKCS#11 attributes.  (Customer ID: CS1461611, CS1462968, CS1544973)
ASAC-19221	H	Facing certificate enrollment issue with IDPrime SIS 840.  (Customer ID: CS1551052)

Issue	Severity	Synopsis
ASAC-19711	H	If the Admin PIN gets locked, SAC is unable to detect SafeNet eToken 5110 CC (940).  (Customer ID: CS1567263, CS1580863)
ASAC-21050	M	Getting the <code>CKR_ARGUMENTS_BAD</code> with <code>eTPKCS11.dll</code> but not with <code>IDPrimePKCS11.dll</code> .  (Customer ID: CS1611285)
ASAC-21341	M	SAC crashes when SafeNet eToken 5110+ L2, L3 tokens are connected.  (Customer ID: CS2164999)

## Known Issues

Issue	Severity	Synopsis
ASAC-9244	H	<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. <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> .
ASAC-21293	M	<b>Summary:</b> When switching back from other machines, certificates are not visible in the SAC Tools after the Pairing Code Verification is performed on IDPrime PIV card/token in a contactless mode. <b>Workaround:</b> Complete the Pairing Code Verification and refresh the SAC Tools using "Refresh" icon.
ASAC-21263	M	<b>Summary:</b> The PIN Pad does not ask to change digital signature PUK and signature PIN during or after the initialization operation. <b>Workaround:</b> None.
ASAC-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. <b>Workaround:</b> None
ASAC-15318	M	<b>Summary:</b> The <i>Card type</i> shows unknown in SAC Tools for the legacy SafeNet eToken 5110. <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-9288 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 <i>/etc/eToken.conf</i>.</p>
ASA C-9108 ASA C-6191	H 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-11099	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 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.</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>
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>



Issue	Severity	Synopsis
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\eToken.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-4141	M	<p><b>Summary:</b> During the unblock operation, no other application can access the device until the unblock operation is finished or canceled.</p> <p><b>Workaround:</b> None.</p>
ASA C-15319	L	<p><b>Summary:</b> Free space is constant in SAC Tools for the legacy SafeNet eToken 5110.</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>
ASA C-20340	L	<p><b>Summary:</b> An unclear text is displayed in the <i>Initialize Token -Password Settings</i> window on Fedora 41.</p> <p><b>Workaround:</b> None</p>
ASA C-20137	L	<p><b>Summary:</b> In SAC Tools, the alignment of "Advanced" window in the <i>Token's Settings</i> is not proper.</p> <p><b>Workaround:</b> None</p>

## 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 black 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).