# SafeNet Authentication Client 10.9 R3 (GA)

## WINDOWS RELEASE NOTES

**Issue Date:** April 2026

**Build:** 10.9.7449.0
**Document Part Number:** 007-013559-010 Rev. J

### Contents


**Product Description** ..... **3**
Release Description ..... 3
New Features and Enhancements ..... 3
Advisory Notes ..... 3
Licensing ..... 4
Localization ..... 4
SafeNet Authentication Client Certification ..... 5
Default Password ..... 6
- Password Recommendations ..... 6
- Initialization Key Recommendations ..... 7

Compatibility Information ..... 7
- Operating Systems ..... 7
- CPU ..... 7
- Hardware and Screen Resolution Requirements ..... 7

Tokens ..... 7
- Certificate-based USB Tokens ..... 7
- Software Tokens ..... 8
- Smart Cards ..... 8
- Smart Cards and Tokens that Support Common Criteria ..... 9
- Smart Card Readers supported in Contact and Contactless modes ..... 9
- Smart Card Readers supported in Contact mode ..... 10
- Secure PIN Pad Readers: ..... 10

Device Features Supported by SAC ..... 10
Compatibility with Third-Party Applications ..... 13
Compatibility with Thales Applications ..... 14
Installation and Upgrade Information ..... 15
- Installation ..... 15




April 2026, Copyright © 2026 Thales Group. All rights reserved.

Upgrade ..... 15
Uninstall ..... 15
Supported ATRs ..... 15
**Resolved and Known Issues** ..... **18**
Resolved Issues ..... 18
Known Issues ..... 18
Known Limitations ..... 21
**Product Documentation** ..... **23**
**Support Contacts** ..... **24**


April 2026, Copyright © 2026 Thales Group. All rights reserved.

# 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 R3 (GA) includes enhancements made since SAC previous versions.

## New Features and Enhancements

This release offers the following:

- SAC Tools now includes a *Token ID* label for IDPrime cards.
- Some enhancements done in the SAC Customization tool.

  For details, refer to the "Configuration Properties" chapter in the *SafeNet Authentication Client Administrator Guide.*
- Performance enhancement.
- Security improvements.
- Fix from previous release. Refer to "Resolved Issues" on page 18.

## Advisory Notes

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

- Release Quality Limitation

  On Windows supported versions, the total number of readers that an administrator can allocate is limited to 10 from among the following: eToken readers, third-party readers, and reader emulations.
- 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*.
  - Smart Card Logon is not supported on IDPrime 930C/3930C cards because the default hashing algorithm, SHA-1, is disallowed under FIPS certification requirements.
- SafeNet IDPrime 930 L3 cards:
  - SafeNet IDPrime 930 L3 cards do not support windows authentication.
  - 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


April 2026, Copyright © 2026 Thales Group. All rights reserved.

available to use with sign operation is the SHA-2 mechanism with the following supported lengths: 256, 384, and 512 bits.

- 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.
- For IDPrime 930C L3 cards, CSP-based certificate enrollment is not supported because it relies on SHA-1 as the default hashing algorithm, which is restricted under FIPS specifications.

> eToken 5110 FIPS:

- Supported on OpenTrust versions 4.9.2 or 5.6.
- 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 10.9 R3 (GA) does not support RSA 1024 key size signing with SHA-1. If you need it, use the `Disable-Crypto` setting mentioned in *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 DLL(s) with any third party applications is supported but should be used diligently by the third party applications.

> A vulnerability has been fixed in the windows installer (MSI) built with InstallScript custom action. This vulnerability was allowing a privilege escalation when invoked ‘repair’ of the MSI, which has an InstallScript custom action.

  For detailed information, refer to https://community.flexera.com/t5/InstallShield-Knowledge-Base/CVE-2024-3310-Privilege-Escalation-Vulnerability-During-MSI/ta-p/315134/message-revision/315134:2

> For enabling the contactless mode in IDPrime PIV cards and tokens, make sure the SAC service is running.

> Support for IDClassic 410 cards has been discontinued.

# Licensing

From SAC 10.8 R2 release onward, no license is required for SAC on Windows.

# Localization

This release support the following languages:

> Bulgarian

> Chinese (Simplified)

> Chinese (Traditional)

> Croatian

> Czech

> English


April 2026, Copyright © 2026 Thales Group. All rights reserved.

- 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.

# SafeNet Authentication Client Certification

SafeNet Authentication Client (SAC) 10.9 R3 (GA) has the following certifications:

- Citrix Ready: https://citrixready.citrix.com/thales-e-security/safenet-authentication-client.html
- SAC 10.9 R3 (GA) is compliant with Microsoft LSA (Local Security Authority) and Microsoft Credential Guard.

> **NOTE** If you encountered an issue with LSA or Credential Guard, try configuring them in Audit mode, to assess which process or service has been blocked.
> For more information, refer to the "Using SafeNet Authentication Client with Windows Defender Credential Guard" Chapter in *SafeNet Authentication Client Compatibility Guide*.


April 2026, Copyright © 2026 Thales Group. All rights reserved.

# 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 “010203040506070801020304050607080”

> 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

> **NOTE** These recommendations are not applicable for IDPrime PIV cards and tokens, IDPrime SIS 840, and IDPrime 940 SIS cards.

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

> 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, 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.*


April 2026, Copyright © 2026 Thales Group. All rights reserved.

### 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

### Operating Systems

Following operating systems are supported:

- Windows 11(64-bit)
- Windows 10 (32-bit, 64-bit)
- Windows Server 2025 (64-bit)
- Windows Server 2022 (64-bit)
- Windows Server 2019 (64-bit)
- Windows Server 2016 (64-bit)
- Windows Server 2012 R2 (64-bit)

### CPU

Following CPU's are supported

- Intel (32 and 64-bit)
- Snapdragon (Surface ProXSQ2/16/256 M1501)

### Hardware and Screen Resolution Requirements

Following hardware are required:

- USB port, for physical token devices and readers
- Recommended display resolution (for SafeNet Authentication Client Tools) 1024 x 768 pixels and higher

## 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


April 2026, Copyright © 2026 Thales Group. All rights reserved.

- SafeNet eToken 5110+
- 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 (upcoming)

> **NOTE** The Contactless functionality is not supported on IDPrime PIV tokens, as the necessary keys are not available or provisioned on the device.

## Software Tokens

- SafeNet IDPrime Virtual Smart Card

## Smart Cards

- SafeNet IDPrime PIV 3.0
- SafeNet IDPrime PIV 4.0
- SafeNet IDPrime PIV 4.1
- SafeNet IDPrime 940B FIDO
- SafeNet IDPrime MD 830nc
- SafeNet IDPrime 930
- SafeNet IDPrime 930nc
- SafeNet IDPrime 3930
- SafeNet IDPrime 3930 FIDO
- SafeNet IDPrime 930C
- SafeNet IDPrime 3930C
- SafeNet IDPrime 940
- SafeNet IDPrime 940B
- SafeNet IDPrime 940C
- SafeNet IDPrime 3940


April 2026, Copyright © 2026 Thales Group. All rights reserved.

- SafeNet IDPrime 3940C
- SafeNet IDPrime 3940 FIDO
- SafeNet IDPrime 940 SIS
- SafeNet IDPrime SIS 840

> **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 *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

## Smart Card Readers supported in Contact and Contactless modes

- HID OMNIKEY 5422
- HID OMNIKEY 5022 (Contactless only)
- Identiv uTrust 4701 F

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


April 2026, Copyright © 2026 Thales Group. All rights reserved.

## Smart Card Readers supported in Contact mode

- Gemalto IDBridge K30*
- Gemalto IDBridge K50*
- Gemalto IDBridge CT30
- Gemalto IDBridge CT30- C
- Gemalto IDBridge CT40
- HID OMNIKEY 3021
- HID OMNIKEY 3121
- 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-series (same reader in 5x10 and 5x20-models)
- Dell Readers built in Latitude 5x30-model
- Dell Pro Smartcard Keyboard - KB813 (To use this reader, refer to the workaround of "Product Description" on page 3

*Validated with previous SAC version

## Secure PIN Pad Readers:

- Gemalto IDBridge CT700
- Gemalto IDBridge CT710
- Gemalto SWYS
- Thales PKI PIN Pad (Thales Shield M4 Reader)

To know the list of supported products, end of sale, or end of life tokens, refer to https://supportportal.thalesgroup.

# Device Features Supported by SAC

Below table specifies the various features that are supported by SAC:

| Features: | Device: | | | | | |
|---|---|---|---|---|---|---|
| | **Gemalto IDPrime MD 840/3840/3840B/ 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** |


April 2026, Copyright © 2026 Thales Group. All rights reserved.

| Features: | Device: | | | | | |
|---|---|---|---|---|---|---|
| Number of key containers | 14 – default<br>**Note 1** | 20 – default<br>**Note 1** | 15 | 32 | Dynamic<br>**Note 5** | 24 (20 Retired, PIV Authentication, Digital Signature, Key Management, and Card Authenticator)<br>**Note 8** |
| RSA Key sizes | 2048-bit - default<br>3072-bit<br>4096-bit<br>**Note 2 & 7** | 2048-bit - default<br>3072-bit<br>4096-bit - default<br>**Note 2** | 2048-bit<br>**Note 3** | 2048-bit<br>3072-bit<br>4096-bit<br>**Note 3** | 2048-bit<br>**Note 3** | For IDPrime PIV 3.0 :<br>> 1024-bit<br>> 1280-bit<br>> 1536-bit<br>> 2048-bit<br>For IDPrime PIV 4.0/4.1 /eToken Fusion NFC PIV/Enterprise:<br>> 2048-bit<br>> 3072-bit<br>> 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<br>**Note 4** | RAW, PKCS#1 v1.5, PSS, OAEP<br>**Note 3 & 6** | PKCS#1 v1.5, PSS, OAEP |
| ECC Key sizes | 256-bit - default<br>384-bit<br>521-bit<br>**Note 2** | 256-bit - default<br>384-bit<br>521-bit<br>**Note 2** | 256-bit<br>384-bit<br>521-bit | 256-bit<br>384-bit<br>521-bit | 256-bit<br>384-bit | 256-bit - default<br>384-bit |


April 2026, Copyright © 2026 Thales Group. All rights reserved.

| Features: | Device: | | | | | |
|---|---|---|---|---|---|---|
| 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<br>SHA-2 256-bit, 384-bit, 512-bit<br><br>**Note 3** | SHA-1 160-bit<br>SHA-2 256-bit, 384-bit, 512-bit<br><br>**Note 3** | SHA-1 160-bit<br>SHA-2 256-bit, 384-bit, 512-bit<br><br>**Note 3** | 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 *SafeNet Authentication Client Developer Guide*. |
| 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. 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.


April 2026, Copyright © 2026 Thales Group. All rights reserved.

**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.
- For IDPrime PIV cards and tokens, configure the following Windows registry setting to generate RSA keys with a 4096-bit key size. Ensure that the Microsoft-certified driver is installed before applying this setting.
Registry Path: *Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services*
Key: *GemCCID*
DWORD (32-bit) Value: ReadTimeOutInMs
Value data: *0x7A120* (Hexadecimal) or *500000* (Decimal)

# Compatibility with Third-Party Applications

Following third-party applications are supported:

| Solution Type | Vendor | Product Version |
|---|---|---|
| Remote Access VPN | Check Point | Endpoint Security E80.70 |
| | Microsoft | Windows Server 2008 SP2 and later |
| | Cisco | NAM |
| | | AnyConnect Windows 4.7.00136 |
| | Palo Alto | PA-200 GW Appliance |
| | Juniper | Juniper MAG 2600 GW Appliance |
| Virtual Desktop Infrastructure (VDI) | Citrix | Virtual Apps and Desktops 7.2206 (Formerly XenDesktop) |
| | Microsoft | Remote Desktop |
| | VMware View | Horizon 7.8 |


April 2026, Copyright © 2026 Thales Group. All rights reserved.

| Solution Type | Vendor | Product Version |
|---|---|---|
| Identity Access Management (IAM)<br>Identity Management (IDM) | IBM | ISAM for Web 9.0 (eToken only) |
| | Intercede | MyID 11.3 |
| | Microsoft | MIM 2016 4.5.286.0 (Supported with SAC Minidriver profile) |
| | vSEC:CMS | vSEC:CMS 6.9.0.4<br>(Supported with SAC Minidriver profile) |
| | IDnomic | OpenTrust CMS 5.2<br>**NOTE** For eToken 5110 FIPS support, refer to "Advisory Notes" on page 3. |
| Pre Boot Authentication (PBA) | Sophos | SafeGuard Easy (eToken only) |
| | Microsoft | BitLocker 10.0.19041 (RSA only) |
| Certificate Authority (CA) | Entrust | ESP 10 |
| | Microsoft (Local CA) | For All Windows platforms |
| Single-Sign-On (SSO) | Evidian | ESSO (eToken only) |
| Digital Signatures | Entrust | ESP 10 |
| | Adobe Acrobat Pro | 26.001.21431 |
| | Microsoft | Outlook 2016 / Office 365 |
| | Mozilla | Thunderbird 115.4.1 |
| Browsers | Mozilla | Firefox 149.0.2 (TLS 1.3 supported) |
| | Microsoft | Edge Chromium 146.0.3856.84 (TLS 1.3 supported) |
| | Google | Chrome 147.0.7727.102 (TLS 1.3 supported) |

# Compatibility with Thales Applications

IDPrime cards can be used with the following products:

> SafeNet Authentication Service (SAS) / SafeNet Trusted Access (STA)


April 2026, Copyright © 2026 Thales Group. All rights reserved.

> IDPrime User Tool for Windows (V1.2.0)

To work with these products, install SafeNet Minidriver profile by generating a `.msi` file using the SAC Customization Tool.

To generate an MSI installation file, refer to *SafeNet Authentication Client Administrator Guide*.

# Installation and Upgrade Information

> **NOTE** Local administrator rights are required to install, uninstall, and upgrade SAC.

## Installation

SAC must be installed on each computer on which IDPrime cards, as well as SafeNet Tokens or Smart Cards are to be used.

## Upgrade

You can upgrade from SafeNet Authentication Client 10.9 R2 (Post GA) and 10.9 R2 (Post GA-2) to 10.9 R3 (GA) using the MSI file wizard installation, or by using the command line installation.

## Uninstall

Once SAC is installed, it can be uninstalled. After uninstallation, the user configuration and policy files may be deleted.

> **NOTE** You must restart your computer when the uninstall procedure completes.

For more details on installation, uninstallation, and upgrade, refer to *SafeNet Authentication Client Administrator Guide*.

# Supported ATRs

This section lists the ATRs for the supported smart cards. Those figures indicated in bold can differ from one card to another in the same family (other IDPrime MD cards may be added for later versions). All values are in hexadecimal.

> SafeNet eToken 5110 CC USB Token

> SafeNet IDPrime 940, 940B, 940C, 3940, 3940C, 830nc, 930nc Cards

- [IDPrime MD T=0] 3B 7F **00** 00 00 80 31 80 65 B0 **00 00 00 00** 12 0F FE 82 90 00
- [IDPrime MD T=1] 3B FF **00** 00 00 81 31 **00** 43 80 31 80 65 B0 **00 00 00 00** 12 0F FE 82 90 00 **00**

> Gemalto IDPrime MD 830-FIPS, 830-ICP, 830 B, 840, 840 B, 3810, 3811, 3840, 3840 B and 8840 Cards Ezio PKI Cards

- [IDPrime MD T=0] 3B 7F **00** 00 00 80 31 80 65 B0 **00 00 00 00** 12 0F FE 82 90 00
- [IDPrime MD T=1] 3B FF **00** 00 00 81 31 **00** 43 80 31 80 65 B0 00 00 00 00 12 0F FE 82 90 00 00
- [IDPrime MD Contactless] 3B 8F 80 01 80 31 80 65 B0 **00 00 00 00** 12 0F FE 82 90 00 **00**
- [IDPrime MD Contactless B] 3B 88 80 01 31 F3 5E 11 **00** 87 95 **00 00**


April 2026, Copyright © 2026 Thales Group. All rights reserved.

- SafeNet IDPrime 930, 3930 Cards, 930C, 3930C
  - [IDPrime v2 T=0] 3B 7F **00** 00 00 80 31 80 65 B0 **00 00 00 00** 12 0F FD 82 90 00
  - [IDPrime v2 T=1] 3B FF **00** 00 00 81 31 **00** 43 80 31 80 65 B0 **00 00 00 00** 12 0F FD 82 90 00 **00**
  - [IDPrime v2 contactless type A] 3B 8F 80 01 80 31 80 65 B0 **00 00 00 00** 12 0F FD 82 90 00 **00**
  - [IDPrime v2 contactless type B] 3B 88 80 01 32 F3 5E 11 **00** 87 95 **00 00**
  - IDPrime 3930C (Contactless) 3B,8F,80,01,80,31,80,65,B0,84,66,6B,39,12,FF,FE,82,90,00,5B
- SafeNet eToken 5300 USB Token, Fusion NFC FIPS (Contactless)
  - [eToken5300] 3B FF **00** 00 00 81 31 **00** 43 80 31 80 65 B0 **00 00 00 00** 12 01 78 82 90 00 **00**
- Optelio R7 Cards
  - [Optelio D72 FXR1 (MD) T=0] 3B 6E 00 00 80 31 80 66 B1 A1 11 01 A0 F6 83 00 90 00
  - [Optelio D72 FXR1 (MD) T=1] 3B EE 00 00 81 31 80 43 80 31 80 66 B1 A1 11 01 A0 F6 83 00 90 00 8F
  - [Optelio R7 Contact] 3B 6E 00 00 80 31 80 66 B0 87 0C 01 6E 01 83 00 90 00
  - [Optelio R7 Contactless] 3B 8E 80 01 80 31 80 66 B1 84 0C 01 6E 01 83 00 90 00 **00**
  - [Optelio R7 with WG10 Contact] 3B 68 00 00 80 66 B0 07 01 01 07 07
  - [Optelio R7 with WG10 Contactless] 3B 88 80 01 80 66 B0 07 01 01 07 **00 00**
  - [Optelio R7 with WG10+2F10 contact] 3B 6F 00 00 80 66 B0 07 01 01 07 **00 00 00 00 00 0**0 90 00
  - [Optelio R7 with WG10+2F10 contactless] 3B 8F 80 01 80 66 B0 07 01 01 07 **00 00 00 00 00 00** 90 00 **00**
- SafeNet IDPrime Virtual Smart Card
  - [IDPrime Virtual] 3B FF 96 00 00 81 31 FE 43 80 31 80 65 B0 00 00 00 00 12 91 78 82 90 00 69
- SafeNet IDPrime 940 SIS, 3940 SIS, 840 SIS Cards
  - [IDPrime 940 SIS T=0] 3B 7F **00** 00 00 80 31 80 65 B0 **00 00 00 0**112 02 F0 82 90 00
  - [IDPrime 940 SIS T=1] 3B FF **00** 00 00 81 31 **00** 43 80 31 80 65 B0 **00 00 00 00** 12 02 F0 82 90 00 **00**
  - [IDPrime 940 SIS contactless type A] 3B 8F 80 01 80 31 80 65 B0 **00 00 00 00** 12 02 F0 82 90 00 **00**
  - [IDPrime 840 SIS T=0] 3B 7F **00** 00 00 80 31 80 65 B0 **00 00 00 0**F 12 02 F0 82 90 00
- SafeNet IDPrime 3940 FIDO, 940B FIDO, 3930 FIDO, 3930C FIDO
  - [IDPrime Fido T=1] 3B FF **00** 00 00 81 31 **00** 43 80 31 80 65 B0 **00 00 00 00** 12 0F FC 82 90 00 **00**
  - IDPrime 3940 FIDO (Contactless) 3b,8f,80,01,80,31,80,65,b0,85,05,00,39,12,01,78,82,90,00,00
  - IDPrime 3930C FIDO (Contact)
    3B,FF,96,00,00,81,31,FE,43,80,31,80,65,B0,84,66,6B,39,12,FF,FC,82,90,00,00
  - IDPrime 3930C FIDO (Contactless) 3b,8f,80,01,80,31,80,65,b0,84,66,6B,39,12,ff,fc,82,90,00,00
- SafeNet eToken 5110, 5110 FIPS
  - [eTokenCard/JC1.0] 3B D5 18 00 81 31 FE 7D 80 73 C8 21 10 F4
  - [eTokenCard/JC1.0b] 3B D5 18 00 81 31 3A 7D 80 73 C8 21 10 30
- eToken 5110+ CC (940C)
  - [eToken5300] 3B FF 00 00 00 81 31 FE 43 80 31 80 65 B0 85 05 00 39 12 01 78 82 90 00 40


April 2026, Copyright © 2026 Thales Group. All rights reserved.

- SafeNet eToken 5300 USB A TS, 5300-C, 5300-C TS, 5110 CC (940), 5110+ CC (940B), 5110+FIPS, Fusion, Fusion FIPS, Fusion CC, Fusion NFC FIPS (Contact)
  - [eToken5300] 3B FF **00** 00 00 81 31 **00** 43 80 31 80 65 B0 **00 00 00 00** 12 01 78 82 90 00 **00**
- SafeNet IDPrime PIV v3.00 (Contact)
  - [PIV3.0] 3B FD 96 00 00 81 31 FE 43 80 31 80 65 B0 87 5C 17 FB 83 00 90 00 A6
- SafeNet IDPrime PIV v4.0 and PIV v4.1 (Contact)
  - [PIV FIDO] 3B FF 96 00 00 81 31 FE 43 80 31 80 65 B0 88 66 6B 39 12 0E FC 82 90 00 **00**
- SafeNet eToken Fusion NFC PIV (Contact)
  - [eToken5300] 3B FF **00 00 00** 81 31 FE 43 80 31 80 65 B0 88 **00 00 00** 12 01 78 82 90 **00 00**
- SafeNet IDPrime PIV v3.0 (Contactless)
  - [PIV3.0_CL] 3B 8D 80 01 80 31 80 65 B0 87 5C 17 FB 83 00 90 00 CC
- SafeNet IDPrime PIV v4.0 (Contactless)
  - [PIV4.0_CL] 3B 8F 80 01 80 31 80 65 B0 88 66 6B 39 12 0E FE 82 90 00 A6
- SafeNet IDPrime PIV v4.1 (Contactless)
  - [PIV4.1_CL] 3B 8F 80 01 80 31 80 65 B0 84 66 6B 39 12 FF FE 82 90 00 5B
- SafeNet eToken Fusion NFC PIV, SafeNet eToken Fusion NFC PIV Enterprise (Contactless)
  - [PIV_FUSION_CL] 3B 8F 80 01 80 31 80 65 B0 88 66 6B 39 12 01 78 82 90 00 2F
- SafeNet eToken Fusion NFC FIPS (Contactless), eToken Fusion NFC FIPS 930C (USB-A/USB-C)
  - [eToken5300_CL] 3B 8F 80 01 80 31 80 65 b0 84 65 **00 00** 12 01 78 82 90 00 **00**
  - eToken Fusion NFC FIPS 930C (USB-A/USB-C) (Contact)
    3b,8f,80,01,80,31,80,65,B0,84,66,6B,39,12,01,78,82,90,00,00
  - eToken Fusion NFC FIPS 930C (USB-A/USB-C) (Contactless)
    3B,8F,80,01,80,31,80,65,B0,84,66,6B,39,12,FF,FE,82,90,00,5B
- SafeNet eToken FIDO NFC USB A & C
  - eToken FIDO NFC (USB-A/USB-C) (Contact)
    3B,FF,96,00,00,81,31,FE,43,80,31,80,65,B0,84,66,6B,39,12,ff,7c,82,90,00,00
  - eToken FIDO NFC (USB-A/USB-C) (Contactless)
    3b,8f,80,01,80,31,80,65,b0,84,66,6b,39,12,ff,7c,82,90,00,00


April 2026, Copyright © 2026 Thales Group. All rights reserved.

# Resolved and Known Issues

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.

| Priority | Classification | Definition |
|---|---|---|
| C | Critical | No reasonable workaround exists. |
| H | High | Reasonable workaround exists. |
| M | Medium | Medium level priority problems. |
| L | Low | Lowest level priority problems. |

## Resolved Issues

| Issue | Severity | Synopsis |
|---|---|---|
| ASAC-21377 | H | The cryptographic operations on eToken 5110+ FIPS take significantly longer time.<br><br>(Customer ID: CS2180325) |

## Known Issues

| Issue | Severity | Synopsis |
|---|---|---|
| ASAC-21556 | M | **Summary:** A user PIN prompt appears multiple times during the enrollment of multiple certificates in a single MMC session.<br>**Workaround:** None. |
| ASAC-21552, ASAC-21557 | M | **Summary:** Unable to enroll sign only or exchange certificate when all the 24 containers are filled in the IDPrime PIV cards and tokens.<br>**Workaround:** None. |
| ASAC-21293 | M | **Summary:** 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.<br>**Workaround:** Complete the Pairing Code Verification and refresh the SAC Tools. |
| ASAC-21263 | M | **Summary:** The PIN Pad does not ask to change digital signature PUK and signature PIN during or after the initialization operation.<br>**Workaround:** None. |


April 2026, Copyright © 2026 Thales Group. All rights reserved.

| Issue | Severity | Synopsis |
|---|---|---|
| ASAC-20072 | M | **Summary:**Upgrade fails from SAC 10.9 GA (and previous versions) to SAC 10.9 R1 GA in case of Swedish customized msi.<br>**Workaround:** Either uninstall previous version msi and install the SAC 10.9 R1 GA version or run the repair option of the msi. |
| ASAC-19614 | M | **Summary:** In the standard SAC msi (PKCS#11), the SAC Monitor does not show the *Change Token PIN* option for USB port 8, 9, and 10 when cards are connected on all the 10 ports through a multislot USB device.<br>**Workaround:** None. |
| ASAC-16028 | M | **Summary:** Old registry entries are not getting removed in case of upgrade with customized MSIs.<br>**Workaround:** Delete registries of old MSI from the registry editor. |
| ASAC-14425 | L | **Summary:** Mozilla Thunderbird stops working if a smart card is swapped while performing the send email operation.<br>**Workaround:** Relaunch Thunderbird and perform the operation with a valid smart card. |
| ASAC-13750 | M | **Summary:** DLL (`SACUI.cs-Cz.dll`) missing when upgrading SAC Typical from 10.2 to 10.8 R6.<br>**Workaround:** Firstly, upgrade SAC Typical from 10.2 to 10.8 R5. Thereafter, upgrade SAC Typical from 10.8 R5 to 10.8 R6. |
| 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.<br>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.<br>**Workaround:** On IDPrime based devices, use the PSS parameters with the salt length equal to the hash length. |
| ASAC-10910 | M | **Summary:** It was not possible to authenticate to the VMWare Horizon Client with a smart card when SingleLogon is configured to 2. This is the expected behavior as Horizon uses explicit login and Microsoft Base Provider cannot run explicit login for SingleLogon scenarios.<br>**Workaround:** Disable SingleLogon by adding the process name (vmware-view.exe) to the registry and set SingleLogon to 0.<br>(Refer to 'Defining a Per Process Property' in the *SafeNet Authentication Client Administrator Guide*). |


April 2026, Copyright © 2026 Thales Group. All rights reserved.

| Issue | Severity | Synopsis |
|---|---|---|
| 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.<br>**Workaround:** Add the property `RetryCountCached=0` under the [General] section: `SafeNet\Authentication\SAC\General registry key`. |
| ASAC-8923 | M | **Summary:** Common Criteria devices (840, 940 and 5110CC) do not work with SAC default in conjunction with OpenTrust client 5.2.0.<br>**Workaround:** Disable the Multi-slot support property. See the SAC Administrator Gudie for more information. |
| 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.<br>**Workaround:** Delete the cache folder (C:\Windows\Temp\eToken.cache) after initialization and before changing the password. |
| ASAC-5201 | M | **Summary:** When connecting a non-Pin Pad reader, an incorrect message is displayed in the event viewer.<br>**Workaround:** To disable Pin Pad support, create a REG_DWORD value called "NoPinPad" under the key<br>`HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC\General` and set its value to 1.<br>On 64-bit machines, you additionally need to do the same under the key:<br>`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SafeNet\Authentication\SAC\General` |
| ASAC-4516 | M | **Summary:** Generating a customized .msi file with a previous xml file (taken from an earlier SAC version) is not supported.<br>**Workaround:** Make sure you create a new configuration with the same settings in the current SAC version. |
| 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.<br>**Workaround:** Connect the device that is not under the "Shared" devices list in order to work with the eToken device. |
| ASAC-2284 | M | **Summary:** When a user attempts to generate a customized SAC file with no administrator privileges, the process fails.<br>**Workaround**: Create customized SAC msi file with administrator privileges. |


April 2026, Copyright © 2026 Thales Group. All rights reserved.

| Issue | Severity | Synopsis |
|---|---|---|
| ASAC-1740<br>ASAC-2262 | M | **Summary:**<br>Scenario 1 - When using jarsigner.exe to sign JAR files, the jarsigner command fails to respond for a while.<br>Scenario 2 - When performing an Identrust enrollment on Windows Server 2008, Windows 7 or Windows Server 2008 R2, the enrollment fails.<br>**Cause:**<br>In Windows 7, Windows Server 2008, and Windows Server 2008 R2, when an application using a smartcard has been terminated unexpectedly, it causes other applications that try to connect to the smartcard to stop responding. This occurs in both local and RDP environments. This is a Microsoft issue. Microsoft have released Hotfixes that resolve this issue.<br>**Workaround:** Download the following two hotfixes from Microsoft:<br>Local Scenario: http://support.microsoft.com/kb/2427997<br>RDP: http://support.microsoft.com/kb/2521923 |
| ASAC-1702 | M | **Summary:** When the application runs as a service without the Local System Account permissions, smart card communication fails.<br>**Workaround:** Make sure the service runs with the Local System Account permissions by adding it manually.<br>This is a Microsoft by-design known issue. For more details refer to the following Microsoft support ticket number: 114092811845001. |
| SACINT-38 | M | **Summary:** Unable to sign a Word document via Office 365 (Office on Demand) using SAC.<br>**Workaround:** Open the saved document from the local machine itself. This enables you to sign the document successfully. |

# Known Limitations

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

- Windows logon does not work for IDPrime PIV cards and tokens in contactless mode.
- If multiple readers are connected to the system, a pop-up appears after the *Save Configuration Setting* during uninstallation.
- Generate key operation fails with `CKR_DEVICE_MEMORY` error while using RSA 4096 on the SafeNet eToken Fusion NFC PIV and SafeNet eToken Fusion NFC FIPS - BAI.
- SAC gets installed if SafeNet Minidriver is already installed in the system.
- Import Certificate fails with "incorrect password" message in Window Server 2016 .
- Free space is not updated in SAC Tools for SafeNet IDPrime SIS 840 and SafeNet IDClassic 410 smart cards.
- A Digital Signature PIN operation fails if the Digital Signature PIN (Role#3) and Digital Signature PUK (Role#4) have different PIN Pad configurations (PIN Type and Extended PIN Flags).
- Changing the PIN on Firefox using the CT710 PIN Pad does not work.
- IDPrime smart cards cannot sign plain data longer than 36 bytes for RSA or ECC keys.


April 2026, Copyright © 2026 Thales Group. All rights reserved.

- When SAC (with the SafeNet Minidriver profile) is used with an IDPrime 830 smart card on Windows 10, the PIN prompt is displayed only after 10 seconds between the signing operations.
- Performing smart card authentication to the WiFi network on Windows 10 (1709) is not possible as the smart card logon window is not displayed.
- 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.
- VPN fails using IDPrime 930 L3 (with KSP SHA2 certificate) cards.
- The memory allocated on an IDPrime 930 card for keys or data objects may not be completely freed up when these data objects are deleted. This memory is occupied by the card for future use (allocation of internal structures).

  Therefore, the ‘Free Memory’ reported by SAC (UI or API) may show slightly less memory than there was before creating these data objects.
- 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).
- When a p12 file is imported using Net ID - PKCS#11, it is not visible in *Find all objects* method of the SAC-PKCS#11.
- When working in a VDI environment, configure the `CacheMarkerTimeout` property in the registry. On the host machine go to: `\SafeNet\Authentication\SAC\General`.

  CacheMarkerTimeout=1

  For more details, refer to *SafeNet Authentication Client Administrator Guide*.
- After connecting and using an IDPrime 3811 device (on a contactless reader) the smart card is not recognized (loss of identification).
- On IDPrime MD cards, only CA private certificate objects are supported.
- 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.
- SafeNet eToken 5110 FIPS does not support RSA 1024 and SHA1 on board, as per FIPS/NIST regulations.
- SafeNet Authentication Client does not support RSA 3072 and 4096 on IDPrime MD and eToken devices. SafeNet Authentication Client does not support Single Sign On with IDPrime MD cards via PKCS#11 API interface. For more information, refer to the smart card specification guide.
- When 'Smart Card is required for interactive logon' is enabled, the ‘Synchronize with Domain Password’ feature of SAC is not supported (domain passwords cannot be changed when this option is enabled).


April 2026, Copyright © 2026 Thales Group. All rights reserved.

# 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.


April 2026, Copyright © 2026 Thales Group. All rights reserved.

# 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).


April 2026, Copyright © 2026 Thales Group. All rights reserved.