SafeNet Authentication Client 10.8 (R6) GA

WINDOWS RELEASE NOTES

Issue Date: October 2021

Build: 2154
Document Part Number: 007-013559-007 Rev. K

Contents

Product Description

SafeNet Authentication Client (SAC) is public key infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities. It utilizes a system of digital certificates, certificate authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction.

Release Description

SafeNet Authentication Client 10.8 (R6) GA includes new enhancements and bug fixes from previous SAC versions.

New Features and Enhancements

This release offers the following:

- Added functionality to bypass the Firefox PIN Dialog in SAC Customization Tool for eToken and IDPrime cards.
- Added functionality to support for ICC Public Key in the SAC Customization Tool.

  For details, refer to *SafeNet Authentication Client Administrator Guide*.
- Added support for TLS 1.3.
- Added support for Windows 11 (21H2).
- Improvements in SAC uninstallation process.
- Performance Improvements of IDClassic 340 Cards.

Advisory Notes

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

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

    For more information, refer to *IDPrime 930/3930 Card Configuration Guide*.
- eToken 5110 FIPS:
  - 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.
- SafeNet eToken 5300:
  - To retrieve touch sense capabilities using the SafeNet Minidriver API, refer to the `CCP_TS_CONTAINER` and `CP_CARD_TS_FEATURE` properties in the *SafeNet Authentication Client Developer Guide*.

- In the event of a time out (due to the SafeNet eToken 5300 not being touched in time), the following specific API error messages are shown:
  - `PKCS11 - CKR_FUNCTION_CANCELED(0x00000050)`
  - SafeNet Minidriver - `SCARD_E_CANCELLED (0x80100002)`

    These error messages replace the previous Generic error message.

> SAC 10.8 (R6) 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*.

Licensing

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

Localization

This release support the following languages:

> Chinese (Simplified)
> Chinese (Traditional)
> Czech
> English
> French (Canadian)
> French (European)
> German
> Slovakian (new)
> Hungarian
> Italian
> Japanese
> Korean
> Lithuanian
> Polish
> Portuguese (Brazilian)
> Serbian (new)
> Romanian
> Russian
> Spanish
> Thai
> Vietnamese
> Turkish
> Slovenian (new)

- Croatian (new)

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

SafeNet Authentication Client Certification

SafeNet Authentication Client (SAC) 10.8 (R6) GA has the following certifications:

- Citrix Ready: https://citrixready.citrix.com/thales-e-security/safenet-authentication-client.html
- SAC 10.8 (R6) 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*.

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 zeros). 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)

Password Recommendations

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.*

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 Server 2019 (64-bit)
- Windows Server 2016 (64-bit)
- Windows Server 2012 and 2012 R2 (64-bit)
- Windows 11 (21H2)
- Windows 10 (32-bit, 64-bit) up to 21H1
- Windows 8.1 (32-bit, 64-bit)

Hardware and Screen Resolution Requirements

Following hardware are required:

- USB port, for physical token devices
- 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
- SafeNet eToken 5110
- SafeNet eToken 5110 CC
- SafeNet eToken 5110 FIPS
- SafeNet eToken 5300 C

Software Tokens

- SafeNet IDPrime Virtual Smart Card

Smart Cards

- SafeNet IDPrime 940 SIS
- IDPrime 3940 FIDO
- SafeNet IDPrime 930
- SafeNet IDPrime 3930
- SafeNet IDPrime 940
- SafeNet IDPrime 3940

> **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.

- Gemalto IDCore 30B eToken
- Gemalto IDPrime MD 840 (EOS)
- Gemalto IDPrime MD 840 B
- Gemalto IDPrime MD 3840 (EOS)
- Gemalto IDPrime MD 3840 B
- Gemalto IDPrime MD 830-FIPS
- Gemalto IDPrime MD 830-ICP
- Gemalto IDPrime MD 830 B
- Gemalto IDPrime MD 3810 (EOS)
- Gemalto IDPrime MD 3811
- Gemalto IDPrime MD 8840 (8GB) Micro SD card (EOS)
- Gemalto IDPrime .NET (only SAC PKCS#11 and SafeNet Minidriver interfaces)
- Optelio R7

> **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 IDPrime 940
- SafeNet IDPrime 3940
- 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
- SafeNet eToken 5110 CC

Smart Card Readers supported in Contact and Contactless modes

- CL3000 Prox-du (EOL)
- ACR128U (EOL)
- Omnikey Cardman 5422

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

Smart Card Readers

- Gemalto IDBridge K30
- Gemalto IDBridge K50
- Gemalto IDBridge CT30
- Gemalto IDBridge CT40
- ACR128U (EOL)
- OMNIKEY 5422
- IDBridge CL3000 (EOS)

Secure PIN Pad Readers:

- Gemalto IDBridge CT700

> **NOTE** PIN Pad readers are supported only on IDPrime and .NET cards.

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**

Features:	Device:				
Number of key containers	14 – default **Note 1**	20 – default **Note 1**	15	32	Dynamic **Note 5**
RSA Key sizes	2048-bit - default 3072-bit 4096-bit **Note 2 & 7**	2048-bit - default 3072-bit 4096-bit - default **Note 2**	2048-bit **Note 3**	2048-bit 3072-bit 4096-bit **Note 3**	2048-bit **Note 3**
RSA Padding	PKCS#1 v1.5, PSS, OAEP	PKCS#1 v1.5, PSS, OAEP	PKCS#1 v1.5, PSS, OAEP	PKCS#1 v1.5, PSS, OAEP **Note 4**	RAW, PKCS#1 v1.5, PSS, OAEP **Note 3 & 6**
ECC Key sizes	256-bit - default 384-bit 521-bit **Note 2**	256-bit - default 384-bit 521-bit **Note 2**	256-bit 384-bit 521-bit	256-bit 384-bit 521-bit	256-bit 384-bit
Hash	SHA-1 160-bit SHA-2 256-bit, 384-bit, 512-bit	SHA-1 160-bit SHA-2 256-bit, 384-bit, 512-bit	SHA-1 160-bit SHA-2 256-bit, 384-bit, 512-bit **Note 3**	SHA-1 160-bit SHA-2 256-bit, 384-bit, 512-bit **Note 3**	SHA-1 160-bit SHA-2 256-bit, 384-bit, 512-bit **Note 3**
Activation PIN	N/A	Available	N/A	Available	N/A
Re-init feature	N/A	N/A	N/A	Available	Available
SKI	N/A	N/A	Available	Available	N/A
Non-managed profile	N/A	N/A	N/A	Available	Available

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.
7. RSA 3072 and 4096-bit only key import available (no OBKG).

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 7.1903 (Formerly XenDesktop)
	Microsoft	Remote Desktop
	VMware View	Horizon 7.8
Identity Access Management (IAM) 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 5.8 (Supported with SAC Minidriver profile)
	IDnomic	OpenTrust CMS 5.2 **NOTE** For eToken 5110 FIPS support, refer to "Advisory Notes" on page 3.

Solution Type	Vendor	Product Version
Pre Boot Authentication (PBA)	Sophos	SafeGuard Easy (eToken only)
	Microsoft	BitLocker (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	2020.009.20063
	Microsoft	Outlook 2016 / Office 365
	Mozilla	Thunderbird 52.9.1 **NOTE** As of SAC 10.8, the PKCS#11 module is registered automatically.
Browsers	Mozilla	Firefox 92.0.1 (TLS 1.3 supported)
	Microsoft	> Internet Explorer 11.0.9600.20120 (TLS 1.2 supported) > Edge Chromium 94.0.992.38 (TLS 1.3 supported)
	Google	Chrome 94.0.4606.71 (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)

> IDPrime User Tool for Windows (V1.2.0)

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

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

Installation and Upgrade Information

Installation

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

Upgrade

For earlier versions of SAC, it is recommended that an upgrade is performed to the latest version on each computer that uses a Token or Smart Card. Local administrator rights are required to upgrade SAC.

For more Installation and Upgrade details, refer to *SafeNet Authentication Client Administrator Guide*.

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-13212	H	More checks to add in the SAC installer since `eToken.dll` remains in the system after uninstall and reboot. (Customer ID: CS1037418, CS1030312, CS1030472)
ASAC-13111	H	Installation and uninstallation issues on SAC 10.7 and 10.8 . Registry keys are left in the HKCU hive. (Customer ID: CS1018607)
ASAC-13247	H	Error while unblocking a Token by the Challenge-Response Method. (Customer ID: CS1040451)
ASAC-13031	H	Review maximum password length setting in SAC. (Customer ID: CS0998552)
ASAC-13034	H	In SAC 10.8, TLS 1.3 failing the authentication request due to PSS mechanisms. (Customer ID: CS1006242, CS1001654)
ASAC-13087	H	Login process with IDCore 340 cards is slower than IDPrime MD 940 cards. (Customer ID: CS1029120)

Issue	Severity	Synopsis
ASAC-13168	H	PIN request for website authentication on Firefox browser. (Customer ID: CS1042179)
ASAC-13353	H	DLL Hijacking using SAC . (Customer ID: CS1054011)
ASAC-13072	H	Fail to import ECC 521 key from the SAC Customization Tool. (Customer ID: CS1024721)
ASAC-12671	M	Uninstalling SAC via command line does not clear HKCU settings. (Customer ID: CS0990423)

Known Issues

Issue	Severity	Synopsis
ASAC-11163	H	**Summary:** After locking the Administrator Key (due to an incorrect password being entered too many times), the IDPrime 940/3940 smart card switches to a locked state and as a result the device cannot be used (device is unrecognized). **Workaround:** None – this is a smart card design feature.
ASAC-11167	M	**Summary:** Changing the Initialization Key to a non-compliant value causes the Initialization process to fail on a non-managed IDPrime 930 device. **Workaround:** Ensure the Initialization Key that's used complies with SAC's Initialization key Password Policy (A secure password has at least 8 characters (up to 32 characters) and contains at least 3 from 4 complexity rules). For more details, refer to *SafeNet Authentication Client User Guide*.
ASAC-11099	M	**Summary:** Using the salt length in the PSS parameter that is not equal to the hash length of the appropriate PSS mechanism, causes the C_Verify() command to fail with the CKR_ SIGNATURE_INVALID return value. Effected environment: All IDPrime based devices and any of the following mechanisms: CKM_SHA1_RSA_PKCS_PSS, CKM_SHA256_RSA_PKCS_PSS, CKM_SHA384_RSA_PKCS_PSS and CKM_SHA512_RSA_PKCS_PSS. **Workaround:** On IDPrime based devices, use the PSS parameters with the salt length equal to the hash length.

Issue	Severity	Synopsis
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. **Workaround:** Disable SingleLogon by adding the process name (vmware-view.exe) to the registry and set SingleLogon to 0. (Refer to 'Defining a Per Process Property' in the *SafeNet Authentication Client Administrator Guide*).
ASAC-10608	M	**Summary:** 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. **Workaround:** None (this is the card's expected behavior)
ASAC-9288	M	**Summary:** By default, the retry counter cache causes the following problem in SAC: when switching the card between different machines, the true retry counter is not shown until it is changed on the current machine and the cache is updated. **Workaround:** Add the property `RetryCountCached=0` under the [General] section: `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. **Workaround:** Disable the Multi-slot support property. See the SAC Administrator Gudie for more information.
ASAC-8267	M	**Summary:** A Digital Signature PIN operation fails if the Digital Signature PIN (Role#3) and Digital Signature PUK (Role#4) have different PINPad configurations (PIN Type and Extended PIN Flags). **Workaround:** Ensure that the Digital Signature PIN (Role#3) and Digital Signature PUK (Role#4) have the same PINPad configuration.
ASAC-7969	M	**Summary:** Using the eToken Pro (no hash on-board functionality) and eToken 5110 FIPS (both hash and sign functionalities on-board) device when there are two or more threads running two PKCS#11 sessions in the same application, the signing operation fails. **Workaround:** Peform either one of the following: > Update the application to use the hash off-board mechanism and then perform the RSA operation with the token. > Update the application to synchronize between threads - make the `C_SignInit - C_SignUpdate - C_SignFinal` a solid block. > If there is no option to update the application, enable the hash offboard property: **'HashOffboard'** in SAC. This allows SAC PKCS#11 to perform the hash off-board instead of the token.

Issue	Severity	Synopsis
ASAC-7932	M	**Summary:** Changing the PIN on Firefox using the CT710 PIN Pad does not work. **Workaround:** Change the PIN using SAC Tools or SAC tray icon.
ASAC-7849	M	**Summary:** When ClassicClient and SAC are installed side-by-side propagation is done via regtool only. **Workaround:** None.
ASAC-7602	M	**Summary:** An error occurred after a banner was added to the SAC Customization Tool, followed by the generation of an MSI file. **Workaround:** Run the Customization Tool as an Administrator.
ASAC-7228	M	**Summary:** When connecting a .net smart card to the reader on a Windows OS with SAC installed, the `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards] registry changed` From: Smart Card Key Storage Provider=SafeNet Smart Card Key Storage Provider To: Smart Card Key Storage Provider=Microsoft Smart Card Key Storage Provider **Workaround:** Uninstall SAC or use the repair option by going to Control Panel > Add Remove Programs.

Issue	Severity	Synopsis
ASAC-6788 ASAC-2429	M	**Summary:** Performing a remote desktop connection from a system which has Minidriver installed, to a system with SAC installed, causes RDP errors after entering the smart card PIN. **NOTE** This is the default behavior of the RDP, when the CredSSP protocol is used during an RDP session, and when the CSP names differ on a client and a server. https://winprotocoldoc.blob.core.windows.net/productionwindowsarchives/MS-CSSP/[MS-CSSP].pdf|https://winprotocoldoc.blob.core.windows.net/productionwindowsarchives/MS-CSSP/%5bMS-CSSP%5d.pdf CSP name is passed from the client to the server during the CredSSP handshake, which is why the first attempt fails, but the second one succeeds because it uses the CSP name that's local to the server. For more information, refer to the official document: 2.2.1.2.2 TSSmartCardCreds. **Workaround:** 1. Upgrade the RDP version on the machine. 2. Edit the RDP file (on the Client) by following these steps: a. Open the Remote Desktop connection window. b. Click Show Options. c. Under Connection Settings, click Save as, and save the RDP file locally. d. Open the file using Notepad. e. Add enablecredsspsupport:i:0 at the end of the RDP file and then save the file. f. Connect to the server using the edited RDP file. For more details, refer to: > https://support.microsoft.com/en-us/kb/941641 > https://technet.microsoft.com/en-us/library/ff393660(v=ws.10).aspx
ASAC-6585	M	**Summary:** When using PKCS#11 mechanisms CKM_SHA256_RSA_PKCS (eToken 5110 GA and FIPS) and CKM_SHA1_RSA_PKCS (eToken 5110 GA), and the data hashing is done on-board. The on-board hashing causes the process to slow down and possible failure in multi-threading implementations. **Workaround:** > Use separate hashing and signing mechanisms. > Synchronize multi-threading implementations. > Define a new DWORD32 with the name "HashOffboard" and value = 1 under `HKLM\Software\SafeNet\Authentication\SAC\Crypto`. This enables SAC to perform off-board hashing instead of on-board.

Issue	Severity	Synopsis
ASAC-6344	M	**Summary:** Generating an msi file when the My Documents folder is redirected to the network does not work. **Workaround:** Create a folder named Documents under \Users%username%.
ASAC-6214	M	**Summary:** VMView client may not work properly with SAC when using a smart card certificate. **Workaround:** Install SAC before installing the VMView Client.
ASAC-6191	M	**Summary:** IDPrime smart cards cannot sign plain data longer than 36 bytes for RSA or ECC keys. **Workaround**: None
ASAC-6098	M	**Summary:** 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. **Workaround:** This is Windows default 'Power Saving' mode. This feature sends the Power Off command (63 00 00 …) to the reader after about 20-30 seconds after any transaction to the smart card is completed. Configure the following registry key to change the delay period in seconds: `CardDisconnectPowerDownDelay in HK_local_machine\software\microsoft\cryptography\calais` http://opensc.1086184.n5.nabble.com/smart-card-reset-after-5-seconds-on-Windows-td15563.html.
ASAC-6079	M	**Summary:** Windows 10 (1709) crashes when verifying SafeNet Drivers using the Microsoft Windows Driver Verifier tool. **Workaround:** Use the CCID drivers (without installing eToken drivers).
ASAC-6058	M	**Summary:** Performing smart card authentication to the WiFi network on Windows 10 (1709) was not possible as the smart card logon window was not displayed. **Workaround:** Install Microsoft KB 4089848. (Customer ID: CS0514040, CS0543595)
ASAC-5815	M	**Summary:** When working with a token or a PIN pad reader on a VM Workstation, the token might be unrecognized when selecting the "Shared" device in VM > Removable Devices menu. **Workaround:** Connect the device that is not under the "Shared" devices list in order to work with the eToken/reader device.
ASAC-5343	M	**Summary:** When using a PIN Pad reader with the Smart Card initialized with the 'Must change password' flag enabled, and the password is changed on the same machine, the user may encounter an issue and receive an "Incorrect password" message. The issue will not occur if the card is initialized on one machine and the password is changed on another. **Workaround:** Delete the cache folder (C:\Windows\Temp\eToken.cache) after initialization and before changing the password.

Issue	Severity	Synopsis
ASAC-5306	M	**Summary:** When trying to log onto a locked device, two messages are shown instead of one. **Workaround:** Close both windows.
ASAC-5201	M	**Summary:** When connecting a non-Pin Pad reader, an incorrect message is displayed in the event viewer. **Workaround:** To disable Pin Pad support, create a REG_DWORD value called "NoPinPad" under the key `HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC\General` and set its value to 1. On 64-bit machines, you additionally need to do the same under the key: `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. **Workaround:** Make sure you create a new configuration with the same settings in the current SAC version.
ASAC-4504	M	**Summary:** When rebooting a PC after placing an IDPrime 3811 MD contactless card on a reader, the following error message appears: “No valid certificates were found on this smart card….”. **Workaround:** Remove the card and then place it back on the reader, the certificate will be seen, and may be used.
ASAC-4497	M	**Summary:** When Configuring the Maximum Password Usage value to a value other than zero (0), the password will expire a day later than was defined. For example: set it to 166 days, SAC will show 167 days. **Workaround:** None.
ASAC-4141	M	**Summary:** During the unblock operation, no other application can access the device until the unblock operation is finished or canceled. **Workaround:** None.
ASAC-4116	M	**Summary:** When entering an incorrect Digital Signature PIN while enrolling a CC Certificate onto a CC device in unlinked mode, the enrollment process fails. **Workaround:** Retry enrolling the certificate with the correct Digital Signature PIN.
ASAC-4024	M	**Summary:** When unlocking a Common Criteria device (that’s in linked mode) via SAC Tools and an incorrect Challenge Response is sent, a general error message is received. **Workaround:** None.
ASAC-2653	M	**Summary:** When working with a token on VM Workstation, the token might be unrecognized when selecting the "Shared" device in VM > Removable Devices menu. **Workaround:** Connect the device that is not under the "Shared" devices list in order to work with the eToken device.

Issue	Severity	Synopsis
ASAC-2284	M	**Summary:** When a user attempts to generate a customized SAC msi file with no administrator privileges, the process fails. **Workaround**: Create customized SAC msi file with administrator privileges.
ASAC-2146	M	**Summary:** The process of creating a signed customized MSI with the Customization Tool takes a while. **Workaround:** Wait for the process to end.
ASAC-1740 ASAC-2262	M	**Summary:** Scenario 1 - When using jarsigner.exe to sign JAR files, the jarsigner command fails to respond for a while. Scenario 2 - When performing an Identrust enrollment on Windows Server 2008, Windows 7 or Windows Server 2008 R2, the enrollment fails. **Cause:** 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. **Workaround:** Download the following two hotfixes from Microsoft: Local Scenario: http://support.microsoft.com/kb/2427997 RDP: http://support.microsoft.com/kb/2521923
ASAC-1722	M	**Summary:** When running the repair option from the MSI file wizard, the operation fails. **Workaround:** Use the repair option by going to Control Panel > Add Remove Programs.
ASAC-1702	M	**Summary:** When the application runs as a service without the Local System Account permissions, smart card communication fails. **Workaround:** Make sure the service runs with the Local System Account permissions by adding it manually. This is a Microsoft by-design known issue. For more details refer to the following Microsoft support ticket number: 114092811845001.
ASAC-819	M	**Summary:** When the MS KB http://support.microsoft.com/kb/2830477 is installed in a Windows 7 environment, you are prompted for the token password when you start the RDP. But after entering the remote machine, you are prompted for the standard user name and password. **Workaround:** Uninstall the MS KB.
ASAC-378	M	**Summary:** Smart card logon is not supported by default when using tokens with ECC certificates. **Workaround:** Perform the following: In the Local Group Policy Editor, under Local Computer Policy\Administrative Templates\Windows Components\Smart Card, enable Allow ECC certificates to be used for logon and authentication.

Issue	Severity	Synopsis
ASAC-277 ASAC-525	M	**Summary:** The SAC installation does not load the PKCS#11 module for 32-bit Firefox on a 64-bit OS. **Workaround:** Use 64-bit Firefox, or load the 32-bit PKCS#11 module manually from the System32 folder.
SACINT-38	M	**Summary:** Unable to sign a Word document via Office 365 (Office on Demand) using SAC. **Workaround:** Open the saved document from the local machine itself. This enables you to sign the document successfully.
ASAC-11149	M	**Summary:** VPN fails using IDPrime 930 L3 (with KSP SHA2 certificate) cards. **Workaround:** None.
ASAC-13750	M	**Summary:** DLL (`SACUI.cs-Cz.dll`) missing when upgrading SAC Typical from 10.2 to 10.8 R6. **Workaround:** Firstly, upgrade SAC Typical from 10.2 to 10.8 R5. Thereafter, upgrade SAC Typical from 10.8 R5 to 10.8 R6.

Known Limitations

Issue	Severity	Synopsis
ASAC-12144	H	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*.
ASAC-8203	M	After connecting and using an IDPrime 3811 device (on a contactless reader) the smart card was not recognized (loss of identification).
ASAC-7318	M	On IDPrime MD cards, only CA private certificate objects are supported.
ASAC-6261	M	The profile whereby a PUK replaces the Admin Key does not support initializing a device.
ASAC-4872	M	IDPrime MD 840 and eToken 5110 CC do not support history size of Password Quality.
ASAC-4531	M	IDPrime MD 830B (applet 4.3.5) FIPS L3 does not support RSA 1024, ECC signing with SHA1 algorithms, as per FIPS/NIST regulations.

Issue	Severity	Synopsis
ASAC-4363	M	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.
ASAC-4081	M	SafeNet eToken 5110 FIPS does not support RSA 1024 and SHA1 on board, as per FIPS/NIST regulations.
ASAC-3980	M	SafeNet Authentication Client does not support RSA 3072 and 4096 on IDPrime MD, .NET and eToken devices. SafeNet Authentication Client does not support Single Sign On with IDPrime .NET and IDPrime MD cards via PKCS#11 API interface. For more information, refer to the smart card specification guide.
ASAC-3769	M	The following PIN pad limitations exist: > SC Logon using the PIN Pad via eToken CSP is not supported. The PIN is entered via the keyboard. Customers can use SafeNet Minidriver to logon via the PIN Pad. > 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.
ASAC-2320	M	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).

Product Documentation

The following product documentation is associated with this release:

- 007-013560-005_SafeNet Authentication Client 10.8-R6 Windows GA Administrator Guide
- 007-013561-005_SafeNet Authentication Client 10.8-R6 Windows GA User 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.