SafeNet Authentication Client

RELEASE NOTES

Version:	10.7 – Windows (GA)
Build	167
Issue Date:	April 2019
Document Number:	007-013559-007 Rev E

Contents

Product Description 3
Release Description 3
New Features and Enhancements 3
Advisory Notes 3
Licensing 3
SafeNet Authentication Client Certification 4
Default Password 4
    Password Recommendations 4
    Initialization Key Recommendations 4
Compatibility Information 5
    Browsers 5
    Operating Systems 5
Hardware and Screen Resolution Requirements 5
Tokens 5
        Certificate-based USB Tokens 5
        Software Tokens 5
        Smart Cards 6
        Smart Cards and Tokens that Support Common Criteria 7
        Smart Cards and Tokens that Support ECC Certificates 7
        External Smart Card Readers 7
        End-of-Sale Tokens/Smart Cards 8
        End-of-Life Tokens/Smart Cards 8
Localizations 9
Compatibility with Gemalto Applications 9
Compatibility with Third-Party Applications 10
Installation and Upgrade Information 11

Installation 11
Upgrade 11
Resolved Issues 11
Known Limitations 12
Known Issues 13
Known Issues – Deprecated Devices 19
Product Documentation 20
Support Contacts 20

Product Description

SafeNet Authentication Client 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 10.7 (GA) includes support for the IDPrime Virtual Smart Card Solution as well as bug fixes.

New Features and Enhancements

SafeNet Authentication Client 10.7 (GA) offers the following new features:

- Support for Optelio R7 Smart Card with SAC PKCS#11.
- Support for SafeNet IDPrime Virtual Smart Card - this Smart Card emulates the functionality of a physical smart card. The SafeNet IDPrime Virtual Solution offers comparable security benefits to physical smart cards by using Client/Server technology. For more details, see the SafeNet IDPrime Virtual Solution Guide.
- SAC Event Viewer logs – Microsoft Event Viewer logs are supported for user authentication operations.
- Bug fixes - this release includes bug fixes from previous SAC versions.

Advisory Notes

- In order to comply with best security practices, Linked Mode is no longer enabled by default in SAC 10.6 and above. To enable it, refer to the SafeNet Authentication Client Administrator Guide (LinkMode property). We strongly advise that Linked Mode be used only with the new IDPrime 940 smart card, which is fully supported by SAC.
- If the PKCS#11 module is not added to the Firefox security settings after installing SAC 10.7, add it manually.

Licensing

The use of this product is subject to the terms and conditions as stated in the End User License Agreement. A valid license must be obtained from the SafeNet License Center: https://lc.cis-app.com/.

SafeNet Authentication Client Certification

SafeNet Authentication Client 10.7 (GA) has the following certification:

- Citrix Ready
  https://citrixready.citrix.com/gemalto/gemalto-safenet-authentication-client.html
- SafeNet Authentication Client 10.7 (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, see the SafeNet Authentication Client Compatibility Guide - Using SafeNet Authentication Client with Windows Defender Credential Guard.

Default Password

SafeNet eToken devices are supplied with the following default token password: 1234567890**.**

IDPrime cards are supplied with the following default token password: “0000” (4 digits). The administrator password must be entered using 48 hexadecimal zeros (24 binary zeros).

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

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

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 (See the SafeNet Authentication Client User Guide for more details on the Friendly Admin Password)
- Digital Signature PUK, when using a friendly name, should include at least 16 characters of different types.

> **NOTE:** Character types include upper case, lower case, numbers, and special characters. For more information see the ‘Configuration Recommendations’ section in Chapter 3 - SAC Secured Environment (Configure restrictive password policies) of the SafeNet Authentication Client Administrator Guide.

Initialization Key Recommendations

We strongly recommend changing the Initialization Key using either one of the following methods:

- The customization process (CPB)
- The SAC Initialization process (See the SafeNet Authentication Client User Guide for more details on Initialization Key settings)

Compatibility Information

Browsers

SafeNet Authentication Client 10.7 (GA) Windows supports the following browsers:

- Firefox 65
- Internet Explorer 11.195.17763.0
- Chrome version 73
- Microsoft Edge 44.18262.1000.0

Operating Systems

SafeNet Authentication Client 10.7 (GA) Windows supports the following operating systems:

- Windows Server 2008 R2 SP1 (32-bit, 64-bit)
- Windows Server 2008 SP2 (32-bit, 64-bit)
- Windows Server 2012 and 2012 R2 (64-bit)
- Windows Server 2016 (64-bit)
- Windows 7 SP1 (32-bit, 64-bit)
- Windows 8 (32-bit, 64-bit)
- Windows 8.1 (32-bit, 64-bit)
- Windows 10 (32-bit, 64-bit) up to and including Redstone 5 (1809)

Hardware and Screen Resolution Requirements

Required hardware:

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

Tokens

SafeNet Authentication Client 10.7 (GA) supports the following devices:

Certificate-based USB Tokens

- SafeNet eToken 5300
- SafeNet eToken 5110
- SafeNet eToken 5110 CC
- SafeNet eToken 5110 FIPS

Software Tokens

- SafeNet Virtual Token
- SafeNet Rescue Token

Smart Cards

- SafeNet IDPrime Virtual Smart Card
- SafeNet IDPrime 940
- SafeNet IDPrime 3940

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 will be supported by the following readers only:
  - Gemalto IDBridge CL 3000 (ex Prox-DU)
  - Advanced Card System ACR 1281U

- Gemalto IDCore 30B eToken
- Gemalto IDPrime MD 840
- Gemalto IDPrime MD 840 B
- Gemalto IDPrime MD 3840
- Gemalto IDPrime MD 3840 B
- Gemalto IDPrime MD 830-FIPS
- Gemalto IDPrime MD 830-ICP
- Gemalto IDPrime MD 830 B
- Gemalto IDPrime MD 3810
- Gemalto IDPrime MD 3811
- Gemalto IDPrime MD 8840 (8GB) Micro SD card
- Gemalto IDPrime .NET (only SAC PKCS#11 and IDGo 800 Minidriver interfaces)
- Ezio PKI card
- Optelio R7

NOTE: For more information on IDPrime MD Smart Cards, see the IDPrime MD Configuration Guide.

Smart Cards and Tokens that Support Common Criteria

- Gemalto IDPrime MD 840
- Gemalto IDPrime MD 840 B
- Gemalto IDPrime MD 3840
- Gemalto IDPrime MD 3840 B
- Gemalto IDPrime MD 8840 Micro SD Card
- IDPrime 940
- SafeNet eToken 5110 CC

Smart Cards and Tokens that Support ECC Certificates

ECC Certificates are supported by eTokens and Gemalto IDPrime MD cards.

The following devices support ECC Certificates:

- SafeNet eToken 5110
- Gemalto IDPrime MD 830-FIPS
- Gemalto IDPrime MD 830-ICP
- Gemalto IDPrime MD 830 B
- Gemalto IDPrime MD 3810
- Gemalto IDPrime MD 3810 MIFARE 1K
- Gemalto IDPrime MD 3811

External Smart Card Readers

SafeNet Authentication Client 10.7 (GA) supports the following smart card readers:

- Gemalto IDBridge K30
- Gemalto IDBridge K50
- Gemalto IDBridge CT30
- Gemalto IDBridge CT40

NOTE: SC Reader drivers must be compatible with the extended APDU format in order to be used with RSA-2048 (relevant to SafeNet eToken 4100).

Secure PIN Pad Readers:

SafeNet Authentication Client 10.7 (GA) supports the following PIN pad readers:

- Gemalto IDBridge CT700

NOTE: The Secure PIN Pad readers listed above are subject to limitations. Certain readers may not fully support all Smartcards. See the Administrator Guide for full details of supported Smartcard and PIN Pad reader combinations.

End-of-Sale Tokens/Smart Cards

- SafeNet Reader CT1100
- SafeNet Reader K1100

End-of-Life Tokens/Smart Cards

- SafeNet eToken PRO 32K v4.2B
- SafeNet eToken PRO 64K v4.2B
- SafeNet eToken Pro SC 32K v4.2B
- SafeNet eToken Pro SC 64K v4.2B
- SafeNet eToken 7100 (SafeNet eToken NG-Flash)
- SafeNet iKey: 2032, 2032u, 2032i (Windows and Mac only)
- SafeNet smart cards: SC330, SC330u, SC330i
- SafeNet eToken 5000 (iKey 4000)
- SafeNet eToken 4000 (SC400)
- SafeNet eToken PRO Java 72K
- SafeNet eToken PRO Java 72K ECC
- SafeNet eToken PRO Anywhere
- SafeNet eToken PRO Smartcard 72K
- SafeNet eToken 5100/5105
- SafeNet eToken 5100 CC
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID
- SafeNet eToken 4100
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)
- SafeNet eToken 7300
- SafeNet eToken 7300-HID
- Gemalto IDBridge CL 3000 (ex Prox-DU)
- Gemalto IDBridge CT710
- Ezio Shield Pro
- Ezio Bluetooth Reader
- Ezio BLE

NOTE: SafeNet HID tokens are not compatible with Smart Card Logon and CAPI based VPN applications.

Localizations

SafeNet Authentication Client 10.7 (GA) Windows supports the following languages:

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

NOTE:

- When using IDPrime MD, .Net cards and eToken 5110 CC, the user PIN and Admin PIN can be in English only.
- IDPrime features are available in English localization only (e.g. Initializing Common Criteria devices and PIN Pad functionality).

Compatibility with Gemalto Applications

IDPrime MD cards can be used with the following products:

- SafeNet Authentication Service (SAS) / SafeNet Trusted Access (STA)
- Gemalto Bluetooth Device Manager (GBDM V4.0.3.2)
- IDGo 800 Credential Provider (V1.2.4)
- IDPrime User Tool for Windows (V1.2.0)
- IDGo 800 Cert Tool (V 1.0.7)
- WebSigner (V1.3.0)

NOTE: To work with SAC 10.7 (GA) and WebSigner, ensure that you have WebSigner V1.3 in order to be compliant with SAC binary signature validity.

To work with these products, install SafeNet Minidriver profile by generating an .msi file using the SAC Customization Tool. See the SafeNet Authentication Client 10.7 (GA) Administrator Guide for more details on how to generate the MSI installation file.

SafeNet Authentication Client can be used with the following products:

- SafeNet Authentication Manager 9.0 SP3 (Gemalto IDPrime MD 840/3840/940/3940 and .Net devices are not supported on this version of SAM).

Compatibility with Third-Party Applications

Most of the third-party applications listed below have been validated and tested with SafeNet Authentication Client 10.7 (GA).

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 10.8
	Microsoft	MIM 2016 4.5.286.0 (Supported with SAC Minidriver profile)
	vSEC:CMS	vSEC:CMS 5.4 (SafeNet eToken 5110 FIPS is not supported)
	IDnomic	OpenTrust CMS 5.2
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 9.2
	Adobe	Reader XI and DC
	Microsoft	Outlook 2016 / Office 365
	Mozilla	Thunderbird 52.9.1

Installation and Upgrade Information

Installation

SafeNet Authentication Client 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 SafeNet Authentication Client.

Upgrade

For earlier versions of SafeNet Authentication Client, 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 SafeNet Authentication Client.

Gemalto customers migrating from IDGo 800 must uninstall their version of IDGo 800 and install SafeNet Authentication Client 10.7 (GA).

For more Installation and Upgrade details, see the SafeNet Authentication Client 10.7 (GA) Administrator Guide.

NOTE: To upgrade SAC 10.5 (installed on Windows x32 OS via the Customization Tool) with SafeNet Minidriver, SAC 10.5 must be uninstalled before installing SAC 10.7.

Resolved Issues

Issue	Synopsis
ASAC-8782	When key pair was generated using Java 8 application with an empty private key template, the operation failed with a `CKR_ARGUMENTS_BAD` error. Improvements were made to the `PKCS#11 function C_GenerateKeyPair` to support the empty private key template. (Customer ID: CS0882583)
ASAC-8698 ASAC-7628	Changing the User PIN and Digital Signature PIN while preconfigured as 'Must Change Password on first Logon' on IDPrime MD 840 failed using the Gemalto IDBridge CT710. Customer ID: CS0879202, CS0844905
ASAC-7827	SAC Installer did not register the ETPKCS11 provider automatically.
ASAC-7542	Garbage characters were displayed when entering the Password Policy Description in Japanese. (Customer ID: CS0829870)
ASAC-4469	When aborting an import certificate operation (in the middle of the process) while working with a Pin Pad reader, SAC Tools ignored the request to abort and continued with the import certificate operation.

Known Limitations

Issue	Synopsis
ASAC-7318	On IDPrime MD cards, only CA private certificate objects are are supported. Furthermore, the object must be created as private, as we do not support changing from public to private. These limitations are compeled by backward compatibility with IDPrime card file structure, that was optimized for minidriver.
ASAC-6261	**Summary:** The profile whereby a PUK replaces the Admin Key does not support initializing a device. **Workaround:** None.
ASAC-4872	IDPrime MD 840 and eToken 5110 CC do not support history size of Password Quality.
ASAC-4531	IDPrime MD 830B (applet 4.3.5) FIPS L3 does not support RSA 1024, ECC signing with SHA1 algorithms, as per FIPS/NIST regulations.
ASAC-4363	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	SafeNet eToken 5110 FIPS does not support RSA 1024 and SHA1 on board, as per FIPS/NIST regulations.
ASAC-3980	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.
ASAC-3769	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. • Common Criteria Linked mode (not supported) A security contradiction exists whereby the PIN pad provides high protection, but linked mode reduces the security. • 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	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).

Known Issues

Issue	Synopsis
ASAC-8923	**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	**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	**Summary:** Using the eToken Pro (no hash on-board functionality) and eToken 5110 FIPS (both hash and sign functionalities on-board) device when there are two or more threads running two PKCS#11 sessions in the same application, the signing operation fails. **Workaround:** Peform either one of the following: • Update the application to use the hash off-board mechanism and then perform the RSA operation with the token. • Update the application to synchronize between threads - make the `C_SignInit` – `C_SignUpdate` - `C_SignFinal` a solid block. • If there is no option to update the application, enable the hash offboard property: '**HashOffboard**' in SAC. This allows SAC PKCS#11 to perform the hash off-board instead of the token.
ASAC-7932	**Summary:** Chaning the PIN on Firefox using the CT710 PIN Pad does not work. **Workaround:** Change the PIN using SAC Tools or SAC Monitor.
ASAC-7849	**Summary:** When ClassicClient and SAC are installed side-by-side propagation is done via regtool only. **Workaround:** None.
ASAC-7602	**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	**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	Synopsis
ASAC-6788 ASAC-2429	**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, 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 please 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: • Open the Remote Desktop connection window. • Click **Show Options**. • Under **Connection Settings**, click **Save as**, and save the RDP file locally. • Open the file using Notepad. • Add **enablecredsspsupport:i:0** at the end of the RDP file and then save the file. • Connect to the server using the edited RDP file. For more details, see: https://support.microsoft.com/en-us/kb/941641 https://technet.microsoft.com/en-us/library/ff393660(v=ws.10).aspx
ASAC-6585	**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.
ASAC-6344	**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-6310	**Summary:** When a user's IDPrime 830 4.3.5 L2 card is locked on Windows 7 x64, the card remains locked even after performing a badge unlock operation. **Workaround:** Delete the cache folder.

Issue	Synopsis
ASAC-6214	**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	**Summary:** IDPrime smart cards cannot sign plain data longer than 36 bytes for RSA or ECC keys. **Workaround:** None
ASAC-6098	**Summary:** When SAC (with IDGo 800 compatible custom installation) 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	**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	**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	**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	**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.
ASAC-5306	**Summary:** When trying to log onto a locked device, two messages are shown instead of one. **Workaround:** Close both windows.

Issue	Synopsis
ASAC-5201	**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-4950	**Summary**: When an incorrect token password is entered on Metro IE: • The "Incorrect Token Password" message is not displayed. • The retries counter is decreased by 1. • The Token Logon window remains displayed. **Workaround**: If the **Token Logon** window remains displayed after a token password is submitted, assume that the password entered was incorrect. You can use SAC Tools to see the number of remaining retries.
ASAC-4516	**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	**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	**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	**Summary:** During the unblock operation, no other application can access the device until the unblock operation is finished or canceled. **Workaround:** None.
ASAC-4116	**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	**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**.**

Issue	Synopsis
ASAC-3451 ASAC-2278 ASAC-2221 ASAC-1675	**Summary:** Upgrading from previous versions to SAC 10.4 (while a token is connected with Smart Card Logon, MS certificate or SNL profile), caused the session to lock the upgrade process automatically and the upgrade process to fail. **Workaround:** Run the following command to upgrade from previous SAC versions to SAC 10.4: `msiexec /i C:\SafeNetAuthenticationClient-x32-10.4.msi PROP_FAKEREADER=128`
ASAC-3449	**Summary**: When generating an MSI file using the SAC Customization Tool, the eToken.dll file is run over by the eTokenMD.dll when selecting IDGO 800 Minidriver. **Workaround**: Select eToken CSP\KSP provider when using eToken Devices.
ASAC-3112	**Summary**: The SAC token login window on IE11 freezes when the Enhanced Protected Mode feature is on. **Workaround**: Move the mouse cursor to the window and click inside the text box, or disable the Enhanced Protected Mode feature.
ASAC-2653	**Summary:** When working with a token on VM Workstation, the token might be unrecognized when selecting the "Shared" device in **VM > Removable Devices** menu. **Workaround:** Connect the device that is not under the "Shared" devices list in order to work with the eToken device.
ASAC-2299	**Summary:** SafeNet Virtual devices that are locked to flash, and were enrolled on SafeNet Authentication Manager using a USB 3 port, cannot function on a USB 2 port, and vice versa. **Workaround:** If the SafeNet Virtual Token was enrolled on a USB 3 port, then use the token on a USB 3 port only. If the SafeNet Virtual Token was enrolled on a USB 2 port, then use the token on a USB 2 port only.
ASAC-2298	**Summary:** Connection problems occur when SafeNet Virtual devices are locked to flash and enrolled on a VMware environment. **Workaround:** When using a SafeNet Virtual device that is locked to flash, make sure the device is enrolled on a regular environment and not VMware.
ASAC-2295	**Summary:** SAC 9.0 does not support legacy GA configuration profiles. **Workaround:** Create new profiles using SAC 9.0 Customization Tool.
ASAC-2284	**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	**Summary:** The process of creating a signed customized MSI with the Customization Tool takes a while. **Workaround:** Wait for the process to end.
ASAC-1992	**Summary:** Repartitioning the eToken 7300 device with a token password configured with **Maximum usage period** and **Expiration warning period**, the repartition process fails. **Workaround:** Initialize the token.

Issue	Synopsis
ASAC-1740 ASAC-2262	**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	**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	**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-1470	**Summary:** After updating the FW on an eToken 7300, the FW version might not be updated under Token information in SAC Tools. **Workaround:** Restart the machine.
ASAC-1419	**Summary:** When installing SAC via the GPO, SAC is installed successfully on the client computer but the tray icon doesn't appear. **Workaround:** Restart the client computer.
ASAC-1335	**Summary:** Mass storage options using an eToken 7300 protected token are not supported within an RDP session. **Workaround:** None.
ASAC-862	**Summary:** When a partitioned eToken 7300 device is connected, the SafeNet drive eToken 7300 icon is displayed on the desktop but double-clicking it does not open the device's drive. **Workaround:** Open the drive from the computer's directory window.
ASAC-819	**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.

Issue	Synopsis
ASAC-800	**Summary:** If the token was initialized as Common Criteria: • The Challenge Code created during the Unlocking procedure is 13 characters, not 16 characters as expected. • The Response Code created during the Unlocking procedure is 39 characters, not 16 characters as expected. **Workaround:** When unlocking a CC token, the user must be sure to copy the entire **Response Code** string.
AHWENG - 775	**Summary:** When a protected eToken 7300 is connected with the flash partition accessible, the flash partition may not be accessible after returning from sleep mode. **Workaround:** Disconnect and reconnect the device.
ASAC-446	**Summary:** SAC interfered with Citrix's debugging application. **Workaround:** Use Citrix' "Hotfix Rollup Pack 2 for Citrix XenApp 6.5 for Microsoft Windows Server 2008 R2", found at http://support.citrix.com/article/CTX136248.
ASAC-378	**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**.
ASAC-281	**Summary:** Upon successful eToken 7300 partitioning, a Microsoft Windows message opens prompting you to format the disk. **Workaround:** Click **Cancel** to close the message window.
ASAC-277 ASAC-525	**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	**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.

Known Issues – Deprecated Devices

Issue	Synopsis
ASAC-4326	**Summary:** The iKey reader is not installed when upgrading to SAC 10.4. **Workaround:** Uninstall SAC and re-install SAC 10.4.
ASAC-1315	**Summary:** When working with SafeNet smart cards SC330u, iKey 2032u, SC400, and iKey 4000 using SAC Tools, the number of unblocking code retries remaining cannot be changed , unless the token or smart card are locked. (i.e. there is no way of determining how many unblocking code retries remain). **Workaround:** None. This is by design.

Product Documentation

The following product documentation is associated with this release:

- 007-013560-005_SafeNet Authentication Client 10.7 Windows (GA) Administrator Guide - Rev C
- 007-013561-005_ SafeNet Authentication Client 10.7 Windows (GA) User Guide - Rev C

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 make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto 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 Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information
Customer Support Portal	https://supportportal.gemalto.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.
Technical Support contact email	technical.support@gemalto.com