SafeNet Authentication Client

CUSTOMER RELEASE NOTES

Version:	10.2 – Windows (GA)
Build	19
Issue Date:	December 2016
Document Number:	007-013559-003

Contents

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 10.2 introduces support for PIN pad readers as well as Gemalto IDPrime MD 3811 cards.

Administrators and users can use and manage IDPrime MD smart cards seamlessly via the standard PKCS#11 or Microsoft CSP/KSP interface. For more details on the specific list of IDPrime cards and administrator functionalities supported, see the SafeNet Authentication Client 10.2 Administrator Guide.

New Features and Enhancements

SafeNet Authentication Client 10.2 offers the following new features:

- **Support for PIN Pad**
  (See External Smart Card Readers on page 7 for a list of supported PIN Pad readers)
- **Support for Gemalto IDPrime MD 3811 (applet 4.1.3)**
- **Bug fixes** – this release includes bug fixes from previous SAC versions.

Advisory Notes

- Currently, **only** domain credentials are protected by Microsoft Credential Guard. Entering a smart card PIN is not supported at this stage. This is a Microsoft limitation.
- Some contactless readers are not fully compliant with PC/SC v2.0. They do not work properly with the most recent smartcards e.g. the Advanced Card System ACR 122 reader is not compatible with IDPrime MD 3811 and with the DESFire EV1, due to a gap in the PC/SC v2.0 standard.
- To use RSA SHA2 for cryptographic operations, the SafeNet KSP provider must be installed. See the SafeNet Authentication Client 10.2 User Guide for details on how to set a KSP certificate.
- EZIO Shield PRO reader does not support Secure Messaging (SM) protected operations such as import key pair, generate key pair and change administrator key.

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/.

NOTE: Using the Gemalto IDGo 800 Minidriver as a standalone component does not require SAC licensing.

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)

We strongly recommend to change all device passwords upon receipt of a token/card.

Compatibility Information

Browsers

SafeNet Authentication Client 10.2 Windows supports the following browsers:

- Firefox (up to and including version 50)
- Internet Explorer (up to and including version 11 and Metro)
- Microsoft Edge 38.14393.0.0 and 25.10586.672.0 (does not support certificate enrollment)
- Chrome version 54, for authentication only (does not support certificate enrollment)

Operating Systems

SafeNet Authentication Client 10.2 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 Vista SP2 (32-bit, 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)

Tokens

SafeNet Authentication Client 10.2 supports the following tokens:

Certificate-based USB Tokens

- SafeNet eToken 5110
- SafeNet eToken 5110 CC
- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 FIPS HID
- SafeNet eToken 5110 HID

Certificate-based Hybrid USB Tokens

- SafeNet eToken 7300
- SafeNet eToken 7300-HID

Software Tokens

- SafeNet Virtual Token
- SafeNet Rescue Token

Smart Cards

- 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 .NET (only SAC PKCS#11 and IDGo 800 Minidriver interfaces)

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

End-of-Sale Tokens/Smart Cards

- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID
- SafeNet eToken 4100
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)

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

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 Anywhere
- SafeNet eToken PRO Smartcard 72K

External Smart Card Readers

SafeNet Authentication Client 10.2 supports the following smart card readers:

- Gemalto IDBridge K30
- Gemalto IDBridge K50
- Gemalto IDBridge CT30
- Gemalto IDBridge CT40
- Gemalto IDBridge CL 3000 (ex Prox-DU)
- SCR 3310 v2 Reader
- Athena AESDrive IIIe USB v2 and v3
- Advanced Card System ACR 1281U
- Athena Keyboard
- Omnikey 3121
- Dell Broadcom (This reader is found only in laptops)
- Unotron

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).

Mobile PKI Bluetooth Readers:

- SafeNet Reader CT1100
- SafeNet Reader K1100

Secure PIN Pad Readers:

SafeNet Authentication Client 10.2 supports the following PIN pad readers:

- Gemalto IDBridge CT700
- Gemalto IDBridge CT710
- Ezio Shield Pro
- Ezio Bluetooth Reader
- Ezio BLE

Tablets

- Lenovo ThinkPad Tablet running Windows 8.
- Microsoft Surface Pro 4 running Windows 8.1 and Windows 10.

Localizations

SafeNet Authentication Client 10.2 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. Iinitializing Common Criteria devices and PIN Pad functionality).

Compatibility with Gemalto Applications

IDPrime MD cards can be used with the following products:

- IDGo 800 Credential Provider (V1.2.4)
- IDGo 800 User Tool for Windows (V1.1.30)
- IDGo 800 Cert Tool (V1.0.5)
- IDGo 800 Minidriver (V1.2.8) (dll - v8.5.0.5)

To work with these products, install IDGo 800 Minidriver by generating an .msi file using the SAC Customization Tool. See the SafeNet Authentication Client 10.2 Administrator Guide for more details on how to generate the MSI installation file.

SafeNet Authentication Client can be used with the following products:

- SafeNet Network Logon 8.3
- SafeNet Authentication Manager 8.2 with Hotfix 158.749 (Gemalto IDPrime MD 840 / 3840 and .Net devices are not supported on this version of SAM).

Installing SAC with eToken SafeNet Network Logon 8.3

When installing SafeNet Authentication Client together with SafeNet Network Logon, perform the tasks in the following order:

1. Install SafeNet Authentication Client.
2. Install SafeNet Network Logon.
3. You may be required to restart the computer.

> **NOTE:** When installing SAC together with SafeNet Network Logon, you must install SAC as a *Custom* installation (instead of *Typical*) and enable the eTSapi component.

Compatibility with Third-Party Applications

The majority of third-party applications listed below have been validated and tested with SafeNet Authentication Client 10.2.

For more information see the Solution Marketplace section in the Service Portal:

https://serviceportal.safenet-inc.com/eservice_ENU/start.swe?SWECmd=Start&SWEHo=serviceportal.safenet-inc.com

https://kb.safenet-inc.com/kb/link.jsp?id=GUD253

Solution Type	Vendor	Product Version
Remote Access VPN	Check Point	Client E-80 (Security Gateway)
	Microsoft	Windows Server 2008 SP2 and later
	Cisco	NAM
		AnyConnect
	Palo Alto	PA-200 GW Appliance
	Juniper	Juniper MAG 2600 GW Appliance
Virtual Desktop Infrastructure (VDI)	Citrix	XenApp/XenDesktop 7.11
	Microsoft	Remote Desktop
	VMware View	Horizon 6.0
Identity Access Management (IAM) Identity Management (IDM)	IBM	ISAM for Web 9.0 (eToken only)
	Intercede	MyID (eToken only)
	Microsoft	FIM 2010 R2
	IDnomic	OpenTrust CMS 4.9.1
Pre Boot Authentication (PBA)	Sophos	SafeGuard Easy (eToken only)
	Microsoft	BitLocker (RSA only)
Certificate Authority (CA)	Entrust	SMA 8.1 (eToken only)

Solution Type	Vendor	Product Version
	Check Point (Local CA)	For All Check Point platforms
	Microsoft (Local CA)	For All Windows platforms
Local Access	Microsoft	All supported OS
	Evidian	ESSO (eToken only)
Digital Signatures	Entrust	ESP 9.2 (eToken only)
	Adobe	Reader XI and DC
	Microsoft	Outlook 2010 and 2013
	Mozilla	Thunderbird 45

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 10.2.

For more Installation and Upgrade details, see the SafeNet Authentication Client 10.2 Administrator Guide.

Resolved Issues

Issue	Synopsis
ASAC-4150	The DefInitMode registry key was added to allow skipping the first window of the Initialization process. See the SAC 10.2 Administrator Guide for more details.
ASAC-4110	When trying to decrypt encrypted data using one of these mechanisims: CKM_DES_CBC_PAD, CKM_DES3_CBC_PAD and CKM_AES_CBC_PAD, caused the C_DecryptUpdate API output to be corrupted.

Known Limitations

Issue	Synopsis
ASAC-4531	**Summary:** 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 and .NET cards.
	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 via eToken CSP (not supported) Customer must use Minidriver • 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.

Known Issues

Issue	Synopsis
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 SAC 10.2.
ASAC-4504	**Summary:** 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.

Issue	Synopsis
ASAC-4479	**Summary:** When inserting an IDPrime MD card that contains a new certificate friendly name, SAC displays the order of the messages incorrectly. **Workaround:** None.
ASAC-4469	**Summary:** Aborting an import certificate operation (in the middle of the process) while working with a Pin Pad reader, SAC Tools ignores the request to abort and continues with the import certificate operation. **Workaround:** Press cancel on the 'Import Certificate' window to abort the import certificate operation.
ASAC-4326	**Summary:** The iKey reader is not installed when upgrading to SAC 10.2. **Workaround:** Uninstall SAC and re-install SAC 10.2.
ASAC-4155	**Summary:** When the `CalculateCertFriendlyName` is set to `1` (on) and the Friendly Name is set manually, the Calculated Friendly Name appears instead of the manually defined name. **Workaround:** Set the `CalculateCertFriendlyName` registry key to `0` (off) to manually set the Friendly Name.
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-4122	**Summary:** When initializing a device in unlinked mode, and the "Token Password Must be changed at first logon" option is checked, any operation that requires a Digital Signature PIN (Role 3) will fail. **Workaround:** Ensure that both the Token Password and Digital Signature PIN are changed.
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-4095	**Summary:** When objects (keys and/or certificates) are created using SAC PKCS#11/CAPI/CNG and deleted using IDGo 800 Minidriver (or vice versa), the free space on the device is miscalculated showing an inacurrate value. **Workaround:** Use the same API to create and delete the objects.

Issue	Synopsis
ASAC-4091	**Summary:** The PIN dialog is not displayed when performing SSL/TLS 1.2 operations using a smart card via Edge browser. **Workaround:** Go to the domain Group Policy Editor and perform the following: 1. Click **Start>secpol.msc>files box**. (The secpol.msc must be opened with administrator privileges) 2. Disable the following UAC setting: In the console tree, expand **Local Policies** and click **Security Options**. Set the **User access control: Run all administrators in Admin Approval Mode** setting to Disabled. 3. Restart the computer. When trying to perform a SSL operation, login to token window is displayed. Enter the correct PIN and the SSL operation succeeds. (Ensure you are logged in as a non admin user).
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.
ASAC-3999	**Summary:** On Windows 10 Edge browser, when performing SSL, the **SAC Token Logon** window opens, but it is not the dialog box in focus. **Workaround:** Click inside the **Token Logon** window.
ASAC-3994	**Summary:** Support for the Identrust plugin module (Safenet iSign) was removed. **Workaround:** eSigner can be used as an alternative solution.
ASAC-3981	**Summary:** When connecting an IDPrime device (.Net) for the first time after installing SAC, the windows update process (smart card plug and play) automatically downloads IDGo 800 Minidriver. This causes problems whereby the IDPrime devices are registered to Microsoft KSP instead of SAC providers (CAPI/CNG). **Workaround:** Disable Plug and Play on the smart card or repair the SAC installation. https://technet.microsoft.com/en-us/library/dd979547(v=ws.10).aspx
ASAC-3969	**Summary**: Password expiration date is incorrect in SAC when changing the validity period in Minidriver Manager (only with cards arriving from the factory) **Workaround**: Change the cards password once to reset the expiration period.
ASAC-3542	**Summary**: When using Non ASCII characters as a Password, it will not work in PKCS11 login API. **Workaround**: When working with PKCS11 API use an ASCII password
ASAC-3498	**Summary**: When setting a user password on IDPrime MD cards, the 'Logon retries before token is locked' field is missing from the 'Set Token Password window' (SAC Tools>Advanced View>Set Token Password. Note that the default settings are kept. **Workaround**: Initialize the token and change the retry counter or perform unlock to set the retry counter.

Issue	Synopsis
ASAC-3451 ASAC-2278 ASAC-2221 ASAC-1675	**Summary:** Upgrading from SAC 9.0 to SAC 10.2 (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 SAC 9.0 and SAC 10.0 upgrade process to fail. **Workaround:** Run the following command to upgrade from SAC 9.0 to SAC 10.0: `msiexec /i C:\SafeNetAuthenticationClient-x32-9.0.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-3119	**Summary**: When working with Internet Explorer with Enhanced Protection Mode activated, while the following registry is enabled: [HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC\UI] RunExternalDialog = 1 Any secured operation performed (e.g. TLS 1.2 or SSL) on the browser causes the browser to freeze. **Workaround**: Add the relevant link (TLS 1.2, or SSL) to Trusted Sites – open Internet Explorer, click **Internet Options>Security>Trusted Sites>Sites>Add**.
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-2708	**Summary**: The SAC token login window on Edge browser 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-2643	**Summary**: After changing the virtual reader settings, a general error message appears. **Workaround**: Reboot your machine and the reader is refreshed.
ASAC-2493	**Summary**: When setting the user's 'Logon retires before token is locked' parameter to a number that's different to the factory settings defined on the IDPrime MD card, and thereafter initializing the IDPrime MD card using SAC Tools with a number that's higher than the setting defined using the Gemalto Minidriver Management tool, the initialization process fails. **Workaround**: Set a number that is lower than what was defined using the Gemalto Minidriver Management tool, or set the 'Logon retires before token is locked' parameter to the maximum value, which is 15.

Issue	Synopsis
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-2281	**Summary:** Sometimes, when trying to save illegal Password Quality settings in SAC tools, it causes the application to stop responding. **Workaround:** Install the native video card driver and select the default theme.
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-1997	**Summary:** The SAC tray icon fails to respond when connecting and removing the token several times. **Workaround:** Restart the machine.
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 Vista, Windows Server 2008, Windows 7 or Windows Server 2008 R2, the enrollment fails. **Cause:** In Windows Vista, 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-1164	**Summary:** When navigating to an SSL site using an eToken on a Windows 8.1 system with Internet Explorer 11 with **Enhanced Protected mode** enabled, the **Token Logon** window opens but no details can be entered. **Workaround:**.Click inside the **Token Logon** window to activate it, or disable the **Enhanced Protected mode** option.
ASAC-929	**Summary:** After logging on with a smart card, disconnecting, and logging on again, the certificate remains in the certificate store. **Workaround:** Delete the certificate from the store manually.

Issue	Synopsis
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.
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-674	**Summary:** On Metro IE, the **Token Logon** window opens, but it is not the dialog box in focus. **Workaround:** Click inside **Token Logon** window or uncheck the following Internet Option: **Security > Internet > Enable Protected Mode**.
ASAC-674	**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-597	**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-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 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	Synopsis
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.
ASAC-216 ASAC-777	**Summary:** The system did not recognize all of the connected iKey and eToken devices. **Workaround:** On Windows Vista 64-bit and on systems later than Windows 7 and Window 2008 R2, ensure that the total number of readers defined does not exceed 10 from among iKey readers, eToken readers, third-party readers, and reader emulations.

Known Issues – Deprecated Devices

Issue	Synopsis
ASAC-1315	**Summary:** When working with SafeNet smart cards SC330u, iKey 2032u, SC400, and iKey 4000 using SAC Tools, the amount of unblocking codes 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:

- 007-013560-001_SafeNet Authentication Client 10.2 Administrator Guide_Revision A
- 007-013561-001_ SafeNet Authentication Client 10.2 User Guide_Revision A

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	
Address	Gemalto. 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	+1-800-545-6608
	International	+1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.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.	