SafeNet Authentication Client

CUSTOMER RELEASE NOTES

Version: 10.0 – Windows
Build 43
Issue Date: March 2016
Document Part Number: 007-013473-00, Revision A

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 10.0 introduces support for Gemalto IDPrime card range.

This release allows administrators and users to use and manage IDPrime cards 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 Administrator's Guide.

New Features and Enhancements

SafeNet Authentication Client 10.0 offers the following new features:

- **Rebranding:** SAC UI and documentation now have Gemalto branding.
- **Support for the following IDPrime cards**:
  - IDPrime MD 830-FIPS
  - IDPrime MD 830-ICP
  - IDPrime MD 3810 (Contact mode)
  - IDPrime MD 3810 MIFARE 1K (Contact and Contactless mode)
- **Customization Tool:**
  - Was enhanced to include IDGo 800 Minidriver, and Gemalto PKCS#11 proxy library for backward compatibility.
  - Has a new dynamic packaging mechanism, whereby the customized .msi file size varies according to the features selected.
  - .msi Files are now signed using the SHA 2 algorithm.
  - The language field was added to the General Settings window.
- **Bug fixes** – this release includes bug fixes from previous SAC versions.

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**

Gemalto IDPrime cards are supplied with the following default token password: **0000**. The administrator password must be entered using 48 hexadecimal characters.

We strongly recommend that users change the token password upon receipt of their token.

Compatibility Information

Browsers

SafeNet Authentication Client 10.0 Windows supports the following browsers:

- Firefox (up to and including version 45)
- Internet Explorer (up to and including version 11 and Metro)
- Microsoft Edge (does not support certificate enrollment)
- Chrome version 47 and later, for authentication only (does not support certificate enrollment)

Operating Systems

SafeNet Authentication Client 10.0 (GA) Windows supports the following operating systems:

- Windows Vista SP2 (32-bit, 64-bit)
- Windows 2008 R2 SP1 (32-bit, 64-bit)
- Windows Server 2008 SP2 (32-bit, 64-bit)
- Windows Server 2012 and 2012 R2 (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)

NOTE: In Windows 8.1 environments, SafeNet eToken 7300 devices earlier than version 9.0.35 can be used only when SafeNet Authentication Client is installed.

Tokens

SafeNet Authentication Client 10.0 supports the following tokens:

Certificate-based USB tokens

- SafeNet eToken 5110, 5110 HID
- SafeNet eToken 5100/5105 – (EOS June 2016)
- SafeNet eToken 5200/5205 – (EOS June 2016)
- SafeNet eToken 5200/5205 HID – (EOS June 2016)
- eToken NG-OTP – (EOS June 2016)

Smart Cards

- SafeNet eToken 4100 - (EOS June 2016)
- IDPrime MD 830-FIPS
- IDPrime MD 830-ICP
- IDPrime MD 3810
- IDPrime MD 3810 MIFARE 1K

Certificate-based Hybrid USB Tokens

- SafeNet eToken 7300
- SafeNet eToken 7300-HID

Software Tokens

- eToken Virtual
- eToken Rescue

End-of-Sale Tokens/Smart Cards

- iKey 4000
- SafeNet eToken 4000 (SC400)
- SafeNet eToken PRO Java 72K
- eToken PRO Anywhere
- eToken PRO Smartcard 72K

End-of-Life Tokens/Smart Cards

- iKey: 2032, 2032u, 2032i (Windows and Mac only)
- SafeNet smart cards: SC330, SC330u, SC330i
- eToken NG-Flash
- eToken PRO 32K v4.2B
- eToken PRO 64K v4.2B
- eToken Pro SC 32K v4.2B
- eToken Pro SC 64K v4.2B

External Smart Card Readers

SafeNet Authentication Client 10 (GA) supports the following smart card readers:

- Gemalto IDBridge CT30
- Gemalto IDBridge CT40
- Gemalto IDBridge CL 3000 (ex Prox-DU)
- SCR 3310 v2 Reader
- Athena AESDrive IIIe USB v2 and v3
- ACR
- Athena Keyboard
- Omnikey 3121
- Dell Broadcom
- Unotron

Mobile PKI Bluetooth Readers:

- SafeNet Reader CT1100
- SafeNet Reader K1100

NOTE:

- Gemalto PIN Pad readers are not supported.
- SC Reader drivers must be compatible with the extended APDU format in order to be used with RSA-2048 (relevant to SafeNet eToken 4100).

Tablets

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

Thin Clients

SafeNet Authentication Client 10.0 (GA) supports the following Thin Clients (eToken only):

- HP - T310/T410
- Wyse - P Class
- Oracle - SunRay DTU
- Dell - Wyse C10LE

Localizations

SafeNet Authentication Client 10 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 Gemalto IDPrime MD cards, the user PIN must be in ASCII characters and the Administrator PIN must be in 48 hexadecimal characters (without spaces).

Compatibility with Gemalto Applications

IDPrime MD cards can be used with the following Gemalto products:

- IDGo 800 Credential Provider
- IDGo 800 User Tool for Windows (V1.0.16)
- IDGo 800 Cert Tool (V1.0.5)

To work with these products, install IDGo 800 Minidriver by generating an .msi file using the SAC Customization Tool. See the SafeNet Authentication Client 10.0 Administrator's Guide for more details on how to generate an msi file.

Compatibility with SafeNet Applications

eToken devices can be used with the following SafeNet products:

- SafeNet Network Logon 8.3
- SafeNet Authentication Manager 8.2 (eToken only)

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 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 10.0.

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 6.5 and 7.6 XenDesktop 7.6
	Microsoft	Remote Desktop
Identity Access Management (IAM) Identity Management (IDM)	VMware View	Horizon 6.0
	IBM	ISAM for Web 7.0, 8.0 and 9.0 (eToken only)
	Intercede	MyID (eToken only)
	Microsoft	FIM 2010 R2
Pre Boot Authentication (PBA)	Sophos	SafeGuard Easy (eToken only)
	Microsoft	BitLocker (RSA only)
Certificate Authority (CA)	Entrust	SMA 8.1 (eToken only)
	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 X and XI
	Microsoft	Outlook 2010 and 2013
	Mozilla	Thunderbird 38

Installation and Upgrade Information

Installation

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

Upgrade

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 SafeNet 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 10.0.

For more Installation and Upgrade details, see the SafeNet Authentication Client 10.0 Administrator's Guide.

Resolved Issues

Issue	Synopsis
ASAC-3490	When trying to install SAC with the command line parameter: PROP_IKEYREADERCOUNT, iKey readers were installed, when in fact they were not supposed to be installed.
ASAC-3016	When implementing PKCS#11 with C_GetSlotList() the incorrect value was returned.
ASAC-2858	The 'Set Token Password' window was accepting passwords that did not comply with the password quality settings.
ASAC-2852	When importing an EC-P 256 private Key into a token using C_UnwrapKey () PKCS-11 API, the process failed with the following error: CKR_TEMPLATE_INCONSISTENT.
ASAC-2846	On SAC 9.0, when entering the incorrect password for RSA Secondary authentication, SAC did not prompt the user to enter the password again.
ASAC-2832	Microsoft outlook failed to access the ECDH certificate/key associated with SafeNet KSP.
ASAC-2824	When an XML project was saved without generating the MSI, the initial values set in 'Features to Install' were not retained.
ASAC-2815 ASAC-2393	The parameter 'Allow One Factor' was added to SafeNet Authentication Client Customization Tool. See the section: SafeNet Authentication Client Tools UI Access Control List in Chapter 8 of the Administrator's Guide for more details.
ASAC-2730 ASAC-2645	Failed to generate ECDSA keys using the SDK 9.0 Java Wrapper (iaik PKCS11 Wrapper).

Issue	Synopsis
ASAC-2649	When connecting via Citrix Client (Mac) to a Windows server (with SAC 9 installed), the session disconnects immediately. This occurred on a Mac 10.10.X Host machine.
ASAC-2639	When running the test program with C_ EncryptFinal on an AES_CBC_PAD, the program crashed.
ASAC-2596	The 'Create Administrator Passcode' parameter in the Initialize Token Password Settings window is now unchecked by default, and the Passcode field is empty.
ASAC-2534	Old certificates could not be marked as Archived using Entrust Client ESP 9.2.
ASAC-2377	When installing SAC with the KSP feature disabled, SAC Tools still displayed the "Set As KSP" option.
ASAC-2312	The Cancel button in the Token Logon window appeared in English instead of German.

Known Issues

Issue	Synopsis
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 (4.3, 4.1 and 4.1.2) using a 32 – bit operating system, 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**: Either Initialize the token and change the retry counter, or use a x64 machine.
ASAC-3451 ASAC-2278 ASAC-2221 ASAC-1675	**Summary:** Upgrading from SAC 9.0 to SAC 10.0 (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.

Issue	Synopsis
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-2609	**Summary:** On Windows 10 Edge browser, when performing SSL, the **SAC Token Logon** window opens, but loses focus. **Workaround:** Click inside the **Token Logon** window.
ASAC-2494	**Summary:** When adding a license into SAC using the **Disable-Crypto** property, the SAC license is not valid, as the license is hashed with MD5, which is unsupported. **Workaround:** None.
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.
ASAC-2436	**Summary:** When a user attempts to generate a customized SAC msi file with no domain administrator privileges, the process fails. **Workaround:** Create a customized SAC msi file with domain administrator privileges.

Issue	Synopsis
ASAC-2299	**Summary:** eToken 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 eToken Virtual was enrolled on a USB 3 port, then use the token on a USB 3 port only. If the eToken Virtual was enrolled on a USB 2 port, then use the token on a USB 2 port only.
ASAC-2298	**Summary:** Connection problems occur when eToken Virtual devices are locked to flash and enrolled on a VMware environment. **Workaround:** When using an eToken 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-2194	**Summary:** When upgrading SAC 8.3 to SAC 9.0, and in cases where a license was entered in SAC 8.3 using the SAC Customization Tool, the new SAC 9.0 license will not be replaced. **Workaround:** Delete the **SACLicense.lic** file located in: **%ProgramData % \SafeNet\SAC**. For more details, see the SAC 9.0 Administrator's Guide
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-2007	**Summary:**.On iKey 2032 and 4000 tokens, the unlock option is always enabled on the SAC monitor (whether the token is locked or unlocked), and disabled (grayed out) in SAC Tools (Simple View), until the token is physically locked. **Workaround:** None. By design.
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.
ASAC-1761	**Summary:** SAC Monitor is still displayed when uninstalling SAM 8.2 Hotfix 468, and SAC 9.0. **Workaround:** Restart the machine.

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-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.

Issue	Synopsis
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.
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-860	**Summary:** When an iKey token is locked, the **Unlock Token** option in the SAC Tool's **Simple** mode is not enabled. **Workaround:** Click the **Refresh** icon.
ASAC-845	**Summary:** When Firefox is open on a Mac OS, and a SafeNet eToken 7300 HID device is disconnected, Firefox fails to respond. **Workaround:** If the PKCS#11 module has been loaded from the CD, ensure that Firefox is closed before disconnecting the token. An alternate way to load the PKCS#11 module is to copy the appropriate files to the local machine and then load them from there.
ASAC-843	**Summary:** When both the SAM client and SAC client are installed and the user tries to exit SAC using the SAC tray menu, the tray icon continues to be displayed and SACMonitor fails to respond. **Workaround:** Restart **SACMonitor.exe**.
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.

Issue	Synopsis
AHWENG - 764	**Summary:** When logging into an eToken 7300 protected partition (which is by default formatted using the FAT32 file system architecture) on a Windows 7 platform, you may experience a delay from the time the token password is entered, to the time when the partition opens and is shown in windows explorer. The delay is even longer when using virtual environments (i.e. VMware, VSphere, etc.). **Workaround:** On Windows and Linux operating systems, format the partition using the NTFS file system architecture. **Note:** NTFS is not supported on Mac operating systems by default.
ASAC-741	**Summary:** When migrating from BSec, the "Unable to complete Entrust Digital ID migration" error message is displayed. **Workaround:** If the EDS certificate was enrolled as **Public**, define the following Registry settings on the OS that will run the migration process: HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC\CertStore Name: SyncronizeStore Type: Dword Data: 00000000 If the EDS certificate was enrolled as **Private**, there is no workaround.
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-495 ASAC-1708	**Summary:** When using legacy JC Mask 7 tokens on Windows Vista, Server 2008, Windows 7, and Windows 8, 2048-bit keys could not be generated. **Workaround:** Greatly increase the **TransactionTimeoutMilliseconds** Registry value. For example, multiply it by 100.
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.

Issue	Synopsis
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**.
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-260	**Summary:** The smart card could not be used with Citrix XenApp 4.5 with Rollup Pack 07. **Workaround:** Use Citrix 4.5 with Rollup Pack 05 and 06.
ASAC-225	**Summary:** When using SAC with Windows 8 native Metro mail client, emails could not be signed. **Workaround:** Windows 8 Mail does not support the S/MIME message format. For email items in the S/MIME format, use Outlook Web App, Microsoft Outlook, or another email program that supports S/MIME messages.
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.

Product Documentation

The following product documentation is associated with this release:

- 007-013437-001_SafeNet Authentication Client 10.0 (GA) Administrator's Guide_Revision A
- 007-013439-001_ SafeNet Authentication Client 10.0 (GA) User's 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.	