SafeNet Authentication Client

CUSTOMER RELEASE NOTES

Version: 9.0 (GA) - Windows, Linux, and Mac
Build 43
Issue Date: 31 January 2015
Document Part Number: 007-012829-001, 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

The SAC 9.0 (GA) release supports Windows, Linux, and Mac operating systems.

New Features and Enhancements

SafeNet Authentication Client 9.0 (GA) offers the following new features:

- **eToken 7300 Flash usage procedures are now supported on Windows, Linux, and Mac** – Usage operations (performed via all operating systems) include:
  - Log On to Flash/Log Off from Flash
  - CD-ROM update
  - Firmware update (windows only)
- **eToken 7300 is now supported on Mac operating systems** - See SafeNet eToken 7300 on page 4.
- **New Linux operating systems are now supported** – See Operating Systems on page 5.
- **New and enhanced interface across all platforms** – Previous versions of SAC supported the QT cross-platform framework. SAC 9.0 now supports an innovative technology that maintains the unique look and feel of each underlying (native) platform (Windows, Linux, and Mac).
- **Additional custom installation options** – The installation of SAC 9.0 enables selecting specific, customized features to be installed. For example, BSec compatability mode is now available through the custom installation options.
- **Installation file size reduced** – The Windows and Linux installation file size has been reduced significantly.
- **Mac Yosemite support** – SAC 9.0 now supports the MAC Yosemite operating system.
- **SAC (Mac) custom installation file** - This is a separate custom installation file, which enables administrators to distribute the SAC license and configuration installation file (SafeNet Authentication Client Customization 9.0.mpkg) to the organization. See the SAC Administrator's Guide for more details.

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/

Default Password

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

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

Advisory Notes

Reader Quantity Limitation

On Windows Vista 64-bit, and on systems later than Windows 7 and Window 2008 R2, the total number of readers that an administrator can allocate is limited to 10 from among the following: iKey readers, eToken readers, third-party readers, and reader emulations.

SafeNet eToken 7300

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.

Initializing and repartitioning the eToken 7300 can be done only on Windows operating systems.

Mac Unified Bundle

The Mac unified bundle (present on eToken 7300) is now supported on the following operating systems:

- Mac OS X 10.9 (Mavericks)
- Mac OS X 10.10 (Yosemite)

eToken Virtual

eToken Virtual has some limitations on a few Linux operating systems. See Known Issues (Linux), on page 19.

Compatibility Information

Browsers

SafeNet Authentication Client 9.0 (Windows) supports the following browsers:

- Firefox (up to and including version 33)
- Internet Explorer (up to and including version 11 and Metro)
- Chrome version 14 and later, for authentication only (does not support enrollment)

SafeNet Authentication Client 9.0 (Linux) supports the following browsers:

- Firefox (up to and including version 33)

SafeNet Authentication Client 9.0 (Mac) supports the following browsers:

- Safari
- Firefox (up to and including version 33)
- Chrome

Operating Systems

SafeNet Authentication Client 9.0 (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)

SafeNet Authentication Client 9.0 (Linux) supports the following operating systems:

- Red Hat 6.6 (32-bit and 64-bit), 7.0 (64-bit)
- Ubuntu 13.10, 14.04 (32-bit and 64-bit)
- SUSE 11.3 (32-bit and 64-bit), 12.0 (64-bit)
- CentOS 6.6 (32-bit and 64-bit), 7.0 (64-bit)
- Fedora 20 (32-bit and 64-bit)
- Debian 7.7 (32-bit and 64-bit)

The following Mac operating systems support SafeNet eToken 7300 (unified bundle):

- OS X 10.9 (Mavericks)
- OS X 10.10 (Yosemite)

Tablets

SafeNet Authentication Client 9.0 (GA) supports the following tablets:

- Lenovo ThinkPad Tablet, running Windows 8
- Microsoft Surface Pro, running Windows 8.1

Tokens

SafeNet Authentication Client 9.0 (GA) supports the following tokens:

Certificate-based USB tokens

- SafeNet eToken PRO Java 72K
- SafeNet eToken PRO Anywhere
- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID & VSR

Smart Cards

- SafeNet eToken PRO Smartcard 72K
- SafeNet eToken 4100

Certificate-based Hybrid USB Tokens

- SafeNet eToken 7300
- SafeNet eToken 7300-HID
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)

Software Tokens

- SafeNet eToken Virtual
- SafeNet eToken Rescue

End-of-Sale Tokens/Smart Cards

- SafeNet iKey: 2032, 2032u, 2032i (Windows and Mac only)
- SafeNet smart cards: SC330, SC330u, SC330i
- SafeNet eToken 7100 (SafeNet eToken NG-Flash)
- SafeNet eToken 5000 (iKey 4000)
- SafeNet eToken 4000 (SC400)

External Smart Card Readers

SafeNet Authentication Client 9.0 (GA) supports the following smart card readers:

- SCR 3310 v2 Reader
- Athena AESDrive IIIe USB v2 and v3
- ACR
- Athena Keyboard
- GemPC CCID
- Omnikey 3121
- Dell Broadcom
- Unotron

NOTE:

- SC Reader drivers must be compatible with the extended APDU format in order to be used with RSA-2048.
- The latest CCID Driver must be installed when using Athena v3.

Localizations

NOTE:

SafeNet Authentication Client 9.0 (GA) supports all languages for Windows, but only English for Linux and Mac.

SafeNet Authentication Client 9.0 (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

Compatibility with SafeNet Applications

eToken Devices

eToken devices can be used with the following SafeNet products:

- SafeNet Network Logon 8.2 and above
- SafeNet Authentication Manager 8.2 and above
- eToken Minidriver 5.1 (Java cards only)

Installing SafeNet Authentication Client with eToken SafeNet Network Logon 8.2 and above

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 9.0 (GA). Others were tested and validated with previous versions of SafeNet Authentication Client.

Solution Type	Vendor	Product Version
Remote Access VPN	Check Point	NGX R75, R77
	Cisco	ACS 5.4, NAM, ASA 5500, AnyConnect
	Citrix	Netscaler 10.1
	Juniper	Juniper SA 700
	Nortell	Avaya VPN Client 10.04
Virtual Desktop Infrastructure (VDI)	Citrix	XenApp 6.5, 7.5, and 7.6 XenDesktop 7.1, 7.5, and 7.6
	Microsoft	Remote Desktop
	VMware View	Horizon 5.2
Identity Access Management (IAM) Identity Management (IDM)	CA	Siteminder 12.1
	IBM	ISAM for Web 7.0
	Intercede	MyID
	Microsoft	FIM 2010 R2
Pre Boot Authentication (PBA)	Symantec	PGP Desktop 10.3
	WinMagic	SecureDoc

Solution Type	Vendor	Product Version
	Sophos	SafeGuard Easy
	Becrypt	Disk Protect 5.2
	Microsoft	BitLocker
	McAfee	Endpoint 7.x
Certificate Authority (CA)	Entrust	Authority 8.1
	CheckPoint (Local CA)	All CheckPoint platforms
	Microsoft (Local CA)	All Windows platforms
	Verisign	MPKI 8.x
Local Access	Putty	CAC
	Microsoft	All OS
	Cisco	ISR 8200
	OpenSSH	f-secure
	Tectia	SSH Client 6.2
	Evidian	ESSO
	Linux	PAM
Digital Signatures	Entrust	ESP 9.2
	Adobe	Reader X
	Microsoft	Outlook 2013
	IBM	Lotus Notes 9.0
	Mozilla	Thunderbird 1.29

Certification

The following certifications will be available as part of the SAC 9.0 (GA) release process:

- **Citrix Ready**:
  Citrix XenApp 6.5, 7.5, and 7.6 XenDesktop 7.1, 7.5, and 7.6
  http://www.citrix.com/ready/en/safenet/safenet-authentication-client
- **Entrust Ready:**
  ESP 9.2
- **Identrust**
- **Microsoft**

Installation and Upgrade Information

Installation

SafeNet Authentication Client must be installed on each computer on which a SafeNet eToken, iKey token, or SafeNet smart card is to be used. Local administrator rights are required to install or uninstall SafeNet Authentication Client.

Upgrade

It is recommended that eToken PKI Client, BSec, and earlier versions of SafeNet Authentication Client be upgraded to the latest version on each computer that uses a SafeNet eToken, iKey token, or SafeNet smart card. Local administrator rights are required to upgrade SafeNet Authentication Client.

Please see the SafeNet Authentication Client 9.0 (GA) Administrator's Guide for installation and upgrade information.

Resolved Issues (Windows)

Issue	Synopsis
ASAC-2244	When connecting an eToken device with a CA certificate into a locked machine, the CA security dialog is displayed and can be installed by pressing the OK button even though the machine is locked.
ASAC-2047	Previously, when generating an object on an eToken device (with hardly any memory left), deleting the object damaged other SAC objects.
ASAC-1781	After disabling Anywhere mode (AnywhereExtendedMode = 0), and a token with an Anywhere image was connected, the injected browser was automatically launched, and the anywhere functionality options were added automatically to the SAC monitor options.
ASAC-1773	When connecting and removing a SafeNet eToken 5200 HID several times, the token was no longer recognized.
ASAC-1700	When connected to a RemoteApp or RDP from a client to a server, disconnecting the remote session, not via the log off user option, caused the CPU usage to reach 100% on the server machine. This is a Microsoft issue. The hotfix is available as part of the December 2014 update rollup for windows server 2012 R2: http://support.microsoft.com/kb/3013769
ASAC-1461	Importing or adding a SAC license with an ampersand character (&) in the customer name caused the SAC monitor **About** screen to freeze.
ASAC-1400	On some occasions, repartitioning an eToken 7300 with a non-protected flash drive failed.
ASAC-1374	When setting the Microsoft GPO parameter **ForceReadingAllCertificates** to **Disabled**, instead of seeing the smart card default certificate, all smart card logon certificates were visible on the operating system logon screen.
ASAC-1357	Previously, when working with a token on a system that had SAC installed, the token balloon pop-up event was not displayed when connecting the token.

Issue	Synopsis
ASAC-1334	After initializing and partitioning an eToken 7300, a window appeared indicating that the token was initialized and partitioned successfully. This window was not visible as it was hidden behind another window.
ASAC-1323	After **logging on to flash** and the machine was locked and unlocked, the flash was no longer accessible.
ASAC-1296	After initializing the eToken 7300 using the **Copy from Folder** option, reinitializing the token again with the **SafeNet default ISO** option failed with a general error.
ASAC-1256	When uninstalling SAC 8.3 GA, the folders and sub-folders were not removed from: **C:\Program Files\SafeNet**.
ASAC-1178 ASAC-1944	The eToken 7300 unified bundle is now supported on Mavericks and Yosemite operating sytems. For more details, see Operating Systems, on page 5.
AHWENG-1019	Previously, when performing a CD update on the eToken 7300 device with an image file size lareger than 2 gigabytes, the update failed.
ASAC-927	When initializing a token using the SDK, and the token had FIPS or Common Criteria certification, the token was not initialized with the original certification.
ASAC-879	eToken 7300 **Password Expired** and **Certificate Expired** balloon pop-ups were displayed on both the SAC tray menu and on the eToken 7300 tray menu.
ASAC-734	When SAC Monitor tried to download the AnyWhere package/bundle from an unreachable path, such as a different network, SAC Monitor stopped responding for 30 seconds.
ASAC-717	When in debug mode, it was not possible to limit the log sizes of all log files. For Log Setting details, see the SAC *9.0 (GA) Administrator's Guide.*

Resolved Issues (Linux)

Issue	Synopsis
ASAC-2010	It was not possible to read the contents of an eToken 4100 when connected to a Centos 6.4 OS with Athena CCID Reader (Athena ASEDrive IIIe USB v3).
ASAC-1644	On some occasions, the token was not recognized because of a conflict between SAC drivers and openCT drivers.
ASAC-1026	SAC is no longer dependant on Libhal.
ASAC-1025	After inserting the SAC license under: **/home/user** (or importing it using the management interface), the license became visible only to the user, who had already inserted a license on the computer. If the computer was used by multiple users, the other users were not able to use the SAC license.
ASAC-993	After inserting or attaching a token without an Admin PIN, the **Unlock** option was still displayed in the **Tray Icon** menu.
ASAC-992	When an error was displayed within SAC Tools, the message was not closed upon token removal.
ASAC-990	After using SAC Tools to delete a data object from a token, the toolbar options were not refreshed when standing on another node.

Issue	Synopsis
ASACL-207	When attempting to perform an operation on a token with an expired password, an incorrect error message stated that the password will expire in one day, when in fact it had already expired.
ASACL-179	After connecting eToken Rescue, the token was not displayed in SAC Tools.

Resolved Issues (Mac)

Issue	Synopsis
ASAC-2303	SAC 8.2 SP2 (Mac) does not support upgrade from any previous version.
ASAC-2169	Connecting a token and then removing it quickly, caused the monitor to freeze.
ASAC-1941	After upgrading from SAC 8.2 SP2 (Mavericks) to Yosemite caused the smart card to stop functioning. Installing SAC 9.0 resolves this issue.
ASAC-1464	Previously, it was not possible to see a VPN certificate when using Mavericks.
ASAC-1041	When MAC OS resumes after sleep mode, it takes a long time, sometimes longer than a minute, for the token to be recognized in SAC Tools. This problem does not occur with iKey tokens.
ASAC-1036	Summary: The "About" window was opened from the SAC tray menu, and it was not closed. When the user navigated to a different window, the "About" window disappeared, and the tray menu could not be opened from the tray icon.

Known Issues (Windows)

Issue	Synopsis
ASAC-2299	**Summary:** eToken Virtual devices that are locked to flash, and were enrolled on SafeNet Authenticaion Manager using a USB 3 port, cannot function on a USB 2 port, and visa 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-2278 ASAC-2221 ASAC-1675	**Summary:** Upgrading from SAC 8.3 to SAC 9.0 (while a token is connected with Smart Card Logon, MS certificate or SNL profile), caused the session to automatically disconnect during the upgrade process, and the SAC 9.0 upgrade process to fail. **Workaround:** Run the following command to upgrade from SAC 8.3 to SAC 9.0: `msiexec /i C:\SafeNetAuthenticationClient-x32-9.0.msi PROP_FAKEREADER=128`
ASAC-2257	**Summary**: After connecting an iKey 2032, and launching the Token Manager Utility (TMU), the enrollment process does not work when using SAC 9.0. and above with Bsec Utilities 8.2. **Workaround**: Perform the following on SAC 9.0: 1. Install SAC 9.0 with the Bsec Compatible feature (CAPI and PKCS11). 2. Right-click **My Computer**, select **Properties>Advanced system settings>Environment Variables**, and under **System Variables**, select the **Path** variable, and click **Edit**. In the Edit System Variable window, add: **`;C:\Program Files\SafeNet\Authentication\SAC\x32\BSecClient`** to the end of the **Variable value** line. 3. In the Registery, create the **Selected Token** property: **`HKLM or HKCU ; SOFTWARE\SafeNet\Authentication\SAC\UI DWORD "SelectedToken" = 0`** 4. Ensure that Internet Explorer runs in **Compatibility View** mode. For Example: Connect an iKey device and launch the **TMU**. Open **Internet Explorer 10.** Select **Tools>developer tools>Browser Mode: IE10 Compact View>Internet Explorer 10 Compatibility View.**
ASAC-2256	**Summary:** Install SAC 8.3 (GA) with drivers (typical installation), and then perform an upgrade by installing SAC 9.0 without drivers, this causes the upgrade to fail. Both SAC versions (SAC 8.3 and SAC 9.0) appear under 'Add/Remove Programs'. **Workaround:** Install SAC 9.0 (typical installation), and then uninstall SAC 9.0.

Issue	Synopsis
ASAC-2250	**Summary:** Upgrading from SAC 8.3 Post GA Bsec to SAC 9.0 via the command line or installation wizard with a specific feature list does not remove components that existed in SAC 9.0 e.g. : DKidentrus, eTFS, eTSAPI And More, etc. **Workaround:** Manually delete the files.
ASAC-2237	**Summary:** SAC Tools has no visible toolbar tooltips on a Windows 8.1 x64. **Workaround:** None.
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.
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

Issue	Synopsis
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.
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.

Issue	Synopsis
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.
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**.

Issue	Synopsis
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.
ASAC-378	**Summary:** Smart card logon is not supported when using tokens with ECC certificates. **Workaround:** Perform the following steps: 1) In the Registry, rename the following key in: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\eTokenCard/JC1.0b` Name: Crypto Provider_ Type: REG_SZ Data: eToken Base Cryptographic Provider 2) 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.

Issue	Synopsis
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 (Linux)

Issue	Synopsis
ASAC-2299	**Summary:** eToken Virtual devices that are locked to flash, and were enrolled on SafeNet Authenticaion Manager using a USB 3 port, cannot function on a USB 2 port, and visa 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-2277	**Summary**: On some occasions, tokens may not be recognized on Linux. This may be due to the operating system PCSCD internal process, which is not running. **Workaround**: Perform either one of the following: 1. Restart the operating system. 2. Ensure the PCSCD process is running. 3. If the PCSCD process is still not running, then start the process manually via a terminal session.
ASAC-2266	**Summary:** On Linux Debian 7.7, eToken Virtual does not connect to SAC automatically when the flash device is plugged in. **Workaround:** Manually connect the eToken Virtual via SAC Tools.
ASAC-2261	**Summary:** Open SAC Tools>Client Settings>Advanced Tab. The features: Copy user certificate to the local store, Copy CA certificates to the local store, Enable single logon, and Automatic logoff after token inactivity (in minutes) should be grayed out. **Workaround:** None. These settings are not supported by Linux.
ASAC-2097 ASAC-1792 ASAC-1491	**Summary:** When installing SAC 9.0 on Centos 7 (x64), Ubuntu or Suse the SAC Monitor is not displayed. **Workaround:** Log off and then log back on.
ASAC-2084	**Summary:**When you log onto a 7300 device via the SAC Tray icon, selecting the Explore Flash option does not work. **Workaround:** Open the flash partition manually.
ASAC-1999	**Summary:** When inserting the eToken 7300 device on SUSE, the device is recognized twice in SAC tools. It appears as if two tokens are connected, an HID token, and VSR token. **Workaround:** Work with the token that is recognized as the VSR token.
ASAC-1998	**Summary:** Linux operating system sometimes fails to respond with a blue screen after connecting and disconnecting an eToken 7300 protected partition. **Workaround:** Unmount the device before disconnecting it.
ASAC-1988	**Summary:** When inserting the eToken 7300 device on SUSE, the operating system root password is required. **Workaround:** Change the policy setting so that the root password is not required.
ASAC-1964	**Summary:**Importing an ECC certificate in the token causes a general error. **Workaround:** Ensure that the open SSL supports ECC algorithms. This is performed by entering the following command: `openssl list-public-key-algorithms` If the EC algorithm is shown in the list, then ECC is supported.

Issue	Synopsis
ASAC-1913	**Summary:** When installing SAC on x32-bit platforms, the eTPkcs11 module is not added automatically into the Firefox browser. **Workaround:** Add the eTPkcs11 module manually.
ASAC-1872 ASAC-1605 ASAC-1829	**Summary:** The eToken Virtual Generate OTP feature fails. **Summary:** Cannot log in to eToken Virtual on the Linux RedHat operating system. **Summary:** eToken Virtual on the flash drive does not connect to SAC automatically **Workaround:** Connect manually using SAC tools.
ASAC-1636	**Summary:**After switching to a new user, the SAC monitor and SAC tools could not be opened. **Workaround:** Restart the machine.
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-1458	**Summary:** After enabling Selinux on a Linux system, it was not possible to get the smart card log in to work through x-windows or terminal log in. **Workaround:** 1. Copy the **safenet.te** file to the **/tmp** folder on the Linux box. 2. Log in as a root user. 3. Compile the policy file (safenet.te) by running the following commands: **checkmodule –M –m –o /tmp/safenet.mod /tmp/safenet.te** **semodule_package –m /tmp/safenet.mod –o /tmp/safenet.pp** 4. Install the policy module: **semodule –I /tmp/safenet.pp**.
ASAC-997	**Summary:** Certificate that are configured using Secondary authentication on Windows, cannot be used on Linux or Mac, as it is a Crypto API that is supported on Windows only. **Workaround:** None.

Known Issues (Mac)

Issue	Synopsis
ASAC-2299	**Summary:** eToken Virtual devices that are locked to flash, and were enrolled on SafeNet Authenticaion Manager using a USB 3 port, cannot function on a USB 2 port, and visa 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.

Issue	Synopsis
ASAC-2296	**Summary:** eToken Virtual (on a Mac Yosemite) is not recognized in the Keychain application, causing Safari , the default mail application and outlook not to work. See apple bug report: 19613234. **Workaround:** None.
ASAC-2235	**Summary**: After installing SAC, the PKCS11 module was not inserted automatically into Firefox's browser. **Workaround**: Insert the module manually.
ASAC-2233	**Summary:** After opening the KeyChain application and selecting the 'Lock all Keychains' parameter, it is not possible to log on to the token in Keychain, and SSL in Safari cannot be established. **Workaround:** Disconnect the token, and then re-connect it.
ASAC-2227	**Summary:** When two tokens are connected, one of the token's settings are not accessible in SAC Tools. **Workaround:** Work with one connected token at a time.
ASAC-2223	**Summary:** Occasionally, when an eToken is disconnected, and then a different token is connected, the first token is still shown in SAC Tools. This is due to a Mac OS X issue. **Workaround:** Restart the machine.
ASAC-2191	**Summary**: When working with a 5100 token that is recognized via the CCID driver, the token might not be recognized or the system may not respond when the machine returns from sleep mode. **Workaround**: Re-insert the token.
ASAC-2079	**Summary:** Some Keychain related functions do not work on Yosemite when using iKey 2032 and 4000. **Workaround:** Disconnect and then connect the token.
ASAC-1853	**Summary:** When connecting an eToken 7300 for the first time, to a Mac (version 10.9 and 10.0) system, the eToken 7300 is recognized in CCID debug mode. The device is unrecognized when you remove the eToken 7300, and then re-connect it for the second time. **Workaround:** If SAC is installed, use the VSR driver. If SAC is not installed, use HID support.
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:**
ASAC-1053	**Summary:** When re-decrypting an email using Microsoft Outlook on Mac, the decrypt process fails. **Workaround:** Perform the following: 1. Disconnect the token, and close Outlook. 2. Connect the token, and reopen Outlook.

Issue	Synopsis
ASAC-1035	**Summary:** When connecting a CCID Smart Card reader, to a Mac system, the iKey 4000 device is unrecognized. **Workaround:** Perform one of the following: 1. Disconnect the Smart Card reader, and reboot the system. 2. Install the latest Omnikey Smart Card reader driver. ifdokccid_mac_universal-3.1.0.2.bundle. 3. Disable the Mac OS X GENERIC Smart Card reader driver by removing it.

Product Documentation

The following product documentation is associated with this release:

- 007-012830-001_SafeNet Authentication Client 9.0 (GA) Administrator's Guide_WLM_Revision A
- 007-012831-001_SafeNet Authentication Client 9.0 (GA) User's Guide_WLM_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 have questions or need additional assistance, contact SafeNet Customer Support through the listings below:

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	United States	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 SafeNet Knowledge Base.	