SafeNet Authentication Client

CUSTOMER RELEASE NOTES

Version:	8.3
Build	73
Issue Date:	13 July 2014
Document Part Number:	007-012451-001, Revision D

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 8.3 Post GA contains bug fixes reported by customers.

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 their Token Password upon receipt of their token.

Advisory Notes

BSec Compatibility Utilities Package Support

There is no new release of BSec Compatibility Utilities Package.

SafeNet Authentication Client 8.3 supports BSec Compatibility Utilities Package 8.2.

Future versions of SafeNet Authentication Client may not support BSec-compatibility.

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: iKey readers, eToken readers, third-party readers, and reader emulations.

SafeNet eToken 7300 and Windows 8.1

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.

Resolved Issues

Issue	Synopsis
ASAC-1348 ASAC-1237	When selecting the Change Password option via SAC tools or the SAC Tray Icon, and the Password Synchronization feature was activated, no message was displayed indicating that the password entered did not meet the domain password complexity requirements.
ASAC-1339	After initializing and repartitioning an eToken 7300 on SAC 8.3, the 'Explore Flash' option was missing from the list of functions displayed when right-clicking the SafeNet eToken 7300 flash tray icon.
ASAC-1309	When changing the 'Modify Password Policy Description' value in the GPO, the relevant registry key values were not updated.
ASAC-1251 ASAC-524	When running SSL using IE11 (Windows 8.1) in Protected Mode, access was denied and the Token Logon window was not displayed.
ASAC-1245	The Registry Key: 'IgnoreExpiredCertificates' in SAC 8.3 did not work correctly.
ASAC-1156	After connecting and disconnecting the eToken 5200 HID several times, the SAC monitor and SAC Service froze
ASAC-1128	When initializing an NG OTP Token, the NG OTP seed was deleted.
ASAC-1126	Upgrading eToken dll libraries from 8.2 to 8.3.30.0 did not work while working with eToken 7300.
ASAC-925	Customized banners that were displayed in the SAC 8.3 user interface (other than SAC Tools) could not be customized.
ASAC-813	Unlocking the DELL Optiplex 760 & 7010 while a Smart Card 4100/330 was connected to the Smart Card Reader, caused smartcard communication problems.
ASAC-491	Using XenDesktop, with Pass-through authentication configured, and SAC Single Logon enabled, the system continued to request a token logon password.

Known Issues

Issue	Synopsis
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-1416	**Summary:** When creating customized SAC MSI files on a x32 bit computer (using the SAC Customization tool), and the x64 msi file that was created is installed, the standard SAC Logo images are displayed, even though they were customized differently. **Workaround:** Create the MSI files using the customization tool installed on a x64 bit computer and not on a x32 bit computer.
ASAC-1400	**Summary:** On some occasions, repartitioning an eToken 7300 with a non-protected flash drive fails. **Workaround:** Reinsert the token and repartition the token again.
ASAC-1343	**Summary:** Selecting an option from the SAC tray icon using a Microsoft Surface tablet does not open the relevant menu option. **Workaround:** Select the relevant option from within the SAC tools application.
ASAC-1335	**Summary:** Mass storage options using an eToken 7300 protected token, are not supported within an RDP session. **Workaround:** None.
ASAC-1334	**Summary:** After initializing and partitioning an eToken 7300, a window appears indicating that the token was initialized and partitioned successfully. This window is not visible as it is hidden behind another window. **Workaround:** Move the window until you see the hidden window.
ASAC-1315	**Summary:** When working with the SafeNet Smart Card SC330u, iKey 2032u, SC400, and iKey 4000 using SAC Tools, the amount of Unblocking Codes retries remaining is not tracked i.e currently there is no way of determining how many unblocking code retries remain. **Workaround:** None
ASAC-1296	**Summary:** After initializing the eToken 7300 using the 'Copy from Folder' option, reinitializing the token again with the 'SafeNet default ISO' option fails with a General Error. **Workaround:** Initialize the token again.
ASAC-1256	**Summary:** When uninstalling SAC 8.3 GA, the folders and subfolders were not removed from: C:\Program Files\SafeNet. **Workaround:** Manually delete the folders and subfolders.
ASAC-974	**Summary:** When upgrading from SAC 8.2 GA to SAC 8.3, the upgrade fails. **Workaround:** Remove the SafeNet iKey Driver (64-bit) and then perform the upgrade.

Issue	Synopsis
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-927	**Summary:** The default Automatic Certification settings were changed in SAC 8.2 and later to True. As CardOS 4.2B cannot support both FIPS mode and RSA 2048, failure to take this into account this may lead to token initialization failure when using PKCS#11. **Workaround:** Do one of the following: • Set the "Init\Certification" setting via the property setting (registry) to 0(False) – see SAC 8.3 Administrator's Guide for details. • Make the application provide both the FIPS and the RSA 2048 settings as required.
ASAC-879	**Summary:** eToken 7300 "Password Expired" and "Certificate Expired" balloon pop-ups are displayed from both the SAC monitor and from the eToken 7300 tray menu. **Workaround:** Ignore the duplicates.
ASAC-878	**Summary:** After SAC was upgraded, the tray menu was displayed in English and not in the language used in the earlier version. **Workaround:** Run the SAC installation in Repair mode.
ASAC-862	**Summary:** When a partitioned eToken 7300 device is connected, the SafeNet drive's eToken 7300 icon that is displayed on the desktop, but double-clicking it does not open the device's drive. **Workaround:** Open the drive from the computer 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 freezes. **Workaround:** If the PKCS#11 module has been loaded from the CDROM, 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 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 freezes. **Workaround:** Restart the SACMonitor.exe

Issue	Synopsis
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 you enter the remote machine, you are prompted for the standard username 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 and not 16 characters as expected • the Response Code created during the Unlocking procedure is 39 characters and not 16 characters as expected **Workaround:** When unlocking a CC token, the user must be sure to copy the entire Response Code string.
ASAC-783	**Summary:** BSec's "Enrollment" option is not available in the tray menu. **Workaround:** Use the BSec Utilities link in the Start menu to access the "Enroll" option: Start > Programs > SafeNet > SafeNet Authentication Client > BSec > SafeNet Token Manager Utility Note: There is no new release of BSec Compatibility Utilities Package. Future versions of SafeNet Authentication Client may not support BSec-compatibility.
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 registries 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-734	**Summary:** When SACMonitor tries to download the AnyWhere package/bundle from an unreachable path, such as a different network, SACMonitor stops responding after 30 seconds. **Workaround:** Disconnect and then reconnect the token.
ASAC-717	**Summary:** Unable to limit the log sizes of all log files when in debug mode. **Workaround:** While the overall log size cannot be limited, single file sizes can be limited.
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.

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	**Summary:** When using legacy JC Mask 7 tokens on Windows Vista or Server 2008, 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:** Smartcard Logon is not supported when using tokens with ECC certificates. **Workaround:** Do the following two steps: 1) In the registry, define 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 smartcard could not be used with Citrix XenApp 4.5 with Rollup Pack 07. **Workaround:** Use Citrix 4.5 with Rollup Pack 05 and 06.

Issue	Synopsis
ASAC-225	**Summary:** When using SAC with Win8 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.

Compatibility Information

Browsers

SafeNet Authentication Client 8.3 is supported on the following browsers:

- Firefox 5 and later
- Internet Explorer 7, 8, 9, 10, 11, Metro
- Chrome version 14 and later, for authentication only (Does not support enrollment)

Operating Systems

SafeNet Authentication Client 8.3 is supported on the following Windows operating systems:

- Windows XP SP3 (32-bit, 64-bit)
- Windows Server 2003 SP3 (32-bit, 64-bit)
- Windows Server 2003 R2 (32-bit, 64-bit)
- Windows Vista SP2 (32-bit, 64-bit)
- Windows Server 2008 SP2 (32-bit)
- Windows Server 2008 R2 SP1 (64-bit)
- Windows Server 2012 (64-bit)
- Windows Server 2012 R2 (64-bit)
- Windows 7 SP1 (32-bit, 64-bit)
- Windows 8 (32-bit, 64-bit)
- Windows 8.1 (32-bit, 64-bit)

NOTES:

- To use a KSP cryptographic provider, Windows Vista or higher is required.
- 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.

The following Mac operating systems support SafeNet eToken 7300 devices initialized using SafeNet Authentication Client 8.3, and SafeNet eToken 5200/5205 HID devices:

- Mac OS X 10.9.1 (Mavericks)
- Mac OS X 10.8 (Mountain Lion)
- Mac OS X 10.7.3 and 10.7.4 (Lion)

Tablets

SafeNet Authentication Client 8.3 supports the following tablet:

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

Tokens

SafeNet Authentication Client 8.3 supports the following tokens:

- SafeNet eToken PRO
- SafeNet eToken PRO Anywhere
- SafeNet eToken PRO Smartcard
- SafeNet eToken 7300 (standard and HID)
- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID
- SafeNet eToken 4100
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)
- SafeNet eToken 7100 (SafeNet eToken NG-Flash)
- SafeNet eToken NG-Flash Anywhere
- SafeNet eToken Virtual Family
- SafeNet iKey: 2032, 2032u, 2032i
- SafeNet Smartcard: SC330, SC330u, SC330i
- SafeNet Smartcard SC400
- SafeNet iKey 4000

Localizations

SafeNet Authentication Client 8.3 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
- SafeNet Authentication Manager 8.0 and later
- eToken Minidriver 5.1 (Java cards only)

Installing SafeNet Authentication Client with eToken Network Logon 8.2

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

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

Compatibility with Third-Party Applications

SafeNet Authentication Client 8.3 works with the following products:

- Juniper Secure Access
- RDP Windows Logon
- Entrust ESP 9.0 and later
- Citrix XenApp 5.5 and later
- Cisco AnyConnect, Cisco ASA, Cisco VPN Client
- IdenTrust
- MS Office 2007 and later
- Adobe Acrobat 9 and later
- VMware Workstation
- Certificate Authorities
- Microsoft FIM/ILM
- MyID (Intercede) - for iKey devices only

Installation and Upgrade Information

Please see the SafeNet Authentication Client 8.3 Administrator's Guide for installation and upgrade information.

NOTE: When upgrading from SAC 8.3 GA, you must first uninstall it, and then install SAC 8.3 Post GA.

Product Documentation

The following product documentation is associated with this release:

- SafeNet Authentication Client Administrator's Guide
- SafeNet Authentication Client User's Guide

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

Support Contacts

If you 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
Email	support@safenet-inc.com	
Support and Downloads	www.safenet-inc.com/Support Provides access to the SafeNet Knowledge Base and quick downloads for various products.	
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.	