

Gemalto's SafeNet Authentication Client

LINUX CUSTOMER RELEASE NOTES

Version: 9.1 – Linux
Build 7
Issue Date: 24 December 2015
Document Part Number: 007-013386-001, Rev A

Contents

Product Description	2
Release Description.....	2
What's New.....	2
Licensing.....	2
Default Password.....	2
Advisory Notes.....	2
Installation.....	3
Compatibility Information	3
Browsers.....	3
Operating Systems	3
Mail Clients	3
Tokens	4
Certificate-based USB tokens	4
Smart Cards	4
Certificate-based Hybrid USB Tokens.....	4
Software Tokens	4
End-of-Sale Tokens/Smart Cards	4
External Smart Card Readers	5
Localizations	5
Resolved Issues	5
Known Issues	6
Product Documentation	8
Support Contacts	9

Product Description

Gemalto's 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 9.1 Linux release includes new features and covers bug fixes since the last version.

What's New

SAC 9.1 Linux supports the following new features and operating systems:

- Portuguese localization. To install SAC 9.1 with Portuguese localization, run the relevant scripts. See the Installation section on page 3.
- Ubuntu 15.04 and 15.10.

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

Some operating systems do not provide the auto-mounting solution when a USB device is connected. This causes the log in process on eToken 7300 (protected Flash drive) to fail.

Follow the instructions below to enable auto-mounting for eToken 7300:

The auto-mounting `udev` rule for eToken 7300 is installed with SAC 9.1 and is disabled by default. To enable this feature, edit the **90-hid-eToken.rules** file located in: `/lib/udev/rules.d/` and then remove the hash symbol (#) from the line: `#GOTO="eToken7300_manual_mount_end"`.

See **ASAC-2889** in the *Resolved Issues* section.



WARNING: By enabling the auto-mounting `udev` rule, the DVD ROM and Flash drive on the eToken 7300 will be mounted by default with permissions `0x777` (everyone can read write and execute).

Installation

To install SAC 9.1 with Portuguese localization:

1. Install SAC 9.1 Linux by double-clicking **SafenetAuthenticationClient-9.1.7-0.xxx.rpm**, or **SafenetAuthenticationClient-9.1.7-0_xxx.deb**.
2. Run either one of the following scripts:

Operating System	Script
DEB x64	install-portuguese_SafenetAuthenticationClient-9.1.7-0_amd64.deb.sh
DEB x32	install-portuguese_SafenetAuthenticationClient-9.1.7-0_i386.deb.sh
RPM x32	install-portuguese_SafenetAuthenticationClient-9.1.7-0.i386.rpm.sh
RPM x64	install-portuguese_SafenetAuthenticationClient-9.1.7-0.x86_64.rpm.sh

Compatibility Information

Browsers

SafeNet Authentication Client 9.1 Linux supports the following browsers:

- Firefox (up to and including version 41)
- Chrome (up to and including version 47)

Operating Systems

The following Linux operating systems are supported:

- Red Hat 6.6 (32-bit and 64-bit), 7.0 (64-bit)
- Ubuntu 13.10, 14.04, 15.04, 15.10 (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)

Mail Clients

The following Mail Clients are supported:

- Thunderbird 17

Tokens

SafeNet Authentication Client 9.1 supports the following tokens:

Certificate-based USB tokens

- SafeNet eToken 5110
- SafeNet eToken 5110 HID
- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID

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 smart cards: SC330, SC330u, SC330i
- SafeNet eToken 7100 (SafeNet eToken NG-Flash)
- SafeNet eToken 5000 (iKey 4000)
- SafeNet eToken 4000 (SC400)
- SafeNet eToken PRO Java 72K
- SafeNet eToken PRO Anywhere
- 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 9.1 supports the following smart card readers:

- Gemalto IDBridge CT 40
- Gemalto IDBridge CT 30
- 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

SafeNet Authentication Client 9.1 Linux supports English and Portuguese.

Resolved Issues

Issue	Description
ASAC-2889	Opening and closing the protected flash on eToken 7300 does not work in any terminal sessions (tty1 - tty6), due to auto-mounting being disabled. Enable auto-mounting udev rule, which is part of SAC 9.1 installation. See the <i>Advisory Notes</i> section on page 2 for more details.
ASAC-2307	Using the PKCS#11 API... if the C_Finalize function was called, and thereafter the C_GetSlotList function was called, the results showed 'No token connected', even though a token was physically connected.
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 dependent on Libhal.

Issue	Description
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.
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.

Known Issues

Issue	Description
ASAC-2601	<p>Summary: When connecting a device (eToken 5110) in CCID mode, the firmware version is displayed as N/A.</p> <p>Workaround: None.</p>
ASAC-2299	<p>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.</p> <p>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.</p>
ASAC-2298	<p>Summary: Connection problems occur when eToken Virtual devices are locked to flash and enrolled on a VMware environment.</p> <p>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.</p>
ASAC-2277	<p>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.</p> <p>Workaround: Perform either one of the following:</p> <ol style="list-style-type: none"> 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	<p>Summary: On Linux Debian 7.7, eToken Virtual does not connect to SAC automatically when the flash device is plugged in.</p> <p>Workaround: Manually connect the eToken Virtual via SAC Tools.</p>

Issue	Description
ASAC-2261	<p>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.</p> <p>Workaround: None. These settings are not supported by Linux.</p>
ASAC-2103	<p>Summary: When disconnecting eToken Virtual (created as flash locked) from the USB Port, the eToken Virtual reference remains in SAC Tools (Simple and Advanced view).</p> <p>Workaround: None.</p>
ASAC-2097 ASAC-1792 ASAC-1491	<p>Summary: When installing SAC 9.0 on Centos 7 (x64), Ubuntu or Suse the SAC Monitor is not displayed.</p> <p>Workaround: Log off and then log back on.</p>
ASAC-2084	<p>Summary: When you log onto a 7300 device via the SAC Tray icon, selecting the Explore Flash option does not work.</p> <p>Workaround: Open the flash partition manually.</p>
ASAC-1999	<p>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.</p> <p>Workaround: Work with the token that is recognized as the VSR token.</p>
ASAC-1998	<p>Summary: Linux operating system sometimes fails to respond with a blue screen after connecting and disconnecting an eToken 7300 protected partition.</p> <p>Workaround: Un-mount the device before disconnecting it.</p>
ASAC-1988	<p>Summary: When inserting the eToken 7300 device on SUSE, the operating system root password is required.</p> <p>Workaround: Change the policy setting so that the root password is not required.</p>
ASAC-1964	<p>Summary: Importing an ECC certificate in the token causes a general error.</p> <p>Workaround: Ensure that the open SSL supports ECC algorithms. This is performed by entering the following command: <code>openssl list-public-key-algorithms</code> If the EC algorithm is shown in the list, then ECC is supported.</p>
ASAC-1913	<p>Summary: When installing SAC on x32-bit platforms, the eTPkcs11 module is not added automatically into the Firefox browser.</p> <p>Workaround: Add the eTPkcs11 module manually.</p>
ASAC-1872 ASAC-1605 ASAC-1829	<p>Summary: The eToken Virtual Generate OTP feature fails.</p> <p>Summary: Cannot log in to eToken Virtual on the Linux RedHat operating system.</p> <p>Summary: eToken Virtual on the flash drive does not connect to SAC automatically</p> <p>Workaround: Connect manually using SAC tools.</p>
ASAC-1636	<p>Summary: After switching to a new user, the SAC monitor and SAC tools could not be opened.</p> <p>Workaround: Restart the machine.</p>
ASAC-1470	<p>Summary: After updating the FW on an eToken 7300, the FW version might not be updated under Token information in SAC Tools.</p> <p>Workaround: Restart the machine.</p>

Issue	Description
ASAC-1458	<p>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.</p> <p>Workaround:</p> <ol style="list-style-type: none"> 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	<p>Summary: Certificates 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.</p> <p>Workaround: None.</p>

Product Documentation

The following product documentation is associated with this release:

- 007-012830-001_Gemalto's SafeNet Authentication Client 9.0 (GA) Administrator's Guide_WLM_Revision A
- 007-012831-001_ Gemalto's 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 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, Inc. 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.	