

SafeNet Authentication Client

LINUX (POST GA) RELEASE NOTES

Version: 10.0 – Linux (Post GA)
Build RPM 32
DEB 37
Issue Date: August 2017
Document Number: 007-013841-001 Rev B

Contents

Product Description	2
Release Description.....	2
New Features and Enhancements.....	2
Advisory Notes.....	3
Licensing.....	3
Default Password.....	3
Password Recommendations	3
Initialization Key Recommendation	4
Compatibility Information	4
Browsers and Applications.....	4
Operating Systems	4
Tokens	4
Certificate-based USB Tokens	4
Software Tokens	4
Smart Cards	5
End-of-Sale Tokens/Smart Cards	5
End-of-Life Tokens/Smart Cards.....	5
External Smart Card Readers	6
Localizations	6
Installation.....	6
Upgrade.....	6
Known Issues	6
Product Documentation	7
Support Contacts	8

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 Linux introduces full IDPrime support including Multi-Slot support and Password Quality modifications for IDPrime MD cards. Support for Ubuntu, Debian, Fedora and SUSE is also included in this version.

IDPrime MD cards are PKI smart cards. Administrators and users can use and manage IDPrime MD smart cards seamlessly via the standard PKCS#11 interface and without the need for any additional middleware. They offer secure IT Security and ID access and are compatible with the NFC standard.

New Features and Enhancements

SafeNet Authentication Client 10.0 Linux offers the following new features:

- **Rebranding:** SAC Linux UI and documentation have Gemalto branding.
- **Support for the following IDPrime cards:**
 - IDPrime MD 830-FIPS
 - IDPrime MD 830-ICP
 - IDPrime MD 830 B
 - IDPrime MD 3810 Dual Interface Card
 - IDPrime MD 3810 MIFARE 1K (Contact and Contactless mode)
 - IDPrime MD 3811
- **Support for IDPrime .NET cards**
- **Support for the following IDPrime MD Common Criteria cards:**
 - IDPrime MD 840
 - IDPrime MD 840 B
 - IDPrime MD 3840– Dual Interface Card
 - IDPrime MD 3840 B
- **Support for SafeNet eToken 5110 Common Criteria**
- **Support for SafeNet eToken 5110 FIPS**
- **Support for unlocking IDPrime MD card range**
- **Friendly Admin Password** - short user friendly passwords are now supported (on IDPrime MD and eToken 5110 CC devices) instead of using 48 hexadecimal digits. For more details, see the SafeNet Authentication Client 10.0 Linux (Post GA) User Guide.

- **Support for Common Criteria PKCS#11 Multi-Slot** – for Common Criteria devices in unlinked mode. For information on how to work with Multi-Slots, see the PKCS#11 Digital Signature PIN section in the SafeNet Authentication Client 10.0 Linux (Post GA) User Guide.
- **PIN Quality modifications for IDPrime MD cards.**
- **Bug fixes** – this release includes bug fixes from previous SAC Linux versions.

Advisory Notes

- SafeNet Authentication Client 10.0 Linux (Post GA) is supported on systems that do not have IDGo800 or SafeNet Authentication Client previously installed.
- The **Scale for menu and title bars** display setting on Ubuntu must be set to 1.
- SAC supports openssl version 1.0.2.

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.

IDPrime cards are supplied with the following default token password: “0000” (4 digits). The administrator password must be entered using 48 hexadecimal zeros (24 binary zeros).

For IDPrime MD 840/3840/eToken 5110 CC devices:

- The default Digital Signature PIN is “000000” (6 digits)
- The default Digital Signature PUK is “000000” (6 digits)

Password Recommendations

We strongly recommend changing all device passwords upon receipt of a token/smart card according to the following:

- User PIN should include at least 8 characters of different types.
- Admin PIN should include at least 16 characters of different types.
- The *Friendly Admin Password* should include at least 16 characters of different types (See the SafeNet Authentication Client User Guide for more details on the Friendly Admin Password)
- Digital Signature PUK, when using a friendly name, should include at least 16 characters of different types.



NOTE: Character types include upper case, lower case, numbers, and special characters.

Initialization Key Recommendation

We strongly recommend changing the Initialization Key using either one of the following methods:

- The customization process (CPB)
- The SAC Initialization process (See the SafeNet Authentication Client User Guide for more details on Initialization Key settings)

Compatibility Information

Browsers and Applications

SafeNet Authentication Client 10.0 Linux (Post GA) supports the following browsers:

- Firefox up to 54.0
- Firefox (ESR) for SUSE 45.4
- Thunderbird 52.1.0 (except RH 7.3 x64 - 52.1.1)

Operating Systems

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

- Red Hat 7.3, 6.9
- CentOS 7.3, 6.9
- SUSE 12.2
- Debian 9.0
- Fedora 26
- Ubuntu 16.04 and 17.04

Tokens

SafeNet Authentication Client 10.0 Linux (Post GA) supports the following tokens:

Certificate-based USB Tokens

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

Software Tokens

- SafeNet Virtual Token
- SafeNet Rescue Token

Smart Cards

- Gemalto IDCore 30B eToken
- Gemalto IDPrime MD 840
- Gemalto IDPrime MD 840 B
- Gemalto IDPrime MD 3840
- Gemalto IDPrime MD 3840 B
- Gemalto IDPrime MD 830-FIPS
- Gemalto IDPrime MD 830-ICP
- Gemalto IDPrime MD 830 B
- Gemalto IDPrime MD 3810
- Gemalto IDPrime MD 3811
- Gemalto IDPrime .NET



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

End-of-Sale Tokens/Smart Cards

- SafeNet eToken 7300
- SafeNet eToken 7300-HID

End-of-Life Tokens/Smart Cards

- SafeNet eToken PRO 32K v4.2B
- SafeNet eToken PRO 64K v4.2B
- SafeNet eToken Pro SC 32K v4.2B
- SafeNet eToken Pro SC 64K v4.2B
- SafeNet eToken 7100 (SafeNet eToken NG-Flash)
- SafeNet eToken PRO Java 72K
- SafeNet eToken PRO Anywhere
- SafeNet eToken PRO Smartcard 72K
- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID
- SafeNet eToken 4100
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)

External Smart Card Readers

SafeNet Authentication Client 10.0 Linux (Post GA) supports the following smart card readers:

- Gemalto IDBridge CT30
- Gemalto IDBridge CT40
- Gemalto IDBridge CL 3000 (ex Prox-DU)



NOTE: SC Reader drivers must be compatible with the extended APDU format in order to be used with RSA-2048.

Localizations

SafeNet Authentication Client 10.0 Linux supports only English.

Installation

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

Upgrade

Upgrade is not supported and SafeNet Authentication Client Linux must be installed on a clean machine.

Known Issues

Issue	Synopsis
ASAC-5522	Summary: After switching to a new user, the SafeNet Authentication Client (SAC monitor) may not be opened. Workaround: Restart the machine.
ASAC-5497 ASAC-5495	Summary: After installing SAC and even after attempting to restart the machine, the SafeNet Authentication Client icon was not displayed. Workaround: Run SafeNet Authentication client to get the tray icon functionality (SAC Monitor).
ASAC-5260	Summary: Defining "Expiration Warning Period" and "Validity Period" settings does not work. Workaround: None
ASAC-5229	Summary: When trying to log onto a locked device, two messages are shown instead of one. Workaround: Close both windows.
ASAC-2672	Summary: When connecting a SafeNet Virtual Token (created as flash locked) from the USB Port, the SafeNet Virtual Token file does not open automatically in SAC Tools. Workaround: Manually connect the SafeNet Virtual Token

Issue	Synopsis
ASAC-2601	<p>Summary: When connecting an eToken 5110 device in CCID mode, the firmware version is displayed as N/A.</p> <p>Workaround: None</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-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-1913	<p>Summary: When installing SAC.deb 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-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>
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:

- 007-013842-001_SafeNet Authentication Client 10.0_Linux_Post GA_Administrator Guide_Revision B
- 007-013843-001_SafeNet Authentication Client 10.0_Linux_Post GA_User Guide_Revision B

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
Customer Support Portal	https://supportportal.gemalto.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.
Technical Support contact email	technical.support@gemalto.com