SafeNet Authentication Client (Linux)

Version 10.7 (GA)

Administrator Guide

gemalto

security to be free

Table of Contents

Product Version: 10.7 Linux (GA)

Document Number: 007-013842-001, Rev. C

Release Date: June 2019

Support Contacts

We work closely with our reseller partners to offer the best worldwide technical support services. Your reseller is the first line of support when you have questions about products and services. However, if you require additional assistance you can contact us directly at:

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

Additional Documentation

The following publications are available:

- 007-013843-001 SafeNet Authentication Client 10.7 Linux (GA) User Guide (Rev C)
- 007-013841-001 SafeNet Authentication Client 10.7 Linux (GA) Release Notes (Rev D)

Introduction

SafeNet Authentication Client (SAC) is a middleware client that manages Gemalto's extensive SafeNet portfolio of certificate-based authenticators, including eToken, IDPrime smart cards, USB and software-based devices.

With full backward compatibility and incorporating features from previous middleware versions, SafeNet Authentication Client ensures complete support for all currently deployed eToken devices, as well as IDPrime MD and .NET smart cards.

Overview

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.

The SafeNet Authentication Client Tools application and the SafeNet Authentication Client tray icon application are installed with SafeNet Authentication Client, providing easy-to-use configuration tools for users and administrators.

> **NOTE**:
> The term Token is used throughout the document and is applicable to both Smart Cards and Tokens.

License Activation

SafeNet Authentication Client 10.7 Linux (GA) is installed by default as non-licensed.

To activate the license perform the following steps:

1. Obtain a valid SAC License Key from SafeNet Customer Service.
2. Activate the license using one of the following procedures:
    - Manual Activation

    See the *Licensing* chapter in the *SafeNet Authentication Client 10.7 Linux (GA) User Guide*.

> **NOTE**:
> SafeNet Authentication Client retrieves the license file (SACLicense.lic) automatically, if the license file is located in the following default path:
> **Linux (per user): /home/<user name>**
> **Linux (per machine): /etc/**

IDPrime MD Applet 4.0

The IDPrime MD Applet 4.0 is Common Criteria certified on IDPrime MD 840 and 3840. These cards can have certain parameters customized in the factory with different values to the standard default profile. See the SafeNet Authentication Client Release Notes for a list of supported smart cards and tokens.

> **NOTE**:
> The IDPrime MD 840/ 3840 cards or eToken 5110 CC do not support modifying the retry counter on the Admin Key.
> The recommended workaround is to set the profiles with a PUK instead of the Admin Key.
> To ensure maximum security, when using friendly mode, set the password with at least 16 random
> printable characters.

The following parameters can be customized:

- Number and type of key containers
- Support of RSA 4,096-bit key containers (import operation only) - Note: The card needs to be configured by the SAC supported key length.
- Change PIN at first use Secure messaging in contactless mode
- PINs (#1, #3 and #4 only)
- Try Limit
- Unblock PIN (PIN#1 only)
- Policy values
- Properties
- PIN validity period
- Secure messaging in contactless mode

Number and Type of Key Containers

The list below are the default settings. For other options consult your Gemalto representative.

By default, the IDPrime MD Applet 4.0 is pre-personalized with:

- 2 X 2,048-bit CC Sign Only RSA Keys
- 2 X 1,024-bit Standard Sign and Decrypt RSA Keys
- 8 X 2,048-bit Standard Sign and Decrypt RSA Keys
- 2 X 256-bit Standard Sign and Decrypt EC Keys

By default, the IDPrime MD Applet 4.4.2 is pre-personalized with:

- 2 X 2,048-bit CC Sign Only RSA Keys
- 2 X 4096-bit CC Sign Only RSA Keys
- 8 X 256-bit CC Sign Only RSA Keys

> **NOTE**:
> The Key Generation method for CC key containers is either OBKG or Key import.

API Adjustments

The table below provides a high-level description of the adjustments that can be made to the Standard and Extended PKCS#11 API to work with IDPrime MD CC devices. For more detailed information, see the code samples.

Standard PKCS#11 API	Extended PKCS#11 API
The `C_InitToken` function must receive the current Security Officer (SO) Password	The `C_InitToken` function must receive the current Security Officer (SO) Password
When the `C_InitToken` function is called, you can enable linked mode on the IDPrime MD CC device by using the following setting: Set the linked mode value to `1` in `/etc/eToken.conf` under the `[Init]` section and the device must be in the factory initialized state (Admin key = 48 zeros, PUK = 6 zeros) To revert a device back to unlinked mode after it was initialized in linked mode, use the PKCS#11 Extended API, or by using SAC Tools initialization process.	To initialize the IDPrime MD CC device, the `ETCKA_CC` attribute must be set to `CK_TRUE`. To initialize a device in linked mode, set the `ETCKA_IDP_CC_LINK` attribute to `1`. To pass the current Digital Signature PUK value, use the `ETCKA_IDP_CURRENT_PUK` attribute. To revert a device back to unlinked mode after it was initialized in linked mode, set the `ETCKA_IDP_CC_LINK` attribute to `0` and use the `ETCKA_PUK` attribute to set the new Digital Signature PUK value.
If a device is not configured to use linked mode, the `C_InitToken` function ignores the Digital Signature PUK and Digital Signature PIN.	If a device is not configured to use linked mode, use the `ETCKA_PUK` attribute to set the new Digital Signature PUK value.
After the device has been initialized in linked mode, the `C_InitPIN` function initializes the Digital Signature PIN and the User PIN. Both PIN's are set to the same value. The `C_SetPIN` function used with the `CKU_SO` flag changes both the Administrator PIN and Digital Signature PUK to a new value. See the SafeNet Authentication Client User Guide for details on Friendly Admin Password. The C_SetPIN function used with the CKU_USER flag changes both the User PIN and Digital Signature PIN to a new value.	If the device is initialized to use linked mode, the `C_InitPIN` function and `C_SetPIN` function behaves the same as described in the Standard PKCS#11 section.

SafeNet eToken devices vs Gemalto IDPrime MD devices

The table below displays the differences between SafeNet eToken devices and Gemalto IDPrime MD devices.

Feature	eToken 5110, eToken 5110 FIPS (and all other eToken based devices)	IDPrime MD, IDPrime .Net, eToken 5110 CC
Initialization	3 Roles (Initialization key, Admin PIN, User PIN)	2 Roles (Admin PIN and User PIN)
	Device erased by using the Initialization key	Device is cleared by using the Admin PIN (no changes are made to the scheme)
	Initialization key is used only for initializing the device.	If the Admin PIN is locked, the device cannot be cleared
Profile	Dynamic profile that allows an unlimited number of keys depending on the devices memory capacity	FIPS based devices - Dynamic profile limited to 15 key containers
		CC based devices - Static profile defined by perso
Password Policy	Off-Board (saved on token)	On-Board
	Full UTF-8 character encoding capabilities supported	Only ASCII character codes supported
Enhanced Security Mode	Support Propriety RSM mode	Support Secure Key Injection (via IDGo800 Minidriver)
On Board RSAPadding (PSS/OAEP)	Not supported	Supported
Common Criteria	Deprecated	4 Roles (Admin PIN, User PIN, Digital Signature PIN, Digital Signature PUK).
	Digital Signature PIN is derived from the User PIN and the Digital Signature PUK is derived from the Administrator PIN	Linked mode - User PIN and Digital Signature PIN are identical and Digital Signature PUK is derived from Admin PIN Unlinked mode - each role has a different value
	Appropriate Athena CC certified Applet for CC keys	Gemalto CC certified Applet
Symmetric Key operations	Support 3DES and AES	Not supported
Protocol for Contact	Support T1	Support T1, T0 and CTL

Security Recommendations

Enforcing Restrictive Cryptographic Policies

To allow organizations to enforce restrictive cryptographic policies when using SafeNet smart card and USB tokens, the following enhancements were introduced:

- Key Management Security Policy - See Security Settings on page 46 for more details.
- Disable Cryptographic Algorithm Policy - See Security Settings on page 46 for more details.

The motivation behind these enhancements:

- Legacy cryptographic schemes can cause organizations to fail current compliance requirements or expose cryptographic weakness associated with obsolete algorithms and mechanisms.

The following enhancements were made to SafeNet Authentication Client to allow organizations to block the use of such schemes, according to organizational policies.

- Enabling symmetric keys wrapping with other symmetric keys using GCM and CCM modes of operation.
- Preventing legacy algorithms from being used by adding a key wrapping policy that enforces the usage of only GCM and CCM modes of operation for symmetric encryption, and PKCS#1 v2.1 padding for RSA encryption.
- SafeNet introduced a new mechanism that allows administrators to prevent the use of legacy or obsolete algorithms by third-party applications. These cryptographic algorithms conform to the National Institute of Standards and Technology (NIST), preventing third-party applications from using legacy or obsolete algorithms.

Once a restrictive policy has been set, the use of SafeNet Authentication Client with the above algorithms will be blocked. This might have implications on the way in which the third-party's applications currently work.

> **NOTE**:
> Administrators must make sure that the third-party applications used by the organization are configured accordingly and do no use one of the algorithms listed above, as they will be blocked.

Create Symmetric Key Objects using PKCS#11

As part of SafeNet Authentication Client security enhancement campaign, the following was performed:

- Protected memory was used when working with the private cache between PKCS#11 API calls. Private cache is unlocked to retrieve data and then locked immediately after retrieving the data to ensure that there is no sensitive data in the private cache. This ensures that the key cannot be revealed in plain text.
- Sensitive data is securely zeroed prior to freeing up the memory.
- AES and Generic symmetric key files were created with Secured Messaging (SM) protection so that the Microsoft smart card transport layer does not contain any APDU data with plain symmetric key material.
- For Secure Messaging (SM) to support the AES/3DES and Generic symmetric keys, the keys must be created on an eToken Java device that is initialized in FIPS/CC mode. Applying SM to symmetric keys changes the object format on the smart card, resulting in the keys not being backward compatible.
- Keys that are created with previous SAC versions or on eToken Java devices which are formatted in non-FIPS/CC mode will not be protected by SM.

    AES/3DES keys that are created using the `CKA_SENSITIVE = TRUE` and `CKA_EXTRACTABLE = FALSE` attributes are backward compatible (BS Object keys).

Installation

Follow the installation procedures below to install SafeNet Authentication Client 10.7 Linux. Local administrator rights are required to install or uninstall SafeNet Authentication Client.

Installation Files

The software package provided by SafeNet includes files for installing or upgrading to SafeNet Authentication Client 10.7 Linux (GA). The following Linux installation and documentation files are provided:

File		Description/Use
SafenetAuthenticationClient-10.7.xx-0.i386.rpm	32-bit	Installs SafeNet Authentication Client on a 32 bit platform
SafenetAuthenticationClient-10.7.xx-0.x86_64.rpm	64-bit	Installs SafeNet Authentication Client on a 64 bit platform.
RPM-GPG-KEYSafenetAuthenticationClient	32-bit 64-bit	This file is the public key (GnuPG) for SafeNet rpm files. Relevant only for RPM. The signature confirms that the package was signed by an authorized party and also confirms the integrity and origin of your file. Use this file to verify the signature of the RPM files before installing them to ensure that they have not been altered from the original source of the packages.
SafenetAuthenticationClient-core-10.7.xx-0.i386.rpm	32-bit	Installs SafeNet Authentication Client core on 32 bit platform. Installs eToken core library and IFD Handler.
SafenetAuthenticationClient-core-10.7.xx-0.x86_64.rpm	64-bit	Installs SafeNet Authentication Client core on 64 bit platform. Installs eToken core library and IFD Handler.
SafenetAuthenticationClient-10.7.xx-0_i386.deb	32-bit	Installs SafeNet Authentication Client on 32 bit platform.
SafenetAuthenticationClient-10.7.xx-0_amd64.deb	64-bit	Installs SafeNet Authentication Client on 64 bit platform.
SafenetAuthenticationClient-core-10.7.xx-0_i386.deb	32-bit	Installs SafeNet Authentication Client core on 32 bit platform. Installs eToken core library and IFD Handler.
SafenetAuthenticationClient-core-10.7.xx-0_i386.deb	64-bit	Installs SafeNet Authentication Client core on 32 bit platform. Installs eToken core library and IFD Handler.
Documentation Files		
007-013841-001_SafeNet Authentication Client_10.7_Linux_GA_RN_Revision D		SafeNet Authentication Client 10.7 Linux (GA) Release Notes
007-013843-001_SafeNet Authentication Client_10.7_Linux_GA_User_Guide_Revision C		SafeNet Authentication Client 10.7 Linux (GA) User Guide
007-013842-001_SafeNet Authentication Client_10.7_Linux_GA_Administrator_Guide_Revision C		SafeNet Authentication Client 10.7 Linux (GA) Administrator Guide (this document)

Installing SAC on Linux Standard Package

The installation package for SafeNet Authentication Client on Red Hat, SUSE, CentOS and Fedora is the RPM Package. RPM is an installation file that can install, uninstall, and update software packages.

For the PKCS11 module to be installed automatically on a Firefox browser during the SAC installation, make sure the **nss-tools** package is installed prior to installing SAC.

- On SUSE, Fedora, Centos and Red Hat operating systems, in cases where the nss-tool package is not installed, install it as a privileged user by running the following command: `yum install nss-tools`

SafeNet Authentication Client .rpm packages include:

- **.rpm Package Name:**
  - 32-bit - `SafenetAuthenticationClient-10.7.xx-0.i386.rpm`
  - 64-bit - `SafenetAuthenticationClient-10.7.xx-0.x86_64.rpm`

  where: `xx` is the build number

To install from the terminal:

1. On the terminal, log on as a root user.
2. Run the following:

   `rpm --import RPM-GPG-KEY-SafenetAuthenticationClient`

3. Run one of the following:
   - On a 32-bit OS: `rpm -Uvh SafenetAuthenticationClient-10.7.xx-0.i386.rpm`
   - On a 64-bit OS: `rpm -Uvh SafenetAuthenticationClient-10.7.xx-0.x86_64.rpm`

   where: `-hi` is the parameter for installation and `x` is the version number.

Installing on Ubuntu and Debian

The installation packaging for SafeNet Authentication Client running on Ubuntu is the Debian software package (.deb).

> 📝 **NOTE**:
> • For the PKCS#11 module to be installed automatically on a Firefox browser during the SAC installation, make sure the **nss-tools** package is installed prior to installing SAC.
> • Using SAC 32-bit on a 64-bit system is not support for .deb packages. The SAC .deb package does not support Multiarch.

The following is the SafeNet Authentication Client .deb package:

- .deb Package Name:
  - 32-bit: `SafenetAuthenticationClient-10.7.xx-0_i386.deb`
  - 64-bit: `SafenetAuthenticationClient-10.7.xx-0_amd64.deb`
    where: `xx` is the build number

To install from the package installer:

1. Double-click the relevant `.deb` file.
   The package installer opens.

2. Click **Install Package**.
   A password prompt appears.

3. Enter the Super User or root password.
   The installation process runs.

4. To run SafeNet Authentication Client Tools, go to **Applications > SafeNet > SafeNet Authentication Client > SafeNet Authentication Client Tools.**

> 📝 **NOTE**:
> To enable the tray icon menu in the notification area, log out and log back in for the icon to appear.

To install from the terminal:

1. Enter the following:
   - On a 32-bit OS: `sudo dpkg -i SafenetAuthenticationClient-10.7.xx-0_i386.deb`
   - On a 64-bit OS: `sudo dpkg -i SafenetAuthenticationClient-10.7.xx-0_amd64.deb`
     where: `xx` is the build number

   A password prompt appears.

2. Enter the password.
   The installation process runs.

3. If the installation fails due to a lack of dependencies, enter the following:
   ```
   sudo apt-get install -f
   ```

The dependencies are installed and the installation continues.

4. To run the SafeNet Authentication Client Quick Menu, go to: **Applications > SafeNet >SafeNet Authentication Client > SafeNet Authentication Client Tools.**

> 📝 **NOTE**:
> Ensure you log out and log back in to see the tray icon menu.

Installing the Core Package

Installing on Red Hat Enterprise, SUSE, CentOS and Fedora

The installation package for SafeNet Authentication Client running on RedHat and CentOS is the RPM Package Manager. RPM is a command line package management system that can install, uninstall, and update software packages.

SafeNet Authentication Client `.rpm` **packages include:**

.rpm Package Name:

- **32-bit:** `SafenetAuthenticationClient-core-10.7.xx-0.i386.rpm`
- **64-bit:** `SafenetAuthenticationClient-core-10.7.xx-0.x86_64.rpm`

   where: `x` is the build number

To install from the package installer:

1. Double-click the relevant `.rpm` file.
   The package installer opens.
2. Click Install Package.
   A password prompt appears.
3. Enter the Super User or root password.
   The installation process runs.

To install from the terminal:

1. On the terminal, log on as a root user.
2. Run the following:

   `rpm --import RPM-GPG-KEY-SafenetAuthenticationClient`
3. Run one of the following:
   - **On a 32-bit OS:** `rpm -hi SafenetAuthenticationClient-core-10.7.xx-0.i386.rpm`
   - **On a 64-bit OS:** `rpm -hi SafenetAuthenticationClient-core-10.7.xx-0.x86_64.rpm`

      where: `-hi` is the parameter for installation and `x` is the version number.

Installing on Ubuntu and Debian

> 📝 **NOTE**:
> - When installing from the user interface with a user that is not an administrator, the following message is displayed: 'The package is of bad quality'. Click **Ignore and Install** and continue with the installation.
> - After installing SAC on Ubuntu, log off, and then log back on in order for the SAC monitor to run, and to display the tray icon.

The installation packaging for SafeNet Authentication Client running on Ubuntu is the Debian software package (.deb).

The following is the SafeNet Authentication Client .deb package:

- **.deb Package Name:**
    - 32-bit: `SafenetAuthenticationClient-core-10.7.xx-0_i386.deb`
    - 64-bit: `SafenetAuthenticationClient-core-10.7.xx-0_amd64.deb`

    where: `xx` is the build number

To install from the package installer:

1. Double-click the relevant .deb file.

    The package installer opens.

2. Click **Install Package**.

    A password prompt appears.

3. Enter the Super User or root password.

    The installation process runs.

To install from the terminal:

1. Enter the following:
    - On a 32-bit OS: `sudo dpkg -i SafenetAuthenticationClient-core-10.7.xx-0_i386.deb`
    - On a 64-bit OS: `sudo dpkg -i SafenetAuthenticationClient-core-10.7.xx-0_amd64.deb`

    where: n is the version number

    A password prompt appears.

2. Enter the password.

    The installation process runs.

3. If the installation fails due to a lack of dependencies, enter the following:

    `sudo apt-get install -f`

    The dependencies are installed and the installation continues.

Linux External Dependencies

Red Had Enterprise, SUSE, CentOS, Fedora and Ubuntu

- PCSC (Smart Card Resource manager): libpcsclite1
- Prerequisite - SAC 10.7 requires OpenSSL 1.0 or higher to be installed.

Installing the Firefox Security Module on Linux

When SafeNet Authentication Client is installed, it does not install the security module in Firefox. This must be done manually.

To install the security module in Firefox

1. Open **Firefox Preferences > Advanced >Certificates**.

2. On the *Encryption* tab click **Security Devices**.

   The *Device Manager* window opens.

3. Click **Load**.

   The *Load PKCS#11 Device* window opens.

4. In the Module Filename field enter the following string:

   ```
   On 32-bit: /usr/lib/libeTPkcs11.so

   On 64-bit: /usr/lib64/libeTPkcs11.so
   ```

   📝 **NOTE**:
   - To work with CC devices in unlinked mode, enter the following string for Multi-Slot support:
     for 32-bit: /usr/lib/libIDPrimePKCS11.so
     for 64-bit: /usr/lib64/libIDPrimePKCS11.so
   - For information on how to work with Multi-Slots, see the PKCS#11 Digital Signature PIN Authentication section of the SafeNet Authentication Client User Guide.

   The *Confirm* window opens.

5. Click **OK**.

   The new security module is installed.

Installing the Thunderbird Security Module

When SafeNet Authentication Client is installed, it does not install the security module in Thunderbird. This must be done manually.

To install the security module in Thunderbird

1. Select **Thunderbird > Preferences > Advanced**.

2. On the *Security* tab click **Security Devices**.

    The *Device Manager* window opens.

3. Click **Load**.

    The *Load PKCS#11 Device* window opens.

4. In the Module Filename field enter the following string:

    On 32-bit: /usr/lib/libeTPkcs11.so

    On 64-bit: /usr/lib64/libeTPkcs11.so

    > 📝 **NOTE**:
    > - To work with CC devices in unlinked mode, enter the following string for Multi-Slot support:
    >   **for 32-bit: /usr/lib/libIDPrimePKCS11.so**
    >   **for 64-bit: /usr/lib64/libIDPrimePKCS11.so**
    > - For information on how to work with Multi-Slots, see the PKCS#11 Digital Signature PIN Authentication section of the SafeNet Authentication Client User Guide.

    The *Confirm* window opens.

5. Click **OK**.

    The new security module is installed.

Uninstall

After SafeNet Authentication Client 10.7 Linux has been installed, it can be uninstalled. Local administrator rights are required to uninstall SafeNet Authentication Client. When SafeNet Authentication Client is uninstalled, user configuration and policy files may be deleted.

Uninstalling Linux Standard Package

Before uninstalling SafeNet Authentication Client 10.7 Linux, make sure that SafeNet Authentication Client Tools is closed.

Uninstalling on Red Hat Enterprise, SUSE, CentOS and Fedora

To uninstall:

- Enter the following:

    ```
    rpm -e SafenetAuthenticationClient-10.7.xx-0.i386.rpm
    ```

    Where `-e` is the parameter for uninstalling.

Uninstalling on Ubuntu and Debian

To uninstall:

- In the console, enter the following:

    ```
    sudo dpkg --purge safenetauthenticationclient
    ```

    Where `--purge` is the parameter for uninstalling.

Uninstalling the Core Package

Uninstalling on Red Hat Enterprise, SUSE, CentOS and Fedora

To uninstall:

- Enter the following:

  ```
  rpm -e SafenetAuthenticationClient-core-10.7.xx-0.i386.rpm
  ```

  Where -e is the parameter for uninstalling.

Uninstalling on Ubuntu or Debian

To uninstall:

- In the console, enter the following:

  ```
  SafenetAuthenticationClient-core-10.7.xx-0_i386.deb
  ```

  Where --purge is the parameter for uninstalling.

Configuration Properties

SafeNet Authentication Client properties are stored on the computer as ini files which can be added and changed to determine SafeNet Authentication Client behavior. Depending on where an ini value is written, it will apply globally, or be limited to a specific user or application.

> **NOTE**:
> All properties can be manually set and edited.

General Settings

The following settings are written to the `[General]` section in: `/etc/eToken.conf`

> **NOTE**:
> On a Linux machine, the number of slots is determined by the PcscSlots and SoftwareSlots configuration keys described here. The Reader Settings window in SafeNet Authentication Client Linux Tools displays the number of slots that have been configured, but does not allow the user to change the settings.

Description	Value
Unlock Authorization Activates authorization protection for SAC Tools Unlock feature.	**Registry Value Name:** UnlockAuthorization **Value:** **0** - Do not activate authorization protection **1** - Activate authorization protection **Default**: 0
Read Only Mode Prevents deletion of certificates from the Token. **Note:** When a user deletes certificates on a Firefox browser and this property is set to 'Selected', Firefox displays these certificates as deleted when in fact they are not.	**Registry Value Name:** ReadOnlyMode **Values:** **0 - Disabled** - any user with the right permission can delete the certificates and their associated keys. **1 - Enabled** - certificates and their associated keys cannot be deleted. **Default**: **0**

Description (Cont.)	Value (Cont.)
Multi-Slot Support Determines if SafeNet Authentication Client is backward compatible with Gemalto PKCS#11 Common Criteria devices (IDPrime MD 840, IDPrime MD 3840 and eToken 5110 CC). The Multi-Slot feature affects only SAC customized in compatible mode via IDPrimePKCS11.so For more information on Multi-Slots, see the PKCS#11 Digital Signature PIN Authentication section of the SafeNet Authentication Client User Guide. **Note:** Linked Mode is not compatible with the Multi-Slot feature.	**Value Name:** MultiSlotSupport **Values**: **Selected** - Activates this feature **Not Selected** - Normal operation **Default**: Not Selected
Touch Sense Notify Determines if the Touch Sense notification is displayed as balloon or in a window.	**Registry Value Name:** TSNotify **Values:** 0 - Show window 1 - Show balloon 2 - No notification **Default**: 1 (Show balloon)
PIN Pad Notify Determines if the Pin Pad notification is displayed as balloon or in a window.	**Registry Value Name:** PinPadNotify Values: 0 - Show window 1 - Show balloon 2 - No notification -Default: 0 (Show window)
Full SM Mode Enables/disables the full Security Messaging (SM) mode for IDPrime MD FIPS L2 devices. **Note:** SAC cache must be reset after changing the FullSMMode property. This configuration is for applet 4.3.5 L2 cards only.	**Registry Value Name:** FullSMMode **Values:** **0 (False)** - Disabled **1 (True)** - FIPS L2 only **Default:** 0 (Disabled)
No Pin Pad Determines whether or not the PIN Pad reader is used as a regular smart card reader. SAC UI will require entering user credentials.	**Registry Value Name:** NoPinPad **Values:** **0** - Disabled **1** - Enabled **Default:** 0 (Disabled)

Description (Cont.)	Value (Cont.)
ITI Certification Mode Enables ITI Certification, which requires the following: • Administrator and User Passwords must be changed at first logon. • If Initialization is performed without changing the Administrator and User Passwords at first logon, the Administrator Password is required for the initialization process. **Note:** When the ITI Certification Mode property is enabled, the Enable Administrator Password Quality Check property will be disabled.	**Registry Value Name:** MustChangeAdmin **Values**: **0**- None **1** - ITI certification mode **2** - Special administrator PIN policy **Default**: 0
Software Slots Defines the number of virtual readers for SafeNet Virtual Tokens. **Note:** Can be modified in 'Reader Settings' in SafeNet Authentication Client Tools also. On systems later than Windows 7 and Window 2008 R2, the total number of readers is limited to 10 from among: eToken readers, third-party readers, and reader emulations.	**Value Name:** SoftwareSlots **Values**: >=0 (0 = SafeNet Virtual Token is disabled; only physical tokens are enabled) **Default**: 2
PCSC Slots Defines the total number of PC/SC slots for all USB tokens and smartcards. Included in this total: • the number of allocated readers for third-party providers • the number of allocated readers for other SafeNet physical tokens, which can be modified in 'Reader Settings' in SafeNet Authentication Client Tools **Note:** On systems later than Windows 7 and Window 2008 R2, the total number of readers, consisting of this value and any enabled reader emulations, is limited to 10.	**Value Name:** PcscSlots **Values**: >=0 (0 = Physical tokens are disabled) **Default**: 8
Legacy Manufacturer Name Determines if 'Aladdin Knowledge Systems Ltd.' is written as the manufacturer name in token and token slot descriptions Use for legacy compatibility only	**Value Name:** LegacyManufacturerName Values: **1** - The legacy manufacturer name is written **0** - The new manufacturer name is written **Default**: 0
Enable Private Cache Determines if SafeNet Authentication Client allows the token's private data to be cached. Applies only to tokens that were initialized with the private data cache setting. The private data is cached in per process memory. **Note:** Can be set in SafeNet Authentication Client Tools	**Value Name:** EnablePrvCache **Values**: **1 (True)** - Private data caching is enabled **0 (False)** - Private data caching is disabled **Default**:1 (True)

Description (Cont.)	Value (Cont.)
Tolerate Finalize Determines if C_Finalize can be called by DllMain **Note:** Define this property per process Select this setting when using Novell Modular Authentication Service (NMAS) applications only	**Value Name:** TolerantFinalize **Values**: **1 (True)** - C_Finalize can be called by DllMain **0 (False)** - C_Finalize cannot be called by DllMain **Default**: 0 (False)
Tolerate X509 Attributes Determines if CKA_SERIAL_NUMBER, CKA_SUBJECT, and CKA_ISSUER attributes can differ from those in CKA_VALUE during certificate creation **Note:** Enable TolerantX509Attributes when using certificates created in a non- DER encoded binary x.509 format. In some versions of PKI Client, this setting was not selected by default.	**Value Name:** TolerantX509Attributes **Values**: **1 (True)** - The attributes can differ **0 (False**) - Check that the values match **Default**: 0 (False)
Tolerate Find Templates Determines if PKCS#11 tolerates a Find function with an invalid template, returning an empty list instead of an error.	**Value Name:** TolerantFindObjects **Values**: **1 (True)** - A Find function with an invalid template is tolerated and returns an empty list **0 (False)** - A Find function with an invalid template is not tolerated and returns an error **Default**: 0 (False)
Disconnect SafeNet Virtual Token on Logoff Determines if SafeNet Virtual Tokens are disconnected when the user logs off.	**Value Name:** EtvLogoffUnplug **Values**: **1 (True)** - Disconnect SafeNet Virtual Token when logging off **0 (False)** - Do not disconnect SafeNet Virtual Token when logging off **Default**: 0 (False)
Protect Symmetric Keys Determines if symmetric keys are protected **Note:** If selected, even non-sensitive symmetric keys cannot be extracted	**Value Name:** SensitiveSecret **Values**: **1** - Symmetric keys cannot be extracted **0** - Symmetric keys can be extracted **Default**: 0

Description (Cont.)	Value (Cont.)
Cache Marker Timeout Determines if SAC Service periodically inspects the cache markers of connected tokens for an indication that token content has changed **Note:** If tokens were initialized as "eToken PKI Client 3.65 compatible" in SafeNet Authentication Client 8.0 and later, set this value to 0 to improve performance.	**Value Name:** CacheMarkerTimeout **Values**: **1** - Connected tokens' cache markers are periodically inspected **0** - Connected tokens' cache markers are never inspected **Default**: 0
Override Non-Repudiation OIDs Overrides SAC's list of standard certificate OIDs that require a high level of security **Note:** Users must log on to their tokens whenever signing with a certificate defined as non-repudiation. To avoid having to authenticate every time a cryptographic operation is required for certificates containing Entrust certificate OID details, remove the default registration key value.	**Value Name:** NonRepudiationOID **Value**: Empty **Default**: No override
Ignore Silent Mode Determines if the *Token Logon* window is displayed even when the application calls the CSP/KSP in silent mode.	**Value Name:** IgnoreSilentMode **Values**: **1 (True)** - Display the *Token Logon* window even in silent mode **0 (False)** - Respect silent mode **Note:** Set to True when the SafeNet RSA KSP must use SHA-2 to enroll a CA private key to a token **Default**: 0 (False)

Initialization Settings

The following settings are written to the `[INIT]` section in: `/etc/eToken.conf`

> 📝 **NOTE**:
> All setting in this section are not relevant to IDPrime MD cards, except for the LinkMode setting.

Description	Value
Maximum Token Password Retries Defines the default number of consecutive failed logon attempts that lock the token.	**Value Name:** UserMaxRetry **Values**: 1-15 **Default**: 15

Description	Value (Cont.)
Maximum Administrator Password Retries Defines the default number of consecutive failed administrator logon attempts that lock the token.	**Value Name:** AdminMaxRetry **Values**: 1-15 **Default**: 15
Force SO object on Token	**Registry Value Name:** ForceAdmin **Values**: **1(True)** - Token is initialized with SO object **0 (False)** - Token is initialized without SO object **Default:** 1 (True)
Force User object on Token	**Registry Value Name:** ForceUser **Values:** **1(True) -** Token is initialized with User object **0(False)** - Token is initialized without User object **Default:** 1(True)
Legacy Format Version Defines the default token format.	**Value Name:** Legacy-Format-Version **Values**: **0 -** Tokens are formatted as backwardly compatible to eToken PKI Client 3.65 (CardOS tokens only) **4** - Tokens are not formatted as backwardly compatible, and password quality settings can be saved on the token (CardOS tokens only) **5** - Format includes new RSA behavior that is not controlled by key size; each key is created in a separate directory (CardOS 4.20B FIPS or Java Card-based tokens only) **Default**: 4, for CardOS tokens 5, for 4.20B FIPS and Java Card -based tokens
RSA-2048 Determines if the token support 2048-bit RSA keys by default. **Note:** Can be set in SafeNet Authentication Client Tools.	**Value Name:** RSA-2048 **Values**: **1(True)** - 2048-bit RSA keys are supported **0 (False)** - 2048-bit RSA keys are not supported **Default:** 0 (False)

Description	Value (Cont.)
OTP Support Determines if the token supports OTP generation by default. This setting enables HMAC-SHA1 support, required by OTP tokens. **Note:** Can be set in SafeNet Authentication Client Tools.	**Value Name:** HMAC-SHA1 Values: **1 (True)** - OTP generation is supported **0 (False)** - OTP generation is not supported **Default**: 1 (True), for OTP tokens. 0 (False), for other tokens
RSA Area Size For CardOS-based tokens, defines the default size, in bytes, of the area to reserve for RSA keys. • The size of the area allocated on the token is determined during token initialization, and cannot be modified without initializing the token. • RSA-Area-Size is not relevant when Legacy-Format-Version is set to 5. **Note:** Can be set in SafeNet Authentication Client Tools.	**Value Name:** RSA-Area-Size **Default:** depends on the token size: • For 16 K tokens, enough bytes for three 1024-bit keys • For 32 K tokens, enough bytes for five 1024-bit keys • For larger tokens, enough bytes for seven 1024-bit keys
Default Token Name Defines the default Token Name written to tokens during initialization.	Value Name: DefaultLabel **Value**: String **Default**: My Token
API: Keep Token Settings When initializing the token using the SDK, determines if the token is automatically re-initialized with its current settings. **Note:** If selected, this setting overrides all other initialization settings.	Value Name: KeepTokenInit Values: **1 (True) -** Use current token settings **0 (False) -** Override current token settings **Default**: 0 (False)
Automatic Certification When initializing the token using the SDK. If the token has FIPS or Common Criteria certification, the token is automatically initialized with the original certification.	Value Name: Certification **Values**: **1(True)** - initialize the token with the original certification. **0 (False)** - initialize the token without the certification **Default:** 1 (True) **Note:** Previous to SAC 8.2, the default setting was 0 (False). As CardOS 4.2 does not support both FIPS and RSA-2048, failure to take this into account this may lead to token initialization failure when using PKCS#11. To prevent this, ensure that the default is set to False, or else ensure that the application provides both the required FIPS and RSA-2048 settings.

Description	Value (Cont.)
API: Private Data Caching If using an independent API for initialization, and if 'Enable Private Cache' is selected, determines the token's private data cache default behavior.	Value Name: PrvCachingMode Values: **0 -** Always 1 - While user is logged on **2 -** Never **Default:** 0 (Always)
Enable Private Data Caching Modification Determines if the token's Private Data Caching mode can be modified after initialization.	Value Name: PrvCachingModify Values: **1 (True) -** Can be modified **0 (False) -** Cannot be modified **Default**: 0 (False)
Private Data Caching Mode If 'Enable Private Data Caching Modification' is selected, determines who has rights to modify the token's Private Data Caching mode.	Value Name: PrvCachingOwner Values: **0** - Admin **1** - User **Default**: 0 (Admin)
API: RSA Secondary Authentication Mode If using an independent API for initialization, determines the default behavior for protecting RSA private keys on the token.	Value Name: 2ndAuthMode Values: **0** - Never **1** - Prompt on application request **2 -** Always prompt user 3- Always 4 - Token authentication on application request **Default**: **0** -(Never)
Enable RSA Secondary Authentication Modified Determines if the token's RSA secondary authentication can be modified after initialization.	Value Name: 2ndAuthModify Values: **1 (True) -** Can modify **0 (False) -** Cannot modify **Default**: 0 (False)

Description	Value (Cont.)
Use the same token and administrator passwords for digital signature operations.	Value Name: LinkMode Values: **1 (True) -** Linked **0 (False) -** Unlinked **Default**: 0 (False)

SafeNet Authentication Client Tools UI Initialization Settings

The following settings are written to the [AccessControl] section in: /etc/eToken.conf

Description	Value
Enable Advanced View Button Determines if the Advanced View icon is enabled in SAC Tools	**Value Name:** AdvancedView **Values**: **1** - Selected **0** - Not selected **Default**: 1

The following settings are written to the [InitApp] section in: /etc/eToken.conf/

Description	Value
Default Token Password Defines the default Token Password	**Value Name:** DefaultUserPassword **Values**: String **Default**: 1234567890
Enable Change Password on First Logon Determines if the "Token Password must be changed on first logon" option can be changed by the user in the Token Initialization window. **Note:** This option is selected by default. If the option is de-selected, it can be selected again only by setting the registry key.	**Value Name:** MustChangePasswordEnabled **Values**: **1** - Selected **0** - Not selected **Default**: 1
Change Password on First Logon Determines if the *Token Password must be changed on first logon* option is selected by default in the Token Initialization window.	**Value Name:** MustChangePassword **Value**: **1** - Selected **0** - Not selected **Default**: 1
Private Data Caching If *Enable Private Cache* is selected, determines the token's private data cache default behavior. **Note:** Can be set in SafeNet Authentication Client Tools. This option is not supported by IDPrime MD cards.	**Value Name:** PrivateDataCaching **Values**: **0 -** (fastest) private data is cached when used by an application while the user is logged on to the token, and erased only when the token is disconnected **1 -** private data is cached when used by an application while the user is logged on to the token, and erased when the user logs off or the token is disconnected **2** - private data is not cached **Default**: 0

Description (Cont.)	Value (Cont.)
RSA Secondary Authentication Mode Defines the default behavior for protecting RSA private keys on the token **Note:** Can be set in SafeNet Authentication Client Tools. This option is not supported by IDPrime MD cards.	**Value Name:** RSASecondaryAuthenticationMode Values: **0** - Never **1** - Prompt user on application request **2** - Always prompt user **3** - Always **4** - Token authentication on application request **Default**: **0**
RSA Secondary Authentication Mode (continued). **Note:** This option is not supported by IDPrime MD cards.	
Reuse Current Token Name Determines if the token's current Token Name is displayed as the default Token Name when the token is re initialized.	**Value Name:** ReadLabelFromToken **Values**: **1** -The current Token Name is displayed **0** -The current Token Name is ignored **Default**: 1
Maximum number of 1024-bit RSA keys Defines the amount of space to reserve on the token for Common Criteria certificates that use 1024 -bit RSA keys. **Note:** This option is not supported by IDPrime MD cards.	**Value Name:** NumOfCertificatesWith1024Keys_help **Values**: 0-16 certificates **Default**: 0
Maximum number of 2048-bit RSA keys Defines the amount of space to reserve on the token for Common Criteria certificates that use 2048-bit RSA keys. **Note:** This option is not supported by IDPrime MD cards.	**Value Name:** NumOfCertificatesWith2048Keys_help **Values**: 1-16 certificates **Default**: 4

SafeNet Authentication Client Tools UI Settings

The following settings are written to the `[UI]` section in: `/etc/eToken.conf`

Description	Value
Use Default Password Determines if the *Change Password on First Logon* process assumes the current Token Password is the default (defined in the Default Token Password), and does not prompt the user to supply it.	**Value Name**: UseDefaultPassword **Values**: **1 (True)** - The default Token Password is automatically entered in the password field **0 (False)** -The default Token Password is not automatically entered in the password field **Default**: o (False)
Password Term Defines the term used for the token's user password. **Note:** If a language other than English is used, ensure that the Password Terms are translated.	**Value Name**: PasswordTerm **Values** (String): Password PIN Passcode Passphrase **Default**: Password
Decimal Serial Number Determines if the Token Information window displays the token serial number in hexadecimal or in decimal format.	**Value Name:** ShowDecimalSerial **Values**: **1 (True)** -Displays the serial number in decimal format **0 (False)** -Displays the serial number in hexadecimal format **Default**: 0
Enable Tray Icon Determines if the application tray icon is displayed when SafeNet Authentication Client is started.	**Value Name**: ShowInTray **Values**: **0** - Never Show **1 -** Always Show **Default**: Always show
Enable Connection Notification Determines if a notification balloon is displayed when a token is connected or disconnected.	**Value Name**: ShowBalloonEvents **Values**: **0** - Not Displayed **1 -** Displayed **Default**: 0

Description (Cont.)	Value (Cont.)
Enable Logging Control Determines if the *Enable Loggin*g /*Disable Logging* button is enabled in the Client Settings Advanced tab	**Value Name:** AllowLogsControl **Values**: **1** -Enabled **0** -Disabled **Default**: 1
Home URL Overwrites the SafeNet home URL in SafeNet Authentication Client Tools	**Value Name:** HomeUrl **Values** (String): Valid URL **Default**: SafeNet's home URL
eToken Anywhere Determines if eToken Anywhere features are supported	**Value Name:** AnywhereExtendedMode **Values**: **1** -Supported **0** -Not supported **Default**: 1
Enable Certificate Expiration Warning Determines if a warning message is displayed when certificates on the token are about to expire.	**Value Name:** CertificateExpiryAlert **Values**: **1 (True)** - Notify the user **0 (False**) - Do not notify the user **Default**: 1 (True)
Ignore Archived Certificates Determines if archived certificates are ignored, and no warning message is displayed for certificates that are about to expire.	**Registry Value Name:** IgnoreArchivedCertificates **Values:** **1** - Archived certificates are ignored **0** - A warning message is displayed if the token contains archived certificates. **Default**: 1
Ignore Expired Certificates Determines if expired certificates are ignored, and no warning message is displayed for expired certificates	**Value Name:** IgnoreExpiredCertificates Values: **1** - Expired certificates are ignored **0** - A warning message is displayed if the token contains expired certificates **Default**: 0
Certificate Expiration Verification Frequency Defines the minimum interval, in days, between certificate expiration date verifications	**Value Name:** UpdateAlertMinInterval **Values**: > 0 **Default**: 14 days

Description (Cont.)	Value (Cont.)
Certificate Expiration Warning Period Defines the number of days before a certificate's expiration date during which a warning message is displayed.	**Value Name:** ExpiryAlertPeriodStart **Values**: > =0 (0 = No warning) **Default**: 30 days
Warning Message Title Defines the title to display in certificate expiration warning messages	**Value Name:** AlertTitle **Values**: String **Default**: SafeNet Authentication Client
Certificate Will Expire Warning Message Defines the warning message to display in a balloon during a certificate's "Certificate Expiration Warning Period."	**Value Name:** FutureAlertMessage **Values**: String **Default**: A certificate on your token expires in $EXPIRE_IN_DAYS days.
Expiry Date Format Defines the format of the certificate's expiry date (**$EXPIRY_DATE)** displayed in a balloon	**Registry Value Name:** EXPIRY_DATE_FORMAT **Values**: Set the year/month/day in the required order using the following format: %Y/%m/%d **Default**: %Y/%m/%d
Certificate Expired Warning Message Defines the warning message to display in a balloon if a certificate's expiration date has passed.	**Value Name:** PastAlertMessage **Values**: String **Default**: Update your token now.
Warning Message Click Action Defines what happens when the user clicks the message balloon.	**Value Name:** AlertMessageClickAction **Values**: **0 -** No action **1 -** Show detailed message **2 -** Open website **Default**: 0
Detailed Message If "Show detailed message" is selected in "Warning Message Click Action" setting, defines the detailed message to display.	**Value Name:** ActionDetailedMessage **Values**: String No default

Description (Cont.)	Value (Cont.)
Website URL If "Open website" is selected in the "Warning Message Click Action" setting, defines the URL to display	**Value Name:** ActionWebSiteURL **Values** (string): Website address **No default**
Enable Password Expiration Notification Determines if a pop-up message is displayed in the system when the Token Password is about to expire.	**Value Name:** NotifyPasswordExpiration **Values**: **1 (True)**- A message is displayed **0 (False)** - A message is not displayed **Default**: 1 (True)
Display Virtual Keyboard Determines if SafeNet's keystroke-secure Virtual Keyboard replaces standard keyboard entry of password fields in the following windows: • Token Logon • Change Password **Note:** The virtual keyboard supports English characters only.	**Value Name:** VirtualKeyboardOn **Values**: **1 (True)**- Virtual keyboard on **0 (False)** - Virtual keyboard off **Default**: 0 (False)
Password Policy Instructions If not empty, defines a string that replaces the default password policy description displayed in the *Unlock* and *Change Password* windows.	**Value Name:** PasswordPolicyInstructions **Values**: String
Define Initialization Mode Select this option if you want the 'Initialization Options' window (first window displayed when initializing a device) to be ignored.	**Value Name:** DefInitMode **Values**: 0 - Display the 'Initialization Options' window 1 - Set Preserve Mode 2 - Set Configure Mode **Default**: 0
Import Certificate Chain Determines if the certificate chain is imported to the token	**Value Name:** ImportCertChain **Values**: **0 -** Do not import certificate chain **1** - Import certificate chain **2**- User selects import behavior **Default**: 0

Description (Cont.)	Value (Cont.)
Prevent Must Change Password dialog popup Determines if the tray icon will display a popup message to prompt the user to change the user password for tokens that are not initialized.	**Registry Value Name:** DenyMustChangePopup **Values**: **0 -** Must Change Password pop-up message will not be displayed **1** - Must Change Password pop-up message will be displayed **Default**: 0

Token Password Quality Settings

The following settings are written to the [PQ] section in: /etc/eToken.conf

> 📝 **NOTE**:
> These settings are not relevant to IDPrime MD cards and eToken 5110 CC, as the password quality settings reside on the card itself.

Description	Value
Password - Minimum Length Defines the minimum password length. **Note:** Can be set in SafeNet Authentication Client Tools.	**Value Name:** pqMinLen **Values**: >=4 **Default**: 6
Password - Maximum Length Defines the maximum password length. **Note:** Can be set in SafeNet Authentication Client Tools.	**Value Name:** pqMaxLen **Values**: Cannot be less than the Password Minimum Length **Default**: 16
Password - Maximum Usage Period Defines the maximum number of days a password is valid. **Note:** Can be set in SafeNet Authentication Client Tools. **Note:** This parameter is 'Day Sensitive' i.e. the system counts the day's and not the hour in which the user made the change.	**Value Name:** pqMaxAge **Values**: >=0 (0 =No expiration) **Default**: 0
Password - Minimum Usage Period Defines the minimum number of days between password changes. **Note:** Can be set in SafeNet Authentication Client Tools. Does not apply to iKey devices.	**Value Name:** pqMinAge **Values**: >=0 (0 = No minimum) **Default**: 0

Description (Cont.)	Value (Cont.)
Password - Expiration Warning Period Defines the number of days before expiration during which a warning is displayed. **Note:** Can be set in SafeNet Authentication Client Tools.	**Value Name:** pqWarnPeriod **Values**: >=0 (0 = No warning) **Default**: 0
Password - History Size Defines the number of recent passwords that must not be repeated. **Note:** Can be set in SafeNet Authentication Client Tools.	**Value Name:** pqHistorySize **Values**: >= 0 (0 = No minimum) **Default**: 10 (iKey device history is limited to 6)
Password - Maximum Consecutive Repetitions Defines the maximum number of consecutive times a character can be used in a password. **Note:** Can be set in SafeNet Authentication Client Tools. **Note:** Does not apply to iKey devices.	**Value Name:** pqMaxRepeated **Values**: 0 - 16 (0 = No maximum) **Default**: 3
Password - Complexity Determines if there is a minimum number of character types that must be included in a new Token Password The character types are: upper-case letters, lower-case letters, numerals, and special characters. **Note:** Can be set in SafeNet Authentication Client Tools.	**Value Name:** pqMixChars **Values**: **1** - A minimum of 2 or 3 types must be included, as defined in the *Password- Minimum Mixed Character Type*s setting **0** -The rule for each character type is defined in the character type's *Include* setting **Default**: 1
Password - Minimum Mixed Character Types Defines the minimum number of character types that must be included in a new Token Password. The character types are: upper-case letters, lower-case letters, numerals, and special characters. **Note:** • Applies only when the *Password - Complex*ity setting is set to **Standard complexity.** • Can be set in SafeNet Authentication Client Tools.	**Value Name:** pqMixLevel **Values**: **0 -** At least 3 character types **1** - At least 2 character types **Default**:0
Password - Include Numerals Determines if the password can include numerals. **Note:** • Applies only when the *Password - Complex*ity setting is set to **Manual complexity.** • Can be set in SafeNet Authentication Client Tools.	**Value Name:** pqNumbers **Values**: 0 -Permitted 1 - Forbidden 2 - Mandatory **Default**: 0

Description (Cont.)	Value (Cont.)
Password - Include Upper-Case Determines if the password can include upper-case letters. **Note:** • Applies only when the *Password - Complexity* setting is set to **Manual complexity.** • Can be set in SafeNet Authentication Client Tools.	**Value Name:** pqUpperCase **Values**: 0 - Permitted 1 - Forbidden 2 - Mandatory **Default**: 0
Password - Include Lower-Case Determines if the password can include lower-case letters. **Note:** • Applies only when the *Password - Complexity* setting is set to **Manual complexity.** • Can be set in SafeNet Authentication Client Tools.	**Value Name:** pqLowerCase **Values**: 0 - Permitted 1 - Forbidden 2 - Mandatory **Default**: 0
Password - Include Special Characters Determines if the password can include special characters, such as @,!, &. **Note:** • Applies only when the *Password - Complexity* setting is set to **Manual complexity.** • Can be set in SafeNet Authentication Client Tools.	**Value Name:** pqSpecial **Values**: 0 - Permitted 1 - Forbidden 2 - Mandatory **Default**: 0
Password Quality Check on Initialization Determines if the password quality settings are checked and enforced when a token is initialized **Note:** We recommend that this policy not be set when tokens are enrolled using SafeNet Authentication Manager.	**Value Name:** pqCheckInit **Values**: **1 (True)** -The password quality is enforced **0 (False)** - The password quality is not enforced **Default**: 0
Password Quality Owner Defines the owner of the password quality settings on a re initialized token, and defines the default of the *Password Quality Modifiable* setting.	**Value Name:** pqOwner **Values**: **0** - Administrator **1** - User **Default**: 0, for tokens with an Administrator Password. 1, for tokens without an Administrator Password.

Description (Cont.)	Value (Cont.)
Enable Password Quality Modification Determines if the password quality settings on a newly initialized token can be modified by the owner. See the *Password Quality Owner* setting.	**Value Name:** pqModifiable **Values**: **1 (True)**- The password quality can be modified by the owner **0 (False)** - The password quality cannot be modified by the owner **Default**: 1 (True), for administrator-owned tokens 0 (False), for user owned tokens.
Enable Administrator Password Quality Check Determines if the Administrator Password Quality Check is enabled. When enabled, this property enforces an administrator (SO) password (on eToken and IDPrime devices) that has at least 3 different character types and a minimum length of 8 characters. The character types are: upper-case letters, lower-case letters, numerals, and special characters. **Note:** For backward compatibility on IDPrime devices, the Administrator Key can be used with 48 hexadecimal characters via the UI and/or 24 binary bytes via the API call. When disabled, the old behavior is as follows: **eToken:** minimum of 4 characters and no minimum character type enforcement **IDPrime:** minimum of 8 characters and no minimum character type enforcement, or the administrator key can be used. **Note:** When the ITI Certification mode property is enabled, the Enable Administrator Password Quality Check property will be disabled.	**Registry Key Name:** pqAdminPQ **Values**: **1 (Enabled)** - Administrator Password Quality is enforced **0 (Disabled)** - Administrator Password Quality is disabled **Default**: Enabled

SafeNet Authentication Client Tools UI Access Control List

Access Control Properties determine which features are enabled in the SafeNet Authentication Client Tools and Tray Menu.

The following settings are written to the `[AccessControl]` section in: `/etc/eToken.conf`

Access Control Feature	Value
All access control features listed below	**Values**: **1 (True)** - The feature is enabled. **0 (False)** - The feature is disabled. **Default**: 1(True), except where indicated in the table

The table lists all the *Access Control Features*.

> **NOTE**:
> All access control features are enabled by default, except where indicated in the table.

Access Control Feature	Value Name	Description
Crypto Notification Timeout	CryptoNotficationTimeout	Enables/Disables the notification: "The process may take a while..." Enter the time in seconds after which the notification is displayed. for example, the value 30 means the notification is delayed by 30 seconds. **Note:** By default the value is 0 (meaning this feature is disabled).
Rename Token	RenameToken	Enables/Disables the *Rename Token* feature in SafeNet Authentication Client Tools.
Change Token Password	ChangePassword	Enables/Disables the *Change Token Password* feature in SafeNet Authentication Client Tools.
Unlock Token	UnlockEtoken	Enables/Disables the *Unlock Token* feature in SafeNet Authentication Client Tools.
Delete Token Content	ClearEToken	Enables/Disables the *Delete Token Content* feature in SafeNet Authentication Client Tools.
View Token Information	ViewTokenInfo	Enables/Disables the *View Token Information* feature in SafeNet Authentication Client Tools.
Disconnect SafeNet Virtual Token	DisconnectVirtual	Enables/Disables the *Disconnect* SafeNet Virtual Token feature in SafeNet Authentication Client Tools.
Help	ShowHelp	Determines if the user can open the *Help* file in SafeNet Authentication Client Tools.
Advanced View	OpenAdvancedView	Determines if the user can open the Advanced View in SafeNet Authentication Client Tools.
Reader Settings	ManageReaders	Enables/Disables the *Reader Settings* feature in SafeNet Authentication Client Tools.
Connect SafeNet Virtual Token	AddeTokenVirtual	Enables/Disables the *Connect* SafeNet Virtual Token feature in SafeNet Authentication Client Tools.
Initialize Token	InitializeEToken	Enables/Disables the *Initialize Token* feature in SafeNet Authentication Client Tools.

Access Control Feature	Value Name (Cont.)	Description (Cont.)
Import Certificate	ImportCertificate	Enables/Disables the *Import Certificate* feature in SafeNet Authentication Client Tools.
Reset Default Certificate Selection	ClearDefaultCert	Enables/Disables the *Reset Default Certificate Selection* feature in SafeNet Authentication Client Tools.
Delete Certificate	DeleteCertificate	Enables/Disables the *Delete Certificate* feature in SafeNet Authentication ClientTools.
Export Certificate	ExportCertificate	Enables/Disables the *Export Certificate* feature in SafeNet Authentication Client Tools.
Copy Certificate Data to Clipboard	CopyCertificateData	Enables/Disables the *Copy Certificate Data to Clipboard* feature in SafeNet Authentication Client Tools.
Set Certificate as Default	SetCertificateAsDefault	Enables/Disables the *Set Certificate as Default* feature in SafeNet Authentication Client Tools.
Set Certificate as Auxiliary	SetCertificateAsAuxilary	Enables/Disables the *Set Certificate as Auxiliary* feature in SafeNet Authentication Client Tools.
Log On as Administrator	LoginAsAdministrator	Enables/Disables the *Log On as Administrator* feature in SafeNet Authentication Client Tools.
Change Administrator Password	ChangeAdministratorPassword	Enables/Disables the *Change Administrator Password* feature in SafeNet Authentication Client Tools.
Set Token Password	SetUserPassword	Enables/Disables the *Set Token Password* feature in SafeNet Authentication Client Tools.
Token Password Retries	AllowChangeUserMaxRetry	Enables/Disables the *Logon retries before token is locked* feature (for the Token Password) in SafeNet Authentication Client Tools.
Administrator Password Retries	AllowChangeAdminMaxRetry	Enables/Disables the *Logon retries before token is locked* feature (for the Administrator Password) in SafeNet Authentication Client Tools.
Advanced Initialization Settings	OpenAdvancedModeOfInitialize	Enables/Disables the *Advanced* button in the *Token Initialization* window in SafeNet Authentication Client Tools.
Change Initialization Key during Initialization	ChangeInitializationKeyDuringInitialize	Enables/Disables the *Change Initialization key* button in the *Advanced Token Initialization Settings* window in SafeNet Authentication Client Tools
Common Criteria Settings	CommonCriteriaPasswordSetting	Enables/Disables the Common Criteria option in the Certification combo box.
System Tray - Unlock Token	TrayIconUnlockEtoken	Enables/Disables the *Unlock Token* feature in the SafeNet Authentication Client Tray Menu
System Tray - Generate OTP	GenerateOTP	Enables/Disables the *Generate OTP* feature in the SafeNet Authentication Client Tray Menu
System Tray - Delete Token Content	TrayIconClearEToken	Enables/Disables the *Delete Token Content* feature in the SafeNet Authentication Client Tray Menu. **Note:** By default, this feature is **Disabled**
System Tray -Change Token Password	TrayIconChangePassword	Enables/Disables the *Change Token Password* feature in the SafeNet Authentication Client Tray Menu.

Access Control Feature	Value Name (Cont.)	Description (Cont.)
System Tray - Select Token	SwitcheToken	Enables/Disables the *Select Token* feature in the SafeNet Authentication Client Tray Menu.
System Tray - Synchronize Domain-Token Passwords	SyncDomainAndTokenPass	Enables/Disables the *Synchronize Domain Token Passwords* feature in the SafeNet Authentication Client Tray Menu.
System Tray - Tools	OpeneTokenProperties	Enables/Disables the *Tools* menu item (open SafeNet Authentication Client Tools) in the SafeNet Authentication Client Tray Menu.
System Tray - About	About	Enables/Disables the *About* menu item in the SafeNet Authentication Client Tray Menu.
Enable Change IdenTrust Identity	IdentrusChangePassword	Enables/Disables the *Change IdenTrust PIN* feature in SafeNet Authentication Client Tools.
Enable Unblock IdenTrust Passcode	IdentrusUnlock	Enables/Disables the *Unlock IdenTrust* feature in SafeNet Authentication Client Tools.
Delete Data Object	DeleteDataObject	Enables/Disables the *Delete Data Object* feature in SafeNet Authentication Client Tools.
Allow One Factor **Note:** This property cannot be set in the Access Control Properties window. It must be set in the registry key.	AllowOneFactor	Enables/Disables the *Allow One Factor* feature in the *Advanced Token Initialization Settings* window in SafeNet Authentication Client Tools.
PIN Type	PinType	Defines which GUI PIN Properties are enabled/disabled in SAC Tools 'Advanced' PIN Properties tab and the 'Initialization' window.
PIN Purpose	PinPurpose	
Cache Type	PinCacheType	
Cache Timeout	PinCacheInfo	
PIN Flags	PinFlags	
Ext. PIN Flags	PinFlagsEx	
Validity period (days)	PinValidity	
Expiration warning period (days)	PinWarning	

Access Control Feature	Value Name (Cont.)	Description (Cont.)
Minimum length (characters)	PinMinLen	Defines which GUI PIN Quality parameters are enabled/disabled in SAC Tools 'Advanced' tab and the 'Initialization' window.
Maximum length (characters)	PinMaxLen	
History size	PinHistory	
Number of different characters that can be repeated at least once	PinNumDiffCharRepeat	
Maximum number a characters can appear	PinMaxNumCharAppear	
Maximum number of characters in a sequence	PinMaxNumCharSequence	
Maximum number a character can be repeated in adjacent positions	PinMaxNumCharRepeatPos	
Numeric	PinNumber	
Alpha Upper	PinUpper	
Alpha Lower	PinLower	
Non alpha	PinSpecial	
Alpha	PinAlphabetic	
Non Ascii	PinNonAlphabetic	
Minimum usage period (days)	PinMinUse	
Maximum usage period (days)	PinMaxUse	
Must meet complexity requirements	PinComplexity	
Maximum consecutive repetitions	PinMaxRepeat	

Security Settings

The following settings are written to the `[Crypto]` section in: `/etc/eToken.conf`

Description	Value
Key Management Defines key creation, export, unwrap, and off-board crypto policies. SAC default behavior may be updated in future versions in order to comply with NIST requirements. It is up to the customer to check that it will be compatible with third-party applications.	**Value Name:** Key-Management-Security **Values**: (String) **Compatible** - enables the use of features that are deprecated in the Optimized and Strict configurations below. This was the default value for SAC versions below 10.5. Setting this value will cause SAC to be compatible with SAC 10.5 and below. It is strongly recommended to read *SAC Configuration Recommendations* on page 17 before applying legacy values. **Optimized:** Disable the generation or creation of exportable keys. Disable the exporting of keys, regardless of how they were generated. Disable any usage of symmetric keys off-board including unwrap. Disable the unwrap-PKCS1.5 and unwrap-AES-CBC on hardware tokens (session enable). **Strict:** Disable the generation or creation of exportable keys. Disable the exporting of keys, regardless of how they were generated. Disable any usage of symmetric keys off-board including unwrap. Disable all unwrap-PKCS1.5 and unwrap-AES-CBC operations. **Default**: Optimized

Description (Cont.)	Value (Cont.)
Deprecated Cryptographic Algorithms and Features The default list of deprecated cryptographic algorithms and features may be enhanced in order to comply with NIST requirements in future versions. It is up to the customer to check that it will be compatible with third-party applications.	**Value Name:** Disable-Crypto **Values**: (String) **None** - All SAC cryptographic algorithms and features are supported. This was the default value for SAC versions below 10.5. Setting this value will cause SAC to be compatible with SAC 10.5 and below. It is strongly recommended to read *SAC Configuration Recommendations* on page 17 before applying legacy values. **Obsolete** - A list of restricted and deprecated cryptographic algorithms and features. The following are deprecated: MD5, RC2, RC4, DES, 2DES, GenericSecret<112, RSA-RAW, RSA<2048, ECC<224, ECB, Sign-SHA1 **Manual** - Create your own list of deprecated algorithms and features. (See the description below). **Default**: Obsolete

The following can be disabled:

Algorithms:	RSA, ECC, DES, 2DES, 3DES, AES, RC2, RC4, GenericSecret
Hash types:	MD5, SHA1, SHA2
Padding types:	RAW, PKCS1, OAEP, PSS
Cipher modes:	ECB, CBC, CTR, CCM
Mechanisms:	MAC, HMAC, ECDSA, ECDH
Operations:	Encrypt, Decrypt, Sign, Verify, Generate, Derive, Wrap, Unwrap, Digest, Create (keys only)
Weak key size:	RSA<2048
Object types:	HWEF – elementary file (EF) objects (used by eToken devices for storing exportable symmetric keys and symmetric keys without on-board implementation) HWALL – all types of objects implemented on token (Base Security Object (BSO) and EF), ETV – eToken Virtual

Example of a manual configuration: Encrypt-DES-ECB, Sign-3DES-MAC, DES-CTR, HMAC-MD5, HMAC-SHA1, HMAC-SHA2, DES-CBC, Unwrap-DES-ECB, RSA-PKCS1-MD5, Verify-RSAPSS-SHA2, AES-CTR, AES-MAC, Decrypt-RC2, Wrap-ECB.

Log Settings

The following settings are written to the `[Log]` section in: `/etc/eToken.conf`

Description	Value
Enabled Determines if the SafeNet Authentication Client Log feature is enabled.	**Value Name:** Enabled **Value**: 1 - Enabled 0 - Disabled **Default**: 0 (Disabled)
Days Defines the number of days log files will be saved from the time the log feature was enabled.	**Value Name:** Days **Value**: Enter the number of days (numerical). **Default**: 1 day
MaxFileSize Defines the maximum size of an individual log file. Once the maximum fil size is reached, SAC removes older log records to allow saving newer log information.	**Value Name:** MaxFileSize **Value**: Enter a value in Bytes. **Default**: 2000000 (Bytes) (Approximately 2MB)
TotalMaxSizeMB Defines the total size of all the log files when in debug mode. (Megabytes).	**Value Name:** TotalMaxSizeMB **Value**: Enter a value in Megabytes. **Default**: 0 (Unlimited)
ManageTimeInterval Defines how often the TotalMaxSize parameter is checked to ensure the total maximum size has not been exceeded.	**Value Name:** ManageTimeInterval **Value**: Enter a value in minutes (numerical). **Default**: 60 minutes