



SafeNet Authentication Client 10.9 R1 (GA)

LINUX ADMINISTRATOR GUIDE



Document Information

Document Information

Product Version	10.9 R1 (GA)
Document Number	007-013842-003
Release Date	December 2025

Revision History

Revision	Date	Reason
Rev. B	December 2025	Updated for 10.9 R1 (GA) release

Trademarks, Copyrights, and Third-Party Software

2025 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales Group and/or its subsidiaries and affiliates, and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Disclaimer

All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and any of its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any information of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as “Thales”).

This document can be used for informational, non-commercial, internal, and personal use only provided that:

- > The copyright notice, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- > This document shall not be posted on any publicly accessible network computer or broadcast in any media, and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service, or loss of privacy.

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording or otherwise without the prior written permission of Thales Group.

CONTENTS

Document Information	2
Preface: About this Document	6
Audience	6
Document Conventions	6
Command Syntax and Typeface Conventions	6
Notifications and Alerts	7
Support Contacts	8
Chapter 1: Introduction	9
Overview	9
API Flow	10
Password Quality Information	10
PIN Retry Counter	12
Administrator PIN Retry Counter	12
User PIN Retry Counter	13
PUK PIN Retry Counter	13
PIN History Settings	13
Collecting SAC Logs	13
Guidelines for multiple certificates enrollment	14
Digital Signature Certificate Enrollment	14
Key Type Restrictions	14
Container Allocation Summary	14
PIV Contact and Contactless Mode	14
Chapter 2: Common Criteria	15
IDPrime Common Criteria Profile	15
Number and Type of Key Containers	15
Common Criteria API Adjustments	16
SafeNet eToken Devices vs SafeNet IDPrime Devices	17
Chapter 3: Installation	19
Installation Files	19
Installing the Standard Package	20
Installing on Red Hat Enterprise, SUSE, CentOS, and Fedora	20
Installing on Ubuntu (.deb)	21
Installing the Core Package	22
Installing on Red Hat Enterprise, SUSE, CentOS and Fedora	22
Installing on Ubuntu (.deb)	23
Linux External Dependencies	24
Installing the Firefox Security Module	24
Installing the Thunderbird Security Module	25

Changing SACTools Language	26
Chapter 4: Uninstall	27
Uninstalling the Standard Package	27
Uninstalling on Red Hat Enterprise, SUSE, CentOS, and Fedora	27
Uninstalling on Ubuntu (.deb)	27
Uninstalling the Core Package	27
Uninstalling on Red Hat Enterprise, SUSE, CentOS and Fedora	27
Uninstalling on Ubuntu (.deb)	27
Chapter 5: Configuration Properties	29
General Settings	29
Initialization Settings	39
SAC Tools UI Initialization Settings	43
SAC Tools UI Settings	46
Token Password Quality Settings	52
SAC Tools UI Access Control List	58
Security Settings	64
Log Settings	68
Chapter 6: Security Recommendations	70
Ensuring a Secured SAC Environment	70
Software Updates	70
Anti-Virus Software	70
Malware Awareness	70
Additional Environment Recommendations	71
Enforcing Restrictive Cryptographic Policies	71
Create Symmetric Key Objects using PKCS#11	72

PREFACE: About this Document

This document describes the operational and administrative tasks you can perform to maintain the functionality and efficiency of your SafeNet Authentication Client.

This section also identifies the audience, explains how to best use the written material, and discusses the documentation conventions used. They are:

- > ["Audience" below](#)
- > ["Document Conventions" below](#)
- > ["Support Contacts" on page 8](#)

For information regarding the document status and revision history, see ["Document Information" on page 2](#).

Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure.

All products manufactured and distributed by Thales Group are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

It is assumed that the users of this document are proficient with security concepts.

Document Conventions

This section describes the conventions used in this document.

Command Syntax and Typeface Conventions

This document uses the following conventions for command syntax descriptions, and to highlight elements of the user interface.

Format	Convention
bold	<p>The bold attribute is used to indicate the following:</p> <ul style="list-style-type: none"> > Command-line commands and options that you enter verbatim (Type dir /p.) > Button names (Click Save As.) > Check box and radio button names (Select the Print Duplex check box.) > Dialog box titles (On the Protect Document dialog box, click Yes.) > Field names (User Name: Enter the name of the user.) > Menu names (On the File menu, click Save.) (Click Menu > Go To > Folders.) > User input (In the Date box, type April 1.)
<i>italics</i>	In type, the italic attribute is used for emphasis or to indicate a related document. (See the <i>Installation Guide</i> for more information.)
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[optional] [<optional>]	Represent optional keywords or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.
{a b c} {<a> <c>}	Represent required alternate keywords or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.
[a b c] [<a> <c>]	Represent optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.

Notifications and Alerts

Notifications and alerts are used to highlight important information or alert you to the potential for data loss or personal injury.

Tips

Tips are used to highlight information that helps to complete a task more efficiently.

TIP This is some information that will allow you to complete your task more efficiently.

Notes

Notes are used to highlight important or helpful information.

NOTE Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss.

CAUTION! Exercise caution. Contains important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury.

****WARNING**** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or [Thales Customer Support](#).

Thales 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 Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at <https://supportportal.thalesgroup.com>, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

NOTE You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone

The support portal also lists telephone numbers for voice contact ([Contact Us](#)).

Email Support

You can also contact technical support by email at technical.support.DIS@thalesgroup.com.

CHAPTER 1: Introduction

SafeNet Authentication Client (SAC) is a middleware that manages Thales'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 smart cards.

Overview

SAC is a 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.

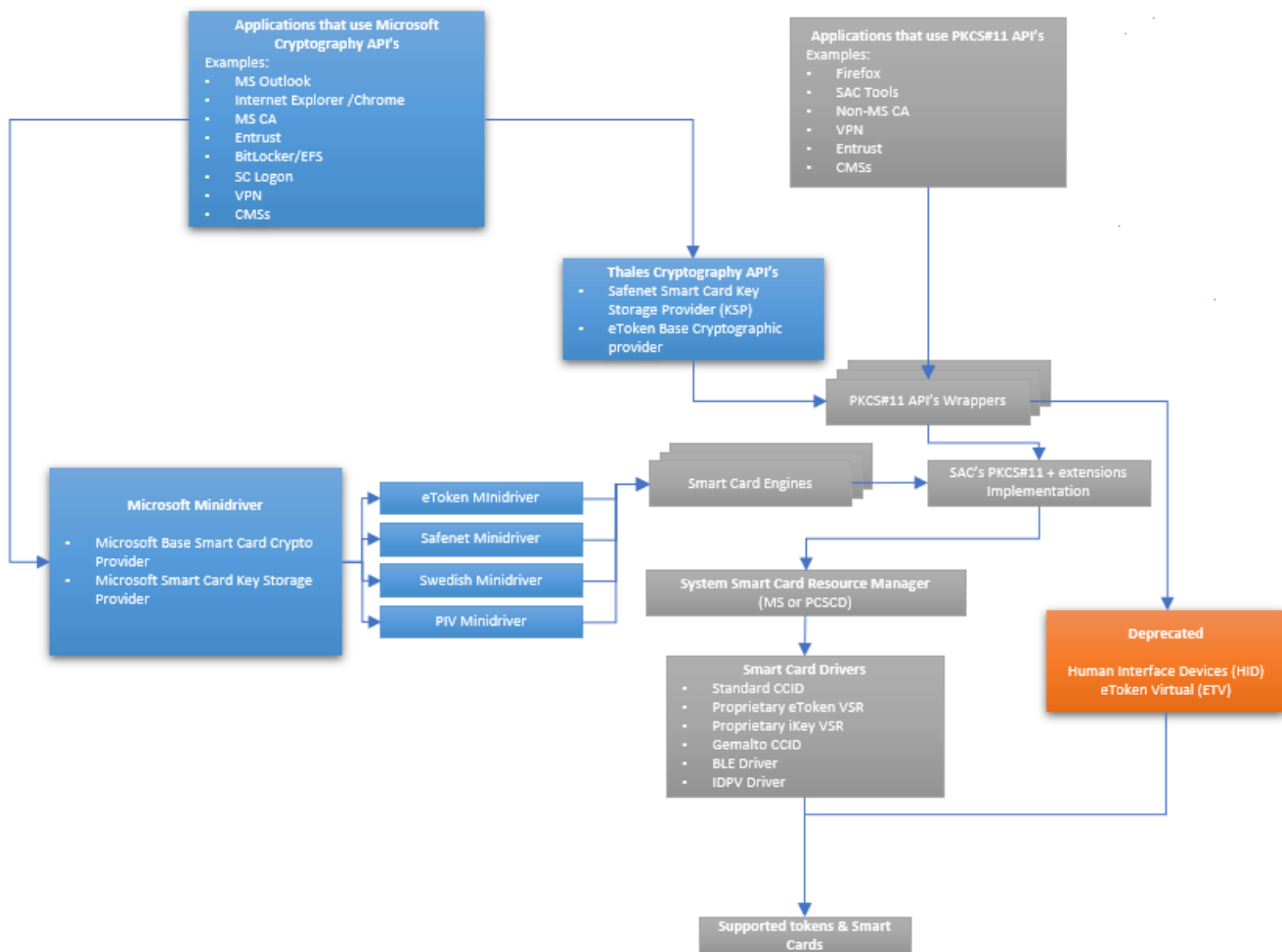
The SafeNet Authentication Client Tools application and the SafeNet Authentication Client tray icon application are installed with SafeNet Authentication Client, providing easy-to-use configuration tools for users and administrators.

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

For SAC system requirement details and compatibility information, refer to *SafeNet Authentication Client Release Notes*.

NOTE SAC is non-compatible with FIPS enabled Linux.

API Flow



Password Quality Information

SAC supports password quality settings for Administrator Passwords (also known as Security Officer (SO) passwords) and Initialization Keys that are implemented by SafeNet Authentication Client software. The setting is the same for all devices and cannot be modified. Though, it can be switched off for backward compatibility.

Additionally, IDPrime supports the insertion of the Administrator Key directly (without derivation), in which case the password policy is not validated. The Administrator Key derivation method is proprietary and may vary depending on the device.

The Administrator Password quality and Initialization Key quality must include three out of the following four rules:

- > English uppercase letters (ASCII 0x41...0x5A)
- > English lowercase letters (ASCII 0x61...0x7A)
- > Numeric (ASCII 0x30...0x39)

> Special characters (ASCII 0x20...0x2F + 0x3A...0x40 + 0x5B...0x60 + 0x7B...0x7F)

For backward compatibility, the Administrator Password quality check can be switched off through the SAC `pgAdminPQ` property.

Initialization Key password quality check cannot be switched off.

NOTE The Password quality is in use only when the Administrator Password and Initialization Keys are used in a 'Friendly' (textual) format. For more information, refer to the 'Friendly Admin Password' section in the *SafeNet Authentication Client User Guide*.

eToken 5110 FIPS and eToken 5110 devices support only *Friendly Admin* passwords.

If a customer does not want to be compliant with these PIN Quality policies, use hexadecimal keys (also through SAC UI and SAC API). Friendly Admin PIN length can be 24 binary or 48 hexadecimal. The Initialization Key length can be 32 binary or 64 hexadecimal. In this case, the keys are used as-is (without derivation) and PIN Quality is not checked.

NOTE The Administrator Key in IDPrime PIV cards and tokens supports 16 bytes or 32 hexadecimal PIN length. The ISD keys in IDPrime PIV cards and tokens are AES 16 byte key (32 in HEX).

SAC supports password quality settings for the User PIN. The implementation of these settings may differ on various devices. User PIN policies are created or modified during a device's initialization process or during the device's life cycle after Administrator (SO) authentication.

NOTE In case of IDPrime PIV cards and tokens, the PIN policy cannot be modified as it is in read only mode.

Depending on the device model (for example: IDPrime or eToken devices) and initialization mode that is set (for example: the device is initialized without password policies), password quality policies are enforced by the device or by the middleware software (SAC).

Device Type	Where the policy is stored:	Policy is enforced by:
<ul style="list-style-type: none"> > eToken 5110 > eToken 5110 FIPS 	Depends on how the device was formatted: On board SAC configuration	Middleware
<ul style="list-style-type: none"> > IDPrime MD 840/3840 > IDPrime 940/3940 > eToken 5110 CC 	On board	Middleware (except for the PIN length, which is validated on board)

Device Type	Where the policy is stored:	Policy is enforced by:
<ul style="list-style-type: none"> > IDPrime MD 830/3811 > IDPrime 930/3930/PIV cards > eToken Fusion NFC PIV > eToken Fusion NFC PIV Enterprise > eToken 5300 	On board	On board

NOTE Each device (IDPrime / eToken) has a different policy setting. For more information, refer to the Token Settings chapter in *SafeNet Authentication Client User Guide*.

The SAC Client Settings policy is currently used only on eToken 5110 and 5110 FIPS. This policy is used in the following cases:

- > The device was initialized without on board policies
- > The default values used during the device initialization flow

PIN Retry Counter

Setting the Administrator/User PIN Retry Counter may vary depending on your device type:

Administrator PIN Retry Counter

- > **IDPrime MD 840** - The Administrator PIN retry counter cannot be modified on this device.
- > **IDPrime 940/3940/940B/940C/SafeNet eToken 5110 CC/SafeNet eToken 5110 CC (940)/SafeNet eToken 5110+ CC (940B)/SafeNet eToken 5110+ CC (940C)/ SafeNet eToken Fusion CC** - The Administrator PIN retry counter is supported. The parameter is configured during factory settings and therefore, cannot be modified.
- > **IDPrime MD 830 B/ IDPrime 930/3930/SafeNet eToken 5300/SafeNet eToken 5110+ FIPS/SafeNet eToken Fusion** - The Administrator PIN retry counter is supported. The parameter can be modified using SAC on initialization.
- > **SafeNet eToken 5110 FIPS** - The Administrator PIN retry counter is supported. The parameter can be modified using SAC on initialization.
- > **IDPrime PIV 4.0 and eToken Fusion NFC PIV (Contact mode only)** - If the Admin key gets blocked (Administrator PIN retry counter is set to zero), it can be reset to default counter by using the Reinit feature of IDPrime PIV cards and tokens available in the SAC SDK. For details, refer to *SafeNet Authentication Client Developer Guide*.

- > **SafeNet IDPrime 940 SIS/840 SIS/IDClassic 410** - Since the Administrator PIN is disabled on these cards, the Administrator PIN retry counter cannot be modified.

User PIN Retry Counter

- > **SafeNet eToken 5110 FIPS or SafeNet eToken 5110** - Due to an eToken applet limitation, the user retry counter cannot be set on these smart cards, unless they are initialized.
- > **SafeNet IDPrime 940/3940/3940C/ 940B/940C/SafeNet eToken 5110 CC/SafeNet eToken 5110 CC (940)/SafeNet eToken 5110+ CC (940B)/SafeNet eToken 5110+ CC (940C)/SafeNet eToken Fusion CC** - The User PIN retry counter is supported. The parameter is configured during factory settings and therefore, cannot be modified.
- > **IDPrime 830/930/3930/SafeNet eToken 5300/SafeNet eToken 5110+ FIPS/SafeNet eToken Fusion** - The User PIN retry counter is supported. The parameter can be modified using SAC on initialization.
- > **IDPrime PIV cards and tokens (Contact mode only)** - If the PUK counter of the IDPrime PIV cards and tokens is active then the User Pin can be reset to its default counter using the SAC Tools Initialization flow and Set User PIN functionality from SAC Tools. But if the PUK counter is blocked, the User PIN can be reset by the Challenge-Response mechanism using the Unlock Token option in the SAC Tools. For details, refer to *SafeNet Authentication Client Developer Guide*.
- > **SafeNet IDPrime 940 SIS/840 SIS/IDClassic 410** - The User PIN retry counter cannot be modified on this device.

PUK PIN Retry Counter

- > **IDPrime PIV cards and tokens (Contact mode only)**- Due to IDPrime PIV applet limitation, the PUK PIN Retry counter cannot be set on this device. On initialization, the PIN or Keys are reset to their default counter.

PIN History Settings

NOTE This feature is not supported on IDPrime Common Criteria devices and IDPrime PIV cards and tokens.

Implementation differences exist in SAC as to how devices run IDPrime and eToken applets:

- > Devices that run eToken applets - old password hashes are remembered
- > Devices that run IDPrime applets - old and new password hashes are remembered

To reach the same behavior, set the History Size for IDPrime devices to '+1'.

Collecting SAC Logs

Collecting SAC logs allows administrators and technical-support personnel to diagnose the source of many problems that may have occurred while working with SafeNet Authentication Client. This information is used for debugging purposes.

SAC logs are collected by the following method:

- > SAC GUI (SAC Tools)

Perform the following steps to enable SAC logs through SAC GUI (SAC Tools):

1. Open **SAC Tools > Advanced View > Client Settings**, and click the **Advanced** tab.
2. Click **Enable Logging**.

The button will change to: Disable Logging. (For more information, see 'Enable Logging' in *SafeNet Authentication Client User Guide*.)

3. Restart the application that requires the debug logs to be created.

NOTE SAC Log files are created in the following directory `/tmp/eToken.log`.

Guidelines for multiple certificates enrollment

When enrolling multiple certificates on the token/smart card, the following behaviors and limitations apply:

Digital Signature Certificate Enrollment

- > Only one digital signature certificate can exist in the active container at a time.

Key Type Restrictions

- > The Digital Signature container accepts only Digital Signature certificates and Key Exchange certificates cannot be assigned to it.

Container Allocation Summary

- > Container 9C is reserved exclusively for Digital Signature certificates.
- > Container 9A, 9D, 9E, and 1 to 20 retired containers are reserved for Key Exchange certificates.

For enrollment of certificates on IDPrime PIV devices (cards/tokens), refer to the *SafeNet Authentication Client Administrator Guide* for Windows.

PIV Contact and Contactless Mode

Both read (data retrieval) and write (data modification) operations can be done in Contact mode of the card while only read operations are performed in Contactless (NFC) mode.

Below is the list of cards and tokens that are supported in contact and contactless modes:

- > SafeNet IDPrime PIV 3.0
- > SafeNet IDPrime PIV 4.0
- > SafeNet eToken Fusion NFC PIV
- > SafeNet eToken Fusion NFC PIV Enterprise

CHAPTER 2: Common Criteria

IDPrime Common Criteria Profile

The IDPrime Applets 4.0, 4.2, 4.4, and 5.2 are Common Criteria certified on Common Criteria based smart cards and tokens. These devices can have certain parameters customized in the factory with values that differ from the default profile. For a detailed list of supported cards, refer to *SafeNet Authentication Client Release Notes*.

NOTE The IDPrime 940 SIS card 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.
- > PINs (#1, #3 and #4 only)
- > Try Limit
- > Unblock PIN (PIN#1 only)
- > PIN validity period
- > Secure messaging in contactless mode

Number and Type of Key Containers

The following are the default settings.

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

- > 2 X 2,048-bit CC Sign Only RSA Keys
- > 8 X 2,048-bit Standard Sign and Decrypt RSA Keys
- > 2 X 256-bit Standard Sign and Decrypt ECC Keys

By default, the IDPrime Applets 4.4.2 and 5.2.0 are pre-personalized with:

- > 2 X 2048-bit CC Sign Only RSA Keys
- > 2 X 4096-bit CC Sign Only RSA Keys
- > 2 X 256-bit CC Sign Only ECC Keys
- > 8 X 2048-bit CC Sign and Decrypt RSA Keys

- > 2 X 4096-bit CC Sign and Decrypt RSA Keys
- > 2 X 256-bit CC Sign and Decrypt ECC Keys

NOTE The Key Generation method for Common Criteria (CC) key containers is either OBKG or Key import.

Common Criteria API Adjustments

Below table provides a high-level description of the adjustments that are made to the Standard and Extended PKCS#11 API to work with IDPrime CC devices. For more detailed information, refer to the code samples.

Standard PKCS#11 API	Extended PKCS#11 API
The <code>C_InitToken</code> function must receive the current Security Officer (SO) Password	The <code>C_InitToken</code> function must receive the current Security Officer (SO) Password
<ul style="list-style-type: none"> > When the <code>C_InitToken</code> function is called, you can enable linked mode on the IDPrime CC device. > 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. 	<ul style="list-style-type: none"> > To initialize the IDPrime CC device, the <code>ETCKA_CC</code> attribute must be set to <code>CK_TRUE</code>. > To initialize a device in linked mode, set the <code>ETCKA_IDP_CC_LINK</code> attribute to 1. > To pass the current Digital Signature PUK value, use the <code>ETCKA_IDP_CURRENT_PUK</code> attribute. > To revert a device back to unlinked mode after it was initialized in linked mode, set the <code>ETCKA_IDP_CC_LINK</code> attribute to 0 and use the <code>ETCKA_PUK</code> attribute to set the new Digital Signature PUK value.
If a device is not configured to use linked mode, the <code>C_InitToken</code> function ignores the Digital Signature PUK and Digital Signature PIN.	If a device is not configured to use linked mode, use the <code>ETCKA_PUK</code> attribute to set the new Digital Signature PUK value.
<ul style="list-style-type: none"> > After the device has been initialized in linked mode, the <code>C_InitPIN</code> function initializes the Digital Signature PIN and the User PIN. Both PIN's are set to the same value. > The <code>C_SetPIN</code> function used with the <code>CKU_SO</code> flag changes both the Administrator PIN and Digital Signature PUK to a new value. For details on Friendly Admin Password, refer to <i>SafeNet Authentication Client User Guide</i>. > The <code>C_SetPIN</code> function used with the <code>CKU_USER</code> flag changes both the User PIN and Digital Signature PIN to a new value. 	If the device is initialized to use linked mode, the <code>C_InitPIN</code> function and <code>C_SetPIN</code> function behaves the same as described in the <i>Standard PKCS#11</i> section.

SafeNet eToken Devices vs SafeNet IDPrime Devices

Below table displays the differences between SafeNet eToken devices and SafeNet IDPrime devices.

Feature	eToken 5110, eToken 5110 FIPS (and all other eToken based devices)	IDPrime, 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 (through Minidriver) <div> NOTE Applicable to Windows only. </div>
On Board RSAPadding (PSS/OAEP)	Not supported	Supported

Feature	eToken 5110, eToken 5110 FIPS (and all other eToken based devices)	IDPrime, eToken 5110 CC
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	Thales CC certified Applet
Symmetric Key operations	Support 3DES and AES	Not supported
Protocol for Contact	Support T1	Support T1, T0 and CTL

CHAPTER 3: Installation

This chapter provides the installation procedures for SafeNet Authentication Client (SAC) 10.9 R1 (GA) Linux. Local administrator rights are required to install or uninstall it.

Installation Files

The software package provided includes files for installing or upgrading to SAC 10.9 R1 (GA) Linux . The following Linux installation and documentation files are provided:

File	Description
Installation Files	
GPG-KEY-SafenetAuthenticationClient.txt	<ul style="list-style-type: none">> This file is the public key (GnuPG).> The signature confirms that the package is signed by an authorized party and also confirms the integrity and origin of your file.> Use this file to verify the signature before installing them to ensure that they are not altered from the original source of the packages.
SafenetAuthenticationClient-10.9.xxxx-1.el[x].x86_64.rpm	<ul style="list-style-type: none">> Installs SafeNet Authentication Client core on 64-bit platform.> Installs eToken core library and IFD Handler.
safenetauthenticationclient_10.9.xxxx_amd64.deb	<ul style="list-style-type: none">> Installs SafeNet Authentication Client core on 64-bit platform.> Installs eToken core library and IFD Handler.
Documentation Files	
SafeNet Authentication Client Release Notes	SafeNet Authentication Client Release Notes. Read before installation for last minute updates that may affect installation; contains important information such as resolved and known issues and troubleshooting for Linux.
SafeNet Authentication Client User Guide	SafeNet Authentication Client User Guide. Provides detailed information for the user and system administrator regarding the use of SafeNet Authentication Client for Linux.

File	Description
SafeNet Authentication Client Administrator Guide	SafeNet Authentication Client Administrator Guide (this document). Provides detailed information for the system administrator regarding the installation, configuration, maintenance, and management of SafeNet Authentication Client for Linux.

Installing the Standard Package

Installing on Red Hat Enterprise, SUSE, CentOS, and Fedora

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

NOTE For the PKCS#11, module to be installed automatically on a Firefox browser during the SAC installation, make sure that the *nss-tools* package is installed prior to installing SAC.

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

```
yum install nss-tools
```

NOTE The SAC tray icon is visible in GNOME Classic(x11) on RHEL/CentOS, you need to perform some steps (below) to view it.

To view SAC tray icon for GNOME Classic(x11) desktops

Perform the following steps:

1. Install the following packages:
 - a. `gnome-shell-extension-top-icons`
 - b. `gnome-tweaks`
2. Run the **Tweaks** application to enable Top icons in the extensions.

Following is the SAC .rpm package name:

- > `SafenetAuthenticationClient-10.9.xxxx-1.el[x].x86_64.rpm`

Where: `xxxx` is the build number

To install from the terminal

Perform the following steps:

1. On the terminal, log on as a root user.
2. Run the following command to import the public key:

```
rpm --import GPG-KEY-SafenetAuthenticationClient.txt
```

3. Run the following command:

```
rpm -Uvh SafenetAuthenticationClient-10.9.xxxx-1.el[x].x86_64.rpm
```

Where: `xxxx` is the version number

4. Run the following command to verify the signature of RPM package:

```
rpm --checksig --verbose SafenetAuthenticationClient-10.9.xxxx-1.el[x].x86_64.rpm
```

Installing on Ubuntu (.deb)

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

Following is the SAC .deb package name:

```
> safenetauthenticationclient_10.9.xxxx_amd64.deb
```

Where: `xxxx` is the build number

To install from the package installer

Perform the following steps:

1. Double-click the relevant .deb file.

The package installer is displayed.

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, do one of the following:

- From the taskbar, select **Applications > SafeNet Authentication Client**.
- Right-click the **SafeNet Authentication Client** tray icon, and select **Tools**.

The **SafeNet Authentication Client Tools** window is displayed.

NOTE Log out and log back in to enable the tray icon menu in the notification area.

To install from the terminal

Perform the following steps:

1. Enter the following command:

```
sudo dpkg -i safenetauthenticationclient_10.9.xxxx_amd64.deb
```

Where: `xxxx` 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 command:

```
sudo apt-get install -f
```

The dependencies are installed and the installation continues.

4. To run SafeNet Authentication Client Tools, do one of the following:

- From the taskbar, select **Applications > SafeNet Authentication Client**.
- Right-click the **SafeNet Authentication Client** tray icon, and select **Tools**.

The **SafeNet Authentication Client Tools** window is displayed.

5. Run the following command to import the public key:

```
gpg --import GPG-KEY-SafenetAuthenticationClient.txt
```

6. Run the following command to verify the signature of .deb package:

```
dpkg-sig --verify safenetauthenticationclient_10.9.xxxx_amd64.deb
```

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 SAC 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.

Following is the SAC .rpm package name:

```
> SafenetAuthenticationClient-core-10.9.xxxx-1.el[x].x86_64.rpm
```

Where: `xxxx` is the build number

To install from the package installer

Perform the following steps:

1. Double-click the relevant .rpm file.

The package installer is displayed.

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

Perform the following steps:

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

```
rpm --import GPG-KEY-SafenetAuthenticationClient.txt
```

3. Run the following command:

```
rpm -hi SafenetAuthenticationClient-core-10.9.xxxx-1.el[x].x86_64.rpm
```

Where: `xxxx` is the build number

4. Run the following command to check the signature of RPM package:

```
rpm --checksig --verbose SafenetAuthenticationClient-core-10.9.xxxx-1.el[x].x86_64.rpm
```

Installing on Ubuntu (.deb)

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

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.

Following is the SAC .deb package name:

```
> safenetauthenticationclient-core_10.9.xxxx_amd64.deb
```

Where: `xxxx` is the build number

To install from the package installer on Ubuntu 22.04

Perform the following steps:

1. Select the relevant .deb file and right-click it.

The context menu opens.

2. Select **Open With Other Application > Software Install and click the **Select** button.**

The package installer is displayed.

3. Click **Install Package.**

A password prompt appears.

4. Enter the Super User or root password.

The installation process runs.

To install from the terminal

Perform the following steps:

1. Enter the following command:

```
sudo dpkg -i safenetauthenticationclient-core_10.9.xxxx_amd64.deb
```

Where: `xxxx` 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. Run the following command to import the public key:

```
gpg --import GPG-KEY-SafenetAuthenticationClient.txt
```

5. Run the following command to verify the signature of .deb package:

```
dpkg-sig --verify safenetauthenticationclient-core_10.9.xxxx_amd64.deb
```

Linux External Dependencies

Red Hat Enterprise, SUSE, CentOS, Fedora and Ubuntu

- > Prerequisite - SAC 10.9 R1 (GA) requires OpenSSL 1.0 or above.

NOTE Thales recommends using the supported OpenSSL that is provided by the system.

- > PCSC (Smart Card Resource manager): libpcsc-lite, pcscd
 - To install on Ubuntu- Run `sudo apt-get install libpcsc-lite pcscd`
 - To install on Red Hat/CentOS/Fedora- Run `yum install pcsc-lite`
- > CCID Driver (version 1.7.0) for SafeNet eToken Fusion, SafeNet eToken Fusion NFC PIV, and SafeNet eToken Fusion FIPS:
 - To install on Ubuntu- Run `sudo dpkg -i sudo libccid_1.7.0-1_amd64.deb`
 - To install on Red Hat/CentOS/Fedora- Run
 - For RHEL9: `sudo rpm -Uvh pcsc-lite-ccid-1.7.0-1.el9.x86_64.rpm`
 - For RHEL10: `sudo rpm -Uvh pcsc-lite-ccid-1.7.0-1.el10.x86_64.rpm`

For other Linux distributions, refer to https://supportportal.thalesgroup.com/csm?id=kb_article_view&sys_kb_id=67bdc3e52b013e9042e3f445fe91bfd6&sysparm_article=KB0030022.

Installing the Firefox Security Module

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

Perform the following steps to install the security module in Firefox:

1. Open **Firefox Settings > Privacy & Security > Certificates**.
2. Click **Security Devices**.

The **Device Manager** window is displayed.

3. Click **Load**.

The **Load PKCS#11 Device** window is displayed.

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

- **On Ubuntu:** `/usr/lib/libeTPkcs11.so`
- **On Red Hat, Fedora, CentOS:** `/usr/lib64/libeTPkcs11.so`

NOTE

- To work with CC devices in unlinked mode, enter the following string for Multi-Slot support:

For Ubuntu: `/usr/lib/libIDPrimePKCS11.so`

For Red Hat, Fedora, CentOS: `/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 is displayed.

5. Click **OK**.

The new security module is installed.

Installing the Thunderbird Security Module

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

Perform the following to install the security module in Thunderbird:

1. Select **Thunderbird > Preferences > Privacy & Security**.

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

The **Device Manager** window is displayed.

3. Click **Load**.

The **Load PKCS#11 Device** window is displayed.

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

- **On Ubuntu:** `/usr/lib/libeTPkcs11.so`
- **On Red Hat, Fedora, CentOS:** `/usr/lib64/libeTPkcs11.so`

NOTE

- To work with CC devices in unlinked mode, enter the following string for Multi-Slot support:

For Ubuntu: `/usr/lib/libIDPrimePKCS11.so`

For Red Hat, Fedora, CentOS: `/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 is displayed.

3. Click **OK**.

The new security module is installed.

Changing SACTools Language

Use the similar configuration as given below to change different languages in the SAC Tools:

```
[GENERAL]
```

```
[UI]
```

```
LanguageId = cs-CZ
```

```
linguist = /usr/share/eToken/languages
```

```
to /etc/eToken.conf
```

To know the supported localization, refer to *SafeNet Authentication Client Release Notes*.

CHAPTER 4: Uninstall

After SafeNet Authentication Client (SAC) 10.9 R1 (GA) Linux is installed, you can uninstall it. Local administrator rights are required to uninstall SAC.

When SAC is uninstalled, user configuration and policy files may be deleted.

NOTE Before uninstalling this version, make sure to close the SAC Tools.

Uninstalling the Standard Package

Before uninstalling SAC 10.9 R1 (GA) Linux, make sure that SafeNet Authentication Client Tools is closed.

Uninstalling on Red Hat Enterprise, SUSE, CentOS, and Fedora

Perform the following step:

1. In the console, enter the following:

```
rpm -e SafenetAuthenticationClient
```

Where: `-e` is the parameter for uninstalling.

Uninstalling on Ubuntu (.deb)

Perform the following step:

1. 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

Perform the following step:

1. In the console, enter the following:

```
rpm -e SafenetAuthenticationClient-core
```

Where: `-e` is the parameter for uninstalling.

Uninstalling on Ubuntu (.deb)

Perform the following step:

1. In the console, enter the following:

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

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

CHAPTER 5: Configuration Properties

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

NOTE All properties are set and edited manually.

General Settings

The following settings are written to the **General** section in the file `/etc/eToken.conf`.

NOTE On a Linux machine, *PcscSlots* and *SoftwareSlots* configuration keys determine the number of slots. The *Reader Settings* window in SAC Tools, displays the configured slots but does not allow the user to change the settings.

Description	Value
EnforcePinPolicyInUnlock_CC_Products Forces PIN policy verification for the User PIN during token unlock via the Challenge-Response mechanism for CC-certified products.	Value Name: EnforcePinPolicyInUnlock_CC_Products Values: <ul style="list-style-type: none">> 0 - PIN Policy verification disabled> 1 - PIN Policy verification enabled Default: 0

Description	Value
<p>Use PIV Card CF</p> <p>Determines whether to use cardCF caching mechanism for IDPrime PIV 4.0 cards and tokens as well as IDPrime PIV 3.0 cards (with cardcf file generated after running the pre-perso script).</p> <p>By default, the PIV caching mechanism is used independently of the cardCF, which results in the performance gain of the caching mechanism.</p> <p>NOTE This setting is supported by SAC only and does not exist in the NIST specification for IDPrime PIV cards and tokens.</p>	<p>Value Name: UsePIVCardCF</p> <p>Value:</p> <ul style="list-style-type: none"> > 0- Uses PIV caching mechanism > 1- Uses CardCF caching mechanism <p>Default: 0</p>
<p>Use PIV 4096</p> <p>Determines if you can generate and create RSA keys -4096 bits using the algo ID personalized already in the IDPrime PIV 4.0 cards and tokens during pre-personalization.</p> <p>By default, if this registry entry does not exist or contains no value, an algo id 0x30 is used. Additionally, any other algo id can also be configured.</p> <p>NOTE The value in the registry entry should be consistent through out all the operations.</p> <p>CAUTION! Be careful when you toggle between the two cards or tokens whose algo id's are different for 4096 key.</p> <p>NOTE This setting is applicable for IDPrime PIV cards and tokens (Contact mode only).</p>	<p>Value Name: UsePIV4096</p> <p>Value:</p> <p>>=0 (Allows configurable Algo ID in hex)</p> <p>Default: 0 (Uses default algo)</p>

Description	Value
<p>Disable IDPV Rsa OAEP</p> <p>Determines whether to disable the Optimal Asymmetric Encryption Padding (OAEP) algorithm, which allows messages to be encrypted using RSA.</p> <div data-bbox="172 489 791 579"> <p>NOTE This setting is applicable to SafeNet IDPrime Virtual smart card.</p> </div> <div data-bbox="172 583 791 674"> <p>NOTE This setting is not applicable for IDPrime PIV cards and tokens.</p> </div>	<p>Value Name:DisableIDPVRsaOAEP</p> <p>Values:</p> <ul style="list-style-type: none"> > 0 - OAEP padding enabled > 1 - OAEP padding disabled <p>Default: 0</p>
<p>Disable IDPV Rsa PSS</p> <p>Determines whether to disable the Probabilistic Signature Scheme (PSS) algorithm, which provides private RSA key to sign the data in combination with random input.</p> <div data-bbox="172 936 791 1026"> <p>NOTE This setting is applicable to SafeNet IDPrime Virtual smart card.</p> </div> <div data-bbox="172 1031 791 1121"> <p>NOTE This setting is not applicable for IDPrime PIV cards and tokens.</p> </div>	<p>Value Name:DisableIDPVRsaPSS</p> <p>Values:</p> <ul style="list-style-type: none"> > 0 - PSS padding enabled > 1 - PSS padding disabled <p>Default: 0</p>
<p>Retry Count Cached</p> <p>Determines in which cache the retry counter is saved. If stored in the public cache, the API (SAC) performance increases, but it does not support transitioning of the device between computers.</p> <p>If stored in the private cache, performance is more accurate, even though it decreases.</p>	<p>Value Name: RetryCountCached</p> <p>Value:</p> <ul style="list-style-type: none"> > 0- The retry counter is stored in the private cache. Cache is updated on each transaction. > 1- The retry counter is stored in the public cache. Cache is updated on login operations. <p>Default: 1</p>
<p>HID Slots</p> <p>Defines the total number of HID slots for all HID USB tokens.</p>	<p>Value Name: HIDSlots</p> <p>Value:</p> <p>=0, =2, >=0</p> <ul style="list-style-type: none"> > 0-5200 token works in VSR mode. > 2- 5200 HID token works in HID mode (2 slots) <p>Default: 1</p>

Description	Value
<p>Disable SIS Determines whether to disable the support for IDPrime SIS card profile.</p> <p>NOTE This setting is applicable to SAC component (PKCS11).</p>	<p>Value Name: DisableSIS</p> <p>Values:</p> <ul style="list-style-type: none"> > 0 - SAC supports IDPrime SIS card profile > 1 - SAC does not support IDPrime SIS card profile <p>Default: 0</p>
<p>Disable Role3 CR Config Determines whether to disable the support for an IDPrime customer specific profile, where Role#3 is linked to Challenge/response mechanism of the admin key.</p> <p>NOTE This setting is applicable to all SAC component (PKCS11).</p>	<p>Value Name:DisableRole3CRConfig</p> <p>Values:</p> <ul style="list-style-type: none"> > 0 - SAC supports this IDPrime customer specific profile (Role#3 Challenge/response) > 1 - SAC does not support this IDPrime customer specific profile (Role#3 Challenge/response) <p>Default: 0</p>
<p>Disable Check Profile Determines whether to disable internal checks for IDPrime cards profile as received from factory.</p> <p>In most cases, these checks are not needed since the card profiles are correctly set in factory and disabling them enhances the performance of middleware.</p> <p>NOTE This setting is applicable to all SAC component (PKCS11).</p>	<p>Value Name:DisableCheckProfile</p> <p>Values:</p> <ul style="list-style-type: none"> > 0 - SAC performs internal checks for IDPrime cards profile > 1 - SAC does not performs internal checks for IDPrime cards profile <p>Default: 0</p>
<p>Skip User Pin Non Repudiation Check It skips checking if the user PIN authentication is lost at card level after a signing operation when the PIN associated with key is the User PIN.</p> <p>In most cases of IDPrime cards, the User PIN remains authenticated after a signing operation. So, this check can be skipped, which enhances the performance of signing operation.</p> <p>NOTE This setting is applicable to all SAC component (PKCS11).</p>	<p>Value Name:SkipUserPinNonRepudiationCheck</p> <p>Values:</p> <ul style="list-style-type: none"> > 0 - SAC checks if User PIN authentication is lost at card level after a signing operation > 1 - SAC does not checks if User PIN authentication is lost at card level after a signing operation > <p>Default: 0</p>

Description	Value
Dialog Type Determines the PIN dialog type for the MS Edge browser based on the registry value.	Value Name: DialogType Values: <ul style="list-style-type: none"> > 0 - Automatic (MS Edge Windows Credential Dialog is displayed whereas all other applications use regular SAC Dialog. If error <code>rv</code> access is denied, try one more time) > 1 - Windows PIN Dialog is displayed > 2 - SAC PIN Dialog is displayed Default: 0
Enable Log Events Enables event viewer messages.	Value Name: EnableLogEvents Values: <ul style="list-style-type: none"> > 0 - Not Selected > 1 - Selected Default: 0 - (not selected)
Allow Sign Final Pin Check Displays SAC digital signature pin pop up in case of multi part signing with sign only key on a CC card. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> NOTE To display digital signature PIN pop up, EnablePrompt must be set to 1 in [GENERAL] section. </div>	Value Name: AllowSignFinalPinCheck Value: <ul style="list-style-type: none"> > 0- SAC does not display digital signature PIN pop up in case of multi part signing > 1- SAC displays the digital signature PIN pop up in case of multi part signing Default: 0
Unlock Authorization Activates authorization protection for SAC Tools Unlock feature.	Value Name: UnlockAuthorization Value: <ul style="list-style-type: none"> > 0 - Do not activate authorization protection > 1 - Activate authorization protection Default: 0

Description	Value
<p>Read Only Mode</p> <p>Prevents deletion of certificates from the Token.</p> <div data-bbox="172 348 791 506"> <p>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.</p> </div>	<p>Value Name: ReadOnlyMode</p> <p>Values:</p> <ul style="list-style-type: none"> > 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. <p>Default: 0</p>
<p>Multi-Slot Support</p> <ul style="list-style-type: none"> > Determines if SAC is backward compatible with 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 through <code>libIDPrimePKCS11.so</code>. <p>Following are the two ways to work with IDPrime MD 840/940 or CC Cards, where a login is required for the Digital Signature Role:</p> <ol style="list-style-type: none"> 1. Use <code>libIDPrimePKCS11.so</code>, where the user has two smart cards: <ol style="list-style-type: none"> a. Physical Smart Card b. Virtual Smart Card (where Digital Signature Role is exposed as ROLE1 in the virtual smart card) 2. To enable the prompt login through a flag in the <code>/etc/eToken.conf</code> file, add the following line to Section [GENERAL]: <pre>[GENERAL] EnablePrompt=1</pre> <p>This allows C_Login with Null or when a ROLE is not Logged in, a prompt is shown to enter the PIN/Password to complete the operation, such as C_SIGN / C_Encrypt/C_Decrypt</p> <p>For more information on Multi-Slots, see the PKCS#11 Digital Signature PIN Authentication section of the <i>SafeNet Authentication Client User Guide</i>.</p> <div data-bbox="172 1722 791 1812"> <p>NOTE Linked Mode is not compatible with the Multi-Slot feature.</p> </div> 	<p>Value Name: MultiSlotSupport</p> <p>Values:</p> <ul style="list-style-type: none"> > Selected - Activates this feature > Not Selected - Normal operation <p>Default: Not Selected</p>

Description	Value
Touch Sense Notify Determines if the Touch Sense notification is displayed as balloon or in a window.	Value Name: TSNotify Values: <ul style="list-style-type: none"> > 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.	Value Name: PinPadNotify Values: <ul style="list-style-type: none"> > 0 - Show ballon > 1 - Show balloon > 2 - No notification Default: 0 (Show window)
Full SM Mode <ul style="list-style-type: none"> > Enables/disables the full Security Messaging (SM) mode for IDPrime FIPS L2 devices. <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> NOTE SAC cache must be reset after changing the <i>FullSMMMode</i> property. </div> <ul style="list-style-type: none"> > This configuration is for L2 applets 4.3.5 and above. 	Value Name: FullSMMMode Values: <ul style="list-style-type: none"> > 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 requires entering user credentials.	Value Name: NoPinPad Values: <ul style="list-style-type: none"> > 0 - Disabled > 1 - Enabled Default: 0 (Disabled)

Description	Value
<p>ITI Certification Mode</p> <p>Enables ITI Certification, which requires the following:</p> <ul style="list-style-type: none"> > 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. <p>NOTE When the <i>ITI Certification Mode</i> property is enabled, the <i>Enable Administrator Password Quality Check</i> property will be disabled.</p>	<p>Value Name: MustChangeAdmin</p> <p>Values:</p> <ul style="list-style-type: none"> > 0- None > 1 - ITI certification mode > 2 - Special administrator PIN policy <p>Default: 0</p>
<p>PCSC Slots</p> <p>Defines the total number of PC/SC slots for all USB tokens and smart cards.</p> <p>Included in this total:</p> <ul style="list-style-type: none"> > The number of allocated readers for third-party providers. > The number of allocated readers for other SafeNet physical tokens, which can be modified in <i>Reader Settings</i> in SAC Tools. 	<p>Value Name: PcscSlots</p> <p>Values: >=0 (0 = Physical tokens are disabled)</p> <p>Default: 8</p>
<p>Enable Private Cache</p> <ul style="list-style-type: none"> > Determines if SAC allows the token's private data to be cached. > Applies only to tokens that are initialized with the private data cache setting. > The private data is cached in per process memory. <p>NOTE Can be set in SAC Tools.</p>	<p>Value Name: EnablePrvCache</p> <p>Values:</p> <ul style="list-style-type: none"> > 1 (True) - Private data caching is enabled > 0 (False) - Private data caching is disabled <p>Default: 1 (True)</p>
<p>Tolerate Finalize</p> <p>Determines if C_Finalize can be called by DIIMain.</p> <p>NOTE Define this property per process. Select this setting when using Novell Modular Authentication Service (NMAS) applications only.</p>	<p>Value Name: TolerantFinalize</p> <p>Values:</p> <ul style="list-style-type: none"> > 1 (True) - C_Finalize can be called by DIIMain > 0 (False) - C_Finalize cannot be called by DIIMain <p>Default: 0 (False)</p>

Description	Value
<p>Tolerate X509 Attributes</p> <p>Determines if CKA_SERIAL_NUMBER, CKA_SUBJECT, and CKA_ISSUER attributes can differ from those in CKA_VALUE during certificate creation.</p> <div data-bbox="172 457 791 646"> <p>NOTE Enable TolerantX509Attributes when using certificates created in a non-DER encoded binary x.509 format. In some versions of PKI Client, this setting is not selected by default.</p> </div>	<p>Value Name: TolerantX509Attributes</p> <p>Values:</p> <ul style="list-style-type: none"> > 1 (True) - The attributes can differ > 0 (False) - Check that the values match <p>Default: 0 (False)</p>
<p>Tolerate Find Templates</p> <p>Determines if PKCS#11 tolerates a <i>Find</i> function with an invalid template, returning an empty list instead of an error.</p>	<p>Value Name: TolerantFindObjects</p> <p>Values:</p> <ul style="list-style-type: none"> > 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 <p>Default: 0 (False)</p>
<p>Protect Symmetric Keys</p> <p>Determines if symmetric keys are protected.</p> <div data-bbox="172 1192 791 1283"> <p>NOTE If selected, even non-sensitive symmetric keys cannot be extracted.</p> </div>	<p>Value Name: SensitiveSecret</p> <p>Values:</p> <ul style="list-style-type: none"> > 1 - Symmetric keys cannot be extracted > 0 - Symmetric keys can be extracted <p>Default: 0</p>
<p>Cache Marker Timeout</p> <p>Determines if SAC Service periodically inspects the cache markers of connected tokens for an indication that token content has changed.</p> <p>A common usage of this property is while using remote sessions or crossing between the machines.</p>	<p>Value Name: CacheMarkerTimeout</p> <p>Values:</p> <ul style="list-style-type: none"> > 1 - Connected tokens' cache markers are periodically inspected > 0 - Connected tokens' cache markers are never inspected <p>Default: 0</p>

Description	Value
<p>Override Non-Repudiation OIDs</p> <ul style="list-style-type: none"> > Overrides SAC's list of standard certificate OIDs that require a high level of security. <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>NOTE Users must log on to their tokens whenever signing with a certificate defined as non-repudiation.</p> </div> <ul style="list-style-type: none"> > Avoid authenticating every time when a cryptographic operation is required for certificates containing <i>Entrust certificate OID</i> details, remove the default registration key value. 	<p>Value Name: NonRepudiationOID</p> <p>Value: Empty</p> <p>Default: No override</p>
<p>Ignore Silent Mode</p> <p>Determines if the <i>Token Logon</i> window is displayed even when the application calls the CSP/KSP in silent mode.</p>	<p>Value Name: IgnoreSilentMode</p> <p>Values:</p> <ul style="list-style-type: none"> > 1 (True) - Display the Token Logon window even in silent mode > 0 (False) - Respect silent mode <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>NOTE Set to True when the SafeNet RSA KSP must use SHA-2 to enroll a CA private key to a token</p> </div> <p>Default: 0 (False)</p>
<p>Force Create Without Touch Sense</p> <p>Determines whether to ignore Touch Sense configuraion of the device when creating keys.</p> <p>This setting applies to only newly created keys.</p>	<p>Value Name: ForceCreateWithoutTouchSens</p> <p>Values:</p> <ul style="list-style-type: none"> > 0 - Touch Sense configuration of the device applies when creating the keys. > 1 - Touche Sense configuration of the device is ignored for the newly created keys. New keys are created as standard keys with Touch Sense disabled. <p>Default: 0</p>
<p>Force New Key A</p> <p>Determines the deletion of either User or Admin keys associated with the role different from the user.</p>	<p>Value Name: ForceNewKeyA</p> <p>Value:</p> <ul style="list-style-type: none"> > 0 - Keys can be deleted by either User or Admin > 1 - Keys associated with a Role different from user can be deleted only by the Admin <p>Default: 0</p>

Initialization Settings

NOTE The following settings are applicable to IDPrime Cards only:

- In **Init Key** folder: `ForceInitExternalPinPolicy` and `ForceDefaultInitKey`
- In **InitApp Key** folder: `HideInitCreateAdmin` and `HideInitPinPolicy`

The following settings are written to the **Init** section in the file `/etc/eToken.conf`.

NOTE None of the settings in this section are relevant to IDPrime cards, except for the *LinkMode* and *UserMaxRetry* settings.

Properties relevant to end of life tokens and cards can be found in previous versions of the Administrator Guide.

Description	Value
<p>Always Use Default Initialization Key Defines the use of default initialization key during token initialization.</p> <p>NOTE If Selected, the following windows on the SAC Tools UI are skipped while Initializing IDPrime FIPS Devices (with initialization key):</p> <ul style="list-style-type: none"> -Administrator Logon -Initializing Key Settings 	<p>Value Name: <code>ForceDefaultInitKey</code></p> <p>Values:</p> <ul style="list-style-type: none"> > 1: Token is initialized with the default initialization key > 0: Token is initialized with the initialization key entered by the user <p>Default:</p> <ul style="list-style-type: none"> > 0
<p>Use PIN Quality Parameters From Policy Defines if the PIN Quality parameters in the SAC Client Settings are used during initialization.</p> <p>NOTE If Selected, user cannot modify the Pin Policy of the card manually through <i>Initialize Token</i> setting. Also, all the fields in the <i>PIN Quality</i> and <i>Advanced</i> tabs on the SAC Tools are disabled.</p>	<p>Value Name: <code>ForceInitExternalPinPolicy</code></p> <p>Values:</p> <ul style="list-style-type: none"> > 1: Token is initialized with PIN Quality parameters stored in SAC Client Settings > 0: Token is initialized with PIN Quality parameters stored on the card or entered by the user <p>Default:</p> <ul style="list-style-type: none"> > 0
<p>Maximum Token Password Retries Defines the default number of consecutive failed logon attempts that lock the token.</p>	<p>Value Name: <code>UserMaxRetry</code></p> <p>Values: 1-15</p> <p>Default: 15</p>

Description	Value
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	Value Name: ForceAdmin Values: <ul style="list-style-type: none">> 1(True) - Token is initialized with SO object> 0 (False) - Token is initialized without SO object Default: 1 (True)
Force User object on Token	Value Name: ForceUser Values: <ul style="list-style-type: none">> 1(True) - Token is initialized with User object> 0(False) - Token is initialized without User object Default: 1(True)

Description	Value
<p>Legacy Format Version Defines the default token format.</p>	<p>Value Name: Legacy-Format-Version</p> <p>Values:</p> <ul style="list-style-type: none"> > 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) <p>Default:</p> <ul style="list-style-type: none"> > 4 - For CardOS tokens > 5 - For 4.20B FIPS and Java Card - based tokens
<p>Default Token Name Defines the default Token Name written to tokens during initialization.</p>	<p>Value Name: DefaultLabel</p> <p>Value: String</p> <p>Default: My Token</p>
<p>API: Keep Token Settings When initializing the token using the SDK, this setting determines if the token is automatically re-initialized with its current settings.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>NOTE If selected, this setting overrides all other initialization settings.</p> </div>	<p>Value Name: KeepTokenInit</p> <p>Values:</p> <ul style="list-style-type: none"> > 1 (True) - Use current token settings > 0 (False) - Override current token settings <p>Default: 0 (False)</p>

Description	Value
<p>Automatic Certification</p> <p>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.</p>	<p>Value Name: Certification</p> <p>Values:</p> <ul style="list-style-type: none"> > 1(True) - initialize the token with the original certification > 0 (False) - initialize the token without the certification <p>Default: 1 (True)</p>
<p>API: Private Data Caching</p> <p>If using an independent API for initialization, and if <i>Enable Private Cache</i> is selected, this setting determines the token's private data cache default behavior.</p>	<p>Value Name: PrvCachingMode</p> <p>Values:</p> <ul style="list-style-type: none"> > 0 - Always > 1 - While user is logged on > 2 - Never <p>Default: 0 (Always)</p>
<p>Enable Private Data Caching Modification</p> <p>Determines if the token's <i>Private Data Caching</i> mode can be modified after initialization.</p>	<p>Value Name: PrvCachingModify</p> <p>Values:</p> <ul style="list-style-type: none"> > 1 (True) - Can be modified > 0 (False) - Cannot be modified <p>Default: 0 (False)</p>
<p>Private Data Caching Mode</p> <p>If <i>Enable Private Data Caching Modification</i> is selected, this setting determines who has rights to modify the token's <i>Private Data Caching</i> mode.</p>	<p>Value Name: PrvCachingOwner</p> <p>Values:</p> <ul style="list-style-type: none"> > 0 - Admin > 1 - User <p>Default: 0 (Admin)</p>

Description	Value
<p>API: RSA Secondary Authentication Mode</p> <p>If using an independent API for initialization, this setting determines the default behavior for protecting RSA private keys on the token.</p>	<p>Value Name: 2ndAuthMode</p> <p>Values:</p> <ul style="list-style-type: none"> > 0 - Never > 1 - Prompt on application request > 2 - Always prompt user > 3- Always > 4 - Token authentication on application request <p>Default: 0 -(Never)</p>
<p>Enable RSA Secondary Authentication Modified</p> <p>Determines if the token's RSA secondary authentication can be modified after initialization.</p>	<p>Value Name: 2ndAuthModify</p> <p>Values:</p> <ul style="list-style-type: none"> > 1 (True) - Can modify > 0 (False) - Cannot modify <p>Default: 0 (False)</p>
<p>Use the same token and administrator passwords for digital signature operations</p> <p>If LinkMode is set to zero, or not defined, the SAC Tools UI does not show the Link Mode option.</p> <p>The Linked Mode is not compatible with the Multi-Slots feature. When using a Common Criteria smart card (SafeNet IDPrime 940 or IDPrime MD 840), if the Admin PIN is set to default, the unlock button is disabled until changed.</p> <p>For example: When using a SafeNet IDPrime 940 or IDPrime MD 840 card in linked mode, the Unlock Token button (in SAC Tools) is disabled until the default Admin PIN is changed.</p>	<p>Value Name: LinkMode</p> <p>Values:</p> <ul style="list-style-type: none"> > 1 (True) - Linked > 0 (False) - Unlinked <p>Default: 0 (False)</p>

SAC Tools UI Initialization Settings

The following settings are written to the **InitApp** section in the file `/etc/eToken.conf`.

Description	Value
Display FIPS Setting Defines if SAC Enforce FIPS settings for the etoken is FIPS compatible to initialize them in FIPS mode.	Value Name: DisplayFipsSetting Value: <ul style="list-style-type: none"> > 0- If this setting is absent or if it is set to 0, then the FIPS initialization checkbox is not displayed > 1- If this setting is present and set to 1, then the FIPS initialization checkbox is displayed Default: 0
Hide Create Administrator Password Fields Defines if Create Administrator Password fields are hidden/ visible in the Password Settings window.	Value Name: HideInitCreateAdmin Values: <ul style="list-style-type: none"> > 0: Create Administrator Password fields are visible > 1: Create Administrator Password fields are hidden Default: <ul style="list-style-type: none"> > 0
Hide PinPolicy Button Defines if the Pin Policy button is hidden/ visible in the Password Settings window.	Value Name: HideInitPinPolicy Values: <ul style="list-style-type: none"> > 0: PIN Policy button is visible > 1: PIN Policy button is hidden Default: <ul style="list-style-type: none"> > 0
Default Token Password Defines the default Token Password.	Value Name: DefaultUserPassword Values: String Default: 1234567890

Description	Value
<p>Enable Change Password on First Logon Determines if the <i>Token Password must be changed on first logon</i> option can be changed by the user in the <i>Token Initialization</i> window.</p> <p>NOTE This option is selected by default. If the option is deselected, it can be selected again.</p> <p>NOTE This feature is not applicable for IDPrime PIV cards and tokens.</p>	<p>Value Name: MustChangePasswordEnabled</p> <p>Values:</p> <ul style="list-style-type: none"> > 1 - Selected > 0 - Not selected <p>Default: 1</p>
<p>Change Password on First Logon Determines if the <i>Token Password must be changed on first logon</i> option is selected by default in the <i>Token Initialization</i> window.</p> <p>NOTE This feature is not applicable for IDPrime PIV cards and tokens.</p>	<p>Value Name: MustChangePassword</p> <p>Value:</p> <ul style="list-style-type: none"> > 1 - Selected > 0 - Not selected <p>Default: 1</p>
<p>Private Data Caching If <i>Enable Private Cache</i> is selected, this setting determines the token's private data cache default behavior.</p> <p>NOTE Can be set in SAC Tools. This option is not supported by IDPrime cards.</p>	<p>Value Name: PrivateDataCaching</p> <p>Values:</p> <ul style="list-style-type: none"> > 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 <p>Default: 0</p>

Description	Value
<p>RSA Secondary Authentication Mode</p> <p>Defines the default behavior for protecting RSA private keys on the token.</p> <div> <p>NOTE Can be set in SAC Tools. This option is not supported by IDPrime cards.</p> </div>	<p>Value Name: RSASecondaryAuthenticationMode</p> <p>Values:</p> <ul style="list-style-type: none"> > 0 - Never > 1 - Prompt user on application request > 2 - Always prompt user > 3 - Always > 4 - Token authentication on application request <p>Default: 0</p>
<p>Reuse Current Token Name</p> <p>Determines if the token's current Token Name is displayed as the default Token Name when the token is re-initialized.</p>	<p>Value Name: ReadLabelFromToken</p> <p>Values:</p> <ul style="list-style-type: none"> > 1 -The current Token Name is displayed > 0 -The current Token Name is ignored <p>Default: 1</p>

SAC Tools UI Settings

The following settings are written to the **UI** section in the file `/etc/eToken.conf`.

Description	Value
<p>Use Default Password</p> <p>Determines if the <i>Change Password on First Logon</i> process assumes the current Token Password is the default (defined in the Default Token Password), and does not prompt the user to supply it.</p>	<p>Value Name: UseDefaultPassword</p> <p>Values:</p> <ul style="list-style-type: none"> > 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 <p>Default: 0 (False)</p>

Description	Value
<p>Password Term Defines the term used for the token's user password.</p> <div data-bbox="199 399 952 466"> <p>NOTE If a language other than English is used, ensure that the Password Terms are translated.</p> </div>	<p>Value Name: PasswordTerm</p> <p>Values (String):</p> <ul style="list-style-type: none"> > Password > PIN > Passcode > Passphrase <p>Default: Password</p>
<p>Decimal Serial Number Determines if the Token Information window displays the token serial number in hexadecimal or in decimal format.</p>	<p>Value Name: ShowDecimalSerial</p> <p>Values:</p> <ul style="list-style-type: none"> > 1 (True) -Displays the serial number in decimal format > 0 (False) -Displays the serial number in hexadecimal format <p>Default: 0</p>
<p>Enable Tray Icon Determines if the application tray icon is displayed when SAC is started.</p>	<p>Value Name: ShowInTray</p> <p>Values:</p> <ul style="list-style-type: none"> > 0 - Never Show > 1 - Always Show <p>Default: Always show</p>
<p>Enable Connection Notification Determines if a notification balloon is displayed when a token is connected or disconnected.</p>	<p>Value Name: ShowBalloonEvents</p> <p>Values:</p> <ul style="list-style-type: none"> > 0 - Not Displayed > 1 - Displayed <p>Default: 0</p>

Description	Value
Enable Logging Control Determines if the <i>Enable Logging /Disable Logging</i> button is enabled in the Client Settings > Advanced tab.	Value Name: AllowLogsControl Values: <ul style="list-style-type: none"> > 1 - Enabled > 0 - Disabled Default: 1
Home URL Overwrites the SafeNet home URL in SAC Tools.	Value Name: HomeUrl Values (String): Valid URL Default: SafeNet's home URL
Enable Certificate Expiration Warning Determines if a warning message is displayed when certificates on the token are about to expire.	Value Name: CertificateExpiryAlert Values: <ul style="list-style-type: none"> > 1 (True) - Notify the user > 0 (False) - Do not notify the user Default: 0 (False)
Ignore Archived Certificates Determines if archived certificates are ignored, and no warning message is displayed for certificates that are about to expire.	Value Name: IgnoreArchivedCertificates Values: <ul style="list-style-type: none"> > 1 - Archived certificates are ignored > 0 - A warning message is displayed if the token contains archived certificates. Default: 1

Description	Value
Ignore Expired Certificates Determines if expired certificates are ignored, and no warning message is displayed for expired certificates.	Value Name: IgnoreExpiredCertificates Values: <ul style="list-style-type: none"> > 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
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: SAC
Certificate Will Expire Warning Message Defines the warning message to display in a balloon during a certificate's <i>Certificate Expiration Warning Period</i> .	Value Name: FutureAlertMessage Values: String Default: A certificate on your token expires in \$EXPIRE_IN_DAYS days.

Description	Value
Expiry Date Format Defines the format of the certificate's expiry date (\$EXPIRY_DATE) displayed in a balloon.	Value Name: EXPIRY_DATE_FORMAT Values: Set the year/month/day in the required order using the 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: <ul style="list-style-type: none"> > 0 - No action > 1 - Show detailed message > 2 - Open website Default: 0
Detailed Message If <i>Show detailed message</i> is selected in Warning Message > Click Action setting, defines the detailed message to display.	Value Name: ActionDetailedMessage Values: String No default
Website URL If <i>Open website</i> is selected in the Warning Message > Click Action setting, defines the URL to display.	Value Name: ActionWebSiteURL Values (string): Website address No default

Description	Value
<p>Enable Password Expiration Notification</p> <p>Determines if a pop-up message is displayed in the system when the Token Password is about to expire.</p>	<p>Value Name: NotifyPasswordExpiration</p> <p>Values:</p> <ul style="list-style-type: none"> > 1 (True) - A message is displayed > 0 (False) - A message is not displayed <p>Default: 1 (True)</p>
<p>Password Policy Instructions</p> <p>If not empty, defines a string that replaces the default password policy description displayed in the <i>Unlock and Change Password</i> windows.</p>	<p>Value Name: PasswordPolicyInstructions</p> <p>Values: String</p> <p>No default</p>
<p>Define Initialization Mode</p> <p>Select this option if you want the <i>Initialization Options</i> window (first window displayed when initializing a device) to be ignored.</p>	<p>Value Name: DeflntMode</p> <p>Values:</p> <ul style="list-style-type: none"> > 0 - Display the <i>Initialization Options</i> window > 1 - Set Preserve Mode > 2 - Set Configure Mode <p>Default: 0</p>
<p>Import Certificate Chain</p> <p>Determines if the certificate chain is imported to the token.</p>	<p>Value Name: ImportCertChain</p> <p>Values:</p> <ul style="list-style-type: none"> > 0 - Do not import certificate chain > 1 - Import certificate chain > 2- User selects import behavior <p>Default: 0</p>

Description	Value
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.	Value Name: DenyMustChangePopup Values: <ul style="list-style-type: none"> > 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 the file `~/ .eToken.conf`.

NOTE Password and PIN related registry entries are not supported on IDPrime PIV cards and tokens.

Description	Value
Password - Include Non ASCII Characters Determines if the password can be included for non-ASCII characters.	Value Name: pqNonAscii Values: <ul style="list-style-type: none"> > 0: Permitted > 1: Forbidden > 2: Mandatory Default: 0
Password - Number Of Different Repeating Characters Determines the number of different characters that can be repeated at least once.	Value Name: pqNumDiffCharRepeat Values: <ul style="list-style-type: none"> >= 0 (0 = No check) Default: 0

Description	Value
<p>Password - Maximum Number A Character Can Appear Determines the maximum number a character can appear.</p>	<p>Value Name: pqMaxNumCharAppear</p> <p>Values: >= 0 (0 = No check)</p> <p>Default: 0</p>
<p>Password - Maximum Number Of Characters In A Sequence Determines the maximum number of characters in a sequence. For example: If the value is set to 4, the sequence 1,2,3,4,a,5 is allowed but 1,2,3,4,5,a is not allowed.</p>	<p>Key Name: pqMaxNumCharSequence:</p> <p>Values: >= 0 (0 = No check)</p> <p>Default: 0</p>
<p>Password - Maximum Adjacent Repetitions Of A Character Determines the maximum number a character can be repeated in adjacent positions.</p> <div data-bbox="199 978 904 1050"> <p>NOTE If pqMaxNumCharRepeatPos = 0, then the value of pqMaxRepeated is applicable.</p> </div>	<p>Value Name: pqMaxNumCharRepeatPos</p> <p>Values: >= 0 (0 = No check)</p> <p>Default: 0</p>
<p>Password - Minimum Length Defines the minimum password length.</p> <div data-bbox="199 1249 595 1281"> <p>NOTE Can be set in SAC Tools.</p> </div> <p>For more information on how to configure the 'Password Minimum Length' property as permanent. See "Changing the Password Minimum Length Permanently" on page 1</p>	<p>Value Name: pqMinLen</p> <p>Values: >=4</p> <p>Default: 6</p>

Description	Value
<p>Password - Maximum Length Defines the maximum password length.</p> <div data-bbox="172 388 930 445"> <p>NOTE Can be set in SAC Tools.</p> </div> <ul style="list-style-type: none"> > Devices that have an eToken applet (such as: eToken 5110, 5110 FIPS or IDCore 830B) the max pin length property is not saved on the device. This property has only a UI meaning (i.e.no security meaning). > The value of the proprietary PKCS#11 attribute <code>ETCKA_PIN_MAX_LEN</code> on these devices is always read from SAC's <code>pqMaxLen</code> property. > If the <code>pqMaxLen</code> property is not explicitly defined, it receives the default value (20). > In addition, SAC Tools has it's own limitation for the <code>ETCKA_PIN_MAX_LEN</code> attribute with a max of 16 characters. Even though the <code>pqMaxLen</code> value has a value that is greater than 16. 	<p>Value Name: <code>pqMaxLen</code></p> <p>Values: Cannot be less than the Password Minimum Length</p> <p>Default: 16</p>
<p>Password - Maximum Usage Period Defines the maximum number of days a password is valid.</p> <div data-bbox="172 1056 930 1113"> <p>NOTE Can be set in SAC Tools.</p> </div> <div data-bbox="172 1123 930 1245"> <p>NOTE This parameter is <i>Day Sensitive</i> that is the system counts the days and not the hour in which the user made the change.</p> </div>	<p>Value Name: <code>pqMaxAge</code></p> <p>Values: ≥ 0 (0 =No expiration)</p> <p>Default: 0</p>
<p>Password - Minimum Usage Period Defines the minimum number of days between password changes.</p> <div data-bbox="172 1402 930 1459"> <p>NOTE Can be set in SAC Tools.</p> </div>	<p>Value Name: <code>pqMinAge</code></p> <p>Values: ≥ 0 (0 = No minimum)</p> <p>Default: 0</p>
<p>Password - Expiration Warning Period Defines the number of days before expiration during which a warning is displayed.</p> <div data-bbox="172 1623 930 1680"> <p>NOTE Can be set in SAC Tools.</p> </div>	<p>Value Name: <code>pqWarnPeriod</code></p> <p>Values: ≥ 0 (0 = No warning)</p> <p>Default: 0</p>

Description	Value
<p>Password - History Size Defines the number of recent passwords that must not be repeated.</p> <p>NOTE Can be set in SAC Tools. Maximum value of History size for IDPrime devices is 10.</p>	<p>Value Name: pqHistorySize</p> <p>Values: >= 0 (0 = No minimum)</p> <p>Default: 10</p>
<p>Password - Maximum Consecutive Repetitions Defines the maximum number of consecutive times a character can be used in a password.</p> <p>NOTE Can be set in SAC Tools. If pqMaxNumCharRepeatPos = 0, then the value of pqMaxRepeated is applicable.</p>	<p>Value Name: pqMaxRepeated</p> <p>Values: 0 - 16 (0 = No maximum)</p> <p>Default: 3</p>
<p>Password - Complexity</p> <ul style="list-style-type: none"> > 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. <p>NOTE Can be set in SAC Tools.</p>	<p>Value Name: pqMixChars</p> <p>Values:</p> <ul style="list-style-type: none"> > 1 - A minimum of 2 or 3 types must be included, as defined in the <i>Password- Minimum Mixed Character Types</i> setting > 0 -The rule for each character type is defined in the character type's <i>Include</i> setting <p>Default: 1</p>
<p>Password - Minimum Mixed Character Types</p> <ul style="list-style-type: none"> > 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. <p>NOTE</p> <ul style="list-style-type: none"> - Applies only when the <i>Password - Complexity</i> setting is set to <i>Standard complexity</i>. - Can be set in SAC Tools. 	<p>Value Name: pqMixLevel</p> <p>Values:</p> <ul style="list-style-type: none"> > 0 - At least 3 character types > 1 - At least 2 character types <p>Default: 0</p>

Description	Value
<p>Password - Include Numerals Determines if the password can include numerals.</p> <div> <p>NOTE</p> <ul style="list-style-type: none"> - Applies only when the <i>Password - Complexity</i> setting is set to <i>Manual complexity</i>. - Can be set in SAC Tools. </div>	<p>Value Name: pqNumbers</p> <p>Values:</p> <ul style="list-style-type: none"> > 0 - Permitted > 1 - Forbidden > 2 - Mandatory <p>Default: 0</p>
<p>Password - Include Upper-Case Determines if the password can include upper-case letters.</p> <div> <p>NOTE</p> <ul style="list-style-type: none"> - Applies only when the <i>Password - Complexity</i> setting is set to <i>Manual complexity</i>. - Can be set in SAC Tools. </div>	<p>Value Name: pqUpperCase</p> <p>Values:</p> <ul style="list-style-type: none"> > 0 - Permitted > 1 - Forbidden > 2 - Mandatory <p>Default: 0</p>
<p>Password - Include Lower-Case Determines if the password can include lower-case letters.</p> <div> <p>NOTE</p> <ul style="list-style-type: none"> - Applies only when the <i>Password - Complexity</i> setting is set to <i>Manual complexity</i>. - Can be set in SAC Tools. </div>	<p>Value Name: pqLowerCase</p> <p>Values:</p> <ul style="list-style-type: none"> > 0 - Permitted > 1 - Forbidden > 2 - Mandatory <p>Default: 0</p>
<p>Password - Include Special Characters Determines if the password can include special characters, such as @,!, &.</p> <div> <p>NOTE</p> <ul style="list-style-type: none"> - Applies only when the <i>Password - Complexity</i> setting is set to <i>Manual complexity</i>. - Can be set in SAC Tools. </div>	<p>Value Name: pqSpecial</p> <p>Values:</p> <ul style="list-style-type: none"> > 0 - Permitted > 1 - Forbidden > 2 - Mandatory <p>Default: 0</p>

Description	Value
<p>Password Quality Check on Initialization</p> <p>Determines if the password quality settings are checked and enforced when a token is initialized.</p> <div data-bbox="172 422 930 548"> <p>NOTE It is recommended that this policy must not be set when tokens are enrolled using SafeNet Authentication Manager.</p> </div>	<p>Value Name: pqCheckInit</p> <p>Values:</p> <ul style="list-style-type: none"> > 1 (True) -The password quality is enforced > 0 (False) - The password quality is not enforced <p>Default: 0</p>
<p>Password Quality Owner</p> <p>Defines the owner of the password quality settings on a re-initialized token, and defines the default of the <i>Password Quality Modifiable</i> setting.</p>	<p>Value Name: pqOwner</p> <p>Values:</p> <ul style="list-style-type: none"> > 0 - Administrator > 1 - User <p>Default:</p> <ul style="list-style-type: none"> > 0 - For tokens with an Administrator Password > 1 - For tokens without an Administrator Password
<p>Enable Password Quality Modification</p> <p>Determines if the password quality settings on a newly initialized token can be modified by the owner.</p> <p>See the <i>Password Quality Owner</i> setting.</p>	<p>Value Name: pqModifiable</p> <p>Values:</p> <ul style="list-style-type: none"> > 1 (True) - The password quality can be modified by the owner > 0 (False) - The password quality cannot be modified by the owner <p>Default:</p> <ul style="list-style-type: none"> > 1 (True) - For administrator owned tokens > 0 (False) - For user owned tokens

Description	Value
<p>Enable Administrator Password Quality Check</p> <ul style="list-style-type: none"> > 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. <p>The character types are: upper-case letters, lower-case letters, numerals, and special characters.</p> <p>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.</p> <ul style="list-style-type: none"> > When disabled, the old behavior is as follows: <ul style="list-style-type: none"> • 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. <p>NOTE When the <i>ITI Certification mode</i> property is enabled, the <i>Enable Administrator Password Quality Check</i> property will be disabled.</p>	<p>Value Name: pqAdminPQ</p> <p>Values:</p> <ul style="list-style-type: none"> > 1 (Enabled) - Administrator Password Quality is enforced > 0 (Disabled) - Administrator Password Quality is disabled <p>Default: Enabled</p>

SAC Tools UI Access Control List

Access Control Properties determine which features are enabled in the SAC Tools and Tray Menu.

NOTE This setting enables /disables SAC UI buttons only and does not control any security restrictions or SAC functionality. The integration of SAC libraries with any third party applications is supported but should be used diligently by the third party applications.

The following settings are written to the **AccessControl** section in the file `/etc/eToken.conf`.

Access Control Feature	Value
All access control features are listed in below table	<p>Values:</p> <ul style="list-style-type: none"> > 1 (True) - The feature is enabled. > 0 (False) - The feature is disabled. <p>Default: 1(True) - except where indicated in the table</p>

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

Access Control Feature	Value Name	Description
Change Digital Signature PUK	ChangeDigitalSignaturePUK	Enables/Disables the <i>Change Digital Signature PUK</i> feature in SafeNet Authentication Client Tools.
Change Digital Signature PIN	ChangeDigitalSignaturePIN	Enables/Disables the <i>Change Digital Signature PIN</i> feature in SafeNet Authentication Client Tools.
Set Digital Signature PIN	SetDigitalSignaturePIN	Enables/Disables the <i>Set Digital Signature PIN</i> feature in SafeNet Authentication Client Tools.
Crypto Notification Timeout	CryptoNotificationTimeout	<ul style="list-style-type: none"> > 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. <div> NOTE By default, this feature is disabled. </div>
Rename Token	RenameToken	Enables/Disables the <i>Rename Token</i> feature in SAC Tools.
Change Token Password	ChangePassword	Enables/Disables the <i>Change Token Password</i> feature in SAC Tools.
Unlock Token	UnlocksToken	Enables/Disables the <i>Unlock Token</i> feature in SAC Tools.
Delete Token Content	CleareToken	Enables/Disables the <i>Delete Token Content</i> feature in SAC Tools.
View Token Information	ViewTokenInfo	Enables/Disables the <i>View Token Information</i> feature in SAC Tools.

Access Control Feature	Value Name	Description
Help	ShowHelp	Determines if the user can open the Help file in SAC Tools.
Advanced View	OpenAdvancedView	Determines if the user can open the <i>Advanced View</i> in SAC Tools.
Reader Settings	ManageReaders	Enables/Disables the <i>Reader Settings</i> feature in SAC Tools.
Initialize Token	InitializeEToken	Enables/Disables the <i>Initialize Token</i> feature in SAC Tools.
Import Certificate	ImportCertificate	Enables/Disables the <i>Import Certificate</i> feature in SAC Tools.
Reset Default Certificate Selection	ClearDefaultCert	Enables/Disables the <i>Reset Default Certificate Selection</i> feature in SAC Tools.
Delete Certificate	DeleteCertificate	Enables/Disables the <i>Delete Certificate</i> feature in SAC Tools.
Export Certificate	ExportCertificate	Enables/Disables the <i>Export Certificate</i> feature in SAC Tools.
Set Certificate as Default	SetCertificateAsDefault	Enables/Disables the <i>Set Certificate as Default</i> feature in SAC Tools.
Copy Certificate Data to Clipboard	CopyCertificateData	Enables/Disables the <i>Copy Certificate Data to Clipboard</i> feature in SAC Tools.
Log On as Administrator	LoginAsAdministrator	Enables/Disables the <i>Log On as Administrator</i> feature in SAC Tools.
Change Administrator Password	ChangeAdministratorPassword	Enables/Disables the <i>Change Administrator Password</i> feature in SAC Tools.
Set Token Password	SetUserPassword	Enables/Disables the <i>Set Token Password</i> feature in SAC Tools.

Access Control Feature	Value Name	Description
Token Password Retries	AllowChangeUserMaxRetry	Enables/Disables the <i>Logon retries before token is locked</i> feature (for the Token Password) in SAC Tools.
Administrator Password Retries	AllowChangeAdminMaxRetry	Enables/Disables the <i>Logon retries before token is locked</i> feature (for the Administrator Password) in SAC Tools.
Advanced Initialization Settings	OpenAdvancedModeOfInitialize	Enables/Disables the <i>Advanced</i> button in the <i>Token Initialization</i> window in SAC Tools. NOTE If disabled, IDPrime CC card cannot be initialized.
Change Initialization Key during Initialization	ChangeInitializationKeyDuringInitialize	Enables/Disables the <i>Change Initialization key</i> button in the <i>Advanced Token Initialization Settings</i> window in SAC Tools.
Common Criteria Settings	CommonCriteriaPasswordSetting	Enables/Disables the <i>Common Criteria</i> option in the Certification combo box.
System Tray - Unlock Token	TrayIconUnlockEToken	Enables/Disables the <i>Unlock Token</i> feature in the SAC Tray Menu.
System Tray - Delete Token Content	TrayIconClearEToken	Enables/Disables the <i>Delete Token Content</i> feature in the SAC Tray Menu. NOTE By default, this feature is Disabled.
System Tray - Change Token Password	TrayIconChangePassword	Enables/Disables the <i>Change Token Password</i> feature in the SAC Tray Menu.
System Tray - Select Token	SwitchToken	Enables/Disables the <i>Select Token</i> feature in the SAC Tray Menu.

Access Control Feature	Value Name	Description
System Tray - Tools	OpeneTokenProperties	Enables/Disables the <i>Tools</i> menu item (open SAC Tools) in the SAC Tray Menu.
System Tray - About	About	Enables/Disables the <i>About</i> menu item in the SAC Tray Menu.
System Tray- Generate OTP	GenerateOTP	Enables/Disables the System Tray- Generate OTP menu item in the SAC Tray Menu.
Enable Change IdenTrust Identity	IdetrusChangePassword	Enables/Disables the <i>Change IdenTrust PIN</i> feature in SAC Tools.
Enable Unblock IdenTrust Passcode	IdetrusUnlock	Enables/Disables the <i>Unlock IdenTrust</i> feature in SAC Tools.
Delete Data Object	DeleteDataObject	Enables/Disables the <i>Delete Data Object</i> feature in SAC Tools.
Allow One Factor	AllowOneFactor	Enables/Disables the <i>Allow One Factor</i> feature in the <i>Advanced Token > Initialization Settings</i> window in SAC Tools.
Verisign Serial Number <div> NOTE This property cannot be set in the Access Control Properties window. It must be set in the <code>conf</code> file. </div>	VerisignSerialNumber	Enables/Disables the <i>VerisignSerialNumber</i> feature in SAC Tools.

Access Control Feature	Value Name	Description
PIN Type	PinType	Defines which GUI PIN Properties are enabled/disabled in SAC Tools <i>Advanced PIN Properties</i> tab and the <i>Initialization</i> 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	Description
Minimum length (characters)	PinMinLen	Defines which GUI PIN Quality parameters are enabled/disabled in SAC Tools <i>Advanced</i> tab and the <i>Initialization</i> 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 the file `/etc/eToken.conf`.

Description	Value
<p>Opacity CA Certificate</p> <p>Defines the certificate for IDPrime PIV cards and tokens used in contactless mode for secure data exchange.</p> <p>If certificate is available then SAC can communicate with IDPrime PIV cards and tokens in contactless mode.</p>	<p>Value Name:CACert</p> <p>Value:</p> <p>> Base64(String)- Binary format (AAXXXBBB) of customCA certificate.</p> <p>Default: Base64(String) of default CA certificate</p>

Description	Value
<p>Key Management</p> <ul style="list-style-type: none"> > 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. 	<p>Value Name: Key-Management-Security</p> <p>Values: (String)</p> <ul style="list-style-type: none"> > Compatible: <ul style="list-style-type: none"> • Enables the use of features that are deprecated in the Optimized and Strict configurations below. • This is the default value for SAC versions below 10.5. Setting this value causes SAC to be compatible with SAC 10.5 and below. • It is strongly recommended to read "Security Recommendations" on page 70 before applying legacy values. > Optimized: <ul style="list-style-type: none"> • Disable the generation or creation of exportable keys. • Disable the exporting of keys, regardless of how they are 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: <ul style="list-style-type: none"> • Disable the generation or creation of exportable keys. • Disable the exporting of keys, regardless of how they are generated. • Disable all the unwrap-PKCS1.5 and unwrap-AES-CBC operations. • Disable any usage of symmetric keys off-board including unwrap. <p>Default: Optimized</p>

Description	Value
<p>Deprecated Cryptographic Algorithms and Features</p> <ul style="list-style-type: none"> > 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 if it is compatible with third-party applications. 	<p>Value Name: Disable-Crypto</p> <p>Values: (String)</p> <ul style="list-style-type: none"> > None - All SAC cryptographic algorithms and features are supported. <ul style="list-style-type: none"> • This is the default value for SAC versions below 10.5. Setting this value causes SAC to be compatible with SAC 10.5 and below. • It is strongly recommended to read "Security Recommendations" on page 70 before applying legacy values. > Obsolete - A list of restricted and deprecated cryptographic algorithms and features. <p>The following are deprecated: MD5, RC2, RC4, DES, 2DES, GenericSecret<112, RSA-RAW, RSA<2048, ECC<224, ECB, Sign-SHA1.</p> > Manual - Create your own list of deprecated algorithms and features. (See the description below). <p>Default: Obsolete</p>
<p>HashOffboard</p> <p>Determines the hash behavior used by the combined mechanisms CKM_SHA1_RSA_PKCS (eToken 5110) and CKM_SHA256_RSA_PKCS (eToken 5110 and eToken 5110 FIPS).</p>	<p>Value Name: HashOffboard</p> <p>Value:</p> <ul style="list-style-type: none"> > 1 (True) - Run hash off board > 0 (False) - Run hash on board <p>Set to True when required to run hash off-board.</p> <p>Default: 0 (False)</p>

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),

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.

To allow a cryptographic algorithm or feature, remove it from the list. For example, if the administrator wants to allow usage of RSA < 2048, it must be removed from the list.

Log Settings

The following settings are written to the **Log** section in the file `/etc/eToken.conf`.

Description	Value
Enabled Determines if the SAC 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

Description	Value
MaxFileSize Defines the maximum size of an individual log file. Once the maximum file 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 that the total maximum size is not exceeded.	Value Name: ManageTimeInterval Value: Enter a value in minutes (numerical). Default: 60 minutes

CHAPTER 6: Security Recommendations

The information in this chapter helps you maintain a secured SAC environment and keep your information safe.

Ensuring a Secured SAC Environment

This section provides short guidelines on how to maintain a safe PC computer environment. The information is based on the security recommendations defined by RedHat/Ubuntu.

Software Updates

The best way to keep your machine secure is to run the latest software. When new updates are available, a notification is received. Just accept the updates with a click and they download automatically. Keep checking for new updates every day, so it's easy to always have the latest and safest version.

Anti-Virus Software

Make sure to choose an effective Anti-Virus/Malware software to protect your client machines. It is essential to keep the Anti-Virus/Malware software updated.

Malware Awareness

Malware authors use several common tricks to install their malicious software on your PC. Understanding the most common ways they do this can help you stay protected.

- > **Email** – Malware often arrives on your PC in an email attachment. You should never open an attachment from someone you don't know or if an email looks suspicious. Instant messages and requests for file transfers can also spread malware.
- > **Websites** – Never open links to webpages that you don't recognize or that are sent from people you don't know. Malicious websites can install malware on your PC when you visit them.
- > **Use caution** – If you view a website that doesn't look quite right, or unexpected things happen when you visit, close your browser, download the latest updates for your security software and run a quick scan on your PC.
- > **Pirated software** – Malware is often bundled together with pirated software. When you install the pirated software you may also install malware.
- > **Social engineering** – Malware authors often try and trick you into doing what they want. This can be clicking or opening a file because it looks legitimate, paying money to unlock your PC or visiting a malicious webpage. These deceptive appeals are known as social engineering.
- > **Passwords** – Attackers may try to guess your Windows account or other passwords. This is why you should always use a password that can't be guessed easily. A strong password has at least eight characters and includes letters, numbers, and symbols.

- > **Removable drives** – Some types of malware, such as worms, can spread by copying themselves to any USB flash drives or other removable drives that are connected to your computer. Always be careful when sharing removable drives, and make sure you scan them.

Additional Environment Recommendations

The following actions will help keep your information as safe as possible:

- > Control access to your computer by locking your screen after a period of inactivity.
- > Set up secure file sharing.
- > Make sure you're running only those sharing services that you really need.
- > Disable Flash and Java. These frequently report security vulnerabilities.
- > Encrypt hard drive. This will protect your data if your computer accessed directly.

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
- > Disable Cryptographic Algorithm Policy

For more details, see ["Security Settings" on page 64](#).

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.

NOTE Once a restrictive policy is set, the use of SafeNet Authentication Client with the above algorithms is blocked.

- This might have implications on the way in which the third-party's applications currently work.
- Administrators must make sure that the third-party applications used by the organization are configured accordingly, and do not use one of the algorithms listed above, as they will be blocked.

Create Symmetric Key Objects using PKCS#11

The following are performed as part of SafeNet Authentication Client security enhancement campaign:

- > Protected memory is 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 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.

NOTE Keys that are created with previous SAC versions or on eToken Java devices which are formatted in non-FIPS/CC mode are not 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).