

**THALES**

# SafeNet Authentication Client

## LINUX USER GUIDE



## Document Information

<b>Product Version</b>	10.8 (GA)
<b>Document Number</b>	007-013843-002
<b>Release Date</b>	June 2021

## Revision History

<b>Revision</b>	<b>Date</b>	<b>Reason</b>
Rev. A	June 2021	Updated for release 10.8 (GA)

## Trademarks, Copyrights, and Third-Party Software

2021 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

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
Chapter 2: SafeNet Authentication Client User Interface .....	10
Overview .....	10
SafeNet Authentication Client Tray Icon .....	10
Running the SafeNet Authentication Client Monitor .....	11
SAC Tray Menu Functions .....	11
Opening the SafeNet Authentication Client Tray Menu .....	11
Closing SafeNet Authentication Client Monitor .....	12
SafeNet Authentication Client Tools .....	12
SafeNet Authentication Client Tools Toolbar .....	13
Opening the Simple View .....	13
Opening the Advanced View .....	15
Chapter 3: PIN Pad Readers .....	25
Using PIN Pad Readers with SAC .....	25
PIN Pad Readers with IDPrime Cards .....	25
PIN Pad Management Scenarios .....	25
PIN Pad Functions .....	26
PIN Pad Functional Limitations .....	26
Chapter 4: Token Management .....	28
Selecting the Active Token .....	28
Viewing and Copying Token Information .....	28
Logging On to the Token as a User .....	29
Renaming a Token .....	30
Changing the Token Password .....	30
Activating a Token .....	32
Unlocking a Token by the Challenge-Response Method .....	33
Deleting Token Content .....	36
Importing a Certificate to a Token .....	36
Importing Common Criteria Certificates .....	37
Exporting a Certificate from a Token .....	39

Deleting a Certificate .....	39
Logging On to the Token as an Administrator .....	40
Changing the Administrator Password .....	40
Setting a Token Password by an Administrator .....	41
<b>Chapter 5: Token Initialization .....</b>	<b>43</b>
Overview .....	43
Initializing eToken Devices .....	43
Initializing IDPrime Devices .....	49
Initializing IDPrime Common Criteria Devices .....	49
Initializing IDPrime Based Devices (Non Common Criteria/FIPS Devices) .....	55
Friendly Admin Password .....	59
<b>Chapter 6: Common Criteria .....</b>	<b>60</b>
Working with Common Criteria Certified Tokens and Cards .....	60
PKCS#11 Digital Signature PIN Authentication .....	60
Must Change Password .....	60
Common Criteria Extended Functions .....	61
Change Digital Signature PIN .....	61
Change Digital Signature PUK .....	62
Set Digital Signature PIN .....	63
Operational Differences and Role Protection .....	65
<b>Chapter 7: SafeNet eToken 5300 .....</b>	<b>66</b>
eToken 5300 Certificates .....	66
Viewing eToken 5300 Information .....	67
Using the eToken 5300 Touch Sense .....	69
eToken 5300 Touch Sense Timeout and Grace period .....	69
Touch Sense Timeout .....	69
Touch Sense Grace Period .....	69
<b>Chapter 8: Client Settings .....</b>	<b>70</b>
Setting Password Quality (eToken Devices only) .....	70
Allowing Password Quality Configuration on Token after Initialization (eToken Devices only) .....	71
Allowing Only an Administrator to Configure Password Quality on Token .....	71
Showing the SafeNet Authentication Client Tray Icon .....	72
Enabling Logging .....	72
To activate the logging function manually on a Linux System .....	72
To disable the logging feature manually on a Linux System .....	72
<b>Chapter 9: Token Settings .....</b>	<b>74</b>
Setting eToken Password Quality (Password Quality Tab) .....	74
Setting Private Data Caching Mode (Advanced Tab) .....	76
Setting Key Secondary Authentication (Advanced Tab) .....	77
Setting IDPrime PIN Quality (PIN Quality Tab) .....	78
Setting IDPrime PIN Properties (Advanced Tab) .....	79

# 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. This includes SafeNet Authentication Client users and administrators.

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
<b>bold</b>	The bold attribute is used to indicate the following: <ul style="list-style-type: none"> <li>&gt; Command-line commands and options that you enter verbatim (Type <b>dir /p</b>.)</li> <li>&gt; Button names (Click <b>Save As</b>.)</li> <li>&gt; Check box and radio button names (Select the <b>Print Duplex</b> check box.)</li> <li>&gt; Dialog box titles (On the <b>Protect Document</b> dialog box, click <b>Yes</b>.)</li> <li>&gt; Field names (<b>User Name</b>: Enter the name of the user.)</li> <li>&gt; Menu names (On the <b>File</b> menu, click <b>Save</b>.) (Click <b>Menu &gt; Go To &gt; Folders</b>.)</li> <li>&gt; User input (In the <b>Date</b> box, type <b>April 1</b>.)</li> </ul>
<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.
[ <b>optional</b> ] [<optional>]	Represent optional <b>keywords</b> 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.
{ <b>a b c</b> } {<a> <b> <c>}	Represent required alternate <b>keywords</b> 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.
[ <b>a b c</b> ] [<a> <b> <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](#)).

# CHAPTER 1: Introduction

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

## Overview

---

SafeNet Authentication Client is Public Key Infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities. It utilizes a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an internet transaction.

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

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

# CHAPTER 2: SafeNet Authentication Client User Interface

This section describes the SafeNet Authentication Client (SAC) Linux user interfaces.

**NOTE** In some instances, the word *Password* is replaced by *PIN* or *Passcode*.

## Overview

---

Administrators use SAC Tools to set token policies, and users use SAC Tools to perform basic token management functions, such as changing passwords and viewing certificates on the tokens. In addition, SAC Tools provides users and administrators with a quick and easy way to import digital certificates and keys between a computer and a token.

SAC Tools includes an initialization feature allowing administrators to initialize tokens according to specific organizational requirements or security modes, and a password quality feature, which sets parameters to calculate a token password quality rating.

SAC Tools provides information about the token, including its identification and capabilities. It has access to information stored on the token such as keys and certificates, and enables management of content, such as password profiles.

**CAUTION!** Do not disconnect a token from the USB port, or remove a smart card from the reader, during an operation. This can corrupt the data on the token or smart card.

SAC provides two user interfaces:

- > ["SafeNet Authentication Client Tray Icon" below](#)
  - For quick access to several token operations.
- > ["SafeNet Authentication Client Tools " on page 12](#)
  - Provides information about each connected token, including its identification and capabilities.
  - Allows to access information stored on each connected token, such as keys and certificates.
  - Enables management of token content, such as password policy.

## SafeNet Authentication Client Tray Icon

---

The SAC tray icon offers a shortcut menu to several token operations, and the tray icon is displayed as follows:

No Tokens Connected	One Token Connected	Multiple Tokens Connected
		

**NOTE** The SAC tray icon is visible only in GNOME Classic(x11) desktops such as Red Hat Enterprise Linux v8 and CentOS v8.  
For this, you need to perform some steps mentioned in the **Installation** chapter of *SafeNet Authentication Client Administrator Guide*.

## Running the SafeNet Authentication Client Monitor

The SafeNet Authentication Client tray icon is displayed only when the SAC Monitor is running.

**NOTE** If SAC is open and the tray icon is not displayed in the task bar, see ["Showing the SafeNet Authentication Client Tray Icon" on page 72](#).

### To open SafeNet Authentication Client Monitor on Linux:

- > Select **Applications > SafeNet Authentication Client**.

## SAC Tray Menu Functions

The following functions can be accessed quickly by right-clicking the tray menu:

- > **Tools:** Opens *SafeNet Authentication Client Tools*.
- > **About:** Displays product version information.
- > **Token selection:** Allows you to select one of the connected tokens to be the active token. This function is available only when more than one token is connected.
- > **Change Token Password:** Opens the *Change Password* window for the selected token. See ["Changing the Token Password" on page 30](#).
- > **Unlock Token:** opens the Token window for the selected token. See ["Activating a Token" on page 32](#).
- > **Certificate Information:** opens the Token Certificate Information window for the selected token.
- > **Exit:** Closes SafeNet Authentication Client and the tray icon.

## Opening the SafeNet Authentication Client Tray Menu

To access the shortcut menu from the SafeNet Authentication Client tray icon:

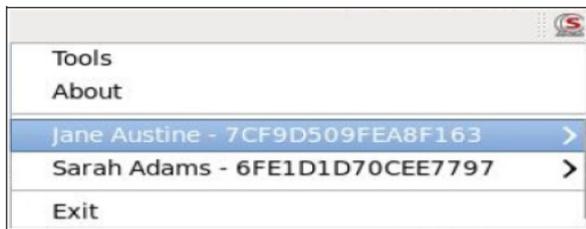
- > Right-click the **SafeNet Authentication Client** tray icon.

### Selecting the Token from the SAC Tray Menu

If more than one token is connected, select the required token from the tray menu by performing the following steps:

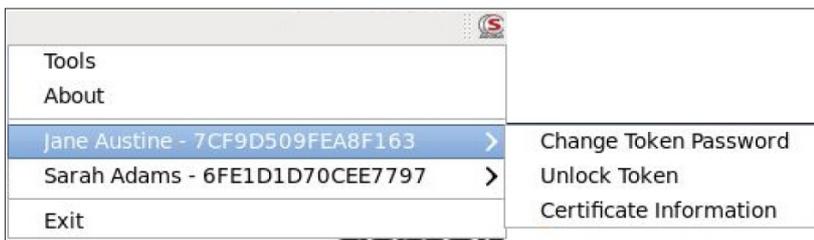
1. Right-click the **SafeNet Authentication Client** tray icon.

The **SafeNet Authentication Client** tray menu is displayed. Among the options, a list is displayed of the names and serial numbers of the connected tokens.



2. Select the required token.

Options for the selected token are displayed.



3. Select the required option.

## Closing SafeNet Authentication Client Monitor

Perform the following steps to close SafeNet Authentication Client monitor:

1. Right-click the **SafeNet Authentication Client** tray icon, and select **Exit**.  
A warning message is displayed.
2. Click **OK**.

## SafeNet Authentication Client Tools

SafeNet Authentication Client Tools includes two viewing options:

1. **Simple View:** To perform common tasks. See ["Opening the Simple View" on the next page](#).
2. **Advanced View:** For extensive control over SafeNet Authentication Client and your connected tokens. See ["Opening the Advanced View" on page 15](#).

Each view displays two panes:

1. The left pane indicates which token (Simple View) or which object (Advanced View) is to be managed.
2. The right pane enables the user to perform specific actions to the selected token or object.

A toolbar at the top of the window enables certain actions to be initiated in both views.

**CAUTION!** Do not disconnect a token from the USB port, or a smart card from the reader, during an operation. This can corrupt the data on the token or smart card.

## SafeNet Authentication Client Tools Toolbar

A toolbar is displayed at the top of the SafeNet Authentication Client Tools window, in both *Simple* and *Advanced* views. The toolbar contains the following icons:

Icon	Action
	<b>Advanced View</b> – Switches from the <i>Simple View</i> to the <i>Advanced View</i>
	<b>Simple View</b> – Switches from the <i>Advanced View</i> to the <i>Simple View</i>
	<b>Refresh</b> – Refreshes the data for all connected tokens
	<b>About</b> – Displays product version information
	<b>Help</b> – Opens the <i>Help</i> feature
	<b>Home</b> – Opens the company website ( <a href="http://cpl.thalesgroup.com/">cpl.thalesgroup.com/</a> )

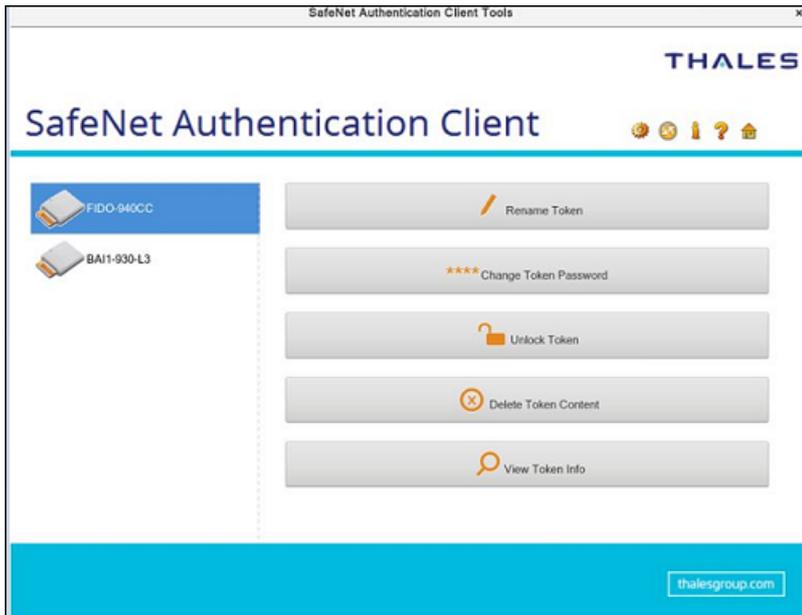
## Opening the Simple View

When SafeNet Authentication Client Tools is opened, the *Simple View* is displayed.

Perform the following step:

1. 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 in the *Simple View*.



When at least one token is connected, an icon representing each connected token is displayed in the left pane. The selected token is marked by a shaded rectangle.

### Token Icons

The icon displayed indicates the type of token that is connected.

Icon	Token Type
	Token Connected For a full list of supported devices, see <i>SafeNet Authentication Client Release Notes</i> .
	Smart Card reader – no card connected
	Smart Card reader – card connected For a full list of supported devices, see <i>SafeNet Authentication Client Release Notes</i> .
	Token with corrupted data This icon is also displayed when connecting a device needed to activate using an Activation PIN, see " <a href="#">Activating a Token</a> " on page 32
	Unknown token

### Simple View Functions

In the right pane, select an enabled button to perform the action described:

Function	Description
Rename Token	Sets a new name for the token
Change Token Password	Changes the token password
Unblock Token	Unblocks the token and resets the token password
Delete Token Content	Removes deletable data from the token (enabled by default)
View Token Info	Provides detailed information about the token

## Opening the Advanced View

The *SafeNet Authentication Client Tools > Advanced View* provides additional token management functions.

Perform the following steps:

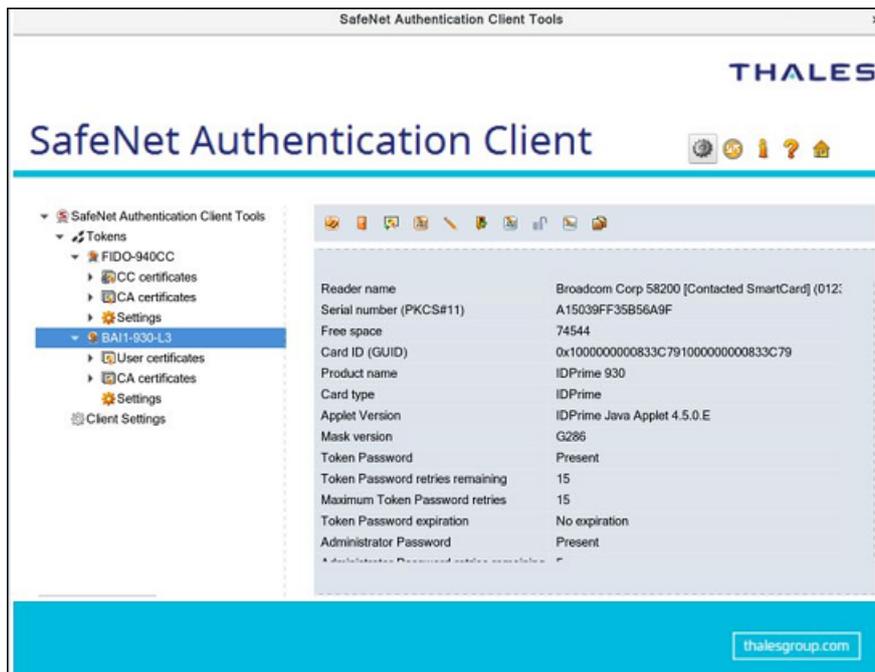
1. Do one of the following:

- 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 in the *Simple View*.

2. Click the **Advanced View** icon.

The **SafeNet Authentication Client Tools** window is displayed in the *Advanced View*.



The left pane provides a tree view of the different objects to be managed. The tree expands to show objects of the connected tokens.

### Advanced View Functions

You can access the advanced functions by selecting the required object from the left pane in the *SafeNet Authentication Client Tools > Advanced View* window.

Perform the following steps to access the advanced functions:

1. In the **SafeNet Authentication Client Tools > Advanced View** window, expand the tree in the left pane to display the required object.

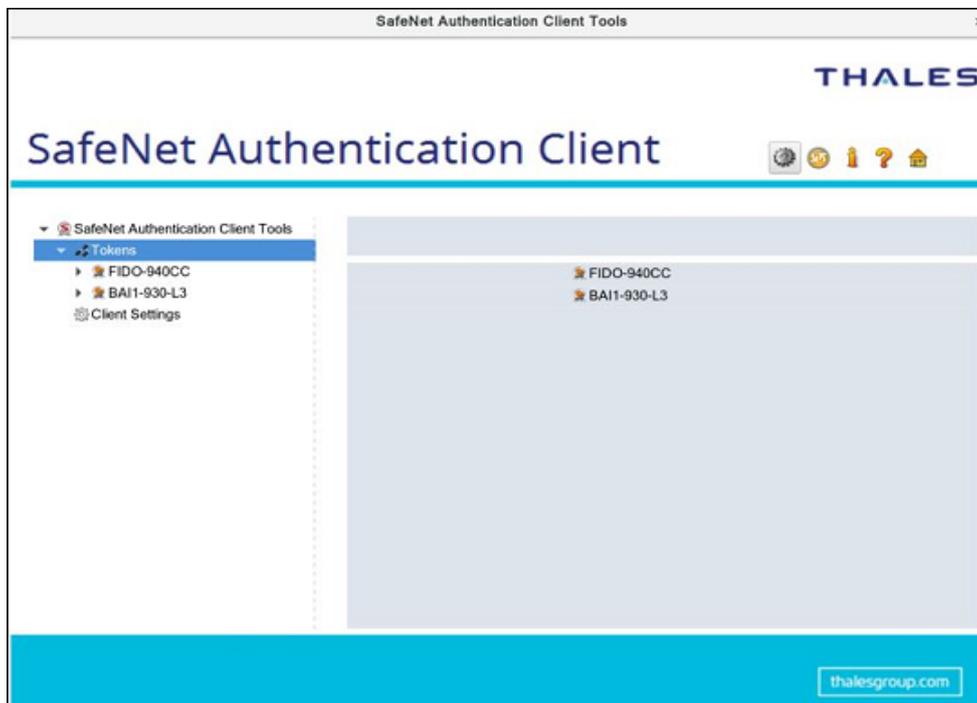
The relevant functions are displayed in the right pane.

2. Do one of the following:

- In the left pane, right-click the object, and select the required function.
- In the left pane, select the object. In the right pane, click the appropriate icon, or select the required tab.

### Tokens Node

When you select the *Tokens* node in the left pane, a list of connected tokens is displayed in the right pane.



### Selected Token Node

The token names are displayed in the left pane. When you select a token name, the following occurs:

- > Information about the token is displayed in the right pane, and function icons are displayed above it.
- > The name of the token reader is displayed in the tool-tip.

Right-click a token name to open a drop-down menu of the functions available for that token.

The following user functions are available:

User Function	Icon	Right-Click Menu Item
Initialize Token See <a href="#">"Token Initialization" on page 43</a>		Initialize Token
Log On to Token See <a href="#">"Logging On to the Token as a User" on page 29</a>		Log On to Token
Import Certificate See <a href="#">"Importing a Certificate to a Token" on page 36</a>		Import Certificate
Change Password See <a href="#">"Changing the Token Password" on page 30</a>		Change Password
Rename Token See <a href="#">"Renaming a Token" on page 30</a>		Rename Token
Copy to Clipboard See <a href="#">Chapter 4: Viewing and Copying Token Information, on page 34.</a>		(None)
Change Digital Signature PIN See <a href="#">"Change Digital Signature PIN" on page 1</a>		Change Digital Signature PIN
Change Digital Signature PUK See <a href="#">"Change Digital Signature PUK" on page 1</a>		Change Digital Signature PUK
Set Digital Signature PIN See <a href="#">"Set Digital Signature PIN" on page 1</a>		Set Digital Signature PIN

**NOTE** Depending on the token type, additional options may be displayed in the drop-down menu.

Some administrator functions are available only if an Administrator Password has been set for the token. The administrator icons are located on the right side of the window:



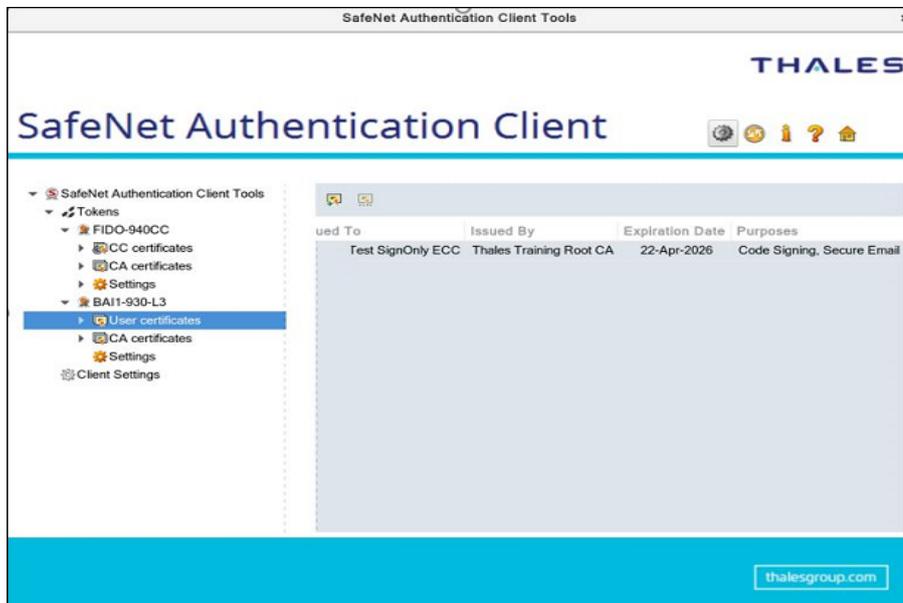
See ["Logging On to the Token as an Administrator" on page 40.](#)

### Certificate Type Node

If the selected token contains certificates, the following Certificate Type nodes are displayed in the left pane under the *Tokens* node:

- > User Certificates
- > Administrator (ECC)
- > Certificate Authority Certificates (CA)
- > Common Criteria Certificates (CC)

When you select a Certificate Type node, a list of the appropriate certificates on the token is displayed in the right pane.



Depending on the certificate type, the following functions may be available:

User Function	Icon	Right-Click Menu Item
Import Certificate See <a href="#">"Importing a Certificate to a Token" on page 36.</a>		Import Certificate
Reset Default Certificate Selection		Reset Default Certificate Selection ( <b>Windows only</b> )

A node for each certificate is displayed in the left pane under the Certificate Type node.

### Common Criteria Certificates

Common Criteria (CC) Certificates are supported by eTokens and IDPrime cards.

Common Criteria certified devices require a common criteria certificate to be imported onto the token/card. This provides an extra authentication layer for digital signing purposes. See ["Importing Common Criteria Certificates" on page 37.](#)

**NOTE** Standard Common Criteria devices support only ECC 256. For more information, refer to IDPrime documentation.

For a full list of devices supporting CC Certificates, see *SafeNet Authentication Client Release Notes*.

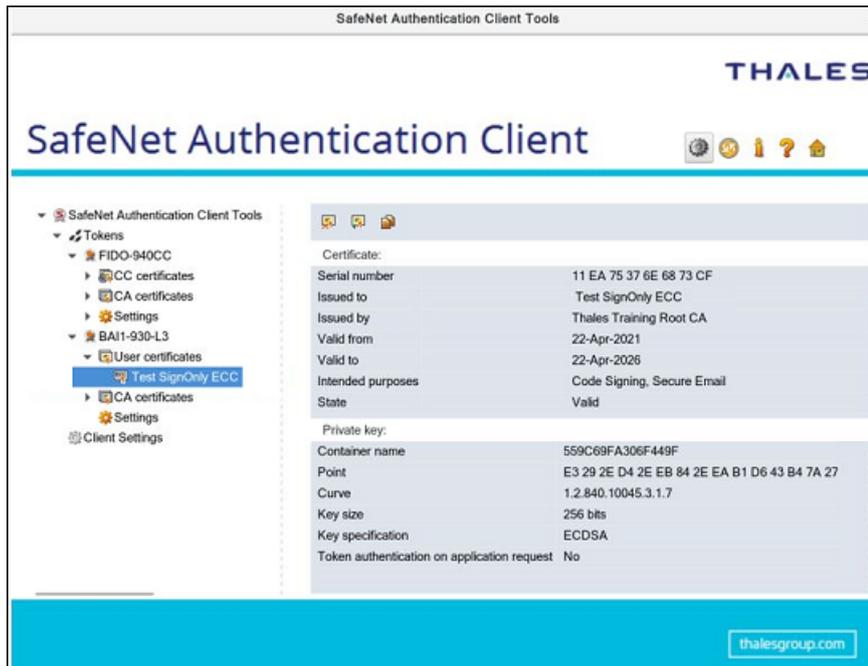
### ECC Certificates

ECC Certificates are supported by eTokens and IDPrime cards.

For a full list of devices supporting ECC Certificates, see *SafeNet Authentication Client Release Notes*.

### Selected Certificate Node

When you select a certificate under the *User certificates*, *CA certificates*, or *CC certificates* node, information about the certificate is displayed in the right pane.



Some or all of the following functions are available:

User Function	Icon	Right-Click Menu Item
Delete Certificate See <a href="#">"Deleting a Certificate"</a> on page 39.		Delete Certificate
Export Certificate See <a href="#">"Exporting a Certificate from a Token"</a> on page 39.		Export Certificate
Copy to Clipboard See <a href="#">"Viewing and Copying Token Information"</a> on page 28.		(None)

### Settings Node

Each connected device has a *Settings node*. Select it to see the settings in the right pane.

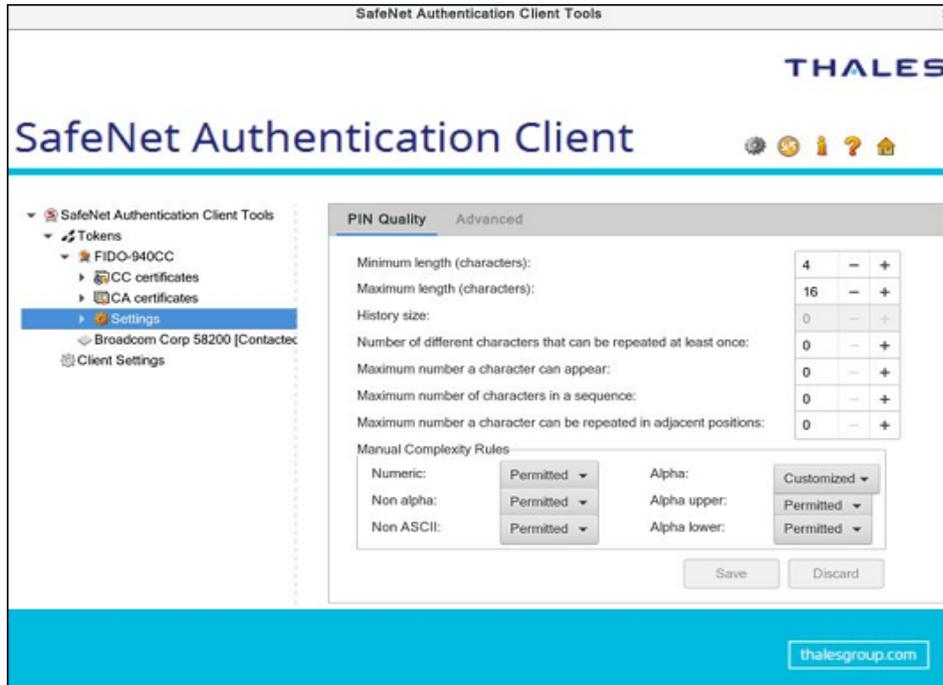
The following tabs exist for IDPrime and eToken Common Criteria devices:

> **PIN Quality**

See "[Setting IDPrime PIN Quality \(PIN Quality Tab\)](#)" on page 78.

> **Advanced**

See "[Setting IDPrime PIN Properties \(Advanced Tab\)](#)" on page 79.



The following tabs exist for eToken devices:

> **Password Quality**

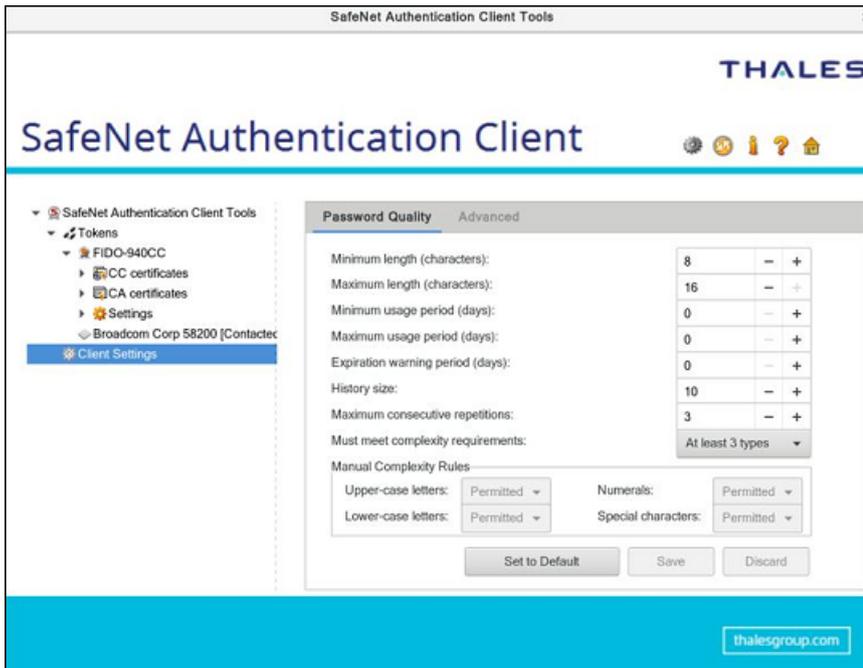
See "[Setting eToken Password Quality \(Password Quality Tab\)](#)" on page 74.

> **Advanced**

See "[Setting Private Data Caching Mode \(Advanced Tab\)](#)" on page 76.

**Client Settings Node**

Even when no tokens are connected, the left pane includes a *Client Settings* node. Select it to view your computer's SafeNet Authentication Client Settings in the right pane.



The changes you make to the *Client Settings* window affects eToken devices (excluding eToken CC) that is initialized using this computer after the changes have been saved.

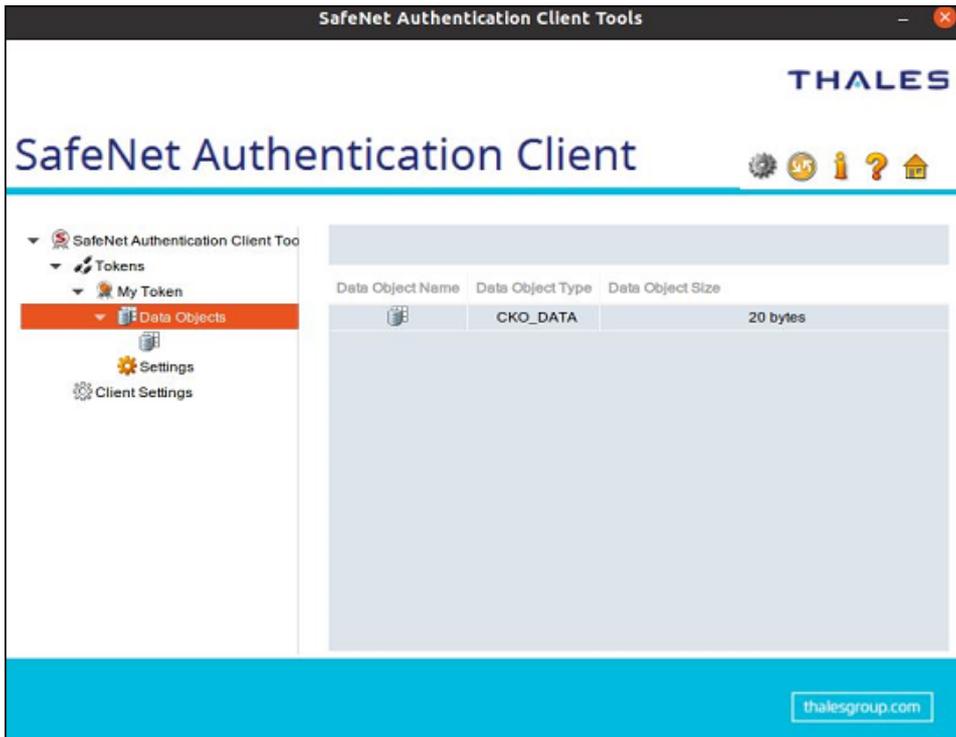
Similar to the *Settings* window, the *Client Settings* window contains two tabs:

- > Password Quality
- > Advanced

See "[Client Settings](#)" on page 70.

### Data Objects Node

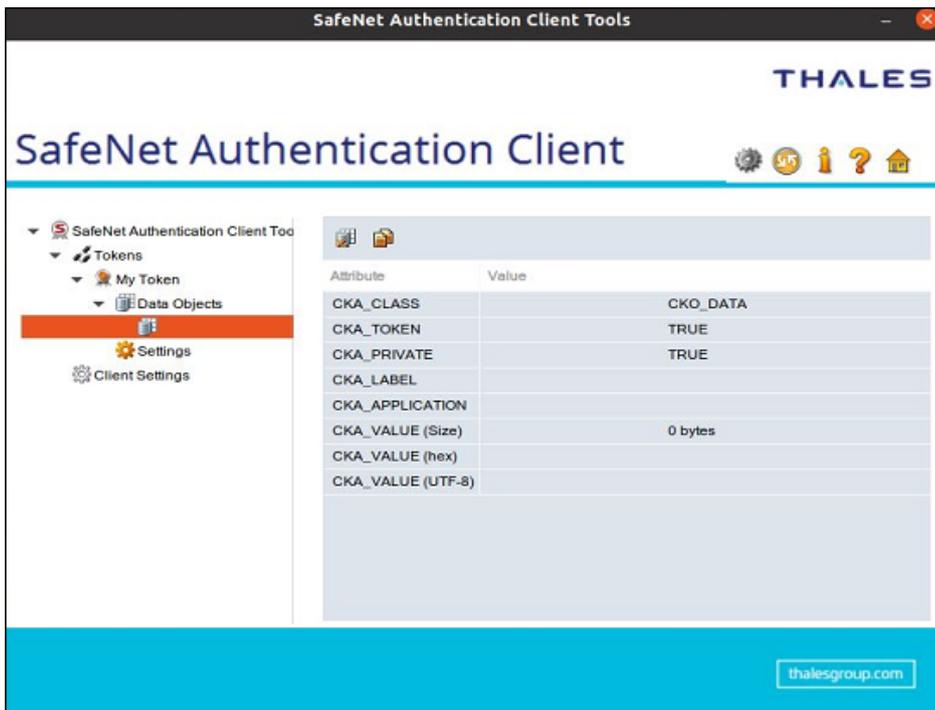
Tokens used with some applications (for example, Entrust) have a *Data Objects* node, which contains PKCS#11 data objects.



### To view the contents of a data object

Perform the following steps:

1. In the left pane, under the **Tokens** node, expand the **Data Objects** node.  
Details of all the data objects (Name, Type, and Size) are displayed in the right pane.
2. Select a data object.  
The contents of the data object (Value Name and Value Type) are displayed in the right pane.



### To delete a data object

Perform the following steps:

1. Select the value to be deleted.
2. Click the **Delete Data Object** icon .

### Orphan Objects Node

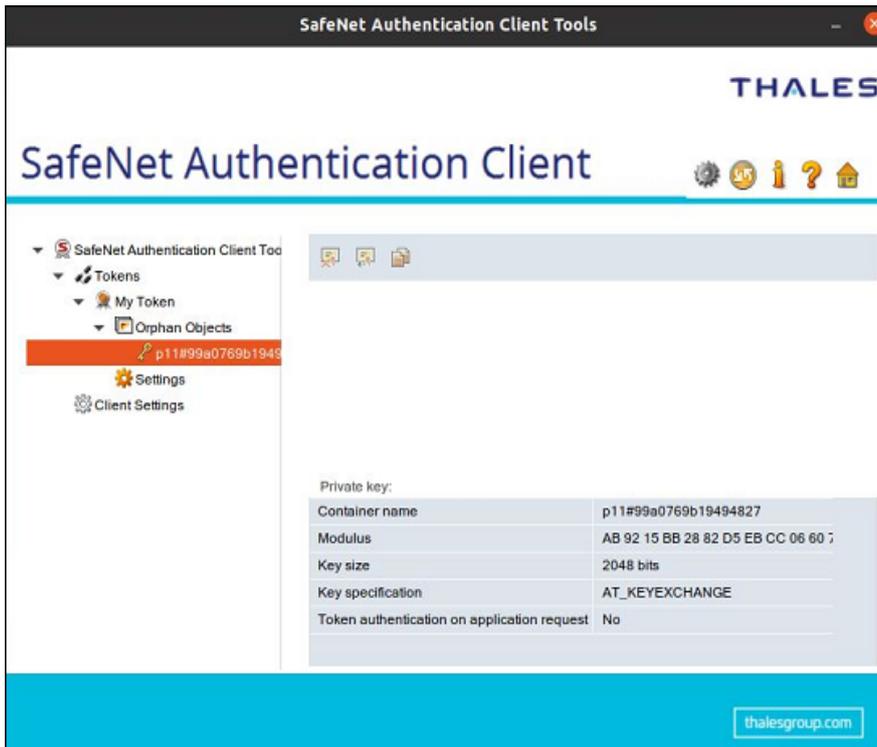
An orphan object is a certificate without its key or a key without its certificate. A token's *Orphan Objects* node displays these objects.

### To view a token's orphan objects

Perform the following steps:

1. In the left pane, under the **Tokens** node, expand the **Orphan Objects** node.
2. Select an orphan object.

The certificate data or the key data of the orphan object is displayed in the right pane.



### To delete an orphan object

Perform the following steps:

1. Right-click the **Orphan Object** on the left, and select **Delete**.
2. Click the **Delete Orphan Object** icon .

# CHAPTER 3: PIN Pad Readers

## Using PIN Pad Readers with SAC

This chapter describes the capabilities and limitations of using PIN Pad readers with IDPrime cards. A PIN Pad reader can be any device that has a keyboard for secure PIN entry, this could be, for example, a keyboard with an embedded smart card reader. PIN Pad readers are usually associated with smart cards that have the PIN type set up as External PIN.

For a complete list of smart cards supported with PIN Pad readers, see *SafeNet Authentication Client Release Notes*.

## PIN Pad Readers with IDPrime Cards

The following PINs are configured as external PINs. They are supported by PKCS#11 and SafeNet Minidriver:

- > IDPrime MD 3840/840 and SafeNet IDPrime 3940/940 Cards - Role 1 (User), Role 3 (Digital Signature PIN) and Role 4 (Digital Signature PUK)
- > IDPrime MD 830/3810/930/3930 - Role 1 (User) only

**NOTE** The PIN entry is requested for each signature performed with Role 3, as Role 3 protects Certificates with Non-repudiation Key usage.

## PIN Pad Management Scenarios

Below table describes the different scenarios for PINs and PIN Pad readers:

Scenario	Initial PIN Type	Connected Reader	PIN Operating Mode
1	Regular	Normal	Regular
2	Regular	PIN Pad	External
3	External	Normal	Regular
4	External	PIN Pad	External

- > **Regular** - PIN is entered using the computer keyboard
- > **External** - PIN is entered using an external PIN pad reader
- > **Setting the NoRegularFallback flag changes the third scenario as follows:**  
External PIN & Normal Reader - Login refused

> **Setting the `NoAutoPINpad` flag changes the second scenario as follows:**

Regular PIN & PIN Pad Reader - Regular PIN

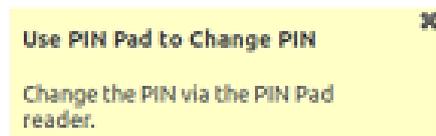
## PIN Pad Functions

When performing the functions below using a PIN pad reader, the 'Use PIN pad to...' notification window appears requiring the PIN to be entered using the PIN pad reader.

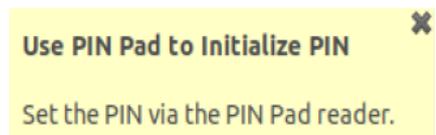
> Logging on to the token (See "[Logging On to the Token as a User](#)" on page 29).



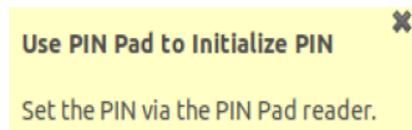
> Change PIN (See "[Changing the Token Password](#)" on page 30).



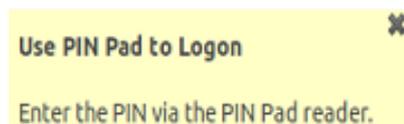
> Unlock Token by the Challenge-Response Method (See "[Unlocking a Token by the Challenge-Response Method](#)" on page 33).



> Setting a Token Password by an Administrator (See "[Setting a Token Password by an Administrator](#)" on page 41).



When performing a See What You Sign (SWYS) operation, information is displayed on a SWYS reader and must be signed using the SWYS PIN Pad reader.



## PIN Pad Functional Limitations

The following functional limitations exist with the PIN pad:

- > When using an IDPrime MD 840/3840 device with the **Must change password on first logon** feature enabled, you are required to log in again.
- > Secure Messaging (SM) PINs are not supported (FIPS level 3).

- > EZIO Shield PRO reader does not support Secure Messaging (SM) protected operations such as import key pair, generate key pair and change administrator key.
- > Some PIN pad readers (for example: EZIO Bluetooth) have their built-in password policies. When changing the password via these readers, the new password must comply with both the reader's password quality and card password quality policies.

# CHAPTER 4: Token Management

SafeNet Authentication Client Tools and the SafeNet Authentication Client tray menu enable you to control the use of your tokens.

When running a management task, ensure that the appropriate token remains connected until the process completes.

## Selecting the Active Token

---

If more than one token is connected, select which token to work with.

### To set a token as the active token from the SafeNet Authentication Client Tools window

Perform the following steps:

1. Open **SafeNet Authentication Client Tools**.

See "[Opening the Simple View](#)" on page 1 or "[Opening the Advanced View](#)" on page 1.

2. In the left pane, select the required token.

### To set a token as the active token from the tray icon

Perform the following steps:

1. Left-click the **SafeNet Authentication Client** tray icon.

The **SafeNet Authentication Client** tray menu is displayed.

2. Select the required token from the tray menu by hovering over the relevant token name.

A sub-menu appears displaying a list of tasks that can be performed on the active token.

3. Select the relevant option from the sub-menu.

## Viewing and Copying Token Information

---

Perform the following steps to view and copy token information:

1. Do the following to view token information from the *Simple View*:

- a. Open **SafeNet Authentication Client Tools > Simple View**.

See "[Opening the Simple View](#)" on page 1.

- b. In the left pane, select the required token.

- c. In the right pane, select **View Token Info**.

- d. Continue with step 3.

2. Do the following to view token information from the *Advanced View*:

- a. Open **SafeNet Authentication Client Tools > Advanced View**.

See "Opening the Advanced View" on page 1.

- b. In the left pane, select the node of the required token.
- c. Continue with step 3.
3. The **Token Information** is displayed. The information displayed varies according to the type of token.
4. Do the following to copy the token information to the clipboard:
  - In the **Token Information** window, click **Copy**
  - In **Advanced View**, click the **Copy to Clipboard** icon .
5. To paste the copied token information, click the cursor in the target application, and paste the information.
6. Click **OK**.

## Logging On to the Token as a User

You must log on to the token before you can use or change its token content.

Perform the following steps to log on as a user:

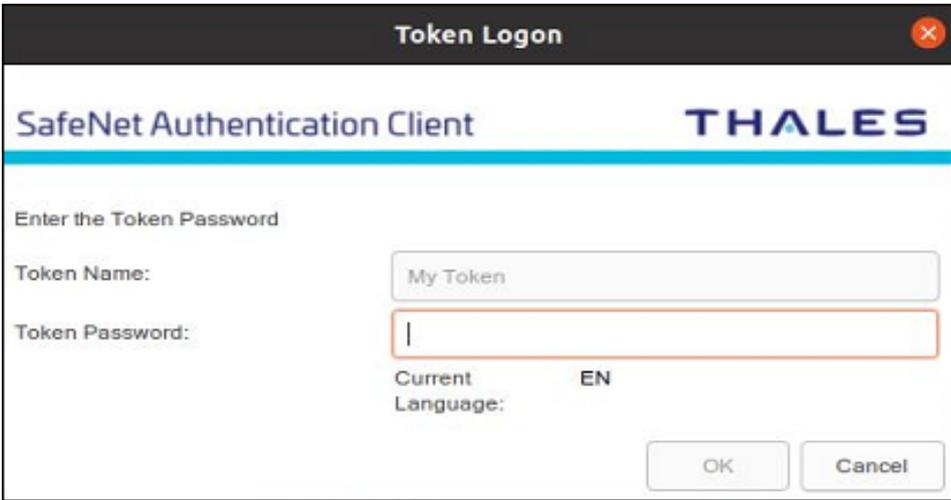
1. Open **SafeNet Authentication Client Tools > Advanced View**.

See "Opening the Advanced View" on page 1.

**NOTE** If the *Log Off from Token* icon or the *Log Off* option is displayed, you are already logged on to the token.

2. Do one of the following:
  - In the left pane, select the node of the required token.
  - In the right pane, click the **Log On to Token** icon .
  - In the left pane, right-click the node of the required token, and select **Log On to Token**.

The **Token Logon** window is displayed.



3. Enter the token password, and click **OK**.

You are logged on to the token.

## Renaming a Token

The token name does not affect the token contents. It is used solely to identify the token.

**NOTE** If you have more than one token, it is recommended assigning each one a unique token name.

Perform following steps to rename a token:

1. Do the following to view token information from the *Simple View*:
  - a. Open **SafeNet Authentication Client Tools > Simple View**.  
See "[Opening the Simple View](#)" on page 1.
  - b. In the left pane, select the required token.
  - c. In the right pane, select **Rename Token**.
  - d. Continue with step 3.
2. Do the following to view token information from the *Advanced View*:
  - a. Open **SafeNet Authentication Client Tools > Advanced View**.  
See "[Opening the Advanced View](#)" on page 1.
  - b. Do one of the following:
    - In the left pane, select the node of the required token.  
  
In the right pane, click the **Rename Token** icon .
    - In the left pane, right-click the node of the required token, and select **Rename Token**.
  - c. Continue with step 3.  
The **Token Logon** window is displayed.
3. Enter the token password, and click **OK**.  
The **Token Rename** window is displayed.
4. Enter the new name in the **New token Name** field, and click **OK**.  
The new token name is displayed in the **SafeNet Authentication Client Tools** window.

## Changing the Token Password

**NOTE** The term *Token Password* may be replaced by another term (for example, Token PIN), depending on your SAC configuration.

SafeNet eTokens are supplied with an initial default token password. In most organizations, the initial token password is **1234567890**.

IDPrime cards are supplied with an initial default token password: **0000**.

To ensure strong, two-factor security, it is important for the user to change the initial token password to a private password as soon as the new token is received.

When a token password is changed, the new password is used for all token applications involving the token. It is the user's responsibility to remember the token password. Without it, the token cannot be used. The administrator can set a token's *Password Quality* settings to certain password complexity and usage requirements.

**NOTE** The token password is an important security measure in safeguarding your company's private information. The best passwords are at least eight characters and include upper-case and lower-case letters, special characters such as punctuation marks, and numbers appearing in random order.

It is recommended not to use easily discovered passwords, such as names or birth dates of family members.

Perform the following steps to change a token's password:

1. Do the following to view token information from the *Simple View*:
  - a. Open **SafeNet Authentication Client Tools > Simple view**.  
See "[Opening the Simple View](#)" on page 1.
  - b. In the left pane, select the required token.
  - c. In the right pane, select **Change Token Password**.
  - d. Continue with step 4.
2. Do the following to change the token password from the *Advanced View*:
  - a. Open **SafeNet Authentication Client Tools > Advanced View**.  
See "[Opening the Advanced View](#)" on page 1.
  - b. Do one of the following:
    - In the left pane, select the node of the required token.  
  
In the right pane, click the **Change Token Password** icon .
    - In the left pane, right-click the node of the required token, and select **Change Token Password**.
  - c. Continue with step 4.
3. Do the following to change the token password using the tray menu:
  - a. Left-click the **SafeNet Authentication Client** tray icon.
  - b. If more than one token is connected, hover over the appropriate token.
  - c. Select **Change Token Password**.
  - d. Continue with step 4.

The **Change Password** window is displayed.

**Change Password: My Token**

SafeNet Authentication Client **THALES**

Current Token Password:

New Token Password:

Confirm Password:

The new password must comply with the quality settings defined on the token.

A secure password has at least 8 characters, and contains upper-case letters, lower-case letters, numerals, and special characters (such as !, \$, #, %).

Current Language: EN  
Enter your current password.

OK Cancel

4. Enter the current token password in the **Current Token Password** field.

**NOTE** If an incorrect password is entered more than a pre-defined number of times, the token becomes locked.

5. Enter a new token password in the **New Token Password** and **Confirm Password** fields.

**NOTE** As you type a new password, the password quality indicator on the right displays a percentage score of how well the new password matches the password quality requirements.

6. Click **OK**.

A message confirms that the token password was changed successfully.

7. Click **OK**.

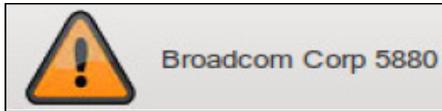
## Activating a Token

Devices that are protected by an activation PIN must be activated before first use. Entering an Activation PIN is required only once.

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

The *Token Activation* function is accessed quickly by right-clicking the tray menu.

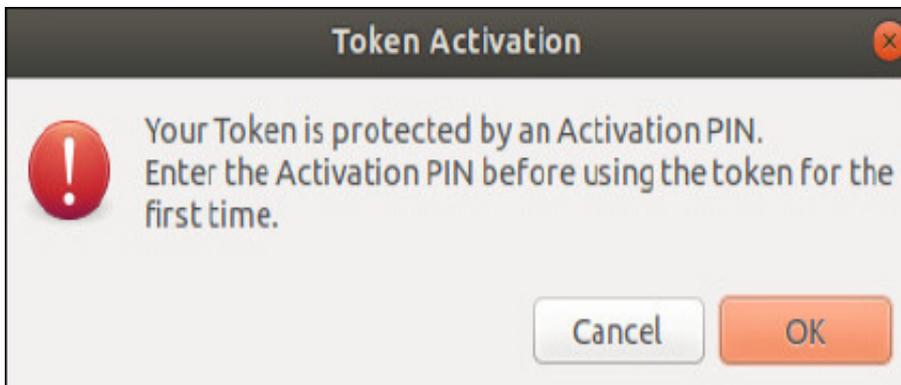
Connecting an unactivated device displays the Token with corrupted data icon in SAC Tools. This does not mean that the device is corrupted, it simply needs to be activated.



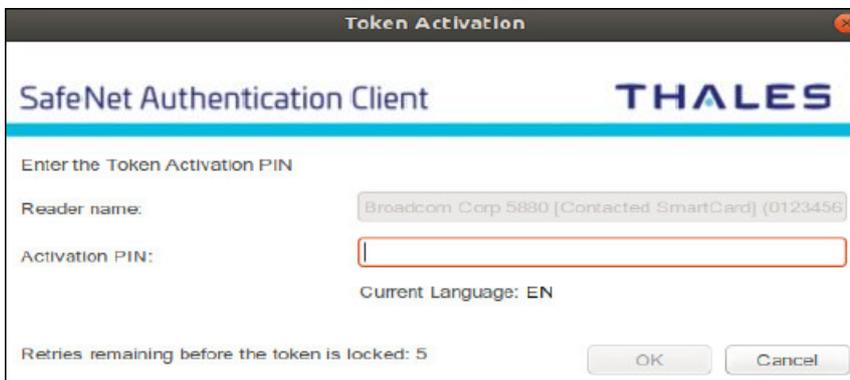
Perform the following steps to activate a token:

1. Connect the token.

The **Token Activation** window is displayed.



2. Click **OK** to continue with the activation process or **Cancel** to close the window without activating the token.
3. Enter activation PIN (Role 1), and click **OK**.



If an incorrect activation PIN is entered more than 5 times, the token becomes locked, leaving the token in an unusable state. The Token Activation retries remaining field is displayed at the bottom of the **Token Activation** window.

4. After activating your token, open SAC Tools to view token information. Your device is ready to be used.

**NOTE** Token functions are enabled only after the correct activation PIN has been entered.

## Unlocking a Token by the Challenge-Response Method

If an incorrect token password is entered more than a pre-defined number of times, the token becomes locked.

Tokens can be unlocked if, and only if, an Administrator Password was set during initialization.

**NOTE**

The unlock feature is supported by eToken and IDPrime devices.  
For Common Criteria devices, the new user password is used for both the token password and Digital Signature PIN when unblocking a device.

When the administrator has access to the user's token, the administrator can unlock the token using the *Set Token Password* feature. See "[Setting a Token Password by an Administrator](#)" on page 41.

Another way to unlock the token and set a new token password is to use the Challenge – Response authentication method. The user sends the administrator the Challenge Code supplied by SafeNet Authentication Client Tools, and then enters the Response Code provided by the administrator. The token becomes unlocked, and the new token password set by the user replaces the previous password.

This method requires a management system, such as SafeNet Authentication Manager, that can generate Response Codes.

**NOTE** Unlocking the User PIN via the Challenge-Response method is not supported on Common Criteria cards when the User PIN is protected by the PUK.

Perform the following steps to unlock a token using the Challenge-Response method:

1. Do the following to unlock a token from the *Simple View*:
  - a. Open **SafeNet Authentication Client Tools > Simple View**.  
See "[Opening the Simple View](#)" on page 1.
  - b. In the left pane, select the required token.
  - c. In the right pane, select **Unlock Token**.
  - d. Continue with step 4.
2. Do the following to unlock a token from the *Advanced View*:
  - a. Open **SafeNet Authentication Client Tools > Advanced View**.  
See "[Opening the Advanced View](#)" on page 1.
  - b. Do one of the following:
    - In the left pane, select the node of the required token.  
In the right pane, click the **Unlock** icon.
    - In the left pane, right-click the node of the required token, and select **Unlock**.
  - c. Continue with step 4.
3. Do the following to change the token password using the tray menu:
  - a. Right-click the **SafeNet Authentication Client** tray icon.
  - b. If more than one token is connected, hover over the appropriate token.
  - c. Select **Unlock Token**.
  - d. Continue with step 4.

4. The **Unlock Token** window is displayed, displaying a value in the **Challenge Code** field.

The *Challenge Code* is 16 characters or, if the token was initialized as Common Criteria, 13 characters.

5. Contact your administrator, and provide the administrator with the Challenge Code value displayed.

**NOTE** To copy the Challenge Code to the clipboard, click the **Copy to Clipboard** icon.

**CAUTION!**

- After providing the Challenge Code to the administrator, do not undertake any activities that use the token until you receive the Response Code and complete the unlocking procedure.
- If any other token activity occurs during this process, it affects the context of the Challenge – Response process and invalidate the procedure.
- For IDPrime devices only - During the unlock operation, any application that attempts to connect to the device is suspended until the unlock operation is completed or canceled.

6. Enter the **Response Code** provided by the administrator.

The Response Code is 16 characters or, if the token is initialized as Common Criteria, 39 characters.

**NOTE** Response Code creation depends on the back-end application being used by the organization. Administrators should refer to the relevant documentation for information on how to generate the Response Code.

7. Enter a new token password in the **New Password** and **Confirm Password** fields.
8. If the new password is known to others and must be changed, select **Token Password must be changed on first logon**.
9. Click **OK**.  
A message confirms that the token was unlocked successfully.
10. Click **OK**.

## Deleting Token Content

---

Objects on your token can include data objects (profiles), keys, and CA or user certificates. Your system configuration determines which objects are deletable.

The *Delete Token Content* function deletes all deletable objects on your token. Non-deletable objects are not removed from the token. The function does not change settings on the token, such as password quality requirements.

The *Delete Token Content* function is less comprehensive than the Initialize function which restores a token to its initial state, removing all objects stored on the token since manufacture and resetting the token password, see "[Token Initialization](#)" on page 43.

Perform the following steps to delete the token content in the *Simple View*:

1. Open **SafeNet Authentication Client Tools > Simple View**.  
See "[Opening the Simple View](#)" on page 1.
  - a. In the left pane, select the required token.
  - b. In the right pane, select **Delete Token Content**.
  - c. Continue with step 3.
2. Depending on the configuration of your system, you can use the tray menu:
  - a. Left-click the **SafeNet Authentication Client** tray icon.
  - b. If more than one token is connected, hover over the appropriate token.
  - c. Select **Delete Token Content**.
  - d. Continue with step 3.The **Token Logon** window is displayed.
3. Enter the token password, and click **OK**.  
The **Delete Token Content** window is displayed, prompting you to confirm the delete action.
4. To continue with the delete process, click **OK**.  
The **Delete Token Content** window is displayed, confirming that the token content is deleted successfully.
5. Click **OK** to finish.

## Importing a Certificate to a Token

---

The following certificate types are supported:

- > .pfx
- > .p12
- > .cer

When importing PFX files, the private key and corresponding certificate are imported to the token. The user is asked to enter the password (if it exists) that protects the PFX file.

Perform the following steps to import a certificate:

**1. Open **SafeNet Authentication Client Tools** > **Advanced View**.**

See "[Opening the Advanced View](#)" on page 1.

**2. Do one of the following:**

- In the left pane, select the node of the required token.

In the right pane, click the **Import Certificate** icon .

- In the left pane, right-click the node of the required token, and select **Import Certificate**.

The **Token Logon** window is displayed.

**3. Enter the token password, and click **OK**.**

The **Certificate Selection** window is displayed.

**4. Select the certificate to import, and click **Open**.**

- a.** If the certificate requires a password, the **Password** window is displayed.

Enter the certificate password, and click **OK**.

- b.** If the certificate is a Common Criteria certificate, the **Import PIN** window is displayed.

Enter the token's Import PIN defined during token initialization, and click **OK**.

The default value is 1234567890.

All requested certificates are imported, and a message confirms that the import was successful.

## Importing Common Criteria Certificates

When importing PFX files, the private key and corresponding certificate are imported to the token. The user is asked if the CA certificates should be imported to the token, and the password (if it exists) that protects the PFX file must be entered.

Perform the following steps to import a Common Criteria Certificate:

**1. Open **SafeNet Authentication Client Tools** > **Advanced View**.**

See "[Opening the Advanced View](#)" on page 15.

**2. Do one of the following:**

- In the left pane, select the node of the required token.

In the right pane, click the **Import Certificate** icon .

- In the left pane, right-click the node of the required token, and select **Import Certificate**.

The **Token Logon** window is displayed.

3. Enter the token password, and click **OK**.

The **Certificate Selection** window is displayed.

4. Select the certificate to import, and click **Open**.

The **Certificate Password** window is displayed.

5. Enter the certificate password, and click **OK**.

The **Digital Signature Logon** window is displayed.

The Digital Signature PIN is required as an additional authentication layer for digital signing purposes.

6. Enter the Digital Signature PIN and click **OK**.

The certificate is imported, and a message confirms that the import is successful.

Common Criteria (CC) certificates are displayed as follows in the left pane:



## Exporting a Certificate from a Token

Perform the following steps to export a certificate:

1. Open **SafeNet Authentication Client Tools > Advanced View**.  
See ["Opening the Advanced View" on page 1](#).
2. In the left pane, expand the node of the required token.
3. Do one of the following:
  - Select the required certificate, and click the **Export Certificate** icon .
  - Right-click the required certificate, and select **Export Certificate**.

The **Save As** window is displayed.
4. Select the location to store the certificate, enter a file name, and click **OK**.

**NOTE** The certificate file must be DER-encoded or Base64, and not PKCS #7.

## Deleting a Certificate

Perform the following steps to remove a certificate from a token:

1. Open **SafeNet Authentication Client Tools > Advanced View**.  
See ["Opening the Advanced View" on page 1](#).
2. In the left pane, expand the node of the required token.
3. Do one of the following:
  - In the left pane, select the required certificate, and click the **Delete Certificate** icon.
  - In the left pane, right-click the required certificate, and select **Delete Certificate**.

The **Delete Certificate** window is displayed.
4. To delete the certificate, click **Yes**.  
The **Token Logon** window is displayed.

5. Enter the token password, and click **OK**.

The **Delete Certificate** window is displayed, confirming that the certificate is deleted successfully.

6. Click **OK**.

## Logging On to the Token as an Administrator

If an Administrator Password was set on the token during token initialization, and the user forgets the token password, use the Administrator Password to unlock the token by setting a new token password. It is recommended to initialize all supported tokens with an Administrator Password.

**NOTE** IDPrime devices have a built-in administrator role.

An administrator has limited permissions on a token. No changes to any user information can be made by the administrator, nor can the user's security be affected. The administrator can change only specific data stored on the token only by using the following functions:

- > ["Changing the Administrator Password" below](#)
- > ["Setting a Token Password by an Administrator" on the next page](#)
- > ["Unlocking a Token by the Challenge-Response Method" on page 33](#)
- > ["Setting eToken Password Quality \(Password Quality Tab\)" on page 74](#)
- > ["Setting IDPrime PIN Properties \(Advanced Tab\)" on page 1](#)

Perform the following steps to log on to a token as an administrator:

1. Open **SafeNet Authentication Client Tools > Advanced View**.

See ["Opening the Advanced View" on page 1](#).

2. Do one of the following:

- In the left pane, select the node of the required token.  
In the right pane, click the **Log On as Administrator** icon.
- In the left pane, right-click the node of the required token, and select **Log On as Administrator**.

The **Administrator Logon** window is displayed.

3. Enter the token's Administrator Password, and click **OK**.

You are logged on as an administrator.

## Changing the Administrator Password

If you are logged on to a token as an administrator, you can change the token's Administrator Password.

Perform the following steps to change the administrator password:

1. Open **SafeNet Authentication Client Tools > Advanced View**.

2. Do one of the following:

- In the left pane, select the node of the required token.

In the right pane, click the **Change Administrator Password** icon.

- In the left pane, right-click the node of the required token, and select **Change Administrator Password**.

The **Change Administrator Password** window is displayed.

3. Enter the current Administrator Password in the **Current Administrator Password** field.

**NOTE** If an incorrect Administrator Password is entered more than a pre-defined number of times, the token becomes locked.

Ensure the password complies with the password quality settings: A secure password has at least 8 characters and at least three of the following rules: Uppercase letters; Lowercase letters; Numerals; Special Characters.

4. Enter the new password in the **New Administrator Password** and **Confirm Password** fields.
5. Click **OK**.

A message confirms that the password was changed successfully.

6. Click **OK**.

## Setting a Token Password by an Administrator

If you are logged on to a token as an administrator, you can unlock the token by setting a new token password.

**NOTE** The *Unlock Token* feature is for eToken devices only, whereas the *Set Token Password* features is for eToken and IDPrime devices. When setting the token password, updating the retry counter can be performed only on IDPrime devices.

Perform the following steps to unlock a token by setting a new token password:

1. Open **SafeNet Authentication Client Tools > Advanced View**.

See "[Opening the Advanced View](#)" on page 1.

2. Do one of the following:

- In the left pane, select the node of the required token.

In the right pane, click the **Set Token Password** icon.

- In the left pane, right-click the node of the required token, and select **Set Token Password**.

The **Administrator Logon** window is displayed.

3. Enter the Administrator Password, and click **OK**.

The **Set Token Password** window is displayed.

4. Enter a new token password in the **New Password** and **Confirm Password** fields.

**NOTE** The new token password must meet *Password Quality* settings defined for the token.

5. Set the **Logon retries before token is locked** field to the required number.
6. Click **OK**.  
A message confirms that the token password is changed successfully.
7. Click **OK**.  
The token is unlocked, and the user can now log on with the new token password.

# CHAPTER 5: Token Initialization

The token initialization process restores a token to its initial state.

## Overview

---

The token initialization process removes all objects stored on the token since manufacture, frees up memory, and resets the token password. Then the token is initialized with specific settings according to the organizational requirements or security modes.

Typically, initialization is carried out on a token when an employee leaves the company, enabling the token to be issued to another employee. It completely removes the employee's individual certificates and other personal data from the token, preparing it to be used by another employee.

The following data is initialized:

- > Token name
- > Token Password
- > IDPrime Cards - A new administrator password may be entered. If the current administrator password is to be maintained, select the option: 'Keep the current administrator password'.
- > Administrator Password (optional)
- > Maximum number of logon failures allowed
- > Requirement to change the token password on the first logon
- > Initialization key
- > All user-generated data, such as certificates and profiles

Using customizable parameters, you may be able to select specific parameters that are applied to certain tokens. These parameters may be necessary if you wish to use a token for specific applications or if you require a specific token password or Administrator Password on multiple tokens in the organization.

## Initializing eToken Devices

---

Depending on the type of token being initialized, certain settings are not enabled. To initialize an eToken 5110 CC device, see ["Initializing IDPrime Common Criteria Devices" on page 49](#).

Perform the following steps to initialize an eToken device:

1. Open **SafeNet Authentication Client Tools > Advanced View**.  
See ["Opening the Advanced View" on page 1](#).
2. Do one of the following:
  - In the left pane, select the node of the required token.

In the right pane, click the **Initialize Token** icon .

- In the left pane, right-click the node of the required token, and select **Initialize Token**.

The **Initialization Options** window is displayed, allowing you to select how to initialize the token.

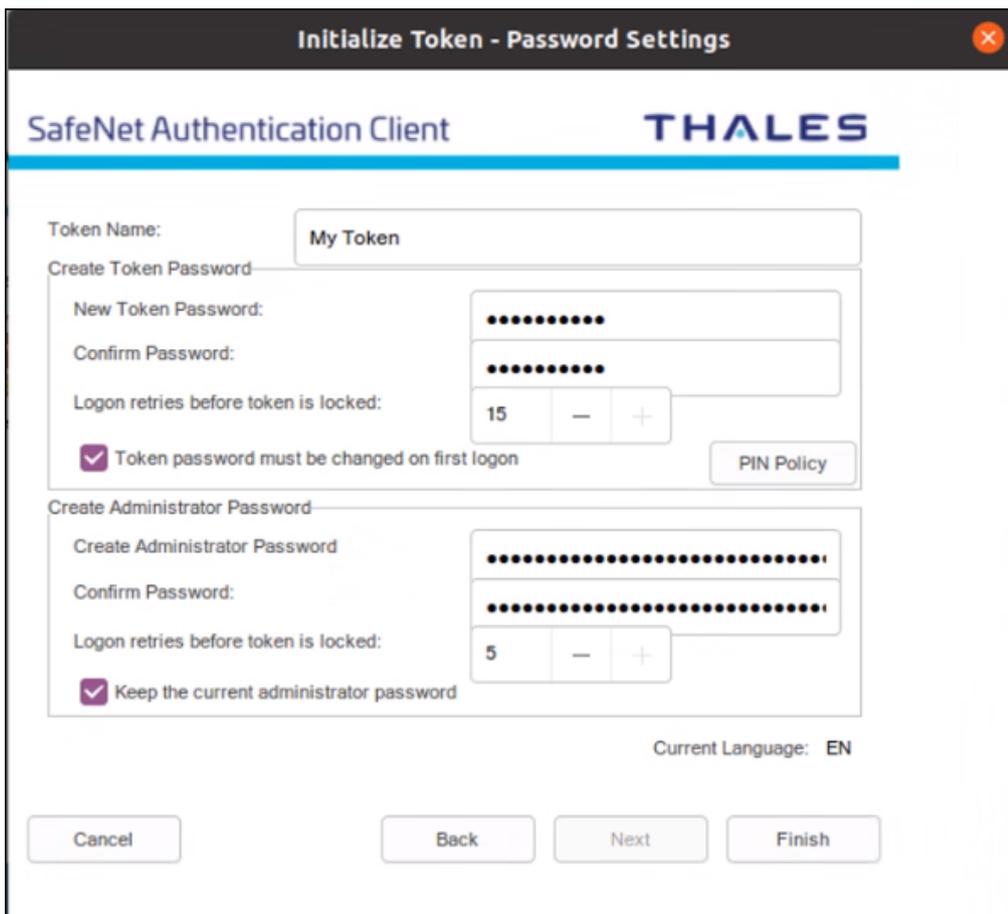
**NOTE** Initializing a token deletes all objects created on the device, while in use.

3. Select one of the following:

- **Preserve the token settings and policies** - Select to keep current token policies and settings.
- **Configure all initialization settings and policies** - Select to change some or all token policies and settings. This option allows to:
  - Create a token password
  - Create an administrator password
  - Enter the default token and administrator passwords
  - Enter Common Criteria passwords (PIN and PUK)

4. Click **Next**.

The **Password Settings** window is displayed.



**NOTE** The Pin Policy button is not visible if *Preserve the token settings and policies* option is selected in step 3.

5. Complete the fields as follows:

Field	Description
Token Name	<ul style="list-style-type: none"> <li>&gt; Enter a name for the token. If no name is entered, a default name is used. In many organizations, the default token name is "My Token".</li> <li>&gt; The token name does not affect the token contents. It is used solely to identify the token.</li> </ul>
New Token Password	Enter a new Token Password. The default password on an eToken device is 1234567890 automatically appears in this field.
Confirm Password	Re-enter the password entered above.
Logon retries before token is locked	Enter the number of times a token password can be entered incorrectly before the token is locked. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b> The retry counter counts only passwords that have a valid length. This field is enabled/disabled based on the card type.</p> </div>
Token password must be changed on first logon	If required, select <i>Token password must be changed on first logon</i> .
PIN Policy	Enables you to set PIN Quality/Property parameters. See <a href="#">"Setting IDPrime PIN Quality (PIN Quality Tab)" on page 78</a> and <a href="#">"Setting IDPrime PIN Properties (Advanced Tab)" on page 79</a> .
Create Administrator Password	Select <i>Create Administrator Password</i> and enter a New Administrator Password. The minimum password length on an eToken device is 8 characters. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b> Setting an Administrator Password enables certain functions to be performed on the token, such as setting a new token password to unlock a token.</p> </div>
Confirm Password	Re-enter the administrator password.
Logon retries before token is locked	<ul style="list-style-type: none"> <li>&gt; Enter a numeric value. This counter specifies the number of times the administrator can attempt to log on to the token with an incorrect password before the token is locked.</li> <li>&gt; The default setting for the maximum number of incorrect logon attempts is 15.</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p><b>NOTE</b> This field is enabled/disabled based on the card type.</p> </div>

Field	Description
Keep the current administrator password	<p>Select this if you want to keep the current administrator password.</p> <p><b>NOTE</b> If this option is selected, the following warning message appears: If the current password is the default password (48 0's), it is strongly recommended to update the administrator password to keep your token secure.</p>

6. Click **Next**.

The **Advanced Security Settings** window is displayed.

The screenshot shows the 'Advanced Security Settings' window in the SafeNet Authentication Client. The window has a title bar with 'SafeNet Authentication Client' on the left and the 'THALES' logo on the right. Below the title bar, there are two settings:

- Private data caching:** A dropdown menu with 'Always (fastest)' selected.
- Secondary Authentication Key:** A dropdown menu with 'Never' selected.

At the bottom of the window, there are four buttons: 'Cancel', '< Back', 'Next >', and 'Finish'.

7. Complete the following fields:

Field	Description
Private data caching	<p>Default: Always (fastest)</p> <p>To enhance performance, SafeNet Authentication Client caches public information stored on the token. This option defines when private information (excluding private keys on the token) can be cached outside the token.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>&gt; <b>Always (fastest):</b> Private information is always cached in the application memory. This enables fast performance, as certain information is cached on the host machine. However, this option is less secure than if no cache is allowed.</li> <li>&gt; <b>While user is logged on:</b> Private information is cached outside the token as long as the user is logged on to the token. Once the user logs out, all the private data in the cache is erased.</li> <li>&gt; <b>Never:</b> Private information is not cached.</li> </ul> <p>See <a href="#">"Setting Private Data Caching Mode (Advanced Tab)" on page 1</a></p>
Secondary Authentication Key	<p>Default: Never</p> <p>Set the number of reserved RSA keys to reserve space in the token memory. This ensures that there is always be memory available for keys.</p> <p>See <a href="#">"Setting Key Secondary Authentication" on page 1</a></p>

**8. Click Next.**

The **Initialization Key Settings** window is displayed.

The screenshot shows the 'SafeNet Authentication Client' window with the 'THALES' logo. It is divided into two main sections: 'Default Initialization Key' and 'Next Initialization Key'. In the 'Default Initialization Key' section, the 'Use Default Initialization Key' radio button is selected. In the 'Next Initialization Key' section, the 'Change the key for the next initialization to:' checkbox is unchecked. Under this checkbox, the 'Default' radio button is selected. There are also 'Random' and 'This value:' radio buttons, with the latter having an associated text input field. Below the 'This value:' field is a 'Confirm value:' field. At the bottom right, it says 'Current Language: EN'. At the bottom, there are three buttons: 'Cancel', '< Back', and 'Next > Finish'.

Use this window to configure Default and Next Initialization Settings.

Change the Initialization Key to protect against accidental token re-initialization in the future. If the Initialization Key is changed from the factory-set default value, the user is required to open the Initialization Key window and enter the correct key during future initialization of the token.

9. Complete the fields as follows:

Field	Description
Use default initialization key	Select this option if the Initialization Key was not changed from its default during the previous token initialization. The factory-set default is used as the key for the current token initialization.
Use this initialization key	Enter the Initialization Key configured in the <b>This Value</b> field during the previous token initialization.
Change the key for the next initialization to:	<p><b>Default:</b> Revert to the factory-set default so that the user is not required to enter an Initialization Key during subsequent token initializations.</p> <p><b>Random:</b> If selected, it will never be possible to re-initialize the token.</p> <p><b>This Value:</b> Select and confirm a unique key. During subsequent token initializations, the user must enter this key in the Use this Initialization Key field.</p>

**NOTE** The initialization key minimum length is 4.

10. Click **Finish**.

## Initializing IDPrime Devices

The initialization process removes all objects stored on the device since manufacture, freeing up memory, and resetting the token/card password.

The following can be performed during the initialization process:

- > All user-generated data, such as certificates and profiles
- > All PKCS#11 objects that were created on the token/card, while in use
- > Token/card name/label
- > Define a user and administrator password (the user password must be according to the card's policy settings).
- > Define password quality settings
- > Define a Digital Signature PIN and Digital Signature PUK password, the password must be according to the card's policy settings (for IDPrime CC and eToken 5110 CC devices). See ["Set Digital Signature PIN" on page 1](#).

**NOTE** The screens displayed during the initialization process are available in English localization only.

**NOTE** If Administrator Password is blocked (applies to all IDPrime devices) or if the Digital Signature PUK is blocked (applies only to IDPrime CC and eToken 5110 CC) then the IDPrime device cannot be initialized unless it comes with an initialization key.

This section explains how to initialize IDPrime based Common Criteria and Non Common Criteria devices.

### Initializing IDPrime Common Criteria Devices

Both eToken 5110 devices and IDPrime based cards that are Common Criteria certified can be initialized using SAC Tools.

Perform the following steps to initialize IDPrime based Common Criteria certified devices (eToken 5110 CC/IDPrime Common Criteria):

1. Open **SafeNet Authentication Client Tools > Advanced View**.
2. Do one of the following:
  - In the left pane, select the node of the required token/card.

In the right pane, click the **Initialize Token** icon .

- In the left pane, right-click the node of the required device, and select **Initialize Token**.

The **Initialization Options** window is displayed, allowing you to select how to initialize the device.

## 3. Select one of the following:

- **Preserve the token settings and policies** - Select to keep current token policies and settings.
- **Configure all initialization settings and policies** - Select this option to change some/all token policies and settings. This option allows to:
  - Create a token password
  - Create an administrator password
  - Enter the default token and administrator passwords
  - Enter Common Criteria passwords (PIN and PUK)

4. Click **Next**.

The **Administrator Logon** window is displayed. This window requires you to enter an **Administrator Password** and a **Digital Signature PUK** to begin the initialization process.

**NOTE** The procedures and screens described in this section are based on the fact that your IDPrime device is being used for the first time.

The above window is displayed if your token/card is in unlinked mode as it's received from the factory.

The above window is displayed if your token/card is in linked mode.

**5.** Do following as per the requirement:

Use factory default administrator password	<ul style="list-style-type: none"> <li>&gt; Select this check-box if the current administrator password is 48 0's. If selected, the <i>Administrator Password</i> field below is shaded showing the default password.</li> <li>&gt; Deselect it, if the current administrator password is different from the factory default.</li> </ul>
Administrator Password	Enter the current administrator password, that's different from the factory default.
Use factory default digital signature PUK	<ul style="list-style-type: none"> <li>&gt; Select this check-box if the current digital signature PUK is 6 zeros (000000). If selected, the <i>Digital Signature PUK</i> field below is shaded showing the default password.</li> <li>&gt; Deselect it, if the current Digital Signature PUK is different from the factory default.</li> </ul>
Digital Signature PUK	Enter the current Digital Signature PUK, that's different from the factory default.

**6.** Click **Next**.

The **Password Settings** window is displayed.

**NOTE** The Pin Policy button is not visible if *Preserve the token settings and policies* option is selected in step 3.

7. Enter the following:

Field	Description
Token Name	<ul style="list-style-type: none"> <li>&gt; Enter a name for the token. If no name is entered, a default name is used. In many organizations, the default token name is "My Token".</li> <li>&gt; The token name does not affect the token contents. It is used solely to identify the token.</li> </ul>

Field	Description
New Token Password	<p>The default password is 1234567890 automatically appears in this field.</p> <div style="border: 1px solid #ccc; padding: 5px;"> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>- If the device is initialized with the default token/card password, and standard password quality requirements are in effect, the user must select the <i>Token Password must be changed on first logon</i> option. Otherwise, the initialization fails because the default password does not meet the password quality requirements.</li> <li>If the <i>Token password must be changed on first logon</i> option is selected, the initialization succeed, and the user is prompted to create a new password when next logging on with the token/card.</li> <li>- The user is required to set a token password that meets the Password Quality requirements configured in the <i>Settings</i> window.</li> </ul> </div>
Confirm Password	<ul style="list-style-type: none"> <li>&gt; The default password (1234567890) automatically appears in this field.</li> <li>&gt; If the above field was changed, then re-enter the password entered in the <i>New Token Password</i> field.</li> </ul>
Logon retries before token is locked	<ul style="list-style-type: none"> <li>&gt; Enter the number of times a token password can be entered incorrectly before the token is locked.</li> <li>&gt; For Common Criteria devices that are in linked mode, the maximum value displayed is 3. When in unlinked mode, the value displayed is 15. This value cannot be changed for both linked and unlinked modes.</li> </ul> <div style="border: 1px solid #ccc; padding: 5px;"> <p><b>NOTE</b> This field is enabled/disabled based on the card type.</p> </div>
Token password must be changed on first logon	<p>If required, select <i>Token password must be changed on first logon</i>.</p> <div style="border: 1px solid #ccc; padding: 5px;"> <p><b>NOTE</b> When initializing a device in Unlinked mode, and this option is selected, both the Token (User) Password and Digital Signature PIN are effected (ensure that both the Token Password and Digital Signature PIN are changed).</p> </div>
PIN Policy	<p>Enables you to set PIN Quality/Property parameters.</p> <p>See "<a href="#">Setting IDPrime PIN Quality (PIN Quality Tab)</a>" on page 1 and "<a href="#">Setting IDPrime PIN Properties (Advanced Tab)</a>" on page 1.</p>
Create Administrator Password	<ul style="list-style-type: none"> <li>&gt; If necessary, enter a new administrator password, that's different from the current administrator password. Your current password may be the default password or a different password. Only you know this password.</li> <li>&gt; You can change the default Administrator Password to a password that is between 8-32 alphanumeric characters. See "<a href="#">Introduction</a>" on page 9.</li> </ul>
Confirm Password	<p>Re-enter the administrator password.</p>

Field	Description
Keep the current administrator password	<p>Select this if you want to keep the current administrator password.</p> <p><b>NOTE</b> If this option is selected, the following warning message appears:  <i>If the current password is the default password (48 0's), it is strongly recommended to update the administrator password to keep your token secure.</i></p>

8. Click **Next**.

The **IDPrime Common Criteria Settings** window is displayed. It allows you to define Common Criteria passwords, which are made up of a Digital Signature PIN (User Password) and Digital Signature PUK (Administrator Password).

**NOTE** Due to Security concerns related to IDPrime MD 840 cards in Linked Mode, the support for Linked Mode in the Initialization window is disabled by default. To enable Linked Mode, refer to *SafeNet Authentication Client Administrator Guide* (LinkMode property). It is recommended to use the Linked Mode feature only with the IDPrime 940 card.

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. 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

9. Enter the following:

Field	Description
New Digital Signature PIN	Enter a <i>New Digital Signature PIN</i> . This option allows you to work in 'unlinked' mode.
Confirm PIN	Re-enter the <i>New Digital Signature PIN</i> .
PIN Policy	Enables you to set PIN Quality/Property parameters. See " <a href="#">Setting IDPrime PIN Quality (PIN Quality Tab)</a> " on page 1 and " <a href="#">Setting IDPrime PIN Properties (Advanced Tab)</a> " on page 1.
New Digital Signature PUK	Enter a <i>New Digital Signature PUK</i> . This option allows you to work in <i>Unlinked</i> mode.
Confirm PUK	Re-enter the <i>New Digital Signature PUK</i> .
PIN Policy	Enables you to set PIN Quality/Property parameters. See " <a href="#">Setting IDPrime PIN Quality (PIN Quality Tab)</a> " on page 1 and " <a href="#">Setting IDPrime PIN Properties (Advanced Tab)</a> " on page 1.

**10. Click Finish.**

A warning message is displayed.

**11. Click OK** when the following warning message appears:

*The token initialization process will delete all token content and reset all token parameters.*

The **Token initialized successfully** message is displayed.

## Initializing IDPrime Based Devices (Non Common Criteria/FIPS Devices)

IDPrime cards that are not Common Criteria certified can be initialized using SAC Tools and the IDPrime cards that are FIPS certified can be configured during factory settings with either one of the following profiles:

- > **Managed** - managed devices have an Administrator PIN and they have to be initialized according to the initialization sections above.
- > **Non-Managed** - non-managed devices have an Administrator PIN that is locked and cannot be used in Managed environments by CMS's. Non-managed devices may have an additional initialization key (for example: SafeNet IDPrime 930/3930 devices), which allows initializing the device without using the Administrator PIN.

A non-managed device is displayed in SAC Tools with the Administrator functions disabled

Perform the following steps to initialize an IDPrime based non common criteria/FIPS device:

**1. Open SafeNet Authentication Client Tools > Advanced View.**

**2. Do one of the following:**

- In the left pane, select the node of the required token/card

In the right pane, click the **Initialize Token** icon 

- In the left pane, right-click the node of the required device, and select **Initialize Token**.

The **Initialization Options** window is displayed, allowing you to select how to initialize the device.

3. Select the relevant option:

- **Preserve the token settings and policies** - Select to keep current token policies and settings.
- **Configure all initialization settings and policies** - Select this option to change some/all token policies and settings. This option allows to:
  - Create a token password
  - Create an administrator password
  - Enter the default token and administrator passwords
  - Enter Common Criteria passwords (PIN and PUK)

4. Click **Next**.

The **Administrator Logon** window is displayed. This window requires you to enter an Administrator Password to begin the initialization process.

**NOTE** This window is not displayed for Non-Managed cards.

5. Do one of the following:

- **Use factory default administrator password**
  - Select this check-box if the current administrator password is 48 0's. If selected, the Administrator Password field is shaded showing the default password.
  - Deselect it if the current administrator password is different from the factory default.
- **Administrator Password** - Enter the current administrator password, that's different from the factory default.

**NOTE** Current administrator password is different from the factory default. The default Administrator Password is 48 zeros.

6. Click **Next**.

The **Password Settings** window is displayed.

**NOTE** For Non-Managed cards, the *Pin Policy* button and the *Create Administrator Password* option are not visible if *Preserve the token settings and policies* option is selected in step 3. While for Managed cards, only the *Pin Policy* button is not visible.

7. Enter the following:

Field	Description
Token Name	<ul style="list-style-type: none"> <li>&gt; Enter a name for the token. If no name is entered, a default name is used. In many organizations, the default token name is <i>My Token</i>.</li> <li>&gt; The token name does not affect the token contents. It is used solely to identify the token.</li> </ul>

Field	Description
New Token Password	<p>The default password is 1234567890 automatically appears in this field.</p> <div style="border: 1px solid black; padding: 5px;"> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>- If the device is initialized with the default token/card password, and standard password quality requirements are in effect, the user must select <i>Token Password must be changed on first logon</i> option.</li> <li>Otherwise, the initialization fails because the default password does not meet the password quality requirements.</li> <li>- If the <i>Token password must be changed on first logon</i> option is selected, the initialization succeed and the user is prompted to create a new password when next logging on with the token/card.</li> <li>- The user is required to set a token password that meets the PIN Quality requirements.</li> </ul> </div>
Confirm Password	<ul style="list-style-type: none"> <li>&gt; The default password (1234567890) automatically appears in this field.</li> <li>&gt; If the above field was changed, then re-enter the password entered in the <i>New Token Password</i> field.</li> </ul>
Logon retries before token is locked	<p>Enter the number of times a token password can be entered incorrectly before the token is locked.</p> <div style="border: 1px solid black; padding: 5px;"> <p><b>NOTE</b> This field is enabled/disabled based on the card type.</p> </div>
Token password must be changed on first logon	<p>If required, select <i>Token password must be changed on first logon</i>.</p>
PIN Policy	<p>Enables you to set PIN Quality/Property parameters.</p> <p>See <a href="#">"Setting IDPrime PIN Quality (PIN Quality Tab)" on page 1</a> and <a href="#">"Setting IDPrime PIN Properties (Advanced Tab)" on page 1</a>.</p>
Create Administrator Password	<ul style="list-style-type: none"> <li>&gt; If necessary, enter a new administrator password, that's different from the current administrator password. Your current password may be the default password or a different password. Only you know this password.</li> <li>&gt; You can change the default Administrator Password to a password that is between 8-32 alphanumeric characters (or to 48 hexadecimal digits). See <a href="#">"Introduction" on page 9</a>.</li> </ul>
Confirm Password	<p>Re-enter the administrator password.</p>
Logon retries before token is locked	<ul style="list-style-type: none"> <li>&gt; The number of times an administrator password can be entered incorrectly before the token is locked. This parameter appears for non IDPrime Common Criteria devices.</li> <li>&gt; This field may be read-only depending on your device type and the card configuration.</li> </ul>

Field	Description
Keep the current administrator password	<p>Select this if you want to keep the current administrator password.</p> <p><b>NOTE</b> If this option is selected, the following warning message appears: If the current password is the default password (48 0's), it is strongly recommended to update the administrator password to keep your token secure.</p>

8. Click **Finish**.

A warning message is displayed.

9. Click **OK** when the following warning message appears:

*The token initialization process will delete all token content and reset all token parameters.*

The **Token initialized successfully** message is displayed.

## Friendly Admin Password

The *Friendly Admin Password* feature permits the use of a short password instead of an admin key made up of 24 binary bytes or 48 Hexadecimal digits.

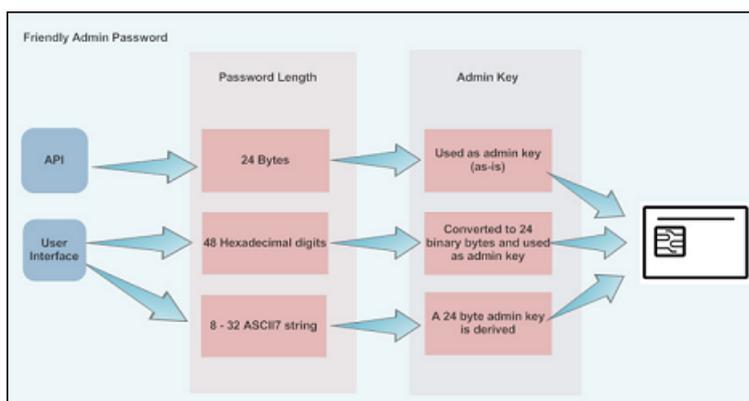
- > The Friendly Admin Password (known as Friendly Admin) works with all IDPrime devices.
- > The Friendly Admin uses a user secret in the range of 8 to 32 ASCII7 characters.

**NOTE** The user secret that is made up of 8-23 or 25-32 ASCII7 characters derives a 24 byte long Admin Key. The user secret that is made up of 24 ASCII7 characters is used without derivation.

### For IDPrime CC devices (840/3840/eToken 5110 CC):

When working in linked mode (see "[Working with Common Criteria Certified Tokens and Cards](#)" on page 60) the Digital Signature PUK is derived from the Admin Key. This is not part of the Friendly Admin feature, but can be used together.

The password sizes: 24 bytes and 48 hexadecimal digits are maintained for backward compatibility with SAC and SafeNet Minidriver.



# CHAPTER 6: Common Criteria

SafeNet Authentication Client supports Thales IDPrime Common Criteria (CC) cards range as well as eToken 5110 CC.

For a detailed list of supported cards, see the *SafeNet Authentication Client Release Notes*.

## Working with Common Criteria Certified Tokens and Cards

IDPrime and eToken devices that are Common Criteria certified are used mainly for digital signing purposes. When working with common criteria certified tokens and cards, 2 additional passwords (Specific to qualified digital signature operations) are required.

## PKCS#11 Digital Signature PIN Authentication

For Common Criteria signature compliance, the Digital Signature PIN must be authenticated before each signing operation. Thus, the PKCS#11 library may prompt the user to enter the Digital Signature PIN.

Logging onto the device is required when a Common Criteria RSA private key operation is performed for the first time using the PKCS#11 library (for example signing operations). With the support of Common Criteria PKCS#11 Multi-Slots, all qualified signature functionalities are available via the Common Criteria virtual slot labeled Digital Signature PIN, which are associated with PIN Role #3. Thus, in order to use Common Criteria keys, the user must ensure that this Common Criteria slot is selected and used by the application.

The application must then call C\_Login on the virtual slot as a CKU\_USER to provide the qualified Digital Signature PIN (PIN role #3).

The device remains in login state unless it was configured otherwise. In this case the user is prompted to enter the Digital Signature PIN when needed.

If the Digital Signature PIN authentication fails, an error message is displayed.

For setting Multi-Slot values, see the *SafeNet Authentication Client Administrator Guide*.

## Must Change Password

When using a PIN Pad with a card configured with Must Change Password (for User PIN and/or Digital Signature PIN), during the first login the password is changed with the keyboard. Subsequently, the PIN Pad must be used to change the password.

**NOTE** Refer to your PIN Pad reader documentation to verify whether the reader permits PIN change with the keyboard.

## Common Criteria Extended Functions

The following Digital Signing function icons are displayed in *SAC Tools > Advanced View*:

User Function	Icon	Right-Click Menu Item
Change Digital Signature PIN		Change Digital Signature PIN
Change Digital Signature PUK		Change Digital Signature PUK
Set Digital Signature PIN		Set Digital Signature PIN

### Change Digital Signature PIN

Use this option to change the Digital Signature PIN.

Perform the following steps:

1. Open **SafeNet Authentication Client Tools > Advanced View**.
2. Do one of the following:
  - In the left pane, select the node of the required token.

In the right pane, click the **Change Digital Signature PIN** icon .

- In the left pane, right-click the node of the required token, and select **Change Digital Signature PIN**.

The **Change Digital Signature PIN** window is displayed.

3. Enter the **Current Digital Signature PIN**.
4. Enter the **New Digital Signature PIN**.
5. Confirm the **New Digital Signature PIN**, and click **OK**.  
The **Password Changed Successfully** window is displayed.
6. Click **OK**.

## Change Digital Signature PUK

Use this option to change the Digital Signature PUK.

Perform the following steps:

1. Open **SafeNet Authentication Client Tools > Advanced View**.
2. Do one of the following:
  - In the left pane, select the node of the required token.  
  
In the right pane, click the **Change Digital Signature PUK** icon .
  - In the left pane, right-click the node of the required token, and select **Change Digital Signature PUK**.  
The **Change Digital Signature PUK** window is displayed.

3. Enter the **Current Digital Signature PUK**.
4. Enter the **New Digital Signature PUK**.
5. Confirm the **New Digital Signature PUK**, and click **OK**.  
The **Password Changed Successfully** window is displayed.
6. Click **OK**.

## Set Digital Signature PIN

Use this option to change the Digital Signature PIN using the Digital Signature PUK.

Perform the following steps:

1. Open **SafeNet Authentication Client Tools > Advanced View**.
2. Do one of the following:
  - In the left pane, select the node of the required token.
  - In the right pane, click the **Change Digital Signature PIN** icon .
  - In the left pane, right-click the node of the required token, and select **Set Digital Signature PIN**.

The **Digital Signature PUK Logon** window is displayed.

3. Enter the **Digital Signature PUK** and click **OK**.

The **Set PIN** window is displayed.

4. Enter a **New Digital Signature PIN**.
5. Confirm the **New Digital Signature PIN**, and click **OK**.  
The **Password Changed Successfully** window is displayed.
6. Click **OK**.

## Operational Differences and Role Protection

Below displays the differences between eToken 5100 CC (legacy) and other tokens regarding the roles that protect the specific operation.

<b>Operation</b>	<b>Password required to perform the specified operation on:</b> > <b>eToken 5100 CC (legacy)</b>	<b>Password required to perform the specified operation on:</b> > <b>SafeNet IDPrime 940/3940</b> > <b>IDPrime 840/840B/3840/3840B</b> > <b>eToken 5110 CC</b>
Initialize	Initialization Key	Administrator Password
Generate sign only key pair	Token Password	Token Password + Digital Signature PIN
Generate exchange key pair	Token Password	Token Password
Import sign only key pair	Import Password	Token Password + Digital Signature PIN
Import exchange key pair	Token Password	Token Password
Delete sign only key pair	Token Password	Token Password
Delete exchange key pair	Token Password	Token Password
Sign with sign only key pair	Token Password	Digital Signature PIN
Sign with exchange only key pair	Token Password	Token Password
Decrypt	Token Password	Token Password
Unlock	Token Password is unlocked by the Digital Signature PUK	> Token Password is unlocked by the Administrator Password > Digital Signature PIN is unlocked by the Digital Signature PUK

# CHAPTER 7: SafeNet eToken 5300

SafeNet eToken 5300 is an ideal solution for enterprises looking to deploy the military-grade security of PKI, while maintaining a convenient solution for employees. The eToken 5300 is a compact, tamper-evident USB with presence detection, which creates a third factor of authentication. Something you have (physical token), something you know (PIN), something you do (enabling touch sensor).

The eToken 5300 offers multi-application dynamic smart card functionality. It can be used with any USB connection for Identity and Access Management applications such as network authentication, digital signatures, email encryption and other advanced services based on Public Key Infrastructure (PKI). The eToken 5300 is certified FIPS 140-2 L3 at the full token boundary.

With the Presence Detection feature, enterprise IT can allow single sign on for employees by requiring a user PIN only at logon. That way, employees can use the advance functionality of PKI, such as digitally signing documents and encrypting email by simply touching the sensor on the token, which provides authentication without entering a PIN multiple times. If enterprise IT want more control of specific certificates they can set rules to either always require the user to enter a password or always require both user password and sensor activation when accessing those particular certificates.

## eToken 5300 Certificates

The eToken 5300 device can have either one or both of the following certificates on the token:

- > **Signature Certificate** - Used to perform digital signature operations only.
- > **Exchange Certificate** - Used to perform various cryptographic operations such as digital signature, encryption of data or authentication.

In addition to the PIN protection available on the token, each or both types of certificates can also be protected using the touch sense on the eToken 5300 device.

The eToken 5300 is available in the following configurations:

- > Signature Certificates that are touch sense protected (default)
- > Exchange Certificates that are touch sense protected.
- > Both Signature and Exchange Certificates that are touch sense protected.

### NOTE

- The eToken 5300 configuration is defined at the factory and cannot be changed.
- When using the eToken 5300 configured with touch sense support for Signature keys, signature operations with an Exchange certificate will not be touch sense protected.

## Viewing eToken 5300 Information

Perform the following steps to view eToken 5300 touch sense configurations in SAC Tools:

1. Do one of the following:
  - Right-click the **SafeNet Authentication Client tray** icon, and select **Tools**.
  - On Linux, select **Applications > SafeNet > SafeNet Authentication Client > SafeNet Authentication Client Tools**.

The **SafeNet Authentication Client Tools** window is displayed in the *Simple View*.

2. Click the **Advanced View** icon.

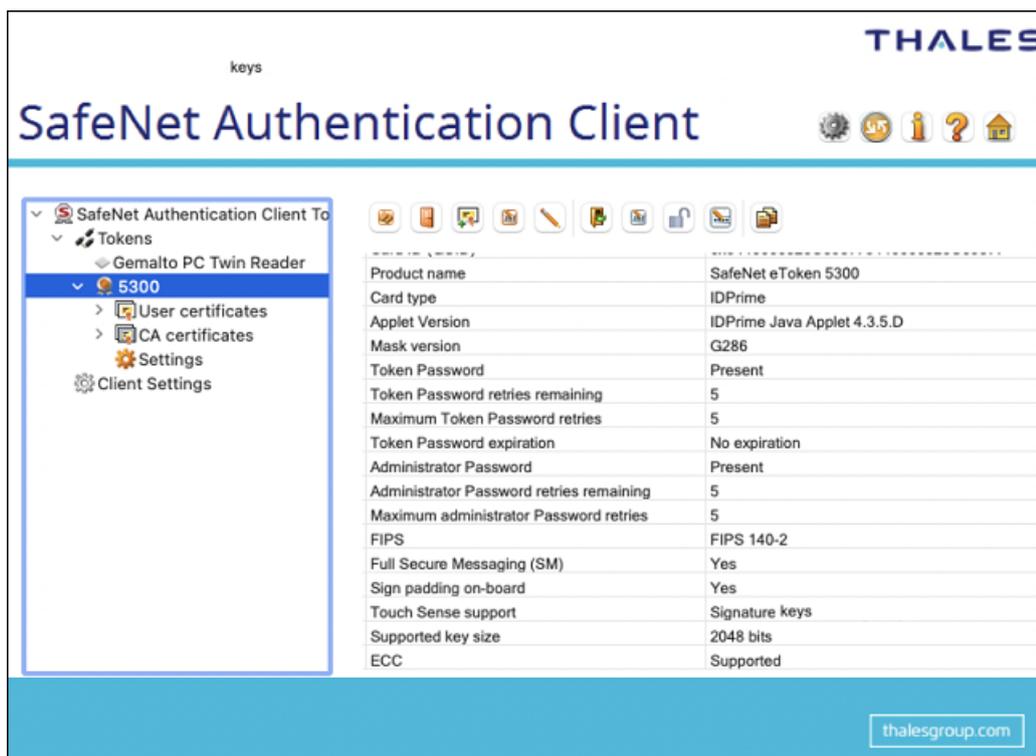
The **SafeNet Authentication Client Tools** window is displayed in the *Advanced View*.

3. In the left pane, select the **eToken 5300** node.

The Token's Information is displayed.

**NOTE** Configuration information displayed in SAC Tools varies according to how the token was received from the factory.

### Touch Sense support - Signature Keys



The screenshot shows the 'SafeNet Authentication Client Tools' window. The left pane is expanded to show the '5300' token node. The main area displays the following configuration table:

Product name	SafeNet eToken 5300
Card type	IDPrime
Applet Version	IDPrime Java Applet 4.3.5.D
Mask version	G286
Token Password	Present
Token Password retries remaining	5
Maximum Token Password retries	5
Token Password expiration	No expiration
Administrator Password	Present
Administrator Password retries remaining	5
Maximum administrator Password retries	5
FIPS	FIPS 140-2
Full Secure Messaging (SM)	Yes
Sign padding on-board	Yes
Touch Sense support	Signature keys
Supported key size	2048 bits
ECC	Supported

The bottom right corner of the window contains the URL [thalesgroup.com](http://thalesgroup.com).

### Touch Sense support - Signature and Exchange Keys

**THALES**

## SafeNet Authentication Client

SafeNet Authentication Client To

- Tokens
  - Gemalto PC Twin Reader
    - 5300**
      - User certificates
      - CA certificates
      - Settings
      - Client Settings

Product name	SafeNet eToken 5300
Card type	IDPrime
Applet Version	IDPrime Java Applet 4.3.5.D
Mask version	G286
Token Password	Present
Token Password retries remaining	5
Maximum Token Password retries	5
Token Password expiration	No expiration
Administrator Password	Present
Administrator Password retries remaining	5
Maximum administrator Password retries	5
FIPS	FIPS 140-2
Full Secure Messaging (SM)	Yes
Sign padding on-board	Yes
Touch Sense support	Signature and Exchange keys
Supported key size	2048 bits
ECC	Supported

thalesgroup.com

### Touch Sense support - Exchange Keys

**THALES**

## SafeNet Authentication Client

SafeNet Authentication Client To

- Tokens
  - Gemalto PC Twin Reader
    - 5300**
      - User certificates
      - CA certificates
      - Settings
      - Client Settings

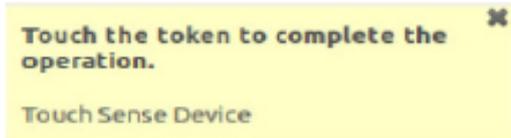
Product name	SafeNet eToken 5300
Card type	IDPrime
Applet Version	IDPrime Java Applet 4.3.5.D
Mask version	G286
Token Password	Present
Token Password retries remaining	5
Maximum Token Password retries	5
Token Password expiration	No expiration
Administrator Password	Present
Administrator Password retries remaining	5
Maximum administrator Password retries	5
FIPS	FIPS 140-2
Full Secure Messaging (SM)	Yes
Sign padding on-board	Yes
Touch Sense support	Exchange keys
Supported key size	2048 bits
ECC	Supported

thalesgroup.com

## Using the eToken 5300 Touch Sense

---

When performing a Digital Signature operation using the eToken 5300 device, the user is prompted to touch the sensor on the token to complete the signing operation.



## eToken 5300 Touch Sense Timeout and Grace period

---

### Touch Sense Timeout

The eToken 5300 touch sense device has a default timeout of 30 seconds. If the cryptographic operation requires the device to be touched and the user does not touch the sensor within the 30 second time frame, the operation fails.

### Touch Sense Grace Period

The eToken 5300 has a 30 second grace period.

After the sensor is touched for the first cryptographic operation (that is within the 30 second time frame mentioned above), all other sequential cryptographic operations performed within the grace period time, will not require the touch sensor.

# CHAPTER 8: Client Settings

Client Settings are parameters that are saved to the computer and apply to all tokens that are initialized on the computer after the settings have been configured. Use token settings to determine behavior that applies to a specific token. See ["Token Settings" on page 74](#).

## Setting Password Quality (eToken Devices only)

The *Password Quality* feature enables the administrator to set certain complexity and usage requirements for token passwords.

To set PIN Quality parameters for IDPrime cards. See ["Setting IDPrime PIN Quality \(PIN Quality Tab\)" on page 78](#).

**NOTE** The token password is an important security measure in safeguarding your company's private information. The best passwords are at least eight characters long, and include upper-case and lower-case letters, punctuation marks, and numerals appearing in a random order.

Perform the following steps to set the Password Quality:

1. Open **SafeNet Authentication Client Tools > Advanced View**.

See ["Opening the Advanced View" on page 1](#).

2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Password Quality** tab.

The **Password Quality** tab is displayed.

4. Do one of the following:
  - Change the **Password Quality** settings, and click **Save**.

**NOTE** The *Password Quality* settings are configured the same way as the *Token Password* quality settings. See ["Setting eToken Password Quality \(Password Quality Tab\)" on page 74](#).

- To ignore your changes, click **Discard**.
- To apply SafeNet Authentication Client's default settings, click **Set to Default**.

**NOTE** When entering a value in the *Expiry warning period* field, you must make sure that a value is also entered in the *Maximum usage period* field. If no value is entered in the *Maximum usage period* field, an error message appears.

---

## Allowing Password Quality Configuration on Token after Initialization (eToken Devices only)

---

This *Allow password quality configuration on token after initialization* option determines whether the password quality parameters on the token can be changed after initialization.

Perform the following steps to enable password quality configuration after initialization:

1. Open **SafeNet Authentication Client Tools > Advanced View**.  
See "[Opening the Advanced View](#)" on page 1.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab.
4. Select **Allow password quality configuration on token after initialization**.
5. Do one of the following:
  - To save your changes, click **Save**.
  - To ignore your changes, click **Discard**.

---

## Allowing Only an Administrator to Configure Password Quality on Token

---

The *Allow only an administrator to configure password quality on token* option determines whether the password quality parameters on the token can be changed after initialization by the administrator only, and not by the user. This option is selected by default.

Perform the following steps to define who can configure password quality on a token:

1. Open **SafeNet Authentication Client Tools > Advanced View**.  
See "[Opening the Advanced View](#)" on page 1.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab.
4. Do one of the following:
  - To enable configuration by the administrator only, select **Allow only an administrator to configure password quality on token**.
  - To enable configuration by the user also, clear **Allow only an administrator to configure password quality on token**.
5. Do one of the following:
  - To save your changes, click **Save**.
  - To ignore your changes, click **Discard**.

## Showing the SafeNet Authentication Client Tray Icon

You can determine whether the SafeNet Authentication Client tray icon is displayed.

Perform the following steps to show the SafeNet Authentication Client tray icon:

**1. Open **SafeNet Authentication Client Tools** > **Advanced View**.**

See "[Opening the Advanced View](#)" on page 1.

**2. In the left pane, select **Client Settings**.**

**3. In the right pane, select the **Advanced** tab.**

**4. In the Show application tray icon drop-down list, select one of the following:**

- **Never:** The tray icon is never displayed
- **Always:** The tray icon is always displayed

**5. Do one of the following:**

- To save your changes, click **Save**.
- To ignore your changes, click **Discard**.

## Enabling Logging

The logging function generates logs for SafeNet Authentication Client activities.

### NOTE

- You must have administrator privileges to use the logging function.
- On Linux operating systems, the Enable Logging feature is activated only if the `eToken.conf` file is configured with privileges.

For Linux - The log files are located in: `/tmp/eToken.log`

### To activate the logging function manually on a Linux System

Perform the following steps:

**1. Edit the following file: `/etc/eToken.common.conf`.**

**2. Add the following:**

```
[LOG]
```

```
Enabled=1
```

### To disable the logging feature manually on a Linux System

Perform the following steps:

**1. Edit the following file: `/etc/eToken.common.conf`.**

**2. Add the following:**

```
[LOG]
```

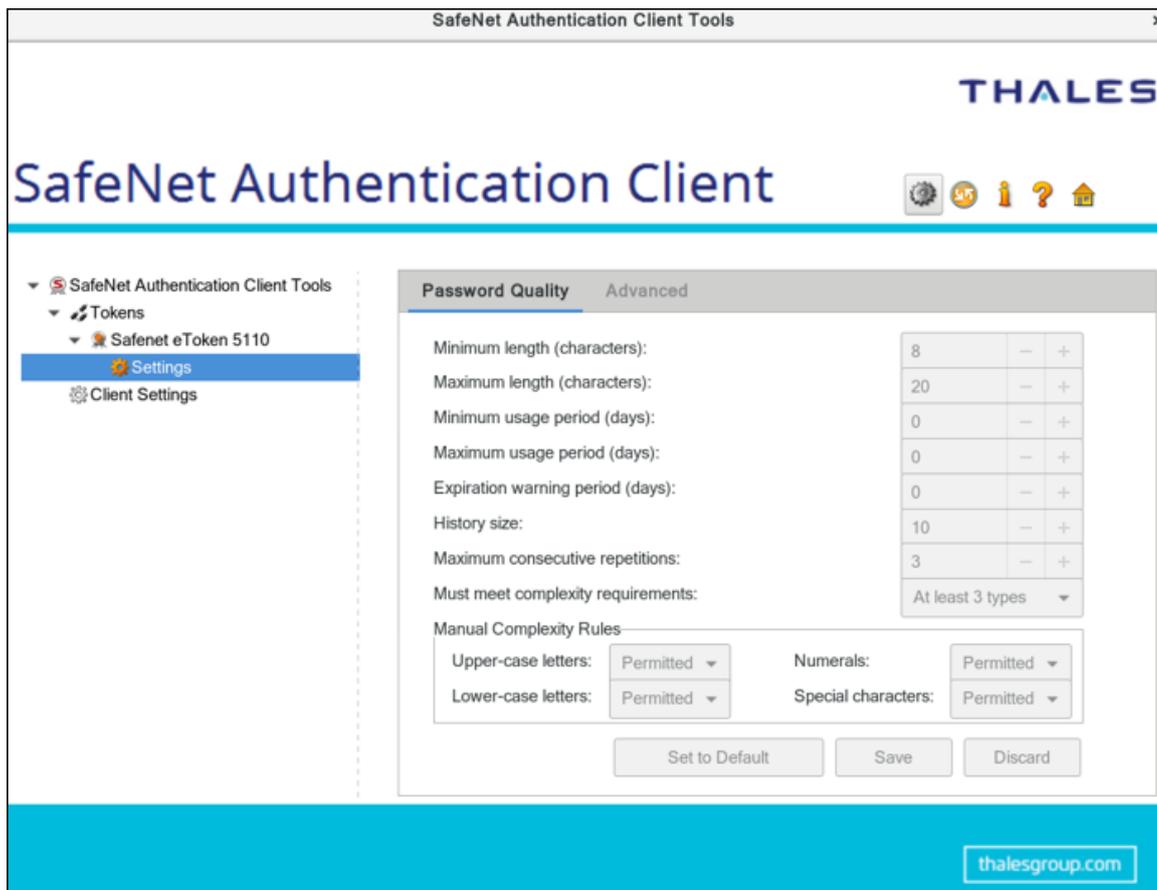
Enabled=0

# CHAPTER 9: Token Settings

Configurations set in the selected token's *Settings* tab determine behavior that applies to the specific token. For configurations set in *Client Settings*, that apply the settings to all tokens that are initialized after the settings have been configured, see "[Client Settings](#)" on page 1.

## Setting eToken Password Quality (Password Quality Tab)

The *Password Quality* tab enables you to set the device's password policies.



Perform following steps to set password quality for a token:

1. Open **SafeNet Authentication Client Tools** > **Advanced View**.  
See "[Opening the Advanced View](#)" on page 1.
2. In the left pane, expand the node of the required token, and select **Settings**.
3. In the right pane, select the **Password Quality** tab.

The **Password Quality** tab is displayed.

4. Enter the password quality parameters as follows:

Password Quality Parameter	Description
Minimum length (characters)	Default: 6 characters
Maximum length (characters)	Default: 16 characters
Maximum usage period (days)	Default: 0 (none) The maximum period, in days, before which the password must be changed.
Minimum usage period (days)	Default: 0 (none) The minimum period before the password can be changed.
Expiration warning period (days)	Default: 0 (none) Defines the number of days before the password expires that a warning message is shown.
History size	Default: 0 > For eToken devices - 10 Defines how many previous passwords must not be repeated.
Maximum consecutive repetitions	Default: 3 The maximum number of repeated characters that is permitted in the password.
Must meet complexity requirements	Determines the complexity requirements that are required in the token password. > <b>At least 2 types:</b> a minimum of 2 complexity rules (out of the 4 shown in the Manual Complexity fields) are enforced. > <b>At least 3 types:</b> a minimum of 3 complexity rules (out of the 4 shown in the Manual Complexity fields) are enforced (Default). > <b>None:</b> Complexity requirements are not enforced. > <b>Manual:</b> Complexity requirements, as set manually in the Manual Complexity settings, are enforced.
Manual complexity rules	For each of the character types (Numerals, Upper-case letters, Lower-case letters, and Special characters) select one of the following options: > <b>Permitted</b> - Can be included in the password, but is not mandatory (Default). > <b>Mandatory</b> - Must be included in the password. > <b>Forbidden</b> - Must not be included in the password.

5. Do one of the following:

- To save your changes, click **Save**.
- To ignore your changes, click **Discard**.

- To apply SafeNet Authentication Client's default settings, click **Set to Default**.

## Setting Private Data Caching Mode (Advanced Tab)

This setting defines when private information (excluding private keys on the eToken PRO/NG OTP/smart card) can be cached outside the token.

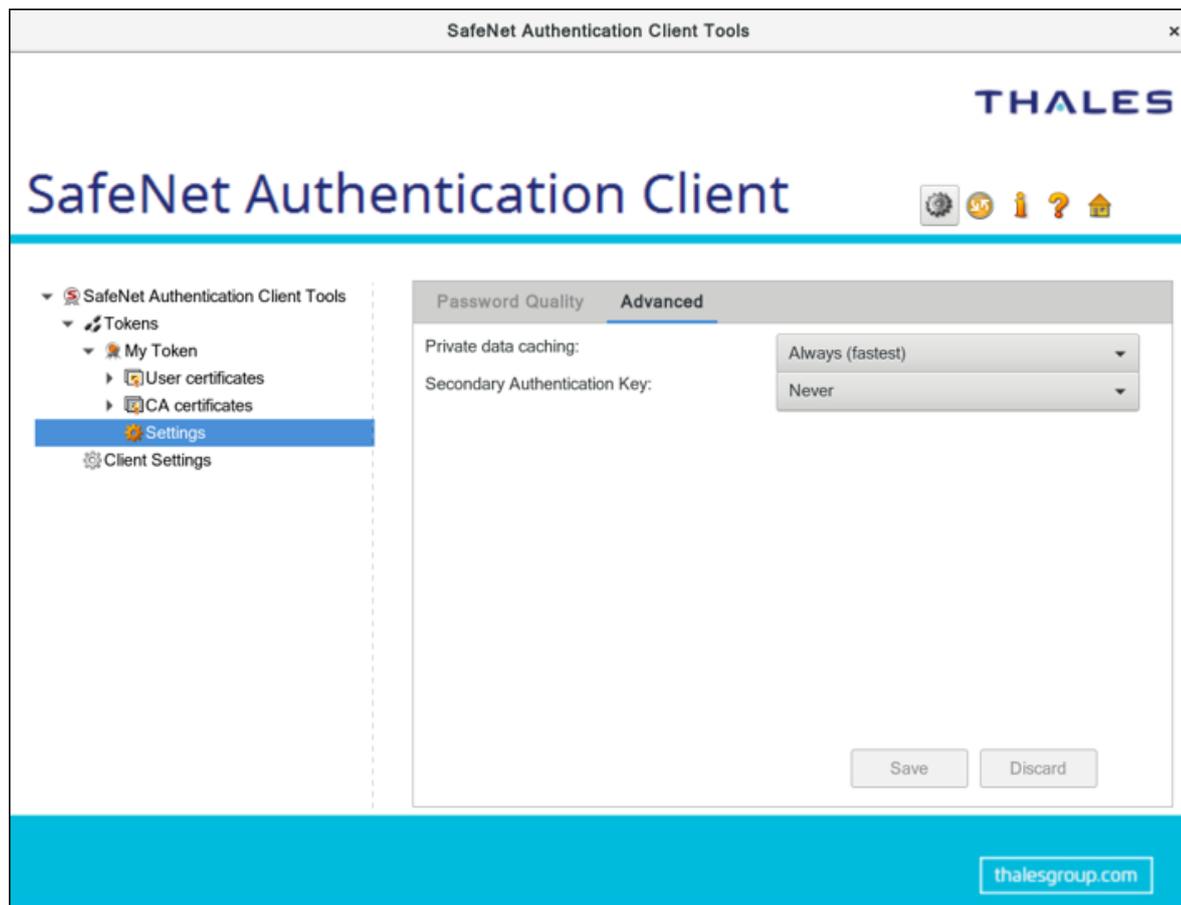
**NOTE** This feature is supported on eToken devices only.

In SafeNet Authentication Client, public information stored on the token is cached to enhance performance.

Perform the following steps to set private data caching mode:

1. Open **SafeNet Authentication Client Tools > Advanced View**.  
See "[Opening the Advanced View](#)" on page 1.
2. In the left pane, expand the node of the required token, and select **Settings**.
3. In the right pane, select the **Advanced** tab.

The **Advanced** tab is displayed.



4. In the **Private data caching** field, select one of the following options:

Option	Description
Always (fastest)	Always caches private information in the application memory. This enables fast performance, as certain information is cached on the host machine. However, this option is less secure than if no cache is allowed.
While user is logged on	Caches private data outside the token as long as the user is logged on to the token. Once the user logs off, all the private data in the cache is erased.
Never	Does not cache private data.

5. Do one of the following:

- To save your changes, click **Save**.
- To ignore your changes, click **Discard**.

## Setting Key Secondary Authentication (Advanced Tab)

An authentication password may be set for an RSA key. In addition to having the token and knowing its token password, accessing the RSA key may require knowing the password for that particular key.

This setting defines the policy for using the secondary authentication of RSA keys.

**NOTE** This feature is supported on eToken devices only.

Perform the following steps to set RSA key secondary authentication:

1. Open **SafeNet Authentication Client Tools > Advanced View**. See "Opening the Advanced View" on page 12.
2. In the left pane, expand the node of the required token, and select **Settings**.
3. In the right pane, select the **Advanced** tab.
4. In the **Key Secondary Authentication** field, select one of the following:
  - Always
  - Always prompt user
  - Prompt user on application request
  - Never
  - Token authentication on application request

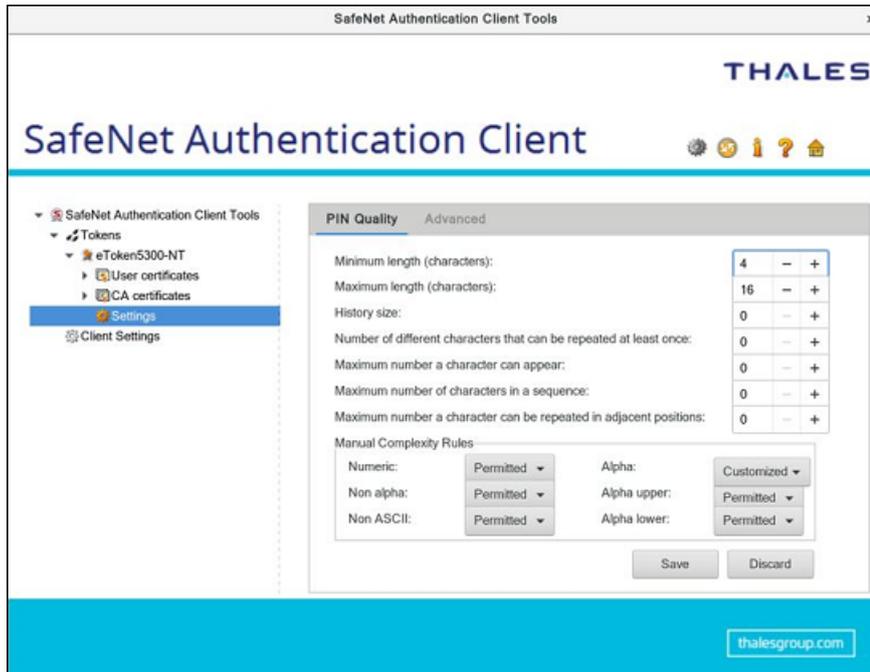
**NOTE** For an explanation of these options, see "[Initializing IDPrime Devices](#)" on page 49.

5. Do one of the following:

- To save your changes, click **Save**.
- To ignore your changes, click **Discard**.

## Setting IDPrime PIN Quality (PIN Quality Tab)

The *PIN Quality* tab provides parameters which define the rules that must be respected in order for the PIN to be accepted.



### NOTE

- In the MD Manager, the unlimited value is equal to FFh
- In SAC Tools, the unlimited value is equal to 00h

For IDPrime cards, the following *PIN Quality* parameters exist:

PIN Quality Parameter	Description
Minimum length (characters)	The minimum value that can be set for the length of a PIN's value. This value must be in the range 04h - 40h for a local PIN and 04h - 10h for the global PIN.
Maximum length (characters)	The maximum value that can be set for the length of a PIN's value. This value must be in the range 04h - 40h for a local PIN and 04h - 10h for the global PIN. This value must be equal to or greater than the PIN minimum length value.
History size	Number of previous PIN values that cannot be matched by a new PIN. Range is 00h-0Ah. 00h = No history
Number of different characters that can be repeated at least once	The number of different characters that can be repeated at least once. Range is 00h-FFh. 00h = No limitation

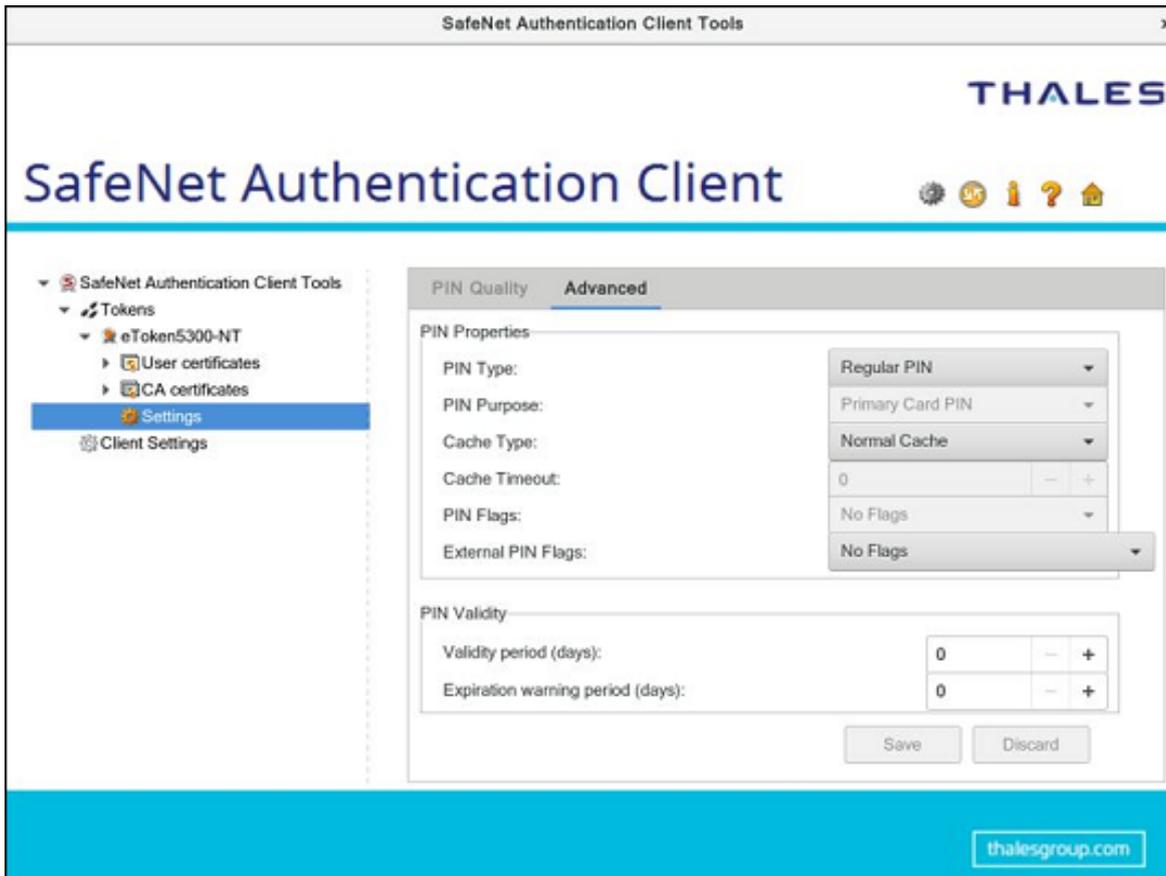
PIN Quality Parameter	Description
Maximum number of times a character can appear	The maximum number of times a character can appear. Range is 00h-FFh. 00h = No limitation
Maximum number of character in a sequence	Maximum length of characters sequences e.g. 1,2,3,4 or a,b,c,d. Range is 00h-FFh. (For example: If set to 4, 1,2,3,4,a,5 is allowed, but 1,2,3,4,5,a is not allowed). 00h = No limitation
Maximum number of times a character can be repeated in adjacent	Maximum number of times that characters can be adjacent. Range is 00h-FFh. > 00h = No limitation > 01h = Repeated characters cannot be adjacent
Manual complexity rules	For each of the character types ( <b>Numeric, Alpha upper, Alpha lower, Alpha, non alpha, Non ASCII</b> ) > Numeric = 30h...39h > Alpha upper = 41h...5Ah > Alpha lower = 61h...7Ah > Alpha = 41h...5Ah + 61h...7Ah > Non alpha = 20h...2Fh + 3Ah...40h + 5Bh...60h + 7Bh...7Fh > Non ASCII = 80h...FFh

## Setting IDPrime PIN Properties (Advanced Tab)

The *PIN Advanced* tab enables you to define PIN properties that must be met in order for the PIN to be accepted.

The **PIN Advanced** tab is available for all IDPrime based devices.

- > Select **Settings** in the left pane, to view the user **PIN Quality/Advanced** fields in the right pane.
- > Select **Digital Signature PIN** in the left pane, to view the Digital Signature **PIN Quality/Advanced** fields in the right pane.
- > Select **Digital Signature PUK** in the left pane, to view the Digital Signature **PUK Quality/Advanced** fields in the right pane.



### For IDPrime MD cards

Following **PIN Property** parameters exist in the *Advanced* Tab:

PIN Property Parameter	Description
PIN Type	<ul style="list-style-type: none"> <li>&gt; Regular PIN - Use the keyboard to enter a PIN</li> <li>&gt; External PIN - Use an external keyboard/key pad</li> </ul>
PIN Purpose	<p>Defines the purpose of the PIN. This property is for information only. The following options are available:</p> <ul style="list-style-type: none"> <li>&gt; Authentication PIN</li> <li>&gt; Digital Signature PIN</li> <li>&gt; Encryption PIN</li> <li>&gt; Non Repudiation PIN</li> <li>&gt; Administrator PIN</li> <li>&gt; Primary Card PIN</li> <li>&gt; Unlock Only PIN</li> </ul>

PIN Property Parameter	Description
Cache Type	Select one of the following Cache Type functions: <ul style="list-style-type: none"> <li>&gt; Normal Cache</li> <li>&gt; Timed Cache (Minidriver)</li> <li>&gt; No Cache (Minidriver)</li> <li>&gt; Always Prompt</li> </ul>
Cache Timeout	<ul style="list-style-type: none"> <li>&gt; This field is activated only if <i>Timed Cache (Minidriver)</i> is selected in the Cache Type parameter above.</li> <li>&gt; Defines the number of seconds it takes before the cache times out.</li> </ul>
PIN Flags	These flags are for backward compatibility only. <ul style="list-style-type: none"> <li>&gt; No Flags</li> <li>&gt; Required Security Entry</li> </ul>
Ext. PIN Flags	The following options are available: <ul style="list-style-type: none"> <li>&gt; No Flags - PINs are considered as follows:               <ul style="list-style-type: none"> <li>• Regular PIN &amp; Normal Reader ==&gt; Regular PIN</li> <li>• Regular PIN &amp; PIN Pad Reader ==&gt; External PIN</li> <li>• External PIN &amp; Normal Reader ==&gt; Regular PIN</li> <li>• External PIN &amp; PIN Pad Reader ==&gt; External PIN</li> </ul> </li> <li>&gt; No Regular fallback - changes the third case as follows:               <ul style="list-style-type: none"> <li>• External PIN &amp; Normal Reader ==&gt; Login refused</li> </ul> </li> <li>&gt; No Auto PIN Pad - changes the second case as follows:               <ul style="list-style-type: none"> <li>• Regular PIN &amp; PIN Pad Reader ==&gt; Regular PIN</li> </ul> </li> </ul> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p><b>NOTE</b> PIN Pad readers are currently not supported by SAC 10.7 Linux.</p> </div> <ul style="list-style-type: none"> <li>&gt; No Regular fallback + No Auto PIN Pad (both of the above).</li> </ul>

Following **PIN Validity** parameters exist in the *Advanced* Tab:

PIN Validity Parameter	Description
Validity period (days)	Default: 0 (no validity period) The maximum period, in days, before the PIN must be changed. When the PIN expires, the user is forced to change the PIN value the next time that the PIN is presented.
Expiration warning period (days)	Default: 0 (no warning) Defines the number of days before the PIN expires that a warning message is shown.

**NOTE** *PIN Quality* and *PIN Property* settings can be accessed when Initializing a device. See "[Initializing IDPrime Devices](#)" on page 49.