



SafeNet Authentication Client

WINDOWS USER GUIDE



Document Information

| | |
|-----------------|----------------|
| Product Version | 10.8 R6 (GA) |
| Document Number | 007-013561-005 |
| Release Date | October 2021 |

Revision History

| Revision | Date | Reason |
|----------|--------------|----------------------------------|
| Rev. H | October 2021 | Updated for 10.8 R6 (GA) release |

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 | 7 |
| Audience | 7 |
| Document Conventions | 7 |
| Command Syntax and Typeface Conventions | 7 |
| Notifications and Alerts | 8 |
| Support Contacts | 9 |
| Chapter 1: Introduction | 10 |
| Chapter 2: SafeNet Authentication Client User Interface | 11 |
| Overview | 11 |
| SafeNet Authentication Client Tray Icon | 11 |
| Running the SafeNet Authentication Client Monitor | 12 |
| SAC Tray Menu Functions | 12 |
| Opening the SafeNet Authentication Client Tray Menu | 12 |
| Closing SafeNet Authentication Client Monitor | 13 |
| SafeNet Authentication Client Tools | 13 |
| SafeNet Authentication Client Tools Toolbar | 14 |
| Opening the Simple View | 14 |
| Token Icons | 15 |
| Simple View Functions | 16 |
| Opening the Advanced View | 16 |
| Advanced View Functions | 17 |
| Tokens Node | 17 |
| Selected Token Node | 18 |
| Certificate Type Node | 20 |
| Common Criteria Certificates | 21 |
| ECC Certificates | 21 |
| Selected Certificate Node | 21 |
| Settings Node | 22 |
| Client Settings Node | 23 |
| Data Objects Node | 24 |
| Orphan Objects Node | 25 |
| Using the Virtual Keyboard | 26 |
| Validating Binary Signatures | 27 |
| Verified Binaries | 27 |
| Chapter 3: Token Management | 29 |
| Selecting the Active Token | 29 |
| Viewing and Copying Token Information | 29 |
| Logging On to the Token as a User | 30 |
| Renaming a Token | 30 |

| | |
|---|-----------|
| Changing the Token Password | 31 |
| Activating a Token | 33 |
| Deleting Token Content | 34 |
| Importing a Certificate to a Token | 35 |
| Importing Common Criteria Certificates | 36 |
| Exporting a Certificate from a Token | 38 |
| Clearing a Default Certificate | 38 |
| Deleting a Certificate | 38 |
| Logging On to the Token as an Administrator | 39 |
| Changing the Administrator Password | 40 |
| Unlocking a Token by the Challenge-Response Method | 40 |
| Setting a Token Password by an Administrator | 43 |
| Synchronizing Passwords | 44 |
| Viewing Supported Cryptographic Providers | 44 |
| Setting a Certificate as KSP or CSP | 45 |
| Setting a Certificate as Default or Auxiliary | 45 |
| Chapter 4: Token Initialization | 47 |
| Overview | 47 |
| Initialization Key Recommendations | 47 |
| Initializing eToken Devices | 47 |
| Initializing IDPrime Devices | 53 |
| Initializing IDPrime Common Criteria Devices | 54 |
| Initializing IDPrime Based Devices (Non Common Criteria/FIPS Devices) | 59 |
| Friendly Admin Password | 63 |
| Chapter 5: Token Settings | 65 |
| Setting eToken Password Quality (Password Quality Tab) | 65 |
| Setting eToken Advanced Properties (Advanced Tab) | 67 |
| Setting IDPrime PIN Quality (PIN Quality Tab) | 68 |
| Setting IDPrime PIN Properties (Advanced Tab) | 70 |
| Chapter 6: Client Settings | 73 |
| Setting Password Quality (Password Quality Tab) | 73 |
| Setting Advanced Properties (Advanced Tab) | 74 |
| Chapter 7: Working with Common Criteria | 79 |
| Unlinked Mode (4 Passwords) | 79 |
| Linked Mode (2 Passwords) | 80 |
| Linked Mode PIN Policy Settings | 81 |
| Common Criteria Extended Functions | 81 |
| Change Digital Signature PIN | 81 |
| Change Digital Signature PUK | 82 |
| Set Digital Signature PIN | 83 |
| PKCS#11 Digital Signature PIN Authentication | 85 |
| Operational Differences and Role Protection | 85 |

| | |
|--|----|
| Chapter 8: Working with SafeNet eToken 5300 | 87 |
| eToken 5300 Certificates | 87 |
| Viewing eToken 5300 Information | 88 |
| Using the eToken 5300 Touch Sense | 89 |
| eToken 5300 Touch Sense Timeout and Grace period | 90 |
| Touch Sense Timeout | 90 |
| Touch Sense Grace Period | 90 |
| Chapter 9: Working with PIN Pad Readers | 91 |
| PIN Pad Readers with IDPrime Cards | 91 |
| PIN Pad Management Scenarios | 91 |
| PIN Pad Functions | 92 |
| PIN Pad Functional Limitations | 93 |
| Must Change Password | 93 |

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 9](#)

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

Notifications and Alerts

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

Tips

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

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

Notes

Notes are used to highlight important or helpful information.

NOTE Take note. Contains important or helpful information.

Cautions

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

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

Warnings

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

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

Support Contacts

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

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

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

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

Telephone

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

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.

SAC 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 SAC Tools application and the SAC tray icon application are installed with SAC, 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) user interfaces.

NOTE If a customized version of SafeNet Authentication Client is installed, the graphics you see may be different from those displayed in this guide.

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 13](#)
 - 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 |
|---|---|---|
|  |  |  |

Running the SafeNet Authentication Client Monitor

The SAC 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, refer to ["Show application tray icon" on page 77](#).

To open SafeNet Authentication Client Monitor:

- > **On Windows:** From the taskbar, select **Start > All Programs > SafeNet > SafeNet Authentication Client > 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. Refer to ["Changing the Token Password" on page 31](#).
- > **Unlock Token:** Opens the *Unlock Token* window for the selected token. Refer to ["Activating a Token" on page 33](#).
- > **Certificate Information:** Opens the *Token Certificate Information* window for the selected token.
- > **Exit:** Closes SafeNet Authentication Client and the tray icon.

The following functions may be displayed, depending on the configuration of your system:

- > **Delete Token Content:** Removes the deletable data from the selected token
- > **Synchronize Password:** Synchronizes your token password with your domain password. Use this feature only when requested by your administrator.
- > **Token Activation:** Activates a token that's protected with an Activation PIN.

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:

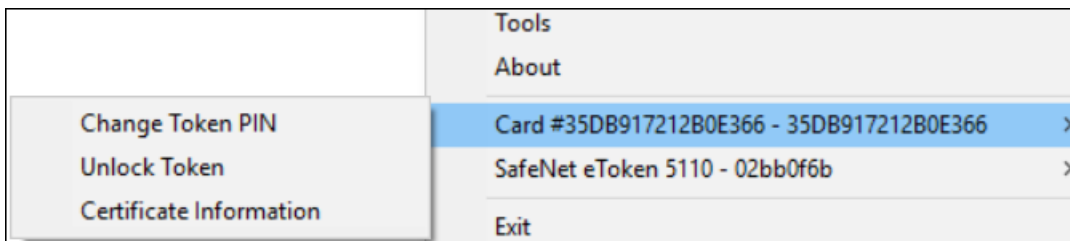
1. Right-click the **SafeNet Authentication Client** tray icon.

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.

Refer to ["Opening the Simple View" on the next page](#).

2. **Advanced View:** For extensive control over SafeNet Authentication Client and your connected tokens.

Refer to ["Opening the Advanced View" on page 16](#).

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 |
|---|--|
|  | Advanced View – Switches from the <i>Simple View</i> to the <i>Advanced View</i> |
|  | Simple View – Switches from the <i>Advanced View</i> to the <i>Simple View</i> |
|  | Refresh – Refreshes the data for all connected tokens |
|  | About – Displays product version information |
|  | Help – Opens the <i>Help</i> feature |
|  | Home – Opens the company website (cpl.thalesgroup.com/) |

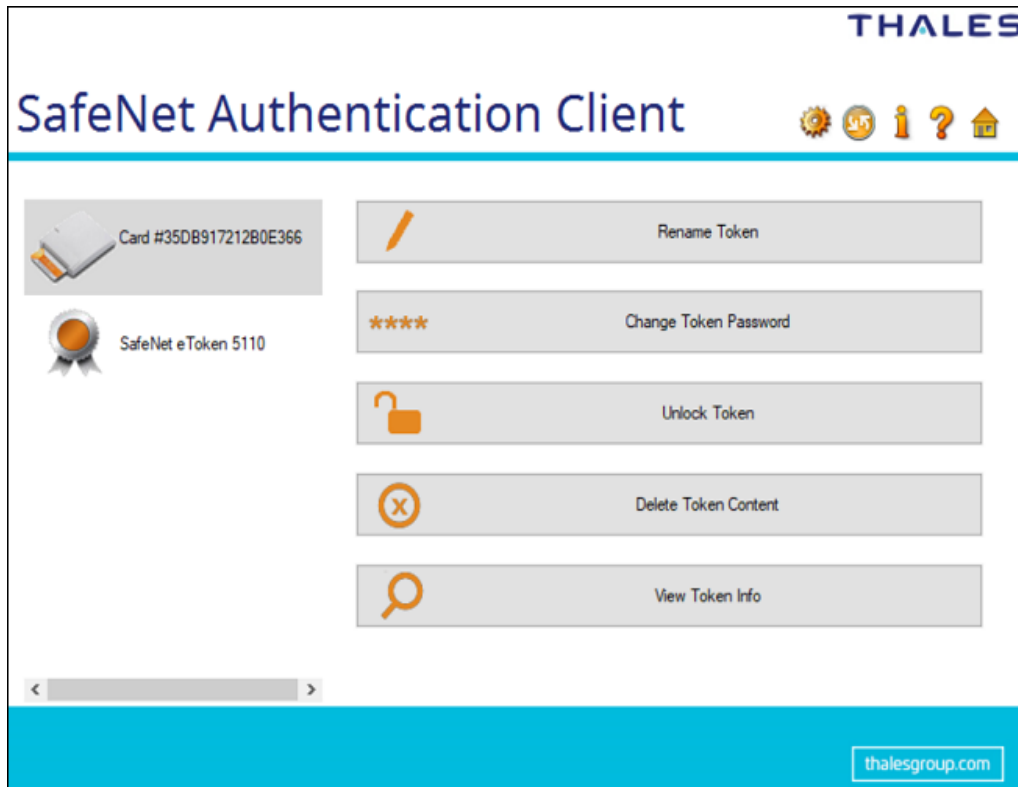
Opening the Simple View

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

Perform the following step:

1. Do one of the following:
 - Right-click the **SafeNet Authentication Client** tray icon, and select **Tools**.
 - From the taskbar, select **Start > All Programs > SafeNet > SafeNet Authentication Client > SafeNet Authentication Client 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, refer to <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, refer to <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, refer to "Activating a Token" on page 33 |

| Icon | Token Type |
|---|---------------|
|  | 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.

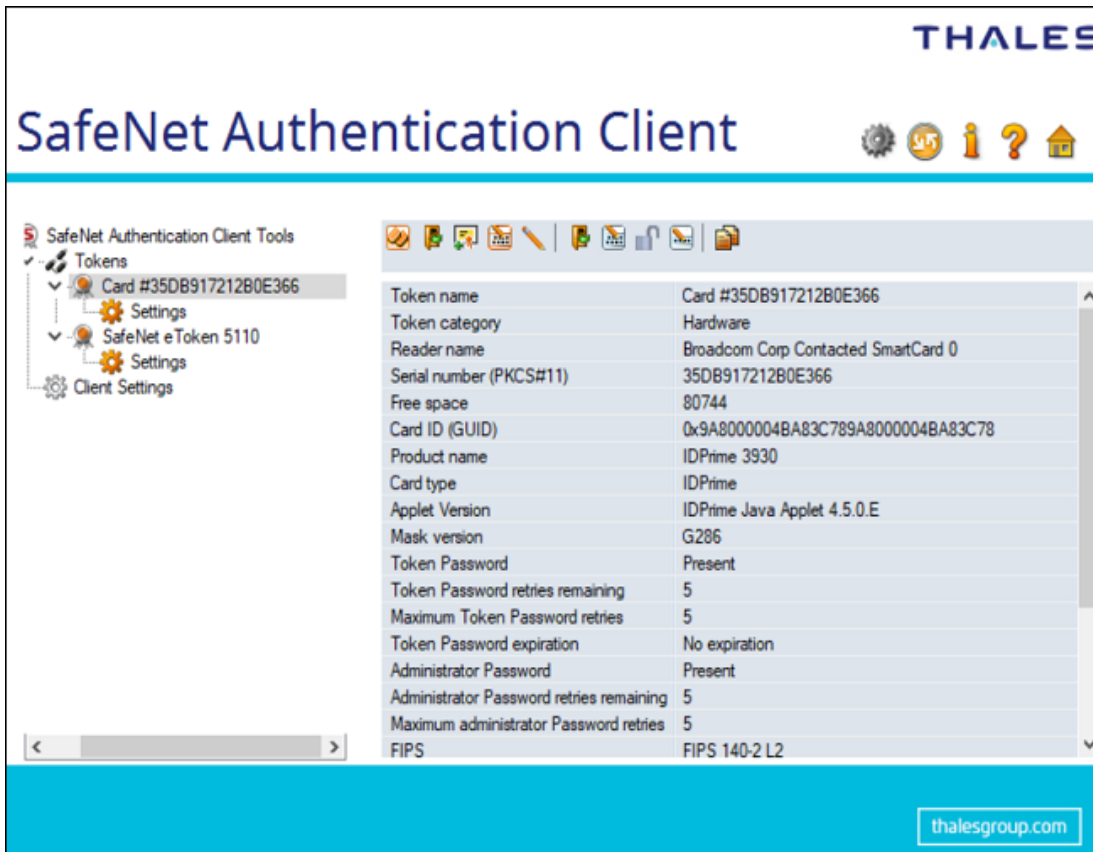
Perform the following steps:

- Do one of the following:
 - Right-click the **SafeNet Authentication Client** tray icon, and select **Tools**.
 - From the taskbar, select **Start > All Programs > SafeNet > SafeNet Authentication Client > SafeNet Authentication Client Tools**.

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

- 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:

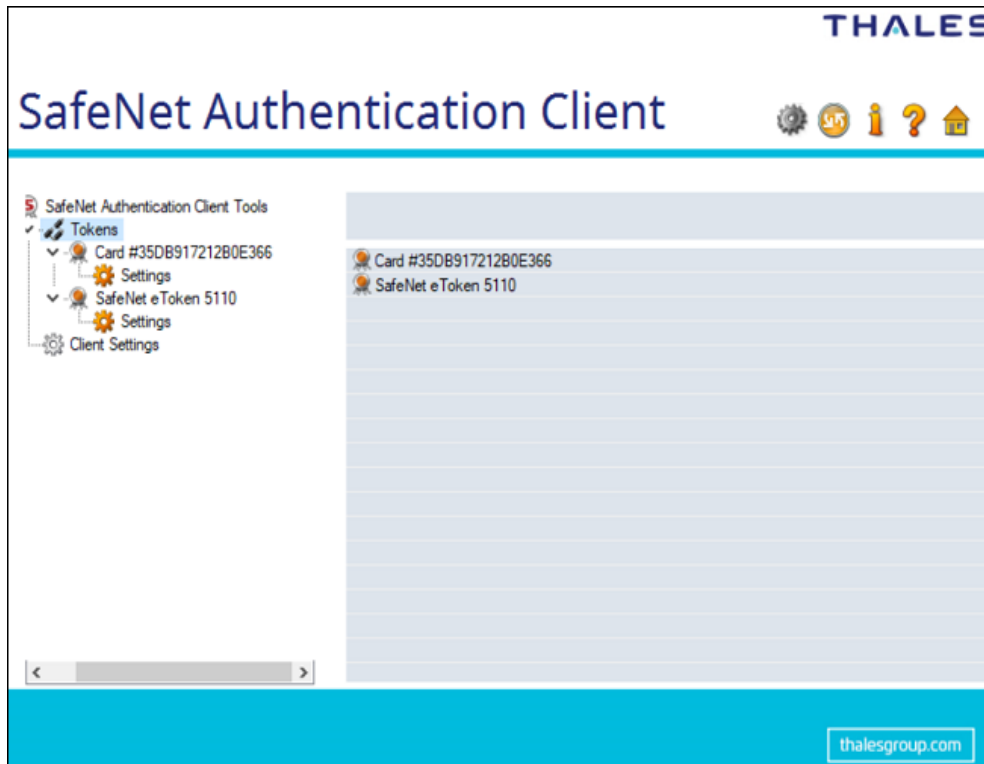
1. In the **SafeNet Authentication Client Tools > Advanced View** window, expand the tree in the left pane to display the required object.

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.

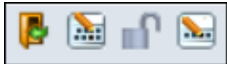
The following user functions are available:

| User Function | Icon | Right-Click Menu Item |
|--|---|-----------------------|
| Initialize Token Refer to "Token Initialization" on page 47 |  | Initialize Token |
| Log On to Token Refer to "Logging On to the Token as a User" on page 30 |  | Log On to Token |
| Import Certificate Refer to "Importing a Certificate to a Token" on page 35 |  | Import Certificate |
| Change Password Refer to "Changing the Token Password" on page 31 |  | Change Password |





| User Function | Icon | Right-Click Menu Item |
|--|---|------------------------------|
| Rename Token Refer to "Renaming a Token" on page 30 |  | Rename Token |
| Copy to Clipboard Refer to "Viewing and Copying Token Information" on page 29 |  | (None) |
| Change Digital Signature PIN Refer to "Change Digital Signature PIN" on page 81 |  | Change Digital Signature PIN |
| Change Digital Signature PUK Refer to "Change Digital Signature PUK" on page 82 |  | Change Digital Signature PUK |
| Set Digital Signature PIN Refer to "Set Digital Signature PIN" on page 83 |  | 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:



The following administrator functions are available:

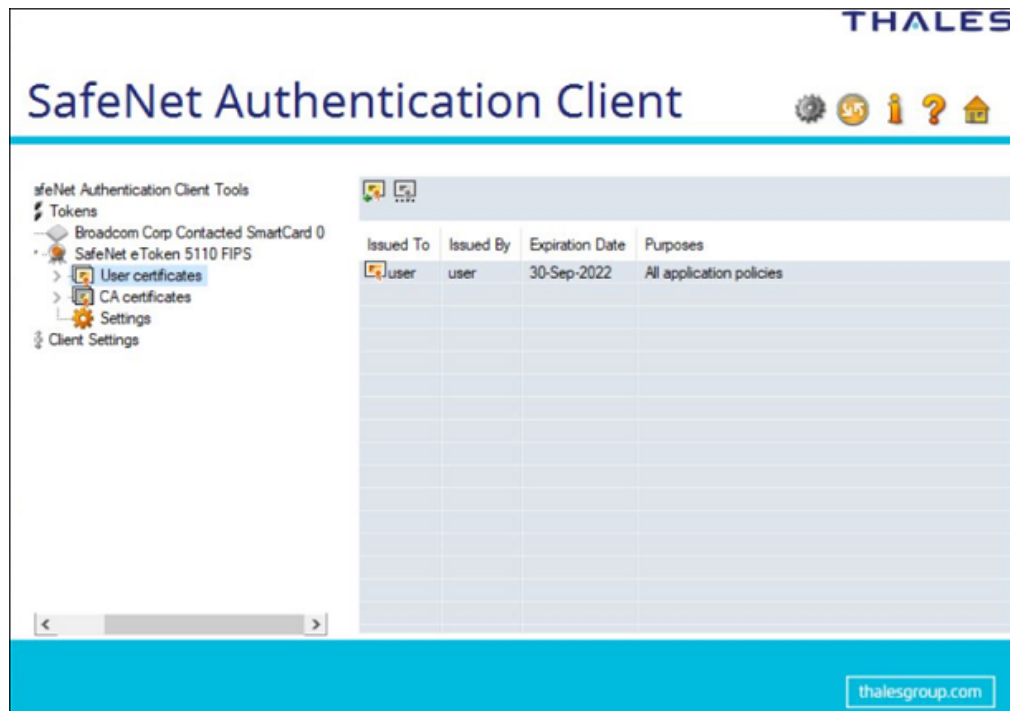
| User Function | Icon | Right-Click Menu Item |
|--|--|-------------------------------|
| Log on as Administrator Refer to "Logging On to the Token as an Administrator" on page 39 |  | Log on as Administrator |
| Change Administrator Password Refer to "Changing the Administrator Password" on page 40 |  | Change Administrator Password |
| Unlock Token Refer to "Unlocking a Token by the Challenge-Response Method" on page 40 |  | Unlock Token |
| Set Token Password Refer to "Setting a Token Password by an Administrator" on page 43 |  | Set Token Password |

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 Refer to "Importing a Certificate to a Token" on page 35 | | Import Certificate |
| Reset Default Certificate Selection Refer to "Clearing a Default Certificate" on page 38 | | Reset Default Certificate Selection |

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. Refer to ["Importing Common Criteria Certificates" on page 36](#).

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, refer to *SafeNet Authentication Client Release Notes*.

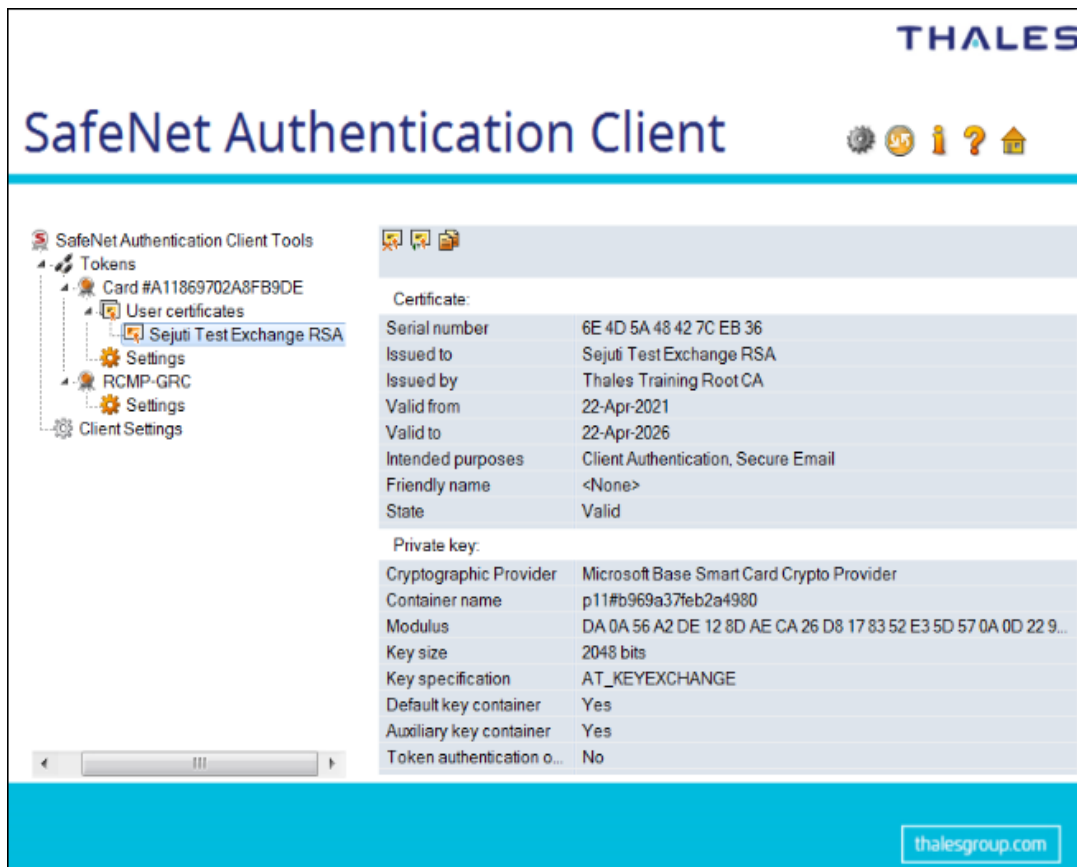
ECC Certificates

ECC Certificates are supported by eTokens and IDPrime cards.




For a full list of devices supporting ECC Certificates, refer to *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.

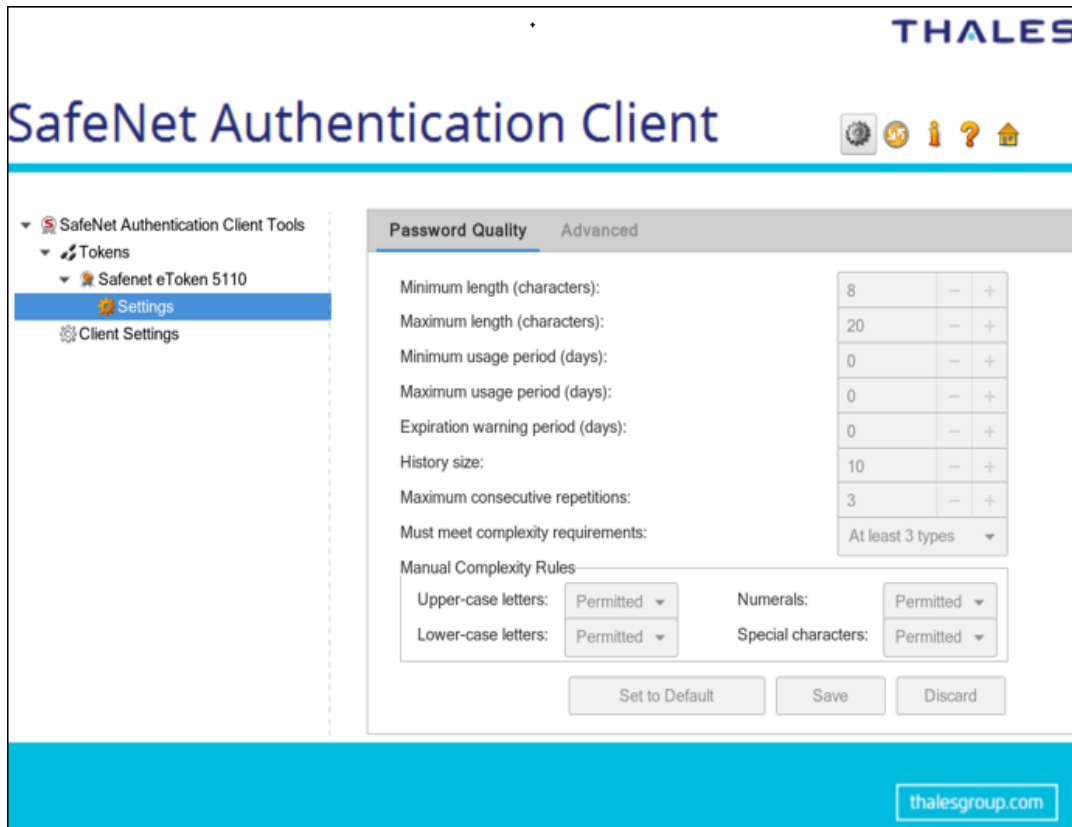


Some or all of the following functions are available:

| User Function | Icon | Right-Click Menu Item |
|--|---|-------------------------|
| Delete Certificate Refer to "Deleting a Certificate" on page 38 |  | Delete Certificate |
| Export Certificate Refer to "Exporting a Certificate from a Token" on page 38 |  | Export Certificate |
| Set as Default Refer to "Setting a Certificate as Default or Auxiliary" on page 45 | (None) | Set as Default |
| Set as Auxilliary Refer to "Setting a Certificate as Default or Auxiliary" on page 45 | (None) | Set as Auxiliary |
| Copy to Clipboard Refer to "Viewing and Copying Token Information" on page 29 |  | (None) |
| Set as KSP / Set as CSP Refer to "Setting a Certificate as KSP or CSP" on page 45 | (None) | Set as KSP / Set as CSP |

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 Common Criteria devices:

> **PIN Quality**

Refer to "[Setting IDPrime PIN Quality \(PIN Quality Tab\)](#)" on page 68.

> **Advanced**

Refer to "[Setting IDPrime PIN Properties \(Advanced Tab\)](#)" on page 70.

The following tabs exist for eToken devices:

> **Password Quality**

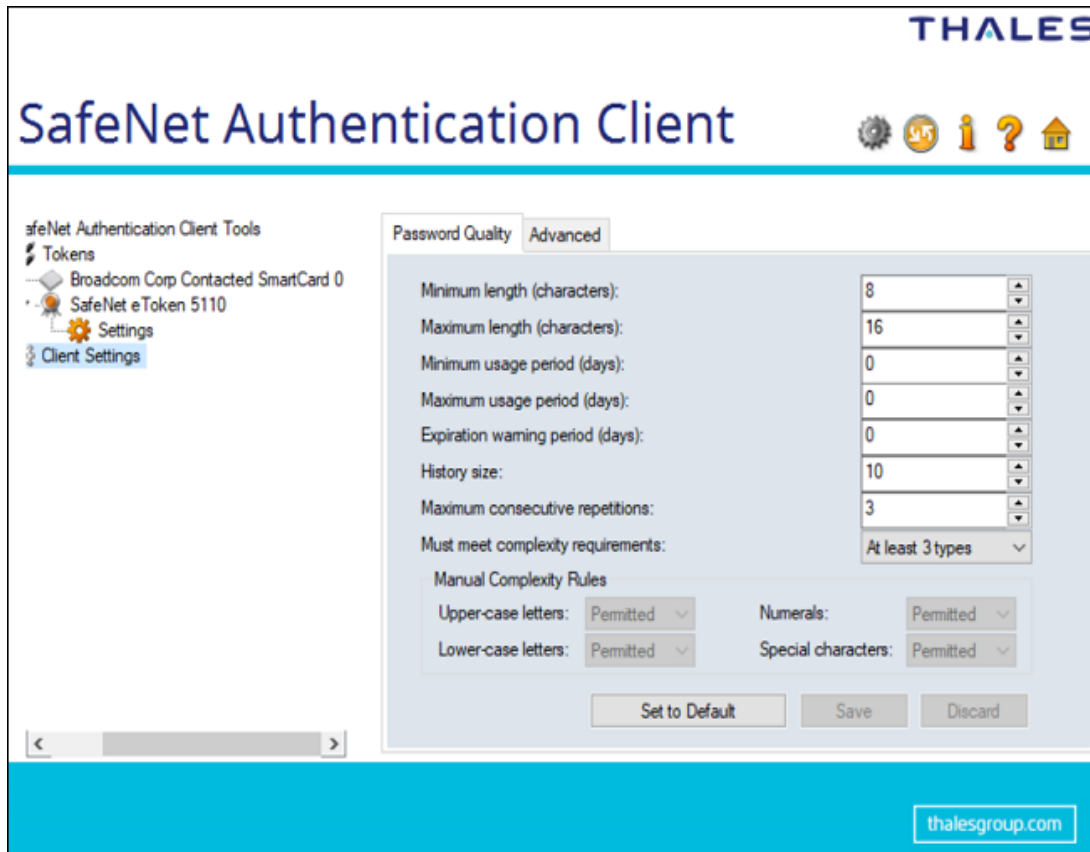
Refer to "[Setting eToken Password Quality \(Password Quality Tab\)](#)" on page 65.

> **Advanced**

Refer to "[Setting eToken Advanced Properties \(Advanced Tab\)](#)" on page 67.

Client Settings Node

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

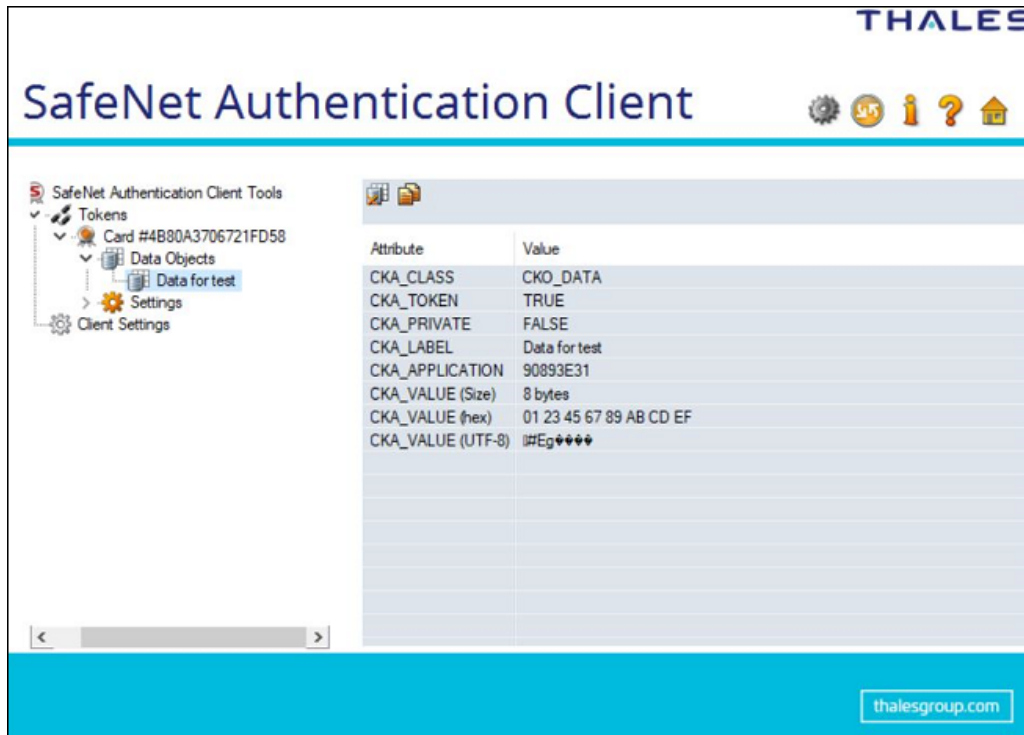
Similar to the *Settings* window, the *Client Settings* window contains two tabs:

- > Password Quality
- > Advanced

Refer to "[Client Settings](#)" on page 73.

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.

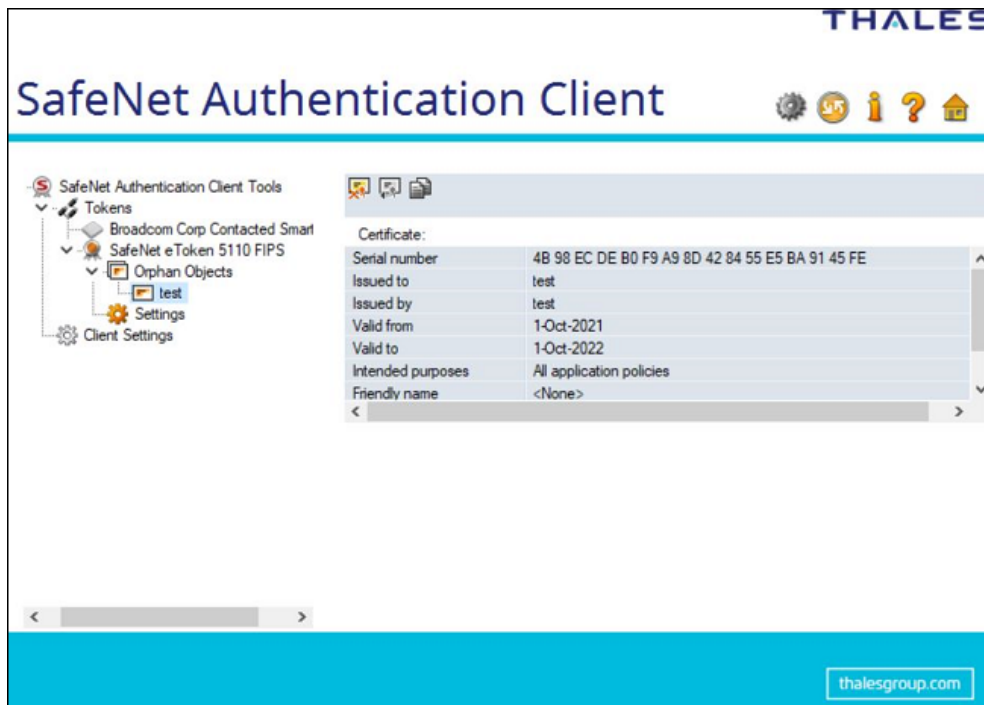
To delete a data object

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 .

Using the Virtual Keyboard

A virtual keyboard provides protection against kernel-level key loggers. It provides an additional layer of security by enabling you to enter passwords without using the physical keyboard.



If your installation has been configured for virtual keyboard use, use it for the following functions:

- > Token Logon

> Change Password

NOTE The virtual keyboard supports English characters only. To type an upper-case character, press Shift on your physical keyboard.

Validating Binary Signatures

This feature verifies the integrity of SafeNet Authentication Client binary files. SAC binary (dll and exe files) signatures can be validated using the About window in SAC Tools.

The binary verification process is performed via the standard Windows functionality (WinVerifyTrust).

WinVerifyTrust checks the following:

- > The certificate used to sign the file chains up to a root certificate located in the trusted root certificate store. This implies that the identity of the publisher has been verified by a certification authority.
- > The end entity certificate has sufficient permission to sign code.

Verified Binaries

The verified binaries are located under `c:\windows\System32` and `c:\windows\SysWoW64`.

The following binaries are verified:

- > etCAPI.dll
- > etCoreInst.dll
- > eTOKCSP.dll
- > eToken.dll
- > eTPKCS11.dll
- > SNSCKSP.dll
- > dkck201.dll
- > eTokenMD.dll
- > axaltocm.dll

NOTE The binary files above are present in the `System32` and `SysWoW64` depending on the customized installation parameters defined.

The DLL and EXE binaries are also verified under the following installation folders:

SafeNet Minidriver Proxy and Minidriver folders:

- > `C:\Program Files (x86)\Gemalto\IDGo 800 PKCS#11\`
- > `C:\Program Files (x86)\Gemalto\IDGo 800 Minidriver\`


SAC installation folder (default):

- > `C:\Program Files\SafeNet\Authentication\SAC\`

To validate SAC binary signatures

Perform the following steps:

1. Do one of the following:

- Right-click the SafeNet Authentication Client tray icon, and from the shortcut menu, select **About**.
- Open SafeNet Authentication Client Tools, and on the toolbar, click the **About** icon .

The **About** window is displayed.

2. Click **Validate Binary Signatures**.

The validation runs in the background and the results are displayed in the Validation Summary window.

3. Click **OK** to close the window.

CHAPTER 3: 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.

NOTE If a customized version of SafeNet Authentication Client is installed, the graphics you see may be different from those displayed in this guide.

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**.

Refer to ["Opening the Simple View" on page 14](#) or ["Opening the Advanced View" on page 16](#).

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. 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**.
Refer to ["Opening the Simple View" on page 14](#).
 - 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**.
Refer to "Opening the Advanced View" on page 16.
- 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:
 - a. In the **Token Information** window, click **Copy**
 - b. 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**.

Refer to "Opening the Advanced View" on page 16.

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.

TIP 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**.
Refer to "Opening the Simple View" on page 14.
 - 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**.
Refer to "Opening the Advanced View" on page 16.
 - 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 default 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.

TIP 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**.
Refer to ["Opening the Simple View" on page 14](#).
 - 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**.
Refer to ["Token Management" on page 29](#).
 - b. Do one of the following:
 - In the left pane, select the node of the required token.

In the right pane, click the **Change Password** icon .
 - In the left pane, right-click the node of the required token, and select **Change Password**.
 - 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 **Change Token Password**.
 - d. Continue with step 4.

The **Change Password** window is displayed.
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 is changed successfully.

7. Click **OK**.

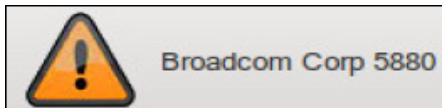
Activating a Token

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.

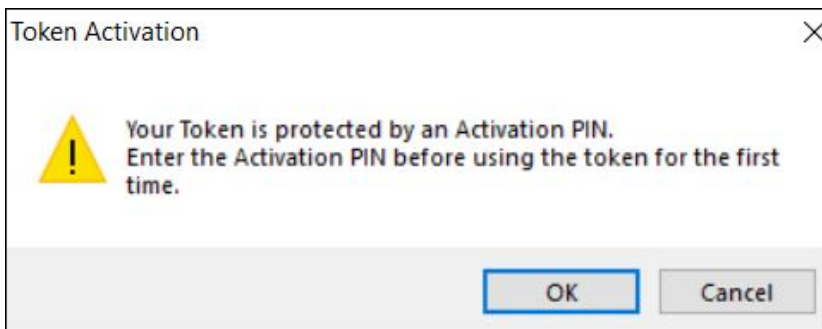
Connecting an unactivated device displays the Token with corrupted data icon in SAC Tools. This does not mean that the device is corrupted, it simply needs to be activated.



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**.

The screenshot shows the 'SafeNet Authentication Client' window with the 'THALES' logo. The main instruction is 'Enter the Token Activation PIN'. Below this, there is a 'Reader name:' field displaying 'Broadcom Corp 5880 [Contacted SmartCard] (0123456)'. An 'Activation PIN:' field is shown as an empty text box. Below the PIN field, it says 'Current Language: EN'. At the bottom left, it indicates 'Retries remaining before the token is locked: 5'. At the bottom right, there are 'OK' and 'Cancel' buttons.

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.

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, refer to "[Token Initialization](#)" on page 47.

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

1. Open **SafeNet Authentication Client Tools > Simple View**.
Refer to "[Opening the Simple View](#)" on page 14.
 - 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. Right-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 if the CA certificates should be imported to the token, and the password (if it exists) that protects the PFX file must be entered.

When downloading a certificate to the computer and then importing the certificate to the token, ensure that the certificate is removed from the local store. Then reconnect the token before using the certificate to sign and encrypt mail. This ensures that the certificate and keys used are those stored on the token and not on the computer.

Perform the following steps to import a certificate:

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

Refer to ["Opening the Advanced View" on page 16](#).

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 **Import Certificate** window is displayed.

4. Select one of the following, and click **OK**:

- Import a certificate from my personal certificate store
- Import a certificate from a file

If you select **Import a certificate from my personal certificate store**, a list of available certificates is displayed. Only certificates that can be imported on the token are listed. These are:

- Certificates with a private key already on the token
- Certificates that can be imported from the computer together with their private key

If you select **Import a certificate from a file**, the **Certificate Selection** window is displayed.

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

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

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

All requested certificates are imported, and a message confirms that the import is 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**.

Refer to ["Opening the Advanced View" on page 16](#).

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** .

- 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 **Import Certificate** window is displayed.

4. Select one of the following, and click **OK**:

- Import a certificate from my personal certificate store
- Import a certificate from a file

If you select **Import a certificate from my personal certificate store**, a list of available certificates is displayed. Only certificates that can be imported on the token are listed. These are:

- Certificates with a private key already on the token
- Certificates that can be imported from the computer together with their private key

If you select **Import a certificate from a file**, the **Certificate Selection** window is displayed.

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

The **Certificate Password** window is displayed.

SafeNet Authentication Client THALES

Enter the PFX or P12 password:

Current Language: EN

OK Cancel

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

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

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

SafeNet Authentication Client THALES

Enter the Digital Signature PIN:

Token Name:

Digital Signature PIN:

Current Language: EN

OK Cancel

7. 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**.

Refer to ["Opening the Advanced View" on page 16](#).

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.

Clearing a Default Certificate

If you have set a certificate as Default, you can clear the setting and revert to using the previous Default certificate.

Perform the following steps to clear a default certificate:

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

Refer to ["Opening the Advanced View" on page 16](#).

2. In the left pane, expand the node of the required token.

3. Do one of the following:

- In the left pane, select **User Certificates**.
- In the right pane, click the **Reset Default Certificate Selection** icon.
- In the left pane, right-click **User Certificates**, and select **Reset Default Certificate Selection**.

The **Reset Default Certificate Selection** window is displayed, confirming that the Default certificate has been reset.

4. Click **OK**.

Deleting a Certificate

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

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

Refer to ["Token Management" on page 29](#).

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**.

NOTE If *Read Only* mode is enabled, the certificate is not deleted. For more information, refer to *SafeNet Authentication Client Administrator Guide*.

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.

TIP 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" on the next page](#)
- > ["Setting a Token Password by an Administrator" on page 43](#)
- > ["Unlocking a Token by the Challenge-Response Method" on the next page](#)
- > ["Setting eToken Password Quality \(Password Quality Tab\)" on page 65](#)
- > ["Setting IDPrime PIN Properties \(Advanced Tab\)" on page 70](#)

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

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

Refer to ["Opening the Advanced View" on page 16](#).

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**.

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. Refer to ["Setting a Token Password by an Administrator" on page 43](#).


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**.
Refer to "Opening the Simple View" on page 14.
 - 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**.
Refer to "Opening the Advanced View" on page 16".
 - b. Do one of the following:
 - In the left pane, select the node of the required token.

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

SafeNet Authentication Client

THALES

Challenge Code: 92 F9 69 B3 79 BE 8E BC

Response Code:

☐ Token Password must be changed on first logon

New 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 the Response Code provided by your administrator.

OK Cancel

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 is unlocked successfully.
10. 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**.
Refer to ["Opening the Advanced View" on page 16](#).
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.

Synchronizing Passwords

SafeNet Authentication Client supports synchronization between token/card passwords and domain logon passwords.

Password synchronization can be configured via the **Synchronize with Domain Password** registry key setting (refer to the Token-Domain Password Settings section in the *SafeNet Authentication Client Administrator Guide*), or via the SAC Customization Tool.

The synchronization process ensures that a single password is used for logging on to both the token/card and the Windows domain. The process enforces the password complexity requirements that were set for the token as well as in Active Directory. You must have access to the domain when changing the password.

Perform the following steps to synchronize passwords:

1. Click the **SafeNet Authentication Client** tray icon.

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

2. Select **Synchronize Password**.

The **Synchronize Passwords** window is displayed.

3. Enter the current token password and the current domain password.
4. Enter the new token password, and confirm it.
5. Click **OK**.

You now have a single password for logging on to your token and Windows domain.

Every time you change your token password using SafeNet Authentication Client, your domain logon password is changed to the same value.

NOTE If a token/card is configured with the *Token Password must be changed on first logon* parameter and SAC is configured with the *Synchronize with Domain Password* property, only the Synchronize Password window is displayed.

Viewing Supported Cryptographic Providers

When you select a token node in the SafeNet Authentication Client Tools Advanced view, the cryptographic providers supported by the token (KSP or CSP) are displayed.

Perform the following steps to see which Cryptographic Providers are supported on the token:

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

Refer to ["Opening the Advanced View" on page 16](#).

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

Token data, including the supported cryptographic providers, is displayed in the right pane.

Setting a Certificate as KSP or CSP

When you select a certificate node in the *SafeNet Authentication Client Tools > Advanced View*, the cryptographic provider supported by the specific certificate is displayed under *Private Key Data*.

You can set a certificate type as Key Storage Provider (KSP) or Cryptographic Service Provider (CSP). This is typically required when you have a token enrolled with a legacy CSP that you want to convert to KSP, to enable support for the Suite B set of cryptographic algorithms such as SHA-2.

NOTE Setting a Certificate as KSP or CSP is available on eToken devices only.

Perform the following steps to set the certificate as KSP or CSP:

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

Refer to ["Opening the Advanced View" on page 16](#).

2. In the left pane, expand the node of the required token.
3. Right-click the required certificate, and select **Set as CSP** or **Set as KSP**.

The **Token Logon** window is displayed.

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

The supported cryptographic provider is set.

Setting a Certificate as Default or Auxiliary

If there are multiple certificates on the token, you can determine which one is set as Default and which is set as Auxiliary.

Each option is enabled only if the action can be performed on that particular certificate or key. The following table describes the use of these settings.

| Setting | Description | Scenario |
|---------|---|---|
| Default | Smart card logon uses the certificate defined as the Default. In most Microsoft applications, smart card logon is used. | <p>Your token contains two certificates. One is to logon to domain A and the other to logon to domain B. If your previous logon was to domain A, it means that the certificate used to logon to domain A is now the Default. If you need to log on to domain B from another computer, the following happens:</p> <ul style="list-style-type: none"> > If you first set the domain B certificate as Default, the logon uses the correct certificate, and the logon succeeds. > If you do not set the domain B certificate as Default, the domain A certificate is used, and logon fails. |

| Setting | Description | Scenario |
|-----------|--|--|
| Auxiliary | Some applications use Client Authentication and not smart card logon. Client Authentication provides access to fewer system resources than smart card logon. SafeNet Authentication Client enables a Client Authentication logon process for these applications, such as VPN. If more than one certificate on the token includes Client Authentication as an Intended Purpose, define which certificate to use by setting it as Auxiliary. | Your token contains a certificate intended for VPN connection, but there is another certificate that also includes Client Authentication as its Intended Purpose. The certificate for the VPN connection must be set as Auxiliary, to ensure that it is used as the default for VPN logon. |

To set a certificate as Default or Auxiliary

Perform the following steps:

1. Open **SafeNet Authentication Client Tools > Advanced View**.
Refer to ["Opening the Advanced View" on page 16](#).
2. In the left pane, expand the node of the required token, and right-click the required certificate.
3. From the shortcut menu, select **Set as Default** or **Set as Auxiliary**.
The **Token Logon** window opens.
4. Enter the token password, and click **OK**.
The certificate is set as Default or Auxiliary.

CHAPTER 4: 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.

Initialization Key Recommendations

The Initialization Key can be changed using either one of the following methods:

- > Customization Product Branding (CPB) (Factory settings)
- > SAC Initialization process documented in this section

Initializing eToken Devices

This section refers to the following devices:

- > SafeNet eToken 5110
- > SafeNet eToken 5110 FIPS

> Gemalto IDCore 30B eToken

Depending on the type of token being initialized, certain settings are not enabled. To initialize an eToken 5110 CC device, refer to ["Initializing IDPrime Common Criteria Devices" on page 54](#).

NOTE If a customized version of SafeNet Authentication Client is installed, the graphics you see may be different from those displayed in this guide.

Perform the following steps to initialize an eToken device:

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

Refer to ["Opening the Advanced View" on page 16](#).

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.

The screenshot shows the 'SafeNet Authentication Client' window with the 'THALES' logo. The 'Token Name' field is pre-filled with 'SafeNet eToken 5110'. Below it, the 'Create Token Password' section has 'New Token Password' and 'Confirm Password' fields, both containing masked characters. A 'Logon retries before token is locked' spinner is set to 15. A checkbox 'Token password must be changed on first logon' is checked. The 'Create Administrator Password' section has empty fields for 'Create Administrator Password' and 'Confirm Password', with a 'Logon retries before token is locked' spinner also set to 15. At the bottom left is a checkbox for 'One-factor logon'. At the bottom right is the text 'Current Language: EN'. The bottom of the window features four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

5. Complete the fields as follows:

| Field | Description |
|--------------------|--|
| Token Name | <ul style="list-style-type: none"> > 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". > The token name does not affect the token contents. It is used solely to identify the token. |
| 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. |

| Field | Description |
|---|--|
| 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> <p>NOTE The retry counter counts only passwords that have a valid length. This field is enabled/disabled based on the card type.</p> |
| Token password must be changed on first logon | If required, select this field. |
| Create Administrator Password | <p>Select <i>Create Administrator Password</i> and enter a New Administrator Password. The minimum password length on an eToken device is 8 characters.</p> <p>NOTE 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> |
| Confirm Password | Re-enter the administrator password. |
| Logon retries before token is locked | <p>> 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.</p> <p>> The default setting for the maximum number of incorrect logon attempts is 15.</p> <p>NOTE This field is enabled/disabled based on the card type.</p> |
| One-factor logon | <p>Configures the token without a password. The default value for this setting is disabled.</p> <p>NOTE</p> <ul style="list-style-type: none"> - This One-factor logon feature is used by eToken device only. - The One-factor logon feature is not supported by FIPS devices. - Selecting the One-factor logon option disables the <i>Create Token Password</i> and <i>Create Administrator Password</i> fields. |

6. Click **Next**.

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

SafeNet Authentication Client THALES

Private data caching: Always (fastest)

Secondary Authentication Key: Never

Cancel < Back Next > 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"> > Always (fastest): 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. > While user is logged on: 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. > Never: Private information is not cached. <p>Refer to "Setting eToken Advanced Properties (Advanced Tab)" on page 67.</p> |

| Field | Description |
|------------------------------|---|
| 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 memory is always available for keys.</p> <p>Refer to "Setting eToken Advanced Properties (Advanced Tab)" on page 67.</p> |

8. Click **Next**.

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

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 | Select this option and enter the Initialization Key configured in the This Value field during the previous token initialization. |
| Change the key for the next initialization to: | Select one of the following: <ul style="list-style-type: none"> > Default: Revert to the factory-set default so that the user is not required to enter an Initialization Key during subsequent token initializations. > Random: If selected, it will never be possible to re-initialize the token. > This Value: Select and confirm a unique key. During subsequent token initializations, the user must enter this key in the <i>Use this Initialization Key</i> field. |

NOTE The initialization key minimum length is 4.

NOTE Initialization Key policy:

A secure password has at least 8 characters (up to 32 characters) and contains at least 3 of the following rules:

- Upper case letters
- Lower case letters
- Numerals
- Special characters (&, %, \$, etc.)

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 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). Refer to ["Set Digital Signature PIN" on page 83](#).

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 CC 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 CC device is being used for the first time.

The screenshot shows the 'SafeNet Authentication Client' window with the 'THALES' logo. It features a checkbox for 'Use Initialization key to initialize the Token'. Below this, a section titled 'Enter the current Administrator Password to initialize the Token' contains a checkbox for 'Use factory default administrator password' and a text input field for 'Administrator Password:'. A similar section for 'Enter the current Digital Signature PUK to initialize the Token' includes a checkbox for 'Use factory default digital signature PUK' and a text input field for 'Digital Signature PUK:'. The 'Current Language: EN' is displayed. A note states: 'The default administrator password and digital signature PUK is a known value of 0's set on the standard profile. For the non-default value, please enter it manually.' At the bottom are buttons for 'Cancel', 'Back', 'Next', and 'Finish'.

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

This screenshot is similar to the previous one but for linked mode. It includes the same checkboxes and input fields for the Administrator Password and Digital Signature PUK. However, the 'Current Language: EN' text is positioned to the right of the PUK input field. The explanatory note about default values remains. The 'Cancel', 'Back', 'Next', and 'Finish' buttons are at the bottom.

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

5. Do following as per the requirement:

| | |
|--|---|
| Use Initialization key to initialize the Token | <p>Select this check-box to if you have an initialization key.</p> <div> NOTE This option is enabled only for the devices that have an initialization key. </div> |
| Use factory default administrator password | <ul style="list-style-type: none"> > Select this check-box if the current administrator password is 48 zeros. If selected, the <i>Administrator Password</i> field below 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. |
| Use factory default digital signature PUK | <ul style="list-style-type: none"> > 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. > Deselect it, if the current Digital Signature PUK is different from the factory default. |
| 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"> > 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". > The token name does not affect the token contents. It is used solely to identify the token. |
| New Token Password | <p>The default password is 1234567890 automatically appears in this field.</p> <div> <p>NOTE</p> <ul style="list-style-type: none"> - 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. - If the <i>Token password must be changed on first logon</i> option is selected, the initialization succeeds, and the user is prompted to create a new password when next logging on with the token/card. - The user is required to set a token password that meets the Password Quality requirements configured in the <i>Settings</i> window. </div> |
| Confirm Password | <ul style="list-style-type: none"> > The default password (1234567890) automatically appears in this field. > If the above field was changed, then re-enter the password entered in the <i>New Token Password</i> field. |
| Logon retries before token is locked | <ul style="list-style-type: none"> > Enter the number of times a token password can be entered incorrectly before the token is locked. > 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. <div> <p>NOTE 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> <p>NOTE 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>Refer to "Setting IDPrime PIN Quality (PIN Quality Tab)" on page 68 and "Setting IDPrime PIN Properties (Advanced Tab)" on page 70.</p> |

| Field | Description |
|---|--|
| Create Administrator Password | <ul style="list-style-type: none"> > 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. > You can change the default Administrator Password to a password that is between 8-32 alphanumeric characters. |
| Confirm Password | Re-enter the administrator password. |
| Logon retries before token is locked | <ul style="list-style-type: none"> > 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. > The default setting for the maximum number of incorrect logon attempts is 15. <p>NOTE This field is enabled/disabled based on the card type.</p> |
| Keep the current administrator password | <p>Select this if you want to keep the current administrator password.</p> <p>NOTE If this option is selected, the following warning message appears: <i>If the current password is the default password (48 zeros), 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).

This window defines whether you are going to work in linked or unlinked mode.

SafeNet Authentication Client THALES

Common Criteria Passwords:

New Digital Signature PIN:

Confirm PIN:

PIN Policy

New Digital Signature PUK:

Confirm PUK:

PIN Policy

Cancel Back Next Finish

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. Refer to "Setting IDPrime PIN Quality (PIN Quality Tab)" on page 68 and "Setting IDPrime PIN Properties (Advanced Tab)" on page 70 . |
| 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> . |

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**.

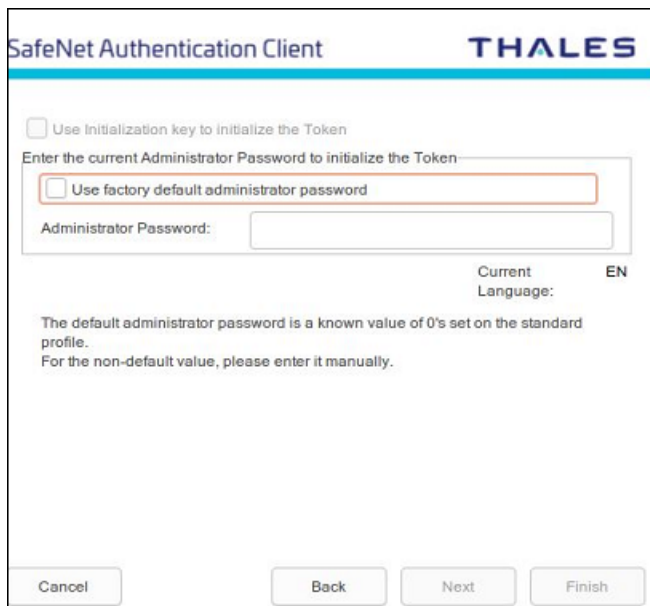
The **Initialization Options** window is displayed, allowing you to select how to initialize the device.

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.



The screenshot shows the 'Administrator Logon' window from the SafeNet Authentication Client. The window has a title bar with 'SafeNet Authentication Client' and the 'THALES' logo. It contains a checkbox for 'Use Initialization key to initialize the Token'. Below this, it says 'Enter the current Administrator Password to initialize the Token'. There is another checkbox for 'Use factory default administrator password'. A text field for 'Administrator Password:' is present. To the right, it shows 'Current Language: EN'. A note at the bottom states: 'The default administrator password is a known value of 0's set on the standard profile. For the non-default value, please enter it manually.' At the bottom are four buttons: 'Cancel', 'Back', 'Next', and 'Finish'.

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

5. Do following as per the requirement:

| | |
|--|---|
| Use Initialization key to initialize the Token | <p>Select this check-box to if you have an initialization key.</p> <p>NOTE This option is enabled only for the devices that have an initialization key.</p> |
| Use factory default administrator password | <p>> Select this check-box if the current administrator password is 48 zeros. If selected, the <i>Administrator Password</i> field below is shaded showing the default password.</p> <p>> Deselect it, if the current administrator password is different from the factory default.</p> |
| Administrator Password | <p>Enter the current administrator password.</p> <p>NOTE Current administrator password is different from the factory default. The default Administrator Password is 48 zeros</p> |

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"> > 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>. > The token name does not affect the token contents. It is used solely to identify the token. |
| New Token Password | <p>The default password is 1234567890 automatically appears in this field.</p> <div> <p>NOTE</p> <ul style="list-style-type: none"> - 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. Otherwise, the initialization fails because the default password does not meet the password quality requirements. - 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. - The user is required to set a token password that meets the PIN Quality requirements. </div> |
| Confirm Password | <ul style="list-style-type: none"> > The default password (1234567890) automatically appears in this field. > If the above field was changed, then re-enter the password entered in the <i>New Token Password</i> field. |
| 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> <p>NOTE 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>Refer to "Setting IDPrime PIN Quality (PIN Quality Tab)" on page 68 and "Setting IDPrime PIN Properties (Advanced Tab)" on page 70.</p> |
| Create Administrator Password | <ul style="list-style-type: none"> > 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. > You can change the default Administrator Password to a password that is between 8-32 alphanumeric characters (or to 48 hexadecimal digits). |
| Confirm Password | <p>Re-enter the administrator password.</p> |

| Field | Description |
|---|--|
| Logon retries before token is locked | <ul style="list-style-type: none"> > 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. > The default setting for the maximum number of incorrect logon attempts is 15. <p>NOTE This field is enabled/disabled based on the card type.</p> <p>></p> |
| Keep the current administrator password | <p>Select this if you want to keep the current administrator password.</p> <p>NOTE If this option is selected, the following warning message appears: If the current password is the default password (48 zeros), 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 digits in binary bytes or 48 digits in hexadecimal digits.

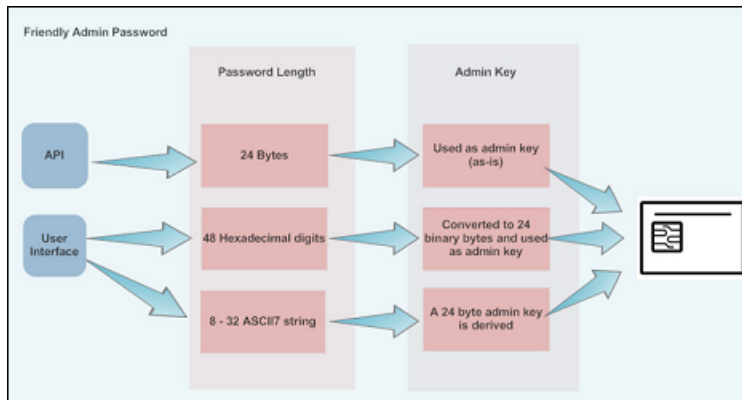
- > The Friendly Admin Password (known as Friendly Admin) works with all IDPrime devices.
- > The Friendly Admin uses a user secret in the range of 8 to 32 ASCII7 characters.

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 (refer to "[Working with Common Criteria](#)" on page 79) 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 5: Token Settings

Configurations set in the selected token's *Settings* tab determine behavior that applies to the specific card/etoken.

To know about the settings applied to all tokens when they are initialized, refer to ["Client Settings" on page 73](#).

Setting eToken Password Quality (Password Quality Tab)

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

The screenshot shows the 'SafeNet Authentication Client' window. On the left, a navigation pane lists 'SafeNet Authentication Client Tools', 'Tokens', 'Safenet eToken 5110', 'Settings' (selected), and 'Client Settings'. The main area displays the 'Password Quality' tab for the 'Safenet eToken 5110'. The tab is divided into 'Basic' and 'Advanced' sections. The 'Advanced' section is active, showing various password policy settings. Each setting has a text input field and a numeric spinner control.

| Setting | Value |
|------------------------------------|------------------|
| Minimum length (characters): | 8 |
| Maximum length (characters): | 20 |
| Minimum usage period (days): | 0 |
| Maximum usage period (days): | 0 |
| Expiration warning period (days): | 0 |
| History size: | 10 |
| Maximum consecutive repetitions: | 3 |
| Must meet complexity requirements: | At least 3 types |

Manual Complexity Rules:

| Rule | Setting |
|---------------------|-----------|
| Upper-case letters: | Permitted |
| Lower-case letters: | Permitted |
| Numerals: | Permitted |
| Special characters: | Permitted |

Buttons: Set to Default, Save, Discard

Footer: thalesgroup.com

Perform the following steps:

1. Open **SafeNet Authentication Client Tools > Advanced View**.
Refer to ["Opening the Advanced View" on page 16](#).
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: 20 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. > At least 2 types: a minimum of 2 complexity rules (out of the 4 shown in the Manual Complexity fields) are enforced. > At least 3 types: a minimum of 3 complexity rules (out of the 4 shown in the Manual Complexity fields) are enforced (Default). > None: Complexity requirements are not enforced. > Manual: 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: > Permitted - Can be included in the password, but is not mandatory (Default). > Mandatory - Must be included in the password. > Forbidden - Must not be included in the password. |

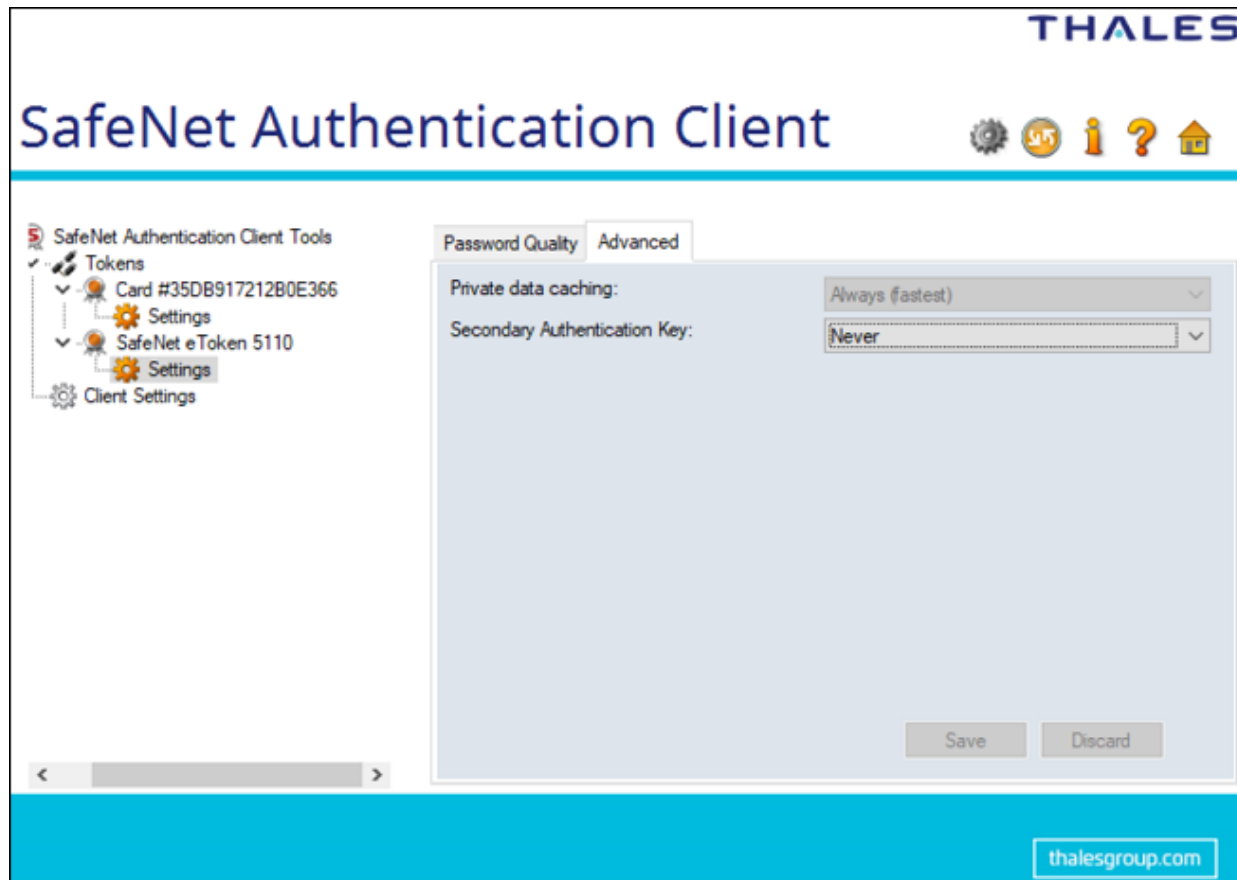
5. Do one of the following:

- 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 eToken Advanced Properties (Advanced Tab)

The eToken's *Advanced* tab enables you to cache public information stored on the token as well as defines the policy used for the secondary authentication of RSA keys.



Perform the following steps :

1. Open **SafeNet Authentication Client Tools > Advanced View**.
Refer to ["Opening the Advanced View" on page 16](#).
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. Select following as per the requirement:

| Option | Description |
|------------------------------|--|
| Private data caching | <p>This option defines when private information (excluding private keys on the eToken PRO/NG OTP/smart card) can be cached outside the token. In SafeNet Authentication Client, public information stored on the token is cached to enhance performance.</p> <p>In SafeNet Authentication Client, public information stored on the token is cached to enhance performance.</p> <p>Select one of the following:</p> <ul style="list-style-type: none"> > 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. |
| Secondary Authentication Key | <p>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.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>NOTE This setting defines the policy for using the secondary authentication of RSA keys.</p> </div> <p>Select one of the following:</p> <ul style="list-style-type: none"> > Always > Always prompt user > Prompt user on application request > Never > Token authentication on application request <p>For an explanation of these options, refer to "Token Initialization" on page 47.</p> |

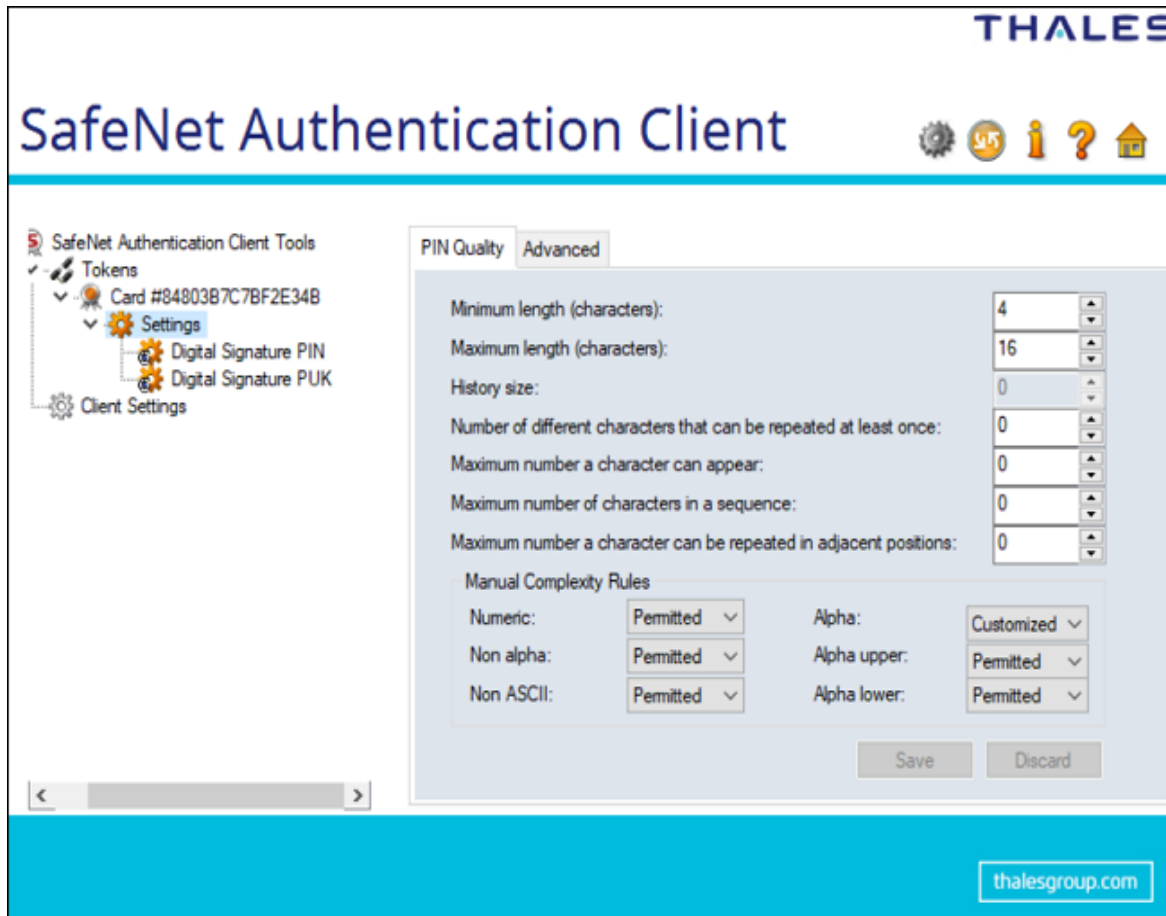
5. Do one of the following:

- 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 For Non-Managed cards, the parameters of this tab are disabled.

**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 |

| PIN Quality Parameter | Description |
|---|---|
| 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 |
| 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 (Numeric, Alpha upper, Alpha lower, Alpha, non alpha, Non ASCII) > 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 |

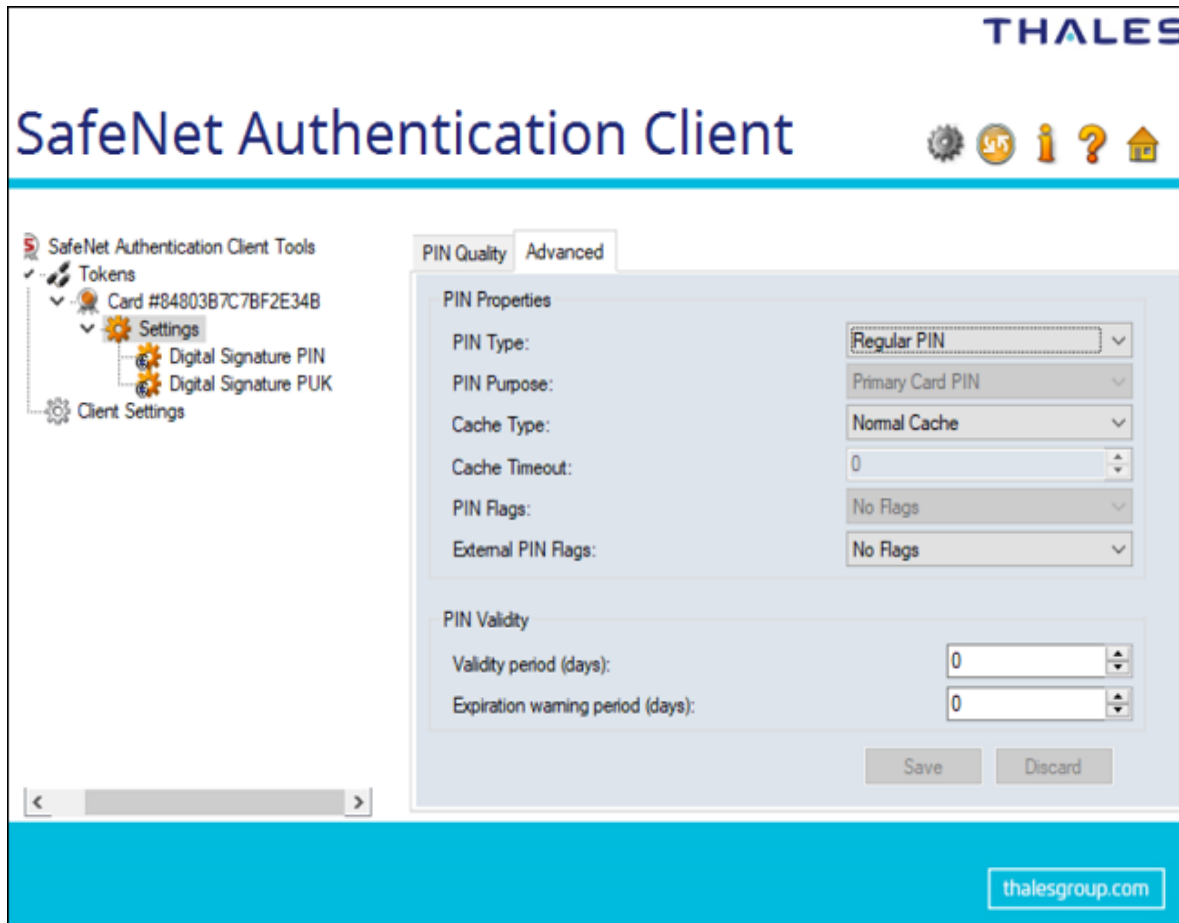
Setting IDPrime PIN Properties (Advanced Tab)

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

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

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

NOTE The setting of *Digital Signature PIN* and *Digital Signature PUK* are disabled in linked mode.



For IDPrime cards

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

| PIN Property Parameter | Description |
|------------------------|--|
| PIN Type | <ul style="list-style-type: none"> > Regular PIN - Use the keyboard to enter a PIN > External PIN - Use an external keyboard/key pad |
| 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"> > Authentication PIN > Digital Signature PIN > Encryption PIN > Non Repudiation PIN > Administrator PIN > Primary Card PIN > Unlock Only PIN |

| PIN Property Parameter | Description |
|------------------------|---|
| Cache Type | <p>Select one of the following Cache Type functions:</p> <ul style="list-style-type: none"> > Normal Cache > Timed Cache (Minidriver) > No Cache (Minidriver) > Always Prompt |
| Cache Timeout | <ul style="list-style-type: none"> > This field is activated only if <i>Timed Cache (Minidriver)</i> is selected in the Cache Type parameter above. > Defines the number of seconds it takes before the cache times out. |
| PIN Flags | <p>These flags are for backward compatibility only.</p> <ul style="list-style-type: none"> > No Flags > Required Security Entry |
| Ext. PIN Flags | <p>The following options are available:</p> <ul style="list-style-type: none"> > No Flags - PINs are considered as follows: <ul style="list-style-type: none"> • Regular PIN & Normal Reader ==> Regular PIN • Regular PIN & PIN Pad Reader ==> External PIN • External PIN & Normal Reader ==> Regular PIN • External PIN & PIN Pad Reader ==> External PIN > No Regular fallback - changes the third case as follows: <ul style="list-style-type: none"> • External PIN & Normal Reader ==> Login refused > No Auto PIN Pad - changes the second case as follows: <ul style="list-style-type: none"> • Regular PIN & PIN Pad Reader ==> Regular PIN > No Regular fallback + No Auto PIN Pad (both of the above). |

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

| PIN Validity Parameter | Description |
|----------------------------------|--|
| Validity period (days) | <p>Default: 0 (no validity period)</p> <p>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.</p> |
| Expiration warning period (days) | <p>Default: 0 (no warning)</p> <p>Defines the number of days before the PIN expires that a warning message is shown.</p> |

NOTE *PIN Quality* and *PIN Property* settings can be accessed when Initializing a device. Refer to ["Initializing IDPrime Devices" on page 53](#).

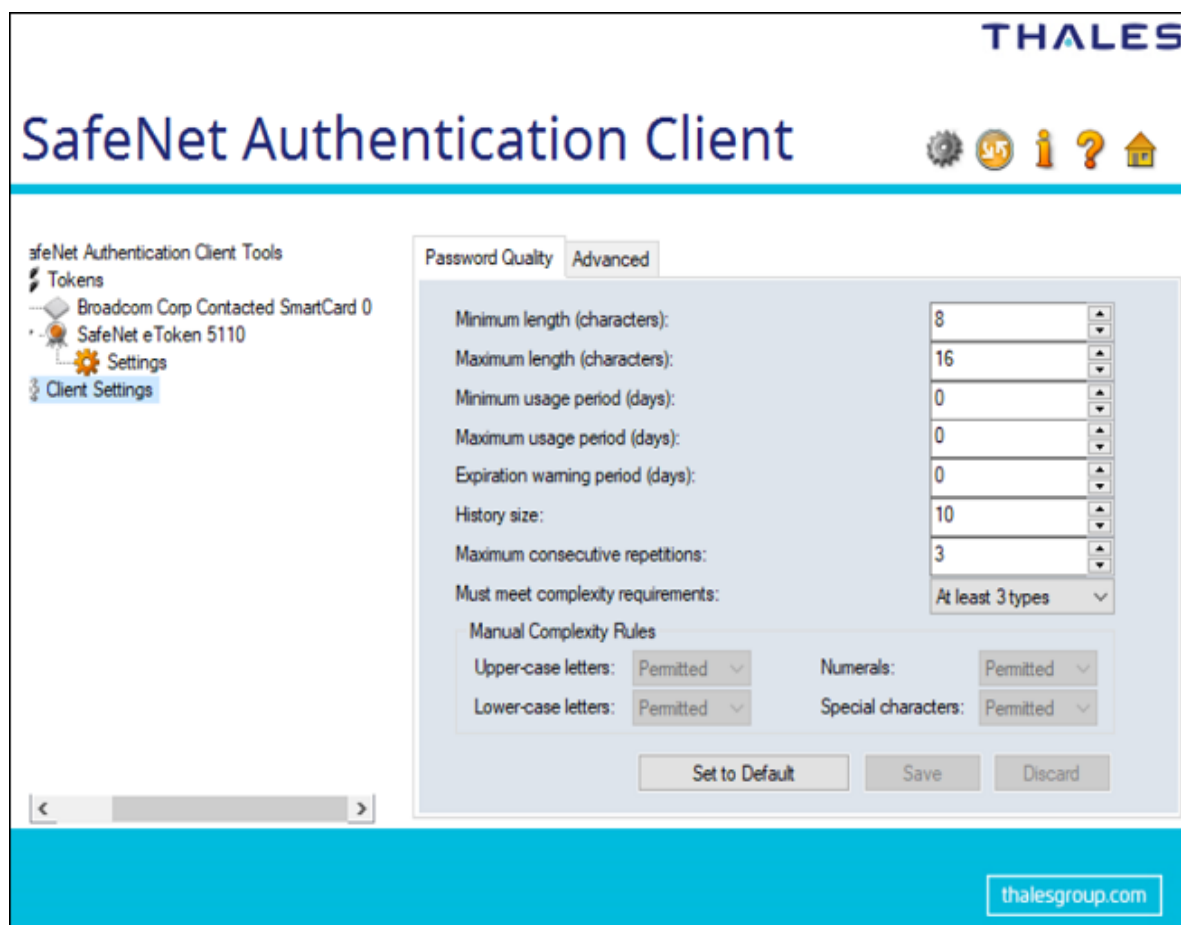
CHAPTER 6: Client Settings

Client Settings are basically the settings of the SAC Tools. It includes the parameters that are saved to the computer and applied to all tokens that are initialized on the computer after the settings have been configured. Client Settings displays two tabs, the *Password Quality* tab and the *Advanced* tab.

To know about the settings applied to a specific token, refer to ["Token Settings" on page 65](#)

Setting Password Quality (Password Quality Tab)

The Client's *Password Quality* tab enables the administrator to set certain complexity and usage requirements for token passwords.



To set PIN Quality parameters for IDPrime cards, refer to ["Setting IDPrime PIN Quality \(PIN Quality Tab\)" on page 68](#).

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**.

Refer to ["Opening the Advanced View" on page 16](#).

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**.

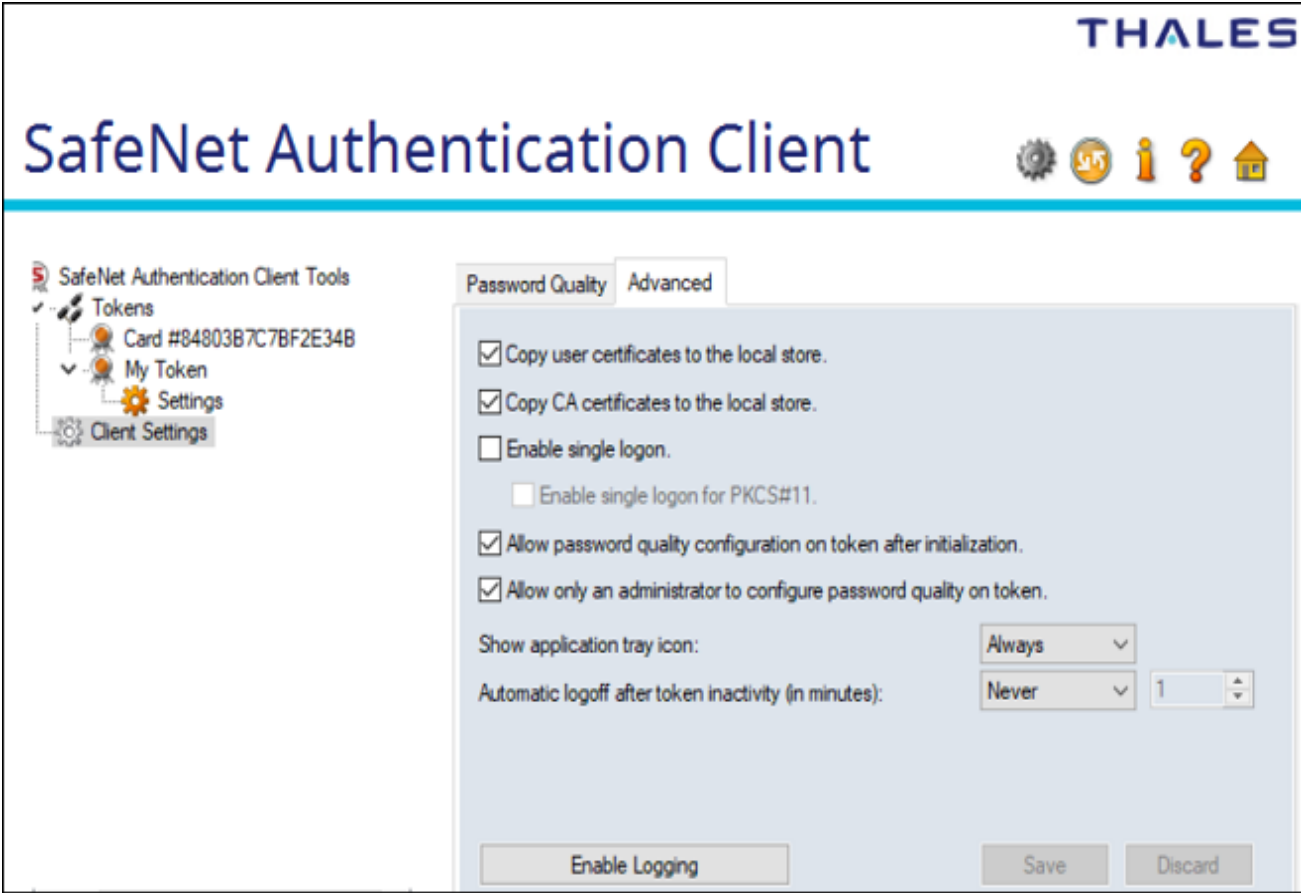
NOTE The Client *Password Quality* settings are configured the same way as the Token *Password Quality* settings. Refer to ["Setting eToken Password Quality \(Password Quality Tab\)" on page 65](#).

- 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.

Setting Advanced Properties (Advanced Tab)

The Client's *Advanced* tab enables you to configure password quality, SAC tray icon visibility, token activity, and more.



Perform following steps to set advanced options for the Client:

- 1. Open **SafeNet Authentication Client Tools > Advanced View**.
Refer to "Opening the Advanced View" on page 16.
- 2. In the left pane, select **Client Settings**.
- 3. In the right pane, select the **Advanced** tab.
The **Advanced** tab is displayed.
- 4. Select following as per the requirement:

| Option | Description |
|---|---|
| Copy user certificates to the local store | <p>SAC operations often require certificates, private keys, and public keys. Private keys should always be stored securely on the token. Certificates should also be stored on the token, ensuring that the certificates are readily available when using the token on a different computer.</p> <p>> Select this option to control the automatic installation of the token's user certificates to the local certificate store upon token connection.</p> <div>NOTE This option is selected by default.</div> |

| Option | Description |
|--|--|
| Copy CA Certificates to the Local Store | <p>When a token is connected to a computer, the system may detect that one or more CA certificates that are installed on the token are not installed on the computer.</p> <p>> Select this option to control the automatic installation of the token's CA certificates to the local certificate store upon token connection.</p> <p>NOTE Microsoft displays a security warning when it detects that CA certificates are be installed to the local store. To permit the certificates to be installed from the token, the user must click Yes.</p> <p>NOTE This option is selected by default.</p> |
| Enable single logon | <p>When single logon is enabled, users can access multiple applications with only one request for the token password during each computer session. This alleviates the need for the user to log on to each application separately.</p> <p>NOTE This option is disabled by default.</p> <p>NOTE When single logon is set using SAC Tools, Windows Logon is not included in the single logon process. Only an administrator can configure Windows Logon as single logon.</p> <p>> Select one of the following:</p> <ul style="list-style-type: none"> To enable Single Logon for MS Cryptography, select Enable single logon. To enable Single Logon for MS Cryptography and PKCS#11 cryptography, select Enable single logon and then select Enable single Logon for PKCS#11. <p>TIP To activate the single logon feature, log off from the computer and log on again.</p> |
| Allow password quality configuration on token after initialization | <p>This option determines whether the password quality parameters on the token can be changed after initialization.</p> <p>> Select this option to enable password quality configuration after initialization.</p> |
| Allow only an administrator to configure password quality on token | <p>This option determines whether the password quality parameters on the token can be changed after initialization by the administrator only, and not by the user.</p> <p>NOTE This option is selected by default.</p> <p>> Select one of the following:</p> <ul style="list-style-type: none"> 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. |

| Option | Description |
|---|---|
| Show application tray icon | <p>This options determines whether the SafeNet Authentication Client tray icon can be displayed or not.</p> <p>NOTE The default value of this option is <i>Always</i>.</p> <p>Select one of the following:</p> <ul style="list-style-type: none"> > Never: The tray icon is never displayed. > Always: The tray icon is always displayed. |
| Automatic logoff after token inactivity | <p>You can determine whether tokens are automatically logged off following a period of token inactivity, even if the tokens are still connected. After a token is logged off, the user must enter the token password again before the token contents can be accessed.</p> <p>> Select one of the following:</p> <ul style="list-style-type: none"> • Never- The token password must be entered once, and the token remains logged on as long as it remains connected. • Always- The token password must be entered each time the token contents are accessed. • After- The token password must be entered if the number of minutes set in the text box has passed since the last token activity. <p>Set the number of minutes in the text box (1 - 240).</p> |
| Enabling Logging | <p>The logging function generates logs for SafeNet Authentication Client activities.</p> <p>NOTE You must have administrator privileges to use the logging function.</p> <p>For details, refer to below steps.</p> |

For Windows - The log files are located in: C : \WINDOWS\Temp\eToken.log

To activate the logging function

Perform the following steps:

1. Open **SafeNet Authentication Client Tools > Advanced View**.
Refer to ["Opening the Advanced View" on page 16](#).
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab, and click **Enable Logging**.

NOTE You must restart your machine for the settings to take effect.

To disable the logging feature

Perform the following steps:

1. Open **SafeNet Authentication Client Tools > Advanced View**.
Refer to ["Opening the Advanced View" on page 16](#).
2. In the left pane, select **Client Settings**.

3. In the right pane, select the **Advanced** tab, and click **Disable Logging**.

CHAPTER 7: Working with Common Criteria

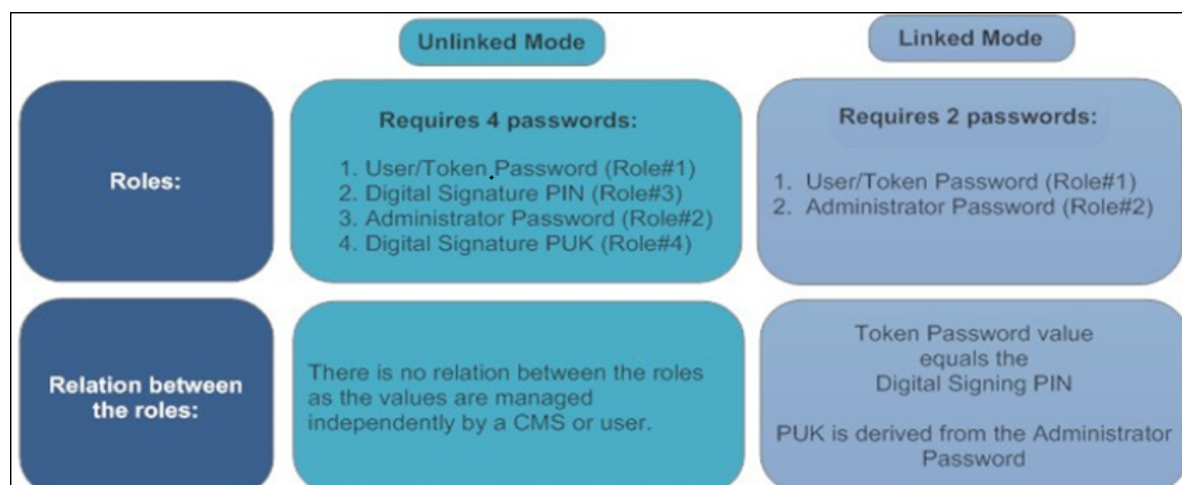
SafeNet Authentication Client (SAC) supports Thales IDPrime Common Criteria (CC) cards range as well as eToken 5110 CC.

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.

For a detailed list of supported cards, refer to *SafeNet Authentication Client Release Notes*.

SAC allows you to work with Common Criteria certified tokens and cards in two modes:

1. Unlinked Mode
2. Linked Mode



Unlinked Mode (4 Passwords)

NOTE Common Criteria devices are set to work in unlinked mode by default.

To work in the unlinked mode, user needs to clear the *Use the same token and administrator passwords for digital signature operation* check-box. For details, refer to ["Initializing IDPrime Devices" on page 53](#).

The following four common criteria device passwords are required in unlinked mode:

1. **Token Password (Role # 1):** Used to perform device write/delete and exchange key operations. The default token password is 4 zero characters "0000".
2. **Digital Signature PIN (Role # 3):** Used to perform Digital Signature operations with Sign only keys (CC keys). The default Digital Signature PIN is 6 zero characters "000000".
3. **Administrator Password (Role # 2):** Used to /unlock a locked token password, or to perform initialization operations. The default administrator password is 48 zeros.

- 4. Digital Signature PUK (Role # 4):** Used to /unlock a locked Digital Signature PIN. The default Digital Signature PUK is 6 zero characters "000000".

NOTE

- If the device is in unlinked mode, the new user password is used for both the *Token Password* and *Digital Signature PIN* when unblocking a device.
- When initializing a device in unlinked mode and the *Token Password Must be changed at first logon* option is selected, both the Token (User) Password and Digital Signature PIN are affected (ensure that both the Token Password and Digital Signature PIN are changed).

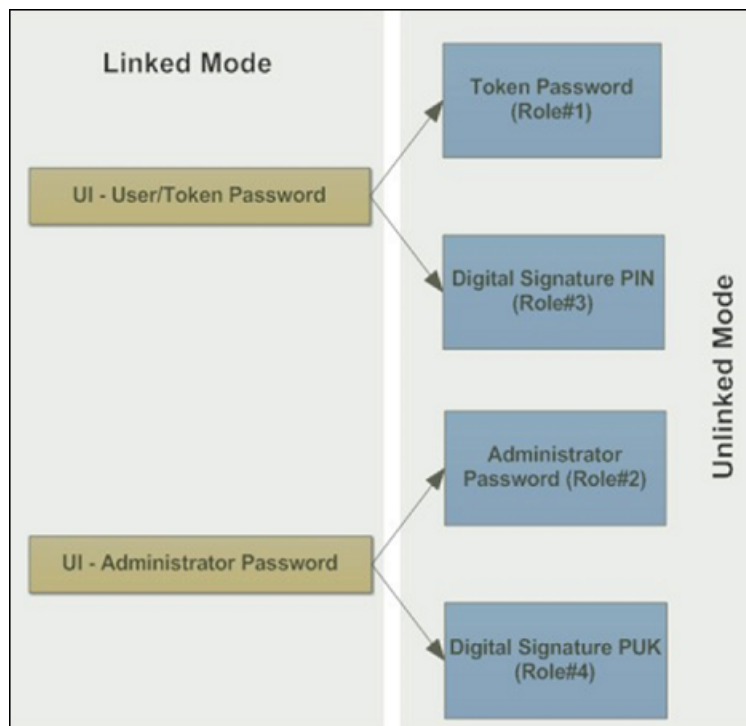
Linked Mode (2 Passwords)

To work in the linked mode, each token/card must be initialized. User needs to select the *Use the same token and administrator passwords for digital signature operation* check-box to perform digital signing operations with only a Token and Administrator password. For details, refer to ["Initializing IDPrime Devices" on page 53](#))

When working in the linked mode, the user enters a Token Password to authenticate both Digital Signature operations (where a Digital Signature PIN is required) and regular token operations (where a Token Password is required).

The user enters the Administrator Password to authenticate operations that require an Administrator Password or Digital Signature PUK.

NOTE If the device is in linked mode, with the default administrator password, the feature is disabled.






Linked Mode PIN Policy Settings

The user password must be compliant with the password quality of the Token Password (Role#1) and the Digital Signature PIN (Role#3). It means the password used as the Token Password must be at least 6 digits long and must also be compliant with the password quality settings of the Token Password (Role#1) and the Digital Signature PIN (Role#3).

The password policy of the Digital Signature PUK (Role#4) must be set to minimum, which means 6 characters long, while other password policies are disabled.

Common Criteria Extended Functions

When in unlinked mode, 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.

The screenshot shows the 'SafeNet Authentication Client' window with the THALES logo. It contains three input fields for PINs: 'Current Digital Signature PIN', 'New Digital Signature PIN', and 'Confirm PIN'. Below these fields, there is instructional text about PIN requirements and the current language setting. At the bottom right, there are 'OK' and 'Cancel' buttons.

SafeNet Authentication Client

THALES

Current Digital Signature PIN:

New Digital Signature PIN:

Confirm PIN:

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

A secure PIN 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 PIN.

OK Cancel

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.


The screenshot shows the 'SafeNet Authentication Client' window with the 'THALES' logo in the top right. The window contains three input fields for PUKs, each with six dots representing masked characters. The first field is labeled 'Current Digital Signature PUK:', the second 'New Digital Signature PUK:', and the third 'Confirm PUK:'. Below the fields, there is instructional text: 'The new PUK must comply with the quality settings defined on the token.' and 'A secure PUK has at least 8 characters, and contains upper-case letters, lower-case letters, numerals, and special characters (such as !, \$, #, %).' At the bottom left, it says 'Current Language: EN'. At the bottom right, there are 'OK' and 'Cancel' buttons.

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.

SafeNet Authentication Client THALES

Enter the Digital Signature PUK:

Token Name: FIDO-940CC

Digital Signature PUK:

Current Language: EN

OK Cancel

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

The **Set PIN** window is displayed.

SafeNet Authentication Client THALES

New Digital Signature PIN:

Confirm PIN:

☐ Token PIN must be changed on first logon

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

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

Current Language: EN

OK Cancel

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**.

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 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, refer to *SafeNet Authentication Client Administrator Guide*.

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.

| Operation | Password required to perform the specified operation on: > eToken 5100 CC (legacy) | Password required to perform the specified operation on: > SafeNet IDPrime 940/3940 > IDPrime 840/840B/3840/3840B > eToken 5110 CC |
|-----------------------------|---|---|
| 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 + Digital Signature PIN |

| Operation | Password required to perform the specified operation on: > eToken 5100 CC (legacy) | Password required to perform the specified operation on: > SafeNet IDPrime 940/3940 > IDPrime 840/840B/3840/3840B > eToken 5110 CC |
|----------------------------------|---|---|
| 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 8: Working with SafeNet eToken 5300

SafeNet eToken 5300 (an IDPrime card) 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 are not 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**.
 - From the Windows taskbar, select **Start > All Programs > SafeNet > SafeNet Authentication Client > SafeNet Authentication Client**.

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

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

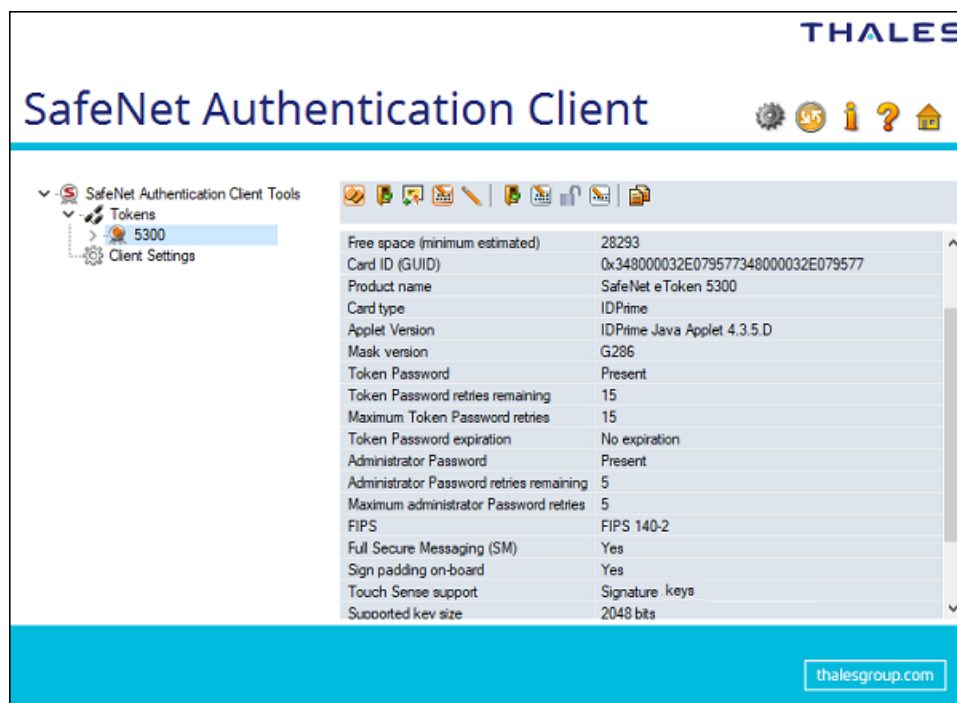
The **SafeNet Authentication Client Tools** window is displayed in the *Advanced View*.

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

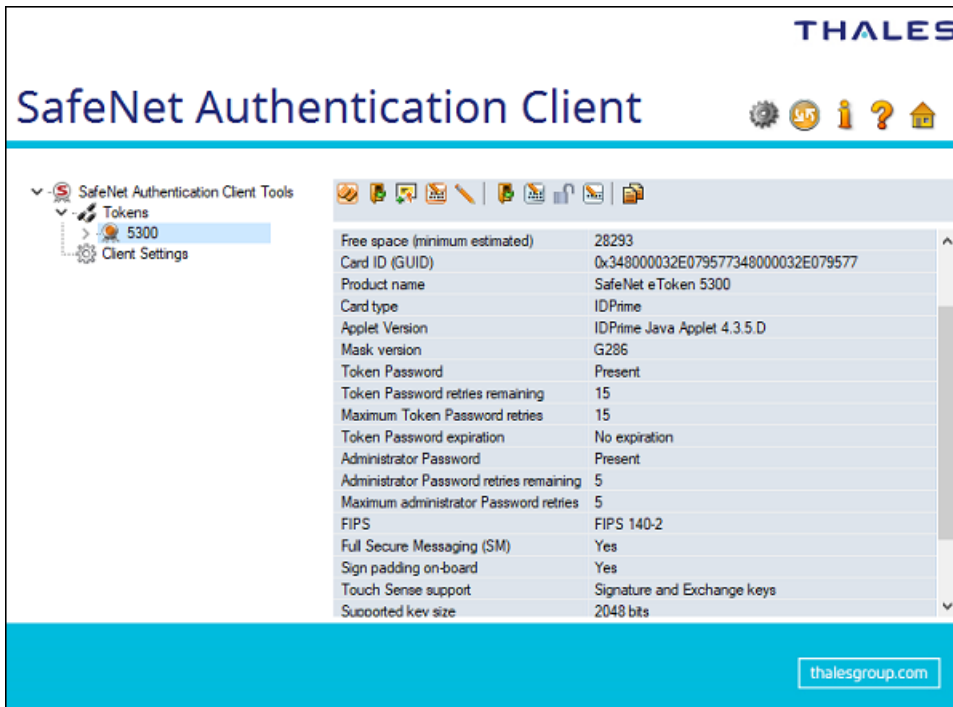
The Token's Information is displayed.

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

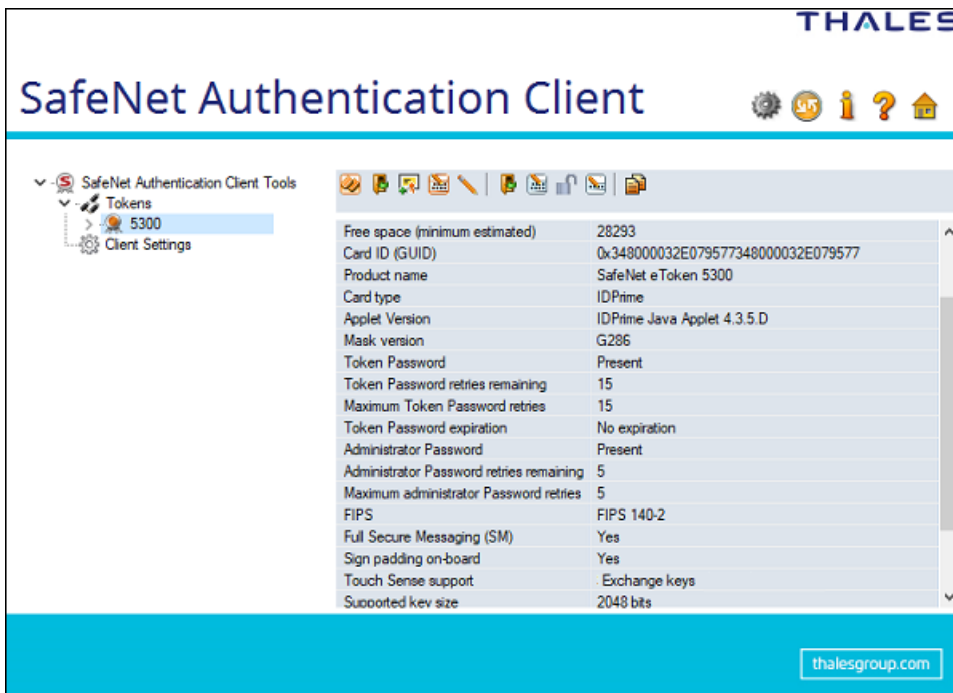
Touch Sense support - Signature Keys



Touch Sense support - Signature and Exchange Keys



Touch Sense support - Exchange Keys



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.

NOTE For more details, refer to the `Touch Sense Notify` property in the *SafeNet Authentication Client Administrator Guide*.

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 9: Working with PIN Pad Readers

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. 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, refer to *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

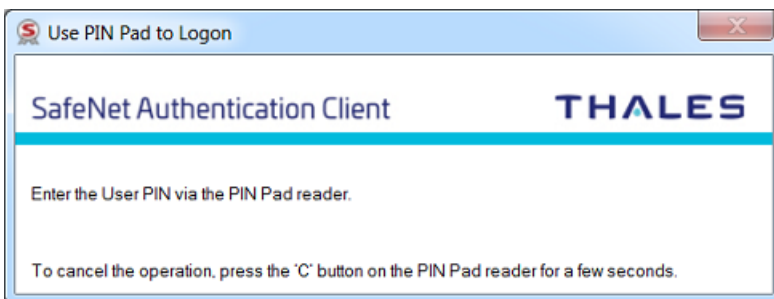
PIN Pad Functions

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

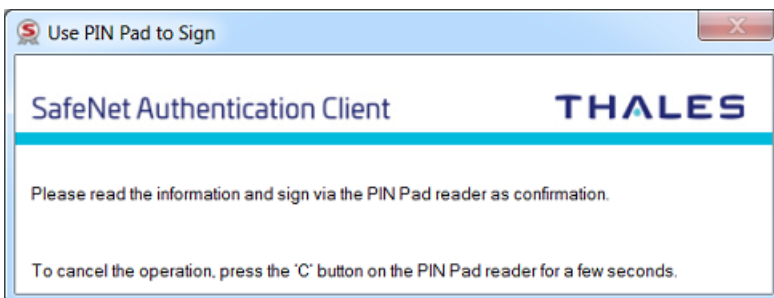
- > Logging on to the token (Refer to ["Logging On to the Token as a User" on page 30](#)).
- > Change PIN (Refer to ["Changing the Token Password" on page 31](#)).
- > Unlock Token by the Challenge-Response Method (Refer to ["Unlocking a Token by the Challenge-Response Method" on page 40](#)).
- > Setting a Token Password by an Administrator (Refer to ["Setting a Token Password by an Administrator" on page 43](#)).

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.

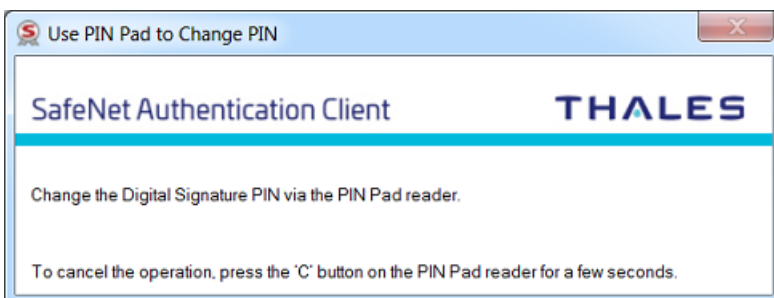
- > When performing a user operation, the following message appears:



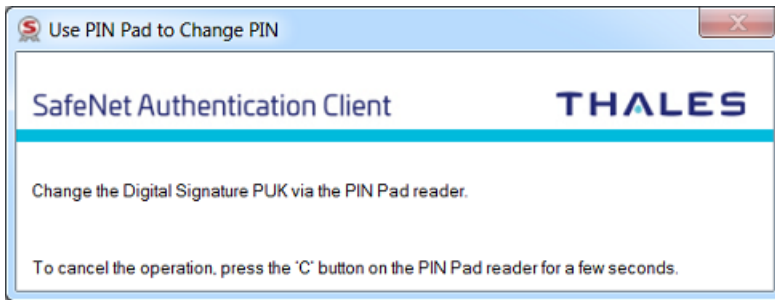
- > When performing a sign operation using a Common Criteria device, the following message appears:



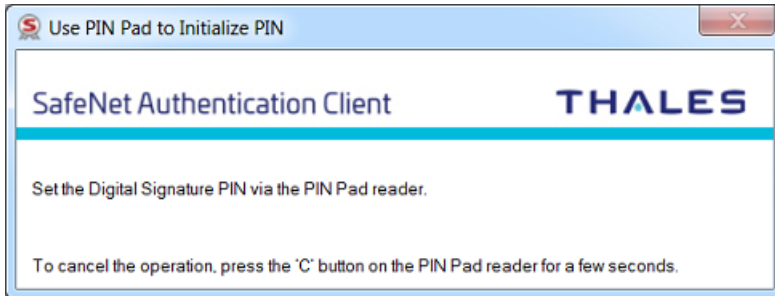
- > When changing a Digital Signature PIN, the following message appears:



- > When changing a Digital Signature PUK, the following message appears:



- > When setting the Digital Signature PIN, the following message appears:



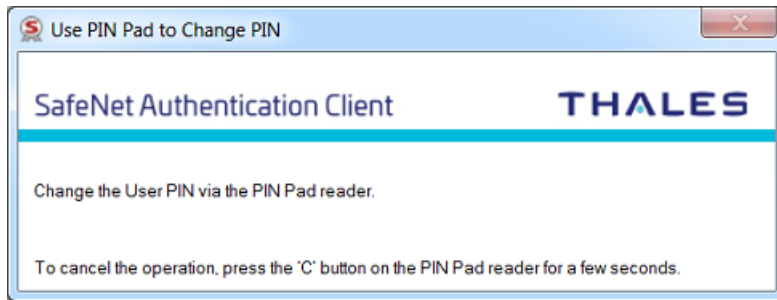
PIN Pad Functional Limitations

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.

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.