SafeNet Authentication Client (Windows)

Version 10.5 (GA)

User Guide

gemalto
security to be free

All information herein is either public information or is the property of and owned solely by Gemalto and/or 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 of Gemalto's information.

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

- The copyright notice below, 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, Gemalto 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, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto 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 Gemalto 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.

Gemalto 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 Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto 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 e functioning could result in damage to persons or property, denial of service or loss of privacy.

© 20010-18 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries 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.

Product Version: 10.5 (GA)

Document Number: 007-013561-005, Rev. A

Release Date: March 2018

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information
Customer Support Portal	https://supportportal.gemalto.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.
Technical Support contact email	technical.support@gemalto.com

Additional Documentation

The following publications are available:

- 007-013560-005 SafeNet Authentication Client 10.5 (GA) Administrator Guide
- 007-013559-007 SafeNet Authentication Client 10.5 (GA) Release Notes (RN) Rev B

Table of Contents

1 Introduction 5
Overview 5
Friendly Admin Password 5

2 SafeNet Authentication Client User Interfaces 7
Overview of SafeNet Authentication Client User Interfaces 7
SafeNet Authentication Client Tray Icon 8
Running the SafeNet Authentication Client Monitor 8
SAC Tray Menu Functions 8
Opening the SafeNet Authentication Client Tray Menu 9
Selecting the Token from the SAC Tray Menu 9
Closing SafeNet Authentication Client Monitor 10
SafeNet Authentication Client Tools 10
SafeNet Authentication Client Tools Toolbar 10
Opening the Simple View 11
Token Icons 13
Simple View Functions 14
Opening the Advanced View 15
Advanced View Functions 16
Tokens Node 16
Selected Token Node 17
Certificate Type Node 18
Common Criteria Certificates 19
ECC Certificates 19
Selected Certificate Node 20
Settings Node 21
Client Settings Node 22
Data Objects Node 22
Orphan Objects Node 23
Using the Virtual Keyboard 24
Validating Binary Signatures 25

3 Using PIN Pad Readers with SAC 27
PIN Pad Readers with IDPrime MD Cards 27
PIN Pad Management Scenarios 27
PIN Pad Functions 28
PIN Pad Functional Limitations 29

4 Token Management 30
Selecting the Active Token 30

Viewing and Copying Token Information 30
Logging On to the Token as a User 31
Renaming a Token 32
Changing the Token Password. 33
Unlocking a Token by the Challenge-Response Method 35
Deleting Token Content 37
Importing a Certificate to a Token. 38
Importing Common Criteria Certificates 39
Exporting a Certificate from a Token 42
Viewing Supported Cryptographic Providers 43
Setting a Certificate as KSP or CSP 44
Setting a Certificate as Default or Auxiliary. 44
Clearing a Default Certificate 45
Deleting a Certificate. 46
Logging On to the Token as an Administrator 46
Changing the Administrator Password 47
Setting a Token Password by an Administrator 48
Synchronizing Passwords. 49
Reader Settings 50

5 Token Initialization 51
Token Initialization Overview 51
Initializing eToken Devices 52
Setting the RSA Key Secondary Authentication Field. 62
Initializing IDPrime Based Devices 64
Initializing IDPrime Based Common Criteria Devices 65
Initializing IDPrime Devices (Non Common Criteria) 71

6 SafeNet Virtual Tokens 75
Overview of SafeNet Virtual Products. 75
Connecting a SafeNet Virtual Token. 75
Disconnecting or Deleting a SafeNet Virtual Token 76
Using a SafeNet Virtual Token to Replace a Lost Token 77
Unlocking a SafeNet Virtual Token 77
Generating a One-Time Password (OTP). 78
Using a SafeNet Virtual Token on an External Storage Device 78
Using an Emulated SafeNet Virtual Token 79

7 Common Criteria 80
Working with Common Criteria Certified Tokens and Cards 80
PKCS#11 Digital Signature PIN Authentication 80
Unlinked Mode (4 Passwords) 81
Unlinked Mode Functions 81
Change Digital Signature PIN 82

Change Digital Signature PUK 83
Set Digital Signature PIN 84
Linked Mode (2 Passwords) 85
Linked Mode PIN Policy Settings 86
Operational Differences and Role Protection 86

8 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

9 SafeNet eToken 7300 91
Introduction to SafeNet eToken 7300 91
SafeNet eToken 7300 Launcher 91
Running the Launcher to Open the Tray Icon on Windows 92
SafeNet eToken 7300 Tray Menu. 92
SafeNet eToken 7300 Tray Menu Functions 93
Using the SafeNet eToken 7300 Tray Icon 93
Selecting the Token from the SafeNet eToken 7300 Tray Menu 93
Closing SafeNet eToken 7300 94
SafeNet eToken 7300 User Storage. 94
Accessing an Unprotected Flash Partition on Windows 94
Accessing a Protected Flash Partition on Windows 94
Partitioning the SafeNet eToken 7300 95

10 Client Settings 96
Setting Password Quality (eToken Devices only). 96
Copying User Certificates to a Local Store 97
Copying CA Certificates to a Local Store 97
Enabling Single Logon 98
Allowing Password Quality Configuration on Token after Initialization (eToken Devices only) 98
Allowing Only an Administrator to Configure Password Quality on Token 99
Showing the SafeNet Authentication Client Tray Icon 99
Defining Automatic Logoff. 100
Enabling Logging 100

11 Token Settings. 101
Setting eToken Password Quality (Password Quality Tab) 101
Setting Private Data Caching Mode (Advanced Tab) 103
Setting RSA Key Secondary Authentication 104
Setting IDPrime PIN Quality (PIN Quality Tab). 105

Setting IDPrime PIN Properties (Advanced Tab) 107

12 Licensing 110

Viewing and Importing Licenses 110

Introduction

SafeNet Authentication Client enables token operations and the implementation of token PKI-based solutions.

Overview

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

SafeNet Authentication Client provides easy-to-use configuration tools for users and administrators..

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

Friendly Admin Password

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

IDGo 800 UI and SAC 10.0 UI require a 48 Hexadecimal PIN to be entered.

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 (Chapter 7: Working with Common Criteria Certified Tokens and Cards (page 80)) 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 10.0 and IDGo 800.

SafeNet Authentication Client User Interfaces

This section describes the SafeNet Authentication Client 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.
- In some installations, the word **Password** is replaced by **PIN** or **Passcode**.
- The term Token in used throughout the document and is application to both Smart Cards and Tokens.

Overview of SafeNet Authentication Client User Interfaces

Administrators use SafeNet Authentication Client Tools to set token policies. 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.

SafeNet Authentication Client provides two user interfaces:

- SafeNet Authentication Client Tray Icon
  - for quick access to several token operations
- SafeNet Authentication Client Tools
  - provides information about each connected token, including its identification and capabilities.
  - can 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 SafeNet Authentication Client tray icon offers a shortcut menu to several token operations.

The SafeNet Authentication Client tray icon is displayed in the Windows taskbar as follows:

No Tokens Connected	One Token Connected	Multiple Tokens Connected

Running the SafeNet Authentication Client Monitor

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

> **NOTE**:
> If SafeNet Authentication Client is open and the tray icon is not displayed in the Windows taskbar, see Chapter 10: *Showing the SafeNet Authentication Client Tray Icon*, on page 99.

To open SafeNet Authentication Client on Windows:

- From the Windows 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 and license information, enables license import and the validation of SAC binary signatures.
- **Token selection:** allows you to select one of the connected tokens to be the active token. This function is available only when more than one token is connected.
- **Change Token Password:** opens the *Change Password* window for the selected token. See Chapter 4: *Changing the Token Password*, on page 33.
- **Unlock Token:** opens the *Token* window for the selected token. See Chapter 4: *Unlocking a Token by the Challenge-Response Method*, on page 35.
- **Certificate Information:** opens the *Token Certificate Information* window for the selected token.
- **Log On to Flash/Log Off from Flash:** displayed when a SafeNet eToken 7300 having a password-protected flash partition is connected. Opens the *Log On to Token* window for the selected token. See Chapter 4: *Logging On to the Token as a User*, on page 31.
- **Exit:** closes SafeNet Authentication Client and the tray icon.

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

- **SAM Agent (Windows):** launches the *SAM Desktop Agent* application. For more information, see the SafeNet Authentication Manager User Guide.
- **Delete Token Content:** removes the deletable data from the selected token.
- **Generate OTP:** generates an OTP on the selected *SafeNet Virtual token*. This function is available only if the selected SafeNet Virtual token is configured to support this function.
- **Synchronize Password (Windows):** Synchronizes your token password with your domain password. Use this feature only when requested by your administrator.

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 which token to work with.

To select from multiple tokens in the tray menu:

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

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

2. Hover the mouse over the required token.

   Options for the selected token are displayed.

3. Select the required option.

Closing SafeNet Authentication Client Monitor

To close SafeNet Authentication Client:

1. Right-click the SafeNet Authentication Client tray icon, and from the shortcut menu, select **Exit**.

   A warning message is displayed.

2. Click **OK**.

SafeNet Authentication Client Tools

Administrators use SafeNet Authentication Client Tools to set token policies. Users use SafeNet Authentication Client Tools to perform basic token management functions, such as changing passwords and viewing certificates on a connected token. In addition, SafeNet Authentication Client Tools provides users and administrators with a quick and easy way to import keys from a computer to a token, and to transfer digital certificates between a computer and a token.

SafeNet Authentication Client Tools allows administrators to initialize tokens according to specific organizational requirements or security modes. It includes a password quality feature that sets parameters to calculate a token password quality rating.

> **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.

SafeNet Authentication Client Tools includes two viewing options:

- **Simple view:** to perform common tasks

  See "Opening the Simple View" on page 11.

- **Advanced view:** for extensive control over SafeNet Authentication Client and your connected tokens

  See "Opening the Advanced View" on page 15.

  Each view displays two panes:

- The left pane indicates which token (*Simple* view) or which object (*Advanced* view) is to be managed.
- 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.

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 *Simple* to the *Advanced* view
	Simple View – switches from the *Advanced* to the *Simple* view

Icon (Cont.)	Action (Cont.)
	Refresh – refreshes the data for all connected tokens
	About – displays product version information, license information, enables license import and the validation of SAC binary signatures
	Help – opens the *Help* feature
	Home – opens the company website

Opening the Simple View

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

To open SafeNet Authentication Client Tools:

Do one of the following:

- Right-click the SafeNet Authentication Client tray icon, and from the shortcut menu, select **Tools**.
- From the Windows taskbar, select **Start > All Programs > SafeNet > SafeNet Authentication Client > SafeNet Authentication Client Tools.**

The *SafeNet Authentication Client Tools* window opens in the *Simple* view.

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

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	
	• SafeNet eToken NG-Flash • SafeNet eToken 7300 • SafeNet eToken 5100/5105 (SafeNet eToken PRO) • SafeNet Virtual Token (without OTP support) • SafeNet eToken 5110	For a full list of supported tokens, see Chapter 1: “Supported Tokens and Smart Cards” on page 6.
	• SafeNet eToken 5200/5205 (SafeNet eToken PRO Anywhere) • SafeNet eToken 7200 (SafeNet eToken NG-Flash Anywhere)	
	• SafeNet eToken NG-OTP • SafeNet Virtual Token (with OTP support)	
	• SafeNet Virtual Temp Token	
	• SafeNet Rescue Token	
	• Smart Card reader – no card connected	
	Smart Card reader – card connected: • SafeNet eToken 5300 • SafeNet eToken 5110 • Gemalto IDPrime MD 840 • Gemalto IDPrime MD 840 B	• Gemalto IDPrime MD 3840 • Gemalto IDPrime MD 3840 B • Gemalto IDPrime MD 830-FIPS For a full list of supported tokens, see the SafeNet Authentication Client Release Notes.
	• Token with corrupted data	
	• 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
Disconnect SafeNet Virtual Token	Disconnects the SafeNet Virtual Token or SafeNet Rescue Token, with an option to also delete it

Opening the Advanced View

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

To open the SafeNet Authentication Client Tools Advanced view:

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

   The *SafeNet Authentication Client Tools* window opens in the *Simple* view.
2. Click the **Advanced View** icon.

   The *SafeNet Authentication Client Tools* window opens 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 Tools Advanced View window.

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 from the shortcut menu.
   - 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, the list of connected tokens is displayed in the right pane, and icons are displayed above them.

The following functions are available:

Function	Icon	Right-Click Menu Item
Reader Settings See Chapter 4: “Reader Settings” on page 50.		Reader Settings
Connect SafeNet Virtual Token See Chapter 6: *Connecting a SafeNet Virtual Token*, on page 75.		Connect SafeNet Virtual Token

Selected Token Node

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

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

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

The following user functions are available:

User Function	Icon	Right-Click Menu Item
Initialize Token See Chapter 5: *Token Initialization*, on page 51.		Initialize Token
Log On to Token See Chapter 4: *Logging On to the Token as a User*, on page 31.		Log On to Token
Import Certificate See Chapter 4: *Importing a Certificate to a Token*, on page 38.		Import Certificate
Change Password See Chapter 4: *Changing the Token Password*, on page 33.		Change Password
Rename Token See Chapter 4: *Renaming a Token*, on page 32.		Rename Token
Disconnect SafeNet Virtual Token (Enabled for SafeNet Virtual Token or SafeNet Rescue Token only) See Chapter 6: *Disconnecting or Deleting a SafeNet Virtual Token*, on page 76.		Disconnect
Copy to Clipboard See Chapter 4: *Viewing and Copying Token Information*, on page 30.		(None)
Change Digital Signature PIN See Chapter 7: Change Digital Signature PIN (page 82)		Change Digital Signature PIN
Change Digital Signature PUK See Chapter 7: Change Digital Signature PUK (page 83)		Change Digital Signature PUK
Set Digital Signature PIN See Chapter 7: Set Digital Signature PIN (page 84)		Set Digital Signature PIN

NOTE:
Depending on the token type, additional options may be displayed in the dropdown 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, enclosed within a border:

See Chapter 4: *Logging On to the Token as an Administrator*, on page 46.

NOTE:
Administrator functions are not supported by iKey devices. The option is available on iKey devices that were initialized using BSec with the keys. After an iKey device is locked the option becomes available.

Certificate Type Node

If the selected token contains certificates, one or two of the following *Certificate Type* nodes are displayed in the left pane under the token's node:

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

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

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

User Function	Icon	Right-Click Menu Item
Import Certificate See Chapter 4: *Importing a Certificate to a Token*, on page 38.		Import Certificate
Reset Default Certificate Selection See Chapter 4: *Clearing a Default Certificate*, on page 45.		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 Gemalto IDPrime MD 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.

NOTE:
Standard Common Criteria devices support only ECC 256. For more information please refer to the IDPrime MD Card Configuration manual.

See Chapter 4: “Importing Common Criteria Certificates” on page 39.

The following devices support CC Certificates:

- SafeNet eToken 5110 CC
- SafeNet eToken 5100 CC
- Gemalto IDPrime MD 840
- Gemalto IDPrime MD 840 B
- Gemalto IDPrime MD 3840
- Gemalto IDPrime MD 3840 B
- Gemalto IDPrime MD 8840 Micro SD Card

ECC Certificates

ECC Certificates are supported by eTokens and Gemalto IDPrime MD cards.

The following devices support ECC Certificates:

- SafeNet eToken PRO Java 72K ECC
- SafeNet eToken 5110, 5110 HID
- Gemalto IDPrime MD 830-FIPS
- Gemalto IDPrime MD 830-ICP
- Gemalto IDPrime MD 830 B
- Gemalto IDPrime MD 3810
- Gemalto IDPrime MD 3810 MIFARE 1K
- Gemalto IDPrime MD 3811

- Gemalto IDPrime MD 840 B
- Gemalto IDCore 30B eToken

Selected Certificate Node

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

Some or all of the following functions are available:

User Function	Icon	Right-Click Menu Item
Delete Certificate See "Deleting a Certificate" on page 46.		Delete Certificate
Export Certificate See "Exporting a Certificate from a Token" on page 42.		Export Certificate
Set as Default See "Setting a Certificate as Default or Auxiliary" on page 44.	(None)	Set as Default.
Set as Auxiliary See "Setting a Certificate as Default or Auxiliary" on page 44.	(None)	Set as Auxiliary.
Copy to Clipboard See "Viewing and Copying Token Information" on page 30.		(None)
Set as KSP / Set as CSP See "Setting a Certificate as KSP or CSP" on page 44.	(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 eToken devices:

- Password Quality
  See Chapter 11: *Setting eToken Password Quality (Password Quality Tab)*, on page 101.
- Advanced
  See Chapter 11: *Setting Private Data Caching Mode (Advanced Tab)*, on page 103

> **NOTE**:
> The *Advanced* tab is not used for iKey devices.

The following tabs exist for IDPrime and eToken 5110 CC devices:

- PIN Quality
  See Chapter 11: *Setting IDPrime PIN Quality (PIN Quality Tab)*, on page 105
- Advanced
  See Chapter 11: *Setting IDPrime PIN Properties (Advanced Tab)*, on page 107

Client Settings Node

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

The changes you make to the *Client Settings* window will affect eToken devices (excluding eToken 5110 CC) that will be initialized using this computer after the changes have been saved.

Like the *Settings* window, the *Client Settings* window contains two tabs:

- Password Quality
- Advanced

See Chapter 10: *Client Settings*, on page 96.

Data Objects Node

Tokens used with Entrust applications have a *Data Objects* node which contains PKCS#11 data objects.

To view the contents of a data object:

1. In the left pane, under the token's 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:

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:

1. In the left pane, under the token's 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:

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

NOTES:
- The virtual keyboard is supported on Windows Operating Systems only.
- 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
- etsapi.dll
- SNSCKSP.dll
- dkck201.dll
- eTokenMD.dll
- axaltocm.dll

> **NOTE**:
> The binary files above will be 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:

IDGo 800 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:

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.
     See "Opening the Advanced View" on page 15.
     On the toolbar, click the **About** icon:

   The *About* window opens.

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.

Using PIN Pad Readers with SAC

This chapter describes the capabilities and limitations of using PIN pad readers with IDPrime cards. A PIN pad reader can be any device that has a keyboard for secure PIN entry, this could for example be 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.

The following cards are supported with PIN Pad readers:

- Gemalto IDPrime MD 830
- Gemalto IDPrime MD 830 B (FIPS level 2)
- Gemalto IDPrime MD 840
- Gemalto IDPrime MD 840 B
- Gemalto IDPrime 3840
- Gemalto IDPrime 3840 B
- Gemalto IDPrime 3810
- Gemalto IDPrime 3811

PIN Pad Readers with IDPrime MD Cards

The following PINs can be External PINs for SAC PKCS#11 and IDGo 800 PKCS#11 libraries (and therefore used with PIN pad readers):

- IDPrime MD 840 and 3840 Cards - Roles 1 and 3
- IDPrime MD 830 and 3810 - Role 1 only

The other PIN roles can be External PINs only for the PKCS#11 libraries.

NOTE:
PIN Pad Readers can be used for Role 3 (Digital Signature PIN) of IDPrime MD cards. Note that the PIN entry will be requested for each signature performed with Role 3 as Role 3 protects Certificates with Non repudiation Key usage.

PIN Pad Management Scenarios

The table below describes the different scenarios for PINs and PIN pad readers:

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

Regular - PIN is entered using the computer keyboard

External - PIN is entered using an external PIN pad reader

Setting the `NoRegularFallback` flag changes the third scenario as follows:

External PIN & Normal Reader - Login refused

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

Regular PIN & PIN Pad Reader - Regular PIN

PIN Pad Functions

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

- Logging on to the token (See Chapter 4: Logging On to the Token as a User (page 31))

- Change PIN (See Chapter 4: Changing the Token Password (page 33))

- Unlock Token by the Challenge Response Method (See Chapter 4: Unlocking a Token by the Challenge-Response Method (page 35))

- Setting a Token Password by an Administrator (See Chapter 4: Setting a Token Password by an Administrator (page 48))

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

PIN Pad Functional Limitations

The following functional limitations exist with the PIN pad:

- 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 (i.e. EZIO Bluetooth and EZIO BLE) have their own 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.

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 Tools window:

1. Open SafeNet Authentication Client Tools.
   See Chapter 2: *Opening the Simple View*, on page 11 or *Opening the Advanced View* on page 15.
2. In the left pane, select the required token.

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

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

   The SafeNet Authentication Client tray menu opens.
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

To view and copy token information:

1. To use the *Simple* view to view token information, do the following:
   a. Open SafeNet Authentication Client Tools Simple view.
      See "Opening the Simple View" on page 11.
   b. In the left pane, select the required token.
   c. In the right pane, select **View Token Info**.
   d. Continue with step 3.
2. To use the *Advanced* view to view token information, do the following:
   a. Open SafeNet Authentication Client Tools *Advanced* view.
      See "Opening the Advanced View" on page 15.
   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.

> **NOTE**:
> The *Unblocking Codes retries remaining* field for iKey devices is displayed only when the token is locked.

4. To copy the token information to the clipboard, do one of the following:
   - In the *Token Information* window, click **Copy**.
   - In *Advanced* view, click the **Copy to Clipboard** icon:
5. To paste the copied token information, click the cursor in the target application, and paste the information.
6. Click **OK**.

Logging On to the Token as a User

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

To log on as a user:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.

> **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** from the shortcut menu.
3. The *Token Logon* window opens.

4. 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, we recommend assigning each one a unique token name.

To rename a token:

1. To use the *Simple* view to rename a token, do the following:
   a. Open SafeNet Authentication Client Tools *Simple* view.
   See "Opening the Simple View" on page 11.
   b. In the left pane, select the required token.
   c. In the right pane, select **Rename Token**.
   d. Continue with 3 below.
2. To use the *Advanced* view to rename a token, do the following:
   a. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
   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** from the shortcut menu.
   c. Continue with step 3 below.

   The *Token Logon* window opens.
3. Enter the token password, and click **OK**.

   The *Token Rename* window opens.
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

TIP:
The term *Token Password* may be replaced by another term (for example, *Token PIN*), depending on your SafeNet Authentication Client configuration.

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

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

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

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

NOTE:
The token password is an important security measure in safeguarding your company's private information. The best passwords are at least eight characters long, and include upper- and lower-case letters, special characters such as punctuation marks, and numbers appearing in a random order. We recommend against using passwords that can be easily discovered, such as names or birth dates of family members.

To change a Token's Password:

1. To use the *Simple* view to change the token password, do the following:
   a. Open SafeNet Authentication Client Tools *Simple* view.
   See "Opening the Simple View" on page 11.
   b. In the left pane, select the required token.
   c. In the right pane, select **Change Token Password**.
   d. Continue with step 4.
2. To use the *Advanced* view to change the token password, do the following:
   a. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
   b. Do one of the following:
      - In the left pane, select the node of the required token.

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

3. To use the tray menu to change the token password, do the following:
   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.
4. The *Change Password* window opens.

5. 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.

6. Enter a new token password in the *New Token Password* and *Confirm Password* fields.
7. Click **OK**.

   A message confirms that the token password was changed successfully.
8. 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, including SafeNet Virtual 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 IDPrime MD CC devices (IDPrime MD CC 840/3840) and eToken 5110 CC:
- If the device is in linked mode, the new user password is used for both the token password and Digital Signature PIN when unblocking a device.
- If the device is in linked mode, with the default administrator password, the feature is disabled.

SafeNet Rescue Token devices cannot be unlocked.

CAUTION:
The administrator can limit the number of times that a token can be unlocked. If this number is exceeded, the token becomes unusable.
This feature is available only for:
- Software tokens (for example: eToken Virtual)
- Legacy iKey profiles - not managed by SAM and based on SO PIN derivation

It is not supported by eToken based devices (nor by IDPRime).

When the administrator has access to the user's token, the administrator can unlock the token using the *Set Token Password* feature.
See Chapter 4: *Setting a Token Password by an Administrator*, on page 48.

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:
In SafeNet Authentication Client version 8.2 (standard mode) and later, the Challenge-Response unlock method supports both SafeNet eTokens and SafeNet iKey devices.

To unlock a token using the Challenge-Response method:

1. To use the *Simple* view to unlock a token, do the following:
   a. Open SafeNet Authentication Client Tools *Simple* view.
   See "Opening the Simple View" on page 11.
   b. In the left pane, select the required token.
   c. In the right pane, select **Unlock Token**.
   d. Continue with step 4.
2. To use the *Advanced* view to unlock a token, do the following:

a. Open SafeNet Authentication Client Tools *Advanced* view.
See "Opening the Advanced View" on page 15.

b. Do one of the following:
   - In the left pane, select the node of the required token.
     In the right pane, click the **Unlock** icon.
   - In the left pane, right-click the node of the required token, and select **Unlock** from the shortcut menu.

c. Continue with step 4.

3. To use the tray menu to change the token password, do the following:
   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 opens, displaying a value in the *Challenge Code* field.
   The *Challenge Code* is 16 characters or, if the token was initialized as Common Criteria, 13 characters.

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

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

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

6. The administrator provides you with the *Response Code* to be entered.
   The *Response Code* is 16 characters or, if the token was 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 Token Password* and *Confirm Password* fields.
8. If the new password is known to others and must be changed, select **Token Password must be changed on first logon**.
9. Click **OK**.

   A message confirms that the token was unlocked successfully.

10. Click **OK**.

Deleting Token Content

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

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

The *Delete Token Content* function is less comprehensive than the *Initialize* function which restores a token to its initial state, removing all objects stored on the token since manufacture and resetting the token password.
See Chapter 5: *Token Initialization*, on page 51.

To delete the token content:

1. To use the *Simple* view, do the following:
   a. Open SafeNet Authentication Client Tools *Simple* view.
      See "Opening the Simple View" on page 11.
   b. In the left pane, select the required token.
   c. In the right pane, select **Delete Token Content**.
   d. 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.
3. The *Token Logon* window opens.
4. Enter the token password, and click **OK**.

   The *Delete Token Content* window opens, prompting you to confirm the delete action.

5. To continue with the delete process, click **OK.**

   The *Delete Token Content* window opens, confirming that the token content was deleted successfully.

6. 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.

> **NOTE**:
> It is not possible to import a certificate to a SafeNet Rescue Token.

To import a certificate:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
2. Do one of the following:
   - In the left pane, select the node of the required token.

     In the right pane, click the **Import Certificate** icon:
   - In the left pane, right-click the node of the required token, and select **Import Certificate** from the shortcut menu.
3. The *Token Logon* window opens.
4. Enter the token password, and click **OK**.

   The *Import Certificate* window opens.

5. Select one of the following:
   - Import a certificate from my personal certificate store
   - Import a certificate from a file

> **NOTE**:
> Importing a certificate from my personal certificate store is applicable only to Windows operating systems.

6. 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 to 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

7. If you select **Import a certificate from a file**, the *Certificate Selection* window opens.

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

8. If the certificate requires a password, the *Password* window opens.

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

9. If the certificate is a Common Criteria certificate, the *Import PIN* window opens.

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

   The default value is **1234567890**.

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

Importing Common Criteria Certificates

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

To import a common criteria certificate:

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

      In the right pane, click the Import Certificate

   b. In the left pane, right-click the node of the required token, and select **Import Certificate** from the shortcut menu.
3. The **Token Logon** window opens.

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

   The **Import Certificate** window opens.

5. Select one of the following:
   a. Import a certificate from my personal certificate store
   b. Import a certificate from a file
6. 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 to 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
7. If you select Import a certificate from a file, the Certificate Selection window opens.
8. Select the certificate to import, and click **Open**.

   The **Certificate Password** window opens.

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

   The **Digital Signature Logon** window opens

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

10. Enter the **Digital Signature PIN** and click **OK**.
11. The certificate is imported, and a message confirms that the import was successful.
12. Common Criteria certificates are displayed as follows in the left pane:

Exporting a Certificate from a Token

To export a certificate:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
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** from the shortcut menu.

   The *Save As* window opens.
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.

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.

To see which Cryptographic Providers are supported on the token:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
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.

To set the certificate as KSP or CSP:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
2. In the left pane, expand the node of the required token.
3. Right-click the required certificate, and from the shortcut menu, select **Set as CSP** or **Set as KSP**.

   The *Token Logon* window opens.
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.

> **NOTE**:
> iKey does not support Auxiliary certificates. It treats an Auxiliary certificate as a Default certificate.

Setting	Description	Scenario
Default	Smart card logon uses the certificate defined as the *Default*. In most Microsoft applications, smart card logon is used.	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: • 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 (Cont.)	Scenario (Cont.)
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:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
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*.

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.

To clear a Default certificate:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
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** from the shortcut menu.
4. The *Reset Default Certificate Selection* window opens, confirming that the Default certificate has been reset.
5. Click **OK**.

Deleting a Certificate

To remove a certificate from a token, follow the procedures below:

To delete a certificate from a token:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
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** from the shortcut menu.
4. The *Delete Certificate* window opens.
5. To delete the certificate, click **Yes.** The *Token Logon* window opens.
6. Enter the token password, and click **OK**.

   The *Delete Certificate* window opens, confirming that the certificate was deleted successfully.
7. Click **OK.**

Logging On to the Token as an Administrator

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

NOTE:
- IDPrime devices have a built-in administrator role.
- iKey devices do not support administrator functions.

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 (*not supported by iKey devices)
- *Setting a Token Password by an Administrator*
- *Unlocking a Token by the Challenge-Response Method (*not supported by iKey devices)
- *Setting eToken Password Quality (Password Quality Tab)*
- *Setting IDPrime PIN Properties (Advanced Tab)*
- *Setting RSA Key Secondary Authentication*

To log on to a token as an administrator:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
2. Do one of the following:
   - In the left pane, select the node of the required token.
     In the right pane, click the **Log On as Administrator** icon.
   - In the left pane, right-click the node of the required token, and select **Log On as Administrator** from the shortcut menu.
3. The *Administrator Logon* window opens.
4. 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.

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** from the shortcut menu.

   The *Change Administrator Password* window opens.
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.
4. Enter the new password in the *New Administrator Password* and *Confirm Password* fields.
5. Click **OK**. A message confirms that the password was changed successfully.
6. Click **OK**.

Setting a Token Password by an Administrator

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

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

To unlock a token by setting a new Token Password:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
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** from the shortcut menu.

   The *Administrator Logon* window opens.
3. Enter the Administrator Password, and click **OK**. The *Set Token Password* window opens.
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 was 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 (See 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.

To synchronize passwords:

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

   The SafeNet Authentication Client tray menu opens.

2. Select **Synchronize Password.**

   The *Synchronize Passwords* window opens.

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.

Reader Settings

A token is connected to a reader when one of the following occurs:

- A token is physically inserted into a USB port
- A SafeNet Virtual Token is connected
- A smart card is physically inserted into a reader

During the default installation of SafeNet Authentication Client, the following numbers of virtual readers are installed on the computer:

- 2 SafeNet eToken readers
- 2 iKey readers
- 1 virtual reader for SafeNet Virtual Token smart card emulation
- 2 SafeNet Virtual Token slots

The number of readers defined on the computer determines the maximum number of these types of tokens that can be recognized upon connection.

The number of virtual SafeNet eToken readers and SafeNet Virtual Token slots for a computer can be changed by a user with local administrator rights on that computer.

> **NOTE**:
> If SAC is already installed, the number of iKey readers can be configured during installation via the command line.

To change the number of readers:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
2. Do one of the following:
   - In the left pane, select the **Tokens** node.

     In the right pane, click the **Reader Settings** icon:
   - In the left pane, right-click the **Tokens** node, and select **Reader Settings** from the shortcut menu.

   The *Reader Settings* window opens.

3. Set the required number of virtual hardware or software readers in the appropriate field.

   The default numbers of available readers are:

   - SafeNet eToken readers: 2
   - SafeNet Virtual Token slots: 2
4. Click **OK** to close the window.

   The number of available readers is changed.
5. Restart SafeNet Authentication Client Tools to make the changes effective.

Token Initialization

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

> **NOTE**:
> You cannot use SafeNet Authentication Client to initialize a SafeNet Virtual product.

Token Initialization 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 MD 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) - not supported by iKey devices
- Maximum number of logon failures allowed
- Requirement to change the token password on the first logon
- Initialization key - not supported by IDPrime MD cards
- All user-generated data, such as certificates and profiles

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

Initializing eToken Devices

NOTE:
- Depending on the type of token being initialized, certain settings may not be enabled.
- If a customized version of SafeNet Authentication Client is installed, the graphics you see may be different from those displayed in this guide.
- To initialize an eToken 5110 Common Criteria device, see *Initializing IDPrime Based Common Criteria Devices* on page 65

To initialize an eToken device:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
2. Do one of the following:
   - In the left pane, select the node of the required token.

     In the right pane, click the **Initialize Token** icon:
   - In the left pane, right-click the node of the required token, and select **Initialize Token** from the shortcut menu.

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

NOTE:
Initializing a token deletes all objects that were created on the device, while it was in use.

3. Select either 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 all token policies and settings.

The *Password Settings* window opens.

4. Enter the following:

Token Name	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.
Logon retries before token is locked	Enter the number of times a token password can be entered incorrectly before the token is locked. **Note:** The retry counter will count only passwords that have a valid length.
Token password must be changed on first logon	If required, select token password must be changed on first logon.

Create Administrator Password	Select Create Administrator Password and enter a New Administrator Password. The minimum password length on an eToken device is 8 characters. **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. • iKey tokens do not support Administrator Passwords.
Confirm Password	Re-enter the administrator password.
Logon retires before token is locked	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
One-factor logon	Configures the token without a password. The default value for this setting is **disabled**. **Note:** • Selecting the One-factor logon option disables the Create Token Password and Create Administrator Password fields. • The One-factor logon feature is used by eToken device only.

5. Click **Next**.

   The *Password Quality Settings* window opens.

6. Complete the fields as follows:

Field	Description
Enforce password quality settings (recommended)	Select this option if you want to define password quality settings when initializing a token. When selected, all options in the window become available.
Minimum length (characters)	Default: 6 characters
Maximum length (characters)	Default: 16 characters
Minimum usage period (days)	The minimum period before the password can be changed. Default: 0 (none) For iKey devices, the periods are rounded up to periods of weeks (7 days), even though the period is displayed in days. For example, if the period is displayed as less than a week, say 6 days, iKey regards it as a week. If the period is more than two weeks, say 15 days, iKey regards it as three weeks.
Maximum usage period (days)	The maximum period, in days, before which the password must be changed. Default: 0 (none) For iKey devices, the periods are rounded up to periods of weeks. See row above for more information.
Expiration warning period (days)	Defines the number of days before the password expires that a warning message is shown. Default: 0 (none)
History size	Defines how many previous passwords must not be repeated. Default: For eToken devices - 10 For iKey devices - 6
Maximum consecutive repetitions	The maximum number of repeated characters that is permitted in the password. Default: 3 This feature is not supported by iKey devices.
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.

Field (Cont.)	Description (Cont.)
Manual Complexity Rules	For each of the character types (**Upper-case letters, Lower-case letters, Numerals** 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. **Note:** The **Forbidden** option is not supported by iKey devices.

7. Click **Next**.

   If the device is FIPS or Common Criteria, the *FIPS and Common Criteria Settings* window opens.

   If the device is not FIPS or Common Criteria, this window will not be displayed.

   Use this window to configure certification and common criteria settings.

8. Enter the following:

Field	Description
Enforce FIPS settings	Check this options to define FIPS settings. **FIPS:** Federal Information Processing Standards is a U.S. government-approved set of standards designed to improve the utilization and management of computer and related telecommunication systems
Enforce Common Criteria settings	Check this options to define Common Criteria settings. When selected, the Certificate Import Password and maximum number of certificates for which to reserve space on the token can be set. **Common Criteria:** an international standard for computer security certification.

New Import Password	Enter a New Import Password. Defines the Password that must be entered when a Common Criteria certificate is imported to the token. The minimum Password length is 4 characters. The default value is: **1234567890**.
Confirm Password	Re-enter the password entered above.
Set the maximum number of common criteria certificates to be stored:	
Certificates with 1024-bit keys	To reserve adequate space on the token, set the maximum number of Common Criteria certificates with 1024-bit keys that will be imported to the token. Select a number within the range 0 -16.
Certificates with 2048-bit keys	To reserve adequate space on the token, set the maximum number of Common Criteria certificates with 2048-bit keys that will be imported to the token. Select a number within the range 1- 16.

9. Click **Next**.

   The *Optional Cryptography Settings* window opens.

   Use this window to configure Cryptography and RSA Authentication Settings.

10. Under *Optional cryptography mechanism*, complete the fields as follows:

Field	Description
OTP Support	Default: disabled Select to enable OTP support (on compatible tokens).
2048-bit RSA key support	Default: enabled Select to enable 2048-bit RSA key support (on compatible tokens).
Private data caching	Default: Always (fastest) 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. Select one of the following options: • 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.
RSA key secondary authentication	Default: Never An authentication password may be set for an RSA key. Depending on how this option is set, in addition to having the token and knowing its token password, accessing the RSA key may require knowing the password set for that particular key. Having a password for the key is known as *secondary authentication*. Select one of the following: • Always • Always prompt user • Prompt user on application request • Never • Token authentication on application request For an explanation of these options, see *Setting the RSA Key Secondary Authentication Field* on page 62. If the token was initialized as Common Criteria and the secondary authentication *Always*, *Always prompt user* or *Prompt upon application request*, then the secondary authentication setting cannot be changed to *Never* or *Token authentication on application request*. This limitation applies to Common Criteria certificates only.
Manually set the number of reserved RSA keys	Default: disabled Set the number of reserved RSA keys to reserve space in the token memory. This ensures that there will always be memory available for keys.

11. Click **Next**.

    The *Initialization Key Settings* window opens.

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 will be required to open the *Initialization Key* window and enter the correct key during future initialization of the token.

12. Under *Default Initialization Key*, complete the fields as follows:

Field	Description
Use default initialization key	Select this option if the Initialization Key was not changed from its default during the previous token initialization. The factory-set default is used as the key for the current token initialization.
Use this initialization key	Enter the Initialization Key configured in the *This Value* field during the previous token initialization.
Change the key for the next initialization to:	• **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 *Use this Initialization Key* field.

NOTE:
The initialization key minimum length is 4.

13. Click **Next**.

    The *eToken 7300 Partitioning Settings* window opens.

Use this window to partition your SafeNet eToken 7300 device's flash storage area. The partitioning process allows you to do the following:

- Divide the flash drive into a DVD partition and a user storage partition
- Configure the flash drive partitioning settings

The partitioning process can take several minutes. After entering your token's *Administrator Password* to begin the partitioning process, do not disconnect your token until a confirmation message is displayed.

NOTE:
To enable the use of the SafeNet eToken 7300 flash tray icon, ensure that the ISO file or other content written to the DVD partition includes the contents of the SafeNet default ISO file.

Either one of the following can be performed on the SafeNet eToken 7300:

- **Partition without initialization**: Replace the flash drive's DVD partition and user storage partition.
- **Initialize and partition**: Before the partition process is run, the data is deleted from the smart card and new data is written to it.

NOTE:
- The SafeNet eToken 7300 initialization process always initializes the smart card and partitions the flash drive.
- If partitioning settings are not set before the initialization proceeds, the default partitioning settings are used.

14. Under *DVD Partition*, complete the fields as follows:

Field	Description
DVD Source	Select one of the following: • **None:** DVD is not partitioned, options are disabled • **Burn SafeNet default ISO file:** burns the SafeNet default ISO file located in the SAC folder • **Burn ISO file:** burns an ISO file located elsewhere on the computer • **Copy from folder:** copies an entire folder from the computer • **Copy from ROM drive:** copies files from the selected CD ROM drive

15. Under *Protection*, complete the fields as follows:

    The Protection area determines the token content's security level.

Field	Description
Repartitioning	Password-protection requirements for future partitioning.
User Storage	Select the password requirements for accessing the user storage.

NOTE:
For future partitioning without initialization to be password-protected, the token must be initialized with an Administrator Password.

16. Under *Size*, the following fields are displayed, and may not be edited:

Field	Description
Total flash	Total size of the flash memory (DVD + user storage).

17. Under *Allow Boot*, complete the fields as follows:.

Field	Description
From DVD partition	Select to load contents from DVD partition when the SafeNet eToken 7300 device is connected.
From user storage partition	Select to load contents from user storage partition when the SafeNet eToken 7300 device is connected.

18. Click **Finish**. The *Initialize Token Notification* window opens.

NOTE:
The partitioning process can take several minutes. Do not disconnect the token until a confirmation message is displayed.

19. Click **OK**.

NOTE:
If a Microsoft Windows message opens prompting you to format the disk, click **Cancel**.

When the partitioning process is complete, a confirmation message is displayed.

Setting the RSA Key Secondary Authentication Field

The following table explains the options for the RSA key secondary authentication setting.

> **NOTE**:
> This feature is available on eToken device only.

<table>
<tr><th>Setting</th><th colspan="3">Description</th></tr>
<tr><td rowspan="2">Always</td><td colspan="3">Every time an RSA key is generated, the user is prompted to create a secondary password for accessing the key.</td></tr>
<tr><td colspan="2">If the user clicks OK, the RSA key is generated, and the password entered becomes the new key's secondary password.
When using the certificate, the user must authenticate once using the token password. For each operation that requires the RSA key, the user must authenticate using the secondary password.</td><td>If the user clicks Cancel, RSA key generation fails.</td></tr>
<tr><td rowspan="2">Always prompt user</td><td colspan="3">Every time an RSA key is generated, the user is prompted to create a secondary password for accessing the key.</td></tr>
<tr><td colspan="2">If the user clicks OK, the RSA key is generated, and the password entered becomes the new key's secondary password.
When using the certificate, the user must authenticate once using the token password. For each operation that requires the RSA key, the user must authenticate using the secondary password.</td><td>If the user clicks Cancel, the RSA key is generated without a secondary password.
When using the certificate, the user must authenticate once using the token password. No additional authentication is required for operations that require the RSA key.</td></tr>
<tr><td rowspan="2">Prompt user on application request</td><td colspan="2">When using an RSA key generation application that requires secondary passwords for strong private key protection (such as Crypto API with a user-protected flag, or the PKCS#11 CKA_ALWAYS_AUTHENTICATE attribute), the user is prompted to create a secondary password for accessing the RSA key.</td><td rowspan="2">When using applications that do not require secondary passwords for strong private key protection, the RSA key is generated without a secondary password.
When using the certificate, the user must authenticate once using the token password. No additional authentication is required for operations that require the RSA key.</td></tr>
<tr><td>If the user clicks OK, the RSA key is generated, and the password entered becomes the new key's secondary password.
When using the certificate, the user must authenticate once using the token password. For each operation that requires the RSA key, the user must authenticate using the secondary password.</td><td>If the user clicks Cancel, RSA key generation fails.</td></tr>
</table>

Setting	Description	
Never	Secondary passwords are not created for new RSA keys. When using the certificate, the user must authenticate once using the token password. No additional authentication is required for operations that require the RSA key.	
Token authentication on application request	Secondary passwords are not created for new RSA keys. When using the certificate, the user must authenticate once using the token password.	
	When using an RSA key generated by an application that requires secondary passwords for strong private key protection (such as Crypto API with a user protected flag, or the PKCS#11 CKA_ALWAYS_AUTHENTICATE attribute), the user must authenticate using the token password for each operation that requires the RSA key.	When using an RSA key that was not generated by an application that requires secondary passwords for strong private key protection, no additional authentication is required for operations that require the RSA key.

Initializing IDPrime Based Devices

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

The following can be performed during the initialization process:

- All user-generated data, such as certificates and profiles
- All PKCS#11 objects that were created on the token/card, while in use
- Token/card name/label
- Define a user and administrator password (the user password must be according to the card's policy settings).
- Define password quality settings
- Define a Digital Signature PIN and Digital Signature PUK password the password must be according to the card's policy settings (for IDPrime CC and eToken 5110 CC devices). See Chapter 7: Set Digital Signature PIN (page 84)

NOTE:

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

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

Initializing IDPrime Based Common Criteria Devices

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

To initialize an IDPrime based Common Criteria certified device (eToken 5110 CC /IDPrime MD Common Criteria):

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

      In the right pane, click the Initialize Token icon .
   b. In the left pane, right-click the node of the required device, and select Initialize Token from the shortcut menu.

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

3. Select 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 all token policies and settings. Selecting this option will allow you 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 opens. This window requires you to enter an **Administrator Password** and a **Digital Signature PUK** to begin the initialization process.

NOTE:
- Gemalto IDPrime MD cards that are Common Criteria certified, are in unlinked mode by default.
- The procedures and screens described in this section are based on the fact that your IDPrime MD token/card is being used for the first time.

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

The above window is displayed if your device is in linked mode.

5. Enter the current Administrator Password and current Digital Signature PUK. The default Administrator Password is 48 zeros. The default Digital Signature PUK is 6 zeros.

   Enter the following:

Use factory default administrator password	• Select this check-box if the current administrator password is 48 0's. If selected, the Administrator Password field 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	• Select this check-box if the current digital signature PUK is 6 zeros (000000). If selected, the Digital Signature PUK 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 opens.

7. Enter the following:

Token Name	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	The default password: 1234567890 automatically appears in this field. **Note:** If the device is initialized with the default token/card password, and standard password quality requirements are in effect, the user must select the Token Password must be changed on first logon option. Otherwise the initialization will fail because the default password does not meet the password quality requirements. If the token password must be changed on first logon option is selected, the initialization will succeed and the user will be prompted to create a new password when next logging on with the token/card. The user will be required to set a token password that meets the Password Quality requirements configured in the Settings window.
Confirm Password	The default password: 1234567890 automatically appears in this field. If the above field was changed, then re-enter the password entered in the 'New Token Password' field.
Logon retries before token is locked	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.

Token password must be changed on first logon	If required, select token password must be changed on first logon. **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).
PIN Policy	Enables you to set PIN Quality/Property parameters. See Chapter 11: Setting IDPrime PIN Quality (PIN Quality Tab) (page 105) and Chapter 11: Setting IDPrime PIN Properties (Advanced Tab) (page 107)
Create Administrator Password	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). See Chapter 1: Friendly Admin Password (page 5).
Confirm Password	Re-enter the administrator password.
Keep the current administrator password	Select this if you want to keep the current administrator password. **Note:** If this option is selected, the following warning message appears: If the current password is the default password (48 0's), it is strongly recommended to update the administrator password to keep your token secure.

8. Click **Next**.
   The **IDPrime Common Criteria Settings** window opens.
   The IDPrime Common Criteria Settings window 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 IDPrime Common Criteria Settings window defines whether you are going to work in linked or unlinked mode.

9. To work in linked mode, enter the following:

Use the same token and administrator passwords for digital signature operation	Select this option to perform digital signing operations using your current Token and Administrator passwords. **Note:** Selecting this option does not require entering a Digital Signature PIN and Digital Signature PUK. The fields below will be unavailable.

10. To work in unlinked mode, enter the following:

New Digital Signature PIN	Enter a New Digital Signature PIN. This option allows you to work in 'unlinked' mode.
Confirm PIN	Re-enter the New Digital Signature PIN.
PIN Policy	Enables you to set PIN Quality/Property parameters. See Chapter 11: Setting IDPrime PIN Quality (PIN Quality Tab) (page 105) and Chapter 11: Setting IDPrime PIN Properties (Advanced Tab) (page 107)
New Digital Signature PUK	Enter a New Digital Signature PUK. This option allows you to work in 'unlinked' mode.

Confirm PUK	Re-enter the New Digital Signature PUK.
PIN Policy	Enables you to set PIN Quality/Property parameters. See Chapter 11: Setting IDPrime PIN Quality (PIN Quality Tab) (page 105) and Chapter 11: Setting IDPrime PIN Properties (Advanced Tab) (page 107)

11. Click **Finish**. A warning message is displayed.
12. Click **OK** when the warning message: **The token initialization process will delete all token content and reset all token parameters** appears.

    The T**oken initialized successfully** message is displayed.

Initializing IDPrime Devices (Non Common Criteria)

IDPrime cards that are not Common Criteria certified can be initialized using SAC Tools.

To initialize an IDPrime card that is non Common Criteria:

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

      In the right pane, click the Initialize Token icon .
   b. In the left pane, right-click the node of the required device, and select Initialize Token from the shortcut menu.

The *Initialization Options* window opens, allowing you to select how to initialize the device

.

3. Select 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 all token policies and settings. Selecting this option will allow you to: • Create a token password • Create an administrator password • Enter the default token and administrator passwords

4. Click **Next**.
The **Administrator Logon** window opens. This window requires you to enter an **Administrator Password**.

5. Enter the current Administrator Password. The default Administrator Password is 48 zeros.
Enter the following:

Use factory default administrator password	• Select this check-box if the current administrator password is 48 0's. If selected, the Administrator Password field 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.

6. Click **Next**.
   The **Password Settings** window opens.

7. Enter the following:

Token Name	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	The default password on an eToken device is 1234567890 automatically appears in this field. The default password on an IDPrime MD card is 4 zeros (0000) **Note:** If the device is initialized with the default token/card password, and standard password quality requirements are in effect, the user must select the Token Password must be changed on first logon option. Otherwise the initialization will fail because the default password does not meet the password quality requirements. If the token password must be changed on first logon option is selected, the initialization will succeed and the user will be prompted to create a new password when next logging on with the token/card. The user will be required to set a token password that meets the PIN Quality requirements configured in the Settings window.
Confirm Password	The default password (1234567890) automatically appears in this field. If the above field was changed, then re-enter the password entered in the 'New Token Password' field.
Logon retries before token is locked	Enter the number of times a token password can be entered incorrectly before the token is locked.

Token password must be changed on first logon	If required, select token password must be changed on first logon. **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).
PIN Policy	Enables you to set PIN Quality/Property parameters. See Chapter 11: Setting IDPrime PIN Quality (PIN Quality Tab) (page 105) and Chapter 11: Setting IDPrime PIN Properties (Advanced Tab) (page 107)
Create Administrator Password	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. See Chapter 1: Friendly Admin Password (page 5).
Confirm Password	Re-enter the administrator password.
Logon retires before token is locked	Enter the number of times an administrator password can be entered incorrectly before the token is locked. This field is read only.
Keep the current administrator password	Select this if you want to keep the current administrator password. **Note:** If this option is selected, the following warning message appears: If the current password is the default password (48 0's), it is strongly recommended to update the administrator password to keep your token secure.

8. Click **Finish**. A warning message is displayed.
9. Click **OK** when the warning message: **The token initialization process will delete all token content and reset all token parameters** appears.

   The T**oken initialized successfully** message is displayed.

SafeNet Virtual Tokens

SafeNet Authentication Client supports the SafeNet Virtual Token line of products. This includes SafeNet Virtual Token and SafeNet Rescue Token devices.

To obtain a SafeNet Virtual Token file, contact your administrator.

Overview of SafeNet Virtual Products

SafeNet Authentication Client supports tokens from the SafeNet Virtual Token family. These tokens are stored as files on your computer or on an external storage device.

The following types of software tokens are available:

- **SafeNet Rescue Token:** provides a solution when a staff member loses or damages their token when away from the office. A SafeNet Rescue Token is a read-only token which functions for a limited period of time. You cannot import certificates to it.
- **SafeNet Virtual Token:** performs all the functions of an eToken NG-OTP. It can store the same data, including key pairs and certificates. Its configuration may enable it to support OTP generation.

  An eToken Virtual is “locked” to a particular computer or storage device, such as a flash drive. This means that it can be used only on the computer or storage device on which it was enrolled.
- **SafeNet Virtual Temp Token**: identical to an eToken Virtual, but its certificates become invalid after a pre-defined time period.

Connecting a SafeNet Virtual Token

To use your eToken Virtual product as a token, connect its file to SafeNet Authentication Client.

Under certain conditions, the token is connected automatically. See "Using a SafeNet Virtual Token on an External Storage Device" on page 78.

To connect a SafeNet Virtual device from the file:

1. Double-click the SafeNet Virtual (.etvp) or SafeNet Rescue Token (.etv) file.

   The SafeNet Virtual or SafeNet Rescue Tokens connect to the computer and display a confirmation message.

2. Click **OK**.

To use SafeNet Authentication Client Tools to connect a SafeNet Virtual Token:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
2. Do one of the following:
   - In the left pane, select the **Tokens** node.
     In the right pane, click the **Connect SafeNet Virtual Token** icon:

   - In the left pane, right-click the **Tokens** node, and select **Connect SafeNet VirtualToken** from the shortcut menu.
3. Navigate to the SafeNet Virtual Token file (*.etvp) or SafeNet Rescue Token file (*.etv), and double-click it.

   The SafeNet Virtual product is connected.

Disconnecting or Deleting a SafeNet Virtual Token

For security purposes, disconnect your SafeNet Virtual or SafeNet Rescue Token from its connected reader when you are not using it.

Under certain conditions, the token is disconnected automatically. See "Using a SafeNet Virtual Token on an External Storage Device" on page 78.

When your SafeNet Virtual product is no longer required, disconnect and also delete it. For example, if your SafeNet Rescue Token temporarily replaced a lost token, disconnect and delete it when you receive a permanent replacement token.

To disconnect or delete a SafeNet Virtual Token:

1. To use the *Simple* view to disconnect, do the following:
   a. Open SafeNet Authentication Client Tools *Simple* view.
      See "Opening the Simple View" on page 11.
   b. In the left pane, select the required eToken Virtual or SafeNet Rescue Token.
   c. In the right pane, select **Disconnect SafeNet Virtual Token** (or **Disconnect**).
   d. Continue with step 3.
2. To use the *Advanced* view to disconnect, do the following:
   a. Open SafeNet Authentication Client Tools *Advanced* view.
      See "Opening the Advanced View" on page 15.
   b. Do one of the following:

- In the left pane, select the node of the required eToken Virtual or SafeNet Rescue Token.
  In the right pane, click the **Disconnect SafeNet Virtual Token** icon:

- In the left pane, right-click the node of the required eToken Virtual or SafeNet Rescue Token, and select **Disconnect** from the shortcut menu.

c. Continue with step .

The *Disconnect SafeNet Virtual Token* window opens.

3. Do one of the following:
   - To keep the SafeNet Virtual Token or SafeNet Rescue Token file on the computer or device for later use, click **Disconnect**.
     Only the token connection to SafeNet Authentication Client is disconnected. It can be reconnected later. See "Connecting a SafeNet Virtual Token" on page 75.
   - To disconnect the token from SafeNet Authentication Client, and also remove the SafeNet Virtual Token or SafeNet Rescue Token file from the computer, click **Delete**.
     After a SafeNet Virtual Token or SafeNet Rescue Token is deleted, it cannot be reconnected later. A new file must be installed before it can be connected.

Using a SafeNet Virtual Token to Replace a Lost Token

To use a SafeNet Virtual Token or SafeNet Rescue Token to replace a lost token, the SafeNet Virtual Token or SafeNet Rescue Token must be enrolled using SafeNet Authentication Manager.

For more information, refer to the SafeNet Authentication Manager documentation.

Unlocking a SafeNet Virtual Token

If you enter an incorrect password more than a pre-defined number of times, the eToken Virtual becomes locked. To unlock the token, see Chapter 4: *Unlocking a Token by the Challenge-Response Method*, on page 35.

NOTE:
The number of times that a SafeNet Virtual Token can be locked can be limited to a specific amount. If this number is exceeded, the SafeNet Virtual Token becomes unusable. This function is not available for a SafeNet Rescue Token.

Generating a One-Time Password (OTP)

The ***Generate OTP*** function is available only if an eToken Virtual or eToken Rescue, with the OTP feature activated, is stored on your computer.

To generate an OTP:

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

   The SafeNet Authentication Client tray menu opens.

2. Select **Generate OTP**.

   The *Generate OTP* window opens.

3. Click **Generate OTP**.

   The *Token Logon* window opens.

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

   A unique OTP is generated, and it is displayed in the *Generate OTP* window.

5. Copy the OTP to authenticate yourself to your application.

> **NOTE**:
> Depending on your SafeNet Authentication Client configuration, you may need to include other secure information, such as your OTP PIN or Windows password.

6. Click **Close** to close the *Generate OTP* window.

Using a SafeNet Virtual Token on an External Storage Device

The operating system automatically connects a SafeNet Virtual product when all of the following conditions are met:

- The SafeNet Virtual Token file is locked to an external storage device, such as a flash drive.
- The file is located in the `eTokenVirtual` folder on the storage device.
- The storage device is connected to the computer.

When the storage device is removed from the computer, the operating system automatically disconnects the SafeNet Virtual Token that was automatically connected.

If the SafeNet Virtual Token is located on an external storage device in a location other than the `eTokenVirtual` folder, you must connect the SafeNet Virtual Token manually. See "Connecting a SafeNet Virtual Token" on page 75.

Before removing the storage device, you must disconnect the eToken Virtual manually. See "Disconnecting or Deleting a SafeNet Virtual Token" on page 76. Otherwise, the eToken Virtual will be displayed in SafeNet Authentication Client as a token with corrupted data.
For more information about token icons, see Chapter 2: *Token Icons*, on page 13.

Using an Emulated SafeNet Virtual Token

Certain applications that work with smart card readers require the SafeNet Virtual Token to emulate the action of the smart card reader. To use a SafeNet Virtual product with such applications, you must use an emulated SafeNet Virtual Token.

Typically, the emulated SafeNet Virtual Token is locked to an external storage device.

By default, the emulated SafeNet Virtual Token cannot be locked to your computer's hard drive, as this can cause a malfunction of the Windows logon. This occurs because the Windows logon process cannot deal with multiple smart card readers. However, if you want to work with the SafeNet Virtual Token located on the hard drive, the administrator can configure SafeNet Authentication Client to support this.

It is important to disconnect the emulated SafeNet Virtual Token when you have finished the session, so that the computer reverts to working with the default reader.

Common Criteria

SafeNet Authentication Client supports Gemalto IDPrime MD Common Criteria (CC) card range (See Chapter 1: Supported Tokens and Smart Cards (page 6) for a detailed list of cards), as well as eToken 5110 CC.

Working with Common Criteria Certified Tokens and Cards

IDPrime MD 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.

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

- Unlinked mode
- Linked mode

PKCS#11 Digital Signature PIN Authentication

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

Logging onto the device is required when a Common Criteria RSA private key operation is performed for the first time using the PKCS#11 library (for example signing operations). With the support of Common Criteria PKCS#11 Multi-Slots (in unlinked mode), 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.

See the SafeNet Authentication Client Administrator Guide for details about setting Multi-Slot values.

Unlinked Mode (4 Passwords)

Devices are set to work in unlinked mode by default.

To work in unlinked mode, clear the **Use the same token and administrator passwords for digital signature operation** check-box. The following four common criteria device passwords are required when working in unlinked mode:

- **Token Password (Role # 1)** - Used to perform device write/delete and exchange key operations. The default token password is 4 zero characters "0000".
- **Administrator Password (Role # 2)** - Used to /unblock a locked token password, or to perform initialization operations. The default administrator password is 48 Hexadecimal zeros.
- **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".
- **Digital Signature PUK (Role # 4)** - Used to /unblock 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 T**oken Password Must be changed at first logon** 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).

Unlinked Mode 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.

To change a digital signature PIN:

1. Open SafeNet Authentication Client Tools Advanced view.

   Do one of the following:

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

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

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

      The **Change Digital Signature PIN** window opens.

2. Enter the **Current Digital Signature PIN**.
3. Enter the **New Digital Signature PIN**.
4. Confirm the New Digital Signature PIN and click **OK**.

   The **Password Changed Successfully** window opens.
5. Click **OK**.

Change Digital Signature PUK

Use this option to change the Digital Signature PUK.

To change a digital signature PUK:

1. Open SafeNet Authentication Client Tools Advanced view.

   Do one of the following:

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

      In the right pane, click the **Change Digital Signature PUK** icon:

   b. In the left pane, right-click the node of the required token, and select **Change Digital Signature PUK** from the shortcut menu.

   The **Change Digital Signature PUK** window opens.

2. Enter the **Current Digital Signature PUK**.
3. Enter the **New Digital Signature PUK**.
4. Confirm the **New Digital Signature PUK** and click **OK**.

   The **Password Changed Successfully** window opens.
5. Click **OK**.

Set Digital Signature PIN

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

To set a digital signature PIN:

1. Open SafeNet Authentication Client Tools Advanced view.

   Do one of the following:

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

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

   b. In the left pane, right-click the node of the required token, and select **Set Digital Signature PIN** from the shortcut menu.

   The **Digital Signature PUK Logon** window opens.

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

   The **Set PIN** window opens.

3. Enter a **New Digital Signature PIN**.

4. Confirm the New Digital Signature PIN and click **OK**.

   The **Password Changed Successfully** window opens.

5. Click **OK**.

Linked Mode (2 Passwords)

To work in linked mode, the token/card must be initialized to work in linked mode. 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.

Working in linked mode, the user enters a Token Password to authenticate for 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 is not compatible with the Multi-Slots feature.

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) i.e. 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 i.e. 6 characters long, while other password policies are disabled.

Operational Differences and Role Protection

The table below displays the differences between eToken 5100 CC and eToken 5110 CC/IDPrime 840 and the roles that protect the specific operation.

Operation	eToken 5100 CC	IDPrime 840/3840 and eToken 5110 CC
This column indicates the type of operation performed.	This column indicates which password is required to perform the specified operation on an eToken 5100 CC device.	This column indicates which password is required to perform the specified operation on IDPrime 840/3840 and eToken 5110 CC devices.
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
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 locked by the Digital Signature PUK	Token Password is locked by the Administrator Password Digital Signature PIN is locked by the Digital Signature PUK

SafeNet eToken 5300

SafeNet eToken 5300 is an ideal solution for enterprises looking to deploy the military-grade security of PKI, while maintaining a convenient solution for employees. The eToken 5300 is a compact, tamper-evident USB with presence detection, which creates a third factor of authentication. Something you have (physical token), something you know (PIN), something you do (enabling touch sensor). The eToken 5300 offers multi-application dynamic smart card functionality. It can be used with any USB connection for Identity and Access Management applications such as network authentication, digital signatures, email encryption and other advanced services based on Public Key Infrastructure (PKI). The eToken 5300 is certified FIPS 140-2 L3 at the full token boundary.

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

eToken 5300 Certificates

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

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

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

The eToken 5300 is available in the following configurations:

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

NOTE:

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

Viewing eToken 5300 information

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 from the shortcut menu, select **Tools**.
   - On Windows: From the Windows taskbar, select **Start > All Programs > SafeNet > SafeNet Authentication Client > SafeNet Authentication Client Tools.**

   The *SafeNet Authentication Client Tools* window opens in the *Simple* view.
2. Click the **Advanced View** icon.

   The *SafeNet Authentication Client Tools* window opens in the *Advanced* view.
3. In the left pane, select the eToken 5300 node.

   The *Token's Information* is displayed.

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

Touch Sense support - Signature Keys

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.

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.

SafeNet eToken 7300

SafeNet eToken 7300 devices combine a certificate-based authentication solution with password-protected data and application storage on up to 64GB of encrypted flash memory.

Introduction to SafeNet eToken 7300

The SafeNet eToken 7300 device is a hybrid certificate-based authentication token and a flash token on a single device. SafeNet eToken 7300 addresses the following needs:

- Portable secure applications: Secure access to online resources with the ability to store portable applications on the token that are accessible when the user enters the token password.
- Portable office: secure remote access to corporate resources combined with a fully bootable secure portable office environment that is stored on the token.
- Secure documents and data: Secure access combined with encrypted storage for sensitive documents and data.

SafeNet eToken 7300 devices that have been initialized using SafeNet Authentication Client 10.0 work seamlessly on computers running either Windows, Linux or Mac operating systems. If SafeNet Authentication Client is not installed on your computer, connect your SafeNet eToken 7300 device and run the built-in launcher application. This application temporarily installs the SafeNet eToken 7300 tray menu for token management. If the token's user storage has been password-protected, you must log on to your token to access its contents.

NOTE:

- The SafeNet eToken 7300 initialization process always initializes the smart card and partitions the flash drive.
- If partitioning settings are not set before the initialization proceeds, the default partitioning settings are used.
- In Windows 8.1 environments, SafeNet eToken 7300 devices earlier than version 9.0.35 can be used only when SafeNet Authentication Client is installed.

SafeNet eToken 7300 Launcher

Depending on the configuration of your SafeNet eToken 7300 device, connecting the device to your computer initiates a launcher application that enables the SafeNet eToken 7300 flash tray icon to be displayed:

Running the Launcher to Open the Tray Icon on Windows

After connecting the SafeNet eToken 7300 device, you can run the launcher application from the eToken 7300's *AutoPlay* window or from the **eToken 7300 > SafeNet-Authentication-Client** folder.

To run the launcher from the eToken 7300's *AutoPlay* window:

1. If the SafeNet eToken 7300 device is not connected, connect it, and wait until the operating system recognizes it.

   NOTE:
   If your operating system does not recognize your token, a message may be displayed instructing you to restart your computer.
   To prevent this message from being displayed in the future when this token is connected, restart your computer.

   The eToken 7300's *AutoPlay* window opens.

   Continue with step 3.

   NOTE:
   If the device's user storage is not password-protected, the ETOKEN 7300's *AutoPlay* window opens also.

2. If the eToken 7300's *AutoPlay* window is not open, from the computer directory window, right-click the SafeNet drive's **eToken 7300** icon and from the drop-down menu, select **Open AutoPlay**.
3. Select **Run Launcher.exe**.

   In the menu bar, the SafeNet eToken 7300 flash tray icon is displayed:

To run the launcher from the SafeNet-Authentication-Client folder:

1. From the computer directory window, open the folder **eToken 7300 > SafeNet-Authentication-Client**.
2. Double-click **Launcher**.

   In the menu bar, the SafeNet eToken 7300 flash tray icon is displayed:

SafeNet eToken 7300 Tray Menu

The SafeNet eToken 7300 flash tray icon offers the same shortcut menu to token functions as the SafeNet Authentication Client tray icon. If SafeNet Authentication Client is not installed, use the SafeNet eToken 7300 tray menu for token management.

SafeNet eToken 7300 Tray Menu Functions

The following functions can be accessed quickly by right-clicking the SafeNet eToken 7300 tray menu:

- **About:** displays product version information and license 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 SafeNet eToken 7300 device is connected.
- **Change Token Password:** opens the *Change Password* window for the selected token.
  See Chapter 4: *Changing the Token Password*, on page 33.
- **Unlock Token:** opens the *Token* window for the selected token.
  See Chapter 4: *Unlocking a Token by the Challenge-Response Method*, on page 35.
- **Certificate Information:** opens the *Token Certificate Information* window for the selected token.
- **Log On to Flash/Log Off from Flash:** displayed when a SafeNet eToken 7300 having a password-protected flash partition is connected. Opens the *Log On to Token* window for the selected token.
  See Chapter 4: *Logging On to the Token as a User*, on page 31.
- **Explore Flash:** this option opens Windows explorer, and becomes available only when you have selected the Log On to Flash option.
- **Exit:** closes the SafeNet eToken 7300 flash tray icon.

NOTE:
The SafeNet eToken 7300 shortcut menu options are identical to the SafeNet Authentication Client tray menu options for the connected token.

Using the SafeNet eToken 7300 Tray Icon

After the launcher application is run, the SafeNet eToken 7300 flash tray icon is displayed in the menu bar:

The SafeNet eToken 7300 flash tray icon offers a shortcut menu to the application's functions.

To open the SafeNet eToken 7300 tray menu:

- Right-click the SafeNet eToken 7300 icon.

The SafeNet eToken 7300 shortcut menu opens.

Selecting the Token from the SafeNet eToken 7300 Tray Menu

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

To select from multiple tokens in the SafeNet eToken 7300 tray menu:

1. Right-click the SafeNet eToken 7300 flash tray icon.
2. The SafeNet eToken 7300 shortcut menu opens. Among the options, a list is displayed of the names and serial numbers of the connected SafeNet eToken 7300 tokens.
3. Hover the mouse over the required token. Options for the selected token are displayed.
4. Select the required option.

Closing SafeNet eToken 7300

The SafeNet eToken 7300 flash tray icon closes automatically when all connected SafeNet eToken 7300 devices are disconnected.

To close the SafeNet eToken 7300 tray icon manually:

1. Right-click the SafeNet eToken 7300 flash tray icon, and from the shortcut menu, select **Exit**.
   A warning message is displayed.
2. Click **OK**.

SafeNet eToken 7300 User Storage

The SafeNet eToken 7300 device includes a flash partition for the storage of user data.

The flash partition can be password-protected.

Accessing an Unprotected Flash Partition on Windows

To access a SafeNet eToken 7300 device's user storage that is not password-protected:

1. Connect the SafeNet eToken 7300 device and wait until the operating system recognizes it.
   The ETOKEN 7300's *AutoPlay* window opens.

   NOTE:
   If the SafeNet eToken 7300 device's flash partition is not password-protected, the contents can be accessed even if SafeNet Authentication Client is not installed and the launcher application is not run.

2. Do one of the following:
   - In the ETOKEN 7300's *AutoPlay* window, select **Open folder to view files**.
   - From the computer directory window, open the SafeNet eToken 7300 device's folder **ETOKEN 7300**.

   The user storage contents are displayed.

Accessing a Protected Flash Partition on Windows

If the SafeNet eToken 7300 device's flash partition is password-protected, the contents of the flash can be accessed only after logging on to the token.

To access a SafeNet eToken 7300 device's user storage that is password-protected:

1. Click the SafeNet eToken 7300 flash tray icon, and for the appropriate device, select **Log On to Token**.
2. Log on to the token.

NOTE:
- If SafeNet Authentication Client is installed, you can use the SafeNet Authentication Client tray menu to log on to your token. See Chapter 2: *SafeNet Authentication Client Tray Icon*, on page 8.
- If SafeNet Authentication Client is not installed, use the SafeNet eToken 7300 flash tray menu to log on to your token. See "SafeNet eToken 7300 Launcher" on page 91.

The ETOKEN 7300's *AutoPlay* window opens.

3. Do one of the following:
   - In the ETOKEN 7300's *AutoPlay* window, select **Open folder to view files**.
   - From the computer directory window, open the SafeNet eToken 7300 device's folder **ETOKEN 7300**.

NOTE:
If the *Log On to Token* window opens, re-enter the token password.

The user storage contents are displayed.

Partitioning the SafeNet eToken 7300

For details on how to partition the eToken 7300 Chapter 5: "Token Initialization" on page 51.

Client Settings

Client Settings are parameters that are saved to the computer and apply to all tokens that are initialized on the computer after the settings have been configured. Use token settings to determine behavior that applies to a specific token. See Chapter 11: “Token Settings” on page 101.

Setting Password Quality (eToken Devices only)

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

To set PIN Quality parameters for IDPrime cards, See "Setting IDPrime PIN Quality (PIN Quality Tab)" on page 105.

The Set Password Quality feature is for eToken devices only.

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.

To set the Password Quality:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Password Quality** tab.

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

TIP:
The Password Quality settings are configured the same way as the Token Password quality settings.
See Chapter 11: *Setting eToken Password Quality (Password Quality Tab)*, on page 101.

   - 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.

Copying User Certificates to a Local Store

SafeNet Authentication Client 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.

Use the **Copy user certificates to a local store** option to control the automatic installation of the token's user certificates to the local certificate store upon token connection.

This option is selected by default.

To automatically install the token's user certificates to the local store:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab.

   The *Advanced* tab opens.
4. Select **Copy user certificates to a local store**.
5. Click **Save** to save your changes, or click **Discard,** to ignore your changes.

Copying CA Certificates to a Local Store

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. Use the **Copy CA certificates to a local store** option to control the automatic installation of the token's CA certificates to the local certificate store upon token connection.

> **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**.

This option is selected by default.

To automatically install the token's CA certificates to the local store:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab.
4. Select **Copy CA certificates to a local store**.
5. Click **Save** to save your changes, or click **Discard,** to ignore your changes.

Enabling Single Logon

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. This option is disabled by default.

> **NOTE**:
> When single logon is set using SafeNet Authentication Client Tools, Windows Logon is not included in the single logon process. Only an administrator can configure Windows Logon as single logon.

To enable single logon:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab.
4. Select **Enable Single Logon.**
5. Click **Save** to save your changes, or click **Discard,** to ignore your changes.
6. To activate the single logon feature, log off from the computer and log on again.

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

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

> **NOTE**:
> This feature is not supported by iKey tokens.

To enable password quality configuration after initialization:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab.
4. Select **Allow password quality configuration on token after initialization.**
5. Click **Save** to save your changes, or click **Discard,** to ignore your changes.

Allowing Only an Administrator to Configure Password Quality on Token

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

To define who can configure password quality on token:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab.
4. Do one of the following:
   - To enable configuration by the administrator only, select **Allow only an administrator to configure password quality on token**.
   - To enable configuration by the user also, clear **Allow only an administrator to configure password quality on token**.
5. Click **Save** to save your changes, or click **Discard,** to ignore your changes.

Showing the SafeNet Authentication Client Tray Icon

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

To show the SafeNet Authentication Client tray icon:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab.
4. In the *Show application tray icon* drop-down list, select one of the following:
   - **Never**: The tray icon is never displayed
   - **Always**: The tray icon is always displayed
5. Click **Save** to save your changes, or click **Discard,** to ignore your changes.

Defining Automatic Logoff

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.

To define the automatic logoff setting:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab.
4. In the *Automatic logoff after token inactivity* drop-down list, select one of the following:
   - **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.
     Set the number of minutes in the text box (1 - 240).
5. Click **Save** to save your changes, or click **Discard,** to ignore your changes.

Enabling Logging

The logging function creates a log of SafeNet Authentication Client activities.

> **NOTE**:
> You must have administrator privileges to use the logging function.

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

To activate the logging function on a Windows System:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
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 on a Windows System:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab, and click **Disable Logging**.

Token Settings

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

For configurations set in *Client Settings*, that apply the settings to all tokens that are initialized after the settings have been configured, see Chapter 10: *Client Settings*, on page 96.

Setting eToken Password Quality (Password Quality Tab)

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

To set password quality for a token:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
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 opens.
4. Enter the password quality parameters as follows:

Password Quality Parameter	Description
Minimum length (characters)	Default: 6 characters
Maximum length (characters)	Default: 16 characters
Maximum usage period (days)	The maximum period, in days, before which the password must be changed. Default: 0 (none) For iKey devices, the periods are rounded up to periods of weeks (7 days), even though the period is displayed in days. For example, if the period is displayed as less than a week, say 6 days, iKey regards it as a week. If the period is more than two weeks, say 15 days, iKey regards it as three weeks.
Minimum usage period (days)	The minimum period before the password can be changed. Default: 0 (none) For iKey devices, the periods are rounded up to periods of weeks. See row above for more information.
Expiration warning period (days)	Defines the number of days before the password expires that a warning message is shown. Default: 0 (none)
History size	Defines how many previous passwords must not be repeated. Default: For eToken devices - 10 For iKey devices - 6

Password Quality Parameter	Description (Cont.)
Maximum consecutive repetitions	The maximum number of repeated characters that is permitted in the password. Default: 3 This feature is not supported by iKey devices.
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. **Note:** The **Forbidden** option is not supported by iKey devices.

5. Do one of the following:
   - To save your changes, click **Save.**
   - To ignore your changes, click **Discard.**
   - To apply SafeNet Authentication Client's default settings, click **Set to Default.**

Setting Private Data Caching Mode (Advanced Tab)

NOTE:
This feature is not supported by iKey, IDPrime MD, .NET and eToken 5110 CC devices.

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

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

To set private data caching mode:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
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 opens.

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

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

5. Do one of the following:

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

Setting RSA Key Secondary Authentication

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

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

NOTE:
This feature is not supported by iKey, IDPrime MD, .NET and eToken 5110 CC devices.

To set RSA key secondary authentication:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See "Opening the Advanced View" on page 15.
2. In the left pane, expand the node of the required token, and select **Settings**.
3. In the right pane, select the **Advanced** tab.
4. In the *RSA key secondary authentication* field, select one of the following:
   - Always
   - Always prompt user
   - Prompt user on application request
   - Never
   - Token authentication on application request

   NOTE:
   For an explanation of these options, see Chapter 5: *Setting the RSA Key Secondary Authentication Field*, on page 62.
5. Do one of the following:
   - To save your changes, click **Save**.
   - To ignore your changes, click **Discard**.

Setting IDPrime PIN Quality (PIN Quality Tab)

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

NOTE:
In the MD Manager, the unlimited value = FFh
In SAC Tools, the unlimited value = 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 Min. length value.
History size	Number of previous PIN values that cannot be matched by a new PIN. Range is 00h-0Ah. 00h = No history
Number of different characters that can be repeated at least once	The number of different characters that can be repeated at least once. Range is 00h-FFh. 00h = No limitation
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	Max 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 PIN Advanced tab enables you to define PIN properties that must be met in order for the PIN to be accepted. The PIN Advanced tab is available for all IDPrime based devices.

Select **Settings** in the left pane, to view the User PIN Quality/Advanced fields in the right pane.

Select **Digital Signature PIN** in the left pane, to view the Digital Signature PIN Quality/Advanced fields in the right pane.

Select **Digital Signature PUK** in the left pane, to view the Digital Signature PUK Quality/Advanced fields in the right pane.

For IDPrime MD cards, the following PIN property parameters exist in the Advanced Tab:

PIN Property Parameter	Description
PIN Type	• Regular PIN - Use the keyboard to enter a PIN • External PIN - Use an external keyboard/key PIN Pad
PIN Purpose	Defines the purpose of the PIN. This property is for information only. The following options are available: • Authentication PIN • Digital Signature PIN • Encryption PIN • Non Repudiation PIN • Administrator PIN • Primary Card PIN • Unlock Only PIN
Cache Type	Select one of the following Cache Type functions: • Normal Cache • Timed Cache (Minidriver) • No Cache (Minidriver) • Always Prompt
Cache Timeout	This field is activated only if Timed Cache (Minidriver) is selected in the Cache Type parameter above. Defines the number of seconds it takes before the cache times out.
PIN Flags	These flags are for backward compatibility only. • No Flags • Required Security Entry
Ext. PIN Flags	The following options are available: • No Flags - PINs are considered as follows: 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: External PIN & Normal Reader ==> Login refused • No Auto PIN Pad - changes the second case as follows: Regular PIN & PIN Pad Reader ==> Regular PIN • No Regular fallback + No Auto PIN Pad (both of the above).

PIN Property Parameter	Description (Cont.)
PIN Validity Parameter:	
Validity period (days)	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. Default: 0 (no validity period)
Expiration warning period (days)	Defines the number of days before the PIN expires that a warning message is shown. Default: 0 (no warning)

NOTE:
PIN Quality and PIN Property settings may also be accessed when Initializing a device. See Chapter 5: Initializing IDPrime Based Devices (page 64).

Licensing

Import a SafeNet license for your SafeNet Authentication Client installation.

Viewing and Importing Licenses

SafeNet Authentication Client installations that do not have a SafeNet license can be used for evaluation only, and a message is displayed on all logon windows.

You can view your licenses and import new ones using the SafeNet Authentication Client *About* window.

To view and import licenses:

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.
     See "Opening the Advanced View" on page 15.
     On the toolbar, click the **About** icon:

   The *About* window opens, displaying your license information in the *License Information* box.

2. To import a new license, click **Import New License**.

   The *Import License* window opens.

3. To Validate Binary Signatures, see *Validating Binary Signatures* on page 25
4. Do one of the following:
   - If the SafeNet license box is automatically filled, click **OK**.
   - Copy your new SafeNet license string to the license box, and click **OK**.
   - Click **Import from File**, browse to the file containing your license, open it to copy its contents to the license box, and click **OK**.
   - The *About* window opens, displaying your updated license information in the *License Information* box.