THALES

SafeNet Authentication Client 10.8 (R2)

WINDOWS USER GUIDE

Document Information

Product Version	10.8 (R2)
Document Number	007-013561-005 Rev: E
Release Date	July 2020

Revision History

Revision	Date	Reason
E	July 2020	Thales branding

consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

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

CONTENTS

PREFACE: About This Document

Audience

This Document is intended for personal responsible for maintaining your organization's security infrastructure. This includes SafeNet Authentication Client users and administrators.

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

Related Documents

- 007-013560-005 SafeNet Authentication Client 10.8 (R2) Windows (GA) Administrator Guide Rev E
- 007-013559-007 SafeNet Authentication Client 10.8 (R2) Windows (GA) Release Notes Rev H

Support Contacts

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

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

Customer Support Portal

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

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

Telephone

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

CHAPTER 1: Introduction

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

Overview

SafeNet Authentication Client (SAC) is a middleware client that manages Thales' extensive SafeNet portfolio of certificate-based authenticators, including eToken, IDPrime smart cards, USB and software-based devices. Offering full backward compatibility and incorporating features from previous middleware versions, SafeNet Authentication Client ensures complete support for all currently deployed eToken devices, as well as IDPrime smart cards.

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

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.

CHAPTER 2: SafeNet Authentication Client User Interface

This chapter describes the SafeNet Authentication Client user interface.

> **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 is used throughout the document and is applicable to both Smart Cards and Tokens.

Overview of SafeNet Authentication Client User Interface

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 task bar 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 task bar, see "Showing the SafeNet Authentication Client Tray Icon" on page 88.

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 as well as 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 "Changing the Token Password" on page 29.
- **Unlock Token:** opens the Token window for the selected token. See "Activating a Token" on page 31.
- **Certificate Information:** opens the Token Certificate Information window for the selected token.
- **Exit:** closes SafeNet Authentication Client and the tray icon.

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

- **Delete Token Content:** removes the deletable data from the selected token
- **Synchronize Password (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.

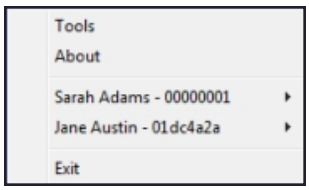
Selecting the Token from the SAC Tray Menu

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

To select from multiple tokens in the tray menu:

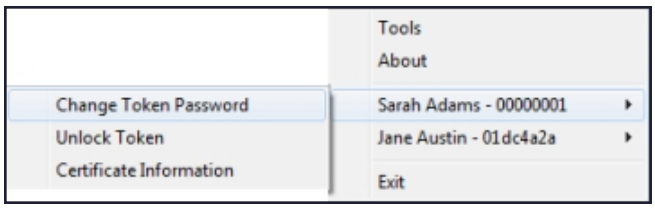
1. Right-click the SafeNet Authentication Client tray icon.

   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

SafeNet Authentication Client Tools includes two viewing options:

- Simple view: to perform common tasks

  See "Opening the Simple View" on the next page.
- 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.

> **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 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
	Refresh – refreshes the data for all connected tokens
	About – displays product version information as well as the validation of SAC binary signatures
	Help – opens the SafeNet Authentication Client User Guide (PDF)
	Home – opens the company website

Opening the Simple View

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

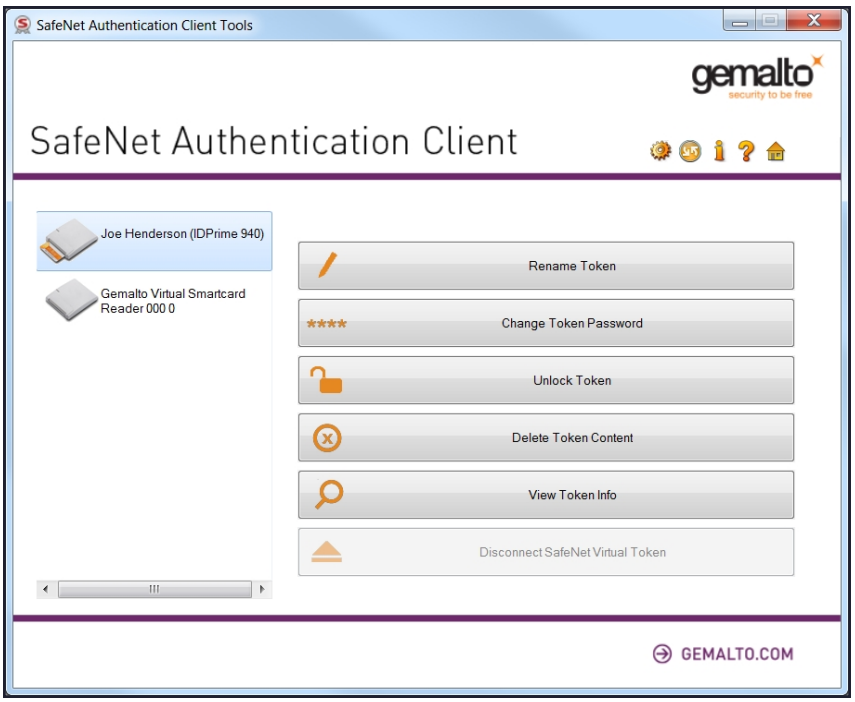
To open SafeNet Authentication Client Tools:

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/Smart Card Type
	Token Connected For a full list of supported devices, see the SafeNet Authentication Client Release Notes.
	Smart Card reader – no card connected
	Smart Card reader – card connected For a full list of supported devices, see the SafeNet Authentication Client Release Notes.
	Token with corrupted data This icon is also displayed when connecting a device which needs to be activated using an Activation PIN See "Activating a Token" on page 31
	Unknown device

Simple View Functions

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

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

Opening the Advanced View

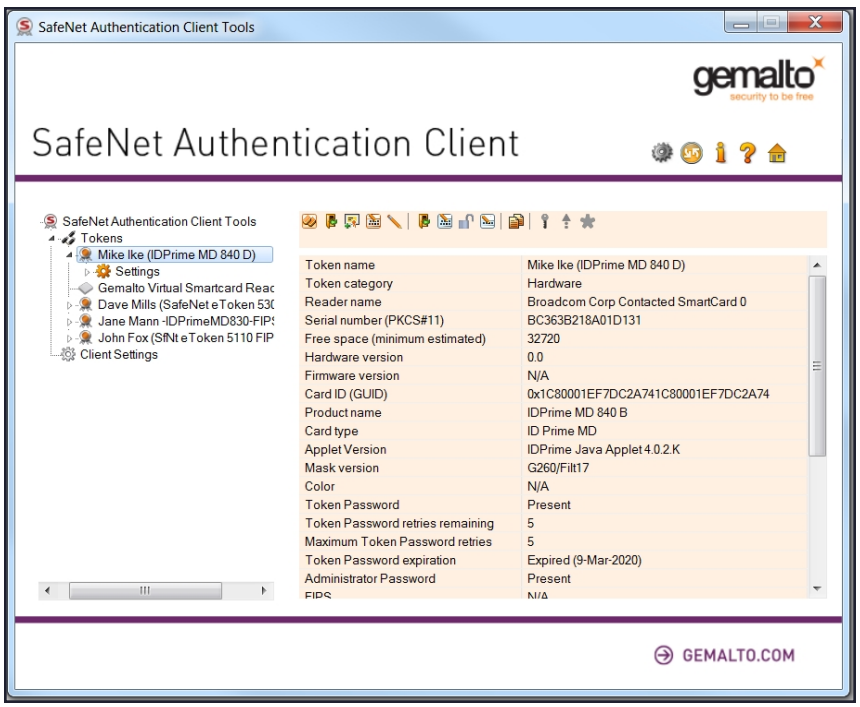
The SafeNet Authentication Client Tools Advanced view provides additional token management functions.

To open the SafeNet Authentication Client Tools Advanced view:

1. Do one of the following:
   a. Right-click the SafeNet Authentication Client tray icon, and from the shortcut menu, select **Tools**.
   b. 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:

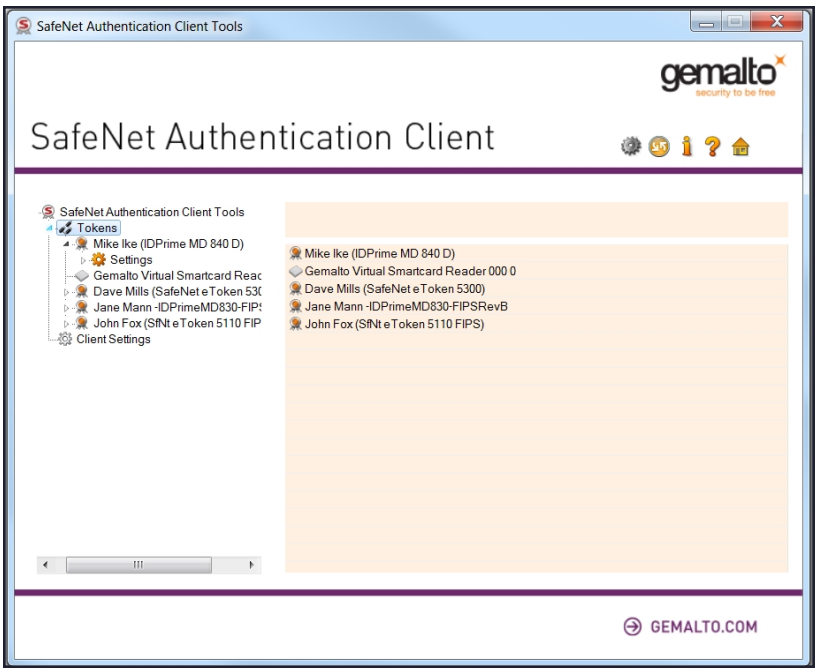
   a. In the left pane, right-click the object, and select the required function from the shortcut menu.

   b. In the left pane, select the object.

   c. 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.



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

> 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 "Token Initialization" on page 52.		Initialize Token
Log On to Token See "Logging On to the Token as a User" on page 27.		Log On to Token
Import Certificate See "Importing a Certificate to a Token" on page 35.		Import Certificate
Change Password See "Changing the Token Password" on page 29.		Change Password
Rename Token See "Renaming a Token" on page 28.		Rename Token
Copy to Clipboard See "Viewing and Copying Token Information" on page 27.		(None)
Change Digital Signature PIN See "Change Digital Signature PIN" on page 76		Change Digital Signature PIN
Change Digital Signature PUK See "Change Digital Signature PUK" on page 78		Change Digital Signature PUK
Set Digital Signature PIN See "Set Digital Signature PIN" on page 79		Set Digital Signature PIN

> **NOTE** Depending on the token type, additional options may be displayed in the dropdown menu.

ome administrator functions are available only if an Administrator Password has been set for the token:

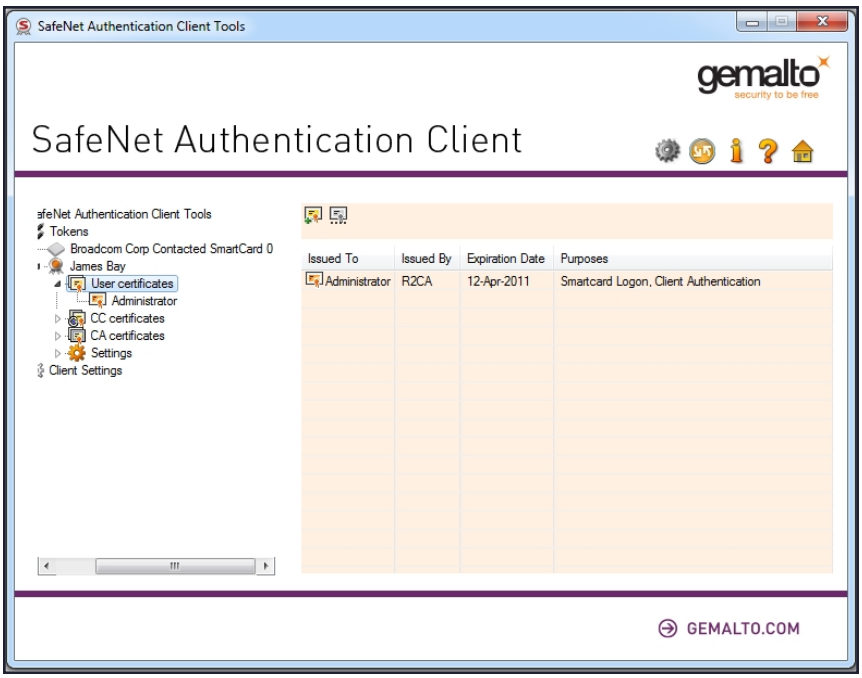
See "Logging On to the Token as an Administrator" on page 40.

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
- 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 "Importing a Certificate to a Token" on page 35.		Import Certificate
Reset Default Certificate Selection See "Clearing a Default Certificate" on page 39.		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 documentation.

See "Importing Common Criteria Certificates" on page 37.

For a full list of devices supporting Common Criteria Certificates, see the SafeNet Authentication Client Release Notes.

ECC Certificates

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

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

Selected Certificate Node

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

Some or all of the following functions are available:

User Function	Icon	Right-Click Menu Item
Delete Certificate See "Deleting a Certificate" on page 40.		Delete Certificate
Export Certificate See "Exporting a Certificate from a Token" on page 39		Export Certificate
Set as Default See "Setting a Certificate as Default or Auxiliary" on page 46.	(None)	Set as Default
Set as Auxiliary See "Setting a Certificate as Default or Auxiliary" on page 46.	(None)	Set as Auxiliary
Copy to Clipboard See "Viewing and Copying Token Information" on page 27.		(None)
Set as KSP / Set as CSP See "Clearing a Default Certificate" on page 39.	(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 "Setting eToken Password Quality (Password Quality Tab)" on page 91.

> Advanced

  See "Setting Private Data Caching Mode (Advanced Tab)" on page 93

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

> PIN Quality

  See "Setting IDPrime PIN Quality (PIN Quality Tab)" on page 95

> Advanced

  See "Setting IDPrime PIN Properties (Advanced Tab)" on page 97

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 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:

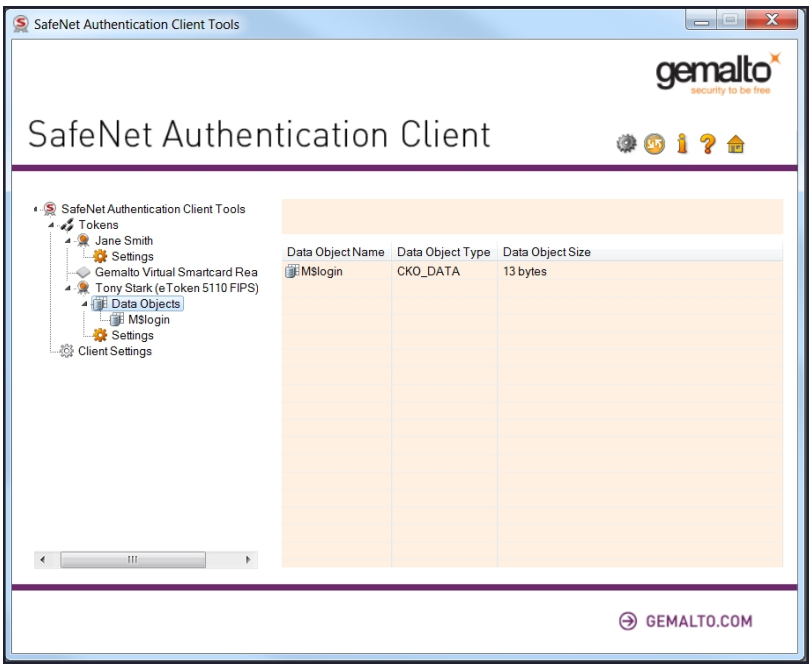
> Password Quality

> Advanced

See "Client Settings" on page 85.

Data Objects Node

Tokens used with some applications (e.g Entrust) may have a Data Objects node which contains PKCS#11 data objects.



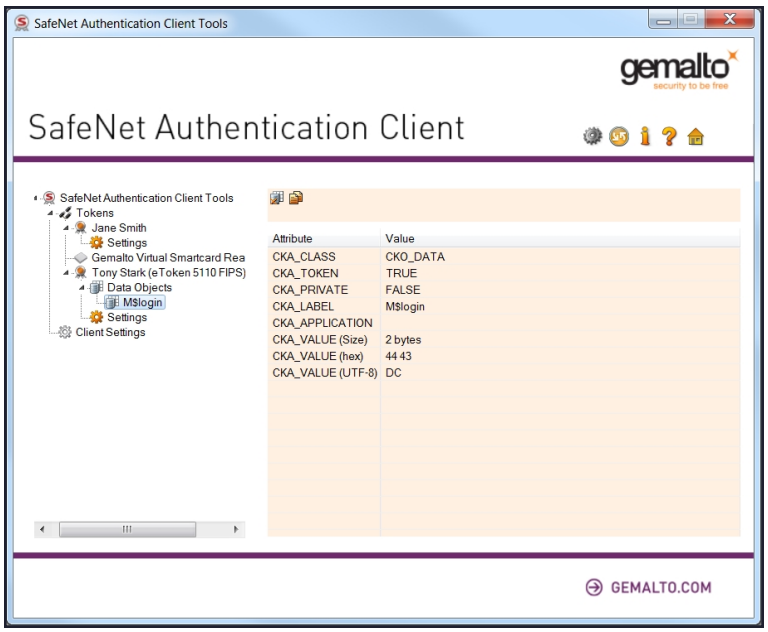
To view the contents of a data object:

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: 

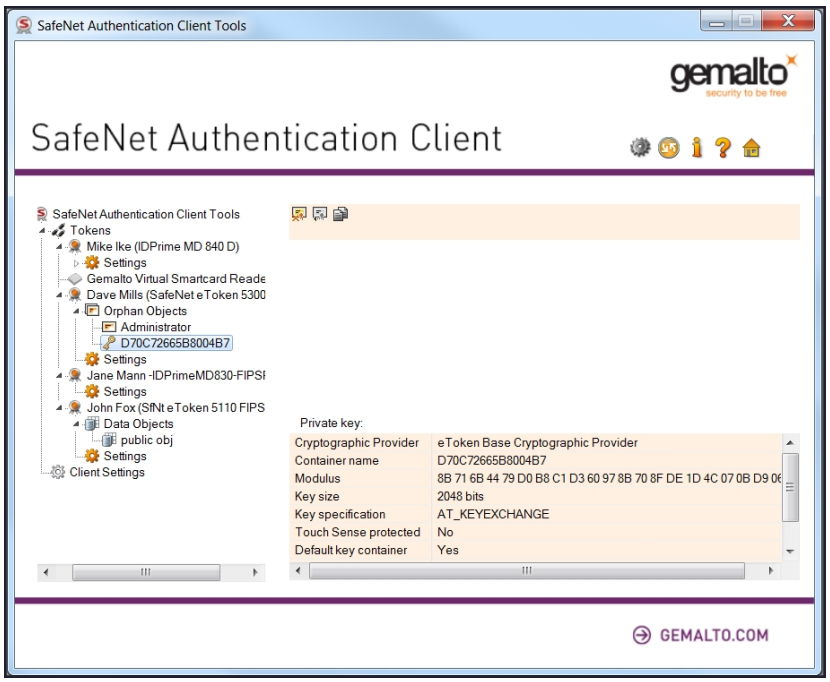
Orphan Objects Node

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

NOTE

- 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

> 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:

SafeNet Minidriver Proxy and Minidriver folders:

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

SAC installation folder (default):

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

To validate SAC binary signatures:

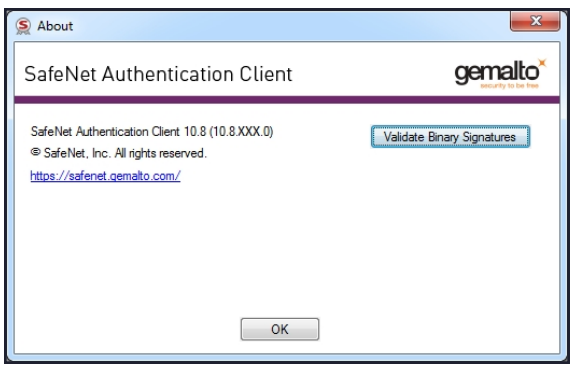
1. Do one of the following:
   a. Right-click the SafeNet Authentication Client tray icon, and from the shortcut menu, select **About**.
   b. Open SafeNet Authentication Client Tools.

      See "Opening the Simple View" on page 13.

      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.

CHAPTER 3: Token Management

SafeNet Authentication Client Tools and the SafeNet Authentication Client tray menu enable you to control the use of your tokens. When running a management task, ensure that the appropriate token remains connected until the process completes.

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

Selecting the Active Token

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

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

1. Open SafeNet Authentication Client Tools.

   See "Opening the Simple View" on page 13, 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.
   b. See "Opening the Simple View" on page 13.
   c. In the left pane, select the required token.
   d. In the right pane, select View Token Info.
   e. 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.
4. To copy the token information to the clipboard, do one of the following:
   a. In the Token Information window, click Copy.
   b. In Advanced view, click the Copy to Clipboard icon:
5. To paste the copied token information, click the cursor in the target application, and paste the information.
6. Click **OK**.

Logging On to the Token as a User

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

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.

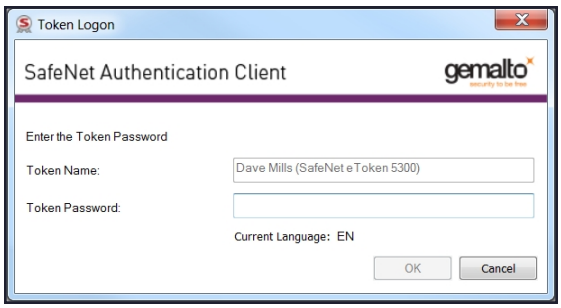
Do one of the following:

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

b. In the right pane, click the **Log On to Token** icon: 

c. In the left pane, right-click the node of the required token, and select Log On from the shortcut menu.

The **Token Logon** window opens.



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

You are logged on to the token.

Renaming a Token

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

> **NOTE** If you have more than one token, 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 13.
   b. In the left pane, select the required token.
   c. In the right pane, select Rename Token.
   d. Continue with step 2 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

> **NOTE** 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 Advanced View" on page 15.

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

c. In the right pane, select Change Token Password.

d. Continue with step 3.

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 3.

2. To use the tray menu to change the token password, do the following:

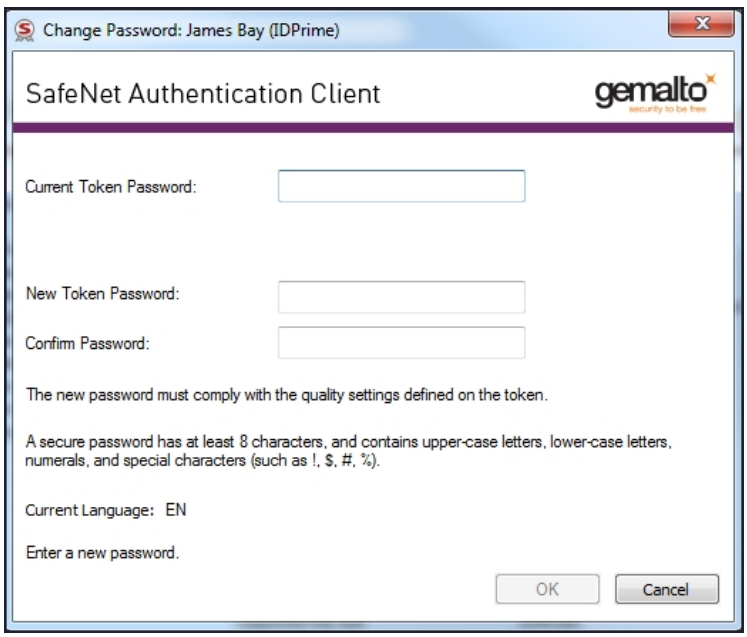
   a. Right-click the SafeNet Authentication Client tray icon.

   b. If more than one token is connected, hover over the appropriate token.

   c. Select Change Token Password.

   d. Continue with step 4.

   The Change Password window opens.



3. 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.
> As you type a new password, the password quality indicator on the right displays a percentage score of how well the new password matches the password quality requirements.

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

5. Click **OK**.

A message confirms that the token password was changed successfully.

6. Click **OK**.

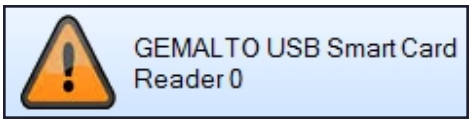
Activating a Token

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

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

The token activation function can also be accessed quickly by right-clicking the tray menu.

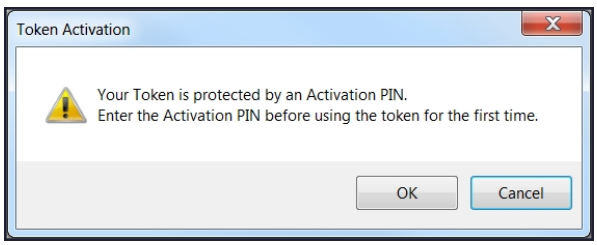
Connecting an unactivated device displays the Token with corrupted data icon in SAC Tools. This does not mean that the device is in fact corrupted, it simply needs to be activated.



To Activate a Token:

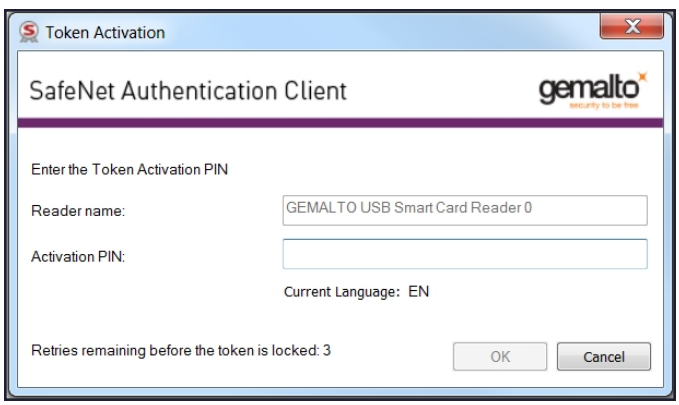
1. Connect the token.

   The Token Activation window opens.



2. Click **OK** to continue with the activation process or **Cancel** to close the window without activating the token.

   Enter the Activation PIN (Role#1) and click **OK**.



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

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

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

Unlocking a Token by the Challenge-Response Method

If an incorrect token password is entered more than a pre-defined number of times, the token becomes locked. Tokens can be unlocked if, and only if, an Administrator Password was set during initialization.

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

When the administrator has access to the user's token, the administrator can unlock the token using the Set Token Password feature.

See "Setting a Token Password by an Administrator" on page 42.

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

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

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

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 13.

   b. In the left pane, select the required token.
   c. In the right pane, select Unlock Token.
   d. Continue with step 4.

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 and click the Unlock icon in the right pane.
   - In the left pane, right-click the node of the required token, and select Unlock from the shortcut menu.

c. Continue with step 4.

2. To use the tray menu to change the token password, do the following:

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

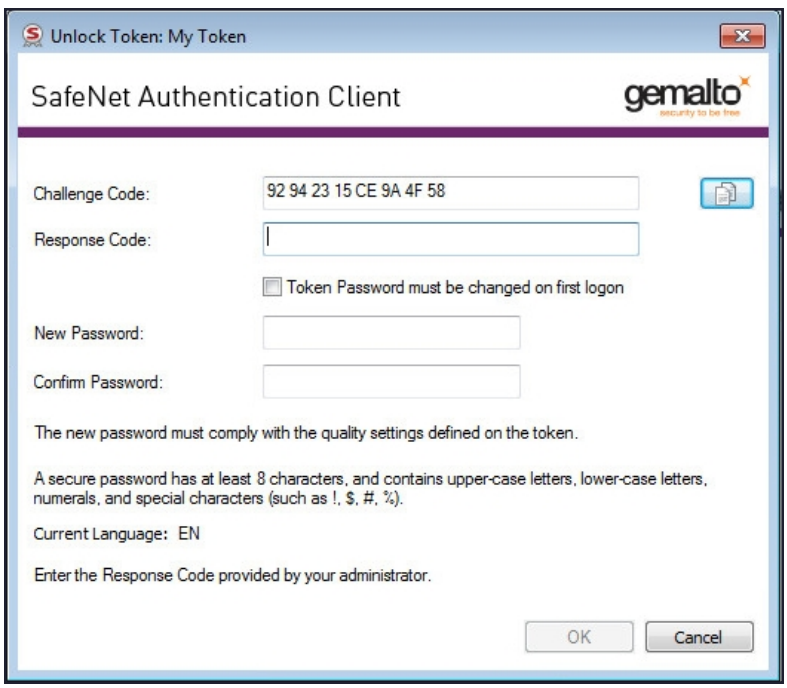
   b. If more than one token is connected, hover over the appropriate token.

   c. Select Unlock Token.

   d. Continue with step 3.

3. 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.



4. 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.

5. 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.

6. Enter a new token password in the New Token Password and Confirm Password fields.
7. If the new password is known to others and must be changed, select **Token Password must be changed on first logon**.
8. Click **OK**.

   A message confirms that the token was unlocked successfully.
9. Click **OK**.

Deleting Token Content

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

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

The Delete Token Content function is less comprehensive than the Initialize function which restores a token to its initial state, removing all objects stored on the token since manufacture and resetting the token password.

See "Token Initialization" on page 52.

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 13.
   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.
      The Token Logon window opens.
3. Enter the token password, and click **OK**.
   The **Delete Token Content** window opens, prompting you to confirm the delete action.
4. To continue with the delete process, click **OK**.
   The **Delete Token Content** window opens, confirming that the token content was deleted successfully.
5. Click **OK** to finish.

Importing a Certificate to a Token

The following certificate types are supported:

- .pfx
- .p12
- .cer

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

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

> **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.

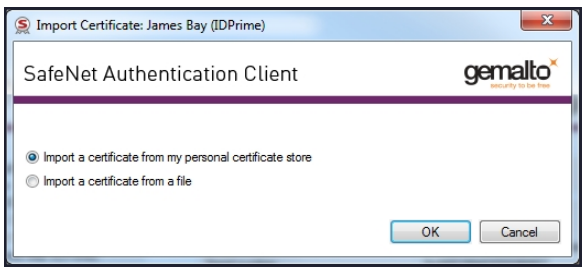
   See "Opening the Advanced View" on page 15.

2. Do one of the following:
   a. In the left pane, select the node of the required token.
   b. In the right pane, click the Import Certificate icon: 
   c. In the left pane, right-click the node of the required token, and select Import Certificate from the shortcut menu.

      The Token Logon window opens.

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

   The Import Certificate window opens.



4. Select one of the following:
   a. Import a certificate from my personal certificate store.
   b. Import a certificate from a file.

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

5. 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

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

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

7. If the certificate requires a password, the Password window opens.

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

8. 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.

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

Importing Common Criteria Certificates

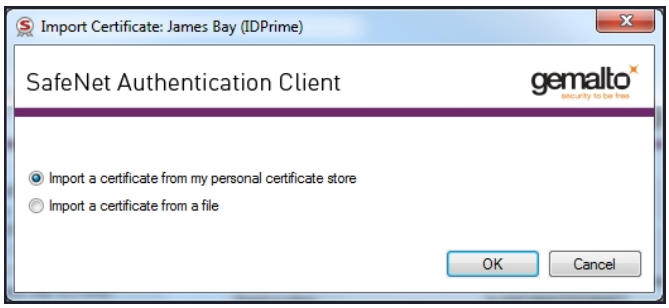
When importing PFX files, the private key and corresponding certificate are imported to the token. The user is asked if the CA certificates should be imported to the token, and the password (if it exists) that protects the PFX file must be entered.

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.
   b. In the right pane, click the Import Certificate icon: 
   c. In the left pane, right-click the node of the required token, and select **Import Certificate** from the shortcut menu.

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

   The Import Certificate window opens.

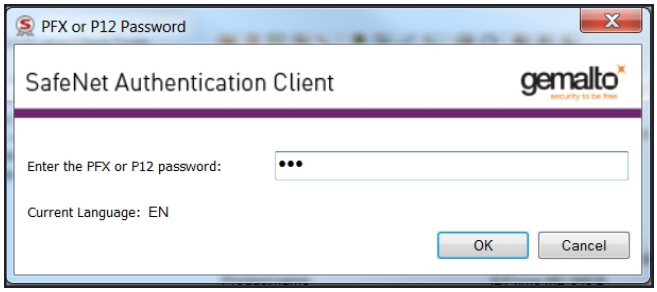


4. Select one of the following:
   a. Import a certificate from my personal certificate store
   b. Import a certificate from a file
5. If you select Import a certificate from my personal certificate store, a list of available certificates is displayed.

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

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

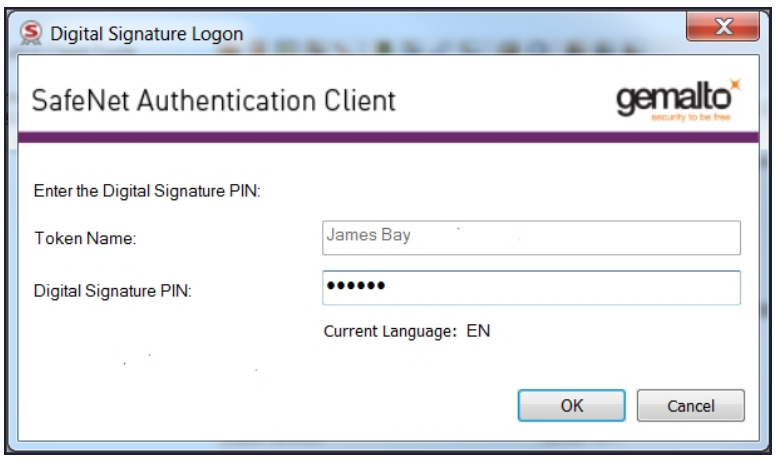
The **Certificate Password** window opens.



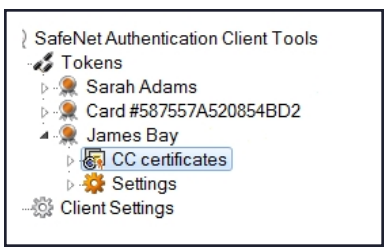
7. Enter the certificate password, and click OK.

   The **Digital Signature Logon** window opens

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



8. Enter the **Digital Signature PIN** and click **OK**.
9. The certificate is imported, and a message confirms that the import was successful.
10. 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:

   a. Select the required certificate, and click the **Export Certificate** icon: 

   b. 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.

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:

   a. In the left pane, select User Certificates.

   In the right pane, click the **Reset Default Certificate Selection** icon.

   b. 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:
   a. In the left pane, select the required certificate, and click the Delete Certificate icon.
   b. In the left pane, right-click the required certificate, and select Delete Certificate from the shortcut menu.

   The **Delete Certificate** window opens.
4. To delete the certificate, click **Yes**.

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

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

> **NOTE** If 'Read Only' mode is enabled, the certificate will not be deleted. For more information, see the SafeNet Authentication Client Administrator Guide.

Logging On to the Token as an Administrator

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

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

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

- Changing the Administrator Password
- Setting a Token Password by an Administrator
- 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:
   a. In the left pane, select the node of the required token.

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

   The **Administrator Logon** window opens.
3. Enter the token's Administrator Password, and click **OK**.

   You are logged on as an administrator.

Changing the Administrator Password

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

To change the Administrator Password:

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 **Change Administrator Password** icon.
   b. 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 device becomes locked.
>
> Ensure the password complies with the password quality settings: A secure password has at least 8 characters and at least three of the following rules:
> Uppercase letters; Lowercase letters; Numerals; Special Characters.

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

Setting a Token Password by an Administrator

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

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

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

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

   A message confirms that the token password was changed successfully.
6. 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.

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.

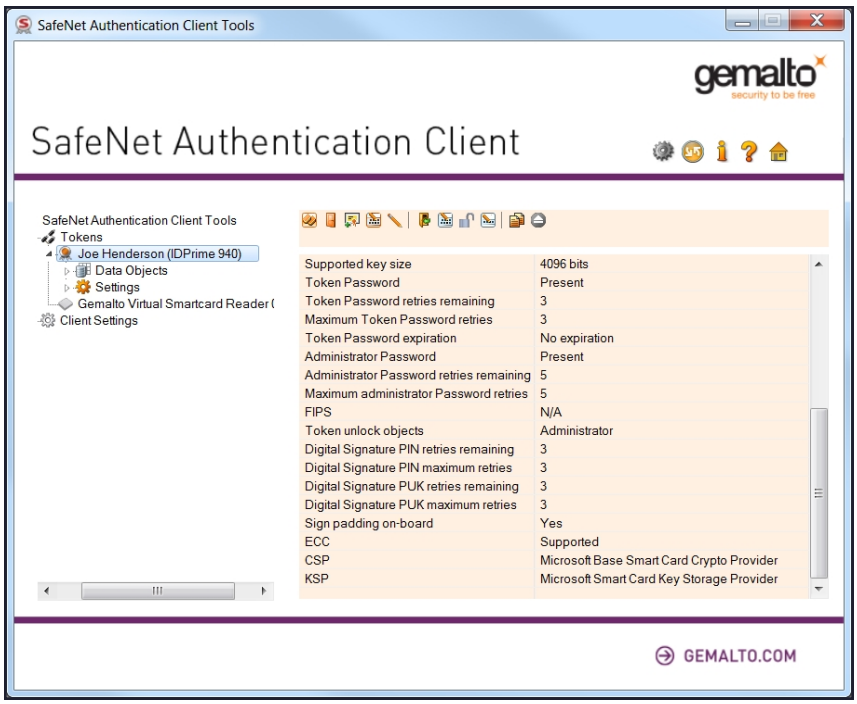
To see which Cryptographic Providers are supported on the token:

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.

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

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.

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.
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.

CHAPTER 4: PIN Pad Readers

Using PIN Pad Readers with SAC

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

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

PIN Pad Readers with IDPrime Cards

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

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

> IDPrime MD 830/3810/930/3930 - Role 1 (User) only

> **NOTE** The PIN entry 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.

Changing a User Password using a PIN Pad Reader

To change a User Password using the PIN Pad Reader:

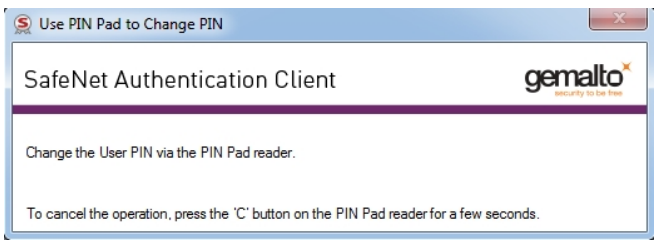
To perform this operation, the Token password must be changed on first logon option must be selected See "Must Change Password" on page 75).

1. Insert the device into the smart card reader.

   The following message appears: **For security reasons, you must change the Token Password.**

2. Click **OK**.

   The Use PIN Pad to Change PIN notification appears.



3. On the PIN Pad Reader, perform the following:

   a. Enter Current PIN and press **OK**.

   b. Enter New PIN and press **OK**.

   c. Confirm New PIN and press **OK**.

   The PIN Pad Reader displays: **PIN Changed**.

   > **NOTE** When using a Gemalto IDPrime 840 device with 'Must change password on first login', you will be required to log in again.

   SAC displays the message: **Password Changed Successfully**.

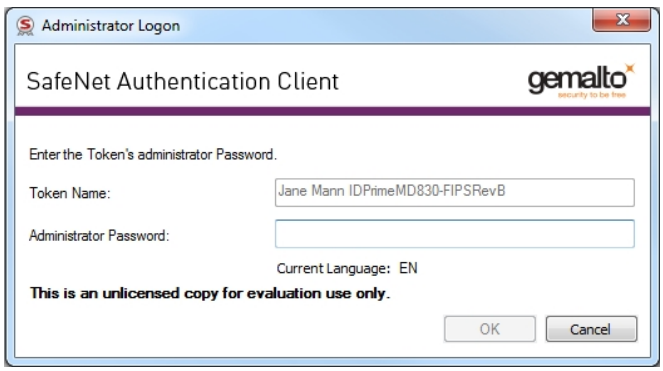
Setting a Token Password by an Administrator

For an Administrator to set a token password:

1. Insert the device into the smart card reader.
2. Click the **Set Token Password** icon .

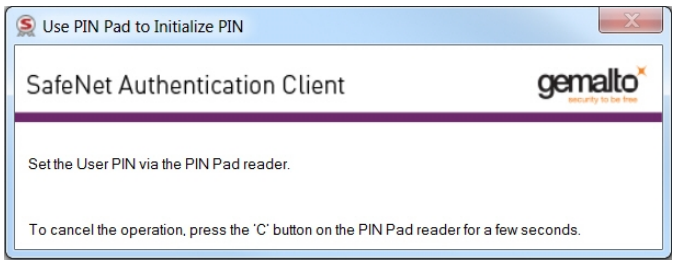
   The Set the User PIN via the PIN Pad reader notification appears.
   For more details, See "Setting a Token Password by an Administrator" on page 42.

   The Administrator Logon window opens.



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

   The **Set the User PIN via the PIN Pad** reader notification appears.



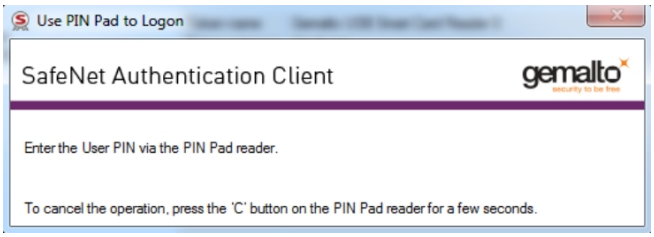
4. On the PIN Pad Reader, perform the following:
   a. Enter New PIN and press **OK**.
   b. Confirm New PIN and press **OK**.

   The PIN Pad Reader displays: **PIN Correct**.

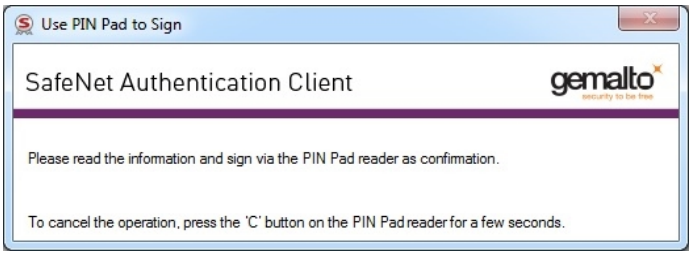
> **NOTE** Unlocking a Token by the Challenge Response Method displays the same PIN Pad notification.

   SAC displays the message: **Password Changed Successfully**.

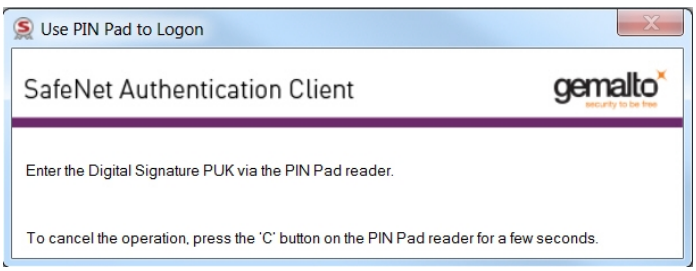
When performing a user operation, the following message appears:



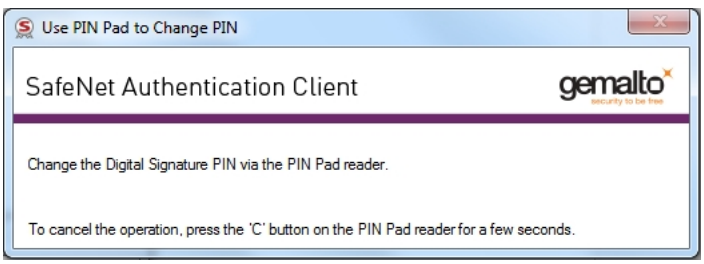
When performing a sign operation using a Common Criteria device, the following message appears:



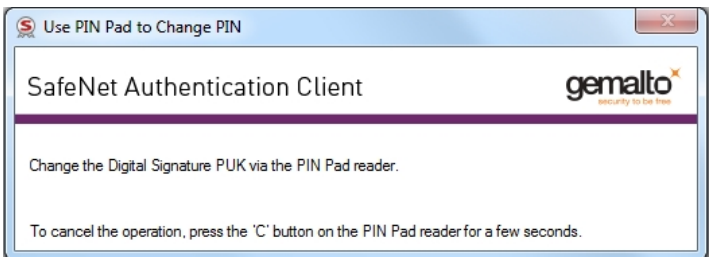
When changing a Digital Signature, the following message appears:



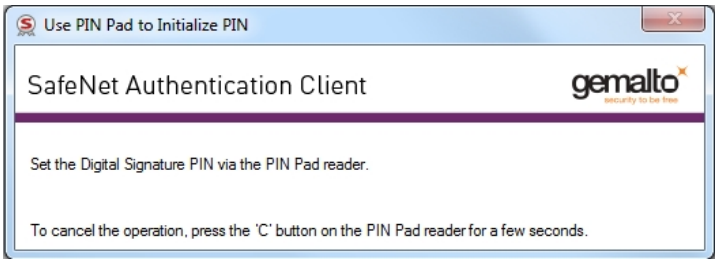
When changing a Digital Signature PIN, the following message appears:



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



When setting the Digital Signature PUK, the following message appears:



PIN Pad Functional Limitations

The following functional limitations exist with the PIN pad:

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

CHAPTER 5: Token Initialization

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

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 Cards - A new administrator password may be entered. If the current administrator password is to be maintained, select the option: 'Keep the current administrator password'.
- Administrator Password (optional)
- Maximum number of logon failures allowed
- Requirement to change the token password on the first logon
- Initialization key - (if supported by the device)
- 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.

Initialization Key Recommendations

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

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

Initializing eToken Devices

This section refers to the following devices:

- SafeNet eToken 5110
- SafeNet eToken 5110 FIPS
- Gemalto IDCore 30B eToken

> **NOTE** To initialize an eToken 5110 CC or eToken 5300 device, see "Initializing IDPrime Common Criteria Devices" on page 59.
>
> 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 device:

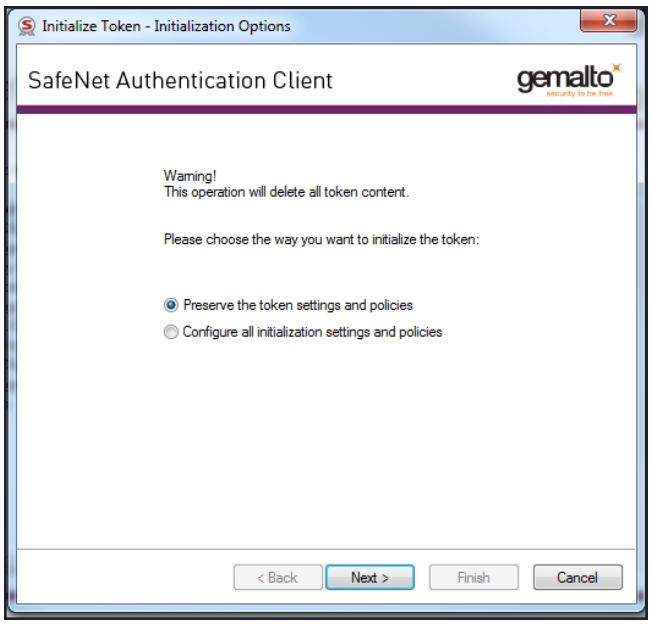
1. Open SafeNet Authentication Client Tools Advanced view.

   See "Opening the Advanced View" on page 15.
2. Do one of the following:
   a. In the left pane, select the node of the required token.

      In the right pane, click the Initialize Token icon: 
   b. 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.

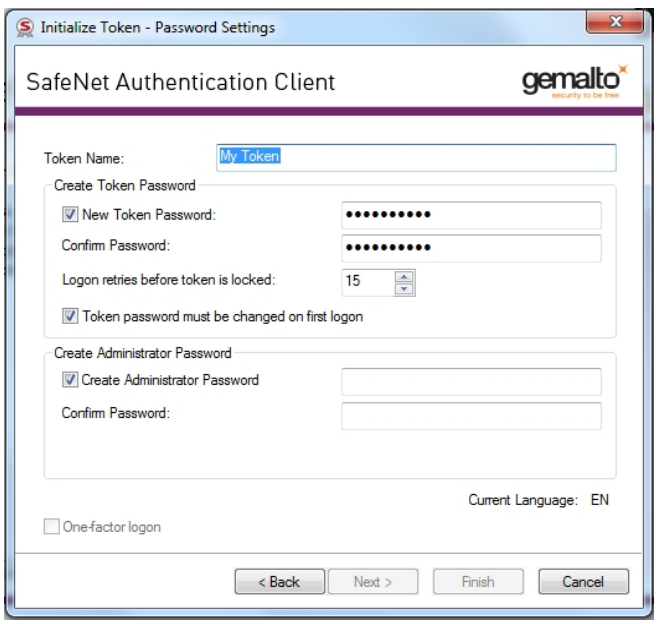
> **NOTE** Initializing a token deletes all objects that were created on the device, while it was in use.



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.



3. 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.
Confirm Password	Re-enter the administrator password.
Logon retries 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:** > The One-factor logon feature is used by eToken device only. > The One-factor logon feature is not supported by FIPS devices. Selecting the One-factor logon option disables the Create Token Password and Create Administrator Password fields. > The One-factor logon feature is used by eToken device only.

4. Click **Next**.

   The **Password Quality Settings** window opens.

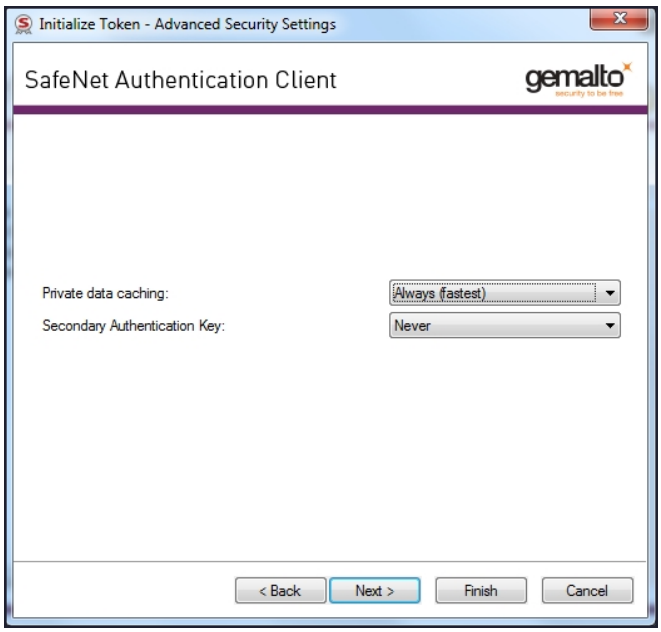
5. Complete the fields as follows:

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: 8 characters
Maximum length (characters)	Default: 16 characters
Minimum usage period (days)	The minimum period before the password can be changed. Default: 0 (none)
Maximum usage period (days)	The maximum period, in days, before which the password must be changed. Default: 0 (none)
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
Maximum consecutive repetitions	The maximum number of repeated characters that is permitted in the password. Default: 3

Field	Description
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 (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.

6. Click Next.

The **Advanced Security Settings** window opens.



Complete the fields as follows:

Field	Description
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. See "Setting Private Data Caching Mode (Advanced Tab)" on page 93.
Secondary Authentication Key	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. See"Setting RSA Key Secondary Authentication" on page 94.

7. Click **Next**.

   The **Initialization Key Settings** window opens.

   Use this window to configure Default 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.

8. 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.

9. Click **Finish**.

Initializing IDPrime Devices

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

The following can be performed during the initialization process:

> All user-generated data, such as certificates and profiles
> All PKCS#11 objects that were created on the token/card, while in use
> Token/card name/label
> Define a user and administrator password (the user password must be according to the card's policy settings).
> Define password quality settings
> Define a Digital Signature PIN and Digital Signature PUK password the password must be according to the card's policy settings (for IDPrime CC and eToken 5110 CC devices). See "Set Digital Signature PIN" on page 79.

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

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

Initializing IDPrime Common Criteria Devices

Common Criteria certified devices can be initialized using SAC Tools.

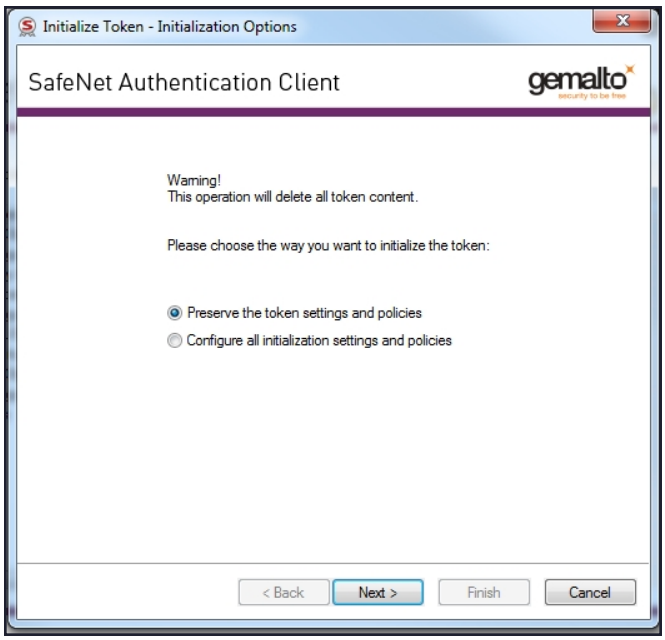
To initialize an IDPrime based Common Criteria certified device:

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.



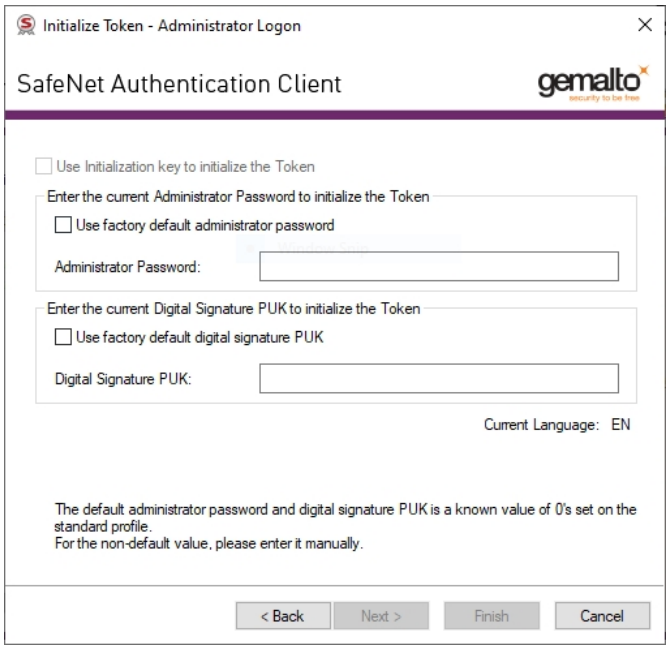
3. Select the following:

Field	Description
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.

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

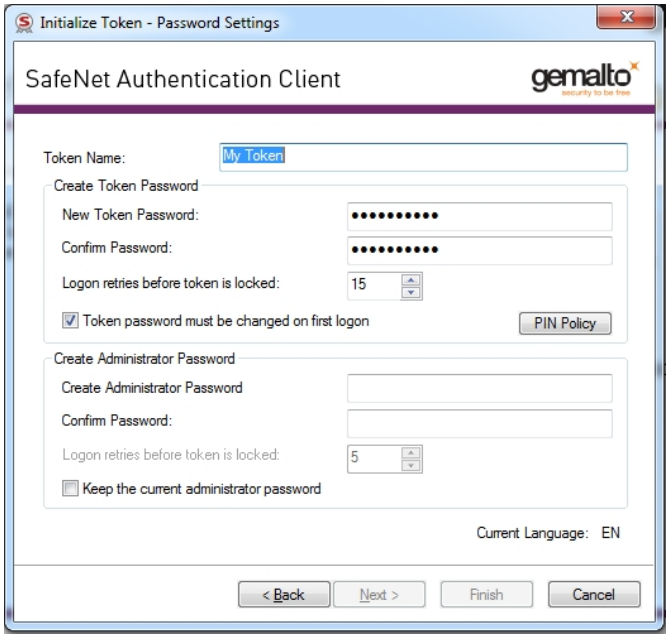


5. Enter the current Administrator Password and current Digital Signature PUK. The default Administrator Password is 48 zeros. The default Digital Signature PUK is 6 zeros.
6. Enter the following:

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.

Click **Next**.

The **Password Settings** window opens.



7. Enter the following:

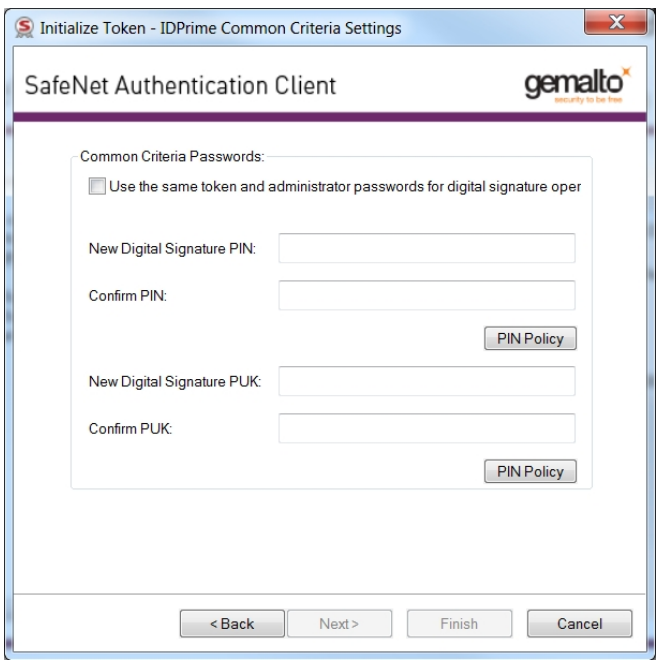
Token Name	Enter a name for the token. If no name is entered, a default name is used. In many organizations, the default token name is "My Token". The token name does not affect the token contents. It is used solely to identify the token.
New Token Password	The default password: 1234567890 automatically 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.

Token password must be changed on first logon	If required, select token password must be changed on first logon.
PIN Policy	Enables you to set PIN Quality/Property parameters. See "Setting IDPrime PIN Quality (PIN Quality Tab)" on page 95 and "Setting IDPrime PIN Properties (Advanced Tab)" on page 97)
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 "Friendly Admin Password" on page 74.
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).



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

When using a Common Criteria smart card (SafeNet IDPrime 940 or Gemalto IDPrime MD 840), if the Admin PIN is set to default, the unlock button will be disabled until changed. For example: When using a SafeNet IDPrime 940 or Gemalto IDPrime MD 840 card in linked mode, the Unlock Token button (in SAC Tools) will be disabled until the default Admin PIN is changed

9. 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 "Setting IDPrime PIN Quality (PIN Quality Tab)" on page 95 and "Setting IDPrime PIN Properties (Advanced Tab)" on page 97)
New Digital Signature PUK	Enter a New Digital Signature PUK.
Confirm PUK	Re-enter the New Digital Signature PUK.

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

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

Initializing IDPrime FIPS Devices (No Initialization Key)

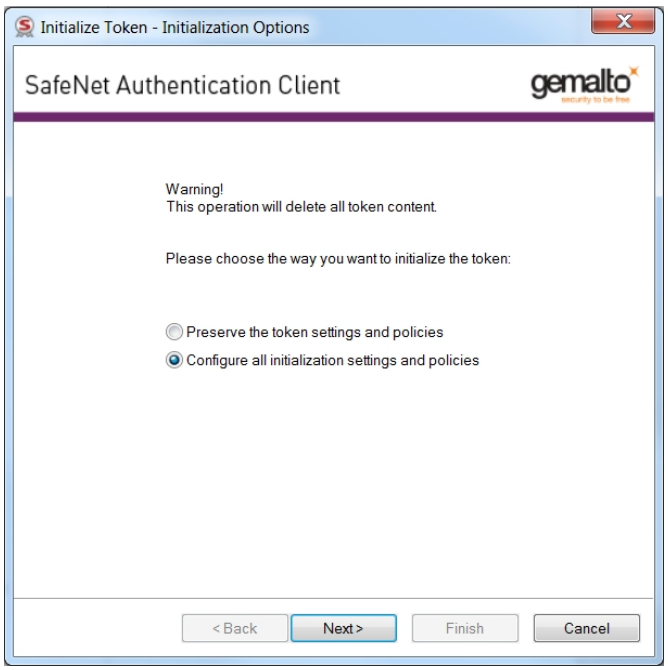
IDPrime cards that are FIPS certified can be initialized using SAC Tools.

To initialize an IDPrime FIPS device without an initialization key:

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

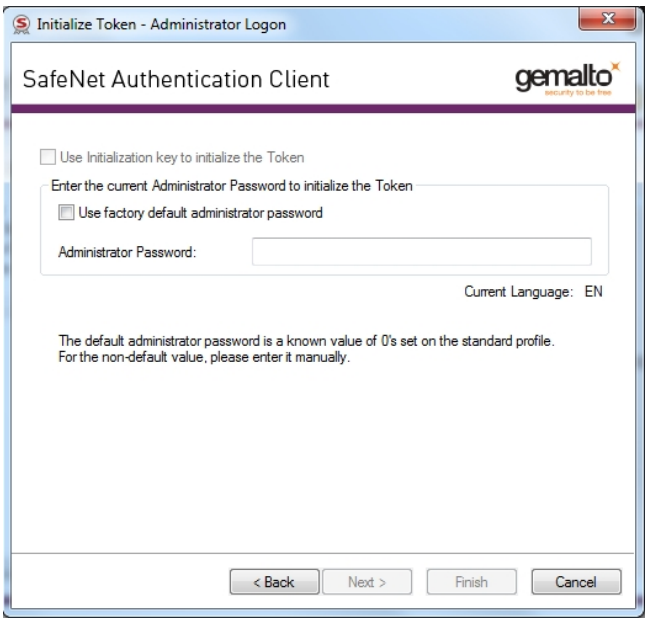


3. Select the following:

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.

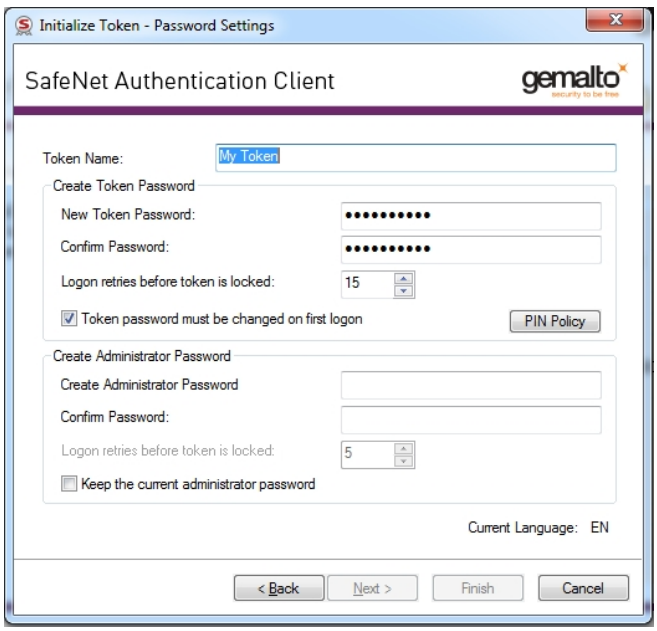
   The Administrator Logon window opens. This window requires you to enter an Administrator Password.



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

Use factory default administrator password	> Select this 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.

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

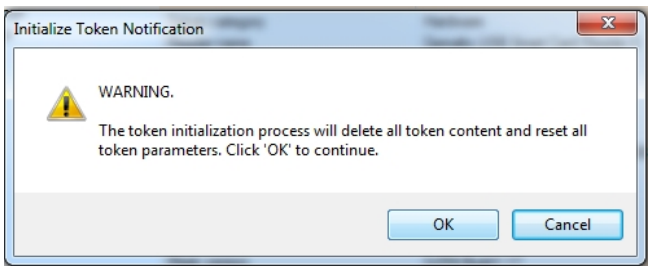


8. Enter the following:

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.
Token password must be changed on first logon	If required, select token password must be changed on first logon.
PIN Policy	Enables you to set PIN Quality/Property parameters. See "Setting IDPrime PIN Quality (PIN Quality Tab)" on page 95 and "Setting IDPrime PIN Properties (Advanced Tab)" on page 97)
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 "Friendly Admin Password" on page 74. **Note:** If the device has an initialization key (e.g. on IDPrime 930/3930 devices), this field can be disabled. If disabled, the Administrator - Logon retires before token is locked value changes to 1 and the Administrator Key becomes locked. This enables switching the device to the Non-Managed profile.
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. **Note:** This field may be read-only. It depends on your device type and the card configuration.
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.

9. Click **Finish**. A warning message is displayed.



10. Click **OK**

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

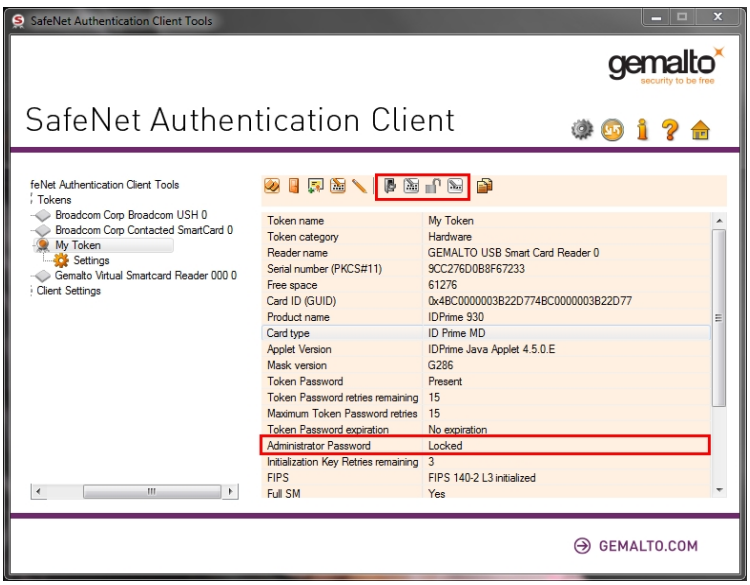
Initializing IDPrime FIPS Devices (with Initialization Key)

IDPrime cards that are FIPS certified can be configured during factory settings with either one of the following profiles:

- **Managed -** managed devices have an Administrator PIN and they have to be initialized according to the initialization sections above (See "Initializing IDPrime Common Criteria Devices" on page 59 and "Initializing IDPrime Devices (Non Common Criteria)").
- **Non-Managed -** non-managed devices have an Administrator PIN that is locked and cannot be used in Managed environments by CMS's. Non-managed devices may have an additional initialization key

  (e.g. SafeNet IDPrime 930/3930 devices), which allows initializing the device without using the Administrator PIN.

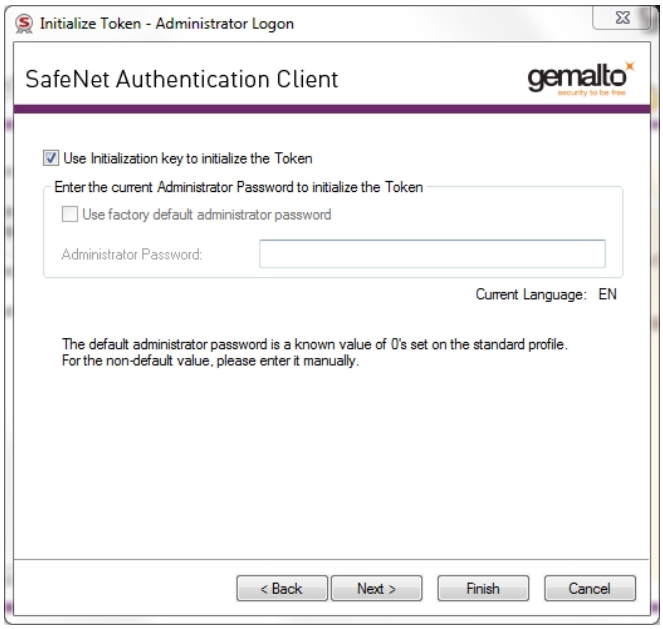
  A non-managed device is displayed in SAC Tools with the Administrator functions disabled:



To initialize a device using an initialization key:

1. Open SafeNet Authentication Client Tools Advanced view.
2. In the left pane, select the node of the required device.
3. In the right pane, click the **Initialize Token** icon .

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



4. Select **Use initialization key to initialize the Token**. This option appears only for devices that have an initialization key.
5. Click **Next**. The **Initialization Key Settings** window opens.

6. In the **Default Initialization Key** section, complete the fields as follows

Use Default initialization Key	Select this for SAC to use the initialization key that is already on the device (configured during factory settings). **Note:** If the default initialization key was not changed during factory settings, select this option.
Use this initialization key	Enter the current initialization key (if the default was changed during the previous initialization process).

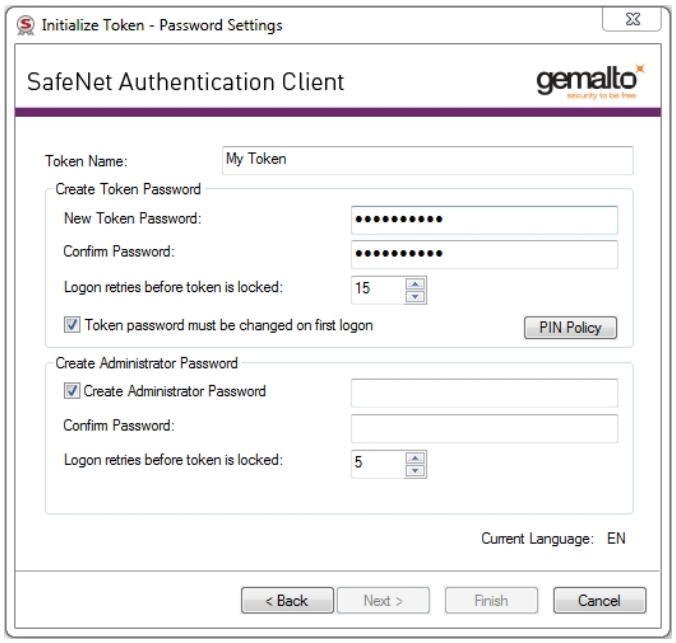
7. Under **Next Initialization Key**, set the new initialization key.

   See "Token Initialization" on page 52 ("To initialize an eToken device:" on page 53)

> **NOTE** Initialization Key policy:
>
> A secure password has at least 8 characters (up to 32 characters) and contains at least 3 of the following rules:
> -Upper case letters
> -Lower case letters
> -Numerals
> -Special characters (&, %, $, etc.)

8. Click **Next**.

   The **Password Settings** window opens.



9. 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.
Token password must be changed on first logon	If required, select token password must be changed on first logon.
PIN Policy	Enables you to set PIN Quality/Property parameters. See "Setting IDPrime PIN Quality (PIN Quality Tab)" on page 95 and "Setting IDPrime PIN Properties (Advanced Tab)" on page 97)
Create Administrator Password	Perform either one of the following: > Create a new Administrator Password by selecting the Create Administrator Password check-box. You can set the Administrator Password to a password that is between 8-32 alphanumeric characters. See "Friendly Admin Password" on page 74. The device will be initialized with the **Managed profile**. > Deselect the Create Administrator Password check-box in order to initialize the device using the **Non-Managed profile**. In the Non-Managed profile, the Administrator - Logon retires before token is locked value changes to 1 and the Administrator Key becomes locked.
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. **Note:** This field may be read-only. It depends on your device type and the card configuration.

10. Click **Finish**. Your device begins the initialization process.

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.

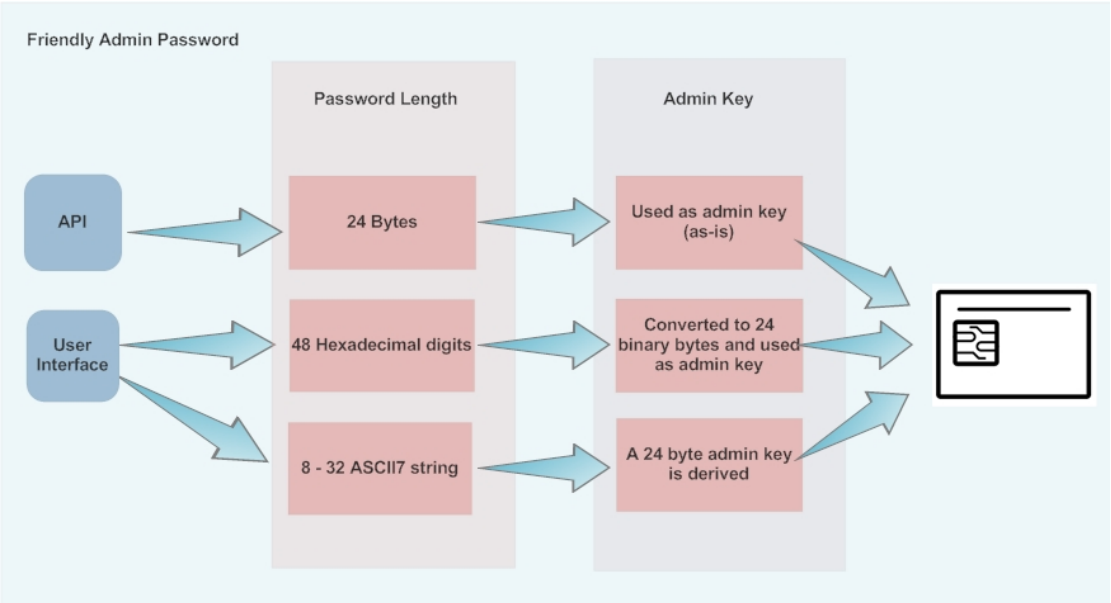
Without the Friendly Admin Password, SafeNet Minidriver and SAC require a 48 Hexadecimal PIN.

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 password is made up of 8-23 or 25-32 ASCII7 characters, which derives a 24 byte long Admin Key. The password is made up of 24 ASCII7 characters and is used without derivation.

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



CHAPTER 6: Common Criteria

SafeNet Authentication Client supports the Gemalto IDPrime Common Criteria card range. See the SafeNet Authentication Client Release Notes for a list of supported cards.

Working with Common Criteria Certified Tokens and Cards

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

PKCS#11 Digital Signature PIN Authentication

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

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

The application must then call C_Login on the virtual slot as a CKU_USER to provide the qualified Digital Signature PIN (PIN role #3).

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

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

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

Must Change Password

When using a PIN Pad with a card that's configured with the Token password must be changed on first logon (for User PIN and/or Digital Signature PIN), when first logging in, the password must be changed using the keyboard. Subsequently, the PIN Pad reader is used to change the password.

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

Common Criteria Extended Functions

The following Digital Signing function icons are displayed in SAC Tools advanced view

User Function	Icon	Right-Click Menu
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

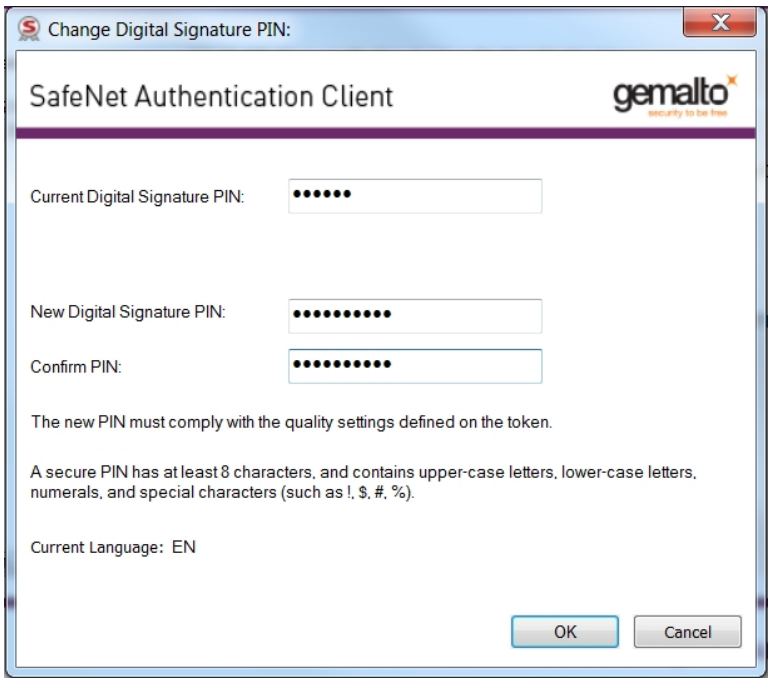
Use this option to change the Digital Signature PIN.

To change a digital signature PIN:

1. Open SafeNet Authentication Client Tools Advanced view.
2. 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.



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

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

Change Digital Signature PUK

Use this option to change the Digital Signature PUK.

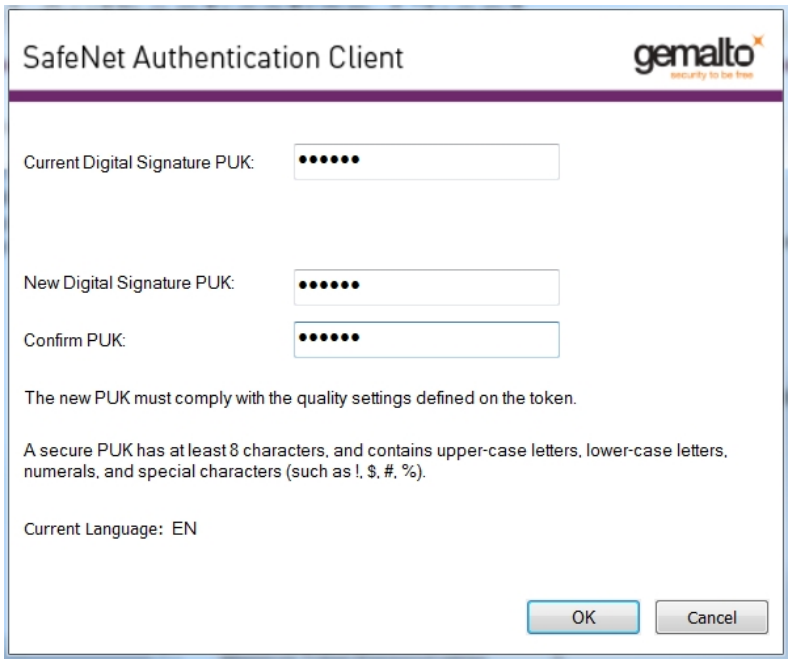
To change a digital signature PUK:

1. Open SafeNet Authentication Client Tools Advanced view.
2. 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.



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

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

Set Digital Signature PIN

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

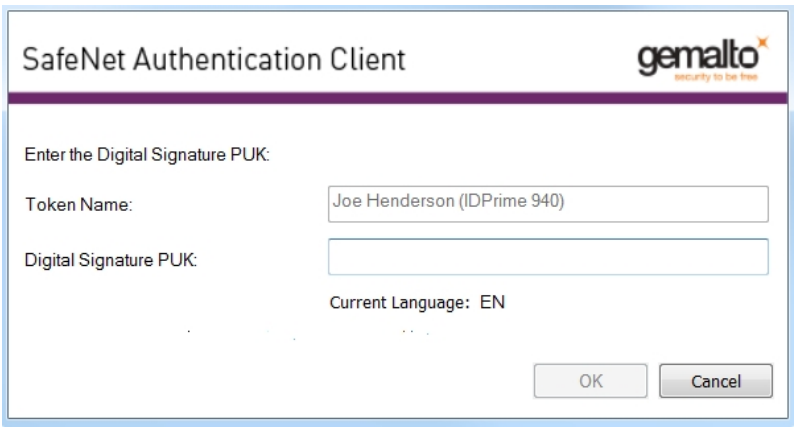
To set a digital signature PIN:

1. Open SafeNet Authentication Client Tools Advanced view.
2. 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.



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

   The **Set PIN** window opens.

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

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

   The **Password Changed Successfully** window opens.

6. Click **OK**.

Operational Differences and Role Protection

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

Operation	**Password required to perform the specified operation on:** > **eToken 5100 CC (legacy)**	**Password required to perform the specified operation on:** > **SafeNet IDPrime 940/3940** > **IDPrime 840/840 B/3840/3840B,** > **IDPrime 8840 Micro SD Card** > **eToken 5110 CC**
Initialize	Initialization Key	Administrator Password
Generate sign only key pair	Token Password	Token Password + Digital Signature PIN
Generate exchange key pair	Token Password	Token Password
Import sign only key pair	Import Password	Token Password + Digital Signature PIN
Import exchange key pair	Token Password	Token Password
Delete sign only key pair	Token Password	Token Password + Digital Signature PIN
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

CHAPTER 7: SafeNet eToken 5300

SafeNet eToken 5300 is an ideal solution for enterprises looking to deploy the military-grade security of PKI, while maintaining a convenient solution for employees. The eToken 5300 is a compact, tamper-evident USB with presence detection, which creates a third factor of authentication. Something you have (physical token), something you know (PIN), something you do (enabling touch sensor). The eToken 5300 offers multi-application dynamic smart card functionality. It can be used with any USB connection for Identity and Access Management applications such as network authentication, digital signatures, email encryption and other advanced services based on Public Key Infrastructure (PKI). The eToken 5300 is certified FIPS 140-2 L3 at the full token boundary. With the Presence Detection feature, enterprise IT can allow single sign on for employees by requiring a user PIN only at logon. That way, employees can use the advance functionality of PKI, such as digitally signing documents and encrypting email by simply touching the sensor on the token, which provides authentication without entering a PIN multiple times. If enterprise IT want more control of specific certificates they can set rules to either always require the user to enter a password or always require both user password and sensor activation when accessing those particular certificates.

eToken 5300 Certificates

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

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

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

The eToken 5300 is available in the following configurations:

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

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

Viewing eToken 5300 information

To view eToken 5300 touch sense configurations in SAC Tools:

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

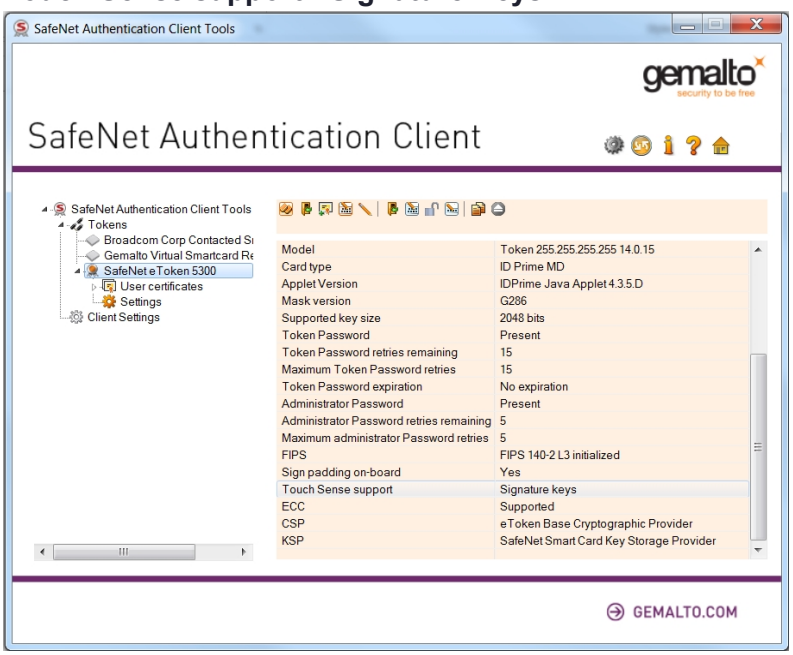
      The SafeNet Authentication Client Tools window opens in the Simple view.
2. Click the Advanced View icon.

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

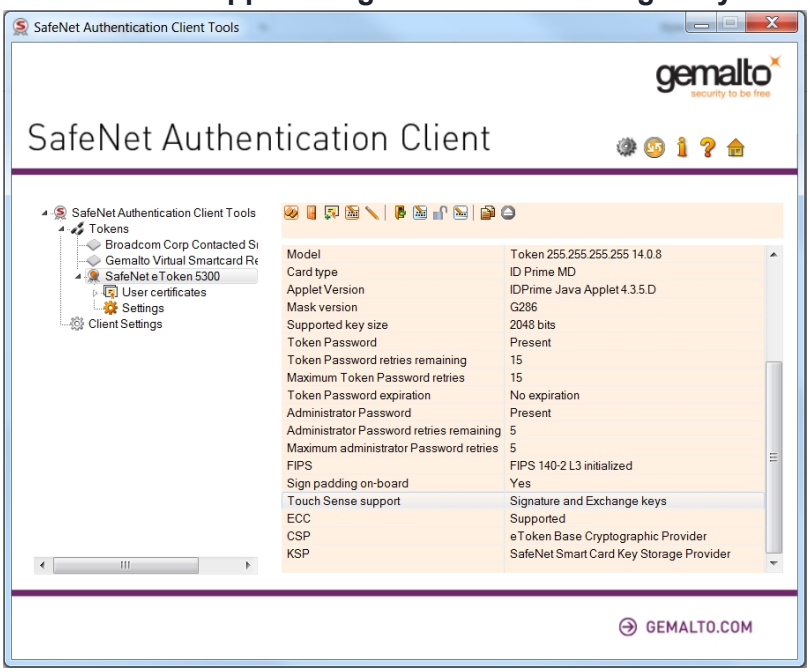
   The Token's Information is displayed.

> **NOTE** Configuration information displayed in SAC Tools varies depending on how the token was received from the factory.

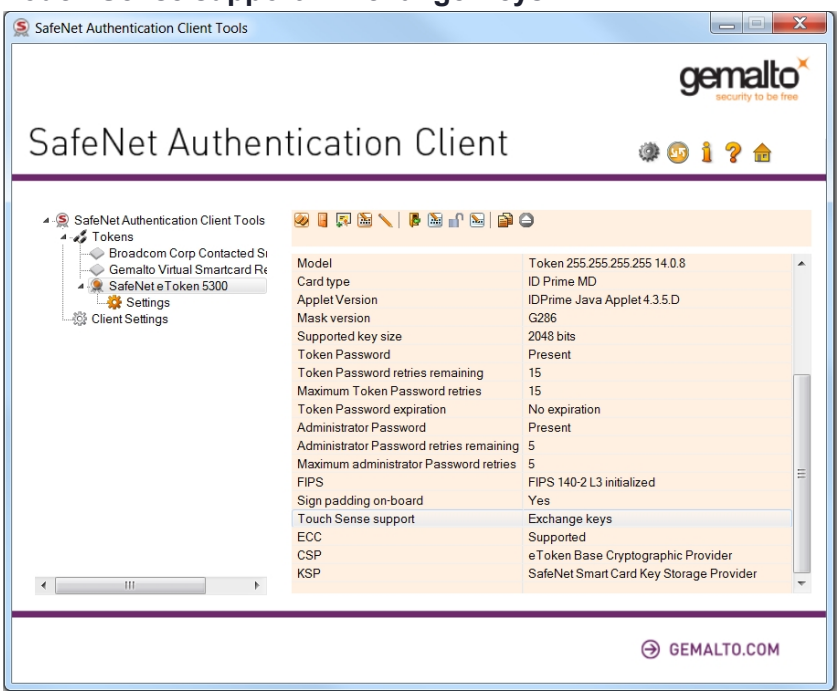
Touch Sense support - Signature Keys



Touch Sense support - Signature and Exchange Keys

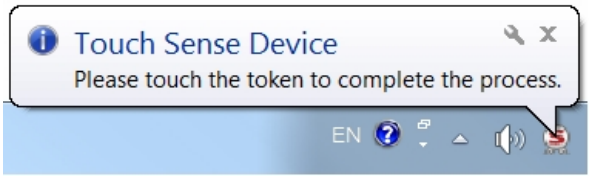


Touch Sense support - Exchange Keys



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.



> **NOTE** For more details, see the Touch Sense Notify property in the SafeNet Authentication Client Administrator Guide.

eToken 5300 Touch Sense Timeout and Grace period

Touch Sense Timeout

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

Touch Sense Grace Period

The eToken 5300 has a 30 second grace period.

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

CHAPTER 8: Client Settings

Client Settings are parameters that are saved to the computer and apply to all tokens that are initialized on the computer after the settings have been configured. Use token settings to determine behavior that applies to a specific token. See Chapter 9: “Token Settings” on page 87.

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 91.
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 12.
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:
   a. Change the Password Quality settings, and click **Save**.

   > **NOTE** The Password Quality settings are configured the same way as the Token Password quality settings. See Chapter 9: Setting eToken Password Quality (Password Quality Tab), on page 87.

   b. To ignore your changes, click Discard.
   c. 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 12.
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 12.
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 12.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab.
4. Do one of the following:
   a. To enable Single Logon for MS Cryptography, select **Enable single logon**.
   b. To enable Single Logon for MS Cryptography and PKCS#11 cryptography, select **Enable single logon** and then select **Enable single Logon for PKCS#11**.

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.

To enable password quality configuration after initialization:

1. Open SafeNet Authentication Client Tools Advanced view.

   See "Opening the Advanced View" on page 12.
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 12.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab.
4. Do one of the following:
   a. To enable configuration by the administrator only, select **Allow only an administrator to configure password quality on token**.
   b. 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 12.
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 12.
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 12.
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 12.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab, and click **Disable Logging**.

CHAPTER 9: Token Settings

Configurations set in the selected token's Settings tab determine behavior that applies to the specific token. For configurations set in Client Settings, that apply the settings to all tokens that are initialized after the settings have been configured, see "Client Settings" on page 85.

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 "SafeNet Authentication Client User Interface" on page 9.
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)
Minimum usage period (days)	The minimum period before the password can be changed. Default: 0 (none)
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

Password Quality Parameter	Description
Maximum consecutive repetitions	The maximum number of repeated characters that is permitted in the password. Default: 3
Must meet complexity requirements	Determines the complexity requirements that are required in the token password. > **At least 2 types:** a minimum of 2 complexity rules (out of the 4 shown in the Manual Complexity fields) are enforced. > **At least 3 types:** a minimum of 3 complexity rules (out of the 4 shown in the Manual Complexity fields) are enforced (Default). > **None:** Complexity requirements are not enforced. > **Manual:** Complexity requirements, as set manually in the Manual Complexity settings, are enforced.
Manual complexity rules	For each of the character types (**Numerals, Upper-case letters, Lower-case letters, and Special characters**) select one of the following options: **Permitted -** Can be included in the password, but is not mandatory (Default). **Mandatory -** Must be included in the password. **Forbidden -** Must not be included in the password.

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

Setting Private Data Caching Mode (Advanced Tab)

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

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 smart card) can be cached outside the token.

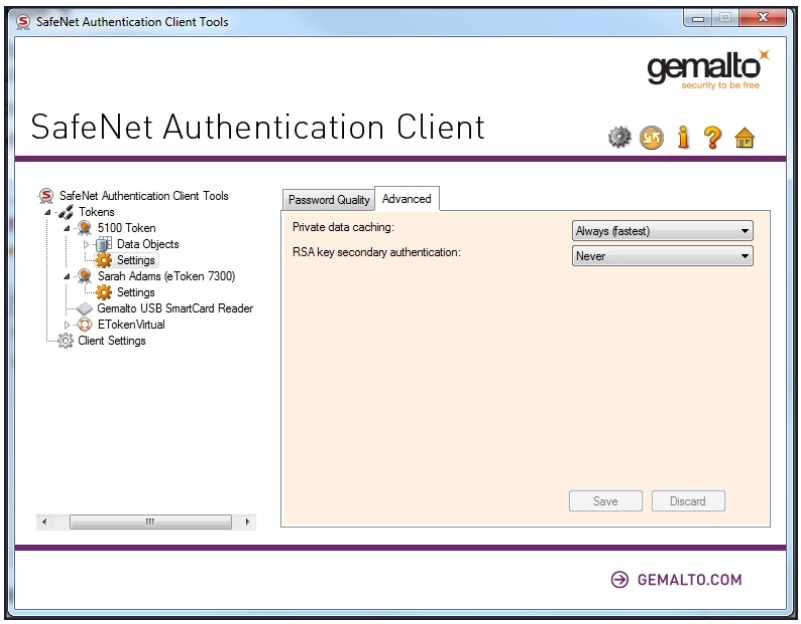
To set private data caching mode:

1. Open SafeNet Authentication Client Tools Advanced view.

   See "Opening the Advanced View" on page 12.

2. In the left pane, expand the node of the required token, and select **Settings**.
3. In the right pane, select the **Advanced** tab.

   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. Click **Save** to save your changes or click **Ignore** to discard your changes.

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 supported on eToken devices only.

To set RSA key secondary authentication:

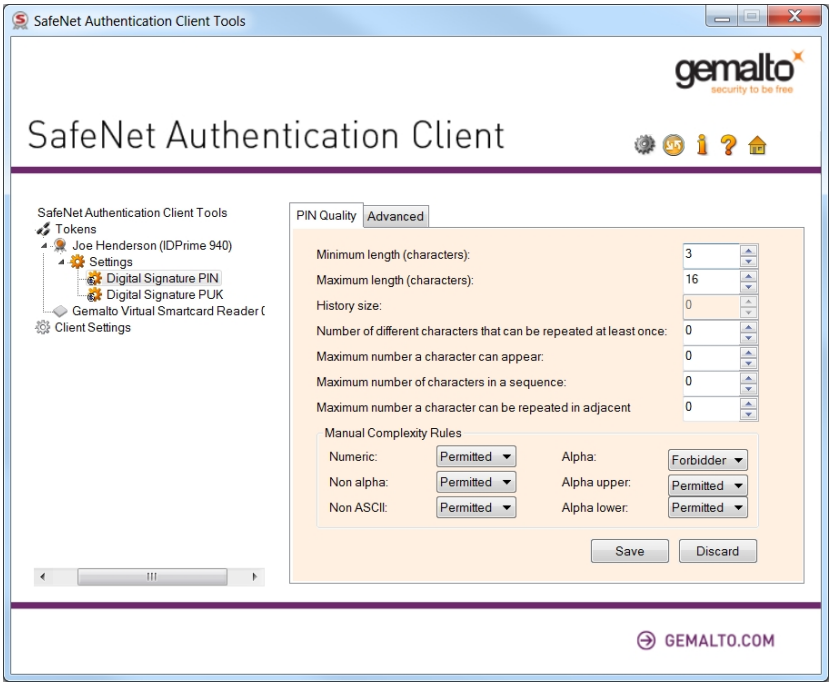
1. Open SafeNet Authentication Client Tools Advanced view.

   See "Opening the Advanced View" on page 12.
2. In the left pane, expand the node of the required token, and select **Settings**.
3. In the right pane, select the **Advanced** tab.
4. In the **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: Initializing IDPrime Devices, on page 57.
5. Do one of the following:
   a. To save your changes, click **Save**.
   b. 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:

Password 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

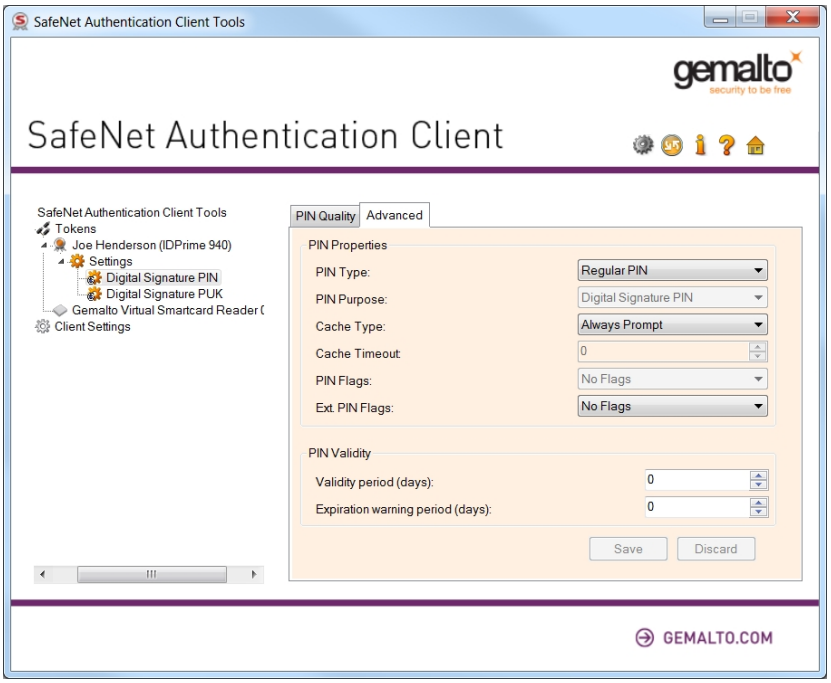
Password Quality Parameter	Description
Maximum number of times a character can appear	The maximum number of times a character can appear. Range is 00h-FFh. 00h = No limitation
Maximum number of character in a sequence	Max length of characters sequences e.g. 1,2,3,4 or a,b,c,d. Range is 00h-FFh. (For 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.

To set IDPrime PIN Properties:

1. Select **Settings** in the left pane, to view the User PIN Quality/Advanced fields in the right pane.
2. Select **Digital Signature PIN** in the left pane, to view the Digital Signature PIN Quality/Advanced fields in the right pane.
3. Select **Digital Signature PUK** in the left pane, to view the Digital Signature PUK Quality/Advanced fields in the right pane.



The following PIN Quality parameters exist on IDPrime devices:

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 Property Parameter	Description
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 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) **Note:** The PIN validity settings (Validity period and Expiration warning period) cannot be modified when using IDPrime MD 830A

PIN Property Parameter	Description
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 Devices (page 57).