SafeNet Authentication Client

Version 9.0 (GA)

Windows, Linux and Mac

User's Guide

All attempts have been made to make the information in this document complete and accurate.

SafeNet, Inc. is not responsible for any direct or indirect damages or loss of business resulting from inaccuracies or omissions. The specifications contained in this document are subject to change without notice.

SafeNet and SafeNet Authentication Client are either registered with the U.S. Patent and Trademark Office or are trademarks of SafeNet, Inc., and its subsidiaries and affiliates, in the United States and other countries. All other trademarks referenced in this Manual are trademarks of their respective owners.

SafeNet Hardware and/or Software products described in this document may be protected by one or more U.S. Patents, foreign patents, or pending patent applications.

Please contact SafeNet Support for details of FCC Compliance, CE Compliance, and UL Notification.

Document Name: SAC 9.0 (GA) - User’s Guide (Windows, Linux and Mac)

Document Part Number: 007-012831-001, Revision B

Date of publication: February 2015

Last update: Sunday, February 08, 2015 8:58 am

Support

We work closely with our reseller partners to offer the best worldwide technical support services. Your reseller is the first line of support when you have questions about products and services. However, if you require additional assistance you can contact us directly at:

Telephone

You can call our help-desk 24 hours a day, seven days a week:
USA: 1-800-545-6608
International: +1-410-931-7520

Email

You can send a question to the technical support team at the following email address:
support@safenet-inc.com

Website

You can submit a question through the SafeNet Support portal:
https://serviceportal.safenet-inc.com

Additional Documentation

The following SafeNet publications are available:

- SafeNet Authentication Client 9.0 (GA) Administrator’s Guide
- SafeNet Authentication Client 9.0 (GA) Customer Release Notes (CRN)

Table of Contents

1 Introduction

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

In this chapter:

Overview

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

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

SafeNet Authentication Client Main Features

SafeNet Authentication Client incorporates features that were supported by previous releases of eToken PKI Client and SafeNet Borderless Security (BSec). It provides a unified middleware client for a variety of SafeNet smartcards, SafeNet iKey tokens, and SafeNet eToken devices.

SafeNet Authentication Client offers full backward compatibility so that customers who have been using eToken PKI Client or SafeNet Borderless Security Client (BSec) can continue to use deployed eToken and iKey devices.

What’s New

SafeNet Authentication Client 9.0 offers the following new features:

- **eToken 7300 Flash usage procedures are now supported on Windows, Linux, and Mac** - Usage operations (performed via all operating systems) include:
  - Log On to Flash/Log Off from Flash
  - CD-ROM update
  - Firmware update (Windows only)
- **eToken 7300 unified bundle is now supported on Mac operating system**
- **New Linux operating systems are now supported New and enhanced UI across all platforms** - Previous versions of SAC supported the QT cross-platform framework. SAC 9.0 now supports an innovative technology that maintains the unique look and feel of each underlying (native) platform (Windows, Linux, and Mac).
- **Additional custom installation options** - The installation of SAC 9.0 enables selecting specific customized features to be installed. For example, BSec compatibility mode is now available through the custom installation options.
- **Installation file size reduced** - The Windows, and Linux installation file size has been reduced significantly.
- **Mac Yosemite support** – SAC 9.0 now supports the MAC Yosemite operating system.

- **Sac (Mac) custom installation and configuration installation file**- This is a separate custom installation file, which enables administrators to distribute the SAC license and configuration installation file (SafeNet Authentication Client Customization 9.0.mpkg) to the organization. For details on how the administrator creates this file, see the SAC Administrator’s Guide.

Supported Browsers

SafeNet Authentication Client 9.0 (Windows) supports the following browsers:

- Firefox
- Internet Explorer 7, 8, 9, 10, 11, Metro
- Chrome version 14 and later, for authentication only (does not support enrollment)

SafeNet Authentication Client 9.0 (Linux) supports the following browsers:

- Firefox

SafeNet Authentication Client 9.0 (Mac) supports the following browsers:

- Safari
- Firefox
- Chrome

Supported Platforms

SafeNet Authentication Client 9.0 (Windows) supports the following operating systems:

- Windows Vista SP2 (32-bit, 64-bit)
- Windows Server 2008 R2 SP1 (32-bit, 64-bit)
- Windows Server 2008 SP2 (32-bit, 64-bit)
- Windows Server 2012 (64-bit)
- Windows Server 2012 R2 (64-bit)
- Windows 7 SP1 (32-bit, 64-bit)
- Windows 8 (32-bit, 64-bit)
- Windows 8.1 (32-bit, 64-bit)

NOTE

- In Windows 8.1 environments, SafeNet eToken 7300 devices earlier than version 9.0.35 can be used only when SafeNet Authentication Client is installed.

SafeNet Authentication Client 9.0 (Linux) supports the following operating systems:

- Red Hat 6.6, 7.0 (32-bit and 64-bit)
- Ubuntu 13.10, 14.04 (32-bit and 64-bit)
- Debian 7.7 (32-bit and 64-bit)
- SUSE Enterprise Desktop 11.3 (32-bit and 64-bit), 12.0 (64-bit)
- CentOS 6.6 (32-bit and 64-bit), 7.0 (64-bit)

- Fedora 20 (32-bit and 64-bit)

SafeNet Authentication Client 9.0 (Mac) supports the following operating systems:

- Mac OS X 10.9 (Mavericks)
- Mac OS X 10.10 (Yosemite)

Tablets

SafeNet Authentication Client 9.0 supports the following Tablets:

- Lenovo ThinkPad Tablet running Windows 8
- Microsoft Surface Pro running Windows 8.1

Thin Clients

SafeNet Authentication Client 9.0 supports the following Thin Clients:

- HP - T310/T410
- Wyse - P Class
- Oracle - SunRay DTU
- Dell - Wyse C10LE

Supported Tokens

SafeNet Authentication Client 9.0 supports the following tokens:

Certificate based USB tokens

- SafeNet eToken PRO Java 72K
- SafeNet eToken PRO Anywhere
- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID

Smart cards

- SafeNet eToken PRO Smartcard 72K
- SafeNet eToken 4100

Certificate based hybrid USB tokens

- SafeNet eToken 7300
- SafeNet eToken 7300-HID
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)

Software tokens

- SafeNet eToken Virtual
- SafeNet eToken Rescue

End-of-Sale tokens/smart cards

- SafeNet iKey: 2032, 2032u, 2032i (Windows and Mac only)
- SafeNet Smartcard: SC330, SC330u, SC330i
- SafeNet eToken 7100 (SafeNet eToken NG-Flash)
- SafeNet eToken 5000 (iKey 4000)
- SafeNet eToken 4000 (SC400)
- SafeNet eToken 4000 (SC400)
- eToken PRO 32K v4.2B
- eToken PRO 64K v4.2B
- eToken Pro SC 32K v4.2B
- eToken Pro SC 64K v4.2B

NOTE
SafeNet Authentication Client 9.0 (Linux) supports only Smart Card manageability for SafeNet eToken 7300. Storage management functionality such as Partitioning, Initialization, Image burning, etc. will only be available in SAC 8.2 for Windows and up.

External Smart Card Readers

SafeNet Authentication Client 9.0 (GA) supports the following smart card readers:

- SCR 3310 v2 Reader

- Athena AESDrive IIIe USB v2 and v3
- ACR
- Athena Keyboard
- GemPC CCID
- Omnikey 3121
- Dell Broadcom
- Unotron

> **NOTE**
>
> - Reader drivers must be compatible with the extended APDU format in order to be used with RSA-2048.
> - The latest CCID Driver must be installed when using Athena v3.

Supported Localizations

> **NOTE**
> SafeNet Authentication Client 9.0 supports **all** languages for Windows and only English for Linux and Mac.

SafeNet Authentication Client 9.0 (Windows) supports the following languages:

- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- English
- French (Canadian)
- French (European)
- German
- Hungarian
- Italian
- Japanese
- Korean
- Lithuanian
- Polish

- Portuguese (Brazilian)
- Romanian
- Russian
- Spanish
- Thai
- Vietnamese

2 SafeNet Authentication Client User Interfaces

This section describes the SafeNet Authentication Client user interfaces.

> **NOTE**
> - If a customized version of SafeNet Authentication Client is installed, the graphics you see may be different from those displayed in this guide.
> - In some installations, the word **Password** is replaced by **PIN** or **Passcode**.
> - The screens displayed in this section have been taken from a Windows operating system. Linux and Mac operating system screens differ slightly from the Windows screens.

In this chapter:

Overview of SafeNet Authentication Client User Interfaces

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

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

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

> **NOTE** Do not remove the token from the USB port during an operation. This may cause corruption of data on the token.

SafeNet Authentication Client provides two user interfaces:

- SafeNet Authentication Client Tray Icon
  - for quick access to several token operations

- SafeNet Authentication Client Tools
    - provides information about each connected token, including its identification and capabilities.
    - can access information stored on each connected token, such as keys and certificates.
    - enables management of token content, such as password policy.

SafeNet Authentication Client Tray Icon

The SafeNet Authentication Client tray icon offers a shortcut menu to several token operations.

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

No Tokens Connected	One Token Connected	Multiple Tokens Connected

Running the SafeNet Authentication Client Monitor

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

NOTE
If SafeNet Authentication Client is open and the tray icon is not displayed in the Windows taskbar, see Chapter 7: *Showing the SafeNet Authentication Client Tray Icon* on page 166.

To open SafeNet Authentication Client on Windows:

- From the Windows taskbar, select **Start** > **Programs > SafeNet > SafeNet Authentication Client > SafeNet Authentication Client**.

To open SafeNet Authentication Client on Linux:

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

To open SafeNet Authentication Client on Mac:

- From the Mac desktop, select **Go** > **Applications > SafeNet > SafeNet Authentication Client > SafeNet Authentication Client**.

SAC Tray Menu Functions

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

- **Tools:** opens *SafeNet Authentication Client Tools*.
- **About:** displays product version information and license information, and enables license import.
- **Token selection:** allows you to select one of the connected tokens to be the active token. This function is available only when more than one token is connected.
- **Change Token Password:** opens the *Change Password* window for the selected token. See Chapter 3: *Changing the Token Password* on page 65.

- **Unlock Token:** opens the *Unlock Token* window for the selected token. See Chapter 3: *Unlocking a Token by the Challenge-Response Method* on page 69.
- **Certificate Information:** opens the *Token Certificate Information* window for the selected token.
- **Log On to Flash/Log Off from Flash:** displayed when a SafeNet eToken 7300 having a password-protected flash partition is connected. Opens the *Log On to Token* window for the selected token. See Chapter 3: *Logging On to the Token as a User* on page 61.
- **Exit:** closes SafeNet Authentication Client and the tray icon.

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

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

Opening the SafeNet Authentication Client Tray Menu from Windows, Linux, and Mac

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

- Right-click the SafeNet Authentication Client tray icon.

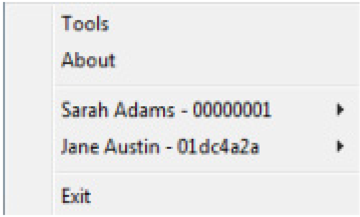
Selecting the Token from the SAC Tray Menu

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

To select from multiple tokens in the tray menu:

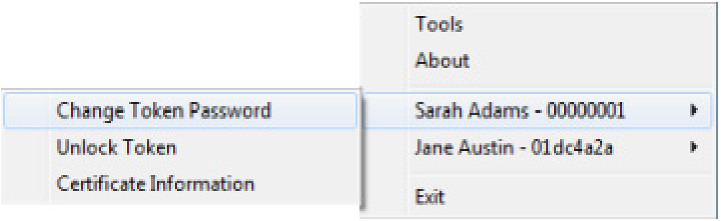
1 Right-click the SafeNet Authentication Client tray icon.

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 from Windows, Linux and Mac

To close SafeNet Authentication Client:

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

A warning message is displayed.

2 Click **OK**.

SafeNet Authentication Client Tools

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

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

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

SafeNet Authentication Client Tools includes two viewing options:

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

  See *Opening the Simple View* on page 33.

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

  See *Opening the Advanced View* on page 38.

Each view displays two panes:

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

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

SafeNet Authentication Client Tools Toolbar

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

Icon	Action
⚙	**Advanced View** – switches from the *Simple* to the *Advanced* view
⚙	**Simple View** – switches from the *Advanced* to the *Simple* view
↻	**Refresh** – refreshes the data for all connected tokens

Icon (Cont.)	Action (Cont.)
ℹ	**About** – displays product version information and license information, and enables license import
?	**Help** – opens the *Help* feature
🏠	**Home** – opens the company website

Opening the Simple View

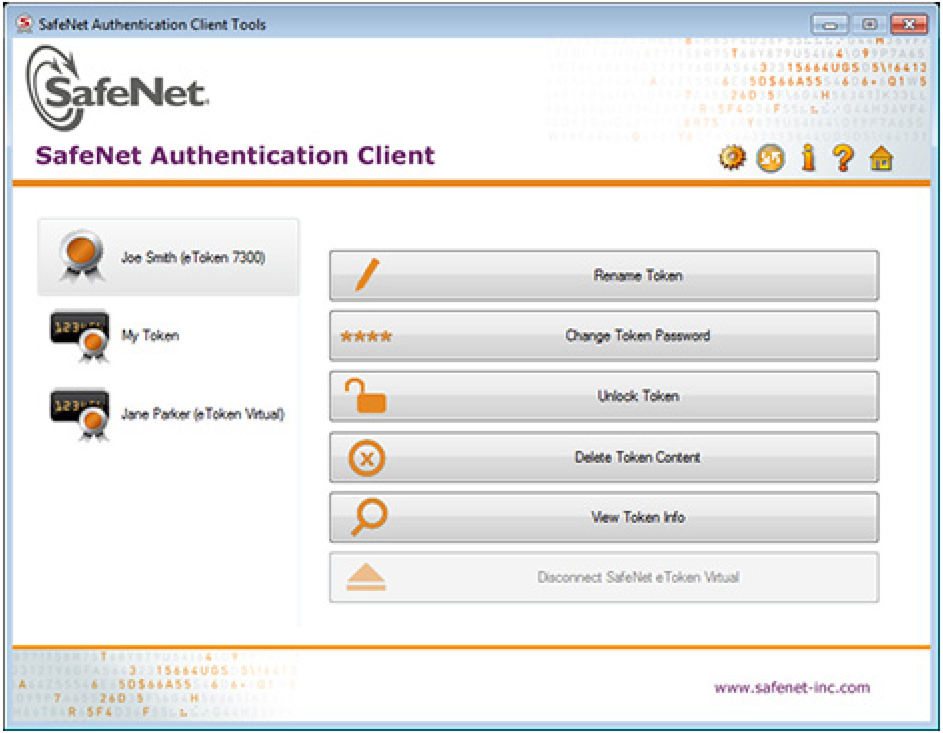
When SafeNet Authentication Client Tools is opened, the *Simple* view is displayed.

To open SafeNet Authentication Client Tools:

Do one of the following:

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

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



NOTE

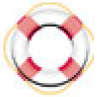
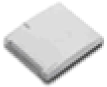
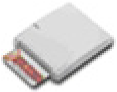
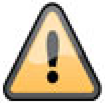
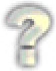
If a customized version of SafeNet Authentication Client is installed, the graphics you see may be different from those displayed in this guide.

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

Token Icons

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

Icon	Token Type
	♦ SafeNet eToken 7100 (SafeNet eToken NG-Flash) ♦ SafeNet eToken 7300 ♦ SafeNet eToken 5100/5105 (SafeNet eToken PRO) ♦ SafeNet eToken Virtual (without OTP support) ♦ SafeNet eToken 5200/5205 HID ♦ SafeNet iKey: 2032, 2032u, 2032i ♦ SafeNet iKey 4000
	♦ SafeNet eToken 5200/5205 (SafeNet eToken PRO Anywhere) ♦ SafeNet eToken 7200 (SafeNet eToken NG-Flash Anywhere)
	♦ SafeNet eToken 7000 (SafeNet eToken NG-OTP) ♦ SafeNet eToken Virtual (with OTP support)
	♦ SafeNet eToken Virtual Temp

Icon (Cont.)	Token Type (Cont.)
	♦ SafeNet eToken Rescue
	♦ Smartcard reader – no card connected
	Smartcard reader – card connected: ♦ SafeNet eToken 4100 (SafeNet eToken PRO Smartcard) ♦ SafeNet SC330 ♦ SafeNet SC400
	♦ Token with corrupted data
	♦ Unknown token

Simple View Functions

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

Function	Description
Rename Token	Sets a new name for the token
Change Token Password	Changes the Token Password
Unlock Token	Unlocks the token and resets the Token Password
Delete Token Content	Removes deletable data from the token (enabled by default)
View Token Info	Provides detailed information about the token
Disconnect SafeNet eToken Virtual	Disconnects the SafeNet eToken Virtual or SafeNet eToken Rescue, with an option to also delete it

Opening the Advanced View

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

To open the SafeNet Authentication Client Tools Advanced view:

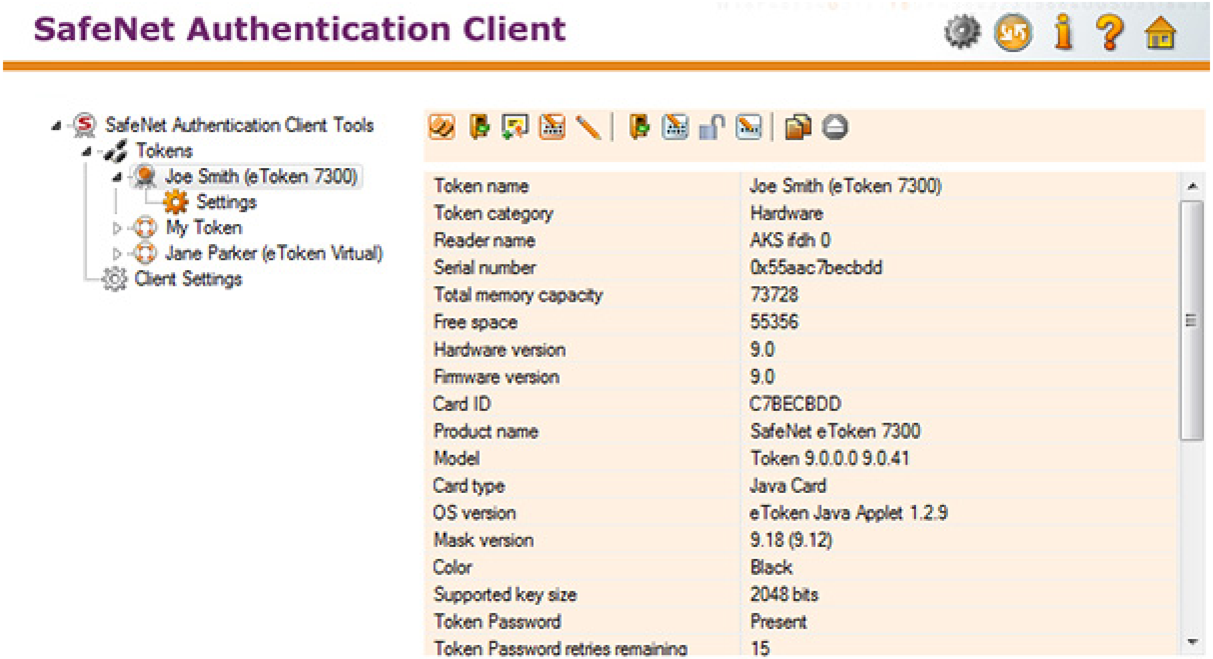
1. Do one of the following:

   - Right-click the SafeNet Authentication Client tray icon, and from the shortcut menu, select **Tools**.
   - On Windows: From the Windows taskbar, select **Start > Programs > SafeNet > SafeNet Authentication Client > SafeNet Authentication Client Tools.**
   - On Linux: From the Windows taskbar, select **Applications > SafeNet> SafeNet Authentication Client > SafeNet Authentication Client Tools.**
   - **On Mac:** From the Mac desktop, select **Go** > **Applications > 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.



SafeNet Authentication Client

- SafeNet Authentication Client Tools
  - Tokens
    - Joe Smith (eToken 7300)
      - Settings
    - My Token
    - Jane Parker (eToken Virtual)
  - Client Settings

Token name	Joe Smith (eToken 7300)
Token category	Hardware
Reader name	AKS ifdh 0
Serial number	0x55aac7becbdd
Total memory capacity	73728
Free space	55356
Hardware version	9.0
Firmware version	9.0
Card ID	C7BECBDD
Product name	SafeNet eToken 7300
Model	Token 9.0.0.0 9.0.41
Card type	Java Card
OS version	eToken Java Applet 1.2.9
Mask version	9.18 (9.12)
Color	Black
Supported key size	2048 bits
Token Password	Present
Token Password retries remaining	15

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

Advanced View Functions

You can access the advanced functions by selecting the required object from the left pane in the Tools Advanced View window.

To access the Advanced functions:

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

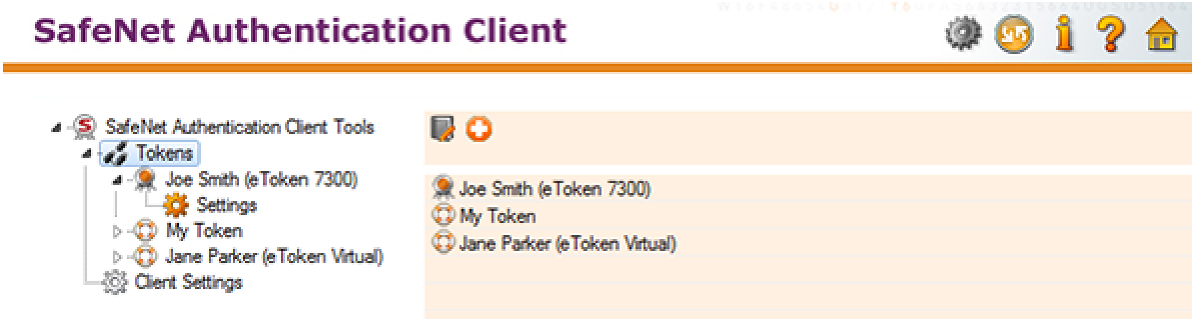
   The relevant functions are displayed in the right pane.

2. Do one of the following:

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

Tokens Node

When you select the *Tokens* node in the left pane, the list of connected tokens is displayed in the right pane, and icons are displayed above them.



SafeNet Authentication Client

- SafeNet Authentication Client Tools
  - Tokens
    - Joe Smith (eToken 7300)
      - Settings
    - My Token
    - Jane Parker (eToken Virtual)
  - Client Settings

Joe Smith (eToken 7300)
My Token
Jane Parker (eToken Virtual)

The following functions are available:

Function	Icon	Right-Click Menu Item
Reader Settings See Chapter 3: *Reader Settings* on page 100.	✎	Reader Settings
Connect SafeNet eToken Virtual See Chapter 5: *Connecting a SafeNet eToken Virtual* on page 132.	⊕	Connect SafeNet eToken Virtual

Selected Token Node

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

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

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

The following user functions are available:

User Function	Icon	Right-Click Menu Item
Initialize Token See Chapter 4: *Token Initialization* on page 103.		Initialize Token
Log On to Token See Chapter 3: *Logging On to the Token as a User* on page 61.		Log On to Token
Import Certificate See Chapter 3: *Importing a Certificate to a Token* on page 79.		Import Certificate
Change Password See Chapter 3: *Changing the Token Password* on page 65.		Change Password
Rename Token See Chapter 3: *Renaming a Token* on page 63.	✏	Rename

User Function (Cont.)	Icon (Cont.)	Right-Click Menu Item
Disconnect SafeNet eToken Virtual (Enabled for SafeNet eToken Virtual or SafeNet eToken Rescue only) See Chapter 5: *Disconnecting or Deleting a SafeNet eToken Virtual Product* on page 134.	⏏	Disconnect
Copy to Clipboard See Chapter 3: *Viewing and Copying Token Information* on page 59.	📋	(None)

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

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

See Chapter 3: *Logging On to the Token as an Administrator* on page 91.

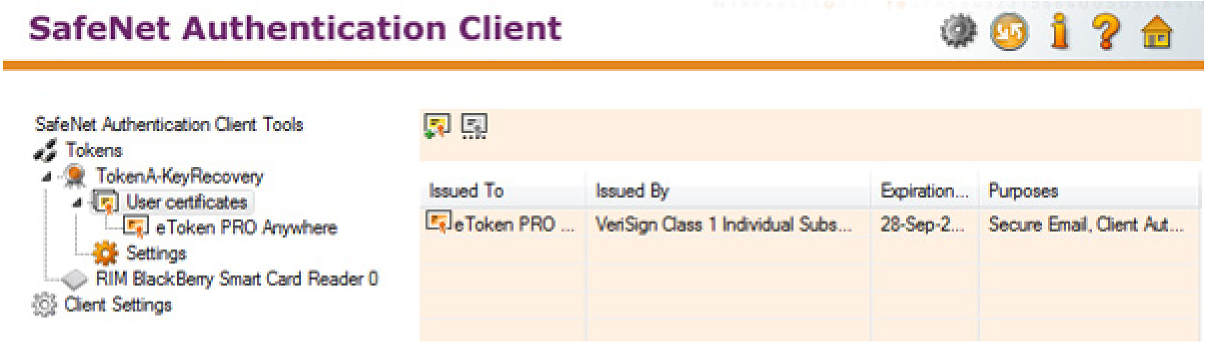
> **NOTE**
> Administrator functions are not supported by iKey devices. The unlock option is available on iKey devices that were initialized using BSec with the unlock keys. After an iKey device is locked the unlock option becomes available.

Certificate Type Node

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

- User Certificates
- 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.


SafeNet Authentication Client
SafeNet Authentication Client Tools
Tokens
TokenA-KeyRecovery
User certificates
eToken PRO Anywhere
Settings
RIM BlackBerry Smart Card Reader 0
Client Settings

Issued To	Issued By	Expiration...	Purposes
eToken PRO ...	VeriSign Class 1 Individual Subs...	28-Sep-2...	Secure Email, Client Aut...

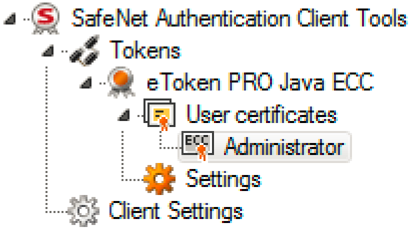
Depending on the certificate type, the following functions may be available:

User Function	Icon	Right-Click Menu Item
Import Certificate See Chapter 3: *Importing a Certificate to a Token* on page 79.		Import Certificate
Reset Default Certificate Selection See Chapter 3: *Clearing a Default Certificate (Windows only)* on page 89.		Reset Default Certificate Selection. (Windows only)

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

ECC Certificates

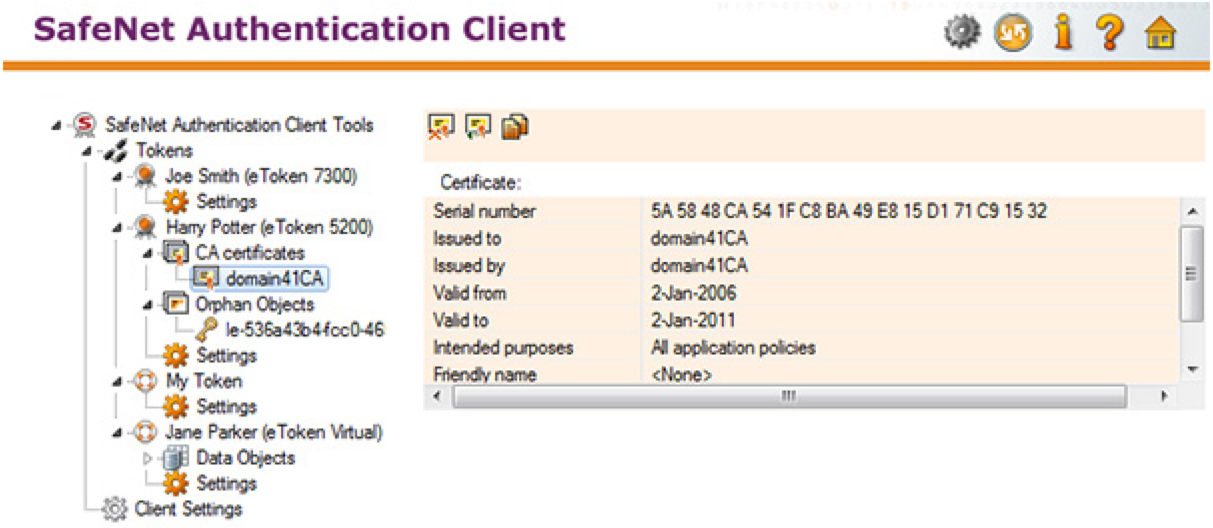
ECC certificates are supported when using ECC tokens only.



SafeNet Authentication Client Tools
Tokens
eToken PRO Java ECC
User certificates
Administrator
Settings
Client Settings

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.



Certificate:

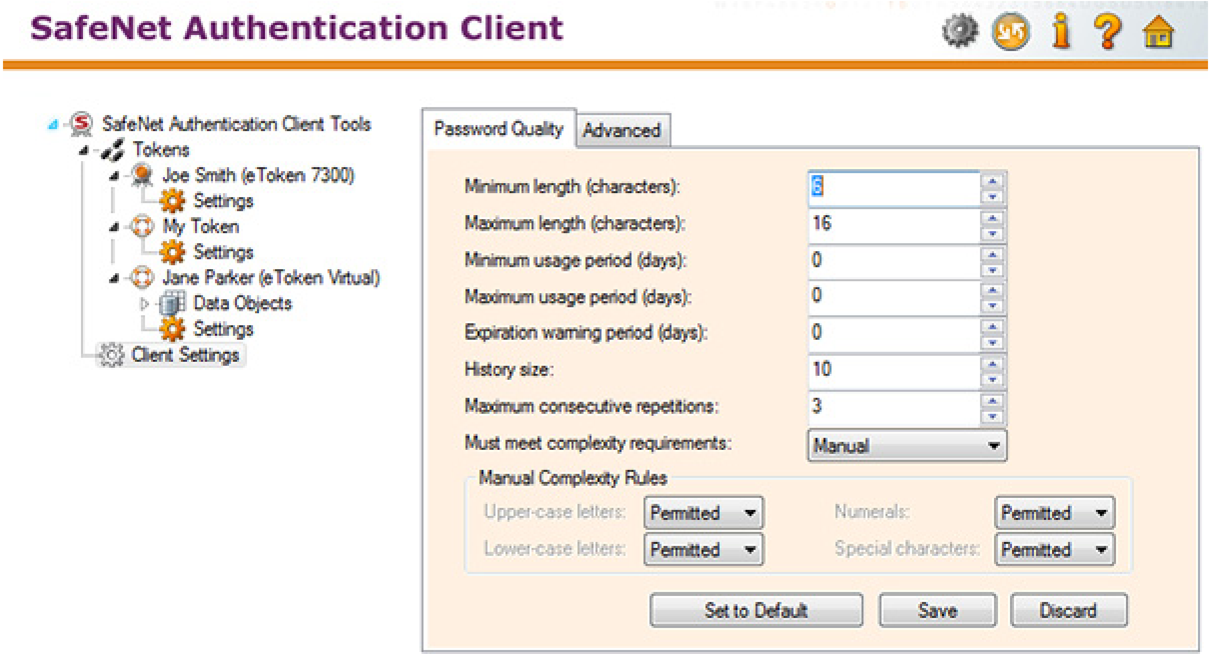
Serial number	5A 58 48 CA 54 1F C8 BA 49 E8 15 D1 71 C9 15 32
Issued to	domain41CA
Issued by	domain41CA
Valid from	2-Jan-2006
Valid to	2-Jan-2011
Intended purposes	All application policies
Friendly name	<None>

Some or all of the following functions are available:

User Function	Icon	Right-Click Menu Item
Delete Certificate See *Deleting a Certificate* on page 90.	📜	Delete Certificate
Export Certificate See *Exporting a Certificate from a Token* on page 82.	📜	Export Certificate
Set as Default See *Setting a Certificate as Default or Auxiliary (Windows only)* on page 87.	(None)	Set as Default. (Windows only)
Set as Auxiliary See *Setting a Certificate as Default or Auxiliary (Windows only)* on page 87.	(None)	Set as Auxiliary. (Windows only)
Copy to Clipboard See *Viewing and Copying Token Information* on page 59.	📋	(None)
Set as KSP / Set as CSP See *Setting a Certificate as KSP or CSP (Windows only)* on page 85.	(None)	Set as KSP / Set as CSP. (Windows only)

Settings Node

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



Minimum length (characters):	6
Maximum length (characters):	16
Minimum usage period (days):	0
Maximum usage period (days):	0
Expiration warning period (days):	0
History size:	10
Maximum consecutive repetitions:	3
Must meet complexity requirements:	Manual

Manual Complexity Rules

Upper-case letters:	Permitted	Numerals:	Permitted
Lower-case letters:	Permitted	Special characters:	Permitted

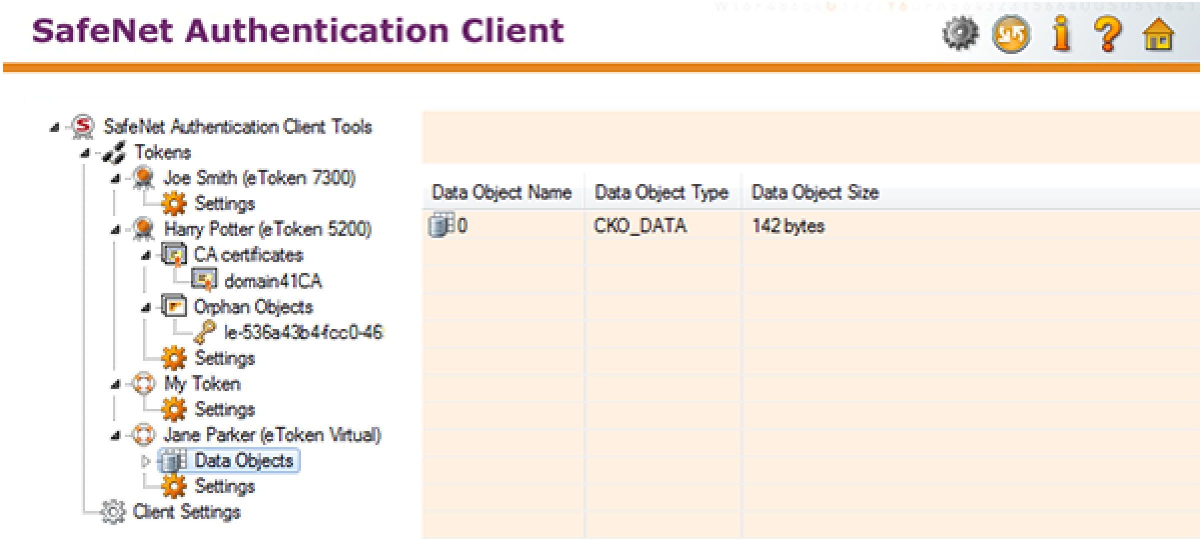
The settings are in two tabs:

- Password Quality
  See Chapter 8: *Setting Token Password Quality* on page 172.
- Advanced
  See Chapter 8: *Setting Private Data Caching Mode* on page 176 and *Setting RSA Key Secondary Authentication* on page 179.

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

Data Objects Node

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



Data Object Name	Data Object Type	Data Object Size
0	CKO_DATA	142 bytes

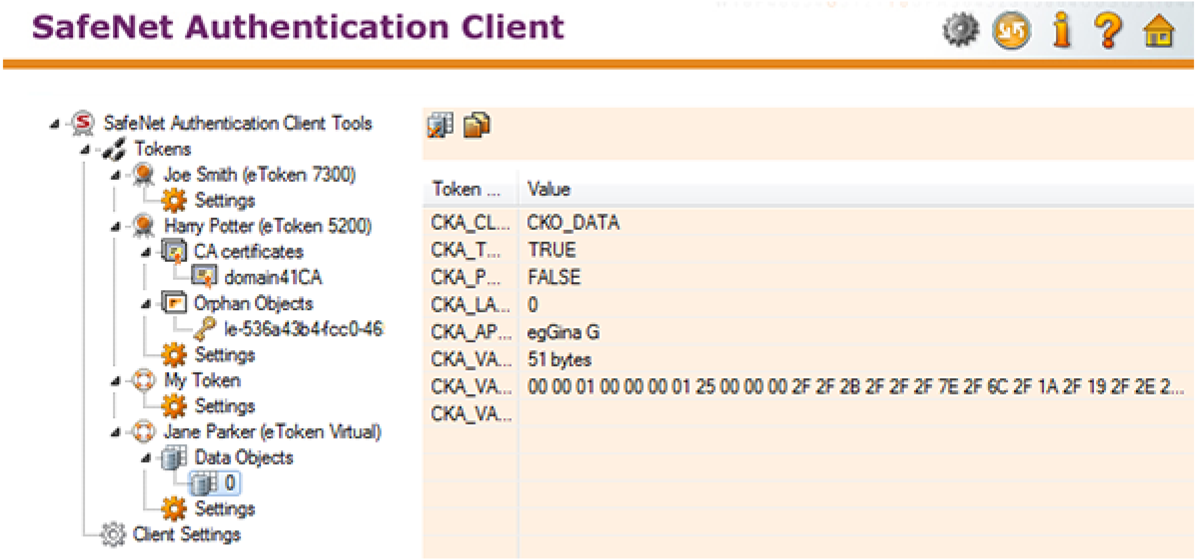
To view the contents of a data object:

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.



Token ...	Value
CKA_CL...	CKO_DATA
CKA_T...	TRUE
CKA_P...	FALSE
CKA_LA...	0
CKA_AP...	egGina G
CKA_VA...	51 bytes
CKA_VA...	00 00 01 00 00 00 01 25 00 00 00 2F 2F 2B 2F 2F 2F 7E 2F 6C 2F 1A 2F 19 2F 2E 2...
CKA_VA...	

To delete a data object:

1 Select the value to be deleted.

2 Click the **Delete Data Object** icon .

Orphan Objects Node

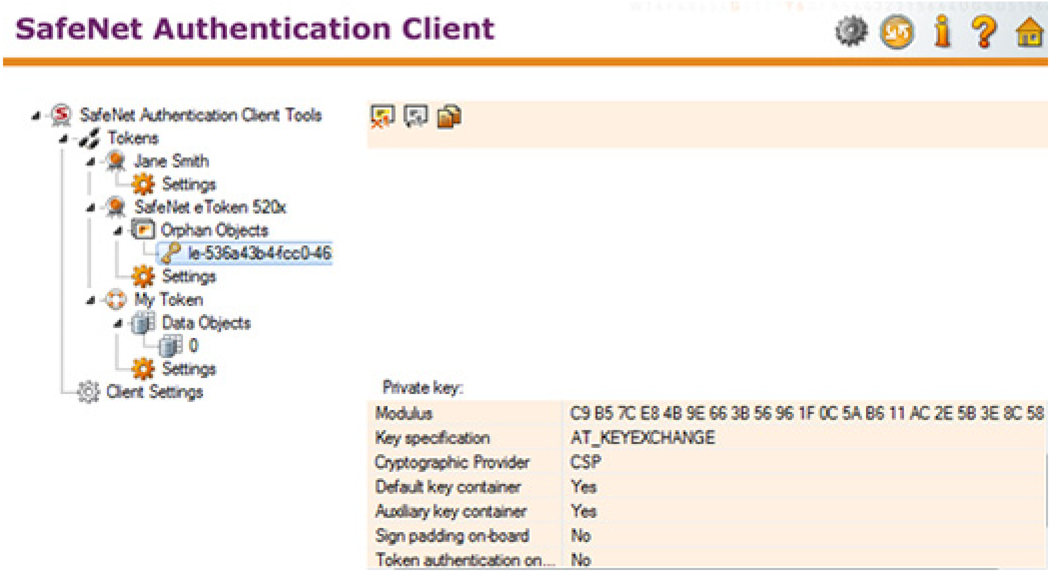
An orphan object is a certificate without its key or a key without its certificate. A token's *Orphan Objects* node displays these objects.

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.



Private key:

Modulus	C9 B5 7C E8 4B 9E 66 3B 56 96 1F 0C 5A B6 11 AC 2E 5B 3E 8C 58
Key specification	AT_KEYEXCHANGE
Cryptographic Provider	CSP
Default key container	Yes
Auxiliary key container	Yes
Sign padding on-board	No
Token authentication on...	No

To delete an orphan object:

Right-click the Orphan Object on the left, and select **Delete**.

Click the **Delete Orphan Object** icon .

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 all tokens that will be initialized using this computer after the changes have been saved.

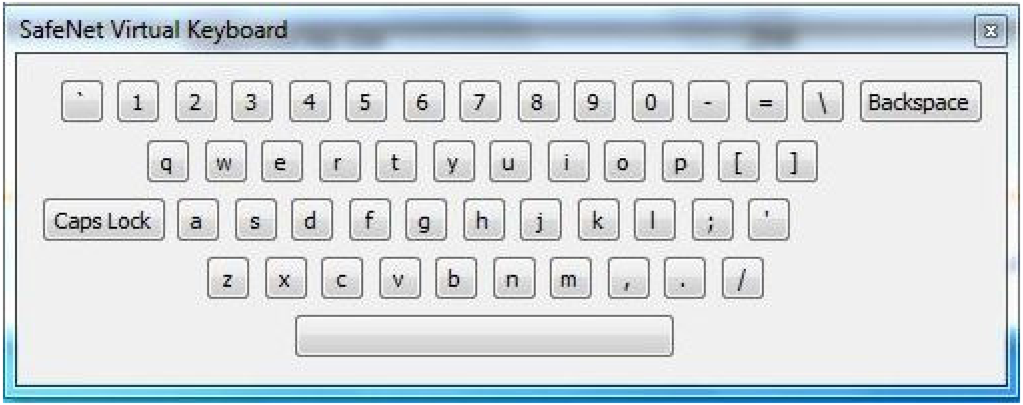
Like the *Settings* window, the *Client Settings* window contains two tabs:

- Password Quality
- Advanced

See Chapter 7: *Client Settings* on page 158.

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.


SafeNet Virtual Keyboard
` 1 2 3 4 5 6 7 8 9 0 - = \ Backspace
q w e r t y u i o p [ ]
Caps Lock a s d f g h j k l ; '
z x c v b n m , . /

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

- Token Logon
- Change Password

NOTES

- The virtual keyboard is supported on Windows Operating Systems only.
- The virtual keyboard supports English characters only.
- To type an upper-case character, press **Shift** on your physical keyboard.

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.

In this chapter:

Selecting the Active Token

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

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

1. Open SafeNet Authentication Client Tools.
   See Chapter 2: *Opening the Simple View* on page 33 or *Opening the Advanced View* on page 38.
2. In the left pane, select the required token.

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

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

   The SafeNet Authentication Client tray menu opens.
2. Select the required token from the tray menu by hovering over the relevant token name. A sub-menu appears displaying a list of tasks that can be performed on the active token.
3. Select the relevant option from the sub-menu.

Viewing and Copying Token Information

To view and copy token information:

1. To use the *Simple* view to view token information, do the following:
   - a. Open SafeNet Authentication Client Tools *Simple* view.
     See *Opening the Simple View* on page 33.
   - b. In the left pane, select the required token.
   - c. In the right pane, select **View Token Info**.
   - d. Continue with step 3.
2. To use the *Advanced* view to view token information, do the following:
   - a. Open SafeNet Authentication Client Tools *Advanced* view.
     See *Opening the Advanced View* on page 38.
   - b. In the left pane, select the node of the required token.
   - c. Continue with step 3.
3. The *Token Information* is displayed.

   The information displayed varies according to the type of token.

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

4. To copy the token information to the clipboard, do one of the following:
   - In the *Token Information* window, click **Copy**.
   - In *Advanced* view, click the **Copy to Clipboard** icon:

5. To paste the copied token information, click the cursor in the target application, and paste the information.

6. Click **OK**.

Logging On to the Token as a User

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

To log on as a user:

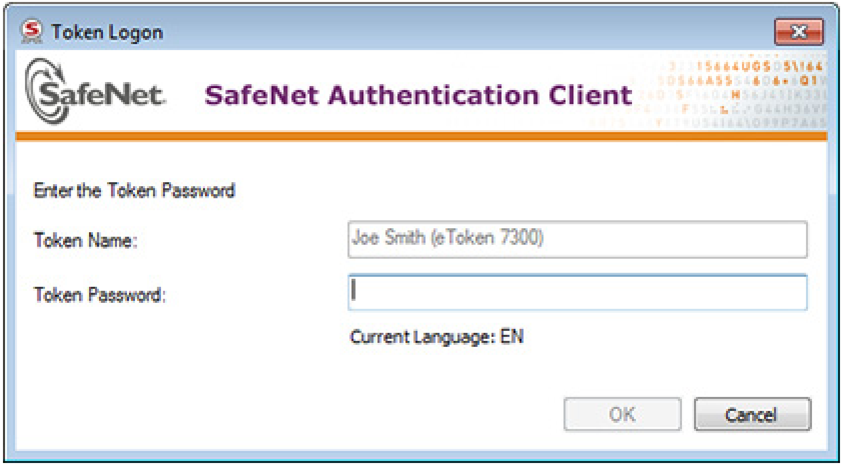
1 Open SafeNet Authentication Client Tools *Advanced* view.
See *Opening the Advanced View* on page 38.

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

2 Do one of the following:

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

3 The *Token Logon* window opens.



Enter the Token Password

Token Name: Joe Smith (eToken 7300)

Token Password:

Current Language: EN

4 Enter the Token Password, and click **OK**.

You are logged on to the token.

Renaming a Token

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

> **TIP**
> If you have more than one token, we recommend assigning each one a unique token name.

To rename a token:

1. To use the *Simple* view to rename a token, do the following:
   - a Open SafeNet Authentication Client Tools *Simple* view.
     See *Opening the Simple View* on page 33.
   - b In the left pane, select the required token.
   - c In the right pane, select **Rename Token**.
   - d Continue with step .
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 38.

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 .

The *Token Logon* window opens.

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

The *Token Rename* window opens.

4 Enter the new name in the *New token name* field, and click **OK**.

The new token name is displayed in the *SafeNet Authentication Client Tools* window.

Changing the Token Password

TIP

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

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

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 Token Password:

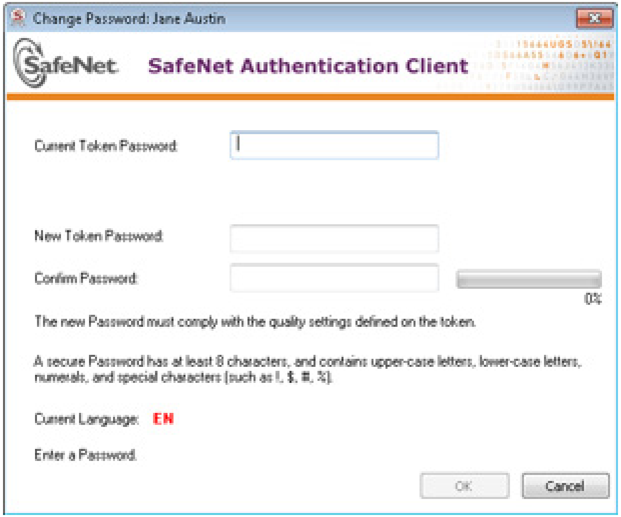
1. To use the *Simple* view to change the Token Password, do the following:
   1. Open SafeNet Authentication Client Tools *Simple* view.
      See *Opening the Simple View* on page 33.
   2. In the left pane, select the required token.
   3. In the right pane, select **Change Token Password**.
   4. Continue with step 4.
2. To use the *Advanced* view to change the Token Password, do the following:
   1. Open SafeNet Authentication Client Tools *Advanced* view.
      See *Opening the Advanced View* on page 38.
   2. 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.
   3. Continue with step 4.
3. To use the tray menu to change the Token Password, do the following:
   1. Right-click the SafeNet Authentication Client tray icon.

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

c Select **Change Token Password**.

d Continue with step 4.

4 The *Change Password* window opens.



Change Password: Jane Austin

SafeNet Authentication Client

Current Token Password:

New Token Password:

Confirm Password:

0%

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

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

Current Language: EN

Enter a Password.

5 Enter the current Token Password in the *Current Token Password* field.

NOTE

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

6 Enter a new Token Password in the *New Token Password* and *Confirm Password* fields.

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

7 Click **OK**.

A message confirms that the Token Password was changed successfully.

8 Click **OK**.

Unlocking a Token by the Challenge-Response Method

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

NOTE
iKey devices cannot be unlocked by the Challenge-Response method.

SafeNet eToken Rescue tokens cannot be unlocked.

CAUTION
The administrator can limit the number of times that a token can be unlocked. If this number is exceeded, the token becomes unusable. If the token is a physical token, it must be initialized. If it is not a physical token, it must be replaced.

When the administrator has access to the user's token, the administrator can unlock the token using the *Set Token Password* feature.
See Chapter 3: *Unlocking a Token by an Administrator* on page 94.

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

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

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

To unlock a token using the Challenge-Response method:

1 To use the *Simple* view to unlock a token, do the following:

  a Open SafeNet Authentication Client Tools *Simple* view.
  See *Opening the Simple View* on page 33.

  b In the left pane, select the required token.

  c In the right pane, select **Unlock Token**.

  d Continue with step 4.

2 To use the *Advanced* view to unlock a token, do the following:

  a Open SafeNet Authentication Client Tools *Advanced* view.
  See *Opening the Advanced View* on page 38.

b Do one of the following:

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

c Continue with step 4.

3 To use the tray menu to change the Token Password, do the following:

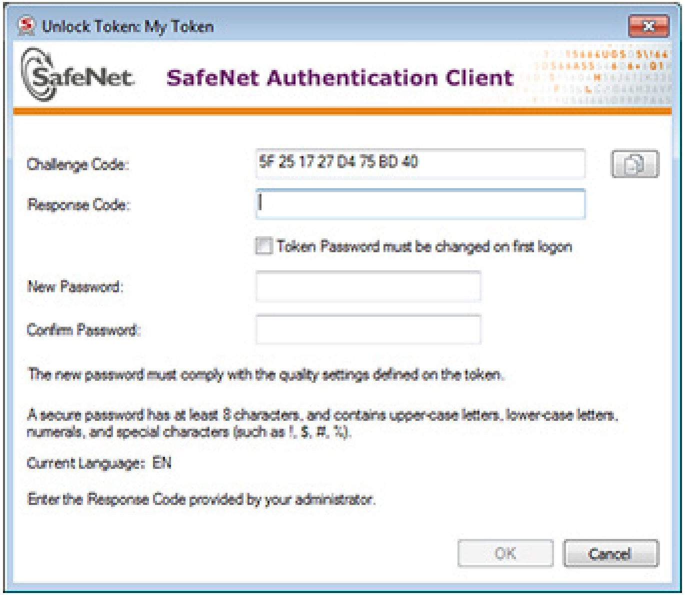
a Right-click the SafeNet Authentication Client tray icon.

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

c Select **Unlock Token**.

d Continue with step 4.

4 *The Unlock Token* window opens, displaying a value in the *Challenge Code* field.
The *Challenge Code* is 16 characters or, if the token was initialized as Common Criteria, 13 characters.



Unlock Token: My Token

SafeNet Authentication Client

Challenge Code: 5F 25 17 27 D4 75 BD 40

Response Code:

□ Token Password must be changed on first logon

New Password:

Confirm Password:

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

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

Current Language: EN

Enter the Response Code provided by your administrator.

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

NOTE

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

CAUTION

After providing the Challenge Code to the administrator, **do not** undertake any activities that use the token until you receive the Response Code and complete the unlocking procedure.

If any other token activity occurs during this process, it will affect the context of the Challenge – Response process and invalidate the procedure.

6 The administrator provides you with the *Response Code* to be entered.
The *Response Code* is 16 characters or, if the token was initialized as Common Criteria, 39 characters.

NOTE

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

7 Enter a new Token Password in the *New Token Password* and *Confirm Password* fields.

8 If the new password is known to others and must be changed, select **Token Password must be changed on first logon**.

9 Click **OK**.

A message confirms that the token was unlocked successfully.

10 Click **OK**.

Unlocking an iKey Token Initialized Using BSec Utilities

An iKey token that was initialized using BSec Utilities can be unlocked if it was configured with unblocking codes.

Linux doesn't support ikey tokens, but ikey smart cards are supported.

Windows and Mac supports all tokens.

> **NOTE**
> iKey Smart Cards are supported by Linux, but iKey tokens are not. Windows and Mac Operating System support all tokens.

To unlock an iKey token:

1 To use the *Simple* view to unlock an iKey token, do the following:

- a Open SafeNet Authentication Client Tools *Simple* view*.*
  See *Opening the Simple View* on page 33.
- b In the left pane, select the required token.
- c In the right pane, select **Unlock Token**.
- d Continue with step 3.

2 To use the *Advanced* view to unlock an iKey token, do the following:

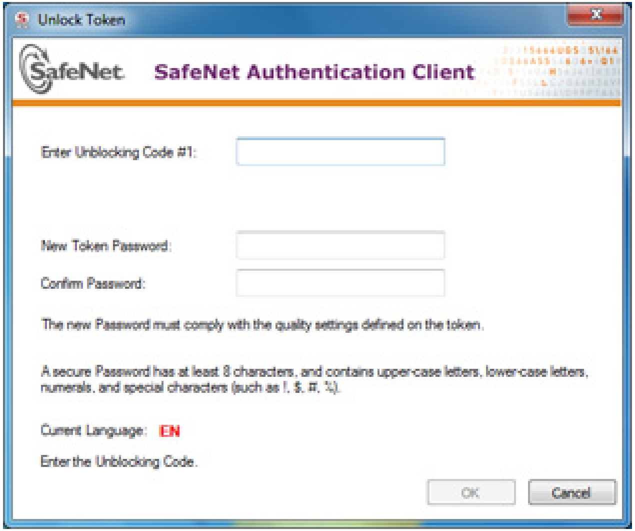
- a Open SafeNet Authentication Client Tools *Advanced* view*.*
  See *Opening the Advanced View* on page 38.

b Do one of the following:

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

c Continue with step 3.

3 The *Unlock Token* window opens.



Enter Unblocking Code #1:

New Token Password:

Confirm Password:

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

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

Current Language: EN

Enter the Unblocking Code.

4 Enter one of the unblocking codes in the *Enter Unlocking Code* field.

NOTE

For iKey 4000:

- Up to six unblocking codes can be stored on each token and each unblocking code can be used only once.
- The unblocking codes can be used in any order.
- If only one unblocking code is configured, it can be re-used an unlimited number of times.

If more than one unblocking code is configured, each unblocking code can be used only once.

5 Enter a new password in the *New Token Password* and *Confirm Password* fields, and click **OK**.

A message confirms that the token was unlocked successfully.

6 Click **OK.**

Deleting Token Content

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

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

The *Delete Token Content* function is less comprehensive than the *Initialize* function which restores a token to its initial state, removing all objects stored on the token since manufacture and resetting the Token Password.
See Chapter 4: *Token Initialization* on page 103.

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 33.

  b In the left pane, select the required token.

  c In the right pane, select **Delete Token Content**.

  d Continue with step 3.

2 Depending on the configuration of your system, you can use the tray menu:

  a Right-click the SafeNet Authentication Client tray icon.

   b. If more than one token is connected, hover over the appropriate token.
   c. Select **Delete Token Content**.
   d. Continue with step 3.

3. The *Token Logon* window opens.
4. Enter the Token Password, and click **OK**.

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

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

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

6. Click **OK** to finish.

Importing a Certificate to a Token

The following certificate types are supported:

- .pfx
- .p12
- .cer

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

For Linux: In the case of a CER file (which contains only X.509 certificates), the program checks if a private key

exists on the token. If the private key is found, the certificate is stored with it. If no private key is found, you are asked if you want to store the certificate as a CA certificate.

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 eToken Rescue.

To import a certificate:

1 Open SafeNet Authentication Client Tools *Advanced* view.
See *Opening the Advanced View* on page 38.

2 Do one of the following:

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

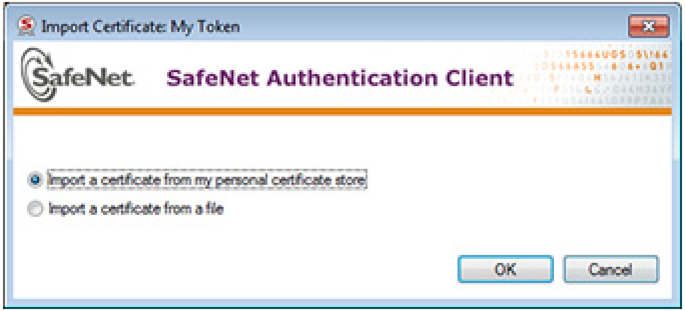
In the right pane, click the **Import Certificate** icon:

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

3 The *Token Logon* window opens.

4 Enter the Token Password, and click **OK**.

The *Import Certificate* window opens.


Import Certificate: My Token

SafeNet Authentication Client

● Import a certificate from my personal certificate store

○ Import a certificate from a file

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

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

6. If you select **Import a certificate from my personal certificate store**, a list of available certificates is displayed.

   Only certificates that can be imported on to the token are listed. These are:
   - Certificates with a private key already on the token
   - Certificates that can be imported from the computer together with their private key
7. If you select **Import a certificate from a file**, the *Certificate Selection* window opens.

   Select the certificate to import, and click **Open**.
8. If the certificate requires a password, the *Password* window opens.

   Enter the certificate password, and click **OK**.
9. If the certificate is a Common Criteria certificate, the *Import PIN* window opens.

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

   The default value is **1234567890**.
10. All requested certificates are imported, and a message confirms that the import was successful**.**

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 38.
2. In the left pane, expand the node of the required token.
3. Do one of the following:
   - Select the required certificate, and click the **Export Certificate** icon:
   - Right-click the required certificate, and select **Export Certificate** from the shortcut menu.

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

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

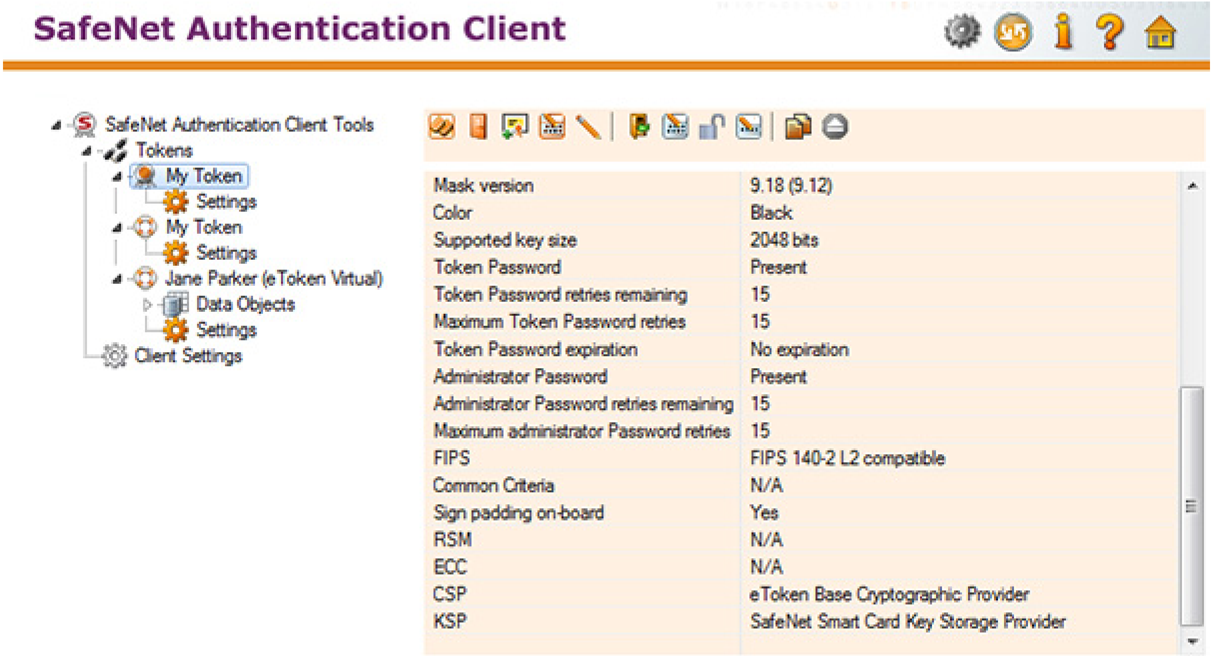
Viewing Supported Cryptographic Providers

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

To see which Cryptographic Providers are supported on the token:

1. Open SafeNet Authentication Client Tools *Advanced* view*.*
   See *Opening the Advanced View* on page 38.
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.


SafeNet Authentication Client
SafeNet Authentication Client Tools
Tokens
My Token
Settings
My Token
Settings
Jane Parker (eToken Virtual)
Data Objects
Settings
Client Settings

Mask version	9.18 (9.12)
Color	Black
Supported key size	2048 bits
Token Password	Present
Token Password retries remaining	15
Maximum Token Password retries	15
Token Password expiration	No expiration
Administrator Password	Present
Administrator Password retries remaining	15
Maximum administrator Password retries	15
FIPS	FIPS 140-2 L2 compatible
Common Criteria	N/A
Sign padding on-board	Yes
RSM	N/A
ECC	N/A
CSP	eToken Base Cryptographic Provider
KSP	SafeNet Smart Card Key Storage Provider

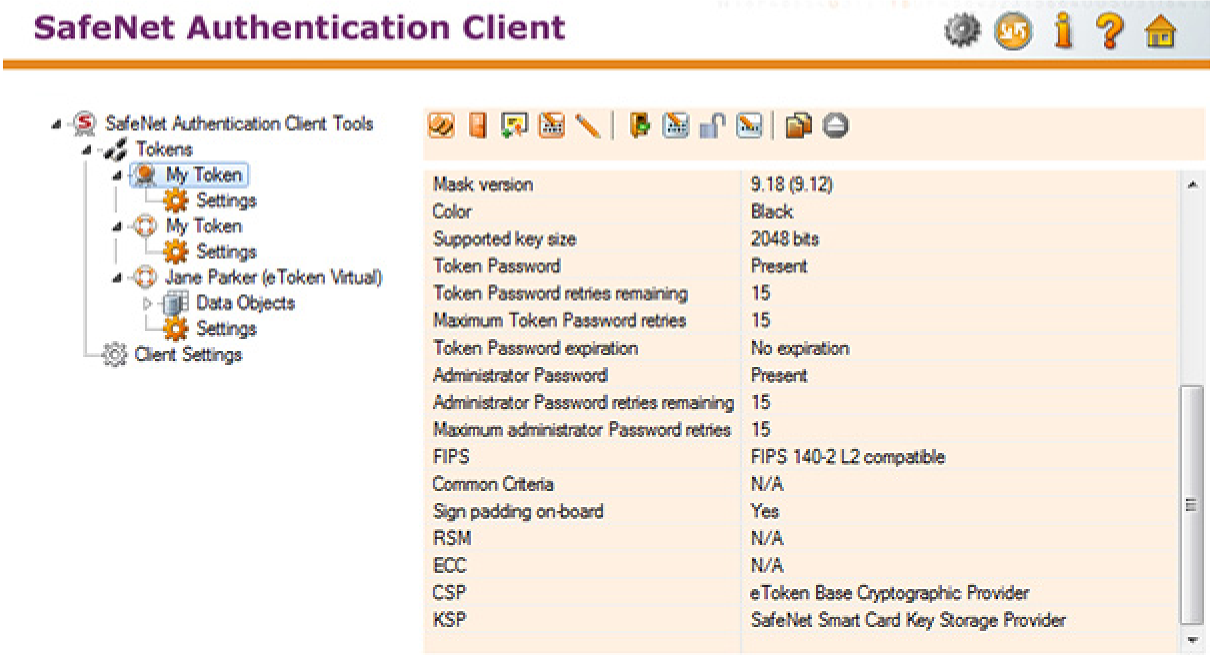
Setting a Certificate as KSP or CSP (Windows only)

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

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

To set the certificate as KSP or CSP:

1. Open SafeNet Authentication Client Tools *Advanced* view*.*
   See *Opening the Advanced View* on page 38.
2. In the left pane, expand the node of the required token.


SafeNet Authentication Client
SafeNet Authentication Client Tools
Tokens
My Token
Settings
My Token
Settings
Jane Parker (eToken Virtual)
Data Objects
Settings
Client Settings

Mask version	9.18 (9.12)
Color	Black
Supported key size	2048 bits
Token Password	Present
Token Password retries remaining	15
Maximum Token Password retries	15
Token Password expiration	No expiration
Administrator Password	Present
Administrator Password retries remaining	15
Maximum administrator Password retries	15
FIPS	FIPS 140-2 L2 compatible
Common Criteria	N/A
Sign padding on-board	Yes
RSM	N/A
ECC	N/A
CSP	eToken Base Cryptographic Provider
KSP	SafeNet Smart Card Key Storage Provider

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 (Windows only)

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

Each option is enabled only if the action can be performed on that particular certificate or key.

The following table describes the use of these settings.

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

Setting	Description	Scenario
Default	Smart card logon uses the certificate defined as the *Default*. In most Microsoft applications, smart card logon is used.	Your token contains two certificates. One is to logon to domain A and the other to logon to domain B. If your previous logon was to domain A, it means that the certificate used to logon to domain A is now the *Default*. If you need to log on to domain B from another computer, the following happens: ♦ If you first set the domain B certificate as *Default*, the logon uses the correct certificate, and the logon succeeds. ♦ If you do not set the domain B certificate as *Default*, the domain A certificate is used, and logon fails.

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

To set a certificate as Default or Auxiliary:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See *Opening the Advanced View* on page 38.
2. In the left pane, expand the node of the required token, and right-click the required certificate.
3. From the shortcut menu, select **Set as Default** or **Set as Auxiliary**.

   The *Token Logon* window opens.
4. Enter the Token Password, and click **OK**.

   The certificate is set as *Default* or *Auxiliary*.

Clearing a Default Certificate (Windows only)

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 38.
2. In the left pane, expand the node of the required token.
3. Do one of the following:
   - In the left pane, select *User Certificates*.
     In the right pane, click the **Reset Default Certificate Selection** icon.
   - In the left pane, right-click *User Certificates*, and select **Reset Default Certificate Selection** from the shortcut menu.
4. The *Reset Default Certificate Selection* window opens, confirming that the Default certificate has been reset.
5. Click **OK**.

Deleting a Certificate

You can remove a certificate from a token.

To delete a certificate from a token:

1. Open SafeNet Authentication Client Tools *Advanced* view*.*
   See *Opening the Advanced View* on page 38.
2. In the left pane, expand the node of the required token.
3. Do one of the following:
   - In the left pane, select the required certificate, and click the **Delete Certificate** icon.
   - In the left pane, right-click the required certificate, and select **Delete Certificate** from the shortcut menu.
4. The *Delete Certificate* window opens.
5. To delete the certificate, click **Yes.** The *Token Logon* window opens.
6. Enter the Token Password, and click **OK**.

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

Logging On to the Token as an Administrator

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

> **NOTE**
> Administrator functions are not supported by iKey devices.

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

- Changing the Administrator Password (not supported by iKey devices)
- Unlocking a Token by an Administrator
- Unlocking a Token by the Challenge-Response Method
- Setting Token Password Quality
- Setting Private Data Caching Mode
- 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 38.

2 Do one of the following:

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

3 The *Administrator Logon* window opens.

4 Enter the token’s Administrator Password, and click **OK**.

You are logged on as an administrator.

Changing the Administrator Password

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

To change the Administrator Password:

1 Open SafeNet Authentication Client Tools *Advanced* view.

2 Do one of the following:

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

The *Change Administrator Password* window opens.

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

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

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

5 Click **OK**. A message confirms that the password was changed successfully.

6 Click **OK**.

Unlocking a Token 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.

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 38.
2. Do one of the following:
   - In the left pane, select the node of the required token.
     In the right pane, click the **Set Token Password** icon.
   - In the left pane, right-click the node of the required token, and select **Set Token Password** from the shortcut menu.

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

   The *Set Token Password* window opens.
4. Enter a new Token Password in the *New Password* and *Confirm Password* fields.

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

5 Set the *Logon retries before token is locked* field to the required number.

> **NOTE**
> The *Logon retries before token is locked* feature is available only on CardOS tokens. Java card tokens are not supported.

6 Click **OK**.

A message confirms that the Token Password was changed successfully.

7 Click **OK**.

The token is unlocked, and the user can now log on with the new Token Password.

Synchronizing Passwords (Windows only)

NOTE
Password synchronization is implemented only in specific installations of SafeNet Authentication Client.

SafeNet Authentication Client supports synchronization between Token Passwords and domain logon passwords.

The synchronization process ensures that a single password is used for logging on to both the token and the Windows domain. The process enforces the password complexity requirements that were set for the token and SafeNet Authentication Client.

NOTE
- The new password must meet the complexity requirements for the token and the domain.
- You must have access to the domain when changing the password.
- Password Synchronization is not set by default, and therefore requires specific configuration by an administrator. For more information on how to Synchronize Passwords, see the SafeNet Authentication Manager Administrator's Guide.

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.

Working with IdenTrust

IdenTrust supports two modes:

- **Token Password** - entered each time a certificate is used. This is supported by all SafeNet eToken and iKey devices.
- **Identity PIN (Legacy)** - used as an Identity PIN and is entered each time an identity certificate is used. This is supported by all SafeNet eToken and iKey devices.

Using the Identity PIN (Legacy)

Changing the Identity PIN

To change the Identity PIN:

1. Open SafeNet Authentication Client Tools *Advanced* view*.*
   See *Opening the Advanced View* on page 38.
2. Right-click the token, and select **Change Identity PIN**.
3. The *Change Identity PIN* window opens.
4. Enter the current PIN, and enter and confirm the new PIN.

Unblocking the Identity PIN

If an incorrect Identity PIN is entered multiple times, the PIN becomes blocked. It must be unblocked to enable you to continue working with the token.

To unblock the Identity PIN:

1. Open SafeNet Authentication Client Tools *Advanced* view*.*
   See *Opening the Advanced View* on page 38.
2. Right-click the token, and select **Unblock Identity**.

   The *Unblock Identrust PIN* window opens.
3. Enter the unblocking code in the *Enter Unblocking Code* field.
4. Enter a new password in the *New Password* and *Confirm Password* fields, and click **OK**.

Reader Settings

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

- A token is physically inserted into a USB port
- A SafeNet eToken Virtual is connected
- A smartcard is physically inserted into a reader

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

- 2 SafeNet eToken readers
- 2 iKey readers
- 1 virtual reader for SafeNet eToken Virtual smartcard emulation
- 2 SafeNet eToken Virtual slots

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

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

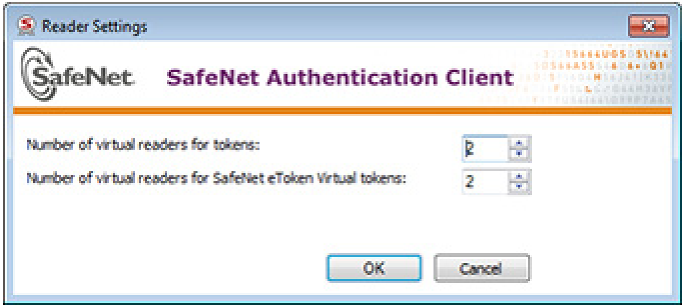
NOTE

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

To change the number of readers:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See *Opening the Advanced View* on page 38.
2. Do one of the following:
   - In the left pane, select the **Tokens** node.
     In the right pane, click the **Reader Settings** icon.
   - In the left pane, right-click the **Tokens** node, and select **Reader Settings** from the shortcut menu.

   The *Reader Settings* window opens.



Number of virtual readers for tokens: 2

Number of virtual readers for SafeNet eToken Virtual tokens: 2

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

The default numbers of available readers are:

- SafeNet eToken readers: 2
- SafeNet eToken Virtual slots: 2

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

   The number of available readers is changed.

5. Restart SafeNet Authentication Client Tools to make the changes effective.

4 Token Initialization

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

NOTE
You cannot use SafeNet Authentication Client to initialize a SafeNet eToken Virtual product.

In this chapter:

- Overview of Token Initialization
- Configuring Initialization Settings
- Under Optional cryptography mechanism, complete the fields as follows:
- Changing the Token Initialization Key
- Configuring Common Criteria Settings

Overview of Token Initialization

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
- Administrator Password (optional) - not supported by iKey devices
- Maximum number of logon failures allowed
- Requirement to change the Token Password on the first logon
- Initialization key
- 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.

Configuring Initialization Settings

NOTE

- Depending on the type of token being initialized, certain settings may not be enabled.
- If a customized version of SafeNet Authentication Client is installed, the graphics you see may be different from those displayed in this guide.

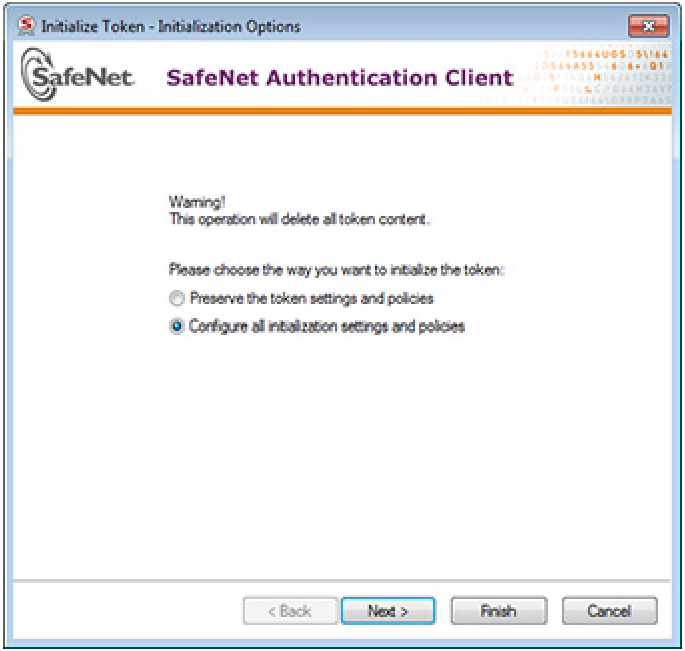
To initialize a token:

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See *Opening the Advanced View* on page 38.
2. Do one of the following:
   - In the left pane, select the node of the required token.
     In the right pane, click the **Initialize Token** icon:
   - In the left pane, right-click the node of the required token, and select **Initialize Token** from the shortcut menu.

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

NOTE

Initializing a token deletes all objects that were created on the Smart Card, while the token was in use.


Initialize Token - Initialization Options
SafeNet
SafeNet Authentication Client

Warning!
This operation will delete all token content.

Please choose the way you want to initialize the token:

○ Preserve the token settings and policies

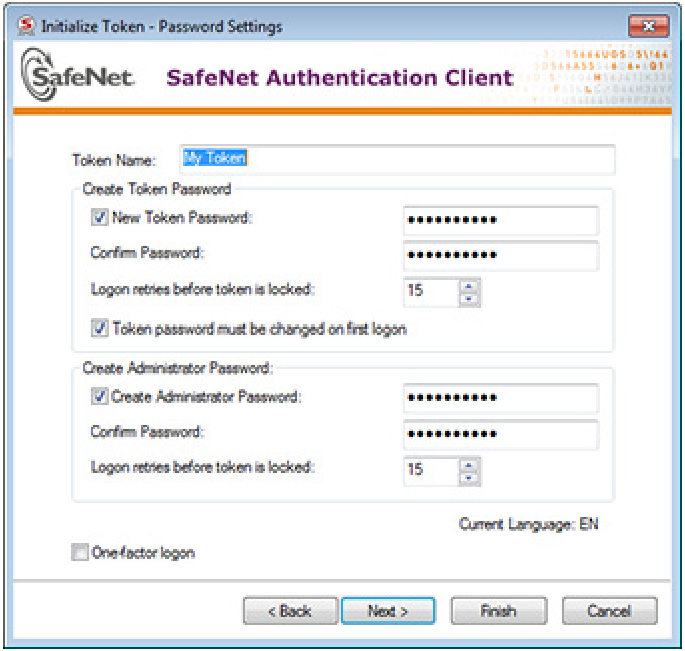
● Configure all initialization settings and policies

< Back
Next >
Finish
Cancel

3 Select either one of the following:

Preserve the token settings and policies	Select to keep current token policies and settings. Selecting this option will allow you to: ♦ Create a Token Password ♦ Create an Administrator Password ♦ Set One-factor Logon ♦ Repartition the token’s flash drive
Configure all initialization settings and policies	Select to change all token policies and settings

The *Password Settings* window opens.



Initialize Token - Password Settings

SafeNet Authentication Client

Token Name: My Token

Create Token Password

☑ New Token Password: •••••••••••

Confirm Password: •••••••••••

Logon retries before token is locked: 15

☑ Token password must be changed on first logon

Create Administrator Password:

☑ Create Administrator Password: •••••••••••

Confirm Password: •••••••••••

Logon retries before token is locked: 15

Current Language: EN

□ One-factor logon

4 Enter a name for the token in the *Token Name* field. 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.

5 Select **Create Token Password** to initialize the token with a Token Password.

If the token is initialized without a Token Password, it will not be usable for token applications.

6 Enter a new Token Password in the *New Token Password* and *Confirm* fields.

NOTE

- The default Token Password is 1234567890.
- If the token is initialized with the default Token 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. The user will be required to set a Token Password that meets the Password Quality requirements configured in the *Settings* window.
  See Chapter 8: *Setting Token Password Quality* on page 172.

7 To initialize an Administrator Password, select **Create Administrator Password** and enter a password in the *New Administrator Password* and *Confirm* fields. The minimum password length is 4 characters.

NOTE

- Setting an Administrator Password enables certain functions to be performed on the token, such as setting a new Token Password to unlock a token.
- iKey tokens do not support Administrator Passwords.

8. In the *Logon retries before token is locked* field, enter a numeric value. This counter specifies the number of times the user or 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.

9. If required, select **Token Password must be changed on first logon**.

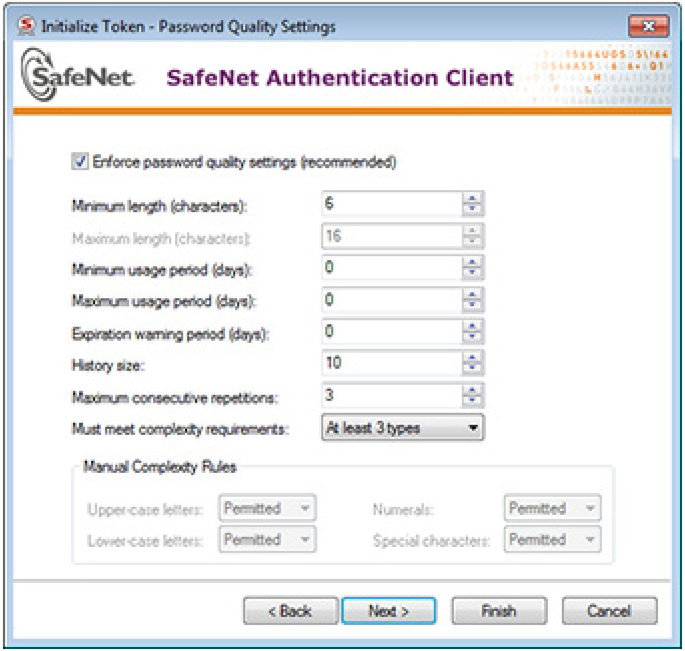
   This is selected by default.

10. Select **One-factor logon** only if the presence of the token is required to log on to applications. The Token Password will not be required. The default value for this setting is **disabled**.

    > **NOTE**
    >
    > Selecting the One-factor logon option disables the Create Token Password and Create Administrator Password fields.

11. Click **Next**.

The *Password Quality Settings* window opens.



Initialize Token - Password Quality Settings
SafeNet
SafeNet Authentication Client

☑ Enforce password quality settings (recommended)

Minimum length (characters):	6
Maximum length (characters):	16
Minimum usage period (days):	0
Maximum usage period (days):	0
Expiration warning period (days):	0
History size:	10
Maximum consecutive repetitions:	3
Must meet complexity requirements:	At least 3 types

Manual Complexity Rules

Upper-case letters:	Permitted	Numerals:	Permitted
Lower-case letters:	Permitted	Special characters:	Permitted

12 Complete the fields as follows:

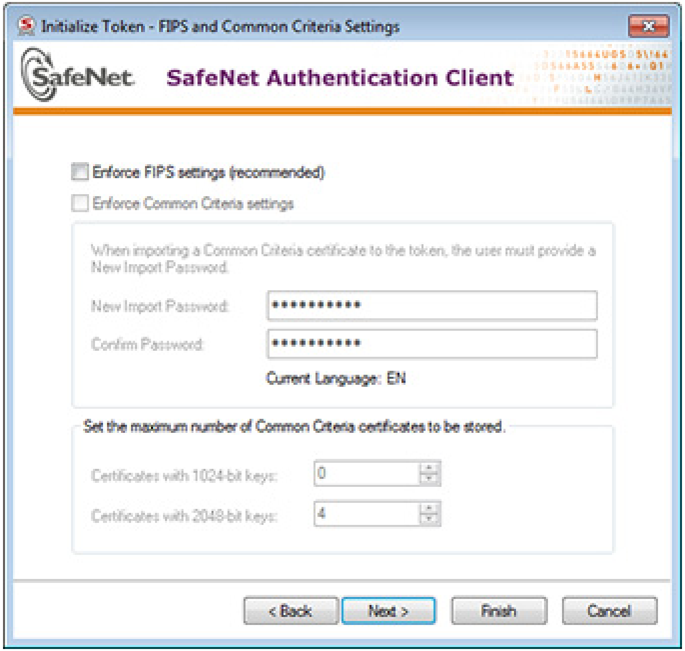
Field	Description
Enforce password quality settings (recommended)	Select this option if you want to define password quality settings when initializing a token. When selected, all options in the window become available.
Minimum length (characters)	Default: 6 characters
Maximum length (characters)	Default: 16 characters
Minimum usage period (days)	The minimum period before the password can be changed. Default: 0 (none) For iKey devices, the periods are rounded up to periods of weeks (7 days), even though the period is displayed in days. For example, if the period is displayed as less than a week, say 6 days, iKey regards it as a week. If the period is more than two weeks, say 15 days, iKey regards it as three weeks.
Maximum usage period (days)	The maximum period, in days, before which the password must be changed. Default: 0 (none) For iKey devices, the periods are rounded up to periods of weeks. See row above for more information.
Expiration warning period (days)	Defines the number of days before the password expires that a warning message is shown. Default: 0 (none)

Field (Cont.)	Description (Cont.)
History size	Defines how many previous passwords must not be repeated. Default: For eToken devices - 10 For iKey devices - 6
Maximum consecutive repetitions	The maximum number of repeated characters that is permitted in the password. Default: 3 This feature is not supported by iKey devices.
Must meet complexity requirements	Determines the complexity requirements that are required in the Token Password. ♦ **At least 2 types:** a minimum of 2 complexity rules (out of the 4 shown in the Manual Complexity fields) are enforced. ♦ **At least 3 types:** a minimum of 3 complexity rules (out of the 4 shown in the Manual Complexity fields) are enforced (Default). ♦ **None:** Complexity requirements are not enforced. ♦ **Manual:** Complexity requirements, as set manually in the *Manual Complexity* settings, are enforced.
Manual Complexity Rules	For each of the character types (**Upper-case letters, Lower-case letters, Numerals** and **Special characters**) select one of the following options: ♦ **Permitted -** Can be included in the password, but is not mandatory (Default). ♦ **Mandatory -** Must be included in the password. ♦ **Forbidden -** Must not be included in the password. **Note:** The **Forbidden** option is not supported by iKey devices.

13 Click **Next**.

The *FIPS and Common Criteria Settings* window opens.

Use this window to configure certification and common criteria settings.



Initialize Token - FIPS and Common Criteria Settings

SafeNet Authentication Client

□ Enforce FIPS settings (recommended)

□ Enforce Common Criteria settings

When importing a Common Criteria certificate to the token, the user must provide a New Import Password.

New Import Password: ***********

Confirm Password: ***********

Current Language: EN

Set the maximum number of Common Criteria certificates to be stored.

Certificates with 1024-bit keys: 0

Certificates with 2048-bit keys: 4

14 Select the certification type for formatting the token:

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

15 Enter a New Import Password in the *New Import Password* and *Confirm Password* fields.

Define and confirm a Password that must be entered when a Common Criteria certificate is imported to the token. The minimum Password length is 4 characters. The default value is: **1234567890**.

16 Under *Set the maximum number of Common Criteria certificates to be stored* complete the fields as follows:

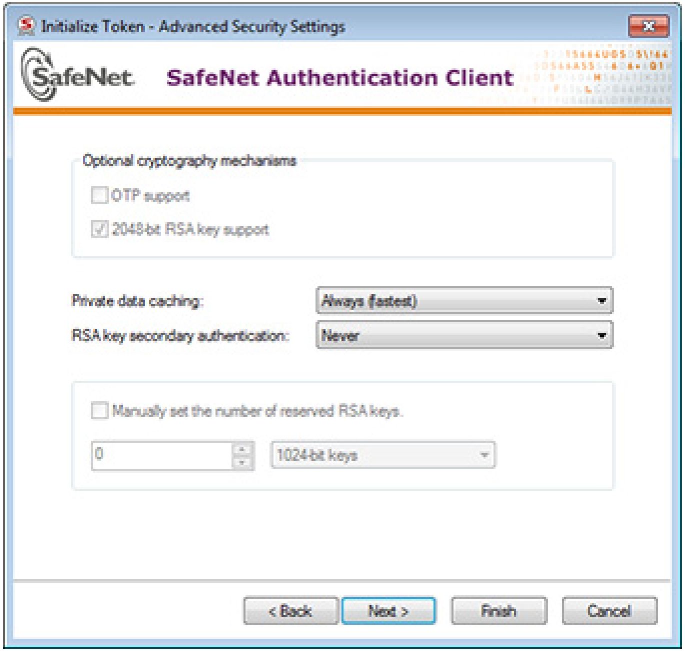
Field	Description
Certificates with 1024-bit keys	To reserve adequate space on the token, set the maximum number of Common Criteria certificates with 1024-bit keys that will be imported to the token. Select a number within the range 0 -16.

Certificates with 2048-bit keys	To reserve adequate space on the token, set the maximum number of Common Criteria certificates with 2048-bit keys that will be imported to the token. Select a number within the range 1- 16.

17 Click **Next**.

The *Advanced Security Settings* window opens.

Use this window to configure Cryptography and RSA Authentication Settings.



Initialize Token - Advanced Security Settings

SafeNet Authentication Client

Optional cryptography mechanisms

□ OTP support

☑ 2048-bit RSA key support

Private data caching: Always (fastest)

RSA key secondary authentication: Never

□ Manually set the number of reserved RSA keys.

0 | 1024-bit keys

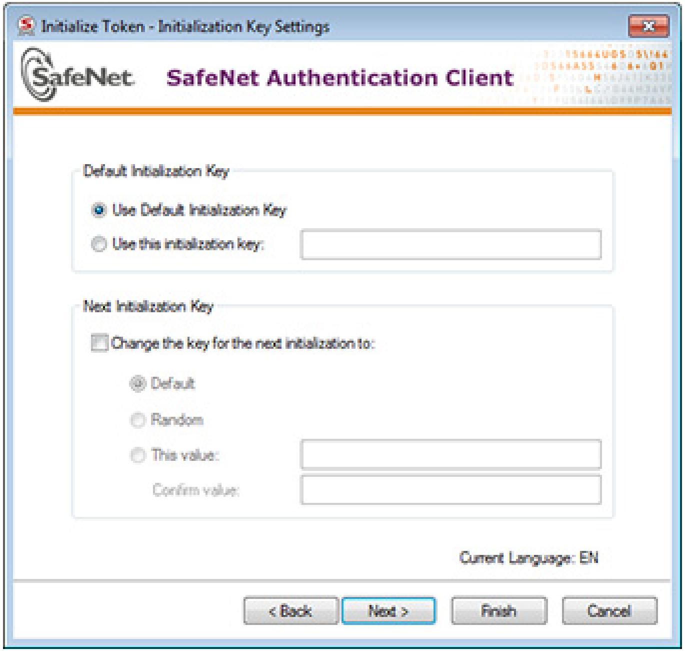
18 Under *Optional cryptography mechanism*, complete the fields as follows:

Field	Description
OTP Support	Default: disabled Select to enable OTP support (on compatible tokens).
2048-bit RSA key support	Default: enabled Select to enable 2048-bit RSA key support (on compatible tokens).
Private data caching	Default: Always (fastest) To enhance performance, SafeNet Authentication Client caches public information stored on the token. This option defines when private information (excluding private keys on the token) can be cached outside the token. Select one of the following options: ♦ Always (fastest): Private information is always cached in the application memory. This enables fast performance, as certain information is cached on the host machine. However, this option is less secure than if no cache is allowed. ♦ While user is logged on: Private information is cached outside the token as long as the user is logged on to the token. Once the user logs out, all the private data in the cache is erased. ♦ Never: Private information is not cached.

RSA key secondary authentication	Default: Never An authentication password may be set for an RSA key. Depending on how this option is set, in addition to having the token and knowing its Token Password, accessing the RSA key may require knowing the password set for that particular key. Having a password for the key is known as *secondary authentication*. Select one of the following: ♦ Always ♦ Always prompt user ♦ Prompt user on application request ♦ Never ♦ Token authentication on application request For an explanation of these options, see *Setting the RSA Key Secondary Authentication Field* on page 126. If the token was initialized as Common Criteria and the secondary authentication *Always*, *Always prompt user* or *Prompt upon application reques*t, then the secondary authentication setting cannot be changed to *Never* or *Token authentication on application request*. This limitation applies to Common Criteria certificates only.
Manually set the number of reserved RSA keys	Default: disabled Set the number of reserved RSA keys to reserve space in the token memory. This ensures that there will always be memory available for keys.

19 Click **Next.**

The *Initialization Key Settings* window opens.



Initialize Token - Initialization Key Settings

SafeNet Authentication Client

Default Initialization Key

● Use Default Initialization Key

○ Use this initialization key:

Next Initialization Key

□ Change the key for the next initialization to:

● Default

○ Random

○ This value:

Confirm value:

Current Language: EN

Use this window to configure Default and Next Initialization Settings.

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

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

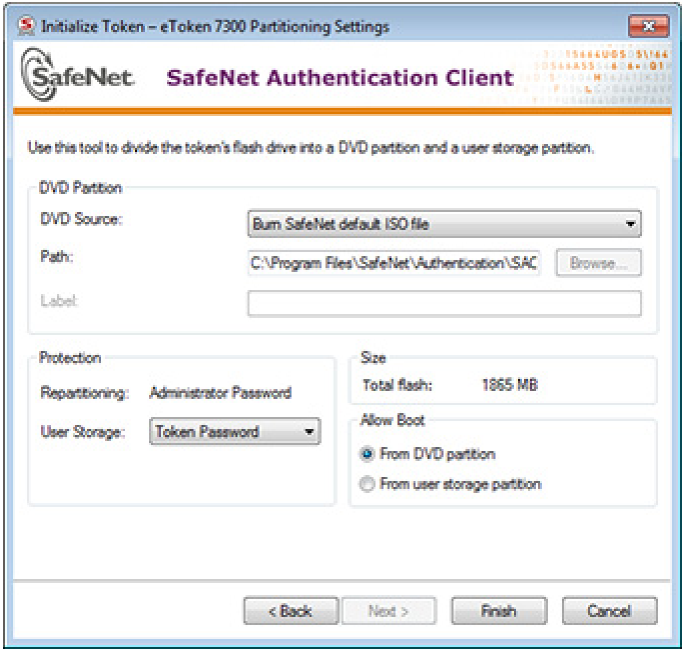
Field	Description
Use default initialization key	Select this option if the Initialization Key was not changed from its default during the previous token initialization. The factory-set default is used as the key for the current token initialization.
Use this initialization key	Enter the Initialization 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.

21 Click **Next**.

The *eToken 7300 Partitioning Settings* window opens.


Initialize Token – eToken 7300 Partitioning Settings
SafeNet
SafeNet Authentication Client

Use this tool to divide the token's flash drive into a DVD partition and a user storage partition.

DVD Partition

DVD Source: Burn SafeNet default ISO file

Path: C:\Program Files\SafeNet\Authentication\SAC

Label:

Protection

Repartitioning: Administrator Password

User Storage: Token Password

Size

Total flash: 1865 MB

Allow Boot

● From DVD partition

○ From user storage partition

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

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

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

NOTE

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

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

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

NOTE

- The SafeNet eToken 7300 initialization process always initializes the smartcard and partitions the flash drive.
- If partitioning settings are not set before the initialization proceeds, the default partitioning settings are used.
- iKey tokens do not support advanced initialization settings.

22 Under *DVD Partition*, complete the fields as follows:

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

23 Under *Protection*, complete the fields as follows:

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

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

NOTE

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

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

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

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

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

26 Click **Finish**.

The *Initialize Token Notification* window opens.

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

27 Click **OK**.

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

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

Setting the RSA Key Secondary Authentication Field

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

RSA Key Secondary Authentication settings

Setting	Description	
Always	Every time an RSA key is generated, the user is prompted to create a secondary password for accessing the key.	
	If the user clicks OK, the RSA key is generated, and the password entered becomes the new key's secondary password. When using the certificate, the user must authenticate once using the Token Password. For each operation that requires the RSA key, the user must authenticate using the secondary password.	If the user clicks Cancel, RSA key generation fails.

RSA Key Secondary Authentication settings

Setting	Description	
Always prompt user	Every time an RSA key is generated, the user is prompted to create a secondary password for accessing the key.	
	If the user clicks OK, the RSA key is generated, and the password entered becomes the new key's secondary password. When using the certificate, the user must authenticate once using the Token Password. For each operation that requires the RSA key, the user must authenticate using the secondary password.	If the user clicks Cancel, the RSA key is generated without a secondary password. When using the certificate, the user must authenticate once using the Token Password. No additional authentication is required for operations that require the RSA key.

RSA Key Secondary Authentication settings

<table>
<tr><th>Setting</th><th colspan="3">Description</th></tr>
<tr><td rowspan="2">Prompt user on application request</td><td colspan="2">When using an RSA key generation application that requires secondary passwords for strong private key protection (such as Crypto API with a user-protected flag, or the PKCS#11 CKA_ALWAYS_AUTHENTICATE attribute), the user is prompted to create a secondary password for accessing the RSA key.</td><td rowspan="2">When using applications that do not require secondary passwords for strong private key protection, the RSA key is generated without a secondary password.
When using the certificate, the user must authenticate once using the Token Password. No additional authentication is required for operations that require the RSA key.</td></tr>
<tr><td>If the user clicks OK, the RSA key is generated, and the password entered becomes the new key's secondary password.
When using the certificate, the user must authenticate once using the Token Password. For each operation that requires the RSA key, the user must authenticate using the secondary password.</td><td>If the user clicks Cancel, RSA key generation fails.</td></tr>
<tr><td>Never</td><td colspan="3">Secondary passwords are not created for new RSA keys.
When using the certificate, the user must authenticate once using the Token Password. No additional authentication is required for operations that require the RSA key.</td></tr>
</table>

RSA Key Secondary Authentication settings

<table>
<tr><th>Setting</th><th colspan="2">Description</th></tr>
<tr><td rowspan="2">Token authentication on application request</td><td colspan="2">Secondary passwords are not created for new RSA keys.
When using the certificate, the user must authenticate once using the Token Password.</td></tr>
<tr><td>When using an RSA key generated by an application that requires secondary passwords for strong private key protection (such as Crypto API with a user protected flag, or the PKCS#11 CKA_ALWAYS_AUTHENTICATE attribute), the user must authenticate using the Token Password for each operation that requires the RSA key.</td><td>When using an RSA key that was not generated by an application that requires secondary passwords for strong private key protection, no additional authentication is required for operations that require the RSA key.</td></tr>
</table>

5 SafeNet eToken Virtual

SafeNet Authentication Client supports the SafeNet eToken Virtual line of products. This includes SafeNet eToken Virtual and eToken Rescue tokens.

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

In this chapter:

Overview of SafeNet eToken Virtual Products

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

The following types of software tokens are available:

- **SafeNet eToken Rescue:** provides a solution when a staff member loses or damages their token when away from the office. A SafeNet eToken Rescue is a read-only token which functions for a limited period of time. You cannot import certificates to it.

  NOTE

  On a Mac System: SafeNet eToken Rescue must be run from a folder where the user has read-write permissions. If not, it will not be recognized by Mac Keychain Access.

- **SafeNet eToken Virtual:** performs all the functions of an eToken NG-OTP. It can store the same data, including key pairs and certificates. Its configuration may enable it to support OTP generation.

  A SafeNet eToken Virtual is “locked” to a particular computer or storage device, such as a flash drive. This means that it can be used only on the computer or storage device on which it was enrolled.

- **SafeNet eToken Virtual Temp**: identical to a SafeNet eToken Virtual, but its certificates become invalid after a pre-defined time period.

Connecting a SafeNet eToken Virtual

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

Under certain conditions, the token is connected automatically. See *Using a SafeNet eToken Virtual on an External Storage Device* on page 140.

To connect a SafeNet eToken Virtual token from the file:

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

   The SafeNet eToken Virtual or eToken Rescue connects to the computer and displays a confirmation message.

2. Click **OK**.

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

1. Open SafeNet Authentication Client Tools *Advanced* view*.*
   See *Opening the Advanced View* on page 38.
2. Do one of the following:
   - In the left pane, select the **Tokens** node.
     In the right pane, click the **Connect SafeNet eToken Virtual** icon:

     ⊕

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

   The SafeNet eToken Virtual product is connected.

Disconnecting or Deleting a SafeNet eToken Virtual Product

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

Under certain conditions, the token is disconnected automatically. See *Using a SafeNet eToken Virtual on an External Storage Device* on page 140.

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

To disconnect or delete a SafeNet eToken Virtual:

1 To use the *Simple* view to disconnect, do the following:

  a Open SafeNet Authentication Client Tools *Simple* view.
  See *Opening the Simple View* on page 33.

  b In the left pane, select the required SafeNet eToken Virtual or eToken Rescue token.

  c In the right pane, select **Disconnect SafeNet eToken Virtual** (or **Disconnect SafeNet eToken Rescue**).

  d Continue with step .

2 To use the *Advanced* view to disconnect, do the following:

  a Open SafeNet Authentication Client Tools *Advanced* view.
  See *Opening the Advanced View* on page 38.

b Do one of the following:

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

  ⏏

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

c Continue with step .

The *Disconnect SafeNet eToken Virtual* window opens.

3 Do one of the following:

♦ To keep the SafeNet eToken Virtual or eToken Rescue file on the computer or device for later use, click **Disconnect**.
Only the token connection to SafeNet Authentication Client is disconnected. It can be reconnected later. See *Connecting a SafeNet eToken Virtual* on page 132.

♦ To disconnect the token from SafeNet Authentication Client, and also remove the SafeNet eToken Virtual or eToken Rescue file from the computer, click **Delete**.
After a SafeNet eToken Virtual or eToken Rescue is deleted, it cannot be reconnected later. A new file must be installed before it can be connected.

Using a SafeNet eToken Virtual to Replace a Lost Token

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

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

Unlocking a SafeNet eToken Virtual

If you enter an incorrect password more than a pre-defined number of times, the SafeNet eToken Virtual becomes locked. To unlock the token, see Chapter 3: *Unlocking a Token by the Challenge-Response Method* on page 69, or *Unlocking a Token by an Administrator* on page 94.

NOTE

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

Generating a One-Time Password (OTP)

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

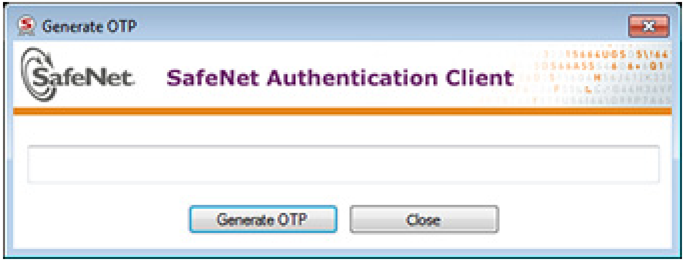
To generate an OTP:

1 Right-click the SafeNet Authentication Client tray icon.

The SafeNet Authentication Client tray menu opens.

2 Select **Generate OTP**.

The *Generate OTP* window opens.



3 Click **Generate OTP**.

The *Token Logon* window opens.

4 Enter the Token Password, and click **OK**.

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

5 Copy the OTP to authenticate yourself to your application.

NOTE

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

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

Using a SafeNet eToken Virtual on an External Storage Device

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

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

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

If the SafeNet eToken Virtual is located on an external storage device in a location other than the `eTokenVirtual` folder, you must connect the SafeNet eToken Virtual manually. See *Connecting a SafeNet eToken Virtual* on page 132.

Before removing the storage device, you must disconnect the SafeNet eToken Virtual manually. See *Disconnecting or Deleting a SafeNet eToken Virtual Product* on page 134. Otherwise, the SafeNet eToken Virtual will be displayed in SafeNet Authentication Client as a token with corrupted data.
For more information about token icons, see Chapter 2: *Token Icons* on page 35.

Using an Emulated SafeNet eToken Virtual

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

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

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

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

6 SafeNet eToken 7300

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

In this chapter:

Introduction to SafeNet eToken 7300

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

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

SafeNet eToken 7300 devices that have been initialized using SafeNet Authentication Client 9.0 work seamlessly on computers running either Windows or Mac operating systems. If SafeNet Authentication Client is not installed on your computer, connect your SafeNet eToken 7300 device and run the built-in launcher application. This application temporarily installs the SafeNet eToken 7300 tray menu for token management. If the token’s user storage has been password-protected, you must log on to your token to access its contents.

NOTE

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

SafeNet eToken 7300 Launcher

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

Running the Launcher to Open the Tray Icon on Windows

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

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

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

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

The eToken 7300's *AutoPlay* window opens.

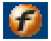
Continue with step 3.

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

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

3 Select **Run Launcher.exe**.

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

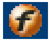


To run the launcher from the SafeNet-Authentication-Client folder:

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

2 Double-click **Launcher**.

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



Running the Launcher to Open the Tray Icon on Mac

Before running the launcher application on a Mac operating system, ensure that the appropriate reader slots have been allocated.

To run the launcher on a Mac operating system:

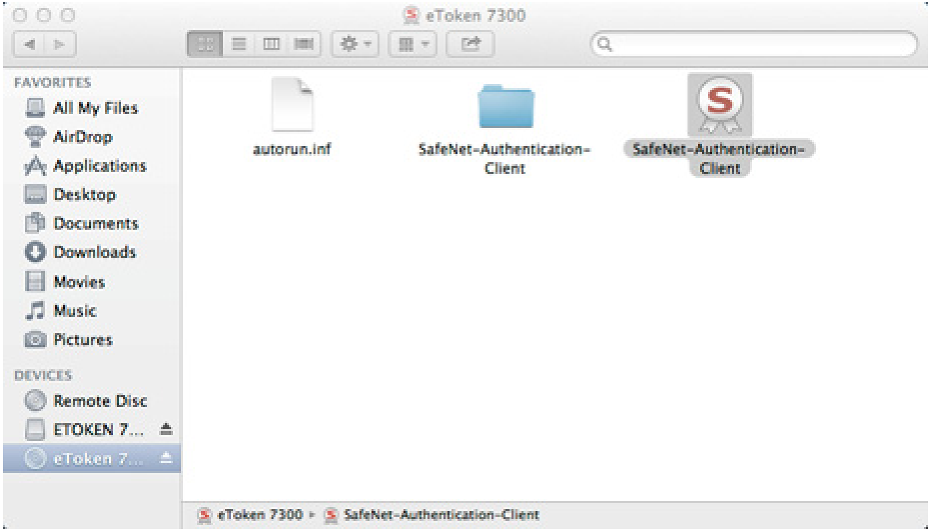
1 Connect the SafeNet eToken 7300 device and wait until the operating system recognizes it.

> **NOTE**
> If the device's user storage is not password-protected, the **ETOKEN 7300** icon is displayed.

2 Do one of the following:

- If the **eToken 7300** icon is displayed on the desktop, click it.
- If the **eToken 7300** icon is not displayed on the desktop, click the *Finder* icon, and under *DEVICES*, select **eToken 7300**.

The *eToken 7300* folder contents are displayed.



3 Click the **SafeNet-Authentication-Client** icon.

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

SafeNet eToken 7300 Tray Menu

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

SafeNet eToken 7300 Tray Menu Functions

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

- **About:** displays product version information and license information.
- Token selection allows you to select one of the connected tokens to be the active token. This function is available only when more than one SafeNet eToken 7300 device is connected.
- **Change Token Password:** opens the *Change Password* window for the selected token.
  See Chapter 3: *Changing the Token Password*, on page 65.
- **Unlock Token:** opens the *Unlock Token* window for the selected token.
  See Chapter 3: *Unlocking a Token by the Challenge-Response Method*, on page 69.
- **Certificate Information:** opens the *Token Certificate Information* window for the selected token.
- **Log On to Flash/Log Off from Flash:** displayed when a SafeNet eToken 7300 having a password-protected flash partition is connected. Opens the *Log On to Token* window for the selected token.
  See Chapter 3: *Logging On to the Token as a User*, on page 61.

- **Explore Flash:** this option opens Windows explorer, and becomes available only when you have selected the Log On to Flash option.
- **Exit:** closes the SafeNet eToken 7300 flash tray icon.

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

Using the SafeNet eToken 7300 Tray Icon

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

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

> **NOTE**
> When using a Mac operating system, click the SafeNet eToken 7300 icon; do not right-click it.

To open the SafeNet eToken 7300 tray menu:

- Right-click the SafeNet eToken 7300 icon.

  The SafeNet eToken 7300 shortcut menu opens.

Selecting the Token from the SafeNet eToken 7300 Tray Menu

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

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

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

Closing SafeNet eToken 7300

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

To close the SafeNet eToken 7300 tray icon manually:

1. Right-click the SafeNet eToken 7300 flash tray icon, and from the shortcut menu, select **Exit**.

   A warning message is displayed.
2. Click **OK**.

SafeNet eToken 7300 User Storage

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

The flash partition can be password-protected.

Accessing an Unprotected Flash Partition on Windows

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

1. Connect the SafeNet eToken 7300 device and wait until the operating system recognizes it.

   The ETOKEN 7300's *AutoPlay* window opens.

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

2. Do one of the following:

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

   The user storage contents are displayed.

Accessing a Protected Flash Partition on Windows

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

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

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

   > **NOTE**
   >
   > ♦ If SafeNet Authentication Client is installed, you can use the SafeNet Authentication Client tray menu to log on to your token. See Chapter 2: *SafeNet Authentication Client Tray Icon*, on page 26.
   >
   > ♦ On a Linux operating system, only the SAC Tray icon can be used to log onto an eToken 7300.
   >
   > ♦ If SafeNet Authentication Client is not installed, use the SafeNet eToken 7300 flash tray menu to log on to your token. See *SafeNet eToken 7300 Launcher* on page 144. (Windows and Mac only)

   The ETOKEN 7300’s *AutoPlay* window opens.

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

NOTE

If the *Log On to Token* window opens, re-enter the Token Password.

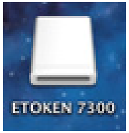
The user storage contents are displayed.

Accessing an Unprotected Flash Partition on Mac

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

1 Connect the SafeNet eToken 7300 device and wait until the operating system recognizes it.

The **ETOKEN 7300** icon is displayed on the desktop.

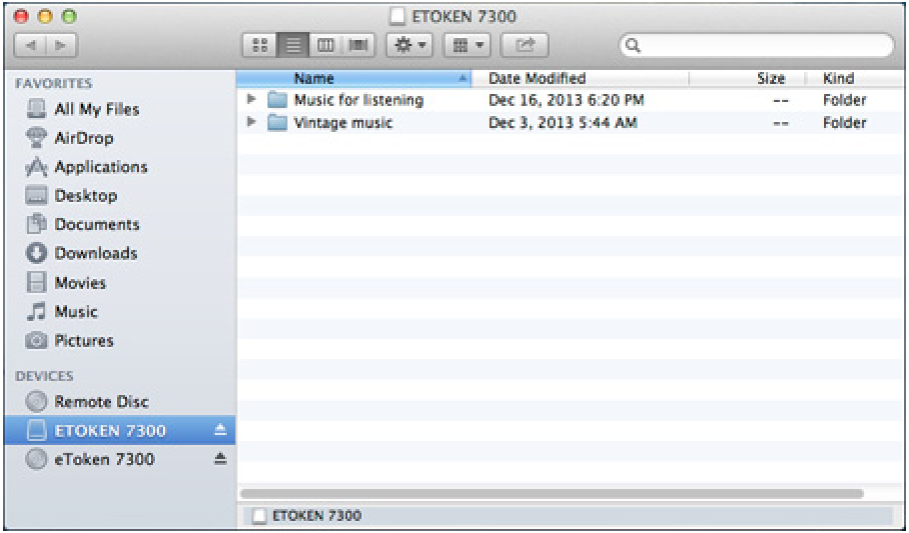


NOTE

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

2 Click the icon.

The user storage contents are displayed.



Name	Date Modified	Size	Kind
Music for listening	Dec 16, 2013 6:20 PM	--	Folder
Vintage music	Dec 3, 2013 5:44 AM	--	Folder

Accessing a Protected Flash Partition on Mac

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

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

1. Right-click the SafeNet eToken 7300 flash tray icon, and for the appropriate device, select **Log On to Token**.

2. Log on to the token.
   See Chapter 3: *Logging On to the Token as a User*, on page 61.

> **NOTE**
>
> ♦ If SafeNet Authentication Client is installed, use the SafeNet Authentication Client tray menu to log on to your token.
> See Chapter 2: *SafeNet Authentication Client Tray Icon*, on page 26.
>
> ♦ If SafeNet Authentication Client is not installed, use the SafeNet eToken 7300 flash tray menu to log on to your token.
> See *SafeNet eToken 7300 Launcher* on page 144.

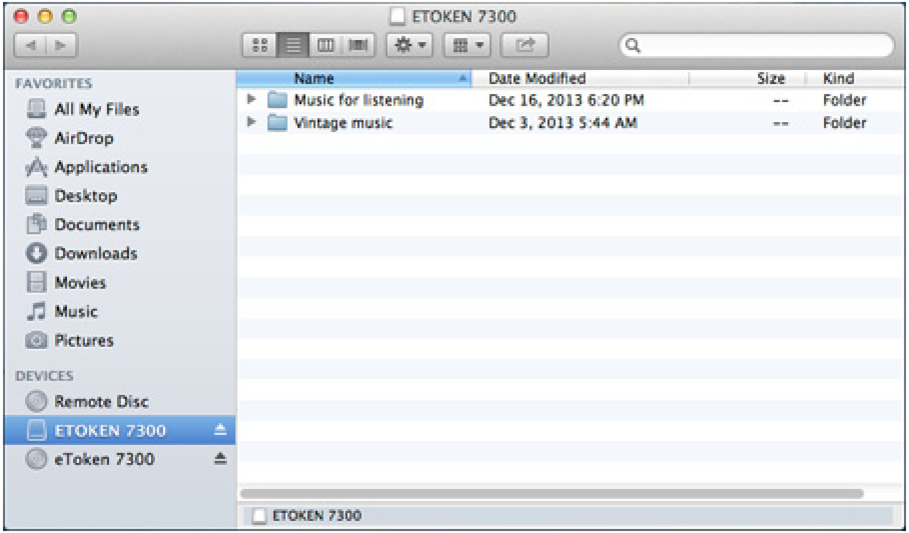
The **ETOKEN 7300** icon is displayed on the desktop.

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

3. Click the icon.

> **NOTE**
>
> If the *Log On to Token* window opens, re-enter the Token Password.

The user storage contents are displayed.



Name	Date Modified	Size	Kind
Music for listening	Dec 16, 2013 6:20 PM	--	Folder
Vintage music	Dec 3, 2013 5:44 AM	--	Folder

Partitioning the SafeNet eToken 7300

For details on how to partition the eToken 7300 see Chapter 4: Token Initialization.

7 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 8: *Token Settings* on page 171.

In this chapter:

Setting Password Quality

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

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 38.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Password Quality** tab.

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

TIP

The Password Quality settings are configured the same way as the Token Password quality settings.
See Chapter 8: *Setting Token Password Quality* on page 172.

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

NOTE

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

Copying User Certificates to a Local Store

SafeNet Authentication Client operations often require certificates, private keys, and public keys.

Private keys should always be stored securely on the token. Certificates should also be stored on the token, ensuring that the certificates are readily available when using the token on a different computer.

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

This option is selected by default.

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

1. Open SafeNet Authentication Client Tools *Advanced* view.
   See *Opening the Advanced View* on page 38.
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. Do one of the following:
   - ♦ To save your changes, click **Save**.
   - ♦ To ignore your changes, click **Discard**.

Copying CA Certificates to a Local Store (Windows only)

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 38.
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. Do one of the following:
   - To save your changes, click **Save.**
   - To ignore your changes, click **Discard.**

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 38.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab.
4. Select **Enable Single Logon.**
5. Do one of the following:
   - To save your changes, click **Save.**
   - To ignore your changes click, **Discard.**
6. To activate the single logon feature, log off from the computer and log on again.

Allowing Password Quality Configuration on Token after Initialization

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

NOTE
This feature is not supported by iKey tokens.

To enable password quality configuration after initialization:

1. Open SafeNet Authentication Client Tools *Advanced* view*.*
   See *Opening the Advanced View* on page 38.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab.
4. Select **Allow password quality configuration on token after initialization.**
5. Do one of the following:
   - To save your changes, click **Save.**
   - To ignore your changes, click **Discard.**

Allowing Only an Administrator to Configure Password Quality on Token

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

To define who can configure password quality on token:

1. Open SafeNet Authentication Client Tools *Advanced* view*.*
   See *Opening the Advanced View* on page 38.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab.
4. Do one of the following:
   - To enable configuration by the administrator only, select **Allow only an administrator to configure password quality on token**.
   - To enable configuration by the user also, clear **Allow only an administrator to configure password quality on token**.
5. Do one of the following:
   - To save your changes, click **Save.**
   - To ignore your changes, click **Discard.**

Showing the SafeNet Authentication Client Tray Icon

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

To show the SafeNet Authentication Client tray icon:

1. Open SafeNet Authentication Client Tools *Advanced* view*.*
   See *Opening the Advanced View* on page 38.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab.
4. In the *Show application tray icon* drop-down list, select one of the following:
   - ♦ **Never**: The tray icon is never displayed
   - ♦ **Always**: The tray icon is always displayed
5. Do one of the following:
   - ♦ To save your changes, click **Save.**
   - ♦ To ignore your changes, click **Discard.**

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 38.
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 - 254).
5. Do one of the following:
   - To save your changes, click **Save**.
   - To ignore your changes, click **Discard**.

Enabling Logging

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

NOTE

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

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

For Linux - The log files are located in: `\tmp\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 38.
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 38.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab, and click **Disable Logging**.

To activate the logging feature manually on a Linux System:

1. Edit the following file: `\etc\eToken.conf` file.
2. Add the following:

```
[LOG]

Enabled=1
```

To disable the logging feature manually on a Linux System:

1. Edit the following file: `\etc\eToken.conf` file.
2. Add the following:

```
[LOG]

Enabled=0
```

To activate the logging feature manually on a Mac system:

> **NOTE**
> The file must be opened using Administrator (write) privileges only.

1. Edit the following file: `\etc\eToken.conf file.`
2. Add the following:

```
 [LOG]

Enabled=0
```

8 Token Settings

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

For configurations set in *Client Settings*, that apply the settings to all tokens that are initialized after the settings have been configured, see Chapter 7: *Client Settings* on page 158.

In this chapter:

- Setting Token Password Quality
- Setting Private Data Caching Mode
- Setting RSA Key Secondary Authentication [Windows only?]

Setting Token Password Quality

If a token is initialized after Token Password quality parameters are set for the token, all future Token Passwords are automatically checked against these parameters to determine the password's level of acceptability.

If a token was initialized in early eToken PKI Client versions (RTE), no password policy is stored on the token.

If an iKey token was initialized in BSec Utilities, its password quality parameters will continue to be supported by SafeNet Authentication Client.

To set password quality for a token:

1. Open SafeNet Authentication Client Tools *Advanced* view*.*
   See *Opening the Advanced View* on page 38.
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

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

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

5 Do one of the following:

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

Setting Private Data Caching Mode

NOTE
This feature is not supported by iKey devices.

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

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

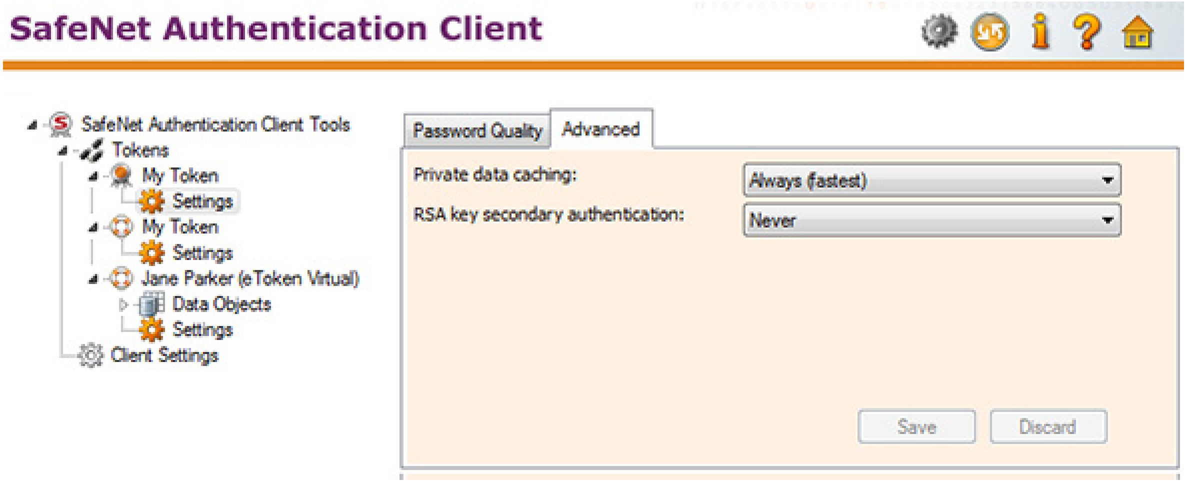
To set private data caching mode:

1 Open SafeNet Authentication Client Tools *Advanced* view*.*
See *Opening the Advanced View* on page 38.

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.



Private data caching: Always (fastest)

RSA key secondary authentication: Never

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

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

5. Do one of the following:
   - To save your changes, click **Save.**
   - To ignore your changes, click **Discard.**

Setting RSA Key Secondary Authentication

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

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

> **NOTE**
>
> This feature is not supported by iKey devices.

To set RSA key secondary authentication:

1. Open SafeNet Authentication Client Tools *Advanced* view*.*
   See *Opening the Advanced View* on page 38.
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 4: *Setting the RSA Key Secondary Authentication Field* on page 126.

5 Do one of the following:

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

9 Licensing

Import a SafeNet license for your SafeNet Authentication Client installation.

In this chapter:

Viewing and Importing Licenses

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

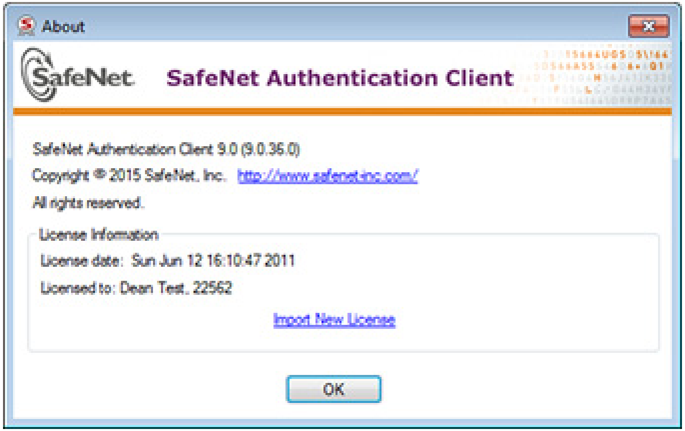
> **NOTE**
> After you have copied and saved the license file to the license dialog, a .lic file is generated in your home directory.

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

To view and import licenses:

1. Do one of the following:
   - Right-click the SafeNet Authentication Client tray icon, and from the shortcut menu, select **About**.
   - Open SafeNet Authentication Client Tools.
     See *Opening the Advanced View* on page 38.
     On the toolbar, click the **About** icon:

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



SafeNet Authentication Client 9.0 (9.0.36.0)

Copyright © 2015 SafeNet, Inc. http://www.safenet-inc.com/

All rights reserved.

License Information

License date: Sun Jun 12 16:10:47 2011

Licensed to: Dean Test, 22562

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

The *Import License* window opens.

3 Do one of the following:

- If the SafeNet license box is automatically filled, click **OK**.
- Copy your new SafeNet license string to the license box, and click **OK.**
- Click **Import from File**, browse to the file containing your license, open it to copy its contents to the license box, and click **OK**.
- The *About* window opens, displaying your updated license information in the *License Information* box.