

SafeNet Authentication Client (Linux)

Version 8.3 Revision A

User's Guide

Copyright © 2013 SafeNet, Inc. All rights reserved.

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 Manager 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.

Date of publication: March 2013

Last update: Thursday, March 28, 2013 5:28 pm

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:

<http://c3.safenet-inc.com/secure.asp>

Additional Documentation

The following SafeNet publications are available:

- SafeNet Authentication Client 8.3 (Linux) Administrator's Guide
- SafeNet Authentication Client 8.3 (Linux) CRN

Table of Contents

Chapter 1: Introduction	1
Overview.	2
SafeNet Authentication Client Main Features.	3
What's New.	4
Supported Browsers.	5
Supported Platforms.	6
. Supported Tokens	7
Supported Localizations	8
Chapter 2: SafeNet Authentication Client User Interfaces.	9
Overview of SafeNet Authentication Client User Interfaces.	10
SafeNet Authentication Client Tray Icon	11
Starting SafeNet Authentication Client	11
Closing SafeNet Authentication Client.	12
Opening the Tray Menu.	12
SafeNet Authentication Client Tray Menu Functions	12
SafeNet Authentication Client Tools	14
SafeNet Authentication Client Tools Toolbar	16
Opening the Simple View.	17
Token Icons	19

Simple View Functions	21
Opening the Advanced View	22
Advanced View Functions	24
Tokens Node	25
Selected Token Node	26
Certificates Nodes	29
Selected Certificate Node	32
Settings Node	34
Data Objects Node	36
Client Settings Node	38

Chapter 3: Token Management 39

Working with IdenTrustSelecting the Active Token	41
Viewing and Copying Token Information	43
Logging On to the Token as a User	46
Renaming a Token	48
Changing the Token Password	51
Unlocking a Token by the Challenge-Response Method	55
Deleting Token Content	59
Importing a Certificate onto a Token	62
Exporting a Certificate from a Token	67
Deleting a Certificate	70
Logging On to the Token as an Administrator	72

Changing the Administrator Password	74
Unlocking a Token by an Administrator	76
Working with IdenTrust	80
Chapter 4: Token Initialization	81
Overview of Token Initialization.	82
Configuring Initialization Settings.	83
Configuring Advanced Initialization Settings	87
Changing the Token Initialization Key.	90
Configuring Common Criteria Settings	93
Chapter 5: SafeNet eToken Virtual.	96
Overview of SafeNet eToken Virtual Products	97
Connecting a SafeNet eToken Virtual	98
Disconnecting or Deleting a SafeNet eToken Virtual Product.	99
Using a SafeNet eToken Virtual to Replace a Lost Token	102
Unlocking a SafeNet eToken Virtual	103
Using a SafeNet eToken Virtual on an External Storage Device	104
Chapter 6: Client Settings	105
Setting Password Quality	106

Allowing Password Quality Configuration on Token after Initialization	109
Allowing Only an Administrator to Configure Password Quality on Token	110
Enabling Logging	112
 Chapter 7: Token Settings	 114
Setting Token Password Quality.	115
Setting Private Data Caching Mode	120
 Chapter 8: Licensing	 123
Viewing and Importing Licenses	124

1

Introduction

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

In this chapter:

- Overview
- SafeNet Authentication Client Main Features
- What's New
- Supported Browsers
- Supported Platforms
- Supported Tokens
- Supported Localizations

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 . It provides a unified middleware client for a variety of SafeNet smart cards, and SafeNet eToken devices.

What's New

SafeNet Authentication Client 8.3 (Linux) offers the following new features:

- Alignment with SafeNet's new branding.
- Supports selection of multiple tokens from the tray menu.
- Support for SafeNet eToken 7300.

NOTE

SafeNet eToken 7300 manageability functionality (Partition, Initialization, Image burn, etc.) will only be available with SafeNet Authentication Client for Windows version 8.2 onwards.

Supported Browsers

SAC 8.3 (Linux) supports the following browsers:

- Firefox 18

SAC 8.3 (Linux) supports the following mail clients:

- Thunderbird 17

Supported Platforms

SAC 8.3 (Linux) supports the following operating systems:

- Red Hat 5.8 (32-bit and 64-bit)
- Red Hat 6.3 (32-bit and 64-bit)
- Red Hat 5.7 (32-bit and 64-bit)
- Red Hat 6.1 (32-bit and 64-bit)
- Ubuntu 12.04 (32-bit and 64-bit)
- Ubuntu 12.10 (32-bit and 64-bit)
- Debian 6.0 (32-bit and 64-bit)
- SUSE 11 (32-bit and 64-bit)
- CentOS 6.3 (32-bit and 64-bit)
- Fedora 17 (32-bit and 64-bit)
- Fedora 18 (32-bit and 64-bit)

Supported Tokens

SafeNet Authentication Client 8.3 (Linux) supports the following tokens:

- SafeNet eToken 7300
- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 4100
- SafeNet eToken PRO
- SafeNet eToken PRO Anywhere (SC Operations only)
- SafeNet eToken PRO Smartcard
- SafeNet eToken NG-OTP
- SafeNet eToken NG-Flash
- SafeNet eToken NG-Flash Anywhere (Not protected Flash and SC operations only)
- SafeNet eToken Virtual Family

NOTE

SafeNet Authentication Client 8.3 (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.

Supported Localizations

SafeNet Authentication Client 8.3 (Linux) supports the following languages:

- English

2

SafeNet Authentication Client User Interfaces

This section describes the SafeNet Authentication Client user interfaces.

In this chapter:

- Overview of SafeNet Authentication Client User Interfaces
- SafeNet Authentication Client Tray Icon
- SafeNet Authentication Client Tools

Overview of SafeNet Authentication Client User Interfaces

SafeNet Authentication Client provides two user interfaces:

- SafeNet Authentication Client Tray Icon
 - ◆ for quick access to many of the functions in the application
- SafeNet Authentication Client Tools
 - ◆ provides information about each connected token, including its identification and capabilities
 - ◆ has access to information stored on each connected token, such as keys and certificates
 - ◆ enables management of token content, such as password profiles

SafeNet Authentication Client Tray Icon

The SafeNet Authentication Client tray icon offers a shortcut menu to many of the application's functions.

NOTE

The SafeNet Authentication Client tray icon appears faded until a token is connected.

When SafeNet Authentication Client is closed, the tray icon is not displayed.

In the standard SafeNet Authentication Client installation, when one token is connected, the tray icon is displayed as:



When more than one token is connected, the tray icon is displayed as:



Starting SafeNet Authentication Client

To start SafeNet Authentication Client:

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

Closing SafeNet Authentication Client

To close SafeNet Authentication Client:

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

Opening the Tray Menu

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

- Click the SafeNet Authentication Client tray icon.

SafeNet Authentication Client Tray Menu Functions

The following functions can be accessed quickly from the tray menu:

- **Change Token Password:** opens the *Change Password* window for the selected token.
- **Certificate Information:** opens the *Token Certificate Information* window.
- **Unlock Token:** opens the *Unlock Token* window.
- **Tools:** opens *SafeNet Authentication Client Tools*.
- **About:** displays product version information and license information, and enables license import.
- **Exit:** closes SafeNet Authentication Client and the tray icon.

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

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

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 transfer digital certificates and keys between a computer and a token.

SafeNet Authentication Client 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.

CAUTION

Do not disconnect a token from the USB port, or a smart card from the reader, during an operation. This may cause corruption of the data on the token or smart card.

SafeNet Authentication Client Tools includes two viewing options:







- **Simple view:** to perform common tasks.
See *Opening the Simple View* on page 17.
- **Advanced view:** for extensive control over SafeNet Authentication Client and your connected tokens.
See *Opening the Advanced View* on page 22.

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 SafeNet Authentication Client Tools, in both *Simple* and *Advanced* views. The toolbar contains the following icons:

Icon	Action
	Advanced View - switches from the Simple to the Advanced view
	Simple View – switches from the Advanced to the Simple view
	Refresh – refreshes the data for all connected tokens
	About – displays product version information and license information, and enables license import
	Help – opens the Help feature
	Home – opens the company website

Opening the Simple View

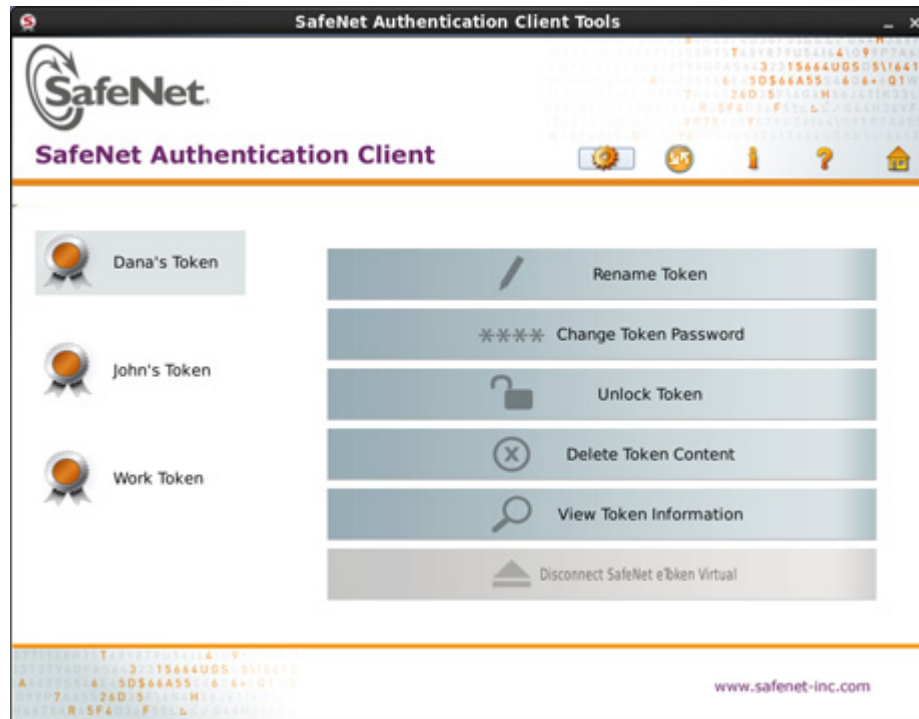
When SafeNet Authentication Client Tools is opened, the *Simple* view is displayed.

To open SafeNet Authentication Client Tools:

Do one of the following:

- Click the SafeNet Authentication Client tray icon, and from the shortcut menu, select **Tools**.
- Go to **Applications > SafeNet Authentication Client Tools**.

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







When tokens are connected, icons representing each connected token are 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	Type
	eToken PRO (SafeNet eToken 5100) eToken NG Flash (SafeNet eToken 7100) SafeNet eToken Virtual
	eToken PRO Anywhere (SafeNet eToken 5200)
	eToken NG-OTP (SafeNet eToken 7000) SafeNet eToken Virtual, OTP enabled
	SafeNet eToken Virtual Temp
	SafeNet eToken Rescue

Icon (Cont.)	Type (Cont.)
	Smart card reader – no card connected
	Smart card reader – card connected: ◆ eToken PRO smart card (SafeNet eToken 4100)
	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 the token name
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 Information	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 SafeNet Authentication Client Tools Advanced View:

1 Do one of the following:

- ◆ Click the SafeNet Authentication Client tray icon, and from the shortcut menu, select **Tools**.
- ◆ From the Windows taskbar, select **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.



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

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

Tokens Node

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



The following functions are available:

Function	Icon	Right-Click Menu Item
Connect SafeNet eToken Virtual See <i>Connecting a SafeNet eToken Virtual</i> on page 98.		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
- the name of the token reader is displayed in the tool-tip



The following user functions are available:

User Function	Icon	Right-Click Menu Item
<p>Initialize Token</p> <p>See <i>Token Initialization</i> on page 81.</p>		Initialize
<p>Log On to Token</p> <p>See <i>Logging On to the Token as a User</i> on page 46.</p>		Log On
<p>Import Certificate</p> <p>See <i>Importing a Certificate onto a Token</i> on page 62.</p>		Import Certificate
<p>Change Password</p> <p>See <i>Changing the Token Password</i> on page 51.</p>		Change Password
<p>Rename Token</p> <p>See <i>Renaming a Token</i> on page 48.</p>		Rename
<p>Disconnect SafeNet eToken Virtual (SafeNet eToken Virtual or SafeNet eToken Rescue only)</p> <p>See <i>Disconnecting or Deleting a SafeNet eToken Virtual Product</i> on page 99.</p>		Disconnect

User Function (Cont.)	Icon (Cont.)	Right-Click Menu Item (Cont.)
Copy to Clipboard See <i>Viewing and Copying Token Information</i> on page 43.		None

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



Certificates Nodes


If the selected token contains certificates, one or two appropriate nodes are displayed in the left pane under the token:

- User certificates
- CA certificates
- CC certificates

When you select one of these nodes, a list of the appropriate certificates on the token is displayed in the right pane.



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




User Function	Icon	Right-Click Menu Item
Import Certificate See <i>Importing a Certificate onto a Token</i> on page 62.		Import Certificate

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.



The following functions are available:

User Function	Icon	Right-Click Menu Item
Delete Certificate <i>See Deleting a Certificate on page 70.</i>		Delete Certificate
Export Certificate <i>See Exporting a Certificate from a Token on page 67.</i>		Export Certificate
Copy to Clipboard <i>See Viewing and Copying Token Information on page 43.</i>		None

Settings Node

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



The *Settings* window contains two tabs:

- Password Quality (See *Setting Token Password Quality* on page 115.)
- Advanced (See *Setting Private Data Caching Mode* on page 120 and *To ignore your changes, click Discard.* on page 122.)

Data Objects Node

Tokens used together with Entrust applications contain PKCS#11 data objects.




To view the contents of a data object:

- 1 Expand the **Data Objects** node.
- 2 Select a data object.

The contents of the data object (**Name**, **Type** and **Size**) are displayed in the right pane.



To delete a data object:

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

Client Settings Node

Select the *Client Settings* node to open the *Client Settings* window in the right pane.

The changes you make to the *Client Settings* window will affect all tokens that will be initialized after the changes have been saved.

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

- Password Quality
- Advanced

See *Client Settings* on page 105.

3

Token Management

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

NOTE

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

In this chapter:

- Working with IdemTrustSelecting the Active Token
- Viewing and Copying Token Information
- Logging On to the Token as a User
- Renaming a Token
- Changing the Token Password
- Unlocking a Token by the Challenge-Response Method
- Deleting Token Content

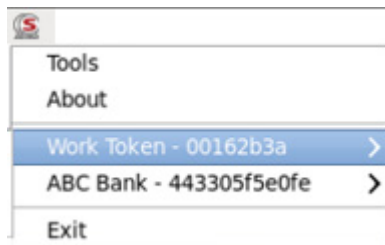
- Importing a Certificate onto a Token
- Exporting a Certificate from a Token
- Deleting a Certificate
- Logging On to the Token as an Administrator
- Changing the Administrator Password
- Unlocking a Token by an Administrator

If more than one token is connected, you can select the active token using the tray menu. This allows you to perform specific tasks for the token selected.

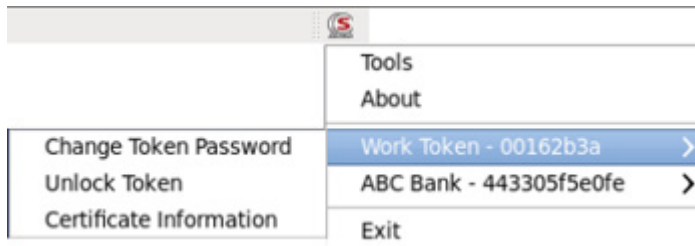
To use the tray menu to set a token as the active token:

- 1 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 is appears displaying a list of tasks that can be performed on the active token.



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

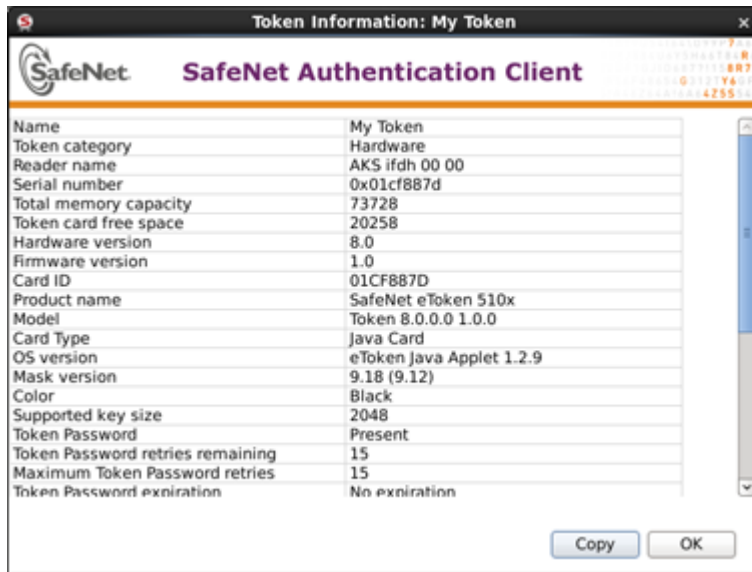
To use SafeNet Authentication Client Tools to set a token as the active token:

- 1 Open SafeNet Authentication Client Tools.
See Opening the Simple View on page 17 or See Opening the Advanced View on page 22.
- 2 In the left pane, select the required token.

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 17.
 - b** In the left pane, select the required token.
 - c** In the right pane, select **View Token Information**.
 - 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 22.
 - b** In the left pane, select the node of the required token.
 - c** Continue with step 3.
- 3** The *Token Information* window is displayed.



The information displayed may vary according to the type of token.

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 22.
- 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:

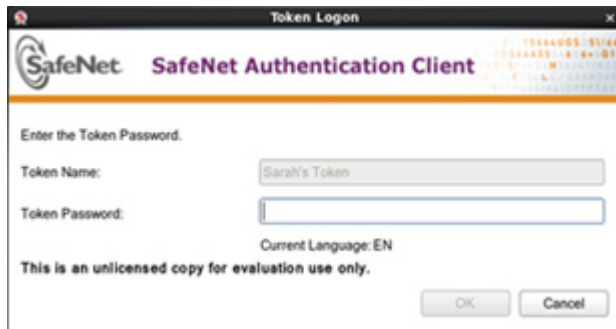


- ◆ In the left pane, right-click the node of the required token, and select **Log On** from the shortcut menu.

NOTE

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

- 3 The *Token Logon* window opens.



- 4 Enter the Token Password, and click **OK**.
You are logged on to the token.

Renaming a Token

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

TIP

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

To rename a token:

- 1 To use the Simple View to rename a token, do the following:
 - a Open SafeNet Authentication Client Tools *Simple View*.
See Opening the Simple View on page 17.
 - b In the left pane, select the required token.
 - c In the right pane, select **Rename Token**.
 - d Continue with step 3.
- 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 22.

b Do one of the following:

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

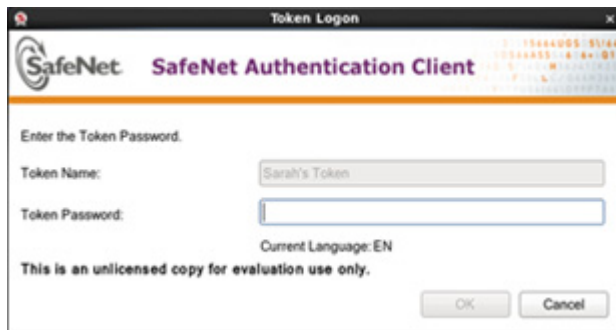
In the right pane, click the **Rename Token** icon:



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

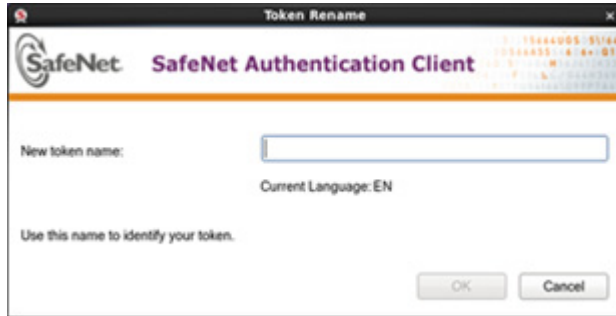
c Continue with step 3.

3 The *Token Logon* window opens.



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

The *Rename Token* window opens.



- 5 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: **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 user cannot use the token.

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

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, 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 the Token Password:

1 To use the Simple View to change the Token Password, do the following:

- a** Open SafeNet Authentication Client Tools *Simple View*.
See Opening the Simple View on page 17.
- b** In the left pane, select the required token.
- c** In the right pane, select **Change Token Password**.
- d** Continue with step 4.

2 To use the Advanced View to change the Token Password, do the following:

- a** Open SafeNet Authentication Client Tools *Advanced View*.
See Opening the Advanced View on page 22.
- b** Do one of the following:

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

In the right pane, click the **Change Token Password** icon:



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

- c** Continue with step 4.

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

- a Right-click the SafeNet Authentication Client tray icon.
 - b Select **Change Token Password**.
 - c Continue with step 4.
- 4 The *Change Password* window opens.

Change Password: My Token

SafeNet 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 new Password.

OK Cancel

- 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 will be 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 will be locked. Tokens, including SafeNet eToken Virtual tokens, can be unlocked if, and only if, an Administrator Password was set during initialization.

SafeNet eToken Rescue tokens cannot be unlocked.

CAUTION

The number of times that a token can be unlocked can be limited to a specific amount. If this number is exceeded and the token is locked, 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 Unlocking a Token by an Administrator on page 76.)

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 new Token Password set by the user replaces the previous password, and the token is unlocked.

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

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 17.
 - 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 a token, do the following:
 - a** Open SafeNet Authentication Client Tools *Advanced View*.
See Opening the Advanced View on page 22.
 - 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:

 - c** 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, displaying a value in the *Challenge Code* field.

Unlock Token: My Token

SafeNet Authentication Client

Challenge Code: 

Response Code:

☐ Token Password must be changed on first login

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 a new Password.

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

NOTE

To copy the Challenge Code to the clipboard, click the Copy Challenge Code to clipboard icon:



CAUTION

After providing the Challenge Code to the administrator, **do not** undertake any activities that use the token until receiving the Response Code and completing 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.

- 5 The administrator provides you with the *Response Code* to be entered.

NOTE

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

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

Deleting Token Content

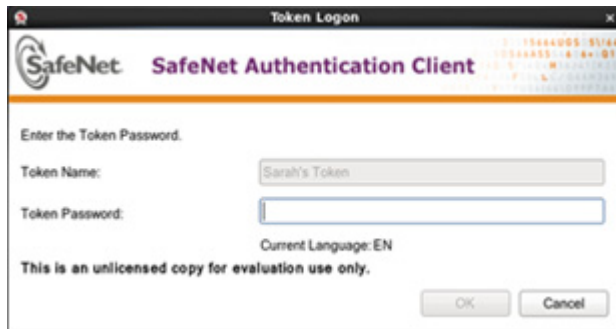
Objects on your token include data objects (profiles), keys, and CA or user certificates. Your system configuration determines which objects are deletable.

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

The *Delete Token Content* function is less comprehensive than the *Initialize* function which restores a token to its initial state, removing all objects stored on the token since manufacture and resetting the Token Password. (See Token Initialization on page 81.)

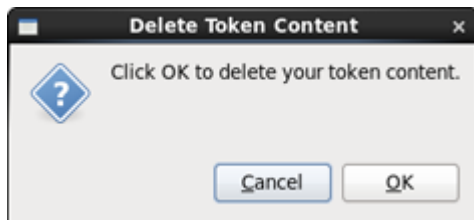
To delete token content:

- 1 To use the Simple View to delete the token content, do the following:
 - a Open SafeNet Authentication Client Tools *Simple View*.
See Opening the Simple View on page 17.
 - b In the left pane, select the required token.
 - c In the right pane, select **Delete Token Content**.
- 2 The *Token Logon* window opens.



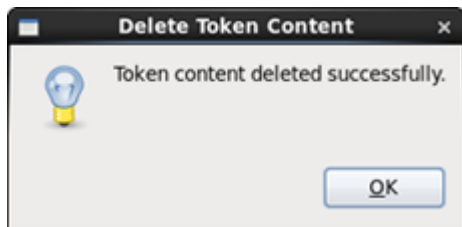
- 3 Enter the Token Password, and click **OK**.

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



- 4 To continue with the delete process, click **OK**.

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



- 5 Click **OK** to finish.

Importing a Certificate onto a Token

The following certificate types are supported:

- .pfx
- .p12
- .cer

In the case of a PFX file, the private key and corresponding certificate will be imported to the token. If so configured, you will be asked if CA certificates should be imported to the token, and you will be asked to enter the password (if it exists) that protects the PFX file.

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, then 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, be sure to remove the certificate from the local store and then reconnect the token before using the certificate to sign and encrypt mail. This ensures that you are using the certificate and keys stored on the token and not on the computer.

NOTE

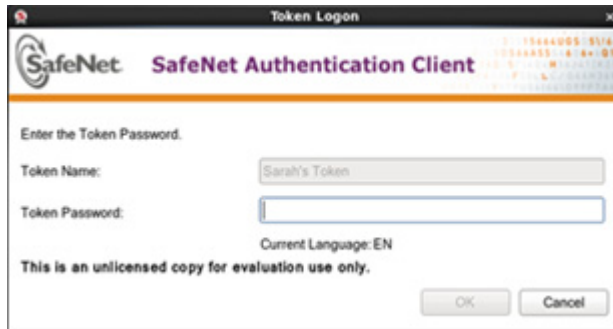
It is not possible to import a certificate onto a SafeNet eToken Rescue.

To import a certificate:

- 1 Open SafeNet Authentication Client Tools *Advanced View*.
See Opening the Advanced View on page 22.
- 2 Do one of the following:
 - ◆ In the left pane, select the node of the required token.
In the right pane, click the **Import Certificate** icon.

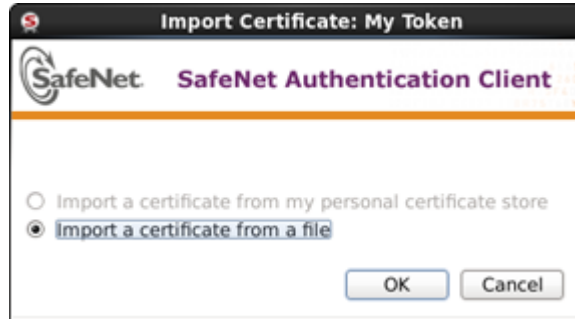


- ◆ In the left pane, right-click the node of the required token, and select **Import Certificate** from the shortcut menu.
- 3 The *Token Logon* window opens.



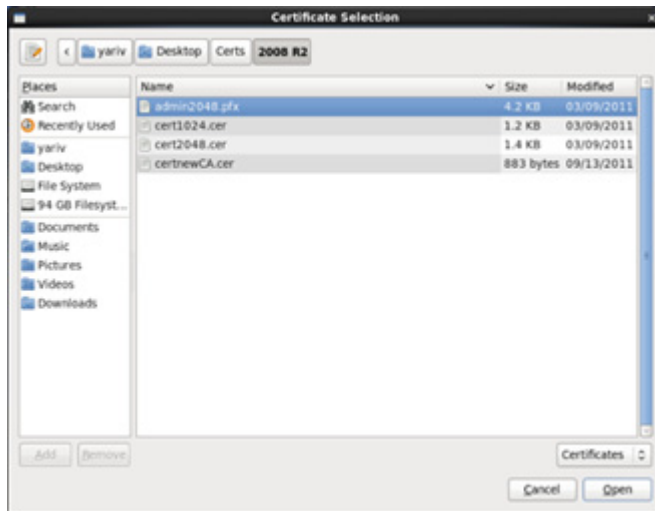
- 4 Enter the Token Password, and click **OK**.

The *Import Certificate* window opens.



- 5 Select *Import a certificate from a file*.

The *Certificate Selection* window opens.



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

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



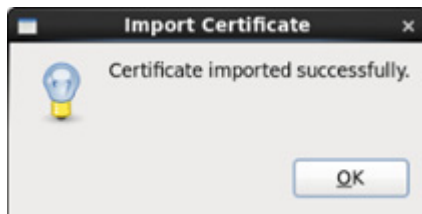
Enter the certificate password, and click **OK**.

- 7** 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**.

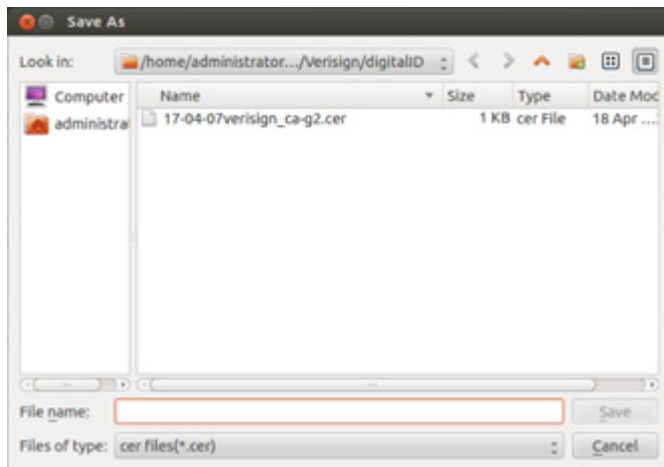
- 8** All requested certificates are imported, and a message confirms that the import was successful.



Exporting a Certificate from a Token

To export a certificate:

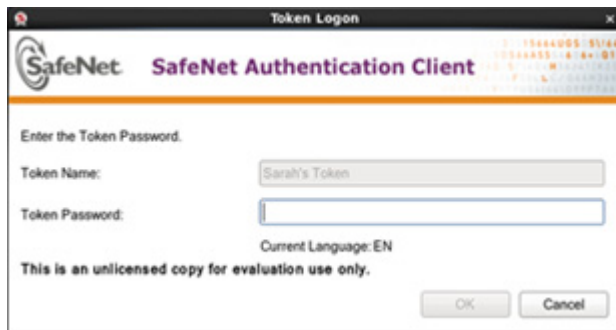
- 1 Open SafeNet Authentication Client Tools *Advanced View*.
See Opening the Advanced View on page 22.
- 2 In the left pane, expand the node of the required token.
- 3 Do one of the following:
 - ◆ Select the required certificate, and click the **Export Certificate** icon:

 - ◆ Right-click the required certificate, and select **Export Certificate** from the shortcut menu.
- 4 The *Save As* window opens.



- 5 Select the location to store the certificate, enter a file name, and click **OK**.

NOTE

The certificate file must be DER encoded or Base64 (not PKCS #7).



Deleting a Certificate

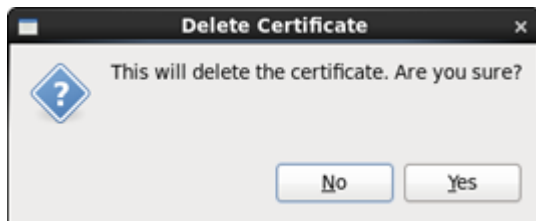
You can remove a certificate from a token.

To delete a certificate from a token:

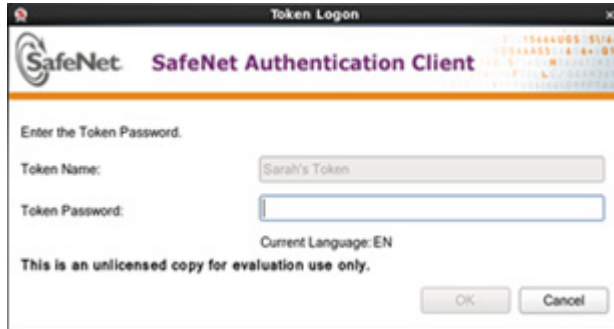
- 1 Open SafeNet Authentication Client Tools *Advanced View*.
See Opening the Advanced View on page 22.
- 2 In the left pane, expand the node of the required token.
- 3 Do one of the following:
 - ◆ In the left pane, select the required certificate, and click the **Delete Certificate** icon.



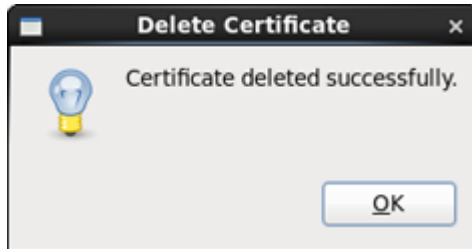
- ◆ In the left pane, right-click the required certificate, and select **Delete Certificate** from the shortcut menu.
- 4 The *Delete Certificate* window opens.



- 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, the Administrator Password can be used to unlock the token by setting a new Token Password. We recommend initializing all supported tokens with an Administrator Password.

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

- Changing the Administrator Password
- Unlocking a Token by an Administrator
- Unlocking a Token by the Challenge-Response Method
- Setting Token Password Quality
- Setting Private Data Caching Mode
- To ignore your changes, click Discard.

To log on to a token as an administrator:

- 1 Open SafeNet Authentication Client Tools *Advanced View*.
See Opening the Advanced View on page 22.

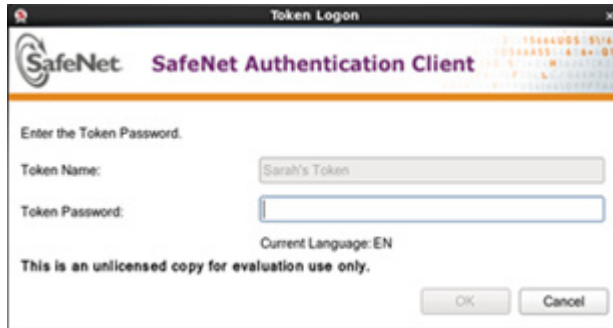
2 Do one of the following:

- ◆ 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 *Token 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*.
See Opening the Advanced View on page 22.
- 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.

Change Administrator Password: My Token

SafeNet Authentication Client

Current Administrator Password

New Administrator 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 a new Password.

OK Cancel

- 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 will be 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** again.

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.

NOTE

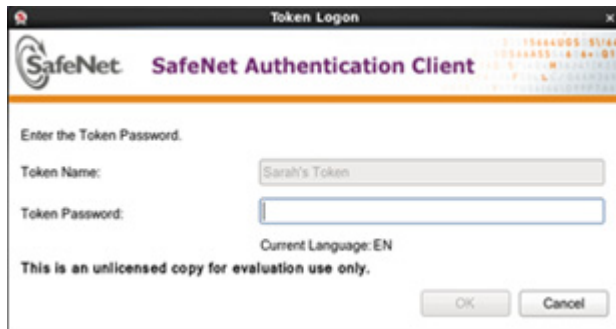
The unlock feature may also be accessed by right-clicking the tray icon.

To unlock a token using *Set Token Password*:

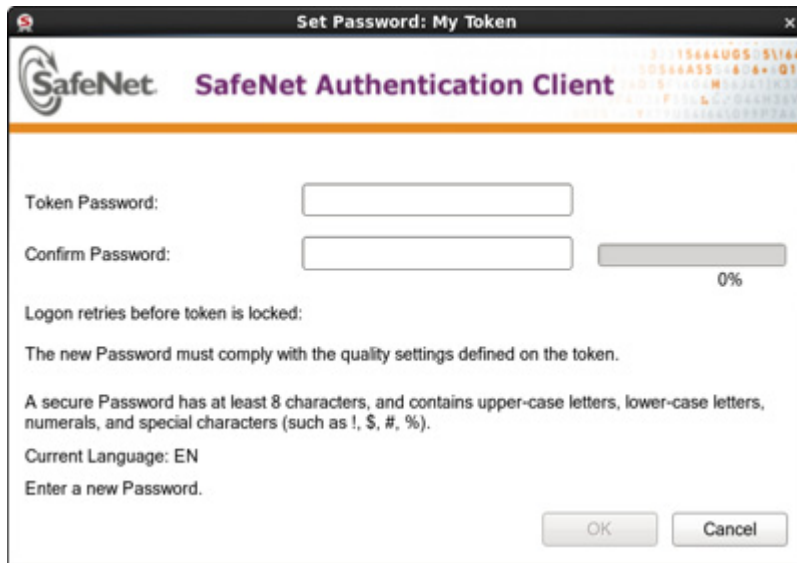
- 1 Open SafeNet Authentication Client Tools *Advanced View*.
See Opening the Advanced View on page 22.
- 2 In the left pane, select the appropriate token.
- 3 Click the **Set Token Password** icon:



The *Token Logon* window opens.



- 4 Enter the Administrator Password, and click **OK**.
The *Set Token Password* window opens.



Set Password: My Token

SafeNet SafeNet Authentication Client

Token Password:

Confirm Password: 0%

Logon retries before token is locked:

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 new Password.

OK Cancel

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

NOTE

The new Token Password must meet password quality settings as defined for the token.

- 6 Set the *Set maximum number of logon failures* field to the required number.

NOTE

The *Set maximum number of logon failures* feature is available only on CardOS tokens. Java card tokens are not supported.

7 Click **OK**.

A message confirms that the Token Password was changed successfully.



8 Click **OK**.

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

Working with IdenTrust

IdenTrust supports the following mode:

- **Token Password** - Token Password is used as an Identity PIN and is entered every time that an identity certificate is used.

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
- Configuring Advanced Initialization Settings
- 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)
- 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.

To initialize a token:

- 1 Open SafeNet Authentication Client Tools *Advanced View*.
See <Emphasis>Opening the Advanced View on page 22.

- 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** from the shortcut menu.

The *Token Initialization* window opens.

Initialize Token

SafeNet SafeNet Authentication Client

Token Name:

☒ Create Token Password

New Token Password:

Confirm:

Set maximum number of logon failures:

☐ Create Administrator Password

New Administrator Password:

Confirm:

Set maximum number of logon failures:

Note: Many tokens can be unlocked only if they have an Administrator Password.

☒ Token Password must be changed on first logon

[Partitioning Settings](#)
[Advanced Settings](#)

- 3 Enter a name for the token in the *Token Name* field. If no name is entered, the default name, “My Token”, is applied.

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

- 4 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.
- 5 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 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 default 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 Setting Token Password Quality on page 115.

- 6 To initialize an Administrator Password, select **Set 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.

- 7 In the *Logon retries before token is locked* field, enter a value between 1 and 15. 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.
- 8 If required, select **Token Password must be changed on first logon**.
This is selected by default.
- 9 To configure advanced settings, see Configuring Advanced Initialization Settings on page 87.

10 Click **Start**.

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

Configuring Advanced Initialization Settings

To configure advanced initialization settings:

- 1 Open the *Token Initialization* window.
See *Configuring Initialization Settings* on page 83.
- 2 Click **Advanced Settings**.

The *Advanced Token Initialization Settings* window opens.



3 Complete the fields as follows:

Field	Description
One-factor logon	Default: disabled. When one factor logon is enabled, only the presence of the token is required to log on to applications. The Token Password is not required.
Password quality settings on token	Default: enabled Select to keep password quality requirements on the token device.
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: <ul style="list-style-type: none">◆ Always (fastest): Private information is always cached in the application memory. This enables fast performance, as certain information is cached on the host machine. However, this option is less secure than if no cache is allowed.◆ While user is logged on: Private information is cached outside the token as long as the user is logged on to the token. Once the user logs out, all the private data in the cache is erased.◆ Never: Private information is not cached.

Field (Cont.)	Description (Cont.)
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.
Certification	Default: N/A Select the certification type for formatting the token. Select one of the following options: <ul style="list-style-type: none"> ◆ N/A: None ◆ FIPS: Federal Information Processing Standards is a US government approved set of standards designed to improve the utilization and management of computer and related telecommunication systems ◆ Common Criteria: an international standard for computer security certification
Change Initialization Key (link)	The initialization key protects against accidental initialization and requires a separate password to be entered before initialization can occur.
Common Criteria Settings (link)	If <i>Certification</i> is set to Common Criteria , click this button to set the certificate import PIN and the maximum number of certificates for which to reserve space on the token.

4 You can do the following:

- ◆ To change the token initialization key, see Changing the Token Initialization Key on page 90.
- ◆ To define the Common Criteria settings, see Configuring Common Criteria Settings on page 93.

5 To return to the *Token Initialization* window, click **OK**.

Changing the Token Initialization Key

Change the Initialization Key to protect against accidental token 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 key during future initialization of the token.

To change the Token Initialization Key:

- 1 Open the *Advanced Settings* window.
See *Configuring Advanced Initialization Settings* on page 87.
- 2 Click **Change Initialization Key**.
The *Initialization Key* window opens.



3 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 <i>This Value</i> 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.

4 Click **OK** to return to the *Advanced Token Initialization Settings* window.

Configuring Common Criteria Settings

When the selected certification type is **Common Criteria**, set the certificate import PIN and the maximum number of certificates for which to reserve space on the token.

NOTE

This section is relevant only to tokens that are Common Criteria supported.

To define the Common Criteria settings:

- 1 Open the *Advanced Settings* window.
See *Configuring Advanced Initialization Settings* on page 87.
- 2 In the *Certification* field, select **Common Criteria**.
- 3 Click **Common Criteria Settings**.
The *Common Criteria Settings* window opens.

4 Complete the fields as follows:

Field	Description
Import PIN, Confirm PIN	Define and confirm a PIN that must be entered when a Common Criteria certificate is imported to the token. The minimum PIN length is 4 characters. The default value is 1234567890 .
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.

- 5 Click **OK** to return to the *Configuring Advanced Initialization Settings* window.

5

SafeNet eToken Virtual

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

TIP

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

In this chapter:

- Overview of SafeNet eToken Virtual Products
- Connecting a SafeNet eToken Virtual
- Disconnecting or Deleting a SafeNet eToken Virtual Product
- Using a SafeNet eToken Virtual to Replace a Lost Token
- Unlocking a SafeNet eToken Virtual
- Using a SafeNet eToken Virtual on an External Storage Device

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.
- **SafeNet eToken Virtual:** performs all the functions of an eToken NG-OTP.
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 104.

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 22.

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.

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 104.

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.

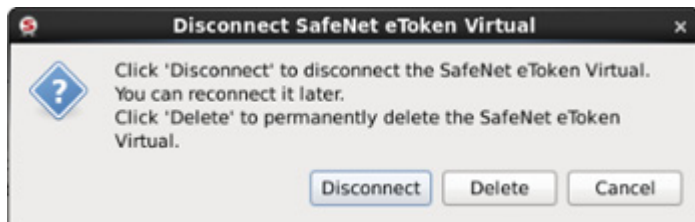
To disconnect or delete a SafeNet eToken Virtual product:

- 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 17.
 - 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 3.
- 2 To use the Advanced View to disconnect, do the following:

- a Open SafeNet Authentication Client Tools *Advanced View*. See Opening the Advanced View on page 22.
- 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 3.
 - 3 The *Disconnect SafeNet eToken Virtual* window opens.



4 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 98.
- ◆ 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 will become locked. To unlock the token, See Unlocking a Token by the Challenge-Response Method on page 55, or See Unlocking a Token by an Administrator on page 76.

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.

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 will need to connect the SafeNet eToken Virtual manually. See [Connecting a SafeNet eToken Virtual](#) on page 98.

Before removing the storage device, you will need to disconnect the SafeNet eToken Virtual manually. See [Disconnecting or Deleting a SafeNet eToken Virtual Product](#) on page 99. Otherwise, the SafeNet eToken Virtual will be displayed in SafeNet Authentication Client as a token with corrupted data. See [Token Icons](#) on page 19.

6

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 7 Token Settings.

In this chapter:

- Setting Password Quality
- Allowing Password Quality Configuration on Token after Initialization
- Allowing Only an Administrator to Configure Password Quality on Token
- Enabling Logging

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 numbers 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 22.
- 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 Client Settings password quality settings are configured the same way as the Token Password quality settings. See [Setting Token Password Quality](#) on page 115

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

NOTE

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

Allowing Password Quality Configuration on Token after Initialization

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

To enable password quality configuration after initialization:

- 1 Open SafeNet Authentication Client Tools *Advanced View*.
See Opening the Advanced View on page 22.
- 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 may 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 22.
- 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**.

Enabling Logging

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

NOTES

- ◆ You must have administrator privileges to use the logging feature.
- ◆ The Enable Logging feature is activated only if the eToken.conf file is configured with write privileges.

The log files are located in: `/Temp/eToken.log`

To activate the logging feature manually:

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

```
[LOG]
Enabled=1
```

To disable the logging feature manually:

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

```
[LOG]
Enabled=0
```

To activate the logging feature:

- 1 Open SafeNet Authentication Client Tools *Advanced View*.
See Opening the Advanced View on page 22.
- 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:

- 1 Open SafeNet Authentication Client Tools *Advanced View*.
See Opening the Advanced View on page 22.
- 2 In the left pane, select **Client Settings**.
- 3 In the right pane, select the **Advanced** tab, and click **Disable Logging**.



Token Settings

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

For configurations set in *Client Settings*, that apply the settings to all tokens that are initialized after the settings have been configured, see Chapter 6 Client Settings.

In this chapter:

- Setting Token Password Quality
- Setting Private Data Caching Mode

Setting Token Password Quality

If a token is initialized after Token Password quality parameters are set for the token, all future Token Password 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.

To set password quality for a token:

- 1 Open SafeNet Authentication Client Tools *Advanced View*.
See Opening the Advanced View on page 22.
- 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.
- 4 The *Password Quality* tab opens.



5 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)	<p>The maximum period, in days, before which the password must be changed.</p> <p>Default: 0 (none)</p> <p>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.</p>
Minimum usage period (days)	<p>The minimum period before the password can be changed.</p> <p>Default: 0 (none)</p> <p>For iKey devices, the periods are rounded up to periods of weeks. See row above for more information.</p>
Expiration warning period (days)	<p>Defines the number of days before the password expires that a warning message is shown.</p> <p>Default: 0 (none)</p>
History size	<p>Defines how many previous passwords must not be repeated.</p> <p>Default:</p> <p>For eToken devices - 10</p> <p>For iKey devices - 6</p>

Password Quality Parameter	Description (Cont.)
Maximum consecutive repetitions	<p>The maximum number of repeated characters that is permitted in the password.</p> <p>Default: 3</p> <p>This feature is not supported by iKey devices.</p>
Must meet complexity requirements	<p>Determines the complexity requirements that are required in the Token Password.</p> <ul style="list-style-type: none"> ◆ 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 <i>Manual Complexity</i> settings, are enforced.
Manual complexity rules	<p>For each of the character types (Numerals, Upper-case letters, Lower-case letters, and Special characters) select one of the following options:</p> <ul style="list-style-type: none"> ◆ 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. <p>Note: The Forbidden option is not supported by iKey devices.</p>

6 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

In SafeNet Authentication Client, public information stored on the token is cached to enhance performance. This option 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 22.
- 2 In the left pane, expand the node of the required token, and select **Settings**.
- 3 In the right pane, select the **Advanced** tab.
The *Advanced* tab opens.



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

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

- 5 Do one of the following:

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

8

Licensing

Import a SafeNet license for your SafeNet Authentication Client installation.

In this chapter:

- Viewing and Importing Licenses

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.

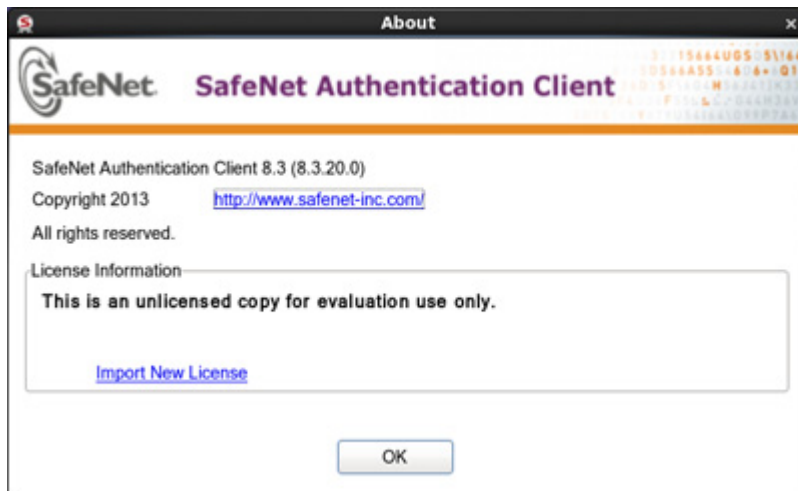
You can view your licenses and import new ones using the SafeNet Authentication Client *About* window.

To view and import licenses:

- 1 Do one of the following:
 - ◆ 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 22. On the toolbar, click the **About** icon.



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



- 2 To import a new license, 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.