



eToken PKI Client (Linux)

User's Guide

Version 5.0 Revision B



All attempts have been made to make the information in this document complete and accurate. Aladdin is not responsible for any direct or indirect damages or loss of business resulting from inaccuracies or omissions. The specifications in this document are subject to change without notice.

Date of publication: July 2009

Last update: Sunday July 12 2009

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

We recommend reading the following Aladdin eToken publication:

- eToken PKI Client (Linux) 5.0 Revision B Administrator's Guide
- eToken PKI Client (Linux) 5.0 ReadMe
- eToken PKI Client (Linux) 5.0 SP1 ReadMe

Table of Contents

1. Introduction.....	1
Overview	2
New Features	3
2. eToken PKI Client User Interface	5
Overview of eToken PKI Client User Interface	6
eToken PKI Client Tray Icon	6
Launching the eToken PKI Client Tray Menu	6
eToken PKI Client Tray Icon Functions.....	7
Hiding and Unhiding the eToken PKI Client Properties Tray Icon	7
eToken PKI Client Properties Main Screen.....	8
eToken PKI Client Properties Main Screen Toolbar	8
Simple View.....	10
Advanced View.....	13
3. eToken Initialization	23
Overview of eToken Initialization	24
Initializing an eToken	24
Configuring Advanced Initialization Settings.....	26
Changing the eToken Initialization Key.....	30
4. eToken Management.....	33
Selecting the Active eToken	34
Changing the eToken Password	34
Unlocking an eToken	37
Unlocking an eToken Using Set User Password	38
Unlocking an eToken using Challenge - Response.....	39
Clearing an eToken.....	41
Viewing eToken Information	42
Copying eToken Information to the Clipboard.....	42
Renaming an eToken	43
Logging On to an eToken	44

Importing a Certificate onto an eToken.....	45
Exporting a Certificate from an eToken	48
Deleting a Certificate.....	49
Changing an eToken Password.....	50
Managing Readers.....	52
5. eToken Virtual	55
Overview of eToken Virtual and eToken Rescue.....	56
Connecting an eToken Virtual or eToken Rescue	56
Disconnecting or Deleting an eToken Virtual or eToken Rescue	57
Using an eToken Virtual/eToken Rescue to Replace a Lost eToken	58
Unlocking an eToken Virtual	59
Generating a One Time Password (OTP)	59
6. eToken Settings	61
Setting eToken Password Quality	62
Setting Private Data Caching Mode	65
Setting RSA Key Second Authentication Mode	67
7. PKI Client Settings.....	71
Opening PKI Client Settings	72
Setting PKI Client Settings Password Quality	73
Enabling CA Certificate Management	73
Enabling Configuration after Initialization	74
Enabling Configuration by Administrator or User	74
A. Copyrights and Trademarks	77
B. FCC Compliance.....	79
FCC Warning	79
CE Compliance	80
UL Certification.....	80
C. Aladdin eToken Patent Protection	81

Introduction

eToken PKI Client enables eToken operations and the implementation of eToken PKI-based solutions.

Note:

This document refers to eToken PKI Client 5.0 and eToken PKI Client 5.0 SP1.

eToken PKI Client 5.0 SP1 supports only Ubuntu 8.04 and 9.04.

In this chapter:

- Overview
- New Features

Overview

Public Key Infrastructure (PKI) is a framework for creating a secure method for exchanging information based on public key cryptography, providing for trusted third-party vetting of, and vouching for, user identities. It is an arrangement that consists of 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.

Aladdin's eToken PKI Client enables integration with various security applications. It enables eToken security applications and third party applications to communicate with the eToken device so that it can work with various security solutions and applications. These include eToken PKI solutions using PKCS#11 or proprietary eToken applications.

eToken PKI Client enables the implementation of strong two-factor authentication using standard certificates as well as encryption and digital signing of data. Generic integration with PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications offering secure web access, PC and data security, secure email, and more. PKI keys and certificates can be created, stored, and used securely from within eToken hardware or software devices.

eToken PKI Client can be deployed and updated using any standard software distribution system.

The eToken PKI Client Properties application and the eToken PKI Client Monitor process are installed with eToken PKI Client, providing easy-to-use configuration tools for users and administrators.

New Features

The following features were introduced in eToken PKI Client (Linux) 5.0:

- Improved usability and customization options for the eToken PKI Client user interface
- Improved user interface
- Support for administrator and non-administrator privilege levels for screen access and actions performed in the eToken PKI Client user interface
- Simplified supportability by providing option logging as part of the standard shipping release
- Support for the *Clear* function in addition to the *Initialize* option (**Warning:** This feature deletes all eToken content including certificates, RSA Keys and other data)
- A logon retry counter is displayed in the eToken logon window on logon failure
- Enhanced password complexity support - manual password complexity settings and character repeat count
- Support for 64-bit Red Hat Enterprise and CentOS operating systems
- Support for 2048 RSA keys, including Java Cards using Applet 1.1 or later
- Support for the new eToken Virtual
- Support for eToken Pro Anywhere (in PKI mode only)

The following features were introduced in eToken PKI Client (Linux) 5.0 SP1:

- Support for Ubuntu 9.04 (32-bit)
- Support for SSH Agent



Chapter 2

eToken PKI Client User Interface

This section describes how to find your way around the the eToken PKI Client user interface.

eToken PKI Client provides two user interfaces: eToken PKI Client Properties and the eToken PKI Client tray icon.

In this chapter:

- Overview of eToken PKI Client User Interface
- eToken PKI Client Tray Icon
- eToken PKI Client Properties Main Screen

Overview of eToken PKI Client User Interface

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

eToken PKI Client Properties 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 remove the eToken from the USB port during an operation. This may cause corruption of data on the eToken.


eToken PKI Client Properties 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.

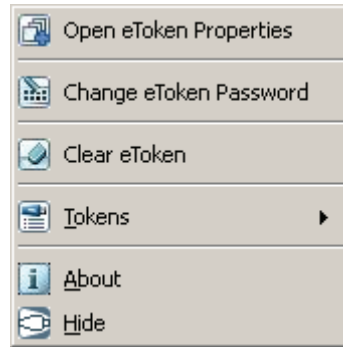
eToken PKI Client Tray Icon

The eToken PKI Client Tray Icon gives you quick access to many of the functions in the application.

Launching the eToken PKI Client Tray Menu

To access the eToken PKI Client tray menu:

- Right-click the eToken PKI Client icon . The eToken PKI Client tray menu opens.



eToken PKI Client Tray Icon Functions

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

- **Open eToken Properties:** launches eToken PKI Client Properties. eToken PKI Client Properties can also be launched by double-clicking the eToken PKI Client Tray Icon.
- **Generate OTP:** generates OTP for eToken Virtual. This function is available only if the eToken Virtual is configured to support this function.
- **Change eToken Password**
- **Clear eToken:** removes the deletable data from the token
- **Tokens:** selects the active eToken when more than one is inserted
- **About:** displays product information
- **Hide:** hides the icon

Hiding and Unhiding the eToken PKI Client Properties Tray Icon

To hide the eToken PKI Client Properties Tray Icon:

- Select **Hide**.

To unhide the eToken PKI Client Properties Tray Menu:

Do one of the following

- Remove and re-insert the token
- Re-boot the computer

eToken PKI Client Properties Main Screen

eToken PKI Client Properties includes two viewing options:

- **Simple view:** to perform basic and common tasks.
See on page 10.
- **Advanced view:** for complete control over the PKI Client and the inserted tokens.
See *Advanced View* on page 13.


Each view displays two panes:






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

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

eToken PKI Client Properties Main Screen Toolbar

The main screen toolbar is displayed in both simple and advanced view. The toolbar contains the following icons:

Icon	Action
	Advanced – switches from the simple to the advanced view

Icon (Continued)	Action (Continued)
	Simple - switches from the advanced to the simple view
	Refresh – refreshes the data for all connected tokens
	About – displays product version information
	Help – launches the help
	eToken Home Page - opens the eToken website

Simple View

When eToken PKI Client Properties is launched, the *eToken PKI Client Properties* window opens in the simple view.



When an eToken is inserted or an eToken Virtual is present, a device specific icon representing the inserted token is displayed in the left pane.






Each token has a name displayed to the right of the icon. *eToken* is the default name if no name has been assigned to the token.

The selected eToken is marked by a shaded rectangle in the left pane.

eToken Device Icons

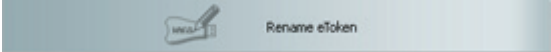
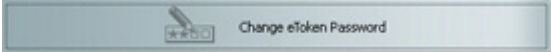
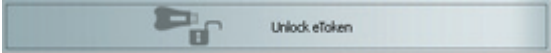
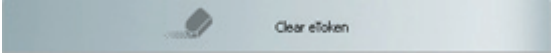


The icon indicates the type of device that is attached.

Icon	Type
	eToken PRO
	eToken Virtual
	eToken Rescue
	eToken NG-OTP

Icon (Continued)	Type (Continued)
	eToken NG-FLASH
	Smart Card Reader – with no card
	Smart Card Reader – with card
	eToken or eToken Virtual with corrupted data
	Unknown token


Simple View Functions

In the right pane, you can select any of the enabled buttons to perform the action described.:

Function	Button
Rename eToken - sets the eToken name	 A button with a pencil icon and the text "Rename eToken".
Change Password – changes the eToken user password	 A button with a key icon and the text "Change eToken Password".
Unlock eToken – resets the user password via a challenge response mechanism .Enabled only when an administrator password has been initialized on the eToken	 A button with a key icon and the text "Unlock eToken".
Clear eToken - removes deletable data from the eToken	 A button with a trash can icon and the text "Clear eToken".
View eToken Info – provides detailed information about the token	 A button with an information icon (i) and the text "View eToken Info".
Disconnect eToken Virtual – disconnects the eToken Virtual or eToken Rescue, with an option for deleting it	 A button with a disconnect icon (two people with a crossed-out line) and the text "Disconnect eToken Virtual".

Advanced View

The eToken PKI Properties Advanced view provides additional token management functions.

To see the advanced view, click the **Advanced** icon  in the Simple view.

The *eToken PKI Client Properties* 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 inserted tokens.

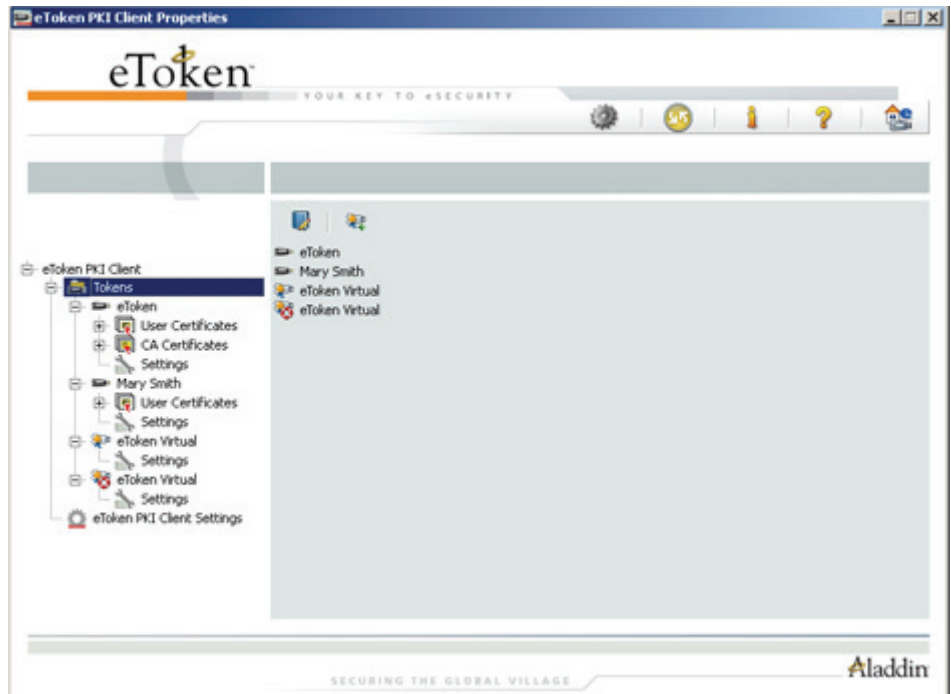
When you select an object, the relevant functions are available by clicking on the icons in the right pane, or by right clicking on the object and selecting the required function from the menu.

Advanced View Functions



You can access the advanced functions by selecting the required object from the left pane in the eToken PKI Client Properties Advanced View window.

Tokens Node

When you select the Tokens node, the list of attached eTokens is displayed in the right pane.

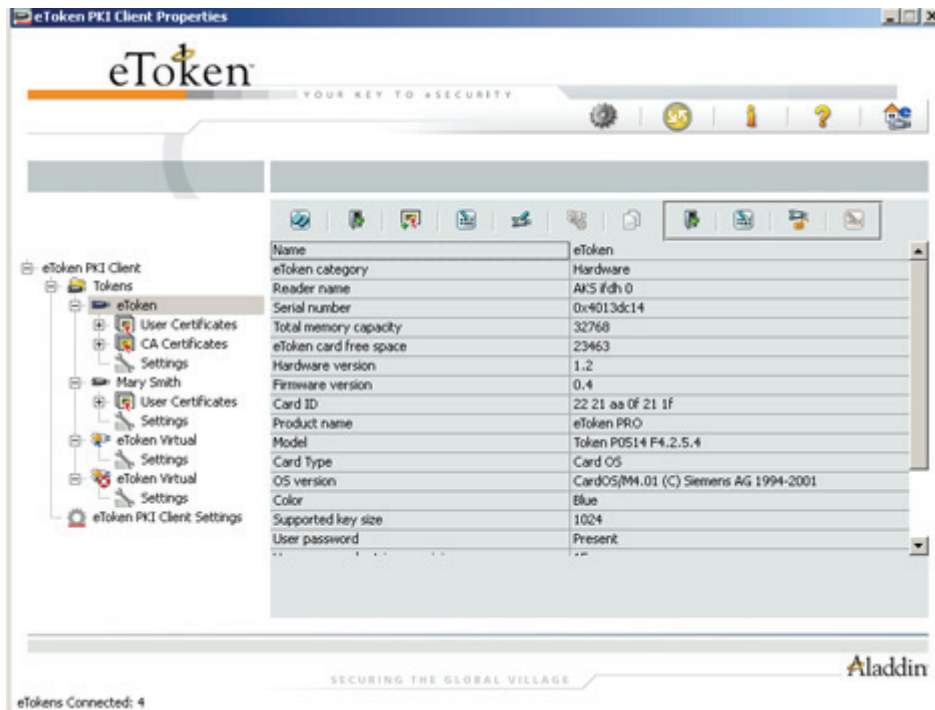


The following functions are available

Function	Icon	Right-Click Menu Item
Manage Readers See <i>Managing Readers</i> on page 52		Manage Readers
Add an eToken Virtual See <i>Connecting an eToken Virtual</i> or <i>eToken Rescue</i> on page 56		Add eToken Virtual

Attached eTokens

The names of the eToken devices are displayed in the left pane. When you select an eToken, information about the eToken is displayed in the right pane. When you select an eToken, the name of the eToken reader is displayed in the tool-tip.







The following user functions are available

User Function	Icon	Right-Click Menu Item
Initialize eToken See <i>eToken Initialization</i> on page 23		Initialize
User Logon to eToken See <i>Logging On to an eToken as a User</i> on page 44		Log on
Import Certificate See <i>Importing a Certificate onto an eToken</i> on page 45		Import Certificate
Change Password See <i>Changing an eToken Password</i> on page 50		Change Password
Rename eToken See <i>Renaming an eToken</i> on page 43		Rename
Disconnect eToken Virtual (eToken Virtual or eToken Rescue only) See <i>Disconnecting or Deleting an eToken Virtual or eToken Rescue</i> on page 57		Disconnect
Copy to Clipboard See <i>Copying eToken Information to the Clipboard</i> on page 42		Not available

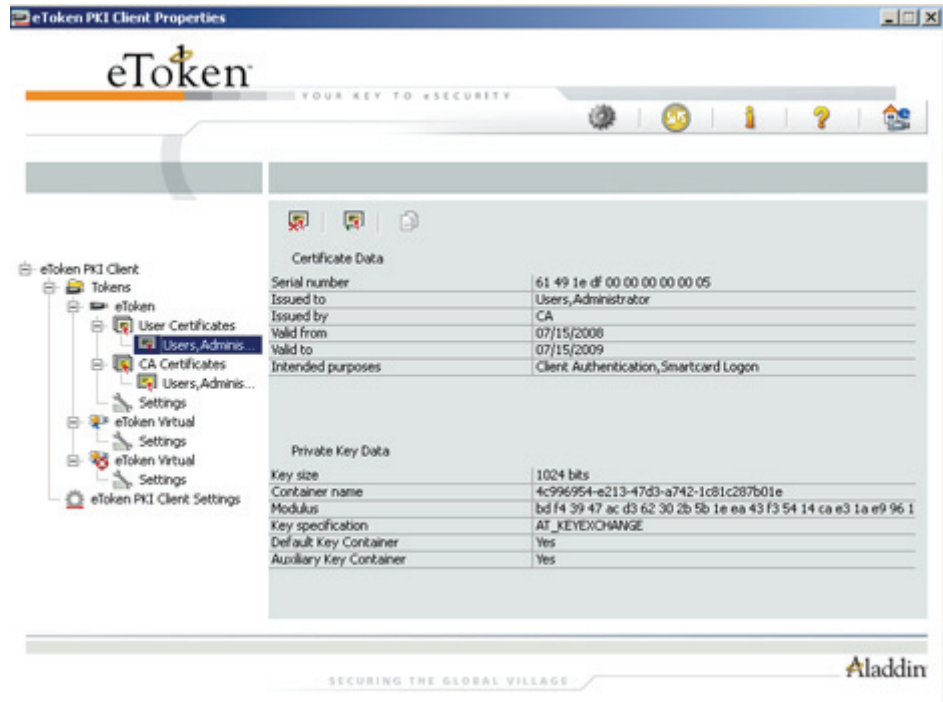
Some functions are available only if an administrator password has been set for the eToken. The administrator icons are located on the right of the window, enclosed within a border:






Administrator Function	Icon	Right-Click Menu Item
Administrator Logon to eToken See <i>Logging On to an eToken as an Administrator</i> on page 45		Administrator Logon
Change Administrator Password See <i>Changing an eToken Password</i> on page 50		Change Administrator Password
Unlock eToken See <i>Unlocking an eToken using Challenge - Response</i> on page 39		Unlock
Set User Password (Is activated only when you have logged on to the eToken with an administrator password) See <i>Unlocking an eToken Using Set User Password</i> on page 38		Set User Password

User Certificates

If the eToken contains certificates, a *User Certificates* node is displayed in the left pane under the eToken. Information about the certificates on the eToken is displayed in the right pane.

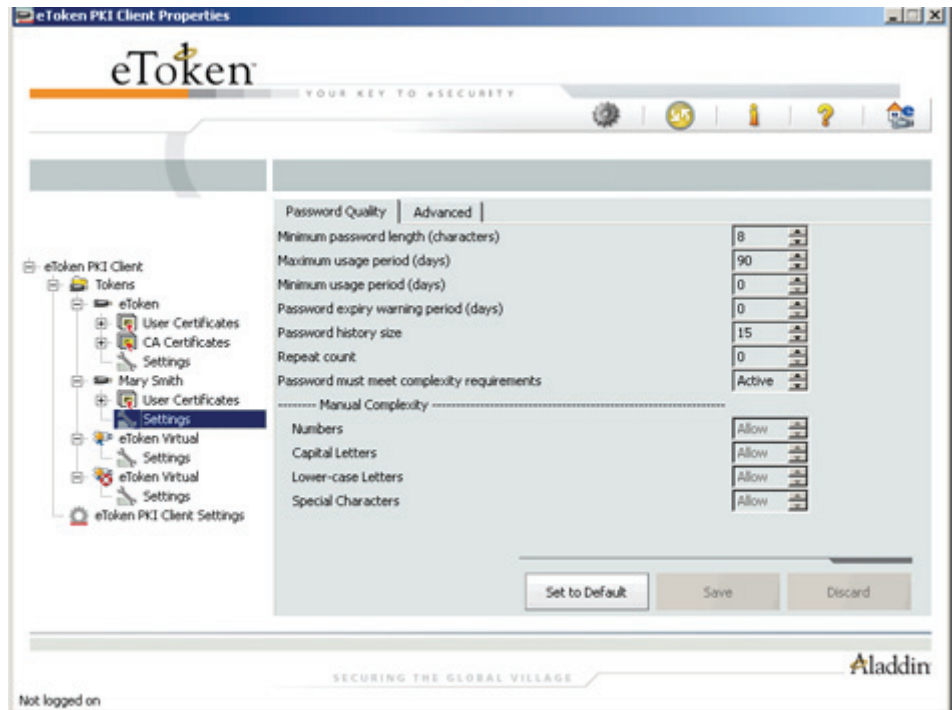


The following functions are available:

User Function	Icon	Right-Click Menu Item
Import Certificate See <i>Importing a Certificate onto an eToken</i> on page 45		Import Certificate
Export Certificate See <i>Exporting a Certificate from an eToken</i> on page 48		Export Certificate
Delete Certificate See <i>Deleting a Certificate</i> on page 49		Delete Certificate

Settings

Each attached eToken has a *Settings* window.



The settings window contains two tabs:

- Password Quality (See *Setting eToken Password Quality* on page 62)
- Advanced (See *Setting Private Data Caching Mode* on page 65 and *Setting RSA Key Second Authentication Mode* on page 67)

PKI Client Settings

The PKI Client Settings will affect all eTokens that will be initialized after the settings have been configured.

The *PKI Client Settings* window contains two tabs, as in the *Settings* window:

- Password Quality
- Advanced

See *PKI Client Settings* on page 71



Chapter 3

eToken Initialization

eToken initialization restores an eToken to its initial state, removing all objects stored on the eToken since manufacture, frees up memory, and resets the eToken password.

Typically, initialization is carried out on an eToken when an employee leaves the company, enabling the eToken to be issued to another employee.

Note:

You cannot initialize an eToken Virtual with eToken PKI Client

In this chapter:

- Overview of eToken Initialization
- Initializing an eToken

Overview of eToken Initialization

The eToken initialization option restores an eToken to its initial state. It removes all objects stored on the eToken since manufacture, frees up memory, and resets the eToken password, allowing administrators to initialize the eToken according to specific organizational requirements or security modes.

Initializing an eToken is useful, for example, after an employee has left a company. It completely removes the employee's individual certificates and other personal data from the eToken, preparing it to be used by another employee.

The following data is initialized:

- eToken name
- User password
- Administrator password (optional)
- Maximum number of logon failures allowed (for user and administrator passwords)
- Requirement to change the password on the first logon
- Initialization key

The initialization process loads the Aladdin eToken file system on the eToken.

Using customizable parameters, you can select specific parameters that will apply to certain tokens. These parameters may be necessary if you wish to use the eToken for specific applications or if you require a specific user or administrator password on all the tokens in the organization.

Initializing an eToken

To initialize an eToken:

1. Click **Initialize eToken** on the toolbar, or right-click the token name in the left pane and select **Initialize** from the shortcut menu. The *Initialize eToken* window opens.

The screenshot shows the 'Initialize eToken' window. The 'eToken Name' field is set to 'eToken'. The 'Create User Password' checkbox is checked, and the password fields are filled with asterisks. The 'Set maximum number of logon failures' is set to 15. The 'Create Administrator Password' checkbox is unchecked. A note at the bottom states: 'Note: Use the administrator password to unlock the token.' Below this is an 'Additional Settings' section with 'Password must be changed on first logon' checked and an 'Advanced' button. At the bottom are 'Start' and 'Close' buttons.

2. Enter a name for the eToken in the *eToken Name* field. If no name is entered, the default name, "eToken", is applied.
3. Select **Create User Password** to initialize the token with an eToken user password. Otherwise, the token is initialized without an eToken password, and it will not be usable for eToken applications.
4. If **Create User Password** is selected, enter a new eToken user password in the *Create User Password* and *Confirm* fields.

Note:

The default password for a new token is 1234567890. If the user uses the default password during initialization, and default password quality requirements are used, the user must select the *Password must be changed at first logon* option. Otherwise the initialization will fail, as the default password will not meet default password quality requirements (See *Setting eToken Password Quality* on page 62). If the *Password must be changed at first logon* field 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 then be required to set a password meeting password quality requirements, as configured in the settings window (See *Setting eToken Password Quality* on page 62).

5. To initialize an administrator password, select **Create Administrator Password** and enter a password in the *Create Administrator Password* and *Confirm* fields. (Minimum password length is 4 characters.)

Note:

Creating an administrator password enables certain functions to be performed on the token, such as resetting a user password on a locked token.

6. In the *Set maximum number of logon failures* 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.
7. If required, select **Password must be changed on first logon**. This is selected by default.
8. If you want to configure advanced settings, continue from the next section (see *Configuring Advanced Initialization Settings* on page 26).
9. Click **Start**.
When the initialization process is complete, a confirmation message is displayed.

Configuring Advanced Initialization Settings

To configure advanced settings:

1. In the *Initialize eToken* window click **Advanced**.

Note:

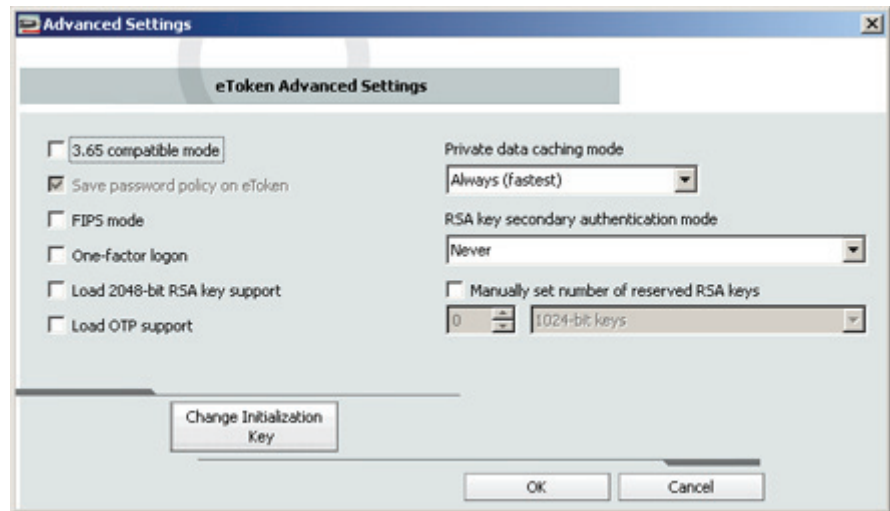
To change the settings on the Advanced tab, you must be logged on as root.

In Ubuntu, you must open eToken PKI Client Properties as root with `sudo` and root passwords:

1. From the terminal, go to `/usr/bin`
2. Run the command `sudo ./eTProps`
3. Type the root password.

eToken PKI Client Properties opens and the settings can be changed.

The *eToken Advanced Settings* window opens.



2. Complete the fields as follows:

Field	Description
3.65 compatible mode	Select to maintain compatibility with eToken RTE 3.65.
Save password policy on eToken	Select to keep password policy on the eToken device. (This is enabled only when the 3.65 compatible mode is selected).
FIPS mode	Select to enable FIPS support. 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. The eToken PRO can be configured in FIPS mode.
One-factor logon	Default: disabled. When one factor logon is enabled, only the presence of the eToken is required to log on to applications. A password is not required. Note: For security reasons, one-factor logon is not applied to eToken PKI Client Properties.
Load 2048-bit RSA key support	Select to enable 2048-bit RSA key support (on compatible token).

Field (Continued)	Description (Continued)
Load OTP	Select to enable OTP support (on compatible token).
Private data caching mode	<p>In PKI Client, public information stored on the eToken is cached to enhance performance. This option defines when private information (excluding private keys on the eToken PRO / NG OTP / Smartcard) can be cached outside the eToken.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none">■ Always (fastest): always caches private information in the application memory. This enables fast performance, as certain information is cached on the host machine. However, this option is less secure than if no cache is allowed.■ While user is logged on: caches private data outside the eToken as long as the user is logged on to the eToken. Once the user logs out, all the private data in the cache is erased.■ Never: does not cache private data.

Field (Continued)	Description (Continued)
RSA key secondary authentication mode	<p>An authentication password may be set for an RSA key. If this option is used, then in addition to having the eToken and knowing the eToken's password, accessing the RSA key requires knowing the password set for that particular key.</p> <p>This option defines the policy for using this secondary authentication of RSA keys.</p> <ul style="list-style-type: none"> ■ Always: every time an RSA key is generated, you are prompted to enter a secondary password for accessing this key. Clicking OK generates the key and uses the entered password as the secondary RSA password for that key. Clicking Cancel causes key generation to fail. ■ Always prompt user: every time an RSA key is generated, a secondary password for accessing this key is requested. However, the user can choose to dismiss the prompt (by clicking Cancel), and key generation will continue without using a secondary password for the generated RSA key. ■ Prompt on application request: this enables applications that use secondary authentication for RSA keys to make use of this feature on the eToken (when creating the key in Crypto API with a user protected flag). ■ Never: secondary passwords are not created for any RSA key and the authentication method uses only the eToken password to access the key.
Manually set number of reserved RSA keys	Set the number of reserved RSA keys to reserve space in the token memory. This ensures that there will always be memory available for the keys.
Change Initialization Key	The initialization key protects against accidental initialization and requires a separate password to be entered before initialization can occur.

3. If you want to change the eToken initialization key continue from the next section (see *Changing the eToken Initialization Key* on page 30), else, click **OK** to return to the *Initialize eToken* window.
4. Click **Start**.

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

Changing the eToken Initialization Key

To change the eToken Initialization Key:

1. In the *eToken Advanced Settings* window, click **Change Initialization Key**.

The *eToken Initialization Key* window opens.



2. Complete the fields as follows:

Field	Description
Use Default Initialization Key	Select to use factory-set default.
Use Specified Initialization Key	Enter the password previously configured in the <i>This Value</i> field below.
Change Initialization Key to:	<ul style="list-style-type: none">■ Default: Revert to default.■ Random: If selected, it will never be possible to re-initialize the token.■ This Value: Select and confirm a password.

3. Click **OK** to return to the *eToken Advanced Settings* window, then click **OK** again to return to the *eToken Initialization Parameters* window.
4. Click **Start**.
When the initialization process is complete, a confirmation message is displayed.



Chapter 4

eToken Management

The eToken PKI Client Properties application and the eToken PKI Client tray menu enable you to configure the options that control the use of eToken devices.

In this chapter:

- Selecting the Active eToken
- Changing the eToken Password
- Unlocking an eToken
- Clearing an eToken
- Viewing eToken Information
- Copying eToken Information to the Clipboard
- Renaming an eToken
- Logging On to an eToken
- Importing a Certificate onto an eToken
- Changing an eToken Password
- Managing Readers


Selecting the Active eToken

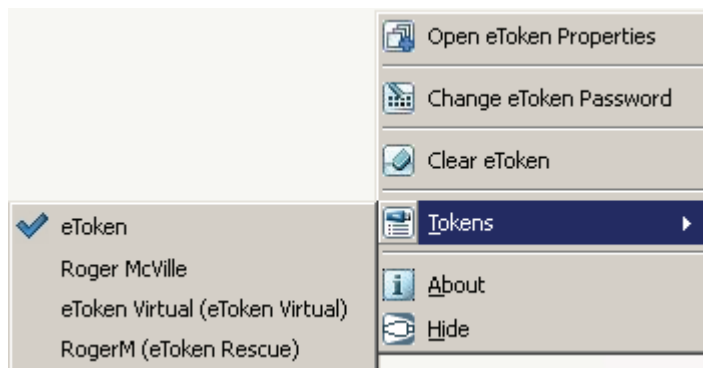
If more than one eToken is attached, you must select which device you want to work with.

Note:

The eToken selected here is relevant only for tray menu functions.

To select the active eToken:

1. Right-click the eToken PKI Client tray icon .
The eToken PKI Client tray menu opens.
2. Select **Tokens**.
A list of inserted eTokens is displayed.



3. Select the required eToken.

Changing the eToken Password

All the manufactured eToken devices are configured with the factory initial password, 1234567890. To ensure strong, two factor security, it is important for the user to change the eToken password to a private user password as soon as the new eToken is received.

When an eToken password has been changed, the new password is used for all eToken applications involving the token. It is the user's responsibility to remember the eToken password. Without it, the user cannot use the token.


Setting an administrator password on the token enables the administrator to unlock a locked token by resetting a new user password if it is forgotten. We recommend initializing all tokens with an administrator password.

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

Note:

The eToken user 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 created 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 eToken Password:

1. To open eToken PKI Client Properties, right-click the eToken tray icon  and select **Open eToken Properties** from the menu. The *eToken PKI Client Properties* window opens.
2. In the left pane of the eToken PKI Client Properties window, select the token to which the new password will be assigned.
3. Click **Change Password** in the right pane.

Tip:

You can change the eToken Password also by right-clicking on the eToken PKI Client Properties tray icon and selecting **Change eToken Password**.

The *Change Password* window is displayed.

4. Enter the current eToken password in the *Current eToken Password* field.
5. Enter the new eToken password in the *New eToken Password* and *Confirm* 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 policy.

6. Click **OK**.
The eToken password is changed.

Unlocking an eToken

If you enter an incorrect password more than a specified number of times, the eToken hardware device, eToken Virtual or eToken Rescue will be locked.

You can unlock the eToken only if an administrator password was set during initialization.

The unlock feature is available for eToken hardware devices, eToken Virtual and eToken Rescue.

CAUTION:

The number of times that an eToken or eToken Virtual can be unlocked can be limited to a specified number. If this number is exceeded, the eToken or eToken Virtual becomes unusable. The eToken must be initialized and the eToken Virtual must be replaced. This feature is not available for eToken Rescue.

If the administrator has access to the user's computer, the token may be unlocked using the *Set User Password* feature (see *Unlocking an eToken Using Set User Password* on page 38).

When the administrator is located remotely, for example when an employee is out of the office, a Challenge – Response authentication method can be employed to unlock the token (see *Unlocking an eToken using Challenge - Response* on page 39). With this method, the user sends the administrator the Challenge Data supplied by eToken PKI Client Properties, and then enters the Response Data provided by the administrator. The user then enters a new password and the token is unlocked.

Unlocking an eToken Using Set User Password

To unlock a token using **Set User Password**:

1. Log on to the eToken as an administrator (see *Logging On to an eToken as an Administrator* on page 45).
2. Do one of the following:
 - ♦ Click the **Set User Password** icon:



- ♦ Right-click the eToken in the left pane and select **Set User Password** from the shortcut menu.

The *Set eToken Password* window opens.



3. Enter a new password in the *New Password* and *Confirm Password* fields.

Note:

The new password must meet password quality settings as defined for the eToken.

4. Set the *Set maximum number of logon failures* to the required number.
5. Click **OK**.

The eToken is unlocked.

You can now log on as a user with the new password.

Unlocking an eToken using Challenge - Response

To unlock a token using Challenge – Response:

1. To open eToken PKI Client Properties, right-click the eToken tray icon  and select **Open eToken Properties** from the menu. The *eToken PKI Client Properties* window opens.



2. In the left pane of the *eToken PKI Client Properties* window, select the eToken to be unlocked.
3. Click **Unlock eToken** in the right pane. The *Unlock eToken* window is displayed.



4. Contact the administrator and provide the Challenge Data.

Note:

To copy the challenge data to the clipboard, click on the **Copy challenge data to clipboard** icon:



CAUTION:

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

The administrator provides the Response Data to be entered.

Note:

The creation of response data depends on the backend application being used by the organization. System administrators should refer to the relevant documentation for details on how to generate the response data.

5. Enter a new token password in the **Password** and **Confirm** fields.
6. Select **Change password on first logon** if the new password is known to others and must be changed.

7. Click **OK**.

The token is unlocked and a confirmation message is displayed.


Clearing an eToken

The *Clear* function enables you to delete all deletable objects on your token. Objects types include data objects (profiles), keys and certificates (CA or user).

Non-deletable objects will not be removed. Non-deletable objects are created when the administrator configures the object attributes.

The *Clear* function leaves the data structure your eToken intact. It is less wide-reaching than the *Initialize* function which restores an eToken to its initial state, removing all objects stored on the eToken since manufacture and resets the eToken password (See Chapter 3 eToken Initialization on page 23).

To Clear an eToken:

1. Right-click the eToken tray icon  and select **Clear eToken** from the menu.

The *Clear eToken* window opens, prompting you to confirm the clear action.

2. To continue with the clear process, click **OK**, else click **Cancel**.

The *Log On* window opens.


3. Enter the eToken password and click **OK**.

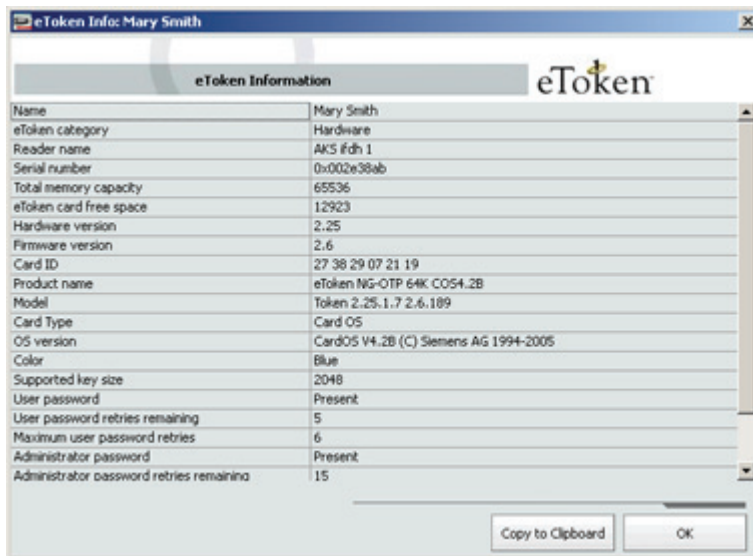
The *Clear eToken* window opens, confirming that the clear process has been successful.

4. Click **OK** to finish.

Viewing eToken Information

To view eToken information:

1. To open eToken PKI Client Properties, right-click the eToken tray icon  and select **Open eToken Properties** from the menu. The *eToken PKI Client Properties* window opens.
2. In the left pane of the *eToken PKI Client Properties* window, select the required eToken.
3. Click **View eToken Info** in the right pane. The eToken Information window opens.



Copying eToken Information to the Clipboard

To copy and paste eToken information:

1. Do one of the following
 - ◆ In the *View eToken Information* window click **Copy to Clipboard**.

- ◆ In Advanced view, select the required eToken in the left pane and click the Copy to Clipboard icon:




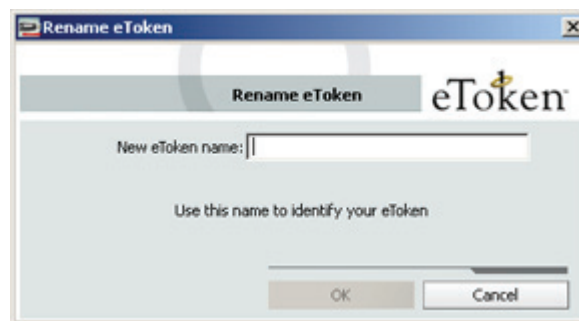
2. Place the cursor in the target application and paste the information.

Renaming an eToken

You can change the eToken name.

To rename a token:

1. To open eToken PKI Client Properties, right-click the eToken tray icon  and select **Open eToken Properties** from the menu. The *eToken PKI Client Properties* window opens.
2. In the left pane of the *eToken PKI Client Properties* window, select the token to be renamed.
3. Click **Rename eToken** in the right pane.
4. If prompted, enter the eToken password. The *Rename eToken* window opens.



5. Enter the new name in the *New eToken* name field.
6. Click **OK**.
The new token name is displayed in the *eToken PKI Client Properties* window.


Logging On to an eToken

You can log on to an eToken as a user or as an administrator.

An administrator has limited permissions on a token. No changes to any user information may be made, nor may the user's security be affected. The administrator's functions are restricted to *Change Administrator Password*, *Set User Password*, *Unlocking eToken using Challenge-Response* and *Change Password Quality Settings* that are stored on the token.

Logging On to an eToken as a User

To log on as a user:

1. To open eToken PKI Client Properties, right-click the eToken tray icon  and select **Open eToken Properties** from the menu. The *eToken PKI Client Properties* window opens.

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



The *Advanced View* window opens.

3. Do one of the following:
 - ◆ Select the required eToken in the left pane and click the **Log On to eToken** icon:



- ◆ Right-click the required eToken in the left pane and select **Log On** from the shortcut menu.


The *Log On* window opens.

4. Enter the eToken user password in the *Password* field and click **OK**.

The user is logged on.

Logging On to an eToken as an Administrator

To log on as an administrator:

1. To open eToken PKI Client Properties, right-click the eToken tray icon  and select **Open eToken Properties** from the menu. The *eToken PKI Client Properties* window opens.

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



The *Advanced View* window opens.

3. Do one of the following:
 - ◆ Select the required eToken in the left pane and click the **Log On As Administrator** icon:



- ◆ Right-click the required eToken in the left pane and select **Log On As Administrator** from the shortcut menu.

The *Administrator Logon to eToken* dialog box opens.

4. Enter the administrator password in the *Password* field and click **OK**.

The user is logged on as the Administrator.

Importing a Certificate onto an eToken

The following certificate types are supported:

- .pfx
- .p12
- .cer


If a PFX file is selected, the private key and corresponding certificate will be imported to the eToken. You will be asked if CA certificates should be imported to the eToken, and you will be asked to enter the password (if it exists) protecting 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 eToken. 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.

Note:

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

To import a certificate:

1. To open eToken PKI Client Properties, right-click the eToken tray icon  and select **Open eToken Properties** from the menu. The *eToken PKI Client Properties* window opens.

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



The *Advanced View* window opens.

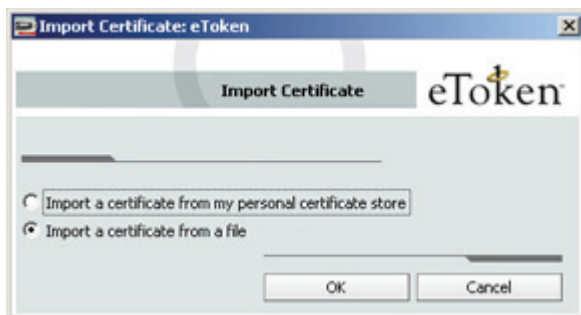
3. In the left pane of the *eToken PKI Client Properties Advanced View* window, select the required eToken.
4. Do one of the following:

- ◆ In the left pane of the Advanced View window, select the required eToken and click the **Import Certificate** icon



- ◆ In the left pane of the Advanced View window, right click the required eToken and select **Import Certificate** from the menu.

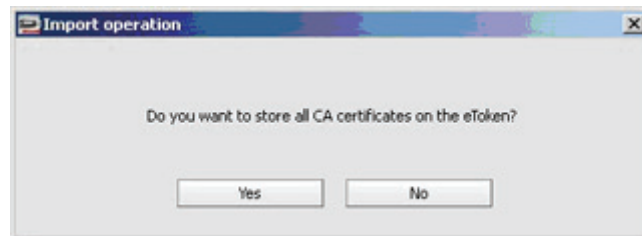
The *Import Certificate* window opens.



5. Select the following
 - ♦ **Import a certificate from a file**
6. Click **OK**.
The *Choose a certificate* dialog box opens.
7. Select the certificate file to import and click **Open**.
If the certificate requires a password, the *Password* dialog box opens.



8. Enter the certificate password.
A window opens asking if you want to store the CA certificates on the eToken.



9. Select **Yes** or **No**.
All requested certificates are imported, and a confirmation message opens.


Exporting a Certificate from an eToken

A physical eToken exports only the certificate, while an eToken Virtual exports the certificate with its key.

Note:

In Linux it is possible to export only to *.cer format.

To export a certificate:

1. To open eToken PKI Client Properties, right-click the eToken tray icon  and select **Open eToken Properties** from the menu. The *eToken PKI Client Properties* window opens.

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

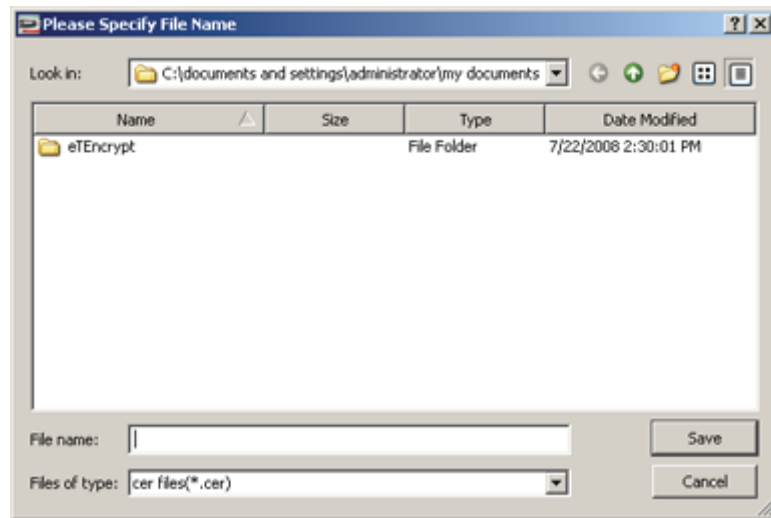


The *Advanced View* window opens.

3. In the left pane of the *eToken PKI Client Properties Advanced View* window, select the required eToken.
4. In the left pane of the Advanced View window, select the required eToken and click the **Export Certificate** icon



The *Please Specify File Name* 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 an eToken.

To delete a certificate from an eToken:

1. To open eToken PKI Client Properties, right-click the eToken tray icon  and select **Open eToken Properties** from the menu. The *eToken PKI Client Properties* window opens.
2. Click the **Advanced View** icon.



The *Advanced View* window opens.

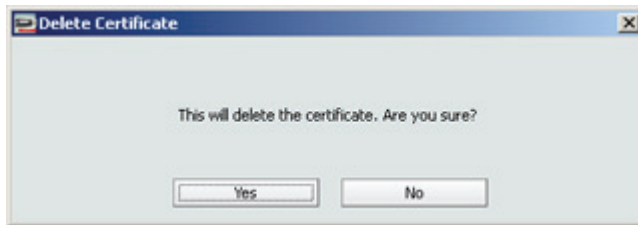
3. Do one of the following:

- ◆ In the left pane of the Advanced View window, expand the required eToken , select the required certificate and click the **Delete Certificate** icon.



- ◆ In the left pane of the Advanced View window, expand the required eToken , right-click the required certificate and select **Delete Certificate** from the shortcut menu.

The *Delete Certificate* window opens.



4. Do one of the following:
 - ◆ To cancel the deletion click **No**
 - ◆ To delete the certificate click **Yes**

Changing an eToken Password

All eToken devices are configured with the factory initial password, 1234567890. To ensure strong, two factor security, it is important for the user to change the eToken password to a private user password as soon as the new eToken is received.

When an eToken password has been changed, the new password is used for all eToken applications involving the token. It is the user's responsibility to remember the eToken password. Without it, the user cannot use the token.

Setting an administrator password on the token enables the administrator to unlock a locked token by resetting a new user password if it is forgotten. We recommend initializing all tokens with an administrator password.




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

See *Setting eToken Password Quality* on page 62.

Note:

The eToken user 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 created 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 eToken Password:

1. To open eToken PKI Client Properties, right-click the eToken tray icon  and select **Open eToken Properties** from the menu.
2. Do one of the following:
 - ♦ In the left pane of the *eToken PKI Client Properties* window, select the required eToken and click the *Change Password* icon: 
 - ♦ In the left pane of the *eToken PKI Client Properties* window, right-click the required eToken and select **Change Password** from the menu.
3. To change the administrator password, do one of the following:
 - ♦ In the left pane of the *eToken PKI Client Properties* window, select the required eToken and click the *Change Administrator Password* icon: 

The *Change Administrator Password* icon is located at the right of the window, enclosed within a border:



- ♦ In the left pane of the *eToken PKI Client Properties* window, right-click the required eToken and select **Change Administrator Password** from the menu.

The *Change Password* window opens.

4. Enter the current eToken password in the *Current eToken Password* field.

Note:

If an incorrect password is entered more than a specified number of times, the eToken will be locked.

5. Enter the new eToken password in the *New eToken Password* and *Confirm* 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 policy.

6. Click **OK**.
The eToken password is changed.


Managing Readers


During the eToken PKI Client installation, four virtual smart card readers and two eToken Virtual readers are installed.

When an eToken is inserted into a USB port, or an eToken Virtual is added, the effect is the same as inserting a smartcard into one of the readers.

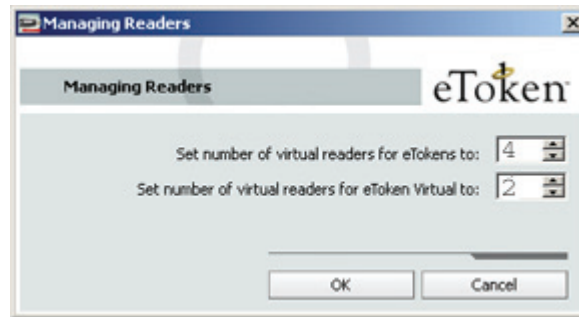
The number of default readers on a computer can be changed by a user with local administrator rights on that computer.

To change the number of readers:

1. To open eToken PKI Client Properties, right-click the eToken tray icon  and select **Open eToken Properties** from the menu.
2. The *eToken PKI Client Properties* window opens.
3. Do one of the following:

- ◆ Click the **Manage Readers** icon .
- ◆ Right-click the *Tokens* node and select **Manage Readers** from the shortcut menu

The *Managing Readers* window opens.



The *Set number of virtual readers for eTokens* field displays the number of available readers for eTokens (the default is 4). This value cannot be changed in the *Managing Readers* window.

In Linux, the smart card service (pcscd) loads the smartcard driver dynamically. The number of virtual readers available for eTokens is determined by the **pcscslots** property value in the **eToken.conf** file. For more details see the *eToken PKI Client (Linux) Administrator's Guide*.

4. In the *Set number of virtual readers for eToken Virtual to* field, enter the required number (the default is 2).
5. Click **OK** to close the window.
The number of available readers has been changed.
6. Restart *eToken PKI Client Properties* to make the changes effective.



Chapter 5

eToken Virtual

eToken PKI Client supports the eToken Virtual line of products. This includes eToken Virtual and eToken Rescue. These are stored as files on your computer or on a mass storage device.

Tip:

To obtain eToken Rescue or eToken Virtual, contact your system administrator.

In this chapter:

- Overview of eToken Virtual and eToken Rescue
- Connecting an eToken Virtual or eToken Rescue
- Disconnecting or Deleting an eToken Virtual or eToken Rescue
- Using an eToken Virtual/eToken Rescue to Replace a Lost eToken
- Unlocking an eToken Virtual
- Generating a One Time Password (OTP)

Overview of eToken Virtual and eToken Rescue




eToken PKI Client supports eToken software tokens. The eToken software tokens are stored as files on the computer.

The following types of eToken software tokens are available:

- **eToken Rescue:** provides a solution when a staff member loses or damages an eToken when away from the office. eToken Rescue is a read-only token. You cannot import certificates. It operates for a limited period of time.
- **eToken Virtual:** performs all the functions of an eToken NG-OTP. It supports OTP generation (if so configured).
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 where it was enrolled.
- **eToken Virtual Temp:** identical to eToken Virtual, but contains certificates which become invalid after a specified time period.

Connecting an eToken Virtual or eToken Rescue

To connect an eToken Virtual or eToken Rescue:

1. To open eToken PKI Client Properties, right-click the eToken tray icon  and select **Open eToken Properties** from the menu. The *eToken PKI Client Properties* window opens.
2. Click the **Advanced View** icon.

The *Advanced View* window opens.
3. Select **Tokens** in the left pane.
4. Click the **Connect eToken Virtual** icon , or right-click **Tokens** and select **Connect eToken Virtual** from the menu. The *Choose eToken Virtual file* window opens.
5. Navigate to the eToken Virtual file, select it and click **Open**. The *eToken Virtual* is added and a confirmation message opens.




6. Click **OK**.

Disconnecting or Deleting an eToken Virtual or eToken Rescue

When the eToken Virtual is no longer necessary, disconnect it from its attached reader.

To disconnect an eToken Virtual or eToken Rescue:

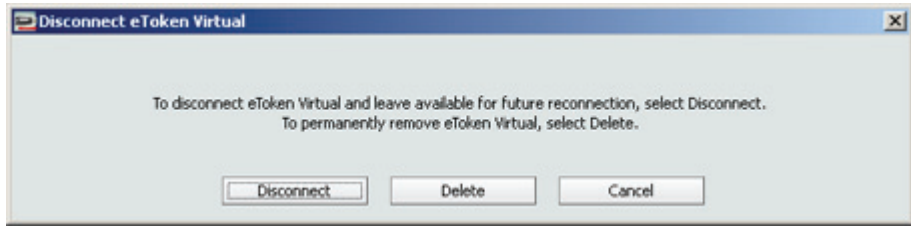
1. To open eToken PKI Client Properties, right-click the eToken tray icon  and select **Open eToken Properties** from the menu. The *eToken PKI Client Properties* window opens.
2. In the left pane of the *eToken Properties* window, select the eToken Virtual or eToken Rescue to be disconnected.
3. In the right pane, click **Disconnect eToken Virtual** (or **Disconnect eToken Rescue**).

Tip:

You can also disconnect an eToken Virtual or eToken Rescue in the Advanced window by clicking the *Disconnect eToken Virtual* icon:



The *Disconnect eToken Virtual* message is displayed.



4. Do one of the following:
- ◆ To keep the eToken Virtual/eToken Rescue file on the computer, click **Disconnect**; only the connection from the eToken Virtual to eToken Properties is disconnected.
 - ◆ To remove the eToken Virtual/eToken Rescue file from the computer, click **Delete**.

Note:

Disconnecting the eToken Virtual/eToken Rescue is applicable when the user is out of the office and may need to use the eToken Virtual/eToken Rescue on the road later.

When the lost eToken is replaced, the eToken Virtual/eToken Rescue should be deleted from the computer.

After the eToken Virtual/eToken Rescue is deleted, it can be recreated only by reinstalling it.

Using an eToken Virtual/eToken Rescue to Replace a Lost eToken

To use an eToken Virtual/eToken Rescue to replace a lost eToken, the eToken Virtual/eToken Rescue must be enrolled using the eToken TMS Client.

For more details, refer to the eToken TMS Client documentation.

Unlocking an eToken Virtual

If you enter an incorrect password more than a specified number of times, the eToken Virtual will be locked. See *Unlocking an eToken using Challenge - Response* on page 39 or *Unlocking an eToken Using Set User Password* on page 38.


Note:

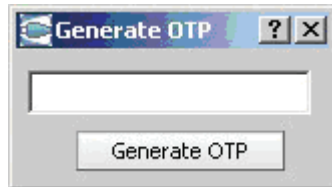
The number of times that an eToken Virtual can be unlocked can be limited to a specified number. If this number is exceeded, the eToken Virtual becomes unusable. This function is not available for eToken Rescue.

Generating a One Time Password (OTP)

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

To generate an OTP:

1. Right-click the eToken PKI Client tray icon .
The eToken PKI Client tray menu opens.
2. Select **Generate OTP**.
The *Generate OTP* window opens.



3. Click **Generate OTP**.
The *Log On to eToken* window opens.
4. Enter the token password.
The generated OTP is displayed in the *Generate OTP* window.



Chapter 6

eToken Settings

Configurations set in eToken Settings determine behavior that applies to the specific eToken.

In this chapter:



- [Setting eToken Password Quality](#)
- [Setting Private Data Caching Mode](#)
- [Setting RSA Key Second Authentication Mode](#)

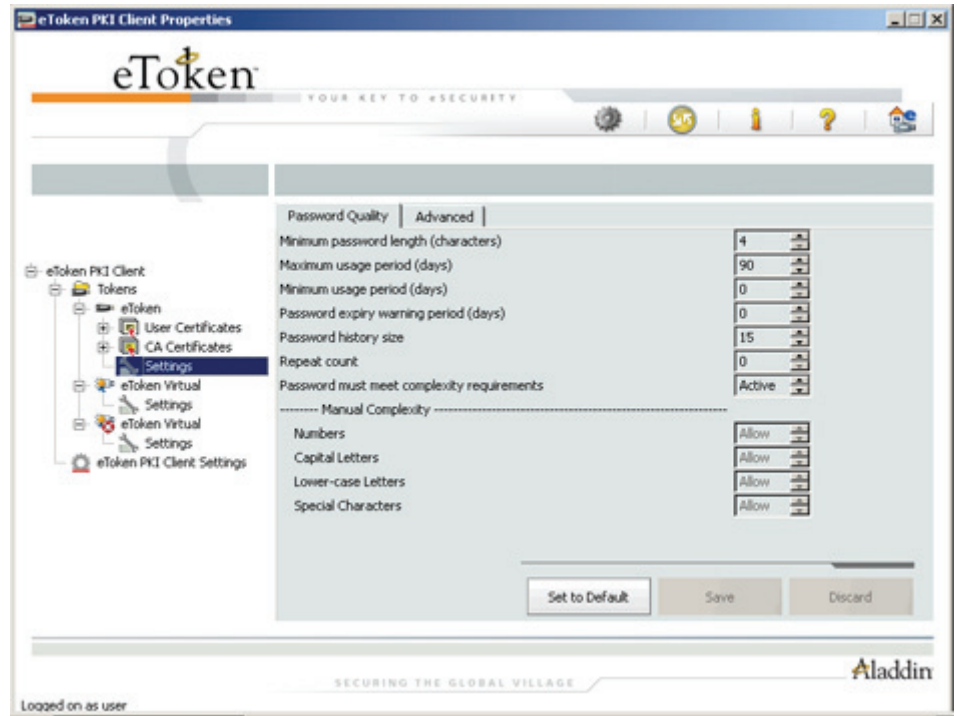
Setting eToken Password Quality

Once password quality parameters are set, any future passwords are automatically checked against these parameters to determine the password's level of acceptability.

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

To set password quality:

1. To open eToken PKI Client Properties, right-click the eToken tray icon  and select **Open eToken Properties** from the menu. The *eToken PKI Client Properties* window opens.
2. Click the **Advanced View** icon.

The *Advanced View* window opens.
3. In the left pane of the *eToken PKI Client Properties Advanced View* window, expand the required eToken and select **Settings**.
4. In the right pane select the **Password Quality** tab.



5. Enter the password quality parameters as follows:

Password Quality Parameter	Description
Minimum password length (characters)	Default: 6 characters
Maximum usage period (days)	The maximum period before which the password must be changed. Default: 0 (none)
Minimum Usage Period (days)	The minimum period before the password can be changed Default: 0 (none)
Password expiry warning period (days)	Defines the number of days before the password expires that a warning message is shown. Default: 0 (none)
Password history size	Defines how many previous passwords should not be repeated. Default: 10

Password Quality Parameter	Description (Continued)
Repeat Count	The number of times that each character can be repeated in the password. Default: 3
Password must meet complexity requirements	Determines if the complexity requirements are required in the eToken password. <ul style="list-style-type: none">■ Active: Complexity requirements are enforced■ None: Complexity requirements are not enforced■ Manual: Complexity requirements, as set manually in the <i>Manual Complexity</i> settings, are enforced (Default)
Manual Complexity	For each of the character types (Capital Letters , Lower-Case Letters , Numbers and Special Characters) select one of the following options: <ul style="list-style-type: none">■ Allow - Can be included in the password, but is not mandatory (Default).■ Must - Must be included in the password.■ Forbid - Must not be included in the password.


6. Do one of the following:

- ◆ To save your changes click **Save**
- ◆ To ignore your changes click **Discard**
- ◆ To return to default settings click **Set to Default**

Setting Private Data Caching Mode

In PKI 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 / Smartcard) can be cached outside the eToken.

To set private data caching mode:

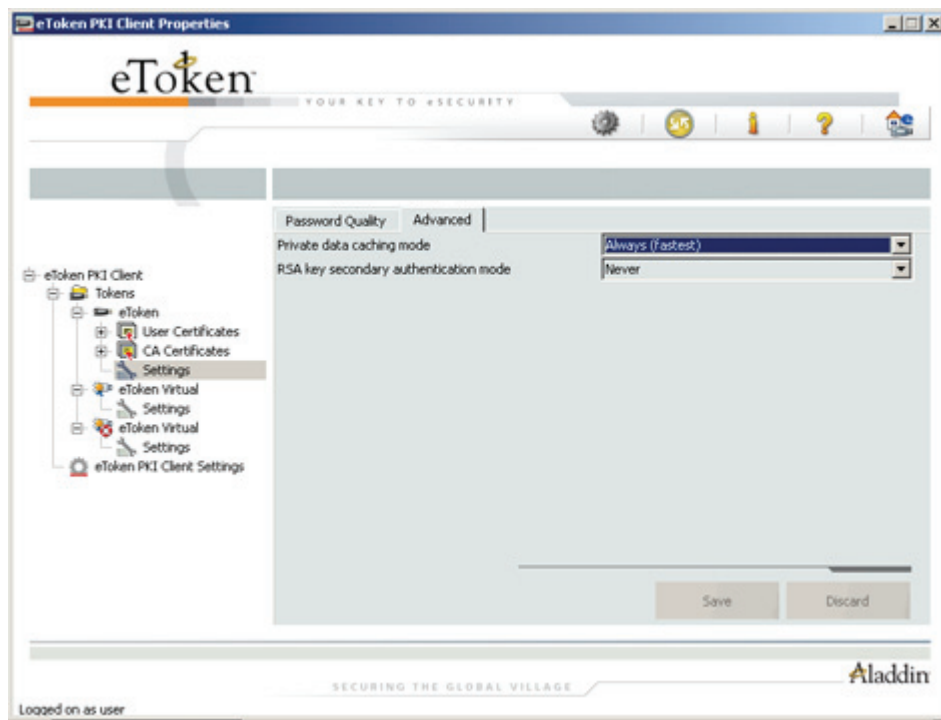
1. To open eToken PKI Client Properties, right-click the eToken tray icon  and select **Open eToken Properties** from the menu. The *eToken PKI Client Properties* window opens.

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



The *Advanced View* window opens.

3. In the left pane of the *eToken PKI Client Properties Advanced View* window, expand the required eToken and select **Settings**.
4. In the right pane select the **Advanced** tab.



5. In the *Private data caching mode* 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 eToken as long as the user is logged on to the eToken. Once the user logs out, all the private data in the cache is erased.
Never	Does not cache private data.

6. Do one of the following:

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

Setting RSA Key Second Authentication Mode

An authentication password may be set for an RSA key. If this option is used, then in addition to having the eToken and knowing the eToken's password, accessing the RSA key requires knowing the password set for that particular key.

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

To set RSA key second authentication mode:

1. To open eToken PKI Client Properties, right-click the eToken tray

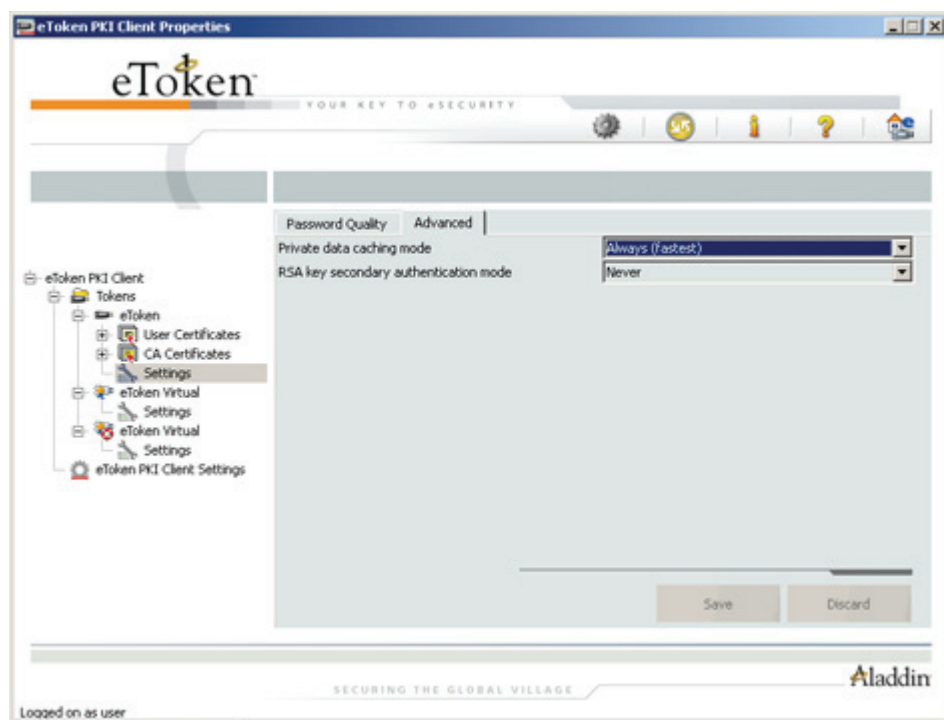
icon  and select **Open eToken Properties** from the menu. The *eToken PKI Client Properties* window opens.

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



The *Advanced View* window opens.

3. In the left pane of the *eToken PKI Client Properties Advanced View* window, expand the required eToken and select **Settings**.
4. In the right pane select the **Advanced** tab.



5. In the *RSA key second authentication mode* field, select one of the following options:

Option	Description
Always	Every time an RSA key is generated, you are prompted to enter a secondary password for accessing this key. Clicking OK generates the key and uses the entered password as the secondary RSA password for that key. Clicking Cancel causes key generation to fail..
Always prompt user	Every time an RSA key is generated, a secondary password for accessing this key is requested. However, the user can choose to dismiss the prompt (by clicking Cancel), and key generation will continue without using a secondary password for the generated RSA key.
Prompt on application request	This enables applications that use secondary authentication for RSA keys to make use of this feature on the eToken (when creating the key in Crypto API with a user protected flag).
Never	Secondary passwords are not created for any RSA key and the authentication method uses only the eToken password to access the key.

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



Chapter 7

PKI Client Settings


The PKI Client Settings set the parameters that apply to all eTokens that are initialized after the settings have been configured.

In this chapter:

- Opening PKI Client Settings
- Setting PKI Client Settings Password Quality
- Enabling CA Certificate Management
- Enabling Configuration after Initialization
- Enabling Configuration after Initialization
- Enabling Configuration by Administrator or User

Opening PKI Client Settings

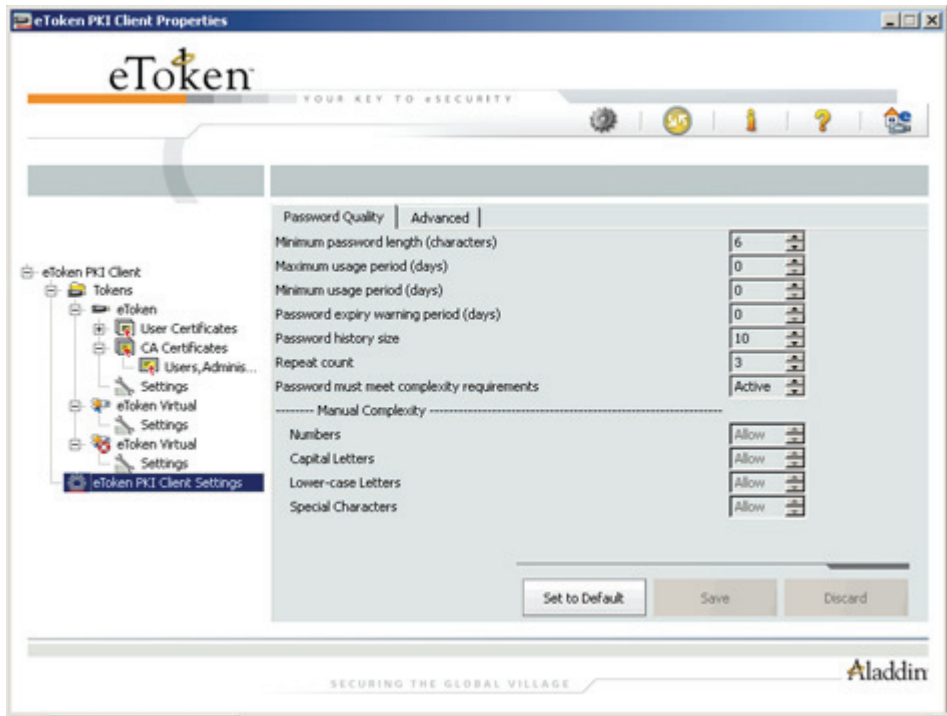
To open PKI Client Settings:

1. To open eToken PKI Client Properties, right-click the eToken tray icon  and select **Open eToken Properties** from the menu. The *eToken PKI Client Properties* window opens.
2. Click the **Advanced View** icon.



The *Advanced View* window opens.

3. In the left pane of the *eToken PKI Client Properties Advanced View* window, select **PKI Client Settings**.



Setting PKI Client Settings Password Quality

To set the PKI Client Settings Password Quality:

1. Open PKI Client Settings (See *Opening PKI Client Settings* on page 72).
2. Select the **Password Quality** tab.
3. Change the password quality settings.

Tip:

The PKI Client Settings password quality is configured in the same way as the eToken password quality settings. See *Setting eToken Password Quality* on page 62)

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

Enabling CA Certificate Management

CA certificates can be downloaded onto an eToken. When the eToken is inserted into the computer, one or more of these CA certificates may not be on the computer. In such a case, the CA certificate may be loaded onto the computer.

This option is selected by default.

To enable CA certificate management:

1. Open PKI Client Settings (See *Opening PKI Client Settings* on page 72).
2. Select the **Advanced** tab.
3. Select **CA certificate management**.

Note:

On Linux Platforms, selecting CA certificate management causes the CA certificate to be trusted.

4. Do one of the following:

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

Enabling Configuration after Initialization

The *Configurable after initialization* option defines whether the password quality parameters may be changed after initialization.

This option is selected by default.

To enable configuration after initialization:

1. Open PKI Client Settings (See *Opening PKI Client Settings* on page 72).
2. Select the **Advanced** tab.
3. Select **Configurable after initialization**.
4. Do one of the following:
 - ◆ To save your changes click **Save**
 - ◆ To ignore your changes click **Discard**

Enabling Configuration by Administrator or User

The *Configurable by Administrator (uncheck for user)* option defines whether the password quality parameters may be changed after initialization by the administrator, or, if unchecked, by the user.

This option is selected by default.

To enable configuration by administrator or user:

1. Open PKI Client Settings (See *Opening PKI Client Settings* on page 72).
2. Select the **Advanced** tab.
3. Do one of the following:
 - ◆ To enable configuration by administrator, check *Configurable by administrator*.

- ◆ To enable configuration by user, un-check *Configurable by administrator*.
4. Do one of the following:
- ◆ To save your changes click **Save**
 - ◆ To ignore your changes click **Discard**



Copyrights and Trademarks

The eToken™ system and its documentation are copyrighted © 1985 to present, by Aladdin Knowledge Systems Ltd.

All rights reserved.

eToken™ is a trademark and ALADDIN KNOWLEDGE SYSTEMS LTD is a registered trademark of Aladdin Knowledge Systems Ltd.

All other trademarks, brands, and product names used in this Manual are trademarks of their respective owners.

This manual and the information contained herein are confidential and proprietary to Aladdin Knowledge Systems Ltd. (hereinafter "Aladdin"). All intellectual property rights (including, without limitation, copyrights, trade secrets, trademarks, etc.) evidenced by or embodied in and/or attached/connected/related to this manual, information contained herein and the Product, are and shall be owned solely by Aladdin. Aladdin does not convey to you an interest in or to this manual, information contained herein and the Product, but only a limited right of use. Any unauthorized use, disclosure or reproduction is a violation of the licenses and/or Aladdin's proprietary rights and will be prosecuted to the full extent of the Law.

NOTICE

All attempts have been made to make the information in this document complete and accurate. Aladdin is not responsible for any direct or indirect damages or loss of business resulting from inaccuracies or omissions. The specifications in this document are subject to change without notice.



FCC Compliance

eToken USB has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- a. Reorient or relocate the receiving antenna.
- b. Increase the separation between the equipment and receiver.
- c. Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- d. Consult the dealer or an experienced radio/TV technician.

FCC Warning

Modifications not expressly approved by the manufacturer could void the user authority to operate the equipment under FCC rules.

All of the above applies also to the eToken USB.

FCC authorities have determined that the rest of the eToken product line does not contain a Class B Computing Device Peripheral and therefore does not require FCC regulation.

CE Compliance

The eToken product line complies with the CE EMC Directive and related standards*. eToken products are marked with the CE logo and an eToken CE conformity card is included in every shipment or upon demand.

*EMC directive 89/336/EEC and related standards EN 55022, EN 50082-1.

UL Certification

The eToken product line successfully completed UL 94 Tests for Flammability of Plastic Materials for Parts in Devices and Appliances. eToken products comply with UL 1950 Safety of Information Technology Equipment regulations.

ISO 9002 Certification

The eToken product line is designed and manufactured by Aladdin Knowledge Systems, an ISO 9002-certified company. Aladdin's quality assurance system is approved by the International Organization for Standardization (ISO), ensuring that Aladdin products and customer service standards consistently meet specifications in order to provide outstanding customer satisfaction.

Certificate of Compliance

Upon request, Aladdin Knowledge Systems will supply a Certificate of Compliance to any software developer who wishes to demonstrate that the eToken product line conforms to the specifications stated. Software developers can distribute this certificate to the end user along with their programs

Aladdin eToken Patent Protection

eToken Hardware and/or Software products described in this document are protected by one or more of the following Patents: US 6,748,541, US 6,554,621, US 7,249,266, US 6,763,399, and EP 1001329, and may be protected by other U.S. Patents, foreign patents, or pending applications.

