eToken PKI Client

Version 4.5

Reference Guide

June 2007

Contact Information

Support

If you have any questions regarding this package, its documentation and content or how to obtain a valid software license you may contact your local reseller or Aladdin's technical support team:

Country / Region	Telephone
USA	1-212-329-6658 1-866-202-3494 etoken.ts.us@aladdin.com
EUROPE: **Austria, Belgium, France, Germany, Italy, Netherlands, Spain, Switzerland, UK**	00800-22523346
Ireland	0011800-22523346
Rest of the World	+972-3-9781299

You can submit a question to the Aladdin eToken technical support team at the following web page:

http://www.aladdin.com/forms/etoken_question/form.asp

Website:

http://www.aladdin.com/eToken

Text Conventions

The following conventions are followed throughout this guide.

Convention	Meaning
Boldface	Used to indicate text that you enter, type or execute. Example: Click **Enter** or **Save** or **Delete**.
Italics	Used to highlight importance terms. Example: The *Production Domain* window opens, The *Connectors* window opens.
Note	Indicates additional information related to the task being discussed.
Caution	Identifies potential problems that the user should look out for when completing a task, or problems to be addressed before completing a task.
Sidebar	Provides ancillary information on the topic being discussed. Refer to sidebars to learn additional information about the topic that is not absolutely necessary for completing the task.
The greater than sign (>)	Used as a shortcut to indicate the path to be followed. Example: Programs>eToken>TMS>DB Tools, indicates: From the Programs menu, choose the eToken submenu. From eToken, choose the TMS submenu. From TMS, choose the DB Tools option.

Table of Contents

Chapter 1
Introduction

This chapter introduces Aladdin's eToken PKI Client, the software that enables eToken USB operations and the implementation of eToken PKI-based solutions.

This chapter includes the following:

- Overview
- System Architecture
- 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 either PKCS#11 or CAPI, proprietary eToken applications such as SSO (Single Sign-On), eToken for Network Logon, and management solutions like eToken TMS – a Token Management System that is a complete framework for managing all aspects of token assignment, deployment and personalization within an organization.

The 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 both Microsoft CAPI and PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications offering secure web and VPN access, secure network logon, PC and data security, secure email and more. PKI keys and certificates can be securely created, stored, and used from within eToken smart card-based devices.

The eToken PKI Client can be deployed and updated using any standard software distribution system, such as GPO and SMS.

The eToken Properties application and the PKI Client Monitor Service are installed with the eToken PKI Client, providing friendly configuration tools for users and administrators.

System Architecture

New Features

- Java Card-based token support
- Windows Vista full support
- Windows 64-bit OS support
- FIPS support
- Accessibility from the system tray via the PKI Client icon
- Optional evaluation version supporting 32-bit installation
- Simplified custom installation
- Common root folder for all eToken products
- Optional clearing of all registries during uninstall
- Availability in several languages

Chapter 2
System Requirements

Supported Operating Systems	Windows 2000® with SP4 or later
	Windows Server 2003®
	Windows XP® 32-bit and 64-bit with SP2 or later
	Windows Vista™ 32-bit and 64-bit
Supported Browsers	IE 6 and 7
	Firefox 2
	Netscape 7.2
Supported eToken Devices	eToken PRO (both Siemens CardOS and Java Card-based)
	eToken NG-OTP
	eToken NG-FLASH
	eToken PRO Smartcard
Required Hardware	USB port
Recommended Screen Resolution	1024 x 768 pixels or higher (for eToken Properties)

Notes:

Low level APIs used in eToken RTE 3.65 and earlier are not supported.

The evaluation version does not support 64-bit operating systems.

Chapter 3
Installation

The eToken PKI Client includes all the necessary files and drivers to support eToken integration. It also includes the eToken Properties configuration tool, which enables easy user management of the eToken password and name.

This chapter includes the following:

- Upgrading
- Installing via the Wizard
- Installing via the Command Line
- Installing in Silent Mode
- Uninstalling

Upgrading

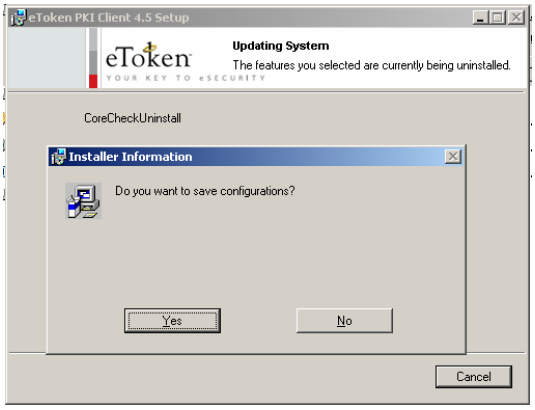
The eToken RTE 3.65 and later are automatically upgraded during the eToken PKI Client 4.5 installation.

eToken RTE versions earlier than 3.65 must be uninstalled or upgraded to eToken RTE 3.65 before installing the eToken PKI Client 4.5.

Machine and user registry settings are not cleared when PKI Client versions earlier than 4.5 are upgraded or uninstalled.

To clear all registries set by any PKI Client implementation:

1. Uninstall any eToken RTE version earlier than 3.65.
2. Install the eToken PKI Client 4.5.
3. Uninstall the eToken PKI Client 4.5. A *save configurations* dialog box opens.



4. Click **No**. The uninstall continues and previous configurations are deleted.

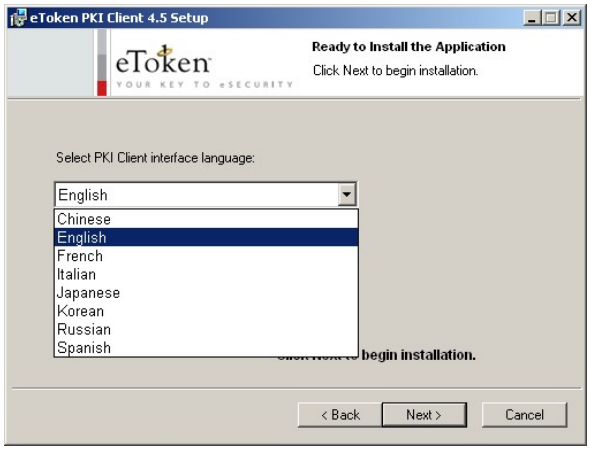
Installing via the Wizard

The eToken PKI Client must be installed on each computer on which an eToken device is to be used. The installation must be performed by a user with administrator privileges.

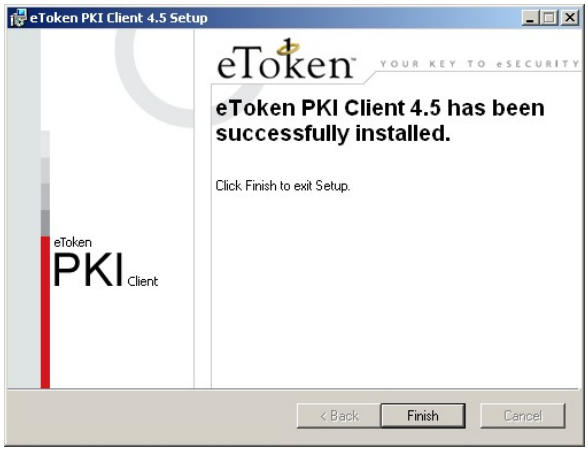
To install via the wizard:

1. Log on as an administrator.
2. Close all applications.

3. Double-click the appropriate 32-bit or 64-bit PKIClient msi file. The *eToken PKI Client 4.5 Installation Wizard* opens.
4. Click **Next**. If the eToken PKI Client is already installed, the repair begins.
5. If the eToken PKI Client is not installed, the *Select interface language* dialog box is displayed.



6. From the dropdown list, select the language in which the PKI Client user screens will appear, and click **Next**. The License Agreement is displayed.
7. Read the license agreement carefully and select the **I accept the license agreement** option.
8. Click **Next** and the installation begins. During the installation, an *Updating System* window is displayed providing progress on the installation. When the installation is complete, a *successfully installed* message is displayed.



9. Click **Finish**. The eToken PKI Client 4.5 is installed.
10. Follow the instructions to restart the computer if they are displayed.

Installing via the Command Line

Command line installation enables full control of installation properties. This is done by identifying each desired property as a parameter and assigning each a value.

Note: Properties may be set only during installation, and not when performing repairs.

The `msiexec` command used for command line installation takes the format:

`msiexec /i` *`PKICLIENT4.5`*`.msi` *`PROPERTY=VALUE PROPERTY=VALUE`*

where

- *`PKICLIENT4.5`*`.msi` is the appropriate (32-bit or 64-bit) PKIClient installation file
- *`PROPERTY`* is the name of a configurable property, usually identified by the prefix PROP_
- *`VALUE`* is the value assigned to the property

See the Installation Properties chapter on page 13 for the list of properties and their values that can be set during installation.

To install via the command line:

1. Open **Start > Programs > Accessories > Command Prompt**.
2. When running on Windows Vista, right-click **Command Prompt** and select **Run as**. Set the user to administrator.
3. Type the `msiexec` command with all desired property settings.

For example, to install the Spanish version of the PKI Client, with the eToken Properties Advanced Mode setting disabled, all registries to be cleared automatically upon uninstall, and all other properties assigned their default values, type the following command:

```
msiexec /i PKIClient-x32-4.5.msi
ET_LANG_NAME=Spanish
PROP_ADVANCED_VIEW=0
PROP_CLEAR_REG=1
```

Installing in Silent Mode

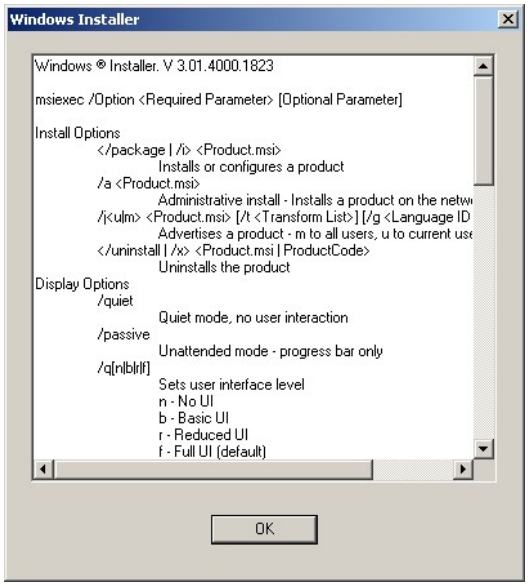
The PKI Client command line installation uses the standard *Windows Installer* `msiexec` syntax. Installing the PKI Client via the command line enables the administrator to define a silent mode installation in addition to optional property settings.

To run the installation in silent mode, add **`/q`** to the end of the `msiexec` command which is described in the Installing via the Command Line section on page 10:

`msiexec /i PKICLIENT4.5.msi /q`

To view optional parameters for the msiexec command:

1. Open **Start > Run**.
2. Type **msiexec** and click **OK**. *Windows Installer* opens, displaying the available parameters and their explanations.



Uninstalling

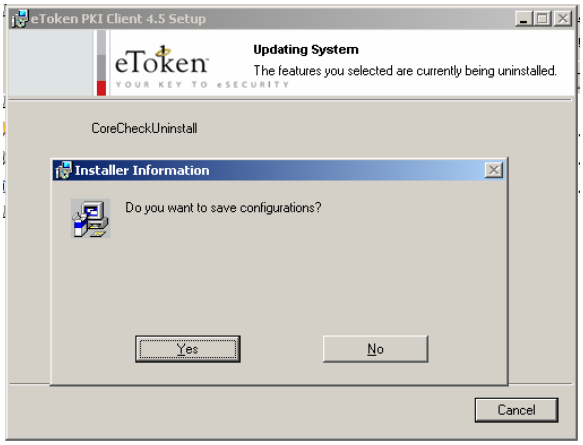
The eToken PKI Client may be uninstalled via:

- **Start > Settings > Control Panel > Add or Remove Programs**
- The installation wizard
  See the Installing via the Wizard section on page 8
- The command line utility `msiexec /x PKICLIENT4.5.msi`
  where `PKICLIENT4.5.msi` is the PKIClient installation file

  To uninstall in silent mode, add **`/q`** to the end of the `msiexec` command:
  `msiexec /x PKICLIENT4.5.msi /q`

If the PROP_CLEAR_REG=1 (enabled) property was defined when the PKI Client was installed, all machine and user registry settings are automatically cleared during uninstall.

If the property was not enabled during installation, a save configurations dialog box appears during the uninstall.



Click **Yes** to save configurations or **No** to delete configurations.

The uninstall continues and previous configurations are saved or deleted.

Chapter 4
Installation Properties

This chapter describes the properties that may be defined during the PKI Client 4.5 command line installation.

This chapter describes the following:

- Installation Properties Overview
- General Registry Key
- InitApp Registry Key
- CAPI Registry Key
- Certificate Store Registry Key
- Password Policies Registry Key
- Additional Properties

Installation Properties Overview

The properties described in this chapter may be set during the PKI Client 4.5 command line installation. See the Installing via the Command Line section on page 10 for details on this procedure.

Most PKI Client 4.5 properties are stored as values in registry key folders. The names of the registry keys and their values are not relevant when setting the properties during installation.

The registry key values listed in this chapter, as well as others, may be changed after installation. Some values may be changed using the eToken Properties application. Most values may be changed manually. The registry keys' names and values are needed when they are changed manually after installation. See the Setting Registry Keys Manually section on page 23 in the Configurable Settings chapter.

General Registry Key

The following properties are saved as registry settings in the **GENERAL** registry key:

Property	PROP_SINGLELOGONTO
DWORD Value	>=0
Default	0
Explanation	Timeout of single logon in seconds 0 = no timeout
Name	SingleLogonTimeout

The following properties may be set by the eToken Properties application:

Property	PROP_SINGLELOGON
DWORD Value	0/1
Default	0
Explanation	eToken Properties requests the user password only once (not including other applications) - enabled/disabled
Name	SingleLogon

Notes: If the SingleLogonTimeout value is >0, the SingleLogon value is automatically set to 1.

Property	PROP_SOFTWARESLOTS
DWORD Value	1-10
Default	1
Explanation	Number of software slots
Name	SoftwareSlots

Property	PROP_PCSCSLOTS
DWORD Value	1-16
Default	16
Explanation	Number of PC/SC slots
Name	PcscSlots

InitApp Registry Key

The following properties are saved as registry settings in the **InitApp** registry key, and may be set by the eToken Properties application:

Property	PROP_ADVANCED_VIEW
DWORD Value	0/1
Default	1
Explanation	*Advanced* button in eToken Properties application - enabled/disabled
Name	AdvancedView

CAPI Registry Key

The following properties are saved as registry settings in the **CAPI** registry key:

Property	PROP_EXPLORER_DEFENROL
DWORD Value	0/1
Default	1 for the IEXPLORE.EXE process 0 otherwise
Explanation	Download an enrollment certificate from the Microsoft CA service to use for creating a user certificate - enabled/disabled
Name	DefEnrollType

Note: The DefEnrollType value is set per process on a per machine basis.

Certificate Store Registry Key

The following properties are saved as registry settings in the **CertStore** registry key, and may be set by the eToken Properties application:

Property	PROP_PROPAGATEUSERCER
DWORD Value	0/1
Default	1
Explanation	Export all user certificates on the token to the user store - enabled/disabled
Name	PropagateUserCertificates

Note: The PropagateUserCertificates value is saved on a per user basis in `HKEY_CURRENT_USER`, and not in `HKEY_LOCAL_MACHINE`.

Property	PROP_PROPAGATECACER
DWORD Value	0/1
Default	1
Explanation	Export all CA certificates on the token to the Trusted CA store - enabled/disabled
Name	PropagateCACertificates

Password Policies Registry Key

The following properties are saved as registry settings in the **PQ** registry key, and may be set by the eToken Properties application:

Property	PROP_PQ_MINLEN
DWORD Value	>=4
Default	6
Explanation	Minimum password length
Name	pqMinLen

Property	PROP_PQ_MIXCHARS
DWORD Value	0/1
Default	1
Explanation	Mixed characters required
Name	pqMixChars

Property	PROP_PQ_MAXAGE
DWORD Value	>=0
Default	0
Explanation	Total number of days password is valid 0 = no expiration
Name	pqMaxAge

Property	PROP_PQ_MINAGE
DWORD Value	>=0
Default	0
Explanation	Total number of days required before change 0 = none
Name	pqMinAge

Property	PROP_PQ_WARNPERIOD
DWORD Value	>=0
Default	0
Explanation	Total number of days before expiration to display warning 0 = no warning
Name	pqWarnPeriod

Property	PROP_PQ_HISTORYSIZE
DWORD Value	>=0
Default	10
Explanation	Number of recent passwords that may not be repeated
Name	pqHistorySize

Additional Properties

The following properties may be set during a command line installation, but may not be modified afterward:

Property	PROP_CLEAR_REG
DWORD Value	0/1
Default	0
Explanation	Automatically clear all registry settings upon uninstall - enabled/disabled

Property	ET_LANG_NAME
String Value	`English / French / Korean / Russian / Spanish / Italian / Japanese / Chinese`
Default	English
Explanation	Language in which GUI is displayed

Property	READER_COUNT
DWORD Value	0-16
Default	2
Explanation	Number of physical reader device nodes

Property	PROP_UPD_INFPATH
DWORD Value	0/1
Default	0
Explanation	Update driver search path on install/uninstall - enabled/disabled

Note: For more information on the PROP_UPD_INFPATH property, please contact Aladdin customer support.

Property	PROP_FAKE_READER
DWORD Value	0/1
Default	1
Explanation	Virtual reader device node - present/absent

Note: For more information on the PROP_FAKE_READER property, please contact Aladdin customer support.

Chapter 5
Configurable Settings

This chapter provides administrator guidelines for manually setting registry keys.

This chapter also describes registry key values that may not be defined as properties during the PKI Client 4.5 command line installation. For a description of registry key values that may be defined during the installation, see the Installation Properties chapter on page 13.

This chapter describes the following:

- Registry Keys Overview
- Setting Registry Keys Manually
- General Registry Key
- CAPI Registry Key
- Certificate Store Registry Key

Registry Keys Overview

Registry key values set by the PKI Client 4.5 command line installation as properties, and by the eToken Properties application, are saved on a per machine basis unless otherwise noted.

Registry key values are saved per machine in `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\eToken\MIDDLEWARE`.

The administrator may set registry key values manually on a per machine basis.

The administrator may also set registry key values manually on a per user basis in `HKEY_CURRENT_USER\Software\Aladdin\eToken\MIDDLEWARE`.

Within these registry folders, some key values may be fine-tuned per specific process.

The priority in applying registry key values is:

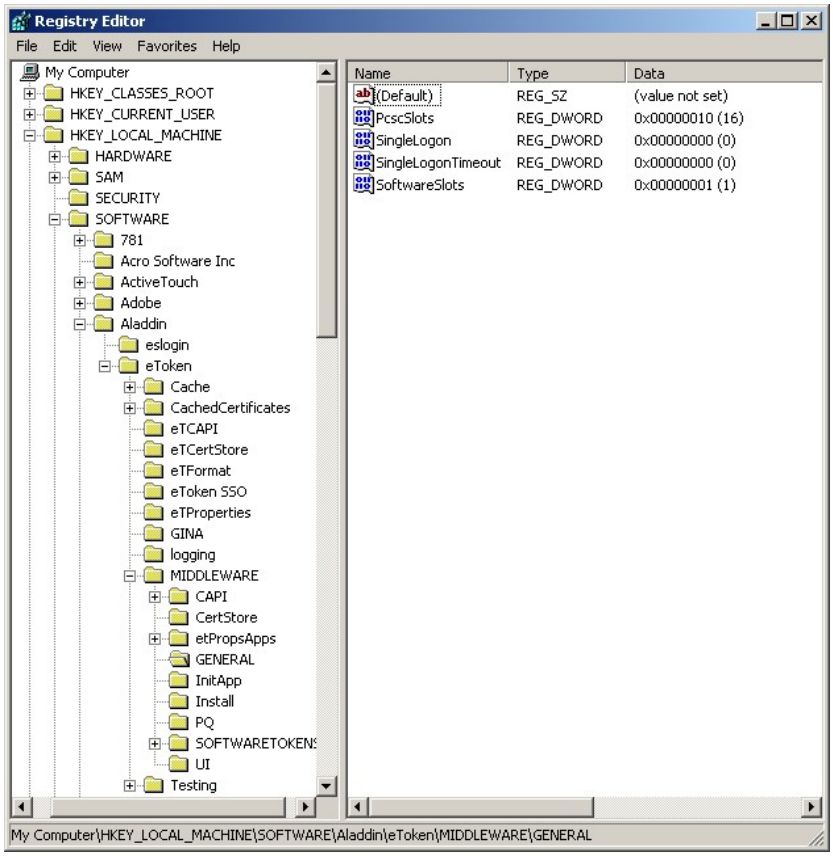
1. If a value is defined on the user level (and not limited to a different process), that value is applied.
2. Otherwise, if a value is defined on the machine level (and not limited to a different process), that value is applied.
3. If no value is found, the system default is applied.

Setting Registry Keys Manually

To set a registry key value manually:

1. Open **Start > Run**.
2. Type **regedit** and click **OK**. *Registry Editor* opens, displaying the registry folders tree in the left pane.
3. Expand the tree and select the desired registry key's folder. The names and settings of the values in the registry key are displayed in the right pane.

   In the example, the GENERAL registry key is selected in `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\eToken\MIDDLEWARE`.



4. To rename or delete a value, or to modify its data, right-click its Name.
5. To add a new value to the registry key, or to add a new registry key in the tree, right-click the white space in the right pane.

General Registry Key

The following registry settings are saved in the **GENERAL** registry key:

Name	TolerantFinalize
DWORD Value	0/1
Default	0
Explanation	DllMain may call C_Finalize - enabled/disabled

Note: Enable TolerantFinalize only for Novell Modular Authentication Service (NMAS) applications.

Name	TolerantX509Attributes
DWORD Value	0/1
Default	0
Explanation	CKA_SERIAL_NUMBER, CKA_SUBJECT, and CKA_ISSUER may differ from CKA_VALUE during certificate creation - enabled/disabled

Name	MechHardwareOnly
DWORD Value	0/1
Default	0
Explanation	Restrict the usage of software mechanisms - enabled/disabled

CAPI Registry Key

The following registry settings are saved in the **CAPI** registry key:

Name	PasswordTimeout
DWORD Value	>0
Default	None
Explanation	Number of minutes the CAPI UI-required password is valid

Name	LogoutMode
DWORD Value	0/1
Default	0
Explanation	User must enter password for each operation requiring user to be logged on - enabled/disabled

Certificate Store Registry Key

The following registry settings are saved in the **CertStore** registry key:

Name	RemoveUserCertsOnTokenRemove
DWORD Value	0/1
Default	1
Explanation	Remove user certificates from the user store when the token from which they were exported is removed - enabled/disabled

Name	AddToTokenOnNewCertInStore
DWORD Value	0/1
Default	1
Explanation	Offer to import the certificate to the selected token when a new certificate with exportable keys is added to the user store - enabled/disabled

Name	RemoveFromStoreOnRemoveFromToken
DWORD Value	0/1
Default	1
Explanation	Remove the certificate from the user store when that certificate is removed from the token - enabled/disabled

Name	RemoveFromTokenOnRemoveFromStore
DWORD Value	0/1/2
Default	0
Explanation	Offer to remove the certificate from the token when that certificate is removed from the user store - enabled/disabled 2 = Offer to remove only those certificates whose templates are listed in the registry setting `RemoveFromTokenOnRemoveFromStoreTemplates`

Name	RemoveFromTokenOnRemoveFromStoreTemplates
String Value	None
Default	None
Explanation	Templates of the certificates to be removed from the token when the certificates are removed from the user store

Name	CertsToRemoveStorePeriod
String Value	>=0
Default	7
Explanation	Number of days to attempt to remove certificates from a token

Note: This applies when the token from which a certificate was exported is not inserted when the certificate is removed from the user store.

Chapter 6
Administration

This chapter describes the following:

- Initializing a Token
- Setting Up a New User
- Replacing a Token
- Resetting a Token

Initializing a Token

The process of initializing a token:

- Erases all data and configurable parameters on the token
- Resets the token to the default password
- Restores a token with corrupted data to a usable state
- Enables the administrator to set an administrator password on the token, thus allowing an eToken user password to be reset in the future without data being erased from the token
- Enables the administrator to set configurable parameters on the token
- Enables a CardOS 4.01 or 4.2B-based eToken PRO device to be initialized either as a standard eToken PRO or as a FIPS eToken PRO

For detailed information on performing eToken initialization in eToken Properties, see the Initializing eToken section on page 52.

Setting Up a New User

To set up a new user:

1. Install the eToken PKI Client on the user's computer.
2. Initialize a token for the user.
   See the Initializing eToken section on page 52.
3. Issue the token to the user, with instructions to personalize it as soon as possible by renaming it and changing the password.
   See the Renaming the eToken and Changing the eToken Password sections on page 42.

Replacing a Token

When a user's token is lost or damaged, the administrator should initialize another token and issue it to the user, with instructions to personalize it as soon as possible.

Resetting a Token

If a user forgets the eToken password, the administrator should take the token and either:

- Reinitialize the token, whereby the token's data and configurable parameters are erased and the default eToken password is reset.
  See the Initializing eToken section on page 52.
- Reset only the user password, whereby all of the token's data and configurable parameters are retained. See the Setting User Password section on page 61.
  This option is available only if the token was initialized with an eToken administrator password.

Note: eToken TMS 2.0 offers a Virtual eToken solution, specially designed for employee on-the-road situations where the replacement of a lost or missing token is not practical.

Chapter 7
eToken Properties Application

This chapter provides an explanation of the eToken Properties application and the various configuration options available to the administrator and to the user.

This chapter describes the following:

- eToken Properties Overview
- Quick Functions
- Views
- Logging On
- Simple View
- Advanced View

eToken Properties Overview

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

eToken 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 an eToken password quality rating.

Caution: Do not remove the token from the USB port during an operation! Many operations, such as key generation, certificate enrollment, and certificate removal require multiple actions. If the token is removed during one of these actions, the data structure on the token may be damaged and data lost. The eToken may need to be reinitialized as a result.

---

eToken Properties provides information about the eToken, including its identification and capabilities. It has access to information stored on the token such as keys and certificates, and enables management of content only, such as password profiles, which is understood by the user (that is, not PKCS#11 objects) and by the PKI Client.

Quick Functions

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

- **Open eToken Properties**
- **Generate OTP**: generates OTP for supported eTokens
- **Change eToken Password**
- **eTokens**: selects the activated token when more than one is inserted
- **About**: displays product information
- **Hide**: hides the icon

To access the quick functions menu:

- Right-click the eToken icon  in the system tray.

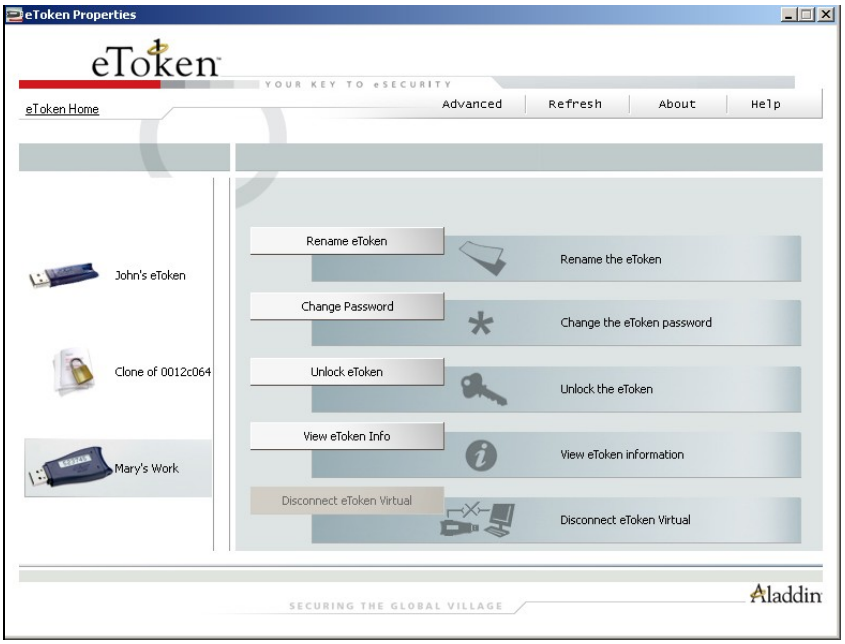
  The quick functions menu opens.

To open eToken Properties:

- Select **Open eToken Properties**.

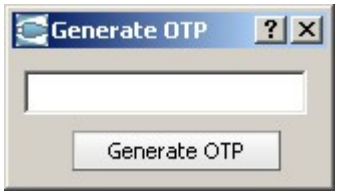
Note: eToken Properties may also be started from **Start > Programs > eToken > eToken Properties**.

The *eToken Properties* window opens in the Simple view, displaying all tokens that are connected to your computer.



To generate a one time password (OTP):

1. Select **Generate OTP**. The *Generate OTP* dialog box opens.



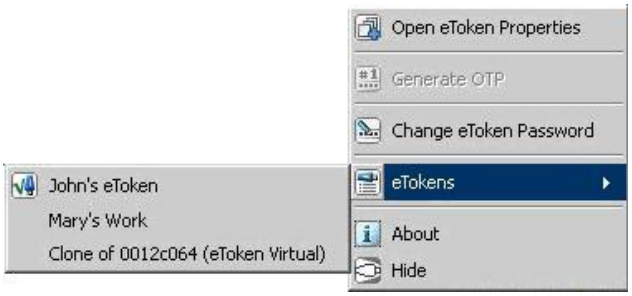
2. Click **Generate OTP**. The *Log On to eToken* dialog box opens.
3. Enter the eToken password. The generated OTP is displayed in the *Generate OTP* dialog box.

To change the eToken password:

- Select **Change eToken Password**. The *Change Password* dialog box opens. See the Changing the eToken Password section on page 42.

To select the active eToken:

1. Select **eTokens**. A list of inserted eTokens is displayed.



2. Select the desired eToken.

To view product information:

- Select **About**.

To hide the quick functions icon:

- Select **Hide**.

Tip: If the system tray menu does not open, try opening it manually by running the following file:
`[local drive]:\Program Files\Common Files\Aladdin Shared\eToken\PKIClient\[x32 or x64]\PKIMonitor.exe`.

Views

eToken Properties includes two viewing options:

- Simple view: to perform basic and common tasks
  See the Simple View section on page 40.
- Advanced view: for complete control over the PKI Client and the inserted tokens
  See the Advanced View section on page 48.

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 along the top enables certain actions to be initiated in both views.

Logging On

Certain operations which change token configurations require entering either the eToken user password or the eToken administrator password.

When the eToken user password is required, the *Log On to eToken* dialog box is displayed:

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

You may only log on as an administrator if an administrator password is present on the token.

When the eToken administrator password is required, the *Administrator Logon to eToken* dialog box is displayed:

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

Note: If you are logged on as an administrator and wish to access functions that require a user password, the *Log On to eToken* dialog box is displayed, requesting the eToken user password.

Simple View

When eToken Properties is launched, the *eToken Properties* window opens in the Simple view.

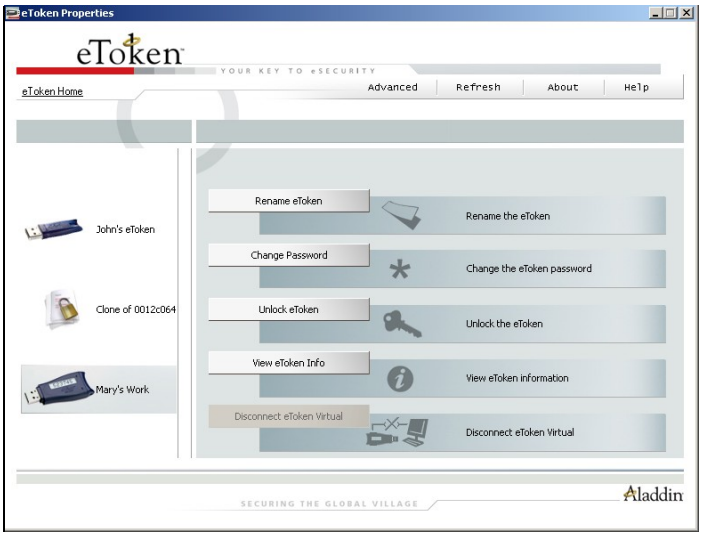
When a token is inserted or an eToken Virtual is present, a device specific icon representing the inserted token is displayed in the left pane.

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

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

eToken icons

	eToken PRO
	eToken Virtual
	eToken NG-OTP
	eToken NG-FLASH
	Smart Card Reader – with no card
	Smart Card Reader – with card
	eToken with corrupted data
	Unknown token



In the right pane, the user may select any of the following actions that are enabled:

- **Rename eToken** – sets the token name
- **Change Password** – changes the eToken user password
- **Unlock eToken** – resets the user password via a challenge response mechanism (Only enabled when an administrator password has been initialized on the token)
- **View eToken Info** – provides detailed information about the token
- **Disconnect eToken Virtual** – disconnects the eToken Virtual, with an option for deleting it

The toolbar along the top contains these functions:

- **Advanced** – switches to the Advanced view
- **Refresh** – refreshes the data for all connected tokens
- **About** – displays information about the product version
- **Help** – launches the online help

A hyperlink to the eToken website, *eToken Home*, appears at the top left of the window.

Renaming the eToken

The token name may be personalized.

To rename a token:

1. In the left pane of the *eToken Properties* window, select the token to be renamed.
2. Click **Rename eToken** in the right pane, and the *Rename eToken* dialog box is displayed.

3. Enter the new name in the New eToken name field.
4. Click **OK**. The new token name is displayed in the *eToken Properties* window.

Changing the 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 the Password Quality section on page 67.

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. In the left pane of the *eToken Properties* window, select the token to which the new password will be assigned.
2. Click **Change Password** in the right pane, and the *Change Password* dialog box is displayed.

3. Enter the current eToken password in the Current eToken Password field.
4. 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.
To view information used to determine the password quality score, click **Show Tips >>**.

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

Unlocking the eToken using Challenge - Response

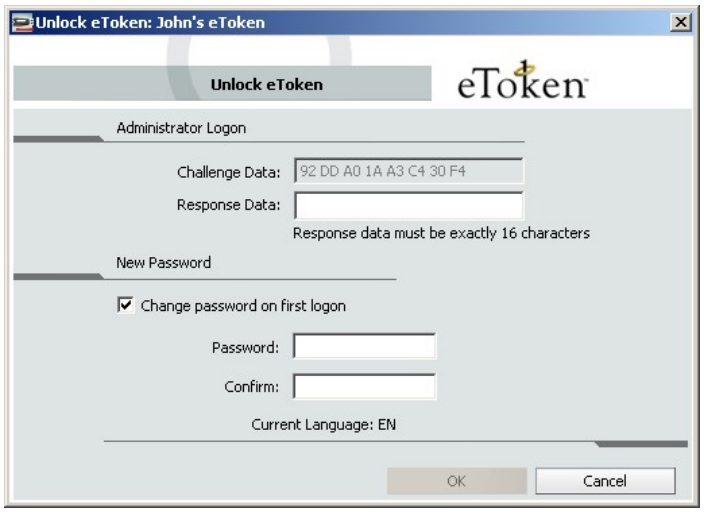
A token becomes locked if the eToken password is entered too many times incorrectly.

If the token had been initialized with an administrator password, and the administrator is present, the token may be unlocked using the eToken Properties Advanced view. See the Setting User Password section on page 61.

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. In this method, the user sends the administrator the Challenge Data supplied by eToken Properties, and then enters the Response Data provided by the administrator. The user then enters a new password and the token is unlocked.

To unlock a token using Challenge – Response:

1. In the left pane of the *eToken Properties* window, select the token to be unlocked.
2. Click **Unlock eToken** in the right pane, and the *Unlock eToken* dialog box is displayed.



3. Contact the administrator and provide him with the Challenge Data.

Caution: After providing the Challenge Data to the administrator, the user MUST NOT undertake any activities that use the token until after receiving the Response Data and completing the unlocking procedure.

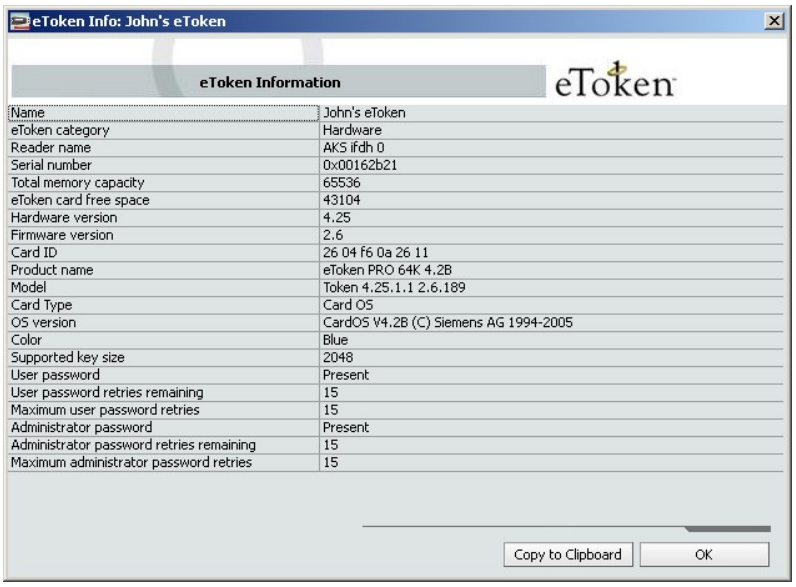
If any other eToken activity occurs during this process, it will affect the context of the Challenge – Response process and invalidate the procedure.

4. The administrator provides the Response Data to be entered.
5. Enter a new eToken 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.

Note: Response Data creation depends on the backend application being used by the organization. Please refer to the relevant documentation for details on how to generate the Response Data.

Viewing eToken Information

Information relating to a specific token can be viewed by selecting the token in the left pane of the *eToken Properties* window, and clicking **View eToken Info** in the right pane. The *eToken Information* dialog box is displayed:



The information in this dialog box can be copied to the clipboard.

To paste the information into an application:

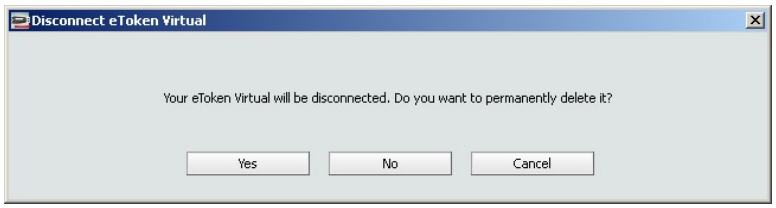
1. Click **Copy to Clipboard**.
2. Place the cursor in the target application and paste the information.

Disconnecting eToken Virtual

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

To disconnect an eToken Virtual:

1. In the left pane of the *eToken Properties* window, select the eToken Virtual to be disconnected.
2. Click **Disconnect eToken Virtual** in the right pane, and the *Disconnect eToken Virtual* dialog box is displayed.



3. To keep the eToken Virtual file on the computer, click **No**, and only the connection from the eToken Virtual to eToken Properties is disconnected.
4. To remove the eToken Virtual file from the computer, click **Yes**.

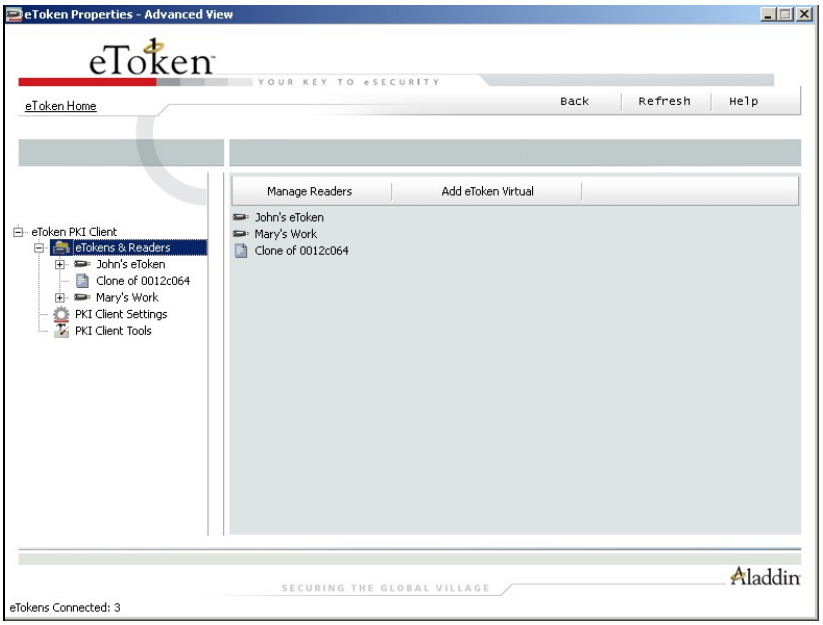
Note: Disconnecting the eToken Virtual without removing it completely is applicable when the user is out of the office and may need to use the eToken Virtual on the road later.

When the lost eToken is replaced, the eToken Virtual should be completely removed from the computer.

Advanced View

The eToken Properties Advanced view provides additional token management functions.

Click **Advanced** on the Simple view toolbar, and the *eToken Properties* window opens in the Advanced view.



The toolbar along the top offers these functions:

- **Back**: switches to the Simple view
- **Refresh**: refreshes the data for all connected tokens
- **Help**: launches the online help

A hyperlink to the eToken website, *eToken Home*, appears at the top left of the window.

A status bar at the bottom of the window displays additional information about the highlighted object, such as the number of connected readers, or the current logon state.

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

- Left-click an object in the tree, and information about that object appears in the right pane.
- Right-click an object in the tree, and a shortcut menu of commands for that object appears.

eTokens & Readers

This node manages the readers (slots) that are available on the system.

When the eTokens & Readers node is selected, the toolbar displays the following:

- Manage Readers
- Add eToken Virtual

The same commands are available when you right-click the eTokens & Readers node.

Managing Readers

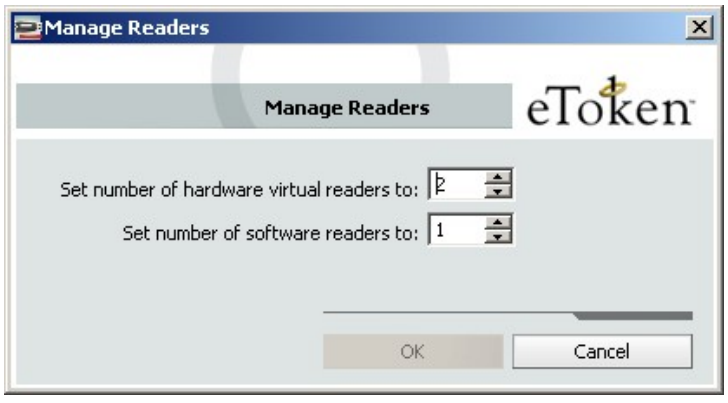
During the eToken PKI Client installation, eToken Properties installs two virtual smart card readers and one eToken Virtual reader.

When an eToken is inserted into a USB port, or an eToken Virtual is added, or a smart card is inserted into the smart card reader, the effect is the same as inserting a smart card 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. Click **Manage Readers** on the toolbar, or right-click **eTokens & Readers** and select **Manage Readers** from the shortcut menu. The *Manage Readers* dialog box opens.



2. Set the number of hardware or software readers in the appropriate field to the number desired.

The default number of available readers is:

- Hardware readers: 2
- Software readers: 1

3. Click OK to close the dialog box. The number of available readers has been changed.
4. Restart eToken Properties to make the changes effective.

Adding an eToken Virtual

The PKI Client 4.5 supports eToken Virtual, a software token. The eToken Virtual is stored in a file on the computer.

The eToken Virtual is specially designed as a solution for "employee on-the-road" issues, where the replacement of a lost or missing eToken is not practical.

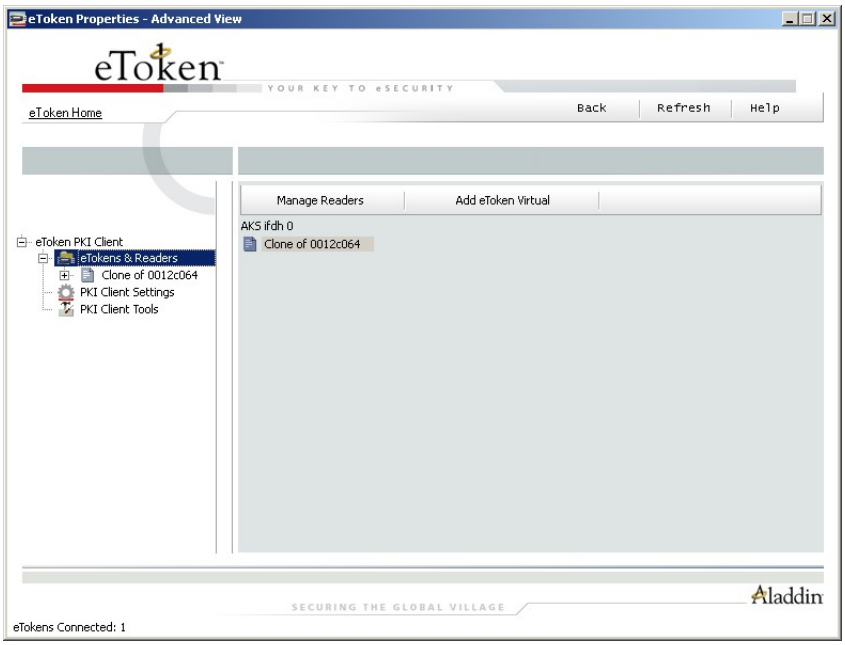
To add an eToken Virtual:

1. Click **Add eToken Virtual** on the toolbar, or right-click **eTokens & Readers** and select **Add eToken Virtual** from the shortcut menu.
2. Navigate to the eToken Virtual file (*.etv) and double-click it. The eToken Virtual is added and a confirmation dialog box opens.

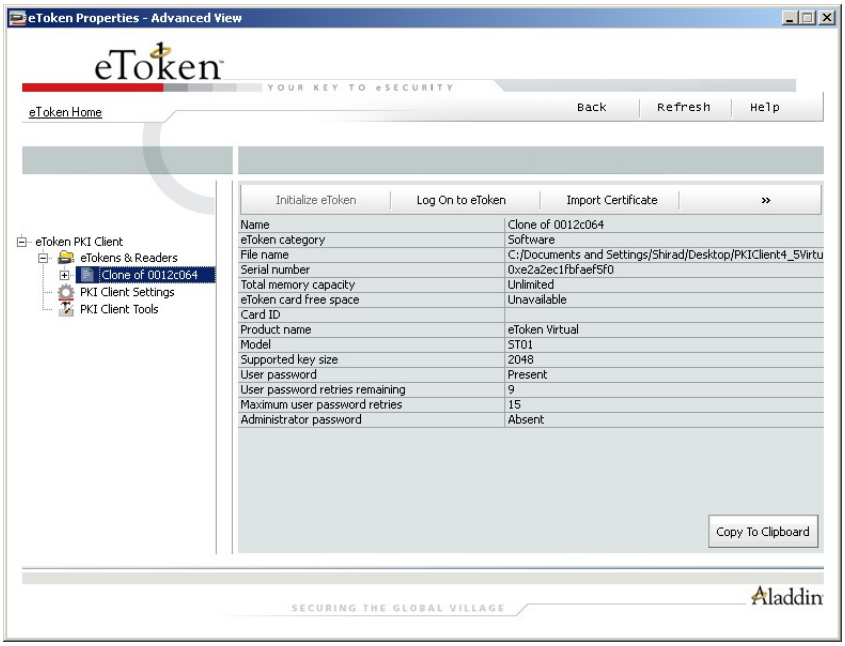
3. Click **OK.**

Viewing Inserted eTokens

When the eTokens & Readers node is expanded, the names of all inserted tokens, physical and virtual, are displayed.



To display all information about a token in the right pane, select it in the left pane.



This is the same information that is displayed in the Viewing eToken Info command in the Simple view.

The toolbar displays key commands that can be performed with or on this object, such as logging on and importing certificates.

The expand arrow to the right of the toolbar shows all other commands available with this object.

These commands are also available by right-clicking the object in the left pane.

Certain commands are disabled if not applicable. For example, administrator functions are disabled for an eToken Virtual.

Some Advanced view commands are identical to those in the Simple view:

- Rename eToken
- Change Password
- Unlock eToken
- Disconnect eToken Virtual

Initializing eToken

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:

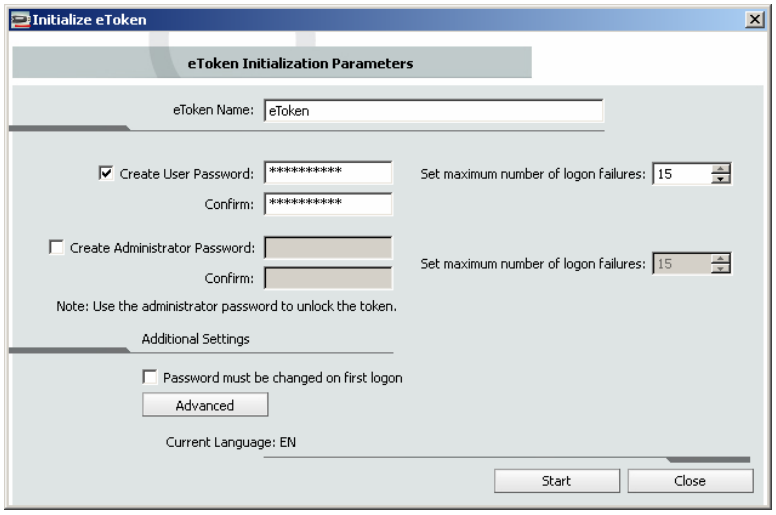
- eToken name
- User password
- Administrator password (optional)
- Maximum number of logon failures (for user and administrator passwords
- Requirement to change the password on the first logon
- Initialization key

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

Using customizable parameters, you can select specific parameters that will apply to certain eTokens. 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.

To initialize an eToken:

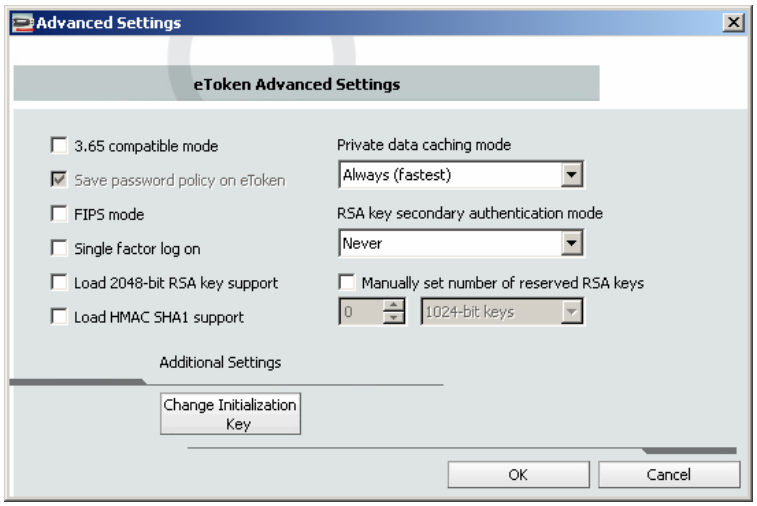
1. Click **Initialize eToken** on the toolbar, or right-click the token name in the left pane and select **Initialize eToken** from the shortcut menu. The *eToken Initialization Parameters* dialog box opens.



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.
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 fields, 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 eToken with an incorrect password before the eToken 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**.
8. To configure advanced settings, click **Advanced.** The *eToken Advanced Settings* dialog box opens.



9. 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.
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.

Field	Description
Single factor logon	Default: disabled When starting an application using an inserted eToken, the eToken password is required. This occurs for each application even if it is during the same computer session. Single factor logon enables users multiple access to the eToken with only one request for the password. This alleviates the need to log on each application separately. Note: For security reasons, single factor logon is not applied to eToken Properties.
Load 2048-bit RSA key support	Select to enable 2048-bit RSA key support (on compatible token).
Load HMAC SHA1 support	Select to enable HMAC SHA1 support (on compatible token).
Private data caching mode	In PKI Client 4.5, 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. Select one of the following options: **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	Description
RSA key secondary 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. **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.

10. If required, click **Change Initialization Key.** The *eToken Initialization Key* dialog box opens.

11. 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 This Value field below.
Change Initialization Key to:	**Default**: Revert to default. **Random**: If selected, it will never be possible to re-initialize the eToken. **This Value**: Select and confirm a password.

12. Click **OK** to return to the *eToken Advanced Settings* dialog box, then click **OK** again to return to the e*Token Initialization Parameters* dialog box.

13. Click **Start**.

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

Logging On as a User

To log on as a user:

1. Click **Log On to eToken** on the toolbar, or right-click the token name in the left pane and select **Log On** from the shortcut menu. The *Log On to eToken* dialog box opens.
2. Enter the eToken user password in the Password field and click **OK**. The user is logged on.

Logging On 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 and Change Password Quality Settings that are stored on the token.

To log on as an administrator:

1. Click **Administrator Logon** on the toolbar, or right-click the token name in the left pane and select **Administrator Logon** from the shortcut menu. The A*dministrator Logon to eToken* dialog box opens.
2. Enter the administrator password in the Password field and click **OK**. The user is logged on as the Administrator.

Importing a Certificate

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.

When downloading a certificate to the computer and then importing the certificate to the eToken, remove the certificate from the local store and reinsert the eToken before using the certificate to sign and encrypt mail. This ensures you are using the certificate and keys stored on the eToken.

To import a certificate:

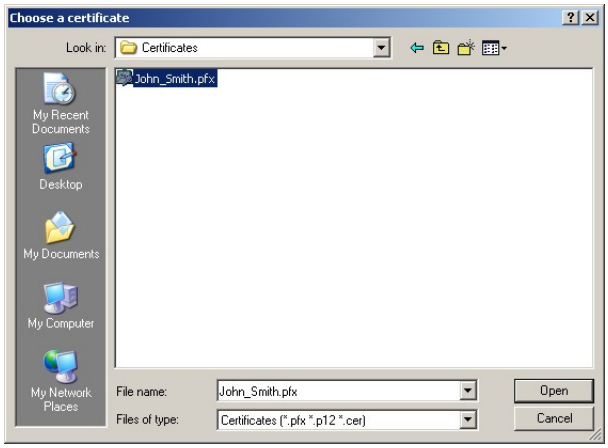
1. Click **Import Certificate** on the toolbar, or right-click the token name in the left pane and select **Import Certificate** from the shortcut menu. The *Import Certificate* dialog box opens.

2. Select whether the certificate to import is on your personal certificate store on the computer, or on a file.

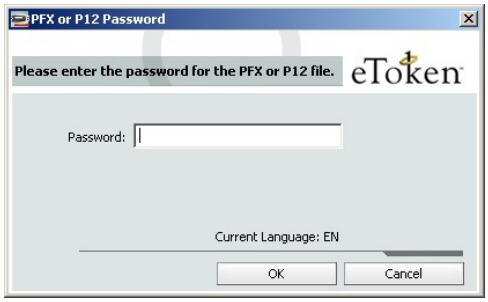
   If you select the personal certificate store, a list of available certificates is displayed. Only certificates that can be imported on to the eToken are listed. These are:

   - Certificates with a private key already on the eToken
   - Certificates that may be imported from the computer together with its private key

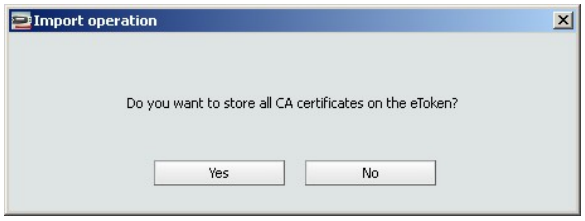
3. If you select Import a certificate from a file, the *Choose a certificate* dialog box opens.



4. Select the certificate to import and click **Open**.
5. If the certificate requires a password, a *Password* dialog box opens.



6. Enter the certificate password. A dialog box opens asking if you want to store the CA certificates on the eToken.



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

Changing the Administrator Password

To change the Administrator password:

1. Click **Change Administrator Password** on the toolbar, or right-click the token name in the left pane and select **Change Administrator Password** from the shortcut menu. The *Change Administrator Password* dialog box opens.

2. Enter the current administrator password in the Current Password field.
3. Enter the new administrator password in the New Password and Retype fields.
4. Click **OK**. The administrator password is changed.

Setting User Password

Setting a user password to unlock an eToken can be performed only if an administrator password has been set during initialization.

A challenge-response authentication system can also be used to unlock a locked eToken. See the Unlocking the eToken using Challenge - Response section on page 44.

To unlock a token using Set User Password:

1. Log on to the selected token as the administrator. See the Logging On as an Administrator section on page 58.
2. Click **Set User Password** on the toolbar, or right-click the token name in the left pane and select **Set User Password** from the shortcut menu. The *Set eToken Password* dialog box opens.

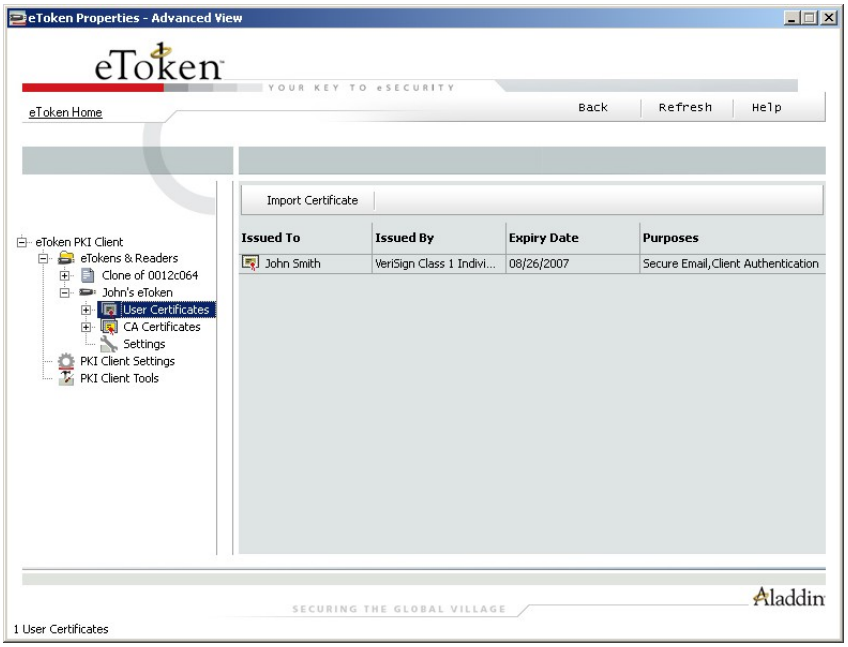
3. Enter a new password in the New Password and Confirm fields.
4. Set the Set Error Retry Counter from 0 to 15.
5. Click **OK**. The eToken is unlocked.

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

Certificates

When an eToken node is expanded, certificate nodes are displayed if the token contains certificates.

Click on the User Certificates node or the CA Certificates node to itemize the certificates in the right pane, or to import another certificate.



Expand the Certificates node to select individual certificates.

Select a certificate to enable the following commands:

- Delete Certificate
- Export Certificate
- Set as Enrollment Agent
- Set as Default
- Set as Auxiliary
- Copy to Clipboard

To initiate certificate activity, do one of the following:

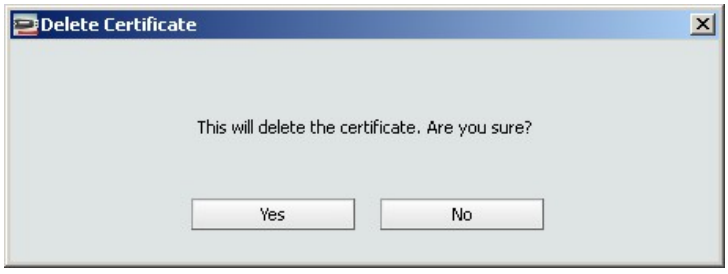
- Select the certificate in the left pane and click the appropriate action on the toolbar
- Right-click the certificate name in the left pane and select the appropriate action from the shortcut menu.

Deleting a Certificate

The eToken PKI Client copies certificates from the eToken to the registry store. When the application closes, the certificates are deleted from the registry store and remain on the eToken. As a result, the certificates are copied again on the next token insertion unless they are deleted from the token.

To delete a certificate:

1. Select **Delete Certificate**. The *Delete Certificate* dialog box opens.



2. Click Y**es**.

Exporting a Certificate

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

To export a certificate:

1. Select **Export Certificate**. The *Export Certificate* dialog box opens.
2. Select the location to store the certificate and click **OK**.

Setting a Certificate as Default, Enrollment Agent or Auxiliary

You can set a certificate as:

- **Default**
- **Enrollment Agent**
- **Auxiliary**

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

Certain applications that use CAPI do not say explicitly which key should be used for their operations, for example, Microsoft VPN. The PKI Client logic is such that if there is a default key (used for Smartcard Logon) on the token, this key will be used for such applications. If no default key exists, the PKI Client chooses which key to use.

Most users do not have multiple keys on their tokens, so this mechanism works satisfactorily. If a user needs to explicitly set a key to be used in such an application, the Auxiliary setting serves this purpose.

To set a certificate as Default, Enrollment Agent or Auxiliary:

1. Select the appropriate setting.
2. Enter the password and click **OK**.

Settings

The settings node under a specific object refers to settings for that object only. There are two types of settings:

- **Password Quality**: configures password policy on the eToken
- **Other**: configures settings relating to cache policies and RSA secondary authentication

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 RTE versions, no password policy is stored on the token.

The password quality parameters are:

- **Minimum password length:** default is 6 characters
- **Maximum usage period:** in days; default is 0 = none
- **Minimum usage period:** default is 0 days
- **Password expiry warning period:** defines the number of days before the password expires that a warning message is shown; default is 0 = none
- **Password history size:** defines how many old passwords should not be repeated (default is 10)
- **Password must meet complexity requirements:** defines whether mixed characters are required in the eToken password; default = yes

Other

These settings are:

- **Private data caching mode**
- **RSA key secondary authentication mode**

Private data caching mode	In PKI Client 4.5, 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. Select one of the following options: **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.
RSA key secondary 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. **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.

PKI Client Settings

This node refers to generic eToken settings unless superseded by a change to a specific object. There are two types of settings:

- **Password Quality**: configures password policy on eTokens
- **Other**: configures settings relating to certificate storage, certificate management, logon modes and administrator privileges

Password Quality

These PKI Client settings share the same parameters as the settings for individual eTokens. They are used to set a global password policy for eTokens with no password quality parameters, such as those in use with versions of eToken RTE 3.65 and earlier.

The password quality parameters are:

- **Minimum password length:** default is 6 characters
- **Maximum usage period:** in days; default is 0 = none
- **Minimum usage period:** default is 0 days
- **Password expiry warning period:** defines the number of days before the password expires that a warning message is shown; default is 0 = none
- **Password history size:** defines how many old passwords should not be repeated (default is 10)
- **Password must meet complexity requirements:** defines whether mixed characters are required in the eToken password; default = yes

In addition to the above password quality parameters that may also be set per token, two global parameters are set:

- **Configurable after initialization:** defines whether the password quality parameters may be changed after initialization; default = yes
- **Configurable by Administrator (uncheck for user):** defines whether the password quality parameters may be changed after initialization by the administrator, and not by the user only; default = yes

Note: If the Configurable after initialization parameter is disabled, the Configurable by Administrator (uncheck for user) parameter is not relevant.

Other

These settings are:

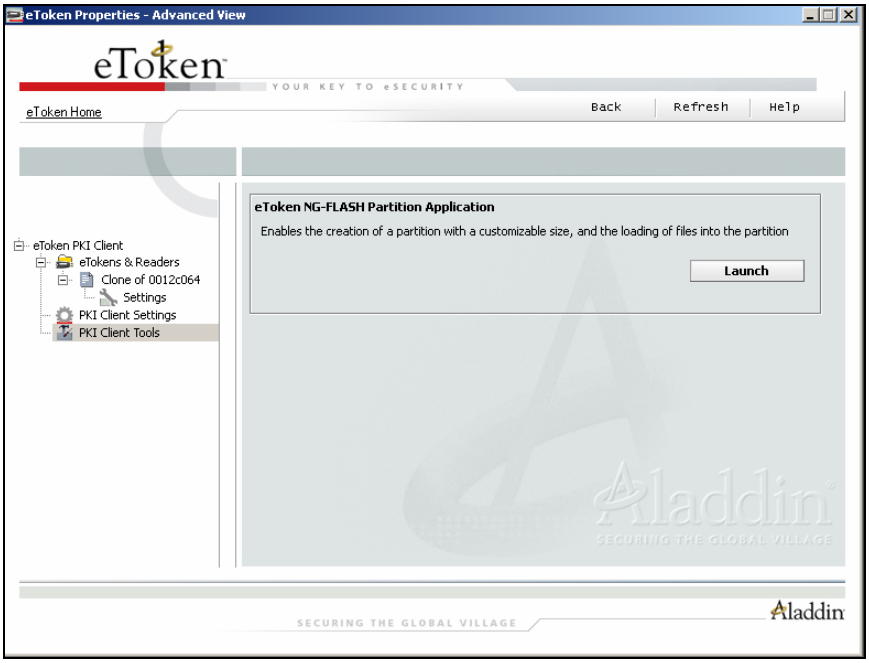
- **Copy user certificates to a local store**
- **CA certificate management**
- **Enable Single Logon mode**

Copy user certificates to a local store	Default: enabled PKI operations usually require certificates, private and public keys. Private keys should always be securely stored on the eToken. Certificates should also be stored on the eToken as this enables mobility (the certificate will be readily available when using the eToken on a different computer). This option controls the action of automatically copying all user certificates to the Certificate store upon eToken insertion.

CA certificate management	Default: enabled 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. **Note:** Despite the settings chosen, it is possible that another window from Microsoft opens asking if you wish to continue this action. This is standard Microsoft operating procedure because the action to be undertaken may affect security matters on the computer. If you want to copy the CA certificate, click **Yes**.
Enable Single Logon mode	Default: disabled When starting an application using an inserted eToken, the eToken password is required. This occurs for each application even if it is during the same computer session. Single logon mode enables users multiple access to the eToken with only one request for the password. This alleviates the need to log on each application separately. Note: For security reasons, the single logon mode is not applied to eToken Properties.

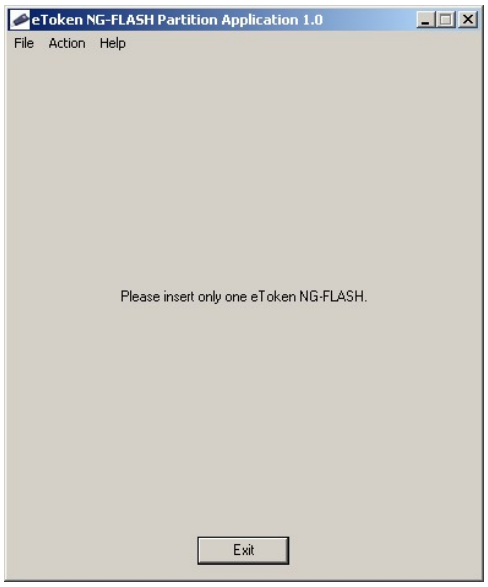
PKI Client Tools

This section provides a link to additional tools that may be applicable to different kinds of tokens. Currently, the only option available is to launch a mass storage application.



To launch mass storage application:

1. Click **Launch**. The *eToken NG-FLASH Partition Application* dialog box opens.



2. Insert an eToken-Flash. The application displays information about the inserted eToken NG-FLASH.
3. Set the eToken parameters as required and click **Run Partition**. The eToken NG-Flash is reconfigured.

Appendix 1
Copyrights and Trademarks

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.

Appendix 2
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.