



eToken PKI Client (Windows)

Administrator's Guide

Version 5.1 SP1 Rev A



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: January 2010

Last update: Thursday, January 21, 2010 3:49 pm

Support

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

Telephone

You can call our help-desk 24 hours a day, seven days a week:

USA: 1-800-545-6608

International: +1-410-931-7520

Email

You can send a question to the technical support team at the following email address:

support@safenet-inc.com

Website

You can submit a question through the SafeNet Support portal:

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

Additional Documentation

We recommend reading the following eToken publications:

- eToken PKI Client (Windows) 5.1 User's Guide
- eToken PKI Client (Windows) 5.1 SP1 ReadMe

Table of Contents

1. Introduction.....	1
Overview.....	2
New Features in eToken PKI Client 5.1 SP1	3
2. Architecture Overview.....	5
eToken PKI Client Architecture.....	6
eToken PKI Client Modules	7
eToken PKI Client Monitor.....	7
eToken Properties	8
eToken Service.....	8
3. System Requirements	9
Remote Desktop Connection	11
4. Checklist of Administrator Tasks.....	13
5. Installation.....	15
Upgrading from eToken PKI Client 5.1.....	16
Upgrading from eToken PKI Client 5.1 via the Wizard	16
Upgrading from eToken PKI Client 5.1 via the Command Line.....	17
Upgrading from Earlier Versions	18
Upgrading from eToken PKI Client 4.0 and Later	18
Upgrading from Versions Earlier than eToken PKI Client 4.0.....	18
Installing via the Wizard.....	19
Installing via the Command Line	24
Viewing Command Line Parameters	24
Installing in Silent Mode	25
Setting Application Properties via the Command Line	26
Limiting and Adding Installation Features via the Command Line	30
Removing Features via the Command Line	31

Installing Without Drivers	33
Uninstalling.....	34
Uninstalling via the Add or Remove Programs Option	34
Uninstalling via the Wizard	35
Uninstalling via the Command Line.....	38
6. eToken PKI Client Settings	39
eToken PKI Client Settings Overview.....	40
Accessing eToken PKI Client Settings in Windows Server Platforms	41
Adding eToken PKI Client Settings in Windows Server Platforms	41
Opening eToken PKI Client Settings in Windows Server Platforms.....	44
Accessing eToken PKI Client Settings in Windows XP	48
Adding eToken PKI Client Settings in Windows XP.....	48
Opening eToken PKI Client Settings in Windows XP	52
Editing eToken PKI Client Settings	54
Applying eToken PKI Client Settings	57
7. Properties and Configuration.....	59
Overview of Application Properties.....	60
Application Properties Hierarchy	60
Setting Registry Keys Manually.....	61
Registry Key Tables	62
General Registry Key	63
SyncPin Registry Key.....	68
Init Registry Key.....	69
InitApp Registry Key	72
CAPI Registry Key.....	72
Certificate Store Registry Key	75
Monitor Registry Key	79
Password Policies Registry Key.....	79
User Interface Registry Keys.....	85
Access Control Registry Key.....	86

A. Copyrights and Trademarks	89
B. FCC Compliance	91
FCC Warning	91
CE Compliance.....	92
UL Certification	92
ISO 9001 Certification	92
Certificate of Compliance	93
C. Aladdin eToken Patent Protection	95

Introduction

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

In this chapter:

- [Overview](#)
- [New Features in eToken PKI Client 5.1 SP1](#)

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.

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 eToken SSO (Single Sign-On), eToken Network Logon, and management solutions such as eToken TMS (Token Management System). TMS manages all aspects of token assignment, deployment and personalization within an organization.

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 access, secure network logon, 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, such as GPO and SMS.

The *eToken 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 in eToken PKI Client 5.1 SP1

eToken PKI Client 5.1 SP1 introduces the following new features:

- **Support for more Microsoft platforms:** Supports Windows 7 and Windows Server 2008 R2, Internet Explorer 8.0
- **Support for more token devices:** Supports the flash partition application on eToken NG-Flash 4.50 CardOS, eToken NG-Flash 5.30 Java, and eToken NG-Flash 5.30 Java Anywhere devices
- **Support for more hash algorithms:** Supports the SHA-2 family of algorithms
- **More dependable:** Resolves customer-reported issues from earlier releases

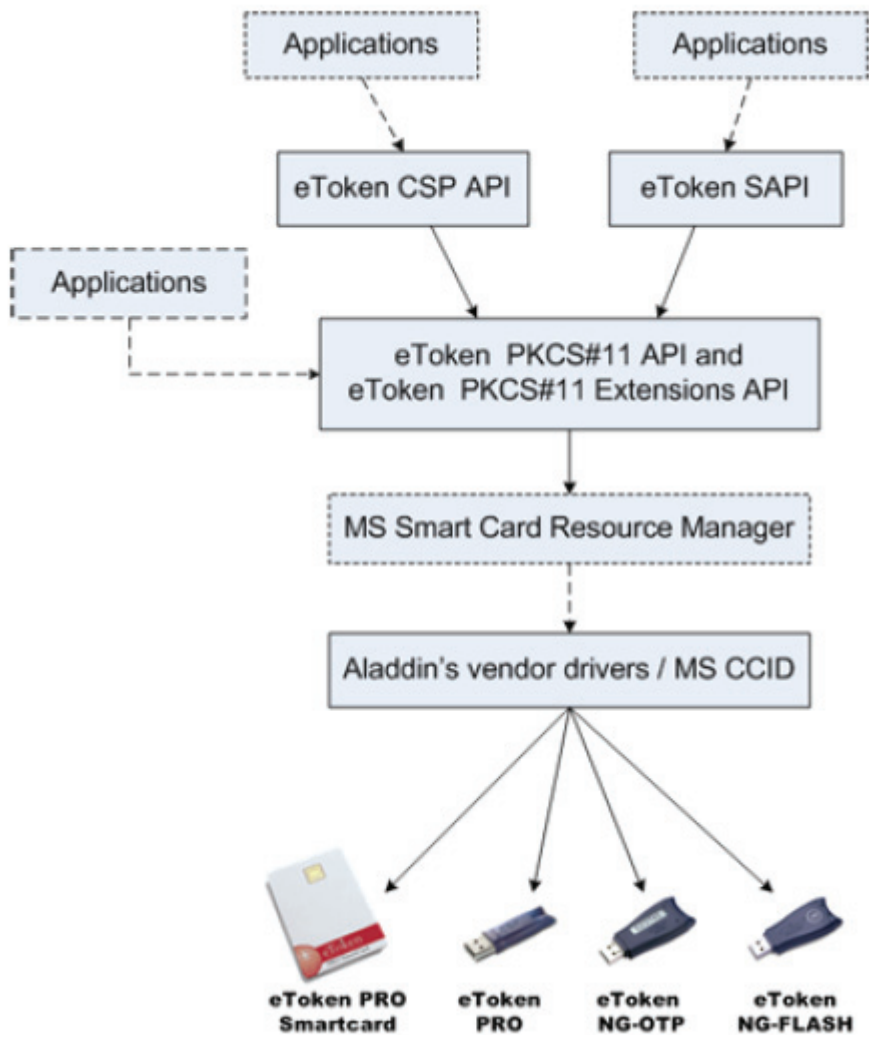
Architecture Overview

This chapter describes the eToken PKI Client 5.1 SP1 architecture.

In this chapter:

- eToken PKI Client Architecture
- eToken PKI Client Modules

eToken PKI Client Architecture



eToken PKI Client Modules

eToken PKI Client 5.1 SP1 contains three modules:

- eToken PKI Client Monitor
- eToken Properties
- eToken Service


eToken PKI Client Monitor

eToken PKI Client Monitor starts automatically with Windows start-up. It can also be launched from the Windows *Start* menu.

This module enables:

- Certificate propagation
- Password expiry pop-up messages
- eToken PKI Client tray icon functionality

Depending on the properties set, you can use the

eToken PKI Client tray icon  to:

- Launch eToken Properties
- View all the connected tokens, and select one as active
- Change a token's eToken Password
- Delete a token's eToken Content
- Generate an OTP for an eToken Virtual
- Hide the eToken PKI Client tray icon
- Synchronize the domain password with the token's eToken Password
- Launch eToken SSO Client

eToken Properties

This module can be launched from the eToken PKI Client tray icon or from the Windows *Start* menu.

Use eToken Properties to:

- View all the connected tokens, and select one as active
- Set and change a token's eToken Password
- Change a token's Administrator Password
- Unlock a locked token
- Delete a token's eToken Content
- Connect and disconnect an eToken Virtual
- Initialize a token
- View, import, export, and delete certificates on a token
- Set a certificate on a token as the default
- View and set eToken settings
- View and set eToken and eToken PKI Client password quality parameters

eToken Service

This module is a system service added to the Windows Services Manager. The operating system automatically recognizes the connection of an eToken Virtual found in the appropriate folder on a mass storage device as an emulation of a smartcard connection.

System Requirements

Before installing eToken PKI Client, ensure that your system meets the minimum requirements.

In this chapter:

- [System Requirements](#)
- [Remote Desktop Connection](#)

System Requirements

Supported Operating Systems	Windows XP SP3 (32-bit), SP2 (64-bit)
	Windows Vista SP2 (32-bit and 64-bit)
	Windows 7 (32-bit and 64-bit)
	Windows Server 2003 SP2 (32-bit and 64-bit)
	Windows Server 2008 (32-bit and 64-bit)
	Windows Server 2008 R2
Supported Browsers	Firefox 3.0.x
	Internet Explorer 6.0, 7.0, and 8.0
Supported eToken Devices	eToken PRO
	eToken NG-OTP
	eToken NG-FLASH
	eToken PRO Smartcard
	eToken PRO Anywhere
Required Hardware	USB port (for physical eToken devices)
Recommended Screen Resolution	1024 x 768 pixels or higher (to use eToken Properties)

Remote Desktop Connection

The following table lists the requirements for eToken PKI Client to work with Remote Desktop Connection.

Operating Systems	Windows Server 2003
	Windows Server 2008
	Windows Server 2008 R2
eToken Hardware Tokens	Supported
eToken Virtual Products on the Client	Not Supported
eToken Virtual Products on the Server	<ul style="list-style-type: none">■ eToken Virtual■ eToken Rescue <p>Note: To work with eToken Virtual products on the server, eToken Network Logon must be installed.</p>

Checklist of Administrator Tasks

The following tasks are performed by the administrator:

1. If upgrading from a version of eToken PKI Client earlier than 5.1, determine if the registry keys are to be cleared before installing eToken PKI Client 5.1 SP1.
 - ◆ See Chapter 5: *Upgrading from Earlier Versions*, on page 18 in this document.
2. Upgrade to, or install, eToken PKI Client 5.1 SP1 on each computer on which a token is to be used.
 - ◆ For upgrading from eToken PKI Client 5.1, see Chapter 5: *Upgrading from eToken PKI Client 5.1*, on page 16 in this document.
 - ◆ For installing via the installation wizard, see Chapter 5: *Installing via the Wizard*, on page 19 in this document.
 - ◆ For installing via the command line, see Chapter 5: *Installing via the Command Line*, on page 24 in this document.
3. Customize the *eToken PKI Client Settings* if required, and update all client computers.
 - ◆ See Chapter 6: *eToken PKI Client Settings*, on page 39 in this document.
4. Create new users.
 - ◆ See the *eToken Initialization* chapter in the eToken PKI Client 5.1 User's Guide.
5. Manage users.
 - ◆ See the *eToken Management* chapter in the eToken PKI Client 5.1 User's Guide.

Installation

eToken PKI Client includes all the necessary files and drivers to support eToken integration. It also includes the *eToken Properties* application, which enables easy user management of token names and passwords.

eToken PKI Client must be installed on each computer on which a token is to be used. Local administrator rights are required to install or uninstall eToken PKI Client.

In this chapter:

- [Upgrading from eToken PKI Client 5.1](#)
- [Upgrading from Earlier Versions](#)
- [Installing via the Wizard](#)
- [Installing via the Command Line](#)
- [Installing Without Drivers](#)
- [Uninstalling](#)

Upgrading from eToken PKI Client 5.1

If eToken PKI Client 5.1 is already installed on the computer, use the msp upgrade file to upgrade to SP1.

Note:

Once SP1 is installed, there is no rollback. Uninstalling SP1 uninstalls the complete eToken PKI Client application.

Upgrading from eToken PKI Client 5.1 via the Wizard

To upgrade via the installation wizard:

1. Log on as an administrator.
2. Close all applications.
3. Double-click the appropriate 32-bit or 64-bit eToken PKI Client 5.1 SP1 msp file.

The *eToken PKI Client 5.1 SP1 Installation Wizard* opens.



4. Click **Next**.
5. Follow the wizard until the installation finishes, and click **Finish**.

Upgrading from eToken PKI Client 5.1 via the Command Line

The eToken PKI Client command line upgrade uses the standard Windows Installer `msiexec` syntax.

Note:

When upgrading from eToken PKI Client 5.1, do not include any application properties.

To upgrade via the command line:

1. Log on as an administrator.
2. Close all applications.
3. Open **Start > Programs > Accessories > Command Prompt**.
When running on Windows Vista, right-click **Command Prompt** and select **Run as**. Set the user to administrator.
4. Type the `msiexec` command:

```
msiexec /update PKIClient-x32-5-1-SP1.msp
```

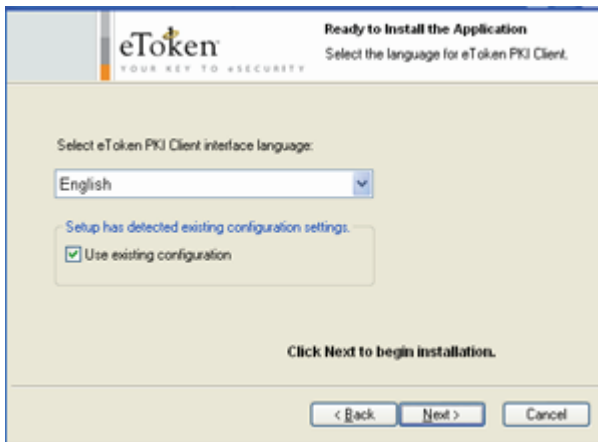
where
`PKIClient-x32-5-1-SP1.msp` is the 32-bit PKIClient upgrade file.
For 64-bit, use `PKIClient-x64-5-1-SP1.msp`.
To upgrade in silent mode, add `/q` to the end of the command.

Upgrading from Earlier Versions

Upgrading from eToken PKI Client 4.0 and Later

eToken PKI Client 4.0 and later are automatically upgraded during the eToken PKI Client 5.1 SP1 installation, but their machine and user registry settings are not cleared.

If these settings are detected during the eToken PKI Client 5.1 SP1 wizard installation, a **Use existing configuration** option appears on the *Select interface language* dialog box.



To maintain the registry settings from the earlier eToken PKI Client installation, select **Use existing configuration**.

Upgrading from Versions Earlier than eToken PKI Client 4.0

eToken RTE versions earlier than eToken PKI Client 4.0 must be uninstalled before installing eToken PKI Client 5.1 SP1.

Machine and user registry settings are not cleared when eToken PKI Client versions earlier than 4.0 are uninstalled.

To clear all registry keys set by any eToken PKI Client implementation:

1. Uninstall any eToken RTE version earlier than 4.0.
2. Install eToken PKI Client 5.1 SP1.
See the *Installing via the Wizard* section on page 19.
3. Uninstall eToken PKI Client 5.1 SP1, and on the *Save settings* dialog box, select **No** to not save the eToken PKI Client settings.
See the *Uninstalling* section on page 34.

Installing via the Wizard

Use the eToken PKI Client 5.1 SP1 Installation Wizard to install the default properties and features with the application.

The properties that can be set using the wizard are:

- Interface language: the language in which the eToken Properties user interface is displayed
- Destination folder: the installation library for this and all future eToken application installations (if no other eToken application has been installed on the computer)

To install via the installation wizard:

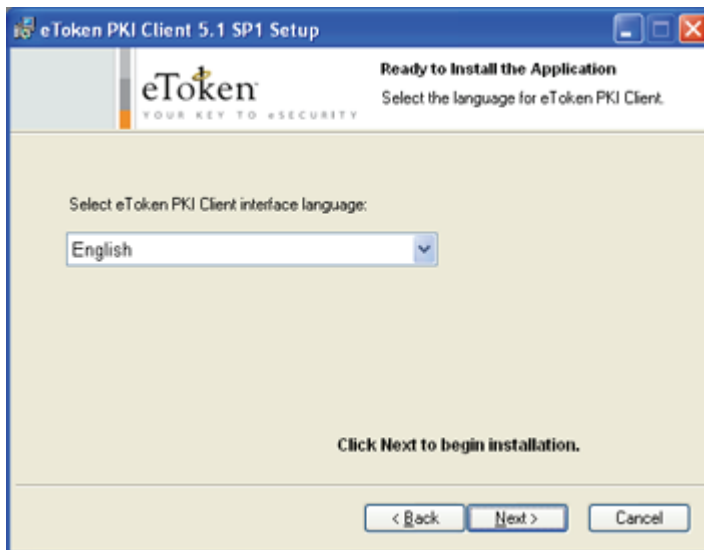
1. Log on as an administrator.
2. Close all applications.
3. Double-click the appropriate 32-bit or 64-bit PKIClient msi file.

The *eToken PKI Client 5.1 SP1 Installation Wizard* opens.



4. Click **Next**.

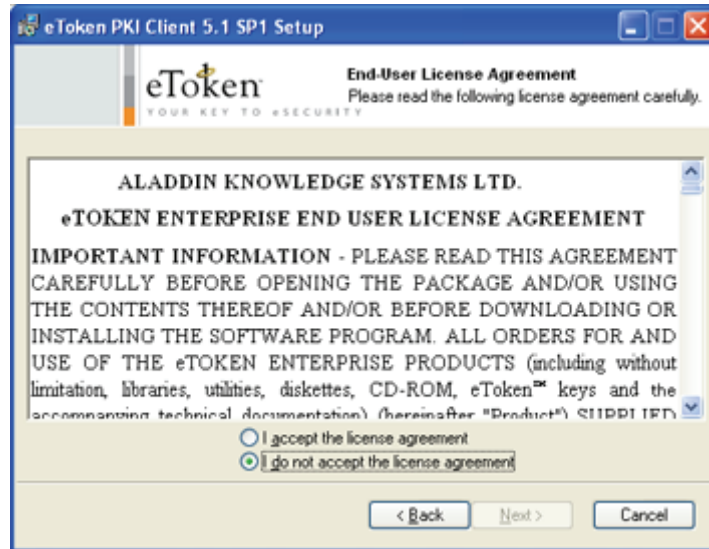
The *Select interface language* dialog box is displayed.



5. From the dropdown list, select the language in which the eToken PKI Client user screens will appear.

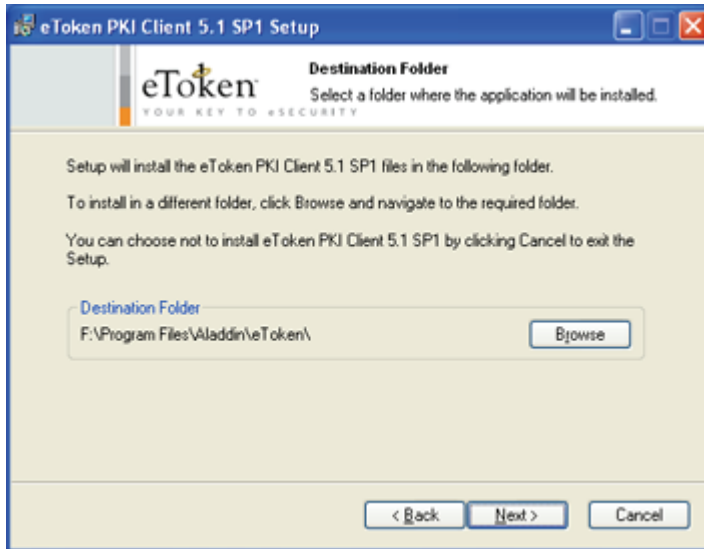
6. If configuration settings are detected from a previous version of eToken PKI Client, you can select the option to maintain the existing settings. For more information, see *Upgrading from eToken PKI Client 5.1* on page 16.
7. Click **Next**.

The *License Agreement* is displayed.



8. Read the license agreement, and select the option, **I accept the license agreement**.
9. Click **Next**.

The *Destination Folder* window opens, displaying the default installation folder.



10. If there are no other eToken applications installed, you can click **Browse** to select a different destination folder.

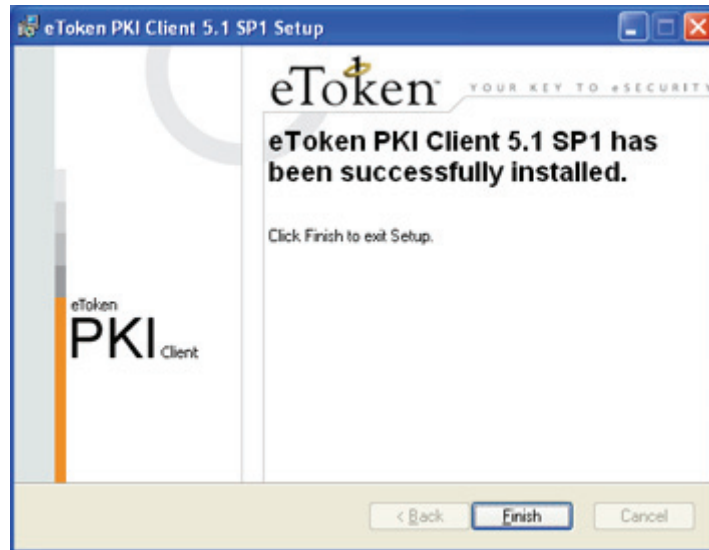
This folder will be used as the installation library for all future eToken application installations.

Note:

If an eToken application is already installed, the destination folder cannot be changed.

11. Click **Next**.
The installation begins.

When the installation is complete, a confirmation message is displayed.



12. Click **Finish** to complete the installation.

Installing via the Command Line

Command line installation gives the administrator full control of installation properties and features.

The eToken PKI Client command line installation uses the standard Windows Installer `msiexec` syntax:

```
msiexec /i PKIClient-x32-5.1-SP1.msi
```

where

`PKIClient-x32-5.1-SP1.msi` is the 32-bit PKIClient installation file. For 64-bit, use `PKIClient-x64-5.1-SP1.msi`.

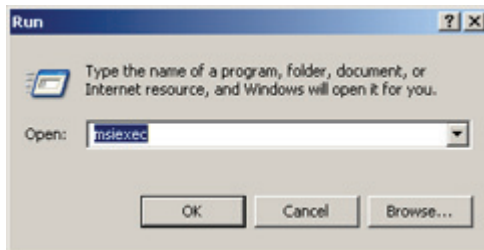
To install via the command line:

1. Log on as an administrator.
2. Close all applications.
3. Open **Start > Programs > Accessories > Command Prompt**.
When running on Windows Vista, right-click **Command Prompt** and select **Run as**. Set the user to administrator.
4. Type the `msiexec` command with the appropriate parameters, properties, and feature settings, as described in this chapter.

Viewing Command Line Parameters

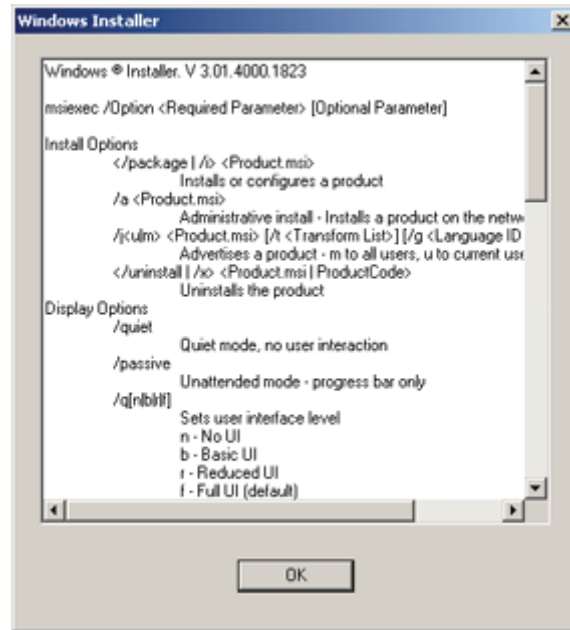
To view optional parameters for the `msiexec` command:

1. Open **Start > Run**.
The *Run* dialog box opens.



2. Type `msiexec`, and click **OK**.

The *Windows Installer* opens, displaying the available parameters and their explanations.



Installing in Silent Mode

Installing 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:

```
msiexec /i PKIClient-x32-5.1-SP1.msi /q
```

where

PKIClient-x32-5.1-SP1.msi is the 32-bit PKIClient installation file. For 64-bit, use PKIClient-x64-5.1-SP1.msi .

Note:

To have a basic user interface level, use the `/qb` parameter.

Setting Application Properties via the Command Line

During command line installation, the administrator can override the application's default values by including specific properties, and assigning each a value. These new values are saved in

HKEY_LOCAL_MACHINE\Software\Aladdin\eToken\MIDDLEWARE.

Note:

PROP_REG_FILE, on page 29, does not follow this rule.

Properties can be set only during installation, and not during repair.

To set properties during installation, use the following command format:

```
msiexec /i PKIClient-x32-5.1-SP1.msi PROPERTY=VALUE  
PROPERTY=VALUE /qb
```

where

- PKIClient-x32-5.1-SP1.msi is the 32-bit PKIClient installation file. For 64-bit, use PKIClient-x64-5.1-SP1.msi
- PROPERTY is the name of a configurable property, often identified by the prefix PROP_
- VALUE is the value assigned to the property

See the *eToken PKI Client Command Line Installation Properties* table on page 27 for the list of properties that can be set during installation.

Some properties are stored as registry keys and can be set or modified after installation. These properties are described in the *Registry Key Tables* section on page 62.

Some properties can be set only during command line installation, and may not be modified afterward. These properties are described in the *Installation-Only Properties* section on page 28.

Example: To install the Spanish version of eToken PKI Client, with the eToken Properties Advanced Mode setting disabled, all registry keys to be cleared automatically upon uninstallation, and all other properties assigned their default values, type the following command:

```
msiexec /i PKIClient-x32-5.1-SP1.msi  
ET_LANG_NAME=Spanish  
PROP_ADVANCED_VIEW=0  
PROP_CLEAR_REG=1 /qb
```

Command Line Installation Properties

eToken PKI Client Command Line Installation Properties

Property	Description
ET_LANG_NAME	See page 28
PROP_ADVANCED_VIEW	See page 72
PROP_CLEAR_REG	See page 28
PROP_EXPLORER_DEFENROL	See page 73
PROP_FAKEREADER	See page 28
PROP_PCSCSLOTS	See page 64
PROP_PQ_HISTORYSIZE	See page 80
PROP_PQ_MAXAGE	See page 80
PROP_PQ_MINAGE	See page 81
PROP_PQ_MINLEN	See page 81
PROP_PQ_MIXCHARS	See page 82
PROP_PQ_WARNPERIOD	See page 84
PROP_PROPAGATECACER	See page 76
PROP_PROPAGATEUSERCER	See page 77
PROP_REG_FILE	See page 29
PROP_SINGLELOGON	See page 65
PROP_SINGLELOGONTO	See page 65
PROP_SOFTWARESLOTS	See page 66
PROP_UPD_INFPATH	See page 29
READER_COUNT	See page 30
TARGETDIR	See page 30

Installation-Only Properties

The following properties, unless stated otherwise, can be set only during command line installation, and may not be modified afterwards:

ET_LANG_NAME Property

Property Name	ET_LANG_NAME
Description	Determines the eToken PKI Client interface language
Value in the Command Line	Chinese / English / French / French (Canadian) / German / Italian / Japanese / Korean / Polish / Portuguese / Russian / Spanish / Thai
Default	English

PROP_CLEAR_REG Property

Property Name	PROP_CLEAR_REG
Description	Determines if all registry settings are automatically cleared upon uninstall
Value	1 (True) - Registry settings are cleared upon uninstall 0 (False)- Registry settings are not cleared upon uninstall
Default	0 (False)

PROP_FAKEREADER Property

Property Name	PROP_FAKEREADER
Description	Determines if a virtual reader device node is present
Value	1 (True) - A virtual reader device node is present 0 (False)- A virtual reader device node is not present 128- No eToken driver files are installed
Default	1 (True)

Note:

For more information on the PROP_FAKEREADER property, please contact eToken customer support.

PROP_REG_FILE Property

Property Name	PROP_REG_FILE
Description	Determines if the settings defined in a registry file are imported during the eToken PKI Client installation The contents of the HKEY_LOCAL_MACHINE registry folder in the saved file are imported to the HKEY_LOCAL_MACHINE registry folder of the computer
Value	The path to a saved registry file
Default	none

Note:

While other command line installation properties set values only in HKEY_LOCAL_MACHINE\Software\Aladdin\eToken\MIDDLEWARE, values set in the PROP_REG_FILE file are written to the HKEY_LOCAL_MACHINE subfolders specified in the file.

PROP_UPD_INFPATH Property

Property Name	PROP_UPD_INFPATH
Description	Determines the update driver search path on install/uninstall
Value	The update driver search path on install/uninstall
Default	none

Note:

For more information on the PROP_UPD_INFPATH property, please contact eToken customer support.

READER_COUNT Property

Property Name	READER_COUNT
Description	Determines the number of physical reader device nodes
Value	0-16
Default	2

Note:

This feature can be set using eToken Properties also.

TARGETDIR Property

Property Name	TARGETDIR
Description	If there are no other eToken applications installed, this value determines which installation folder to use as the installation library for this and all future eToken application installations
Value	The path to the installation library
Default	none - the application is installed in the default eToken installation folder

Note:

Important! Only include the TARGETDIR property if there are no other eToken applications installed on the computer.

Limiting and Adding Installation Features via the Command Line

To exclude specific features from the eToken PKI Client installation, use the `ADDDEFAULT` parameter to install only those features required. The excluded features can be added afterwards to the installed application.

To install only specific features, use the following command format:

```
msiexec /i PKIClient-x32-5.1-SP1.msi ADDDEFAULT=F1,F2...Fn  
/qb
```

where

- PKIClient-x32-5.1-SP1.msi is the 32-bit PKIClient installation file. For 64-bit, use PKIClient-x64-5.1-SP1.msi
- ADDDEFAULT indicates that only the following features are included in the installation, or added to the installed application
- FX is the name of each feature to be included

See the *eToken PKI Client Features to Add or Remove* table on page 32 for the list of features that can be included during installation.

Example: Installing eToken PKI Client without eToken Properties

To install eToken PKI Client with many standard features, but without the eToken Properties application, type the following command:

```
msiexec /i PKIClient-x32-5.1-SP1.msi  
ADDDEFAULT=DriverFeature,CoreFeature,UIFeature,  
etMonitor,etFSFeature,etVerifierFeature,NgFlashFeature /qb
```

To add the eToken Properties application to eToken PKI Client after installation, type the following command:

```
msiexec /i PKIClient-x32-5.1-SP1.msi  
ADDDEFAULT=etPropsFeature /qb
```

Removing Features via the Command Line

Installed features can be removed from the eToken PKI Client installation. To remove features, use the following format:

```
msiexec /i PKIClient-x32-5.1-SP1.msi REMOVE=F1,F2...,Fn /qb
```

where

- PKIClient-x32-5.1-SP1.msi is the 32-bit PKIClient installation file. For 64-bit, use PKIClient-x64-5.1-SP1.msi
- REMOVE indicates that the following features are to be removed

- FX is the name of each feature to be removed

See the *eToken PKI Client Features to Add or Remove* table on page 32 for the list of features.

Note:

Only optional features can be removed.

Example: To remove the eToken Properties application after it was installed with eToken PKI Client, type the following command:

```
msiexec /i PKIClient-x32-5.1-SP1.msi REMOVE=etPropsFeature /qb
```

Command Line Installation Features

eToken PKI Client Features to Add or Remove

Feature	Description	Optional or Required
DriverFeature	Installs all drivers and the custom DLL files needed for their correct initialization	Optional, but required for eToken physical devices
CoreFeature	Installs functionality for full operation of eToken PKI Client; can be installed without DriverFeature (to work with eToken Virtual or foreign readers)	Required
UIFeature	Installs GUI components and the UI DLL	Required for etPropsFeature and etMonitor
etPropsFeature	Installs the eToken Properties application	Optional, but required for the eToken Properties application
etMonitor	Installs the eToken PKI Client tray icon and its plug-ins	Required
etVerifierFeature	Installs etVerifier COM object	Optional, but required by various Web applications (including TMS Client)

eToken PKI Client Features to Add or Remove (Continued)

Feature	Description	Optional or Required
NgFlashFeature	Installs the NGFlash application	Optional, but required for formatting flash memory on eToken NG-Flash devices
etFSFeature	File System API	Optional
ETOKSRV	Creates and activates eTSrv.exe, a service that tracks the connection and removal of flash devices, and looks for eToken Virtual files on flash devices. Default: installed	Required for eToken SSO single sign-on solution

Note:

To enable eToken device support without installing the eToken PKI Client application, use the eToken PKI Client command line installation with the `DriverFeature` feature only.

Installing Without Drivers

To install eToken PKI Client 5.1 SP1 without eToken drivers:

1. On the command line, include the `PROP_FAKEREADER=128` property.
The installation program will not attempt to install eToken driver files.
2. On the command line, do one of the following:
 - ◆ List the features to install, and do not include `DriverFeature`.

For example:

```
msiexec /i PKIClient-x32-5.1-SP1.msi
PROP_FAKEREADER=128
ADDDEFAULT=CoreFeature,UIFeature,etMonitor,etFSFeature,etVerifierFeature,etPropsFeature /qb
```

During installation, the eToken driver files will not be copied to the driver setup folder.

- ◆ Include `DriverFeature` by default.

For example:

```
msiexec /i PKIClient-x32-5.1-SP1.msi  
PROP_FAKEREADER=128
```

During installation, the eToken driver files will be copied to the driver setup folder.

Note:

The driver setup folder is:

```
c:\Windows\system32\Setup\Aladdin\eToken\
```

Uninstalling

To remove eToken PKI Client 5.1 SP1, use one of the following methods:

- *Uninstalling via the Add or Remove Programs Option* on page 34
- *Uninstalling via the Wizard* on page 35
- *Uninstalling via the Command Line* on page 38

If the `PROP_CLEAR_REG` property was enabled when eToken PKI Client was installed, all machine and user registry settings are automatically cleared during uninstallation.

Notes:

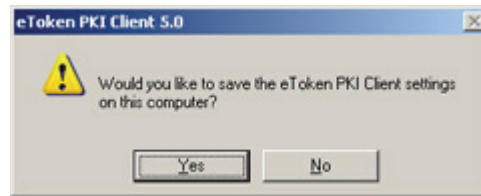
- Uninstalling eToken PKI Client 5.1 SP1 uninstalls the complete eToken PKI Client application, not just the service pack.
 - If a DLL is in use by another application, a *Files in Use* dialog box is displayed. Click **Ignore** to continue the uninstallation, and when the uninstallation completes, restart the computer.
-

Uninstalling via the Add or Remove Programs Option

To uninstall via the Add or Remove Programs option:

1. Go to **Start > Settings > Control Panel**.
2. Double-click **Add or Remove Programs**.

3. Select **eToken PKI Client 5.1 SP1**, and click **Remove**.
4. Follow the instructions to remove the application.
If the PROP_CLEAR_REG property was not enabled during installation, a *Save settings* dialog box is displayed.



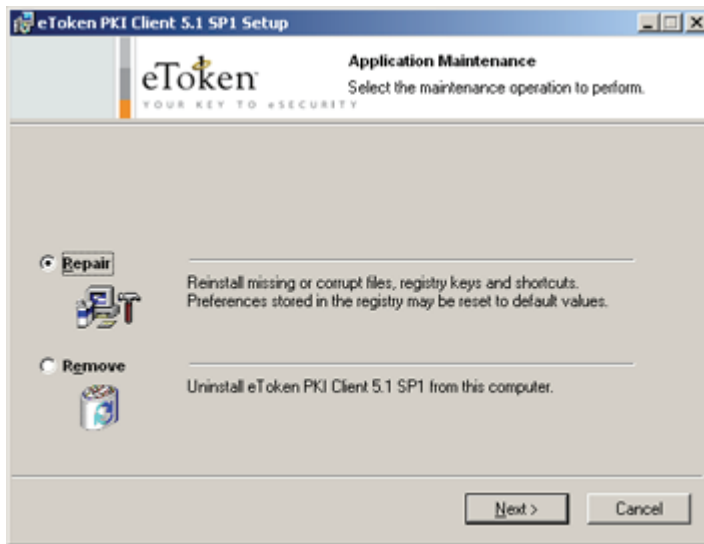
5. Click **Yes** to save the machine and user registry settings, or **No** to delete them.
6. Continue with the uninstallation.
7. When the uninstallation completes, restart the computer.

Uninstalling via the Wizard

To uninstall via the installation wizard:

1. Log on as an administrator.
2. Close all applications.
3. Double-click the appropriate 32- or 64-bit eToken PKI Client 5.1 SP1 `msi` installation or `msp` upgrade file.

The *Application Maintenance* dialog box is displayed.



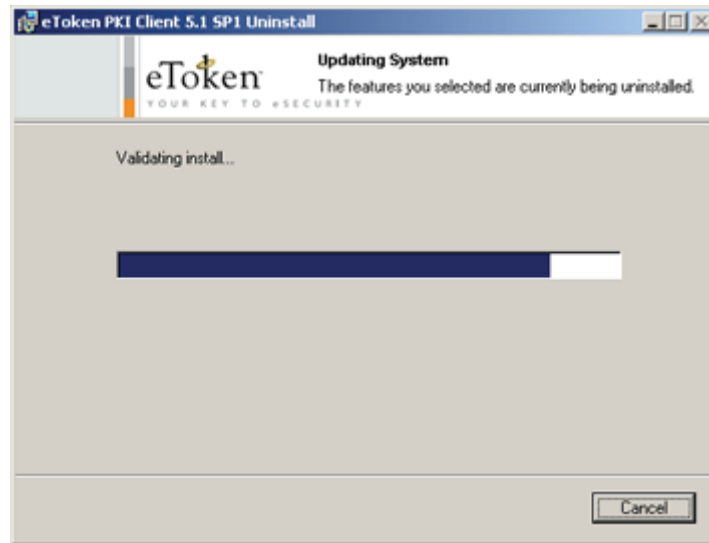
4. Select **Remove**, and click **Next**.

The *eToken PKI Client 5.1 SP1 Uninstall Wizard* opens.

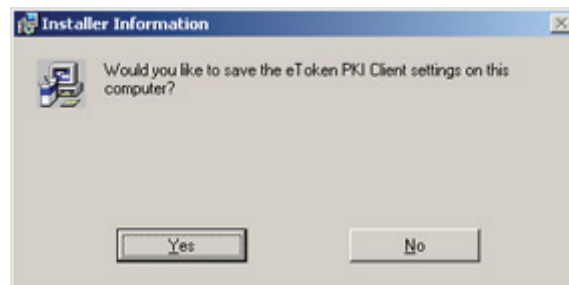


5. Click **Next**.

The *Updating System* dialog box is displayed.



6. If the PROP_CLEAR_REG property was not enabled during installation, a *Save settings* dialog box is displayed.



7. Click **Yes** to save the machine and user registry settings, or **No** to delete them.
8. The uninstallation continues.
9. When the uninstallation completes, click **Finish**, and restart the computer.

Uninstalling via the Command Line

If the PROP_CLEAR_REG property is not enabled, the registry settings are not cleared during uninstallation via the command line.

To uninstall via the command line:

1. Log on as an administrator.
2. Close all applications.
3. Open **Start > Programs > Accessories > Command Prompt**.
When running on Windows Vista, right-click **Command Prompt** and select **Run as**. Set the user to administrator.
4. Type the command line utility:
`msiexec /x PKIClient-x32-5.1-SP1.msi`
where
PKIClient-x32-5.1-SP1.msi is the appropriate 32- or 64-bit eToken PKI Client 5.1 SP1 msi installation or msp upgrade file.
To uninstall in silent mode, add `/q` to the end of the command.
5. When the uninstallation completes, restart the computer.

eToken PKI Client Settings

eToken PKI Client Settings is a snap-in application that enables you to configure certain application features without editing the registry keys directly.

In this chapter:

- [eToken PKI Client Settings Overview](#)
- [Accessing eToken PKI Client Settings in Windows Server Platforms](#)
- [Accessing eToken PKI Client Settings in Windows XP](#)
- [Editing eToken PKI Client Settings](#)
- [Applying eToken PKI Client Settings](#)

eToken PKI Client Settings Overview

eTokenPKIClient_5_1.adm file is a sample file for controlling the eToken PKI Client configuration. It is found in the same directory as this administration guide.

The adm file is used to configure *eToken PKI Client Settings* with one of the following tools:

- In Windows Server platforms: *Active Directory Group Policy Object Editor (GPO)*
- In Windows XP: *Microsoft Management Console (MMC)*

eToken PKI Client Settings determine the eToken PKI Client configuration by setting registry keys.

Note:

See Chapter 7: *Registry Key Tables*, on page 62, for an explanation of the registry key settings.

The sample adm file is configured to write registry settings to:

HKEY_LOCAL_MACHINE\Software\Policies\Aladdin\eToken\MIDDLEWARE.

The values in this folder have a higher priority than values in any other registry folder.

To write settings to a different registry folder, modify the sample adm file.

Note:

See Chapter 7: *Application Properties Hierarchy*, on page 60 for an explanation of the registry folders.

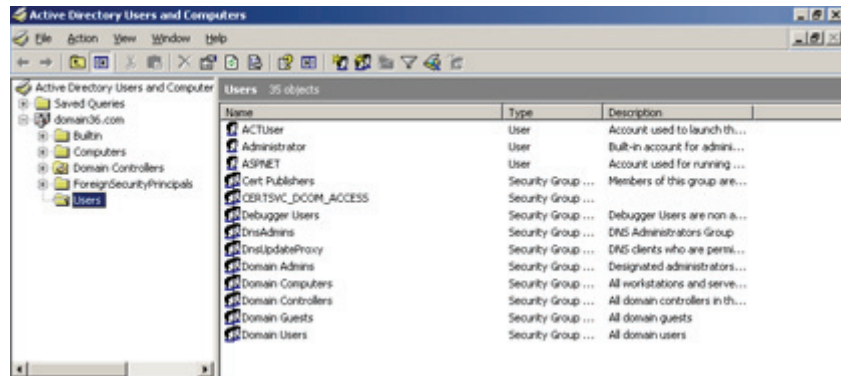
Accessing eToken PKI Client Settings in Windows Server Platforms

Before you can modify *eToken PKI Client Settings*, add the snap-in to the *Group Policy Object Editor*.

Adding eToken PKI Client Settings in Windows Server Platforms

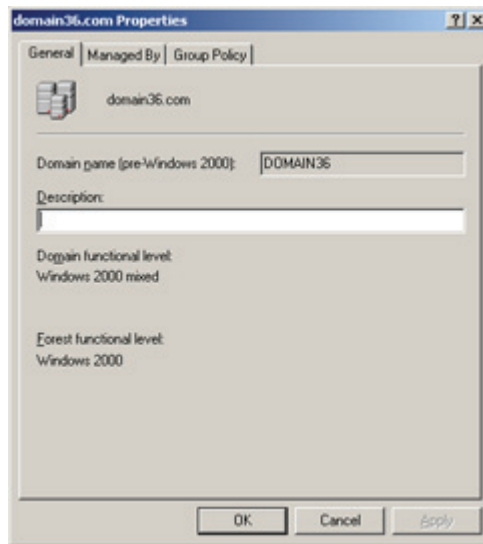
1. Select **Start>Programs>Administrative Tools>Active Directory Users and Computers**.

The *Active Directory Users and Computers* window opens.

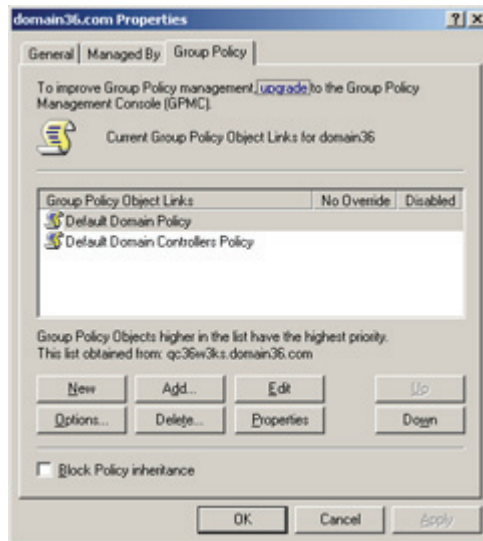


2. Right-click the domain node, and select **Properties**.

The *Properties* window opens.

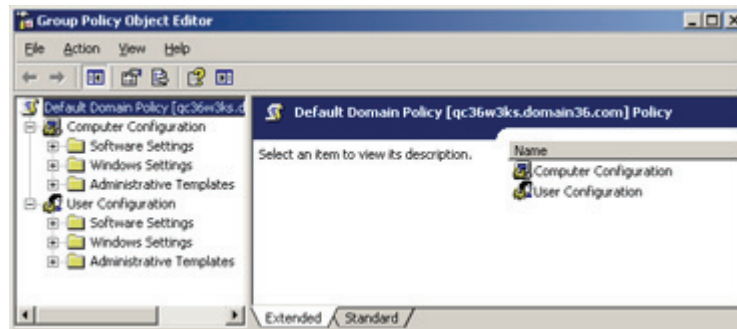


3. Select the *Group Policy* tab.

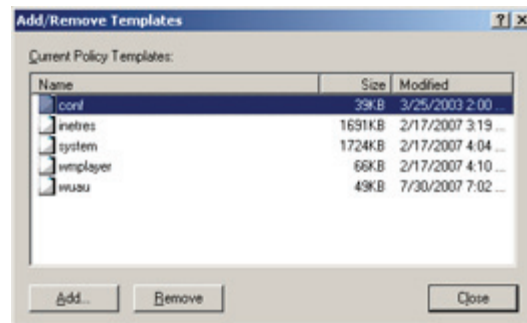


4. Select **Default Domain Policy**, and click **Edit**.

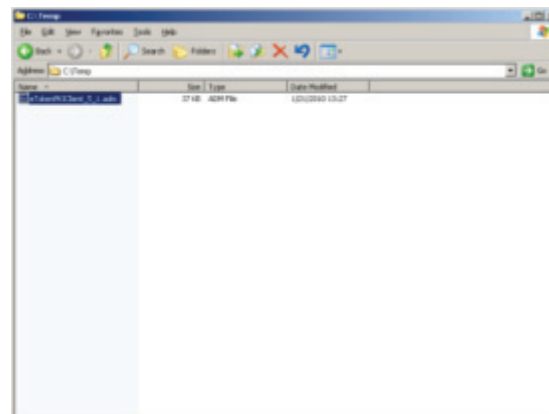
The *Group Policy Object Editor* opens.



5. Under the **Computer Configuration** node, right-click **Administrative Templates**, and select **Add/Remove Templates**. The *Add/Remove Templates* window opens.

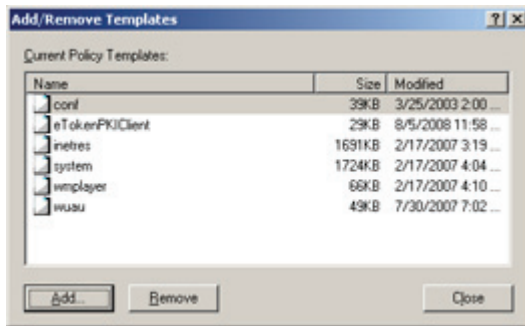


6. Click **Add**, and browse to the `eTokenPKIClient_5_1.adm` file, found in the same directory as this administration guide.



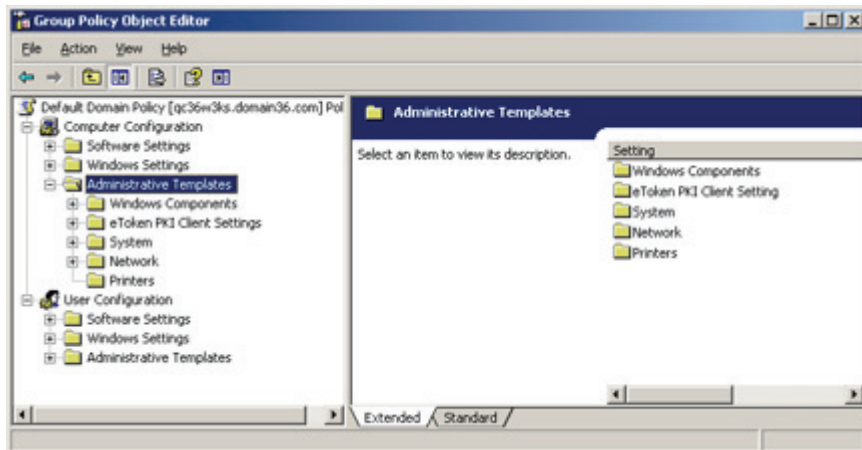
7. Select the file, and click **Open**.

eTokenPKIClient is displayed in the *Add/Remove Templates* window.



8. Click **Close**.

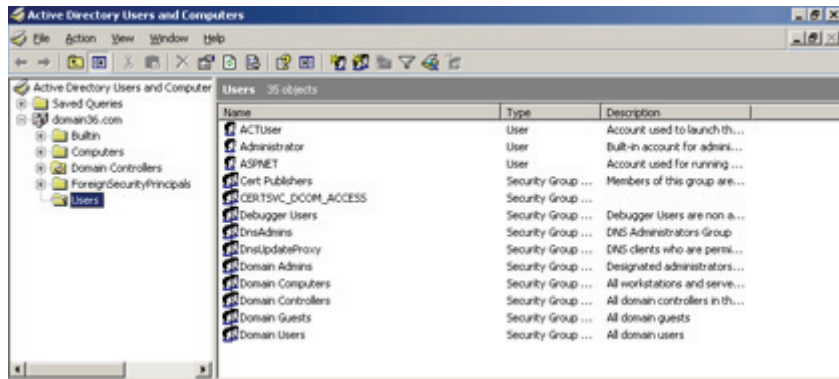
In the *Group Policy Object Editor* window, the *eToken PKI Client Settings* node is added under *Administrative Templates*.



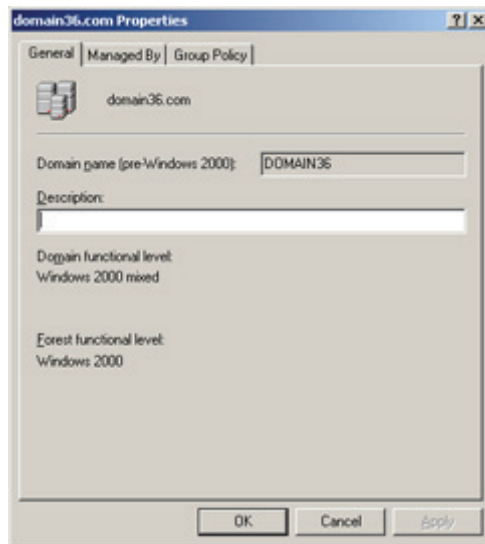
Opening eToken PKI Client Settings in Windows Server Platforms

1. Select **Start>Programs>Administrative Tools>Active Directory Users and Computers**.

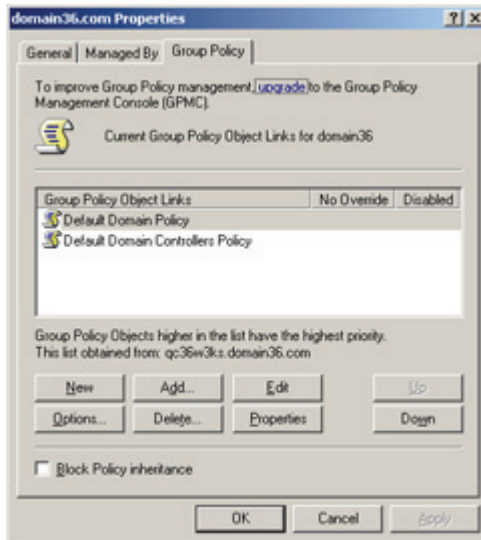
The *Active Directory Users and Computers* window opens.



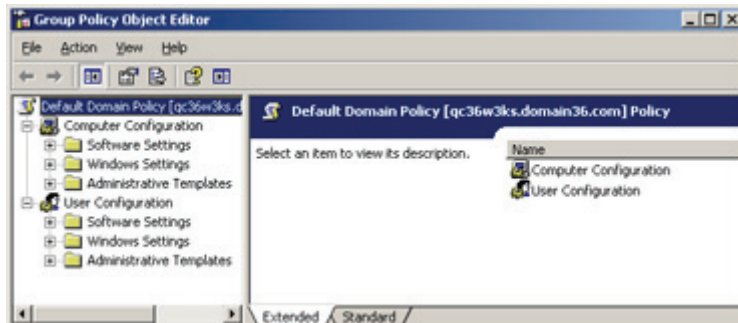
2. Right-click the domain node, and select **Properties**.
The *Properties* window opens.



3. Select the *Group Policy* tab.

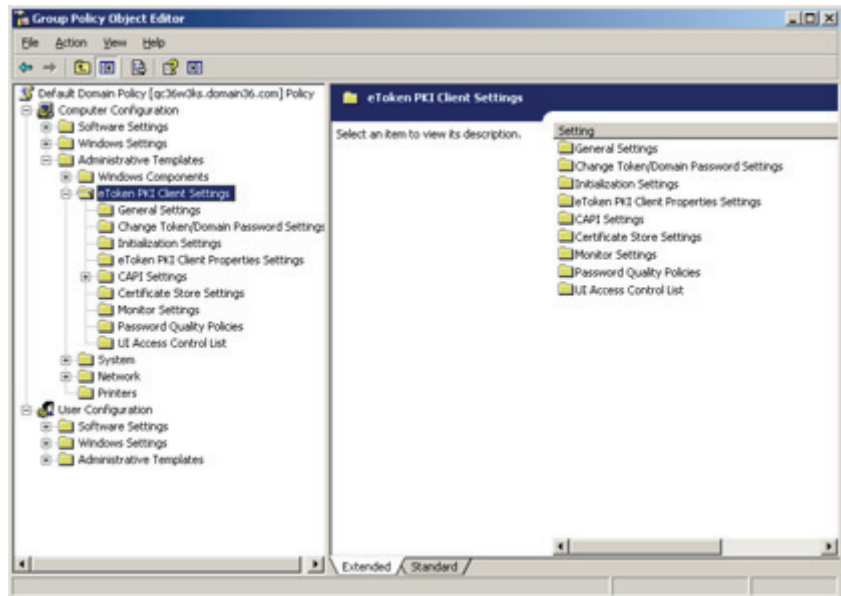


4. Select **Default Domain Policy**, and click **Edit**.
The *Group Policy Object Editor* opens.



5. Navigate to **Computer Configuration>Administrative Templates>eToken PKI Client Settings**.

eToken PKI Client Settings folders are displayed in the right pane.



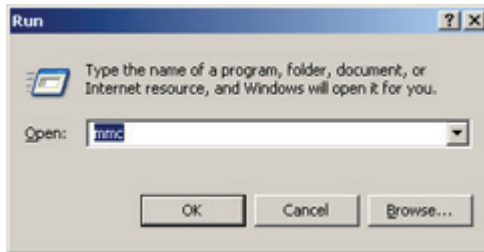
Accessing eToken PKI Client Settings in Windows XP

Before you can modify *eToken PKI Client Settings*, add the snap-in to MMC.

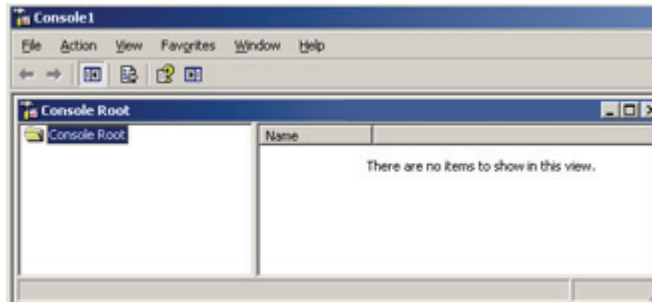
Adding eToken PKI Client Settings in Windows XP

To add eToken PKI Client Settings to MMC:

1. Select **Start>Run**, and in the command line, enter MMC.

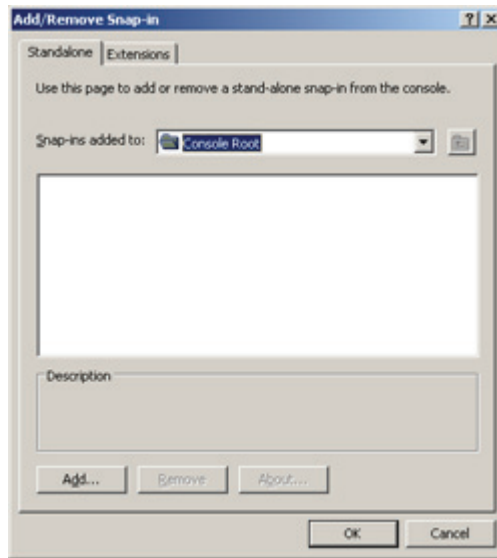


2. Click **OK**.
The *Console* window opens.



3. Select **File>Add/Remove Snap-in**.

The *Add/Remove Snap-in* window opens.



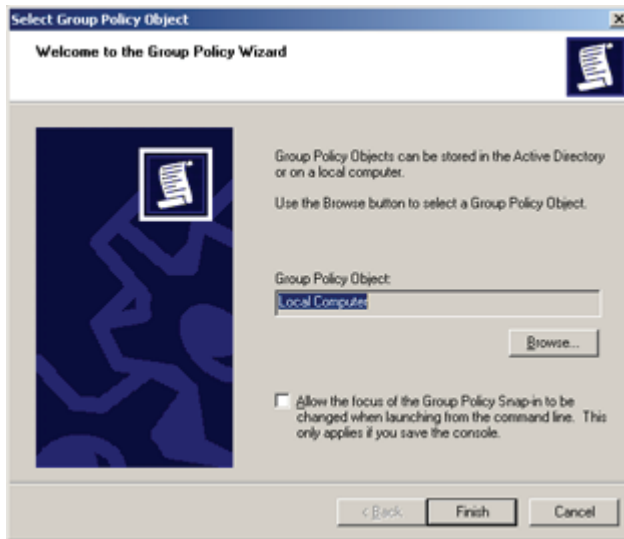
4. Click **Add**.

The *Add Standalone Snap-in* window opens.

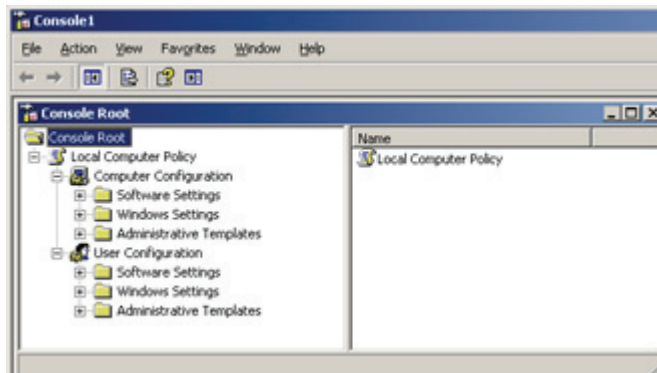


5. Select **Group Policy Object Editor**, and click **Add**.

The *Group Policy Wizard* opens.

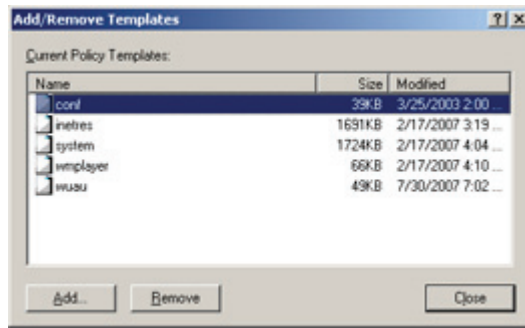


6. Accept **Local Computer** (default) to save the *Group Policy Object* to the local computer, or click the **Browse** button to select a different location.
7. Click **Finish** to close the *Group Policy Wizard*.
8. Click **Close** to close the *Add Standalone Snap-in* window.
The *Console Root* now contains the selected policy object.

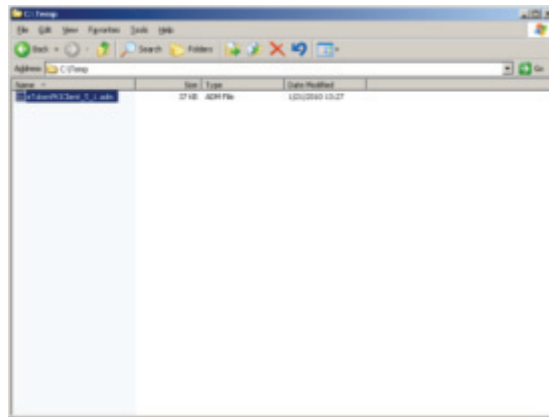


9. Under the **Computer Configuration** node, right-click **Administrative Templates**, and select **Add/Remove Templates**.

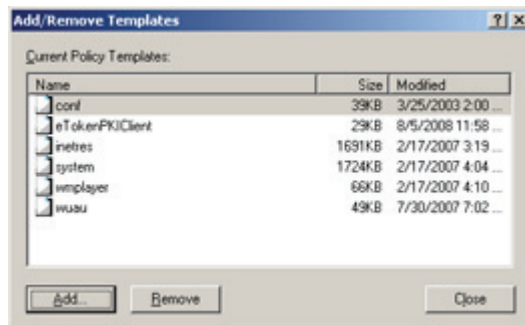
The *Add/Remove Templates* window opens.



10. Click **Add**, and browse to `eTokenPKIClient_5_1.adm` file, found in the same directory as this administration guide.

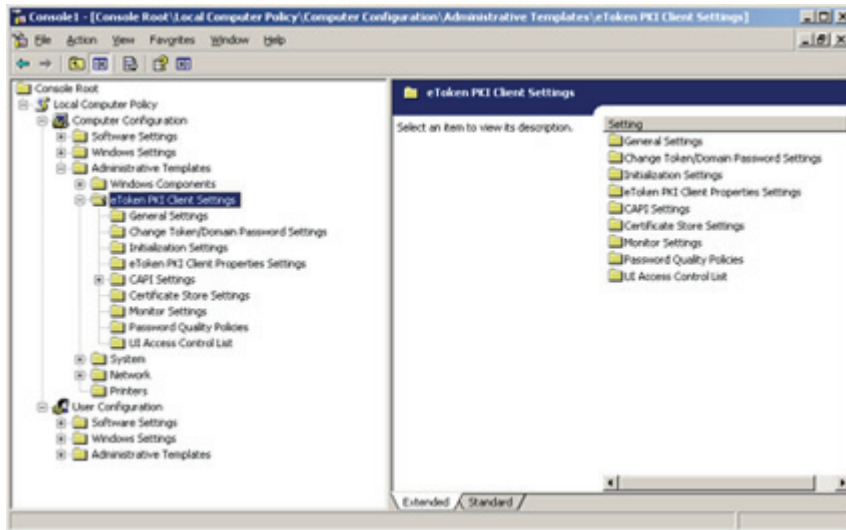


11. Select the file, and click **Open**.
eTokenPKIClient is displayed in the *Add/Remove Templates* window.

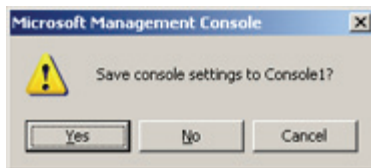


12. Click **Close**.

In the *Console Root* window, the *eToken PKI Client Settings* node is added under *Administrative Templates*.



13. When you close the *Console* window, you are prompted to save the file.



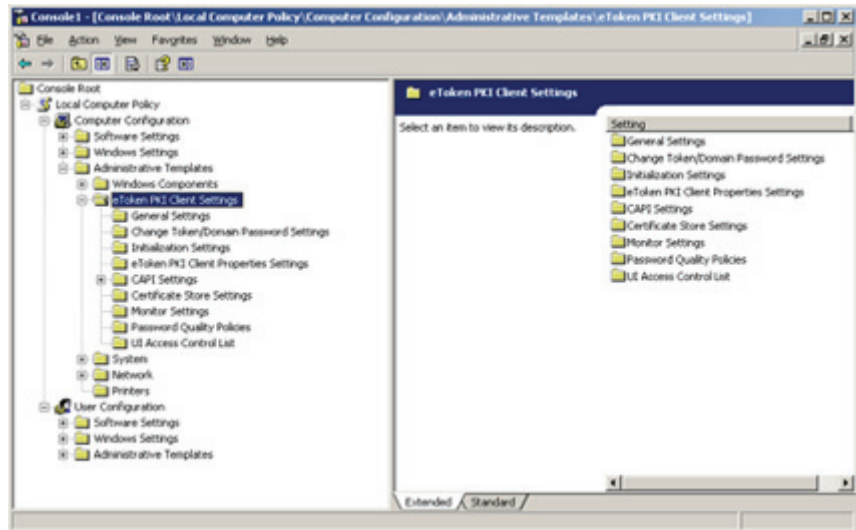
14. Click **Yes**.
15. Enter a file name, and save the `.msc` file.

Opening eToken PKI Client Settings in Windows XP

To open *eToken PKI Client Settings*:

1. Select **Start>Run**, and in the command line, enter MMC.
2. Click **OK**.
The *Console* window opens.
3. Select **File>Open**, and browse to the console `.msc` file that you saved in *Adding eToken PKI Client Settings in Windows XP*, step 15, on page 52.

4. Navigate to **Computer Configuration>Administrative Templates>eToken PKI Client Settings**.
eToken PKI Client Settings folders are displayed in the right pane.



Editing eToken PKI Client Settings

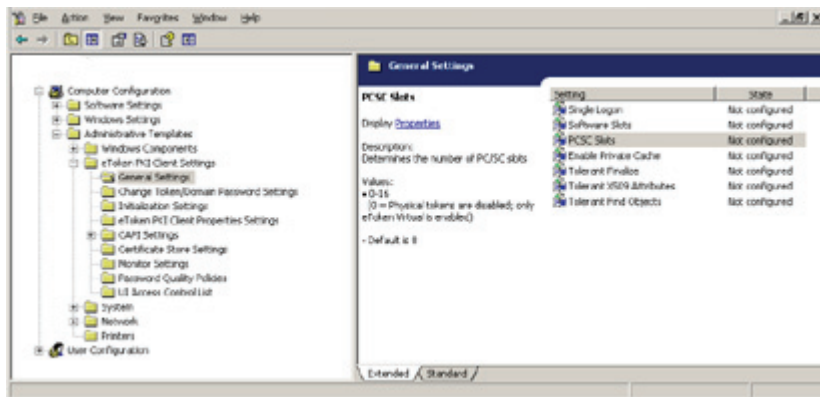
Each *eToken PKI Client Settings* folder contains settings that can be configured to have priority over the eToken PKI Client application's defaults.

For the description of each setting, see Chapter 7: *Registry Key Tables*, on page 62, or read the description displayed on each setting's *Explain* tab.

To edit eToken PKI Client Settings:

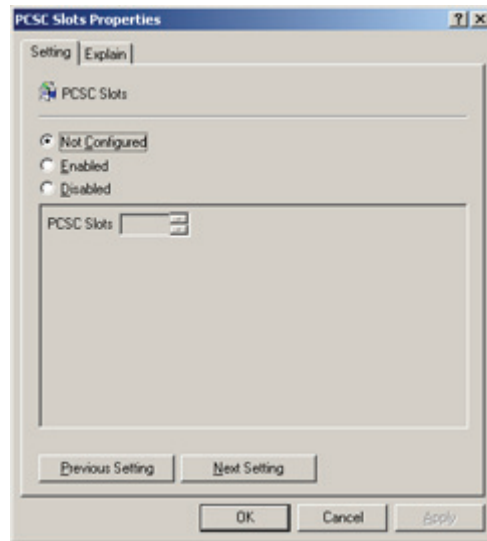
1. Open the *eToken PKI Client Settings* window.
See *Opening eToken PKI Client Settings in Windows Server Platforms* on page 44 or *Opening eToken PKI Client Settings in Windows XP* on page 52.
2. Under **Computer Configuration**>**Administrative Templates**>**eToken PKI Client Settings**, select the settings folder to edit.

The settings are displayed in the right pane.

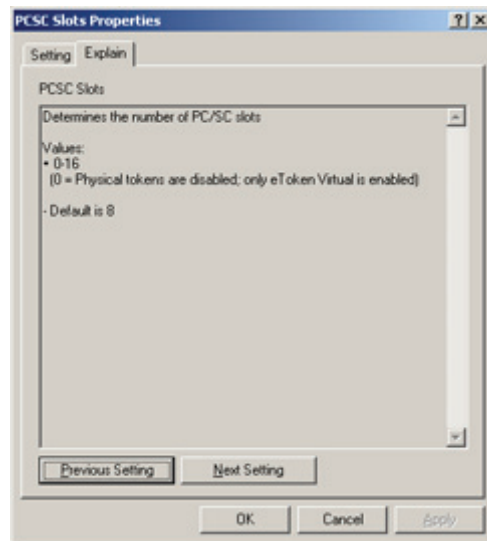


3. Double-click a setting to edit it.

In this example, the *PCSC Slots* setting is selected.



4. Select the *Explain* tab for an explanation of the setting and its values.



-
5. In the *Setting* tab, select one of the following:
 - ◆ **Not Configured:** the policy is inherited; if there is no policy to inherit, the application default is applied
 - ◆ **Enabled:** enables input into property value fields, and marks the registry key as Enabled
 - ◆ **Disabled:** the application default is always applied

For further information about `adm` file policy settings, see Microsoft documentation.
 6. If you select **Enabled**, enter the required value(s) in the box.
 7. Click **Previous Setting** or **Next Setting** to progress through the settings in the same folder, or click **OK** to return to the list of settings in the folder.

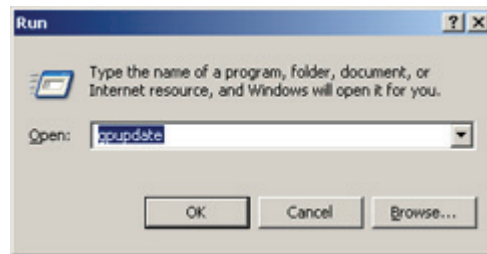
Applying eToken PKI Client Settings

After using the *Group Policy Object Editor* to edit *eToken PKI Client Settings* on the server, do the following:

1. Update the registry settings on the server.
2. Update the registry settings on all client computers on which eToken PKI Client is installed.

To apply eToken PKI Client Settings:

1. On the server, select **Start>Run**, and in the command line, enter gpupdate.



2. Click **OK**.
The registry values on the server are updated to the *eToken PKI Client Settings* values.
3. On each client computer, select **Start>Run**, and in the command line, enter gpupdate.
4. Click **OK**.
The registry values are copied from the server to the client computer.

Properties and Configuration

The administrator can override the application's default behavior by assigning values to specific properties. Most eToken PKI Client properties are stored as registry key values.

In this chapter:

- [Overview of Application Properties](#)
- [Application Properties Hierarchy](#)
- [Setting Registry Keys Manually](#)
- [Registry Key Tables](#)

Overview of Application Properties

Properties and registry key values can be added and changed to determine the eToken PKI Client application's behavior. Depending on the property, values can be set using at least one of the following methods:

- Define the property during command line installation of eToken PKI Client (but not during repair).
See Chapter 5:*Limiting and Adding Installation Features via the Command Line*, on page 30.
The property name, and not the registry key name, is used when setting the value during command line installation.
- Set a value using the eToken Properties application.
See the *eToken PKI Client User's Guide*.
Neither the registry key name, nor the property name, is needed.

Note:

Values set using the eToken Properties application are saved on a per user basis in `HKEY_CURRENT_USER`, and not in `HKEY_LOCAL_MACHINE`.

-
- Set a value using the eToken PKI Client Settings snap-in application.
See Chapter 6:*eToken PKI Client Settings*, on page 39.
The registry key name, and not the property name, is used when setting the value.
 - Manually edit the registry setting.
See *Setting Registry Keys Manually* on page 61.
The registry key name, and not the property name, is used when setting the value.

Application Properties Hierarchy

Each property can be defined in up to four registry key folders. If a property is set in a folder which requires administrator permissions, that setting overrides any other settings for that property.

For each property, the setting found in the highest level of the following hierarchy determines the application's behavior:

1. HKEY_LOCAL_MACHINE\Software\Policies\Aladdin\ eToken\MIDDLEWARE
Requires administrator permissions
2. HKEY_CURRENT_USER\Software\Policies\Aladdin\ eToken\MIDDLEWARE
Requires administrator permissions
3. HKEY_CURRENT_USER\Software\Aladdin\eToken\MIDDLEWARE
Does not requires administrator permissions
4. HKEY_LOCAL_MACHINE\Software\Aladdin\eToken\MIDDLEWARE
Does not requires administrator permissions
5. eToken PKI Client default value

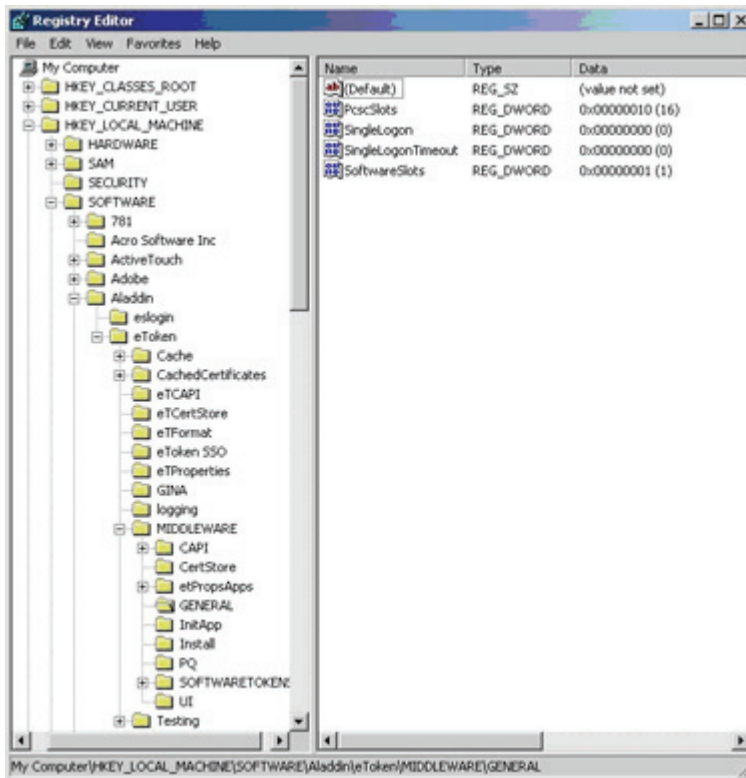
Setting Registry Keys Manually

To set a registry key:

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

The registry key name, and not the property name, is used when setting the value manually.

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



Registry settings that are not displayed in the right pane can be added.

Registry Key Tables

All registry keys can be set manually.

See the *Setting Registry Keys Manually* section on page 61.

All registry keys can be set using the *eToken PKI Client Settings* snap-in application.

See Chapter 6:*eToken PKI Client Settings*, on page 39.

If a Property Name is defined in the table, the property can be set during the eToken PKI Client 5.1 SP1 command line installation. See the *Setting Application Properties via the Command Line* section on page 26.

Note:

The location of the registry keys described in this section is: HKEY_LOCAL_MACHINE \ SOFTWARE \ Aladdin \ eToken \ MIDDLEWARE.

General Registry Key

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

Emulate Connected Virtual Reader

Property Name	(Cannot be set by command line installation)
Registry Key Name	EmulateConnectedVR
Description	Determines if the most recently connected eToken Virtual on the disk emulates a smartcard whose readername is "Aks VR 0"; Relevant only for Windows XP
DWORD Value	1 (True) - The most recently connected eToken Virtual emulates a smartcard 0 (False) - The eToken Virtual does not emulate a smartcard
Default	0 (False)

Note:

Regardless of the **Emulate Connected Virtual Reader** setting, the most recently connected eToken Virtual always emulates a smartcard if it is on a USB flash device.

Enable Private Cache

Property Name	(Cannot be set by command line installation)
Registry Key Name	EnablePrvCache
Description	<p>Determines if eToken PKI Client is enabled to cache private data in per process memory</p> <p>If enabled, private data is cached if one of the following conditions is met:</p> <ul style="list-style-type: none"> ■ The token was initialized with the private data caching option ■ The PrivateDataCaching registry key is not set to 0 See Private Data Caching on page 70
DWORD Value	<p>1 (True) - Private data caching is enabled</p> <p>0 (False) - Private data caching is disabled</p>
Default	1 (True)
Can be set by	<ul style="list-style-type: none"> ■ eToken Properties application

PCSC Slots

Property Name	PROP_PCSCSLOTS
Registry Key Name	PcscSlots
Description	Determines the number of PC/SC slots
DWORD Value	<p>0-16</p> <p>0 = Physical tokens are disabled; only eToken Virtual is enabled</p>
Default	8
Can be set by	<ul style="list-style-type: none"> ■ Command line installation

Single Logon

Property Name	PROP_SINGLELOGON
Registry Key Name	SingleLogon
Description	Determines if the user password is requested only once by the eToken Properties application
DWORD Value	1 (True) - User password is requested only once 0 (False) - User password is requested as needed
Default	0 (False)
Can be set by	<ul style="list-style-type: none"> ■ Command line installation ■ eToken Properties application

Note:

If **Single Logon Timeout** is > 0, **Single Logon** is automatically set to 1.

Single Logon Timeout

Property Name	PROP_SINGLELOGONTO
Registry Key Name	SingleLogonTimeout
Description	Determines the timeout, in seconds, of Single Logon
DWORD Value	>=0
Default	0 (no timeout)
Can be set by	<ul style="list-style-type: none"> ■ Command line installation

Software Slots

Property Name	PROP_SOFTWARESLOTS
Registry Key Name	SoftwareSlots
Description	Determines the number of software slots
DWORD Value	0-10 0 = eToken Virtual use is disabled; only physical tokens are enabled
Default	2
Can be set by	<ul style="list-style-type: none">■ Command line installation■ eToken Properties application

Tolerant Finalize

Property Name	(Cannot be set by command line installation)
Registry Key Name	TolerantFinalize
Description	Determines if C_Finalize can be called by DllMain Define this property per process
DWORD Value	1 (True) - C_Finalize can be called by DllMain 0 (False) - C_Finalize cannot be called by DllMain
Default	0 (False)

Note:

Enable **TolerantFinalize** when using Novell Modular Authentication Service (NMAS) applications only.

Tolerant Find Objects

Property Name	(Cannot be set by command line installation)
Registry Key Name	TolerantFindObjects
Description	Determines if PKCS#11 tolerates a <code>Find</code> function with an invalid template, returning an empty list instead of an error
DWORD Value	1 (True) - A <code>Find</code> function with an invalid template is tolerated and returns an empty list 0 (False) - A <code>Find</code> function with an invalid template is not tolerated and returns an error
Default	0 (False)

Tolerant X509 Attributes

Property Name	(Cannot be set by command line installation)
Registry Key Name	TolerantX509Attributes
Description	Determines if <code>CKA_SERIAL_NUMBER</code> , <code>CKA_SUBJECT</code> , and <code>CKA_ISSUER</code> attributes can differ from those in <code>CKA_VALUE</code> during certificate creation
DWORD Value	1 (True) - The attributes can differ 0 (False) - Check that the values match
Default	1 (True)

Notes:

- Ensure that **TolerantX509Attributes** is `True` when using certificates created in a non- DER-encoded binary x.509 format.
- In some earlier eToken PKI Client versions, **TolerantX509Attributes** was `False` by default.

eToken Virtual Disconnected when Logging Off

Registry Key Name	EtvLogoffUnplug
Description	Determines if an eToken Virtual is disconnected when logging off
DWORD Value	1 (true) - Disconnect the eToken Virtual when logging off 0 (false)- Do not disconnect the eToken Virtual when logging off
Default	Does not exist

Protect Symmetric Keys

Registry Key Name	SensitiveSecret
Description	Determines if symmetric keys are protected Note: If True, symmetric keys cannot be extracted, even non-sensitive keys
DWORD Value	1 (true) - Symmetric keys cannot be extracted 0 (false)- Symmetric keys can be extracted
Default	0 (False)

SyncPin Registry Key

The following properties are saved as registry settings in the **SyncPin** registry key.

Domain

Property Name	(Cannot be set by command line installation)
Registry Key Name	Domain
Description	Determines if synchronization is enabled between the eToken Password and the domain password
String Value	Name of the domain (written without a suffix) whose password is synchronized with the eToken Password None - Password synchronization is not enabled
Default	None

Init Registry Key

The following properties are saved as registry settings in the **Init** registry key.

HMAC-SHA1

Property Name	(Cannot be set by command line installation)
Registry Key Name	HMAC-SHA1
Description	Determines if the 'Load OTP Support' option, required by OTP tokens, is enabled
DWORD Value	1 (True) - HMAC-SHA1 support is enabled 0 (False)- HMAC-SHA1 support is disabled
Default	1 (True) for OTP tokens 0 (False) for other tokens
Can be set by	■ eToken Properties application

Legacy Format Version

Property Name	(Cannot be set by command line installation)
Registry Key Name	Legacy-Format-Version
Description	Determines the token format during initialization
DWORD Value	0 - Tokens are formatted as backwardly compatible (CardOS) 4 - Tokens are not formatted as backwardly compatible (CardOS) 5 - Format includes new RSA behavior that is not controlled by key size. Each key is created in a separate directory (CardOS 4.20 FIPS or Java Card-based).
Default	4
Can be set by	■ eToken Properties application

Private Data Caching

Property Name	(Cannot be set by command line installation)
Registry Key Name	PrivateDataCaching
Description	If EnablePrvCache is true, determines if private data is cached See Enable Private Cache on page 64
DWORD Value	0 - Private data is not cached 1 - Private data is cached when the token is logged on, and erased when the token is logged off 2 - Private data is cached and saved
Default	2 (Full caching)
Can be set by	<ul style="list-style-type: none"> ■ eToken Properties application

RSA Area Size

Property Name	(Cannot be set by command line installation)
Registry Key Name	RSA-Area-Size
Description	Determines the size, in bytes, of the area to reserve for RSA keys on CardOS-based tokens. The size of the area allocated on the token is determined during token initialization, and cannot be modified without re-initializing the token.
DWORD Value	>=0 0 = RSA keys cannot be created on the token
Default	Depending on the token size: <ul style="list-style-type: none"> ■ For 16K tokens, enough bytes for three 1024-bits keys ■ For 32K tokens, enough bytes for five 1024-bits keys ■ For larger tokens, enough bytes for seven 1024-bits keys

Note:

RSA-Area-Size is not relevant when **Legacy-Format-Version** is set to 5.

For information regarding the size of the RSA key space, see the eToken Knowledge Base article, *Reserved RSA Key Space*.

RSA Secondary Authentication Mode

Property Name	(Cannot be set by command line installation)
Registry Key Name	RSASecondaryAuthenticationMode
Description	Determines how RSA private keys are created
DWORD Value	<p>0 - ETCK_2NDAUTH_PROMPT_NEVER New RSA private keys are not protected by an additional password</p> <p>1 - ETCK_2NDAUTH_PROMPT_CONDITIONAL</p> <ul style="list-style-type: none"> ■ If an external application has set the CKA_ALWAYS_AUTHENTICATE attribute to true, new RSA private keys are protected by an additional password ■ If the attribute has not been set, a prompt appears asking if a new RSA private key is to be protected by an additional password <p>2 - ETCK_2NDAUTH_PROMPT_ALWAYS A prompt appears asking if a new RSA private key is to be protected by an additional password</p> <p>3 - ETCK_2NDAUTH_MANDATORY New RSA private keys must be protected by an additional password</p>
Default	3
Can be set by	<ul style="list-style-type: none"> ■ eToken Properties application

RSA-2048

Property Name	(Cannot be set by command line installation)
Registry Key Name	RSA-2048
Description	Determines if the 'RSA-2048 Support' option is enabled
DWORD Value	<p>1 (True) - RSA-2048 support is enabled</p> <p>0 (False) - RSA-2048 support is disabled</p>
Default	0 (False)
Can be set by	<ul style="list-style-type: none"> ■ eToken Properties application

InitApp Registry Key

The following properties are saved as registry settings in the **InitApp** registry key.

Advanced View

Property Name	PROP_ADVANCED_VIEW
Registry Key Name	AdvancedView
Description	Determines if the <i>Advanced</i> button is enabled in the eToken Properties application
DWORD Value	1 (True) - The button is enabled 0 (False)- The button is disabled
Default	1 (True)
Can be set by	■ Command line installation

Show Tray Icon

Property Name	(Cannot be set by command line installation)
Registry Key Name	ShowInTray
Description	Determines if the eToken PKI Client tray icon is displayed when eToken PKI Client is launched
DWORD Value	1 (True) - The tray icon is displayed 0 (False)- The tray icon is not displayed
Default	1 (True)

CAPI Registry Key

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

Logout Mode

Property Name	(Cannot be set by command line installation)
Registry Key Name	LogoutMode
Description	Determines if the user is prompted to enter a password for each operation requiring the user to be logged on
DWORD Value	1 (True) - A password prompt is displayed each time 0 (False)- A password prompt is not displayed each time
Default	0 (False)

No Default Key Container

This property is relevant for the `scrdenrl.dll` ActiveX control that is responsible for the "enrollment on behalf" feature when using Internet Explorer. This ActiveX control is used by the Microsoft CA website and the eToken TMS Management Center.

Property Name	PROP_EXPLORER_DEFENROL
Registry Key Name	NoDefaultKeyContainer (DefEnrollType in previous versions)
Description	Determines if an enrollment certificate from the Microsoft CA service is downloaded to use for creating a user certificate
DWORD Value	1 (True) - A Microsoft CA service enrollment certificate is downloaded 0 (False)- A Microsoft CA service enrollment certificate is not downloaded
Default	1 (True) for the Internet Explorer process 0 (False) otherwise
Can be set by	■ Command line installation

Note:

The NoDefaultKeyContainer value is set per process on a per machine basis.

Default Enrollment Container

Registry Key Name	DefEnrollType
Description	Determines if the Enrollment Container is used instead of the Default Container
DWORD Value	1 (true) - During "enrollment on behalf", the Enrollment Container (the last container where the certificate with Enrollment Agent key usage has been stored) is set as the default. 0 (false) - The Default Container (the last container where the certificate with Smartcard Logon key usage has been stored) is set as the default.
Default	Does not exist

Password Timeout

Property Name	(Cannot be set by command line installation)
Registry Key Name	PasswordTimeout
Description	Determines the number of minutes the CAPI UI-required password is valid
DWORD Value	>=0 0 = No timeout
Default	0

ASCII Password

eToken PKI Client uses UTF-8 format to encode eToken Passwords. Some applications, such as Microsoft's smartcard logon, use code page encoding and not UTF-8. Non-ASCII characters are represented differently in each of these encoding formats.

To correctly interpret smartcard passwords containing non-ASCII characters, such as ç, from code page format, set the **AsciiPassword** property to `True`.

Property Name	(Cannot be set by command line installation)
Registry Key Name	AsciiPassword
Description	Determines if non-ASCII characters are supported in eToken Passwords, enabling a string containing non-ASCII characters to be used as a smartcard logon password
DWORD Value	1 (True) - Non-ASCII character are supported 0 (False)- Only ASCII characters are supported
Default	0 (False)

Certificate Store Registry Key

The following properties are saved as registry settings in the **CertStore** registry key.

Add to Token upon New Certificate in Store

Property Name	(Cannot be set by command line installation)
Registry Key Name	AddToTokenOnNewCertInStore
Description	Determines if an option is displayed to import the certificate to the selected token when a new certificate with exportable keys is added to the user store
DWORD Value	1 (True) - An option is displayed to import a new certificate 0 (False)- An option is not displayed to import a new certificate
Default	1 (True)

Certificates to Remove Storage Period

Property Name	(Cannot be set by command line installation)
Registry Key Name	CertsToRemoveStorePeriod
Description	Determines the number of days to attempt to remove certificates from a token that is not connected; Relevant only when the registry setting RemoveFromTokenOnRemoveFromStore is set to 1 or 2
DWORD Value	>=0
Default	7

Note:

This setting applies when a certificate is removed from the user store when the token from which it was exported is not connected.

Propagate CA Certificates

Property Name	PROP_PROPAGATECACER
Registry Key Name	PropagateCACertificates
Description	Determines if all CA certificates on the token are exported to the Trusted CA store
DWORD Value	1 (True) - CA certificates are exported to the Trusted CA store 0 (False)- CA certificates are not exported to the Trusted CA store
Default	1 (True)
Can be set by	<ul style="list-style-type: none"> ■ Command line installation ■ eToken Properties application

Propagate User Certificates

Property Name	PROP_PROPAGATEUSERCER
Registry Key Name	PropagateUserCertificates
Description	Determines if all user certificates on the token are exported to the user store
DWORD Value	1 (True) - User certificates are exported to the user store 0 (False)- User certificates are not exported to the user store
Default	1 (True)
Can be set by	<ul style="list-style-type: none"> ■ Command line installation ■ eToken Properties application

Remove from Store upon Removal from Token

Property Name	(Cannot be set by command line installation)
Registry Key Name	RemoveFromStoreOnRemoveFromToken
Description	Determines if a certificate is removed from the user store when that certificate is removed from the token
DWORD Value	1 (True) - The certificate is removed from the user store 0 (False)- The certificate is not removed from the user store
Default	1 (True)

Remove from Token upon Removal from Store

Property Name	(Cannot be set by command line installation)
Registry Key Name	RemoveFromTokenOnRemoveFromStore
Description	Determines if an option is displayed to remove the certificate from the token when that certificate is removed from the user store
DWORD Value	0 - Never; an option is not displayed to remove the certificate 1 - Always; an option is displayed to remove the certificate 2 - An option is displayed to remove only those certificates whose templates are listed in the registry setting RemoveFromTokenOnRemoveFromStoreTemplates
Default	0

Remove from Token upon Removal from Store Templates

Property Name	(Cannot be set by command line installation)
Registry Key Name	RemoveFromTokenOnRemoveFromStoreTemplates
Description	Lists the templates of the certificates to be removed from the token when the certificates are removed from the user store; Relevant only when the registry setting RemoveFromTokenOnRemoveFromStore is set to 2
String Value	Template name(s)
Default	None

Remove User Certificates upon Token Removal

Property Name	(Cannot be set by command line installation)
Registry Key Name	RemoveUserCertsOnTokenRemove
Description	Determines if user certificates are removed from the user store when the token from which they were exported is removed. Not limited to the selected token.
DWORD Value	1 (True) - User certificates are removed from the user store 0 (False)- User certificates are not removed from the user store
Default	1 (True)

Synchronize Store

Property Name	(Cannot be set by command line installation)
Registry Key Name	SynchronizeStore
Description	Determines if store synchronization is enabled
DWORD Value	1 (True) - Store synchronization is enabled 0 (False)- Store synchronization is disabled
Default	1 (True)

Monitor Registry Key

The following properties are saved as registry settings in the **Monitor** registry key.

Notify Password Expiration

Property Name	(Cannot be set by command line installation)
Registry Key Name	NotifyPasswordExpiration
Description	Determines if the user is notified by a pop-up message in the system tray when the connected token's eToken Password is about to expire
DWORD Value	1 (True) - Notify the user 0 (False)- Do not notify the user
Default	1 (True)

Password Policies Registry Key

The following properties are saved as registry settings in the **PQ** registry key.

Password Quality History Size

Property Name	PROP_PQ_HISTORYSIZE
Registry Key Name	pqHistorySize
Description	Determines the number of recent passwords that may not be repeated
DWORD Value	>=0
Default	10
Can be set by	<ul style="list-style-type: none"> ■ Command line installation ■ eToken Properties application

Password Quality Include Lower-Case

Property Name	(Cannot be set by command line installation)
Registry Key Name	pqLowerCase
Description	Determines if the password may include lower-case characters
DWORD Value	0 - Lower-case characters are permitted 1 - Lower-case characters are forbidden 2 - Lower-case characters are mandatory
Default	0

Password Quality Expiry Period

Property Name	PROP_PQ_MAXAGE
Registry Key Name	pqMaxAge
Description	Determines the maximum number of days a password is valid
DWORD Value	>=0 0 = No expiration
Default	0
Can be set by	<ul style="list-style-type: none"> ■ Command line installation ■ eToken Properties application

Password Quality Maximum Repeated

Property Name	(Cannot be set by command line installation)
Registry Key Name	pqMaxRepeated
Description	Determines the maximum number of times each character can be repeated in a password
DWORD Value	>=0 0 = No maximum
Default	3

Password Quality Minimum Period

Property Name	PROP_PQ_MINAGE
Registry Key Name	pqMinAge
Description	Determines the minimum number of days required before a password change
DWORD Value	>=0 0 = No minimum
Default	0
Can be set by	<ul style="list-style-type: none"> ■ Command line installation ■ eToken Properties application

Password Quality Minimum Length

Property Name	PROP_PQ_MINLEN
Registry Key Name	pqMinLen
Description	Determines the minimum password length
DWORD Value	>=4
Default	6
Can be set by	<ul style="list-style-type: none"> ■ Command line installation ■ eToken Properties application

Password Quality Force Mixed Characters

Property Name	PROP_PQ_MIXCHARS
Registry Key Name	pqMixChars
Description	Determines if complexity requirements are enforced, requiring mixed characters in a password. The characters to mix are: upper-case letters, lower-case letters, numbers, and special characters
DWORD Value	1 (True) - Mixed characters are automatically required because the standard complexity requirements are enforced 0 (False)- Mixed characters are not automatically required because the manual complexity requirements are enforced
Default	1 (True)
Can be set by	<ul style="list-style-type: none"> ■ Command line installation ■ eToken Properties application

Password Quality Modifiable

Property Name	(Cannot be set by command line installation)
Registry Key Name	pqModifiable
Description	Determines if the password policy on a newly initialized token can be modified by the owner. See the pqOwner registry key.
DWORD Value	1 (True) - The password policy can be modified by the owner 0 (False)- The password policy cannot be modified by the owner
Default	1 (True) for administrator-owned tokens 0 (False) for user-owned tokens

Password Quality Include Numbers

Property Name	(Cannot be set by command line installation)
Registry Key Name	pqNumbers
Description	Determines if the password may include numbers
DWORD Value	0 - Numbers are permitted 1 - Numbers are forbidden 2 - Numbers are mandatory
Default	0

Password Quality Owner

Property Name	(Cannot be set by command line installation)
Registry Key Name	pqOwner
Description	Determines the owner of the password policy on a newly initialized token; used to determine the default of the pqModifiable registry key
DWORD Value	0 - The owner of the password policy is an administrator 1 - The owner of the password policy is a user
Default	0 (Administrator) if the token has an Administrator Password 1 (User) if the token does not have an Administrator Password

Password Quality Include Special Characters

Property Name	(Cannot be set by command line installation)
Registry Key Name	pqSpecial
Description	Determines if the password may include special characters, such as @, !, &
DWORD Value	0 - Special characters are permitted 1 - Special characters are forbidden 2 - Special characters are mandatory
Default	0

Password Quality Include Upper-Case

Property Name	(Cannot be set by command line installation)
Registry Key Name	pqUpperCase
Description	Determines if the password may include upper-case characters
DWORD Value	0 - Upper-case characters are permitted 1 - Upper-case characters are forbidden 2 - Upper-case characters are mandatory
Default	0

Password Quality Expiration Warning Period

Property Name	PROP_PQ_WARNPERIOD
Registry Key Name	pqWarnPeriod
Description	Determines the number of days before expiration during which a warning is displayed
DWORD Value	>=0 0 = No warning
Default	0
Can be set by	<ul style="list-style-type: none">■ Command line installation■ eToken Properties application

Password Quality Check on Initialization

Property Name	(Cannot be set by command line installation)
Registry Key Name	ppCheckInit
Description	<p>Determines if the eToken Password quality is checked and enforced when a token is initialized</p> <p>Notes:</p> <ul style="list-style-type: none"> ■ We recommend that this policy not be set when tokens are enrolled using TMS. ■ When token initializations are performed by the eToken Properties application, this policy is ignored, and password policy is enforced.
DWORD Value	<p>1 (true) - The password policy is enforced</p> <p>0 (false) - The password policy is not enforced</p>
Default	0

User Interface Registry Keys

The following properties are saved as registry settings in the **UI** registry key.

Display Serial Number in Decimal Format

Registry Key Name	ShowDecimalSerial
Description	Determines if the eToken Properties <i>Information</i> window displays the eToken Serial number in hexadecimal or decimal format
DWORD Value	<p>1 (true) - displays the serial number in decimal format</p> <p>0 (false) - displays the serial number in hexadecimal format</p>
Default	Does not exist

Use Default Password

Property Name	(Cannot be set by command line installation)
Registry Key Name	UseDefaultPassword
Description	Determines if the <i>Change Password at First Logon</i> process uses the default password (1234567890) to change the password, without requiring the user to supply it
DWORD Value	1 (True) - The default password is automatically inserted in the password field 0 (False)- The default password is not automatically inserted in the password field
Default	0 (False)

Access Control Registry Key

The following properties control the user interface display and are saved as registry settings in the **AccessControl** registry key.

About

AddTokenVirtual

ChangeAdministratorPassword

ChangeInitializationKeyDuringInitialize

ChangePassword

ClearDefaultCert

ClearEToken

CopyCertificateData

DeleteCertificate

DisconnectVirtual

ExportCertificate

GenerateOTP

Hide

ImportCertificate

InitializeEToken

LaunchNGFlashPartitionApplication**LoginAsAdministrator****ManageReaders****OpenAdvancedModeOfInitialize****OpenAdvancedView****OpeneTokenProperties****RenameToken****SetCertificateAsAuxiliary****SetCertificateAsDefault****SetUserPassword****SwitcheToken****SyncDomainAndTokenPass****TrayIconChangePassword****TrayIconClearEToken****UnlockEToken****ViewTokenInfo**

The following information applies to the **AccessControl** registry keys listed above.

Description	Determines if the option is enabled in the eToken Properties application
DWORD Value	1 (True) - The option is enabled 0 (False)- The option is disabled
Default	1 (True)

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 products have 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 products.

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 9001 Certification

The eToken product line is designed and manufactured by Aladdin Knowledge Systems, an ISO 9001-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.

