User Documentation for EIDAuthenticate

Version 1.4

Prepared by: "Vincent Le Toux"

Date: 27/01/2014

Table of Contents

Troubleshooting

Revision History

This section records the change history of this document.

Name	Date	Reason For Changes	Version
Vincent Le Toux	01/12/2012	Creation	1.0
Frédéric Bourgeois	23/02/2013	Update	1.1
Nathan J. Lichtenstein	19/04/2013	Review	1.2
Vincent Le Toux	22/07/2013	Update to EIDAuthenticate 1.0	1.3
Vincent Le Toux	27/01/2014	Update to EIDAuthenticate 1.2	1.4

System Specifications

Operating system supported are :

- Windows XP, Windows Server 2003
- Windows Vista, Windows 7, Windows Server 2008
- Windows 8, Windows Server 2012

Windows XP and Windows 2003 are supported only not joined to a domain.

Remote Desktop protocol (terminal services), SMB protocol (network share), programs using the “Negotiate authentication package” directly or through the SSPI Authentication are not supported (like *runas /smartcard*).

Installation

GUI mode

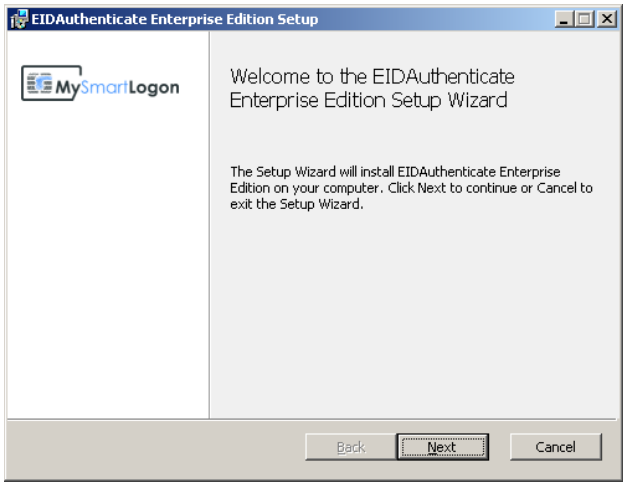
The user performing the installer must have administrator privilege.

EIDAuthenticate can be used immediately on Windows Vista and later. If the product is used on servers, it is recommended to reboot because password reset are handled only using the password filter component loaded after the first reboot.

At the removal of EIDAuthenticate, the system will need to reboot.

To start the installation, run EIDAuthenticate.msi.

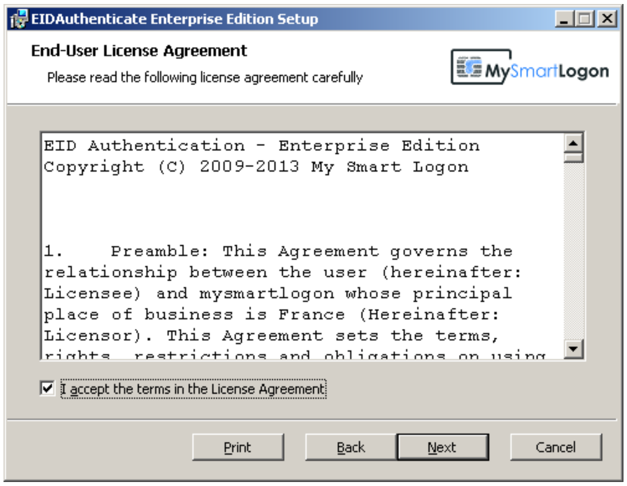
Press Next.



Welcome to the EIDAuthenticate Enterprise Edition Setup Wizard

The Setup Wizard will install EIDAuthenticate Enterprise Edition on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Validate the license agreement.



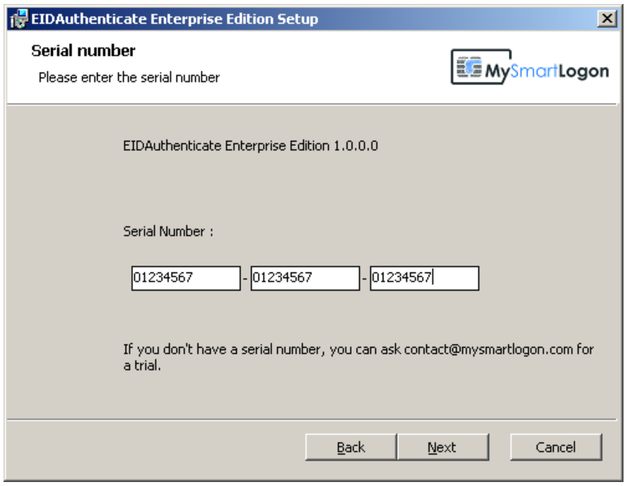
End-User License Agreement

Please read the following license agreement carefully

```
EID Authentication - Enterprise Edition
Copyright (C) 2009-2013 My Smart Logon


1.    Preamble: This Agreement governs the
relationship between the user (hereinafter:
Licensee) and mysmartlogon whose principal
place of business is France (Hereinafter:
Licensor). This Agreement sets the terms,
rights, restrictions and obligations on using
```

☑ I accept the terms in the License Agreement

Enter the serial number.



Serial number

Please enter the serial number

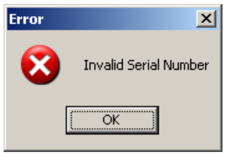
EIDAuthenticate Enterprise Edition 1.0.0.0

Serial Number :

01234567 - 01234567 - 01234567

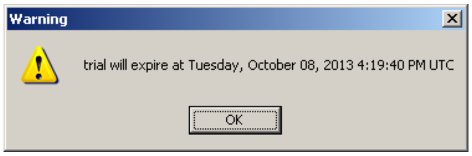
If you don't have a serial number, you can ask contact@mysmartlogon.com for a trial.

If the serial number is not correct, an error dialog will be shown.



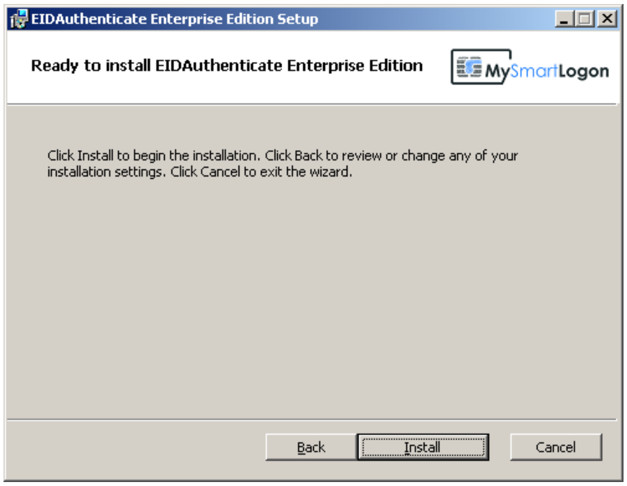
Invalid Serial Number

If the serial number is a trial, a dialog will display the date at which the trial will end.



trial will expire at Tuesday, October 08, 2013 4:19:40 PM UTC

Press Install to start the installation.

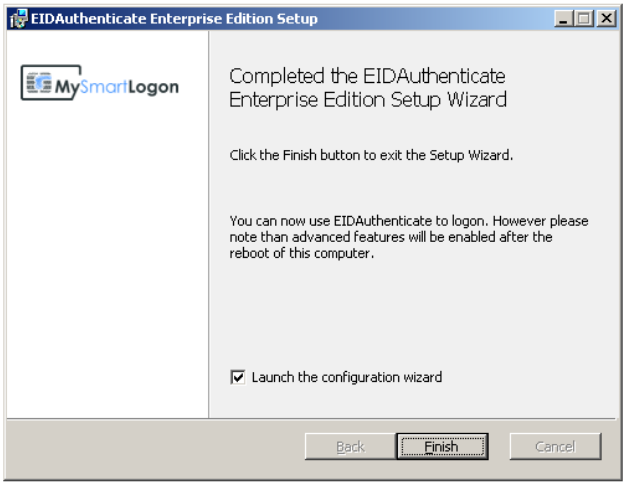


EIDAuthenticate Enterprise Edition Setup

Ready to install EIDAuthenticate Enterprise Edition

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

After the installation, the following dialog is shown.



EIDAuthenticate Enterprise Edition Setup

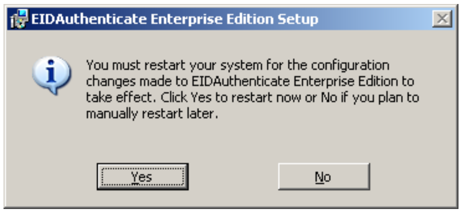
Completed the EIDAuthenticate Enterprise Edition Setup Wizard

Click the Finish button to exit the Setup Wizard.

You can now use EIDAuthenticate to logon. However please note than advanced features will be enabled after the reboot of this computer.

☑ Launch the configuration wizard

When run on Windows XP or Windows 2003, a reboot is required.

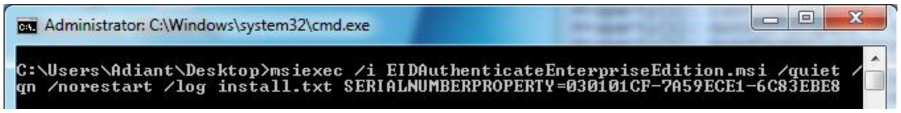


EIDAuthenticate Enterprise Edition Setup

You must restart your system for the configuration changes made to EIDAuthenticate Enterprise Edition to take effect. Click Yes to restart now or No if you plan to manually restart later.

Unattended mode

The software can be installed on a unattended mode.



```
C:\Users\Adiant\Desktop>msiexec /i EIDAuthenticateEnterpriseEdition.msi /quiet /
qn /norestart /log install.txt SERIALNUMBERPROPERTY=030101CF-7A59ECE1-6C83EBE8
```

The exact command line is :

msiexec /i EIDAuthenticateEnterpriseEdition.msi /quiet /qn /norestart /log install.txt SERIALNUMBERPROPERTY=<serialnumber>

Any problem can be found on the install.txt log and the command to uninstall it is :

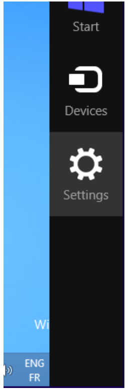
msiexec /x EIDAuthenticateEnterpriseEdition.msi /quiet /qn /norestart /log install.txt

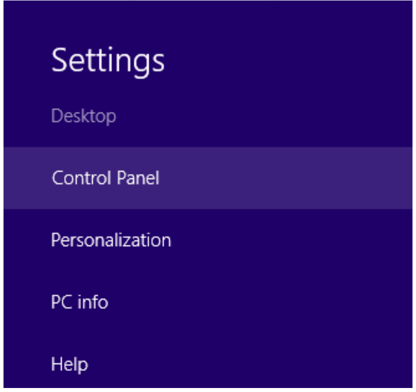
Configure the smart card logon

Launch the wizard to configure your account

For Windows 8 and Windows 2012

Open the "Settings" of the computer then open the "Control Panel".



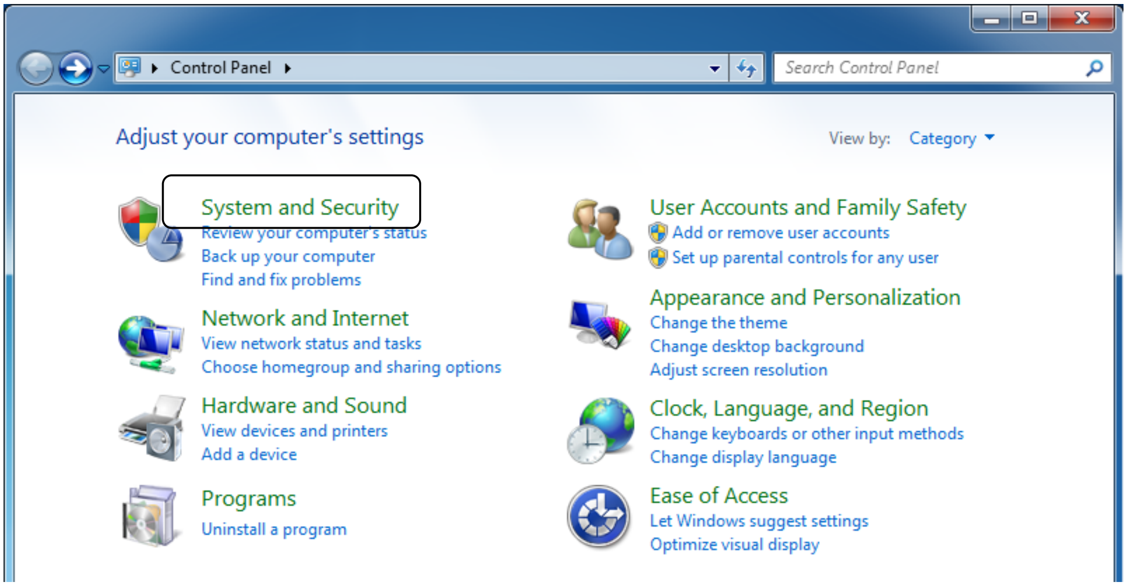


You can then follow the same instructions than for Windows Vista

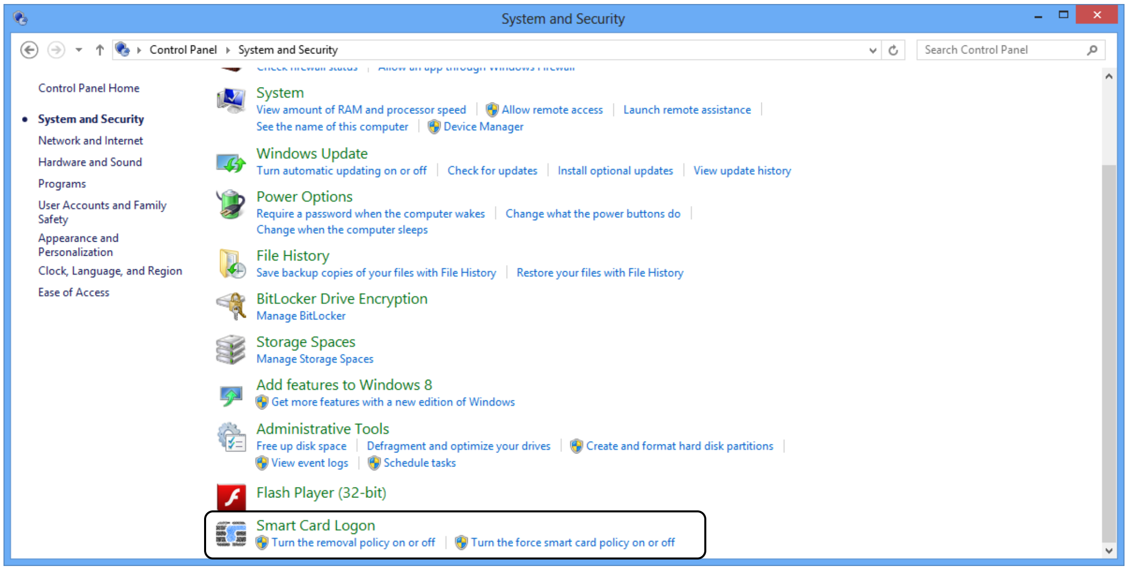
For Windows Vista, Seven, Windows Server 2008 and 2008 R2

Click on the "start" menu then choose "Control Panel"

Once the control panel is opened, select "System and Security" at the upper left of the page


Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Change display language
Ease of Access
Let Windows suggest settings
Optimize visual display

Select "Smart card logon" at the bottom of the page

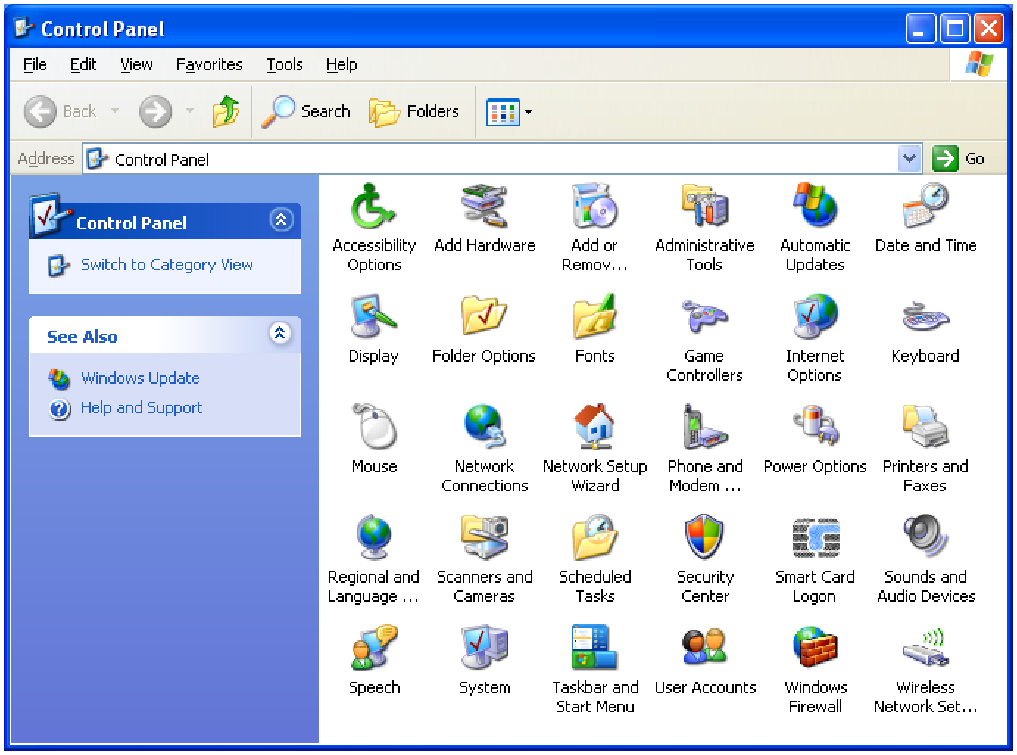

System and Security
Control Panel ▸ System and Security
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts and Family Safety
Appearance and Personalization
Clock, Language, and Region
Ease of Access
System
View amount of RAM and processor speed | Allow remote access | Launch remote assistance
See the name of this computer | Device Manager
Windows Update
Turn automatic updating on or off | Check for updates | Install optional updates | View update history
Power Options
Require a password when the computer wakes | Change what the power buttons do
Change when the computer sleeps
File History
Save backup copies of your files with File History | Restore your files with File History
BitLocker Drive Encryption
Manage BitLocker
Storage Spaces
Manage Storage Spaces
Add features to Windows 8
Get more features with a new edition of Windows
Administrative Tools
Free up disk space | Defragment and optimize your drives | Create and format hard disk partitions
View event logs | Schedule tasks
Flash Player (32-bit)
Smart Card Logon
Turn the removal policy on or off | Turn the force smart card policy on or off

Note: At this page, you can also configure the removal policy or configure the force smart card policy. These policy are described later in this documentation.

For Windows XP and 2003

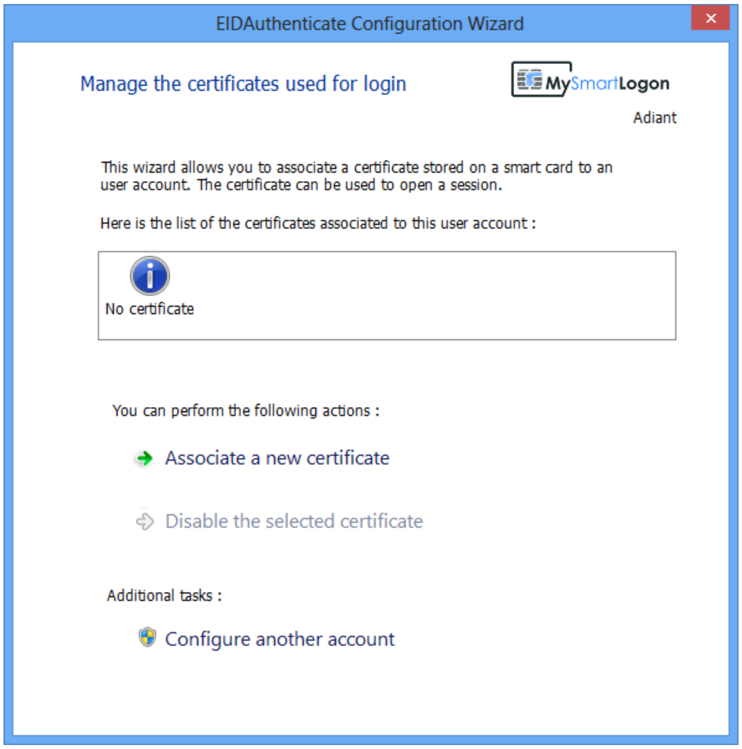
Click on the "start" menu then choose "Control Panel"

Select "Smart card logon" at the bottom of the page.



The configuration wizard

The main screen of the configuration wizard shows the certificate already mapped to the account, allows the associate of a new certificate, the deletion of an existing mapping and to configure other accounts.



EIDAuthenticate Configuration Wizard

Manage the certificates used for login

Adiant

This wizard allows you to associate a certificate stored on a smart card to an user account. The certificate can be used to open a session.

Here is the list of the certificates associated to this user account :

No certificate

You can perform the following actions :

Associate a new certificate

Disable the selected certificate

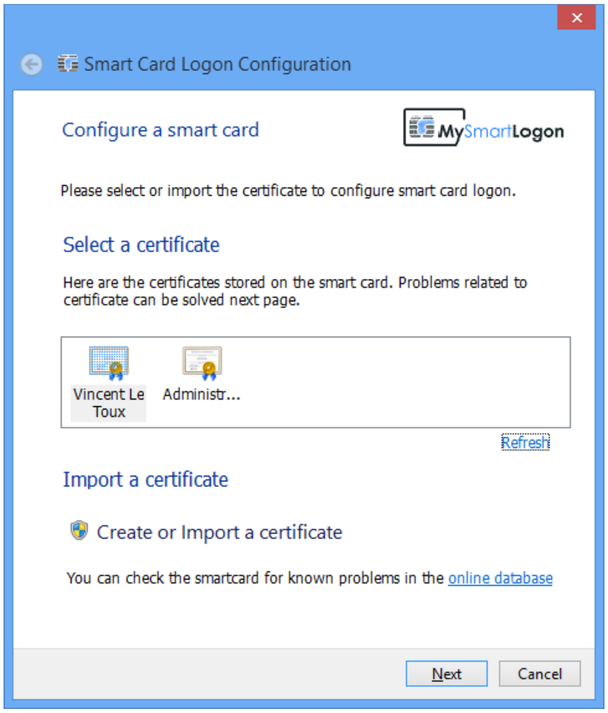
Additional tasks :

Configure another account

Click on “associate a new certificate” to map a new smart card to the user account.

Associate a new certificate

The wizard asks for a smart card and reads its content. Existing certificates are shown. You can view the certificate by double clicking on the icon.



Smart Card Logon Configuration

Configure a smart card

Please select or import the certificate to configure smart card logon.

Select a certificate

Here are the certificates stored on the smart card. Problems related to certificate can be solved next page.

Import a certificate

Create or Import a certificate

You can check the smartcard for known problems in the online database

If the smart card doesn’t contain a certificate, you can use the “*Create or Import*” function.

If you remove the smart card and insert a new one, click on *refresh* to update the screen.

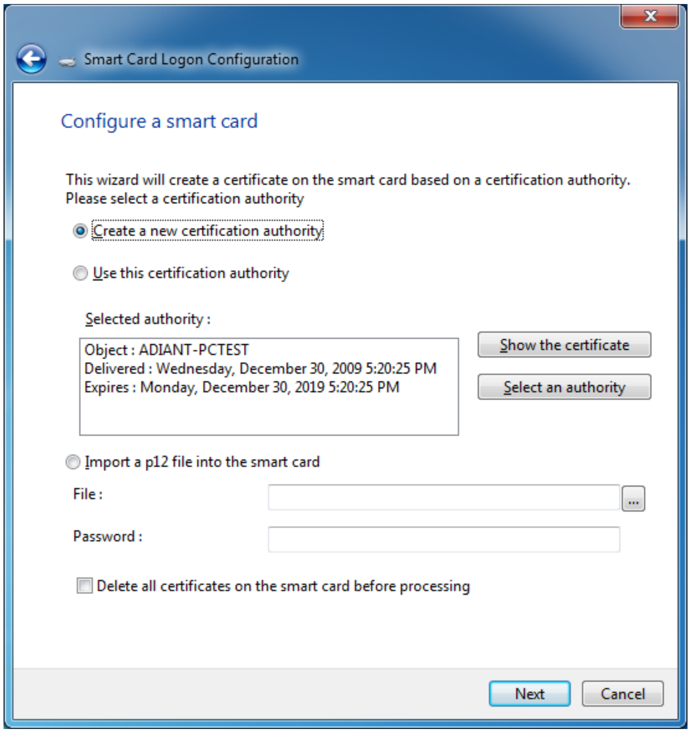
After having selected a certificate, press “*Next*”.

Optionally create or import a certificate to a smart card

If you click on *Create or Import a certificate*, a new page will be shown.

This page allows you to create a new certificate on the smart card. Because this certificate is not self signed, a certification authority must be used. You can create a new certificate authority (default choice if this is the first time you run this wizard) or to use an existing one (default choice if a certificate with a private key already exists). You can also import a certificate with its private key using a PKCS12 file. Because a PKCS12 is encrypted, you must input the password used to protect the keys. An option exists to enable you to clear the card (removing all certificates and key containers) before proceeding.

You will be prompted for your PIN to create the cryptographic material on the smart card. An error can be show if you don’t have the right on the smart card to perform these operations.



Configure a smart card

This wizard will create a certificate on the smart card based on a certification authority.
Please select a certification authority

● Create a new certification authority

○ Use this certification authority

Selected authority :

Object : ADIANT-PCTEST
Delivered : Wednesday, December 30, 2009 5:20:25 PM
Expires : Monday, December 30, 2019 5:20:25 PM

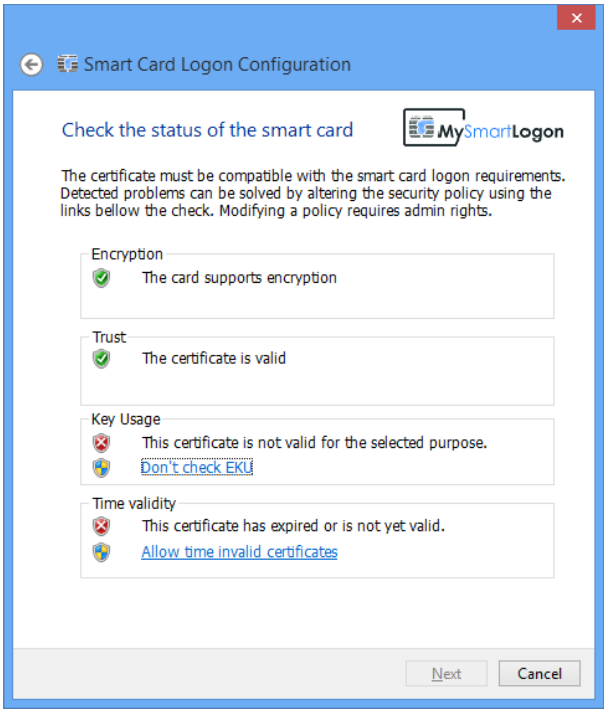
○ Import a p12 file into the smart card

File :

Password :

□ Delete all certificates on the smart card before processing

Checking the certificate to configure


Smart Card Logon Configuration
MySmartLogon
Don't check EKU
Allow time invalid certificates
Next
Cancel

Check the status of the smart card

The certificate must be compatible with the smart card logon requirements. Detected problems can be solved by altering the security policy using the links bellow the check. Modifying a policy requires admin rights.

Encryption
✓ The card supports encryption

Trust
✓ The certificate is valid

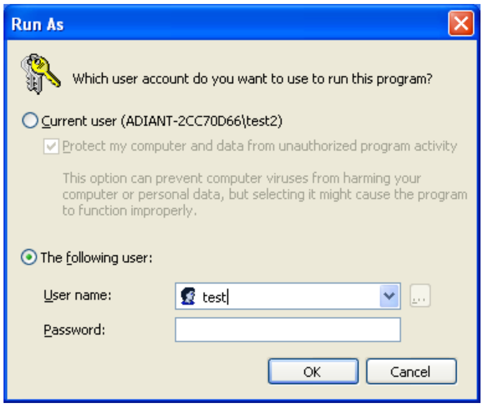
Key Usage
✗ This certificate is not valid for the selected purpose.

Time validity
✗ This certificate has expired or is not yet valid.

To be used by EIDAuthenticate, a certificate MUST be trusted, time valid and having the right attributes. Like the Active Directory smart card logon, the certificate MUST have the "Smart card logon EKU" and provide encryption services. However this behavior can be altered by modifying the security policy.

This page checks the certificates against the current policy and shows the problems or warnings. The security policy can be altered by clicking on the links next to the checks. For example : "*Don't check EKU*".

The program proposes if you are not authorized to elevate or to run as a another user.



Run As

Which user account do you want to use to run this program?

○ Current user (ADIANT-2CC70D66\test2)

☑ Protect my computer and data from unauthorized program activity

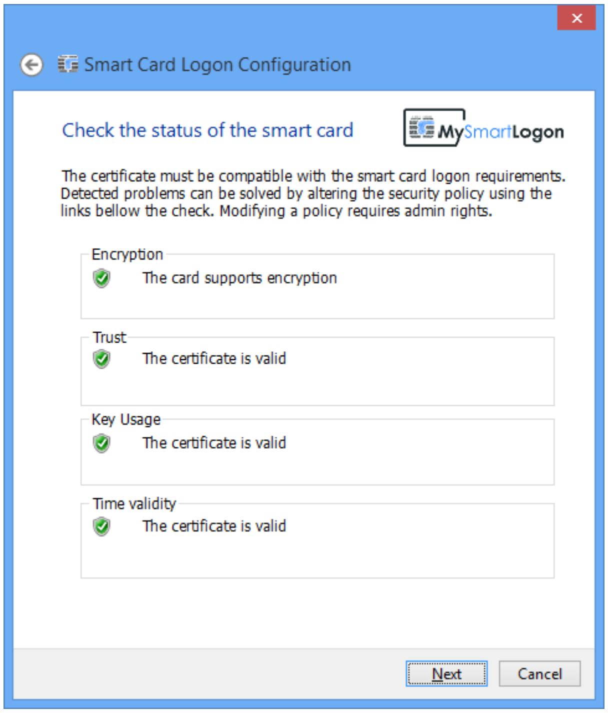
This option can prevent computer viruses from harming your computer or personal data, but selecting it might cause the program to function improperly.

● The following user:

User name: test

Password:

There must be no red checks to continue the configuration.



Smart Card Logon Configuration

Check the status of the smart card

The certificate must be compatible with the smart card logon requirements. Detected problems can be solved by altering the security policy using the links bellow the check. Modifying a policy requires admin rights.

Encryption
✓ The card supports encryption

Trust
✓ The certificate is valid

Key Usage
✓ The certificate is valid

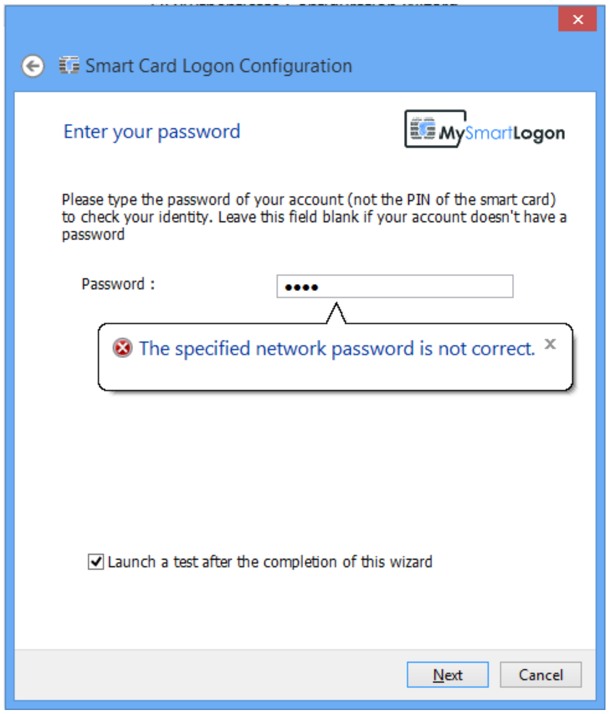
Time validity
✓ The certificate is valid

Press *Next*.

Note : if the security policy is altered AFTER the certificate has been configured, the logon possibility will be undetermined. It MAY allow the logon or deny it, depending of the current security policy.

Note : EIDAuthenticate uses the computer certificate store (accessed using mmc -> certificates -> computer) instead of the current user certificate store (mmc -> certificates -> current user or certmgr.msc) to perform these verifications.

Map a password



Smart Card Logon Configuration

Enter your password

Please type the password of your account (not the PIN of the smart card) to check your identity. Leave this field blank if your account doesn't have a password

Password : ••••

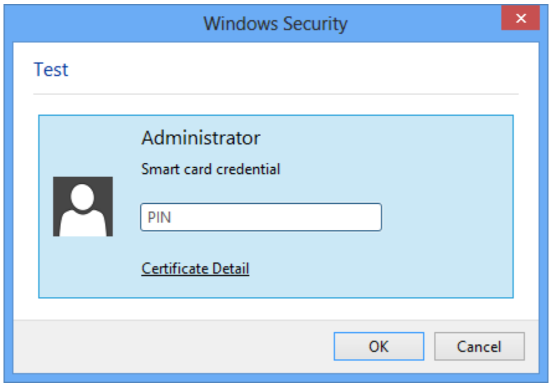
The specified network password is not correct.

☑ Launch a test after the completion of this wizard

Because you are configuring another credential, we MUST check the identity to avoid identity theft. Indeed, somebody can install and configure EIDAuthenticate to provide future access to a restricted account.

If the account doesn't have a password, don't fill any password. If it is not correct, a warning will be showed, as on the screenshot.

If the check "launch a test" is checked, you will be asked for the PIN of your smart card to try a logon. You can click on "certificate detail" to check that the certificate shown is the one you are configuring.



Windows Security

Test

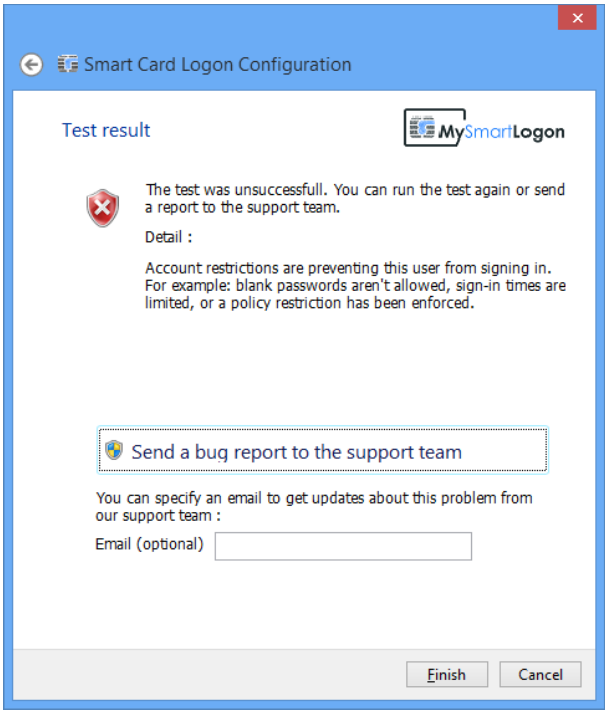
Administrator

Smart card credential

PIN

Certificate Detail

Results



Smart Card Logon Configuration
Test result
MySmartLogon
Send a bug report to the support team
Finish
Cancel

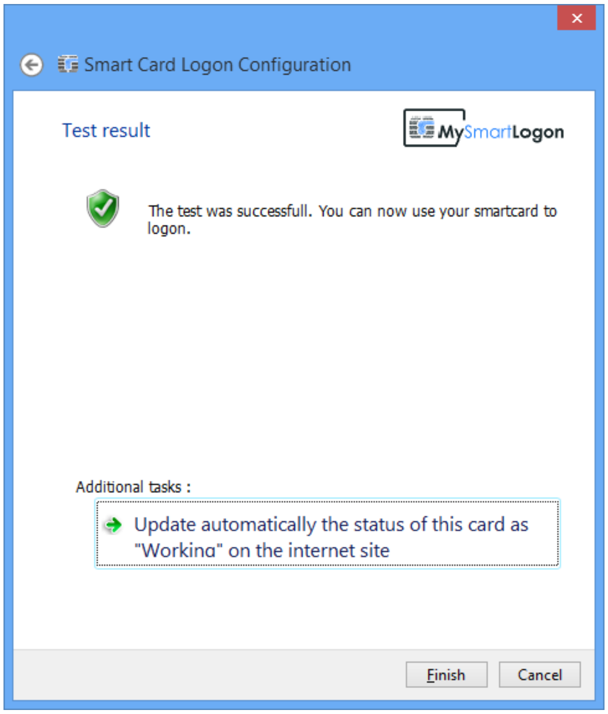
The test was unsuccessfull. You can run the test again or send a report to the support team.

Detail :

Account restrictions are preventing this user from signing in. For example: blank passwords aren't allowed, sign-in times are limited, or a policy restriction has been enforced.

You can specify an email to get updates about this problem from our support team :

Email (optional)



Smart Card Logon Configuration
Test result
MySmartLogon
Update automatically the status of this card as "Working" on the internet site
Finish
Cancel

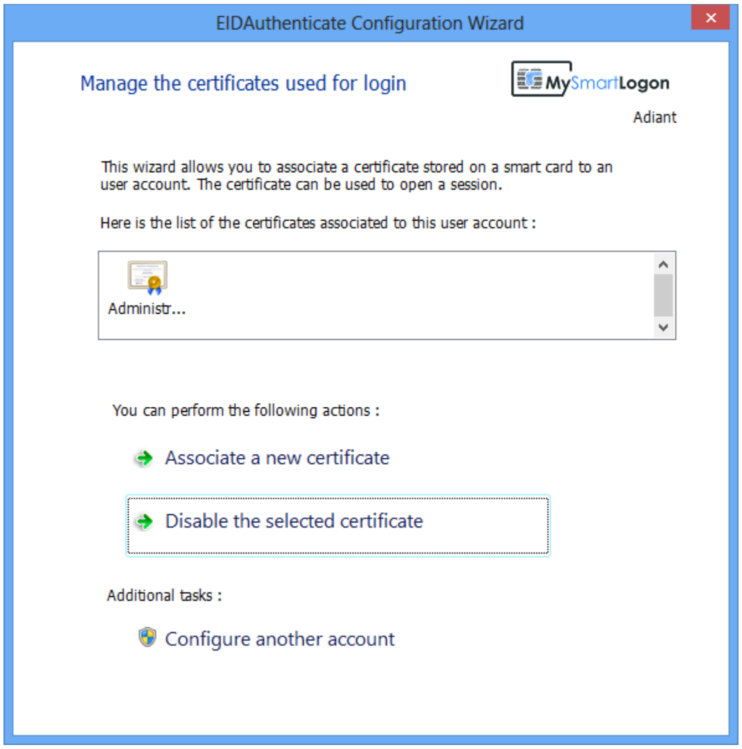
The test was successfull. You can now use your smartcard to logon.

Additional tasks :

If you made a test, the next screen will show you its result.

Optionnaly, you can send a bug report to our support team or send a report that the card you were configuring is working with our software. Results can be looked at : http://database.mysmartlogon.com.

Disable the smart card logon



EIDAuthenticate Configuration Wizard
Manage the certificates used for login
MySmartLogon
Adiant
Administr...
Associate a new certificate
Disable the selected certificate
Configure another account

This wizard allows you to associate a certificate stored on a smart card to an user account. The certificate can be used to open a session.

Here is the list of the certificates associated to this user account :

You can perform the following actions :

Additional tasks :

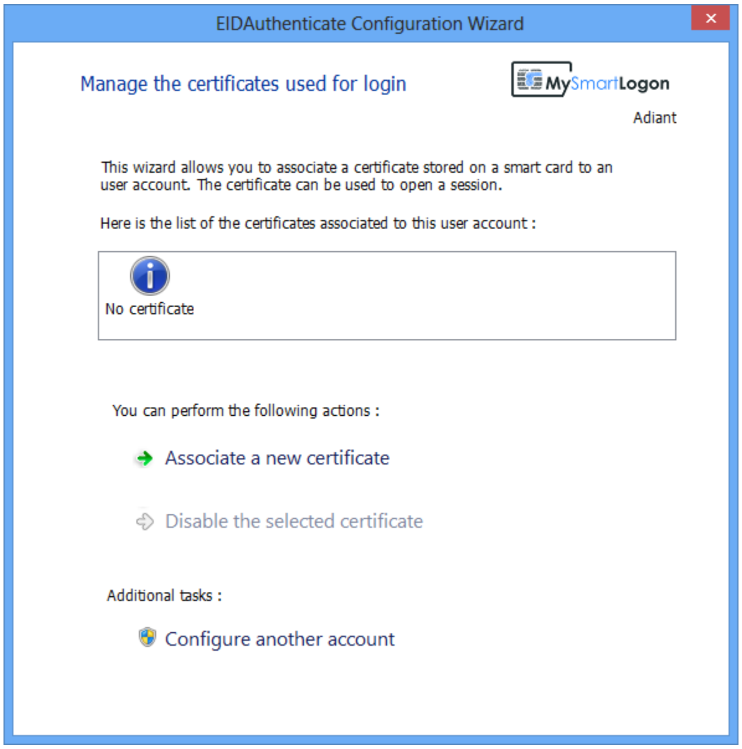
Once a certificate has been configured, you can disabled it by selecting it and by clicking on "disable the selected certificate". You have to do this for each certificate if you want to disable the smart card logon for this account.

Limitation

A certificate can be used to configure only one account. If a certificate is used on a second account, the certificate will be unmapped from the old account.

Administration

Configure another account



EIDAuthenticate Configuration Wizard

Manage the certificates used for login

This wizard allows you to associate a certificate stored on a smart card to an user account. The certificate can be used to open a session.

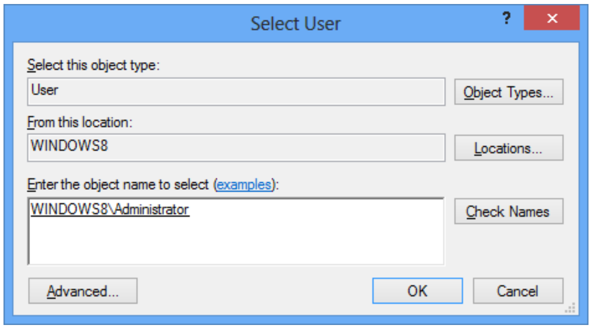
Here is the list of the certificates associated to this user account :

No certificate

You can perform the following actions :

MySmartLogon
Adiant
Associate a new certificate
Disable the selected certificate
Additional tasks :
Configure another account

If you want to configure account, press “configure another account”, type the account you want to edit then press OK. An elevation will be needed.

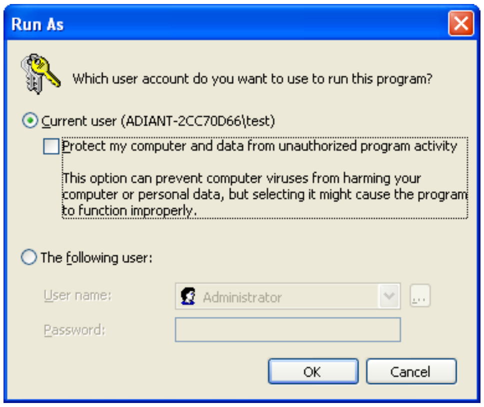


Select User

Select this object type: User

From this location: WINDOWS8

Enter the object name to select (examples): WINDOWS8\Administrator



Run As

Which user account do you want to use to run this program?

● Current user (ADIANT-2CC70D66\test)

□ Protect my computer and data from unauthorized program activity

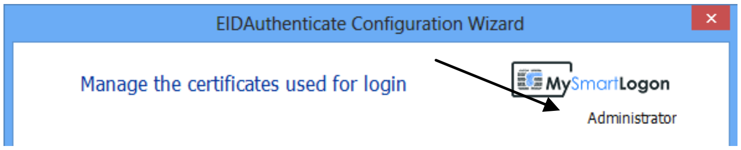
This option can prevent computer viruses from harming your computer or personal data, but selecting it might cause the program to function improperly.

○ The following user:

User name: Administrator

Password:

When running on Windows XP, you have to uncheck "Protect my computer and data from unauthorized program activity".



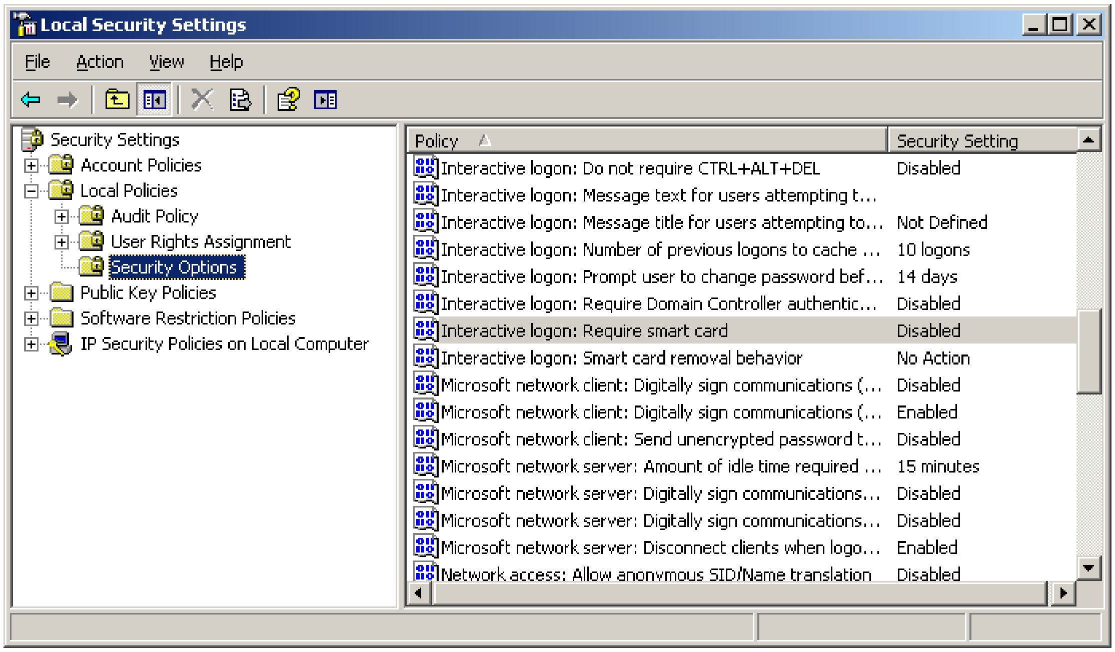
EIDAuthenticate Configuration Wizard

Manage the certificates used for login

You can remark that the account name printed on the upper right corner will change.

Note : In this example we configured the administrator account. Please note that this account is disabled by default and despite the fact that you'll be able to configure it, the logon will fail.

Security policies

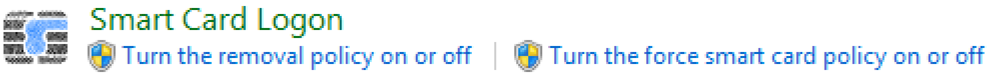


Policy	Security Setting
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Message text for users attempting t...	
Interactive logon: Message title for users attempting to...	Not Defined
Interactive logon: Number of previous logons to cache ...	10 logons
Interactive logon: Prompt user to change password bef...	14 days
Interactive logon: Require Domain Controller authentic...	Disabled
Interactive logon: Require smart card	Disabled
Interactive logon: Smart card removal behavior	No Action
Microsoft network client: Digitally sign communications (...	Disabled
Microsoft network client: Digitally sign communications (...	Enabled
Microsoft network client: Send unencrypted password t...	Disabled
Microsoft network server: Amount of idle time required ...	15 minutes
Microsoft network server: Digitally sign communications...	Disabled
Microsoft network server: Digitally sign communications...	Disabled
Microsoft network server: Disconnect clients when logo...	Enabled
Network access: Allow anonymous SID/Name translation	Disabled

The product is compatible with the two following Windows policies :

- Interactive logon : require smart card
- Interactive logon : Smart card removal behavior

These policies can be set by the control panel link "Local Security Settings" or using the new links provided by EIDAuthenticate on the control panel bellow the smart card logon icon.



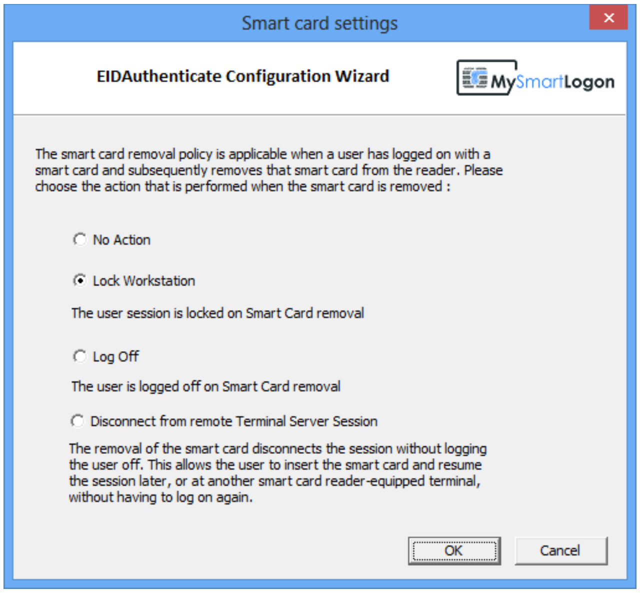
Smart Card Logon

Turn the removal policy on or off
Turn the force smart card policy on or off

Configure the remove policy

This page allows you to configure what happens if you remove the smart card you have used to log on. These settings can be found in the control panel bellow the link to the wizard.

It is exactly the same policy at the same registry key than the Windows Policy. Please refer to the functional documentation for more information.



Smart card settings

EIDAuthenticate Configuration Wizard

The smart card removal policy is applicable when a user has logged on with a smart card and subsequently removes that smart card from the reader. Please choose the action that is performed when the smart card is removed :

○ No Action

● Lock Workstation

The user session is locked on Smart Card removal

○ Log Off

The user is logged off on Smart Card removal

○ Disconnect from remote Terminal Server Session

The removal of the smart card disconnects the session without logging the user off. This allows the user to insert the smart card and resume the session later, or at another smart card reader-equipped terminal, without having to log on again.

Note : The configuration changes are taken in account at the next logon. You must logoff to enable the remove policy.

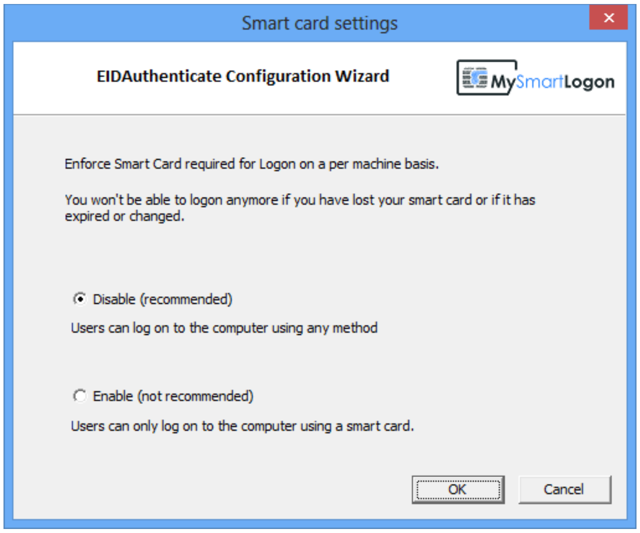
Configure the force smart card policy

These settings can be found in the control panel bellow the link to the wizard.

This page allows you to configure if **all users** MUST use their smart card to logon.

It is exactly the same policy at the same registry key than the Windows Policy. Please refer to the functional documentation for more information.

Important : It is advised to not enable this policy because you won't be able to logon if your certificate expires, is changed or if the smart card is lost.



Smart card settings

EIDAuthenticate Configuration Wizard

Enforce Smart Card required for Logon on a per machine basis.

You won't be able to logon anymore if you have lost your smart card or if it has expired or changed.

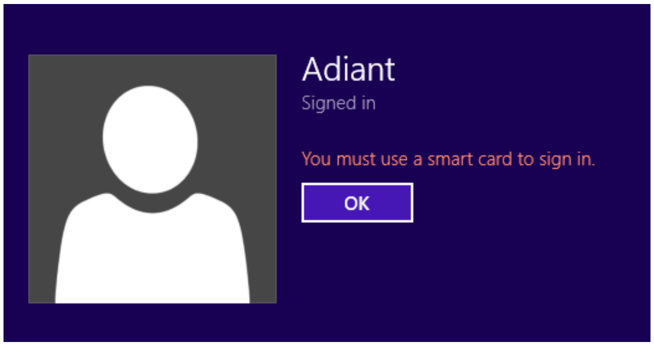
● Disable (recommended)

Users can log on to the computer using any method

○ Enable (not recommended)

Users can only log on to the computer using a smart card.

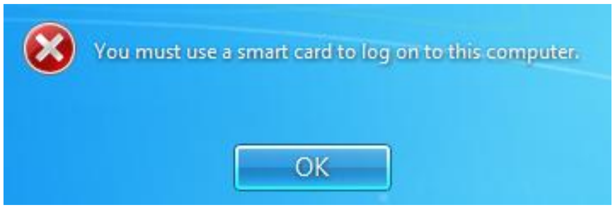
When this policy is enabled and if a login attempt using a password is made, the following message is shown.



Adiant

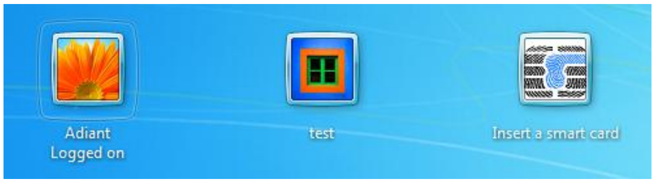
Signed in

You must use a smart card to sign in.

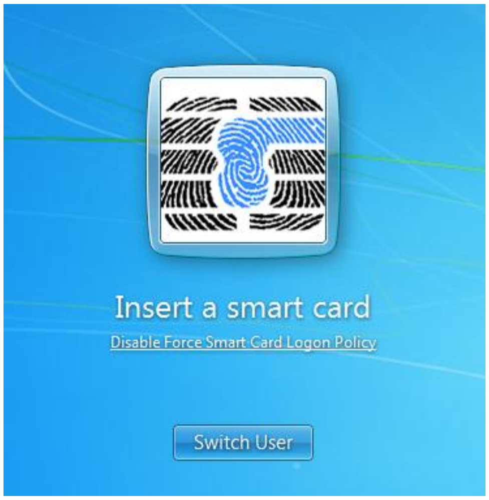


You must use a smart card to log on to this computer.

There are an emergency procedure to disable this policy. When it is applied, an icon with the message "Insert a smart card" appears.

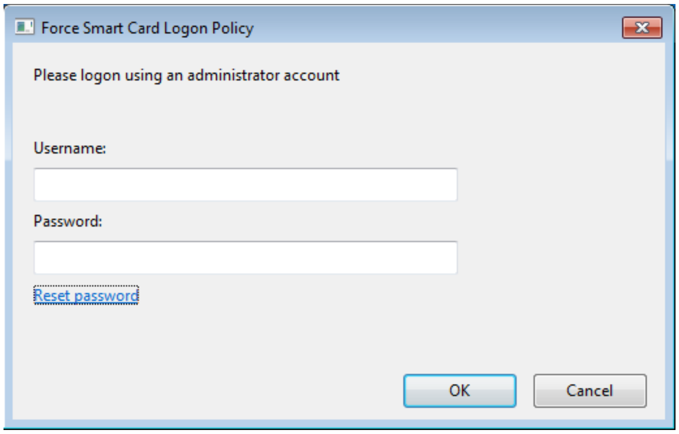


When it is active, a link named "Disable Force Smart Card Logon Policy" is shown.



Insert a smart card

You can login using an administrator account and disable the policy.



Force Smart Card Logon Policy

Please logon using an administrator account

Also the reset password wizard can be called if you lost the administrator password and if you prepared a recovery disk.

This emergency procedure can be deactivated by setting the registry key `HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\scdisablerecovery` to 1.

The force smart card policy can be disabled by modifying the policy setting offline.

The procedure is to disconnect the hard drive from the computer and to connect it another computer. Then open regedit on the other computer. Click HKEY_LOCAL_MACHINE. In the File menu, click “Load Hive.” and open the file %windir%\system32\config\SOFTWARE from the connected hard drive. Enter an arbitrary key name when prompted. Then edit from your node the subkey Software\Microsoft\Windows\CurrentVersion\Policies\System. Change the value of scforceoption from 1 to 0. Click the root folder of your node, and then click “Unload hive” in the File menu. Your changes will be written to the offline Registry. Then disconnect the hard drive and connect it back.

Such recovery can be mitigated by encrypting the system disk.

Windows Safe Mode

By default, Windows does not load custom credential like EIDAuthenticate providers in safe mode.

This is not a bug. SAFE mode is intended to serve as a workaround in order to correct repair Operating Systems malfunctioning due to incorrectly configured components such as device drivers. By default, only the in-box Password Provider is loaded in SAFE mode. This provides a fallback in case of a bad error. To over-ride the fallback logic and force logonUI to load Credential Provider filters in SAFE Mode, create and set the following registry key:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers] “ProhibitFallbacks”=dword:1

Command line

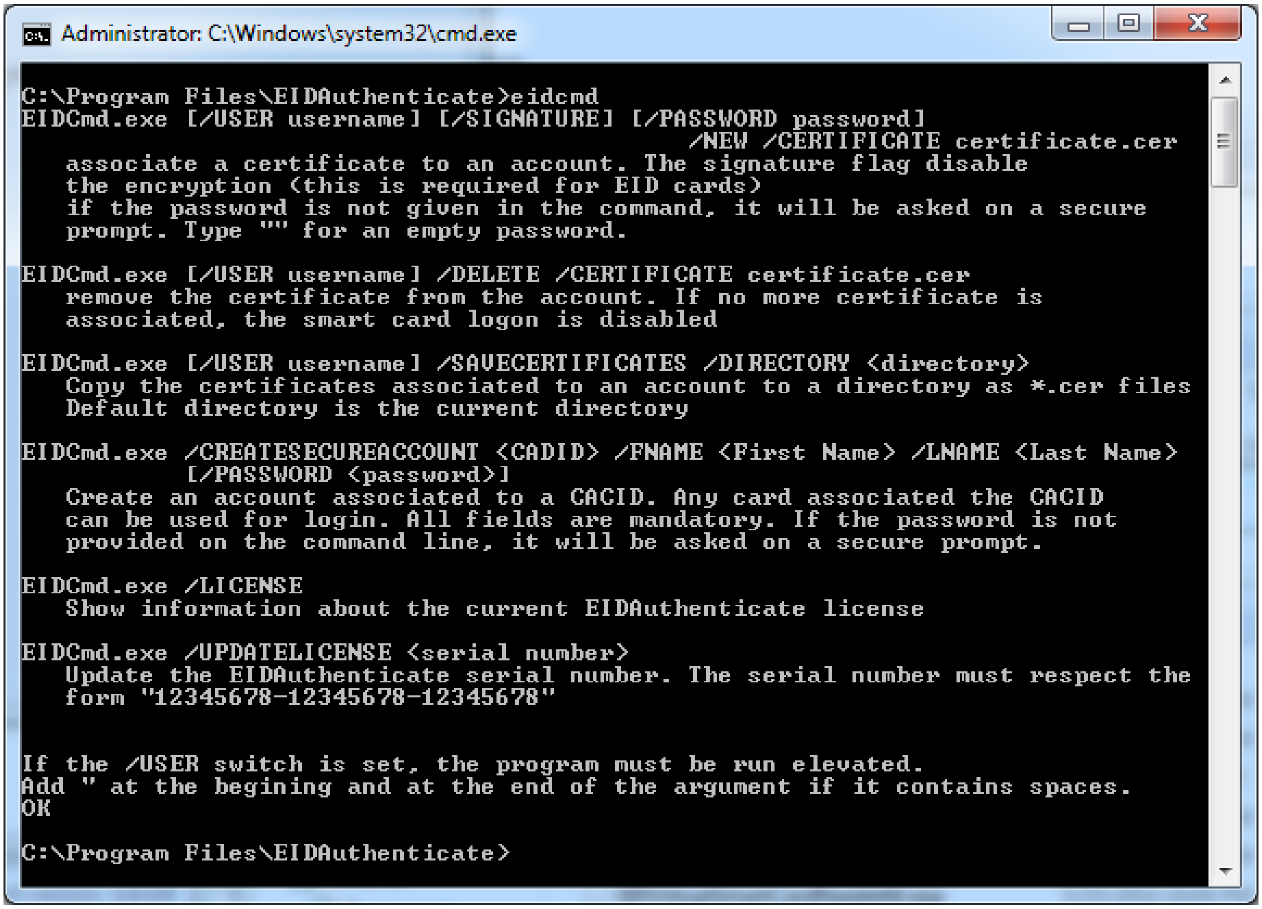
The Wizard can be launched with command line options.

Switch	Comment
/USER username	Configure the user "username"
/ADVANCED	Enable advanced options like the experimental feature allowing the requirement of smart cards just for a specific user
/ENABLESIGNATUREONLY	Enable the policy "allow signature only smart card"
/DISABLESIGNATUREONLY	Disable the policy "allow signature only smart card"
/ENABLENOEKU	Enable the policy "allow certificate with no EKU"

/DISABLENOEKU	Disable the policy "allow certificate with no EKU"
/ENABLETIMEINVALID	Enable the policy "allow time invalid certificate "
/DISABLETIMEINVALID	Disable the policy "allow time invalid certificate "

EIDCmd.exe

Starting with EIDAuthenticate version1.0.2, a command line program named EIDCmd.exe can perform some of the configuration task made by the configuration wizard. This program is located in the program files folder.



Administrator: C:\Windows\system32\cmd.exe

```
C:\Program Files\EIDAuthenticate>eidcmd
EIDCmd.exe [/USER username] [/SIGNATURE] [/PASSWORD password]
                                             /NEW /CERTIFICATE certificate.cer
   associate a certificate to an account. The signature flag disable
   the encryption (this is required for EID cards)
   if the password is not given in the command, it will be asked on a secure
   prompt. Type "" for an empty password.

EIDCmd.exe [/USER username] /DELETE /CERTIFICATE certificate.cer
   remove the certificate from the account. If no more certificate is
   associated, the smart card logon is disabled

EIDCmd.exe [/USER username] /SAVECERTIFICATES /DIRECTORY <directory>
   Copy the certificates associated to an account to a directory as *.cer files
   Default directory is the current directory

EIDCmd.exe /CREATESECUREACCOUNT <CADID> /FNAME <First Name> /LNAME <Last Name>
           [/PASSWORD <password>]
   Create an account associated to a CACID. Any card associated the CACID
   can be used for login. All fields are mandatory. If the password is not
   provided on the command line, it will be asked on a secure prompt.

EIDCmd.exe /LICENSE
   Show information about the current EIDAuthenticate license

EIDCmd.exe /UPDATELICENSE <serial number>
   Update the EIDAuthenticate serial number. The serial number must respect the
   form "12345678-12345678-12345678"


If the /USER switch is set, the program must be run elevated.
Add " at the begining and at the end of the argument if it contains spaces.
OK

C:\Program Files\EIDAuthenticate>
```

For example, you can configure the smart card logon using a certificate file only and without having the smart card connected (/NEW).

You can also dump the certificates associated to an account for audit purpose (/SAVECERTIFICATES) or remove an existing association (/DELETE).

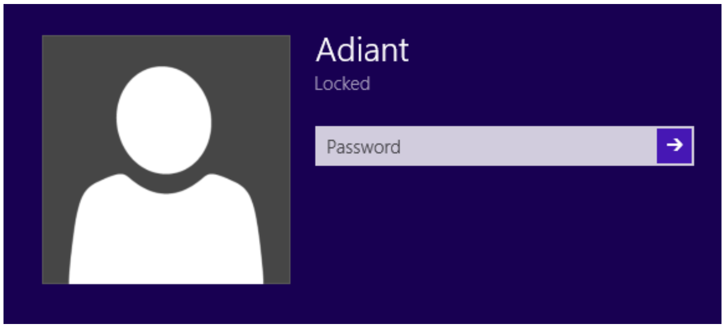
It can create an account where the smart card is mandatory. The smart card must have one certificate with the subject which ends with a point followed by a 10 digits number and a UPN set in the SAN attribute which ends with "@mil". The password is used for network interoperability with NTLM. The account created has its name which begins with "EID" and the configuration setting is invisible from the wizard. To remove the smart card configuration, delete the account.

Use your smart card

Login to Windows

On Windows 8 and Windows Server 2012

Windows 8 and Windows Server 2012 show by default the last method used and in particular, it asks for the password.

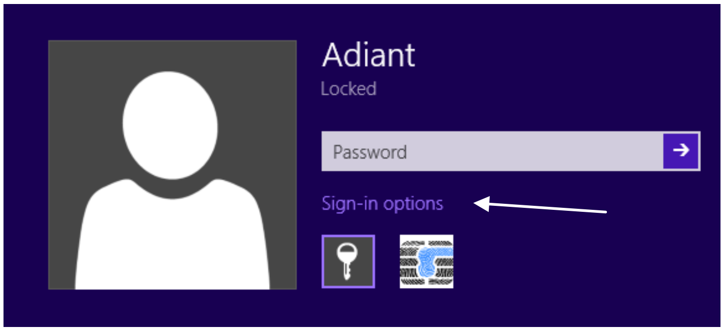


Adiant

Locked

Password

When a smart card is inserted, a new Sign-in option appears. Select the MySmartLogon Icon to switch to the smart card mode. If the icon doesn't appear, click on "Sign-in options" or click on the ← image which may appear on the left of the user picture to switch between user accounts.



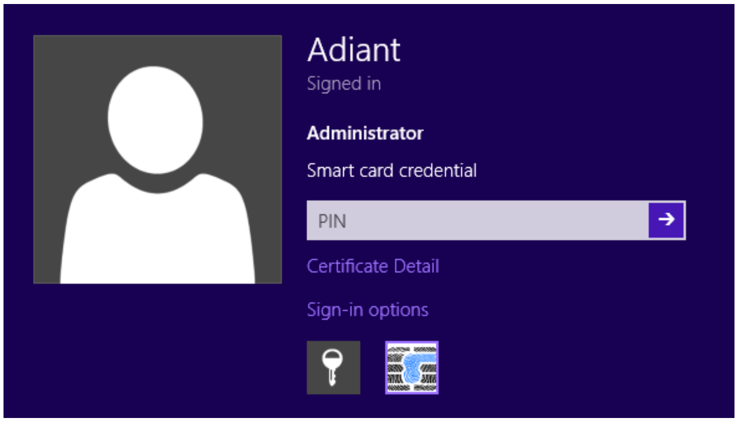
Adiant

Locked

Password

Sign-in options

Then enter your PIN to login.



Adiant

Signed in

Administrator

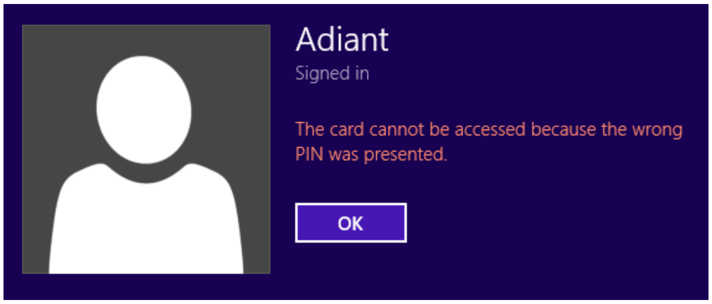
Smart card credential

PIN

Certificate Detail

Sign-in options

If everything went fine, the session will be opened. Else, an error message will be shown.

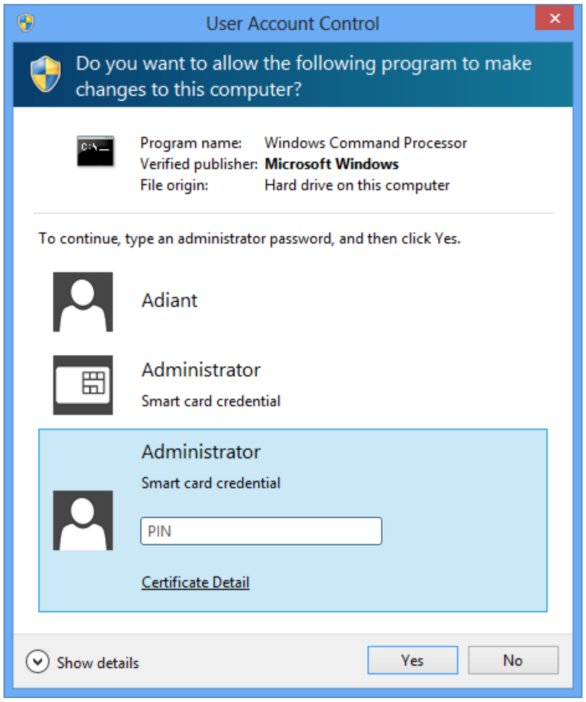


Adiant
Signed in

The card cannot be accessed because the wrong PIN was presented.

EIDAuthenticate can be used for UAC prompt even for administrator when the local policy "*User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode*" is set to "*Prompt for credentials*".

Be careful to use EIDAuthenticate and not kerberos. You can look at the icons or the "certificate detail" link to make the difference.



User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Windows Command Processor
Verified publisher: **Microsoft Windows**
File origin: Hard drive on this computer

To continue, type an administrator password, and then click Yes.

Adiant

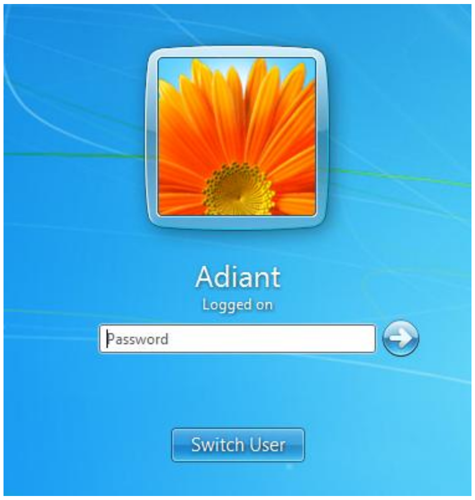
Administrator
Smart card credential

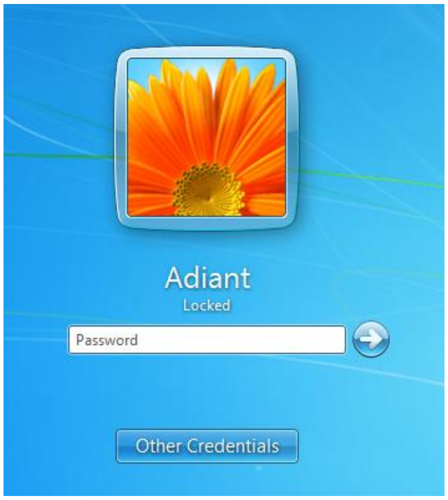
Administrator
Smart card credential

On Windows Visa / Seven and Windows Server 2008 / 2008 R2

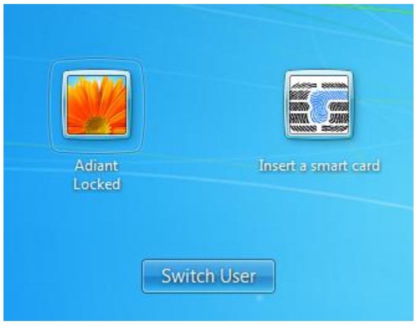
When only one user account is configured on a computer and that the last logon used the password, Windows shows by default the password prompt.

You have to click on "Switch User" or "Other Credentials" to display the smart card login option.



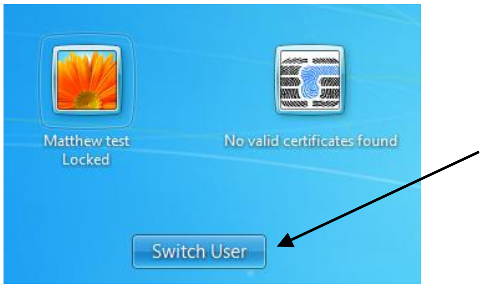


If there is no smart card inserted, an icon will be added if the computer is locked, nothing will be displayed on the normal logon.

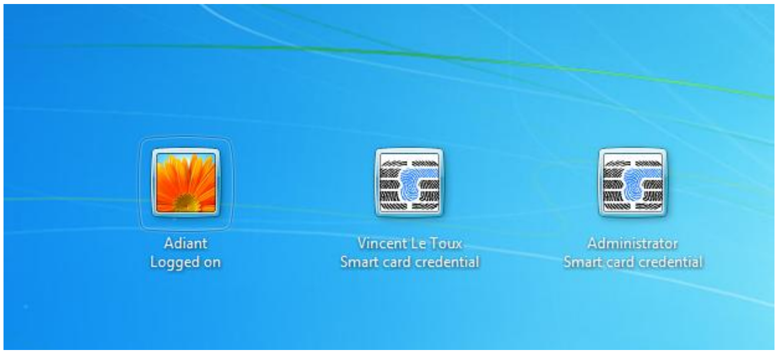


Insert a smart card

When a smart card is inserted, an icon is added for every certificates configured. Only certificate matching the current user is shown when the computer is locked. In this case, if there no certificate matching the current user but a certificate matching another user, the message "no valid certificates found". Press "Switch User" to select the other user and see the certificate which can be used for login.

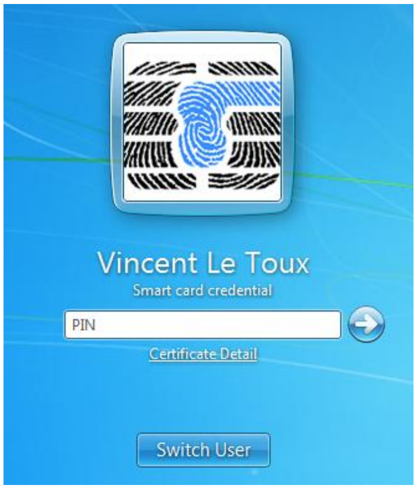


No valid certificates found

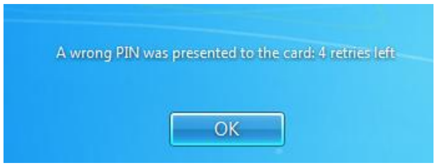


You can click on the icon to enter to the login procedure.

Enter the PIN to activate the login procedure.

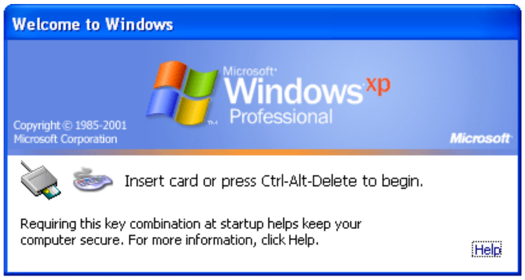


If no problem occures, the session will be opened. Else, an error message will be shown.


A wrong PIN was presented to the card: 4 retries left

On Windows XP and Windows Server 2003

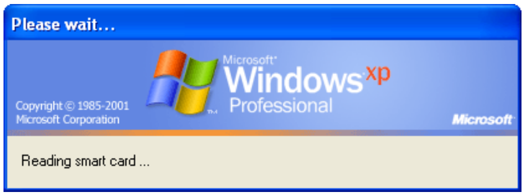
The welcome screen is modified to show "Insert Card".


Welcome to Windows
Microsoft Windows xp Professional
Copyright © 1985-2001 Microsoft Corporation
Microsoft
Help

Insert card or press Ctrl-Alt-Delete to begin.

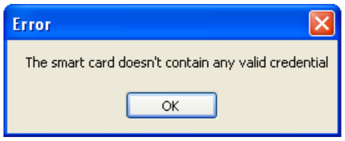
Requiring this key combination at startup helps keep your computer secure. For more information, click Help.

When a smart card is inserted, a cinematic is shown while the card is read.


Please wait...
Microsoft Windows xp Professional
Copyright © 1985-2001 Microsoft Corporation
Microsoft

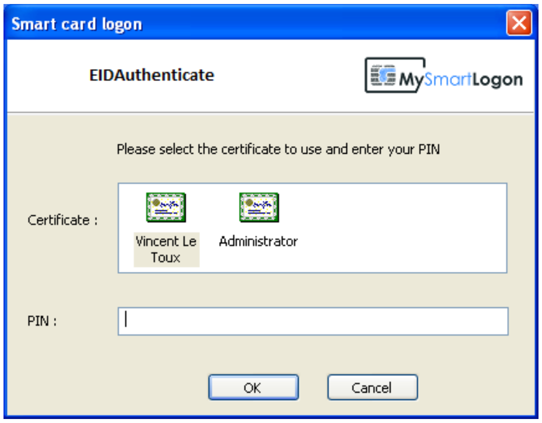
Reading smart card ...

If the program doesn't find certificates already mapped to an account, an error is shown.



The smart card doesn't contain any valid credential

Else, the logon screen appears.

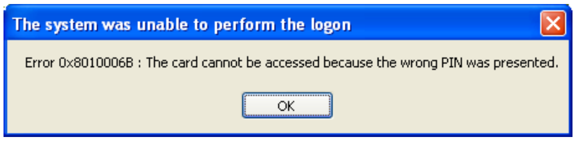


Please select the certificate to use and enter your PIN

Certificate :

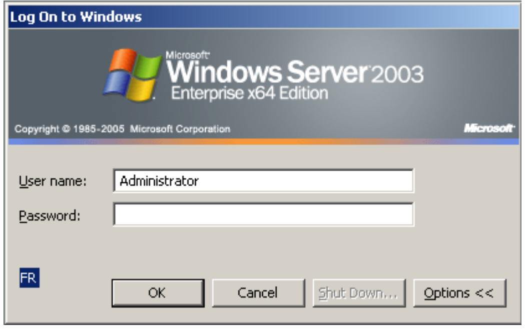
PIN :

If everything went fine, the session will be opened. Else, an error message will be shown.



Error 0x8010006B : The card cannot be accessed because the wrong PIN was presented.

On Windows 2003, by default when a user log off, the following dialog is shown.

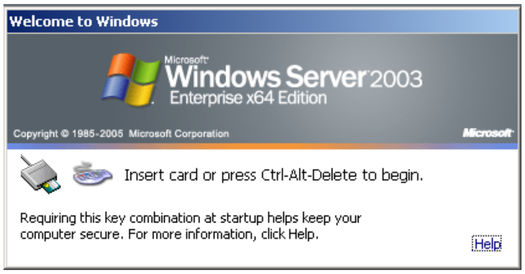


Log On to Windows

User name: Administrator

Password:

This dialog doesn't receive the smart card events. Press cancel to return to the "Ctrl-Alt-Delete" screen.



Welcome to Windows

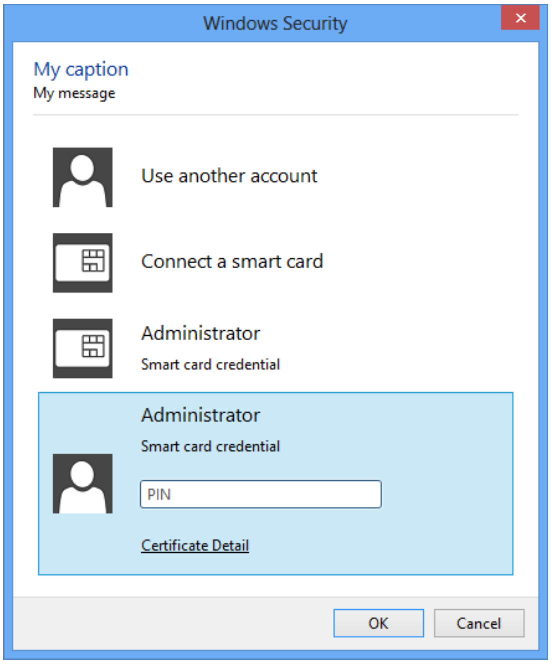
Insert card or press Ctrl-Alt-Delete to begin.

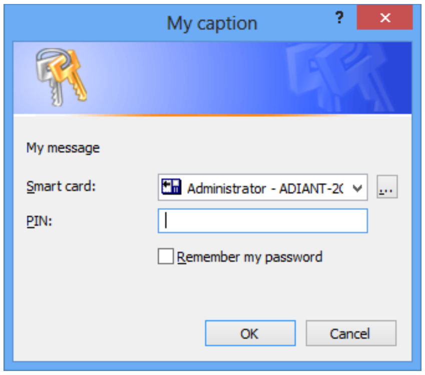
Requiring this key combination at startup helps keep your computer secure. For more information, click Help.

With other applications

EIDAuthenticate can also be used by third applications.

Note : this functionality is not available on Windows XP and Windows 2003 on terminal server when the smart card is remotely connected.





Smart card: Administrator - ADIANT-2(

Application should use CredUIPromptForWindowsCredentials or CredUIPromptForCredentials to collect credentials then call LsaLogonUser to open an interactive session or call AcquireCredentialsHandle / InitializeSecurityContext / AcceptSecurityContext / ImpersonateSecurityContext to open a network session using a custom client / server protocol.

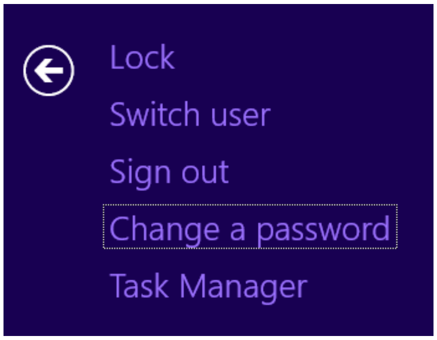
Contact support@mysmartlogon.com for more information.

PIN Change

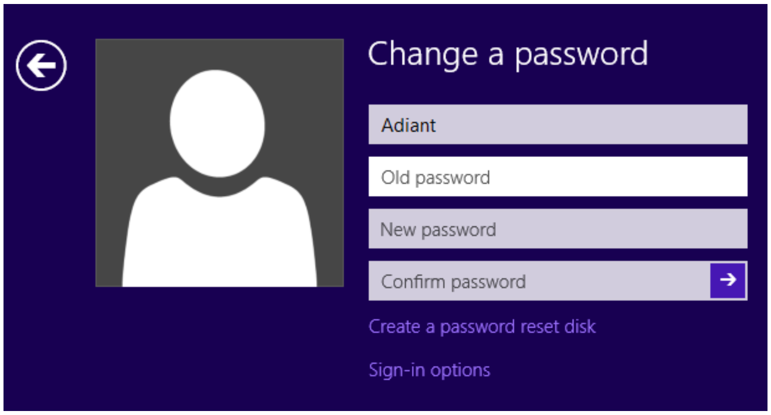
This procedure describes how to change the user PIN (not the admin PIN) of a smart card using the Microsoft Base Smart Card Cryptographic Provider (smart card having a minidriver). Smart card using their own cryptographic service provider (CSP) can't use these service.

On Windows 8 / Windows 2012 Server

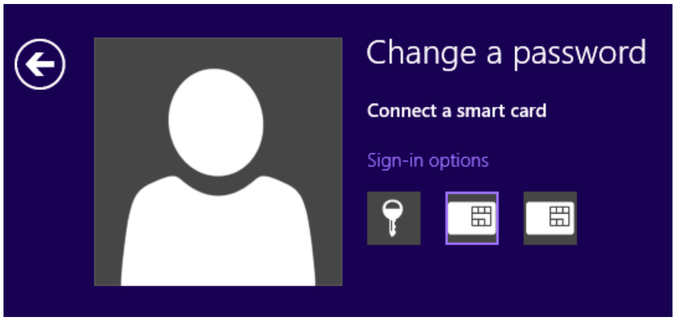
Press Ctrl+Alt+Del and choose "Change a password"



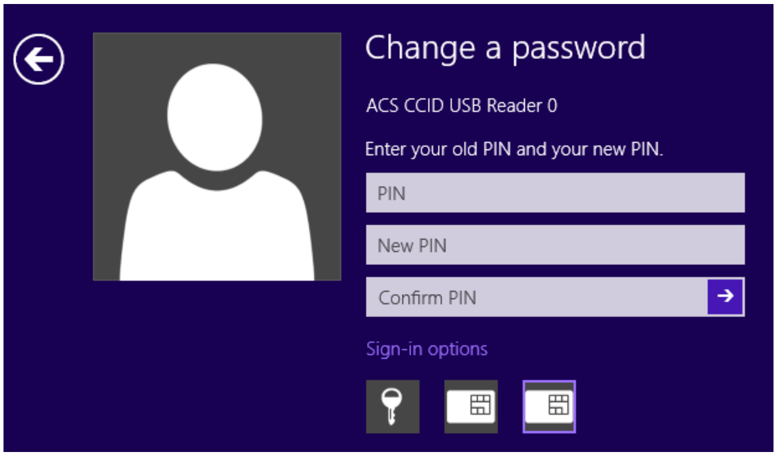
Click on "Sign-in options"



Click on the icon which represents your smart card reader



Enter the old PIN, the new PIN and press Enter.



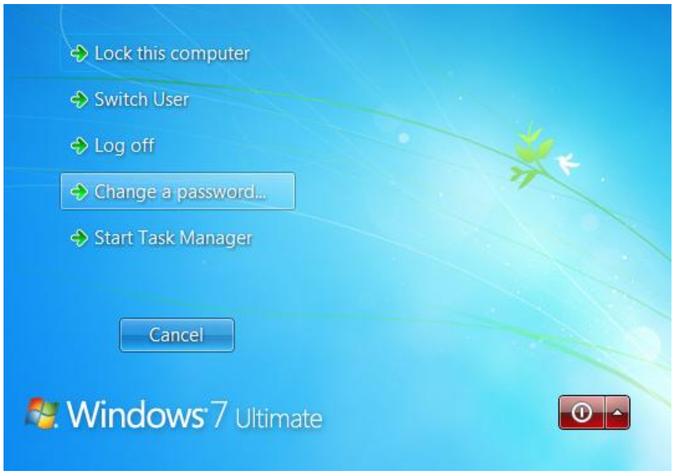
Change a password

ACS CCID USB Reader 0

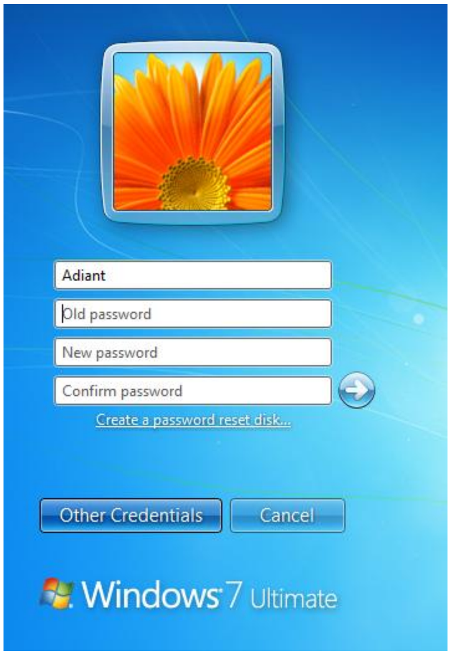
Enter your old PIN and your new PIN.

On Windows Vista / Seven / Windows Server 2008 and Windows Server 2008 R2

Press Ctrl+Alt+Del and choose "Change a password"

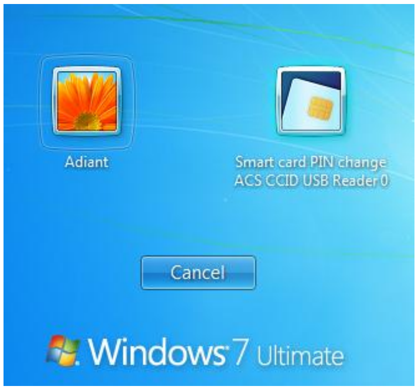


Click on "Other credentials"

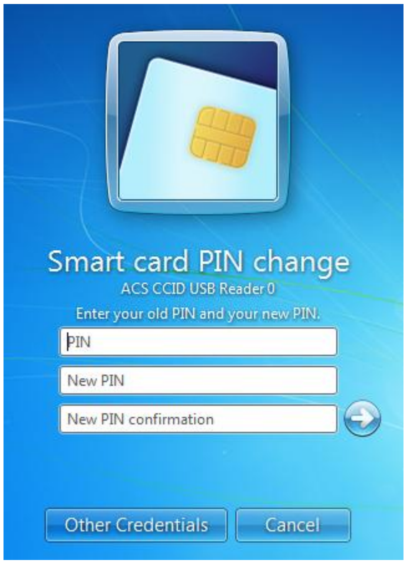


Adiant

Click on the icon which represents your smart card reader



Enter the old PIN, the new PIN and press Enter.



Smart card PIN change

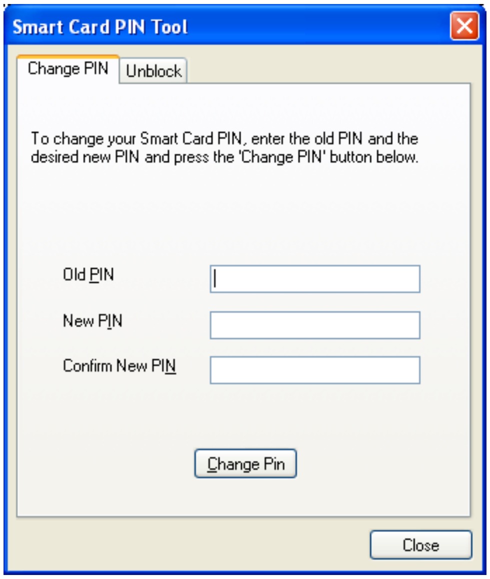
ACS CCID USB Reader 0

Enter your old PIN and your new PIN.

Reference : http://msdn.microsoft.com/en-us/library/bb905527.aspx

On Windows XP / Windows 2003

Clic on start -> run then enter "pintool"



To change your Smart Card PIN, enter the old PIN and the desired new PIN and press the 'Change PIN' button below.

Reference : http://download.microsoft.com/download/f/4/f/f4f3c957-057c-4acb-b10c-bb6087045025/WSCFDepl.doc

Terminal Server

Microsoft introduced NLA starting Windows Vista.

Windows XP or Windows 2003 acting as a server

The EIDAuthenticate logon prompt is embedded inside the RDP session.

Windows 2008 or greater with Windows XP or Windows 2003 as client

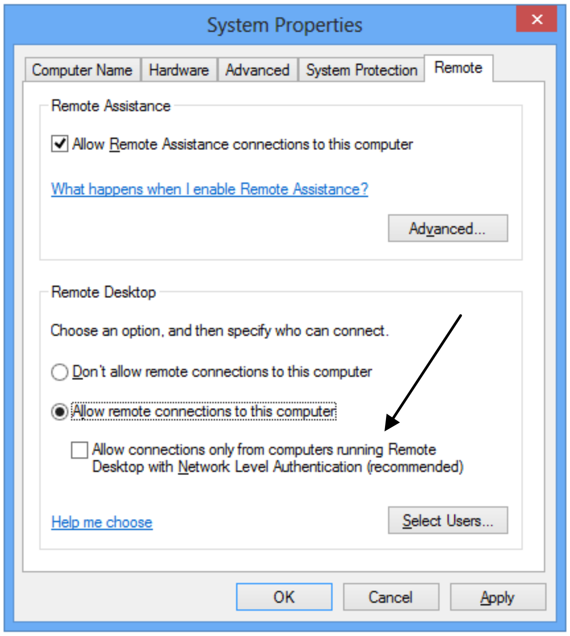
Windows 2008 and Vista introduced a security enhancement named NLA (network level authentication). By authenticating the user at the very beginning of the session, it limits the resources allocated and prevents denial of service attacks.

Non NLA authentication must be allowed (as classic password authentication) to work.

Windows Vista as a client to Vista / 2008

You must connect without NLA Authentication.

Verify that non NLA session is authorized. You can disable NLA on the server using the system properties. Just **deselect** "*Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)*".



☑ Allow Remote Assistance connections to this computer

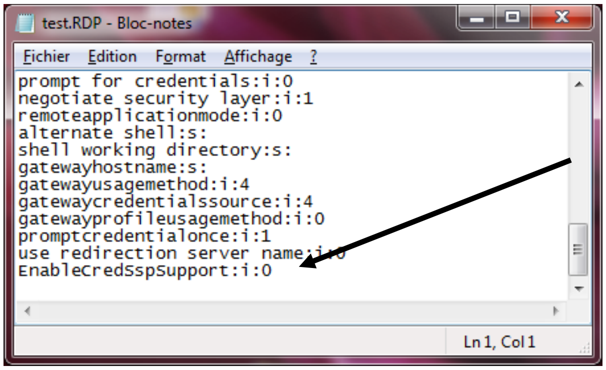
Choose an option, and then specify who can connect.

○ Don't allow remote connections to this computer

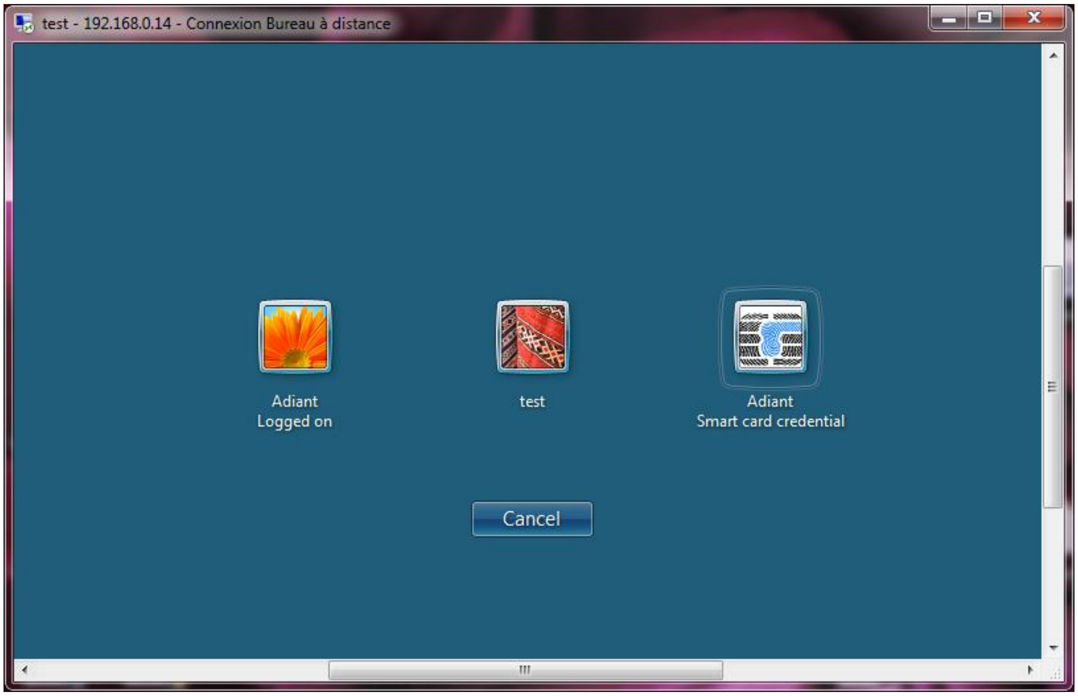
● Allow remote connections to this computer

□ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

You have to disable NLA on the client for this session by editing the rdp file related to this connexion using notepad and append the following line : **EnableCredSspSupport:i:0**



```
prompt for credentials:i:0
negotiate security layer:i:1
remoteapplicationmode:i:0
alternate shell:s:
shell working directory:s:
gatewayhostname:s:
gatewayusagemethod:i:4
gatewaycredentialssource:i:4
gatewayprofileusagemethod:i:0
promptcredentialonce:i:1
use redirection server name:i:0
EnableCredSspSupport:i:0
```



Windows Seven / 2008 R2 to Seven / 2008 R2 or later

You can connect without NLA (see above) or with NLA (see below).

You MUST install EIDAuthenticate on both server and client if you want to use Network Layer Authentication. However two authentications will be needed. The first is the NLA authentication, the second when the logon screen will be opened inside the Terminal session.

The two authentications are by design and can't be bypassed.

EIDAuthenticate is NLA compliant only since the version 1.0.0.0 and with x64 systems.

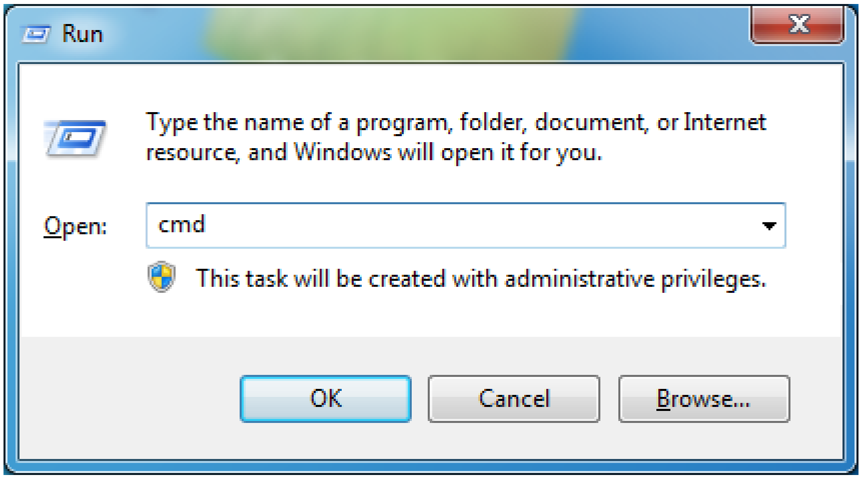
Troubleshooting

Using certutil

Certutil is a troubleshooting tool edited by Microsoft.

Note : certutil.exe is installed by default starting Windows Vista and Windows 2008. Certutil can be installed on Windows XP by the package "WindowsServer2003-KB304718-AdministrationToolsPack"

You can run certutil by typing Windows +R



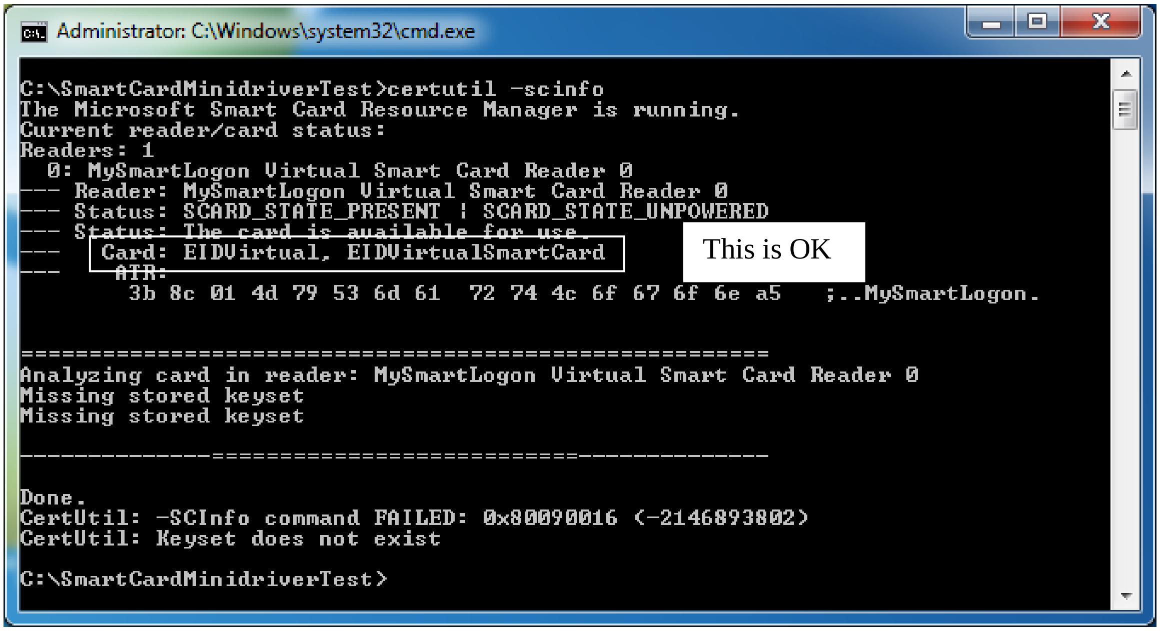
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

This task will be created with administrative privileges.

Then “cmd” then “certutil -scinfo”

Expected diagnostic of a healthy smart card



```
C:\SmartCardMinidriverTest>certutil -scinfo
The Microsoft Smart Card Resource Manager is running.
Current reader/card status:
Readers: 1
  0: MySmartLogon Virtual Smart Card Reader 0
--- Reader: MySmartLogon Virtual Smart Card Reader 0
--- Status: SCARD_STATE_PRESENT | SCARD_STATE_UNPOWERED
--- Status: The card is available for use.
---   Card: EIDVirtual, EIDVirtualSmartCard
---    ATR:
        3b 8c 01 4d 79 53 6d 61  72 74 4c 6f 67 6f 6e a5   ;..MySmartLogon.


=======================================================
Analyzing card in reader: MySmartLogon Virtual Smart Card Reader 0
Missing stored keyset
Missing stored keyset

--------------===========================--------------

Done.
CertUtil: -SCInfo command FAILED: 0x80090016 (-2146893802)
CertUtil: Keyset does not exist

C:\SmartCardMinidriverTest>
```

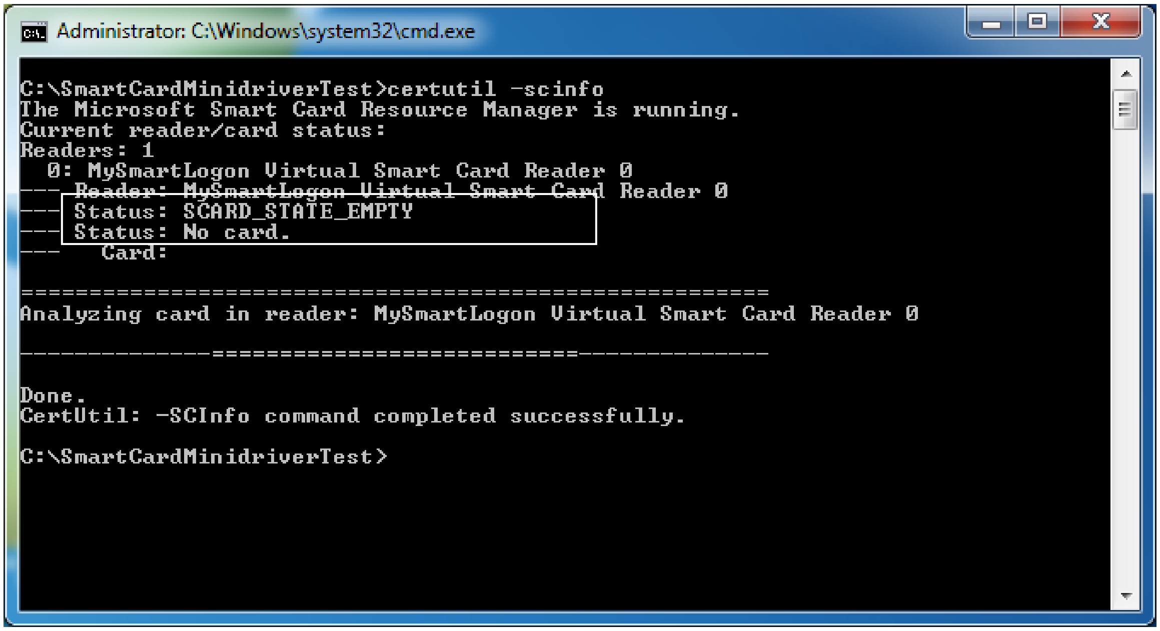
This is OK

The previous screenshot shows an empty smart card, without any certificate or private key stored (the KeySet does not exist)

(Look at the ATR and the mention “SCARD_STATE_PRESENT”)

Smart card absent

An empty smart card reader will produce the following output :



```
C:\SmartCardMinidriverTest>certutil -scinfo
The Microsoft Smart Card Resource Manager is running.
Current reader/card status:
Readers: 1
  0: MySmartLogon Virtual Smart Card Reader 0
--- Reader: MySmartLogon Virtual Smart Card Reader 0
--- Status: SCARD_STATE_EMPTY
--- Status: No card.
---   Card:

=======================================================
Analyzing card in reader: MySmartLogon Virtual Smart Card Reader 0

--------------===========================--------------

Done.
CertUtil: -SCInfo command completed successfully.

C:\SmartCardMinidriverTest>
```

(Look at the mention “SCARD_STATE_EMPTY”)

Causes :

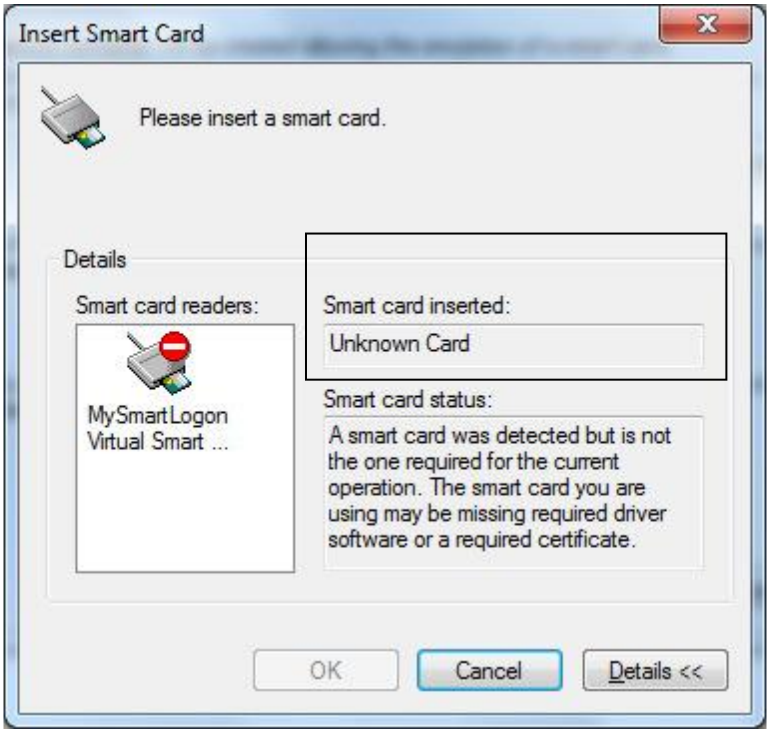
- A smart card not compatible has been connected
- The smart card reader doesn’t recognize the smart card

Solutions :

- Check the connections between the smart card and the reader

A minidriver or a CSP has not been installed

A minidriver or a CSP (the driver of the smart card and not for the reader) not installed will produce the following results :



Insert Smart Card

Please insert a smart card.

Details

Smart card readers:

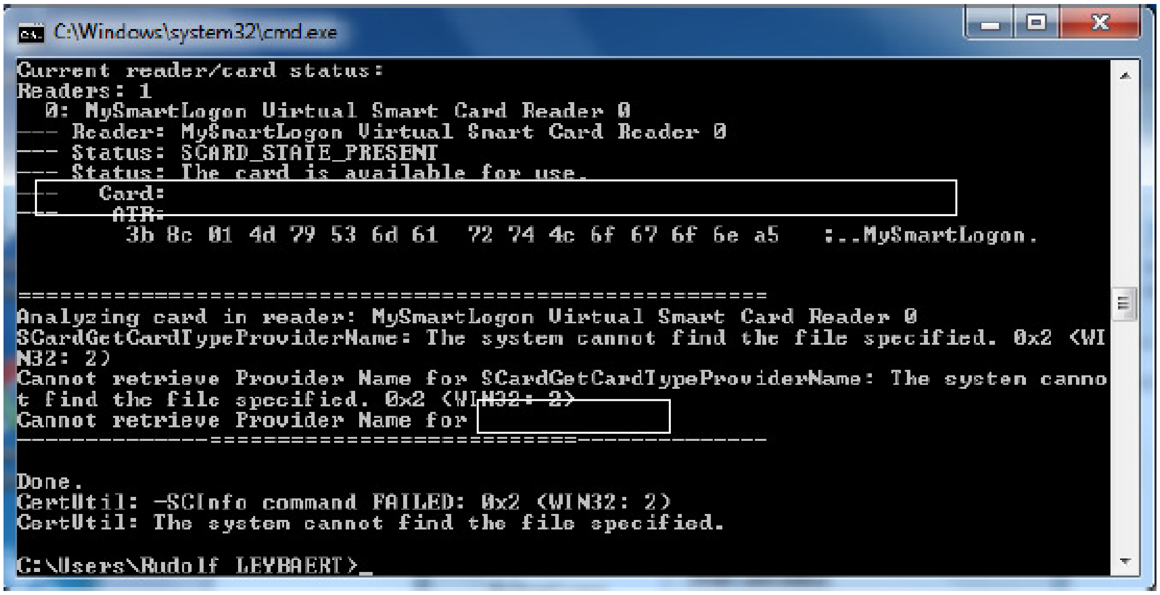
MySmartLogon Virtual Smart ...

Smart card inserted:

Unknown Card

Smart card status:

A smart card was detected but is not the one required for the current operation. The smart card you are using may be missing required driver software or a required certificate.



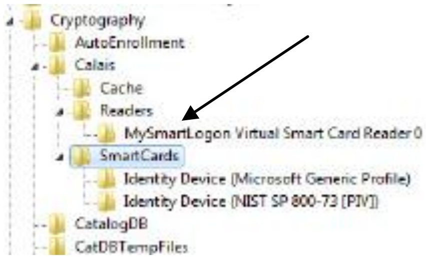
C:\Windows\system32\cmd.exe

```
Current reader/card status:
Readers: 1
  0: MySmartLogon Virtual Smart Card Reader 0
--- Reader: MySmartLogon Virtual Smart Card Reader 0
--- Status: SCARD_STATE_PRESENT
--- Status: The card is available for use.
---   Card:
---    ATR:
        3b 8c 01 4d 79 53 6d 61  72 74 4c 6f 67 6f 6e a5   ;..MySmartLogon.


=======================================================
Analyzing card in reader: MySmartLogon Virtual Smart Card Reader 0
SCardGetCardTypeProviderName: The system cannot find the file specified. 0x2 (WI
N32: 2)
Cannot retrieve Provider Name for SCardGetCardTypeProviderName: The system canno
t find the file specified. 0x2 (WIN32: 2)
Cannot retrieve Provider Name for
-------------------------------------------------------

Done.
CertUtil: -SCInfo command FAILED: 0x2 (WIN32: 2)
CertUtil: The system cannot find the file specified.

C:\Users\Rudolf LEYBAERT>_
```

An ATR entry, here 3b 8c 01 …, means that a smart card has been inserted.

However the empty line for “Card” means that the system couldn’t find a driver. Moreover, the system returns an error about “Cannot retrieve Provider Name for <null>“.

Also the “CALAIS” database in the registry won’t show an entry for the smart card.



```
Cryptography
  AutoEnrollment
  Calais
    Cache
    Readers
      MySmartLogon Virtual Smart Card Reader 0
    SmartCards
      Identity Device (Microsoft Generic Profile)
      Identity Device (NIST SP 800-73 [PIV])
  CatalogDB
  CatDBTempFiles
```

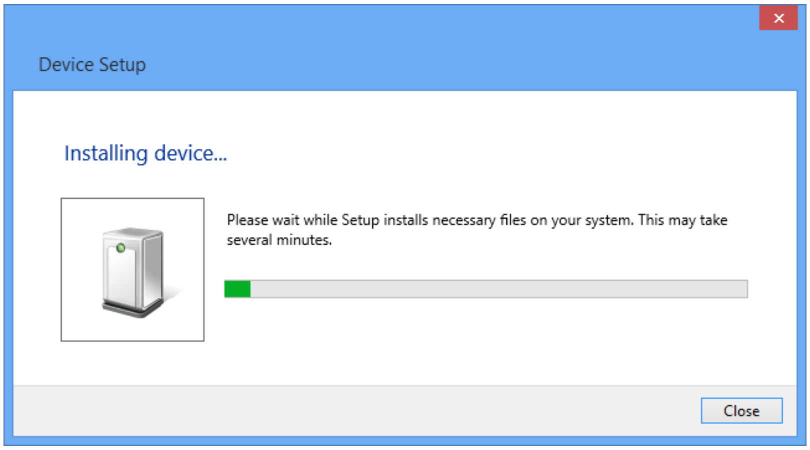
Note : on 64 bits systems there are two CALAIS database : the 64 bits one and the other in *WOW6432Node*.

Causes :

- No CSP or minidriver has been installed
- A 32 bits but not 64 bits CSP or minidriver has been installed on a 64 bits system
- The smart card don’t have cryptographic capabilities exposed (EMV cards, NFC, …)

Solutions :

1. Ask your manufacturer for proper software
2. Use compatible smart card
3. Wait for the installation of the driver if it is auto downloaded from Microsoft Update.



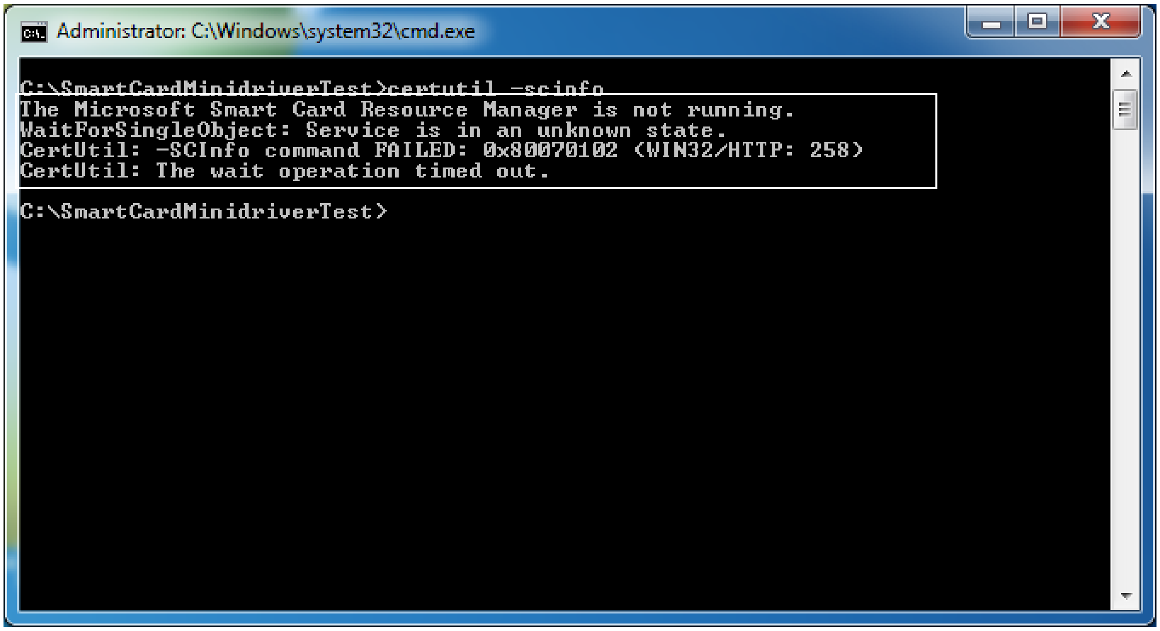
Device Setup

Installing device...

Please wait while Setup installs necessary files on your system. This may take several minutes.

The smart card resource manager is not running

If the smart card service is not runing, the following error will be showed :



```
C:\SmartCardMinidriverTest>certutil -scinfo
The Microsoft Smart Card Resource Manager is not running.
WaitForSingleObject: Service is in an unknown state.
CertUtil: -SCInfo command FAILED: 0x80070102 (WIN32/HTTP: 258)
CertUtil: The wait operation timed out.

C:\SmartCardMinidriverTest>
```

Causes :

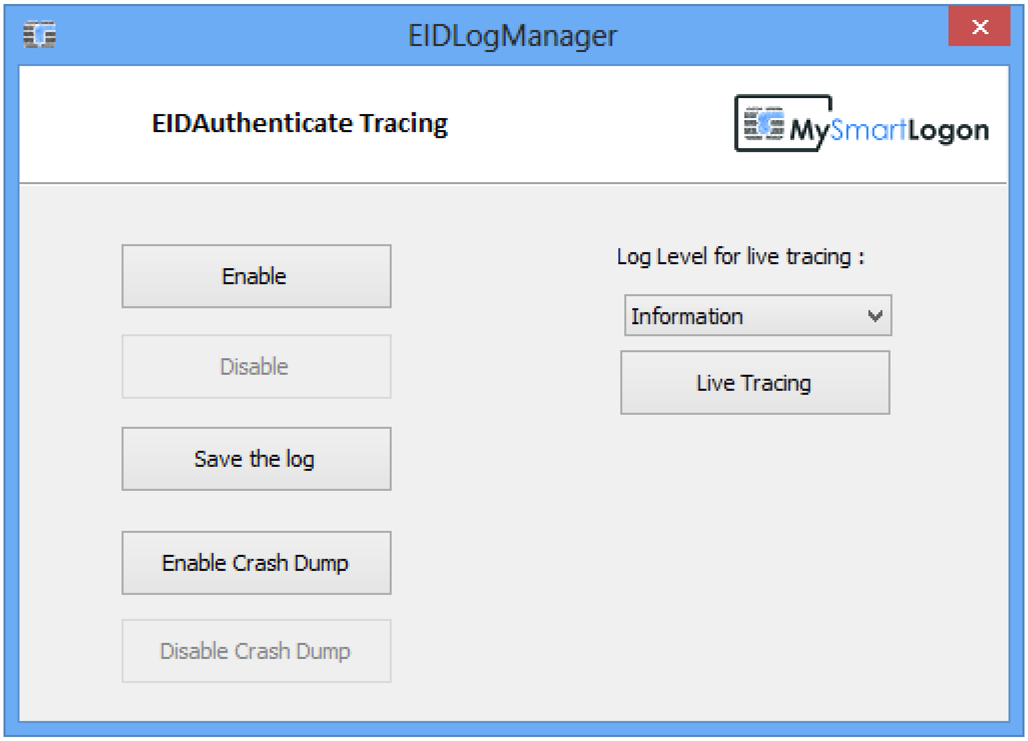
- The “Smart card” service has been disabled
- A smart card reader has not been connected

Solutions

- Go to “service” (administrative tools), find the service and start it

Using the log manager

By default the Tracing tool named "EIDLogmanager" is installed in "C:\Program Files\EIDAuthenticate"



Log Level for live tracing : Information

Record a trace

A recorded trace is the preferred way when contacting the support.

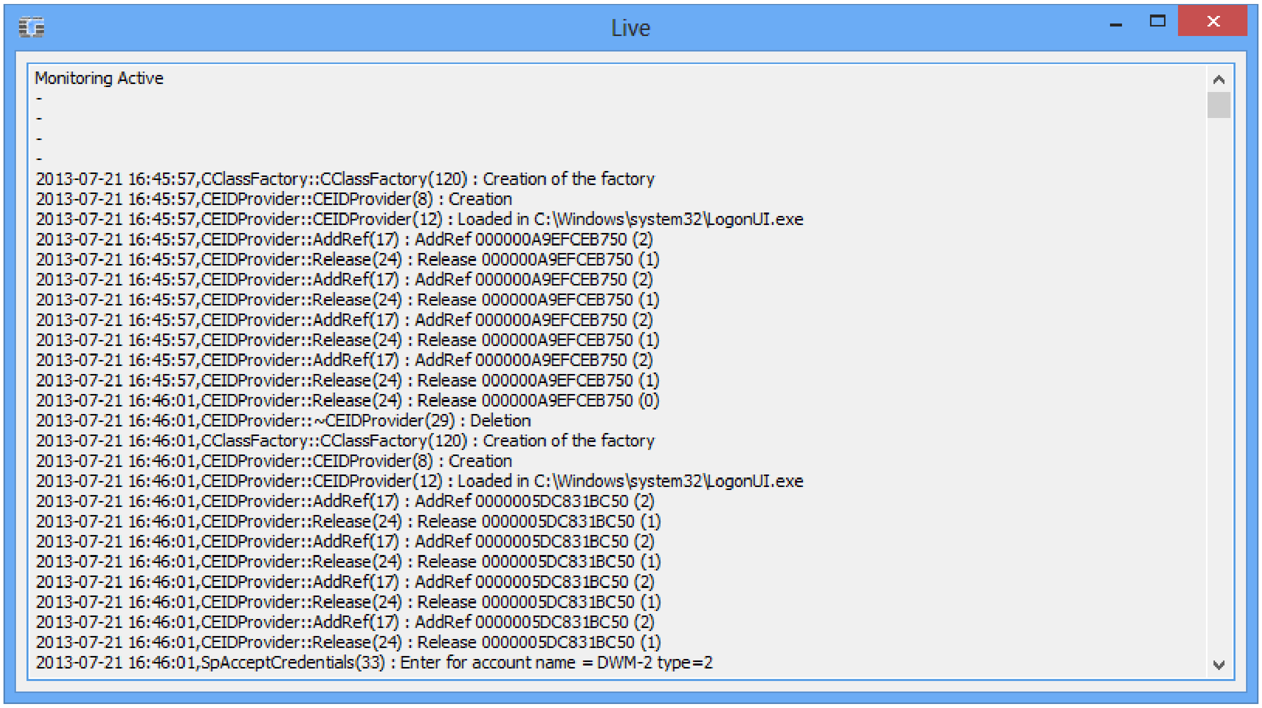
1. Click on "Enable log"
2. Do some action with EIDAuthenticate (run the wizard, try to log on, ...)
3. Click on "Save Log"
4. Select an output file (default named Report.txt on the desktop)

Note : The PIN or password is not written to the log. However, this log may contains user names or smart card informations like its brand or serial number.

Note : Logging is still active after a reboot

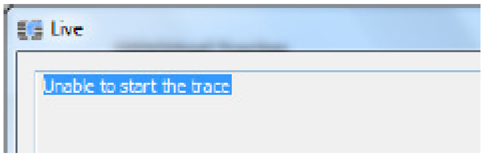
View live tracing

1. Select the level for live tracing (default is : information)
2. Click on “Live Tracing”



```
Monitoring Active
-
-
-
-
2013-07-21 16:45:57,CClassFactory::CClassFactory(120) : Creation of the factory
2013-07-21 16:45:57,CEIDProvider::CEIDProvider(8) : Creation
2013-07-21 16:45:57,CEIDProvider::CEIDProvider(12) : Loaded in C:\Windows\system32\LogonUI.exe
2013-07-21 16:45:57,CEIDProvider::AddRef(17) : AddRef 000000A9EFCEB750 (2)
2013-07-21 16:45:57,CEIDProvider::Release(24) : Release 000000A9EFCEB750 (1)
2013-07-21 16:45:57,CEIDProvider::AddRef(17) : AddRef 000000A9EFCEB750 (2)
2013-07-21 16:45:57,CEIDProvider::Release(24) : Release 000000A9EFCEB750 (1)
2013-07-21 16:45:57,CEIDProvider::AddRef(17) : AddRef 000000A9EFCEB750 (2)
2013-07-21 16:45:57,CEIDProvider::Release(24) : Release 000000A9EFCEB750 (1)
2013-07-21 16:45:57,CEIDProvider::AddRef(17) : AddRef 000000A9EFCEB750 (2)
2013-07-21 16:45:57,CEIDProvider::Release(24) : Release 000000A9EFCEB750 (1)
2013-07-21 16:46:01,CEIDProvider::Release(24) : Release 000000A9EFCEB750 (0)
2013-07-21 16:46:01,CEIDProvider::~CEIDProvider(29) : Deletion
2013-07-21 16:46:01,CClassFactory::CClassFactory(120) : Creation of the factory
2013-07-21 16:46:01,CEIDProvider::CEIDProvider(8) : Creation
2013-07-21 16:46:01,CEIDProvider::CEIDProvider(12) : Loaded in C:\Windows\system32\LogonUI.exe
2013-07-21 16:46:01,CEIDProvider::AddRef(17) : AddRef 0000005DC831BC50 (2)
2013-07-21 16:46:01,CEIDProvider::Release(24) : Release 0000005DC831BC50 (1)
2013-07-21 16:46:01,CEIDProvider::AddRef(17) : AddRef 0000005DC831BC50 (2)
2013-07-21 16:46:01,CEIDProvider::Release(24) : Release 0000005DC831BC50 (1)
2013-07-21 16:46:01,CEIDProvider::AddRef(17) : AddRef 0000005DC831BC50 (2)
2013-07-21 16:46:01,CEIDProvider::Release(24) : Release 0000005DC831BC50 (1)
2013-07-21 16:46:01,CEIDProvider::AddRef(17) : AddRef 0000005DC831BC50 (2)
2013-07-21 16:46:01,CEIDProvider::Release(24) : Release 0000005DC831BC50 (1)
2013-07-21 16:46:01,SpAcceptCredentials(33) : Enter for account name = DWM-2 type=2
```

If the live trace can’t start, you may have not the permission to run ETW (event tracing). This happens in large organization were permissions are restricted. You can run Process Monitor on the tracing process to look for errors.



```
Unable to start the trace
```

Capturing manually the traces

The logs can be captured manually using ETW tools.

Using a command line :

1) Register the trace provider

logman create trace EIDAuthenticateTrace -p {4AE3C5F9-BB41-41A5-A82B-80EEE8C38C52} -o trace.etl

The registration can be deleted later using the command : *logman delete EIDAuthenticateTrace*

2) Start the trace provider

logman start EIDAuthenticateTrace

3) Do the actions to be traced

4) Stop the trace provider to flush the trace file to the disk

logman stop EIDAuthenticateTrace

The etl file produced can be sent to the support.

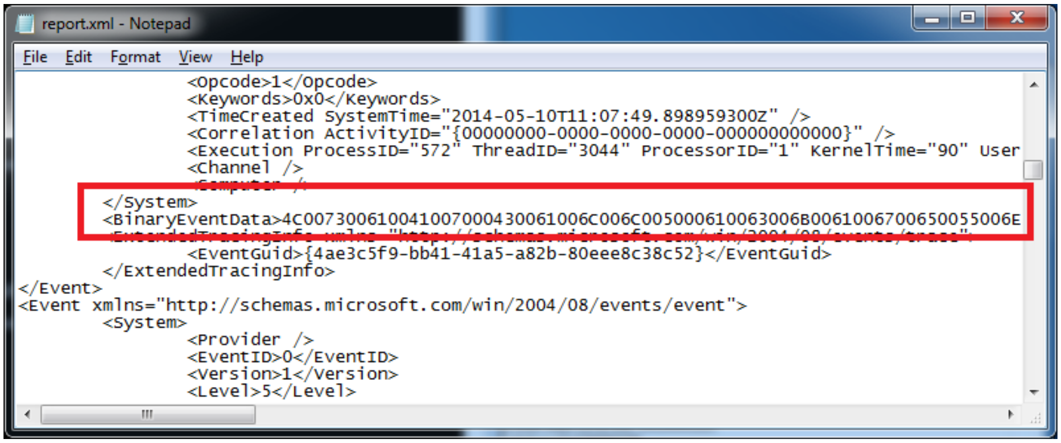
The trace messages can be extracted from the etl file using the command :

tracerpt trace_000001.etl -o report.xml

This command produce a xml file which contains the trace in hexadecimal encoding.

In this case 4C00 7300 6100 4100 7000 4300 6100 6C00 ...

L s a A p C a l ...



```
                <Opcode>1</Opcode>
                <Keywords>0x0</Keywords>
                <TimeCreated SystemTime="2014-05-10T11:07:49.898959300Z" />
                <Correlation ActivityID="{00000000-0000-0000-0000-000000000000}" />
                <Execution ProcessID="572" ThreadID="3044" ProcessorID="1" KernelTime="90" User
                <Channel />
                <Computer />
        </System>
        <BinaryEventData>4C0073006100410070004300610 06C006C0050006100630 06B00610067006500550 06E
        <ExtendedTracingInfo xmlns="http://schemas.microsoft.com/win/2004/08/events/trace">
                <EventGuid>{4ae3c5f9-bb41-41a5-a82b-80eee8c38c52}</EventGuid>
        </ExtendedTracingInfo>
</Event>
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
        <System>
                <Provider />
                <EventID>0</EventID>
                <Version>1</Version>
                <Level>5</Level>
```

How to enable crash dump

On some exceptional circumstance, EIDAuthenticate may crash the Local Security Authority (LSA - lsass.exe).

Click on Enable Crash Dump to create a memory dump on the desktop each time the process lsass.exe crashes. (this program set the right keys in the registry).

Note : most crashes are caused by buggy smart card drivers. While this as a few effects on day-to-day program, the LSA is very sensitive to memory problems.

Note : a memory dump of the lsass.exe program may contain sensitive information like account names or passwords.

Troubleshooting the setup

You can run the msi tracing procedure :

msiexec /i EIDVirtualpackage.msi /L*v log.txt