

User Guide

ActivClient for Windows 6.2

ACTIVIDENTITY

Table of Contents

Chapter 1: Introduction 5
About ActivClient 5
Getting Started 6
Your First Steps with ActivClient 6
Working with the User Console 8
What can you do with the User Console? 8
Access the User Console 9

Chapter 2: Managing Smart Cards 11
Initialize a Smart Card with the PIN Initialization Tool 11
Supported Smart Cards 11
Blank Smart Cards 11
Standalone Smart Cards 11
Access the PIN Initialization Tool 12
Initialize your Smart Card using the PIN Initialization Tool 12
Reset a Smart Card 13
Change your Smart Card PIN 15
Access the PIN Change Tool 15
Unlock your Smart Card 16
View your Unlock Code 16
Unlock a Smart Card Initialized with ActivClient 17
Unlock a Smart Card Initialized by the Administrator 18
Access the Unlock Smart Card Dialog 19
Update your Smart Card 20
Automatic Check for Updates 20
Manual Check for Updates 21
Smart Card or Certificate Expiration 22
View Smart Card Information 23

Chapter 3: Managing Digital Certificates 25
Download a Certificate with Microsoft Internet Explorer 25
Prerequisites 25
Download a Certificate with Firefox 26
Download an Entrust Profile 26
Manage User and CA Certificates 31
View your Certificate 31
Import a User Certificate 32
Import a CA Certificate 33

Document Version 06.2.09 | ©2009 ActivIdentity, Inc.

Export a Certificate . . . 33
Delete a Certificate . . . 34
Select Certificates for Windows PKI Logon . . . 34
Deselect a Logon Certificate . . . 35
Make Certificates Available to Windows . . . 36
Manage Certificates in Microsoft Outlook . . . 36
Automatically Configure your Microsoft Outlook Security Profile . . . 36
Automatically Publish your Certificates to the Global Address List . . . 37
Automatically Add Certificates to Microsoft Outlook Contacts . . . 38

Chapter 4: Using Digital Certificates . . . 39
Log on to Windows with a Certificate . . . 39
Prerequisites . . . 39
Lock your Workstation on Smart Card Removal . . . 40
Card Unattended Notification . . . 41
Use Windows Dial-Up/VPN for Remote Access . . . 41
Use a Non-Microsoft VPN for Remote Access . . . 42
Access a Secure Web Site . . . 42
Access a Secure Web Site with Internet Explorer . . . 42
Access a Secure Web Site with Firefox . . . 43
Log on to Entrust Entelligence . . . 44
Send/Read Signed and Encrypted Email Messages with Microsoft Outlook . . . 45
Send/Read Signed Email Messages . . . 45
Send Signed Email Messages . . . 45
Read Signed Email Messages . . . 46
Send/Read Encrypted Email Messages . . . 46
Send Encrypted Email Messages . . . 47
Read Encrypted Email Messages . . . 47
Automatically Decrypt and Save Emails . . . 47
Send/Read Signed and Encrypted Mails with Thunderbird . . . 48
Send/Read Signed Email Messages . . . 48
Send Signed Email Messages . . . 48
Read Signed Email Messages . . . 48
Send/Read Encrypted Email messages . . . 49
Send Encrypted Email Messages . . . 49
Read Encrypted Email Messages . . . 49
Encrypt/Decrypt Files with EFS . . . 50
Configure your Workstation for EFS and Select/Generate a Smart Card Encryption Certificate . . . 50
Encrypt a File or Folder with EFS . . . 50
Decrypt a File or Folder with EFS . . . 51
Update EFS Certificates and Re-Encrypt Files . . . 51

Recover Encrypted Files . . . 52

Chapter 5: Managing Remote Access/OTP . . . 53
Synchronize your Smart Card . . . 53
Prerequisites . . . 53
Configure your Remote Access User Name . . . 54

Chapter 6: Using Remote Access/OTP . . . 56
Log on to Check Point VPN-1 with a One-Time Password . . . 56
Prerequisites . . . 56
Automatically Generate a One-Time Password . . . 57
Manually Generate a One-Time Password . . . 58

Chapter 7: Viewing Personal Information . . . 59
About Personal Information . . . 59
View “My Personal Info” on CAC and PIV Cards . . . 59

Chapter 8: Using and Managing ActivClient . . . 61
View ActivClient System Information . . . 61
Troubleshoot ActivClient . . . 62
Perform Advanced Diagnostics . . . 64
Use the Forget state for all cards Option . . . 66
Activate Log Files from the ActivClient User Console . . . 67
Configure ActivClient . . . 68
Auto-Update Service . . . 69

Chapter 9: Using ActivClient with Terminal Services . . . 70
Log on to a Citrix Session . . . 70
Prerequisites . . . 70
Sample Citrix Sessions . . . 71
Log on using Citrix ICA Client Program Neighborhood . . . 71
Log on using Citrix ICA Client Program Neighborhood Agent . . . 71
Log on using Citrix Web Interface . . . 71
Use your Smart Card Inside a Citrix Session . . . 72
Log on to a Remote Desktop Session . . . 72
Use your Smart Card in a Remote Desktop Session . . . 73
Lock a Remote Desktop Session . . . 73

Appendix A: Terms and Acronyms . . . 74
Terms . . . 74
Acronyms . . . 75

Chapter 1: Introduction

In This Chapter

5 About ActivClient
6 Getting Started

This guide presents how to use ActivClient for authentication using your smart card. It also explains how to manage your smart card credentials and ActivClient itself.

This guide applies to all editions of ActivClient:

- ActivClient 32-bit
- ActivClient 64-bit
- ActivClient CAC 32-bit
- ActivClient CAC 64-bit

The differences related to specific editions are indicated where applicable.

Note: ActivClient CAC is an ActivClient edition configured for the US Department of Defense Common Access Card (CAC) deployment.

About ActivClient

ActivClient is the latest smart card and USB token middleware from ActivIdentity that allows enterprise and government customers to easily use smart cards and USB tokens for a wide variety of desktop, network security and productivity applications.

ActivClient enables the use of PKI certificates and keys, one-time password and static password credentials on a smart card or USB token to secure:

- Desktop applications
- Network logon
- Remote access
- Web logon
- E-mail
- Electronic transactions

For a complete overview of the capabilities and functions of ActivClient, see the *ActivClient for Windows Overview*.

This document is for:

- End users

Getting Started

This section explains the first steps you need to take with ActivClient and introduces the User Console.

Your First Steps with ActivClient

Depending on your organization's deployment process, you may need to configure your smart card before you can use it for authentication or digital signature operations.

Your first steps with ActivClient are determined by your:

- Smart card status (whether your administrator has prepared the card for you and it is ready to use, or not)
- ActivClient configuration (defined during ActivClient setup)

Table 1.1 lists the actions to take according to your smart card status:

Table 1.1: Getting started according to your smart card status

Smart card status	Action
You have a blank smart card (no PIN)	Your administrator has given you a blank smart card. You need to initialize the card before you can use it. 1. Log on to your workstation using the same user name and password that you used before installing ActivClient. 2. Initialize your new smart card and create your PIN, see "Initialize a Smart Card with the PIN Initialization Tool" on page 11". 3. Load credentials on to your smart card as described in "Managing Digital Certificates" on page 25". 4. Use your card to log on to your workstation (if your administrator instructs you to do so), sign emails, access secure Web sites, etc. 5. At any time, you can access the ActivClient User Console to configure ActivClient, your smart card, or your credentials. For more information, see "Working with the User Console" on page 8.

Table 1.1: Getting started according to your smart card status

Smart card status	Action
Your smart card is personalized with a PIN but is not configured for Windows PKI logon	Your administrator has given you a smart card and a PIN, and the smart card has already been personalized with your credentials (for example, with digital certificates - but not configured for Windows logon). Your card is ready to use. 1. Log on to your workstation using the same user name and password you used before installing ActivClient. 2. Use your card to sign emails, access secure Web sites, etc. 3. At any time, you can access the ActivClient User Console to configure ActivClient, your smart card, or your credentials. For more information, see "Working with the User Console" on page 8.
Your smart card is personalized with a PIN and a Windows PKI logon digital certificate	Your administrator has given you a smart card and a PIN, and the smart card has already been personalized with your credentials (including a digital certificate configured for Windows logon). Your card is ready to use. 1. Log on to your workstation using your smart card and your PIN. For more information, see "Log on to Windows with a Certificate" on page 39". 2. Use your card to sign emails, access secure Web sites, etc. 3. At any time, you can access the ActivClient User Console to configure ActivClient, your smart card, or your credentials. For more information, see "Working with the User Console" on page 8.

Working with the User Console

What can you do with the User Console?

Table 1.2 provides an overview of the ActivClient User Console tasks:

Table 1.2: User Console Tasks

You can	Action
Manage your digital certificates	• Import a CA digital certificate, see "Import a CA Certificate" on page 33 • Import a User digital certificate, see "Import a User Certificate" on page 32 • Export a digital certificate, see "Export a Certificate" on page 33 • View a digital certificate, see "View your Certificate" on page 31 • Delete a digital certificate, see "Delete a Certificate" on page 34 • Set a default certificate, see "Open the ActivClient User Console." on page 35 • Make your certificates available to Windows, see "Make Certificates Available to Windows" on page 36 • Add your certificates to the Global Address List (GAL), see "Automatically Publish your Certificates to the Global Address List" on page 37
Manage your one-time passwords	• Generate a one-time password, see "Automatically Generate a One-Time Password" on page 57 • Re-synchronize a one-time password, see "Synchronize your Smart Card" on page 53 • Configure a user name for OTP-based remote access, see "Configure your Remote Access User Name" on page 54
View your personal information	Only available for the US Department of Defense on Common Access Cards (CAC) or US Government Personal Identity Verification (PIV) cards. See "About Personal Information" on page 59.

Table 1.2: User Console Tasks

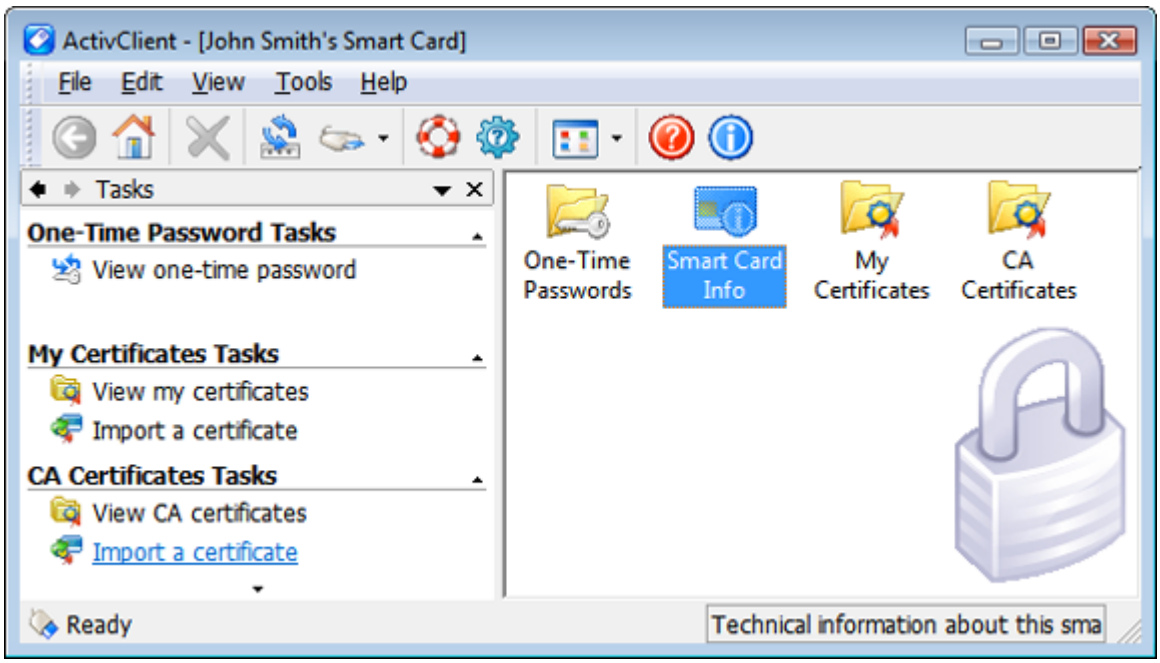
You can	Action
Manage your smart card	• Change your PIN code, see "Change your Smart Card PIN" on page 15 • View your smart card information, see "View Smart Card Information" on page 23 • Unlock your smart card, see "Unlock your Smart Card" on page 16 • Initialize your new smart card, see "Initialize a Smart Card with the PIN Initialization Tool" on page 11 • Reset your smart card, see "Reset a Smart Card" on page 13 • Update your smart card with ActivID CMS, see "Update your Smart Card" on page 20 • View your unlock code, see "View your Unlock Code" on page 16 • Select a smart card reader, from the Reader List icon on the Standard toolbar
Use ActivClient Tools to: • Troubleshoot • Diagnose • Configure advanced settings	• Run the Troubleshooting Wizard, see "Troubleshoot ActivClient" on page 62 • Run the Advanced Diagnostics Tool, see "Perform Advanced Diagnostics" on page 64 • Run the Advanced Configuration Manager, see "Configure ActivClient" on page 68

Access the User Console

To access the User Console, either:

- From the ActivClient Agent icon located in the Windows notification area:
  - Double-click the ActivClient Agent icon .
  - Left or right-click on the ActivClient Agent icon  and select **Open**.
- From the Windows Start menu, go to **Programs**, **ActivIdentity**, **ActivClient**, and select **User Console**.

  The ActivClient User Console is displayed.



For more information on the ActivClient User Console, see the *ActivClient for Windows Overview*.

Chapter 2: Managing Smart Cards

In This Chapter

11 Initialize a Smart Card with the PIN Initialization Tool
13 Reset a Smart Card
15 Change your Smart Card PIN
16 Unlock your Smart Card
20 Update your Smart Card
22 Smart Card or Certificate Expiration
23 View Smart Card Information

This chapter explains how to manage your smart card and your PIN code.

Initialize a Smart Card with the PIN Initialization Tool

To initialize your smart card you need to access the PIN Initialization Tool.

The PIN Initialization Tool allows you to:

- Initialize your smart card by setting a PIN code.
- Reset a PIN code while erasing the content of the smart card.

Before initializing, you need to verify that your smart card is supported by the tool.

Supported Smart Cards

PIN Initialization Tool supports blank and standalone smart cards.

Blank Smart Cards

Blank smart cards are cards with no applets uploaded. Once initialized by the PIN Initialization Tool, the smart cards is ready to use.

No unlock mechanism is available. If the smart card is locked due to too many wrong PIN entries or if you forget the PIN code, the smart card can be run through the PIN Initialization Tool again. You will be able to choose a new PIN code, but the previous content of the smart card will be completely erased.

Standalone Smart Cards

Standalone smart cards are cards with pre-loaded applets. They have an identifier such as S1, S4, O4 or S5 engraved on the lower right section of the back of the card.

At the end of initialization process, an unlock code is displayed. Write it down in a secure place. You will need the unlock code or a PIN code if you want to re-initialize the smart card and erase its content.

For the list of supported blank (ActivClient Standalone / Mini configuration) and standalone (ActivClient Standalone configuration) smart cards, see the *ActivClient for Windows Overview*.

Important

Repeated attempts to initialize a smart card that is not in a supported configuration can render the smart card permanently unusable.

Access the PIN Initialization Tool

Your options to access the PIN Initialization Tool depend on whether you have installed the User Console and ActivClient Agent.

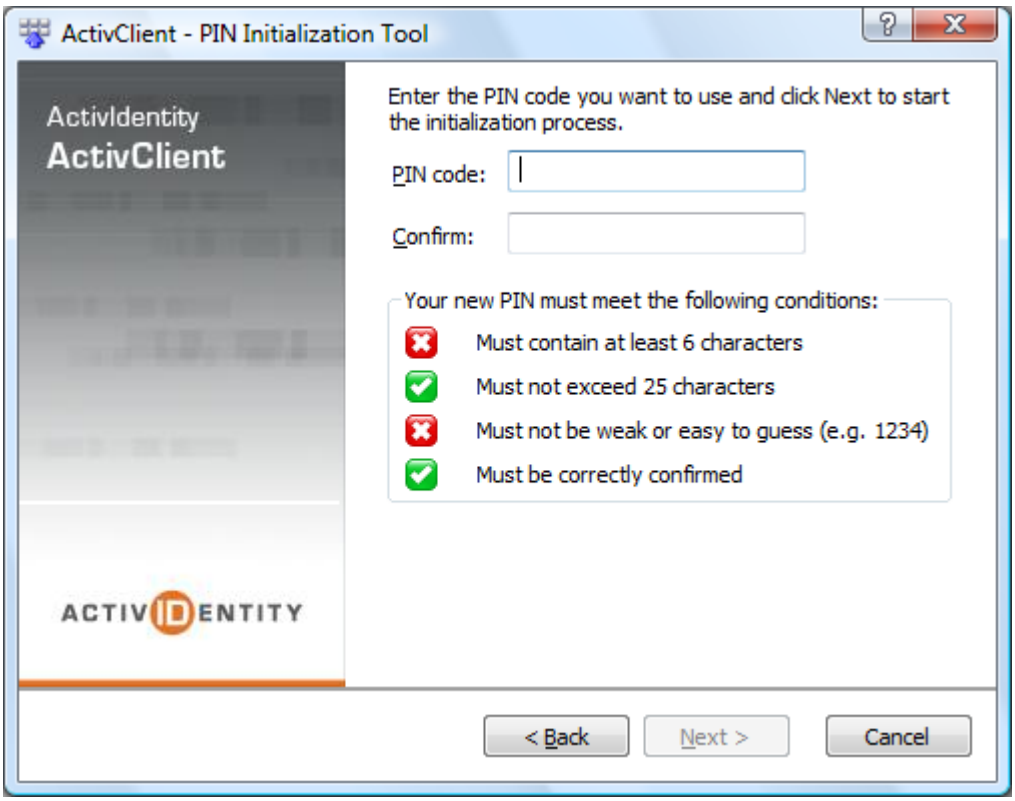
- On the ActivClient Agent icon  in the Windows notification area, left or right-click and select **PIN Initialization Tool**.
- From ActivClient User Console, insert your smart card and then, from the **Tools** menu, select **New Card**.
- From the Windows Start menu, go to **Programs**, **ActivIdentity**, **ActivClient** and select **PIN Initialization Tool**.

  The PIN Initialization Tool wizard is displayed.

Initialize your Smart Card using the PIN Initialization Tool

Use the following procedure to initialize your smart card using the PIN Initialization Tool.

1. Start the PIN Initialization Tool (see "Access the PIN Initialization Tool" on page 12).
2. Follow the wizard's instructions.



3. Enter your new PIN code, confirm it, and click **Next**.
4. If you have a standalone smart card that is already initialized (with an unlock code), you must enter a PIN or unlock code.

   When the initialization is complete, the Finish window is displayed.
5. If an unlock code is displayed, write it down in a secure location.
6. Click **Finish** to close the tool.

PIN selection rules

- Enter a PIN that is easy for you to remember, but difficult for others to guess!
- The PIN code must conform with the PIN conditions displayed by the tool. All the conditions must display a green check ✅ for the PIN Initialization Tool to let you proceed.

Warning

- Entering too many wrong PIN codes will lock your smart card! Make sure you view your **unlock code** and write it down in a secure place before you inadvertently lock your smart card.
- If the smart card is already initialized, the PIN Initialization Tool will reformat the card: all content present on the card (including private keys) will be permanently deleted.

Reset a Smart Card

Resetting a smart card removes most of the information stored on your smart card, including your digital certificates, your PIN code and any ActivIdentity AAA Server or SecureLogin SSO information. It only preserves the smart card pre-loaded applets.

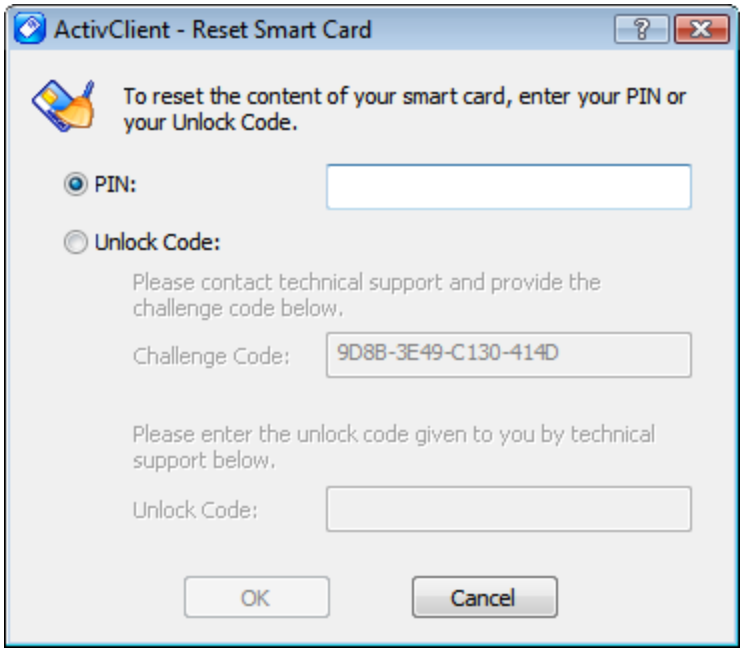
In order to reset the smart card, you need to know either the smart card's PIN or the unlock code.

Note

Depending on how your card was initialized, you might not have access to the reset function.

1. Open the ActivClient User Console.
2. Insert your smart card (chip-side up and chip first) into the smart card reader.
3. Click **Reset Card** from the **Tools** menu.
4. When a confirmation message is displayed, click **Yes**.

   The **Reset Smart Card** dialog box is displayed.



If...	Action
You know the smart card PIN	Make sure the **PIN** option is selected, enter your PIN in the field, and click **OK**.
You do not know the smart card PIN and the smart card was initialized with ActivClient in standalone mode	1. Select **Unlock Code**. 2. Enter the unlock code that you saved at initialization, and click **OK**. For more information, see "View your Unlock Code" on page 16.
You do not know the smart card PIN, and the smart card was initialized by your administrator	1. Select **Unlock Code**. 2. Call your help desk. You may be asked to give the challenge displayed in the **Challenge Code** field. 3. In the **Unlock Code** field, enter the unlock code that the help desk operator gives you, and click **OK**.

Note

You can also “Reset” and “Re-initialize” your smart card using the PIN Initialization tool. The tool also allows you to reset your PIN in the same process.

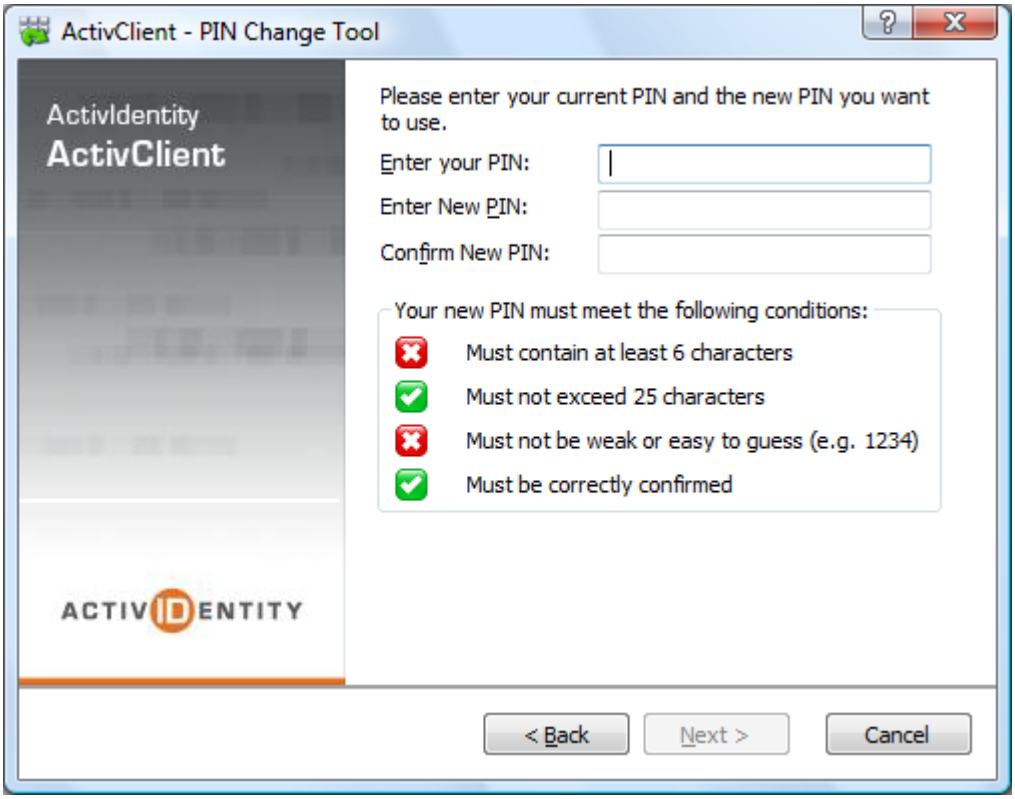
Change your Smart Card PIN

You should change your smart card PIN regularly to ensure that you are the only person accessing your smart card.

Access the PIN Change Tool

You can access the PIN Change tool by either:

- On the ActivClient Agent icon , left or right-click and select **PIN Change Tool**.
- From the User Console, either:
  - Select **Change PIN** from the **Tools** menu.
  - Select the **Change PIN** icon  from the **Standard** toolbar.
- From the Windows Start menu, go to **Programs**, **ActivIdentity**, **ActivClient**, and select **PIN Change Tool**.



All conditions must be met (indicated by a green check) before you can proceed to the **Next** step.

Unlock your Smart Card

If you enter too many consecutive wrong PINs when trying to use your smart card, your card is automatically locked. You must then unlock it before you can re-use your smart card.

The unlock procedure depends on the method used to initialize your smart card as explained in Table 2.1.

Table 2.1: Smart Card Unlock Actions

Initialization method	Unlock procedure
If you initialized your smart card directly with ActivClient in standalone mode	You are also responsible for the unlock code. You should view your unlock code and save it in a secure location. This unlock code helps you unlock the smart card if you lock it by entering multiple incorrect PINs. See: • "View your Unlock Code" on page 16 • "Unlock a Smart Card Initialized with ActivClient" on page 17
If you received an already initialized smart card	Your administrator/help desk is responsible for your unlock code. See "Unlock a Smart Card Initialized by the Administrator" on page 18.
If your smart card was initialized with ActivClient in a Standalone / Mini mode	There is no code as the smart card cannot be unlocked. However, you can re-initialize your smart card with the PIN Initialization Tool. See "Initialize a Smart Card with the PIN Initialization Tool" on page 11.

ActivClient detects the method used to initialize the smart card and displays the relevant unlock dialog box.

View your Unlock Code

1. Select **View Unlock Code** from the **Tools** menu.

   The **Display Smart Card Unlock Code** dialog box is displayed.

2. Enter your **PIN** code when prompted.

Note

Some smart card models (such as DoD CAC and US Government PIV cards) cannot be unlocked with ActivClient. Instead, you should contact your help desk to unlock your card.

Important

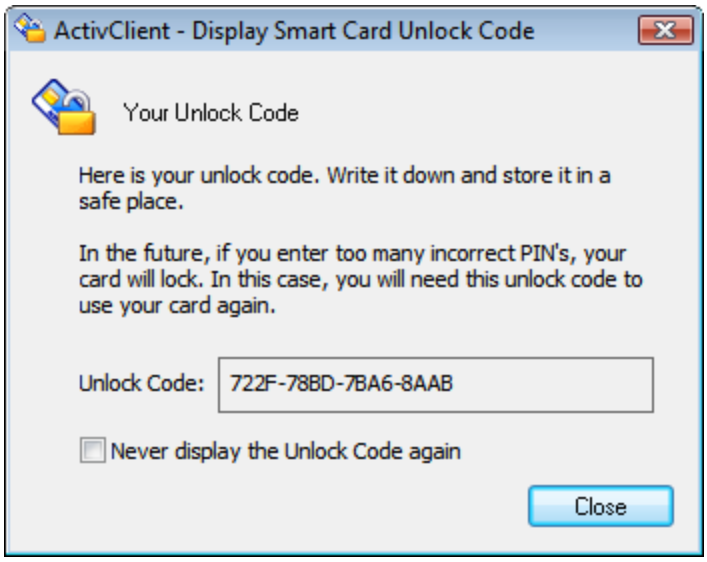
You cannot view your unlock code if your smart card is locked.

If you do not know your unlock code, contact your help desk.

Prerequisites

- ActivClient User Console is open.
- Your smart card has been initialized with ActivClient in standalone mode.

3. Write down your unlock code and save it in a secure location. You need this unlock code in case you lock your smart card in the future.



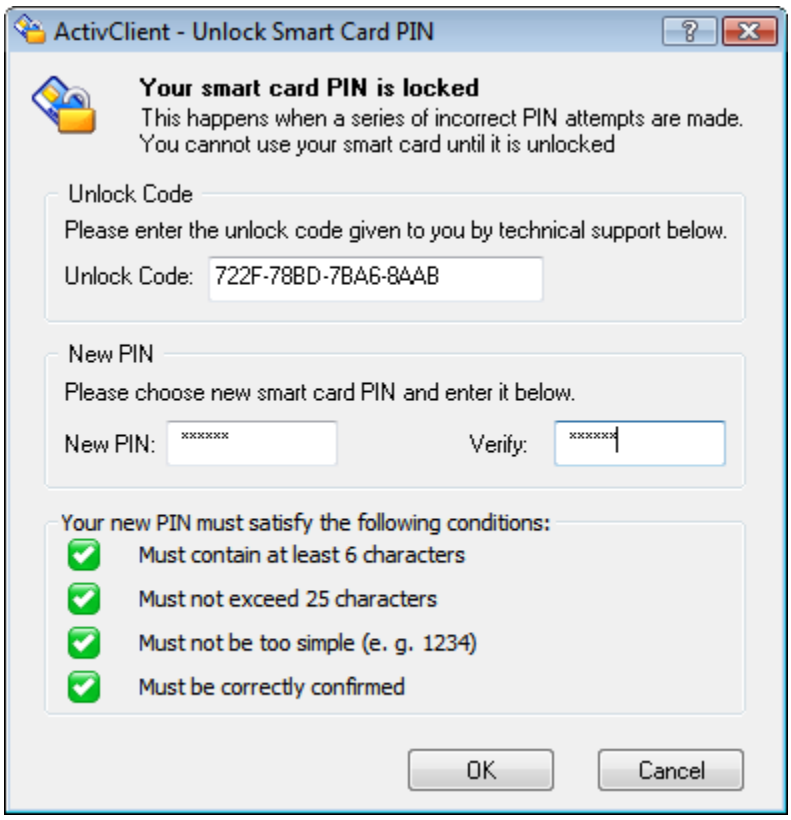
Important

If you select the **Never display the Unlock Code again** option, the **Display Smart Card Unlock Code** dialog box will never display again.

Consequently, your Unlock Code will never display again!

Unlock a Smart Card Initialized with ActivClient

When ActivClient detects that the locked smart card was initialized with ActivClient, the **Unlock Smart Card PIN** dialog box asking for your Unlock Code and a New PIN is displayed.



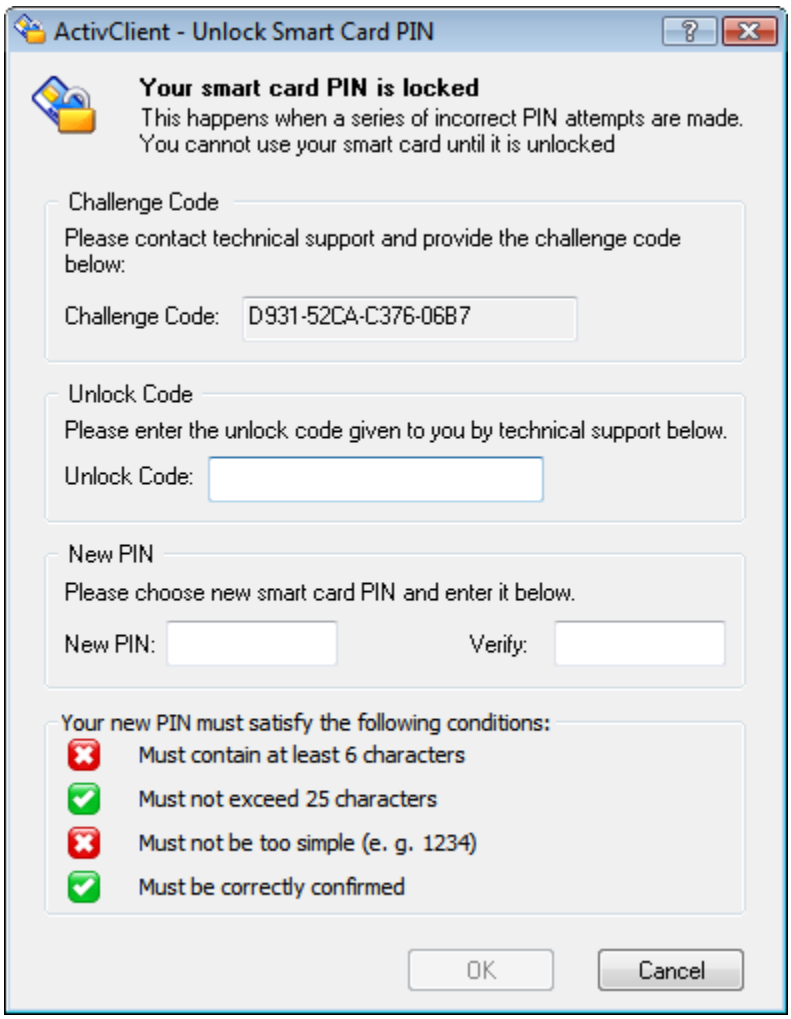
1. Retrieve the unlock code that you saved when you initialized your smart card.
2. In the **Unlock Code** field, enter the unlock code.
3. In the **New PIN** field, enter a new PIN.
4. In the **Verify** field, re-enter the new PIN, and click **OK**.

Unlock a Smart Card Initialized by the Administrator

When ActivClient detects that the locked smart card was initialized by the administrator, the **Unlock Smart Card PIN** dialog box is displayed with a Challenge Code.

Note

- ActivClient can be configured to display the unlock screen as soon as a locked smart card is inserted in the system.
- All conditions must be met (indicated by a green check).



1. Call your help desk and give them the code displayed in the **Challenge Code** field.
2. In the **Unlock Code** field, enter the unlock code that the help desk operator gives you.
3. In the **New PIN** field, enter a new PIN.
4. In the **Verify** field, re-enter the new PIN, and click **OK**.

Note

All conditions must be met (indicated by a green check).

Access the Unlock Smart Card Dialog

If the unlock dialog box does not automatically display, you can manually initiate the unlock process.

1. From the ActivClient User Console **Tools** menu, select **Unlock Card**.
2. Re-insert the locked smart card into your smart card reader.
3. Depending on the unlock dialog displayed, see either:
   - "Unlock a Smart Card Initialized with ActivClient" on page 17
   - "Unlock a Smart Card Initialized by the Administrator" on page 18

Update your Smart Card

When you log on with your smart card or insert your smart card in the reader, the ActivClient Smart card auto-update feature automatically checks if there are any updates for your smart card.

You will only be alerted if there is a pending update for your smart card available on the ActivID Card Management System (CMS).

The update could be one of the following:

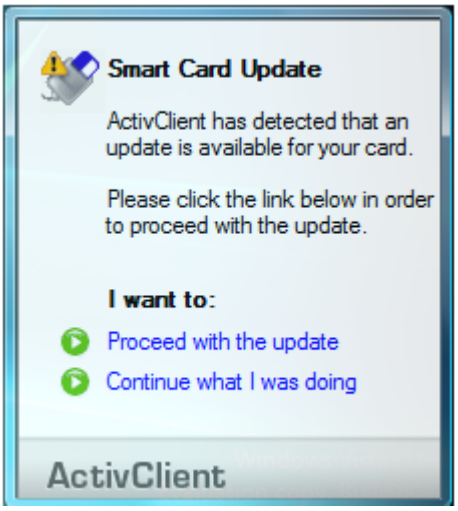
- Certificate renewal
- Addition/removal of credentials
- Card lock/unlock
- Card issuance (if already assigned)
- Temporary and permanent card replacement (when the replacement card is inserted in the reader)

Prerequisites

- This feature is enabled only if the **Smart Card Auto-Update** component is installed.
- You must have a valid connection to the CMS server that manages your smart card.
- The CMS root certificate is installed (required for the actual update but not for the update check).
- You must be able to install the CMS Synchronization Client (ActiveX control).
- CMS version 4.2 or later.

Automatic Check for Updates

When an update is available, ActivClient automatically displays the following notification:



You can either:

- Proceed with the update:

  A window opens with the configured ActivID CMS My Digital ID Card portal.

  a. Follow the displayed instructions to update your smart card.

  b. When the update is complete, close your browser.

  c. To apply your new credentials, remove and then re-insert your smart card when prompted.

- Continue what you were doing:

  The alert will disappear and you can continue with your original task.

Note

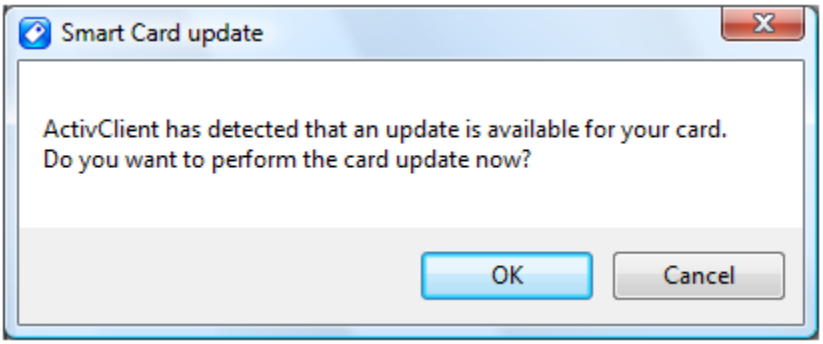
If you do not select an option or you remove the card from the reader, the alert will disappear.

Manual Check for Updates

If necessary, you can also manually check for smart card updates (for example, for troubleshooting purposes).

1. In the User Console, make sure the correct smart card reader is selected.
2. From the Tools menu, select Advanced and then **Check for card update**.

- If a card update is available, you are prompted to perform the card update:



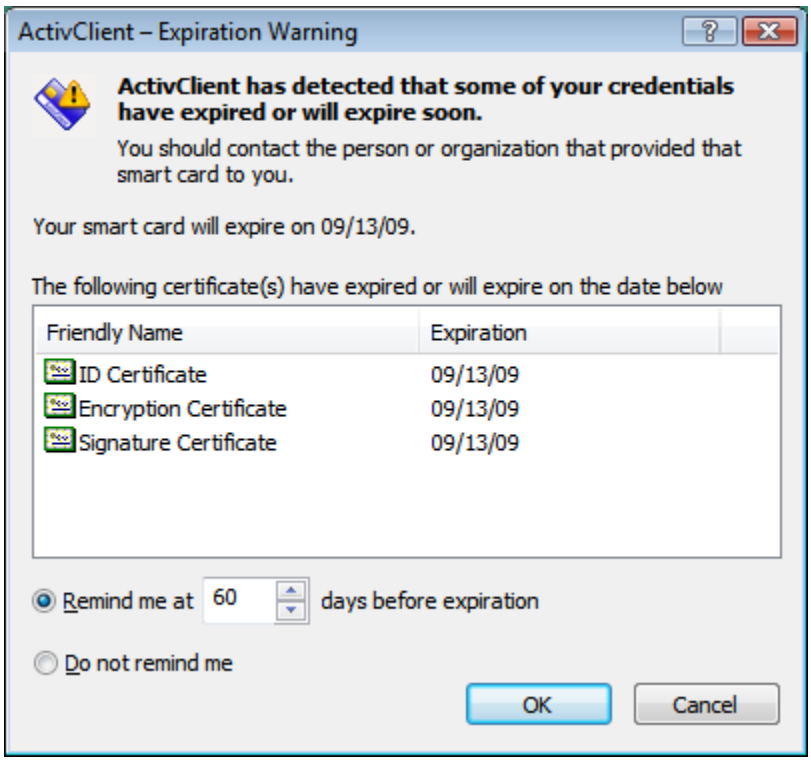
  - To proceed, click **OK** and follow the procedure described on page 21.
  - If you do not want to update your card, click **Cancel**.
- If no update is available, a message is displayed stating so. Click **OK** to close the message.

Smart Card or Certificate Expiration

ActivClient can inform you that your card or certificates are about to expire. This enables you to obtain a replacement card or replacement certificates before the current ones expire.

1. Insert your smart card (chip-side up and chip first) into the smart card reader.

   If ActivClient detects that your card or certificates has expired or is about to expire, it displays the following message:



2. If you want to be reminded of this expiration, select the number of days before expiration and click **OK**.

   If not, select **Do not remind me** and click **OK**.

   We recommend that you request a replacement card or certificate as soon as possible.

Prerequisites

At least one of the following ActivClient policies is enabled:

- Display card expiration notification
- Display certificate expiration notification

By default these policies are:

- Disabled in ActivClient editions
- Enabled ActivClient CAC editions

Your administrator may have enabled these features.

Notes

- The *card expiration* option is only available for CAC and PIV cards.
- The *certificate expiration* option is available for all card models.

View Smart Card Information

You can use the User Console to view the technical information about your smart card, such as:

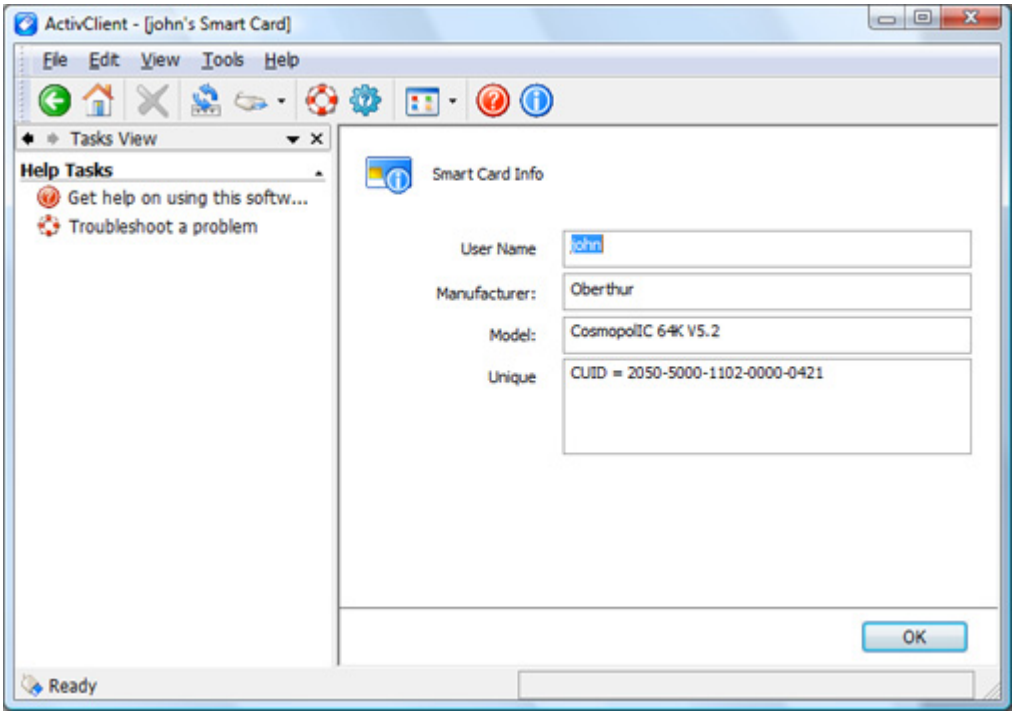
- User name
- Smart card manufacturer name (when known)
- Smart card type (when known)
- Serial number

Note

Smart card information is set by default and cannot be modified.

To access smart card information from ActivClient User Console, either:

- From the User Console tasks pane, insert your smart card and click **Smart Card Info**.
- From the User Console right pane, insert your smart card and either:
  - Double-click the **Smart Card Info** icon .
  - Right-click the **Smart Card Info** icon and select **View smart card info**.



Note

Your user name is supplied by ActivClient from either:

- Your remote access (AAA) user name (if present on smart card).
- Windows logon user name of your default certificate which is determined by your smart card settings.

Chapter 3: Managing Digital Certificates

In This Chapter

25 Download a Certificate with Microsoft Internet Explorer
26 Download a Certificate with Firefox
26 Download an Entrust Profile
31 Manage User and CA Certificates
34 Select Certificates for Windows PKI Logon
36 Make Certificates Available to Windows
36 Manage Certificates in Microsoft Outlook
31 Manage User and CA Certificates

This chapter explains how to download and configure your digital certificates for authentication.

The availability of the operations described in this chapter (such as importing/deleting a certificate from your smart card) vary according to your smart card policy.

Download a Certificate with Microsoft Internet Explorer

You can use a PKI key pair (unique to you, generated directly on your smart card) and an associated digital certificate (proving your identity inside your organization) in order to use a variety of security services.

Prerequisites

- Microsoft CAPI Support (sub-component of the Digital Certificate Services component) was installed during setup.
- Your administrator provided you with a Web site URL to access your organization's Certificate Authority. To download a smart card logon certificate, your organization's Certificate Authority must be either one of the following:
  - Windows 2000, Windows Server 2003 and Windows Server 2008 Certificate Authority
  - A Certificate Authority trusted by your Active Directory

1. Insert your smart card (chip-side up and chip first) into the smart card reader.
2. Launch Internet Explorer and go to your Certificate Authority's Web site.
3. Navigate to the page where you can generate or download a certificate (the steps to reach this page vary depending on the CA that you are using).
4. When you are asked for the Cryptographic Service Provider (CSP), select **ActivClient Cryptographic Service Provider** from the list of providers.
5. Follow the CA's instructions to generate or download a certificate.

   When your smart card is full (that is, if there is not enough space for the certificate that you are downloading), the ActivClient CSP overwrites the

default certificate with the new certificate. In this case, a message is displayed that you are about to replace the existing credentials on the card. Select **Yes** to overwrite the default certificate.

6. Enter your PIN when prompted.

7. Verify that the key pair and associated certificate have been loaded on your smart card using the ActivClient User Console (optional).

Download a Certificate with Firefox

You can use a PKI key pair (unique to you, generated directly on your smart card) and an associated digital certificate (proving your identity inside your organization) in order to use a variety of security services.

1. Insert your smart card (chip-side up and chip first) into the smart card reader.

2. Launch Firefox and go to your Certificate Authority's Web site.

3. Follow the instructions to request a certificate.

4. Enter your PIN when prompted.

5. Verify that the key pair and associated certificate have been loaded on your smart card using the ActivClient User Console (optional).

Note

Once your certificate is downloaded, Microsoft applications, such as Internet Explorer and Outlook, display the certificate name and information.

However, the private key associated with the certificate is not stored on the personal computer. Therefore, you still need the smart card in order to use the certificate information.

Prerequisites

- A supported version of Firefox is installed on your computer.
- If you use ActivClient 32-bit, Firefox support was installed during setup.
- If you use ActivClient 64-bit, the ActivClient PKCS#11 library was installed during setup and then installed in Firefox. For details, see the *ActivClient for Windows Installation Guide*.
- Your administrator provided you with a Web site URL to access your organization's Certificate Authority.

Download an Entrust Profile

If you plan to use Entrust Entelligence™ Desktop Solution with ActivClient, you must store your Entrust profile on your ActivClient smart card. This profile includes signature and encryption keys and certificates, along with certificates for key history.

1. Insert your smart card (chip-side up and chip first) into the smart card reader.

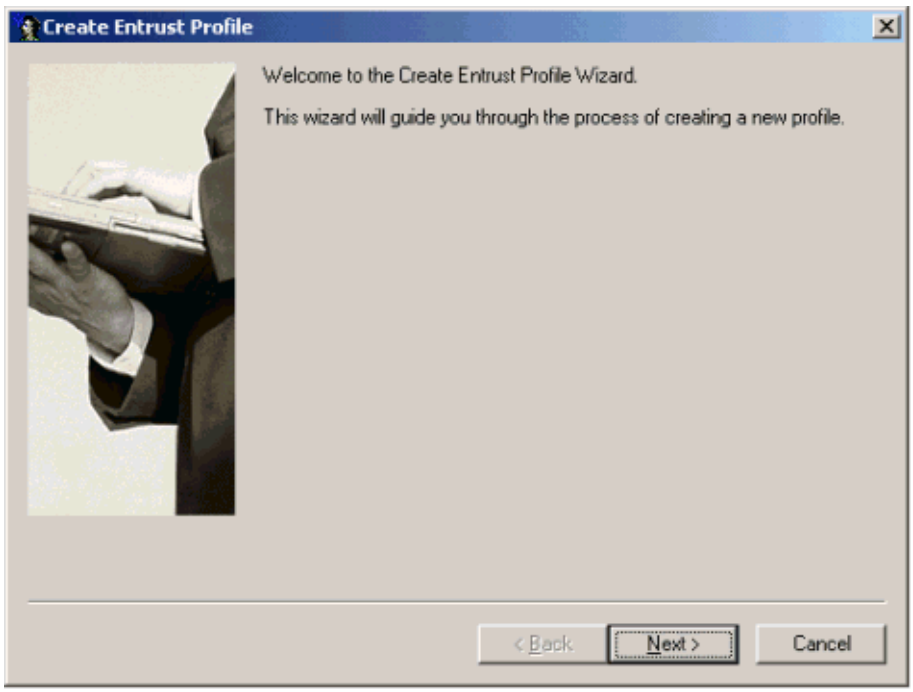
2. In the Windows notification area, right-click the **Entrust** icon  and then click **Create Entrust Profile**.

Prerequisite

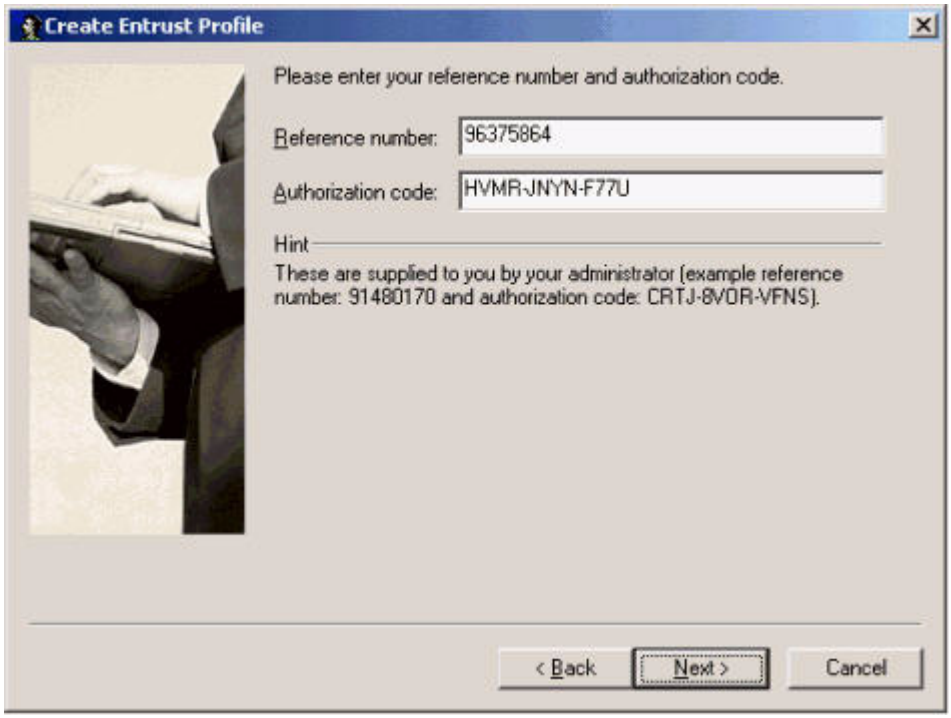
The Entrust Entelligence Desktop Solution support was installed during setup.

Notes

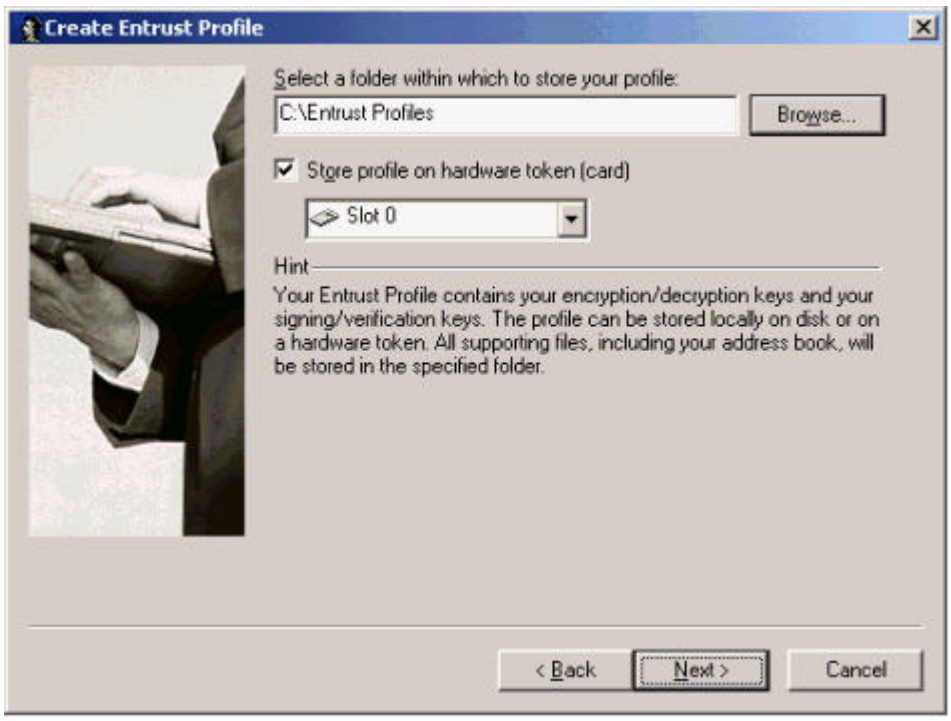
- This feature is only available with ActivClient 32-bit.
- As an alternative, you can download an Entrust Profile to your smart card using the Entrust Self-Administration Server.
- This section only applies to Entrust Entelligence Desktop Solution. It does not apply to Entrust Entelligence Security Provider.



3. When the **Create Entrust Profile** Wizard is displayed, click **Next**.



4. In the **Reference number** and **Authorization code** fields, enter the information supplied by your Entrust administrator, and click **Next**.



Note

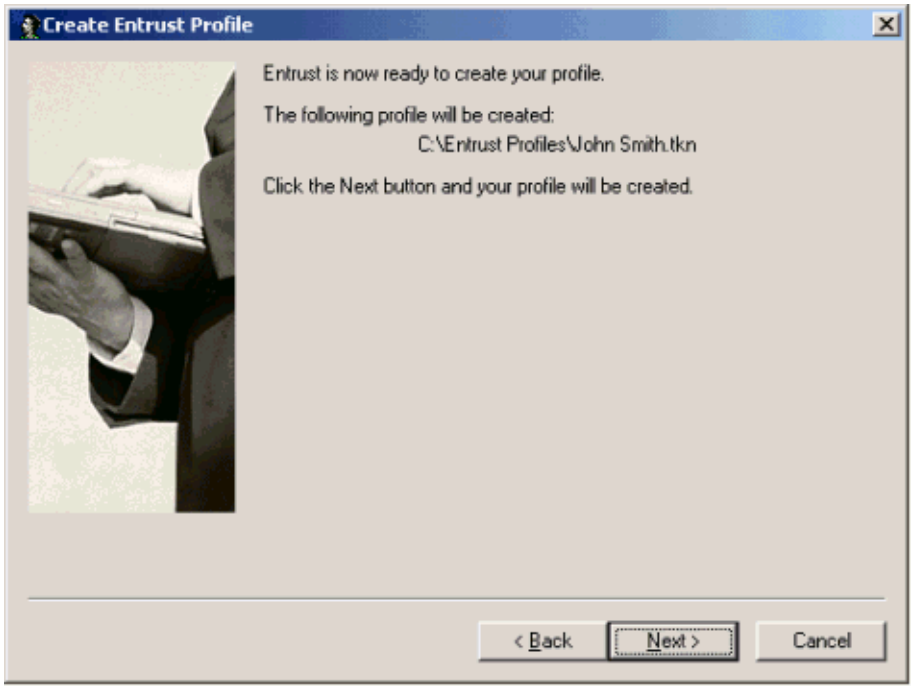
Although the Entrust profile is stored on the smart card, all the supporting Entrust files are stored in the specified folder. If necessary, enter a different folder location.

5. Use the following table to determine how to store your profile and then click **Next**.

If...	Then...
The **Store profile on hardware token (card)** option is not already selected as the default	Verify that: • The smart card is properly inserted in the smart card reader. • The Entrust Entelligence Desktop support was installed during setup. If necessary, select the **Store profile...** option.
The correct reader does not appear in the drop-down list	Select the correct reader from the list.



6. Enter a name for the Entrust profile (usually your username) in the **Profile name** box, and click **Next**.



7. When a window displays a message that Entrust is now ready to create your profile, click **Next**.

   The profile is downloaded onto your smart card.

   After a few minutes, the following window is displayed.



8. In the **New Password** field, enter a password for the Entrust profile.

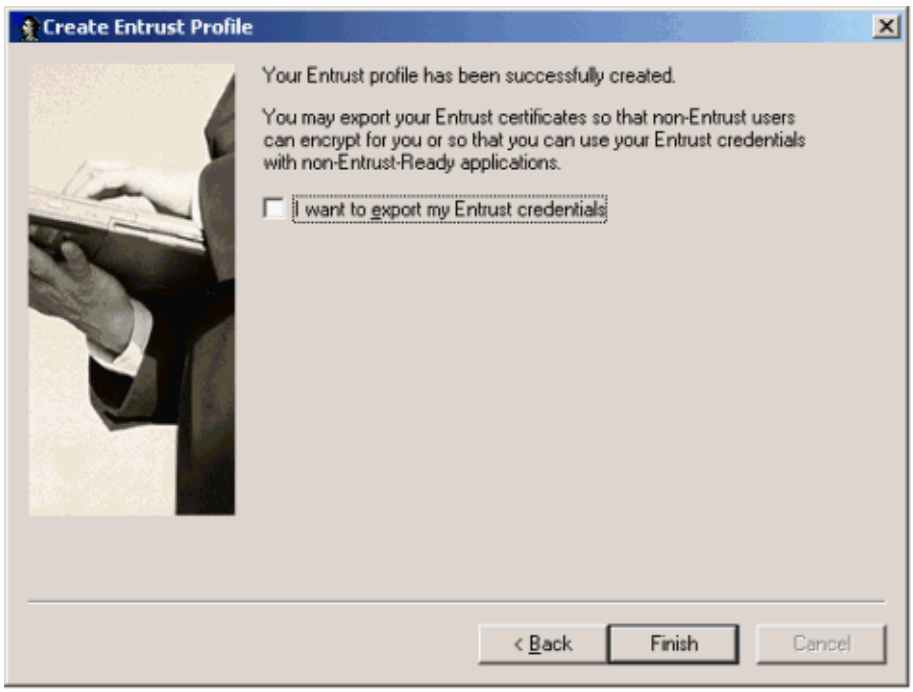
   This password is the initial PIN for the smart card.

9. In the **Confirm Password** field, re-enter your password, and click **Next**.

Note

If your card is already initialized, you are prompted to enter your current PIN instead.

You can use the ActivClient User Console to change your PIN later.



10. When the window is displayed with the message that your Entrust profile has been successfully created, click **Finish**.

Manage User and CA Certificates

Once you have one or more certificates on your smart cart, ActivClient allows you to view, import, export and delete them.

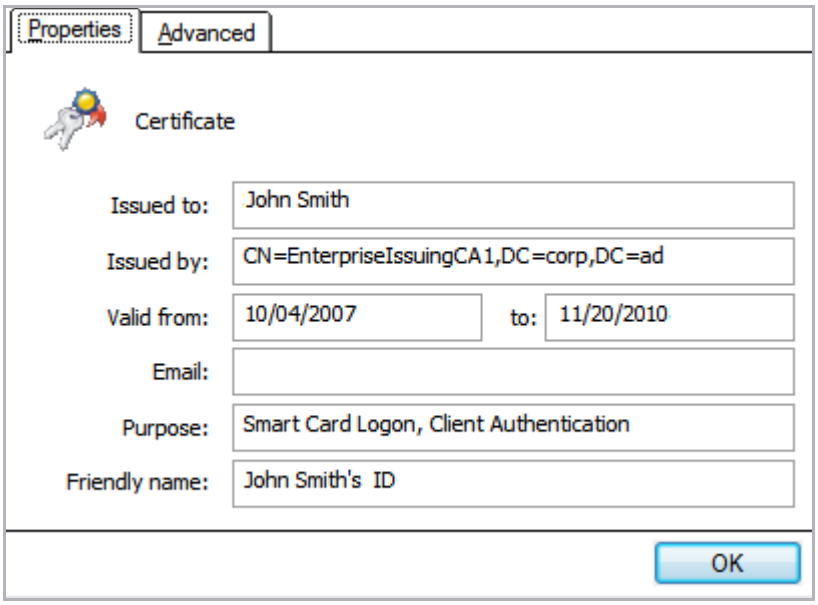
View your Certificate

You can view details of your certificates on your smart card using the ActivClient User Console.

1. Open the ActivClient User Console.
2. Either:
   - From the tasks pane under **My Certificate Tasks**, click **View My Certificates**.
   - From the right pane, double-click the **My Certificates** icon.

   An icon for each of your certificates is displayed.
3. Double-click the certificate that you want to view.

The **Properties** tab is displayed.



Note

In the **Advanced** tab, you can copy a value to another application, use the **Copy** command (CTRL + C) to move the selected text to the clipboard, and then use the **Paste** command (CTRL + V) to add the value.

4. To view advanced properties, click the **Advanced** tab.

Import a User Certificate

If you are already using your personal PKI key pair and certificates, you can import them to your smart card as `.pfx` or `.p12` file formats. This guarantees that your private credentials are portable and more secure inside your smart card.

Prerequisites

- ActivClient User Console is installed.
- A certificate is available as a PKCS#12 file on your workstation. To obtain this file, export your certificate by using, for example, the Microsoft Internet Explorer Export function.

1. Open the ActivClient User Console.
2. From the **File** menu, select **Import** and then click **Certificate**.
3. Select or browse to the certificate that you want to import, and click **Open**.

   If the certificate is password-protected, the **Password Request** dialog box is displayed prompting you to enter your password.

Note

Make sure that **Personal Information Exchange (*.pfx;*.p12)** is selected as the file type.

4. In the **Password** field, type the certificate password, and click **OK**.
5. When the confirmation message is displayed, click **OK**.

Import a CA Certificate

You can store the Certificate Authority's root certificate on your smart card. This guarantees that the certificate chain is portable with your smart card, and that you can use your own certificates from any ActivClient workstation.

1. Open the ActivClient User Console.
2. From the **File** menu, select **Import** and then click **Certificate**.
3. Select or browse to the certificate that you want to import, and click **Open**.

   If the certificate is password protected, the **Password Request** dialog box is displayed prompting you to enter your password.
4. In the **Password** field, type the certificate password, and click **OK**.
5. When a confirmation message is displayed, click **OK**.

Prerequisites

- ActivClient User Console is installed.
- A certificate is available as a `.cer` or `.crt` file on your workstation. To obtain this file, export your CA certificate by using for example the Microsoft Internet Explorer Export function.

Note

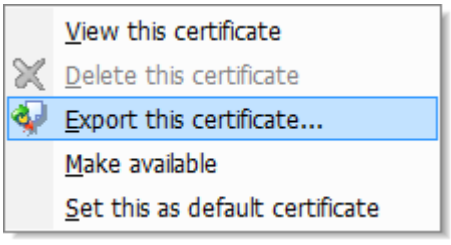
Make sure that **X.509 Certificate (*.cer;*.crt)** is selected as the file type.

Export a Certificate

You can send your user certificate or CA certificate to someone by exporting it from your smart card into a file.

1. Open the ActivClient User Console.
2. Either:
   - Select **View My Certificates** or **View CA Certificates** from the Tasks pane related section.
   - Double-click the **My Certificates** or **CA Certificates** icon from the right pane.

   An icon representing each of your certificates or CA certificates is displayed.
3. Select the certificate you want to export and either:
   - Select **Export this certificate** in the left pane.
   - Right-click on the certificate and select **Export this certificate** from the menu.



Prerequisites

- ActivClient User Console is installed on your workstation.
- A certificate is available on your smart card.

Note

For security reasons, you cannot export the private key located in your smart card. You can only export certificates from your smart card.

4. Select the location and the file name for the exported certificate, and click **Save**.

   A confirmation message is displayed.

5. Click **OK**.

Delete a Certificate

If a certificate is obsolete (expired or revoked), you can delete it from your smart card before you download a new certificate. Deleting a certificate applies both to **user** certificates (in My Certificates folder) and to **CA** certificates (in CA Certificates folder).

1. Open the ActivClient User Console.
2. Either:
   - Select **View My Certificates** or **View CA Certificates** from the Tasks pane related section.
   - Double-click the **My Certificates** or **CA Certificates** icon from the right pane.

   An icon representing each of your certificate or CA certificates is displayed.
3. Select the certificate(s) you want to delete and either:
   - Select **Delete this certificate** from **My Certificate Tasks** section in the left pane.
   - Right-click on the certificate and select **Delete this certificate** from the menu.
   - Select one or several certificates in the right pane and then select the **Delete** red cross icon  from the **Standard** toolbar.

   A confirmation message is displayed asking you to confirm you want to delete your certificate.
4. Click **Yes** to confirm.

Important

Do not delete a certificate if you may need it to decrypt old documents or messages

Prerequisites

- ActivClient User Console is installed.
- A certificate is available on your smart card.

Note

You may not be able to delete some of your certificates depending of your smart card configuration.

Select Certificates for Windows PKI Logon

The logon process for Windows 2000, Windows XP and Windows Server 2003 does not allow a user to select a logon certificate. If your smart card contains two or more certificates configured for Windows PKI logon (that is, with specific attributes needed for Windows logon), you can select which certificate to use for the Windows logon process using ActivClient User Console.

With Windows Vista, Windows 7 and Windows Server 2008, the Windows logon process allows you to select a logon certificate when you log on (among certificates

compatible with Windows logon). In these configurations, there is no need to select any certificate to use with ActivClient User Console.

Prerequisite

You have a Windows logon compatible certificate available on your smart card. For more information, see "Download a Certificate with Microsoft Internet Explorer" on page 25.

1. Open the ActivClient User Console.
2. To display your certificates, either:
   - Select **View My Certificates** from the Tasks pane related section.
   - Double-click the **My Certificates** icon from the right pane.

   An icon for each of your certificate is displayed.
3. Select the certificate you want to use for Windows PKI logon.
4. Select **Set this as default certificate** from either the:
   - Certificate right-click menu.
   - **My Certificate Tasks** section in the **Tasks** pane.

   The certificate icon is updated with a green check mark  .

Deselect a Logon Certificate

Prerequisite

One of your certificates is set as default.

When you do not need to set your logon certificate as default, follow these steps:

1. Open the ActivClient User Console.
2. To display your certificates, either:
   - Click **View My Certificates** from the **My Certificate Tasks** section in the Tasks pane.
   - Double-click the **My Certificates** icon located in the right pane.

   An icon for each of your certificate is displayed.
3. Right-click the certificate set as default (highlighted by a green check mark ).
4. Select **Set this as default certificate** to invalidate the check mark.

   The certificate icon is updated and the green check mark disappears  .

Make Certificates Available to Windows

Before you can use the certificates on your smart card, you must make them available to Windows-based applications (for example, Microsoft Internet Explorer, Outlook, and Windows logon).

By default, ActivClient automatically registers all certificates on your smart card to make them automatically available to your desktop applications when you insert your smart card. No further action is required.

You need to make the certificates available to Windows manually when your administrator has configured ActivClient so that certificates are not automatically registered at card insertion. For information on configuration, see the *ActivClient for Windows Administration Guide*.

This operation is needed only once, the first time you use a new smart card on a new workstation.

1. Open the ActivClient User Console.
2. Either:
   - Go to **Tools**, **Advanced**, and select **Make Certificates Available to Windows**.
   - Select **Make available** from your certificate right-click menu.

   A message displays, informing you that the certificates have been made available for use with most desktop applications.

Manage Certificates in Microsoft Outlook

Automatically Configure your Microsoft Outlook Security Profile

To sign and encrypt/decrypt emails with Microsoft Outlook, a security profile must be created in Outlook for your email Exchange account. This profile identifies the signature and encryption certificates.

ActivClient can automatically create your security profile.

1. Start Microsoft Outlook configured with a Microsoft Exchange account.
2. Insert your smart card (chip-side up and chip first) into the smart card reader.

Prerequisites

- Microsoft Outlook is installed on your workstation.
- Microsoft Outlook Usability Enhancements (sub-component of the Digital Certificates Services component) was installed during setup.
- The ActivClient policy, **Setup email certificate in Outlook on card insertion**, is enabled (it is enabled by default).
- Your smart card contains certificates for email signature and encryption.

Note

For further information about this ActivClient feature, see the *ActivClient for Windows Administration Guide*.

3. If you do not have an existing Outlook security profile, ActivClient automatically creates the profile.

4. If you already had an Outlook security profile, ActivClient automatically updates it with your smart card certificates.

   ActivClient also makes sure that the most current certificates are used and that the email address in the certificate matches that of the Outlook account.

Automatically Publish your Certificates to the Global Address List

To allow other users to send you encrypted email, they need access to your encryption digital certificate. A common method is to publish all users' certificates in the Exchange Global Address List (GAL).

ActivClient can automatically publish your certificates in the Global Address List.

1. Start Microsoft Outlook configured with a Microsoft Exchange account.

2. Insert your smart card (chip-side up and chip first) into the smart card reader.

3. Enter your PIN when prompted.

   ActivClient automatically publishes your smart card-based certificates to the Global Address List.

Alternatively, you can publish your certificates to the GAL from the ActivClient User Console.

From the User Console, select Tools, Advanced and then **Publish to GAL**.

- Your Outlook security profile is created or updated.
- Your certificates are published to the Global Address List.

Prerequisites

- Microsoft Outlook is installed on your workstation.
- Microsoft Outlook Usability Enhancements (sub-component of the Digital Certificates Services component) was installed during setup.
- The ActivClient policy, **Automatically publish certificates to the Global Address List**, is enabled (it is disabled by default configuration; your administrator may have enabled this feature).
- The ActivClient policy, **Setup email certificate in Outlook on card insertion**, is enabled.
- Your smart card contains certificates for email signature and email encryption.

Note

For further information about this ActivClient feature, see the *ActivClient for Windows Administration Guide*.

Automatically Add Certificates to Microsoft Outlook Contacts

To send an encrypted email to one of your contacts, you need access to their digital encryption certificate. A common method is to add your contact's information (including encryption certificates) to your Outlook Contacts. ActivClient can automatically add the information.

1. Open a signed email that you received from your contact. It contains your contact's encryption certificate.

   ActivClient will ask you to either confirm the creation of the Outlook Contact entry or update an existing entry.

2. To proceed, accept the creation/update.

   Your contact's information and encryption certificate is saved in your Outlook Contacts.

Prerequisites

- Microsoft Outlook is installed on your workstation.
- Microsoft Outlook Usability Enhancements (sub-component of the Digital Certificates Services component) was installed during setup.
- The ActivClient policy, **Automatically add sender's certificate to Outlook Contacts**, is enabled (it is enabled by default).

Note

For further information about this ActivClient feature, see the *ActivClient for Windows Administration Guide*.

Document Version 06.2.09 | ©2009 ActivIdentity, Inc.

Chapter 4: Using Digital Certificates

This chapter explains how to use your smart card-based certificates for authentication, digital signature and encryption.

In This Chapter

39 Log on to Windows with a Certificate
40 Lock your Workstation on Smart Card Removal
41 Use Windows Dial-Up/ VPN for Remote Access
42 Use a Non-Microsoft VPN for Remote Access
42 Access a Secure Web Site
44 Log on to Entrust Entelligence
45 Send/Read Signed and Encrypted Email Messages with Microsoft Outlook
48 Send/Read Signed and Encrypted Mails with Thunderbird
50 Encrypt/Decrypt Files with EFS

Log on to Windows with a Certificate

You can use a smart card certificate to securely log on to Windows.

Prerequisites

- Your smart card is configured with a certificate for Windows PKI logon.
- Your workstation is configured for PKI logon: the workstation must be attached to a domain, a root certificate must be available and a CRL server accessible.
- Microsoft CAPI Support (sub-component of the Digital Certificate Services component) was installed during setup.

1. Start your workstation.
2. Insert your smart card (chip-side up and chip first) into the smart card reader.

   A **Log On** window relevant to your operating system is displayed.



- Or -



3. On Windows Vista, Windows 7 or Windows Server 2008, select a certificate among the smart card certificates compatible with Windows logon.

4. Enter your PIN in the **PIN** field and click **OK**.

   After a few moments, you are logged on and your desktop is displayed.

Lock your Workstation on Smart Card Removal

To increase the security of your computer and its contents, lock your computer when you are away from it and keep your smart card safely in a separate place or on your person.

To lock your workstation, simply remove your smart card from the smart card reader.

Note

Your administrator may have changed the Card Removal Behavior property.

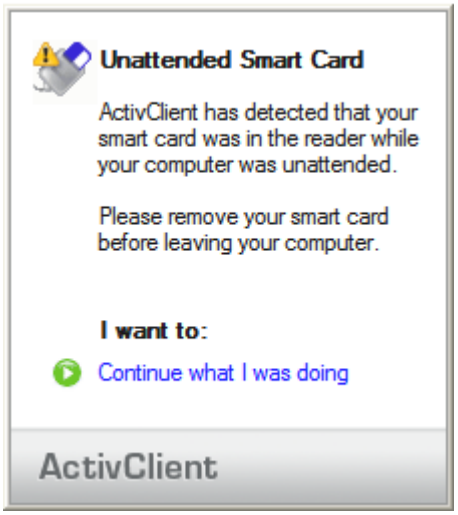
For further information on ActivClient customization, see to the *ActivClient for Windows Administration Guide*.

Prerequisites

- ActivClient is configured to lock the workstation on smart card removal (default setting).
- You used your smart card to log on to your workstation.

Card Unattended Notification

If you forget to remove your smart card when you log off, or when you lock your workstation, ActivClient reminds you that you should take your smart card with you.



Prerequisite

The ActivClient policy, **Display unattended smart card alert**, is enabled (it is enabled by default).

Notes

- On Windows Vista, Windows 7, Windows Server 2008, there is no visual notification. Instead, there is an audio notification (a beep).
- For further information about this ActivClient feature, see the *ActivClient for Windows Administration Guide*.

Use Windows Dial-Up/VPN for Remote Access

You can use your smart card-based digital certificate for secure remote access inside a Microsoft Windows environment.

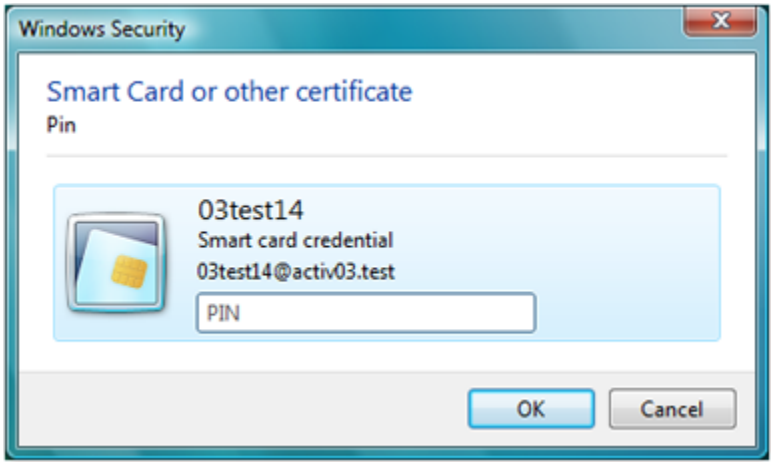
Prerequisites

- Your smart card contains a certificate configured for Windows PKI logon
- You configured a Dial-Up or VPN connection on your workstation with the Windows Network Connection Wizard and selected the **Use my smart card** option

1. Insert your smart card (chip-side up and chip first) into the smart card reader.
2. From the **Start** menu, go to **Settings**, and select **Network Connections**.

   The **Network Connections** dialog box is displayed.
3. Choose your remote connection (Dial-Up or VPN).

   The **Connect Virtual Private Connection** dialog box is displayed.



4. Enter your PIN in the **Smart card PIN** field and click **OK**.

   Once authentication is successful, the Dial-Up or VPN session is established.

Use a Non-Microsoft VPN for Remote Access

You can use your smart card-based digital certificate for authentication with several VPN products.

1. Insert your smart card (chip-side up and chip first) into the smart card reader.
2. Start your VPN connection.
3. When prompted, enter your smart card PIN, and click **OK**.

   When you are authenticated, the VPN session is established.

Prerequisites

- You can access a VPN product supported by ActivClient. For the complete list, see the *ActivClient for Windows Overview*
- Your smart card contains a certificate configured for VPN logon
- You have configured your VPN to use an ActivClient-based digital certificate. Depending on the VPN products, you may need to select the cryptographic library.
  - Select the "ActivClient Cryptographic Service Provider" for Microsoft CAPI compatible applications
  OR
  - Select the ActivClient PKCS#11 library (`acpkcs211.dll` in the ActivClient installation directory) for PKCS#11 compatible applications and the certificate for the VPN authentication

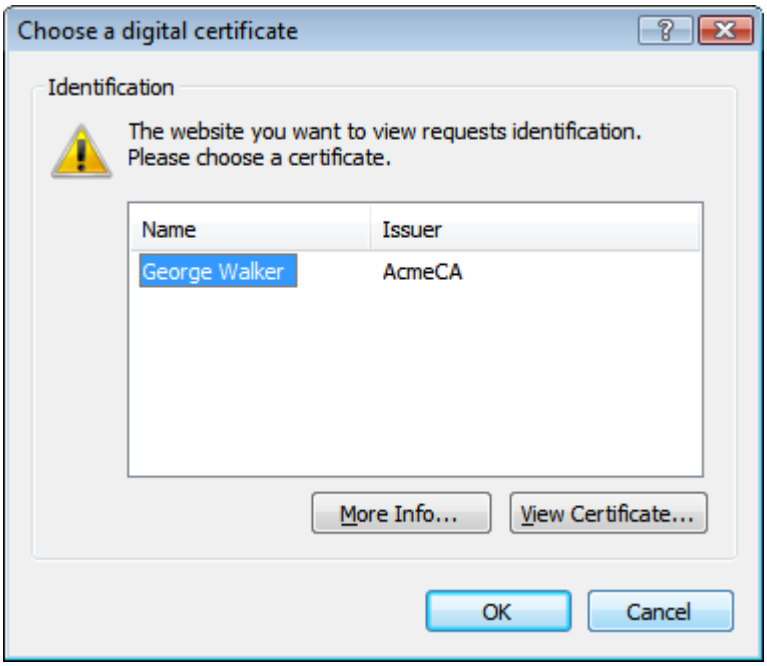
Access a Secure Web Site

Access a Secure Web Site with Internet Explorer

You can use your smart card-based digital certificate to access a Web site protected by SSL v3 or TLS for strong user authentication.

1. Insert your smart card (chip-side up and chip first) into the smart card reader.
2. Access the secure Web site or page using Microsoft Internet Explorer.

The **Choose a digital certificate** dialog box is displayed.



3. From the certificate list, select the appropriate ActivClient certificate, and click **OK**.
4. Enter your PIN in the **Smart card PIN** field and click **OK**.

   The browser sends your certificate and a digital signature to the web server. The server verifies your signature and grants access to the secured site or page.

Prerequisites

- Your smart card contains a certificate configured for authentication to this Web site
- Microsoft CAPI Support (sub-component of the Digital Certificate Services component) was installed during setup

Access a Secure Web Site with Firefox

You can use your smart card-based digital certificate to access a Web site protected by SSL v3 for strong user authentication.

1. Insert your smart card (chip-side up and chip first) into the smart card reader.
2. Start your browser from your desktop.
3. Access the secure Web site or page.
4. When Firefox prompts you to enter a Master Password, enter your **PIN**.

   Your browser sends your certificate and a digital signature to the web server. The server verifies your signature and grants access to the secured site or page.

Prerequisites

- Firefox is installed on you computer.
- Your smart card contains a certificate configured for authentication to this Web site.
- If you use ActivClient 32-bit, Firefox support was installed during setup.
- If you use ActivClient 64-bit, the ActivClient PKCS#11 library was installed during setup and then installed in Firefox.

For details, see the *ActivClient for Windows Installation Guide*.

Log on to Entrust Entelligence

With ActivClient, your Entrust private keys and digital certificates are stored securely on your smart card. You can use them with the **Entrust Entelligence Desktop Solution**.

1. Insert your smart card (chip-side up and chip first) into the smart card reader.

2. Right-click the **Entrust** icon located in the Windows notification area and select **Log In to Entrust**.

   The **Entrust Login** dialog box is displayed. Entrust automatically retrieves the profile name from the smart card.



3. Enter your PIN in the **Password** field, and click **OK**.

   When you are logged on, the red **X** is no longer displayed above the **Entrust** icon in the notification area.

Note

- This feature is only available with ActivClient 32-bit
- This section only applies to Entrust Entelligence Desktop Solution. It does not apply to Entrust Entelligence Security Provider

Prerequisite

An Entrust profile is downloaded on to your smart card. For more information, see "Download an Entrust Profile" on page 26.

Send/Read Signed and Encrypted Email Messages with Microsoft Outlook

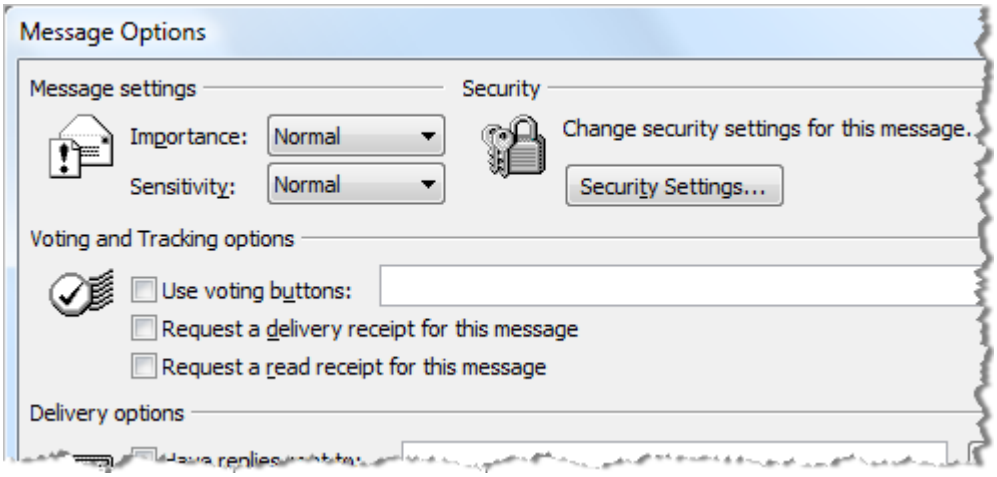
Send/Read Signed Email Messages

A digital signature is a combination of your private key and the message. It authenticates you as the message sender and verifies the integrity of the message. With ActivClient, the digital signature is performed directly on your smart card.

Send Signed Email Messages

1. Insert your smart card (chip-side up and chip first) into the smart card reader.
2. Create the email message.
3. Either:
   - From the Outlook toolbar, click the **Digitally Sign Message** icon .
   - Click **Options** on the **View** menu (or the **Options** icon on the toolbar).

   The **Message Options** dialog box is displayed.

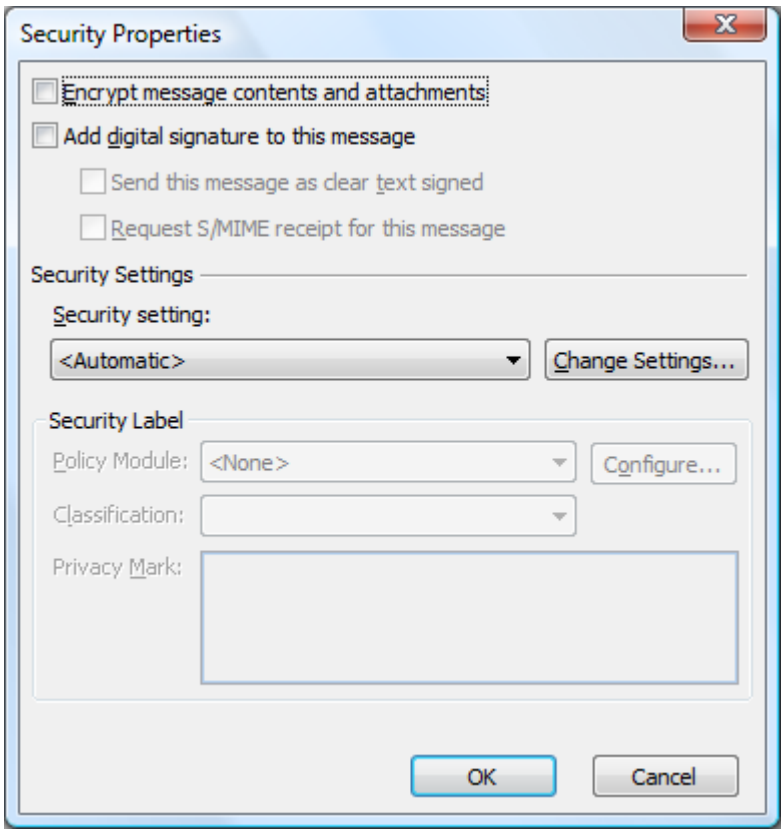


   a. Click **Security Settings**.

      The **Security Properties** dialog box is displayed.

Prerequisites

- Microsoft Outlook is installed on your workstation.
- Microsoft CAPI Support (sub-component of the Digital Certificate Services component) was installed during setup.
- Microsoft Outlook Usability Enhancements (sub-component of the Digital Certificates Services component) was installed during setup. This option allows you to sign an email message with a single click (optional).
- A certificate with email signature capabilities is available on your smart card.
- You have configured your security profile in Outlook (see "Automatically Configure your Microsoft Outlook Security Profile" on page 36).



b. Select **Add digital signature to this message** and click **OK**.

c. Close the **Message Options** dialog box.

4. Complete and send the email message.

Read Signed Email Messages

If you receive a digitally signed email message, you can use your email client to validate the sender's identity.

Click the signed message that you want to read. If the sender is successfully authenticated, the message appears with a secure message icon.

Send/Read Encrypted Email Messages

Encrypting an email message guarantees that only the proper recipient can open and read the message and its attachments. Email encryption is based on the public key infrastructure.

Decrypting an encrypted email message is performed directly on your smart card for increased security.

Send Encrypted Email Messages

1. Create the email message.
2. Do one of the following:
   - From the Outlook toolbar, click the **Encrypt Message Contents and Attachments** icon .
   - Click **Options** on the **View** menu (or the **Options** icon on the toolbar).

   The **Message Options** dialog box is displayed.
3. Select **Security Settings**.

   The **Security Properties** dialog box is displayed.
4. Select **Encrypt message contents and attachments** and click **OK**.
5. Close the **Messages Options** dialog box.
6. Complete and send the email message.

Prerequisites

- Microsoft Outlook is installed on your workstation.
- You have access to the certificate of the person to whom you want to send an encrypted email message (see "Automatically Add Certificates to Microsoft Outlook Contacts" on page 38).
- You have configured your security profile in Outlook (see "Automatically Configure your Microsoft Outlook Security Profile" on page 36).

Read Encrypted Email Messages

1. Insert your smart card (chip-side up and chip first) into the smart card reader.
2. Click the encrypted message you want to read.
3. Enter your PIN.

   The email message and attachments are displayed along with the secure message icon informing you of the encryption status.

Prerequisites

- Microsoft Outlook is installed on your workstation.
- A certificate with email encryption capabilities is available on your smart card.
- Your encryption certificate is available to other users (see "Automatically Publish your Certificates to the Global Address List" on page 37).
- Microsoft CAPI Support (sub-component of the Digital Certificate Services component) was installed during setup.

Automatically Decrypt and Save Emails

ActivClient allows you to save a decrypted version of encrypted emails. This enables you to access these emails even after your encryption email is no longer available (for example if your card management system and policy do not support recovery of expired certificates).

1. Open the encrypted email.
2. Enter your PIN.

   ActivClient automatically decrypts and saves the email, replacing the encrypted version.

Prerequisites

- Microsoft Outlook is installed on your workstation.
- Microsoft Outlook Usability Enhancements (sub-component of the Digital Certificates Services component) was installed during setup.
- The ActivClient policy, **Automatically decrypt encrypted e-mails**, is enabled (it is disabled by default; your administrator may have enabled this feature).

The email message and attachments are displayed. In addition, the secure message icon is no longer displayed, indicating that the message is not encrypted.

Send/Read Signed and Encrypted Mails with Thunderbird

Send/Read Signed Email Messages

A digital signature is a combination of your private key and the message. It authenticates you as the message sender and verifies the integrity of the message. With ActivClient, the digital signature is performed directly on your smart card.

Send Signed Email Messages

1. Insert your smart card (chip-side up and chip first) into the smart card reader.
2. Start your email client.
3. Click **Write.**
4. Compose your mail and go to **Security** (on the top toolbar of your mail) and select **Digitally Sign this message and encrypt**.
5. Click **Send.**
6. Enter your **PIN.**
7. Verify the sent email has been signed.

Prerequisites

- Thunderbird is installed on your computer.
- A certificate with email signature capabilities is available on your smart card.
- If you use ActivClient 32-bit, Thunderbird support was installed during setup.
- If you use ActivClient 64-bit, the ActivClient PKCS#11 library was installed during setup and then installed in Thunderbird.

For details, see the *ActivClient for Windows Installation Guide*.

Read Signed Email Messages

1. Insert your smart card (chip side up and chip first) into the smart card reader.
2. Start your email client.
3. In your Inbox, click on the signed message you want to read. If the sender is successfully authenticated, the message appears with a secure message icon.

Document Version 06.2.09 | ©2009 ActivIdentity, Inc.

Send/Read Encrypted Email messages

Encrypting an email message guarantees that only the proper recipient can open and read the message and its attachments. Email encryption is based on the public key infrastructure.

Decrypting an encrypted email message is performed directly on your smart card for increased security.

Prerequisites

- Thunderbird is installed on your workstation.
- A certificate with email signature capabilities is available on your smart card.
- If you use ActivClient 32-bit, Thunderbird support was installed during setup.
- If you use ActivClient 64-bit, the ActivClient PKCS#11 library was installed during setup and then installed in Thunderbird.

For further information about the setup, see the *ActivClient for Windows Installation Guide*.

Send Encrypted Email Messages

1. Insert your smart card (chip-side up and chip first) into the smart card reader.
2. Start your email client.
3. Click **Write**.
4. Compose your mail and go to **Security** (on top of the email toolbar) and select **Encrypt this message.**
5. Encrypt your mail.
6. Click **Send.**
7. Enter your PIN.
8. Look in your Sent Items for the sent email and verify it is encrypted.

Read Encrypted Email Messages

1. Insert your smart card (chip-side up and chip first) into the smart card reader.
2. Start your email client.
3. Select the encrypted email.
4. Enter your PIN when prompted.
5. Read the encrypted mail in clear text.

Encrypt/Decrypt Files with EFS

Windows Vista, Windows 7 and Windows Server 2008 allow the Encryption File System (EFS) feature to use smart card certificates for files and folder encryption. Depending on your smart card content and your platform configuration, you can seamlessly encrypt and decrypt files.

Configure your Workstation for EFS and Select/Generate a Smart Card Encryption Certificate

In order to encrypt and decrypt files on your workstation, you may need to configure EFS during your first file encryption (depending on your platform configuration).

1. Start Microsoft Explorer.
2. Insert your smart card.
3. Select the file or folder to encrypt.
4. Update your file or folder properties to enable encryption (via the **Advanced** button and then the **Encrypt contents to secure data** option).
5. When prompted to choose an existing encryption certificate or create a new one on your smart card, either:
   - Select your existing smart card EFS certificate in the certificate list.
   - Choose to create either a smart card self-signed certificate or a certificate issued by your domain's certification authority.
6. Enter your smart card PIN and click **OK**.

   The selected or new certificate will be used for all file encryption and decryption operations. The selected file or folder is encrypted and appears in green in Microsoft Explorer.

Encrypt a File or Folder with EFS

1. Start Microsoft Explorer.
2. Insert your smart card.
3. Select the file or the folder to encrypt.
4. Update your file or folder properties to enable encryption (via the **Advanced** button and then the **Encrypt contents to secure data** option).

EFS Encryption/Decryption Prerequisites

- Your operating system is either Windows Vista, Windows 7 or Windows Server 2008.
- Your platform is configured for EFS.
- Your platform is configured to require the use of a smart card for EFS.
- Your smart card contains a certificate configured for EFS.

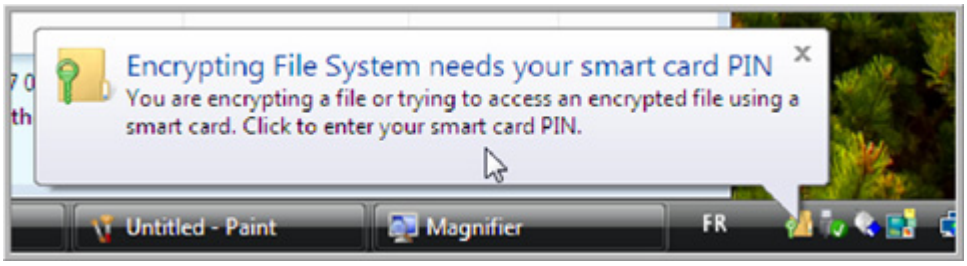
5. Enter your smart card PIN and click **OK**.

   The file or the folder is then encrypted and appears in green in Microsoft Explorer.

Decrypt a File or Folder with EFS

1. Start Microsoft Explorer.
2. Insert your smart card.
3. Open the file or the folder to decrypt.

   A window is displayed at the lower right corner of your desktop prompting you to enter your smart card PIN.



4. Click on the displayed link.
5. Enter your smart card PIN and click **OK**.

   The file or folder is opened in clear text.

Update EFS Certificates and Re-Encrypt Files

If you have already encrypted some files with a certificate and if you want to update the encryption certificate (for example, it expired), Windows allows you to re-encrypt encrypted files with a new or existing encryption certificate.

If your old certificate is on a different smart card than the new certificate, then both smart cards need to be available / inserted during this process.

1. In the Windows Control Panel, select **User Accounts**.
2. Click **User Accounts** and then, from the left pane, select **Manage your file encryption certificates**.

   The Manage your file encryption certificates wizard is displayed.

EFS Update Prerequisites

- Your operating system is either Windows Vista, Windows 7 or Windows Server 2008.
- Your platform is configured to allow EFS.
- Your platform is configured to require a smart card for EFS.
- You have the smart card containing the EFS certificate currently configured for EFS on this platform.
- You have a smart card containing a new certificate.
- You have files encrypted with your current EFS certificate.

3. When prompted to select an existing encryption certificate or create a new one on your smart card, either:

- Choose to create either a new smart card self-signed certificate or a certificate issued by your domain's certification authority:
  a. Insert your smart card.
  b. Click **Next**.
  c. Back up your key (optional) and click **Next**.
- Choose to select an existing smart card EFS certificate from the certificate list.

  A tree representing your file system is displayed.

4. Select the folders to re-encrypt. Make sure all folders containing your encrypted files are selected.

5. Enter your smart card PIN when prompted and click **OK**.

   The wizard completes successfully.

Note

The old EFS certificate and the new one will co-exist on the same card.

Recover Encrypted Files

When you loose or damage your smart card, you need to recover the content of your encrypted files.

1. Import the backup EFS certificate in your new smart card using the ActivClient User Console.

2. In Microsoft Explorer, select one of the encrypted files you need to recover.

3. When prompted, insert your smart card containing the new EFS certificate.

4. Enter your smart card PIN and click **OK**.

   You can access your file in clear text.

EFS Recovery Prerequisites

- Your operating system is either Windows Vista, Windows 7 or Windows Server 2008.
- Your platform is configured to allow EFS.
- Your platform is configured to require smart card for EFS.
- You have backed up your EFS certificate in a certificate file in a secure location.
- You have a new smart card.
- You have files encrypted with your lost or damaged EFS certificate smart card.

Note

Depending on your configuration, a recovery agent may be configured to help you recover your data. For more information on file/folder recovery, see the Microsoft Windows Help on your Windows platform.

Chapter 5: Managing Remote Access/OTP

This chapter explains how to synchronize your smart card and configure remote access.

In This Chapter

53 Synchronize your Smart Card

54 Configure your Remote Access User Name

Synchronize your Smart Card

If you are unable to authenticate using one-time passwords, contact your help desk to diagnose the problem. Your help desk may determine that your smart card is out of sync with the authentication server. In this case, perform the following steps in order to solve the problem.

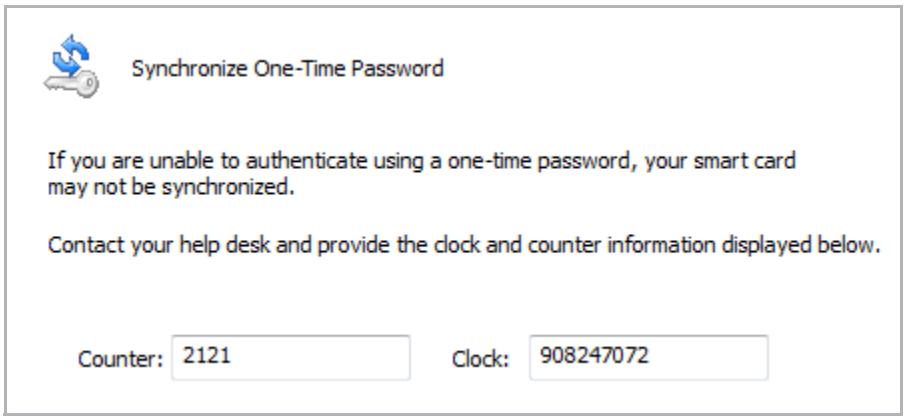
Prerequisites

- Your smart card is initialized to use one-time passwords.
- The One-Time Password Services component was installed during setup.

1. Open the ActivClient User Console.
2. To select a server to authenticate to, either:
   - From the **Tasks** pane, under **One-Time Password Tasks**, click **View one-time password**.
   - From the right pane, double-click the **One-Time Password** icon .

   An icon for each authentication server is displayed (usually only one server is available, hence only one icon is displayed) in the right pane.
3. To start the synchronization process, either:
   - From the right-pane, right-click the **One-Time Password** icon and select **Synchronize one-time password**.
   - From the **Tasks** pane, under **One-Time Password Tasks**, click **Synchronize one-time password**.

   The **Synchronize One-Time Password** dialog box is displayed.



4. Provide the **Clock** and **Counter** values to your help desk.

   Your help desk will synchronize or re-synchronize your device on the authentication server.

Configure your Remote Access User Name

If you want to use your smart card for remote access with one-time password, the smart card must also contain the user name used to logon to the remote service. Depending on your configuration, you may need to define or update the user name.

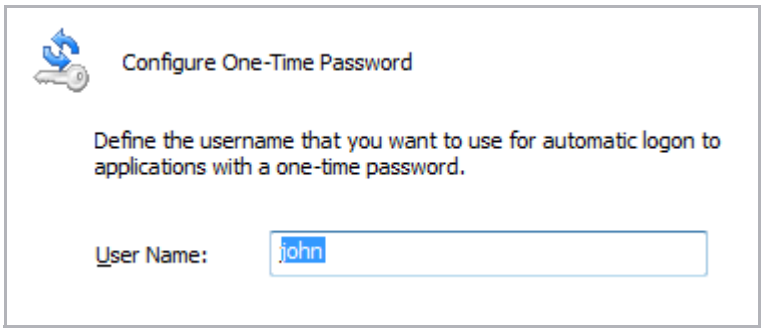
Prerequisites

- Your smart card is initialized to use one-time passwords.
- The One-time Passwords Services component was installed during setup.

1. Open the ActivClient User Console.
2. Either:
   - From the **Tasks** pane, under **One-Time Password Tasks**, click **View one-time password**.
   - From the right pane, double-click the **One-Time Password** icon .

   An icon for each authentication server is displayed (usually only one server is available, hence only one icon is displayed) in the right pane.
3. Select the server to which you want to authenticate.
4. To configure your remote access user name, either:
   - Right-click the server and select **Configure one-time password**.
   - From the **Tasks** pane, under **One-Time Password Tasks**, click on **Configure one-time password**.

   The **Configure One-Time Password** dialog box is displayed.



5. Enter your name in the **User Name** field and click **OK**.

   Your remote access user name is configured.

Chapter 6: Using Remote Access/OTP

This chapter explains how to generate and log on with a one-time password (OTP).

In This Chapter

56 Log on to Check Point VPN-1 with a One-Time Password

57 Automatically Generate a One-Time Password

58 Manually Generate a One-Time Password

Log on to Check Point VPN-1 with a One-Time Password

Note: The Check Point VPN feature is only available in ActivClient 32-bit versions.

ActivClient integrates seamlessly with the Check Point VPN1 SecureClient.

ActivClient generates one-time passwords and sends them to the VPN client transparently each time you perform a secure connection.

Prerequisites

- Check Point VPN1 SecureClient is installed on your workstation.
- One-Time Password Services and Check Point VPN-1 support components have been installed during ActivClient setup.
- Your smart card is initialized to use one-time passwords.

1. Start Check Point VPN1 SecureClient.
2. Make sure your smart card is inserted.
3. Enter your PIN.

   You are authenticated.

   If you do not have a smart card, you need an emergency password. Contact your help desk.

Automatically Generate a One-Time Password

ActivClient provides an automatic way to log on to some remote access applications using one-time passwords.

The **Get One-Time Password** (OTP) option:

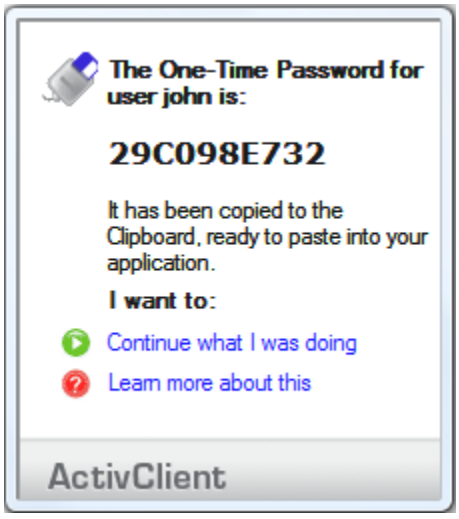
- Generates the OTP in a synchronous mode.
- Displays the OTP in a notification window (a tool tip is displayed in the Windows notification area).
- Automatically copies the OTP to the clipboard so it is ready to be pasted into any application.

Prerequisites

- ActivClient Agent is installed.
- One-Time Password Services component was installed during setup.
- Your smart card is initialized to use one-time passwords.

1. Left or right-click on the ActivClient Agent icon in the Windows notification area and select **Get One-Time Password.**

   The ActivClient notification window is displayed, showing the one-time password generated on your smart card. The password is automatically copied to your clipboard.



2. Place your cursor in the password field of the application to which you want to authenticate.

3. Select **Paste** (or press Ctrl + V).

   The one-time password generated by ActivClient is pasted into the application of your choice.

Manually Generate a One-Time Password

You can also manually log on to some remote access applications by generating a one-time password using the ActivClient User Console. You can then use this password with any application (whether running on your workstation or not).

Prerequisites

- ActivClient User Console is open.
- One-Time Password Services component was installed during setup.
- Your smart card has been initialized to use one-time passwords.

1. To display the **Generate One-Time Password** dialog box, either:

   – From the ActivClient User Console tasks pane, select **Generate one-time password**.
   – From the ActivClient User Console right pane, double-click the server's icon.

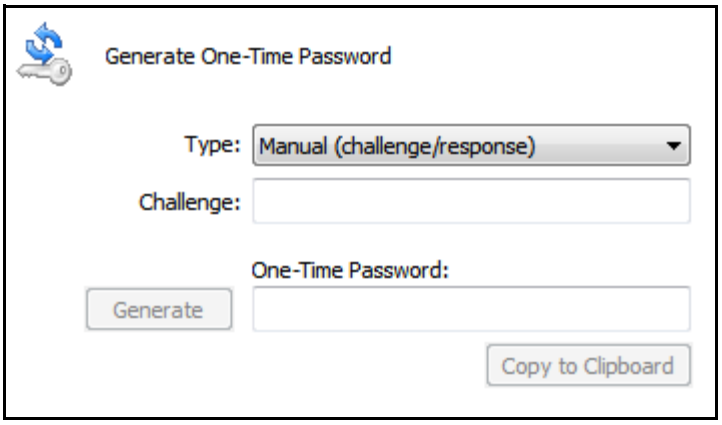
   The **Generate One-Time Password** dialog box is displayed.

2. Depending on your administrator's recommendations, either:

   – If your administrator recommends to authenticate in **Automatic** mode, click **Generate**.

     A one-time password is displayed which you can type or copy/paste into any authentication window.
   – If your administrator recommends to authenticate in a **Challenge/Response** mode, select **Manual** (Challenge/Response) from the **Type** drop-down list.

     A **Challenge** field is displayed in the **Generate One-Time Password** dialog box.



   a. Locate the challenge on the application you are authenticating to. (For challenge/response applications, the challenge is displayed in the dialog box used when logging in).

   b. Type the challenge in the **Challenge** field.

   c. Click **Generate**.

      Your newly generated one-time password is displayed.

   d. Type (or copy and paste) it into any authentication window.

Chapter 7: Viewing Personal Information

This chapter explains how to display the personal information stored on your smart card.

In This Chapter

59 About Personal Information

59 View “My Personal Info” on CAC and PIV Cards

About Personal Information

US Department of Defense CAC smart cards and US Government Personal Identity Verification PIV smart cards allow you to access personal information.

The personal information displayed may vary according to your type of card and profile. It includes:

- Cardholder identification and general information
- Benefits
- Employment information
- Cardholder’s facial image

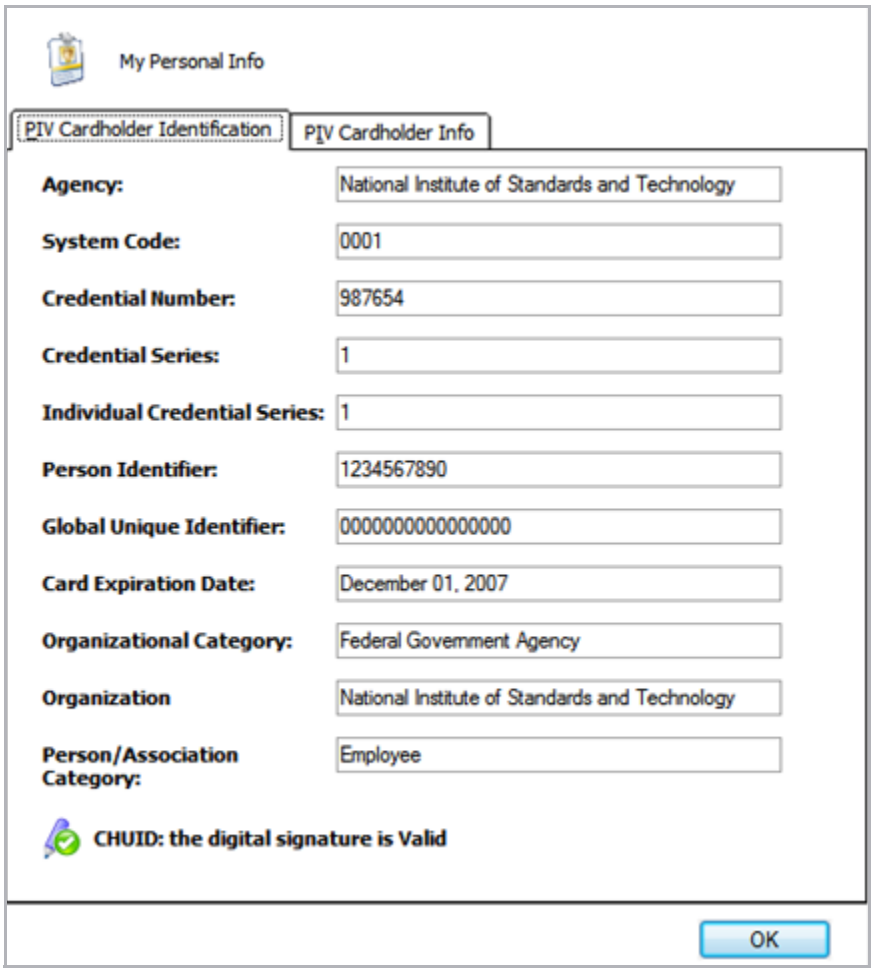
Important: The View my personal info feature is a read-only feature!

View “My Personal Info” on CAC and PIV Cards

To view your personal information, either:

- From the User Console left pane, click on **View my personal info** under **My Personal Info Task**.
- From the User Console right pane, either:
  - Double-click **My Personal Info** icon .
  - Right-click on the **My Personal Info** icon and select **Open**.

  The **Personal Information** dialog box is displayed on the right pane.



For PIV smart cards, the User Console displays the digital signature’s validity for:

- CHUID (Card Holder Identification)
- Fingerprints
- Facial Image

Chapter 8: Using and Managing ActivClient

This chapter explains how to use the non-authentication and management functions of ActivClient.

In This Chapter

61 View ActivClient System Information
62 Troubleshoot ActivClient
64 Perform Advanced Diagnostics
66 Use the Forget state for all cards Option
67 Activate Log Files from the ActivClient User Console
68 Configure ActivClient
69 Auto-Update Service

View ActivClient System Information

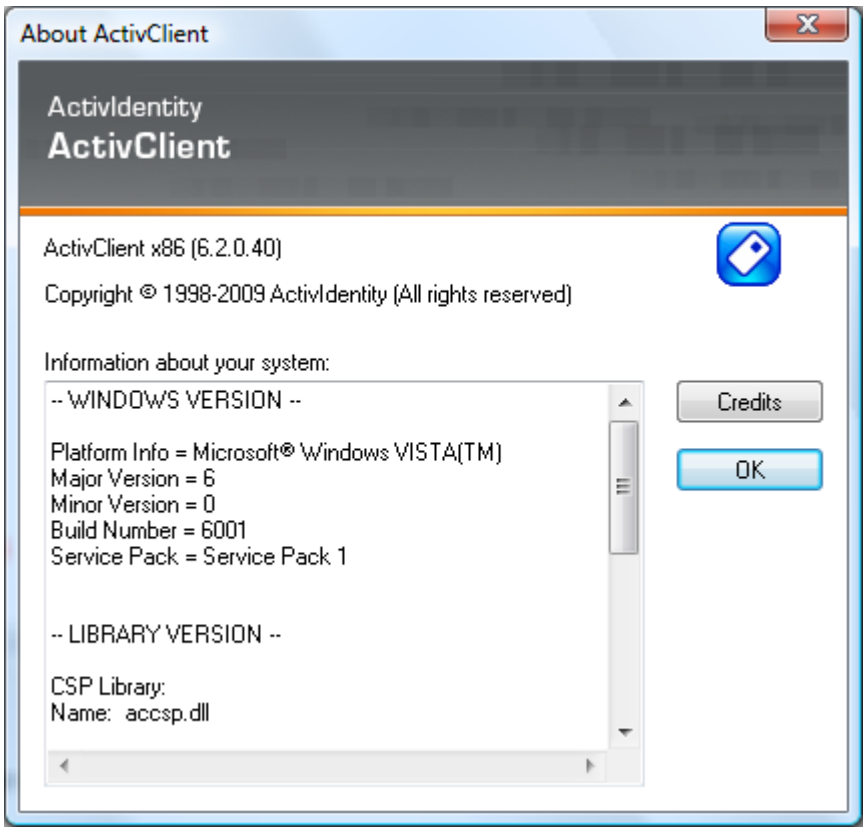
To help troubleshoot ActivClient issues, your help desk may ask you to provide system information about your ActivClient installation.

The About ActivClient window displays information such as:

- ActivClient edition and version number
- Build Number
- Copyright information
- Information about your system, such as Windows version and web browser version
- Credits information (click the **Credits** button)

1. To view the ActivClient system information, either:
   - From ActivClient User Console, select **About ActivClient** from the **Help** menu.
   - On ActivClient Agent icon  in the Windows notification area, left or right-click and select **About**.

   The About ActivClient window is displayed.



Troubleshoot ActivClient

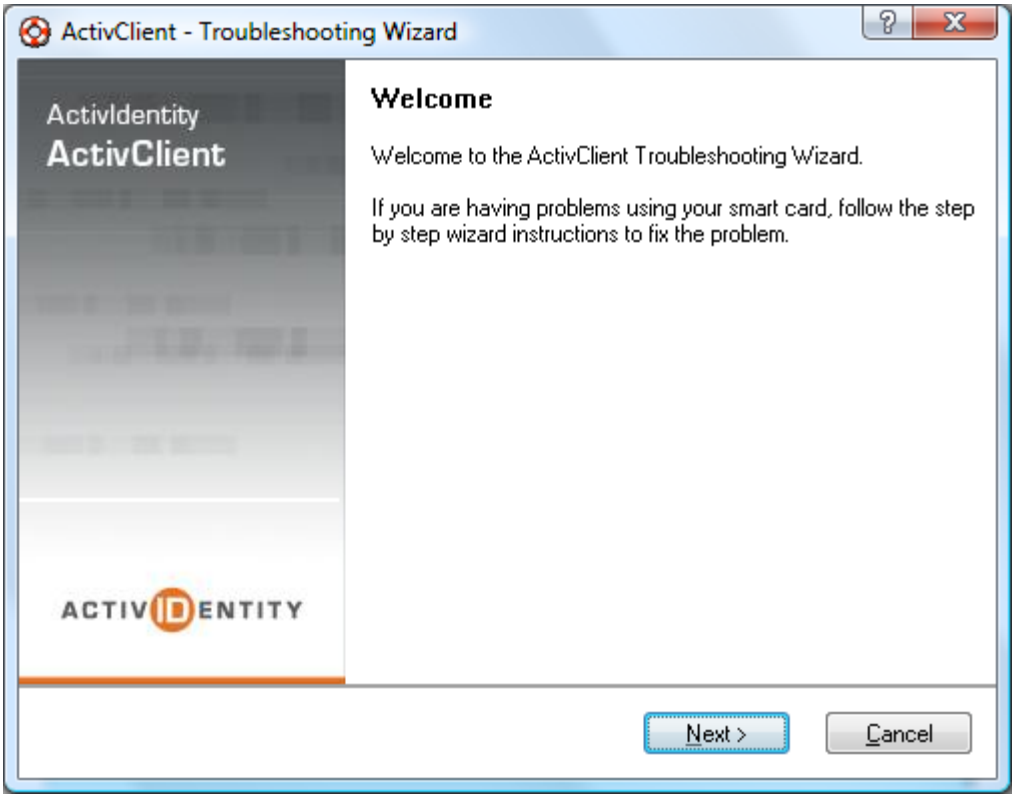
The Troubleshooting Wizard:

- Helps you to resolve issues you may encounter while using a smart card with ActivClient
- Analyzes your system
- Diagnoses problems
- Displays the results in the Diagnosis And Resolutions window
- Provides instructions on how to correct problems

1. To access the Troubleshooting Wizard, either:

   – From the ActivClient User Console **Standard** toolbar, select the **Troubleshoot Wizard icon** .
   – From the ActivClient User Console **Help** menu, select **Troubleshoot**.
   – From the ActivClient User Console **Help Tasks** section, select **Troubleshoot a problem**.
   – From the Windows Start men, go to **Programs**, **ActivIdentity**, **ActivClient** and select **Troubleshooting**.

   The Troubleshooting wizard is displayed.



2. Click **Next** on the **Welcome** screen and follow the instructions to proceed.

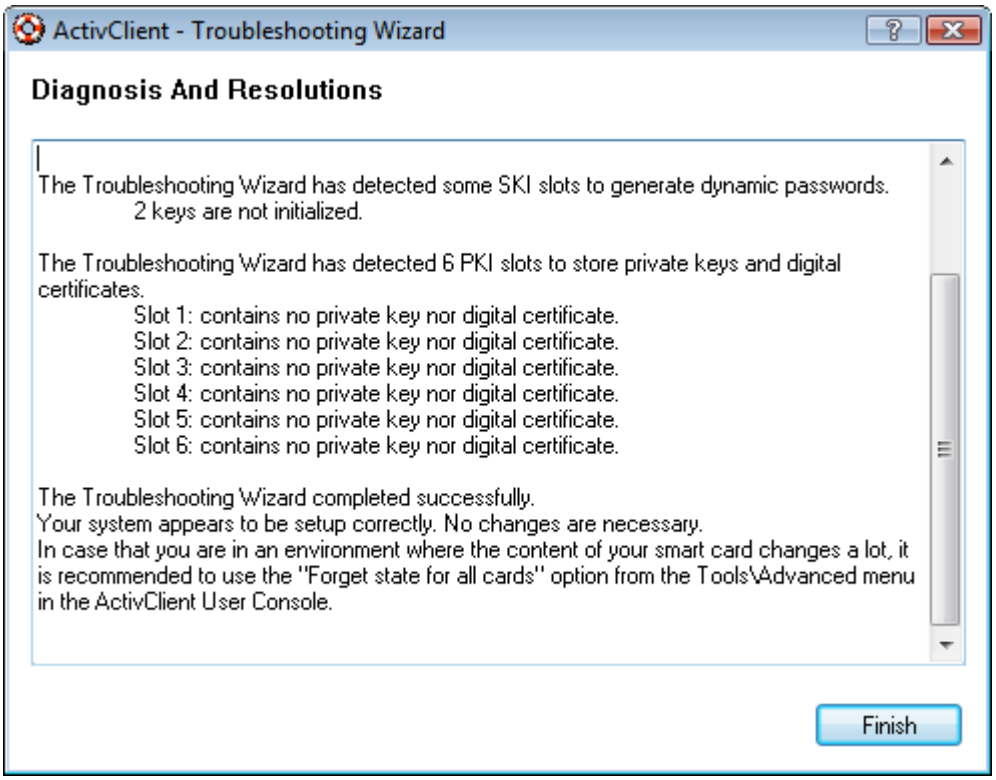
3. Enter your PIN and click **Next**.

   If you do not enter your PIN, the **Diagnosis and Resolutions** report will not proceed with PIN related operations such as:

   – Test encrypt and decrypt
   – Digital signature
   – Web authentication

   If problems are detected, the **Problems found** page is displayed.

4. Click **Next**.



5. Follow the instructions displayed in the **Diagnosis and Resolutions** page and click **Finish**.

Perform Advanced Diagnostics

The Advanced Diagnostics tool:

- Helps administrators perform a thorough examination of your environment.
- Provides information synthesized in one single report which you can send to your help desk.

1. To access the Advanced Diagnostics wizard, either:
   - On the ActivClient Agent icon  in the Windows notification area, left or right-click and select **Advanced Diagnostics**.
   - From the ActivClient User Console **Standard** toolbar, select the **Advanced Diagnostics** icon .
   - From the ActivClient User Console **Help** menu, select **Diagnose**.
   - From the Windows Start menu, go to **Programs**, **ActivIdentity** and select **Advanced Diagnostics**.

The Advanced Diagnostics wizard is displayed.

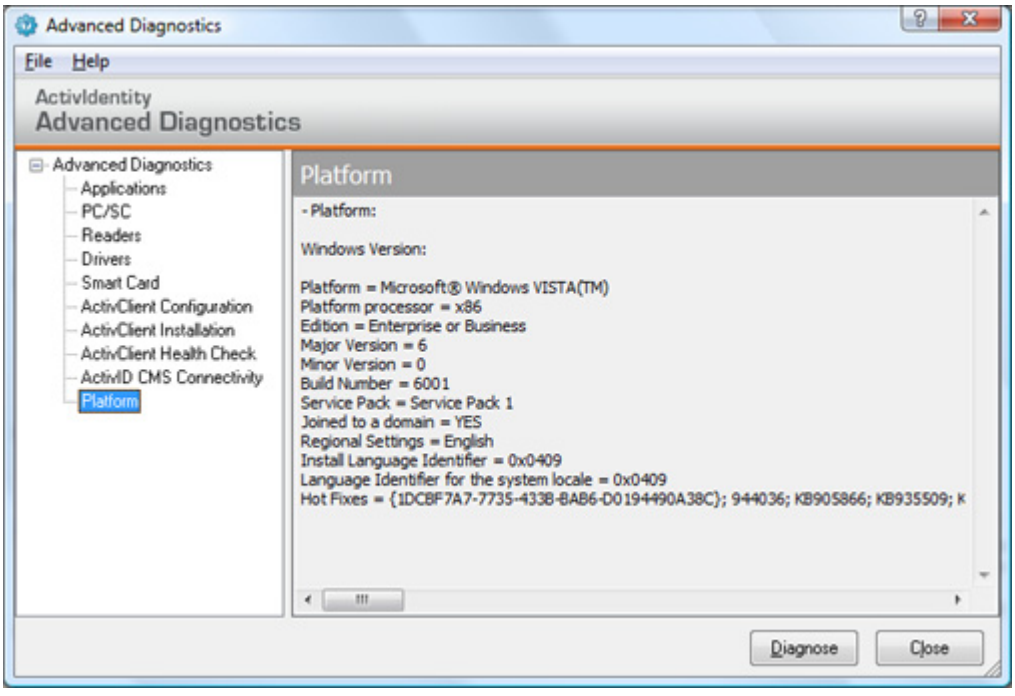
2. To generate a report, make sure you have inserted a smart card.

3. Click **Diagnose**.

   A single report is generated and stored in a log file which you can send to your help desk.

   The generated report is displayed in eight categories which you can access by clicking on the corresponding nodes:

   – Applications
   – PC/SC
   – Readers
   – Drivers
   – Smart Card
   – ActivClient Configuration
   – ActivClient Installation
   – ActivClient Health Check
   – ActivID CMS Connectivity
   – Platform



4. Select one of the eight categories you want to display.

5. To copy part of your report, select the required view, and select **File** and click **Copy.**

   The content of the option you selected is copied to the clipboard and can be pasted into a file and location of your choice.

6. To save your report, select **File** and click **Save as**.

   All the information is saved in a single log file.

7. To print the report, select **File** and click **Print**.

   The entire report is sent to your default printer.

8. If your administrator has enabled the option, you can email the report to your help desk by selecting **File** and then clicking **Email**.

   The report is saved as a log file and your default email application (for example, Outlook) opens with a new message.

   The log file is then attached to the new mail message.

9. Add any additional information and send the message to your help desk.

Warning!

The diagnostic report may consist of hundreds of pages. If you only want to print part of the report, either save it as a log file first or copy the relevant option(s) to a file, and then print only the relevant sections.

Note

The destination email address may be pre-defined by your administrator.

Use the Forget state for all cards Option

To optimize performance, ActivClient stores some smart card information on the workstation. This is limited to smart card configuration data (such as smart card profile) and does NOT include any credentials such as user names, passwords, keys or digital certificates.

In most environments, ActivClient will refresh this information as needed when your smart card content is updated. In some cases, in order to solve potential problems, your technical support may suggest to "tell" ActivClient to "forget" any smart card information it may have saved.

1. Open the ActivClient User Console.

2. Go to the **Tools** menu.

3. Select **Advanced** then, **Forget state for all cards**.

   The information stored on your workstation about card configuration is reset.

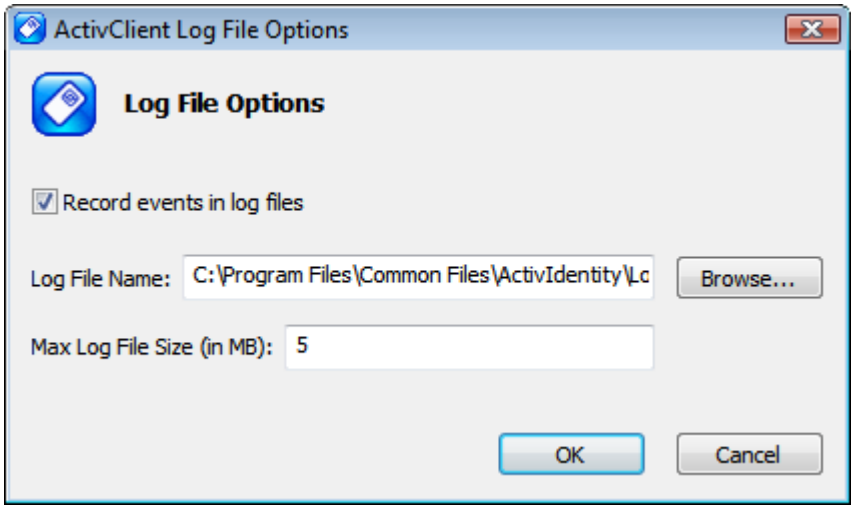
Activate Log Files from the ActivClient User Console

The ActivClient log files contain detailed information for every action performed by ActivClient. The information contained in these files may be useful to your technical support when trying to solve problems.

ActivClient allows you to configure log files without having administrator rights. You can configure log system activity from the ActivClient User Console.

1. From the ActivClient User Console, go to the **Tools** menu.
2. Select **Advanced**, **Log File Options.**

   The **ActivClient Log File Options** dialog box is displayed.



3. Select the **Record events in log files** option.
4. Enter a name for the log file in the **Log File Name** field.
5. Type a size for the log file in the **Max Log File Size (in MB)** field.
6. Click **OK**.

   You are prompted to reboot in order to enable logging for all ActivClient components.

7. Save and close all your applications and select **Reboot Now** (or **Reboot Later** if you prefer to enable logging later).

Security Note

In order to guarantee privacy and security, no secret (such as private key) nor personally identifiable information (such as digital certificate) are recorded in the ActivClient log files.

Log Activity Recommendations

- Turn off logging system activity in normal use cases.
- Turn on logging system activity only when required by your system administrator or help desk.
- After log file creation, ActivIdentity recommends disabling log system activity!

Configure ActivClient

Only local administrators can configure ActivClient. Administrators can select specific security policies, such as "**smart card removal behavior"**. For example, when users remove their smart card from the smart card reader, the workstation behaves either way depending of pre-set configuration:

- Lock workstation
- Log off session
- No action

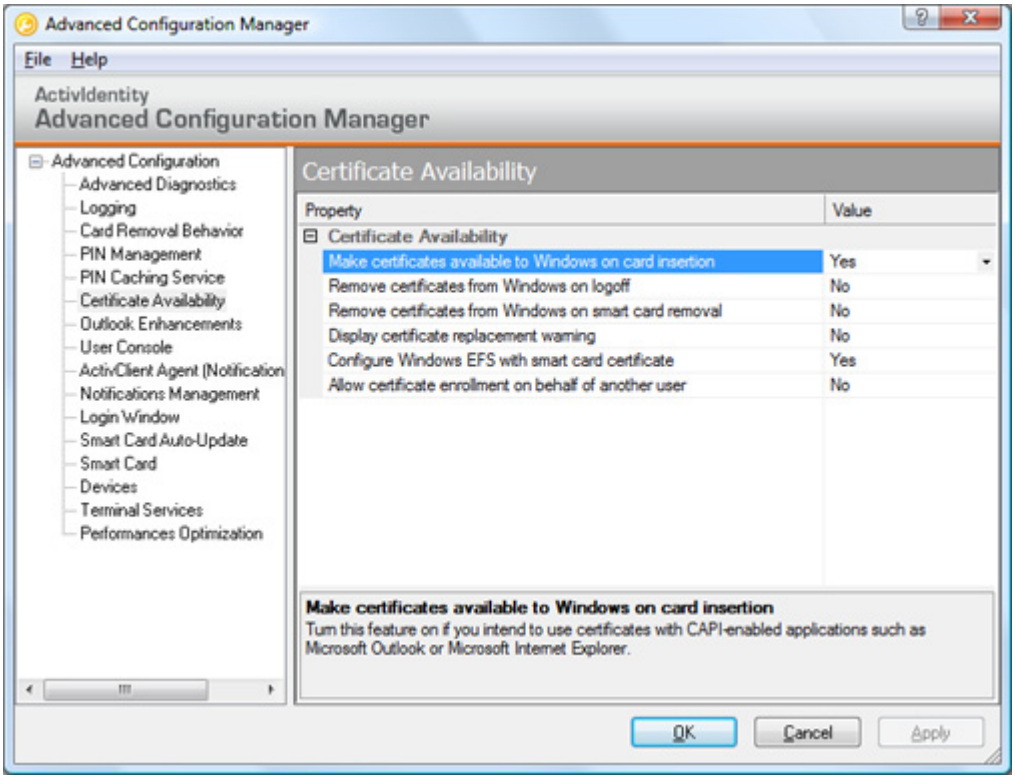
ActivClient configuration is handled by the Advanced Configuration Manager. For more specific information, see the policy definition chapter in the *ActivClient for Windows Administration Guide*.

Prerequisite

The Advanced Configuration Manager was installed during the ActivClient setup.

1. To access the Advanced Configuration Manager, either:
   - On the ActivClient Agent icon  in the Windows notification area, left or right-click and select **Advanced Configuration Manager**.
   - From the ActivClient User Console's **Tools** menu, select **Advanced** then, **Configuration**.
   - From the Windows Start menu, go to **Programs**, **ActivIdentity** and select **Advanced Configuration Manager**.

   The Advanced Configuration Manager window is displayed.



For information on the settings and their values, read the description displayed at the bottom of the window each time you select an option.

Auto-Update Service

ActivClient can be configured so that software updates are automatically downloaded and installed on your workstation.

Prerequisite

This feature is enabled only if the **Auto-Update** component is installed and if your organization has set up an auto-update server. For further information, see the *ActivClient for Windows Administration Guide*.

Chapter 9: Using ActivClient with Terminal Services

This chapter explains how to use ActivClient in Citrix and Remote Desktop environments.

In This Chapter

70 Log on to a Citrix Session
72 Use your Smart Card Inside a Citrix Session
72 Log on to a Remote Desktop Session
73 Use your Smart Card in a Remote Desktop Session
73 Lock a Remote Desktop Session

Log on to a Citrix Session

You can use Citrix products to run an application on a Citrix server. ActivClient provides smart card-based authentication to Citrix for increased security.

It is not necessary to install ActivClient on the Citrix client unless you intend to log on to the client workstation with a smart card.

Prerequisites

- ActivClient is installed on the Citrix XenApp Server. For more information on supported versions of Citrix server, see the *ActivClient for Windows Overview*.
- Your workstation is configured with Citrix client (Program Neighborhood, Program Neighborhood Agent, or Web Interface).
- You have a smart card and a smart card reader up and running and connected to your workstation.

How you log on to a Citrix session depends on your configuration. There are three cases you might encounter:

- You log on to your workstation with a smart card and digital certificate and your Citrix authentication mode is “Smart Card with Pass-through”.
  - You are logged in automatically as soon as you start a Citrix session
- You log on to your workstation with a user name and password (standard Windows authentication) and your Citrix authentication mode is “Local User with Pass-through”.
  - You are logged in automatically as soon as you start a Citrix session.
- You log on to a workstation or thin terminal that is not part of the domain, and that does not have ActivClient installed.
  - You are prompted to authenticate with your smart card and PIN code (see "Log on to Windows with a Certificate" on page 39).

Sample Citrix Sessions

Three Citrix clients can be used to log on to a Citrix session:

- Citrix ICA Client Program Neighborhood
- Citrix ICA Client Program Neighborhood Agent
- Citrix Web Interface

The following sections are examples of Citrix logon sessions from a Windows client for “Smart Card with Pass-through” authentication mode with each of the Citrix clients.

Log on using Citrix ICA Client Program Neighborhood

1. Log on to Windows using your smart card.
2. Double-click the **Citrix Program Neighborhood** icon.

   The Citrix Program Neighborhood opens.
3. Double-click your custom ICA connection in the Citrix Program Neighborhood window.

   You are automatically logged on to the Citrix remote session.

Log on using Citrix ICA Client Program Neighborhood Agent

1. Log on to Windows using your smart card.
2. Right-click on the Citrix Program Neighborhood Agent icon located in the Windows notification area and select your Citrix server desktop.

   You are automatically logged on to the Citrix remote session.

Log on using Citrix Web Interface

1. Log on to Windows using your smart card.
2. Open your browser.
3. Enter your Web Interface server URL.

   You are automatically authenticated and you access your Citrix Web Interface web page.
4. Double-click your Citrix server desktop icon in your Citrix Web Interface web page.

Prerequisites

- Microsoft CAPI Support (sub-component of the Digital Certificate Services component) was installed during setup on the Citrix XenApp server and on the local workstation (if the local workstation is a Windows workstation used for smart card logon to the domain).
- You have a smart card and a certificate with PKI logon capabilities.
- Citrix ICA Client Program Neighborhood is installed.
- A custom ICA connection is configured for your Citrix Server.
- The Citrix authentication mode is “Smart Card with Pass-through”.
- Your Web Interface Server URL is configured in Citrix ICA Client Program Neighborhood Agent.

Note

For further information on Citrix client configuration, see the Citrix documentation available on Citrix Web site.

The Windows logon interface of your Citrix server desktop displays within your browser window.

5. Enter your PIN code.

   You are automatically logged on to the Citrix remote session within your browser window.

Use your Smart Card Inside a Citrix Session

You can use Citrix XenApp Server to run an application on a Citrix server. ActivClient provides smart card-based services for applications running in the Citrix session.

1. Start the application you are using with your smart card, for example, Microsoft Outlook.
2. Use one of the smart card-based services (for example, prepare to send a signed email message).
3. When you are prompted for the PIN, enter your smart card PIN, and click **OK**.

   The application running on the Citrix server communicates with your smart card that is connected locally to your computer.

Notes

- It is not necessary to install ActivClient on the Citrix client workstation.
- Smart card management operations such as certificate download operations are not available within the Citrix session.

Prerequisites

- ActivClient is installed on the Citrix XenApp Server. For more information on supported versions of Citrix Presentation Server, refer to *ActivClient for Windows Overview*.
- Your workstation is configured with Citrix client (Program Neighborhood, Program Neighborhood Agent, or Web interface).
- You have a smart card and a smart card reader up and running and connected to your workstation.
- You are logged on to a Citrix session.

Log on to a Remote Desktop Session

Microsoft Remote Desktop allows you:

- To remotely control your computer from another office, home, or while traveling in order to use the data, applications, and network resources that are on your office computer.
- To connect to a Windows server with Windows Terminal Services enabled, to access applications not available on your local workstation.

ActivClient provides smart card-based authentication to the Remote Desktop for increased security.

1. Log on to your workstation.
2. Start the **Remote Desktop Connection**.
3. Select the server or workstation you want to access and click **Connect**.
4. Make sure your smart card is inserted.
5. Enter your PIN to start the session.

Use your Smart Card in a Remote Desktop Session

You can use Microsoft Remote Desktop to run an application on a remote computer (workstation or server). ActivClient provides smart card-based services for applications running in the Remote Desktop session.

1. Start the application that is using your smart card, for example, Microsoft Outlook.
2. Use one of the smart card-based services (for example, prepare to send a signed email message).
3. When you are prompted for the PIN, enter your smart card PIN, and click **OK**.

   The application running on the Remote Desktop (remote computer) communicates with your smart card that is connected locally to your computer. After a few moments, the operation is completed (for example, the signed email is sent).

Note

Smart card management operations such as certificate download operations are not available within a Remote Desktop session.

Prerequisites

- ActivClient is installed on the remote Windows workstation or server.
- Remote Desktop Connection is installed on your local Windows workstation.
- You have a smart card and a smart card reader up and running connected to your workstation.

Lock a Remote Desktop Session

To lock the Remote Desktop session, remove your smart card from the smart card reader.

The session remains open on the remote computer. You will find the session in the same state the next time you log on, that is, the same applications will remain open in the state they were in when you locked the session.

The default configuration for ActivClient (running on the remote computer) is to lock on smart card removal. If your administrator changes this configuration (for example, to log off on smart card removal), the behavior may differ (for example, the Remote Desktop session may close).

Prerequisites

- ActivClient is installed on the remote Windows workstation or server.
- Remote Desktop Connection is installed on your local Windows workstation.
- You have a smart card and a smart card reader up and running connected to your workstation.
- You are logged on to a Remote Desktop session with your smart card.

Appendix A: Terms and Acronyms

In This Appendix

74 Terms
75 Acronyms

This appendix lists terms and acronyms used throughout the full set of ActivIdentity ActivClient for Windows technical publications. Not all terms and acronyms appear in all documents.

Terms

Certificate Authority (CA) - The CA issues and manages security credentials and public keys for message encryption in a networked environment. As part of a Public Key Infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA issues a certificate.

ActivID Card Management System (CMS) - Formally known as ActivCard Identity Management System (AIMS), CMS is a web-based, smart card, credential and application lifecycle management system. CMS augments and works in concert with an enterprise's primary identity management infrastructure components, including popular directory, database, and PKI components.

Cryptographic Service Provider (CSP) - An independent software module that performs cryptography algorithms for authentication, encoding, and encryption.

Federal Information Processing Standard (FIPS 140-2) - FIPS 140-2 is the standard for crypto-module security. FIPS 140-2 level 3 adds additional requirements to FIPS 140-2 level 2. These requirements concern physical security and a trusted path for entering a Cryptographic Service Provider, such as a PIN. FIPS 140-2 level 3 uses local ports and the key pad to enforce such security.

Federal Information Processing Standard 201 (FIPS 201) - FIPS 201 is the standard for Personal Identity Verification (PIV) cards defined for US Government employees and contractors.

My Digital ID Card (MDIDC) - This CMS component allows end users to access the self-service CMS functions, which includes card and credential management.

One-Time Password (OTP) - A one-time password is a password used only once to authenticate to remote applications. One-Time Passwords are only present on smart cards issued with SKI credentials.

Personal Identification Number (PIN) - Is used to authenticate to your smart card in order to perform actions such as Windows PKI logon, remote access and email signature.

Public Key Infrastructure (PKI) - PKI describes the laws, policies, standards, and software that regulate or manipulate certificates and public and private keys.

Registration Authority (RA) - RA is an authority in a network that verifies user requests for a digital certificate and instructs the CA to issue it. An RA is part of a PKI, a networked system that enables companies and users to exchange information safely and securely.

Symmetric Key Infrastructure (SKI) - SKI keys are used to perform strong authentication on remote applications. SKI keys encrypt passwords in:
- Synchronous mode (generates 1 password without any challenge. The server uses the same method to create a password than the smart card)
- Asynchronous: encrypts a challenge

Standalone smart card - Smart card with pre-loaded applets issued by the manufacturer.

Acronyms

Acronym

What does it stand for

CA

Certificate Authority

CAC

Common Access Card (for the United States Department of Defense)

CSP

Cryptographic Service Provider

FIPS

Federal Information Processing Standard

GAL

Global Address List

GP

GlobalPlatform

Replaces OpenPlatform (OP).

OTP

One-Time Password

PKI

Public Key Infrastructure

PIV

Personal Identity Verification

Smart card issued by the United States government to federal employees and contractors.

RA

Registration Authority

SKI

Symmetric Key Infrastructure

Document Information

ActivIdentity, Inc. welcomes your comments and suggestions.

Your input is an important factor in future revisions of this publication. Please let us know your opinion.

Product: ActivClient for Windows

Document: ActivClient for Windows User Guide

Document Reference: AC/WIN/UG/06.2009/v6.2

Please send your feedback via email to: tpd@actividentity.com. If you find errors or have general suggestions for improvement, please indicate the chapter, section and page number. If you would like a reply, please include your name, company, email address, and telephone number.

Americas +1 510.574.0100
US Federal +1 571.522.1000
Europe +33 (0) 1.42.04.84.00
Asia Pacific +61 (0) 2.6208.4888
Email info@actividentity.com
Web www.actividentity.com

ActivIdentity Intellectual Property: This document or deliverable(s) contain proprietary information of ActivIdentity Corporation and/or its subsidiaries and affiliates (collectively, “ActivIdentity”) embodying confidential information, ideas, and expressions, no part of which may be reproduced or transmitted in any form or by any means, electronic, mechanical, or otherwise, without prior written permission from ActivIdentity. This document may not be modified, copied, distributed, transmitted, displayed, performed, reproduced, published, licensed, used to create derivative works therefrom, transferred, or sold unless expressly agreed by ActivIdentity. The furnishing of this document does not imply or expressly provide a license to any of the ActivIdentity intellectual property.

Trademarks: ActivIdentity, ActivIdentity (logo), and/or other ActivIdentity products or marks referenced herein are either registered trademarks or trademarks of ActivIdentity in the United States and/or other countries. The absence of a mark, product, service name or logo from this list does not constitute a waiver of the ActivIdentity trademark or other intellectual property rights concerning that name or logo. The names of actual companies, trademarks, trade names, service marks, images and/or products mentioned herein may be the trademarks of their respective owners. Any rights not expressly granted herein are reserved.