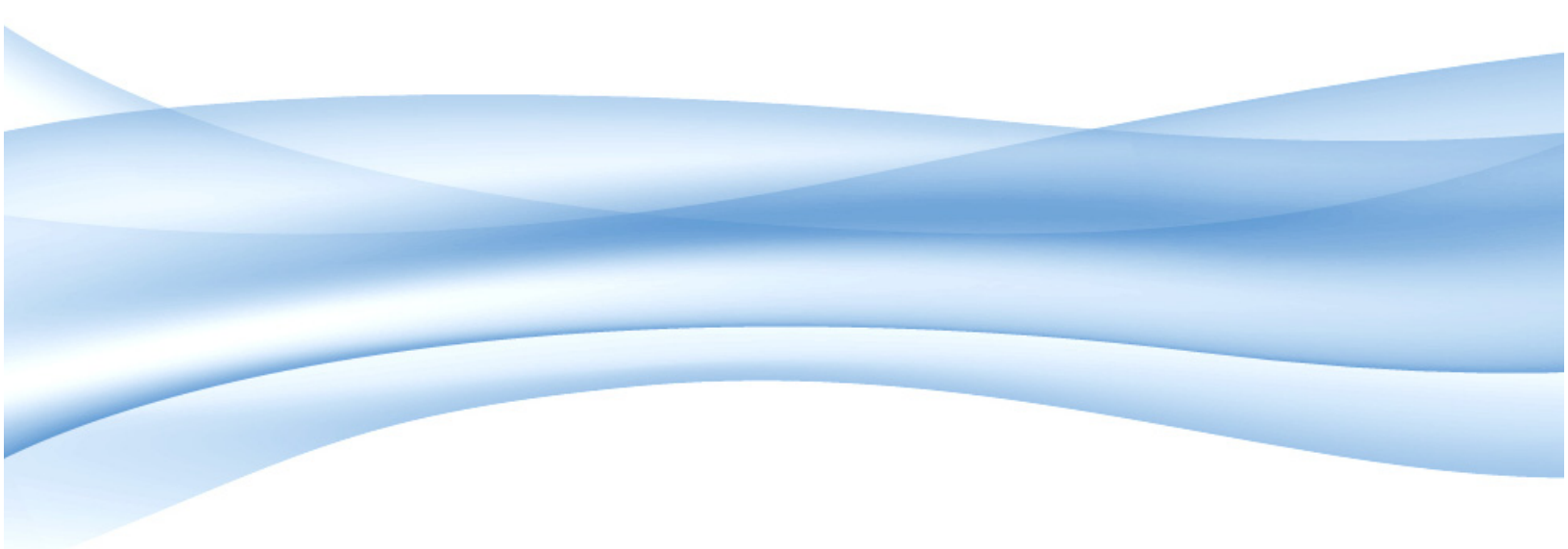


# ActivClient CAC 64-bit edition

## User Guide

**Product Version: 6.1**



**Actividentity®**

*The trusted choice for identity assurance*



# Legal Information and Notice

## ActivIdentity North America Corporate Headquarters

6623 Dumbarton Circle, Fremont, CA 94555 USA  
Tel: 1.800.529.9499  
Fax: 1.510.574.0101

## Australia

Tel: +61 (2) 62 08 48 88  
Fax: +61 (2) 62 81 74 60

## EMEA

Tel: +33 (1) 42 04 84 00  
Fax: +33 (1) 42 04 84 84

**Web Site Address:** [www.actividentity.com](http://www.actividentity.com)

**Document Reference No:** AC/x64/CAC/UG/06.2007/6.1

**ActivIdentity Intellectual Property:** This document and/or deliverable (collectively, the “document”) 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 without the prior written permission of ActivIdentity. The furnishing of this document does not imply or expressly provide a license to any of ActivIdentity’s intellectual property.

**Copyright Notice:** © 2007 ActivIdentity, Inc., 6623 Dumbarton Circle, Fremont, California 94555 USA. All rights reserved. This document and ActivIdentity software products are protected by United States copyright laws and international treaty provisions.

**Trademarks:** ActivIdentity®, the ActivIdentity logo, Protocol SecureLogin, Secure Console, and/or other ActivIdentity products or marks referenced herein are among the trademarks, service marks, or registered trademarks of ActivIdentity and may not be copied, imitated, or used, in whole or in part, without the prior written permission of ActivIdentity. Novell, NetWare, NDS, and eDirectory are registered trademarks of Novell, Inc. Microsoft and Windows are registered trademarks of Microsoft Corporation. Other Microsoft products are trademarks or registered trademarks of Microsoft Corporation. All other names of actual companies, trademarks, tradenames, service marks, images, and/or products mentioned herein are the property of their respective owners. The absence of a mark, product, service name or logo from this list does not constitute a waiver of ActivIdentity’s trademark or other intellectual property rights concerning that name or logo. Any rights not expressly granted herein are reserved.

**Patents:** ActivIdentity may have patents, pending patent applications, and/or other intellectual property rights covering subject matter contained in this document.

**Export Control:** ActivIdentity products, programs, or services referenced in this document may not be available in all countries in which ActivIdentity operates due to export restrictions or changes in market conditions. Recipient agrees to comply fully with all relevant export laws and regulations, including but not limited to the U.S. Export Administration Regulations (collectively, “Export Controls”). Without limiting the generality of the foregoing, Recipient expressly agrees that it shall not, and shall cause its representatives not to, export, directly or indirectly, re-export, direct, or transfer the software, programs, documentation, materials, specifications or any direct product thereof to any destination, person or entity restricted or prohibited by Export Controls. In the event that Recipient provides the software, programs, documentation, materials, specifications, or any direct product thereof to a third party located in any destination outside the country of delivery by ActivIdentity, Recipient shall ensure that it enters into a written agreement with such third party that protects ActivIdentity’s rights and interests to the same extent protected hereunder and specifies ActivIdentity as a third party beneficiary. Recipient agrees to provide a copy of such agreement to ActivIdentity at ActivIdentity’s request and to assist ActivIdentity, at Recipient’s expense, in enforcing ActivIdentity’s rights if ActivIdentity is not recognized as a third party beneficiary in the applicable jurisdiction.

**Disclaimer:** Unless provided otherwise in a valid License Agreement, this document is intended for informational purposes only. To the fullest extent permissible under applicable law, ActivIdentity expressly disclaims all warranties of any kind, express or implied, including warranties of merchantability, fitness for a particular purpose, satisfactory quality, accuracy, title, non-infringement, and any warranties that may arise out of course of performance, course of dealing, or usage of trade. Unless provided otherwise in a valid License Agreement, the information contained in this document has not been submitted to any formal testing and is distributed “AS IS” and usage of this information or the implementation of any of these techniques is the recipient’s responsibility and depends on the recipient’s ability to evaluate and integrate them into an operational environment. While each item may have been reviewed by ActivIdentity for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Attempts to adapt these techniques to any environment are done so at the recipient’s own risk. Information in this document was developed in conjunction with the use of the hardware, software, and networking arrangements specified and is thus limited in application to those specific hardware and software products and levels. This document may contain information about product functionality not available in your product release. This document is subject to change without notice and does not represent a commitment on the part of ActivIdentity.



# ActivClient CAC 64-bit edition

## User Guide

### Table of Contents

|   |           |
|---|-----------|
| <b>CHAPTER 1: INTRODUCTION</b>                                    | <b>9</b>  |
| <b>About this Guide</b>   | <b>9</b>  |
| Audience  | 9         |
| Assumed knowledge and prerequisites                               | 9         |
| Other documents   | 9         |
| <b>CHAPTER 2: GETTING STARTED</b>                                 | <b>10</b> |
| <b>Your first steps with ActivClient</b>                          | <b>10</b> |
| <b>Working with the User Console</b>                              | <b>12</b> |
| What can you do with the User Console?                            | 12        |
| To access the User Console  | 13        |
| <b>CHAPTER 3: MANAGING SMART CARDS</b>                            | <b>15</b> |
| <b>Initializing a smart card with the PIN Initialization Tool</b> | <b>15</b> |
| Supported smart cards   | 15        |
| Blank smart cards   | 15        |
| Standalone smart cards  | 16        |
| To access the PIN Initialization Tool                             | 16        |
| To initialize your smart card using the PIN Initialization Tool   | 17        |
| <b>Resetting a smart card</b>                                     | <b>18</b> |
| To reset your smart card  | 18        |
| <b>Changing a smart card PIN</b>                                  | <b>19</b> |
| To access the PIN Change Tool                                     | 19        |
| <b>Unlocking a smart card PIN</b>                                 | <b>21</b> |
| Viewing your unlock code  | 21        |
| To view your unlock code  | 21        |
| Unlocking your smart card PIN                                     | 22        |
| To unlock a smart card initialized by the administrator           | 22        |
| To unlock a smart card initialized with ActivClient               | 24        |
| To access the Unlock Smart Card PIN dialog box                    | 25        |
| <b>Viewing smart card information</b>                             | <b>25</b> |
| To access the Smart Card Info window                              | 25        |
| <b>CHAPTER 4: MANAGING DIGITAL CERTIFICATES</b>                   | <b>27</b> |
| <b>Downloading a certificate with Microsoft Internet Explorer</b> | <b>27</b> |
| To download a certificate with Microsoft Internet Explorer        | 27        |
| <b>Downloading a certificate with Firefox</b>                     | <b>28</b> |
| To download a certificate with Firefox                            | 29        |
| <b>Managing user and CA certificates</b>                          | <b>29</b> |
| Viewing your certificate  | 29        |
| To view a certificate   | 30        |
| Importing a user certificate                                      | 31        |
| To import a user certificate                                      | 31        |
| Importing a CA certificate  | 31        |
| To import a CA certificate  | 31        |
| Exporting a certificate   | 32        |
| To export a certificate   | 32        |

|  |               |
|--|---------------|
| Deleting a certificate . . . . .   | 33            |
| To delete a certificate from your smart card . . . . .                       | 34            |
| <b>Selecting certificates for Windows PKI login . . . . .</b>                | <b>35</b>     |
| To select a certificate for Windows PKI login . . . . .                      | 35            |
| To unselect a login certificate . . . . .                                    | 36            |
| To temporarily disable the default certificate automatic selection . . . . . | 37            |
| To enable this feature again . . . . .                                       | 37            |
| <b>Making certificates available to Windows . . . . .</b>                    | <b>37</b>     |
| To make certificates available to Windows . . . . .                          | 38            |
| <br><b>CHAPTER 5: MANAGING REMOTE ACCESS AND OTP . . . . .</b>               | <br><b>39</b> |
| <b>Synchronizing smart cards . . . . .</b>                                   | <b>39</b>     |
| To synchronize your smart card . . . . .                                     | 39            |
| <b>Configuring a remote access user name . . . . .</b>                       | <b>40</b>     |
| To configure your remote access user name . . . . .                          | 41            |
| <br><b>CHAPTER 6: USING AND MANAGING ACTIVCLIENT . . . . .</b>               | <br><b>43</b> |
| <b>Viewing ActivClient system information . . . . .</b>                      | <b>43</b>     |
| To view ActivClient system information . . . . .                             | 43            |
| <b>Troubleshooting ActivClient . . . . .</b>                                 | <b>44</b>     |
| To use the Troubleshooting Wizard . . . . .                                  | 44            |
| To access the Troubleshooting Wizard . . . . .                               | 45            |
| <b>Performing advanced diagnostics . . . . .</b>                             | <b>46</b>     |
| To use the Advanced Diagnostics wizard . . . . .                             | 47            |
| To generate a report . . . . .   | 47            |
| To display your report . . . . .   | 47            |
| To save your report . . . . .  | 47            |
| To copy part of your report . . . . .  | 48            |
| To email your report . . . . .   | 48            |
| To print your report . . . . .   | 48            |
| To access the Advanced Diagnostics wizard . . . . .                          | 48            |
| <b>Using the Forget state for all cards option . . . . .</b>                 | <b>49</b>     |
| To forget state for all cards . . . . .                                      | 49            |
| <b>Using log system activity . . . . .</b>                                   | <b>50</b>     |
| To turn on/off log system activity . . . . .                                 | 50            |
| To activate log files from ActivClient User Console . . . . .                | 50            |
| <b>Configuring ActivClient . . . . .</b>                                     | <b>51</b>     |
| To access the Advanced Configuration Manager . . . . .                       | 52            |
| <b>Auto-Update service . . . . .</b>   | <b>53</b>     |
| <br><b>CHAPTER 7: USING DIGITAL CERTIFICATES . . . . .</b>                   | <br><b>54</b> |
| <b>Logging on to Windows with a certificate . . . . .</b>                    | <b>54</b>     |
| To log on to Windows with a certificate . . . . .                            | 54            |
| <b>Locking your workstation on smart card removal . . . . .</b>              | <b>55</b>     |
| To lock your workstation . . . . .   | 56            |
| Prerequisites . . . . .  | 56            |
| <b>Using Windows Dial-Up/VPN for remote access . . . . .</b>                 | <b>56</b>     |
| To use Windows Dial-Up/VPN for remote access . . . . .                       | 56            |

|  |           |
|--|-----------|
| <b>Using a non-Microsoft VPN for remote access</b>   | <b>57</b> |
| To use a non-Microsoft VPN for remote access   | 57        |
| <b>Accessing a secure Web site</b>   | <b>58</b> |
| Access a secure Web site with Internet Explorer  | 58        |
| To access a secure Web site with Internet Explorer   | 58        |
| Access a secure Web site with Netscape, Mozilla and Firefox  | 59        |
| To access a secure Web site with Netscape, Mozilla or Firefox  | 59        |
| <b>Sending/Receiving signed and encrypted email messages with Microsoft Outlook</b>  | <b>60</b> |
| Sending/Receiving signed email messages  | 60        |
| To send signed email messages  | 60        |
| To receive signed email messages   | 62        |
| Sending/Receiving encrypted email messages   | 63        |
| To send encrypted email messages   | 63        |
| To receive encrypted email messages  | 63        |
| <b>Sending/Receiving signed/encrypted mails with Netscape or Thunderbird</b>   | <b>64</b> |
| Sending/Receiving signed email messages  | 64        |
| To send signed email messages  | 64        |
| To receive signed email messages   | 65        |
| Sending/Receiving encrypted email messages   | 65        |
| To send encrypted email messages   | 65        |
| To receive encrypted email messages  | 66        |
| <b>Encrypting/Decrypting files with EFS</b>  | <b>67</b> |
| Configuring your workstation for EFS   | 67        |
| To configure your workstation for EFS with your smart card encryption certificate  | 67        |
| To configure your workstation for EFS and generate a smart card encryption certificate   | 68        |
| Encrypting/Decrypting files or folders with EFS  | 69        |
| To encrypt a file or folder with EFS   | 69        |
| To decrypt a file or folder with EFS   | 69        |
| Updating EFS Certificate and re-encrypting files   | 70        |
| To re-encrypt files and folders with a new EFS certificate   | 70        |
| To re-encrypt files and folders with an EFS certificate already on your smart card   | 71        |
| Recovering encrypted files   | 72        |
| To recover encrypted files   | 72        |
| <b>CHAPTER 8: USING REMOTE ACCESS/OTP</b>  | <b>74</b> |
| <b>Getting a one-time password automatically</b>   | <b>74</b> |
| To get a one-time password automatically   | 74        |
| <b>Getting a one-time password manually</b>  | <b>75</b> |
| To get a One-time password manually  | 75        |
| <b>CHAPTER 9: VIEWING PERSONAL INFORMATION</b>   | <b>77</b> |
| <b>About Personal Information</b>  | <b>77</b> |
| To access "My Personal Info" on CAC and PIV cards  | 77        |
| <b>CHAPTER 10: USING ACTIVCLIENT WITH TERMINAL SERVICES</b>  | <b>79</b> |
| <b>Logging on to a Citrix session</b>  | <b>79</b> |
| To log on using a Citrix product   | 79        |
| To open a Citrix session-examples  | 80        |
| To log on to a Citrix session in a "Smart Card with Pass-through" authentication mode using Citrix ICA Client Program Neighborhood | 80        |

|  |               |
|--|---------------|
| To log on to a Citrix session in “Smart Card with Pass-through” authentication mode using Citrix ICA Client Program Neighborhood Agent ..... | 81            |
| To log on to a Citrix session in “Smart Card with Pass-through” authentication mode using Citrix Web Interface .....                         | 81            |
| <b>Using a smart card inside a Citrix session .....</b>  | <b>82</b>     |
| To use your smart card inside a Citrix session .....   | 83            |
| <b>Logging on to a Remote Desktop session .....</b>  | <b>83</b>     |
| To log on to a Remote Desktop session .....  | 84            |
| <b>Using a smart card in a Remote Desktop session .....</b>  | <b>84</b>     |
| To use your smart card in a Remote Desktop session .....   | 85            |
| <b>Locking a Remote Desktop session .....</b>  | <b>85</b>     |
| To lock a Remote Desktop session .....   | 86            |
| <br><b>TERMS AND ACRONYMS .....</b>  | <br><b>87</b> |
| <b>Terminology .....</b>   | <b>87</b>     |
| <b>Acronyms .....</b>  | <b>88</b>     |



# Chapter 1: Introduction

## About this Guide

You are going to learn about the following topics:

- Your first steps with ActivClient
- Smart cards
- Digital certificates
- Remote Access and one-time passwords
- ActivClient usage and management
- Personal Information
- ActivClient and Terminal Services

## Audience

- Network or system administrators
- IT support staff
- End users

## Assumed knowledge and prerequisites

This document assumes the audience has a good computer knowledge and some understanding of Public Key Infrastructure.

## Other documents

This Guide is part of ActivClient set of documents including:

- ActivClient CAC User Guide (this document)
- ActivClient CAC Installation Guide
- ActivClient CAC Overview
- ActivClient CAC Quick Start

# Chapter 2: Getting started

In this section, you will learn about the following topics:

- ["Your first steps with ActivClient" on page 10.](#)
- ["Working with the User Console" on page 12.](#)

## Your first steps with ActivClient

Depending on your organization, 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).

Here is a list of actions to be taken according to your smart card status:

Table 2-1: Getting started according to your smart card status

| Smart card status  | Action  |
|--|---|
| If you have a blank smart card (no PIN).   | <p>Your administrator has given you a blank smart card. You need to initialize the card before you can use it.</p> <ol style="list-style-type: none"> <li>1. Log on to your workstation using the same user name and password that you used before installing ActivClient.</li> <li>2. Initialize your new smart card and create your PIN. For more information, see <a href="#">"Initializing a smart card with the PIN Initialization Tool" on page 15</a>.</li> <li>3. Load credentials on your smart card as described in <a href="#">"Managing Digital Certificates" on page 27</a>.</li> <li>4. Use your card to log on to your workstation (if your administrator instructs you to do so), to sign email, to access secure Web sites, etc.</li> <li>5. At any time, you may access the ActivClient User Console to configure ActivClient, your smart card, or your credentials. For more information, see <a href="#">"Working with the User Console" on page 12</a>.</li> </ol> |
| If your smart card is personalized with a PIN but is not configured for Windows PKI logon. | <p>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.</p> <ol style="list-style-type: none"> <li>1. Log on to your workstation using the same user name and password you used before installing ActivClient.</li> <li>2. Use your card to sign email, to access secure Web sites, etc.</li> <li>3. At any time, you may access the ActivClient User Console to configure ActivClient, your smart card, or your credentials. For more information, see <a href="#">"Working with the User Console" on page 12</a>.</li> </ol>   |
| If your smart card is personalized with a PIN and a Windows PKI logon digital certificate. | <p>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.</p> <ol style="list-style-type: none"> <li>1. Log on to your workstation using your smart card and your PIN. For more information, see <a href="#">"Logging on to Windows with a certificate" on page 54</a>.</li> <li>2. Use your card to sign email, to access secure Web sites, etc.</li> <li>3. At any time, you may access the ActivClient User Console to configure ActivClient, your smart card, or your credentials. For more information, see <a href="#">"Working with the User Console" on page 12</a>.</li> </ol>   |

## Working with the User Console

### What can you do with the User Console?

Here is a summary of the tasks you can do from ActivClient User Console:

| You can                          | Action  |
|----------------------------------|---|
| Manage your digital certificates | <ul style="list-style-type: none"><li>• Import a CA digital certificate, see <a href="#">"Managing user and CA certificates" on page 29.</a></li><li>• Import a User digital certificate, see <a href="#">"Managing user and CA certificates" on page 29.</a></li><li>• Export a digital certificate, see <a href="#">"Managing user and CA certificates" on page 29.</a></li><li>• View a digital certificate, see <a href="#">"Managing user and CA certificates" on page 29.</a></li><li>• Delete a digital certificate, see <a href="#">"Deleting a certificate" on page 33.</a></li><li>• Set as default, see <a href="#">"To select a certificate for Windows PKI login" on page 35.</a></li><li>• Make your certificates available to Windows, see <a href="#">"To make certificates available to Windows" on page 38.</a></li></ul> |
| Manage your one-time passwords   | <ul style="list-style-type: none"><li>• Generate a one-time password, see <a href="#">"Getting a one-time password automatically" on page 74.</a></li><li>• Re-synchronize a one-time password, see <a href="#">"Synchronizing smart cards" on page 39.</a></li><li>• Configure a user name for one-time password-based remote access, see <a href="#">"Configuring a remote access user name" on page 40.</a></li></ul>  |
| View your personal information   | Available for the US Department of Defense on Common Access Cards (CAC) or US Government Personal Identity Verification (PIV) cards only. See <a href="#">"About Personal Information" on page 77.</a>  |

| You can   | Action  |
|---|---|
| Manage your smart card  | <ul style="list-style-type: none"><li>• Change a PIN, "<a href="#">Changing a smart card PIN</a>" on page 19.</li><li>• View your smart card information, "<a href="#">Viewing smart card information</a>" on page 25.</li><li>• Unlock your smart card, "<a href="#">Unlocking a smart card PIN</a>" on page 21.</li><li>• Initialize your new smart card, "<a href="#">Initializing a smart card with the PIN Initialization Tool</a>" on page 15.</li><li>• Reset your smart card, "<a href="#">Resetting a smart card</a>" on page 18.</li><li>• View your unlock code, "<a href="#">Viewing your unlock code</a>" on page 21.</li><li>• Select a smart card reader, from the <b>Reader List</b> icon on the <b>Standard</b> toolbar.</li></ul> |
| Run ActivClient Tools to: <ul style="list-style-type: none"><li>• Troubleshoot</li><li>• Diagnose</li><li>• Configure advanced settings</li></ul> | <ul style="list-style-type: none"><li>• Run the <b>Troubleshooting</b> wizard. "<a href="#">Troubleshooting ActivClient</a>" on page 44.</li><li>• Run the <b>Advanced Diagnostics</b> Tool. "<a href="#">Performing advanced diagnostics</a>" on page 46.</li><li>• Go to the <b>Advanced Configuration Manager</b> window. "<a href="#">Troubleshooting ActivClient</a>" on page 44.</li></ul>  |


## To access the User Console

- From the ActivClient Agent icon located on the workstation's taskbar:

Double-click ActivClient Agent .

The ActivClient User Console is displayed.

–Or–

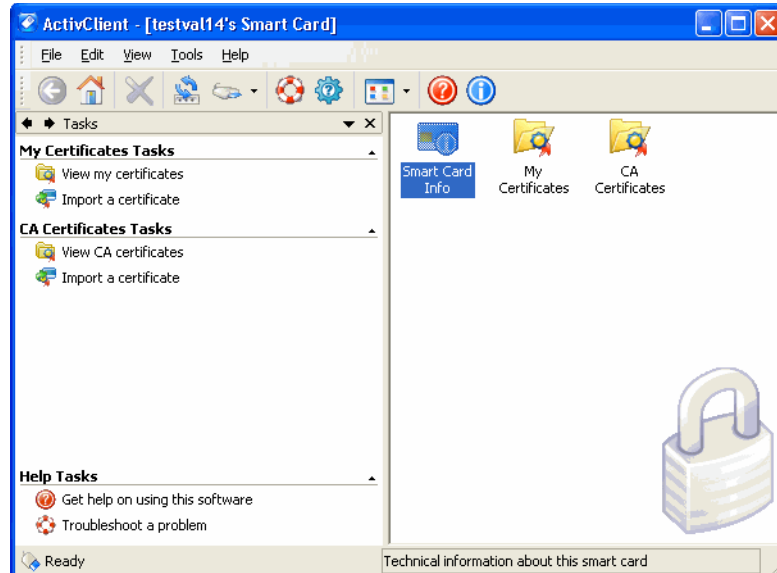
Right-click ActivClient Agent  and select **Open**.

The ActivClient User Console is displayed.

- From the 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, you can refer to *ActivClient CAC Overview*.

# Chapter 3: Managing smart cards

This section discusses the following topics:

- ["Initializing a smart card with the PIN Initialization Tool" on page 15.](#)
- ["Resetting a smart card" on page 18.](#)
- ["Changing a smart card PIN" on page 19.](#)
- ["Unlocking a smart card PIN" on page 21.](#)
- ["Viewing smart card information" on page 25.](#)

## Initializing 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.

But first, you need to check if your smart card belongs to the two types of supported smart cards.

## Supported smart cards

Blank and standalone smart cards are the two types of smart cards supported by the PIN Initialization Tool.

### Blank smart cards

Blank smart cards are smart cards with no applets uploaded. Once initialized by the PIN Initialization Tool, those smart cards are ready to use. No PIN unlock mechanism is available. If the PIN code is locked due to too many wrong PIN entries or if the PIN code is forgotten, the smart card can be run through the PIN Initialization Tool again and 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 smart cards with preloaded applets. Those type of smart cards have an identifier such as S1, S4, O4 or S5 engraved on the lower right of their back. At the end of PIN Initialization, an unlock code is displayed. Write it down in a secure place. An unlock code or a PIN code will be needed later if you want to re-initialize those smart cards and erase their content.


For the list of blank smart cards (ActivClient Standalone / Mini configuration) and standalone smart cards (ActivClient Standalone configuration), refer to *chapter 4 of ActivClient CAC Overview*.

**Important:** Trying repeatedly to initialize a smart card that is not in a supported configuration can make the smart card permanently unusable.

## To access the PIN Initialization Tool

You can access the PIN Initialization from different locations, depending if you have installed or not the User Console and ActivClient Agent.

- From ActivClient Agent icon located on the workstation's taskbar:

Right-click ActivClient Agent icon  and select PIN Initialization Tool.  
The PIN Initialization Tool wizard is displayed.

–Or–

- From ActivClient User Console:

1. Insert your smart card.
2. Go to the **Tools** menu and select **New Card**.  
The PIN Initialization Tool wizard is displayed.

–Or–

- From the Start menu:

Go to Programs, ActivIdentity, ActivClient and select PIN Initialization Tool.  
The PIN Initialization Tool wizard is displayed.



## To initialize your smart card using the PIN Initialization Tool

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

1. Start the PIN Initialization Tool. To learn how, see ["To access the PIN Initialization Tool" on page 16](#).
2. Follow the PIN Initialization wizard.
3. Enter your new PIN code, confirm it, and click **Next**.

ActivClient - PIN Initialization Tool

Enter the PIN code you want to use and click Next to start the initialization process.

PIN code:

Confirm:

Your new PIN must satisfy the following conditions:

- ☒ Must contain at least 4 characters
- ☒ Must not exceed 25 characters
- ☒ Must be correctly confirmed

< Back   Next >   Cancel

**Note:** Enter a PIN that is easy for you to remember, but difficult for others to guess! The PIN code must conform with the PIN rules displayed by the tool. All the rules must display a green check for the PIN Initialization Tool to let you move forward.

4. In the case of an already initialized standalone smart card (with an unlock code), you must enter a PIN or unlock code.  
When the initialization is complete, the Finish window is displayed.

5. In the case where an unlock code is displayed, write it down in a secure location and click **Finish** to close the window.

**Note:** 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.

## Resetting 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 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.

### To reset your smart card

1. Open 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 is selected, type your PIN in the box, and click <b>OK</b> .  |
| You do not know the smart card PIN and the smart card was initialized with ActivClient in standalone mode. | <ol style="list-style-type: none"><li>1. Select <b>Unlock Code</b>.</li><li>2. Type the unlock code that you saved after initialization, and click <b>OK</b>.</li></ol> For more information, see " <a href="#">Viewing your unlock code</a> " on page 21.  |
| You do not know the smart card PIN, and the smart card was initialized by your administrator.              | <ol style="list-style-type: none"><li>1. Select <b>Unlock Code</b>.</li><li>2. Call your IT administrator. You may be asked to give the challenge Code displayed in the <b>Challenge Code</b> box.</li><li>3. In the <b>Unlock Code</b> box, type the unlock code that the administrator gave you, and click <b>OK</b>.</li></ol> |

**Note:** The “Reset” and “Re-initialization” procedures can also be done using the PIN Initialization tool.

## Changing a smart card PIN

Changing your smart card PIN should be done regularly to ensure that you are the only person accessing your smart card.

### To access the PIN Change Tool

You can access the PIN Change tool by taking either one of the following actions:

- From ActivClient Agent icon's right-click menu:  
Select **PIN Change Tool**.  
The **PIN Change tool** wizard is displayed.
  - From ActivClient User Console:  
Select **Change PIN** from the **Tools** menu.  
The **PIN Change tool** wizard is displayed.
- Or–
- Select **Change PIN** from the **Standard** toolbar.  
The **PIN Change tool** wizard is displayed.
- From the Start menu:  
Go to Programs, ActivIdentity, ActivClient, and select **PIN Change Tool**.  
The **PIN Change tool** wizard is displayed.

ActivClient - PIN Change Tool

Please type your current PIN and the new PIN you want to use

Enter your PIN:

Enter New PIN:

Confirm New PIN:

Your new PIN must satisfy the following conditions:

- ☒ Must contain at least 4 characters
- ☒ Must not exceed 25 characters
- ☒ Must be correctly confirmed

< Back   Next >   Cancel

All conditions (green marks) must be filled and green checked before you can proceed to the **Next** step.

**WARNING:** Attempting to enter too many wrong PIN's will lock your smart card! Make sure you view your unlock code and write it down in a secure place before you lock your smart card inadvertently.

## Unlocking a smart card PIN

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 use your smart card.

Make sure you know your unlock code! An unlock code helps you unlock your smart card whenever it is locked.

Unlocking your smart card is necessary to access all of the information stored on it.

## Viewing your unlock code

You are probably in one of the three following cases:

- If you initialized your smart card directly with ActivClient in standalone mode, you are also responsible for the unlock code. You need to view your unlock code in order to save it in a secure location. This unlock code helps you unlock the smart card if you lock it by entering multiple incorrect PINs.
- If you received an already initialized smart card, your administrator is responsible for your unlock code.
- If your smart card was initialized with ActivClient in a Standalone / Mini mode (see "[Supported smart cards](#)" on page 15), the smart card cannot be unlocked. However, you can re-initialize your smart card with the PIN Initialization Tool.

## To view your unlock code

### Prerequisites

- ActivClient User Console is open.
  - Your smart card has been initialized with ActivClient in standalone mode.
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.
  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 check the **Never display the Unlock Code again** check box, the **Display Smart Card Unlock Code** dialog box will never display again. Consequently, your Unlock Code will never display again!

## Unlocking your smart card PIN

The information displayed in the **Unlock your smart card** dialog box is based on your configuration.

### To unlock a smart card initialized by the administrator

When ActivClient detects that a smart card initialized by the administrator is locked, the **Unlock Smart Card PIN** dialog box is displayed. You can then retrieve a Challenge code.

**ActivClient - Unlock Smart Card PIN**

**Your smart card PIN is locked**  
This happens when a series of incorrect PIN attempts are made.  
You cannot use your smart card until it is unlocked

**Challenge Code**  
Please contact technical support and provide the challenge code below:  
Challenge Code:

**Unlock Code**  
Please enter the unlock code given to you by technical support below.  
Unlock Code:

**New PIN**  
Please choose new smart card PIN and enter it below.  
New PIN:       Verify:

Your new PIN must satisfy the following conditions:

- ☐ Must contain at least 6 characters
- ☒ Must not exceed 25 characters
- ☐ Must not be too simple (e. g. 1234)
- ☒ Must be correctly confirmed

1. Call your IT administrator and give the challenge code displayed in the **Challenge Code** box.
2. In the **Unlock Code** box, type the unlock code that the administrator gives you.
3. In the **New PIN** box, type the new PIN.
4. In the **Verify** box, retype the new PIN, and click **OK**.

## To unlock a smart card initialized with ActivClient

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

**ActivClient - Unlock Smart Card PIN**

**Your smart card PIN is locked**  
This happens when a series of incorrect PIN attempts are made.  
You cannot use your smart card until it is unlocked

Unlock Code  
Please enter the unlock code given to you by technical support below.  
Unlock Code: 956A-EE5B-E555-4D28

New PIN  
Please choose new smart card PIN and enter it below.  
New PIN: xxxxxx Verify: xxxxxx

Your new PIN must satisfy the following conditions:

- ☒ Must contain at least 4 characters
- ☒ Must not exceed 25 characters
- ☒ Must be correctly confirmed

OK Cancel

1. Retrieve the unlock code that you saved when you initialized your smart card.
2. In the **Unlock Code** box, type the unlock code that you retrieved.
3. In the **New PIN** box, type the new PIN.
4. In the **Verify** box, retype the new PIN, and click **OK**.

**Note:** ActivClient can be configured so that the unlock screen is displayed as soon as a locked smart card is inserted in the system.



## To access the Unlock Smart Card PIN dialog box

- From ActivClient User Console:  
Select **Unlock Card** from the **Tools** menu.  
The **Unlock Smart Card** dialog box is displayed.
- Insert a locked smart card into your smart card reader.  
The **Unlock Smart Card** dialog box is displayed.

## Viewing smart card information

ActivClient User Console provides you with technical information about your smart card such as:

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

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

## To access the Smart Card Info window

You can use different ways to access smart card information from ActivClient User Console:

- From the User Console tasks pane:
  1. Insert your smart card.
  2. Click on **Smart Card Info**.  
The **Smart Card Info** window is displayed on the right pane.

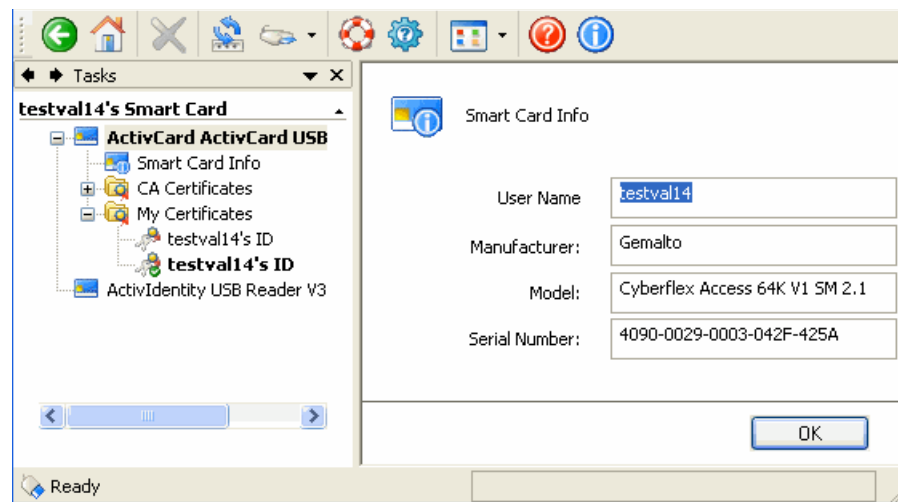
–Or–

- From the User Console right pane:
  1. Insert your smart card.
  2. Double-click the **Smart Card Info** icon.  
The **Smart Card Info** window is displayed on the right pane.

–Or–

- From the User Console right pane:
  1. Insert your smart card.
  2. Right-click the **Smart Card Info** icon.
  3. Select **View smart card info**.

The **Smart Card Info** window is displayed on the right pane.



**Note:** Your user name is supplied by ActivClient from either one of the following items:

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

# Chapter 4: Managing Digital Certificates

This section discusses the following topics:

- ["Downloading a certificate with Microsoft Internet Explorer" on page 27.](#)
- ["Downloading a certificate with Firefox" on page 28.](#)
- ["Managing user and CA certificates" on page 29.](#)
- ["Selecting certificates for Windows PKI login" on page 35.](#)
- ["Making certificates available to Windows" on page 37.](#)

**Note:** Some of the operations described in this chapter (such as importing/deleting a certificate from your smart card) are only possible if the policy of your smart card permits it.

## Downloading 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.

### To download a certificate with Microsoft Internet Explorer

#### Prerequisites

- Microsoft CAPI support option has been 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 Certificate Authority
  - Windows 2003 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. From within Internet Explorer, 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 CAs 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. 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 has been 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.

## Downloading 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.

The following instructions also apply to Netscape and Mozilla.

## To download a certificate with Firefox

### Prerequisites

- A supported version of Firefox, Mozilla or Netscape is installed on your computer.
  - Firefox, Mozilla and Netscape support has been installed during setup. The ActivClient PKCS#11 library has been registered to Firefox, Mozilla or Netscape. Refer to *ActivClient Installation Guide* for details.
  - Your administrator provided you with a Web site URL to access your organization's Certificate Authority.
1. Insert your smart card (chip side up and chip first) into the smart card reader.
  2. Use your Firefox browser to go to your Certificate Authority's Web site.
  3. Follow instructions for certificate request.
  4. Enter your PIN when requested.
  5. Verify that the key pair and associated certificate have been loaded on your smart card using the ActivClient User Console (optional).

## Managing user and CA certificates

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

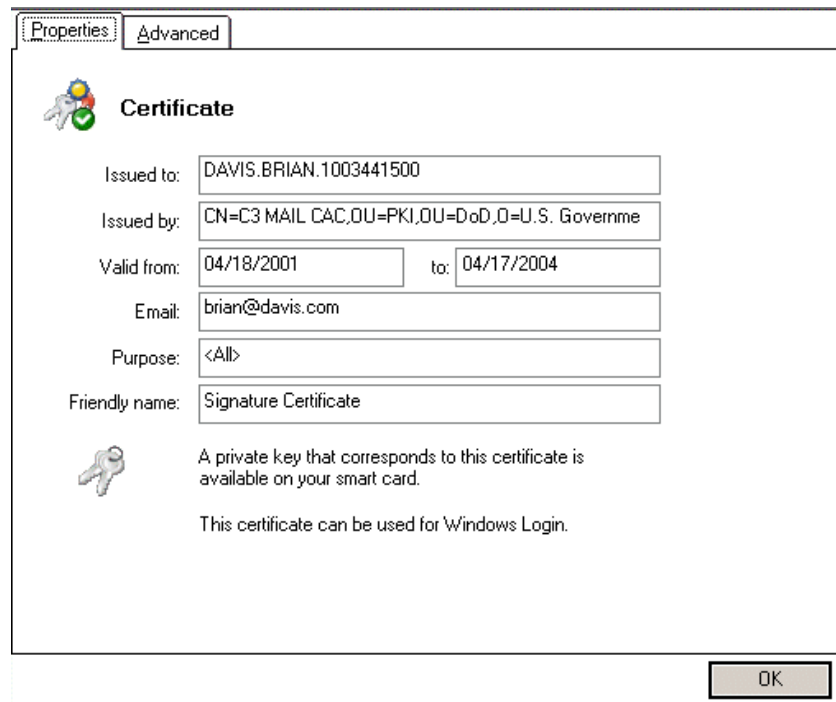
### Viewing your certificate

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

## To view a certificate

1. Open ActivClient User Console.
2. Do one of the following:
  - From the tasks pane under **My Certificate Tasks**, click **View My Certificates**.  
An icon for each of your certificates is displayed.
  - 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.



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

**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.

## Importing 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.

### To import a user certificate

#### 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 ActivClient User Console.
2. From the **File** menu, click **Import**.
3. In the File Browser dialog box, select the location and the file name for the certificate that you want to import, and click **Open**.

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

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

## Importing 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.

### To import a CA certificate

#### 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.
1. Open ActivClient User Console.
  2. From the **File** menu, click **Import**.
  3. In the **File Browser** dialog box, select the location and the file name for the certificate that you want to import, and click **OK**.

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

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

## Exporting a certificate

Use the following procedure to send your certificate or CA certificate to someone by exporting it from your smart card into a file.

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

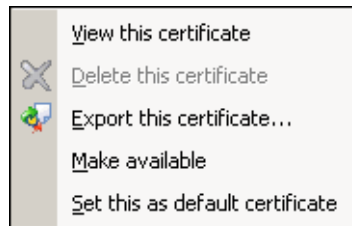
## To export a certificate

### Prerequisites

- ActivClient User Console is installed on your workstation.
  - A certificate is available on your smart card.
1. Open ActivClient User Console.
  2. Do either one of the following:
    - Select **View My Certificates** or **View CA Certificates** from the **Tasks** pane related section.



- An icon representing each of your certificates or CA certificates is displayed.
- 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. Right-click the certificate you want to export.  
A shortcut menu is displayed.



4. Select **Export this certificate**.  
The **Export Certificate** dialog box is displayed.
5. Select the location and the file name for the exported certificate, and click **Save**.  
A confirmation message is displayed.
6. Click **OK**.

## Deleting 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).

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

## To delete a certificate from your smart card

### Prerequisites

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

1. Open ActivClient User Console.
2. Do either one of the following:
  - Select **View My Certificates** or **View CA Certificates** from the **Tasks** pane related section.  
An icon representing each of your certificates is displayed.
  - Or–
  - 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. Do either one of the following:
  - Right-click the certificate that you want to delete.  
A shortcut menu is displayed.
  - Select **Delete this certificate** from the certificate's right-click menu.
  - Or–
  - Select one or several certificates in the right pane.
  - Select **Delete these Certificates** from **My Certificate Tasks** section in the left pane.
  - Or–
  - Select one or several certificates in the right pane.
  - 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.

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

## Selecting certificates for Windows PKI login

If your smart card contains two or more certificates configured for Windows PKI login (i.e. 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, there is no need to select any certificate to use with ActivClient User Console. Windows Vista lets you select which PKI login certificate to use at the time you log on.

### To select a certificate for Windows PKI login


#### Prerequisite

You have a Windows login compatible certificate available on your smart card. For more information, see ["Downloading a certificate with Microsoft Internet Explorer" on page 27](#).

1. Open the ActivClient User Console.
2. Take one of the following actions to display your certificates:
  - Select **View My Certificates** from the **Tasks** pane related section. An icon representing each of your certificates is displayed.
  - Double-click the **My Certificates** icon from the right pane. An icon representing each of your certificates is displayed.
  - Click on **View My Certificates** from the **My Certificate Tasks** section in the **Tasks** pane. An icon for each of your certificate is displayed.
3. Select the certificate you want to use for Windows PKI login.

4. Select **Set this as default certificate** from:

- the certificate right-click menu
- the **My Certificate Tasks** section in the **Tasks** pane.

The certificate icon is updated with a green check mark .

**Note:** If you do not need to set a default logon certificate, then clear the check mark in front of **Set this as default certificate**.


## To unselect a login certificate

### Prerequisites

One of your certificates has been set as default.

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

1. Open ActivClient User Console.
2. Take one of the following actions to display your certificates:
  - Click **View My Certificates** from the **My Certificate Tasks** section in the **Tasks** pane.  
An icon for each of your certificate is displayed.
  - Double-click the **My Certificates** icon located in the right pane.  
An icon for each of your certificate is displayed.
  - Click on **View My Certificates** from the **My Certificate Tasks** section in the **Tasks** pane.  
An icon for each of your certificate is displayed.
3. Right-click the certificate set as default (easily recognized 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 .

## To temporarily disable the default certificate automatic selection

If your smart card contains several certificates, and if one of them is configured for the Windows PKI login, ActivClient automatically selects this certificate for the Windows PKI login operation (if several such certificates are present, ActivClient will automatically select the first one). However, you may want to temporarily disable this automatic selection.

Select **Temporarily disable the default certificate automatic selection** from the **My Certificate Tasks** section in the **Tasks** pane of the User Console. This implies that Windows PKI login and workstation PKI unlock are no longer possible except on Windows Vista. This selection will remain active until next time you remove your smart card.

## To enable this feature again

Select **Enable the default certificate automatic selection** from the **My Certificate Tasks** section in the **Tasks** pane of the User Console.

## Making 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 login).

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.

**Note:** 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, refer to the ActivClient *Customization and Deployment Guide*.

## To make certificates available to Windows

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

1. Open ActivClient User Console.
2. Go to **Advanced** from the **Tools** menu, and select **Make Certificates Available to Windows**.

–Or–

Select **Make available** from your certificate right-click menu.

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

# Chapter 5: Managing Remote Access and OTP

This section discusses the following topics:

- ["Synchronizing smart cards" on page 39.](#)
- ["Configuring a remote access user name" on page 40.](#)

## Synchronizing smart cards

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.

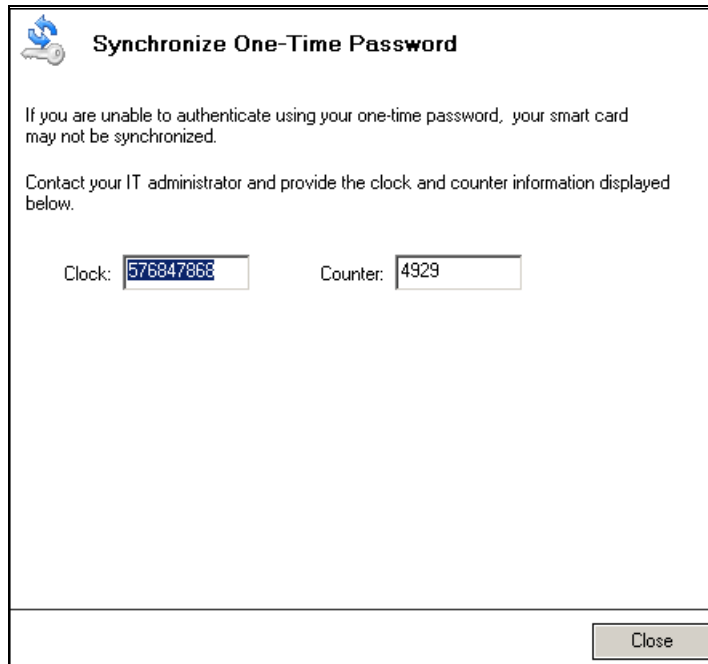
### To synchronize your smart card

#### Prerequisites

- Your smart card is initialized to use one-time passwords.
- One-Time Password Services option has been installed during setup.

1. Open ActivClient User Console.
2. Take one of the following actions to select a server to authenticate to:
  - From the **Tasks** pane, under **One-Time Password Tasks**, click **View one-time password**.  
An icon for each authentication server is displayed (usually only one server is available, hence only one icon is displayed) in the right pane.
  - Or–
  - 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. Take either one of the following action to start the synchronization:
  - From the right-pane, right-click the **One-Time Password** icon and select **Synchronize one-time password**.

- Or–
- 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.



**Synchronize One-Time Password**

If you are unable to authenticate using your one-time password, your smart card may not be synchronized.  
Contact your IT administrator and provide the clock and counter information displayed below.

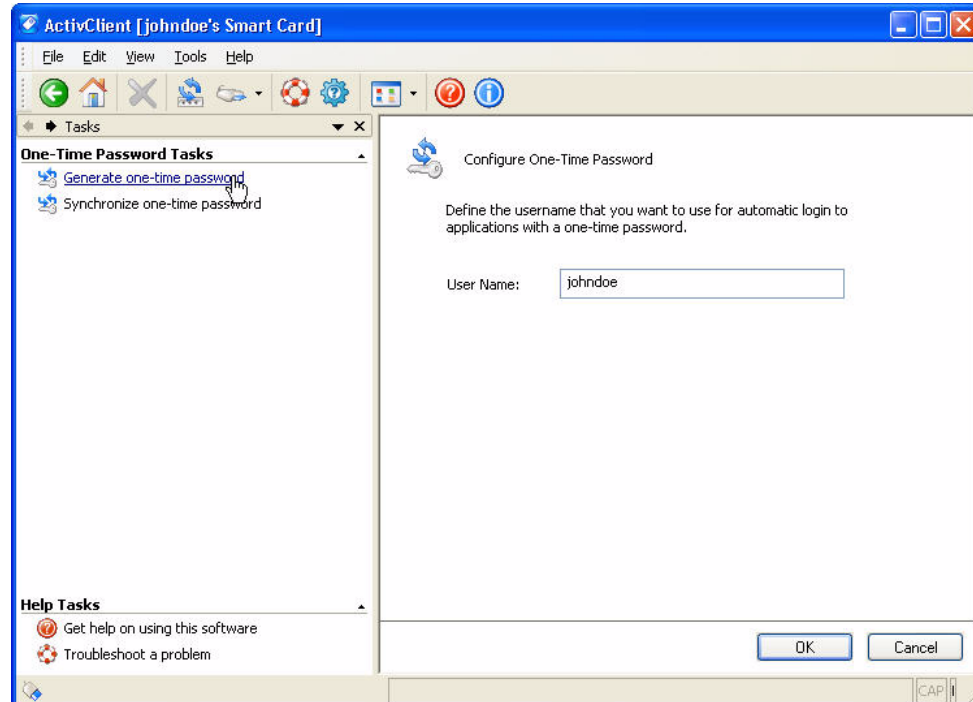
Clock:  Counter:

Close

## Configuring a 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.





## To configure your remote access user name

### Prerequisites

- Your smart card is initialized to use one-time passwords.
- The One-time Passwords Services option has been installed during setup.

1. Open ActivClient User Console.
2. Take one of the following actions:
  - From the **Tasks** pane, under **One-Time Password Tasks**, click **View one-time password**.  
An icon for each authentication server is displayed (usually only one server is available, hence only one icon is displayed) in the right pane.
  - Or–
  - From the right pane, double-click the **One-Time Passwords** 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. Take one the following actions to configure your remote access user name:
  - Right-click the server and select **Configure one-time password**.  
The **Configure One-Time Password** dialog box is displayed.
  - Or–
  - 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** box and click **OK**.  
Your remote access user name is configured.

# Chapter 6: Using and managing ActivClient

This section discusses the following topics:

- ["Viewing ActivClient system information" on page 43.](#)
- ["Troubleshooting ActivClient" on page 44.](#)
- ["Performing advanced diagnostics" on page 46.](#)
- ["Using the Forget state for all cards option" on page 49.](#)
- ["Using log system activity" on page 50.](#)
- ["Configuring ActivClient" on page 51.](#)
- ["Auto-Update service" on page 53](#)

## Viewing 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 on the **Credits** button)

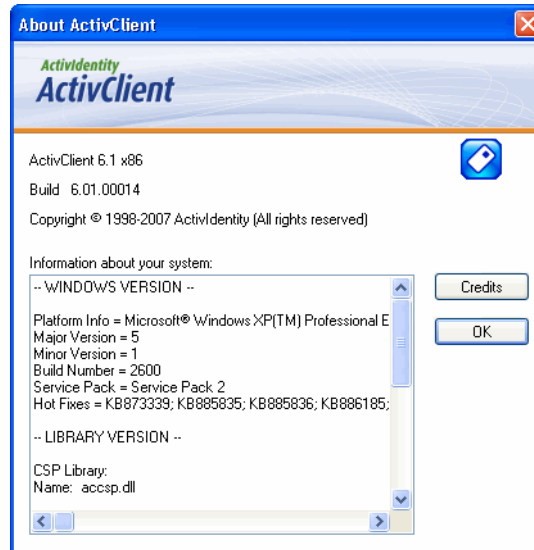
## To view ActivClient system information

- From ActivClient User Console:  
Select **About ActivClient** from the **Help** menu.  
The About ActivClient window is displayed.

–Or–

- From ActivClient Agent icon's right-click menu:

Select **About** from the ActivClient Agent icon's right-click menu.  
The About ActivClient window is displayed.



## Troubleshooting ActivClient

The Troubleshooting Wizard:

- Helps 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!

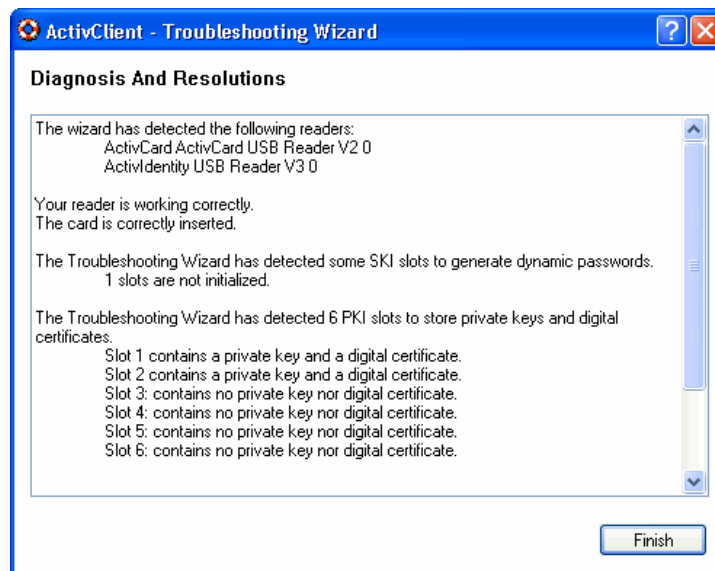
## To use the Troubleshooting Wizard

1. Click **Next** on the **Welcome** screen.
2. Read instructions to proceed.
3. Enter your PIN and click **Next**.

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

- Test encrypt and decrypt.

- Digital signature.
  - Web authentication.
4. If problems are detected, the **Problems found** page is displayed. Click **Next**.
  5. Follow the instructions displayed in the **Diagnosis and Resolutions** page and click **Finish**.



## To access the Troubleshooting Wizard

- From the ActivClient User Console **Standard** toolbar:  
Select **Run Troubleshoot Wizard**.  
The Troubleshooting wizard is displayed.
- Or-
- From the ActivClient User Console **Help** menu:  
Select **Troubleshoot**.  
The Troubleshooting wizard is displayed.
- Or-
- From the ActivClient User Console **Help Tasks** section:

Select **Troubleshoot a problem**.

The Troubleshooting wizard is displayed.

–Or–

- From the Start menu:  
Go to: Programs, ActivIdentity, ActivClient and select Troubleshooting.  
The Troubleshooting wizard is displayed.

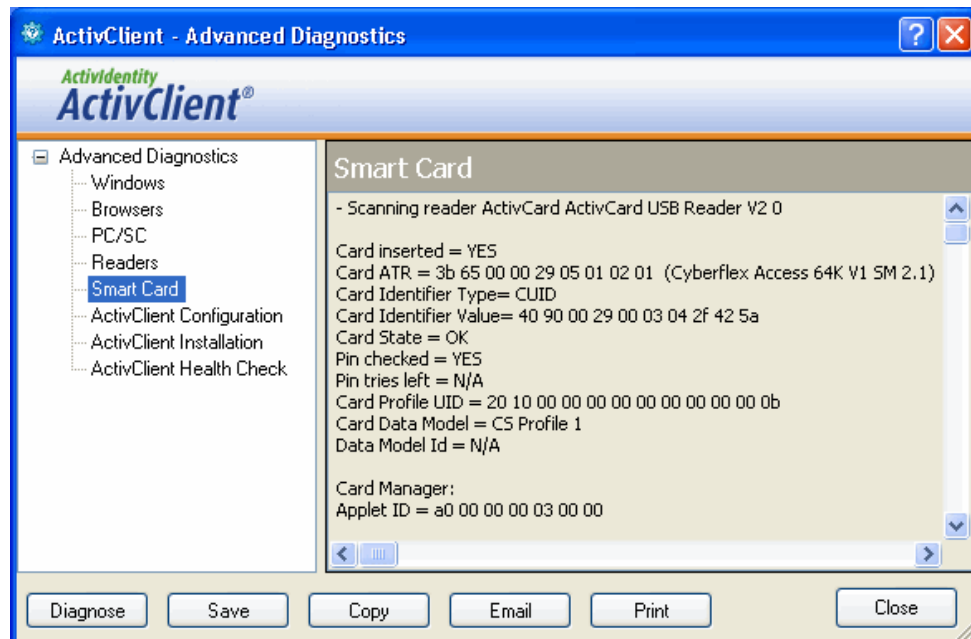
## Performing advanced diagnostics

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.

The generated report is displayed in eight different views which you can access by clicking on corresponding tabs:

- Windows
- Browsers
- PC/SC
- Readers
- Smart Card
- Configuration
- Installation
- Health Check



## To use the Advanced Diagnostics wizard

### To generate a report

1. Make sure you inserted a smart card.
2. Click on the **Diagnose** button.

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

### To display your report

Click on one of the eight views you wish to display.

### To save your report

Click on the **Save** button.

All your report's views are saved in one single log file.

## To copy part of your report

Select a view and click **Copy**.

The content of the view you selected is copied and can now be pasted to the location of your choice.

## To email your report

Click on the **Email** button.

Your report is saved in one single log file while your email programs opens. The log file is attached to the new mail message. You can finish writing your mail and send it to support.

## To print your report

Click on the **Print** button.

Your entire report including all eight views is automatically sent to your printer.

**Important:** Printing your report may imply printing hundreds of pages at the same time. If you want to print part of your report, save it as a log file first and select only the part you wish to print!

**Note:** Your administrator may have pre-configured the email address to send the report to. This setting, along with other ActivClient configuration options, is available in the **Advanced Configuration Manager**. For more information, you can refer to the section about product customization in the *ActivClient Customization and Deployment Guide* (included in the ActivClient Resource Kit).

## To access the Advanced Diagnostics wizard

To access the Advanced Diagnostics wizard, you can either take one of the following actions:

- From the ActivClient Agent's right-click menu:  
Select **Advanced Diagnostics**.



The Advanced Diagnostics wizard is displayed.

- From the ActivClient User Console **Standard** toolbar:  
Select **Advanced Diagnostics**.  
The Advanced Diagnostics wizard is displayed.

–Or–

- From the ActivClient User Console **Help** menu:  
Select **Diagnose**.  
The Advanced Diagnostics wizard is displayed.

–Or–

- From the Start menu:  
Go to: Programs, ActivIdentity and select Advanced Diagnostics.  
The Advanced Diagnostics wizard is displayed.

## Using 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 excludes any user 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, for trying to solve potential problems, your technical support may suggest to "tell" ActivClient to "forget" any smart card information it may have saved.

### To forget state for all cards

1. Open 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.

## Using log system activity

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

ActivClient allows you to configure log files without having necessarily administrator rights. You can configure log system activity from either:

- ActivClient User Console.
- Advanced Configuration Manager window (reserved for system administrators, refer to *ActivClient Resource Kit* for details on product customization).

**Note:** In order to guarantee privacy and security, no private key nor any confidential information are recorded in the ActivClient log files.

### To turn on/off log system activity

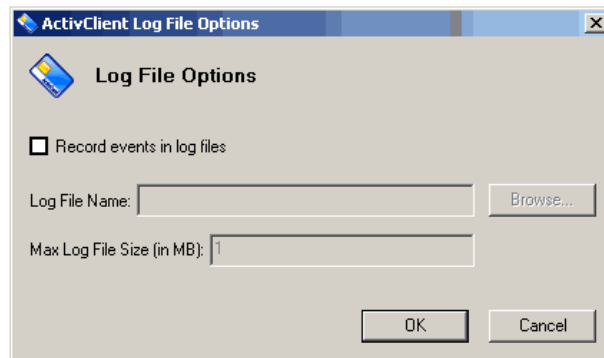
- Turn off logging system activity in normal use cases.
- Turn on logging system activity only when required by your system administrator or help desk.

**Important:** After log file creation, ActivIdentity recommends disabling log system activity!

### To activate log files from ActivClient User Console

The following procedure is a quick way to configure log system activity. You may want to access more options by going to the **Logging** section of the Advanced Configuration Manager.

1. Open ActivClient User Console.
1. Go to the **Tools** menu.
2. Select **Advanced, Log File Options**.  
The **Log File Options** dialog box is displayed.



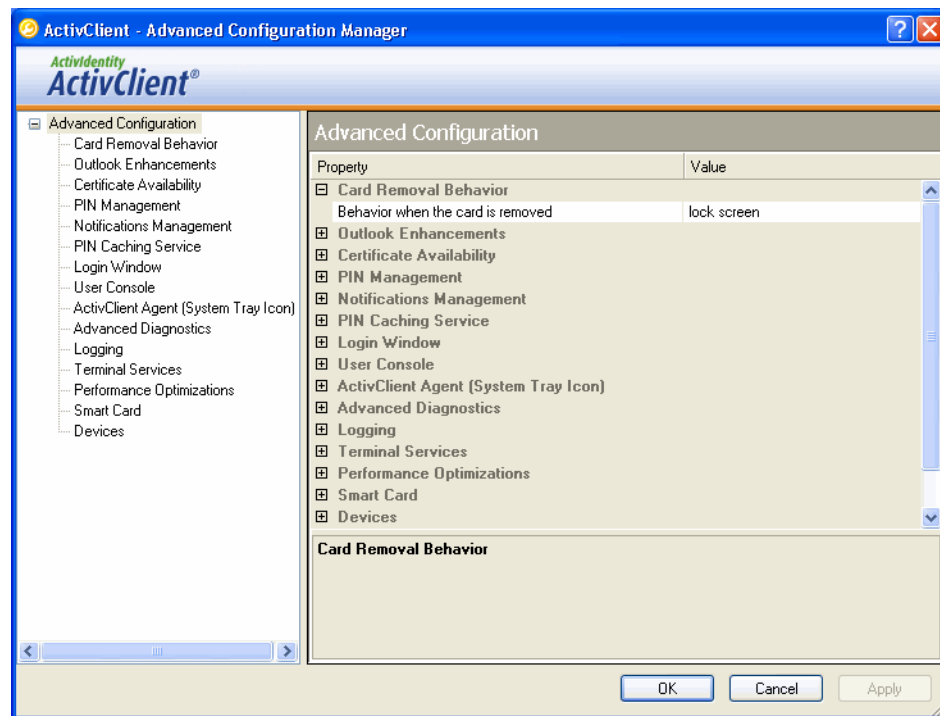
3. Check the **Record events in log files** option.
4. Type a name in the **Log File Name** box.
5. Type a size for the log file in the **Max Log File Size (in MB)** box.
6. Click **OK**.

## Configuring 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

Configuring ActivClient is done in the Advanced Configuration Manager. For more specific information, you can refer to the section on product customization in the *ActivClient Customization and Deployment Guide*.



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

## To access the Advanced Configuration Manager

You can access the Advanced Configuration Manager by taking one of the following actions:

- From the ActivClient Agent's right-click menu:  
Select **Advanced Configuration Manager**.  
The Advanced Configuration Manager window is displayed.

–Or–

- From the ActivClient User Console's **Tools** menu:  
Select **Advanced** then, **Configuration**.  
The Advanced Configuration Manager window is displayed.

–Or–

- From the Start Menu:  
Go to Programs, ActivIdentity and select Advanced Configuration Manager.  
The Advanced Configuration Manager window is displayed.

## Auto-Update service

This feature is enabled only if the **Auto-Update** feature is installed.  
ActivClient can be configured so that software updates are automatically  
downloaded and installed on your workstation.

# Chapter 7: Using Digital Certificates

This section discusses the following topics:

- ["Logging on to Windows with a certificate" on page 54.](#)
- ["Locking your workstation on smart card removal" on page 55.](#)
- ["Using Windows Dial-Up/VPN for remote access" on page 56.](#)
- ["Using a non-Microsoft VPN for remote access" on page 57.](#)
- ["Accessing a secure Web site" on page 58.](#)
- ["Sending/Receiving signed and encrypted email messages with Microsoft Outlook" on page 60.](#)
- ["Sending/Receiving signed/encrypted mails with Netscape or Thunderbird" on page 64.](#)
- ["Encrypting/Decrypting files with EFS" on page 67.](#)

## Logging on to Windows with a certificate

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

### To log on to Windows with a certificate

#### Prerequisites

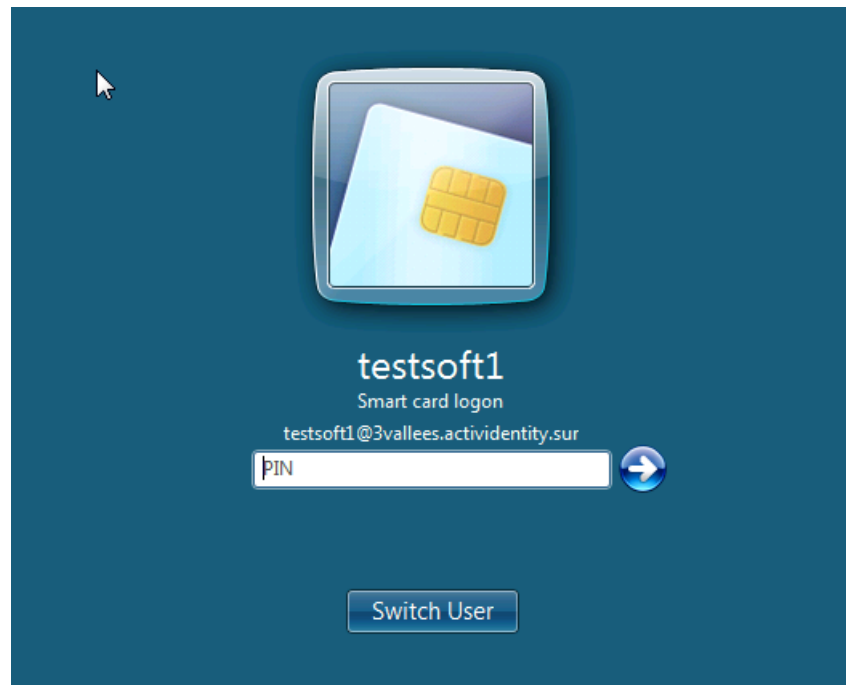
- Your smart card is configured with a certificate for Windows PKI login.
- Your workstation is configured for PKI login: the workstation must be attached to a domain, a root certificate must be available and a CRL server accessible.
- The Microsoft CAPI support option has been installed during setup.

#### 1. Start your workstation.

The Welcome to Windows screen is displayed.

#### 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.



3. For Windows Vista, select a certificate among the smart card certificates compatible with Windows login.
4. Enter your PIN in the **PIN** box and click **OK**.  
After a few moments, you are logged on and your desktop is displayed.

## Locking your workstation on smart card removal

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

**Note:** Your administrator may have changed the Card Removal Behavior property. For more information on customization, refer to the *ActivClient Customization and Deployment Guide*.

## To lock your workstation

### Prerequisites

- ActivClient is configured for “workstation locking on smart card removal” (default setting).
- You used your smart card to log in to your workstation.

Remove your smart card from the smart card reader.  
Your workstation is now locked.

## Using 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.

## To use Windows Dial-Up/VPN for remote access

### Prerequisites

- Your smart card contains a certificate configured for Windows PKI login.
- 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** box and click **OK**.  
Once authentication is successful, the Dial-Up or VPN session is established.

## Using a non-Microsoft VPN for remote access

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

### To use a non-Microsoft VPN for remote access

#### Prerequisites

- You can access a VPN product supported by ActivClient. For the complete list, refer to *ActivClient CAC Overview*.
- Your smart card contains a certificate configured for VPN login.
- 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) and the certificate for the VPN authentication. For more information, refer to your VPN documentation.

1. Insert your smart card (chip side up and chip first) into the smart card reader.
2. Start your VPN connection.
3. When prompted, type your smart card PIN, and click **OK**.  
When you are authenticated, the VPN session is established.

## Accessing a secure Web site

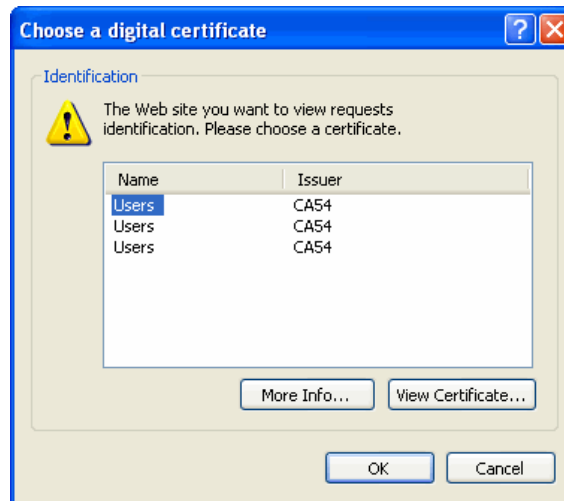
### Access a secure Web site with Internet Explorer

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

### To access a secure Web site with Internet Explorer

#### Prerequisites

- Your smart card contains a certificate configured for authentication to this Web site.
  - The Microsoft CAPI support option has been selected during setup.
1. Insert your smart card 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 stored on your smart card, select the appropriate ActivClient certificate, and click **OK**.
4. Enter your PIN in the **Smart card PIN** box and click **OK**.  
The browser sends your certificate and a digital signature to the Web server. The Web server verifies your signature and grants access to the secured site or page.

## Access a secure Web site with Netscape, Mozilla and Firefox

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

### To access a secure Web site with Netscape, Mozilla or Firefox

#### Prerequisites

- Netscape, Mozilla or Firefox is installed on your computer.
- Your smart card contains a certificate configured for authentication to this Web site.
- The ActivClient PKCS#11 library has been registered to Firefox, Mozilla or Netscape. Refer to *ActivClient Installation Guide* for details.

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

## Sending/Receiving signed and encrypted email messages with Microsoft Outlook

### Sending/Receiving signed email messages

A digital signature is a combination of your private key and a 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.

#### To send signed email messages

##### Prerequisites

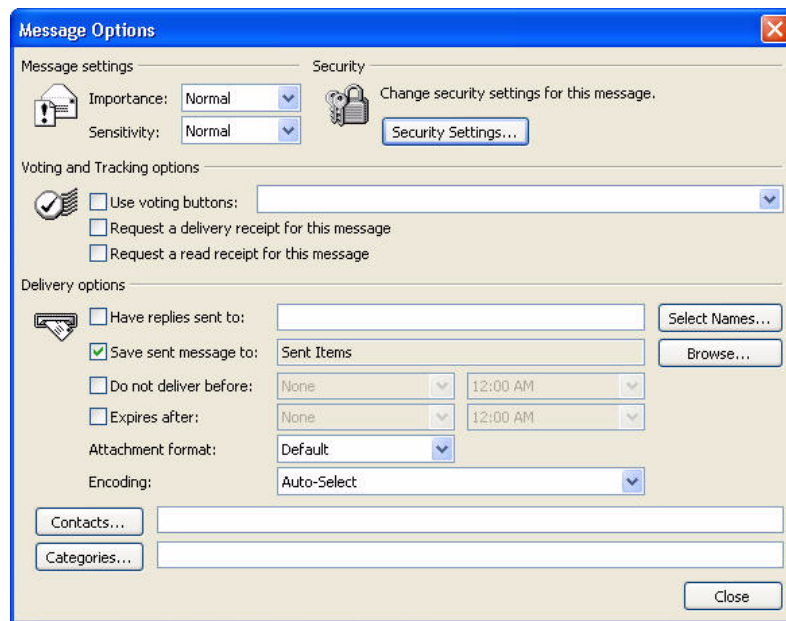
- Microsoft Outlook is installed on your workstation.
  - The Microsoft CAPI support option (from the Digital Certificates Services option) has been installed during setup.
  - A certificate with email signature capabilities is available on your smart card.
1. Insert your smart card (chip side up and chip first) into the smart card reader.
  2. Create the email message.

## 3. Do one of the following:

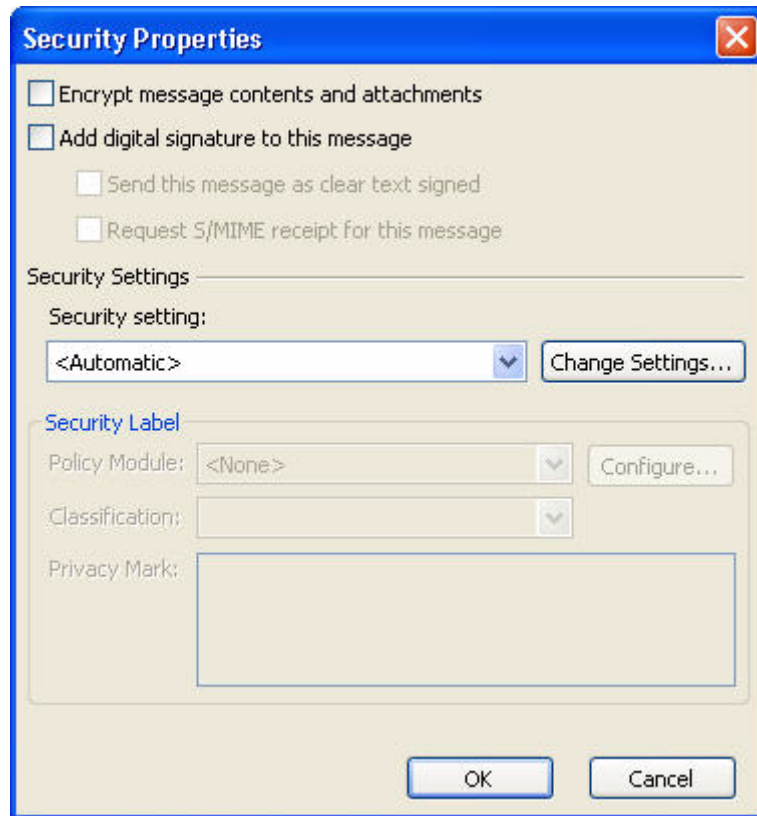
- Click on the **Digitally Sign Message** icon  from the Outlook toolbar.

–Or–

- If the icon does not appear on the toolbar:
  - Click **Options** on the **View** menu (or the **Options** icon on the toolbar). The **Message Options** dialog box is displayed.



- Click **Security Settings**. The **Security Properties** dialog box is displayed.



- Select the **Add digital signature to this message** check box and click **OK**.
  - Close the **Message Options** dialog box.
4. Complete and send the email message.

## To receive 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.

## Sending / Receiving 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.


### To send encrypted email messages

#### 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.

1. Create the email message.

2. Do one of the following:

- On the Outlook toolbar, click the **Encrypt Message Contents and Attachments** icon .

–Or–

- If the icon does not appear on the toolbar:
  - Click **Options** on the **View** menu (or the **Options** icon on the toolbar). The **Message Options** dialog box is displayed.
  - Select **Security Settings**. The **Security Properties** dialog box is displayed.
  - Select the **Encrypt message contents and attachments** check box and click **OK**.
  - Close the **Messages Options** dialog box.

3. Complete and send the email message.

### To receive encrypted email messages

#### Prerequisites

- Microsoft Outlook is installed on your workstation.

- A certificate with email encryption capabilities is available on your smart card.
  - The Microsoft CAPI support option has been installed during setup.
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.

## Sending/Receiving signed/encrypted mails with Netscape or Thunderbird

### Sending/Receiving signed email messages

A digital signature is a combination of your private key and a 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.

#### To send signed email messages

##### Prerequisites

- Netscape Messenger or Thunderbird is installed on your computer.
  - A certificate with email signature capabilities is available on your smart card.
  - The ActivClient PKCS#11 library has been registered to Thunderbird or Netscape. Refer to *ActivClient Installation Guide* for details.
1. Insert your smart card (chip side up and chip first) into the smart card reader.
  2. Start your email client.



3. Open the **Mail&Newsgroups** window.
4. Click **Compose**.
5. Compose your mail and go to **Security** (on the top toolbar of your mail) and select **Digitally Sign this message and encrypt**.
6. Click **Send**.
7. Enter your **PIN**.
8. Verify the sent email has been signed.

## To receive 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. Open the **Mail&Newsgroups** window.
4. Click on the signed message you want to read in your inbox. If the sender is successfully authenticated, the message appears with a secure message icon.

## Sending/Receiving 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.

## To send encrypted email messages

### Prerequisites

- Netscape Messenger or Thunderbird is installed on your workstation.

- The ActivClient PKCS#11 library has been registered to Thunderbird or Netscape. Refer to *ActivClient Installation Guide* for details.
1. Insert your smart card (chip side up and chip first) into the smart card reader.
  2. Start your email client.
  3. Open the **Mail&Newsgroups** window.
  4. Open a signed email (sent from computer).
  5. Click **Reply**.
  6. Compose your mail.
  7. Go to **Security** (on top of the email toolbar) and select **Encrypt this message**.
  8. Encrypt your mail.
  9. Click **Send**.
  10. Enter your PIN.
  11. Look in your inbox for the sent email and verify if it is encrypted.

## To receive encrypted email messages

### Prerequisites

- Netscape Messenger or Thunderbird is installed on your workstation.
  - A certificate with email signature capabilities is available on your smart card.
  - The ActivClient PKCS#11 library has been registered to Thunderbird or Netscape. Refer to *ActivClient Installation Guide* for details.
1. Insert your smart card (chip side up and chip first) into the smart card reader.
  2. Start your email client.

3. Open the **Mail&Newsgroups** window.
4. Select the encrypted email
5. Enter your PIN when prompted.
6. Read the encrypted mail in clear text.

## Encrypting/Decrypting files with EFS

Windows Vista allows Encryption File System (EFS) 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.

### Configuring your workstation for EFS

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

#### To configure your workstation for EFS with your smart card encryption certificate

##### Prerequisites

- Your Operating System is Windows Vista.
  - Your platform is configured for EFS.
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 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, choose to select an existing encryption certificate.
6. Select your smart card EFS certificate in the certificate list.
7. Enter your smart card PIN and click **OK**.  
The selected 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.

## To configure your workstation for EFS and generate a smart card encryption certificate

### Prerequisites

- Your Operating System is Windows Vista.
  - Your platform is configured for EFS.
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 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, choose to create a new encryption certificate.
  6. Choose to create either a smart card self-signed certificate or a certificate issued by your domain's certification authority.
  7. Enter your smart card PIN and click **OK**.  
The 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.

## Encrypting/Decrypting files or folders with EFS

### To encrypt a file or folder with EFS

#### Prerequisites

- Your Operating System is Windows Vista.
- 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.

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 the **Encrypt contents to secure data** option).
5. Enter your smart card PIN and click **OK**.  
The file or the folder is then encrypted and appears in green in Microsoft Explorer.

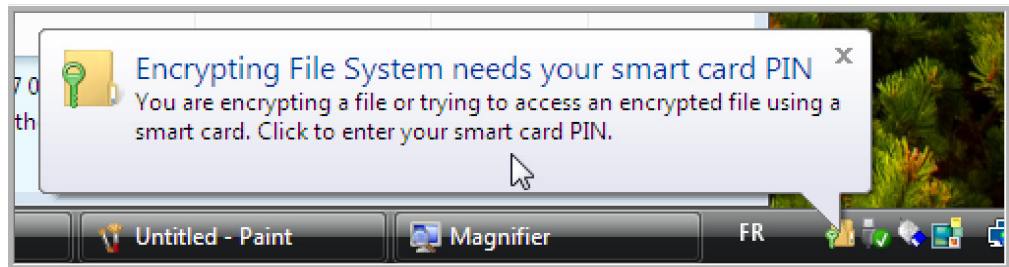
### To decrypt a file or folder with EFS

#### Prerequisites

- Your Operating System is Windows Vista.
- 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.

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 asking for your smart card PIN.



4. Click on the displayed link.
5. Enter your smart card PIN and click **OK**.  
The file is opened in clear text.

## Updating EFS Certificate and re-encrypting files

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

### To re-encrypt files and folders with a new EFS certificate

#### Prerequisites

- Your Operating System is Windows Vista.
- Your platform is configured to allow EFS.
- Your platform is configured to require smart card for EFS.
- You have the smart card containing the EFS certificate currently configured for EFS on this platform.
- You have files encrypted with your current EFS certificate.

1. Select **User Accounts** in Control Panel.
2. Select **User Accounts**.
3. Select **Manage your file encryption certificates** from the left pane.  
The Manage your file encryption certificates wizard is displayed.
4. When prompted to select an existing encryption certificate or create a new one on your smart card, choose to create a new certificate.
5. Choose to create either a smart card self-signed certificate or a certificate issued by your domain's certification authority.
6. Insert your smart card.

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

7. Click **Next**.
8. Back up your key (optional) and click **Next**.  
A tree representing your file system is displayed.
9. Select the folders to re-encrypt. Make sure all folders containing your encrypted files are selected.
10. Enter your smart card PIN and click **OK**.  
The wizard completes successfully.

## To re-encrypt files and folders with an EFS certificate already on your smart card

If you have already encrypted some files with a certificate and if you have updated the encryption certificate (e.g. it expired), Windows allows you to re-encrypt your encrypted files with your new encryption certificate.

### Prerequisites

- Your Operating System is Windows Vista.
- Your platform is configured to allow EFS.
- Your platform is configured to require the use of a smart card for EFS.

- You have a smart card containing an 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.

1. Select **User Accounts** in Control Panel.
2. Select **User Accounts**.
3. Select **Manage your file encryption certificates** from the left pane.

The Manage your file encryption certificates wizard is displayed.

4. When prompted to select an existing encryption certificate or create a new one on your smart card, choose to select an existing encryption certificate.
5. Select your new smart card EFS certificate from the certificate list.  
A tree representing your file system is displayed.
6. Select the folders to re-encrypt. Make sure all the folders containing your encrypted files are selected.
7. Enter your PIN whenever you are prompted to do it.  
The wizard completes successfully.

## Recovering encrypted files

When you lose or damage your smart card, you need to recover your encrypted files content.

## To recover encrypted files

### Prerequisites

- Your Operating System is Windows Vista.
- 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.
1. Import the backup EFS certificate in your new smart card with ActivClient User Console.
  2. In Microsoft Explorer, select any of the encrypted file you need to recover.
  3. When prompted, insert your new EFS certificate smart card.
  4. Enter your smart card PIN and click OK.  
You can access your file in clear text.

**Note:** Depending on your configuration, a recovery agent may be configured to help you recover your data. For more information on files and folders recovery, refer to Microsoft Windows Help on your Windows Vista workstation.

# Chapter 8: Using Remote Access/OTP

This section discusses the following topics:

- ["Getting a one-time password automatically" on page 74](#)
- ["Getting a one-time password manually" on page 75](#)

## Getting a one-time password automatically

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 on the workstation's taskbar)
- Automatically copies the OTP to the clipboard so it is ready to be pasted into any application.

## To get a one-time password automatically

### Prerequisites

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

1. Right click on ActivClient Agent.
2. Select **Get One-Time Password**.  
The ActivClient notification window is displayed, showing the one-time password generated on your smart card.
3. Place your cursor in the password box of the application you want to authenticate to.

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

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

## Getting a one-time password manually

ActivClient also provides a manual way to 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).

### To get a One-time password manually

#### Prerequisites

- ActivClient User Console is open.
  - One-Time Password Services option has been installed during setup.
  - Your smart card has been initialized to use one-time passwords.
1. Display the **Generate One-Time Password** dialog box by taking one of the following actions:

- From the ActivClient User Console tasks pane:

Select **Generate One-Time Passwords**.

The **Generate One-Time Password** window is displayed.

–Or–

- From the ActivClient User Console right pane:

Double-click the server's icon.

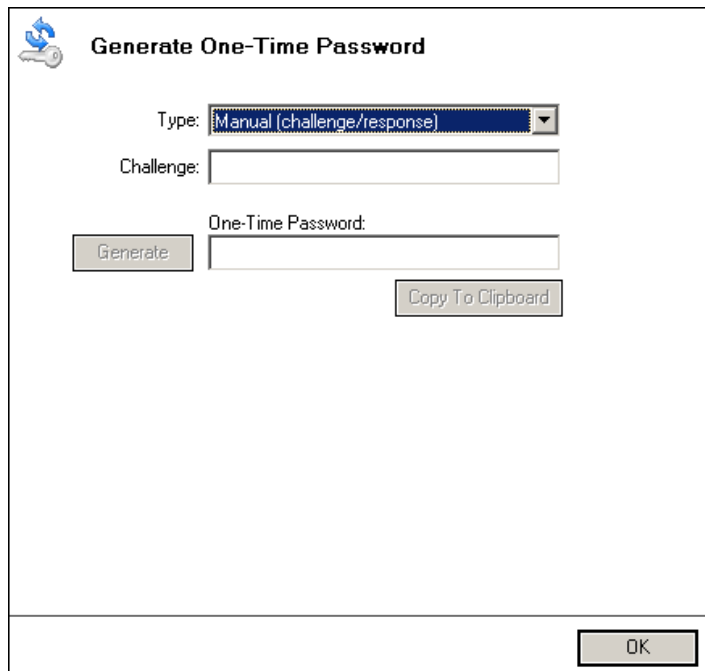
The **Generate One-Time Password** window is displayed.

2. Take one of the following actions depending of your administrator's recommendations:
  - 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.

–Or–

- If your administrator recommends to authenticate in a **Challenge/Response** mode, click **Manual** (Challenge/Response) from the **Type** drop-down list. A **Challenge** box is displayed in the **Generate One-Time Password** window.



The screenshot shows a dialog box titled "Generate One-Time Password". It contains a "Type" dropdown menu with "Manual (challenge/response)" selected. Below this is a "Challenge:" label followed by an empty text input field. Underneath the challenge field is a "One-Time Password:" label followed by another empty text input field. To the left of the "One-Time Password" field is a "Generate" button. To the right is a "Copy To Clipboard" button. At the bottom right corner of the dialog is an "OK" button.

3. 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).
4. Type the challenge in the **Challenge** box.
5. Click **Generate**.  
Your newly generated one-time password is displayed.
6. Type (or copy and paste) it into any authentication window.

# Chapter 9: Viewing personal information

This section discusses the way you can display your smart card personal information.

## About Personal Information

US Department of Defense CAC smart cards and US Government Personal Identity Verification PIV smart cards allow to access personal information for each smart card holder.

Personal information display 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!

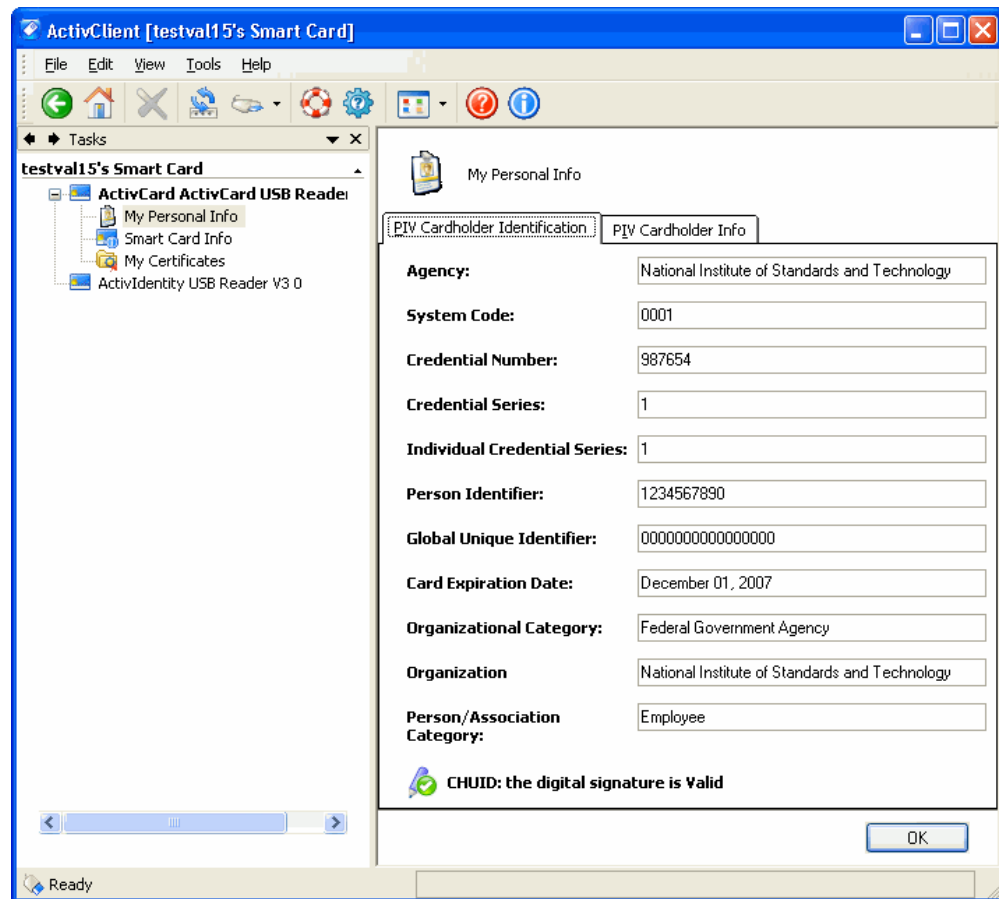
## To access “My Personal Info” on CAC and PIV cards

Take one of the following actions:

- From the User Console left pane:  
Click on **View my personal info** under **My Personal Info Task**.  
The **Personal Information** dialog box is displayed on the right pane
  - From the User Console right pane:  
Double-click **My Personal Info** icon.
- Or–

Select **Open** from it's right-click menu.

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



**Note:** For PIV smart cards, the User Console displays the digital signature's validity for:

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

# Chapter 10: Using ActivClient with Terminal Services

This section discusses the following topics:

- ["Logging on to a Citrix session" on page 79.](#)
- ["Using a smart card inside a Citrix session" on page 82.](#)
- ["Logging on to a Remote Desktop session" on page 83.](#)
- ["Using a smart card in a Remote Desktop session" on page 84.](#)
- ["Locking a Remote Desktop session" on page 85.](#)

## Logging on to a Citrix session

You can use Citrix products to run an application on a Citrix server and interact with the end user on a different terminal (Windows or another). ActivClient provides smart card–based authentication to Citrix for increased security.

**Note:** It is not necessary to install ActivClient on the Citrix client.

## To log on using a Citrix product

### Prerequisites

- ActivClient is installed on the Citrix Presentation Server. For more information on supported versions of Citrix Presentation Server, refer to *ActivClient CAC 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. Here are the four cases you may 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"

then, you are logged in automatically as soon as you start a Citrix session. See [Chapter 7, "Logging on to Windows with a certificate" on page 54.](#)

- 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" then, you are logged in automatically as soon as you start a Citrix session. See [Chapter 7, "Logging on to Windows with a certificate" on page 54.](#)
- You log on to your workstation with a thin terminal (Windows XP Embedded) without ActivClient on the thin terminal and your Citrix authentication mode is "Local User with Pass-through" then, you are logged in automatically as soon as you start a Citrix session.
- You log on to your workstation with a thin terminal (Windows CE) without ActivClient on the thin terminal and no local authentication and your Citrix authentication mode is "Local User Pass-through" then, you are prompted to authenticate with your smart card and PIN code.

## To open a Citrix session-examples

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

Here are examples of Citrix login session for "Smart Card with Pass-through" authentication mode with each of the Citrix clients.

## To log on to a Citrix session in a "Smart Card with Pass-through" authentication mode using Citrix ICA Client Program Neighborhood

### Prerequisites

- Microsoft CAPI support option has been installed during setup.
- You have a smart card and a certificate with PKI login 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".



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

The Citrix Program Neighborhood opens.

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

You are automatically logged on to the Citrix remote session.

## To log on to a Citrix session in “Smart Card with Pass-through” authentication mode using Citrix ICA Client Program Neighborhood Agent

### Prerequisites

- Microsoft CAPI support has been installed during setup.
- You have a smart card and a certificate with PKI login capabilities.
- Citrix ICA Client Program Neighborhood Agent is installed.
- The Citrix authentication mode is “Smart Card with Pass-through”.
- Your Web Interface Server URL is configured in 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 on the workstation’s taskbar and select your Citrix server desktop.  
You are automatically logged on to the Citrix remote session.

## To log on to a Citrix session in “Smart Card with Pass-through” authentication mode using Citrix Web Interface

### Prerequisites

- Microsoft CAPI support has been installed during setup.
- You have a smart card and a certificate with PKI login capabilities.

- Citrix Web interface Client is installed.
- Citrix authentication mode is “Smart Card with Pass-through”.
- Your Web Interface Server URL is configured in Citrix ICA Client Program Neighborhood Agent.

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 on your Citrix server desktop icon in your Citrix Web Interface web page.  
The Windows login interface of your Citrix server desktop appears within your browser window.
5. Enter your PIN code.  
You are automatically logged on to the Citrix remote session within your browser window.

**Note:** You can find more information on Citrix clients configuration in the Citrix documentation available on Citrix website.

## Using a smart card inside a Citrix session

You can use Citrix Presentation Server to run an application on a Citrix server and interact with the end user on a different terminal (Windows or another). ActivClient provides smart card-based services for applications running in the Citrix session.

**Note:** It is not necessary to install ActivClient on the Citrix client workstation.

## To use your smart card inside a Citrix session

### Prerequisites

- ActivClient is installed on the Citrix Presentation Server. For more information on supported versions of Citrix Presentation Server, refer to *ActivClient CACOverview*.
- 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.

1. Start the application you are using with your smart card, for example, Microsoft Outlook.
2. Use the application as usual, and access smart card-based services, for example, prepare to send a signed email message.
3. When you are prompted for the PIN, type 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.

**Note:** Smart card management operations such as certificate download operations are not available within the Citrix session.

## Logging 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 without being in your office.
- 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.

**Note:** It is not necessary to install ActivClient on the client workstation. For information about supported environments, refer to *ActivClient CACOverview*.

## To log on to a Remote Desktop session

### Prerequisites

- The remote computer you intend to access using Remote Desktop Connection can either be Window Vista or Windows Server 2003 with Windows Terminal Services, all of them having ActivClient installed.
- Your workstation is either Windows XP Professional or, Windows Vista with Remote Desktop Connection v5 or v6 installed.
- You have a smart card and a smart card reader up and running connected to your workstation.

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.

## Using a smart card in a Remote Desktop session

You can use Microsoft Remote Desktop to run an application on a PC (workstation or server) and interact with the end user on a different workstation. ActivClient provides smart card–based services for applications running in the Remote Desktop session.

**Note:** It is not necessary to install ActivClient on the client workstation.

## To use your smart card in a Remote Desktop session

### Prerequisites

- The remote computer you intend to access using Remote Desktop Connection can either be Windows XP Professional, Window Vista or Windows Server 2003 with Windows Terminal Services, all of them having ActivClient installed.
  - Your workstation is either Windows XP Professional or, Windows Vista with Remote Desktop Connection v5 or v6 installed.
  - 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.
1. Start the application that is using your smart card, for example, Microsoft Outlook.
  2. Use the application as usual, and access smart card-based services, for example, prepare to send a signed email message.
  3. When you are prompted for the PIN, type 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.

## Locking 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 without being in your office.
- Connect to a Windows Server with Windows Terminal Services enabled, to access applications not available on your local workstation.

## To lock a Remote Desktop session

### Prerequisites

- The remote computer you intend to access using Remote Desktop Connection can either be Windows XP Professional, Windows Vista or Windows Server 2003 with Windows Terminal Services, all of them having ActivClient installed.
- Your workstation is either Windows XP Professional or, Windows Vista with Remote Desktop Connection v5 or v6 installed.
- 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.

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).

# Terms and Acronyms

This chapter presents terms and acronyms used in this publication.

## Terminology

| Terms   | Definitions   |
|---|---|
| <b>Certificate Authority (CA)</b>                     | 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. |
| <b>ActivID Card Management System (CMS)</b>           | 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.                                       |
| <b>Cryptographic Service Provider</b>                 | An independent software module that performs cryptography algorithms for authentication, encoding, and encryption.  |
| <b>Federal Information Processing Standard (FIPS)</b> | 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.                             |
| <b>GlobalPlatform</b>                                 | Replaces OpenPlatform (OP).   |
| <b>My Digital ID Card</b>                             | This CMS component allows end users to access the self-service CMS functions, which includes card and credential management.  |
| <b>One-Time Password</b>                              | 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.  |
| <b>PIN</b>  | Personal Identification Number. Is used to authenticate to your smart card in order to perform actions such as Windows PKI login, remote access and email signature.  |
| <b>Public Key Infrastructure (PKI)</b>                | PKI describes the laws, policies, standards, and software that regulate or manipulate certificates and public and private keys.   |

|                                    |  |
|------------------------------------|--|
| <b>Registration Authority (RA)</b> | 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.   |
| <b>SKI</b>                         | SKI (Symmetric Key Infrastructure) keys are used to perform strong authentication on remote applications. SKI keys encrypt passwords in: <ul style="list-style-type: none"> <li>• Synchronous mode (generates 1 password without any challenge. The server uses the same method to create a password than the smart card)</li> <li>• Asynchronous: encrypts a challenge</li> </ul> |
| <b>Standalone smart card</b>       | Smart card with uploaded applets issued by the manufacturer.   |

## Acronyms

### Acronyms

### Definitions

|             |  |
|-------------|--|
| <b>CA</b>   | Certificate Authority.   |
| <b>CAC</b>  | Common Access Card (for the United States Department of Defense).  |
| <b>CSP</b>  | Cryptographic Service Provider.  |
| <b>FIPS</b> | Federal Information Processing Standard.   |
| <b>GP</b>   | GlobalPlatform. Replaces OpenPlatform (OP).  |
| <b>OTP</b>  | One-Time Password.   |
| <b>PKI</b>  | Public Key Infrastructure.   |
| <b>PIV</b>  | Personal Identity Verification Card issued by the United States government to federal employees and contractors. |
| <b>RA</b>   | Registration Authority.  |
| <b>SKI</b>  | Symmetric Key Infrastructure.  |



# Send us your comments

**Product:** ActivClient CAC 64-bit edition

**Document:** ActivClient CAC User Guide

**Document Reference:** AC/x64/CAC/UG/06.2007/6.1

ActivIdentity welcomes your comments and suggestions. Your input is an important factor in future revisions of this publication. Let us know your opinion.

**Please send your feedback via email to:** [tpd@actividentity.com](mailto:tpd@actividentity.com).

If you would like a reply, please include your name, company, email address, and telephone number (optional).

If you find errors or have general suggestions for improvement, please indicate the chapter, section, title, and page number.

- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct/helpful?
- What did you like most/least about this publication?

**Important:** If you have problems with the software, please contact your local ActivIdentity representative.

ActivIdentity  
Corporate Headquarters  
6623 Dumbarton Circle  
Fremont, CA 94555  
USA