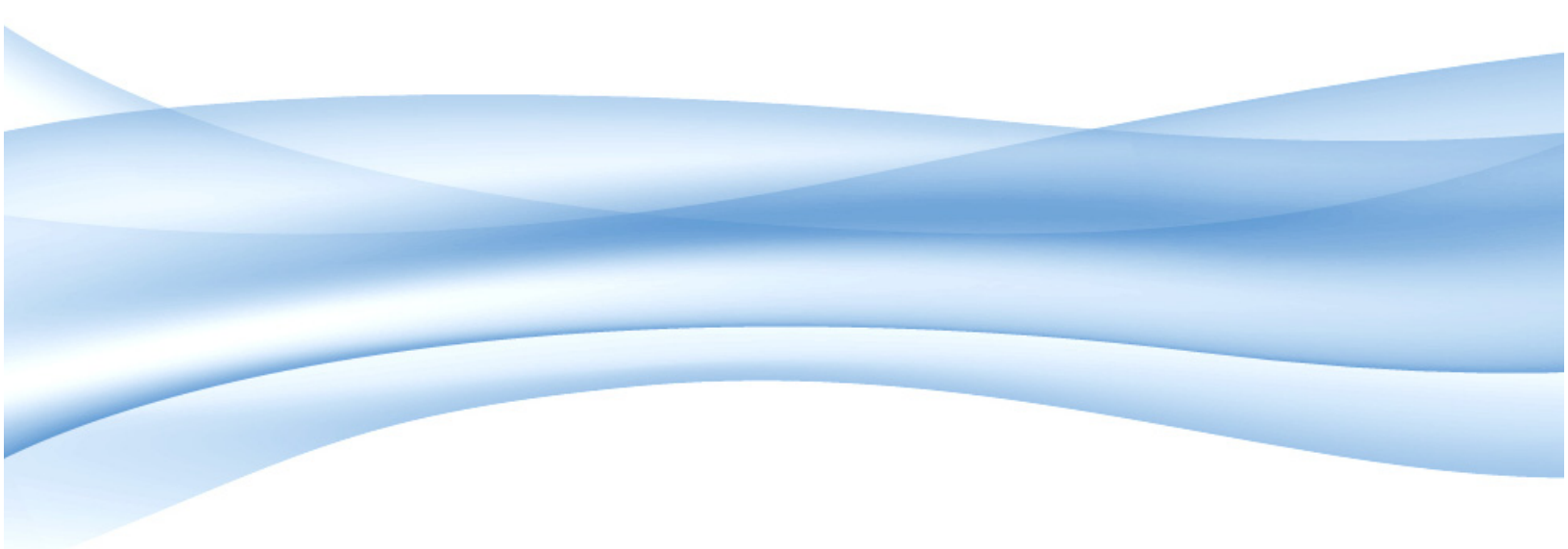


# ActivClient CAC 64-bit edition

## Overview

**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/O/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 Overview



# ActivClient CAC 64-bit edition

## Overview

### 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: ACTIVCLIENT SERVICES</b>	<b>10</b>
<b>About ActivClient</b>	<b>10</b>
<b>Standards</b>	<b>10</b>
<b>PKI services</b>	<b>11</b>
<b>Remote Access and One-Time Password Services</b>	<b>12</b>
To log on to applications using an OTP	13
<b>Remote session services</b>	<b>13</b>
Citrix Presentation Server support	13
Supported Citrix versions	13
Supported services in a Citrix environment	14
Microsoft Remote Desktop Protocol (RDP) support	14
Environments	14
Services	15
<b>Administrative services</b>	<b>15</b>
ActivClient User Console	15
Digital certificates	15
One-Time Passwords	15
Personal information	16
Smart Card PIN	16
Smart Card Initialization	16
Smart card lock/unlock	16
Remote/centralized management	17
ActivClient Agent	17
Troubleshooting Wizard	17
Advanced Diagnostics	17
Log files	17
Installation and deployment	18
Smart card automatic registration	18
Localization	18
Branding	18
Notification	19
ActivClient Resource Kit	19
ActivClient SDK	19
<b>Smart card services and profiles</b>	<b>20</b>
Standalone / Mini mode	20
Standalone mode	20
AAA Server-managed mode	20
CMS-managed mode	21
US Department of Defense Common Access Card mode	21
US Government PIV mode	21

<b>CHAPTER 3: ACTIVCLIENT COMPONENTS</b>	<b>23</b>
<b>ActivClient Agent</b>	<b>23</b>
ActivClient Agent icons on the taskbar	23
ActivClient Agent shortcut menu commands	23
<b>User Console</b>	<b>25</b>
To access shortcut menu commands	27
The Menu toolbar	28
The Standard toolbar	30
<b>PIN Initialization Tool</b>	<b>31</b>
To access the PIN Initialization Tool	32
<b>PIN Change Tool</b>	<b>32</b>
To access the PIN Change tool	32
<b>Troubleshooting Wizard</b>	<b>33</b>
To access the Troubleshooting Wizard	33
<b>Advanced Diagnostics</b>	<b>34</b>
To access the Advanced Diagnostics Tool	35
<b>Advanced Configuration Manager</b>	<b>35</b>
To access the Advanced Configuration Manager	36
 <b>CHAPTER 4: OPERATIONAL ENVIRONMENT</b>	 <b>37</b>
<b>ActivIdentity products</b>	<b>37</b>
<b>Operating systems</b>	<b>37</b>
<b>Smart cards and USB tokens</b>	<b>38</b>
<b>Smart card readers</b>	<b>41</b>
ActivIdentity devices	41
Third-party devices	41
 <b>TERMS AND ACRONYMS</b>	 <b>43</b>
<b>Terminology</b>	<b>43</b>
<b>Acronyms</b>	<b>44</b>

# ActivClient CAC 64-bit version

## Overview

### List of Tables

Table 2-1: Supported standards	10
Table 2-2: List of PKI services	11
Table 2-3: Logging on to applications using an OTP	13
Table 3-4: ActivClient Agent Shortcut commands	24
Table 3-5: User Console left and right panes	26
Table 3-6: Menus and commands from the Menu toolbar	29
Table 3-7: Standard toolbar commands	31
Table 4-8: ActivIdentity Products	37
Table 4-9: Supported Smart Cards and USB tokens	39

# ActivClient CAC 64-bit version

## Overview

### List of Figures

Figure 3-1: Tasks view . . . . .	26
Figure 3-2: Tree view . . . . .	27
Figure 3-3: Right click menu of a user certificate . . . . .	28
Figure 3-4: Menu toolbar . . . . .	29
Figure 3-5: Standard toolbar . . . . .	30
Figure 3-6: Troubleshooting Wizard – Diagnosis and Resolutions window . . . . .	33
Figure 3-7: The Advanced Diagnostics Tool . . . . .	34
Figure 3-8: Sample output from the Advanced Configuration Manager. . . . .	36



# Chapter 1: Introduction

## About this Guide

This guide provides an overview of ActivClient capabilities including the following topics:

- ActivClient services
- ActivClient components
- Operational environment

## Audience

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

## Assumed knowledge and prerequisites

This document assumes the audience has a basic working knowledge of Windows as well as some understanding of Public Key Infrastructure.

## Other documents

This Guide is part of ActivClient set of documents including:

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

# Chapter 2: ActivClient services

In this section you will learn about:

- ["About ActivClient" on page 10](#)
- ["Standards" on page 10](#)
- ["PKI services" on page 11](#)
- ["Remote Access and One-Time Password Services" on page 12](#)
- ["Administrative services" on page 15](#)
- ["Smart card services and profiles" on page 20](#)

## About ActivClient

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

ActivClient enables usage of PKI certificates and keys, one-time password and static password credentials on a smart card or USB token to secure desktop applications, network log on, remote access, web log on, e-mail and electronic transactions.

## Standards

ActivClient supports the following standards.

**Table 2-1: Supported standards**

Feature	Description
Smart cards	ISO 7816
Smart card operating system	Java Card 2.1 and 2.2
Smart card reader architecture	PC/SC
Public Key Mechanisms	1024 and 2048-bit RSA, X509 certificates

Feature	Description
Public Key Cryptography (PKI)	PKCS#7, 10, 11, 12, Microsoft CAPI 2.0, SSL v3 and S/MIME
Symmetric Key Cryptography (one-time passwords)	DES, Triple DES, ANSI x9.9
US Government	<ul style="list-style-type: none"> <li>• U.S Government Smart Card Interoperability Specifications GSC-IS 2.1</li> <li>• FIPS 201 /PIV certified by NIST</li> <li>• U.S DoD CAC Middleware Requirements Release 3.0</li> <li>• GSA Basic Services Interface (BSI) versions 1.8, 2.0 and 2.1</li> </ul>
Smart card Management	GlobalPlatform 2.0.1 and 2.1
Setup	Windows Installer (MSI)
Product Accessibility	Section 508 compliant

## PKI services

The following table lists the PKI services. ActivClient provides digital certificate services using RSA key pairs stored on a smart card.

Table 2-2: List of PKI services

Feature	Description
Windows login	<ul style="list-style-type: none"> <li>• Provides a digital certificate-based mechanism to log on to the domain on Windows Server 2003 64-bit with relevant Service Packs and Windows Vista 64-bit.</li> <li>• Provides the ability to log the user off or lock the workstation on smart card removal.</li> <li>• Provides an automatic certificate registration to Windows on smart card insertion and optional removal on smart card removal.</li> </ul>
Remote access	<ul style="list-style-type: none"> <li>• Microsoft Windows dialer on Windows Server 2003 64-bit, Windows Vista 64-bit</li> <li>• Microsoft Windows VPN on Windows Server 2003 64-bit, Windows Vista 64-bit</li> <li>• Other VPN clients supporting smart cards via CAPI or PKCS11 either in native 64-bit or 32-bit mode</li> </ul>

Feature	Description
Secure web access	<p>Access to any Web server with SSL v3 and a smart card-based digital certificate with the following browsers:</p> <p><b>Microsoft Internet Explorer:</b></p> <ul style="list-style-type: none"><li>• Microsoft Internet Explorer 7</li><li>• Microsoft Internet Explorer 7 32-bit</li></ul> <p><b>Mozilla-based browsers:</b></p> <ul style="list-style-type: none"><li>• Firefox 64-bit edition (tested with a pre-release version of Firefox 3.0)</li><li>• Firefox 1.5.0.4 and 2 (32-bit editions)</li><li>• Mozilla 1.7.3 (32-bit edition)</li><li>• Netscape 4.76, 7.1, 8 (32-bit editions)</li></ul>
Secure email	<p>Email signature, encryption/decryption:</p> <ul style="list-style-type: none"><li>• Microsoft Outlook 2007 (Office 2007)</li><li>• Thunderbird 64-bit edition (tested with a pre-release version of Thunderbird 1.6)</li><li>• Thunderbird 1.5.0.4 (32-bit edition)</li><li>• Netscape Messenger 4.76 (32-bit edition)</li></ul>
Encrypting file system	<p>ActivClient supports the Windows Encrypting File System (EFS) feature of Windows Vista: with a smart card-based certificate, you can encrypt/decrypt files on a Windows Vista workstation.</p>
Examples of other PKI enabled clients	<p>ActivClient also supports other applications that provide PKI services with smart cards using the CAPI (Microsoft Crypto API) or PKCS#11 interfaces. Examples include Microsoft Office 2003 and 2007 that provide file signing capability.</p>

## Remote Access and One-Time Password Services

ActivClient generates a one-time password (OTP) on the smart card and allows users to use the generated one-time password(s) to log on to applications requiring strong authentication via dialup, VPN or web. These one-time password services require an ActivIdentity 4Tress authentication server, such as ActivIdentity 4Tress AAA Server.

## To log on to applications using an OTP

Users have several options to log on to an application using a one-time password. The following table describes those options:

Table 2-3: Logging on to applications using an OTP

Feature	Description
Log on automatically with a one-time password (OTP) using Single Sign On	Combined with ActivIdentity SecureLogin SSO, ActivClient can generate an OTP and submit it automatically to any application supported by SecureLogin.
Log on with a one-time password (OTP) in one-click	From the "Get One-Time Password" entry in the ActivClient Agent (on the Windows taskbar), ActivClient generates an OTP and copies it to the clipboard. Users can simply paste it into any application.
Log on manually with a one-time password (OTP)	From the ActivClient User Console, ActivClient can generate one-time passwords in both synchronous and challenge/response modes. Users can simply paste the OTP into any application.

## Remote session services

ActivClient supports the following two major remote session services:

- Citrix Presentation Server Support
- Microsoft Remote Desktop Protocol (RDP) Support

## Citrix Presentation Server support

### Supported Citrix versions

ActivClient supports the following versions of Citrix Presentation Server, Citrix clients and web interface:

#### Citrix Presentation Server

Citrix Presentation Server v4.0 x64 with rollup pack 3, Citrix Presentation Server v4.5 x64 installed on Windows Server 2003 64-bit.

### Citrix Client:

- Program Neighborhood (Classic) on Windows 2000, Windows XP, Windows Server 2003, Windows Vista. Available in MetaFrame Presentation Server Client Packager 8.1, 9.1, 9.2 or 10.0.
- Program Neighborhood Agent on Windows 2000, Windows XP, Windows Server 2003, Windows Vista. Available in Citrix Presentation Server Client Packager Version 9.1, 9.2 or 10.0.
- Web Interface. Available in Citrix Presentation Server Client Packager Version 9.1, 9.2 or 10.0.
- Thin terminals with Windows XP Embedded operating system and Citrix ICA Client 8.0 or higher.
- Thin Terminals with Windows-CE .NET 4.2 operating system and Citrix ICA Client 8.0 or higher.

## Supported services in a Citrix environment

- You can remotely log on to the Citrix Server machine with your smart card.
- Smart card operations are supported within a Citrix session. Software such as Microsoft Outlook is running on a remote machine, while the smart card reader is connected on a client machine.
- The client machine can access multiple Citrix servers in the same session (with ActivClient running on each Citrix server).

## Microsoft Remote Desktop Protocol (RDP) support

ActivClient provides the following Microsoft Remote Desktop Protocol (RDP) support:

### Environments

The following Remote Desktop Protocol (RDP) environments are supported:

- Windows Server 2003 64-bit Terminal Server
- Remote Desktop Connection v5 or v6 on Windows XP or Windows Vista (32-bit or 64-bit)

## Services

- You can log on with RDP client to a remote machine (on Windows Vista 64-bit or Windows Server 2003 64-bit Terminal Server) with your smart card.
- Smart card operations are supported within a RDP session. Software such as Microsoft Outlook is running on the remote machine but the smart card reader driver is on the client.
- One client accessing multiple Terminal Servers in the same session (with ActivClient running on each Terminal Server).

## Administrative services

The following administrative services are available to end users through the **ActivClient User Console**. Administrators are offered additional services through ActivIdentity management products.

### ActivClient User Console

The User Console allows you to view and manage your smart cards and credentials, including digital certificates.

### Digital certificates

Digital certificates can be Root CA certificates or User certificates. They can be displayed by ActivClient User Console in a user-friendly way and can also be deleted by end users if the smart card policy allows it.

- Root CA certificates can be imported on smart cards and exported from smart cards.
- User certificates can be imported on smart cards (PKCS #12 files).

### One-Time Passwords

The following services are provided in the ActivClient User Console to use and manage your One-Time Password credentials:

- Generate automatic one-time passwords (also known as synchronous mode).
- Generate challenge/response one-time passwords.
- Synchronize counters for one-time passwords.

- Configure user name for remote access with one-time password.

## Personal information

The ActivClient User Console allows users to view personal information stored on their smart card.

Available for:

- PIV (Personal Identity Verification) cards issued to US Federal Employees and Contractors.
- CAC (Common Access Card) issued by the US Department of Defense.

## Smart Card PIN

At any time, your smart card PIN:

- Can be changed.
- Is controlled by you.

## Smart Card Initialization

ActivClient allows users to initialize smart cards before they can be used.

Depending on the smart card configuration, you may want to:

- Initialize a blank smart card including setting the PIN code (the blank smart card may already contain smart card applets or not).
- Reset a smart card (i.e. erase the smart card content) and define a new PIN code.

**Note:** ActivClient also supports smart cards initialized by ActivID Card Management System (CMS).

## Smart card lock/unlock

If you enter several incorrect PINs on the smart card, the smart card locks, preventing any further unauthorized use of it.

In the case your smart card is locked, use an unlock code such as:

- A static unlock code owned by you (stand-alone mode).



- A challenge/response-based unlock code provided by phone by the help desk (requires CMS).
- A challenge/Response-based unlock code performed online through the Self-Service Portal (requires CMS).

**Note:** Depending on your smart card configuration, you can use the PIN Initialization Tool to reinitialize it without needing any unlock process.

## Remote/centralized management

- Provides support for **My Digital ID Smart card**. ActivClient supports the self-service support interface of CMS.
- Allows you to securely update your smart cards.

## ActivClient Agent

- Provides access to common ActivClient operations and shows smart card activity.
- Is displayed as an icon on the Windows taskbar.

## Troubleshooting Wizard

Helps you solve common installation and usage issues, such as:

- Reader not connected
- Smart card inserted on the wrong side
- No reader driver installed.

## Advanced Diagnostics

- Helps advanced users and help desk personnel perform a thorough examination of the ActivClient environment (software and smart card).
- Sends an email of the diagnostic report to the help desk.

## Log files

- Generates log traces to be analyzed by ActivIdentity Customer Support. No confidential information is displayed in the log files.
- Is activated from the Advanced Configuration Manager window or the ActivClient User Console.

## Installation and deployment

ActivClient Setup uses MSI (Microsoft Windows Installer) technology, as well as advanced capabilities to facilitate product installation in large deployments.

Administrators can:

- predefine users options and customize the master installation image.
- customize setup, such as make it silent (all options are already configured, no further intervention is required).
- customize configuration and choose options through Microsoft Transform files (MST) by using standard `msiexec.exe` Windows Installer command line options.
- configure CA certificates installation upon installation of ActivClient.

You can deploy ActivClient using software deployment technology:

- Microsoft SMS 2.0 SP5
- Microsoft SMS 2003 SP1, SP2 and R2
- Microsoft Active Directory push (Windows 2000 and Windows 2003)

ActivClient also provides software Auto-Update feature that allows administrators without software deployment technology to automatically install ActivClient software updates.

## Smart card automatic registration

ActivClient can support new Java Card, US DoD CAC or PIV smart card types that have passed successfully ActivIdentity qualification tests without any ActivClient update.

## Localization

ActivClient is fully localizable. It is available in English and in Japanese versions. For localization in other languages, contact your ActivIdentity reseller.

## Branding

You can customize the User Console with customer-specific graphics.

## Notification

ActivClient displays notification messages to help you resolve common issues as they come up:

- The No Smart Card Reader notification message is displayed above the Windows taskbar at log on when there is no smart card reader connected to the PC or if you unplug inadvertently your smart card reader.
- The Unattended Smart Card notification message is displayed above the Windows taskbar to remind you to take your smart card with you when leaving your workstation. It is displayed only if the smart card has not been removed from the smart card reader and if you attempt to:
  - log off
  - lock your workstation
  - shutdown your workstation
  - restart your workstation
- The Expiration Warning dialog box notifies you that your smart card or one of your smart card certificates is about to expire or has expired. It is displayed:
  - At smart card insertion.
  - At the start of the user session if the smart card is inserted when logging on.

## ActivClient Resource Kit

The ActivClient Resource Kit is:

- Targeted for IT administrators and includes tools to customize and deploy ActivClient.
- A different package from ActivClient. Contact your ActivIdentity reseller for ordering information.

## ActivClient SDK

ActivClient SDK enables integrators to build applications leveraging the ActivClient smart card middleware. It provides documentation, header files/libraries and code samples for the following APIs:

- Microsoft CryptoAPI (CAPI) 2.0
- PKCS#11 v2.11
- Personal Identity Verification (PIV) Middleware API as per National Institute of Standard and Technology (NIST) SP800-73-1 specifications

- Basic Services Interface (BSI) API, defined by the U.S. Government Smart Card Interoperability specifications GSC-IS 2.1
- ActivIdentity ACOMX API

**Note:** ActivClient SDK is a different package from ActivClient. Contact your ActivIdentity reseller for ordering information.

## Smart card services and profiles

This session discusses how the services offered by ActivClient (Initialization, Unlock and Reset) vary depending on the smart card profile. ActivClient supports the following smart card initialization and management modes.

### Standalone / Mini mode

- Smart cards are delivered without applet.
- Smart cards are initialized (including applets loading and PIN definition) using ActivClient PIN Initialization Tool.
- If the smart card becomes locked with too many incorrect PIN codes, you can reset the smart card completely using the PIN Initialization Tool – no need to know any PIN or Unlock code to reset the card. When the card is reset, you can download new credentials on the card.

### Standalone mode

- Smart cards are delivered with applets configured with a default "standalone" profile.
- Smart cards are initialized (i.e. PIN definition) using the ActivClient PIN Initialization Tool, or simply on smart card insertion. A (static) unlock code is displayed to end-users at the end of this initialization process.
- If the smart card becomes locked with too many incorrect PIN codes, you can (via the User Console or on smart card insertion) unlock your smart card with a static unlock code. This allows you to define a new PIN code while your credentials are preserved on the smart card.
- You can reset your smart card completely (from the User Console) if you know the PIN or unlock code.

### AAA Server-managed mode

This is the case where 4TRESS™ AAA Server is used for OTP services.

- Smart cards are delivered with applets configured with a default "standalone" profile.
- Smart cards are initialized (PIN code and OTP credentials) using the AAA Administrator Console.
- If the smart card becomes locked with too many incorrect PIN codes, you can unlock the smart card with a challenge/response mechanism (from the User Console – users have access to the unlock response either on the phone, or online with the AAA Self Help Desk). This allows you to define a new PIN code while your credentials are preserved on the smart card.
- You can reset the smart card completely (from the User Console) if you know the PIN or unlock code (challenge/response).

## CMS–managed mode

- Smart cards are delivered without applets.
- Smart cards are initialized and managed by CMS (including applet loading and loading of user credentials such as certificates).
- If the smart card becomes locked with too many incorrect PIN codes, you can unlock the smart card with a challenge/response mechanism (via ActivClient User Console, users have access to the unlock response either on the phone, or online with the CMS Self Help Desk: My Digital ID Card). This allows you to define a new PIN code while your credentials are preserved on the smart card.
- You can securely update the smart card content (applets and credentials) using the CMS Self Help Desk: My Digital ID Card.
- You can reset the smart card completely using CMS.

## US Department of Defense Common Access Card mode

- ActivClient uses the DOD Common Access Card in read-only mode for usage operations (PKI services and demographic data), in compliance with the DOD middleware requirements. The Change PIN function is supported.
- Issuance, card unlock and card update (update of certificate or demographic data) are services provided by the DOD.

## US Government PIV mode

- Smart cards may be issued by CMS (PIV compliant) or by other smart card management systems.
- ActivClient uses the PIV smart card in read-only mode for usage operations (PKI services and demographic data), in compliance with the PIV specifications. The Change PIN function is supported.

- By FIPS 201 specification, smart card unlock (as known as PIN Reset) needs to be in the presence of an Issuance Officer with cardholder biometric verification. The smart card unlock functionality is not available for PIV smart cards in ActivClient, but can be performed with CMS.

# Chapter 3: ActivClient components

This section provides details about the following ActivClient components:





- ["ActivClient Agent" on page 23.](#)
- ["User Console" on page 25.](#)
- ["PIN Initialization Tool" on page 31.](#)
- ["PIN Change Tool" on page 32.](#)
- ["Troubleshooting Wizard" on page 33.](#)
- ["Advanced Diagnostics" on page 34.](#)
- ["Advanced Configuration Manager" on page 35.](#)

## ActivClient Agent

The ActivClient Agent “watches” for smart card activity (insertion, activity, and removal), and starts ActivClient User Console among other ActivClient tools.

### ActivClient Agent icons on the taskbar

The ActivClient Agent icons display on the workstation’s taskbar:

-  A smart card is inserted in the smart card reader.
-  Your smart card reader is empty.
-  Your smart card is being used. Do not remove!
-  No smart card reader is present.

### ActivClient Agent shortcut menu commands

To display the following commands, right click the ActivClient Agent located on the Windows taskbar.

Table 3–4: ActivClient Agent Shortcut commands

Command	Description
Open	Opens ActivClient User Console.
Get One–Time Password	Generates a one–time password and copies it to the clipboard. OTP support must be installed.
PIN Change Tool	Opens the PIN Change tool to allow you to change your PIN.
PIN Initialization Tool	Opens the PIN Initialization Tool to allow you to initialize and choose a PIN code while erasing the content of your smart card.
Advanced Configuration Manager	Opens the Advanced Configuration Manager window to allow you to view and modify ActivClient configuration directly in ActivClient. Administrators can use this feature without using the Windows registry editor.
Advanced Diagnostics	Opens the Advanced Diagnostics wizard to allow you to perform a thorough examination of your environment and send information in an email to your help desk.
About	Open the About ActivClient window which displays information about ActivClient and your system.
Exit	Removes ActivClient Agent from the Windows taskbar. Smart card services remain available.



## User Console

The User Console helps you manage your logon credentials and certificates. For more information, refer to the *ActivClient CAC User Guide*.

You can	Action
Manage your digital certificates.	<ul style="list-style-type: none"><li>• Import a CA or User certificate</li><li>• Export a certificate</li><li>• View a certificate's attributes</li><li>• Delete a certificate</li><li>• Set as default</li><li>• Make Certificate available to Windows</li></ul>
Manage your one-time passwords.	<ul style="list-style-type: none"><li>• Generate a one-time password</li><li>• Resynchronize a one-time password</li><li>• Configure a user name for one-time password-based remote access</li></ul>
View your personal information.	Available for the US Department of Defense on Common Access Cards (CAC) or Personal Identity Verification (PIV) cards only.
Manage your smart card.	<ul style="list-style-type: none"><li>• View your smart card's properties</li><li>• Change your smart card's PIN</li><li>• Unlock your smart card</li><li>• View your unlock code</li><li>• Initialize your new smart card</li><li>• Reset your smart card</li><li>• Select a smart card reader</li></ul>

The User Console interface is comprised of secondary windows, menus, toolbars and of a right and left pane.

Table 3-5: User Console left and right panes

Pane	Description
Left pane or Tasks pane	<p>The Tasks pane (the default pane on the left) lists common tasks associated with the information in the right pane.</p> <p>You can switch between the Tasks and the Tree view by clicking the right and left arrows at the top of the pane.</p>
Right pane	<p>The right pane displays the content of your smart card. It provides access to:</p> <ul style="list-style-type: none"> <li>• Smart Card Info</li> <li>• My Certificates</li> <li>• CA Certificates</li> <li>• One-time passwords</li> <li>• My Personal Info</li> </ul>

Figure 3-1: Tasks view

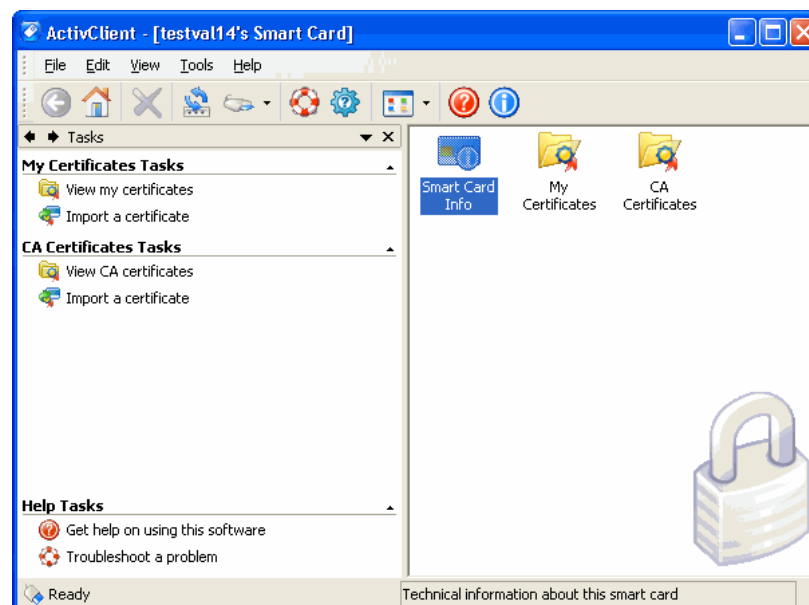
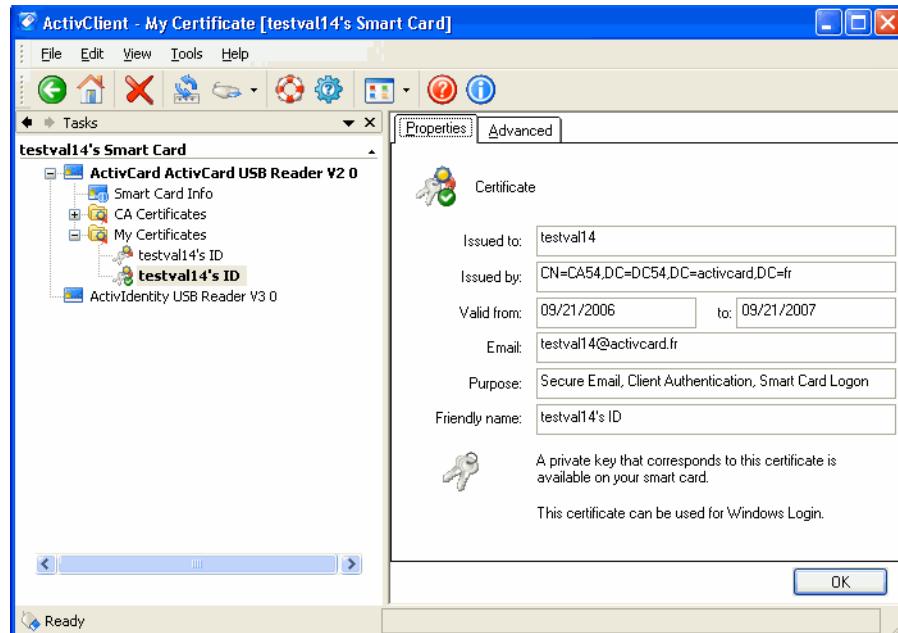


Figure 3-2: Tree view

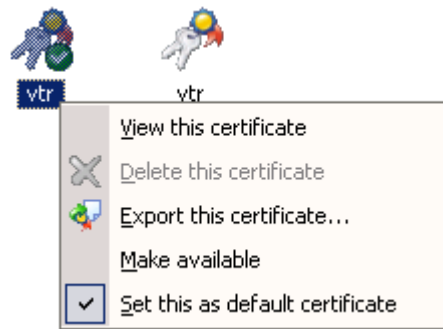


**Note:** Right-clicking some elements in the User Console usually displays a shortcut menu that provides support for the most common tasks. The displayed commands are different for each element.

## To access shortcut menu commands

Click inside the element that you want to work with, and then right click. A list of commands is displayed.

Figure 3–3: Right click menu of a user certificate



## The Menu toolbar

The **Menu** toolbar appears above the **Standard** toolbar in the User Console. Use the Menu toolbar to select menus and commands to perform actions in the software.

Figure 3-4: Menu toolbar

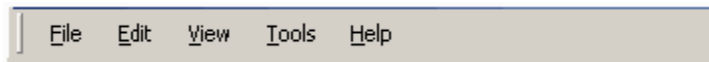


Table 3-6: Menus and commands from the Menu toolbar

Menu	Command	Function	Keystroke Shortcuts
File	Open	Opens selected object.	ENTER
	Delete	Deletes selected object.	DEL
	Import	Imports a certificate.	None
	Export	Exports a certificate.	None
	Use Reader	Specifies what smart card reader to use.	None
	Exit	Closes User Console session.	None
Edit	Paste	Inserts text from the clipboard.	SHIFT+INS
	Cut	Cuts selected text and places it on the Clipboard.	SHIFT+DEL
	Copy	Copies selected text to the Clipboard.	CTRL+C
	Select All	Selects all objects.	CTRL+A
View	Toolbars	Toggles which toolbars are displayed.	None
	Status Bar	Toggles status bar.	None
	Explorer Bar	Toggles between Tasks pane and Tree View pane.	None
	Large Icons	Displays large format icons.	None
	Small Icons	Displays small format icons.	None
	List	Displays objects in List format.	None
	Details	Displays objects in Detail format.	None
	Arrange Icons	Rearranges icons by name or type.	None
	Go to	Goes to specified page.	None
	Refresh	Refreshes current page.	F5

Menu	Command	Function	Keystroke Shortcuts
Tools	New Card	Sets PIN on a new smart card.	None
	Change PIN	Changes smart card PIN.	CTRL+E
	Unlock Card	Allows you to enter unlock code to unlock a locked smart card.	None
	Reset Card	Removes everything stored on smart card, including certificates.	None
	View Unlock Code	Allows you to view and save an unlock code; available after card is initialized with ActivClient.	None
	Advanced	Accesses advanced features: <ul style="list-style-type: none"> <li>• Configuration</li> <li>• Make Certificates Available to Windows</li> <li>• Log File Options</li> <li>• Forget state for all cards</li> </ul>	None
Help	ActivClient Help	Provides user access to ActivClient Online Help.	F1
	Troubleshoot	Starts Troubleshooting Wizard.	None
	Diagnose	Starts Diagnostics Tool.	None
	About ActivClient	Displays information about ActivClient and your system.	None

**Note:** Depending which ActivClient components you installed, some menus may not be available.

## The Standard toolbar











The **Standard** toolbar provides quick access to common functions in the User Console.

Figure 3–5: Standard toolbar



The following commands are available on the **Standard** toolbar:

Table 3-7: Standard toolbar commands

Button	Command	Function
	Back	Goes back to previous page.
	Home	Goes to home page.
	Delete	Deletes currently selected object.
	Change PIN	Changes smart card PIN.
	Reader List	Displays list of attached smart card readers.
	Run Troubleshoot Wizard	Starts Troubleshooting Wizard.
	Run Diagnostics Tool	Starts Diagnostics Tool.
	Views	Displays large or small format icons, or List or Detail format lists.
	Help	Provides user access to Online Help.
	About	Displays information about ActivClient and your system.

Refer to the *ActivClient CAC User Guide* to learn about the User Console Tasks.

## PIN Initialization Tool

The PIN Initialization Tool allows end users to initialize smart cards including setting a new PIN code.

- If the smart card is used in a standalone / Mini mode, see "[Standalone / Mini mode](#)" on page 20, then, re-initialize the smart card at any time. The card content is erased, and you can define a new PIN.
- If the smart card is used in a standalone mode, see "[Standalone mode](#)" on page 20, then:
  - if this is the first time you initialize the card, define the PIN. An unlock code is displayed for future use (in case you lock your smart card);
  - if the card has already been used, enter the PIN code or unlock code (when appropriate) in order to set a new PIN. The smart card content is erased.

## To access the PIN Initialization Tool

You can access the PIN Initialization Tool by doing either one of the following:


- From ActivClient Agent's right-click menu:  
Select **PIN Initialization Tool**.  
The PIN Initialization Tool is displayed.
- From the **Tools** menu of the User Console:  
Select **New Card**.  
The PIN Initialization Tool is displayed.
- From the Start menu:  
Go to Programs, ActivIdentity, ActivClient and select **PIN Initialization Tool**.  
The PIN Initialization Tool is displayed.

## PIN Change Tool

The PIN Change Tool allows end users to change their smart card PIN.

## To access the PIN Change tool

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

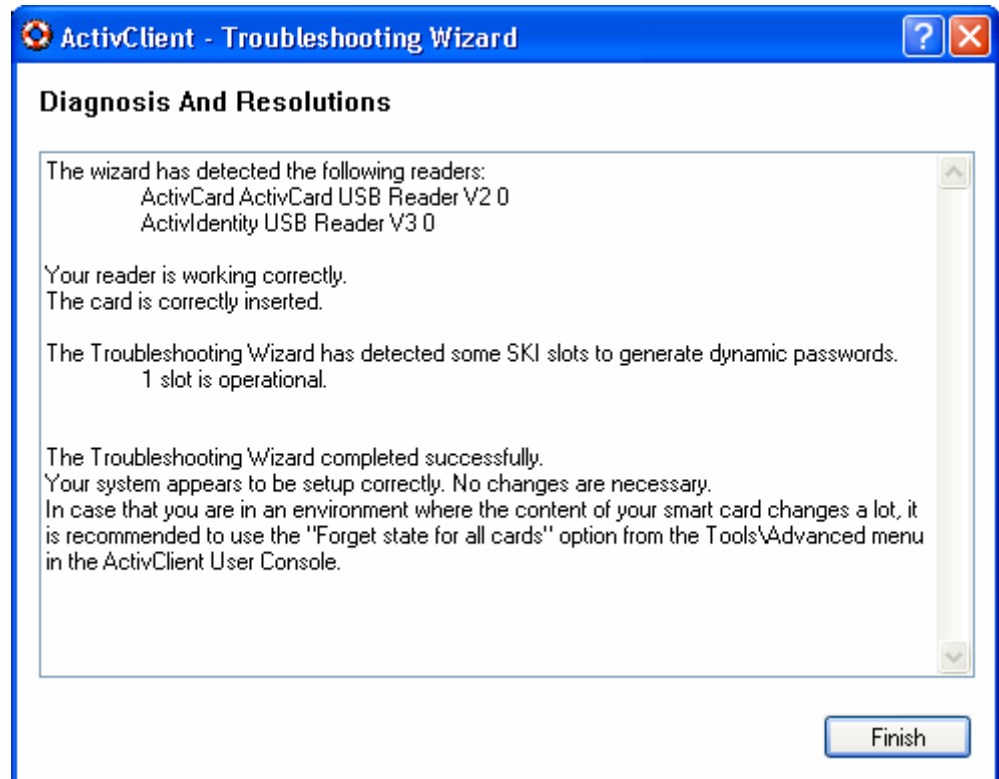
- From ActivClient Agent's right-click menu:  
Select **PIN Change Tool**.  
The PIN Change Tool wizard is displayed.
- From the **Standard** toolbar of the User Console:  
Select **Change PIN**  .  
The PIN Change Tool wizard is displayed.
- From the User Console's **Tasks** pane:  
Select **Change my smart card PIN**.  
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.



## Troubleshooting Wizard

The Troubleshooting Wizard helps resolve issues you may encounter while using a smart card with ActivClient. The wizard analyzes your system, diagnoses the problems, and then displays the results in the Diagnosis and Resolutions window, as illustrated in the following example.


Figure 3-6: Troubleshooting Wizard – Diagnosis and Resolutions window



## To access the Troubleshooting Wizard

You can access the Troubleshooting Wizard by doing either one of the following:

- From the User Console **Standard** toolbar:

Select the **Run Troubleshoot Wizard**  .  
The Troubleshooting wizard is displayed.

- From the **Help Tasks** section of the User Console:

Select **Troubleshoot a problem** task.

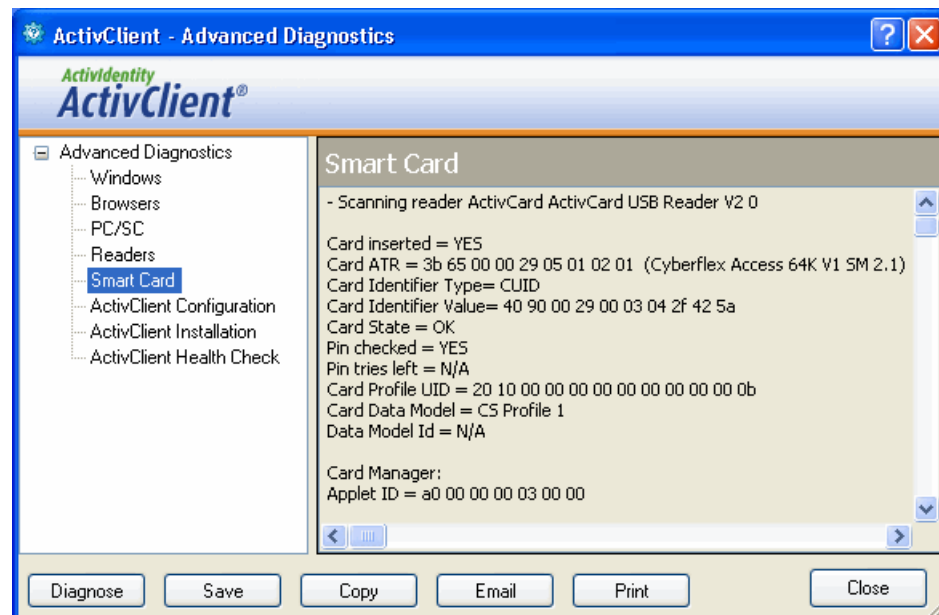
The Troubleshooting wizard is displayed.

- From the User Console **Help** menu:  
Select **Troubleshoot**.  
The Troubleshooting wizard is displayed.
- From the Start menu:  
Go to Programs, ActivIdentity, ActivClient and select **Troubleshooting**.  
The Troubleshooting wizard is displayed.

## Advanced Diagnostics


You can use the Advanced Diagnostics tool to diagnose a problem. If required, you can configure the tool to send the results in an email to the help desk.

Figure 3–7: The Advanced Diagnostics Tool



## To access the Advanced Diagnostics Tool

You can access the Advanced Diagnostics Tool by doing either one of the following:

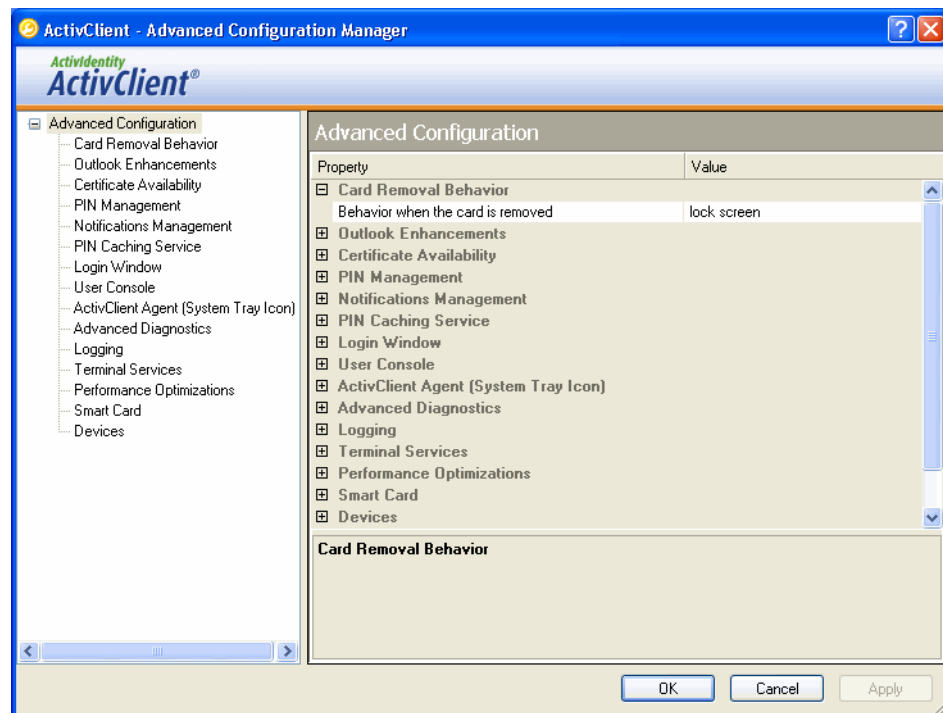
- From ActivClient Agent's right-click menu:  
Select **Advanced Diagnostics**.  
The Advanced Diagnostics wizard is displayed.
- From the User Console **Standard** toolbar:  
Select **Advanced Diagnostics** .  
The Advanced Diagnostics wizard is displayed.
- From the User Console **Help** menu:  
Select **Diagnose**.  
The Advanced Diagnostics wizard is displayed.
- From the Start menu:  
Go to Programs, ActivIdentity, and select **Advanced Diagnostics Tool**.  
The Advanced Diagnostics wizard is displayed.

## Advanced Configuration Manager

The Advanced Configuration Manager is used by administrators or end-users:

- Administrators use the Advanced Configuration Manager to view and modify ActivClient configuration through the interface.
- End-users use the Advanced Configuration Manager to activate log generation.

Figure 3–8: Sample output from the Advanced Configuration Manager.



## To access the Advanced Configuration Manager

You can access the Advanced Configuration Manager by doing either one of the following:

- From ActivClient Agent's right-click menu:  
Select **Advanced Configuration Manager**.  
The Advanced Configuration Manager window is displayed.
- From the Tools menu of the User Console:  
Select **Advanced** then, **Configuration**.  
The Advanced Configuration Manager window is displayed.
- From the Start menu:  
Go to Programs, ActivIdentity and select Advanced Configuration Manager.  
The Advanced Configuration Manager window is displayed.

**Note:** Information about how to configure ActivClient using the **Advanced Configuration Manager** can be found in the *ActivClient Customization and Deployment Guide*, included in the *ActivClient Resource Kit*.

# Chapter 4: Operational environment

This section provides details about:

- ["ActivIdentity products" on page 37](#)
- ["Operating systems" on page 37](#)
- ["Smart cards and USB tokens" on page 38](#)
- ["Smart card readers" on page 41](#)

## ActivIdentity products

ActivClient can be deployed in standalone mode. Combined with additional ActivIdentity products, it provides a fully comprehensive solution: the ActivIdentity Smart Employee ID.

The following table lists ActivIdentity products and their purpose.

**Table 4–8: ActivIdentity Products**

ActivIdentity Security Solution Components	Purpose
ActivClient	Smart Card Security client
SecureLogin SSO 6.1 64-bit edition	Single Sign-On
ActivID Card Management System (CMS) 3.8, 4.0 SP3, 4.1 for smart card issuance and management services.  <b>Note:</b> The "My Digital ID Card" component of CMS is only supported on 64-bit platforms with CMS 4.1	Card Management System
4Tress AAA Server 6.4.1 and 6.5	Authentication server

## Operating systems

The following are the operating systems on which ActivClient can be run.

- Microsoft Windows Vista (all 64-bit editions)

- Microsoft Windows Server 2003 (64-bit) SP1 and SP2

**Note:** If you are using a 32-bit operating system, contact your ActivIdentity reseller for a copy of the ActivClient (32-bit) edition.

## Smart cards and USB tokens

ActivClient supports the following smart cards and USB tokens.

The table below presents the configurations supported for each smart card.

For more details on ActivClient Services available in each configuration, see ["Smart card services and profiles" on page 20](#).

**Note:** Supported smart cards are also supported in additional configurations depending of specific profiles. Contact your ActivIdentity representative for further information.

Table 4–9: Supported Smart Cards and USB tokens

Supported Smart Cards and USB tokens	Standalone/Mini	Standalone	AAA Server Managed	CMS Managed	US DoD CAC	US Government PIV
ActivIdentity Smart Card 8K (Gemalto Cryptoflex 8K)		X	X			
ActivIdentity Smart Card 16K (Gemalto Cryptoflex 16K)		X	X			
ActivIdentity Smart Card 64K v1		X	X	X		
ActivIdentity Smart Card 64K v2	X	X	X	X		
ActivIdentity Smart Card 64K v2c	X	X	X	X		
ActivIdentity ActivKey v1 (Gemalto Cryptoflex 16K)		X	X			
ActivIdentity USB Key 32K v2	X	X	X	X		
ActivIdentity USB Key 64K v2		X	X	X		
ActivIdentity ActivKey SIM	X	X	X	X		
Atmel 6464C Pro 64k	X	X	X	X		
Gemalto Cyberflex Access 32K V2 #1				X		
Gemalto Cyberflex Access 32K V2 SM 7.2				X	X	
Gemalto Cyberflex Access 32K V4 SM 1.3				X		
Gemalto Cyberflex Access e-gate 32K				X		
Gemalto Cyberflex Access 64K V1 SM 2.1		X	X	X		
Gemalto Cyberflex Access 64K V1 Bio SM 3.1				X		
Gemalto Cyberflex Access 64K V1 SM 4.1				X	X	
Gemalto Cyberflex Access 64K v2a SM 2.3				X		
Gemalto Cyberflex Access 64K v2b SM 1.1				X		
Gemalto Cyberflex Access 64K v2c	X	X	X	X	X	
Gemalto Cyberflex Access 128K				X	X	
Gemalto GemXpresso 32K				X		
Gemalto GemXpresso PRO 64K FIPS v1 Dual ATR				X	X	
Gemalto GemXpresso PRO 64K R3 v1 Dual ATR				X		
Gemalto GemXpresso PRO 64K R3 FIPS V2				X	X	

Supported Smart Cards and USB tokens	Standalone/Mini	Standalone	AAA Server Managed	CMS Managed	US DoD CAC	US Government PIV
Gemalto GemXpresso PRO R3 E64 PK – Standard Version	X			X		
Gemalto GemCombi'Xpresso R4 E72 PK	X			X	X	
Gemalto GemCombi'Xpresso R4 E72 PK Standard				X		X
Giesecke & Devrient SmartCafe 32K v1				X		
Giesecke & Devrient SmartCafe Expert 32K v2.0				X		
Giesecke & Devrient SmartCafe Expert 64K FIPS–1024	X	X	X	X		
Giesecke & Devrient SmartCafe Expert 64K FIPS–2048	X			X		
Keycorp MULTOS 64K with StepNexus PIV Application v4.2.1						X
Oberthur Galactic 32K #1				X	X	
Oberthur Galactic 32K #2					X	
Oberthur CosmopolIC 32K V4				X	X	
Oberthur CosmopolIC 32K V4 Fast ATR				X		
Oberthur CosmopolIC 64K v5				X		
Oberthur CosmopolIC 64K V5.2	X	X	X	X	X	
Oberthur CosmopolIC 64K V5.2 Fast ATR				X		
Oberthur ID–One Cosmo 64K v5.2D Fast ATR with PIV application				X		X
Oberthur ID–One Cosmo 64K v5.2D Fast ATR with PIV application SDK				X		X
Oberthur ID–One Cosmo 64K v5.4				X		
Sagem Orga J–ID Mark 64 PIV with Sagem PIV Applet version 01						X

- Note:**
- CMS supports several profiles per smart card type. Refer to the CMS documentation for details.
  - CMS supports smart card issuance with both ActivIdentity v1 applets and ActivIdentity v2 applets, including FIPS 140–2 Level 3 configuration with encrypted PIN.
  - ActivClient supports 1024– and 2048–bit RSA keys on smart cards and USB tokens that support these cryptographic operations.



- Smart cards previously used with ActivCard Gold are supported with ActivClient – with the exception of ActivCard Gold profiles with the Match On Card functionality. Credentials not supported with ActivClient (e.g. QuickFill/Simple Sign On data) are ignored by ActivClient.

## Smart card readers

### ActivIdentity devices

- ActivIdentity USB Reader v2
- ActivIdentity USB Reader v3
- ActivIdentity PCMCIA Reader v2 (supported on Windows Vista x64, not supported on Windows Server 2003 x64)
- ActivIdentity ActivKey v2 (supported on Windows Vista x64, not supported on Windows Server 2003 x64)
- ActivIdentity ActivKey SIM

### Third-party devices

The following devices have been qualified by ActivIdentity on 32-bit platforms. Contact the device vendor to obtain a 64-bit driver for these devices:

- Dell Latitude D600, D800, and D900 and Dell Inspiron 600m with built-in reader
- Dell Keyboard REV A03
- Gemalto / Gemplus GEM PC 430
- IBM laptop with built-in smart card reader
- KSI 1451 keyboard with smart card & biometric reader
- O2micro 0Z773 rev A (Keyboard)
- Omnikey Cardman 3121 (USB)
- Omnikey Cardman 4040 (PCMCIA)
- Omnikey Cardman 5121 (Dual Interface) – in contact mode only
- Omnikey Cardman 5125 (Contact and HID) – in contact mode only
- Omnikey Cardman 5321 RFID (contact and contactless)
- Precise Biometrics 100MC (USB)
- Precise Biometrics 100MC BioKeyboard
- Precise Biometrics 100 PC-Card MC (with SCM SCR243 smart card reader)

- Precise Biometrics 100XS swipe reader
- Precise Biometrics 200 Series bio reader
- SCM Microsystems SPR 337 with biometric device
- SCM Microsystems SCR 338-04 (Keyboard)
- SCM Microsystems SCR 338-03
- SCM Microsystems SCR 3311
- SCM Microsystems SCR 3340 (ExpressCard format)
- SCM Microsystems SDI 010 (contact and contactless)

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

# Send us your comments

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

**Document:** ActivClient CAC Overview

**Document Reference:** AC/x64/CAC/O/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