

Overview

ActivClient for Windows 6.2

ACTIVIDENTITY

Table of Contents

Chapter 1: Introduction 6
About ActivClient 6
Services 7
Standards 7

Chapter 2: ActivClient Services 9
PKI Services 9
Remote Access and One-Time Password Services 11
Log on to Applications Using an OTP 12
Remote Session Services 12
Citrix XenApp Support 13
Supported Citrix Versions 13
Supported Services in a Citrix Environment 13
Microsoft Remote Desktop Protocol (RDP) Support 14
Supported Environments 14
Supported Services 14
Management Services for End Users 15
ActivClient User Console 15
Digital Certificates 15
One-Time Passwords 15
Personal Information 15
Smart Card PIN 16
Smart Card Initialization 16
Smart Card Lock/Unlock 16
Remote/Centralized Management 16
ActivClient Agent 16
Troubleshooting Wizard 17
Advanced Diagnostics 17
Log Files 17
Management Services for Administrators 17
Installation and Deployment 17
Policy Management 18
Smart Card Automatic Registration 18
Localization 18
Branding 18
Notification 19
ActivClient SDK 19
Smart Card Services and Profiles 19

Document Version 06.2.09 | ©2009 ActivIdentity, Inc.

Standalone / Mini Mode . . . 20
Standalone Mode . . . 20
AAA Server-Managed Mode . . . 20
CMS-Managed Mode . . . 20
US Department of Defense Common Access Card Mode . . . 21
US Government PIV Mode . . . 21

Chapter 3: ActivClient Components . . . 23
ActivClient Agent . . . 23
ActivClient Agent Icons in the Notification Area . . . 23
ActivClient Agent Shortcut Menu Commands . . . 23
User Console . . . 24
Access Shortcut Menu Commands . . . 27
Menu Toolbar . . . 27
Standard Toolbar . . . 29
PIN Initialization Tool . . . 30
Access the PIN Initialization Tool . . . 31
PIN Change Tool . . . 31
Access the PIN Change Tool . . . 31
Troubleshooting Wizard . . . 32
Access the Troubleshooting Wizard . . . 32
Advanced Diagnostics . . . 33
Access the Advanced Diagnostics Tool . . . 33
Advanced Configuration Manager . . . 34
Access the Advanced Configuration Manager . . . 34

Chapter 4: Operational Environment . . . 36
ActivIdentity Smart Employee ID . . . 36
System Requirements . . . 37
Operating Systems . . . 37
Virtualization Environments . . . 37
Smart Cards and USB Tokens . . . 37
Smart Card Readers . . . 40
ActivIdentity Smart Card Readers . . . 40
Third-Party Readers . . . 41

Appendix A: Terms and Acronyms . . . 44
Terms . . . 44
Acronyms . . . 45

List of Tables

Table 1.1: Supported Standards 7
Table 2.1: List of PKI Services 9
Table 2.2: Log on to Applications Using an OTP 12
Table 3.1: ActivClient Agent Shortcut Commands 23
Table 3.2: User Console Left and Right Panes 25
Table 3.3: Menus and Commands from the Menu Toolbar 28
Table 3.4: Standard Toolbar Commands 30
Table 4.1: ActivIdentity Products 36
Table 4.2: Supported Smart Cards and USB Tokens 38
Table 4.3: Driver Availability per Operating System 41

Document Version 06.2.09 | ©2009 ActivIdentity, Inc.

List of Figures

Figure 3.1: Tasks View 26
Figure 3.2: Tree View 27
Figure 3.3: User Certificate Right-Click Menu 27
Figure 3.4: Menu Toolbar 28
Figure 3.5: Standard Toolbar 29
Figure 3.6: Troubleshooting Wizard - Diagnosis and Resolutions Window 33
Figure 3.7: Advanced Diagnostics Tool - Report Window 34
Figure 3.8: Advanced Configuration Manager 35

Chapter 1: Introduction

In This Chapter

6 About ActivClient
7 Services
7 Standards

This guide provides an overview of ActivClient™ features and capabilities:

- ActivClient authentication, digital signature, encryption and associated card and credential management services
- ActivClient components that enable you to use these services
- Operational environment including the supported operating systems and authentication devices

This guide applies to all editions of ActivClient:

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

The differences related to specific editions are indicated where applicable.

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

About ActivClient

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

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

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

This document is for:

- System administrators
- Operators/end users
- People with knowledge of Microsoft® Windows® operating systems as well as some understanding of Public Key Infrastructure

Services

ActivClient provides the following range of services:

- PKI services
- Remote access and One-Time Password (OTP) services
- Remote session services
- Management services (for end users and administrators)
- Smart card services and profiles

For complete details of these services, see Chapter 2, "ActivClient Services," on page 9.

Standards

ActivClient supports the latest security algorithms and standards.

Table 1.1: 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
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	• U.S Government Smart Card Interoperability Specifications GSC-IS 2.1 • FIPS 201/PIV certified by NIST • U.S DoD CAC Middleware Requirements Release 3.0 • GSA Basic Services Interface (BSI) versions 1.8, 2.0 and 2.1 • FDCC/SCAP 1.1
Smart card Management	GlobalPlatform 2.0.1, 2.1 and 2.1.1
Setup	Windows Installer (MSI)

Table 1.1: Supported Standards

Feature	Description
Product Accessibility	Section 508 compliant
Microsoft Windows	Microsoft OEM Ready

Document Version 06.2.09 | ©2009 ActivIdentity, Inc.

Chapter 2: ActivClient Services

This chapter describes the authentication, digital signature, encryption and associated card and credential management services provided by ActivClient.

In This Chapter

9 PKI Services
11 Remote Access and One-Time Password Services
12 Remote Session Services
15 Management Services for End Users
17 Management Services for Administrators
19 Smart Card Services and Profiles

PKI Services

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

Table 2.1: List of PKI Services

Feature	Description
Windows logon	• Provides a digital certificate-based mechanism to log on to the domain on Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003 and Windows Server 2008 (and the relevant service packs) • Provides the ability to log off users or lock the workstation on smart card removal • Provides an automatic certificate registration to Windows on smart card insertion and optional removal on smart card removal • On Windows Vista, Windows 7 and Windows Server 2008, enables smart card logon with Fast User Switching
Remote access	• Microsoft Windows dialer on Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7 and Windows Server 2008 • Microsoft Windows VPN on Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7 and Windows Server 2008 • Check Point VPN-1 SecuRemote/SecureClient NG AI R56 HFA-03 and NGX R60 HFA-02 supplement 2 • Cisco VPN Client 4.6 and 5.0 • Cisco AnyConnect VPN Client 2.2 • Nortel Contivity VPN for Windows 6_07.027 and 7_01.280 • Other VPN clients supporting smart cards via CAPI or PKCS11 either in native 64-bit or 32-bit mode

Table 2.1: List of PKI Services

Feature	Description
Secure web access	Access to any web server with SSL v3 and a smart card-based digital certificate with the following browsers. *Microsoft Internet Explorer:* • Microsoft Internet Explorer 6.0 (no SP, SP1 or SP2) • Microsoft Internet Explorer 7 • Microsoft Internet Explorer 8 *Mozilla-based browsers:* • Firefox 1.5.0.4 • Firefox 2 • Firefox 3
Secure email	*Email signature, encryption/decryption:* • Microsoft Outlook 2000 SP3 (Office 2000) • Microsoft Outlook 2002 SP3 (Office XP) • Microsoft Outlook 2003 (no SP, SP1 or SP2) (Office 2003) • Microsoft Outlook 2007 (SP1 and SP2) (Office 2007) • Thunderbird 1.5.0.4 and 2.0 *Microsoft Outlook usability enhancements:* Automatic configuration of the Microsoft Outlook security profile, including: • Setting to "encrypt contents and attachments for outgoing messages" • Setting to "add digital signature to outgoing messages” • Setting to "send clear text signed message when sending signed messages” • Setting to "request S/MIME receipt for all S/MIME signed messages" • Automatic creation of the Outlook security settings by selection of the signature and encryption certificates on the smart card *Additional usability services:* • Automatic publication of users’ smart card-based certificates to the Global Address List (GAL) • Automatic addition of email senders' certificates to users’ Microsoft Outlook Contacts • Automatic decryption of encrypted emails (saving in decrypted form) • Automatic addition of Microsoft Outlook Security icons in the compose email windows

Note

The ActivClient PKCS#11 library is automatically registered in Firefox and Thunderbird during ActivClient installation (on Windows 32-bit platforms).

Table 2.1: List of PKI Services

Feature	Description
Encrypting file system	ActivClient supports the Encrypting File System (EFS) feature of Windows Vista and Windows Server 2008. With a smart card-based certificate, users can encrypt/decrypt files.
Entrust client software	ActivClient supports the following Entrust products: • Entrust Entelligence™ Desktop Solutions 6.1 SP2 and 7.0 (32-bit only) • Entrust Entelligence™ Security Provider for Windows 7.0 SP3, 7.1, 8.0 and 9.0 • Entrust Authority™ Administration Services 7.3 • Entrust Authority™ Security Manager 7.1 SP3 • Entrust Authority™ Security Manager Administration 7.1 SP3 • Entrust TruePass™ 8.0 (no SP and SP2) • Entrust Authority PKCS #7 Toolkit for C (aka File Toolkit) 6.1 • Entrust Authority GSS-API toolkit for C (aka Session Toolkit) 6.1 • Entrust Authority™ Security Toolkit for Java Version 7.2 SP1
Examples of other PKI enabled clients	ActivClient also supports other applications that provide PKI services with smart cards using the CAPI (Microsoft Crypto API) or PKCS#11 interfaces. For example: • Microsoft Office 2003 SP3 and 2007 (SP1 and SP2) that provide file signing capability. • Adobe Acrobat 8.0 and 9.0 • IBM Lotus Notes • Novell Certificate Login

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 OTPs to log on to applications requiring strong authentication via dialup, VPN or web. These OTP services require an ActivIdentity 4TRESS™ authentication server, such as the ActivIdentity 4TRESS AAA Server.

Log on to Applications Using an OTP

Users have several options to log on to an application using an OTP as described in Table 2.2:

Table 2.2: Log on to Applications Using an OTP

Feature	Description
Log on automatically with an OTP (32-bit platforms only)	ActivClient generates an OTP and submits it automatically to the application. ActivClient supports Check Point clients via the SAA API. Check Point VPN-1: • SecuRemote/SecureClient NG AI R56 HFA-03 • SecuRemote/SecureClient NGX R60 HFA-02 supplement 2
Log on automatically with an 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 an OTP in one-click	From the "Get One-Time Password" option in the ActivClient Agent (in the Windows notification area), ActivClient generates an OTP and copies it to the clipboard. Users simply paste it into any application.
Log on manually with an OTP	From the ActivClient User Console, ActivClient can generate OTPs in both synchronous and challenge/response modes. Users simply paste the OTP into any application.

Remote Session Services

ActivClient supports the following remote session environments:

- Citrix® XenApp™, previously known as Citrix Presentation Server
- Microsoft Remote Desktop Connection

In both environments, ActivClient for Windows is installed on the remote server or workstation (typically hosting Citrix XenApp or Windows Terminal Server). On the local workstation (Windows or other), only a smart card reader and PC/SC smart card reader driver are required.

For further information, see "Citrix XenApp Support" on page 13 and "Microsoft Remote Desktop Protocol (RDP) Support" on page 14.

Citrix XenApp Support

Supported Citrix Versions

ActivClient supports the following versions of Citrix XenApp, Citrix clients and Web Interface:

Citrix XenApp server:

- Citrix Presentation Server 4.0 with latest Hot Fix Rollup Pack (Rollup Pack 3 or later)
- Citrix Presentation Server 4.5 with latest Hot Fix Rollup Pack
- Citrix XenApp 5.0

Citrix clients:

- Program Neighborhood (Classic) on Windows 2000, Windows XP, Windows Server 2003, Windows Vista and Windows Server 2008. Available in:
  - Citrix Presentation Server Client Packager versions 9.2, 10.0, 10.2
  - Citrix XenApp plug-in version 11.0
- Program Neighborhood Agent on Windows 2000, Windows XP, Windows Server 2003, Windows Vista and Windows Server 2008. Available in:
  - Citrix Presentation Server Client Packager versions 9.2, 10.0, 10.2
  - Citrix XenApp plug-in version 11.0
- Web Interface. Available in:
  - Citrix Presentation Server Client Packager versions 9.2, 10.0, 10.2
  - Citrix XenApp plug-in version 11.0
- Thin terminals with Windows XP Embedded operating system and Citrix ICA Client 10.2 (or later)
- Thin Terminals with Windows-CE .NET 4.2 (or later) operating system and Citrix ICA Client 10.0 (or later)
- Thin Terminals with Wyse ThinOS™ 6.2 (or later) operating system
- On Mac OS X - Citrix Mac Client version 10.0
- On Linux - Citrix Linux Client version 10.6

Supported Services in a Citrix Environment

- The user can remotely log on to the Citrix Server machine with their 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

Supported Environments

ActivClient supports the following Remote Desktop Protocol (RDP) environments:

Servers:

- Windows Server 2003 Terminal Server
- Windows Server 2008 Terminal Server (including Terminal Services Web Access)

Clients:

- Remote Desktop Connection v5 or v6 on Windows XP, Windows Server 2003, Windows Vista, Windows 7 or Windows Server 2008
- Thin Terminals with Windows XP Embedded operating system
- Thin Terminals with Windows CE .NET 4.2 (or later) operating system
- Thin Terminals with Wyse ThinOS 6.2 (or later) operating system
- Sun™ Secure Global Desktop (SGD) 4.2 client - when configured to send RDP requests to a Windows Terminal Server (where ActivClient for Windows is installed)

Supported Services

- The user can log on with RDP client to a remote machine with their 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).

Management Services for End Users

The following management services are available to end users.

ActivClient User Console

The User Console allows users to view and manage 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 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 OTP credentials:

- Generate automatic OTPs (also known as synchronous mode)
- Generate challenge/response OTPs
- Synchronize counters for OTPs
- Configure user name for remote access with OTP

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

Document Version 06.2.09 | ©2009 ActivIdentity, Inc.

Smart Card PIN

At any time, the smart card PIN:

- Can be changed
- Is controlled by users

Smart Card Initialization

ActivClient allows users to initialize smart cards before they can be used. Depending on the smart card configuration, users can:

- 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 (that is, 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 users enter several incorrect PINs on the smart card, the smart card locks, preventing any further unauthorized use.

If the smart card is locked, users can unlock their card using:

- Static unlock code owned by users (stand-alone mode)
- Challenge/response-based unlock code provided by the help desk (requires ActivID™ CMS, 4TRESS Authentication Server or 4TRESS AAA Server)
- Online and seamless unlock method through the Self Service Portal (requires ActivID CMS)

Note

Depending on the smart card configuration, users can use the PIN Initialization Tool to re-initialize a card without following an unlock process.

Remote/Centralized Management

- Provides support for **My Digital ID Smart card**. ActivClient supports the self-service support interface of ActivID CMS.
- Allows you to securely update your organization's smart cards.
- ActivClient automatically checks if smart card updates are available in ActivID CMS and prompts users to update the smart card.

ActivClient Agent

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

Troubleshooting Wizard

Helps users 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.

Management Services for Administrators

In addition to the end-user services, administrators can also use the additional services provided by the ActivIdentity management products.

Installation and Deployment

ActivClient is available in two editions:

- ActivClient, which includes ActivClient 32-bit and ActivClient 64-bit
- ActivClient CAC, which includes ActivClient CAC 32-bit and ActivClient CAC 64-bit

The 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.

ActivClient can be deployed using software deployment technology:

- Microsoft SMS 2003 SP2 and R2
- Microsoft System Center Configuration Manager 2007
- Microsoft Active Directory push (Windows Server 2000, 2003 and 2008)

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

Note

ActivClient CAC includes and automatically installs the CA certificates relevant for the US Department of Defense Common Access Card deployment.

Policy Management

ActivClient offers a wide range of policies enabling organizations to optimize ActivClient to meet their usability and security requirements.

These policies:

- Are managed locally via Windows registries.
- Can be edited locally using the ActivIdentity Advanced Configuration Manager (also allows importing/exporting policies).
- Are managed centrally from Active Directory using Group Policies.
- Can be edited centrally from Active Directory using Administrative templates.

Smart Card Automatic Registration

Without any product update, ActivClient supports new Java Card, US DoD CAC or PIV smart card types that have successfully passed ActivIdentity qualification tests.

Localization

ActivClient is fully localizable. For localization methodology, contact your ActivIdentity reseller.

Branding

The User Console can be customized with customer-specific graphics.

Notification

ActivClient displays notification messages to help resolve common issues:

- The ‘No Smart Card Reader’ notification message is displayed above the Windows notification area at log on when there is no smart card reader connected to the PC or if it is inadvertently unplugged.
- The ‘Unattended Smart Card’ notification message is displayed above the Windows notification area to remind users to take their smart card with them when leaving the workstation. It is displayed only if the smart card has not been removed from the smart card reader and if users attempt to:
  - Log off
  - Lock the workstation
  - Shutdown the workstation
  - Restart the workstation
- The Expiration Warning message notifies users that their smart card or one of their smart card certificates is about to expire or has expired. It is displayed at:
  - Smart card insertion
  - Start of the user session if the smart card is inserted when logging on

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.

ActivClient SDK 6.1 is compatible with ActivClient 6.2. There is no ActivClient SDK 6.2 package.

Smart Card Services and Profiles

This section describes 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 applets.
- 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, users 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, new credentials can be downloaded onto the card.

Standalone Mode

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

AAA Server-Managed Mode

When 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, users 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 users to define a new PIN code while their credentials are preserved on the smart card.
- Users can reset the smart card completely (from the User Console) if they 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, users 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 users to define a new PIN code while their credentials are preserved on the smart card.
- Users can securely update the smart card content (applets and credentials) using the CMS Self Help Desk: My Digital ID Card.
- Users 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.

Supported with the following CAC models:

- CAC v1
- CAC v2 without CCC
- CAC v2 with CCC
- CAC Contactless Pilot (CCC+CHUID)
- CAC PIV transitional without a PIV Authentication Key
- CAC PIV transitional with a PIV Authentication Key not registered in the CCC (not activated in GSC-IS mode)
- CAC PIV transitional with a PIV Authentication key registered in the CCC (activated in GSC-IS mode)
- CAC PIV End Point with a PIV Authentication Key not registered in the CCC (not activated in GSC-IS mode)
- CAC PIV End Point with a PIV Authentication Key registered in the CCC (activated in GSC-IS mode)
- CAC PIV End Point with Secure Message Anonymous (SMA)

Note

Some CAC models are compatible with both GSC-IS and PIV FIPS 201.

ActivClient includes a policy to use such cards either in GSC-IS compliant mode (default configuration in ActivClient CAC) or in PIV compliant mode (default configuration in ActivClient).

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.
- ActivClient also supports PIV extensions (also known as PIV+). In this configuration, the PIV credentials are supported in ActivClient using standard PIV policies (for example, the PIN complies with the PIV PIN policies). The “extended” credentials (OTPs and additional PKI) are supported in ActivClient based on the card profile (for example, access rights for the extra certificates depend on the card profile defined in CMS).

Chapter 3: ActivClient Components

This chapter describes the ActivClient components.

In This Chapter

23 ActivClient Agent
24 User Console
30 PIN Initialization Tool
31 PIN Change Tool
32 Troubleshooting Wizard
33 Advanced Diagnostics
34 Advanced Configuration Manager

ActivClient Agent

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

ActivClient Agent Icons in the Notification Area

The ActivClient Agent icons display in the Windows notification area:


A smart card is inserted in the smart card reader


Smart card is being used. Do not remove!


Smart card reader is empty


No smart card reader is present


ActivClient is starting up

ActivClient Agent Shortcut Menu Commands

To display the following commands, left or right-click the ActivClient Agent icon in the Windows notification area.

Table 3.1: ActivClient Agent Shortcut Commands

Command	Description
Open	Opens the ActivClient User Console
Get One-Time Password	Generates an OTP and copies it to the clipboard. OTP support must be installed and the card must be configured for OTP.
PIN Change Tool	Opens the PIN Change tool to change the PIN.

Command	Description
PIN Initialization Tool	Opens the PIN Initialization Tool to initialize and choose a PIN code while erasing the content of the smart card.
Advanced Configuration Manager	Opens the Advanced Configuration Manager window to view and modify the ActivClient configuration directly in ActivClient. Administrators can use this feature without using the Windows registry editor.
Advanced Diagnostics	Opens the Advanced Diagnostics wizard to thoroughly examine of the environment and send information in an email to the help desk.
About	Opens the About ActivClient window which displays information about ActivClient and the system.
Exit	Closes ActivClient Agent in the Windows notification area. Smart card services remain available.

User Console

The User Console helps manage logon credentials and certificates. For further information, refer to the *ActivClient for Windows User Guide.*

You can	Action
Manage your digital certificates	• Import a CA or User certificate • Export a certificate • View a certificate's attributes • Delete a certificate • Set as default • Make Certificate available to Windows • Add your certificates to the Global Address List (GAL)
Manage your one-time passwords	• Generate an OTP • Resynchronize an OTP • Configure a user name for OTP-based remote access

You can	Action
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	• View your smart card's properties • Change your smart card's PIN • Unlock your smart card • View your unlock code • Initialize your new smart card • Reset your smart card • Select a smart card reader

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

Table 3.2: User Console Left and Right Panes

Pane	Description
Left pane or Tasks pane	The Tasks pane (the default pane on the left) lists common tasks associated with the information in the right pane. Users can switch between the Tasks and the Tree view by clicking the right and left arrows at the top of the pane.
Right pane	The right pane displays the content of the smart card. It provides access to: • Smart Card Info • My Certificates • CA Certificates • One-time passwords • My Personal Info

Figure 3.1: Tasks View

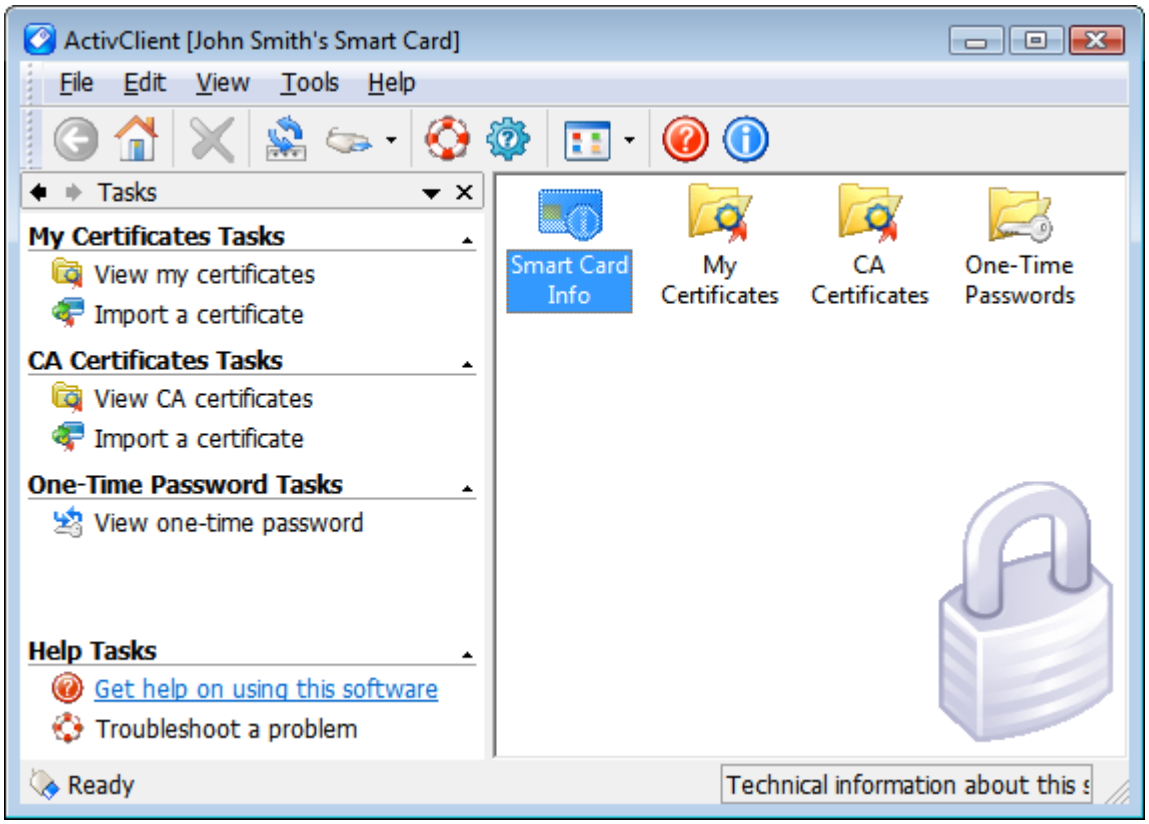
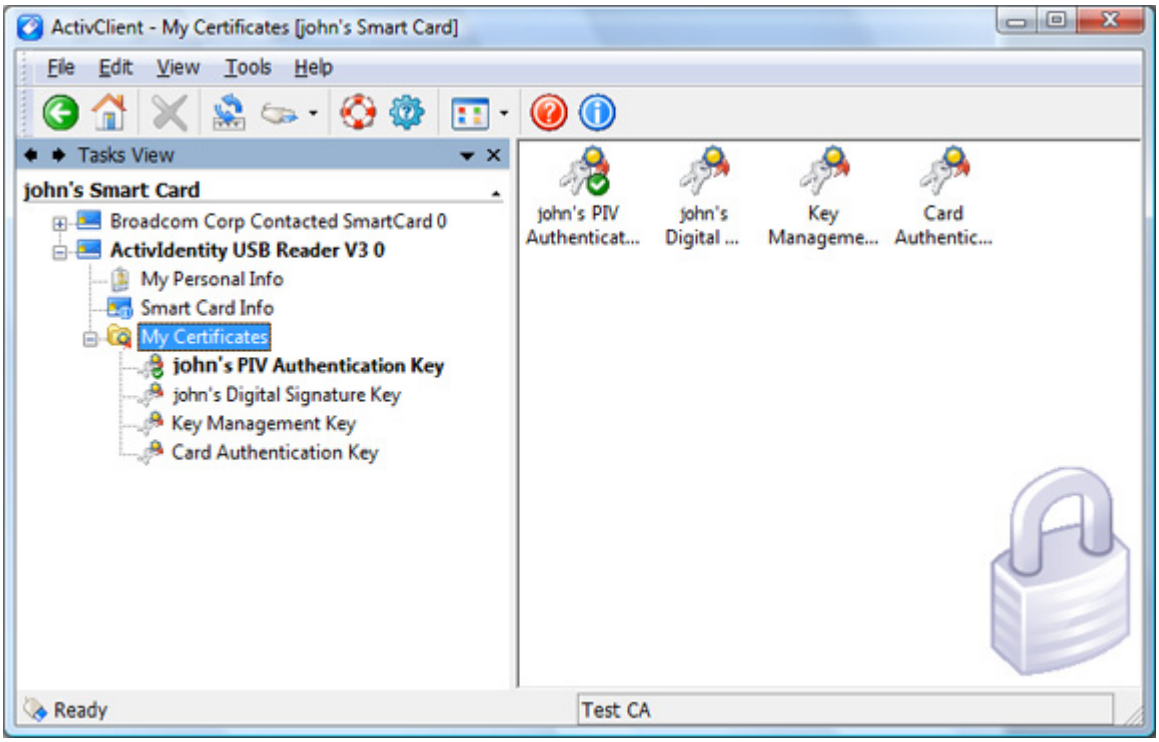


Figure 3.2: Tree View



Access Shortcut Menu Commands

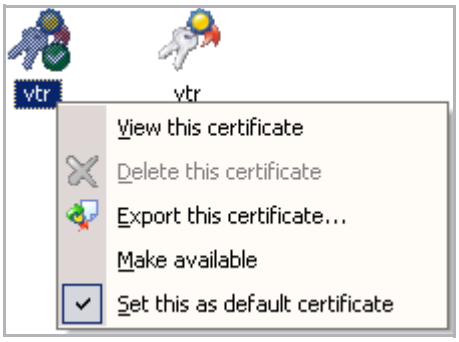
When the users right-clicks on a credential, a command menu is displayed.

Shortcut menus

Right-clicking some elements in the User Console displays a shortcut menu that provides support for the most common tasks.

The displayed commands are different for each element.

Figure 3.3: User Certificate Right-Click Menu



Menu Toolbar

The **Menu** toolbar appears above the **Standard** toolbar in the User Console. It can be used to select ActivClient menus and commands.

Figure 3.4: Menu Toolbar

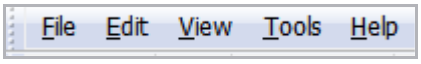


Table 3.3: Menus and Commands from the Menu Toolbar

Menu	Command	Function	Keyboard 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

Note

Depending the ActivClient components you installed, some menus may not be available.

Menu	Command	Function	Keyboard shortcuts
Tools	New Card	Sets PIN on a new smart card	None
	Change PIN	Changes smart card PIN	CTRL+E
	Unlock Card	Allows to enter unlock code to unlock a locked smart card	None
	Reset Card	Removes everything stored on the smart card, including certificates	None
	View Unlock Code	Allows to view and save an unlock code. Available after card is initialized with ActivClient	None
	Advanced	Accesses the advanced features: • Configuration • Make Certificates Available to Windows • Publish to GAL • Check for Card Update • Log File Options • Forget state for all cards	None
Help	ActivClient Help	Provides user access to ActivClient Online Help	F1
	Troubleshoot	Starts the Troubleshooting Wizard	None
	Diagnose	Starts the Diagnostics Tool	None
	About ActivClient	Displays information about ActivClient and the system	None

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 3.4: 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 the Troubleshooting Wizard
	Run Diagnostics Tool	Starts the 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 the system

For further information about the User Console tasks, see the *ActivClient for Windows User Guide*.

PIN Initialization Tool

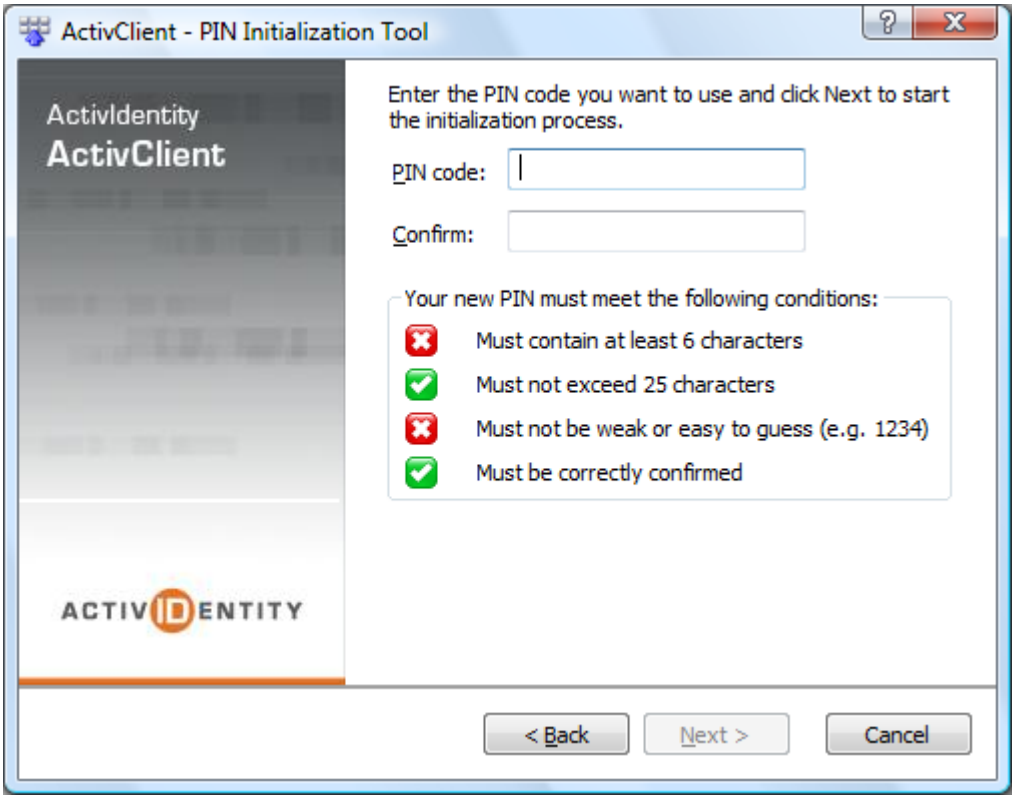
The PIN Initialization Tool allows users to initialize smart cards, including setting a new PIN code.

- If the smart card is used in a standalone / Mini mode, see "Standalone / Mini Mode" on page 20, re-initialize the smart card at any time. The card content is erased, and the user 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 the card is initialized, define the PIN. An unlock code is displayed for future use (in case the user locks the 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.

Access the PIN Initialization Tool

Users can access the PIN Initialization Tool either:

- From the ActivClient Agent's left or right-click menu, select **PIN Initialization Tool**.
- From the **Tools** menu of the User Console, select **New Card**.
- From the **Start** menu, go to Programs, ActivIdentity, ActivClient and select **PIN Initialization Tool**.



PIN Change Tool

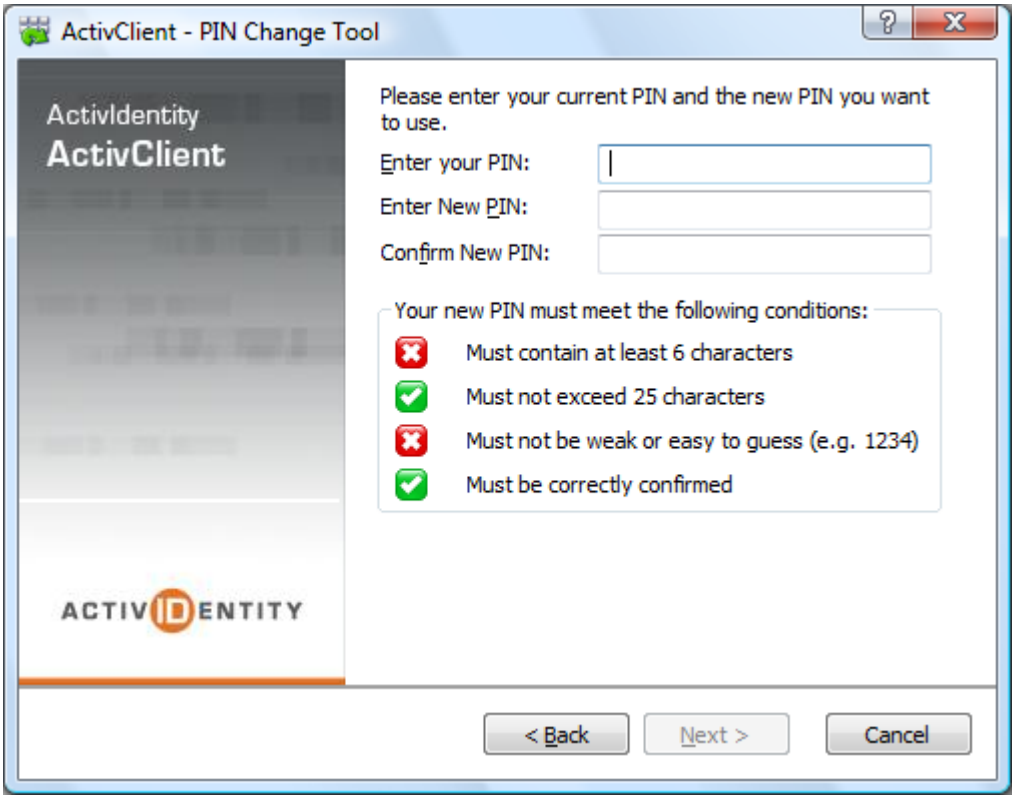
The PIN Change Tool allows users to change their smart card PIN.

Access the PIN Change Tool

Users can access the PIN Change tool either:

- From ActivClient Agent's left or right-click menu, select **PIN Change Tool**.
- From the **Standard** toolbar of the User Console, select **Change PIN**  .

- From the User Console's **Tasks** pane, select **Change my smart card PIN**.
- From the **Start** menu, go to **Programs**, **ActivIdentity**, **ActivClient**, and select **PIN Change Tool**.



Troubleshooting Wizard

The Troubleshooting Wizard helps resolve issues encountered while using a smart card with ActivClient. The wizard analyzes the system, diagnoses the problem, and then displays the results in the Diagnosis and Resolutions window, as illustrated in Figure 3.6.

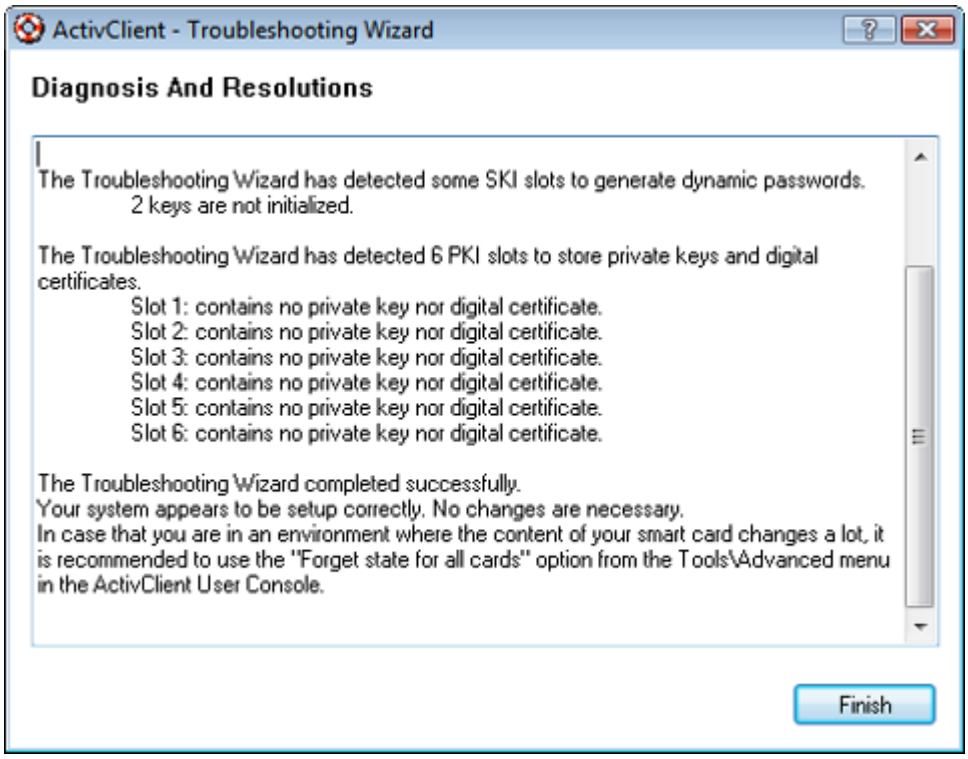
Access the Troubleshooting Wizard

Users can access the Troubleshooting Wizard either:

- From the User Console **Standard** toolbar, select the **Run Troubleshoot Wizard** .
- From the **Help Tasks** section of the User Console, select **Troubleshoot a problem** task.
- From the User Console **Help** menu, select **Troubleshoot**.

- From the **Start** menu, go to **Programs**, **ActivIdentity**, **ActivClient and select Troubleshooting**.

Figure 3.6: Troubleshooting Wizard - Diagnosis and Resolutions Window



Advanced Diagnostics

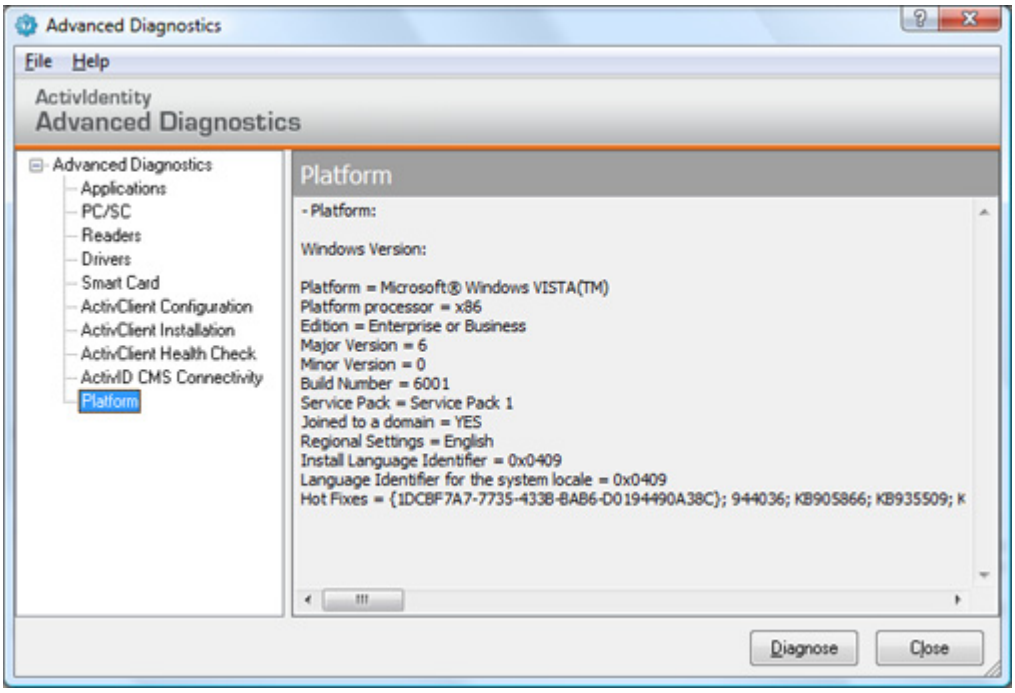
Users can use the Advanced Diagnostics tool to diagnose a problem. If required, the tool can be configured to send the results to the help desk by email.

Access the Advanced Diagnostics Tool

Users can access the Advanced Diagnostics Tool either:

- From ActivClient Agent's left or right-click menu, select **Advanced Diagnostics**.
- From the User Console **Standard** toolbar, select **Advanced Diagnostics** .
- From the User Console **Help** menu, select **Diagnose**.
- From the **Start** menu, go to **Programs**, **ActivIdentity**, and select **Advanced Diagnostics Tool**.

Figure 3.7: Advanced Diagnostics Tool - Report Window



Advanced Configuration Manager

The Advanced Configuration Manager is used by administrators to view and modify ActivClient configuration through the interface.

Access the Advanced Configuration Manager

Administrators can access the **Advanced Configuration Manager** either:

- From ActivClient Agent's left or right-click menu, select **Advanced Configuration Manager**.
- From the Tools menu of the User Console, select **Advanced** then, **Configuration**.
- From the Start menu, go to Programs, ActivIdentity and select **Advanced Configuration Manager**.

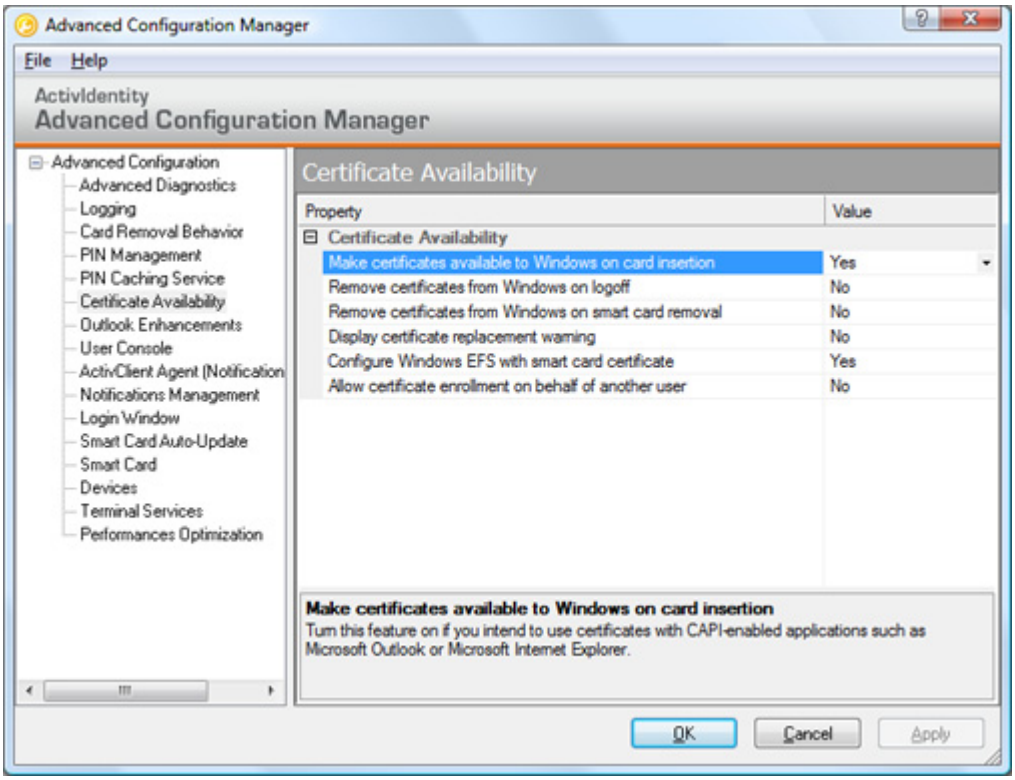
Note

As the Advanced Configuration Manager is an administrative tool, it is not installed by default (except in ActivClient CAC editions).

ActivClient Configuration

For instructions on how to configure ActivClient using the **Advanced Configuration Manager**, see the *ActivClient Administration Guide*.

Figure 3.8: Advanced Configuration Manager



Chapter 4: Operational Environment

This chapter details the ActivClient operational environment.

In This Chapter

36 ActivIdentity Smart Employee ID
37 Operating Systems
37 Smart Cards and USB Tokens
40 Smart Card Readers

ActivIdentity Smart Employee ID

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

Table 4.1 lists the compatible ActivIdentity products and their purpose.

Table 4.1: ActivIdentity Products

ActivIdentity Smart Employee ID Components	Purpose
ActivClient	Smart card security client
ActivIdentity Authentication Client (AAC) 2.0.1	Add-on to ActivClient providing: • Smart Card Password Login, enabling users to log on to Windows with username/ password stored on the card • Emergency Access, enabling users to log on to Windows with questions and answers when the smart card is forgotten or lost • Automated logon to Cisco VPN Client with an OTP generated on a smart card
SecureLogin SSO 6.1 and 6.2 (32-bit and 64-bit editions) (Latest hotfix is optional)	Single Sign-On
ActivID Card Management System (CMS) 3.8, 4.0 SP3, 4.1 and 4.2 **Note:** On 64-bit platforms, the "My Digital ID Card" component of CMS is only supported with CMS 4.1 and 4.2	Card Management System for smart card issuance and management services
4TRESS AAA Server 6.5 and 6.6	Authentication server

System Requirements

The minimum system requirements for ActivClient installation are:

- One of the supported operating systems listed below
- 64 MB of RAM
- 45 MB of free disk space

Note

ActivClient 6.2 has been tested with release candidate versions of Windows 7 and Windows Server 2008 R2.

ActivIdentity will perform further compatibility tests with Windows 7 and Windows Server 2008 R2 after Microsoft releases these products.

Operating Systems

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

- Microsoft Windows 2000 (SP4) - 32-bit
- Microsoft Windows XP Professional (SP1, SP2 and SP3) - 32-bit
- Microsoft Windows XP Home Edition (SP2 and SP3) - 32-bit
- Microsoft Windows Vista (no SP, SP1 and SP2) (all editions) - 32 and 64-bit
- Windows 7 (all editions) - 32 and 64-bit
- Microsoft Windows Server 2003 (SP1, R2 and SP2) - 32 and 64-bit
- Microsoft Windows Server 2008 (no SP, SP2 and R2) - 32 and 64-bit

Virtualization Environments

ActivClient is supported in the following virtual environment when ActivClient is run on one of the supported operating systems:

- VMware® Workstation 6.5

Smart Cards and USB Tokens

Table 4.2 presents the smart cards and USB tokens supported by ActivClient and the configurations supported for each device.

For more details on ActivClient Services available in each configuration, see "Smart Card Services and Profiles" on page 19.

Note

The smart cards are also supported in additional configurations depending on specific profiles. Contact your ActivIdentity representative for further information.

Table 4.2: 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 Smart Card 144K	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		
Athena IDProtect Duo PIV						X
Atmel 6464C Pro 64k	X	X	X	X		
CardLogix Credentsys-J PIV						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		

Notes

- CMS supports several profiles per smart card type. For further information, see the CMS documentation.
- 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 (that is, QuickFill/ Simple Sign On data) are ignored by ActivClient.

Table 4.2: 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
Gemalto Cyberflex Access 64K v2c	X	X	X	X	X	
Gemalto Cyberflex Access 128K				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	
Gemalto GemXpresso PRO R3 E64 PK - Standard Version	X			X		
Gemalto TOP DL GX4 144K FIPS	X			X	X	X
Gemalto TOP DM GX4 72K (FIPS)	X			X	X	
Gemalto TOP DM GX4 72K (FIPS) Standard #1				X		X
Gemalto TOP DM GX4 72K (FIPS) Standard #2				X		
Giesecke & Devrient SmartCafe 32K v1				X		
Giesecke & Devrient SmartCafe Expert 32K v2.0				X		
Giesecke & Devrient SmartCafe Expert 64K Non-FIPS				X		
Giesecke & Devrient SmartCafe Expert 64K FIPS-1024	X	X	X	X		
Giesecke & Devrient SmartCafe Expert 64K FIPS-2048	X			X		
Giesecke & Devrient SmartCafe Expert 80K DI v3.2	X	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		

Table 4.2: 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
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		
Oberthur ID-One Cosmo 128K v5.5					X	
Oberthur ID-One Cosmo v7.0 80K	X	X	X	X		
Oberthur ID-One Cosmo v7.0 128K	X	X	X	X		
Safenet 400 PIV						X
Sagem Orga J-ID Mark 64 PIV with Sagem PIV Applet version 01						X

Smart Card Readers

ActivClient supports any PC/SC certified smart card reader, from ActivIdentity and from third-party vendors.

ActivIdentity Smart Card Readers

Table 4.3 lists the supported ActivIdentity smart card readers and their Windows platform compatibility. For each reader and operating system, the table indicates where you can find the latest drivers, either:

- In Windows (Win) or via Windows Update (WU)
- If ActivIdentity provides a driver for it in the ActivIdentity Device Installer (AIDI), in the \Extras folder
- If it is a Generic Microsoft CCID driver integrated natively in the OS (CCID)

ActivKey Display v2 used with ActivClient in connected mode

- When ActivKey Display is connected, ActivClient can generate OTPs on the device. This is the same "credential" as displayed on the LCD when ActivKey Display is used in offline mode. OTP generation is not PIN-protected, but a server-based PIN may be used.
- When ActivKey Display is connected, ActivClient can use it to store / retrieve the static credentials for a Windows logon (username, password and domain). This credential is PIN protected. This feature is compatible with ActivIdentity Authentication Client 2.0.
- When ActivKey Display is connected and configured with an optional SIM module, ActivClient will use the SIM module for all credentials except for the OTP which is still managed directly in the ActivKey Display (same credential as displayed on the LCD).

Table 4.3: Driver Availability per Operating System

OS	Win 2000		Win XP		Server 2003 32-bit		Server 2003 64-bit		Vista and Win 7 32-bit		Vista and Win 7 64-bit		Server 2008 32-bit		Server 2008 64-bit	
Devices	**Win**	**AIDI**	**Win**	**AIDI**	**Win**	**AIDI**	**Win**	**AIDI**	**Win**	**AIDI**	**Win**	**AIDI**	**Win**	**AIDI**	**Win**	**AIDI**
USB Reader v2	WU	Yes	WU	Yes	CCID	Yes	CCID	No	CCID	No	CCID	No	CCID	No	CCID	No
USB Reader v3	WU	Yes	WU	Yes	CCID	Yes	CCID	No	CCID	No	CCID	No	CCID	No	CCID	No
PCMCIA Reader v1	WU	Yes	WU	Yes	No	No	No	No	No	No	No	No	No	No	No	No
PCMCIA Reader v2	WU	Yes	WU	Yes	WU	Yes	WU	Yes	WU	Yes	WU	Yes	WU	Yes	WU	No
ActivKey v1 and v2	No	Yes	WU	Yes	WU	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	No
ActivKey SIM and Display	WU	Yes	WU	Yes	CCID	Yes	CCID	No	CCID	No	CCID	No	CCID	No	CCID	No
Serial Reader	No	Yes	No	Yes	No	Yes	No	No	No	No	No	No	No	No	No	No

Third-Party Readers

ActivClient supports any third-party PC/SC certified smart card reader. Make sure you install the latest firmware and driver for your smart card reader. Check Windows Update and your vendor's web site for the latest available version.

As an example, the following is a list of third-party readers compatible with ActivClient:

- Compaq® keyboard (with O2micro 0Z773 rev A chip set)

- Dell®:
  - Inspiron 600m laptop with built-in reader (O2Micro O2711EC1 PCMCIA chip set)
  - Latitude D series laptop with built-in reader (O2Micro O2711EC1 PCMCIA chip set or O2Micro OZ77Cxx USB SmartCard Controller)
  - Latitude E series laptop with built-in reader (Broadcom controller)
  - Keyboard REV A03 with smart card reader
  - 104-Key USB Keyboard with smart card reader for Dell OptiPlex / Precision Workstations
- Gemplus®:
  - GemPC 430 (USB)
  - GemPC 432 (USB)
  - GemPC 433-SL, GemPC 433-SW (USB)
  - GemPC USB-SL reader
  - GemPC USB-SW reader
- Hewlett-Packard® keyboard (with SCM Microsystems SCR338-04 smart card reader)
- IBM® laptop with built in smart card reader
- KSI® 1451/ASC keyboard
- Omnikey®:
  - Cardman 3121 (USB)
  - Cardman 4040 (PCMCIA)
  - Cardman 5121 (dual interface) - supported in contact mode only
  - Cardman 5125 (contact and HID Prox) - supported in contact mode only
  - Cardman 5321 (dual interface) - supported in contact mode only
- Precise™ Biometrics:
  - 100MC (USB)
  - 100MC BioKeyboard
  - 100 PC-Card MC (with SCM Microsystems SCR243 smart card reader)
  - 100XS swipe reader
  - 200MC (USB)
- Schlumberger® Reflex 20 PCMCIA reader

- SCM Microsystems:
  - SDI010 (dual interface) - supported in contact mode only
  - SCR331 (USB)
  - SCR3310 (USB)
  - SCR3311 (USB)
  - SCR3340 (ExpressCard)
  - SCR338-03 (bundled in keyboards)
  - SCR338-04 (bundled in keyboards)
  - SPR337 (with fingerprint sensor)

Appendix A: Terms and Acronyms

In This Appendix

44 Terms
45 Acronyms

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

Terms

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

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

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

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

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

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

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

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

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

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

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

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

Acronyms

Acronym

What does it stand for

CA

Certificate Authority

CAC

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

CSP

Cryptographic Service Provider

FIPS

Federal Information Processing Standard

GAL

Global Address List

GP

GlobalPlatform

Replaces OpenPlatform (OP).

OTP

One-Time Password

PKI

Public Key Infrastructure

PIV

Personal Identity Verification

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

RA

Registration Authority

SKI

Symmetric Key Infrastructure

Document Version 06.2.09 | ©2009 ActivIdentity, Inc.

Document Information

ActivIdentity, Inc. welcomes your comments and suggestions.

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

Product: ActivClient for Windows

Document: ActivClient for Windows Overview

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

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

Document Version 06.2.09 | ©2009 ActivIdentity, Inc.

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

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

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