ActivID® ActivClient® for Windows User Guide

DOCUMENT REFERENCE: AC_WIN_7.1_UG_07.2016

PRODUCT VERSION: 7.1

JULY 2016



hidglobal.com

Copyright

© 2008-2016 HID Global Corporation/ASSA ABLOY AB. All rights reserved. This document may not be reproduced, disseminated or republished in any form without the prior written permission of HID Global Corporation.

Trademarks

HID, HID Global, the HID Blue Brick logo, the Chain Design and 4TRESS, ActivIdentity and ActivID are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission. The absence of a mark, product, service name or logo from this list does not constitute a waiver of the HID Global trademark or other intellectual property rights concerning that name or logo. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

Revision History

Date	Description	Document Version
July 2016	Initial release of rebranded document and major technical updates.	1.0

Contacts

Americas		Asia Pacific
United States: +1 510.574.0100	U.S. Federal: +1 571.522.1000	+61 (0) 3.9809.2892
Europe		**Corporate**
+33 (0) 1.42.04.84.00		+1 800.237.7769

Technical Support

If you purchased your product from a third party, then please contact that third party for Technical Support. For products purchased directly from HID Global, please go to http://www.hidglobal.com/support

Typographic and Document Conventions

Typography	Description
blue	Cross-references within the document.
blue, underline	References to external web addresses.
bold	Action steps (paths, buttons, options); field and drop-down list labels; emphasis.
italic	File names, document titles, and file extensions.
`Code snippets`	Highlights `code snippets` within regular content.
`Code samples`	`Highlights code samples`
	**WARNING**: This symbol indicates a critical warning. It applies to actions that if taken or not taken will break the system. Read the warning carefully and follow it.
	**Important**: This symbol indicates something very important to the reader. Ignore this symbol at your own risk.
	**Note**: This symbol indicates a note that should be of interest to the reader. It is not critical. Nevertheless, the reader should pay attention.

Table of Contents

List of Tables **7**

1.0 Introduction **8**

1.1 Product Overview 8
1.2 Document Scope and Audience 8

2.0 Getting Started **9**

2.1 Your First Steps with ActivClient 9
2.2 Using the ActivClient Agent 10
2.2.1 ActivClient Agent Icons in the Notification Area 10
2.2.2 ActivClient Agent Shortcut Menu Commands 11
2.3 Working with the User Console 11
2.3.1 What You Can Do With the User Console 11
2.3.2 Access the User Console 12
2.3.3 ActivClient in the New Microsoft Windows Interface 13

3.0 Managing Smart Cards **15**

3.1 Initializing a Smart Card with the PIN Initialization Tool 15
3.1.1 Supported Smart Cards 15
3.1.2 Access the PIN Initialization Tool 15
3.1.3 Initialize Your Smart Card using the PIN Initialization Tool 16
3.2 Reset a Smart Card 17
3.3 Change Your Smart Card PIN 19
3.4 Unlock Your Smart Card 22
3.4.1 View Your Unlock Code 23
3.4.2 Access the Unlock Smart Card Dialog 23
3.4.3 Unlock a Smart Card Initialized with ActivClient 24
3.4.4 Unlock a Smart Card in the ActivClient User Console 25
3.5 Unlock a Smart Card using the Microsoft Windows Interface 26
3.5.1 Access the Microsoft Windows Unblock Screen 26
3.5.2 Unblock Your Smart Card 27
3.6 Update Your Smart Card 28
3.6.1 Automatic Check for Updates 28
3.6.2 Manually Check for Updates 29
3.7 Smart Card or Certificate Expiration 30
3.8 View Smart Card Information 31

4.0 Managing Digital Certificates **33**

4.1 Download a Certificate with Microsoft Internet Explorer 33
4.2 Download a Certificate with Mozilla Firefox 34
4.3 Managing User and CA Certificates 34
4.3.1 View Your Certificate 34
4.3.2 Import a User Certificate 36
4.3.3 Import a CA Certificate 37
4.3.4 Export a Certificate 38

4.3.5 Delete a Certificate 39
4.3.6 Set a Default Certificate 39
4.3.7 Deselect a Logon Certificate 40
4.4 Managing Certificates in Microsoft Outlook 41
4.4.1 Automatically Configure Your Microsoft Outlook Security Profile 41
4.4.2 Automatically Publish Your Certificates to the Global Address List 41
4.4.3 Automatically Add Certificates to Microsoft Outlook Contacts 42

5.0 Using Digital Certificates 43

5.1 Log On to Windows with a Certificate 43
5.2 Lock Your Workstation on Smart Card Removal 44
5.3 Use Windows Dial-Up/VPN for Remote Access 44
5.4 Use a Non-Microsoft VPN for Remote Access 45
5.5 Access a Secure Web Site 45
5.5.1 Access a Secure Web Site with Internet Explorer, Microsoft Edge or Google Chrome 45
5.5.2 Access a Secure Web Site with Firefox 46
5.6 Send/Read Signed and Encrypted Email Messages with Microsoft Outlook 46
5.6.1 Send/Read Signed Email Messages 46
5.6.1.1 Send Signed Email Messages 47
5.6.1.2 Read Signed Email Messages 47
5.6.2 Send/Read Encrypted Email Messages 47
5.6.2.1 Send Encrypted Email Messages 47
5.6.2.2 Read Encrypted Email Messages 48
5.6.2.3 Automatically Decrypt and Save Emails 48
5.7 Send/Read Signed and Encrypted Mails with Thunderbird 49
5.7.1 Send/Read Signed Email Messages 49
5.7.2 Send Signed Email Messages 49
5.7.3 Read Signed Email Messages 49
5.8 Send/Read Encrypted Email Messages 50
5.8.1 Send Encrypted Email Messages 50
5.8.2 Read Encrypted Email Messages 50
5.9 Encrypt/Decrypt Files with EFS 51
5.9.1 Configure Your Workstation for EFS and Select/Generate a Smart Card Encryption Certificate 51
5.9.2 Encrypt a File or Folder with EFS 51
5.9.3 Decrypt a File or Folder with EFS 52
5.9.4 Update EFS Certificates and Re-Encrypt Files 52
5.9.5 Recover Encrypted Files 53
5.10 Encrypt Drives with BitLocker To Go 54
5.10.1 Protect the Data Drive with Your Smart Card 54
5.10.2 Access the Protected Drive 54

6.0 Managing Remote Access/OTP 55

6.1 Synchronize Your Smart Card 55
6.2 Configure Your Remote Access User Name 56

7.0 Using Remote Access/OTP 57

7.1 Automatically Generate a One-Time Password 57
7.2 Manually Generate a One-Time Password 58

8.0 Viewing Personal Information 61

8.1 About Personal Information 61
8.2 View “My Personal Info” 61

9.0 Using and Managing ActivClient 63

9.1 View ActivClient System Information 63
9.2 Perform Advanced Diagnostics 64
9.3 Use the Reset optimization cache Option 66
9.4 Activate Log Files 66
9.5 View ActivClient Policy Settings 67
9.6 Auto-Update Service 69
9.7 Select a Smart Card Reader 69

10.0 Using ActivClient with Terminal Services 70

10.1 Citrix XenApp Sessions 70
10.1.1 Access a Citrix Published Application via Web Interface 70
10.1.2 Access an Application with the Citrix Online Plug-In for Windows 71
10.2 Microsoft Remote Desktop Sessions 72
10.2.1 Log On to a Microsoft Remote Desktop Session 72
10.2.2 Use Your Smart Card in a Microsoft Remote Desktop Session 72
10.3 Disconnect a Remote Desktop Session 73

Appendix A: Terms and Acronyms 74

A.1. Terms 74
A.2. Acronyms 76

List of Tables

Table 1: Getting Started According to Your Smart Card Status 9
Table 2: ActivClient Agent Shortcut Commands 11
Table 3: Overview of the ActivClient User Console Tasks 11
Table 4: Smart Card Unlock Actions 22

1.0 Introduction



ActivID® ActivClient® guards against an ever-changing threat landscape by providing organizations with risk-appropriate and secure access to corporate IT assets.

1.1 Product Overview

HID Global's ActivID ActivClient is the latest smart card and USB token middleware from that allows enterprise and government customers to easily use smart cards and USB tokens to protect workstations and networks.

ActivClient enables the use of PKI certificates and keys and one-time passwords 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

1.2 Document Scope and Audience

This guide presents how to use ActivClient for authentication using your smart card.

It also explains how to manage your smart card credentials and ActivClient itself.

2.0 Getting Started

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

2.1 Your First Steps with ActivClient

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

Your first steps with ActivClient are determined by your:

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

Table 1 lists the actions to take according to your smart card status:

Table 1: Getting Started According to Your Smart Card Status

Smart card status	Action
You have a blank smart card (no PIN)	Your administrator has given you a blank smart card. **You need to initialize the card before you can use it.** 1. Log on to your workstation using the same user name and password that you used before installing ActivClient. 2. Initialize your new smart card and create your PIN, see Managing Smart Cards on page 15. 3. Load credentials on to your smart card as described in Managing Digital Certificates on page 33. 4. Use your card to log on to your workstation (if your administrator instructs you to do so), sign emails, access secure Web sites, etc.
Your smart card is personalized with a PIN but is not configured for Windows PKI logon	Your administrator has given you a smart card and a PIN, and the smart card has already been personalized with your credentials (for example, with digital certificates – but not configured for Windows logon). **Your card is ready to use.** 1. Log on to your workstation using the same user name and password you used before installing ActivClient. 2. Use your card to sign emails, access secure Web sites, etc.

Smart card status	Action
Your smart card is personalized with a PIN and a Windows PKI logon digital certificate	Your administrator has given you a smart card and a PIN, and the smart card has already been personalized with your credentials (including a digital certificate configured for Windows logon). **Your card is ready to use.** 1. Log on to your workstation using your smart card and your PIN. For more information, see 5.1 Log On to Windows with a Certificate on page 43. 2. Use your card to sign emails, access secure Web sites, etc.

At any time, you can access the ActivClient User Console to configure ActivClient, your smart card, or your credentials. For more information, see section 2.3 Working with the User Console on page 11.

2.2 Using the ActivClient Agent

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

2.2.1 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 the card until the icon turns green!

 Smart card reader is empty

 No smart card reader is detected

 ActivClient is starting up

2.2.2 ActivClient Agent Shortcut Menu Commands

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

Table 2: 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 Initialization Tool	Opens the PIN Initialization Tool to initialize and choose a PIN code while erasing the content of the smart card.
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.

2.3 Working with the User Console

2.3.1 What You Can Do With the User Console

Table 3: Overview of the ActivClient User Console Tasks

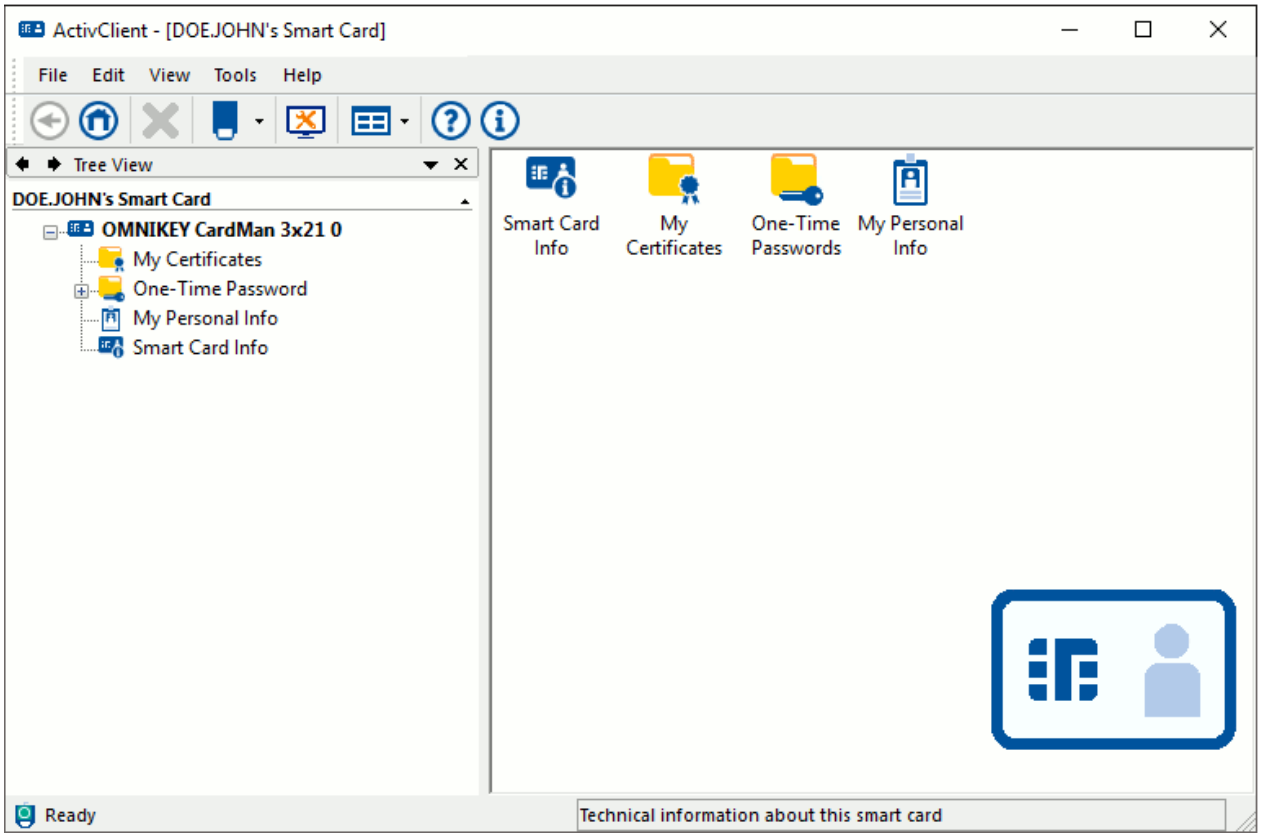
You can…	See
Manage your digital certificates	• Import a CA Certificate on page 37 • Import a User Certificate on page 36 • Export a Certificate on page 38 • View Your Certificate on page 34 • Delete a Certificate on page 39 • Set a Default Certificate on page 39 • Automatically Publish Your Certificates to the Global Address List (GAL) on page 41

You can…	See
Manage your one-time passwords	• Automatically Generate a One-Time Password on page 57 or Manually Generate a One-Time Password on page 58 • Synchronize Your Smart Card on page 55 • Configure Your Remote Access User Name on page 56
View your personal information *Only available for the US Department of Defense on Common Access Cards (CAC) or US Government Personal Identity Verification (PIV) cards.*	Viewing Personal Information on page 61
Manage your smart card	• View Smart Card Information on page 31 • Unlock Your Smart Card on page 22 • Initialize Your Smart Card using the PIN Initialization Tool on page 16 • Reset a Smart Card on page 17 • Update Your Smart Card on page 28 • View Your Unlock Code on page 23 • Select a Smart Card Reader on page 69
Use ActivClient tools to diagnose issues	• Perform Advanced Diagnostics on page 64 • View ActivClient Policy Settings on page 67

2.3.2 Access the User Console

To access the User Console, either:

- From the ActivClient Agent icon located in the Microsoft Windows notification area:
  - Double-click the ActivClient Agent icon .
  - Left or right-click on the ActivClient Agent icon  and select **Open**.
- From the Start menu, go to the programs or apps directory, and select **User Console** under **ActivID ActivClient**.
- In the Start page of the Microsoft Windows ‘modern’ interface, click on the **User Console** tile .

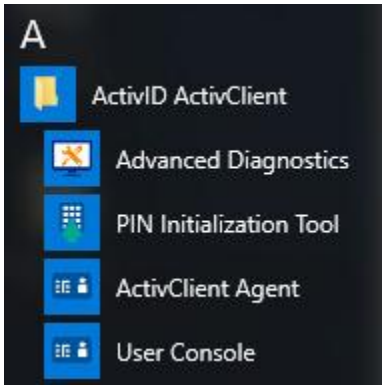


For more information on the ActivClient User Console, see the *ActivID ActivClient for Windows Overview*.

2.3.3 ActivClient in the New Microsoft Windows Interface

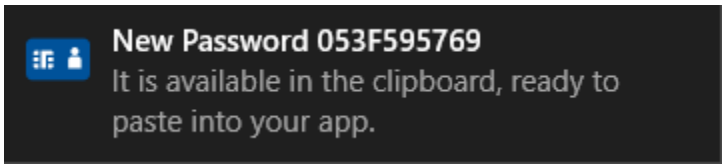
The ActivClient tools and notification features have been adapted to the new Microsoft Windows 'modern' interface.

The ActivClient Agent and tools are displayed as tiles. Simply click the required tile to launch a tool:



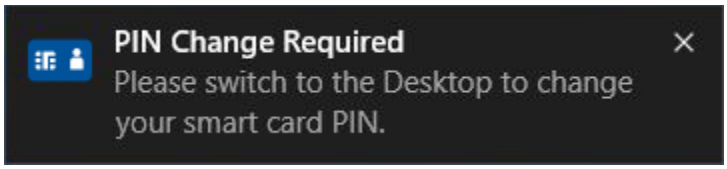
ActivClient notifications are displayed as 'toast' notifications, sliding in from the top right corner of the interface. They are visible for 24 seconds before they disappear.

For example – **Get One-Time Password**:



Some operations require that you manually switch to the Desktop, by clicking on the Desktop tile, in order to access the necessary window or tool.

For example – **PIN Change**:



3.0 Managing Smart Cards

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

3.1 Initializing a Smart Card with the PIN Initialization Tool

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

The PIN Initialization Tool allows you to:

- Initialize your smart card by setting a PIN code.
- Reset a PIN code while erasing the content of the smart card.
- Before initializing, you need to verify that your smart card is supported by the tool.

Important

- Repeated attempts to initialize a smart card that is not in a supported configuration can render the smart card permanently unusable.
- If the smart card is already initialized, the PIN Initialization Tool will reformat the card – all content present on the card (including private keys) will be permanently deleted.

3.1.1 Supported Smart Cards

PIN Initialization Tool supports blank and standalone smart cards:

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

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

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

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

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

3.1.2 Access the PIN Initialization Tool

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

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

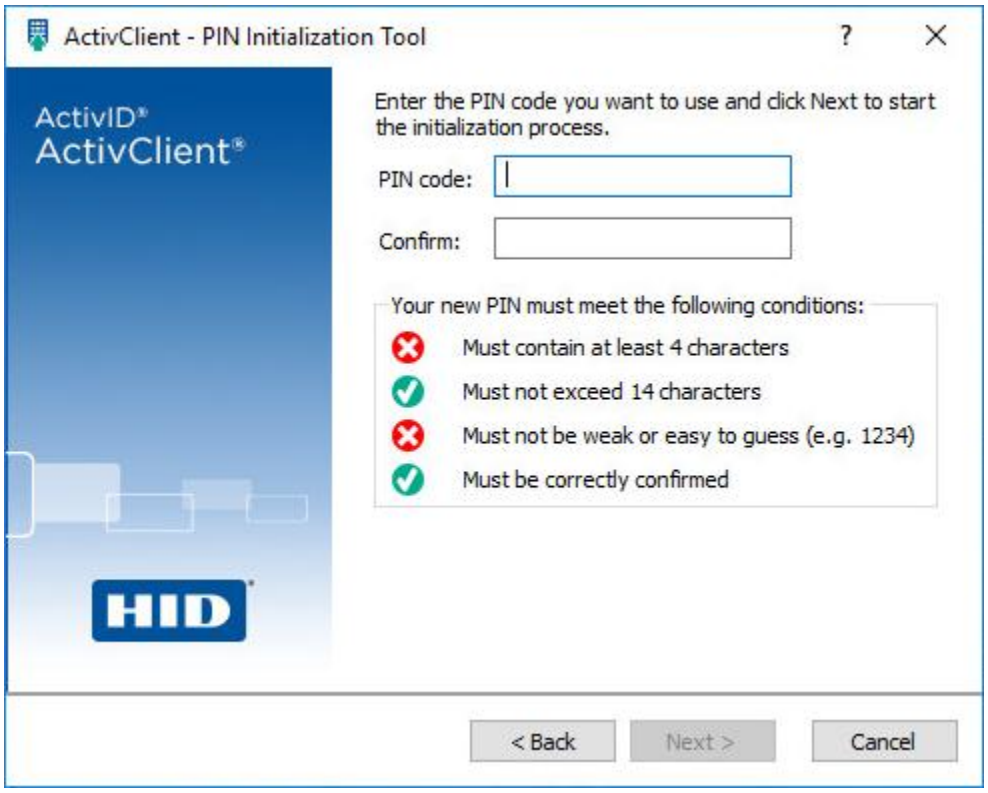
- From the Start menu, go to the programs or apps directory, and select **PIN Initialization Tool** under **ActivID ActivClient**.

- In the Start page of the Microsoft Windows 'modern' interface, click on the **PIN Initialization Tool** tile .

3.1.3 Initialize Your Smart Card using the PIN Initialization Tool

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

1. Start the PIN Initialization Tool (see 3.1.2 Access the PIN Initialization Tool on page 15).
2. Follow the wizard's instructions.



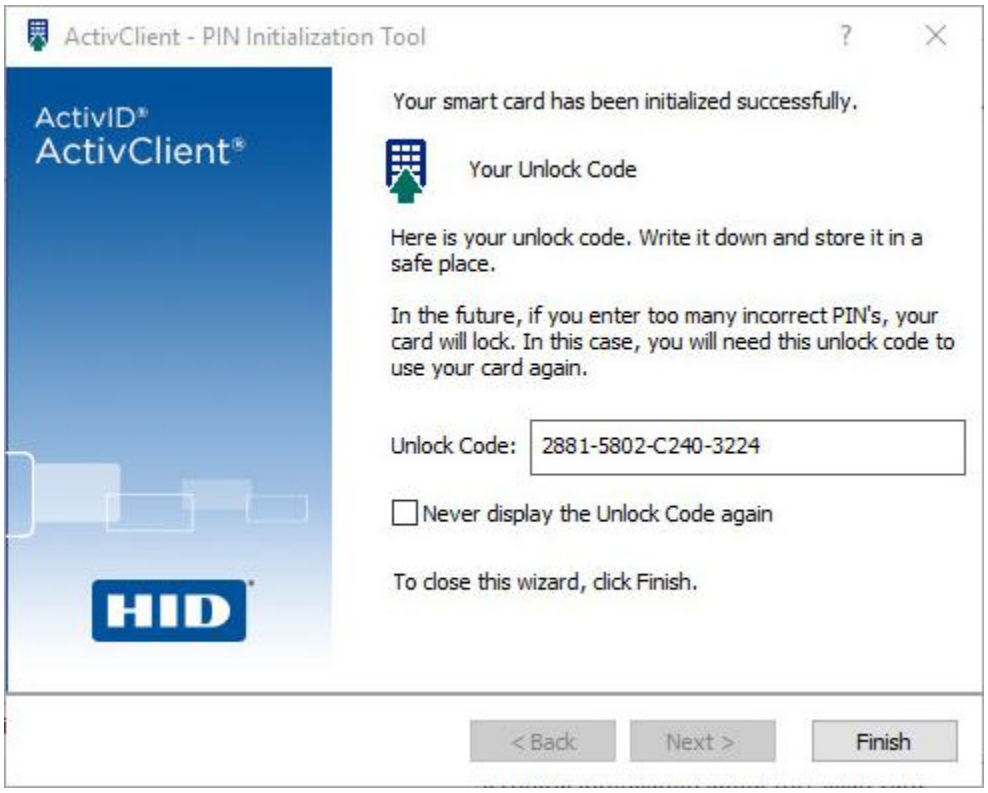
PIN Selection Rules

- Enter a PIN that is easy for you to remember, but difficult for others to guess!
- The PIN code must meet the PIN conditions displayed by the tool.

  All the conditions must display a green check for the PIN Initialization Tool to let you proceed.

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

   When the initialization is complete, the Finish window is displayed.



5. If an unlock code is displayed, write it down in a secure location.

Important: Entering too many wrong PIN codes will lock your smart card!

Make sure you view your unlock code and write it down in a secure place before you inadvertently lock your smart card.

6. Click **Finish** to close the tool.

3.2 Reset a Smart Card

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

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

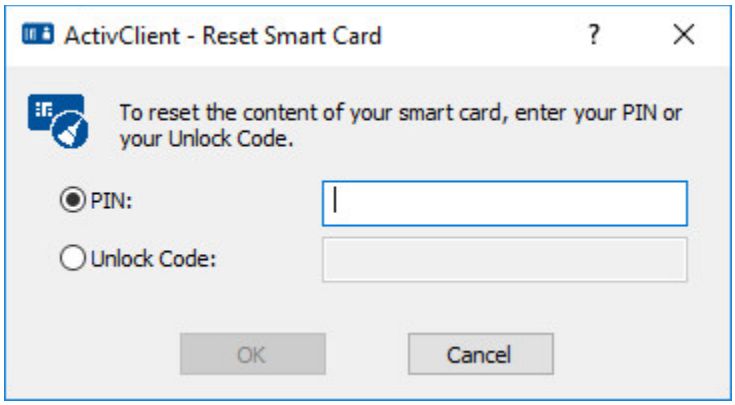
Notes:

- Depending on how your card was initialized, you might not have access to the reset function.
- You can also "Reset" and "Re-initialize" your smart card using the PIN Initialization tool. The tool also allows you to reset your PIN in the same process.

1. Open the ActivClient User Console.
2. Insert your smart card (chip-side up and chip first) into the smart card reader.

3. Click **Reset Card** from the **Tools** menu.
4. When a confirmation message is displayed, click **Yes**.

   The Reset Smart Card dialog box is displayed.



Unlock Code

For more information, see section 3.4.1 View Your Unlock Code on page 23.

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

3.3 Change Your Smart Card PIN

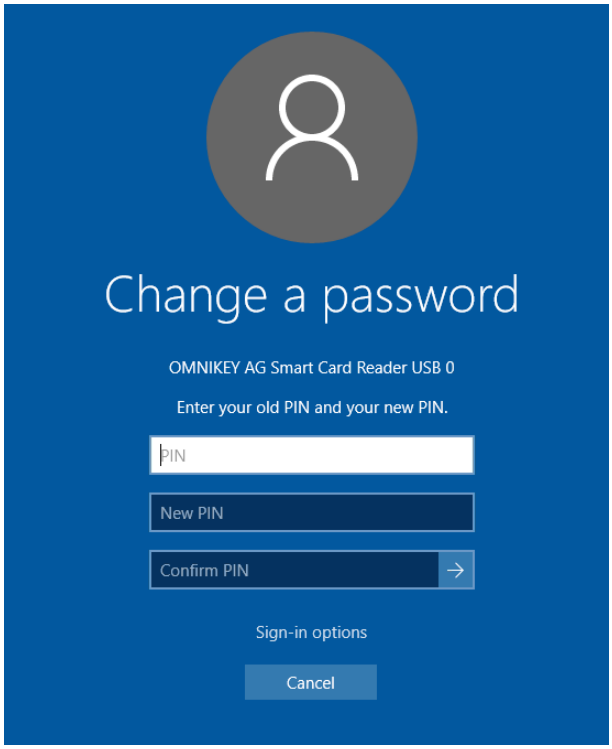
You should change your smart card PIN regularly to make sure that you are the only person accessing your smart card.

ActivClient includes a smart card mini driver that enables you to change your smart card PIN directly from the Microsoft Windows user interface.

Note: Your workstation must be part of a domain.

1. From your Microsoft Windows desktop, press **Ctrl+Alt+Del**.
2. Select **Change a password**.

- If the **Smart card PIN Change** dialog is displayed:



a. Enter your old PIN code and then enter and confirm your new PIN code.

b. Click the arrow button to apply the change.

Note: Use a PIN that complies with the PIN rules in place in your deployment.

- If the **Change a password** dialog is displayed:



a. Select either **Sign-in options** or **Other credentials** (depending on your system).



b. Select the smart card tile.



c. Enter your old PIN code and then enter and confirm your new PIN code.

d. Click the arrow button  to apply the change.

Note: Use a PIN that complies with the PIN rules in place in your deployment.

3.4 Unlock Your Smart Card

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

The unlock procedure depends on the method used to initialize your smart card as explained in Table 4.

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

Table 4: Smart Card Unlock Actions

Initialization method	Unlock procedure
If you initialized your smart card directly with ActivClient in standalone mode	You are also responsible for the unlock code. You should view your unlock code and save it in a secure location. This unlock code helps you unlock the smart card if you lock it by entering multiple incorrect PINs. See: • 3.4.1 View Your Unlock Code on page 23. • 3.4.2 Access the Unlock Smart Card Dialog on page 23.
If you received an already initialized smart card	Your administrator/help desk is responsible for your unlock code. See section 3.4.4 Unlock a Smart Card in the ActivClient User Console on page 25.
If your smart card was initialized with ActivClient in a Standalone / Mini mode	There is no code as the smart card cannot be unlocked. However, you can re-initialize your smart card with the PIN Initialization Tool. See section 3.1.3 Initialize Your Smart Card using the PIN Initialization Tool on page 16.

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

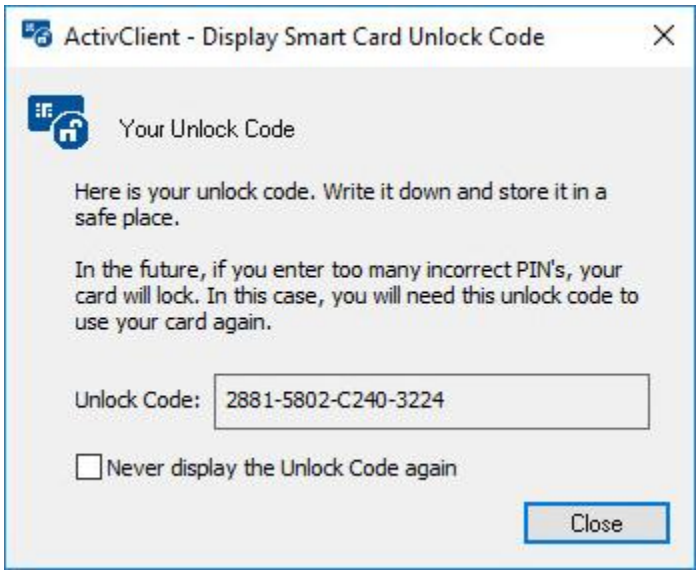
3.4.1 View Your Unlock Code

Prerequisites

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

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

   The Display Smart Card Unlock Code dialog box is displayed.
2. Enter your PIN code when prompted.



3. Write down your unlock code and save it in a secure location.

   You need this unlock code in case you lock your smart card in the future.
4. Click **Close** to return to the User Console.

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

Consequently, your Unlock Code will never display again!

Locked Smart Cards

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

3.4.2 Access the Unlock Smart Card Dialog

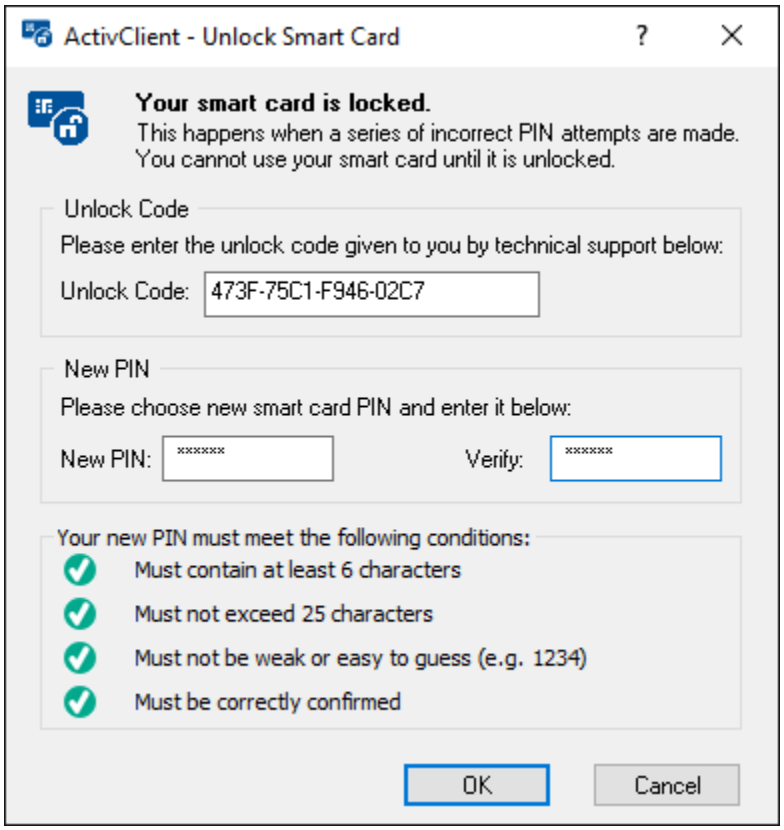
If the unlock dialog box does not automatically display, you can manually initiate the unlock process.

1. From the ActivClient User Console Tools menu, select **Unlock Card**.
2. Re-insert the locked smart card into your smart card reader.
3. Depending on the unlock dialog displayed, see either:
   - 3.4.3 Unlock a Smart Card Initialized with ActivClient on page 24

- 3.4.4 Unlock a Smart Card in the ActivClient User Console on page 25

3.4.3 Unlock a Smart Card Initialized with ActivClient

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



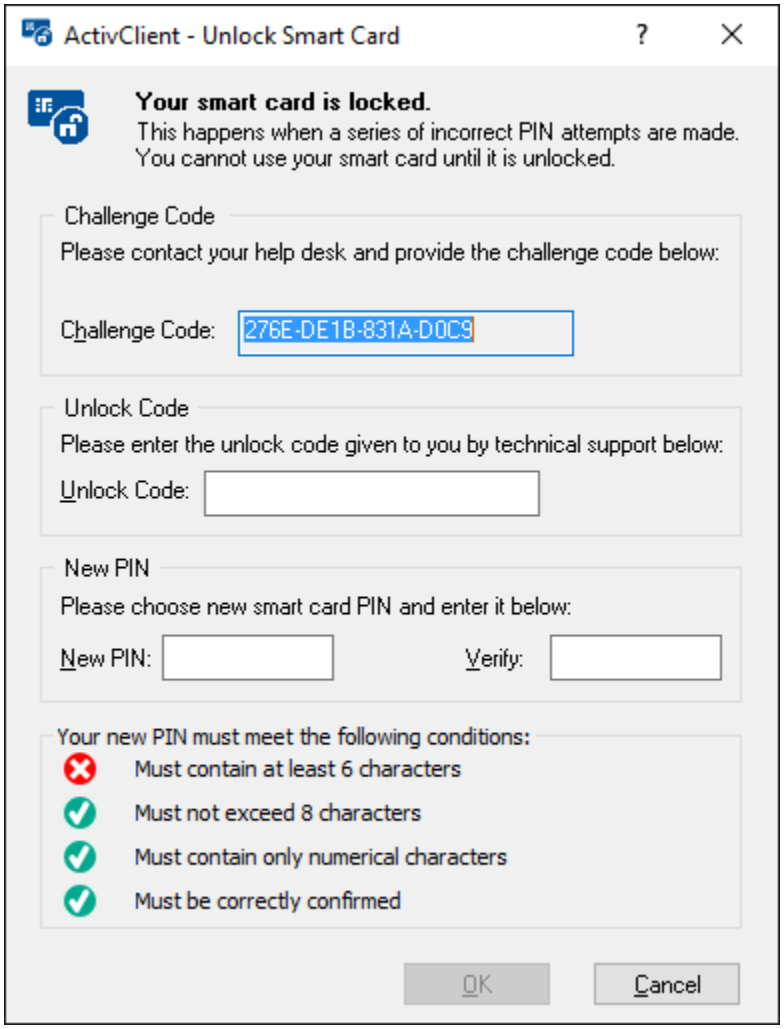
Notes:

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

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

3.4.4 Unlock a Smart Card in the ActivClient User Console

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



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

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

3.5 Unlock a Smart Card using the Microsoft Windows Interface

ActivClient integrates with Microsoft Windows to allow you to unlock a smart card directly from the Windows user interface.

Prerequisites

- Your smart card was initialized by your administrator with a configuration compatible with the Microsoft smart card unlock feature.
- Your administrator has configured Microsoft Windows to enable you to unlock your smart card.

3.5.1 Access the Microsoft Windows Unblock Screen

If your smart card is locked, you have two options to access the Microsoft Windows unlock screen (referred to by Windows as smart card "unblock").

Option 1 – At Microsoft Windows Logon

1. Attempt to log on to Microsoft Windows with your smart card by inserting your smart card, entering your PIN code (even an incorrect PIN code) and clicking **OK**.

   Microsoft Windows displays an error message.

   The message might also contain instructions specific to your deployment (for example, a telephone number for your help desk).

2. Click **OK**.

   The smart card unblock screen is displayed.

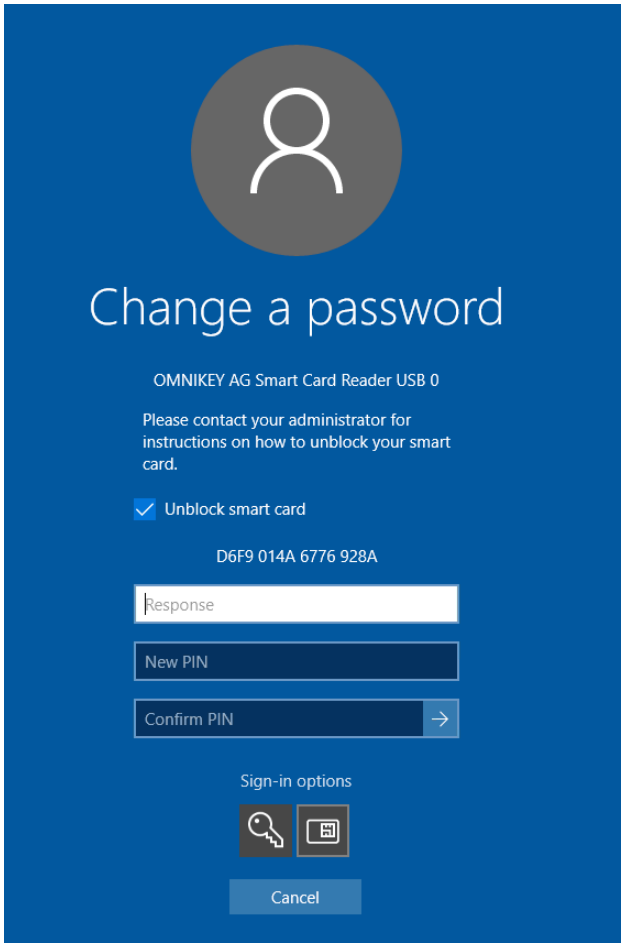
Option 2 – During a Microsoft Windows Session

1. When your Microsoft Windows session is open, press **Ctrl+Alt+Del**.
2. Select **Change a password…**.
3. Select either **Sign-in options** or **Other credentials** (depending on your system).
4. Select **Smart card…**.
5. Select the **Unblock smart card** option.

   The smart card unblock screen is displayed.

3.5.2 Unblock Your Smart Card

The following steps describe how to unlock your smart card from the Microsoft Windows smart card unblock screen.



1. Call your help desk – the telephone number might appear on your screen if your organization has configured Microsoft Windows accordingly.
2. Give your help desk the code displayed above the Response and PIN fields on the screen.
3. In the **Response** field, enter the response that the help desk operator gives you.
4. Enter a new PIN code in the **New PIN** field.
5. Confirm the new PIN code in the **New PIN confirmation** field.
6. Click the **OK** button.

3.6 Update Your Smart Card

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

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

The update could be one of the following:

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

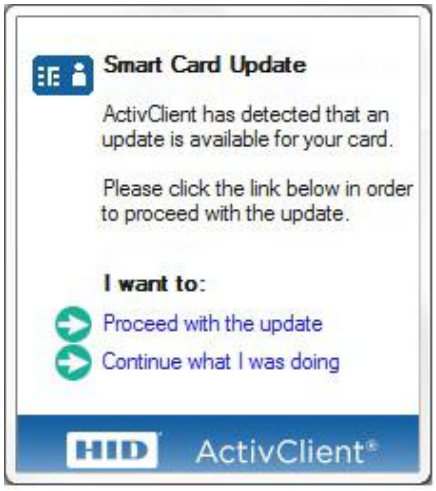
Prerequisites

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

3.6.1 Automatic Check for Updates

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

On Microsoft Windows 7:



You can either:

- Click **Proceed with the update**:

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

  Follow the displayed instructions to update your smart card.

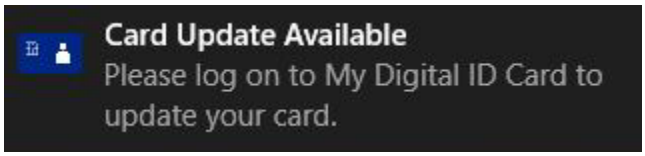
  When the update is complete, close your browser.

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

- Click **Continue what you were doing**:

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

On Microsoft Windows 10:



You can either:

- Proceed with the update:

  Log on to the ActivID CMS My Digital ID Card portal, and follow the displayed instructions to update your smart card.

  When the update is complete, close your browser.

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

- Close the notification:

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

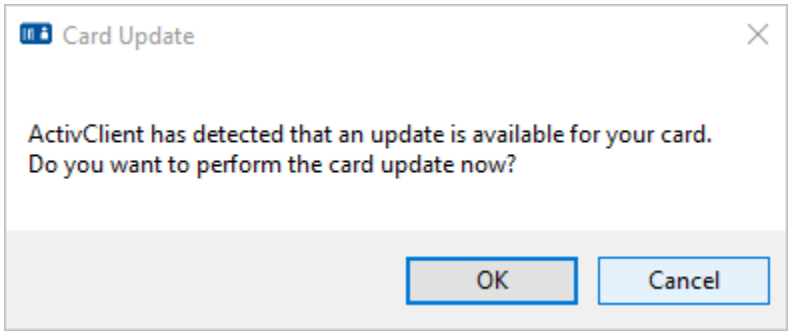
Note: If you do not select an option, or you remove the card from the reader, the alert will disappear.

3.6.2 Manually Check for Updates

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

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

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



   - To proceed, click **OK** and follow the procedure described on page 28.
   - If you do not want to update your card, click **Cancel**.

3. If no update is available, a message is displayed stating so. Click **OK** to close the message.

3.7 Smart Card or Certificate Expiration

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

If you have installed the US Department of Defense configuration feature, these policies are automatically enabled. Otherwise, your administrator might have enabled these features.

Prerequisites

At least one of the following ActivClient policies is enabled:

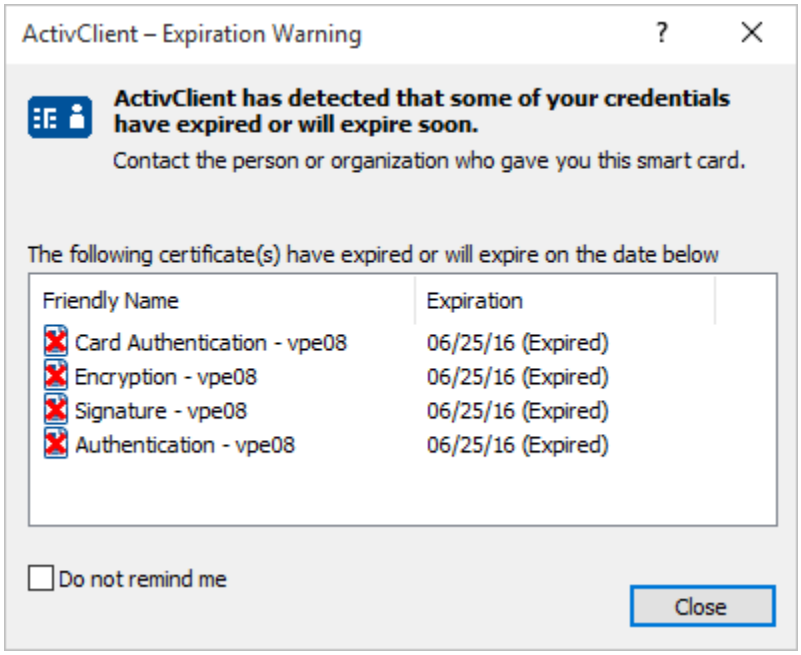
- Display card expiration notification
- Display certificate expiration notification

Notes:

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

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

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



2. If you want to be reminded of this expiration, select the number of days before expiration and click **OK**.
3. If not, select **Do not remind me** and click **OK**.

It is recommended that you request a replacement card or certificate as soon as possible.

3.8 View Smart Card Information

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

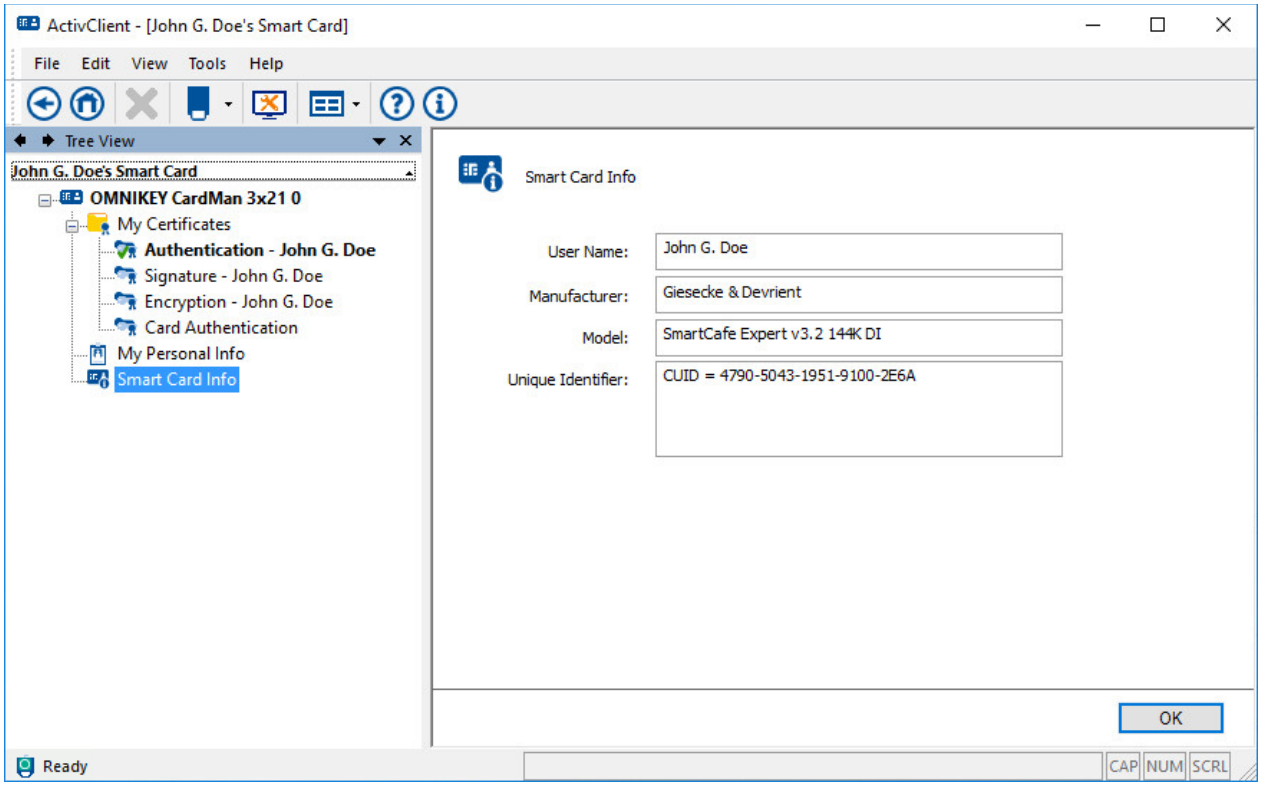
- User name

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

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

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

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



Note: Your user name is supplied by ActivClient from either:

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

4.0 Managing Digital Certificates

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

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

4.1 Download a Certificate with Microsoft Internet Explorer

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

Prerequisites

- Microsoft Smart Card Mini Driver Support (sub-component of the Digital Certificate Services component) was installed during setup.
- Your administrator has provided you with a Web site URL to access your organization's Certificate Authority. To download a smart card logon certificate, your organization's Certificate Authority must be either one of the following:
  - Microsoft Windows Server 2008, Windows Server 2012 or Windows Server 2016
  - A Certificate Authority trusted by your Active Directory

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

   When your smart card is full (that is, if there is not enough space for the certificate that you are downloading), ActivClient overwrites the default certificate with the new certificate. In this case, a message is displayed that you are about to replace the existing credentials on the card. Select **Yes** to overwrite the default certificate.
6. Enter your PIN when prompted.
7. Verify that the key pair and associated certificate have been loaded on your smart card using the ActivClient User Console (optional).



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

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

4.2 Download a Certificate with Mozilla Firefox

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

Prerequisites

- A supported version of Firefox is installed on your computer.
- Firefox support was installed during setup.
- Your administrator provided you with a Web site URL to access your organization's Certificate Authority.

1. Insert your smart card (chip-side up and chip first) into the smart card reader.
2. Launch Firefox and go to your Certificate Authority's Web site.
3. Follow the instructions to request a certificate.
4. Enter your PIN when prompted.
5. Verify that the key pair and associated certificate have been loaded on your smart card using the ActivClient User Console (optional).

4.3 Managing User and CA Certificates

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

ActivClient User Console allows you to access two types of certificates:



User Certificates contain one (or more) certificate and a pair of keys (public/private keys) allowing you to authenticate. In order to use your certificates, you must first install or trust a CA Certificate on your machine.



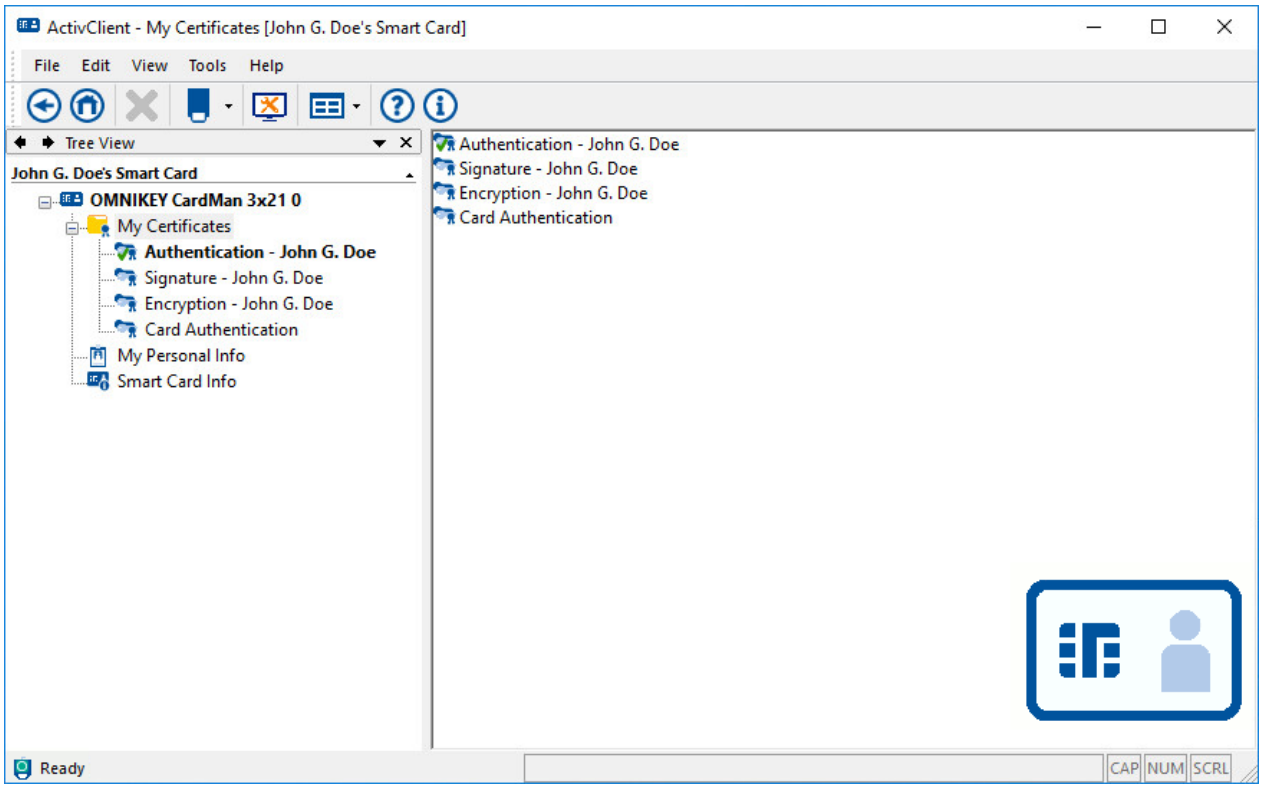
CA Certificates (Certificate Authority Certificates) might contain certificates identifying the authority that issued your certificates.

4.3.1 View Your Certificate

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

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

   An icon for each of your certificates is displayed.

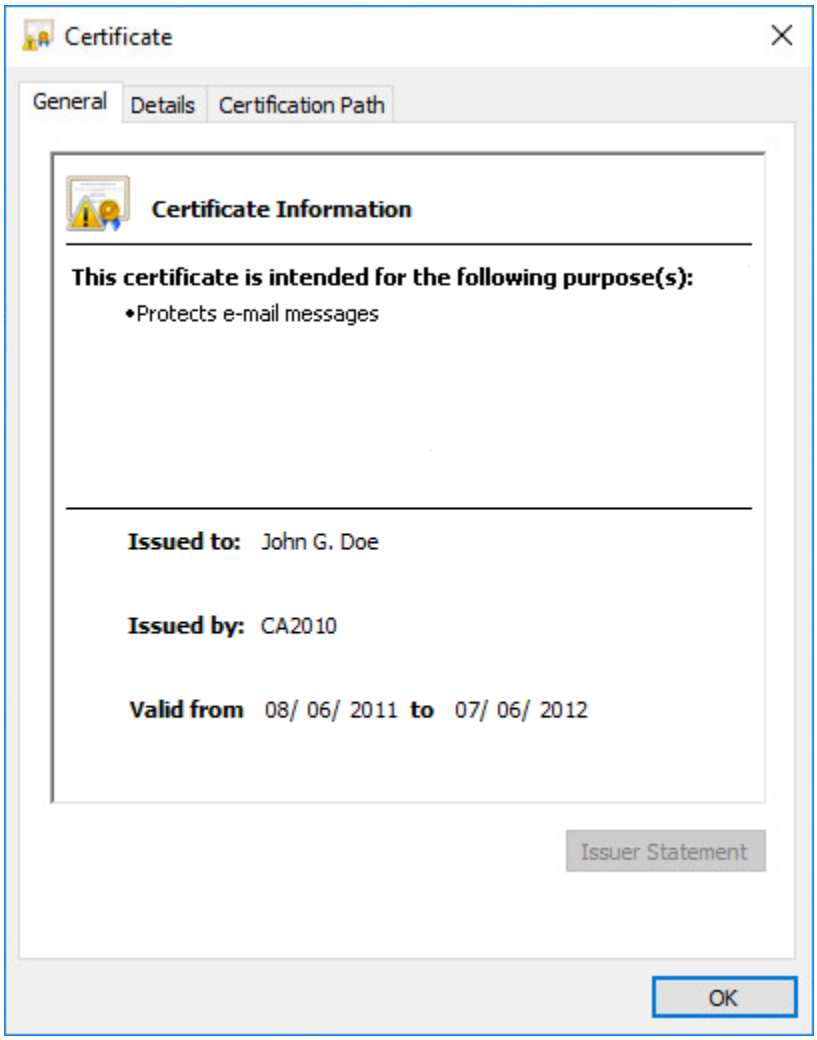


Depending on the card and certificate issuance model, the certificate friendly name can help you identify the certificate purpose.

- For PIV cards, ActivClient automatically displays the following friendly names:
  - Authentication - <username>
  - Signature - <username>
  - Encryption - <username>
  - Archived Encryption #N - <username>
  - Card Authentication
- For CAC cards, ActivClient automatically displays the following friendly names:
  - ID - <username>
  - Signature - <username>
  - Encryption - <username>
- For cards issued by ActivID CMS, you can customize the friendly names during the issuance process.
- In other cases, ActivClient will identify certificates by the user's name and a sequence number.

2. Double-click the certificate that you want to view.

   The Certificate dialog is displayed.



- The General tab displays general information about the certificate such as issuer, issuee and validity dates.
- The Details tab displays information about all certificate attributes.
- The Certification Path displays the certificate validation path.

4.3.2 Import a User Certificate

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

Prerequisites

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

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

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

   If the certificate is password-protected, the Password Request dialog box is displayed prompting you to enter your password.
4. In the **Password** field, enter the certificate password, and click **OK**.
5. When the confirmation message is displayed, click **OK**.
6. To make the certificate available on the computer, remove the card from the reader, and then re-insert it.

4.3.3 Import a CA Certificate

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

Prerequisites

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

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

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

   If the certificate is password protected, the Password Request dialog box is displayed prompting you to enter your password.
4. In the **Password** field, enter the certificate password, and click **OK**.
5. When a confirmation message is displayed, click **OK**.
6. To make the certificate available on the computer, remove the card from the reader, and then re-insert it.

4.3.4 Export a Certificate

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

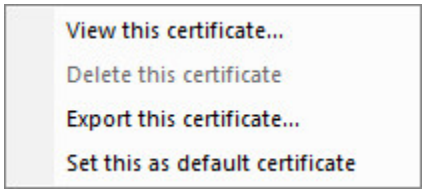
Prerequisites

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

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

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

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



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

   A confirmation message is displayed.
4. Click **OK**.

Note: Alternatively, you can export a certificate using native Microsoft Windows functionality:

- In the ActivClient User Console, double-click on the certificate you want to export.
- Go to the Details tab, and select Copy to File, and then follow the wizard instructions.

4.3.5 Delete a Certificate

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

Prerequisites

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

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

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

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

   A confirmation message is displayed asking you to confirm you want to delete your certificate.

   Note: You might not be able to delete some of your certificates depending of your smart card configuration.
3. Click **Yes** to confirm.

4.3.6 Set a Default Certificate

With Microsoft Windows Vista, Windows 7, Windows 8, Windows 10, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 and Windows Server 2016, the logon process allows you to select a logon certificate when you log on (among certificates compatible with Windows logon).

In Microsoft Windows XP and earlier versions, Microsoft Windows displayed only one certificate, the "default" certificate.

Prerequisite

You have a Microsoft Windows logon compatible certificate available on your smart card. For more information, see 4.1 Download a Certificate with Microsoft Internet Explorer on page 33.

It is also possible to configure Microsoft Windows 7, Windows 8 and Windows 10 to force using the default certificate (this is controlled by a Microsoft Windows policy).

If you will be using your smart card with Microsoft Windows XP or if your environment requires a "default" certificate, you can use the ActivClient User Console to set a default certificate.

In all other configurations, you do not need to do anything.

Note: You cannot change the default certificate for PIV and CAC smart cards.

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

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

   The certificate icon is updated with a green check mark .

Note: The Set this as default certificate option is visible only if your smart card contains two or more certificates.

4.3.7 Deselect a Logon Certificate

When you no longer need to identify your logon certificate as the default, follow these steps:

Prerequisite

One of your certificates is currently set as the default.

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

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

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

4.4 Managing Certificates in Microsoft Outlook

4.4.1 Automatically Configure Your Microsoft Outlook Security Profile

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

ActivClient can automatically create your security profile.

Prerequisites

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

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

1. Start Microsoft Outlook configured with a Microsoft Exchange account.
2. Insert your smart card (chip-side up and chip first) into the smart card reader.
   - If you do not have an existing Microsoft Outlook security profile, ActivClient automatically creates the profile.
   - If you already had an Outlook security profile, ActivClient automatically updates it with your smart card certificates.
   - ActivClient also makes sure that the most current certificates are used and that the email address in the certificate matches that of the Outlook account.

4.4.2 Automatically Publish Your Certificates to the Global Address List

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

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

Prerequisites

- Microsoft Outlook is installed on your workstation.
- Microsoft Outlook Usability Enhancements (sub-component of the Digital Certificates Services component) was installed during setup.

- The ActivClient policy, Turn on automatic publication of certificates to the Global Address List, is enabled (it is disabled by default; your administrator might have enabled this feature).
- The ActivClient policy, Turn off setup email certificates in Microsoft Outlook on card insertion, is disabled (it is disabled by default; your administrator might have enabled this feature).
- Your smart card contains certificates for email signature and email encryption.

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

   ActivClient automatically publishes your smart card-based certificates to the Global Address List.
4. Alternatively, you can publish your certificates to the GAL from the ActivClient User Console – From the User Console, select **Tools**, **Advanced** and then **Publish to GAL**.
   - Your Outlook security profile is created or updated.
   - Your certificates are published to the Global Address List.

4.4.3 Automatically Add Certificates to Microsoft Outlook Contacts

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

Prerequisites

- Microsoft Outlook is installed on your workstation.
- Microsoft Outlook Usability Enhancements (sub-component of the Digital Certificates Services component) was installed during setup.
- The ActivClient policy, Turn off automatic addition of sender's certificates to Microsoft Outlook contacts, is disabled (default setting).

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

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

   ActivClient will ask you to either confirm the creation of the Outlook Contact entry or update an existing entry.
2. To proceed, accept the creation/update.

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

5.0 Using Digital Certificates

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

5.1 Log On to Windows with a Certificate

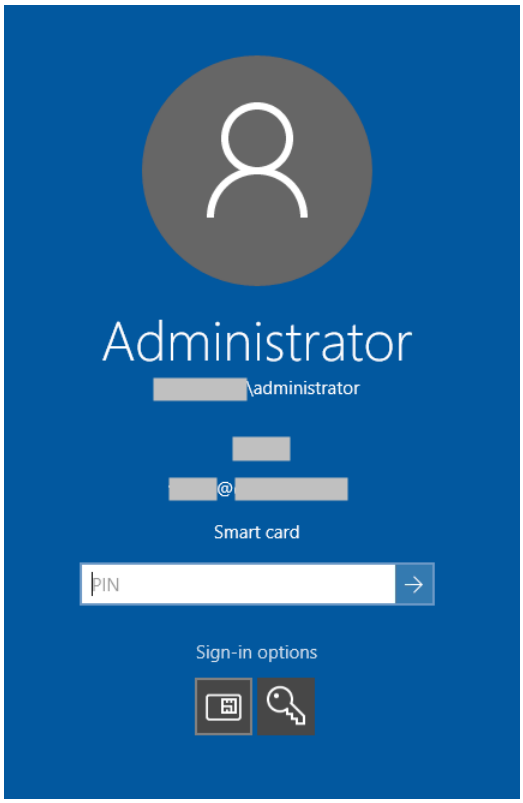
You can use a smart card certificate to securely log on to Windows.

Prerequisites

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

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

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



3. If multiple smart card certificates that compatible with Microsoft Windows logon are displayed, select the one you want to use.
4. Enter your **PIN** in the PIN field and click **OK**.

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

5.2 Lock Your Workstation on Smart Card Removal

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

Prerequisites

- Microsoft Windows is configured to lock the workstation on smart card removal (default setting).
- The ActivClient policy, Unattended smart card alert, is configured to activate at either log off or both log off and screen lock (by default, it is configured for the latter option).

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

Smart Card Unattended Notification

If you forget to remove your smart card when you log off, or when you lock your workstation, ActivClient triggers an audio notification to remind you that you should remove your smart card from the reader.

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

Note: Your administrator might have changed the Card Removal Behavior property.

5.3 Use Windows Dial-Up/VPN for Remote Access

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

Prerequisites

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

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

   The Network Connections dialog box is displayed.

3. Choose your remote connection (Dial-Up or VPN).

   The Connect Virtual Private Connection dialog box is displayed.

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

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

5.4 Use a Non-Microsoft VPN for Remote Access

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

Prerequisites

- You can access a VPN product supported by ActivClient. For the complete list, see the *ActivClient for Windows Overview*.
- Your smart card contains a certificate configured for VPN logon.
- You have configured your VPN to use an ActivClient-based digital certificate. Depending on the VPN products, you might need to select the cryptographic library:
  - Select the "Microsoft Base Smart Card Crypto Provider" for Microsoft CAPI compatible applications.

  OR

  - Select the ActivClient PKCS#11 library (acpkcs211.dll in the ActivClient installation directory) for PKCS#11 compatible applications and the certificate for the VPN authentication.

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

When you are authenticated, the VPN session is established.

5.5 Access a Secure Web Site

5.5.1 Access a Secure Web Site with Internet Explorer, Microsoft Edge or Google Chrome

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

Prerequisites

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

1. Insert your smart card (chip-side up and chip first) into the smart card reader.
2. Access the secure Web site or page using Microsoft Internet Explorer, Microsoft Edge or Google Chrome.
3. From the certificate list, select the appropriate ActivClient certificate, and click **OK**.
4. Enter your PIN in the **Smart card PIN** field and click **OK**.

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

5.5.2 Access a Secure Web Site with Firefox

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

Prerequisites

- Firefox is installed on your computer.
- Your smart card contains a certificate configured for authentication to this Web site.
- Firefox and Thunderbird configuration (sub-component of the Digital Certificates Services | PKCS #11 Support component) was installed during setup.
- If you use Firefox 3.5 or later, Firefox support was installed during setup.
- If you use a version of Firefox earlier than 3.5, see the *ActivID ActivClient for Windows Installation Guide* for Firefox configuration details.

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

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

5.6 Send/Read Signed and Encrypted Email Messages with Microsoft Outlook

5.6.1 Send/Read Signed Email Messages

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

It authenticates you as the message sender and verifies the integrity of the message.

With ActivClient, the digital signature is performed directly on your smart card.

Prerequisites

- Microsoft Outlook is installed on your workstation.
- Microsoft Smart Card Mini Driver Support (sub-component of the Digital Certificate Services component) was installed during setup.
- Microsoft Outlook Usability Enhancements (sub-component of the Digital Certificates

Services component) was installed during setup. This option allows you to sign an email message with a single click (optional).

- A certificate with email signature capabilities is available on your smart card.
- You have configured your security profile in Microsoft Outlook (see section 4.4.1 Automatically Configure Your Microsoft Outlook Security Profile on page 41).

5.6.1.1 Send Signed Email Messages

1. Insert your smart card (chip-side up and chip first) into the smart card reader.
2. Create the email message and either:
   - For Microsoft Outlook 2010 and later, select the **Options** tab and click the **Sign** icon.
   - For Microsoft Outlook 2007, from the Outlook toolbar, click the **Digitally Sign Message** icon.
3. Complete and send the email message.

5.6.1.2 Read Signed Email Messages

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

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

5.6.2 Send/Read Encrypted Email Messages

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

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

5.6.2.1 Send Encrypted Email Messages

Prerequisites

- Microsoft Outlook is installed on your workstation.
- You have access to the certificate of the person to whom you want to send an encrypted email message (see section 4.4.3 Automatically Add Certificates to Microsoft Outlook Contacts on page 42).
- You have configured your security profile in Outlook (see section 4.4.1 Automatically Configure Your Microsoft Outlook Security Profile on page 41).

1. Create the email message and either:
   - For Microsoft Outlook 2010 and later, select the **Options** tab and click the **Encrypt** icon

- For Microsoft Outlook 2007, from the Outlook toolbar, click the **Encrypt Message Contents and Attachments** icon.

2. Complete and send the email message.

5.6.2.2 Read Encrypted Email Messages

Prerequisites

- Microsoft Outlook is installed on your workstation.
- A certificate with email encryption capabilities is available on your smart card.
- Your encryption certificate is available to other users (see section 4.4.2 Automatically Publish Your Certificates to the Global Address List on page 41).
- Microsoft Smart Card Mini Driver Support (sub-component of the Digital Certificate Services component) was installed during setup.

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

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

5.6.2.3 Automatically Decrypt and Save Emails

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

Prerequisites

- Microsoft Outlook is installed on your workstation.
- Microsoft Outlook Usability Enhancements (sub-component of the Digital Certificates Services component) was installed during setup.
- The ActivClient **Turn on automatic decryption of encrypted emails setting** is enabled (it is disabled by default; your administrator might have enabled this feature).

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

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

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

5.7 Send/Read Signed and Encrypted Mails with Thunderbird

5.7.1 Send/Read Signed Email Messages

A digital signature is a combination of your private key and the message. It authenticates you as the message sender and verifies the integrity of the message.

With ActivClient, the digital signature is performed directly on your smart card.

Prerequisites

- Thunderbird is installed on your computer.
- A certificate with email signature capabilities is available on your smart card.
- Firefox and Thunderbird configuration (sub-component of the Digital Certificates Services | PKCS #11 Support component) was installed during setup.
- If you use Thunderbird 3.0 or later, Thunderbird support was installed during setup.
- If you use a version of Thunderbird earlier than 3.0, see the *ActivID ActivClient for Windows Installation Guide* for Thunderbird configuration details.

5.7.2 Send Signed Email Messages

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

5.7.3 Read Signed Email Messages

1. Insert your smart card (chip side up and chip first) into the smart card reader.
2. Start your email client.
3. In your Inbox, click on the signed message you want to read.

   If the sender is successfully authenticated, the message appears with a secure message icon.

5.8 Send/Read Encrypted Email Messages

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

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

Prerequisites

- Thunderbird is installed on your workstation.
- A certificate with email signature capabilities is available on your smart card.
- Firefox and Thunderbird configuration (sub-component of the Digital Certificates Services | PKCS #11 Support component) was installed during setup.
- If you use Thunderbird 3.0 or later, Thunderbird support was installed during setup.
- If you use a version of Thunderbird earlier than 3.0, see the *ActivID ActivClient for Windows Installation Guide* for Thunderbird configuration details.

5.8.1 Send Encrypted Email Messages

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

5.8.2 Read Encrypted Email Messages

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

5.9 Encrypt/Decrypt Files with EFS

Microsoft Windows allows the Encryption File System (EFS) feature to use smart card certificates for files and folder encryption.

Depending on your smart card content and your platform configuration, you can seamlessly encrypt and decrypt files.

EFS Encryption/Decryption Prerequisites

- Your platform is configured for EFS.
- Your platform is configured to require the use of a smart card for EFS.
- Your smart card contains a certificate configured for EFS.

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

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

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

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

5.9.2 Encrypt a File or Folder with EFS

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

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

5.9.3 Decrypt a File or Folder with EFS

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

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



4. Click on the notification (or link).
5. Enter your smart card **PIN** and click **OK**.

   The file or folder is opened in clear text.

5.9.4 Update EFS Certificates and Re-Encrypt Files

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

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

EFS Update Prerequisites

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

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

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

The Manage your file encryption certificates wizard is displayed.

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

     A tree representing your file system is displayed.
4. Select the folders to re-encrypt. Make sure all folders containing your encrypted files are selected.
5. Enter your smart card **PIN** when prompted and click **OK**.

   The wizard completes successfully.

5.9.5 Recover Encrypted Files

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

EFS Recovery Prerequisites

- Your platform is configured to allow EFS.
- Your platform is configured to require smart card for EFS.
- You have backed up your EFS certificate in a certificate file in a secure location.
- You have a new smart card.
- You have files encrypted with your lost or damaged EFS certificate smart card.

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

1. Import the backup EFS certificate in your new smart card using the ActivClient User Console.
2. In Microsoft Explorer, select one of the encrypted files you need to recover.
3. When prompted, insert your smart card containing the new EFS certificate.
4. Enter your smart card **PIN** and click **OK**.

   You can access your file in clear text.

5.10 Encrypt Drives with BitLocker To Go

BitLocker To Go is a feature of Microsoft Windows 7 (and later) that enables you to encrypt removable storage devices (for example, external hard drives or USB memory sticks) with your smart card.

5.10.1 Protect the Data Drive with Your Smart Card

1. Connect the drive to the computer.
2. From the Start menu, click **Computer** to display the available drives on your computer.
3. Right-click on the drive you want to protect, and then select **Turn on BitLocker** to start the BitLocker setup wizard.
4. In the Choose how you want to unlock this drive page, click **Use my smart card to unlock the drive**.
5. Insert your smart card into the smart card reader, and click **Next**.
6. In the Save the recovery key page, select either **Save the key to a file** to save your recovery key to a network drive or other location or select **Print the recovery key** to print the 48-digit recovery password, and then click **Next**.
7. In the Are you ready to encrypt this drive page, confirm that you want to use a smart card to encrypt the drive, and click **Start Encrypting**.

   When the drive is ready for encryption, the Encryption in Progress status bar is displayed.
8. When you are notified that encryption is complete, click **Close**.



Note: Your administrator might have configured additional BitLocker policies that could slightly alter these steps.

5.10.2 Access the Protected Drive

1. Connect the drive to the computer.
2. Insert your smart card to unlock the drive when prompted.
3. Enter your **PIN** code when prompted.

6.0 Managing Remote Access/OTP

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

6.1 Synchronize Your Smart Card

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

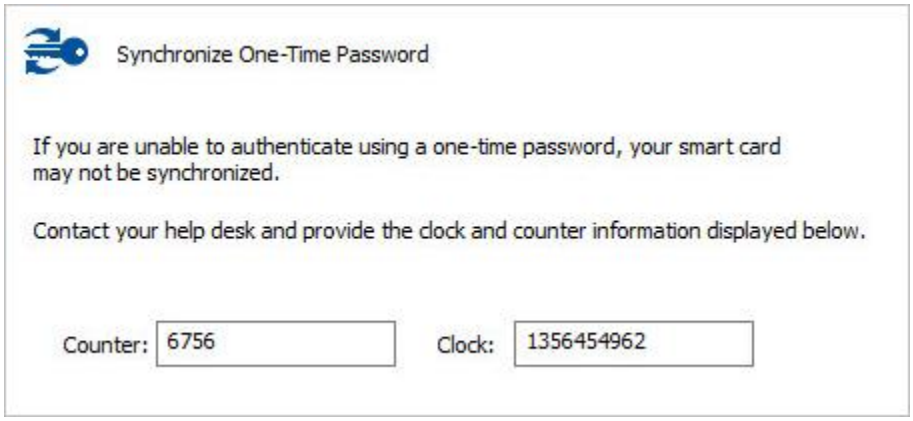
Prerequisites

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

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

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

   The Synchronize One-Time Password dialog box is displayed.



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

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

6.2 Configure Your Remote Access User Name

If you want to use your smart card for remote access with one-time passwords, your remote access application might be able to retrieve your username from the smart card, in addition to generating the OTP on the smart card. Depending on your configuration, you might need to define or update the user name.

Prerequisite

Your smart card is initialized to use one-time passwords.

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

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

   The Configure One-Time Password dialog box is displayed.



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

   Your remote access user name is configured.

7.0 Using Remote Access/OTP

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

7.1 Automatically Generate a One-Time Password

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

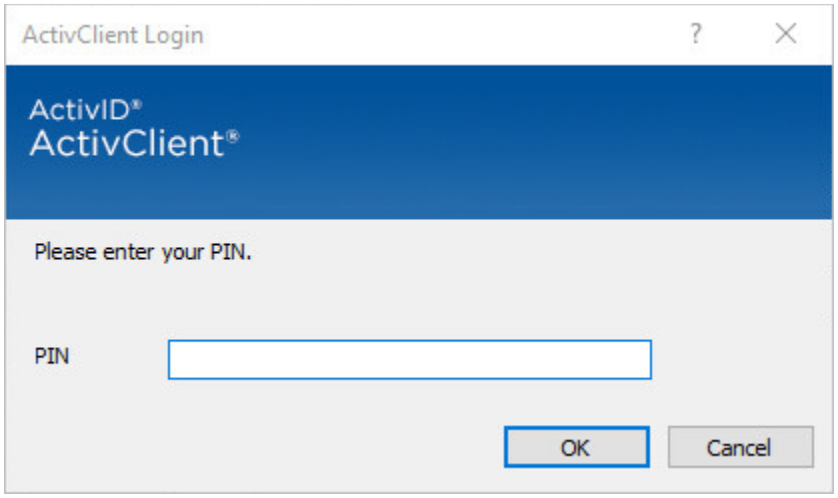
The Get One-Time Password (OTP) option:

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

Prerequisites

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

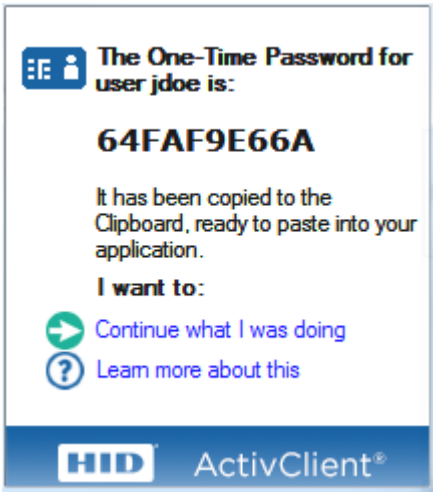
1. Left or right-click on the **ActivClient Agent** icon in the Windows notification area and select **Get One-Time Password**.



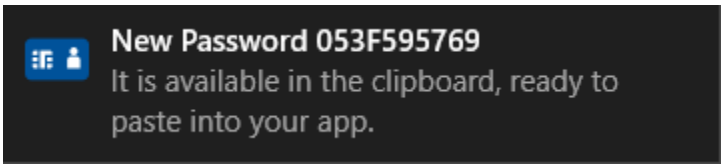
2. Enter your PIN code and click **OK**.

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

On Microsoft Windows 7:



On Microsoft Windows 10:



3. Place your cursor in the password field of the application to which you want to authenticate.
4. Select **Paste** (or press Ctrl + V).

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

7.2 Manually Generate a One-Time Password

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

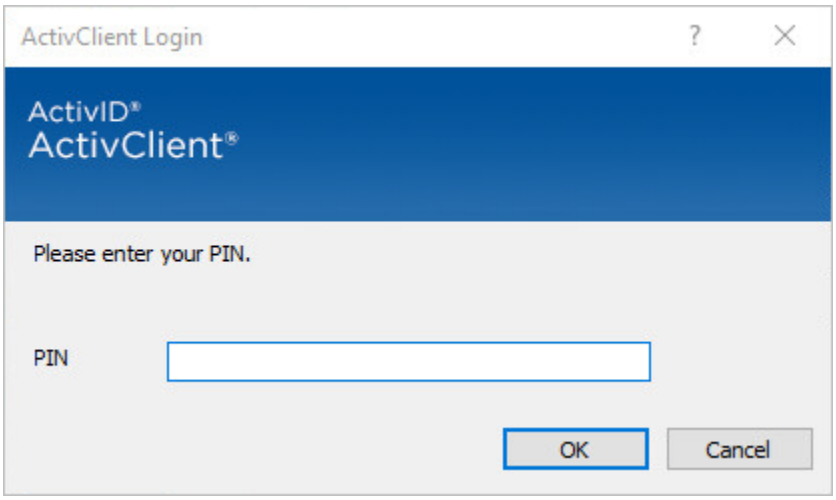
Prerequisites

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

1. To display the Generate One-Time Password dialog box, either:
   - From the ActivClient User Console tasks pane, select **Generate One-Time Password**.
   - From the ActivClient User Console right pane, double-click the server's icon.

   The Generate One-Time Password dialog box is displayed.
2. Depending on your administrator's recommendations, either:
   - If your administrator recommends that you authenticate in **Automatic** mode:

   a. Click **Generate**.



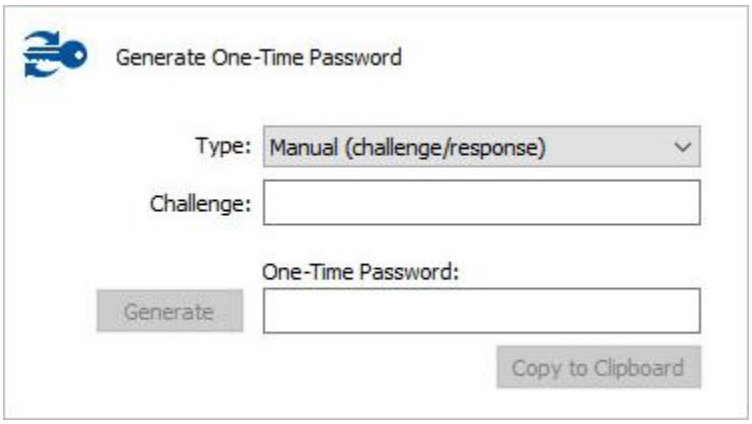
b. Enter your PIN code and click **OK**.

A one-time password is displayed which you can enter or copy/paste into any authentication window.

- If your administrator recommends that you authenticate in a **Challenge/Response** mode:

a. Select **Manual (Challenge/Response)** from the **Type** drop-down list.

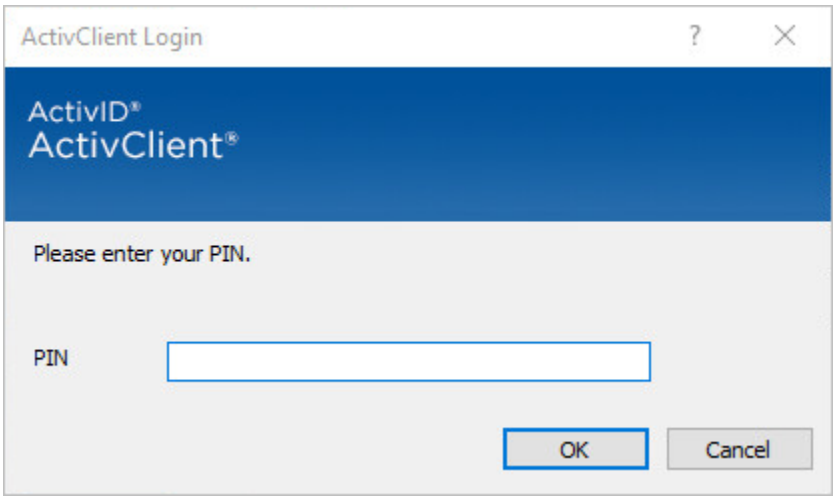
A Challenge field is displayed in the Generate One-Time Password dialog box.



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

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

c. Click **Generate**.



d. Enter your PIN code and click **OK**.

A one-time password is displayed which you can enter or copy/paste into any authentication window

8.0 Viewing Personal Information

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

8.1 About Personal Information

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

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

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

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

8.2 View "My Personal Info"

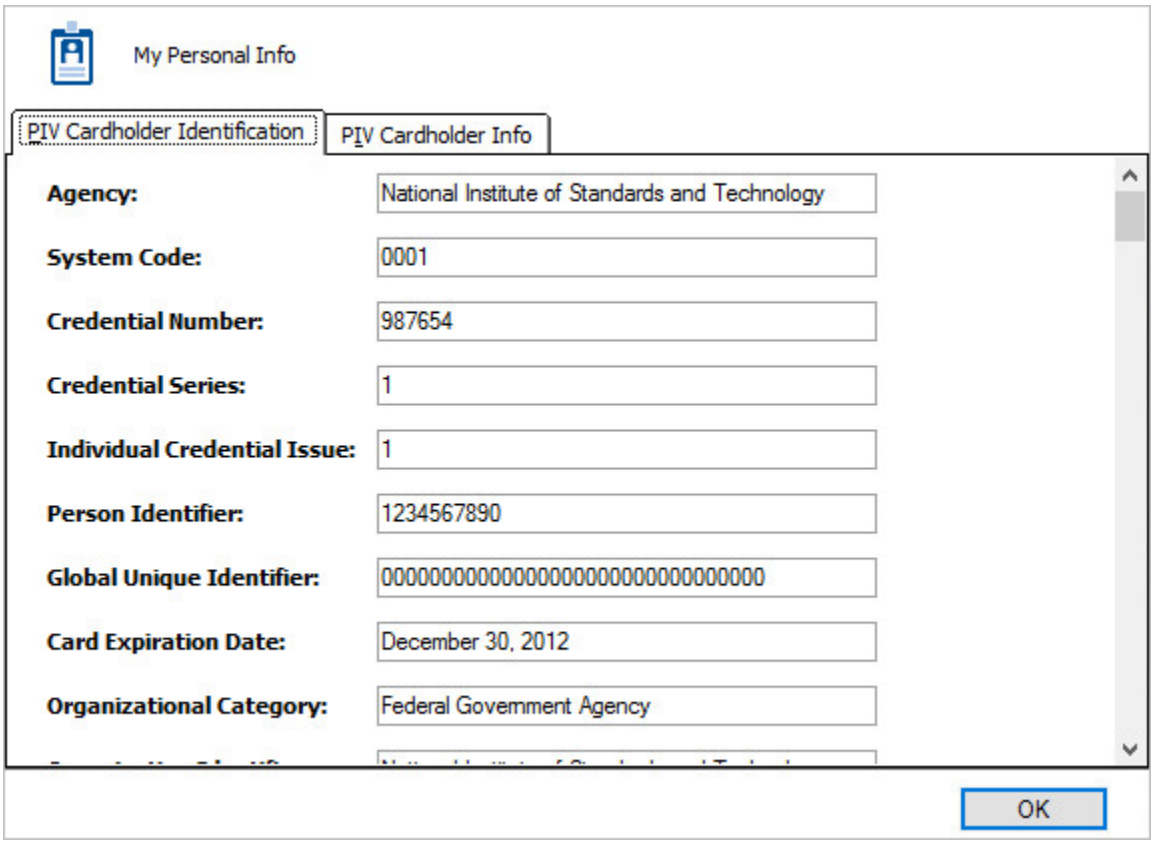
1. To view your personal information, either:
   - From the User Console left pane, click on **View my personal info** under **My Personal Info Task**.
   - From the User Console right pane, double-click the **My Personal Info** icon .
   - From the User Console right pane, right-click on the **My Personal Info** icon and select **Open**.
2. Enter your PIN code when prompted.

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

   The tabs/data available varies according to the type of card and card profile. For example:
   - For PIV cards, the PIV Cardholder Identification and PIV Cardholder Info are displayed.
   - For CAC cards, the Cardholder Info, Employment, Benefits and Other Benefits tabs are displayed (some tabs might not display depending on card personalization).

Note: As recent CAC smart cards are also PIV-compliant, the relevant information is displayed.

 All rights reserved.



For PIV smart cards:

- The PIV Cardholder Identification tab also indicates if the CHUID digital signature is valid.
- The PIV Cardholder Info tab also indicates if the facial image digital signature, the fingerprint digital signature, and the iris image digital signature (if applicable) are valid.

9.0 Using and Managing ActivClient

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

9.1 View ActivClient System Information

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

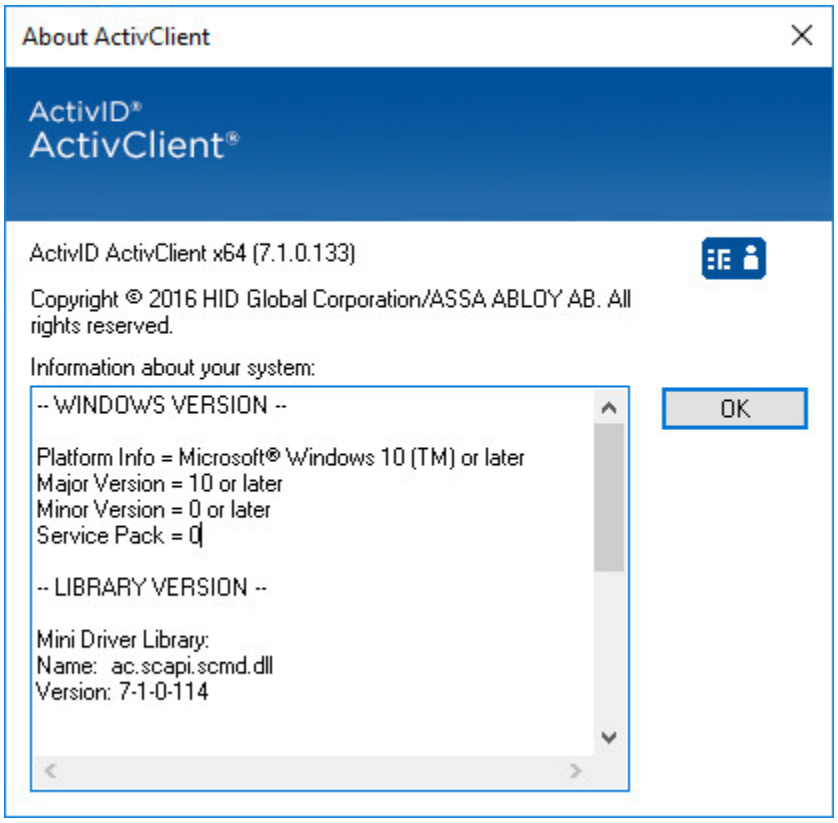
The About ActivClient window displays information such as:

- ActivClient edition and version number
- Build Number
- Copyright information
- Information about your system, such as Windows version and web browser version
- SDK API information:
  - Mini Driver library version
  - PKCS#11 library version
  - BSI library version
  - PIV library version

To view the ActivClient system information, either:

- From ActivClient User Console, select **About ActivClient** from the **Help** menu.
- On ActivClient Agent icon  in the Windows notification area, left or right-click and select **About**.

The About ActivClient window is displayed.



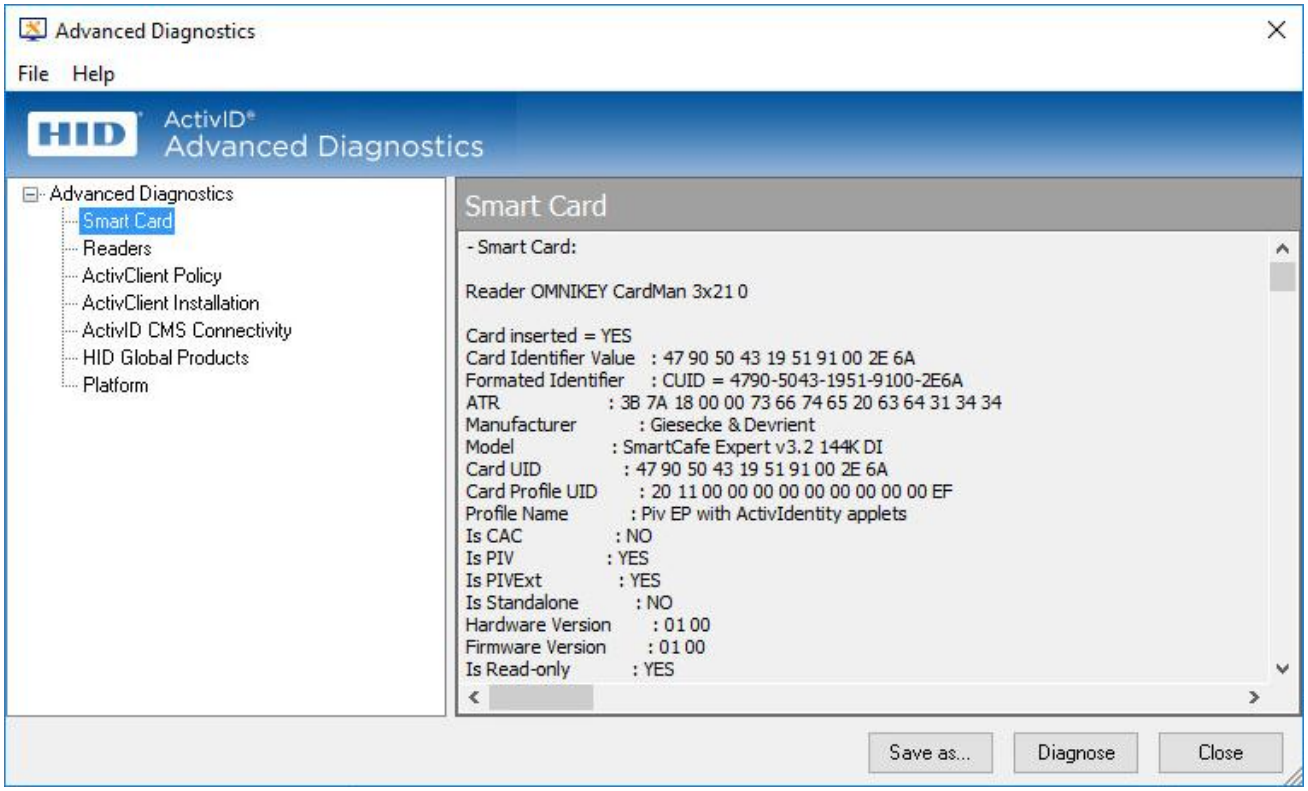
9.2 Perform Advanced Diagnostics

The Advanced Diagnostics tool:

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

1. To access the Advanced Diagnostics wizard, either:
   - On the **ActivClient Agent** icon in the Windows notification area, left or right-click and select **Advanced Diagnostics**.
   - From the ActivClient User Console Standard toolbar, click the **Advanced Diagnostics** icon.
   - From the ActivClient User Console Help menu, select **Diagnose**.
   - From the Start menu, go to the programs or apps directory, and select **Advanced Diagnostics** under **ActivID ActivClient**.
2. To generate a report, make sure you have inserted a smart card.
3. Click **Diagnose**.

4. If your smart card is in your reader, enter your **PIN** code at the prompt and click **OK**.



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

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

- Smart Card
- Readers
- ActivClient Policy
- ActivClient Installation
- ActivID CMS Connectivity
- HID Global Products
- Platform

5. Select one of the eight categories you want to display.
6. To copy part of your report, select the required view, and select **File** and click **Copy**.

   The content of the option you selected is copied to the clipboard and can be pasted into a file and location of your choice.
7. To save your report, select **File** and click **Save as**.

   All the information is saved in a single log file.

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

   Note: The destination email address might be pre-defined by your administrator.

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

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

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

9.3 Use the Reset optimization cache Option

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

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

1. Open the ActivClient User Console.
2. Go to the **Tools** menu.
3. Select **Advanced** and then **Reset optimization cache**.

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

9.4 Activate Log Files

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

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

Log Activity Recommendations:

- Turn off logging system activity in normal use cases.
- Turn on logging system activity only when required by your system administrator or help desk.
- After log file creation, it is recommended that you disable log system activity!

Security Note: In order to guarantee privacy and security, neither secret (such as private key) nor personally identifiable information (such as digital certificate) is recorded in the ActivClient log files.

1. In the ActivClient User Console, go to the **Tools** menu.

2. Select **Advanced**, and then **Enable Logging**.

   A check mark is displayed next to the option.

   The logging options (filename and file size) are defined in the ActivClient policy settings.

   By default, the log files are stored in **C:\Program Files\Common Files\HID Global\Logs** and, for 32-bit applications on a 64-bit Microsoft Windows version, they are stored in **C:\Program Files (x86)\Common Files\HID Global\Logs**.

3. Restart your machine to make sure that all ActivClient components start logging events.

   If you are troubleshooting operations related to Microsoft Windows logon, restart the machine for the logs to be complete.

9.5 View ActivClient Policy Settings

ActivClient can be configured using policy settings. These policies are usually applied globally in your organization and automatically pushed to all workstations.

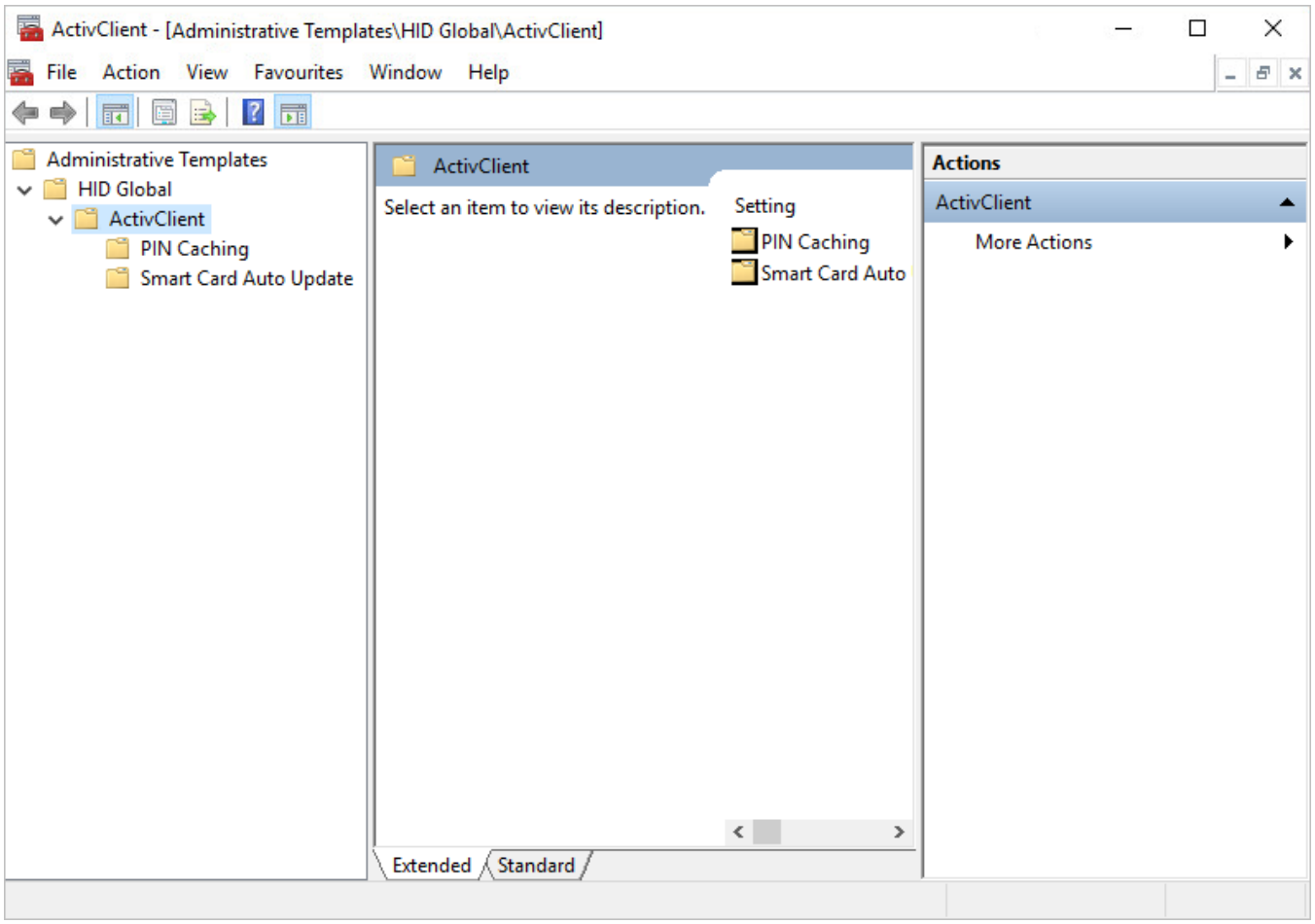
You can also configure specific workstations with specific policy settings. For further information, see the *ActivID ActivClient for Windows Administration Guide*.

To view the policy settings configured for the workstation, ActivClient provides a utility that displays them.

1. In the User Console, from the **Tools** menu, select **Advanced** and then **View policy settings**.

   If you are not logged on with administrator, you are prompted to provide administrative credentials.

   The Resultant Set of Policy is displayed, containing the consolidation of all ActivClient policies relevant to the workstation.



2. Navigate to **Administrative Templates**, **HID Global** and then **ActivClient** to access the ActivClient policies.

Only policies and settings that are configured (that is, that do not use the default ActivClient configuration) are displayed. All those set to the default values are not displayed.

This displayed configuration is read-only. To update the policies and settings, you need to use a policy editor. For further information, see the *ActivID ActivClient for Windows Administration Guide*.

9.6 Auto-Update Service

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

Prerequisite

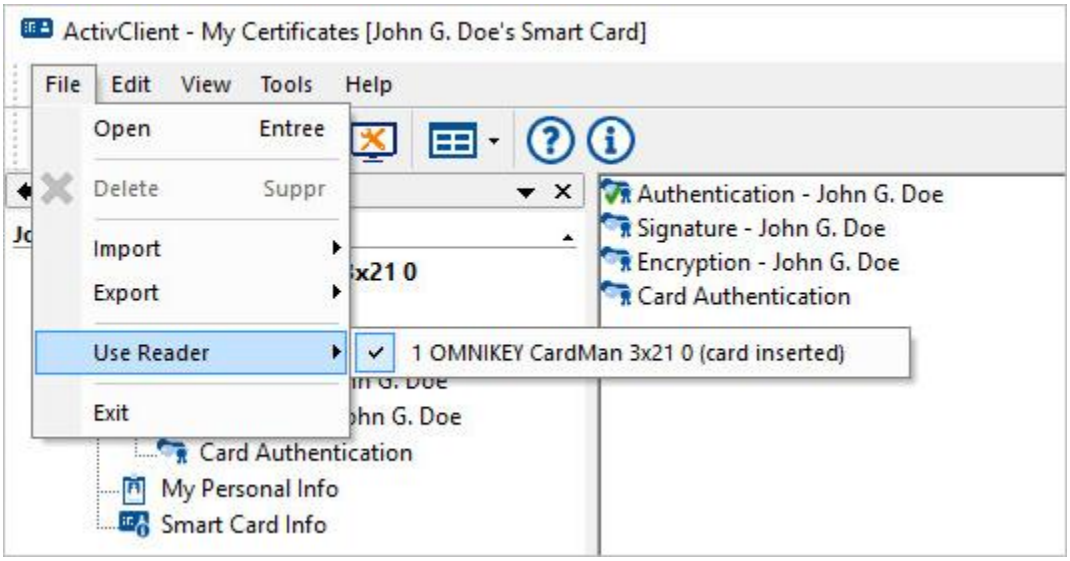
This feature is enabled only if the Auto-Update component is installed and if your organization has set up an auto-update server. For further information, see the *ActivID ActivClient for Windows Administration Guide*.

9.7 Select a Smart Card Reader

If you have more than once smart card reader connected to your machine, you can select the required one from the User Console.

1. Open the ActivClient User Console.

   - From the ActivClient User Console Standard toolbar, click the **Reader List** icon .
   - Go to the **File** menu and select **Use Reader**.



2. Select the required reader from the list.

10.0 Using ActivClient with Terminal Services

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

10.1 Citrix XenApp Sessions

Citrix allows you to connect to a Windows server with Citrix XenApp to access applications not available on your local workstation.

ActivClient provides smart card-based authentication to Citrix XenApp for increased security.

You need to install ActivClient on the Citrix XenApp server in order to provide smart card services within the remote session, and server-based authentication services.

You usually also need to install ActivClient on the Citrix client, as most XenApp configurations require client-based authentication.

How you log on to a Citrix session depends on your configuration.

Notes:

- Smart card management operations such as certificate download operations are not available within the Citrix session.
- For further information on Citrix configurations, see the *ActivID ActivClient for Windows Administration Guide* and the Citrix technical documentation.

10.1.1 Access a Citrix Published Application via Web Interface

Prerequisites

- You have installed the Citrix Online plug-in (full) or the Citrix Online plug-in – Web on your workstation.
- You have a smart card and a smart card reader up and running and connected to your workstation.

If Citrix is configured with the **"smart card" authentication mode**:

1. Log on to your workstation with your smart card.
2. Access the Citrix published application and enter your PIN code when prompted.

   This is required to authenticate to the Citrix session and access the Citrix-published application.

   If the application itself can leverage your smart card (for example Microsoft Outlook to sign or encrypt emails), it will automatically communicate with your smart card that is connected locally to your computer.

   When you remove your smart card, the behavior depends on your Citrix configuration:

   - The Citrix session will disconnect; you can resume using your applications next time you log on to Citrix.
   - You log off from the session; your applications are then closed.

If Citrix is configured with the **"Pass-through with smart card" authentication mode**:

1. Log on to your workstation with your smart card.
2. Access the Citrix published application.

   Authentication is performed automatically. The PIN prompt does not appear.

   If the application itself can leverage your smart card (for example Microsoft Outlook to sign or encrypt emails), it will automatically communicate with your smart card that is connected locally to your computer.

   When you remove your smart card, the behavior depends on your Citrix configuration:

   - The Citrix session will disconnect; you can resume using your applications next time you log on to Citrix.
   - You log off from the session; your applications are then closed.

10.1.2 Access an Application with the Citrix Online Plug-In for Windows

Prerequisites

- You have installed the Citrix Online plug-in (full) on your workstation.
- You have a smart card and a smart card reader up and running and connected to your workstation.

If Citrix is configured with the **"smart card" authentication mode**:

1. Log on to your workstation with your smart card.
2. Access the Citrix published application and enter your PIN code when prompted.

   This is required to authenticate to the Citrix session and access the Citrix-published application.

   If the application itself can leverage your smart card (for example Microsoft Outlook to sign or encrypt emails), it will automatically communicate with your smart card that is connected locally to your computer.

   When you remove your smart card, the behavior depends on your Citrix configuration:

   - The Citrix session will disconnect; you can resume using your applications next time you log on to Citrix.
   - You logoff from the session; your applications are then closed.

If Citrix is configured with the **"Pass-through with smart card" authentication mode**:

1. Log on to your workstation with your smart card.
2. Access the Citrix published application.

   Authentication is performed automatically. The PIN prompt does not appear.

   If the application itself can leverage your smart card (for example Microsoft Outlook to sign or encrypt emails), it will automatically communicate with your smart card that is connected locally to your computer.

   When you remove your smart card, the behavior depends on your Citrix configuration:

- The Citrix session will disconnect; you can resume using your applications next time you log on to Citrix.
- You log off from the session; your applications are then closed.

10.2 Microsoft Remote Desktop Sessions

Microsoft Remote Desktop allows you:

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

Prerequisite

You have a smart card and a smart card reader up and running and connected to your workstation.

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

You need to install ActivClient on the Terminal Server/Remote Desktop Services server in order to provide smart card services within the remote desktop session, and server-based authentication services.

You usually also need to install ActivClient on the Remote Desktop client, as most Terminal Server/Remote Desktop Services configurations require client-based authentication.

10.2.1 Log On to a Microsoft Remote Desktop Session

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

10.2.2 Use Your Smart Card in a Microsoft Remote Desktop Session

ActivClient provides smart card-based services for applications running in the Remote Desktop session.

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

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

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

10.3 Disconnect a Remote Desktop Session

Prerequisite

On the remote Windows workstation or server, the Windows Card Removal policy is configured for "Disconnect if a remote Terminal Services session".

For further information, see the *ActivID ActivClient for Windows Administration Guide*.

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

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

Appendix A: Terms and Acronyms

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

A.1. 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 Credential Management System (CMS)

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

Challenge

Random number generated by the server API for authentication of a user in the asynchronous (challenge/response) mode.

Cryptographic Service Provider (CSP)

An independent software module that performs cryptography algorithms for authentication, encoding, and encryption.

Discovery mode

Discovery mode enables a calling application to find out the size of the data that will be returned to by making a preliminary discovery call and then making a second call after it allocates a buffer large enough to accommodate the data that will be returned.

End-point card

The PIV standard defines two interfaces for communicating with PIV cards:

- The PIV transitional interface.
- The PIV end-point interface.

A PIV end-point card is a card that implements the second of these interfaces.

Note: The PIV transitional interface is not supported by the PIV API.

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.

Force change PIN flag

Flag which indicates whether the user must change the PIN on first use of the card.

Integrated circuit chip (ICC)	The chip on the smart card.
Mini Driver	Smart card middleware for the Microsoft platform that works with the Microsoft Base Smart Card CSP (Cryptographic Service Provider). The ActivClient Mini Driver replaces the ActivClient CSP available in previous versions. The Mini Driver architecture provides stronger cryptographic services.
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)	The Personal Identification Number (PIN) code used to access an HID Global device's services such as Windows PKI logon, remote access and email signature. HID Global devices can only be used after a correct PIN is entered.
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.
Unlock code	Value that the card holder needs to provide in order to unlock a locked smart card. Depending upon the smart card unlock mechanism, the unlock code may or may not be different from the unlock key.
Verification	Process in which a signature that was produced by the signing operation is verified.
Weak PIN	A weak PIN is a PIN in which: • The length is less than three characters or digits, or • The difference between each character or digit, and the following one is a constant. For example, a PIN that is a sequence of the same number (1111) or an increasing/decreasing sequence of numbers (1234, 4321) is a weak PIN.

A.2. Acronyms

CA	Certificate Authority
CAC	Common Access Card (for the United States Department of Defense)
CSP	Cryptographic Service Provider
CUID	Card Unique Identifier
	CUID is a number that uniquely identifies a card.
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

