



15370 Barranca Parkway
Irvine, CA 92618



ADMINISTRATION GUIDE

Product Version C1150

November 2013

HID GLOBAL CONFIDENTIAL AND PROPRIETARY INFORMATION. Use and disclosure of this information is strictly restricted by the terms of a non-disclosure agreement with HID Global Corporation. If you have received this information and are not an intended recipient or are not subject to or do not agree to be bound by the terms of the non-disclosure agreement, please immediately return this document to HID Global Corporation, 15370 Barranca Pkwy, Irvine, CA 92618-3106. © 2013 HID Global Corporation. All rights reserved.

Contents

About this Guide.....	6
1.1 Purpose	6
1.2 Audience.....	7
1.3 Scope of Document	7
1.4 Typographic Conventions.....	7
2.0 Introduction.....	8
2.1 Product Overview	8
2.2 Installation and Upgrades.....	9
2.3 Supported Deployment Modes	9
2.3.1 Standalone Mode with Mini Driver.....	10
2.3.2 Standalone Mode with Advanced Middleware	10
2.3.3 Managed Mode with Microsoft Forefront Identity Manager (FIM)	11
2.3.4 Managed Mode with HID Global naviGO	11
2.3.5 Managed Mode with HID Global 4TRESS AAA Server	11
2.3.6 Managed Mode with HID Global ActivID CMS and ActivID CMS Appliance	12
2.4 Choosing Smart Card Middleware	12
2.4.1 Services Available with Both Mini Driver and ActivClient.....	12
2.4.2 Additional Services Available with ActivClient.....	13
3.0 Installing the Mini Driver.....	15
3.1 Mini Driver System Requirements.....	15
3.2 Automatic Download.....	15
3.3 Manually Download and Install the Mini Driver	15
3.4 Uninstall the Mini Driver.....	19
4.0 Managing a Smart Card with the Mini Driver.....	20
4.1 Prerequisites.....	20
4.2 Issuing a Smart Card using Microsoft Certificate Authority.....	21
4.2.1 Enroll a Smart Card for a User with Internet Explorer.....	21
4.2.2 Enroll a Smart Card for a User with MMC	22
4.3 Importing Certificates Using Microsoft Windows	30
4.3.1 Download a PKI Certificate with Internet Explorer	30
4.3.2 Download a PKI Certificate with MMC	31
4.4 Changing the PIN Code Using Microsoft Windows	40
4.4.1 Change the PIN Code on Microsoft Windows Vista, Windows 7 or Windows 8	40
4.4.2 Change the PIN Code on Microsoft Windows XP	41
4.5 Unlocking the PIN Code Using Microsoft Windows	44
4.5.1 Unlock the PIN Code on Microsoft Windows Vista, Windows 7 or Windows 8	44
4.5.2 Unlock the PIN Code on Microsoft Windows XP	47

5.0	Managing a Smart Card using Microsoft Forefront Identify Manager (FIM).....	50
5.1	Prerequisites.....	50
5.2	Initialize a Permanent Card	51
5.3	Change the PIN Code Using FIM	53
5.4	Unlocking the Smart Card Using FIM - Online	55
5.4.1	Unlock the Smart Card as an Administrator	55
5.4.2	Unlock the Smart Card as an End User	59
5.4.3	Using the Unblock Wizard	60
5.5	Unlocking the Smart Card Using FIM - Offline	61
5.5.1	Verify that the Offline Unlock Policy is Enabled	61
5.5.2	Launch Offline Unlock Request.....	64
5.6	Reset the Smart Card Using FIM	71
6.0	Managing a Smart Card with ActivClient	73
6.1	Issue a Smart Card with ActivClient	73
6.2	Change the PIN Code with ActivClient.....	76
6.3	Unlock the Smart Card Using ActivClient.....	78
6.4	Reset the Smart Card Using ActivClient	80
6.5	Importing Certificates Using ActivClient	83
6.5.1	Request a Certificate	83
6.5.2	Import the Certificate	84
7.0	Managing a Smart Card with naviGO	85
7.1	Prerequisites.....	85
7.2	Initialize a Smart Card	85
8.0	Managing a Smart Card with 4TRESS AAA Server	97
8.1	Issue a Smart Card Using 4TRESS AAA Server	98
8.2	Change the PIN Code	102
8.3	Unlock the Smart Card with 4TRESS AAA Server.....	102
8.3.1	Unlock the Smart Card with the Administration Console	102
8.3.2	Unlock the Smart Card with the Web Help Desk	103
8.3.3	Unlock the Smart Card with the Web Self Help Desk	103
8.4	Importing Certificates.....	105
9.0	Using the Smart Card	106
9.1	Logging On to Microsoft Windows.....	106
9.2	Authenticating to Secure Websites	106
9.3	Sending and Reading Secure Emails.....	107
9.3.1	Send Signed/Encrypted Emails	107
9.3.2	Read Signed/Encrypted Emails.....	107
9.4	Encrypting and Decrypting Files.....	107
9.4.1	Encrypt a File or Folder	107
9.4.2	Decrypt a File or Folder	108

10.0	Troubleshooting	109
10.1	ActiveX Error During Certificate Requests	109
10.2	Smart Card Enrollment Errors	109
10.2.1	Wrong CSP	109
10.2.2	Key Length Setting	109
10.2.3	Enrollment Rights	110
11.0	Security Guidelines	111
11.1	SHA-2 Compliance	111
11.1.1	Card Content Signed with SHA-2	111
11.1.2	Using SHA-2 for Digital Signature Operations	112
11.2	PIN Policies	113
11.3	Log Handling	113
11.4	Additional Recommendations	113

Copyright

© 2013 HID Global Corporation. All rights reserved.

Trademarks

HID GLOBAL, HID, the HID logo, Crescendo, OMNIKEY, ActivID ActivClient, 4TRESS and ActivID CMS are trademarks or registered trademarks of HID Global Corporation, or its licensors, in the U.S. and other countries.

Revision History

Date	Author	Description	Document Version
JAN13	SIS	Added managed with 4TRESS AAA Server procedures.	A.1
NOV13	SIS	Updated with default PIN details and HID Unblock tool.	A.2

Contacts

North America

15370 Barranca Parkway
Irvine, CA 92618
USA

Phone: 800 237 7769

Fax: 949 732 2120

support.hidglobal.com

About this Guide

The information contained in this document is provided “AS IS” without any warranty.

HID GLOBAL HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH REGARD TO THE INFORMATION CONTAINED HEREIN, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT.

IN NO EVENT SHALL HID GLOBAL BE LIABLE, WHETHER IN CONTRACT, TORT OR OTHERWISE FOR ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING FROM USE OF INFORMATION CONTAINED IN THIS DOCUMENT.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

1.1 Purpose

This document describes different options how you can manage and use your HID® Crescendo™ smart card with a variety of software options.

The Crescendo C1150 smart card is versatile and can be deployed in standalone mode (that is, without any central card management system) or in an enterprise-managed environment (that is, with a central card management system).

The Crescendo C1150 smart card can be used on a variety of environments, providing a wide range of strong authentication, digital signature and encryption services – such as secure Windows logon, secure authentication to web sites, secure authentication to remote sessions, email digital signature, email and file encryption.

This document presents the services available via the Crescendo C1150 Mini Driver, a free middleware from HID Global designed specifically for this card. The Mini Driver is compatible with a number of card management systems (such as Microsoft® Forefront Identity Manager or HID Global naviGO™) and end-user applications (such as Microsoft Windows®, Internet Explorer®, Microsoft Office® or Adobe® Acrobat).

The document also presents additional services available via the HID Global ActivID ActivClient™ middleware, bringing support for additional applications (such as Mozilla® Firefox® or remote access / VPN products).

NOTE

The instructions provided for third party products are meant as guidance only. HID Global cannot be held liable for any malfunctioning from configuring these products; refer to the vendor documentation for complete information.

1.2 Audience

This manual is specifically designed for IT administrators, who want to use their HID Crescendo C1150 card to obtain strong authentication in their Microsoft environment.

1.3 Scope of Document

This document assumes that the system administrator has already installed and configured other necessary components (such as Microsoft Windows, a certificate server) and that you have a Crescendo C1150 card.

1.4 Typographic Conventions

Typography	Description
Arial bold	Action steps: paths, buttons, options (checkboxes). Field and drop-down list labels. Notes, important notes, and warnings. Emphasis and captions.
<i>Italic black</i>	File names, document titles, and file extensions.
ARIAL BOLD SMALL CAPS CUSTOM BLUE	“Callouts” used to flag important tips or technical information.
Arial blue	Cross-references within the document (no underlines).

2.0 Introduction

2.1 Product Overview

This release of the Mini Driver is designed to support the Crescendo C1150 and is a key component of the HID logical and physical access convergence solution.

Crescendo smart cards include a PKI chip that provides extended cryptographic capabilities, expanding the number of supported services:

- Authenticate to Microsoft Windows (online or offline).
- Authenticate to secure web sites.
- Authenticate to remote networks via a VPN.
- Authenticate to remote sessions authentication using Citrix® or Microsoft terminal server technologies.
- Sign emails, forms and documents.
- Encrypt emails, documents and disks.

The Mini Driver also enables users to personalize their smart cards by:

- Defining a PIN code.
- Downloading certificates.

If the same smart card is used on a workstation with ActivID ActivClient instead of the Mini Driver, you have access to additional services, such as:

- PKI services with a PKCS#11 library (compatibility with Mozilla Firefox, Thunderbird®).
- Automated configuration for PKI applications (such as Microsoft Outlook).
- One-Time Password services enabling support for a wider range of remote access and VPN services.
- User-based card management services (card content viewer, diagnostics tool, notifications, standalone management services, etc.).

2.2 Installation and Upgrades

The Mini Driver is a free component and can be automatically downloaded from Microsoft Windows Update (applicable to Windows 7, Windows Server 2008 R2 and later versions).

NOTE If a supported middleware is already installed on the machine, the Windows Update download is not triggered.

It is also available for download as a Microsoft Windows installer package (.msi) from the HID web site <http://www.hidglobal.com/main/crescendo/>

This is useful for:

- Older Windows versions where the automatic download is not available.
- Workstations not connected to the internet, or with Windows Update disabled.

For further information about the installation process, see chapter [3.0 Installing the Mini Driver](#) on page [15](#).

In addition, the installer package detects potential middleware existing on the machine and acts accordingly. For example, if the ActivClient middleware is detected, the Mini Driver installation is not possible as you cannot have two middleware for the same card on the same Windows workstation, and as ActivClient provides enhanced services compared to the Mini Driver.

NOTE If the Crescendo C1150 card is used with its Mini Driver (installed either from Windows Update or by the MSI package), you can upgrade to ActivClient 6.2 (version 6.2.0.162 or later) to gain access to additional services. When ActivClient is installed, it takes precedence over the Mini Driver.

2.3 Supported Deployment Modes

This section describes several Crescendo C1150 deployment modes, either in standalone mode (that is without any central card management system), or in an enterprise managed environment (that is, with a central card management system).

Some of these deployment modes require the Crescendo C1150 Mini Driver, which is free middleware from HID Global. Some deployment modes require additional software products, such as ActivID ActivClient, Microsoft Forefront Identity Manager, and HID Global naviGO. Contact the product vendor for licensing information.

2.3.1 Standalone Mode with Mini Driver

This is the simplest (and also least secure) mode in which the Mini Driver can be installed and used with the Crescendo C1150 card to provide the following services:

- The card comes with a default PIN code (00000000) that you can change at any time:
 - On Microsoft Windows Vista and 7 - using the native Ctrl+Alt+Del Change Password feature.
 - On Microsoft Windows XP - using the Microsoft PIN Tool (*pintool.exe*) included with the Base Smart Card CSP package.
- While there is no “simple” PIN unlock feature, if you know the ADMIN Key (set to a default binary value 00) and have a tool to generate a response based on the challenge (3DES algorithm), you can unlock the card.

The user can then use the Microsoft Windows 7 or Windows 8 PIN Unlock user interface. It is recommended that you use card management software to manage these keys.
- You can download a certificate onto the card from the Microsoft Certificate Authority (or other CA), by selecting the Microsoft Base Smart Card CSP.
- You can use certificates for standard PKI services based on the Mini Driver, such as Windows logon, authentication to web sites (with Internet Explorer) and PKI-compatible VPNs, email signature and encryption (with Microsoft Outlook).

For further information, see chapter [4.0 Managing a Smart Card with the Mini Driver](#) on page [20](#).

2.3.2 Standalone Mode with Advanced Middleware

Using advanced middleware such as ActivID ActivClient, you have access to additional card management services, and you can use your card with more applications.

- You can initialize a Crescendo C1150 card with the ActivClient PIN Initialization Tool, resetting the PIN from the default value and obtaining a static unlock code.
- You can change the PIN using the ActivClient PIN Change Tool (on any Windows version).
- If the card PIN is locked, you can unlock it with the static unlock code displayed at initialization.
- You can reset the card with the ActivClient PIN Initialization Tool.
- You can download a certificate onto the card from the Microsoft CA (or other CA) by selecting the ActivClient CSP.
- You can use certificates for standard PKI services based on the CSP or PKCS#11 technologies, which provides more options than in the previous mode – such as Windows logon, authentication to web sites (with Internet Explorer or Mozilla Firefox) and PKI-compatible VPNs, email signature and encryption (with Microsoft Outlook or Lotus Notes).
- The user can use other ActivClient services for improved usability (card management utility, card activity notification, application auto-configuration, etc.).

For further information, see chapter [6.0 Managing a Smart Card with ActivClient](#) on page 73.

2.3.3 Managed Mode with Microsoft Forefront Identity Manager (FIM)

In this mode, the card is managed with Microsoft Forefront Identity Manager (FIM), and end users can use the card on their workstation with either the Mini Driver or with advanced middleware.

- The card is managed by Microsoft FIM 2010 via the Mini Driver.
- The card comes with a default PIN (00000000) and default ADMIN Key (binary value 00). The Administrator imports this data into FIM.
- With FIM, the administrator can load certificates on the card (and update them later), and unlock the card PIN if it is locked.
- If the end user has the Crescendo C1150 Mini Driver on his workstation, he can use certificates for standard PKI services based on the Mini Driver.
- If the end user has ActivClient on his workstation, he can use certificates for standard PKI services based on the CSP or PKCS#11 technologies. He can also use other ActivClient services for improved usability.

For further information, see chapter [5.0 Managing a Smart Card using Microsoft Forefront Identify Manager \(FIM\)](#) on page [50](#).

2.3.4 Managed Mode with HID Global naviGO

In this mode, the card is managed with naviGO; end users use the card on their workstation with the Crescendo Mini Driver.

- The card is managed by naviGO via the Mini Driver.
- With naviGO, the administrator can load certificates on the card (and update them later), and unlock the card PIN if it is locked.
- The default PIN code (00000000) is used during the issuance process.
- The default ADMIN Key is 00 (binary value).
- The end user has the Crescendo C1150 Mini Driver on his workstation; he can use certificates for standard PKI services based on the Mini Driver.
- naviGO also provides emergency access authentication in case the card is lost or forgotten.

For further information, see chapter [7.0 Managing a Smart Card with naviGO](#) on page 85.

2.3.5 Managed Mode with HID Global 4TRESS AAA Server

In this mode, the card is managed with 4TRESS AAA Server 6.7 (version 6.7.2.15 or later), and end users can use the card on their workstation with the ActivClient middleware (version 6.2.0.162 or later).

4TRESS AAA Server adds one-time password services to Crescendo C1150 cards, enabling support for legacy applications that are not PKI-enabled, such as many remote access and VPN applications.

- The card is managed by 4TRESS AAA Server via the ActivClient middleware.
- The administrator initializes the Crescendo C1150 cards with 4TRESS AAA Server, adding one-time password (OTP) capabilities to the cards.
- Administrators or end users can download a certificate onto the card from the Microsoft CA (or other CA), by selecting the ActivClient CSP.
- If the card PIN is locked, you can unlock it with the challenge/response unlock code managed by 4TRESS AAA Server.
- The end user has ActivClient on his workstation; he can use certificates for standard PKI services based on the CSP or PKCS#11 technologies.
- He can also use the Crescendo C1150 for remote access/VPN services using one-time passwords.
- He can also use other ActivClient services for improved usability.

For further information, see section [8.0 Managing a Smart Card with 4TRESS AAA Server](#) on page [97](#).

2.3.6 Managed Mode with HID Global ActivID CMS and ActivID CMS Appliance

To deploy Crescendo cards with ActivID Card Management System (CMS), use the Crescendo C1100 instead of the Crescendo C1150.

To deploy Crescendo cards with ActivID CMS Appliance, use the Crescendo C800 instead of the Crescendo C1150.

2.4 Choosing Smart Card Middleware

You have a choice of Crescendo C1150 smart card middleware for end user workstations:

- You can choose to deploy the Crescendo C1150 Mini Driver, which is available free of charge.
- You can choose to deploy the ActivClient software that provides enhanced capabilities.

This section presents the similarities and differences between the two options.

2.4.1 Services Available with Both Mini Driver and ActivClient

Both middleware options support the same applications for PKI services:

- Windows Logon
- Web authentication with Internet Explorer and Google Chrome
- VPN authentication with Windows, Cisco, Juniper, etc.
- Authentication to Citrix or Terminal Server sessions
- Email signature and encryption with Microsoft Outlook and Exchange

- Document signature with Microsoft Office and Adobe Acrobat
- File encryption with Windows EFS
- Disk encryption with Windows BitLocker To Go
- Compatibility with more applications based on Microsoft CAPI / CNG

Both middleware options support some basic card management services:

- PIN change
- PIN unlock (with Mini Driver, not applicable to all deployment modes – requires a card management system or utility to support the challenge / response unlock model)

2.4.2 Additional Services Available with ActivClient

The following services are available only with the ActivClient middleware:

- ActivClient is compatible with a wider range of PKI-enabled applications thanks to a PKCS#11 compliant library:
 - Web authentication with Firefox.
 - Email signature and encryption with Lotus Notes and Thunderbird.
 - Compatibility with more applications based on PKCS#11.
- ActivClient provides usability enhancements with Microsoft Outlook, enabling users to sign and encrypt emails without the need to learn how to configure and use it.
 - Outlook is automatically configured on card insertion with the user's signature and encryption certificates. This guarantees that users are using up-to-date credentials, and no longer use software certificates. This also automatically configures the hash and encryption algorithms for consistency within an organization.
 - Certificates are automatically published to the Exchange Global Address List (GAL) on card insertion. This guarantees that all email encryption is performed with up-to-date certificates.
 - Contacts' certificates are automatically added to the user's Outlook Contacts upon reception of an email.
 - Option to automatically decrypt and save encrypted emails. This guarantees that older encrypted emails can be read even if old encryption key is not on the card.
- ActivClient provides usability enhancements with Firefox and Thunderbird, making it easier to use PKI services with Mozilla products: ActivClient PKCS#11 library is automatically registered into these apps, to automatically enable new users with smart card services, negating the need for additional configuration and training.

- ActivClient enables using smart cards with additional credentials than PKI keys and certificates. ActivClient supports one-time passwords (OTP) on the Crescendo C1150 card, enabling organizations to use smart cards for remote access (authentication to VPNs) even if these systems are not PKI-capable. Organizations that have deployed an OTP Strong Authentication Server (such as 4TRESS AAA Server) and OTP hardware tokens or soft tokens can now deploy smart cards to additional users and enable a mixed OTP token / Crescendo smart card deployment. This enables a smooth transition to PKI environments.
- ActivClient includes a User Console to view and edit the card content (certificates and other credentials). This console helps identify certificates on the card vs. all the certificates loaded on the PC, as Windows does. The console also enables importing keys and certificates into the card, and exporting certificates from the card. Users can also select a “default certificate” in the case several Windows Logon certificates are present on the card.
- ActivClient includes utilities to manage the Crescendo smart cards in standalone mode: initialization, unlock, reset cards. This provides organizations with a simple and efficient model to deploy and manage smart cards in small deployments when a card management system may be considered too complex.
- ActivClient includes a smart Card indicator icon in Windows notification area, which, helps identify when the card is in use.
- ActivClient provides notifications to end users, helping them use and manage their smart card. For example:
 - Certificate expiration notification, informing users that their certificates need to be updated before they expire, preventing users to log on.
 - Unattended card notification, reminding users to take their card when they leave their workstation.
 - No smart card reader notification, informing users when no reader is detected.
- ActivClient has close to 100 policies, enabling organizations to configure the middleware to match their specific security and usability requirements. For example:
 - Option to unregister certificates on card removal or logoff: this is a security feature for shared workstations.
 - PIN cache for increased usability: the ActivClient PIN Cache provides a sort of SSO for the PIN: users enter the PIN once, use it for multiple services (Windows Logon, secure email, secure web, etc.), and securely! PIN Cache policies provide the right mix of security and usability; for example PIN Cache timeout (by default 15 min – configurable), or “Per-process” PIN cache (one PIN entry per application).
- ActivClient supports additional smart cards in addition to the Crescendo C1150, and is certified by NIST and GSA to support the FIPS 201 PIV standard smart cards.

3.0 Installing the Mini Driver

3.1 Mini Driver System Requirements

One of the following Microsoft operating systems is required:

- Windows XP SP3 (32 and 64-bit)
- Windows Vista SP1 (32 and 64-bit)
- Windows 7 and Windows 7 SP1 (32 and 64-bit)
- Windows 8 (32 and 64-bit)
- Windows Server 2003 (32 and 64-bit)
- Windows Server 2008 and 2008 SP2 (32 and 64-bit)
- Windows Server 2008 R2 (64-bit)
- Windows Server 2012 (64-bit)

NOTES

- Microsoft Windows XP and Server 2003 require a Windows update available at <http://support.microsoft.com/kb/909520> to install the Microsoft Smart Card Base CSP.
- The Crescendo C1150 Mini Driver is supported with PC/SC smart card readers.

3.2 Automatic Download

Crescendo C1150 Mini Driver can be downloaded automatically using the Microsoft Windows Update feature.

When you insert the Crescendo C1150 card into a reader connected to Microsoft Windows 7 or Windows 8 (32 and 64-bit) workstation, or Windows Server 2008 R2 or Windows Server 2012 (64-bit) server, the driver is automatically downloaded and installed.

3.3 Manually Download and Install the Mini Driver

If the automatic download is not available, the Mini Driver can also be downloaded as a Windows Installer (MSI) package from HID's web site:

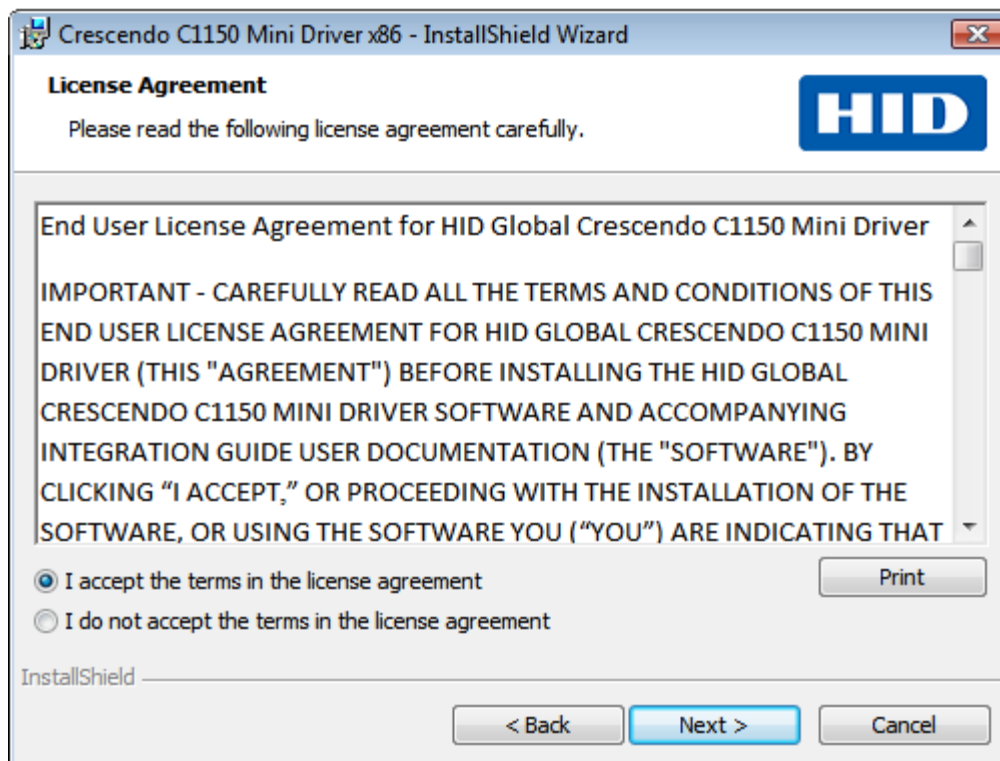
<http://www.hidglobal.com/main/crescendo/>.

- Crescendo C1150 Mini Driver x64 2.0.msi
- Crescendo C1150 Mini Driver x86 2.0.msi

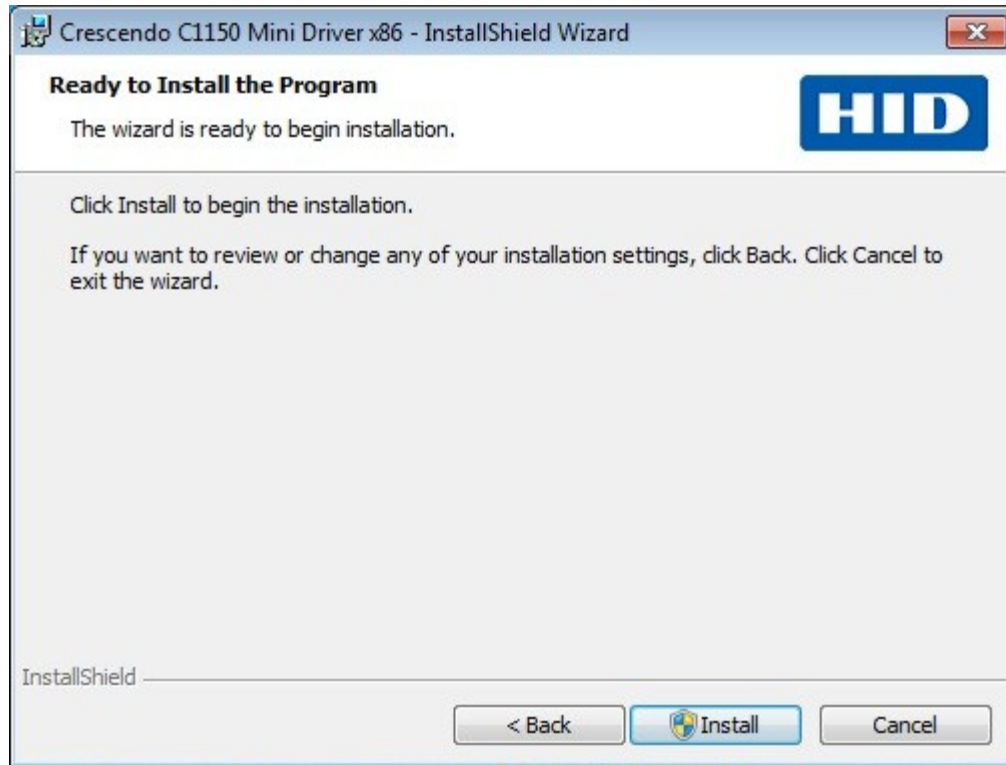
1. Launch the Mini Driver setup using the *.msi* file that corresponds to your operating system.



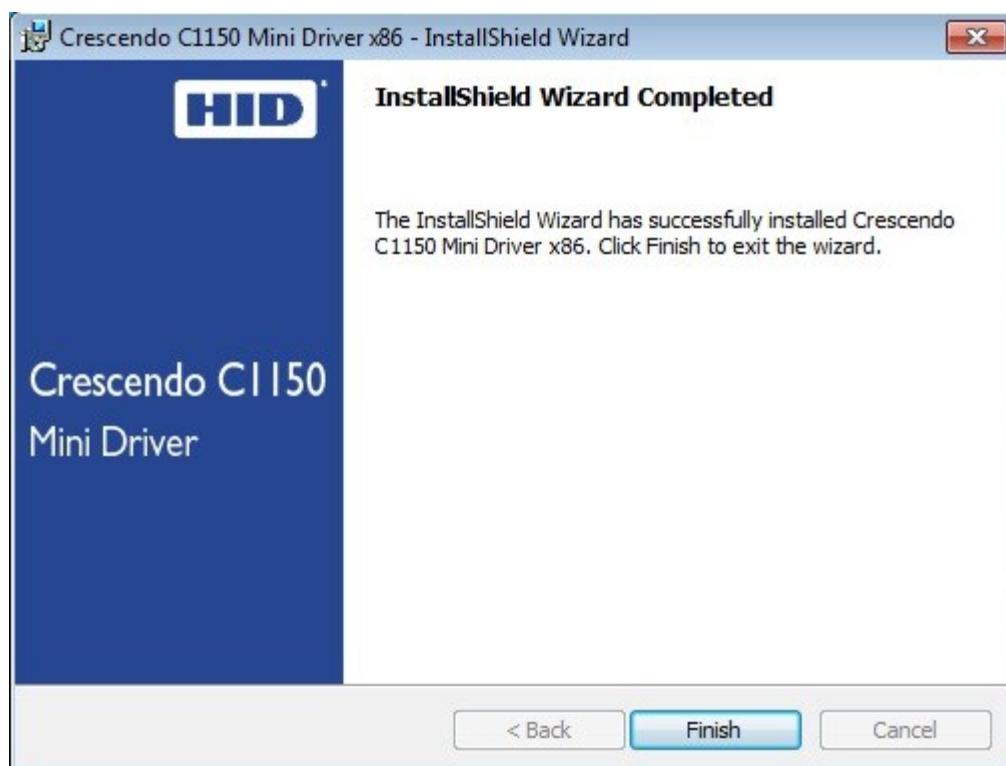
2. Click **Next**.



3. Select **I accept...** and click **Next**.



4. Click **Install**.



5. Click **Finish**.

The Mini Driver is installed in the following directory:

[ProgramFiles]\HID Global\Crescendo C1150 Mini Driver

3.4 Uninstall the Mini Driver

You can remove the Crescendo C1150 Mini Driver using the standard *Add/Remove Programs* (Microsoft Windows XP) or *Programs and Features* (Microsoft Windows 7 and Windows 8) tools.

4.0 Managing a Smart Card with the Mini Driver

This section explains how to issue a smart card for other users as well as for you.

NOTE

Enrollment for a smart card certificate must be a controlled procedure, in the same manner that employee badges are controlled for purposes of identification and physical access.

The recommended method for enrolling users for smart card-based certificates and keys is through the Smart Card Enrollment station that is integrated with Certificate Services in Microsoft Windows Server 2008.

Therefore, section 4.2 describes the process of how to enroll for a smart card user or smart card logon certificate through the Smart Card Enrollment Station. This process is likely completed by your system administrator.

As a user, request your own certificate through the Microsoft Certificate Services interface on your local workstation. In this case, a domain user cannot enroll for a Smart Card Logon certificate (which provides authentication) or a Smart Card User certificate (which provides authentication plus the capability to secure e-mail) unless a system administrator has granted the user access rights to the certificate template stored in Active Directory. This is described in section 4.3.

4.1 Prerequisites

- Microsoft Windows 2008 Server is installed and configured as a Primary Domain Controller.
- Active Directory is configured to manage users and computers.
- DNS Server is configured with your domain name.
- Internet Information Services (IIS) is installed (to be able to request a certificate through the Smart Card Enrollment Station).
- Microsoft Windows Certificate Services is installed and configured.
- Microsoft CA is configured with an issuance Certificate Template for smart card logon onto the domain. It must include the following certificates:
 - **Enrollment Agent** - a certificate intended for the entity that should be able to enroll certificates for other entities than itself. For example, when an administrator wants to deploy smart card logon certificates for the employees in an organization, he would require an “Enrollment Agent” certificate.
 - **Smartcard Logon** - intended for smart card logon onto the domain.
 - **Smartcard User** - an all-round certificate, intended both for smart card logon and, for example, signing and encrypting e-mail messages and web authentication.
- Microsoft CA Registration Authority (RA) station is created with:
 - All the drivers required for your HID Crescendo C1150 card and smart card reader.

- An Enrollment Agent Certificate configured with **Microsoft Enhanced Cryptographic Provider 1.0 or similar** as the CSP.

4.2 Issuing a Smart Card using Microsoft Certificate Authority

4.2.1 Enroll a Smart Card for a User with Internet Explorer

1. From the enrollment station, connect to the “Smart card Certificate Enrollment Station” web page of the CA.

This smart card enrollment web page can be found at **http://<machine-name>/certsrv/** where the <machine-name> is the machine where you have installed the CA.
2. Select Request a certificate.
3. Select advanced certificate request.
4. Select Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.

The Smart Card Certificate Enrollment Station window opens.

NOTE If you encounter an “ActiveX” error upon connecting to this page, see section [10.1 ActiveX Error During Certificate Requests](#) on page 109.

5. Under Enrollment Options:
6. From the Certificate Template drop-down list, choose **Smartcard User**.
7. From the Cryptographic Service Provider drop-down list, select **Microsoft Base Smart Card Crypto Provider**.
8. Ensure the correct Enrollment Agent certificate is selected in the **Administrator Signing Certificate** box.
9. Select a User to Enroll by clicking **Select User**.
10. Enter the user name in which you are enrolling a certificate in the **Enter the object name to select** field.
11. Click **Check Names** to verify the entry, and then click **OK**.
12. Verify the user’s smart card is inserted into the smart card reader.
13. Click **Enroll** to enroll a smartcard user certificate for the user.
14. Enter the PIN, and then click **OK** to continue.

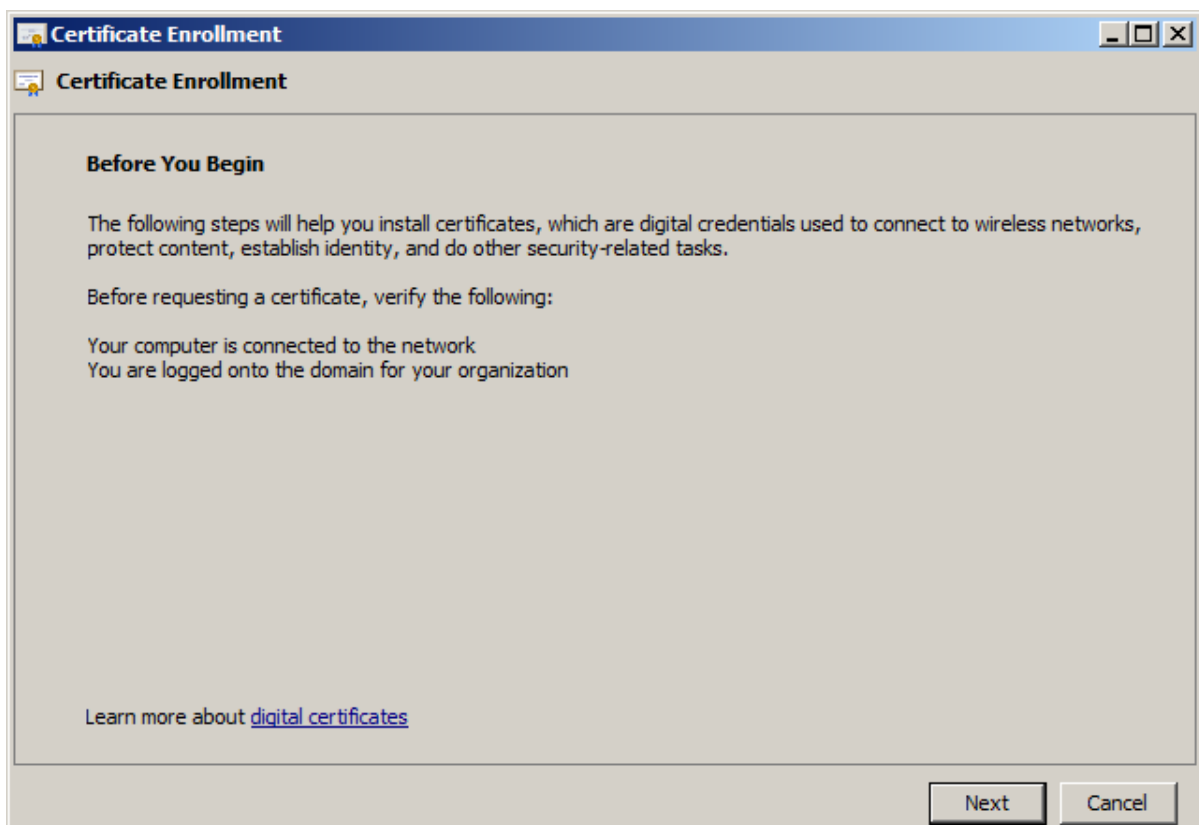
After the certificate request has been made, the CA will sign the request and return a certificate. This certificate is automatically placed on the smart card. You might be prompted to confirm the issuance of a certificate.

At the end of the smart card enrollment process, you are informed that the smart card is ready for use.

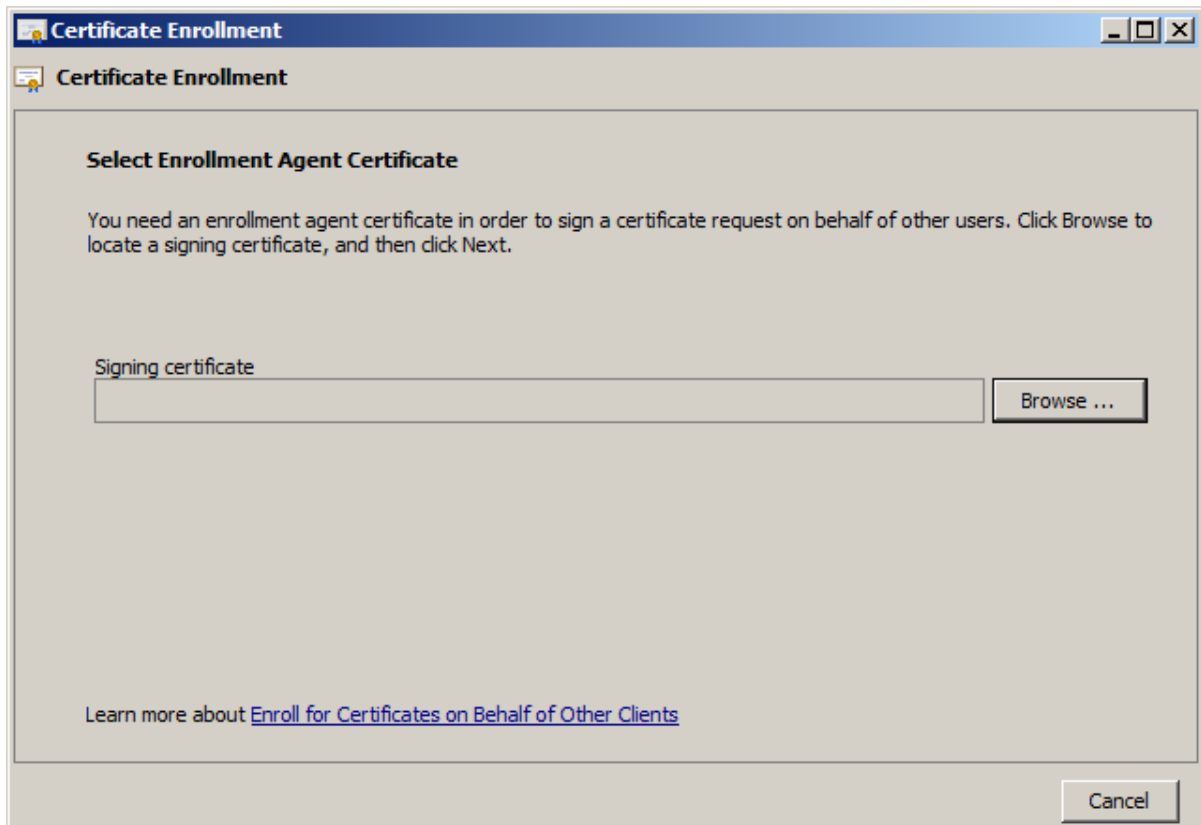
15. You can verify if the certificate contains the correct personal information about the user by clicking **View Certificate**. You also have the opportunity to enroll a new user by clicking **New User**.

4.2.2 Enroll a Smart Card for a User with MMC

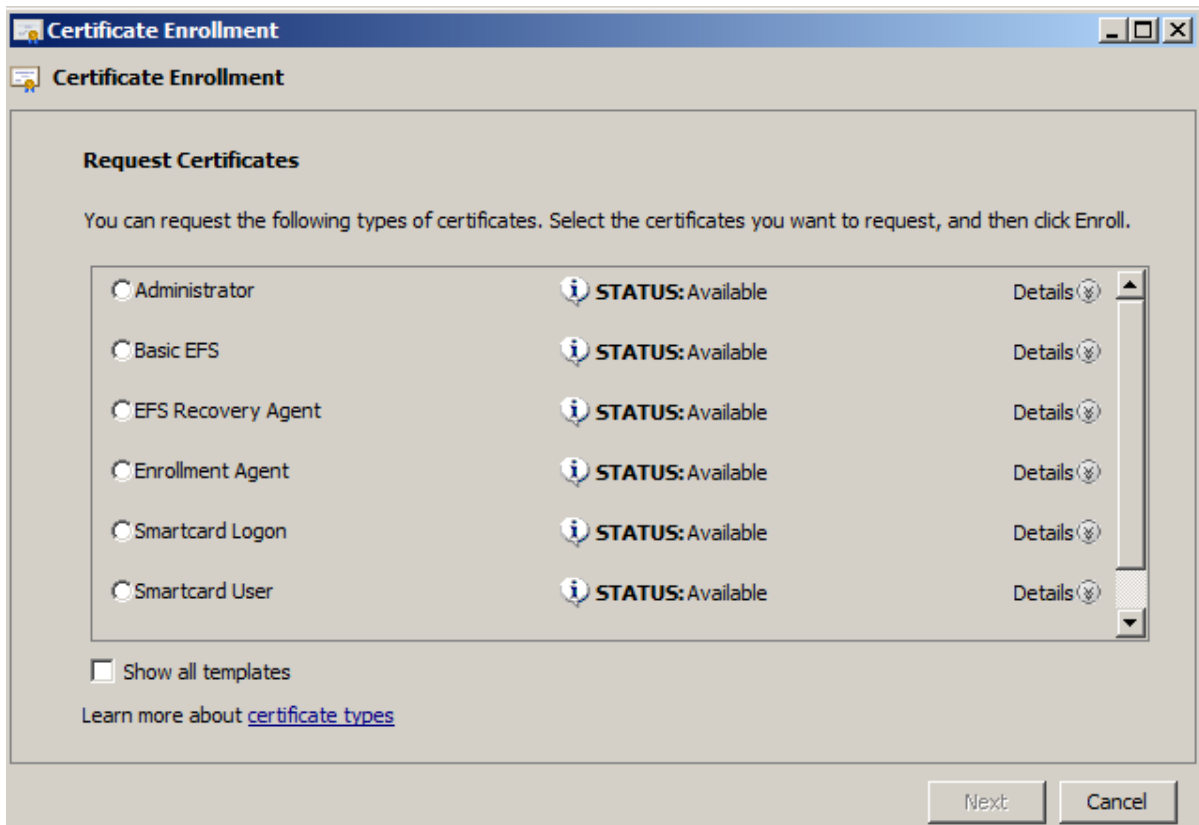
1. Open the management console by typing **mmc** in the **Start > Run** menu.
2. Add the Certificates snap-in from the **File > Add/Remove Snap-in** menu.
3. Right-click on the **Certificates** node.
4. Go to **All Tasks**, then **Advanced Operations**, and then click **Enroll on behalf of**.



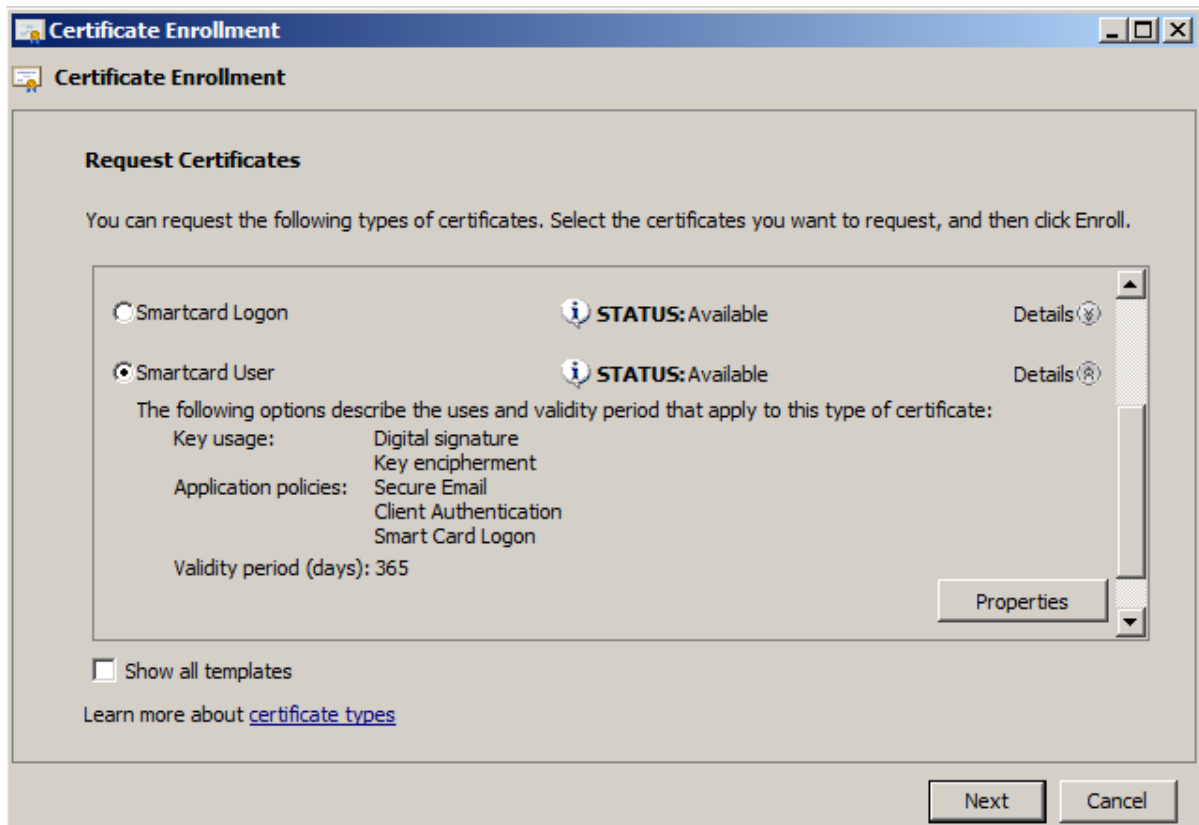
5. Click **Next**.



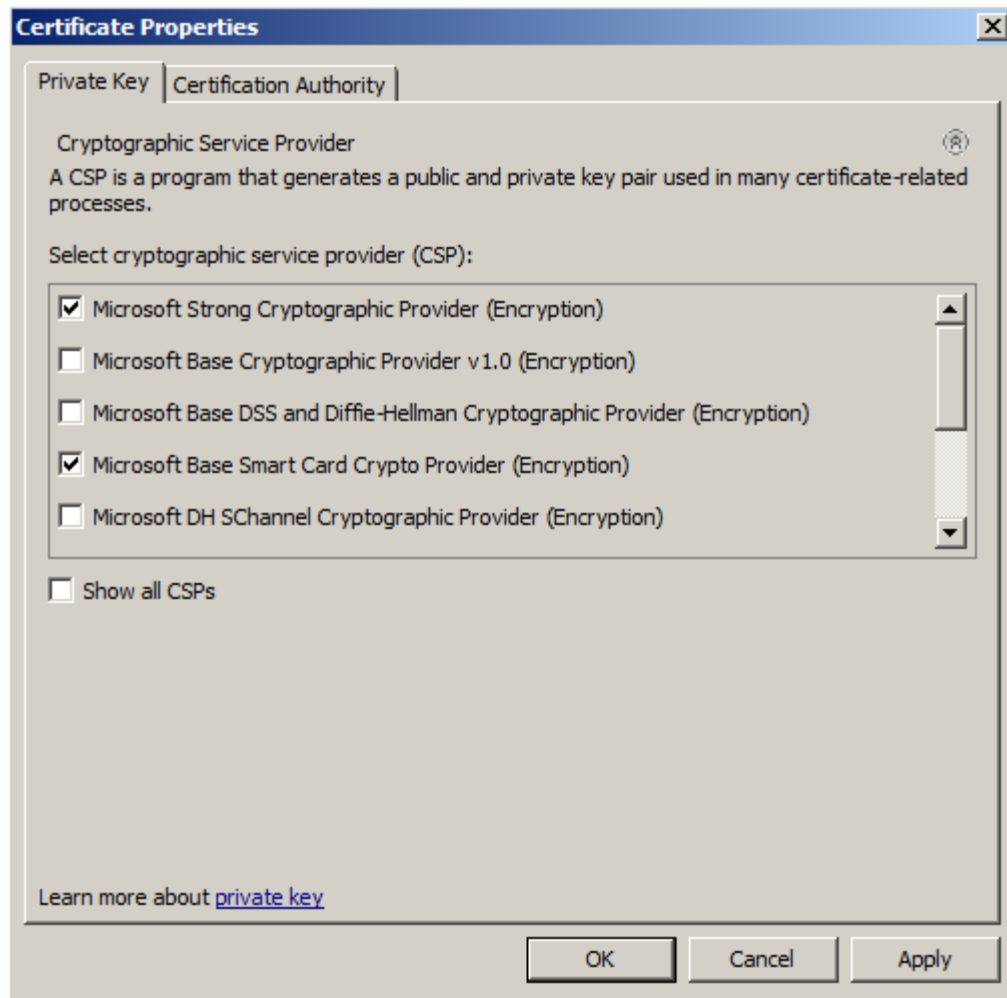
6. Browse to the Enrollment Agent Certificate that you created on the enrollment station.



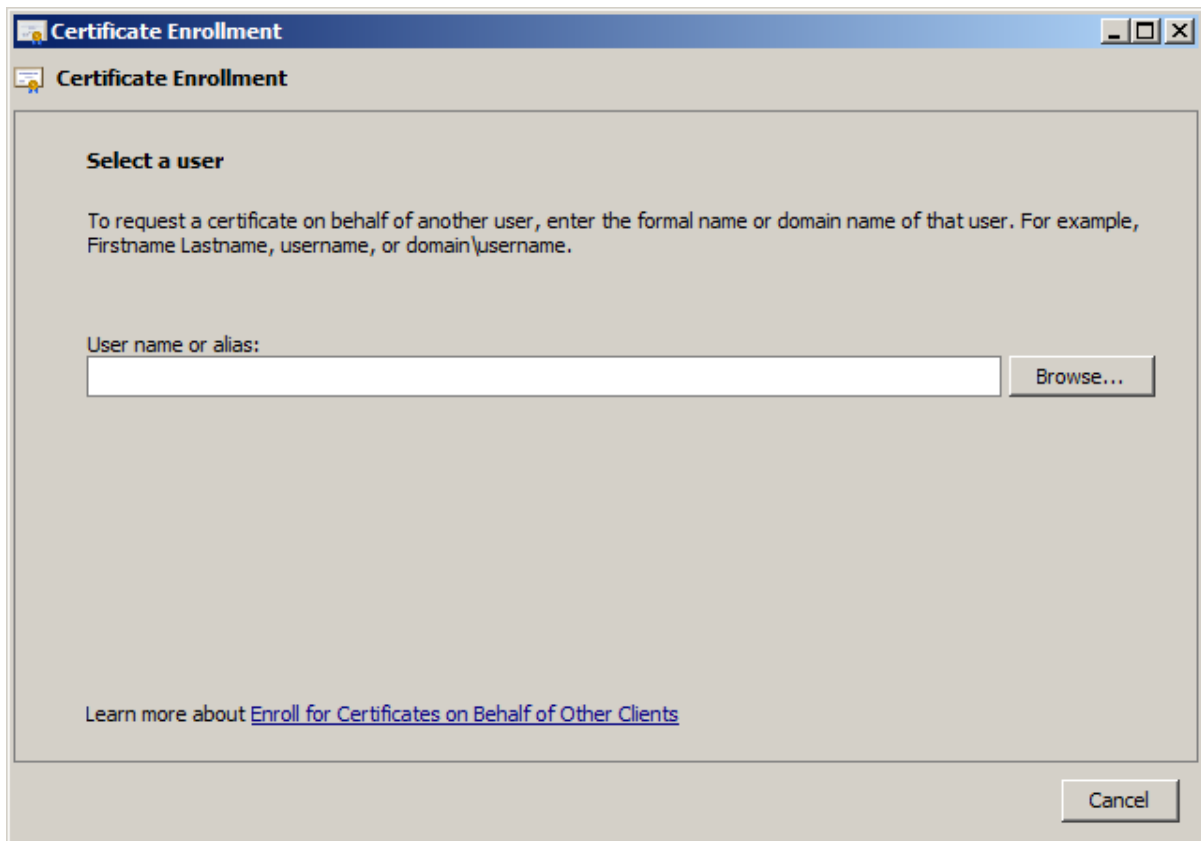
7. Select **Smartcard User**, and expand the **Details** view.



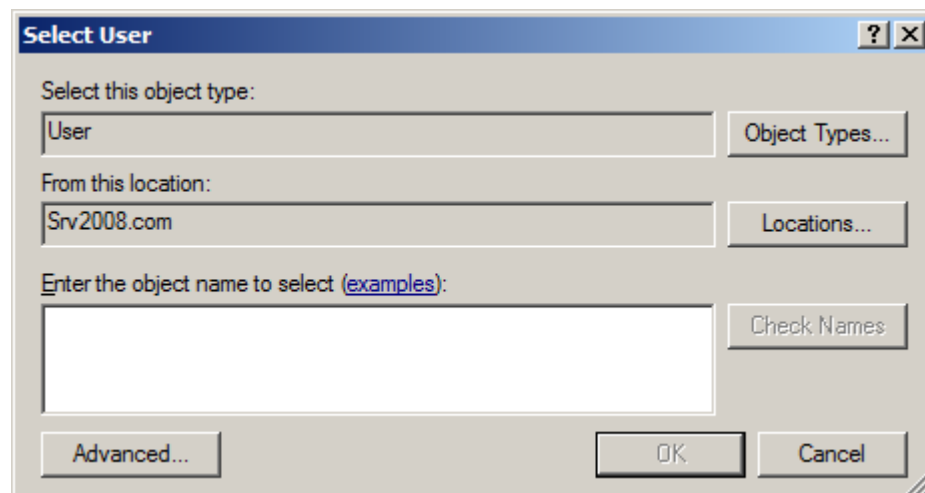
- Click **Properties**.



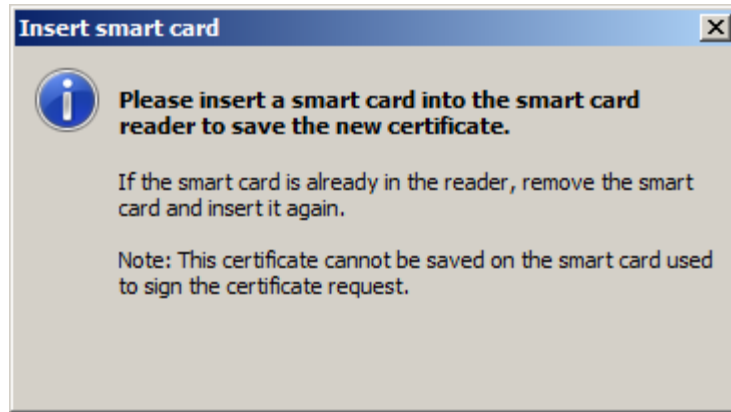
9. Make sure that **Microsoft Base Smart Card Crypto Provider** is selected as the CSP, and click **OK**.



10. Click **Browse** to select the user for whom you want to enroll the smart card.

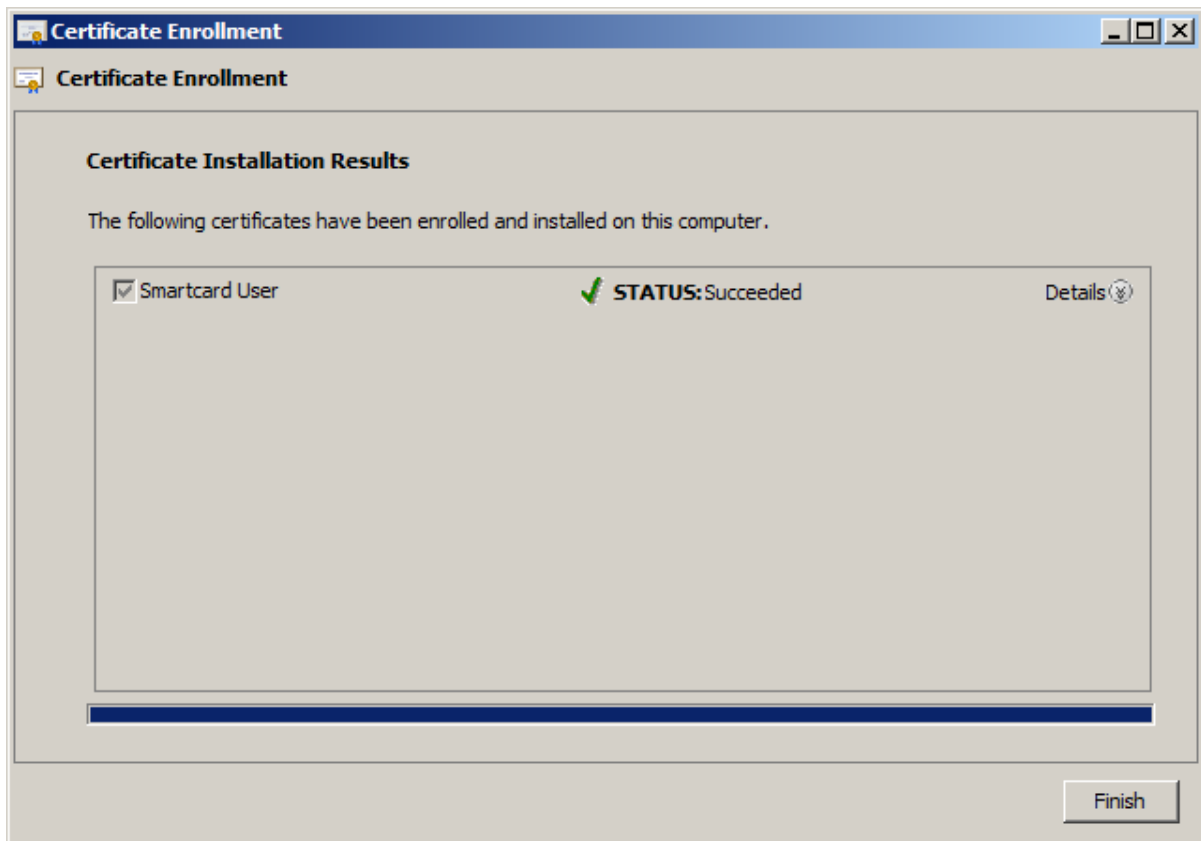


11. Enter the user name, and click **OK**. If necessary, click **Check Names** to make sure you have selected the correct user.



12. When prompted, insert the smart card into the reader.
13. If you are prompted to enter the PIN, do so and then click **OK** to continue.

After the certificate request has been made, the CA will sign the request and return a certificate. This certificate is automatically placed on the smart card.



14. Click **Finish**.

4.3 Importing Certificates Using Microsoft Windows

You can download PKI certificates from the CA onto the smart card using Internet Explorer or Microsoft Management Console (MMC).

4.3.1 Download a PKI Certificate with Internet Explorer

Microsoft Active Directory Certificate Services -- CA2010

Advanced Certificate Request

Certificate Template:

Smartcard User ▼

Key Options:

☒ Create new key set ☐ Use existing key set

CSP: Microsoft Base Smart Card Crypto Provider ▼

Key Usage: ☒ Exchange

Key Size: 1024 Min:1024
Max:2048 (common key sizes: [1024](#) [2048](#))

☒ Automatic key container name ☐ User specified key container name

☐ Mark keys as exportable

☐ Enable strong private key protection

Additional Options:

Request Format: ☒ CMC ☐ PKCS10

Hash Algorithm: sha1 ▼
Only used to sign request.

☐ Save request

Attributes:

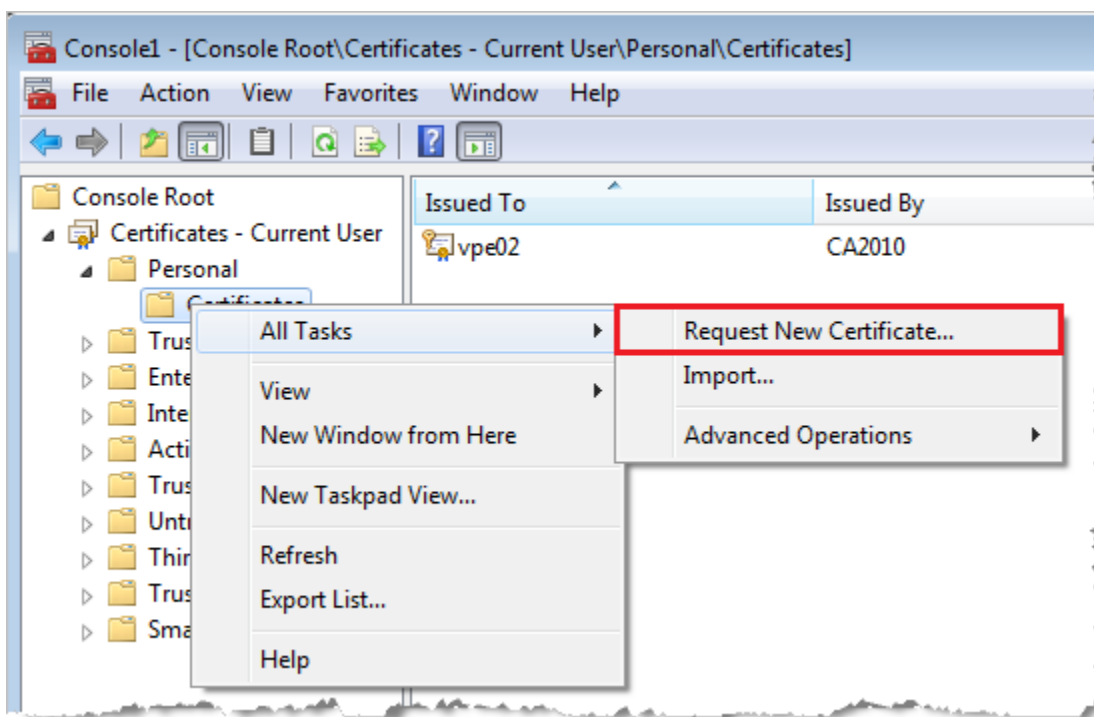
Friendly Name:

When creating the certificate request, make sure that the **Microsoft Base Smart Card Crypto Provider** is selected as the CSP.

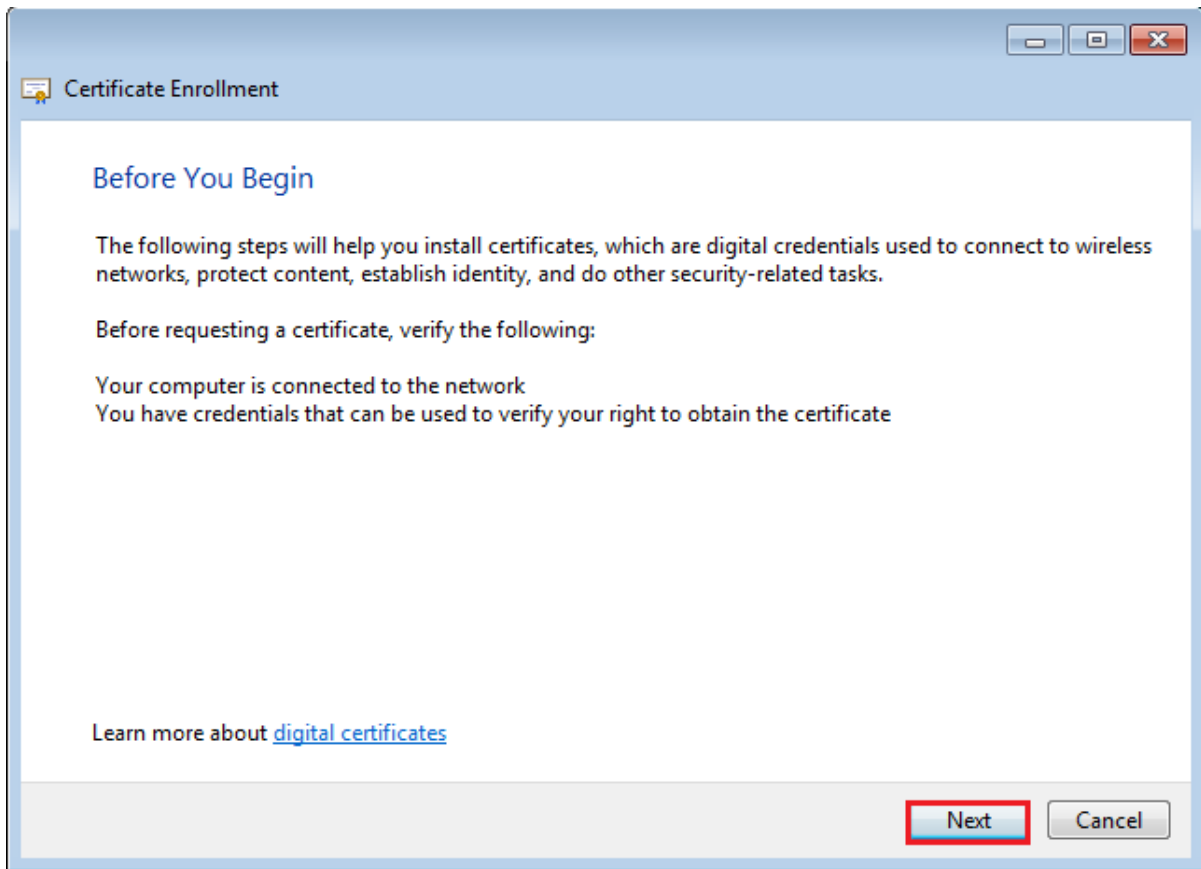
You will then be prompted for your PIN code to sign the certificate request, and asked to install the certificate on your smart card.

4.3.2 Download a PKI Certificate with MMC

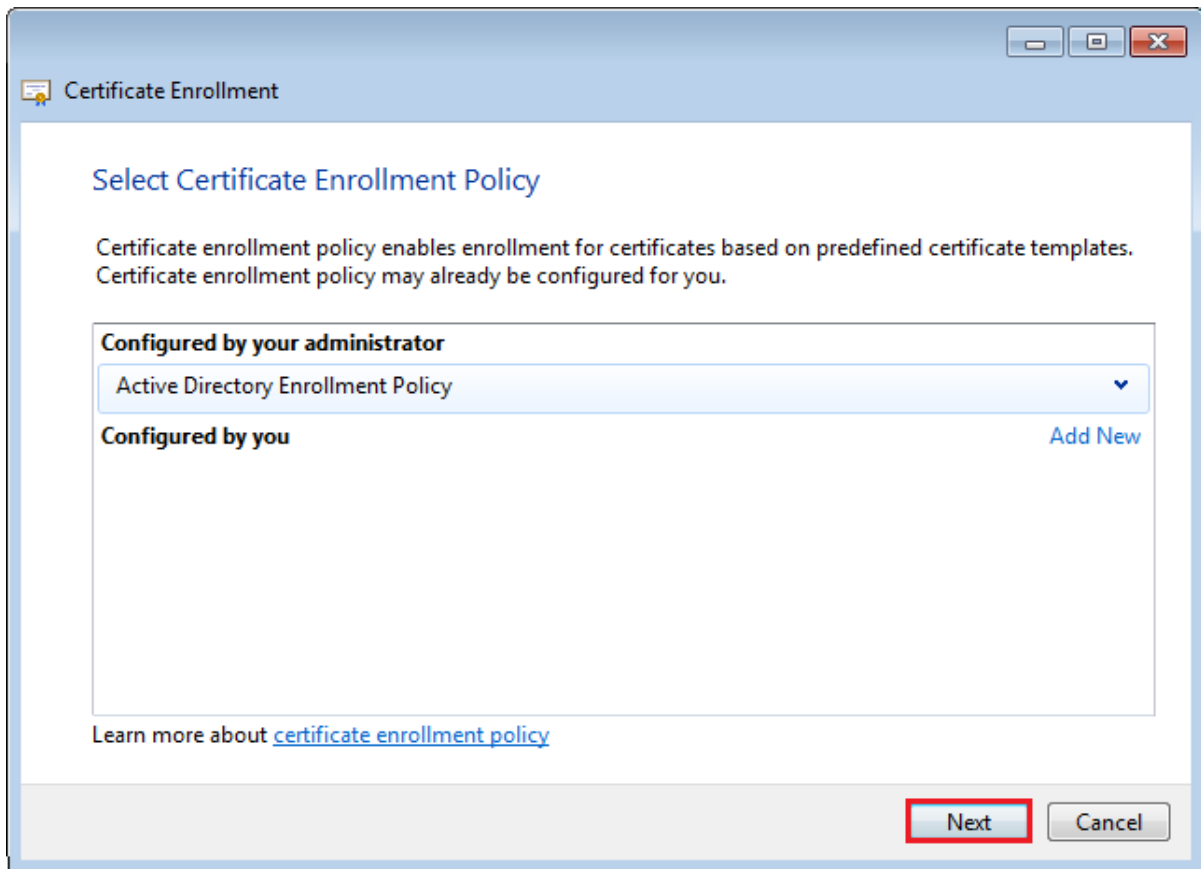
1. Open the management console by typing **mmc** in the **Start > Run** menu.
2. Add the Certificates snap-in from the **File > Add/Remove Snap-in** menu.



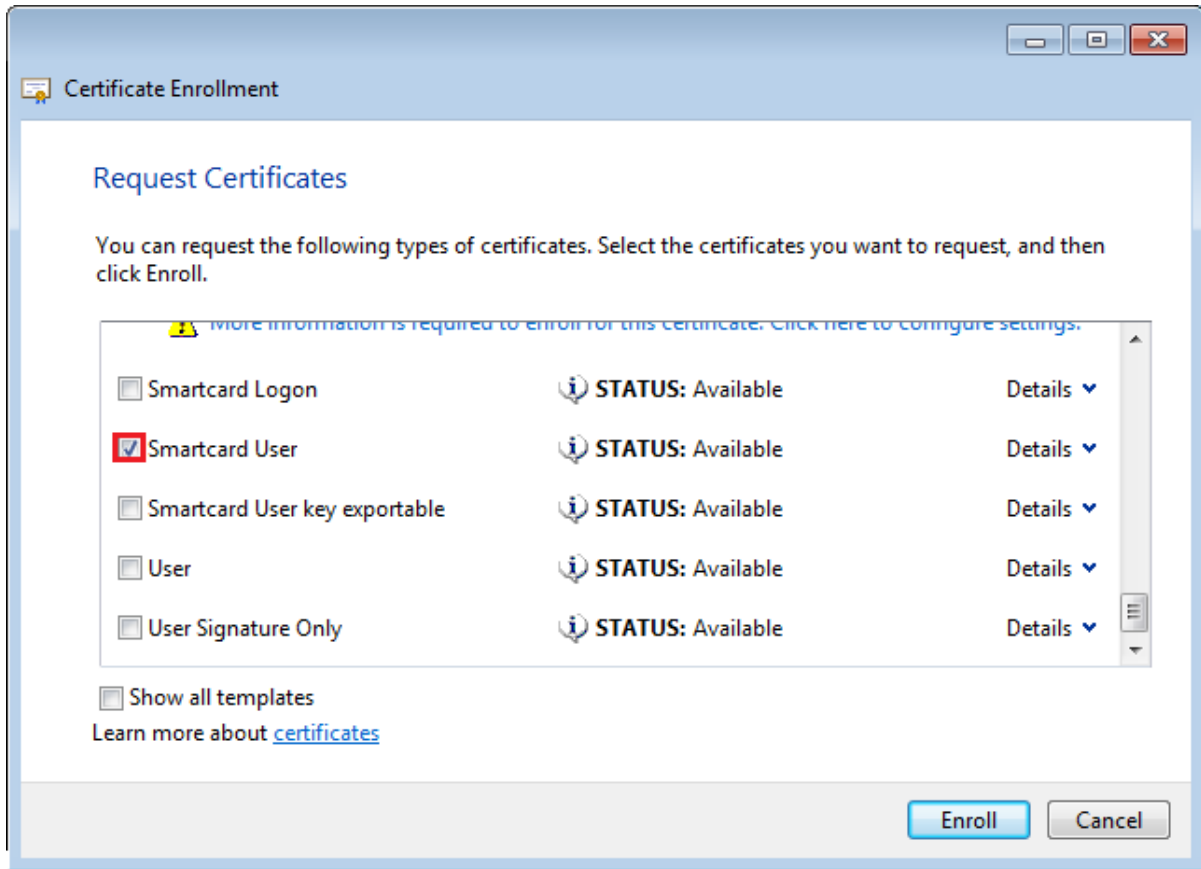
3. Right-click on the **Certificates** node.
4. Go to **All Tasks**, and then click **Request New Certificate**.



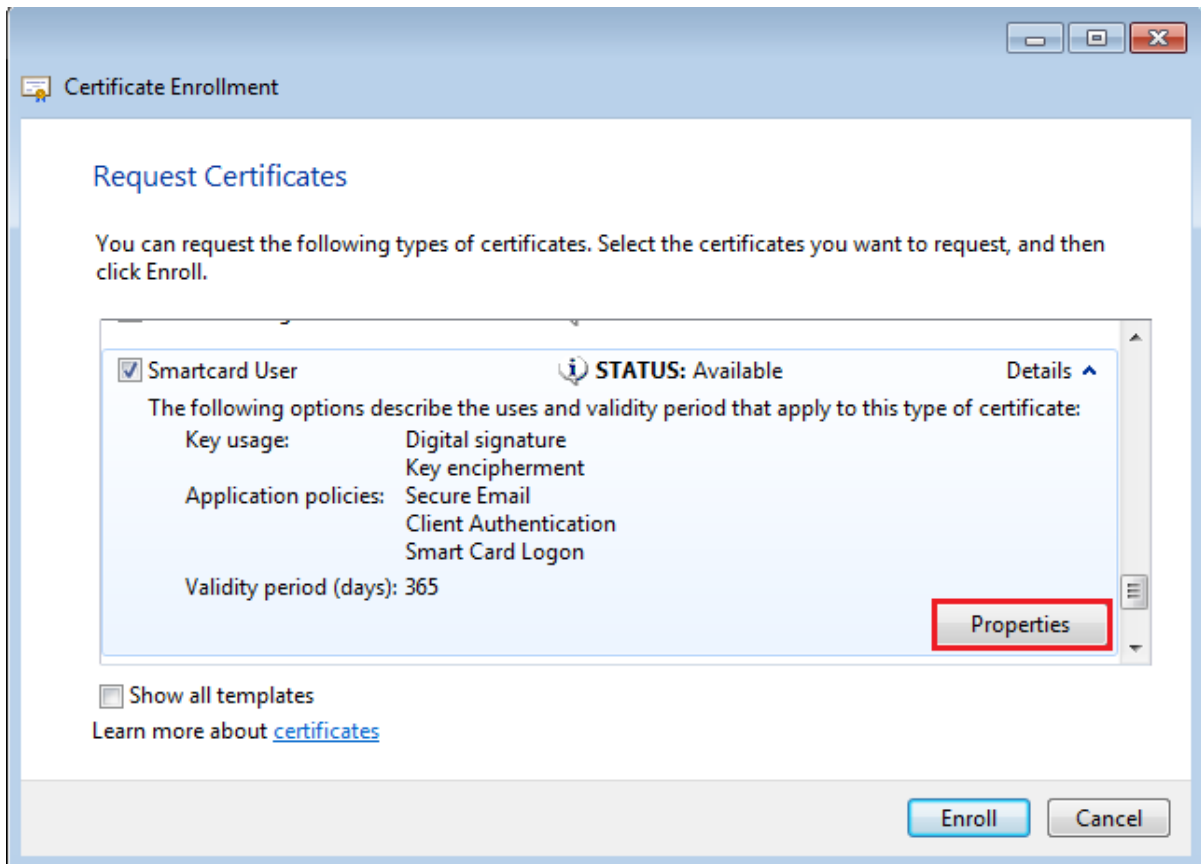
5. Click **Next**.



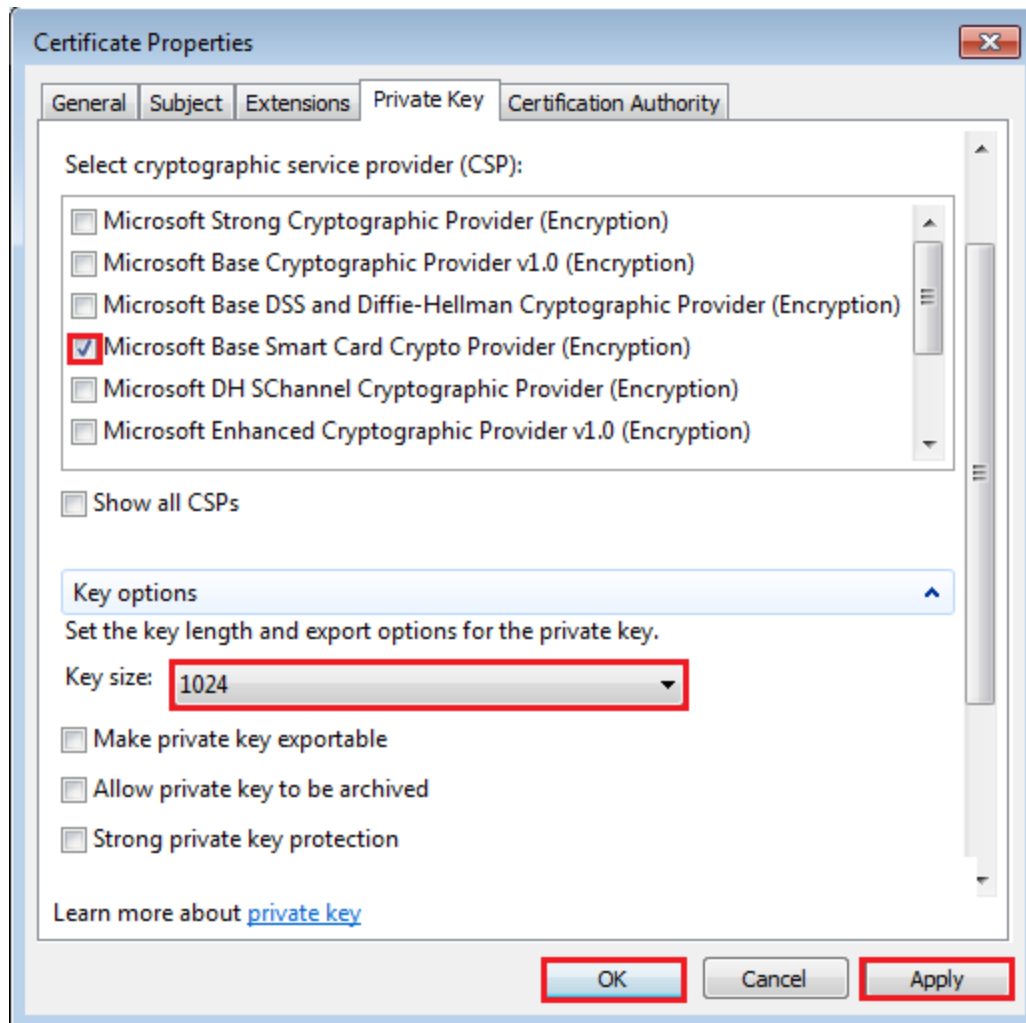
6. Verify that the correct Enrollment Policy is configured and click **Next**.



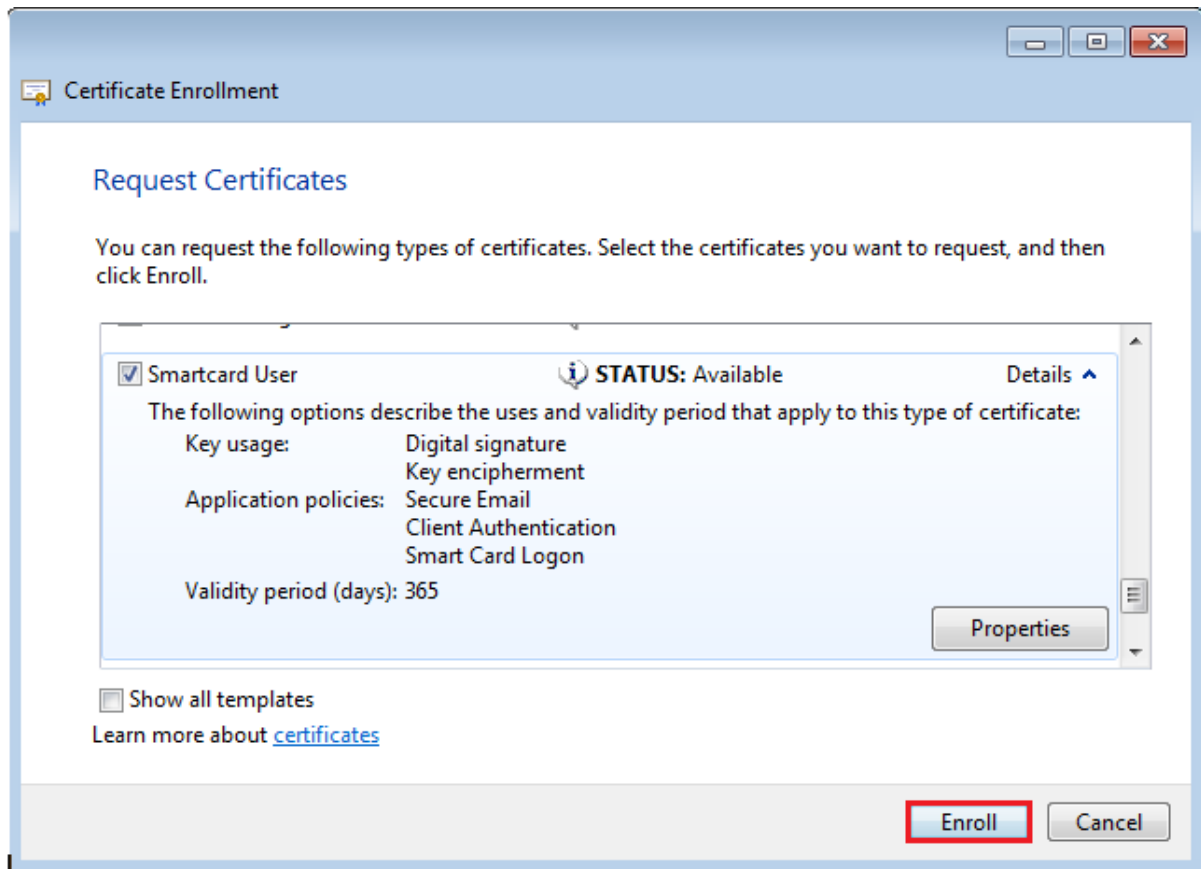
7. Expand the **Details** view to display the template settings.



8. If you need to edit the template settings, click **Properties**, and then select the **Private Key** tab.

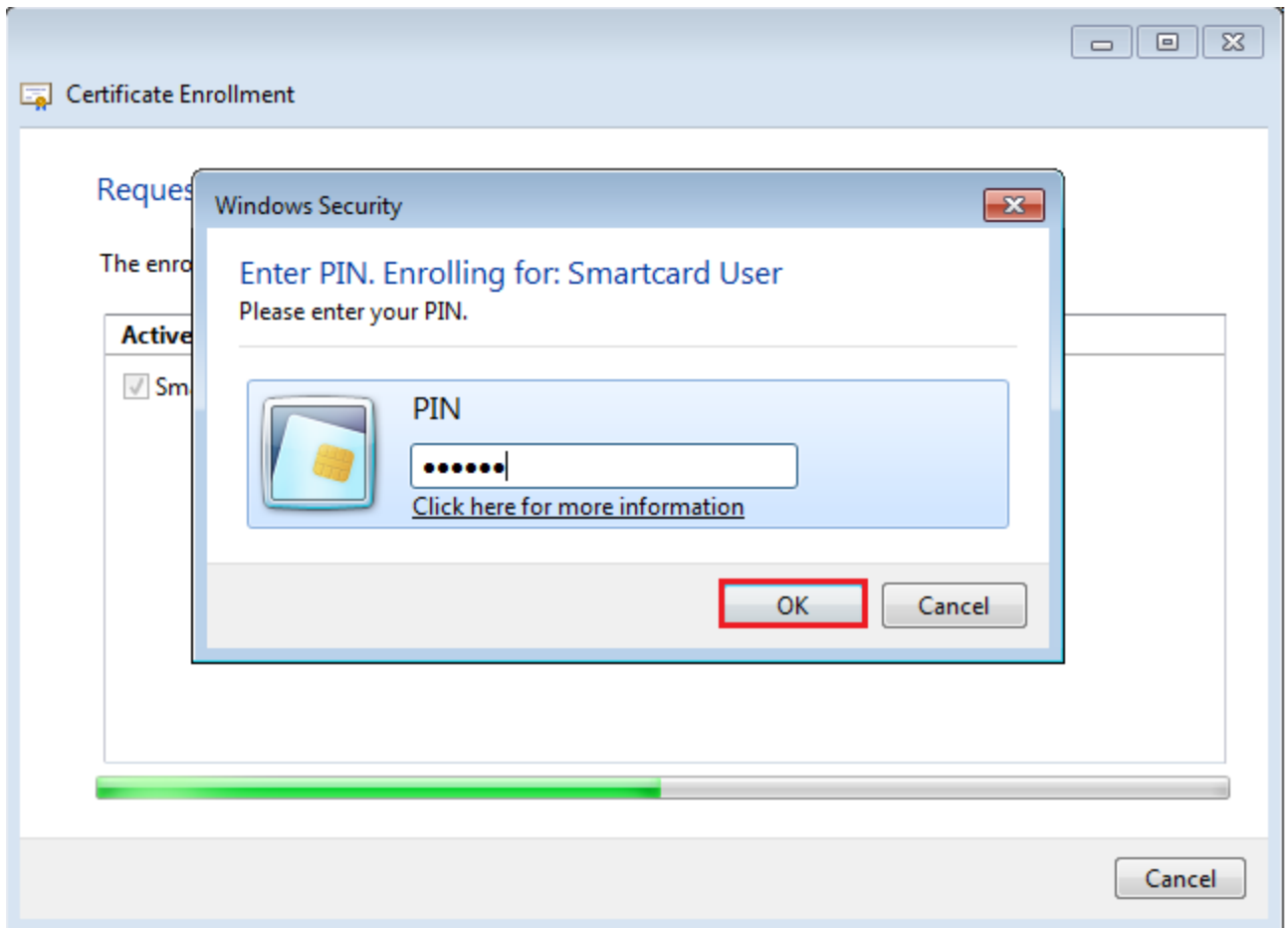


9. Make sure that the **Microsoft Base Smart Card Crypto Provider** is selected as the CSP and that the Key size is set to **1024** or **2048**.
10. Click **Apply** and then **OK**.

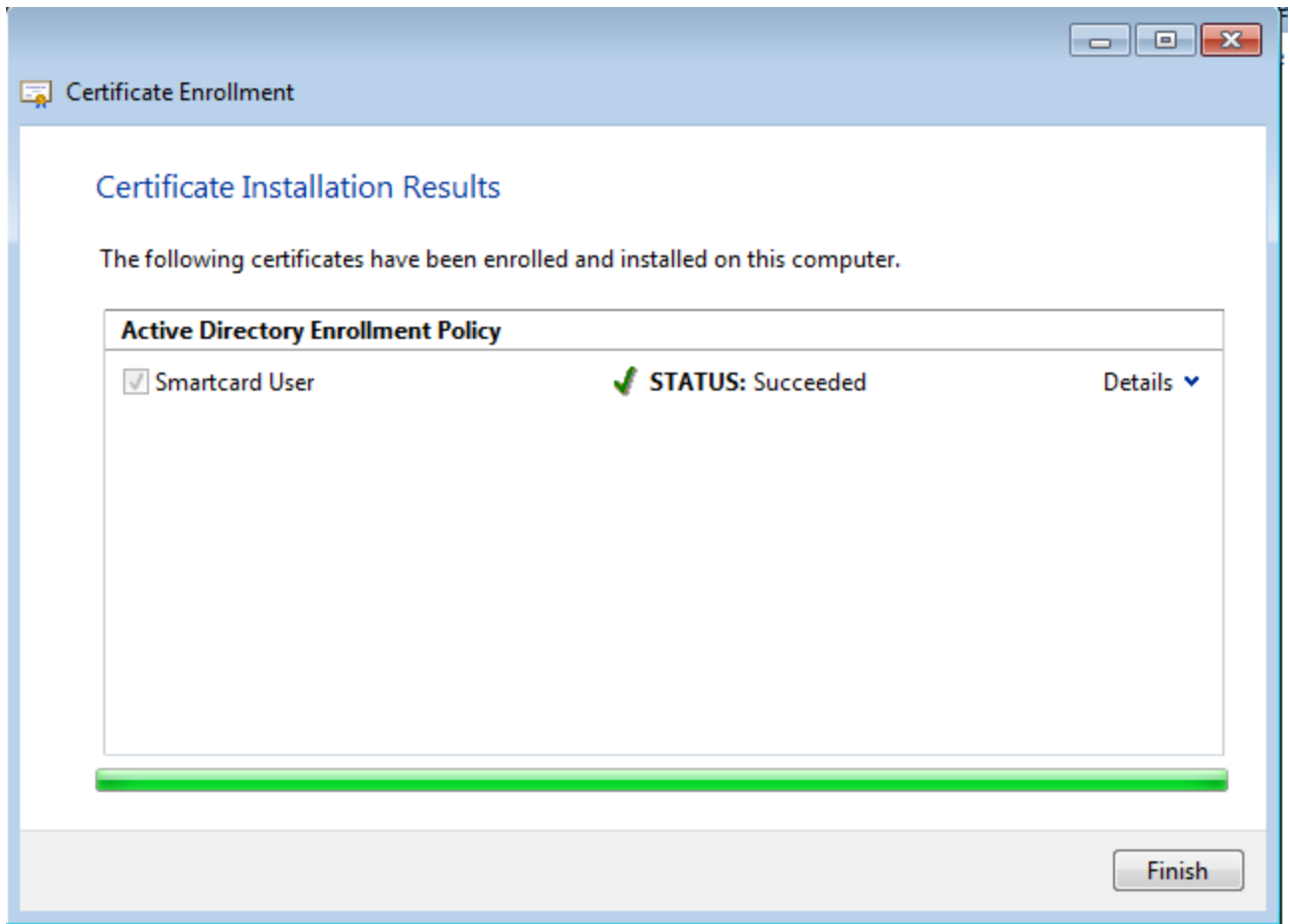


11. Click **Enroll**.

You might be prompted to enter your PIN code.



12. Enter the PIN code and click **OK**.



The new certificate and the corresponding key are stored on your smart card.

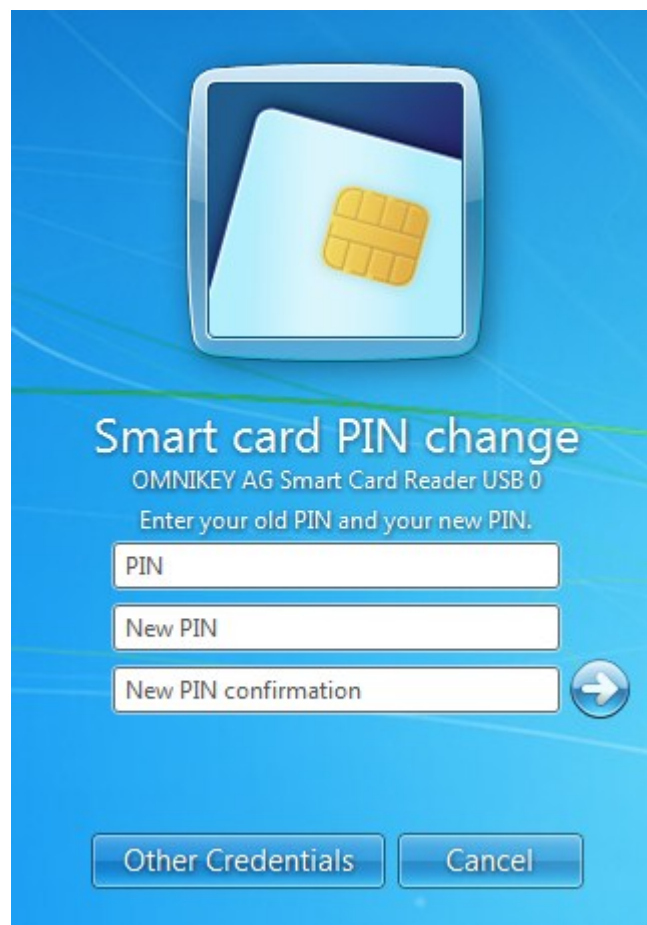
4.4 Changing the PIN Code Using Microsoft Windows

You can change the PIN code using tools specific to your operating system.

NOTE The default PIN code is 00000000.

4.4.1 Change the PIN Code on Microsoft Windows Vista, Windows 7 or Windows 8

You can change the PIN code using the Change Password option from the CTRL+ALT+DELETE feature.

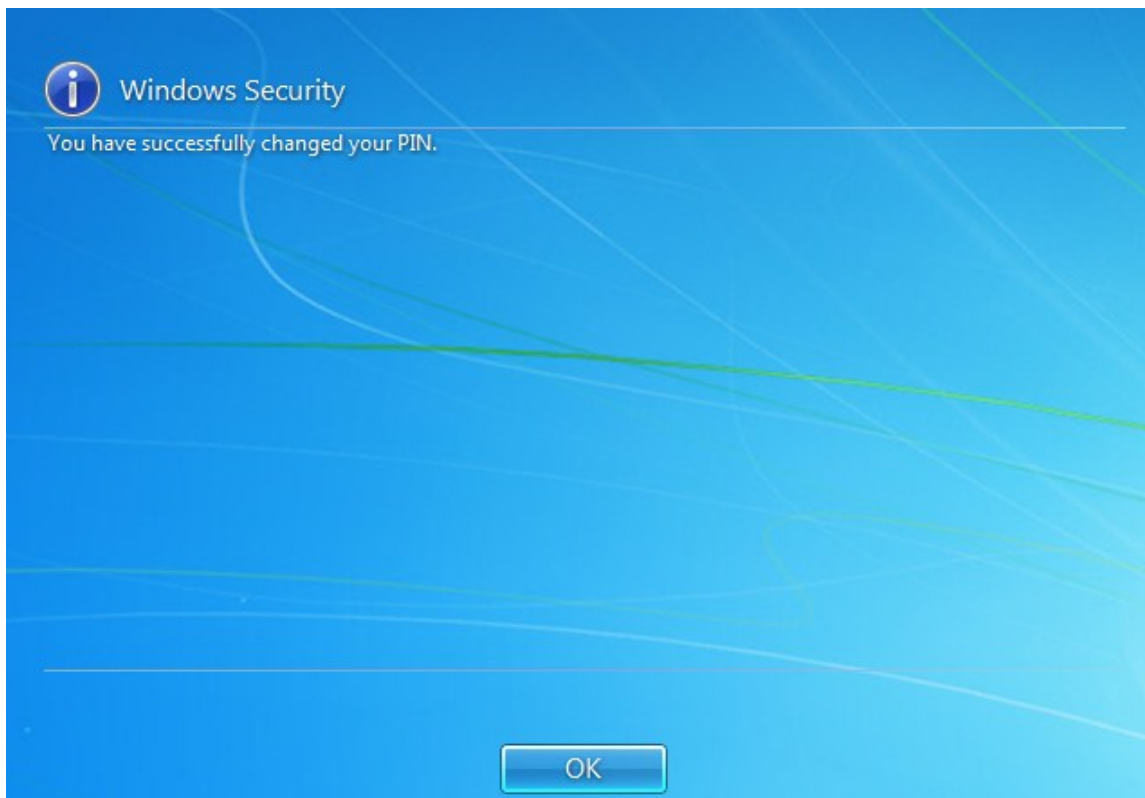


1. Enter the current PIN code in the **PIN** field (the default PIN code is 00000000).
2. Enter and confirm the new PIN code, and then click the arrow (or press **Enter**).

The new PIN code must meet the PIN policy:

- PIN is 4 to 14 characters long.

- Weak PIN values are not allowed (a PIN is considered weak if the difference between consecutive characters is fixed – for example, 1234, ABCD, 86420, acegik are considered weak PINs).



3. Click **OK** to return to your Windows session.

4.4.2 Change the PIN Code on Microsoft Windows XP

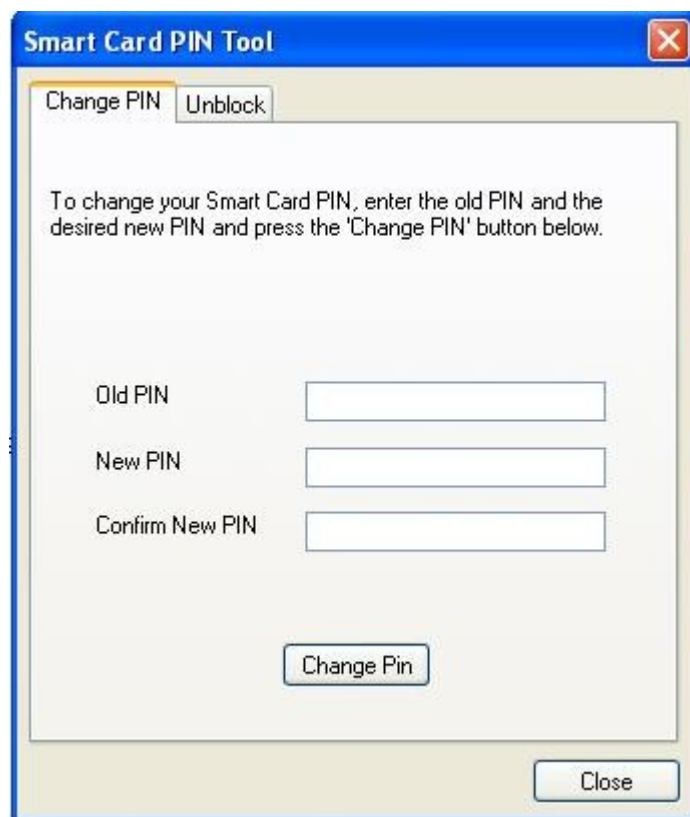
You can change your PIN code using the Microsoft PIN Tool (*pintool.exe*) included with the Base Smart Card CSP Package (for further information, see <http://support.microsoft.com/kb/909520>).

The PINTool.exe is located in the **%WINDOWS%\system32** directory.

1. Insert a valid smart card into the reader.



2. Click **OK**.

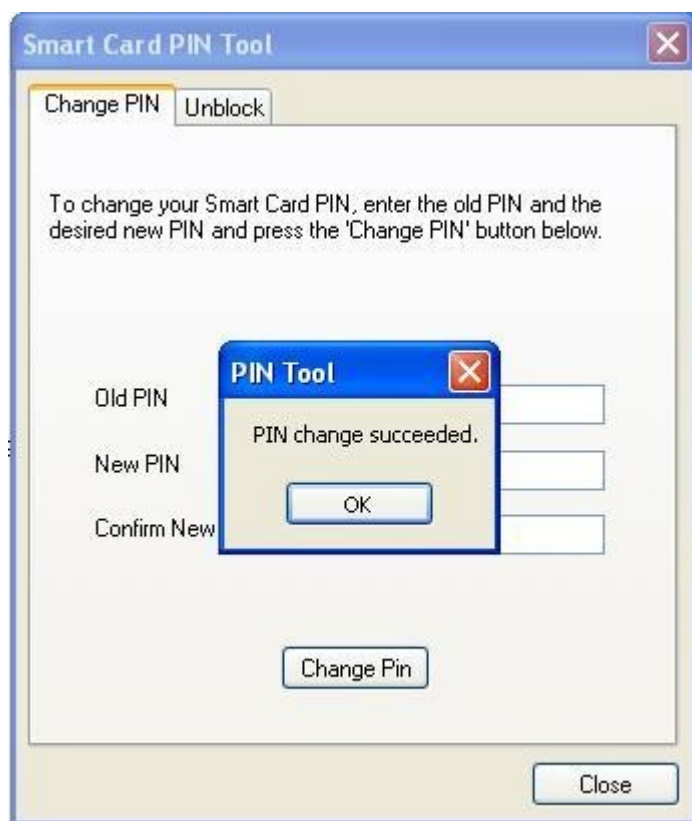


3. Enter your current PIN code in the **Old PIN** field (the default PIN code is 00000000).
4. Enter and confirm the new PIN code, and then click **Change Pin**.

The new PIN code must meet the PIN policy:

- PIN is 4 to 14 characters long.
- Weak PIN values are not allowed (a PIN is considered weak if the difference between consecutive characters is fixed – for example, 1234, ABCD, 86420,

acegik are considered weak PINs).



5. Click **OK**.

4.5 Unlocking the PIN Code Using Microsoft Windows

The Crescendo C1150 PIN will lock if the user presents six consecutive incorrect PINs. When the PIN is locked, you cannot use the card until you unlock the PIN.

In this deployment mode, an additional tool is needed to generate the cryptogram based on the input challenge and the default ADMIN key (binary value 00).

Other deployment modes with a central card management system are recommended for a simplified unlock process.

4.5.1 Unlock the PIN Code on Microsoft Windows Vista, Windows 7 or Windows 8

NOTE

In order to get access to the Microsoft SmartCard Credential Provider Unblock Feature, the following policy must be enabled by launching Microsoft Management Console (mmc), and then by adding the “Group Policy Object” Snap-In:

Local Computer Policy\Computer Configuration\Administrative Templates\Windows Components\Smart Card\Allow Integrated Unblock screen to be displayed at the time of logon

If you try to log on with a blocked smart card, or if you exceed the number of incorrect PIN entries, you are prompted to unlock the smart card.



NOTE

The Microsoft Windows refers to the smart card being “blocked”; this is similar to the smart card PIN being “locked”.

1. Click **OK** to start the procedure.

Alternatively, you can use the Change Password option from the CTRL+ALT+DEL menu. In coordination with your administrator, you obtain an unlock code based on the generated challenge.



2. Select **Unblock smart card**.



3. Provide the **Challenge** to your administrator, who will generate the unlock code.

NOTE If your administrator does not manage your Crescendo card, you can generate the unlock code using the HID Global Crescendo C1150 Unblock utility available at <http://www.hidglobal.com/drivers>.

4. Enter the unlock code in the **Response** field.
5. Enter and confirm a new **PIN** code.



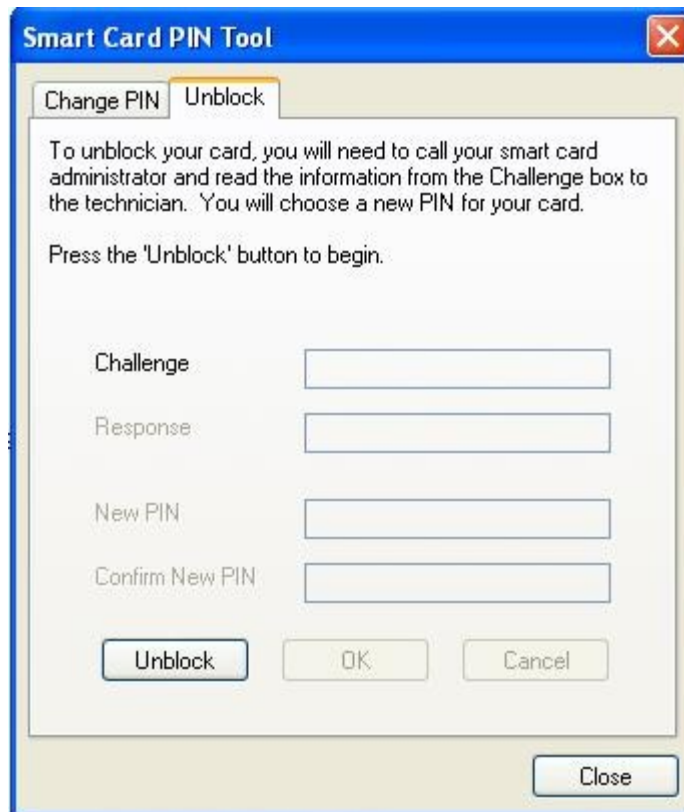
6. Click **OK** to return to your Windows session.

4.5.2 Unlock the PIN Code on Microsoft Windows XP

You can unlock your PIN code using the Microsoft PIN Tool (pintool.exe) included with the Base Smart Card CSP Package (for further information, see <http://support.microsoft.com/kb/909520>).

The PINTool.exe is located in the %WINDOWS%\system32 directory.

1. Select the **Unblock** tab in the Smart Card PIN Tool.



NOTE The Microsoft Windows refers to the smart card being “blocked”; this is similar to the smart card PIN being “locked”.

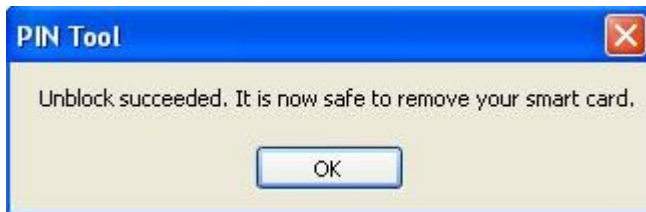
2. Click **Unblock** to generate the unlock challenge.



3. Provide the **Challenge** to your administrator, who will generate the unlock code.

NOTE If your administrator does not manage your Crescendo card, you can generate the unlock code using the HID Global Crescendo C1150 Unblock utility available at <http://www.hidglobal.com/drivers>.

4. Enter the unlock code in the **Response** field.
5. Then, enter and confirm a new **PIN** code, and then click **OK**.



6. Click **OK** to return to your Windows session.

5.0 Managing a Smart Card using Microsoft Forefront Identify Manager (FIM)

Forefront Identity Manager (FIM) 2010 delivers solutions to manage user accounts and access, password- and certificate-based credentials such as smart cards, and identity-based policies across Windows and heterogeneous environments.

5.1 Prerequisites

- Install the Crescendo C1150 Mini Driver (either from the Microsoft Windows Update or from the HID web site <http://www.hidglobal.com/main/crescendo/>).
- Install and configure Microsoft Forefront Identity Manager (FIM) 2010 server as described in the Microsoft technical guide – [http://technet.microsoft.com/en-us/library/fim-cm-getting-started-test-lab-guide\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/fim-cm-getting-started-test-lab-guide(WS.10).aspx)
- Make sure that the profile template is configured so that the ADMIN key is diversified during the initialization.

The screenshot shows the FIM 2010 web console interface. On the left, there is a sidebar with 'Select a view' (Profile Details, Duplicate Policy, etc.) and 'Quick Links' (Manage Profile Templates, Main Menu). The main content area is titled 'You can review and change settings for this profile template.' and contains three sections: 'General Settings', 'Certificate Templates', and 'Smart Card Configuration'. In the 'Smart Card Configuration' section, the 'Diversify Admin Key' option is checked and highlighted with a red rectangular box.

General Settings	
Profile template display name:	FIM CM Sample
Profile template common name:	FIM CM Sample
Profile template version:	2
Description:	Description of
Maximum number of external certificates:	0
Supports smart cards:	✓
Generate encryption keys on server:	X

Certificate Templates	
Selected	Template common name (click to edit)
<input type="checkbox"/>	ACSmartcardUser

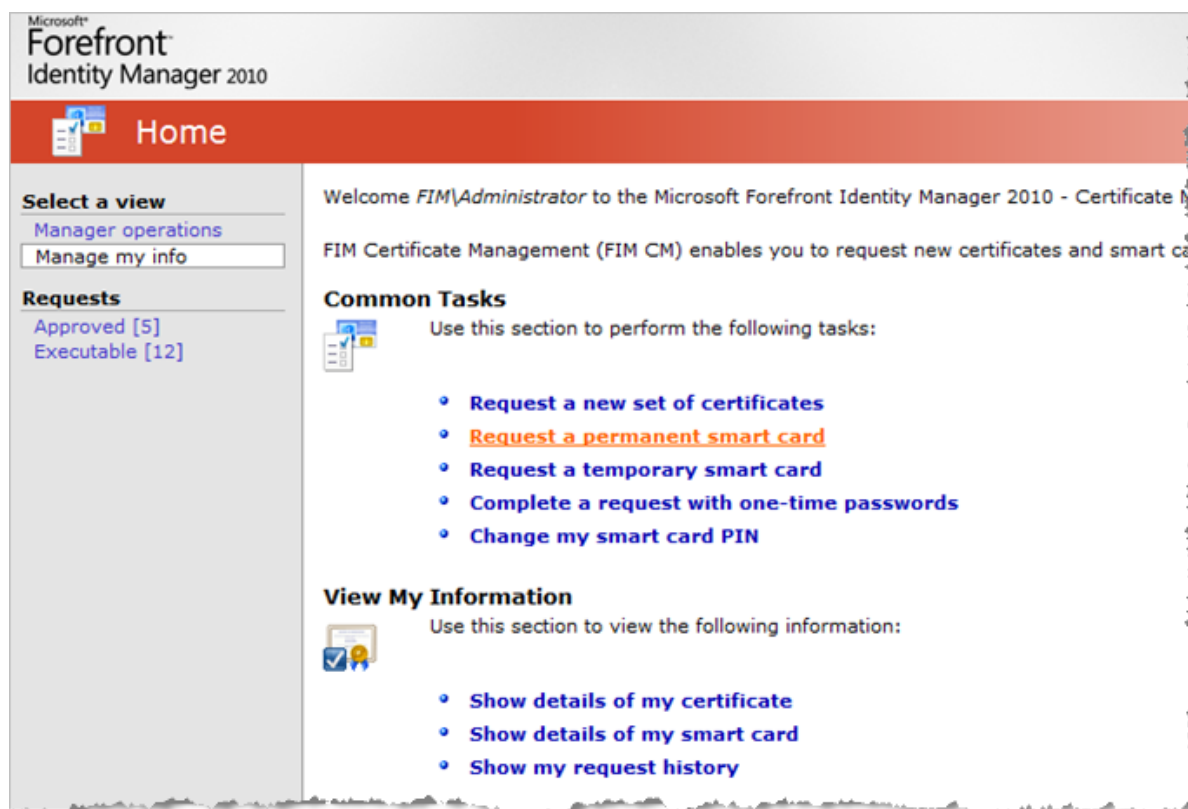
Smart Card Configuration	
Provider name:	Microsoft Smart
Provider id:	MSBaseCSP
Initialize new card prior to use:	✓
Reuse retired card:	✓
Use secure key injection:	X
Install CA Certificate(s):	✓
Certificate label text:	{Template/cn
Maximum number of certificates:	Unlimited
Diversify Admin Key:	✓
Card Initialization Provider Type:	Default
Card Initialization Provider Data:	

5.2 Initialize a Permanent Card

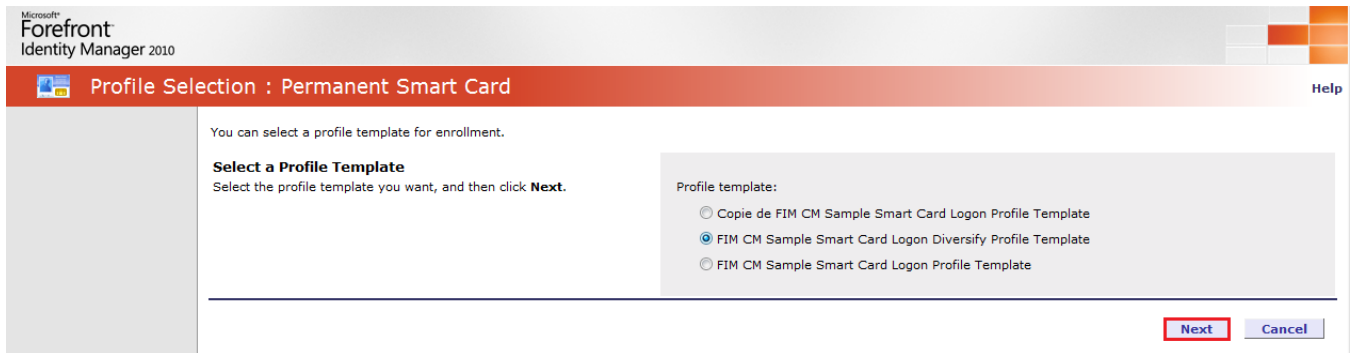
NOTE The default PIN code is 00000000.

The card is also personalized with a default ADMIN Key set to the binary value 00.

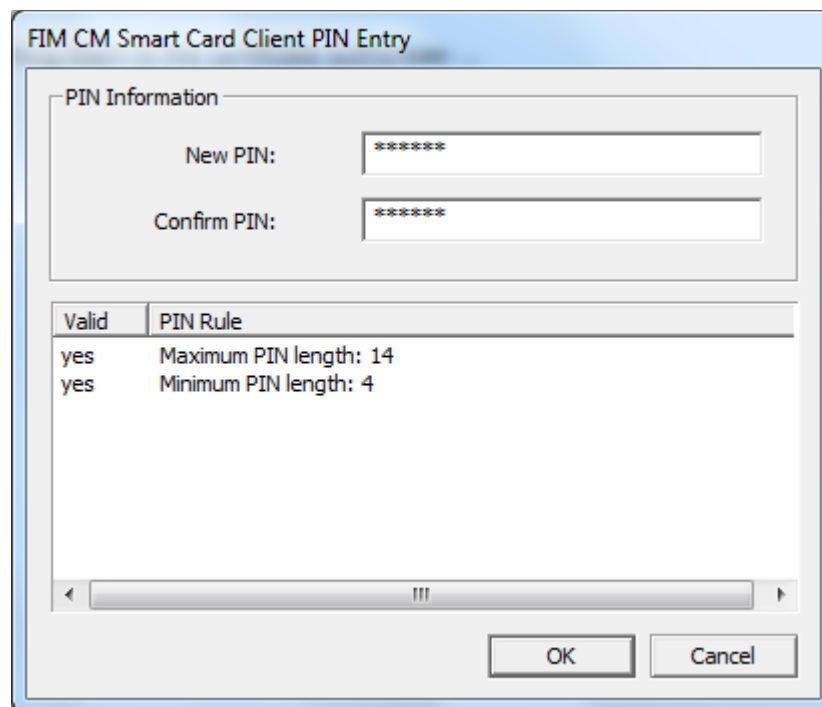
1. Log on to Forefront Identity Manager Certificate Management console.



2. In the Manage my info view, select **Request a permanent smart card**.



3. Select the profile template and then click **Next**.
The certificates are generated and the card is initialized.



4. When prompted, enter and confirm a **PIN** code for the card, and then click **OK**.

Important: The PIN must respect the specified PIN Rules.

- PIN is 4 to 14 characters long;
- Weak PIN values are not allowed (a PIN is considered weak if the difference between consecutive characters is fixed – for example, 1234, ABCD, 86420, acegik are considered weak PINs).

Microsoft
Forefront
Identity Manager 2010

Request Complete [Help](#)

Quick Links
[Request Summary](#)
[Smart Card Details](#)

The following summarizes the request that was just executed.

Request Summary
For more details about the request, click the request type.

Request type:	Enroll
Request status:	Completed
Request originator:	FIM\Administrator
Date of submission:	Monday, January 16, 2012 10:46:41 AM

Smart Card Summary
For more information, click the profile name.

Smart Card:	MSBaseCSP:{33343035-3931-3135-3931-303032443242}
Status:	Active

[View pending requests](#) [Main Menu](#)

The card is now ready to use.

5.3 Change the PIN Code Using FIM

Microsoft
Forefront
Identity Manager 2010

Home [Help](#)

Select a view
[Manager operations](#)
[Manage my info](#)

Requests
[Approved \[5\]](#)
[Executable \[12\]](#)

Welcome *FIM\Administrator* to the Microsoft Forefront Identity Manager 2010 - Certificate Management Portal.

FIM Certificate Management (FIM CM) enables you to request new certificates and smart cards, and manage the certificates and smart cards that have been provided to you.

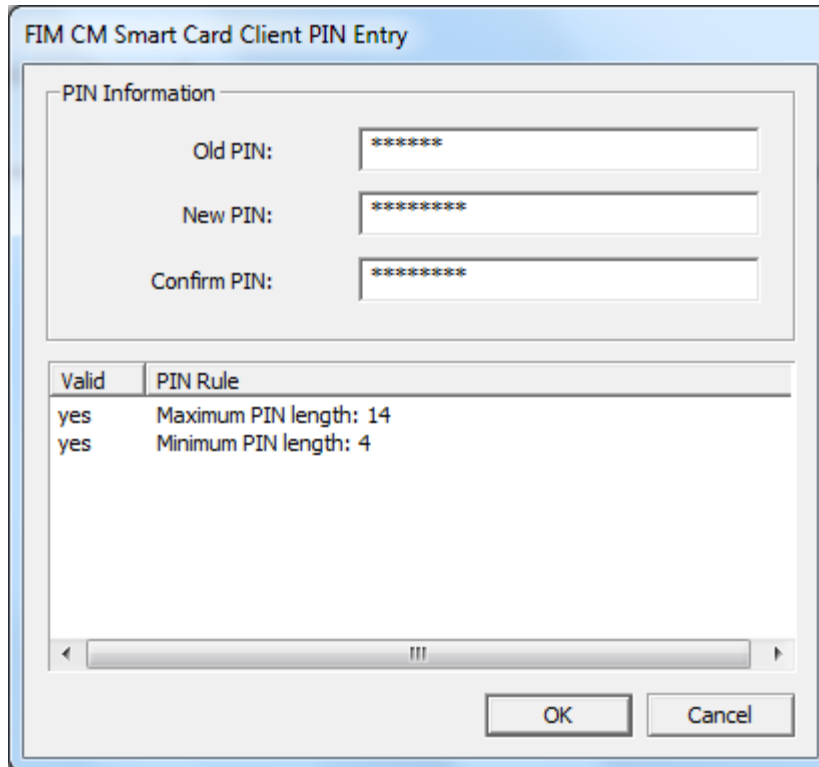
Common Tasks
Use this section to perform the following tasks:

- [Request a new set of certificates](#)
- [Request a permanent smart card](#)
- [Request a temporary smart card](#)
- [Complete a request with one-time passwords](#)
- [Change my smart card PIN](#)

View My Information
Use this section to view the following information:

- [Show details of my certificate](#)
- [Show details of my smart card](#)
- [Show my request history](#)

1. In the Manage my info view, select **Change my smart card PIN**.



FIM CM Smart Card Client PIN Entry

PIN Information

Old PIN:

New PIN:


Confirm PIN:

Valid	PIN Rule
yes	Maximum PIN length: 14
yes	Minimum PIN length: 4


OK Cancel

2. Enter your current PIN code.
3. Enter and confirm your new PIN code, and click **OK**.

NOTE Your PIN code is checked to make sure that it meets the length requirements, and that it is not weak (a PIN is considered weak when the difference between consecutive characters is fixed – for example, 1234, ABCD, 86420, acegik).



Microsoft
Forefront
Identity Manager 2010

 **Change Your Smart Card PIN** Help

Quick Links
[Main Menu](#)

Your smart card PIN has been successfully updated.

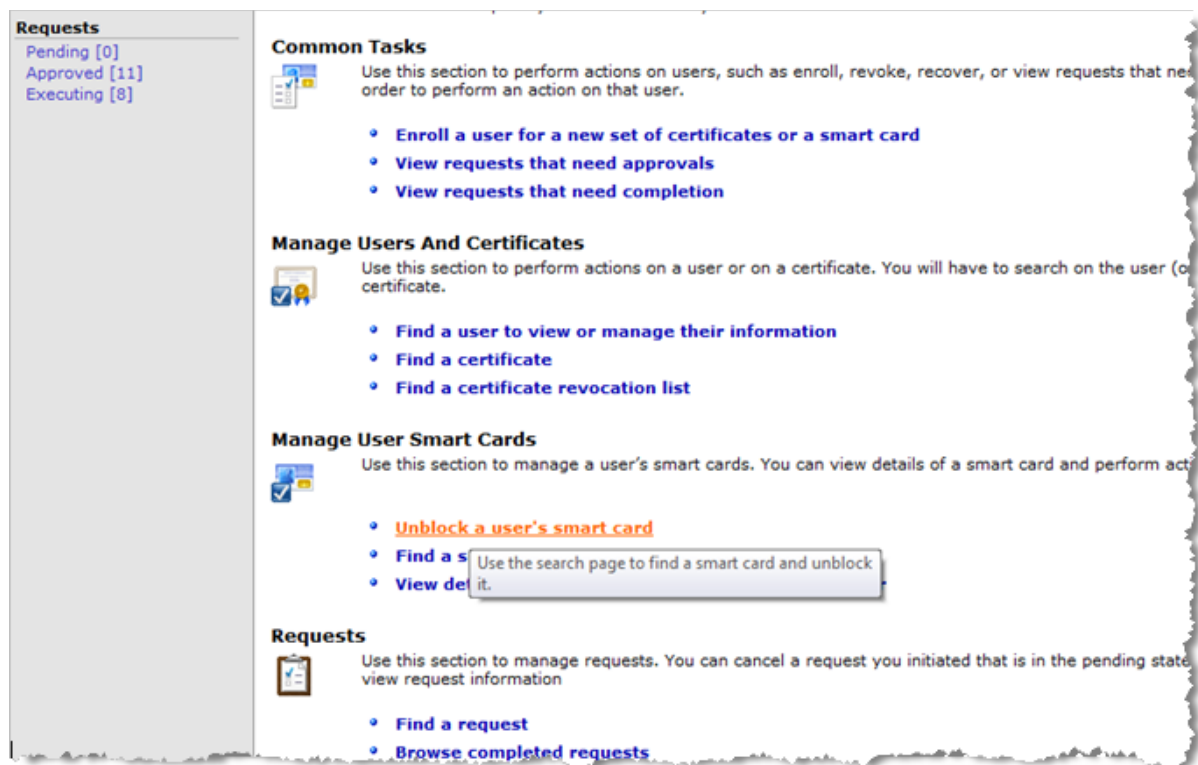
OK

5.4 Unlocking the Smart Card Using FIM - Online

The Crescendo C1150 PIN will lock if the user presents six consecutive incorrect PINs. When the PIN is locked, you cannot use the card until you unlock the PIN.

5.4.1 Unlock the Smart Card as an Administrator

1. Log on to Forefront Identity Manager Certificate Management console and select the **Manager operations** view.



2. Under Manage User Smart Cards, select **Unblock a user's smart card**.

Search for Smart Cards

You can find particular smart cards. Specify your search criteria, and click **Search**.

User Criteria

You can search by the user to whom the cards are assigned. Do one of the following:

- Type the name in the following format:
Domainname\Logonname
- Click **Look Up...**

Smart Card Criteria

You can find smart cards based on properties that include the date range when the smart card was assigned to the user.

Search Result Format

You can select the columns you want to include in your search results.

Name: **Look Up...**

Profile template:
Select profile template ▼

Provider:

Serial number:

Smart card state:
All ▼

Revoked:
Any ▼

Expired:
Any ▼

Assigned on or after:
 M/d/yyyy

Assigned on or before:
 M/d/yyyy

Reused cards:
☐ Display current assignment of cards

[Selected](#) [Column](#)

3. Search for the required user using the **Look Up** function.

Microsoft Forefront Identity Manager 2010 Certificate Management -- Webpage...

Search for Users and Groups

Complete your search criteria and click **Search**

Search for the following:

☐ Both users and groups
☒ Users
☐ Groups

Location:
 (All)

Name:
 a

User Logon

FIM\Administrator

CN= Administrator,CN= Users,DC= FIM,DC= test

https://vmfimad/C Trusted sites | Protected Mode: Off

Search for Smart Cards

Quick Links
Search again

This page displays the list of smartcards that matched your search criteria.

Search Results
Select a specific smart card to:

- View details of the smart card.
- Unlock the smart card.

=Permanent card
 =Duplicate card
 =Temporary card

Set Up Columns ...

Serial number	Provider	Status	Assigned User
{33343035-3630-3433-3931-30303...	MSBaseCSP	Active	FIM\Administrator
{33343035-3630-3433-3931-30303...	MSBaseCSP	Retired	FIM\Administrator
{33343035-3931-3135-3931-30303...	MSBaseCSP	Disabled	FIM\Administrator
{33343035-3931-3135-3931-30303...	MSBaseCSP	Retired	FIM\Administrator
{33343035-3931-3135-3931-30303...	MSBaseCSP	Retired	FIM\Administrator
{33343035-3931-3135-3931-30303...	MSBaseCSP	Retired	FIM\Administrator
{33343035-3931-3135-3931-30303...	MSBaseCSP	Active	FIM\Administrator

4. In the returned results, select the smart card to unlock.

Review Details of a Smart Card Profile Help

Quick Links
Return
User Details
Main Menu

Your smart card contains at least one certificate. If there are multiple certificates, you can manage them together. To define the certificates, your smart card has an associated profile template.

Smart Card Information
This section displays details about your smart card and its certificates, operations you can perform on the card, and associated management operations.

Smart card serial number: {33343035-3630-3433-3931-303030324630}
 Provider: MSBaseCSP
 Card Type: Primary
 Card Sequence: 0
 Profile template name: BSA FIM CM Sample Smart Card Logon Profile Template
 Profile template version: 9
 Smart card status: Active
 Assigned date: 6/23/2011 3:56 PM
 Assigned to: FIM\Administrator
 Supersedes smart card:
 Superseded by smart card:
 Permanent smart card:

Common name	Certificate template	Status	Archived	Expires
Users Administrator	FIMCMUser	Valid	X	7/19/2012 11:04:00 AM
Users Administrator	FIMCMSmartcardLogon	Valid	X	7/19/2012 11:04:00 AM

- Replace smart card that was lost or is no longer available
- Renew this smart card
- Disable this smart card
- Suspend this smart card
- Unblock this smart card**
- Modify the smart card PIN
- Duplicate this smart card
- Retire this smart card

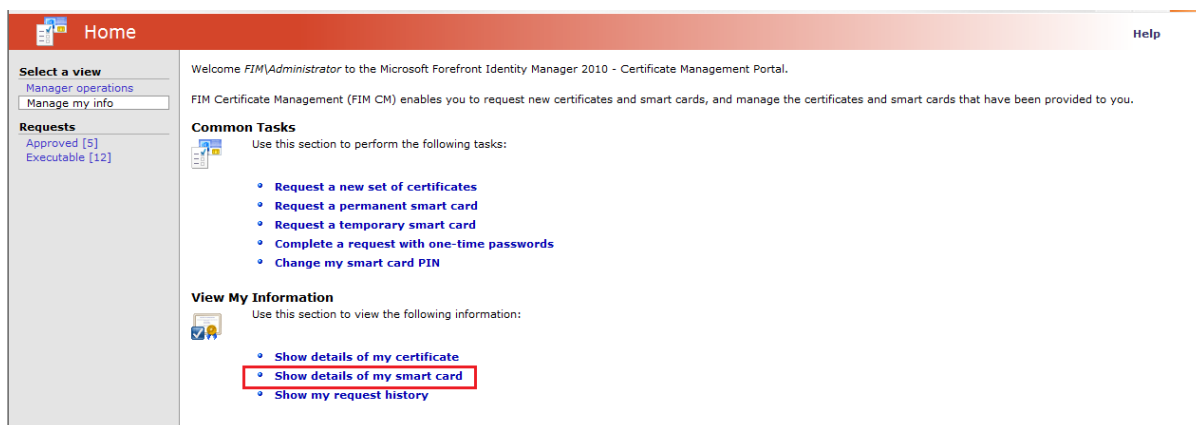
Smart Card Operations
This section lists the operations that have been performed on your smart card. For details, click the operation name.

Request	Originator	Submitted	Completed
Unblock	FIM\Administrator	11/22/2011 3:35 PM	
Enroll	FIM\Administrator	7/20/2011 11:08 AM	7/20/2011 11:14 AM

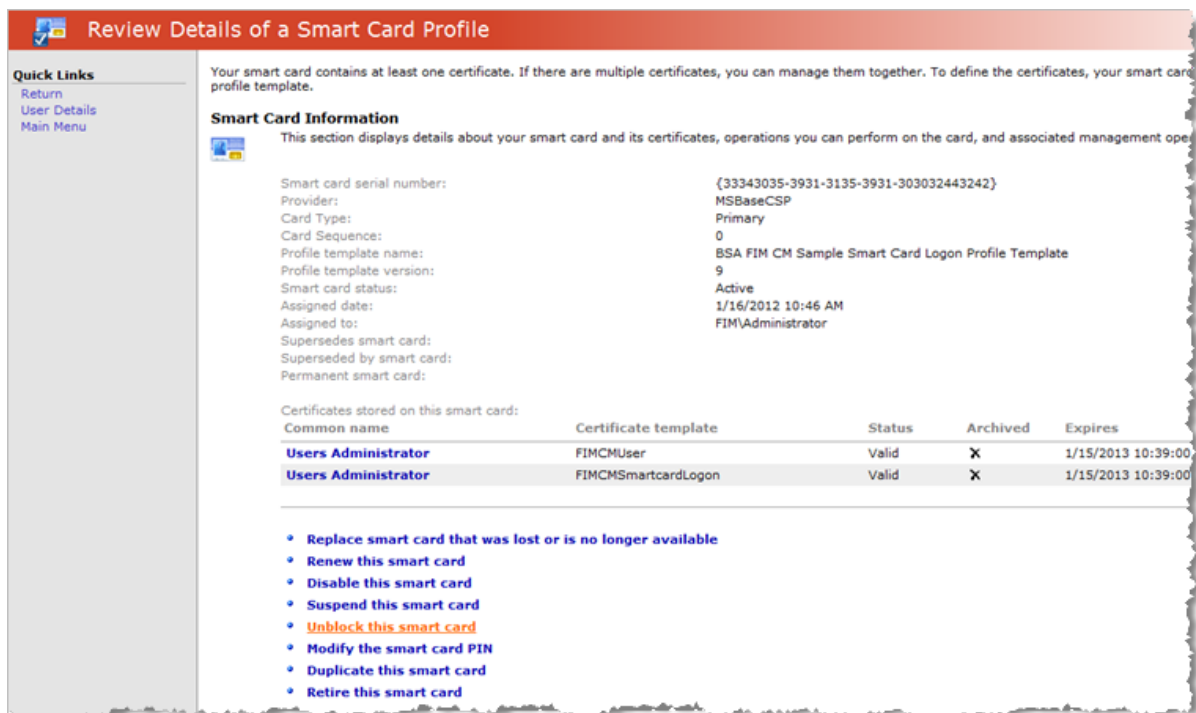
5. Verify the smart card details and then select **Unblock this smart card**.

6. Follow the **Unblock Wizard** instructions (see section [5.4.3 Using the Unblock Wizard](#) on page [60](#)).

5.4.2 Unlock the Smart Card as an End User



1. In the Manage my info view, select **Show details of my smart card**.



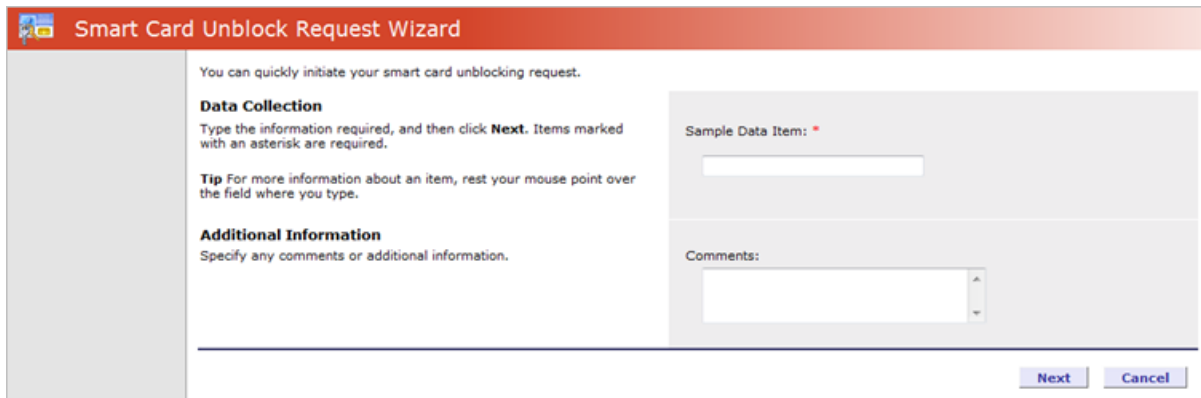
2. Verify the smart card details and then select **Unblock this smart card**.

3. Follow the **Unblock Wizard** instructions (see section [5.4.3 Using the Unblock Wizard](#) on page [60](#)).

5.4.3 Using the Unblock Wizard

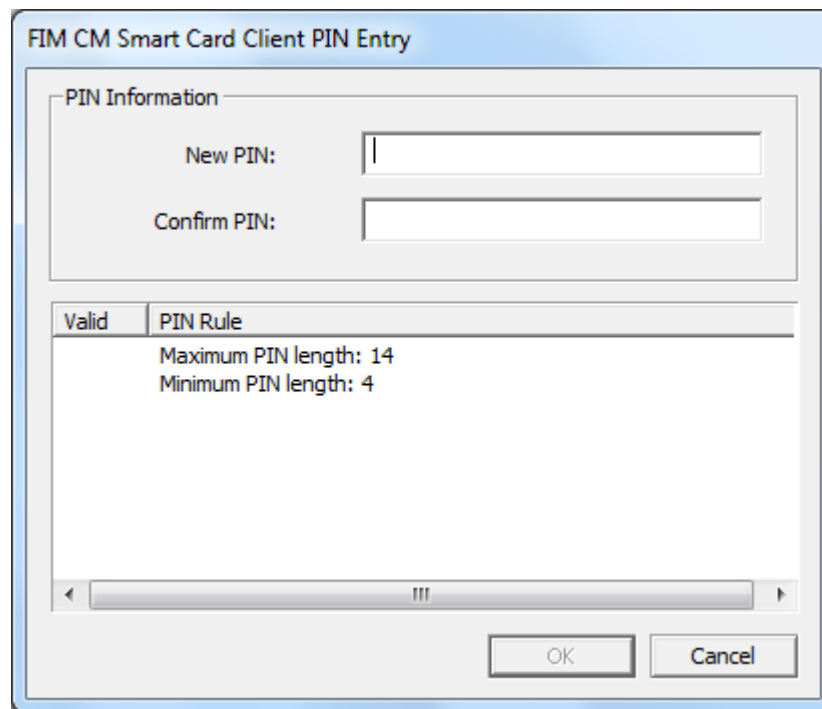
As part of the smart card unlock process, the Unblock Wizard launches.

If configured, the wizard prompts for additional data.



The **Smart Card Unblock Request Wizard** dialog box has a red title bar. The main area contains instructions: "You can quickly initiate your smart card unblocking request." It is divided into two sections: **Data Collection** and **Additional Information**. The **Data Collection** section says "Type the information required, and then click **Next**. Items marked with an asterisk are required." and includes a **Tip** about hovering over fields. The **Additional Information** section says "Specify any comments or additional information." To the right, there is a "Sample Data Item:" label with a text box and a "Comments:" label with a larger text box. At the bottom right are **Next** and **Cancel** buttons.

1. Enter the data and click **Next**.



The **FIM CM Smart Card Client PIN Entry** dialog box has a blue title bar. It contains a "PIN Information" section with "New PIN:" and "Confirm PIN:" labels and corresponding text boxes. Below this is a table showing PIN rules:

Valid	PIN Rule
	Maximum PIN length: 14
	Minimum PIN length: 4

At the bottom are **OK** and **Cancel** buttons.

2. Enter and confirm a **New PIN** code, and then click **OK**.

NOTE Your PIN code is checked to make sure that it meets the length requirements, and that it is not weak (a PIN is considered weak when the difference between consecutive characters is fixed – for example, 1234, ABCD, 86420, acegik).

The new PIN code must respect the specified PIN rules.

Request Complete

Quick Links
Request Summary
Smart Card Details

The following summarizes the request that was just executed.

Request Summary
For more details about the request, click the request type.

Request type:	Unlock
Request status:	Completed
Request originator:	FIM\Administrator
Date of submission:	Monday, January 16, 2012 10:55:02 AM

Smart Card Summary
For more information, click the profile name.

Smart Card:	MSBaseCSP:{33343035-3931-3135-3931-303032443242}
Status:	Active

[View pending requests](#) [Main Menu](#)

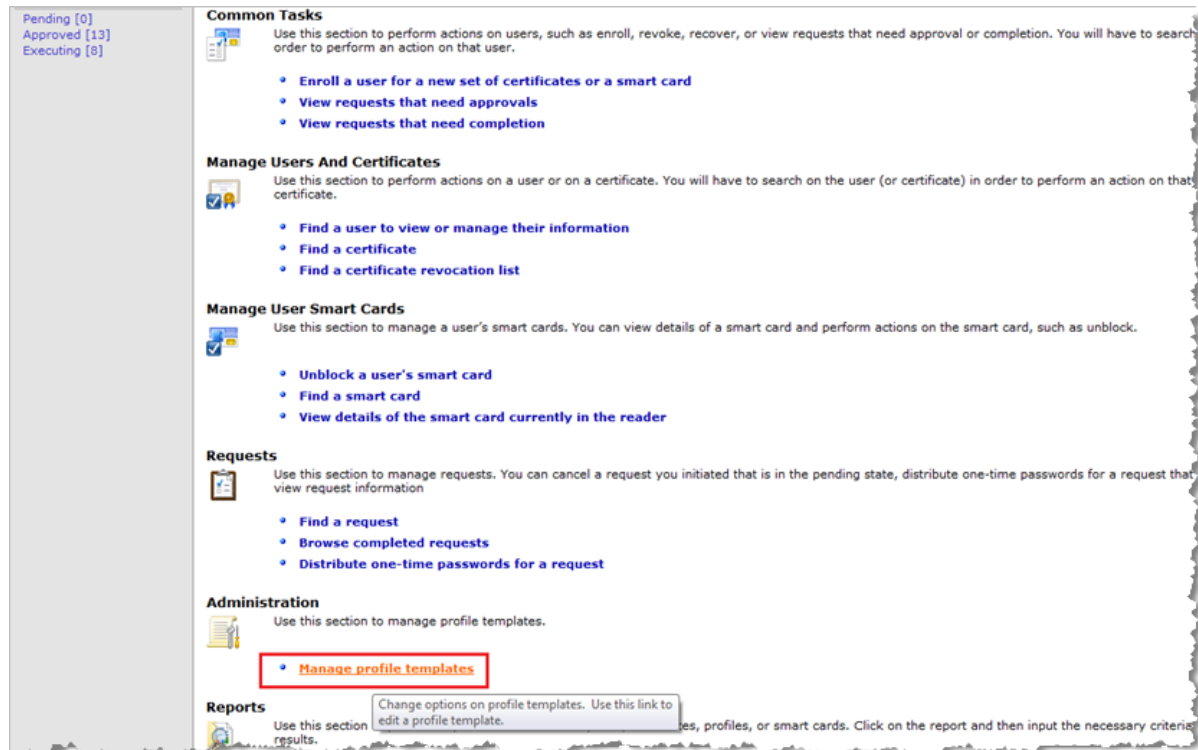
5.5 Unlocking the Smart Card Using FIM - Offline

The Crescendo C1150 PIN will lock if the user presents six consecutive incorrect PINs. When the PIN is locked, you cannot use the card until you unlock the PIN.

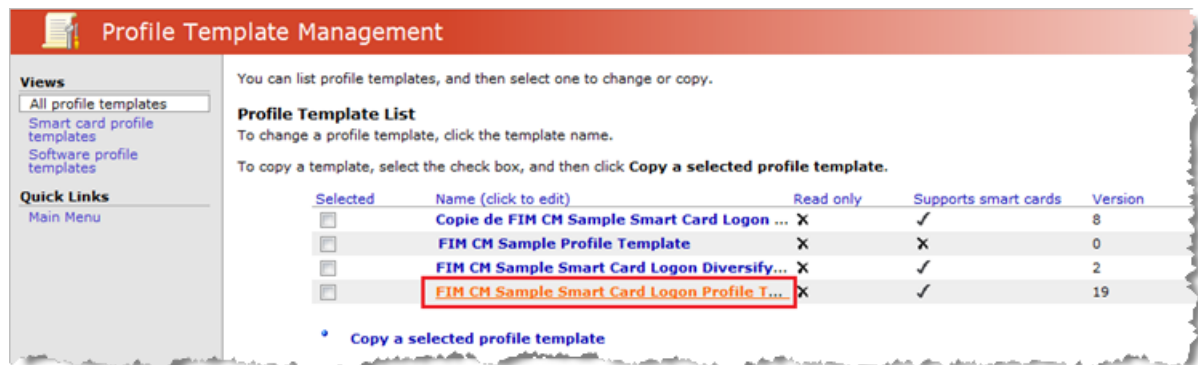
5.5.1 Verify that the Offline Unlock Policy is Enabled

To be able to perform the Offline Unlock operation, the profile template must have the Offline Unlock Policy enabled.

1. Log on to Forefront Identity Manager Certificate Management console, and select the **Manager operations** view.



2. Under Administration, click **Manage profile templates**.



3. Select your profile template.

Select a view

Profile Details

Duplicate Policy

Enroll Policy

Online Update Policy

Replace Policy

Recover On Behalf Policy

Renew Policy

Suspend and Reinstall Policy

Disable Policy

Retire Policy

Temporary Cards Policy

Unblock Policy

Offline Unblock Policy

Quick Links

Manage Profile Templates

Main Menu

You can review and change settings for this profile template:

General Settings

Profile template display name: FIM CM Sample Smart Card Logon Profile Template

Profile template common name: FIM CM Sample Smart Card Logon Profile Template

Profile template version: 19

Description: Description of the template goes here

Maximum number of external certificates: 0

Supports smart cards: ✓

Generate encryption keys on server: ✗

• [Change general settings](#)

Certificate Templates

This section allows you to manage certificate templates for this profile template. This profile template includes the following certificate templates:

Selected	Template common name (click to edit)	Template display name
<input type="checkbox"/>	ACSmartcardUser	AC Smartcard User

• [Add new certificate template](#)

• [Delete selected certificate templates](#)

Smart Card Configuration

This section displays smart card settings, including information about the card provider and certificate authority (CA) certificates.

Provider name: Microsoft Smart Card Base CSP

Provider id: MSBaseCSP

Initialize new card prior to use: ✓

Reuse retired card: ✓

Use secure key injection: ✗

Install CA Certificate(s): ✓

Certificate label text: {Template/cn}

- In the left menu pane, select **Offline Unblock Policy**.

Select a view

- Profile Details
- Duplicate Policy
- Enroll Policy
- Online Update Policy
- Replace Policy
- Recover On Behalf Policy
- Renew Policy
- Suspend and Reinstate Policy
- Disable Policy
- Retire Policy
- Temporary Cards Policy
- Unblock Policy
- Offline Unblock Policy

Quick Links

- Manage Profile Templates
- Main Menu

You can set up how to offline unblock a smart card for another user, including settings for workflow and data collection.

Workflow: General

This section displays workflow settings for offline unblocking a smart card.

Policy enabled:	✓
Allow collection of comments:	✓
Allow collection of request priority:	✗
Default request priority:	0
Number of approvals:	0

[Change general settings](#)

Workflow: Initiate Offline Unblock Requests

This section lists users and groups that can initiate an offline unblock request for this profile template.

Selected	Principal (click to edit)	Offline Unblock initiate
<input type="checkbox"/>	NT AUTHORITY\SYSTEM	Grant
<input type="checkbox"/>	FIM\Domain Admins	Grant
<input type="checkbox"/>	FIM\Administrator	Grant
<input type="checkbox"/>	FIM\vp	Grant

- Add new principal for offline unblock request initiation
- Delete principals for offline unblock request initiation

Workflow: Unblock Agent for Offline Unblock Requests

This section lists users and groups that can execute an offline unblock request for this profile template.

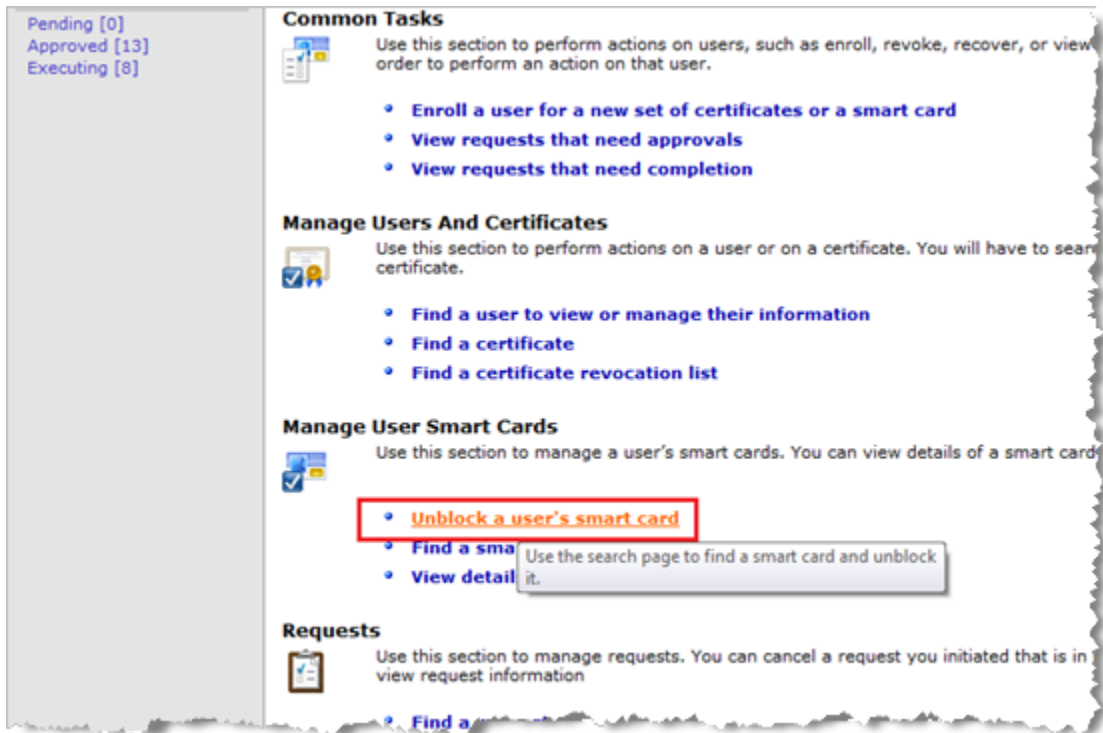
Selected	Principal (click to edit)	Offline Unblock agent
<input type="checkbox"/>	NT AUTHORITY\SYSTEM	Grant
<input type="checkbox"/>	FIM\Administrator	Grant
<input type="checkbox"/>	FIM\vp	Grant

- Add new principal for unblock agent
- Delete principals for unblock agent

- Under the **Workflow: General** section, verify that the policy is enabled.
If it is not, click **Change general settings** to enable the policy.

5.5.2 Launch Offline Unlock Request

- To launch an Offline unlock request, return to the **Manager operations** view.



- Under Manage User Smart Cards, click **Unlock a user's smart card**.

Search for Smart Cards

You can find particular smart cards. Specify your search criteria, and click **Search**.

User Criteria

You can search by the user to whom the cards are assigned. Do one of the following:

- Type the name in the following format:
Domainname\Logonname
- Click **Look Up...**

Smart Card Criteria

You can find smart cards based on properties that include the date range when the smart card was assigned to the user.

Search Result Format

You can select the columns you want to include in your search results.

Name: **Look Up...**

Profile template:
Select profile template ▼

Provider:

Serial number:

Smart card state:
All ▼

Revoked:
Any ▼

Expired:
Any ▼

Assigned on or after:
 M/d/yyyy

Assigned on or before:
 M/d/yyyy

Reused cards:
☐ Display current assignment of cards

[Selected](#) [Column](#)

3. Search for the required user using the **Look Up** function.

Microsoft Forefront Identity Manager 2010 Certificate Management -- Webpage...

Search for Users and Groups

Complete your search criteria and click **Search**

Search for the following:

☐ Both users and groups
☒ Users
☐ Groups

Location:
(All) ▼

Name:
a

Search **Cancel**

[User Logon](#)

FIM\Administrator

CN= Administrator,CN= Users,DC= FIM,DC= test

https://vmfimad/C ✓ Trusted sites | Protected Mode: Off

Search for Smart Cards

Quick Links
Search again

This page displays the list of smartcards that matched your search criteria.

Search Results
Select a specific smart card to:

- View details of the smart card.
- Unblock the smart card.

Permanent card Duplicate card Temporary card

Set Up Columns ...

Serial number	Provider	Status	Assigned User
{33343035-3931-3135-3931-30303... Click to view details	MSBaseCSP	Active	FIM\vp
{33343035-3931-3135-3931-30303...	MSBaseCSP	Retired	FIM\vp
{33343035-3931-3135-3931-30303...	MSBaseCSP	Active	FIM\vp

- Select the smart card to be unlocked.

Review Details of a Smart Card Profile

Quick Links
Return
User Details
Main Menu

Your smart card contains at least one certificate. If there are multiple certificates, you can manage profile template.

Smart Card Information
This section displays details about your smart card and its certificates, operations you can perform.

Smart card serial number:	{33343035-3931-3135-3931-30303...
Provider:	MSBaseCSP
Card Type:	Primary
Card Sequence:	0
Profile template name:	FIM CM Sample Sp
Profile template version:	17
Smart card status:	Active
Assigned date:	1/26/2012 12:05 P
Assigned to:	FIM\vp
Supersedes smart card:	
Superseded by smart card:	
Permanent smart card:	

Certificates stored on this smart card:	Certificate template
Common name Users vpe	ACSmartcardUser

- Unblock this smart card
- Offline unblock this smart card**
- Retire this smart card

- Click **Offline unblock this smart card**.

Smart Card Offline Unblock Request Wizard

Quick Links
Main Menu

You can easily complete required information to initiate an offline unblock request. Complete the information needed, and then click **OK**.

Additional Information
Specify any comments or additional information.

Comments:

Ok

- Enter any additional information and click **OK**.

Request Status

You can check the status of a FIM CM request. If the request is approved and requires a password, this page lists your one-time passwords.

Request Status
This section displays the request status, along with additional information about the request.

Request type:	Offline Unblock
Profile template:	FIM CM Sample Smart Card Logon Profile Template
Current status of your request:	Approved
Submitted date of request:	Thursday, January 26, 2012 3:06:50 PM
Completed date of request:	Not complete
Target user:	FIM\vp
Originating user:	FIM\Administrator
Request priority:	0

Execute

- Click **Execute**.

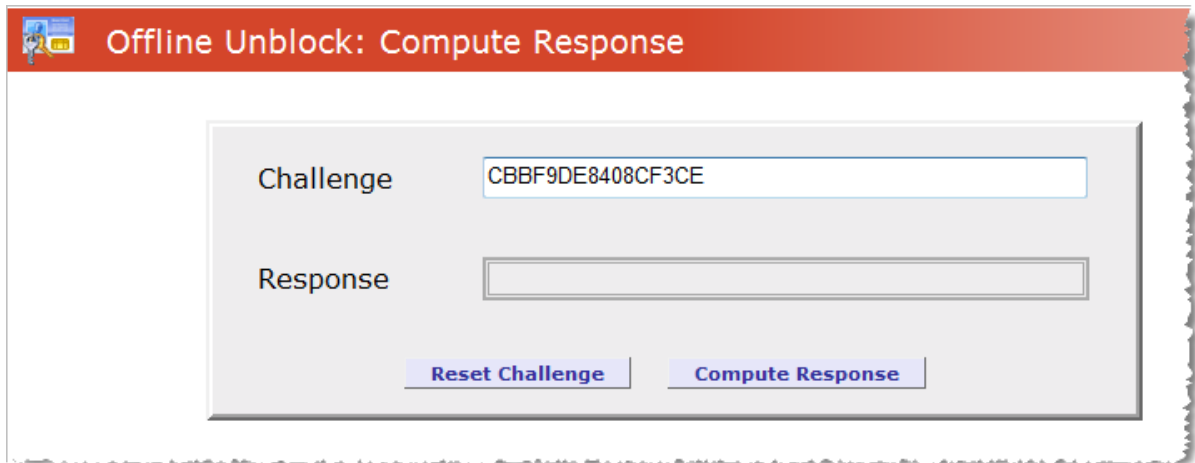
Offline Unblock: Compute Response

Challenge

Response

Reset Challenge **Compute Response**

8. Ask the smart card user to provide the challenge displayed when they attempt to unlock the smart card using the native Windows tools (see section [4.5 Unlocking the PIN Code Using Microsoft Windows](#) on page 44).

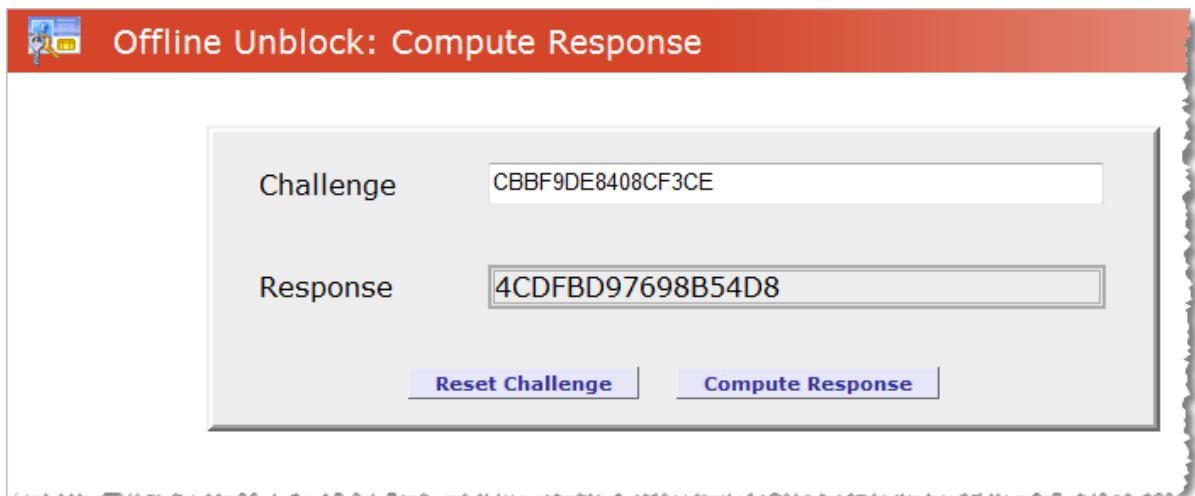


Offline Unblock: Compute Response

Challenge

Response

9. Enter the **Challenge** and click **Compute Response**.



Offline Unblock: Compute Response

Challenge

Response

10. Provide the computed **Response** to the smart card user and instruct him to enter it into the corresponding field in the Windows unlock dialog.

5.6 Reset the Smart Card Using FIM

1. In the Manage my info view, select **Show details of my smart card**.

Review Details of a Smart Card Profile

Your smart card contains at least one certificate. If there are multiple certificates, you can manage them together. To delete a certificate, click the **Remove** link next to the certificate name.

Smart Card Information

This section displays details about your smart card and its certificates, operations you can perform on the card, and the status of the card.

Smart card serial number:	{33343035-3931-3135-3931-303032443}
Provider:	MSBaseCSP
Card Type:	Primary
Card Sequence:	0
Profile template name:	BSA FIM CM Sample Smart Card Logon
Profile template version:	9
Smart card status:	Active
Assigned date:	1/16/2012 10:46 AM
Assigned to:	FIM\Administrator
Supersedes smart card:	
Superseded by smart card:	
Permanent smart card:	

Certificates stored on this smart card:

Common name	Certificate template	Status
Users Administrator	FIMCMUser	Valid
Users Administrator	FIMCMSmartcardLogon	Valid

- [Replace smart card that was lost or is no longer available](#)
- [Renew this smart card](#)
- [Disable this smart card](#)
- [Suspend this smart card](#)
- [Unblock this smart card](#)
- [Modify the smart card PIN](#)
- [Duplicate this smart card](#)
- [Retire this smart card](#)

Smart Card Operations

This section lists the operations that have been performed on your smart card. For details, click the operation name.

2. Click **Retire this smart card**.

Retiring Smart Card

Quick Links
[Main Menu](#)
[Request Details](#)
[Smart Card Details](#)

Below is a list of actions to perform on the smart card as part of the card retirement process.

Smart Card Information
 Details of the smart card being processed in the request.

Smart card serial number: {33343035-3630-3433-3931-303030324536}
 Smart card provider: MSBaseCSP

Common name	Certificate template	Status	Archived	Expires
Users Administrator	ACSmartcardUser	Revoked	X	1/9/2013 3:27 PM

Actions to perform on the smart card
 The following actions will be performed on the smart card. Please ensure the card is inserted into the reader and click "Next" to continue.

Erase user card data:	✓
Block user PIN:	X
Block admin PIN:	X
Reset admin PIN:	✓

[Next](#)

3. Verify the actions that will be performed when the card is retired and click **Next**.

Request Complete

Quick Links
[Request Summary](#)
[Smart Card Details](#)

The following summarizes the request that was just executed.

Request Summary
 For more details about the request, click the request type.

Request type:	Retire
Request status:	Completed
Request originator:	FIM\Administrator
Date of submission:	Tuesday, January 10, 2012 4:14:05 PM

Smart Card Summary
 For more information, click the profile name.

Smart Card:	MSBaseCSP:{33343035-3630-3433-3931-303030324536}
Status:	Retired

[View pending](#)

The smart card ADMIN key is set back to the initial value, all the PKI containers are reset, but the PIN code is unchanged.

6.0 Managing a Smart Card with ActivClient

ActivClient enables the use of PKI certificates and keys, 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 messages
- Electronic transactions

In addition to smart card middleware (Cryptographic Service Provider and PKCS#11 libraries), ActivClient includes additional utilities that enable you to manage your smart card, including:

- User Console
- PIN Initialization Tool
- PIN Change Tool

The next sections present common card management operations with ActivClient. See the ActivClient documentation for complete instructions on installation, management and usage services.

6.1 Issue a Smart Card with ActivClient

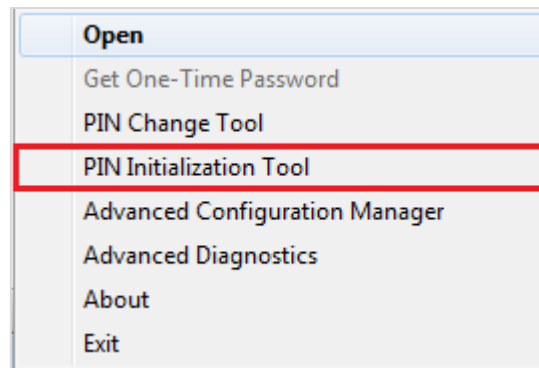
When you receive a blank smart card, you must initialize it using the ActivClient PIN Initialization Tool.

1. Use one of the following options to launch the ActivClient PIN Initialization Tool:

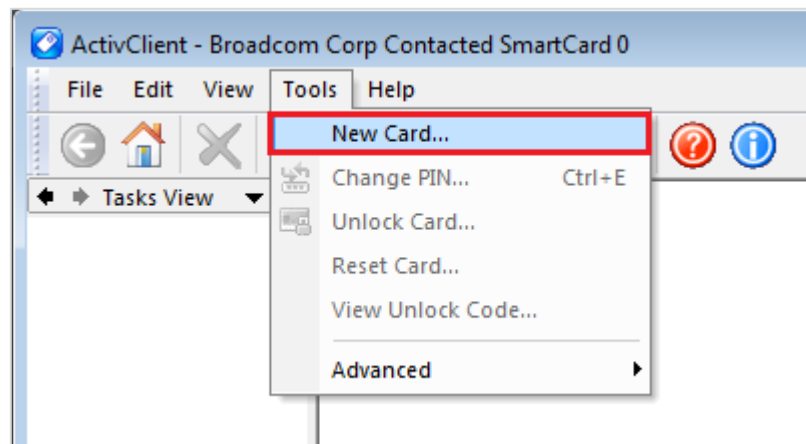
- From the ActivClient notification area icon:



Right-click on the icon and select **PIN Initialization Tool** in the menu:

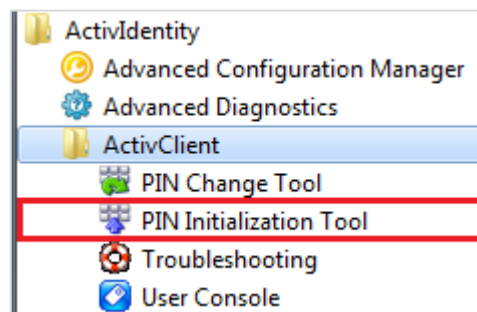


- From the ActivClient User Console:



From the **Tools** menu, select **New Card**.

- From the Start Menu:



Select **PIN Initialization Tool** in the menu.

ActivClient - PIN Initialization Tool

ActivIdentity
ActivClient

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

PIN code:

Confirm:

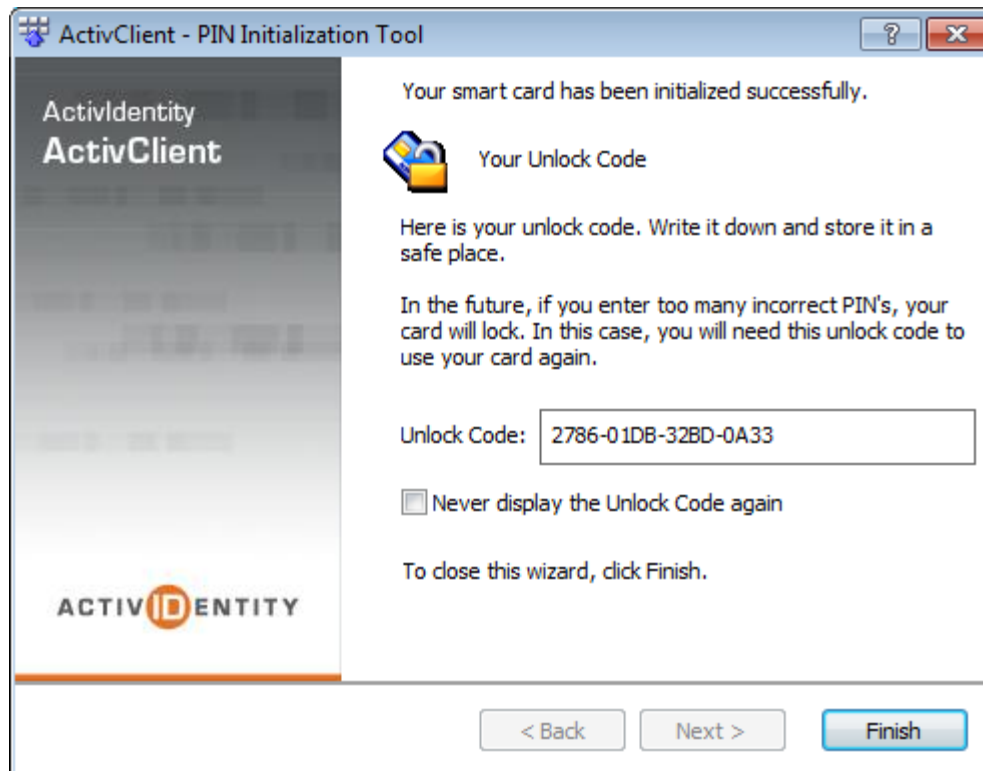
Your new PIN must meet the following conditions:

- ☐ Must contain at least 4 characters
- ☒ Must not exceed 14 characters
- ☐ Must not be weak or easy to guess (e.g. 1234)
- ☒ Must be correctly confirmed

ACTIV IDENTITY

< Back Next > Cancel

2. Enter and confirm a **PIN code** and click **Next**.
The PIN code must meet the specified conditions.



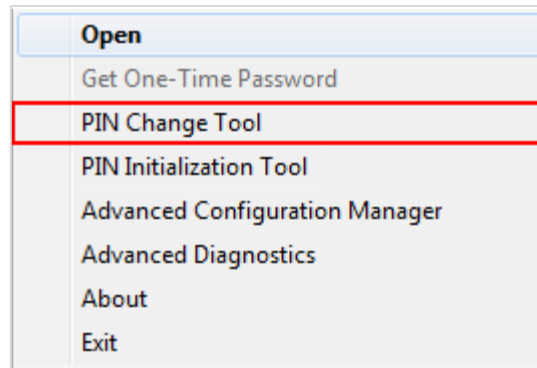
3. Make a note of your unlock code and store it in a safe place.
If you do not select the **Never display the Unlock Code again** option, the unlock code will display each time you enter your smart card PIN code.
4. Click **Finish**.

6.2 Change the PIN Code with ActivClient

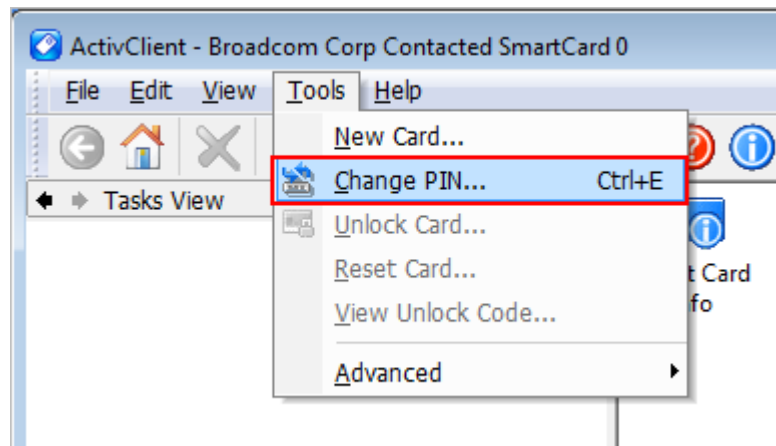
1. Use one of the following options to launch the ActivClient PIN Change Tool:
 - From the ActivClient notification area icon:



Right-click on the icon and select **PIN Change Tool** in the menu:

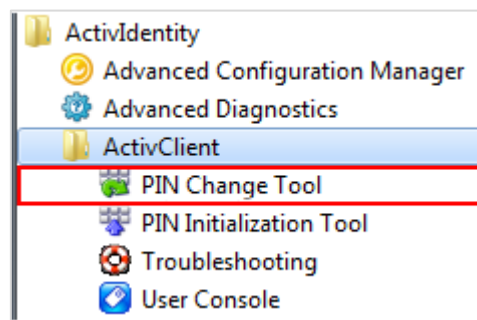


- From the ActivClient User Console:



From the **Tools** menu, select **Change PIN**.

- From the Start Menu:



Select **PIN Change Tool** in the menu.

ActivClient - PIN Change Tool

ActivIdentity
ActivClient

ACTIV IDENTITY

Please enter your current PIN and the new PIN you want to use.

Enter your PIN:

Enter New PIN:

Confirm New PIN:

Your new PIN must meet the following conditions:

- ☒ Must contain at least 4 characters
- ☒ Must not exceed 14 characters
- ☒ Must not be weak or easy to guess (e.g. 1234)
- ☒ Must be correctly confirmed

< Back Next > Cancel

2. Enter your current **PIN** code.
3. Enter and confirm a **PIN code** and click **Next**.

The PIN code must meet the specified conditions.

6.3 Unlock the Smart Card Using ActivClient

If the Unlock Smart Card tool does not display automatically when ActivClient detects that the card is locked, from the ActivClient User Console **Tools** menu, select **Unlock Card**.

- If the smart card was initialized with ActivClient, you can unlock it with the static unlock code displayed during initialization.

ActivClient - Unlock Smart Card

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

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

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

Your new PIN must meet the following conditions:

- Must contain at least 6 characters
- Must not exceed 25 characters
- Must not be weak or easy to guess (e.g. 1234)
- Must be correctly confirmed

OK Cancel

- a. Retrieve the unlock code that you saved when you initialized your smart card.
You might be able to retrieve the code from the ActivClient User Console **Tools** menu, using the **View Unlock Code** option.
 - b. In the **Unlock Code** field, type the unlock code that you retrieved.
 - c. In the **New PIN** field, type the new PIN.
 - d. In the **Verify** field, re-type the new PIN, and click **OK**.
- If the smart card was initialized by your administrator with a card management product (such as the 4TRESS AAA Server, or Microsoft FIM), you can unlock it using a challenge/response unlock process.

ActivClient - Unlock Smart Card

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

Challenge Code
Please contact your help desk and provide the challenge code below:

Challenge Code:

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

Unlock Code:

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

New PIN: Verify:

Your new PIN must meet the following conditions:

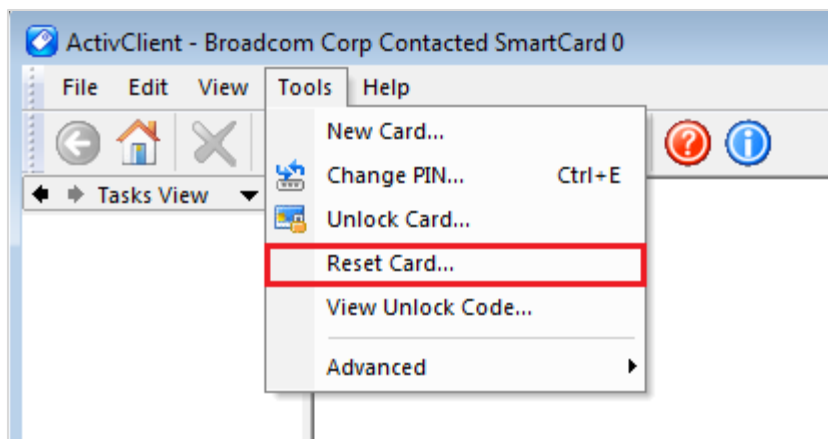
- Must contain at least 6 characters
- Must not exceed 25 characters
- Must not be weak or easy to guess (e.g. 1234)
- Must be correctly confirmed

- a. Provide the **Challenge Code** to your help desk.
- b. In the **Unlock Code** field, type the unlock code that the help desk operator gives you.
- c. In the **New PIN** field, type the new PIN.
- d. In the **Verify** field, re-type the new PIN, and click **OK**.

6.4 Reset the Smart Card Using ActivClient

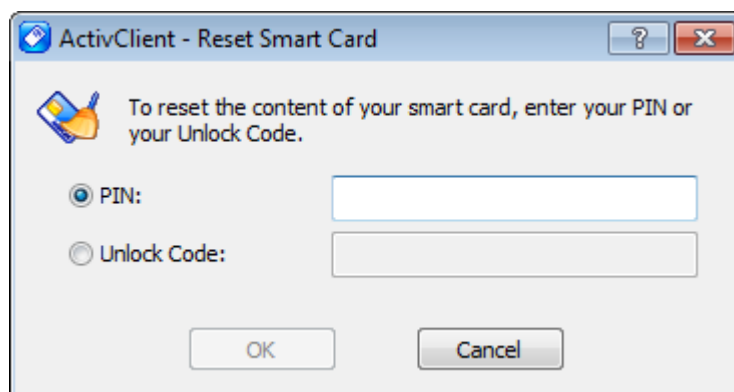
If you want to reset a smart card that is already initialized (either using ActivClient or the Mini Driver), you can use the ActivClient Reset Card function.

1. Open the ActivClient User Console.



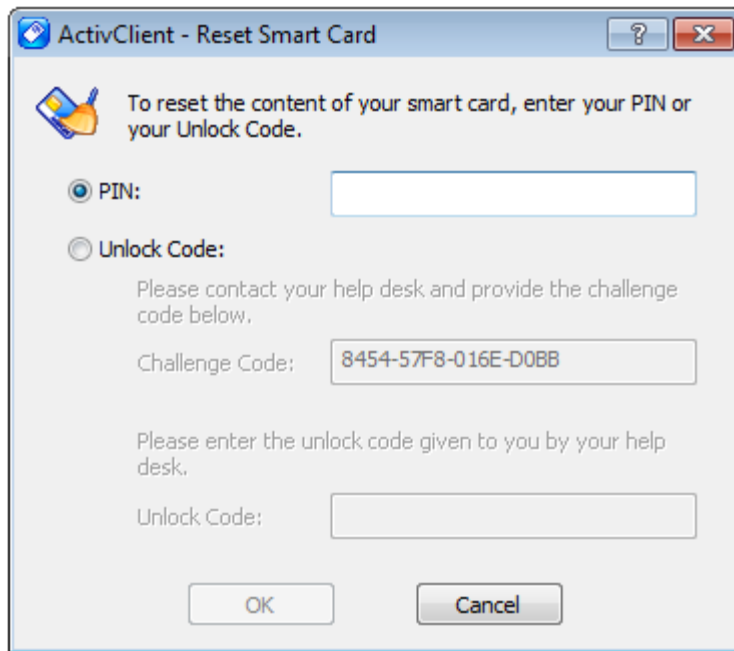
2. From the **Tools** menu, select **Reset Card**.

- If the smart card was initialized with ActivClient, you can reset it with the PIN code or the static unlock code displayed during initialization.

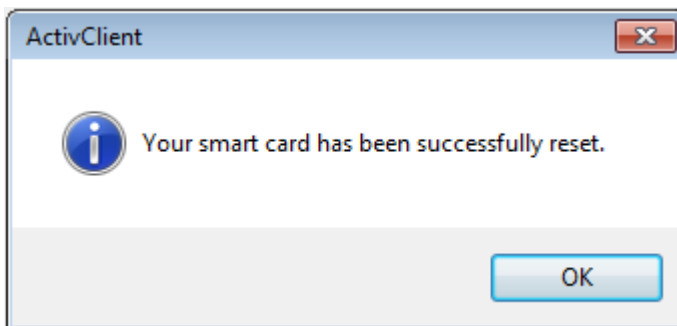


- Select one of the options and enter the corresponding code.
- Click **OK**.

- If the smart card was initialized with ActivClient in a 4TRESS AAA Server deployment or with the Mini Driver, you can reset it with the PIN code or a dynamic unlock code.



- a. Select the **PIN** option and enter your PIN code.
- b. Alternatively, select the **Unlock Code** option and provide the Challenge Code to your Help Desk.
Then enter the **Unlock Code** given to you by your Help Desk.
- c. Click **OK**.



3. Click **OK** when the reset process is complete.
The smart card is now blank and can be initialized for new use.

6.5 Importing Certificates Using ActivClient

You can download PKI certificates from the CA onto the smart card using Internet Explorer or Microsoft Management Console (MMC).

6.5.1 Request a Certificate

Microsoft Active Directory Certificate Services -- CA2010

Advanced Certificate Request

Certificate Template:
Smartcard User

Key Options:
☒ Create new key set ☐ Use existing key set
CSP: **ActivClient Cryptographic Service Provider**
Key Usage: ☒ Exchange
Key Size: 1024 Min: 512 Max: 2048 (common key sizes: [512](#) [1024](#) [2048](#))
☒ Automatic key container name ☐ User specified key container name
☐ Mark keys as exportable
☐ Enable strong private key protection

Additional Options:
Request Format: ☒ CMC ☐ PKCS10
Hash Algorithm: sha1
Only used to sign request.
☐ Save request
Attributes:
Friendly Name:

Submit >

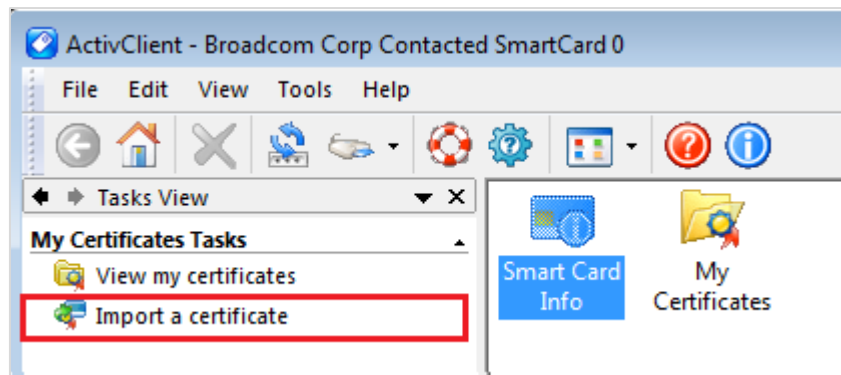
When creating the certificate request, make sure that the **ActivClient Cryptographic Service Provider** is selected as the CSP.

If the ActivClient detects that the card is not initialized, then the PIN Initialization Tool launches (see section [6.1 Issue a Smart Card with ActivClient](#) on page 73).

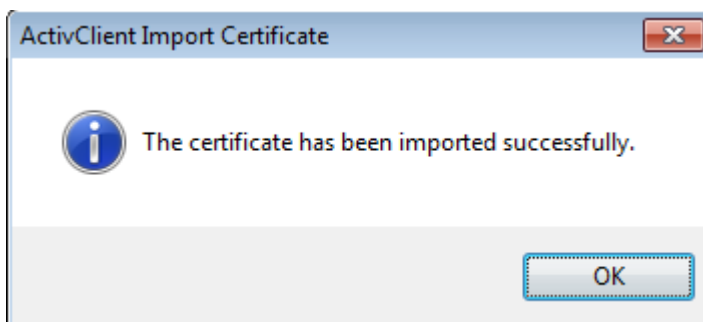
The certificate request process resumes, and you are asked to install the certificate on your smart card.

6.5.2 Import the Certificate

1. Insert your smart card into the reader.
2. Open the ActivClient User Console.



3. Select **Import** from the **File** menu. Alternatively, in the **Tasks** view, under **My Certificates Tasks**, select **Import a certificate**.
4. Browse to the certificate file. If the certificate is password-protected, enter the password and click **OK**.



5. Click **OK**.

7.0 Managing a Smart Card with naviGO

naviGO Server provides the capability for administrators and end-users to enroll Crescendo contact cards with PKI credentials. naviGO also enables the use of emergency credentials (knowledge-based authentication) for cases where users have lost or forgotten their card.

The next sections present common card management operations with naviGO. See the naviGO documentation for complete instructions on installation, management and usage services.

7.1 Prerequisites

- The Crescendo C1150 Mini Driver is installed (either from Microsoft Windows Update or from the HID web site <http://www.hidglobal.com/main/crescendo/>).
- naviGO Server 3.0 is installed.
- The administrator must be assigned the role of `navigo_sys_admin` or Security Officer, or the function of Enroll on Behalf must be manually assigned to the Role for which the administrator is logged into naviGO.

7.2 Initialize a Smart Card

This section presents how administrators can issue a smart card for their end users.

naviGO also enables users to self-enroll using the naviGO self-service portal. The steps below starting at step 8 show this self-enrollment process. See the *naviGO Server User Guide* for additional information.

NOTE

The default PIN is 00000000.

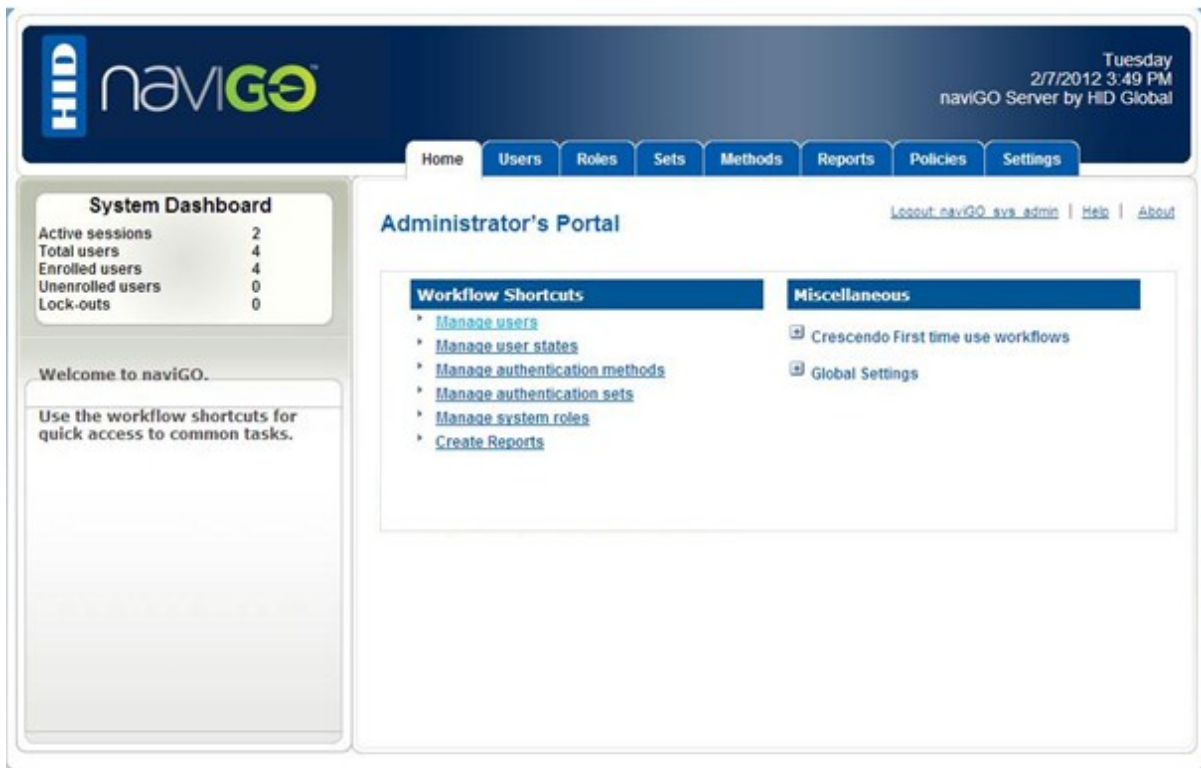
The card is also personalized with a default ADMIN Key set to 00 (binary value).

The screenshot shows the HID naviGO Administrator Portal login page. The header features the HID naviGO logo on the left and the date/time 'Friday 4/1/2011 2:41 PM' and 'naviGO Server by HID Global' on the right. The main content area is titled 'naviGO Validation' and contains a message 'Please logon to naviGO'. Below this message are two input fields labeled 'Username' and 'Domain', followed by a 'Go' button.

1. Log on to the naviGO Administrator Portal.

The screenshot shows the HID naviGO Administrator Portal password validation page. The header features the HID naviGO logo on the left and the date/time 'Tuesday 2/7/2012 3:48 PM' and 'naviGO Server by HID Global' on the right. The main content area is titled 'naviGO Validation' and contains a message 'Please enter your naviGO Password.' Below this message are two input fields labeled 'Username' and 'Password'. The 'Username' field contains the text 'naviGO_sys_admin'. The 'Password' field contains a series of dots. A 'Validate' button is located below the password field.

2. Enter your Administrator **Username** and **Password** and click **Validate**.



3. Click **Manage Users** to select the user to whom you want to issue the smart card.

The screenshot shows the HID naviGO Administrator's Portal. The top navigation bar includes links for Home, Users, Roles, Sets, Methods, Reports, Policies, and Settings. The left sidebar contains a 'User Lookup' section with links for Delete Users, New Users, and Reports. The main content area is titled 'Administrator's Portal' and features a 'Find a User' section. This section includes a search form with fields for Username, Domain, and Email, and a 'Find This User' button. Below the search form is a 'Launch Directory Lookup' button. The search results, titled 'Users found:', display a table with the following data:

Username	Domain	Email
fml02	HIDNAVIGO	fml@actidentity.com

4. Search for the user and then click the **Username** to view the User Information.

The screenshot shows the HID naviGO Administrator's Portal. The top navigation bar includes links for Home, Users, Roles, Sets, Methods, Reports, Policies, and Settings. The left sidebar contains a 'User Lookup' section with links for Delete Users, New Users, and Reports. The main content area, titled 'Administrator's Portal', displays user information for a user named fml02. The information includes Username, Domain, Email, LDAP Unique Identifier, Date of last access, Current User State, Authentication Set, Language, and Role. Below the information, there are buttons for 'Edit User' (highlighted with a red box), 'Generate Offline Unblock', 'Enroll On Behalf', and 'Back to List'. A link for 'User Certificates' is also present.

User information

Username	fml02
Domain	HIDNAVIGO
Email	fml@actidentity.com
LDAP Unique Identifier	HIDNAVIGO\fml02
Date of last access	2/7/2012 2:53:55 PM
Current User State	Steady State
Authentication Set	Crescendo only
Language	English
Role	User

[User Certificates](#)

5. Click **Edit User**.

Edit a User

Please edit the following information:

Username	<input type="text" value="navigo_user"/>
Domain	<input type="text" value="navigo"/>
Email	<input type="text" value="navigo_user@ .com"/>
Language	<input type="text" value="English"/>
Authentication Set	<input type="text" value="Crescendo only"/>
Role	<input type="text" value="User"/>
Current User State	<div><div>Steady State</div><div><div>Deactivated</div><div>Steady State</div><div>New Credential</div><div>Replace Credential</div><div>Revoke Credential</div><div>Reset Credential</div><div>Generate Auth Code</div><div>Reset All Credentials</div><div>Renew Credential</div></div></div>

- From the **Current User State** drop-down list, select **New Credential**, and then click **Save**.

The screenshot shows the HID naviGO Administrator's Portal. The top navigation bar includes links for Home, Users, Roles, Sets, Methods, Reports, Policies, and Settings. The left sidebar contains a 'User Lookup' section with links for Delete Users, New Users, and Reports. The main content area, titled 'Administrator's Portal', displays user information for 'fml02'. The 'Current User State' is highlighted with a red box and labeled 'New Credential'. The 'Enroll On Behalf' button is also highlighted with a red box. Other buttons visible are 'Edit User', 'Generate Offline Unblock', and 'Back to List'.

User information

Username	fml02
Domain	HIDNAVIGO
Email	fml@actidentity.com
LDAP Unique Identifier	HIDNAVIGO\fml02
Date of last access	2/7/2012 2:53:55 PM
Current User State	New Credential
Authentication Set	Crescendo only
Language	English
Role	User

[User Certificates](#)

7. Click **Enroll On Behalf**.



You are re-directed to the naviGO User Portal.

8. Insert the user's smart card into the reader and click **OK**.

The screenshot displays the naviGO User Portal interface. At the top, the HID naviGO logo is on the left, and the date and time 'Tuesday 2/7/2012 3:56 PM' along with 'naviGO Server by HID Global' are on the right. Below the header, there are three navigation tabs: 'Home', 'Manage My Credentials', and 'Manage My Settings'. The main content area is titled 'naviGO User Portal' and contains a section 'Set your smart card PIN'. This section includes two input fields for 'Enter New PIN:' and 'Confirm New PIN:'. Below these fields, there are four validation rules listed with checkmarks: a red 'x' for 'PIN must be at least 4 characters long.', and three green checkmarks for 'PINs must match.', 'PIN must not contain more than three repeated characters.', and 'PIN must not contain more than three consecutive characters.'. An 'OK' button is located at the bottom right of the form.

Instructions:
Set your smart card PIN

naviGO User Portal

► Set your smart card PIN

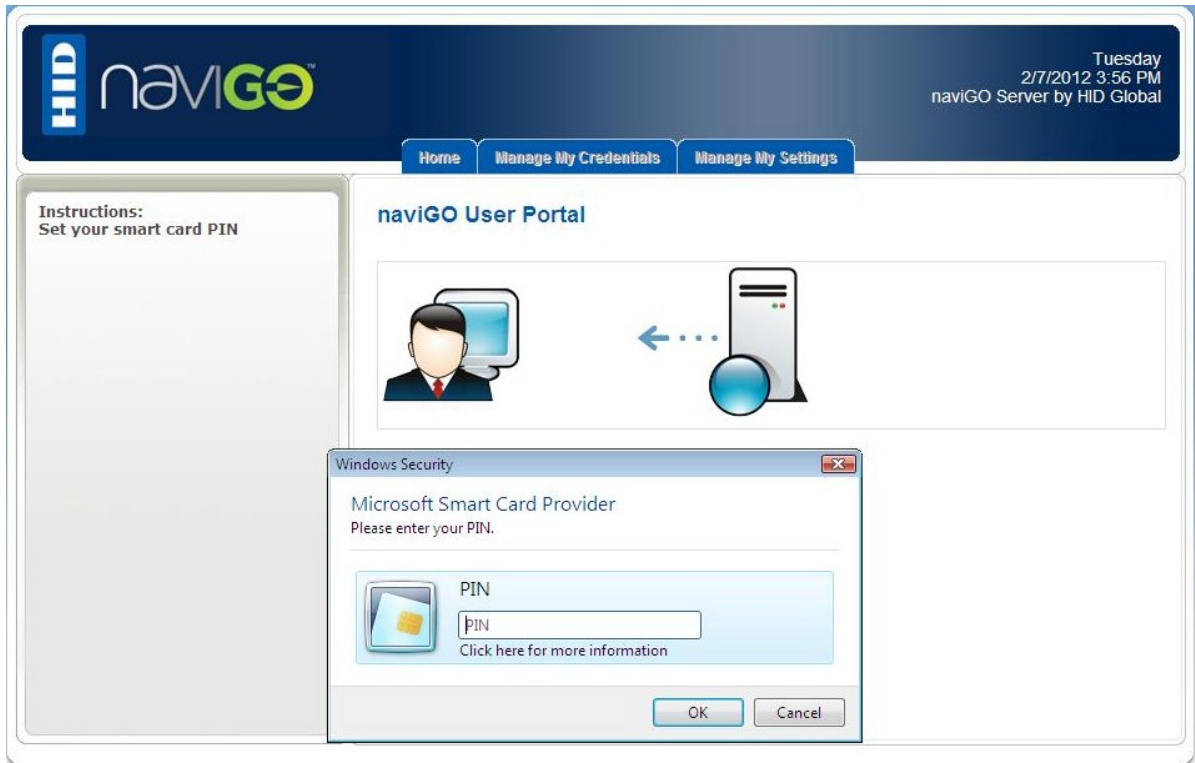
Enter New PIN:

Confirm New PIN:

- ✖ PIN must be at least 4 characters long.
- ✓ PINs must match.
- ✓ PIN must not contain more than three repeated characters.
- ✓ PIN must not contain more than three consecutive characters.

OK

9. Ask the user to set the **PIN** code for the smart card and click **OK**.
The PIN code must meet the specified conditions.



10. Ask the user to enter their PIN code and click **OK**.



When the enrollment process is complete, the user is now in Steady State and can authenticate with his smart card.

The screenshot displays the HID NAVIGO Administrator's Portal. The top navigation bar includes links for Home, Users, Roles, Sets, Methods, Reports, Policies, and Settings. The left sidebar contains a 'User Lookup' section with links for Delete Users, New Users, and Reports. The main content area, titled 'Administrator's Portal', shows user information for 'fml02'. The 'Current User State' is highlighted with a red box and labeled 'Steady State'. Below the user information, there are buttons for 'Edit User', 'Generate Offline Unblock', 'Enroll On Behalf', and 'Back to List'. A link for 'User Certificates' is also present.

Administrator's Portal

Logout: [naviGO_sys_admin](#) | [Help](#) | [About](#)

User information

Username	fml02
Domain	HIDNAVIGO
Email	fml@actividentity.com
LDAP Unique Identifier	HIDNAVIGO\fml02
Date of last access	2/7/2012 2:53:55 PM
Current User State	Steady State
Authentication Set	Crescendo only
Language	English
Role	User

[User Certificates](#)

8.0 Managing a Smart Card with 4TRESS AAA Server

The 4TRESS AAA Server for Remote Access (the AAA Server) is a strong RADIUS, TACACS+ and IEEE 802.1x authentication server that maps to your LDAP directory to provide strong user authentication services for a wide range of access points.

AAA stands for:

- Authentication - accepts or rejects user authentication requests based on stored credentials and/or one-time passwords.
- Authorization - controls user access based on the appropriate attributes transmitted to the network remote access point (VPN, firewall, router etc.,)
- Accounting - stores information concerning user activity while connected remotely (connection times, data transfers etc.,)

Users authenticate through the AAA Server with smart cards, hardware and software tokens, USB keys, mobile devices, PDAs, (and optionally, with static or static LDAP passwords).

A secure remote access solution, the AAA Server enables you to protect the following network access methods:

- Web access
- Remote access via dial-up
- Remote access via VPN
- Remote desktop environments (Microsoft Windows and Citrix®)
- SSL VPN
- Wireless LAN access

The Crescendo C1150 card is initialized with 4TRESS AAA Server Administration Console to add the one-time password (OTP) capabilities.

When the card is initialized, it can be issued (assigned) by the:

- Administrator using the AAA Server Administration Console or the Web Help Desk.
- End user using the self-assignment feature of the AAA Server Web Self Help Desk.

The cards can then be managed by the:

- Administrator (or help desk operator) using the AAA Server Administration Console or the Web Help Desk
- End user using the AAA Server Web Self Help Desk, which provides services such as Unlock PIN and Synchronize Device.

Users can also use and manage the card on their workstation with the ActivClient middleware (to generate OTPs, change the PIN code and import certificates).

The next sections present the initialization and issuance operations with 4TRESS AAA Server, as well as common card management tasks. See the 4TRESS AAA Server documentation for complete instructions on installation, management and usage services.

8.1 Issue a Smart Card Using 4TRESS AAA Server

Before the card can be issued, it must be initialized with 4TRESS AAA Server to add one-time password (OTP) capabilities to the cards.

Once the card is initialized, you can assign it to the required user.

Prerequisites:

- ActivClient 6.2.0.162 or later is installed on the AAA Server Administration Console machine.
 - The *adimCard.spl* file (usually located in \Program Files\ActivIdentity\AAA\spl\card) must be updated to set the **DESKeyType** to **des3**.
 - A PC/SC compatible smart card reader is connected to the machine.
 - On Microsoft Windows 64-bit platforms, you must also install the AAA Server hot fix FIXS1207015.
1. Log on to the AAA Server Administration Console as a Device Manager.
 2. In the tree in the left pane, right-click on **Devices**, then select **Initialize Device** from the menu. Or select **Devices**, and then click **Initialize**.

The image shows a 'Device Initialization' dialog box with the following fields and options:

- Device Type:** A drop-down menu with 'ActivIdentity SmartCard' selected.
- Device Reader:** A drop-down menu with 'ActivIdentity USB Reader' selected.
- Initialization Profile:** An empty drop-down menu.
- Assign user after Initialization:** A checked checkbox.
- Use Initialization Profile Default settings:** An unchecked checkbox.
- PIN Parameters section:**
 - PIN MAX number of tries:** A text box containing '3'.
 - Initial PIN Code:** A text box containing '0151'.
 - Generate random PIN Code:** A checked checkbox.
 - Length:** A text box containing '4'.
- Store Initialized Device in Repository:** A text box containing '/Cards' and a folder icon button.
- Buttons:** 'Initialize' and 'Close' buttons at the bottom.

3. From the **Device Type** drop-down list, select the type of device to initialize (in this case, smart card).
4. From the **Device Reader** drop-down list, select the reader that you want to use with the device that you have selected.
5. Select **Assign user after Initialization** to immediately assign the device to a user after you initialize it.

NOTE You MUST select this option if using ActivClient middleware.

6. In the **PIN Parameters** section of the window, select the required options:
 - **PIN MAX number of tries** - enter the maximum number of consecutive wrong PIN codes that a user can enter on a device before the device automatically locks. When set to zero (0), the user can enter an unlimited number of consecutive wrong PIN codes. The default number for the selected device profile is displayed in this field.
 - **Initial PIN Code** - initializes all the devices with the same initial PIN code value specified in the field. It is recommended that users change the initial PIN code during the first connection. You cannot enter a “weak” PIN code. Examples of weak PIN codes are 1357, 1234, and 1111 (ones with a constant amount between each of the digits).
 - **Generate Random PIN Code** - select this option to have the AAA Server

randomly generate a different initial PIN code for each device during initialization. If you select this option, then in the Length field, enter a length for the random PIN code. This length must be within the minimum and maximum PIN length values for the selected device profile.

7. The **Store Initialized Device in Repository** field displays the default repository where the AAA Server will store the initialized card's information.

If you are logged into the Administration Console as a user who has Device Manager rights, you can select a different repository:

- a. Click to select the repository where you want to store the initialized device.
- b. Select the repository in which to store the device that you are initializing.

The name of the folder is displayed in the field at the top of the window.

(Repositories with arrows indicate there are devices stored in those folders.)

- c. Click **OK**.

The repository name automatically appears in the Repository field in the Device Initialization window.

8. Insert the Crescendo C1150 smart card into your smart card reader, and then click **Initialize**.

NOTE The default PIN code is 1254.

Once the AAA Server has finished initializing the card, a message is displayed stating that the initialization was successful. It also displays the initial PIN code value of the device.

9. Click **OK**.

10. Select either **Group** or the **LDAP query**.
11. Select a value from the drop-down lists in either the **Select group** or the **Select query** fields.

You do not have to define the **User ID** field unless you want to filter more specifically within a large group of users.
12. Click **Search**. The users matching your selected group or query are displayed.
13. Select the required user, and then click **Assign**.

The card's serial number immediately is displayed next to the user's name.

8.2 Change the PIN Code

End users managing the Crescendo C1150 card with ActivClient can change the PIN code using the ActivClient PIN Change Tool.

For further information, see section [6.2 Change the PIN Code with ActivClient](#) on page 76.

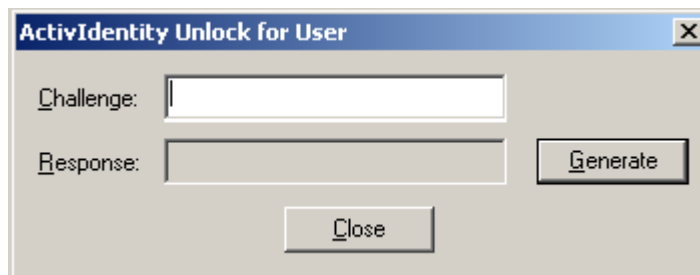
8.3 Unlock the Smart Card with 4TRESS AAA Server

The Crescendo C1150 PIN will lock if the user presents six consecutive incorrect PINs. When the PIN is locked, you cannot use the card until you unlock the PIN.

You can unlock it with the challenge/response unlock code managed by 4TRESS AAA Server.

8.3.1 Unlock the Smart Card with the Administration Console

1. In the tree in the left pane of the Administration Console, select **Help Desk**, and then search for a user via the drop-down list of LDAP queries or Groups.
Optionally, enter a User ID or Device serial number in the appropriate field.
2. Select the user ID that corresponds to the required serial number in the Search Results display, and then click **Help Desk**.
3. Click **Unlock PIN Code**.



4. Ask the user for the unlock challenge displayed in the ActivClient User Console Unlock Smart Card screen.
5. Enter the challenge in the **Challenge** field of your Help Desk, and then click **Generate**.
The unlock code is displayed in the Response field.
6. Give the unlock code to the user.
7. Instruct the user to enter the code in the relevant ActivClient User Console field to unlock the Crescendo smart card.

The user must then enter and confirm new PIN code to complete the procedure.

8.3.2 Unlock the Smart Card with the Web Help Desk

1. Log on to the Web Help Desk and search for the user.
2. Select the corresponding link for the user's device in the **Device ID** column of the search results form.
3. Select **Unlock PIN code** in the device data page.

The screenshot shows a web application interface with two tabs: 'Help Desk' and 'Configuration'. The 'Configuration' tab is active. Below the tabs, there is a table with the following data:

User ID	John Smith	Group	all
Device Serial Number		Authentication	Dual

Below the table, the text 'Please enter the challenge for unlock PIN code:' is displayed. There is a text input field labeled 'Challenge:' followed by a 'Generate unlock code' button. Below this, there is a text input field labeled 'Unlock code:' and a 'Back' button.

4. Ask the user for the unlock challenge displayed in the ActivClient User Console Unlock Smart Card screen.
5. Enter the challenge in the **Challenge** field of your Web Help Desk and click **Generate unlock code**.

The unlock response is displayed in the **Unlock code** field.

6. Instruct the user to enter the response in the relevant ActivClient User Console field to unlock the Crescendo smart card.

The user must then enter and confirm new PIN code to complete the procedure.

8.3.3 Unlock the Smart Card with the Web Self Help Desk

1. Connect to the Web Self Help Desk, enter your logon credentials, and then click **OK**.
2. If you have more than one device, make sure that the Crescendo C1150 card is selected.

Device

Serial Number:

*My device authentications keep failing: **Synchronize.***

*My device is locked: **Unlock my device PIN Code.***

*My device has been lost or stolen: **Lock my lost device.***

- Under **Device**, click **Unlock my device PIN Code**.

Unlock my device PIN Code

Serial Number:

Please enter the challenge for unlock PIN code:

Challenge:

Generate unlock code

Unlock code:

Back

- Open the ActivClient User Console and access the Unlock Card screen in order to display the unlock challenge.
- Enter the generated challenge in the **Challenge** field, then click **Generate unlock code**.
The Unlock code is displayed in the **Challenge** field.
- Enter the response in the relevant ActivClient User Console field to unlock the Crescendo smart card.
Your card unlocks and you are prompted to enter a new PIN code.

8.4 Importing Certificates

Administrators or end users can download a certificate from the Microsoft CA (or other CA), by selecting the ActivClient CSP.

The certificate can then be imported on to the Crescendo C1150 card using ActivClient.

For further information, see section [6.5 Importing Certificates Using ActivClient](#) on page [83](#).

9.0 Using the Smart Card

This chapter provides an overview of how you can use your smart card and PKI certificate to authenticate.

This section presents use cases applicable to both the Crescendo C1150 Mini Driver and ActivClient – differences are noted where applicable. For further information, see section [2.4 Choosing Smart Card Middleware](#) on page 12.

For further instructions on using your smart card, see the ActivClient technical documentation or relevant Microsoft resources.

9.1 Logging On to Microsoft Windows

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.

You can also log off or lock the workstation you remove the smart card, securing the workstation when you are not at your desk.

9.2 Authenticating to Secure Websites

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

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

NOTE Mozilla Firefox support is only available with ActivClient.

3. If you are prompted to select the certificate, select the appropriate certificate, and click **OK**.
4. Enter your PIN 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.

9.3 Sending and Reading Secure Emails

You can use your smart card-based certificate to read and send digitally signed and encrypted emails.

9.3.1 Send Signed/Encrypted Emails

1. Compose your message
2. Add your digital signature or encrypt the message using the menu options of your email client (such as Microsoft Outlook or Mozilla Thunderbird).

NOTE Mozilla Thunderbird support is only available with ActivClient.

3. Click **Send** and, if prompted, enter your PIN code.

9.3.2 Read Signed/Encrypted Emails

Open email you want to read, and, if prompted enter your PIN code.

9.4 Encrypting and Decrypting Files

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.

ActivClient supports the Encrypting File System (EFS) feature of Microsoft Windows.

9.4.1 Encrypt a File or Folder

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. First time, you might need to configure EFS during your first file encryption (depending on your platform configuration) you are 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.

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.

6. For all subsequent encryption operations, you only need to enter your smart card PIN and click **OK**.

9.4.2 Decrypt a File or Folder

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

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

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

The file or folder is opened in clear text.

10.0 Troubleshooting

10.1 ActiveX Error During Certificate Requests

When visiting some CA web pages, you may encounter a so-called 'ActiveX' error. This error is caused by the fact that some ActiveX controls are not trusted within the Internet Explorer browser. As a result, you cannot view the page as it was intended; hence you cannot enroll a certificate from that page.

When visiting the web page of the **Smart Card Certificate Enrollment Station**, you may encounter such an 'ActiveX' error:

There are several ways to resolve this issue. This guide describes a scenario that configures the security of the Internet Explorer browser in such a way that it will accept the ActiveX control components. This implies that you do not have to follow the scenario we describe (as this entails bringing down the security of the Internet Explorer browser). A different solution may be better suited for your situation.

1. Go to Tools > Internet Options.
2. In the Internet Options dialog, select the **Security** tab and **Local intranet**.
3. Click **Default Level**.
4. Drag the slider to **Low**, decreasing the security level.
5. Close this dialog by clicking **OK**.

10.2 Smart Card Enrollment Errors

There are a number of causes for when a smart card Enrollment fails. The most common errors and their possible cause are described.

10.2.1 Wrong CSP

When you have selected the wrong CSP (that is, a CSP that does not correspond to the smart card you have inserted), an error message displays.

Verify that the CSP you have selected from the Cryptographic Service Provider drop-down list corresponds to your deployment model:

- For Mini Driver deployments, select Microsoft Base Smart Card Crypto Provider.
- For ActivClient deployments, select ActivClient Cryptographic Service Provider.

10.2.2 Key Length Setting

When the minimum key size in the Certificate Templates (in this case, the Smart Card User, Smart Card Logon or your own custom template) has been set to a key length not supported by the smart card, the software will nevertheless try to generate a key pair of this size and fail.

Check the Certificate Template and, if necessary, edit the minimum key size to 1024.

10.2.3 Enrollment Rights

When the Administrator Signing Certificate is not available, check that the user who is acting as the enrollment agent has an enrollment agent certificate.

When the Certificate Template required is not available, verify the rights of the enrollment agent on the desired template. The template should provide the enrollment agent with read and enroll rights.

11.0 Security Guidelines

The chapter provides guidelines for ensuring the secure deployment of the Crescendo C1150 Mini Driver.

It is limited to recommendations for securing the environment assets that have an impact on the Crescendo product and environment. Standard best IT security practices should also be considered as part of a secure deployment. The chapter is organized by recommendations.

11.1 SHA-2 Compliance

As part of a security improvement, organizations are transitioning from the SHA-1 hashing algorithm to a SHA-2 (usually SHA-256) hashing algorithm, especially for digital signature operations.

This section describes the impact of these changes on various applications.

11.1.1 Card Content Signed with SHA-2

The Crescendo C1150 Mini Driver supports smart cards whose content (digital certificates) is signed with a SHA-2 hashing algorithm. This change might have an impact on some applications, as indicated in the table below.

Service	Product and versions	Notes
Windows PKI Logon	<ul style="list-style-type: none">Supported Clients – Windows XP SP3, Vista, 7 and 8Supported Servers - Windows Server 2003, 2008, 2008 R2 and 2012	Windows Server 2003 requires two Microsoft hot fixes not available on Windows Update - KB 938397 and 968730
Remote access	Windows, Check Point, Cisco, Juniper, etc. Check with your vendor.	
Secure web access	<ul style="list-style-type: none">Supported browsers - Microsoft Internet Explorer 6 and later, and Google Chrome 11 and later. Browsers have limited impact on SHA-2 certificates.Supported server - IIS 6 and later, Apache 2.2 and later. Check with your vendor for other web servers	IIS 6 on Windows Server 2003 requires two Microsoft hot fixes not available on Windows Update - KB 938397 and 968730.
Secure email	Supported applications: <ul style="list-style-type: none">Microsoft Outlook 2003, 2007, 2010,Outlook Web Access (with Exchange 2003, 2007, 2010)	Email signature is configured for SHA-1. See next section for SHA-2 configuration.

Service	Product and versions	Notes
Document signing	Supported applications: <ul style="list-style-type: none"> Office 2003, 2007, 2010 (e.g. Word, Excel) Adobe Acrobat Professional 9 and later Windows 7 XPS Viewer 	Document signature is configured for SHA-1. See next section for SHA-2 configuration
Document encryption	Supported applications: <ul style="list-style-type: none"> Windows EFS on Windows Vista and 7 BitLocker To Go on Windows 7 and Windows 8 	

11.1.2 Using SHA-2 for Digital Signature Operations

The Crescendo C1150 Mini Driver supports use cases where SHA-2 is used for digital signature operations with the latest Microsoft applications.

Service	Product and versions	Notes
Email signature	Supported applications: <ul style="list-style-type: none"> Microsoft Outlook 2007, 2010 with Exchange 2003 or later Outlook Web Access with Exchange 2007 or later 	<p>Outlook information:</p> <ul style="list-style-type: none"> Requires Windows Vista or later. Sender and recipient both need to comply with these Windows, Outlook and Exchange system requirements (otherwise, they cannot read the SHA-256 signed email). <p>Outlook Web Access information:</p> <ul style="list-style-type: none"> Requires Windows Vista or later. Sender and recipient both need to comply with these Windows, Outlook and Exchange system requirements (otherwise, they cannot read the SHA-256 signed email). Exchange requires a specific registry-based configuration. See details at http://technet.microsoft.com/en-us/library/bb738151(EXCHG.80).aspx, set the "S/MIME Default Signing Algorithm" to SHA 256.

Service	Product and versions	Notes
Document signature	Supported applications: <ul style="list-style-type: none"> Office 2010 (e.g. Word, Excel) Adobe Acrobat Professional 9.1 and later 	Office information: <ul style="list-style-type: none"> Requires a specific policy configuration: “Select digital signature hashing algorithm”. See http://technet.microsoft.com/en-us/library/cc545900.aspx for details. Acrobat information: <ul style="list-style-type: none"> Requires a specific policy configuration. See details at http://learn.adobe.com/wiki/download/attachments/52658564/acrobat_reader_security_9x.pdf?version=1 (pages 16 and 124). <p>Note: The Windows 7 XPS Viewer does not support SHA 256 at this point.</p>

11.2 PIN Policies

HID Global recommends to use a minimum PIN length of six digits to meet FIPS security objectives (1/1,000,000 probability of detection).

11.3 Log Handling

If an issue is identified with the Crescendo C1150 Mini Driver, HID Global support department may request sending some log files in order to diagnose and troubleshoot the problem.

These logs do not contain any sensitive data or personally identifiable information according to HID Global internal security policies.

By default, the log files are not signed or encrypted. As such, as an additional precautionary measure, HID Global recommends protecting logs for confidentiality and integrity during transport to a remote IT group. Usage of such capabilities as signed and encrypted email or secure FTP shall be used to exchange log files with a remote IT department or HID Global support organization.

11.4 Additional Recommendations

The following are generic recommendations that will enable to further increase the security of the Crescendo C1150 solution:

1. Confirm that anti-virus and anti-malware software on the users’ workstations remains up to date. Contact your anti-virus and anti-malware software vendors to inquire if the .dat files have the latest update.

2. Confirm that computer operating systems and desktop applications remain up to date on all security patches.
3. Reconfigure computer operating systems to only allow authorized software. For instance, users of the Windows operating systems should use available technologies such as the Software Restriction Policies and AppLocker, which offer a range of policies to block malicious scripts, help lockdown a computer, or prevent unwanted applications from running.
4. Users should not be using an account with administrator privileges for day-to-day activities.
5. Lockdown the security of the browsers according to the vendor's security best practices.
6. Lockdown the security of email clients according to the vendor's security best practices, especially to guarantee that attachments are handled securely.
7. Lockdown the platform configuration according to industry best practices – for U.S. government customers, leveraging the Federal Desktop Core Configuration (FDCC), United States Government Configuration Baseline (USGCB) approved configurations or the STIGS recommendations, which are part of the DoD Information Assurance.
8. Install anti-key logger software; select software options that cover all desktop applications.
9. Train users on social engineering risks, and best practices to handle their PIN and interacting with applications.

Social media networking websites (such as Facebook and LinkedIn) have become extremely popular for networking professionally and personally, raising the visibility of these sites for potential threats. In particular, educate employees that they should not accept invites from people they do not know, nor execute embedded applications made available through such sites. Also, if your organization has a formal policy on accessing social media sites, it is always good to reinforce the policies.

10. Educate employees on the risks of emails that appear suspicious. In a large proportion of successful attacks, the malware infects a PC via an email attachment. In particular, employees should be extremely cautious about opening unsolicited attachments sent from users outside of the corporate network. If there are concerns about the email alert your IT Department.
11. Instant Messaging is also another approach that can be used to infect a PC with malware or for a person to reach out to acquire confidential employee information or employee email addresses. Educate employees not to accept or respond to such requests, without confirming the authentication of the request by contacting the perspective company.
12. Train users on smart card and PIN best practices: remove your card from the reader when you leave your desk; this will lock the workstation and in parallel prevent any malware from using your card. Be cautious about any application that asks for your PIN; provide it to applications that you know need to access your card for legitimate authentication and signature needs. Also, check if your middleware and smart card reader provide visual clues about smart card activity (icon blinking, LED changing color) – it helps keeping control of your smart card operations.

HID Global Headquarters:

North America: +1 949 732 2000

Toll Free: 1 800 237 7769



hidglobal.com