plusID Manager
Operators Manual

for use with plusID 60 devices

Version 1.0
July 2007

PRIVARIS®

Table of Contents

Section I: GETTING STARTED

1. Introduction

plusID Manager is the software application used to issue plusID™ personal biometric devices. It enables the enrollment and configuration of devices by an authorized Enrollment Administrator, or other designated personnel.

2. What is a plusID Device?

The plusID personal biometric device is a universal credential that replaces access cards used to enter secured buildings and passwords used to log on to computers. plusID uses its owner's fingerprint to verify their identity before granting access. It works in much the same way that a remote control is used to operate a television or a garage door, but requires its authorized owner's fingerprint to "unlock" the device for operation.

3. What is Enrollment?

Enrollment is a key component to plusID device issuance. It is what makes the device work for its enrolled owner and no one else. During enrollment a user's fingerprint images are captured, encoded, and securely stored as templates on the plusID device. During regular operation, any live fingerprint presented to the device is compared to the templates stored on the device to ensure that only the authorized user can operate the device. This comparison, or matching process, is called verification. Enrollment readies a device to be used for verification.

The enrollment process also includes assigning access credentials to the buttons found on the front of the device. This is what enables the plusID device to be used for physical access to doors and facilities.

4. System Components

- One (1) CD-ROM containing the Privaris plusID Manager software application and documentation
- plusID device(s)
- One (1) available USB port on the computer running plusID Manager
- One (1) mini-USB cable (packaged with each plusID device)
- Microsoft® Windows® 2000 SP4, XP Home, XP Professional or Vista
- 64 megabytes of RAM
- 50 megabytes of available hard drive space
- 800x600 minimum screen resolution

5. How It Works

The plusID Manager software communicates with plusID devices over a USB connection. When connected to the USB port of a computer, the blue light on the device stays on to show that a connection between the device and the PC has been made.

6. Securing plusID Devices

a. The Administrator PIN & Device Registration

plusID devices are secured to a specific organization through the assignment of an Administrator PIN. It is what prevents the manipulation of issued plusID devices by outside organizations and malicious or otherwise non-authorized parties.

The Administrator PIN is assigned to the device during registration (when the device is connected to the plusID Manager application for the first time) and is securely stored on the device.

Each issuing organization must select an Administrator PIN (Personal Identification Number) that will be used by Enrollment Administrators to enroll and update all plusID devices. This PIN should be treated as a corporate secret and guarded in the same manner as other keys/passwords that grant access to valuable resources. It is recommended that the Administrator PIN only be accessible by officers of the company and designated Enrollment Administrators/Security Personnel.

! *There is no way to reset the Administrator PIN that is installed on devices during device registration. If the Administrator PIN is lost or forgotten you will **not** be able to access or modify any previously issued devices.*

! *It is highly recommended that each organization select a **single** Administrator PIN for all plusID devices. Creation of more than one PIN will result in a population of devices having different PINs and there is no way to determine what PIN is on a device other than by trial and error (with a limited number of attempts).*

! *If the Administrator PIN were ever to be compromised, issued devices would be susceptible to manipulation by outside organizations, and the security of corporate physical and logical assets would be placed at risk.*

b. Single Administrative Authority

Each device can have only one administrative authority. For security purposes, once issued, the device can only be modified or updated using the same computer on which it was originally registered. A registered device cannot be updated on any another computer running the plusID Manager software (even within the same organization).

! *The plusID Manager software is not intended to be installed on more than one computer/workstation per organization.*

If trying to connect a previously issued device registered by another computer, a Security Advisory will appear (Figure 1). The only menu options available will be “Device Status” and “Settings,” in order to prohibit fingerprint templates from being added or removed.

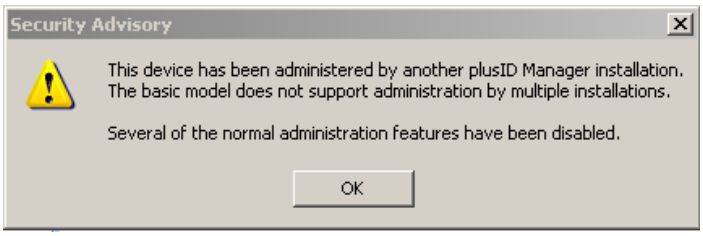


Figure 1
Security Advisory

The only way for a registered device to be updated from a different workstation than the one on which it was registered is for the device to be reset (see Section III, 9.c.). Resetting device erases all stored fingerprint templates, restores its factory default settings, and enables a device to be registered to a new user. Resetting the device does not reset the Administrator PIN (assuming it was changed from the default PIN at the time of device registration).

7. plusID Manager Installation

The CD containing the plusID Manager software will run automatically when inserted in the CD-ROM drive, provided auto run is enabled, and will display the plusID Manager Setup Wizard (Figure 2). If the installation program does not run automatically, navigate to the CD-ROM drive and double click setup.exe.

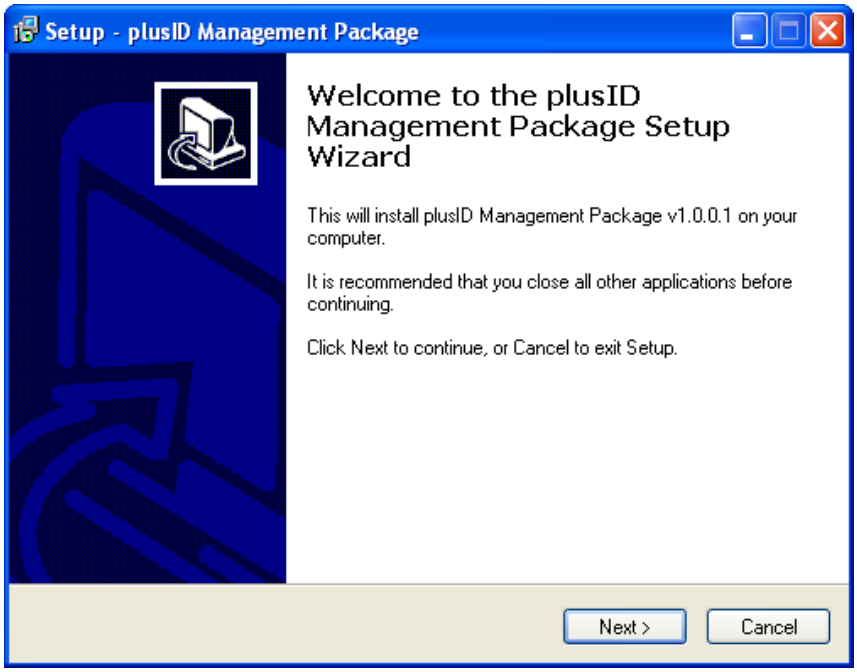


Figure 2
Installation Setup Wizard

Follow the screen prompts to install the software:

- Component selection:
  There are two available components, the plusID Manager software and the minidriver that is required to use the plusID device for computer logon and to issue credentials for computer logon to other device recipients. Select from an Administration Installation (plusID Manager and minidriver), Client Installation (minidriver only) or Custom Installation (either).

  When the component selection is complete, another Setup Wizard window will appear to configure the installation options for the plusID Manager software:

  - Acceptance of the plusID software licensing agreement terms
  - Designation of the software destination location
  - Designation of software icons
  - Automatic installation of Crystal Reports for .Net Framework 2.0 (required for the plusID Manager's reporting tool), if not already resident on computer

8. Connecting to a plusID Device

A plusID device will power on automatically when connected via USB:

- Turn on the computer
- Insert the large end of a mini-USB cable (included with every plusID device) into the computer's USB port
- Insert the smallest end of the mini-USB cable into the USB port at the base of the plusID device

The device's blue light will blink while it is connecting and turn solid once a connection with the computer has been established. As long as the device is connected via USB, the solid blue light will stay on and the device's battery will be being charged (provided the PC is not hibernating).

Found New Hardware Wizard
The first time the device is connected to a computer, the Found New Hardware Wizard will appear to prompt the downloading of a device driver (a standard Microsoft driver) that enables the device to communicate with the computer:

- if the plusID Manager CD-ROM is inserted in the computer, point the hardware wizard to the CD

- if the plusID Manager CD-ROM is not inserted, point the hardware wizard to the Internet, where it will find the standard Microsoft driver

9. Starting the Application

To start the application from the Windows taskbar click Start>Programs>Privaris>plusID Manager (or elsewhere if you modified the default file destination during installation), or double-click the plusID Manager desktop icon shortcut, if created during setup.

The plusID Manager home page and main menu tree will be displayed (Figure 3).

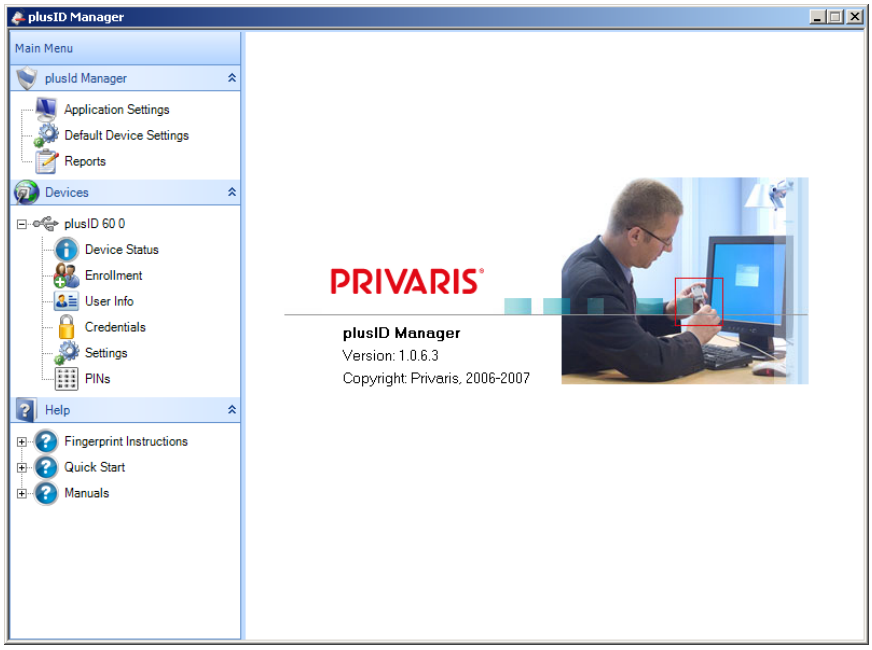


Figure 3
Main Menu

The main menu tree has three branches.

1. plusID Manager
2. Devices
3. Help

Each branch contains several menu options and can be expanded and collapsed using the up/down arrow to the right of the branch's name.

If a plusID device is not connected to the computer when the plusID Manager application is opened, the menu options contained under "Devices" will not be available.

Section II: PLUSID MANAGER MENU OPTIONS

1. **Application Settings**

The "Application Settings" screen (Figure 1) contains three tabs: Settings, Utilities and About:

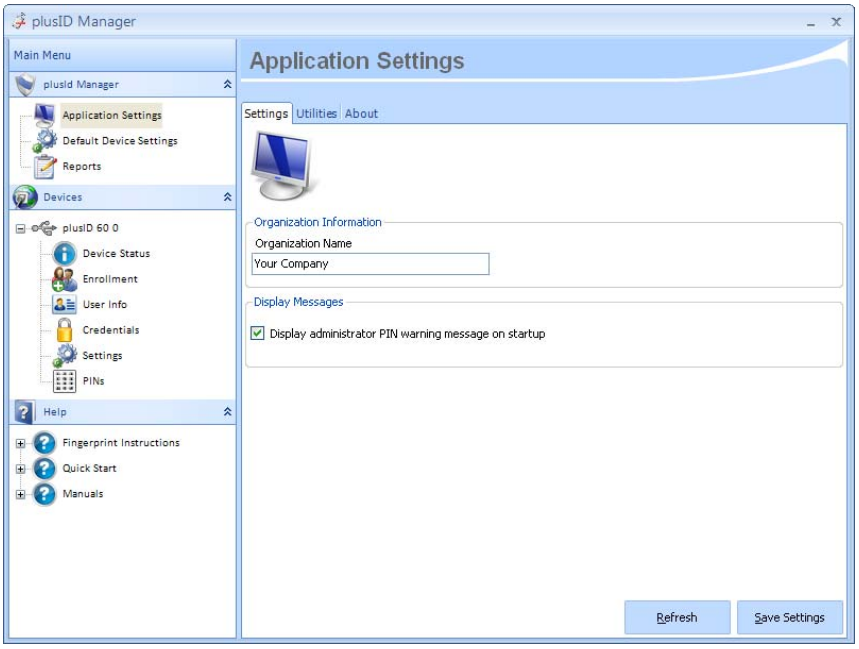


Figure 1
Application Settings

Settings

Enter the issuing organization's name on this screen and it will be included on every report that is run from the plusID Manager software. This field is not mandatory.

Select whether or not the Administrator PIN warning is displayed each time that the plusID Manager is launched.

! *The Administrator PIN function is critical to ensuring the security of devices.*

Utilities

During device registration, the plusID Manager application stores, at a minimum, the name of each user and the serial number of the plusID device issued to that user (additional user data can be entered using the "User Info" screen in the main menu tree). The "Utilities" screen allows an organization to determine if and where this database of device user information is backed-up for safe keeping. If the "Always back-up database on start up…" box is checked, a file location for downloading the back-up data must be designated using the "browse" button. The "Back-up Database Now" button activates a real-time database download (as opposed to the back-up occurring only when the application is started). Once selected, a pop-up appears for designating where on the computer the back-up file should be saved.

About
The "About" screen lists the version number of the plusID Manager software application.

2. **Default Device Settings**

The "Default Device Settings" screen (Figure 2) contains the settings that will be applied to all plusID devices enrolled with the plusID Manager software. These settings can be changed at any time, but changes will apply only to devices enrolled, re-enrolled, or re-configured, after the Default Device Settings have been modified.

Note: These default settings can be changed for individual plusID devices at any time by selecting the "Settings" option under "Devices" from the main menu tree. Changes made on the "Settings" screen override the default device settings only for the individual plusID device that is connected at that time.

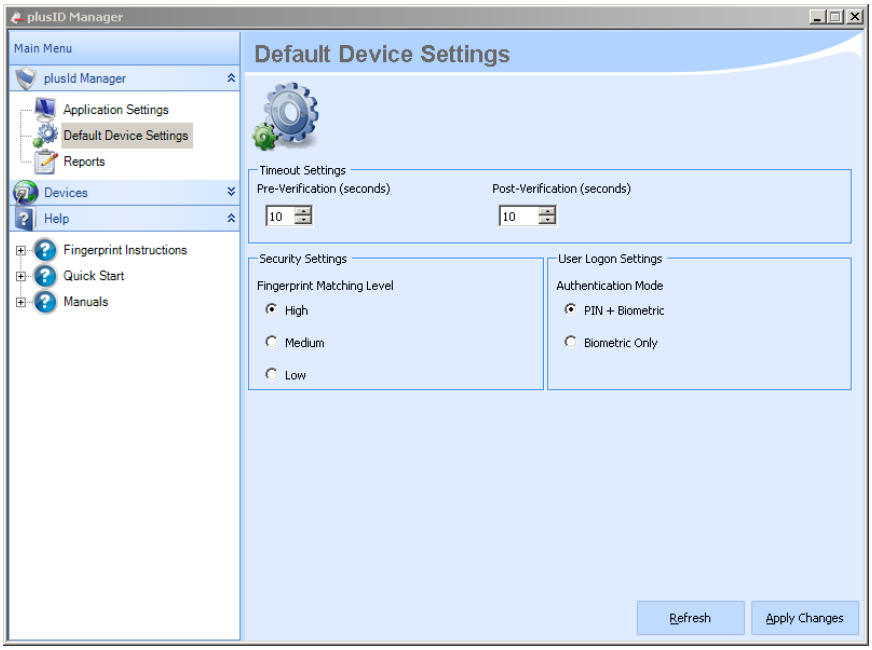


Figure 2
Default Device Settings

To configure the default settings, select "Default Device Settings" from the main menu tree.

Select "Apply Changes" after modifying any of the settings on this screen for the settings to take effect.

The "Refresh" button resets the settings to their default values.

Following are descriptions of the individual setting options.

a. **Timeout Settings**

Pre-Verification

The Pre-Verification timeout setting determines how long the device will wait for a verification (fingerprint swipe) before powering off.

The timeout can be set from 5 to 255 seconds. The default setting is 10 seconds.

Note: This setting only applies to verifications performed after enrollment, during normal device usage, and when the device is not connected to a computer.

Post-Verification

The Post-Verification timeout setting determines how long the device's credentials will remain active after a successful verification. The device is active for as long as its green light is on, post-verification.

The timeout can be set from 5 to 255 seconds. The default setting is 10 seconds.

! *The longer the post-verification timeout setting the greater the demand on the device's battery, which may reduce the average number of verifications available per charge.*

b. **Security Settings**

Fingerprint Matching Level

The plusID device has three configurable security settings: High, Medium, and Low. Each setting corresponds to an associated fingerprint matching level, or False Acceptance Rate (FAR).

Every biometric system has an associated FAR. An FAR is the percentage of unauthorized users that the device will incorrectly match to a valid user's stored fingerprint template. Below are the FARs that can be set in the plusID device:

Security Setting	False Acceptance Rate (FAR)	
Low (Less Strict)	1 in 1,000	(.1%)
Medium (Default)	1 in 10,000	(.01%)
High (More Strict)	1 in 100,000	(.001%)

The low security setting may match (verify) a fingerprint faster than the high security setting, but will allow a higher number of false acceptances, and vice versa.

The recommended, and default security setting for the plusID device is high.

c. **User Logon Settings***

Authentication Mode

The Authentication Mode selection sets the security level required when using the plusID device for computer logon (post-enrollment). If the device is not being used for logon, this setting can be left at its default value.

There are two options:

PIN + Biometric
requires a personal identification number (PIN) and a biometric verification (using the plusID device). *Note*: If this option is selected, a User PIN must be assigned. (See Section III, 7.b. for more information.)

Biometric Only
requires only a biometric verification (using the plusID device)

The first option is a three-factor security solution: something the user has (the plusID device), something they know (a PIN) and something they are (their fingerprint).

The second option is a two-factor security solution: something the user has (the plusID device) and something they are (their fingerprint).

The default value is the highest security level, PIN + Biometric.

**See Appendix E for system requirements for using plusID devices for logon in a Microsoft® Domain Environment.*

3. **Reports**

The Reports screen contains two pre-determined plusID Manager reports which can be generated and run with date and user name filters. The two available reports are:

User Accounts
Displays specific information on every user that has been enrolled using the plusID Manager application

Devices
Displays specific information on every device that has been issued using the plusID Manager application

Highlight and select the desired report, apply the desired filters, then select "Generate Report."

Reports are launched in a pop-up window and can be viewed, exported to a delimited file, or copied from the preview screen.

Report Filters
Reports can be filtered by date or user name, or neither.

To filter by date, select "Filter by Date" and choose the start and end date. This will retrieve **all** data records created between the specified dates, and including those dates.

To filter by a specific user's name to whom a device has been issued, enter the first and/or last name, or any portion of either name. For example, to search for Mary

Jones, enter “Mary” or “Jones” or “Mary Jones” or “Mar” or “Jon” or “M” or “J.” The more specific the search criteria, the more narrow the results will be.

To retrieve **all** data records, do not apply any filters. Select “Ignore Date” and leave the user name filter blank. This will run the report for all users or devices (respectively) regardless of the date registered.

Section III: DEVICES MENU OPTIONS

The “Devices” branch of the main menu tree is only visible when a plusID device is connected to the plusID Manager computer via USB. To expand or collapse the “Devices” branch of the menu tree, click the arrow to the right of “Devices.”

With a plusID device connected, the main “Device” screen will appear (Figure 1). This screen provides a snapshot of the device(s) connected to the plusID Manager. It lists the plusID model number, serial number and the version of the firmware (software) contained in each device. The number listed after the plusID model number (0, 1 or 2) corresponds to the number of plusID devices connected to the plusID Manager.

Figure 1
Devices Screen

If more than one plusID device is connected a separate node of the menu tree will appear for each device (Figure 2), and specify the type of device, its model number. The counter after the device model number (0, 1 or 2) corresponds to the number of devices connected. Clicking on the plus/minus sign to the left of this node expands/collapses the menu options for each device.

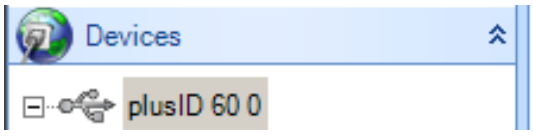


Figure 2
Device Indicator

1. plusID Device Registration

a. Overview

When a device is connected to the plusID Manager software for the first time the "Register plusID Device" screen will appear (Figure 3). This screen registers the device to its user as well as to the issuing organization.

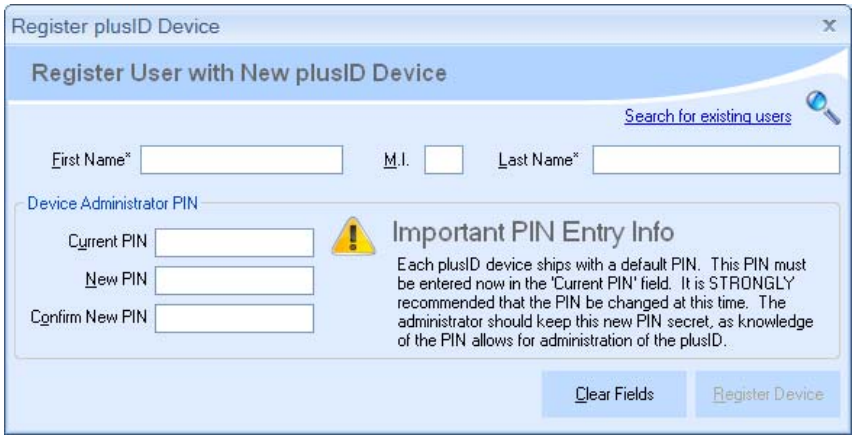


Figure 3
Device Registration Screen

The device is registered to the user by entering the user's first and last name.

The device is registered (and thereby secured) to the issuing organization by issuing an Administrator PIN to the device. The Administrator PIN is a security feature that makes plusID devices unique to each issuing organization, and prohibits the manipulation of issued plusID devices by outside organizations and malicious or otherwise non-authorized parties.

Each plusID device is shipped with a factory default Administrator PIN. To secure a device to the issuing organization, the factory default PIN must be overwritten with the organization's Administrator PIN using the "Device Registration" screen (Figure 3).

! *It is highly recommended that each organization select a **single** Administrator PIN for all plusID devices. Creation of more than one PIN will result in a population of devices having different PINs. There is no way to determine what PIN is on a device other than by trial and error and the number of attempts is limited. This PIN should be treated as a corporate secret and guarded in the same manner as other keys/passwords that grant access to valuable resources. If the Administrator PIN were ever to be compromised, issued devices would be susceptible to manipulation by outside organizations, and the security of corporate physical and logical assets would be placed at risk. (See Section I.6.a. under Getting Started for critical information on Administrator PIN selection and ramifications).*

2. Device Registration

When a new or reset device is connected to the plusID Manager for the first time the "Register plusID Device" screen is displayed (Figure 3).

The three steps below must be repeated each time a new plusID device is connected.

1. Enter the first and last name of the user (mandatory). *Note*: This information is not stored on the user's device. It is stored only in the plusID Manager's database for record keeping purposes.

   If the device is being connected for the first time but a user is not being enrolled, a placeholder first and last name can be entered to register the device, and then changed (using the "User Info" screen) when the device is enrolled.

2. Enter the device's factory default PIN (4321) in the Current PIN field. Then enter the organization's Administrator PIN in the New PIN field and confirm it in the indicated field. This overwrites the default PIN and installs the organization's Administrator PIN on the device. The Administrator PIN can be from four (4) to eight (8) letters, numbers and/or characters.

! *It is imperative that the Administrator PIN be treated as a corporate secret and guarded in the same manner as other keys/passwords that grant access to valuable resources. There is no way to reset the Administrator PIN. If it were lost or forgotten you will not be able to modify any previously issued devices (See Section I.6.a. under Getting Started for critical information on Administrator PIN selection and ramifications).*

! *The current (default) Administrator PIN for all new plusID devices is 4321*

3. Select the Register Device button.

The Administrator PIN is requested only once per plusID Manager session, per device. It will not be requested again during the same session, but will be required each time a new device is connected.

3. Use of the Administrator PIN with Previously Registered Devices

When a registered device is connected to the same plusID Manager computer on which it was registered, it will be recognized as an authorized device. The "Device Registration" screen will not be displayed. The Administrator PIN (the PIN chosen by the Administrator's organization, not the default PIN) will be requested whenever a function requiring security is invoked, such as enrolling an additional finger or loading a credential (Figure 4).

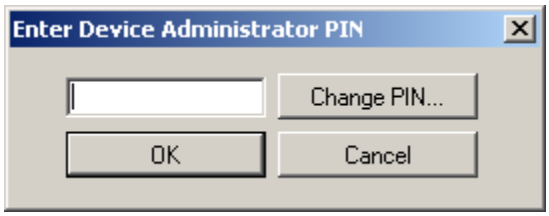


Figure 4
Admin PIN Entry

The Administrator PIN is requested only once per plusID Manager session, per device. It will not be requested again during the same session, but will be required each time a new device is connected.

In the case of a device that has been reset, the Device Registration screen will be presented just as with a new unregistered device. Though the reset device will still have the same Administrator PIN assigned during its initial registration, not the default PIN. The Administrator PIN is not reset when the device is reset.

a. **Incorrect PIN Entry**
If the incorrect Administrator PIN or User PIN is entered an Incorrect PIN message is displayed (Figure 5).

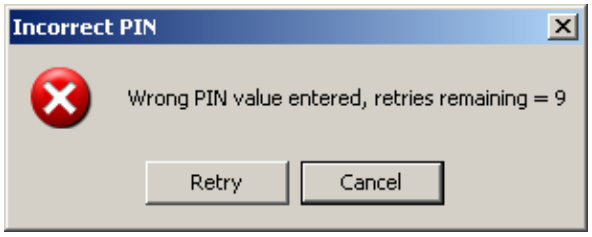


Figure 5
Incorrect PIN Message

To prevent malicious attempts to access plusID devices, only nine incorrect tries are permitted. If the correct PIN is not entered on the tenth try, the device will be inaccessible. The number of retries remaining is shown in the Incorrect PIN message box. In the case of the User PIN the Administrator can reset the PIN to the factory default setting (see below).

! *If the Administrator PIN is entered incorrectly ten times, the connected device will be permanently inaccessible to the Administrator.*

b. **Issuing More than One Device per User**
If issuing an additional or a replacement device to a user, the user information may be retrieved from the database to ensure the accuracy of data entry. Click the “Search for existing users” button on the “Device Registration” screen and select the user from the list of users in the database. All of the same user information will be associated with the new device in the plusID Manager database.

4. Device Status

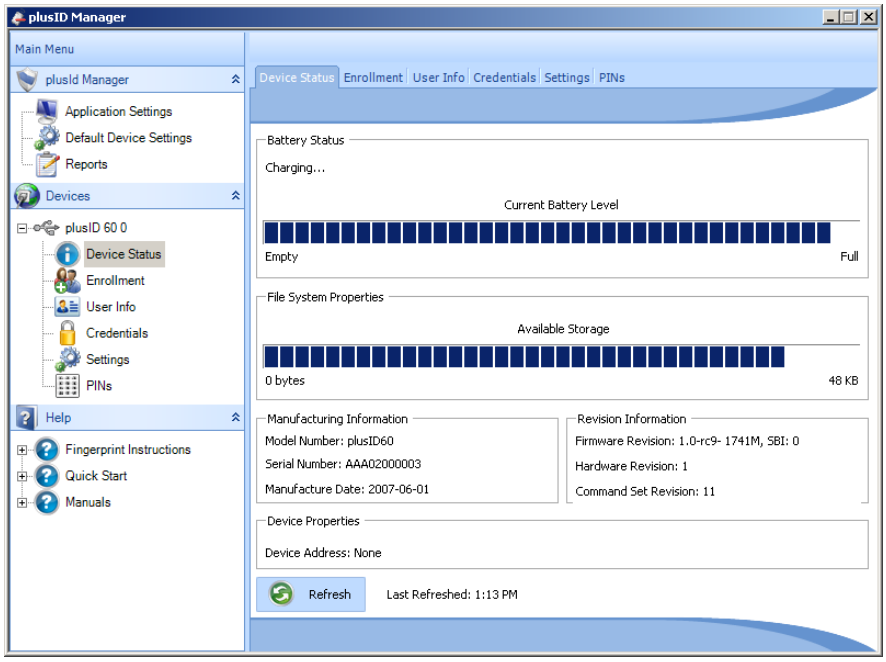


Figure 6
Device Status Screen

The “Device Status” screen (Figure 6) provides a snapshot of the technical specifics of the device that is connected, including:

Battery Status
The plusID device is powered by a rechargeable battery. The Battery Status portion of the screen indicates whether or not the device is currently being charged, and includes a progress bar to indicate the device’s current battery level. The further to the right the bar is, the fuller the battery.

Note: The device is rechargeable over USB. So whenever a plusID device is connected to the plusID Manager computer, it is being charged.

See Appendix C for battery recharging instructions.

File System Properties
File System Properties details the amount of used and available storage space on a device. Each plusID device has 48K of available space for storing fingerprint templates, access credentials, and any additional credentials added by the issuing organization (requires Privaris software development kit).

Manufacturing Information
Manufacturing Information lists the device's model number, serial number, and date of manufacture. This information is typically only needed for customer service inquiries.

Revision Information
Revision Information lists the version information of the hardware and software specific to each device.

Device Properties
Device Properties lists the plusID device's unique MAC address, which refers to a communication channel(s) within the device. This address will only display if required for the operation of the device.

Refresh Status Button
If there has been a change to any of the device specific status information, pressing the Refresh Status button will update the information in real time.

5. Enrollment

Enrollment is the key element of the plusID device issuance process. It is what makes the device work for its enrolled owner and no one else. A precise enrollment is critical for the plusID device to operate properly.

During enrollment the user's fingerprint images are captured, encoded and securely stored as a template on the plusID device. Enrollment readies the plusID for regular day-to-day use, which is called verification. Verification is simply a fingerprint swipe in which the device compares the live fingerprint presented to it with the fingerprint templates stored during enrollment to ensure that only the authorized user can operate the device.

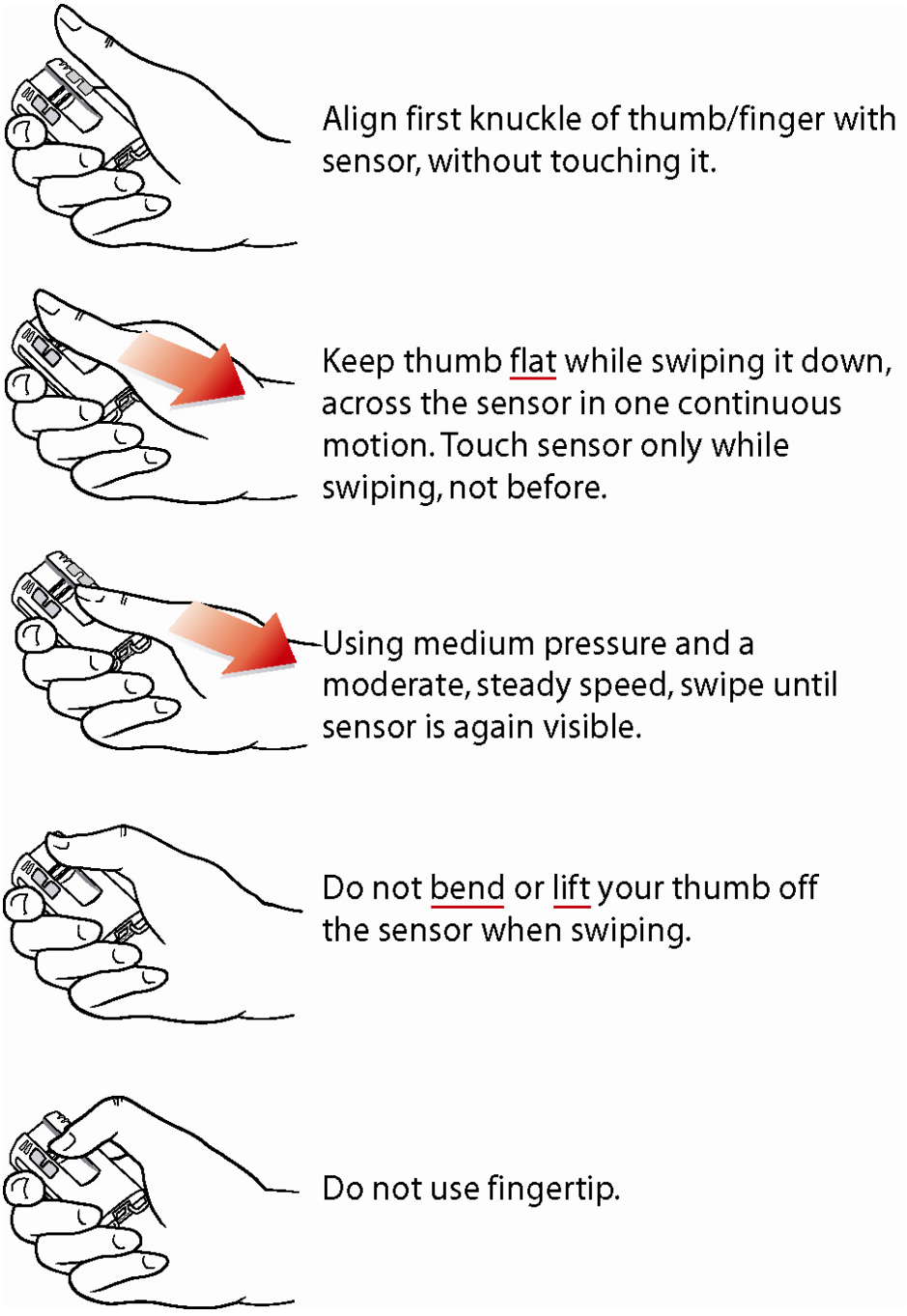
a. Enrollment Administrator Guidelines

1. Always review the "How to Swipe" instructions with each user before beginning enrollment.
2. Always enroll both thumbs to ensure that there is a backup in case of injury.
3. Always enroll the users' primary thumb first.
4. In the event a thumb is not an option, default to the user's index finger(s).
5. More than two thumbs/fingers can be enrolled in a single device, but is likely to result in slower verifications.
6. Remember that as an Enrollment Authority you can erase and re-enroll a user's fingerprint at any time.

b. **Device User Guidelines**

1. Fingers should be free of excessive dirt or grease but otherwise do not need to be washed prior to enrollment.
2. The plusID device should be held with one hand - just as it will be held during normal device use.
3. Review the “How to Swipe” instructions that follow to ensure the proper positioning of the fingerprint relative to the sensor. The central, most feature-rich portion of the fingerprint – not the fingertip – must be swiped over the device’s fingerprint sensor. This is where the fingerprint pattern is centralized and typically forms a bull's eye, U or S shape (see image below).

How to Swipe
Fingerprint Sensor Instructions
Review the instructions below with each user and let them practice swiping with their device. Not doing so will result in a poor quality enrollment and difficulty using the plusID device. (These images are also linked from the "Help" section of the plusID Manager.)



c. **Enrollment Set-Up**

1 Open the plusID Manager software application.

2 Hand the user their new plusID device.

3 Review the “How to Swipe” instructions with the user, letting them practice swiping until they can do so properly and comfortably (see section 2.b. or the Help menu within plusID Manager)

4 Insert the largest end of the mini-USB cable, packaged with the plusID device, into the computer's USB port, and the smallest end into the port at the base of the plusID.

5 For each new device the “Device Registration” screen will appear (Figure 3).

i. Enter the user's first and last name. Employee number is optional, but recommended. Employee number is any unique identifier, i.e., an official employee i.d., or social security number. *Note*: None of this user information is stored on the device. It is stored only in the plusID Manager’s database for record keeping purposes.

ii. Each device is shipped with a default Administrator PIN of 4321. Enter the default Administrator PIN as the “Current PIN.” Before entering a new PIN, see the warning below. The new Administrator PIN can be from four to eight letters, numbers and/or characters.

! *It is highly recommended that each organization select a single Administrator PIN for all plusID devices. This PIN should be selected by an Officer of the company or by Security Personnel. The Administrator PIN should be treated as a corporate secret and guarded in the same manner as other keys/passwords that grant access to valuable resources. If the Administrator PIN were ever to be compromised, issued devices would be susceptible to manipulation by outside organizations, and the security of corporate physical and logical assets would be placed at risk. There is no way to reset the Administrator PIN. For more information on the Administrator PIN, see #9 under Getting Started.*

d. **Enroll the First Thumb**

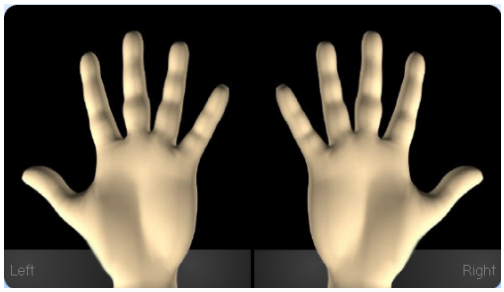
Note: Sit near the user to watch closely and ensure that they are following the Enrollment Guidelines. An enrollment cannot be stopped once begun, but can be easily erased and redone.

1. Always enroll the primary thumb first. Ask if the user is right or left handed.

! *If the plusID will be used only for computer logon, it may be advisable to enroll the primary index finger (in place of the thumb), assuming that the device will regularly be positioned flat on a desk connected to a computer, as opposed to being held and operated in-hand.*

1. Select “Enrollment” from the menu tree.
2. Select the “Enroll” button from the Enrollment screen 

3. To initiate enrollment, select the respective thumb from the on-screen hand diagram.



! *The device has no way of distinguishing which finger is swiped, so be certain that the finger selected on the screen is in fact the same finger that the user is actually applying.*

4. Convey the instructions from the on-screen prompts to the user.

   The prompts will appear above the "Enroll" button and will specify when to swipe a finger as well as provide feedback on the quality of the swipe. If the software deems a swipe "invalid," watch the user closely to ensure that they are following the "How to Swipe" instructions and coach as necessary.

! *Tell the user to swipe whenever they see a blinking green light.*

   A typical enrollment requires three to five swipes. The first few swipes of an enrollment create the fingerprint template. The last swipe is a verification swipe that confirms that the user's live print can be successfully matched to their stored fingerprint template, and is required to complete enrollment. Verification is indicated by a solid green light and should only take about a second.

! *Watch closely to ensure that the user is swiping properly. If the software deems a swipe "invalid," or if the user has difficulty verifying, review the "Troubleshooting" guidelines linked from the "Help" section of the plusID Manager, or Appendix A of this manual for Expanded Troubleshooting guidelines. Modify the user's swiping technique accordingly, and if necessary, erase the finger (see Section 5.i.) and re-enroll it, starting with enrollment step #3.*

The plusID's Light Behavior During Enrollment

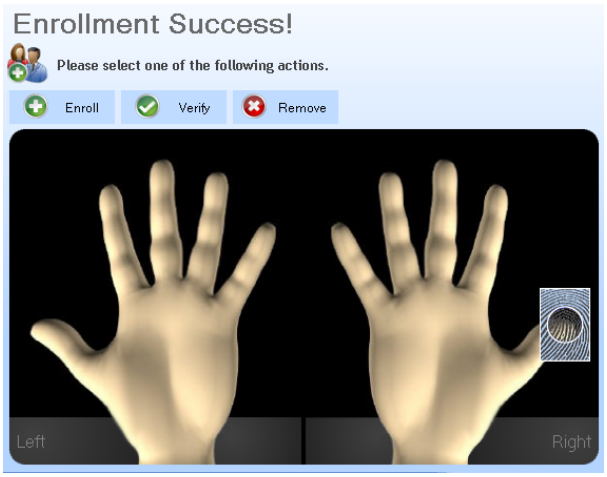
The plusID's solid blue light will remain on as long as the device is connected via USB, while the other lights correspond to the on-screen prompts.

Blinking Green	Requesting a fingerprint swipe
Solid Yellow	Sensor is processing a fingerprint swipe
Brief Solid Green	An image has been successfully captured during fingerprint template creation, or successfully matched during verification

Continuous Solid Green	A successful enrollment
Brief Solid Red, then Blinking Green	The sensor did not get sufficient information from the fingerprint to process the swipe. This often happens if the sensor is touched before a swipe is begun, as opposed to placing the finger and swiping in one continuous motion.
Continuous Solid Red	Enrollment failed. See “Troubleshooting” (Appendix A, or under “Help” in the menu tree). Modify the user's swiping technique accordingly, erase and re-enroll the finger.

5. Upon a successful enrollment the on-screen prompt, will read “Enrollment Success,” and a rectangular fingerprint image will appear atop the enrolled finger on the hand diagram.

! *If enrollment fails, see Section 5.h.*



e. **Enroll the Second Thumb**
Repeat the instructions from 5.c. and 5.d., with the user's secondary thumb.

f. **Completing Device Issuance**
With two thumbs enrolled, enrollment is complete.

To complete the plusID device issuance process, the necessary access credential(s) need to be assigned to the device to ready it for physical and/or logical (IT) access. See Section 7 (“Credentials: Using the plusID for Door Access”) to assign physical access credentials for door entry, and Section 8. (“Credentials: Using the plusID for Windows Logon”) to assign logical access credentials for computer logon.

! *If access credentials were loaded prior to enrollment, device issuance is complete. Disconnect the plusID device from the computer and hand it to the user with the USB cable and plusID Quick Start Guide that was enclosed in their device box.*

g. **Verification**

Verification (the last fingerprint swipe during enrollment) confirms a user's identity by matching their live fingerprint to their stored fingerprint template. This is how the device will be used on a daily basis for access to protected resources. Verification should only take about a second and is indicated by a solid green light.

Each user must be able to quickly and repeatedly verify. If verification was sluggish (two seconds or more), or if verification failed, see the "Troubleshooting" guidelines linked from the "Help" section of the plusID Manager, or Appendix A of this manual for Expanded Troubleshooting guidelines. After reviewing these pointers with the user, erase the finger in question and re-enroll it, starting with step #3 in Section 5.d.

! *A verification can be prompted at any time and is a quick way 1) to test the quality of an enrollment and 2) for the user to practice using their plusID device. It is recommended that after each enrollment the Enrollment Administrator prompt the user to verify two or three times in addition.*

To prompt a verification:

1. Selecting "Verify" from the Enrollment screen. 

2. Selecting an enrolled finger from the on-screen hand diagram
3. Follow the on-screen prompt. Just as during enrollment, the device will blink green to request a verification (swipe), turn solid green upon a successful verification, and solid red upon a failed verification.

h. **Failed Enrollment**

A typical enrollment requires three to five fingerprint swipes, though some fingerprints will require more. The on-screen prompts will continue to request fingerprint swipes until the device has enough data (unique features) to form a fingerprint template. If a high enough quality fingerprint template cannot be obtained, the device will signal a solid red light and the on-screen prompt will say "Enrollment Failed."

This occurs most often because the user was not following the User Guidelines (3.b. above), in particular the "How to Swipe" instructions. Carefully review the following, as necessary, in this order:

1. "How to Swipe" instructions, linked from the "Help" section of the plusID Manager
2. "Troubleshooting" guidelines, linked from the "Help" section of the plusID Manager
3. Expanded Troubleshooting Guidelines in Appendix A of this manual

Modify the user's swiping technique accordingly, erase the finger and re-enroll it.

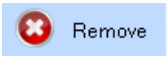
i. **Erasing a Finger/Enrollment**

This option erases the selected finger's fingerprint template from the plusID device. Only an enrolled finger can be erased.

If an Enrollment was successful but the user is having trouble verifying, or verification is sluggish (two seconds or more), it is recommended that the respective finger be erased and then re-enrolled after reviewing the "How to Swipe" and "Troubleshooting" guidelines linked from the "Help" section of the plusID Manager. For Expanded Troubleshooting, see Appendix A of this manual.

Note: The erase feature does not erase a device, only individual fingerprints stored on the device one at a time. For purposes of recycling a device for re-issue, use the device reset feature (see 6.b.iii) which erases all of the stored fingerprints at once, and restores the device to its factory default settings.

To erase a finger/enrollment:

1. Select the "Remove" button from the Enrollment screen. 

2. Select the respective finger from the on-screen hand diagram.
3. Select "Yes" to confirm erasure.

j. **Fingerprint Augmentation**

After an enrollment, the plusID device uses data from successful verifications during regular device use to enhance the quality of the originally stored fingerprint template(s), as necessary. This "learning" feature helps reduce potential false rejections and ensure positive user experiences with the device.

Any swipes/verifications that expose the sensor to more surface area or new fingerprint features, beyond what was captured during enrollment, will result in the automatic augmentation of the original fingerprint template. Up to five augmentations can occur, per fingerprint template. Augmentation

Augmentation is a "behind the scenes" feature of the plusID's fingerprint algorithm and is not indicated in the plusID Manager interface.

6. User Info

With each enrollment performed, the plusID Manager saves a record containing information on the enrolled user and their device. The "User Info" option from the menu tree displays the user portion of this record. The information displayed on the "User Info" screen (Figure 7) pertains to the owner of the connected plusID device.

Note: This information is **not** stored on the user's device. User information is stored only in the plusID Manager database for record keeping purposes and can be accessed through "Reports" on the menu tree.

Before a device is enrolled, the first and last name of the user to whom the device is being issued must be entered during device registration (see 1.a.). Selecting "User Info" from the menu tree displays this information and gives the Enrollment Administrator access to edit it as well as provide additional user specific information, such as an employee number (unique ID), a phone number, and comments. The maximum character limitations for each field are:

Employee number = 50 characters, including spaces

Contact number = 50 characters, including spaces

Comments = 8198 characters, including spaces

The first name, last name, and middle initial from this screen will always appear at the top of the Enrollment screen when it is open to indicate whose device is connected.

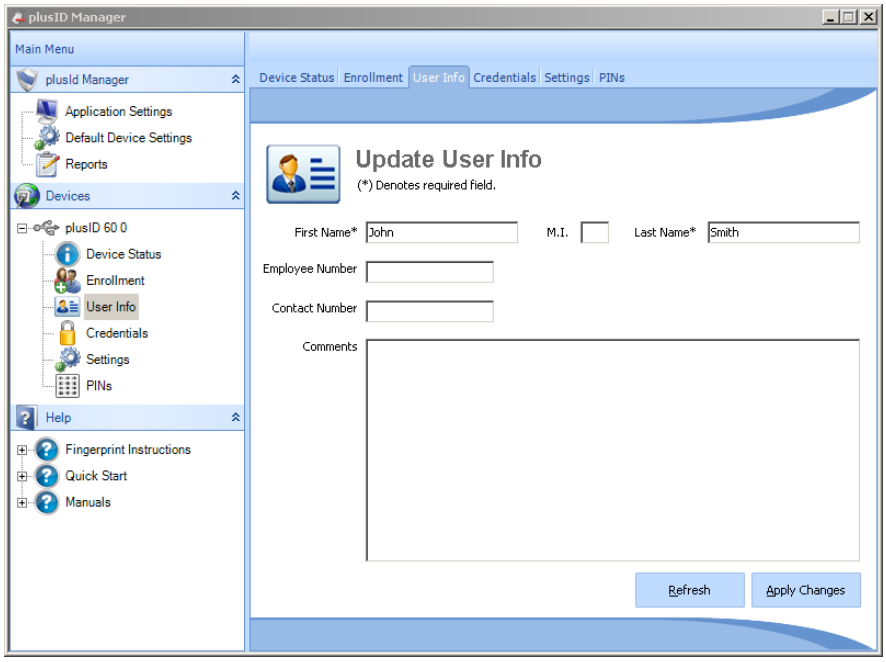


Figure 7
User Info Screen

7. Credentials: Using the plusID for Door Access

The "Credentials" option from the main menu tree (Figure 8) is used for loading physical access credentials (card formats) onto plusID devices so that the device can be used for door/facility access. Different card formats can be assigned to each of the four function buttons on the front of the plusID device.

! *This procedure requires an additional USB port, a smart card reader, and an idBank™ available from HID® or Privaris®. idBank is a smart card containing card*

formats that are securely transferred to plusID devices using the plusID Manager software.

a. **Overview**

If the plusID device will be used in place of access cards or fobs to access doors and facilities, a physical access credential, in the form of a card format, must be loaded onto the plusID device via the plusID Manager. This is done using an HID idBank™, which is a smart card containing HID or Indala prox card formats in quantities of 25, 50, 100, 200 or 300. All HID and Indala prox formats are available. Additional formats will be supported in the future.

! *Once a card format has been loaded on to a plusID device, it cannot be moved off of the device back onto an idBank.*

b. **Loading a Card Format onto a plusID from an idBank**

With the device connected via USB to the Enrollment Administrator's computer:

1. Connect a plusID device to the plusID Manager via USB
2. Register the device if it is not already
3. Connect a smart card reader to computer via USB (if not built into computer).
4. Insert idBank in smart card reader
5. Select "Credentials" from the menu tree. The Credential Management screen is displayed (Figure 8)
6. Select the "Card" tab under "Credentials Source."
7. Select the appropriate smart card reader from the drop down menu. The list of available card formats will be displayed. Previously assigned card formats are sorted to the bottom of the list, grayed out and the status is shown as "In Use."
8. "Drag" an unassigned card format from the list and "drop" it in one of the four white squares above (repeat as necessary). Each square corresponds to one of the device's four function buttons. A progress bar is displayed as the credential is generated.

! *Inform the user what doors/facilities are assigned to each of the buttons (i.e., card formats) so that they will know what buttons to use for daily access.*

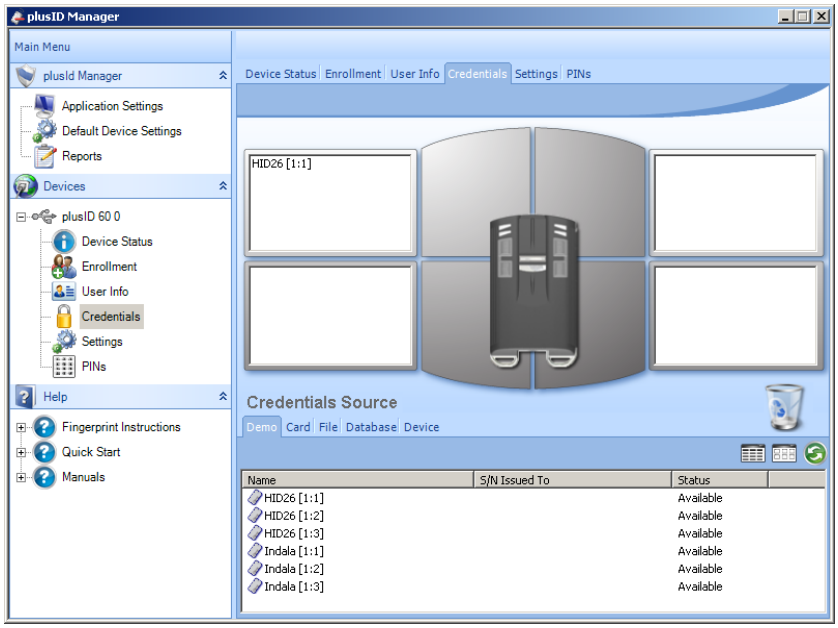


Figure 8
Credential Loading Screen

When credential generation is complete the card format will be shown in the selected location (Figure 8). Different card formats can be loaded for each of the device's four buttons for access to multiple doors and facilities. For user convenience, the same card format can be loaded onto multiple buttons, if desired.

! *If the device is enrolled, but not being used for computer logon, or if a User PIN is not required for logon, device issuance is complete. Disconnect the plusID device from the computer and hand it to the user with their USB cable, and plusID Quick Start Guide that was enclosed in their device box.*

c. **Loading a Card Format from the Database Tab**
All card formats loaded by the plusID Manager are retained in the database. A card format may be reloaded from the database onto the same device.

1. Select the Database tab under Credentials Source.
2. Select Detail view using the icon under and to the left of the recycling bin.
3. Choose a card format associated with the device serial number as shown in the center column of the list.
4. "Drag and drop" it to one of the white rectangles above associated with each of the four device buttons. A progress bar is displayed as the credential is generated.
5. When credential generation is complete the card format will be shown in the selected location.

d. **Loading a Card Format from the Device Tab**
Card formats moved from the device to the recycling bin are retained and can be viewed under the Device tab. A card format that shows an "unassigned" status is still on the device and may be reassigned to any available button.

1. Select the Device tab under Credentials Source.
2. Select Detail view using the icon under and to the left of the recycling bin.
3. Choose a card format with an "unassigned" status
4. "Drag and drop" it to one of the white rectangles above associated with each of the four device buttons. A progress bar is displayed as the credential is generated.
5. When credential generation is complete the card format will be shown in the selected location.

e. **Loading a Card Format from the File Tab**
This function is not implemented.

f. **Removing a Card Format**
To remove a card format, or physical access credential, from a plusID device, "drag" it from one of the white rectangles associated with the device's four buttons and "drop" it into the waste basket / recycle bin located in the middle, right portion of the screen. Removed credentials become "unassigned," and are visible from the "Devices" tab. To re-assign the credential, simply drag and drop it to the desired button above.

g. **Demonstrating Physical Access Functionality**
The plusID Manager software enables you to load demonstration card formats onto a plusID device to demonstrate interaction with a door reader and simulate physical access.

The demonstration card formats can be added to your existing physical access control system (PACS), or used with a battery powered HID demonstration reader included the plusID evaluation kit from Privaris.

In normal use, card formats are loaded from an idBank (see page 7), which is a special smart card that can be purchased from Privaris or an authorized partner, such as HID. The smart card contains card formats that are securely transferred to plusID devices using the plusID Manager.

To load demonstration card formats onto a plusID:

1. select "Credentials" from the main menu of the plusID Managers
2. select the "Demo" tab from the middle of the Credentials screen
3. the available card formats will appear at the bottom of the screen

4. select a card format and “drag and drop” it into one of the four white squares at the top of the screen that correspond to each of the device’s four function buttons. Repeat as necessary.

! *Only HID demo codes will work with battery powered HID demonstration readers*

The demonstration card formats are reusable and can be removed (dragged from a button to the on-screen trash can) and re-loaded as many times as desired.

8. Credentials: Using the plusID for Windows® Computer Logon*

If the plusID device will be used in place of passwords for computer logon in a Microsoft domain environment, follow the instructions below.

With the device connected via USB to the plusID Manager application:

1. Select “Settings” from the menu tree. (See plusID Manager Operator’s Manual for the distinction between “Settings” and “Default Device Settings” menu options.)
2. Under “User Logon Settings,” select the desired authentication mode for logon: PIN + Biometric or Biometric Only, and press “Apply Changes.”
3. If Biometric Only is chosen, instruct the user to enter “1234” when prompted for a PIN during logon. Skip steps 4 – 9 below. Their plusID device is now ready to be used for logon.
4. If PIN + Biometric is chosen, select “PINs” from the menu tree.
5. Select the “User” tab. This screen sets the User PIN required for logon and stores it on the plusID device.
6. Enter the current (default) User PIN: 1234.

! *This is different from the Administrator PIN that was entered when the device was registered.*

7. Ask the user to select a new User PIN (from four to eight letters, numbers and/or characters).
8. Allow the user access to the keyboard to privately enter their User PIN.
9. Press “Change PIN” for the new User PIN to take effect.

* Logon requires Microsoft Windows 2000 Server or later configured as a domain controller and running Microsoft Certificate Services, and the Privaris minidriver (included with Privaris plusID Manager software). See Appendix E for a full description of system requirements.

! *If the device is going to be used for logical/IT access only, and it has already been enrolled, disconnect the plusID device from the computer, hand it to the user along with the USB cable and plusID Quick Start Guide that was enclosed in the device box. Device issuance is complete. If the device is also going to be used for physical (door) access, see Section 7.*

9. Settings

The "Settings" screen includes three tabs across the top for access to Device Settings, Device Utilities, and Reset Options.

a. Device Settings

The first tab of the "Settings" screen, "Device Settings," (Figure 9) lists the settings that will be applied to the plusID device connected to the plusID Manager software. Unless changed, these settings will be the same as the "Default Device Settings." Changing these settings override the Default Device Settings *only* for the device that is connected.

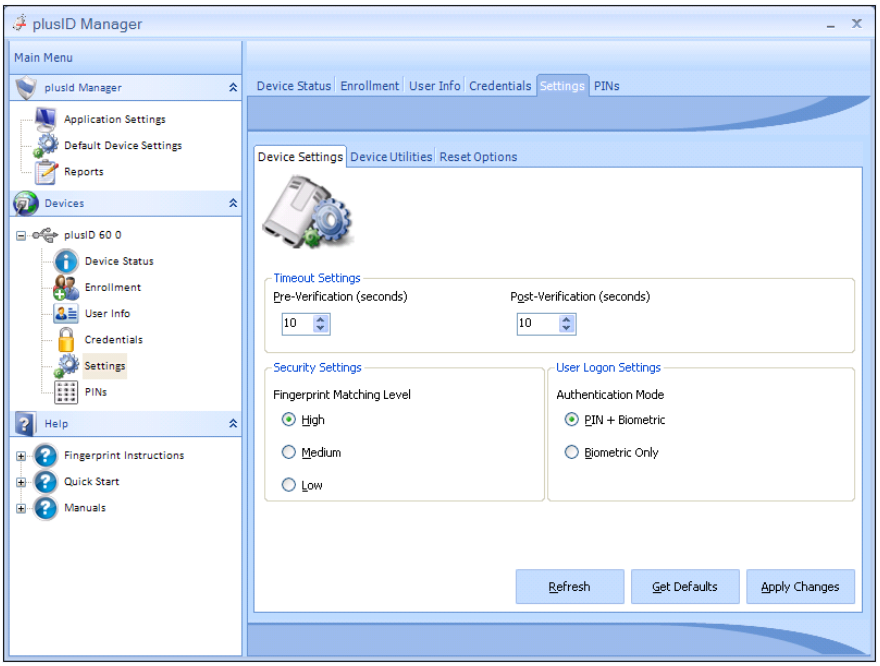


Figure 9
Device Settings Screen

Note: The default settings for all enrolled devices can be changed at any time for by selecting the "Default Device Settings" option under "plusID Manager" from the main menu tree.

To change the settings for an individual plusID device, select "Settings" from the main menu tree, select the new settings, then select "Apply Changes" for the settings to take effect.

The "Get Defaults" button resets the settings to their original values (per the "Default Device Settings" values). To reinstate the default setting values on the device, select "Get Defaults" then select "Apply Changes."

The "Refresh" button cancels changes made prior to the "Apply Changes" being selected.

Following are descriptions of the individual setting options.

i. **Timeout Settings**

Pre-Verification Period
The Pre-Verification Period timeout setting determines 1) how long the device will attempt to match a fingerprint before failing a verification attempt and 2) how long the device will wait for a verification (fingerprint swipe) before powering off.

The timeout can be set from 5 to 255 seconds. The default setting is 10 seconds.

Note: This setting only applies to verifications performed after enrollment, during normal device usage, and when the device is not connected to a computer.

Post-Verification Period
The Post-Verification Period timeout setting determines how long the device's credentials will remain active after a successful verification. The device is active for as long as its green light is on, post-verification.

The timeout can be set from 5 to 255 seconds. The default setting is 10 seconds.

! *The longer the post-verification timeout setting, the greater the demand on the device's battery, which may reduce the average number of verifications available per charge.*

ii. **Security Settings**

Fingerprint Matching Level
The plusID device has three configurable security settings: High, Medium, and Low. Each setting corresponds to an associated fingerprint matching level, or False Acceptance Rate (FAR).

Every biometric system has an associated FAR. An FAR is the percentage of unauthorized users that the device will incorrectly match to a valid user's stored fingerprint template. Below are the FARs that can be set in the plusID device:

Security Setting	False Acceptance Rate (FAR)
Low (Less Strict)	1 in 1,000 (.1%)
Medium (Default)	1 in 10,000 (.01%)
High (More Strict)	1 in 100,000 (.001%)

The low security setting may match (verify) a fingerprint faster than the high security setting, but will allow a higher number of false acceptances, and vice versa.

The recommended, and default security setting for the plusID device is high.

iii. **User Logon Settings**

Authentication Mode
The Authentication Mode selection sets the security level required when using the plusID device for computer logon (post-enrollment). If the device is not being used for logon, this setting can be left at its default value.

There are two options:

PIN + Biometric
requires a personal identification number (PIN) and a biometric verification (using the plusID device). *Note*: If this option is selected, a User PIN must be assigned (see Section 8. for more information).

Biometric Only
this option still requires that a placeholder personal identification number (PIN) be entered, in addition to a biometric verification, but any four random numbers/letters/characters can be entered, as opposed to requiring the same user-defined PIN each time (as above).

The first option is a three-factor security solution: something the user has (the plusID device), something they know (a PIN) and something they are (their fingerprint).

The second option is a two-factor security solution: something the user has (the plusID device) and something they are (their fingerprint).

The default value is the highest security level, PIN + Biometric.

b. **Device Utilities**
The second tab of the "Settings" screen, "Device Utilities," (Figure 10) enables the updating of a plusID device as well as the extraction of the device's log file and security certificate. The functions on the Device Utilities tab apply only to the plusID device that is connected to the plusID Manager software.

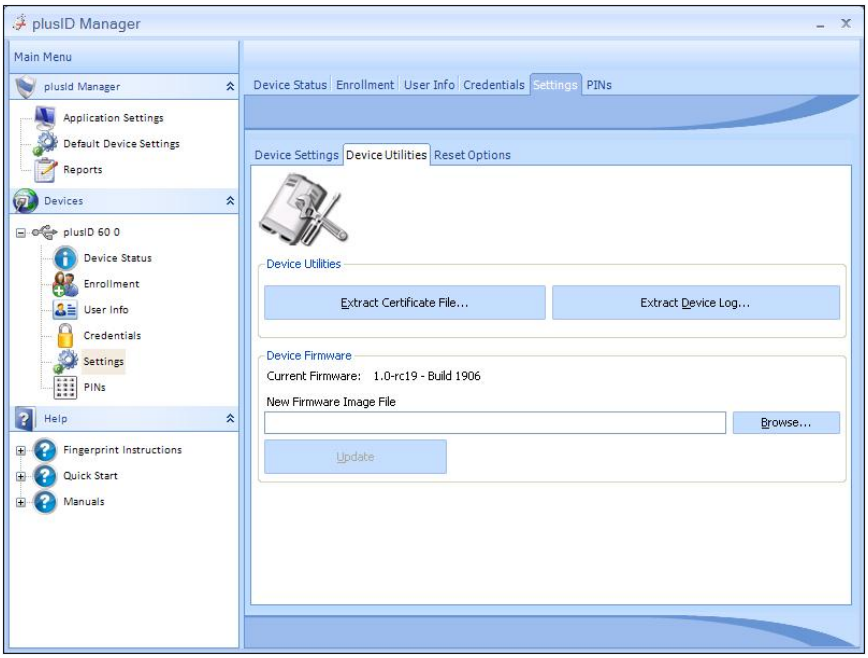


Figure 10
Device Utilities Screen

Following are descriptions of the individual functions on the Device Utilities screen:

i. **Extract Certificate File**
Each plusID device contains a unique security certificate. The certificate is a unique identifier for the device. In the event a security operation needs to be performed in which the device needs to be uniquely identified, the certificate can be extracted (as a file), saved for transfer by selecting the “Extract Certificate File” button.

ii. **Extract Device Log**
Each plusID device maintains a running log of device activity that documents the internal workings of the device. This log file can be extracted by selecting “Extract Device Log” and specifying where to save the file.

The only time the log would need to be extracted was if it was requested by Customer Service in order to diagnose a problem. The device log is made up of engineering code that is only decipherable by engineers.

iii. **Device Firmware**
Firmware is the software that is embedded within the plusID device. The device firmware function enables the updating of firmware on a plusID device. This function is only necessary if you have received updated device firmware from Privaris.

! *A firmware upgrade does not erase or reset the device and has no impact on any of the information that is stored on the device (i.e., device settings, fingerprint templates, Administrator PIN, credentials, etc.)*

If in receipt of updated firmware, with a device connected to the plusID Manager computer:

1. Download and save the firmware file onto the computer which has the plusID Manager installed. When saving, do not change the name or file extension of the file.
2. Click on the "Browse" button to the right of the "New Firmware Image File" field.
3. Browse to and select the saved firmware file.
4. With the path and file name for the firmware file is inserted, click the "Update" button.
5. The new firmware will be downloaded onto the connected device. During the download, the device's lights will cycle green, red, yellow and blue.
6. When the upgrade is complete a confirmation message will appear.

! *Do not unplug the device from the computer until the cycling lights stop and a device upgrade confirmation message is received.*

c. **Device Reset**

The third tab of the "Settings" screen, "Device Reset," (Figure 11) enables all or portions of the information stored on the device to be erased and reset. The options on the Device Reset screen apply only to the plusID device that is presently connected to the plusID Manager software.

Check the boxes next to the appropriate reset option(s) and then select the "Apply Reset" button to implement the changes. All four lights on the device will flash concurrently while the device reboots to implement the changes.

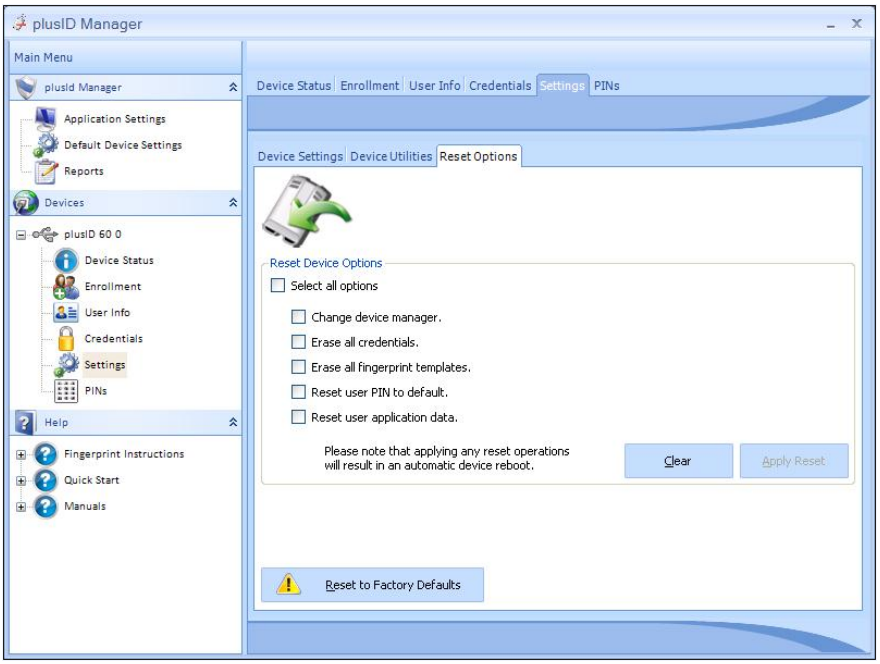


Figure 11
Device Reset Options Tab

The reset options are:

Change Device Manager
Each device can have only one administrative authority, or device manager. The "Change Device Manager" option disassociates the device with its original administrative authority (i.e., workstation running the plusID Manager software) and enables it to be re-registered and administered on another, or the same, workstation running the plusID Manager software.

Selecting this option will require the device to be re-registered.

! *Once the "Change Device Manager" option is implemented, and until the device is re-registered on another workstation within the same organization, the device is susceptible to being administered and manipulated by any other organization with plusID Manager software. However, once it is re-registered, it cannot be updated on any another computer running the plusID Manager software (even within the same organization).*

Erase All Credentials
This option erases all credential files stored on the device, which includes physical access card formats used for entering doors and facilities, and any logical access credentials required for computer logon.

Erase All Fingerprint Templates
This option erases all fingerprint templates that were enrolled in the device.

Reset User PIN to Default

This option changes the Personal Identification Number (PIN) that the device's user defined, and is required in addition to the plusID device for logging onto their computer, and reverts it back to the system default of 1234.

Reset User Application Data (different from erase?)
This option erases all third party software information that has been stored on the device, for example the minidriver that may be resident to enable computer logon. This command does not erase user data from applications that are not registered with the plusID Manager.

Reset to Factory Defaults (button in bottom left of screen)
Selecting the "Reset to Factory Defaults" option will destroy all access credentials, fingerprint templates, and reset both PINS (Administrative and User) and revert the device to its original factory–default state. This is the only function that eliminates all user data stored on the device.

This operation will erase all access credentials from the device. If the credentials exist in the plusID Manager's database, they can be reloaded to the same device. If there is no backup, the credential is permanently lost.

10. PINs

The PIN Management Screen enables the Administrator and User PIN to be changed and for the User PIN (only) to be reset.

a. Changing the Administrator PIN

The Administrator PIN can be changed, but it cannot be reset if lost or forgotten.

! *Once set, it strongly recommended that the Administrator PIN not be changed without a compelling reason. Creation of more than one PIN will result in a population of devices with different PINs and significantly increases the odds of being locked out of a device(s). There is no way to determine what PIN is on a device other than by trial and error (with a limited number of attempts).*

To change the Administrator PIN:

1. Select "PINs" from the main menu tree. The PIN Management screen will be displayed.
2. Select the "Administrator" tab at the top of the dialog box
3. Enter the default Administrator PIN in the Current PIN field: 4321.

   ! *The factory default Administrator PIN for all new plusID devices is 4321*
4. Enter the organization's new Administrator PIN twice, in the indicated fields. The PIN can be from four to eight letters, numbers and/or characters in length.
5. Select "Change PIN."

Changing the PIN overwrites the previous Administrator PIN. This new PIN will now be downloaded onto all future enrolled devices. The computer on which the Administrator PIN was changed will no longer be able to communicate with previously enrolled devices (with the previous Administrator PIN).

b. **User PIN**

The User PIN is used for Windows login* or other smart card functions, post-enrollment. Each plusID device is shipped with a factory default User PIN (separate from the Administrator PIN). If the device is not to be used for smart card functions it is not necessary to change the User PIN.

For more information on using the plusID device for computer logon, see Section 8, "Credentials: Using the plusID for Windows Computer Logon."

* Logon requires Microsoft Windows 2000 Server or later configured as a domain controller and running Microsoft Certificate Services, and the Privaris minidriver (included with Privaris plusID Manager software). See Appendix E for a full description of system requirements.

c. **Changing the User PIN**

To change the User PIN on the device from the factory default:

1. Select "PINs" from the main menu tree. The PIN Management screen will be displayed (Figure 12)
2. Select the "User" tab at the top of the dialog box
3. Enter the default User PIN in the Current PIN field: 1234

! *The factory default User PIN for all new plusID devices is 1234*

4. Ask the user to select a new User PIN, from four (4) to eight (8) letters, numbers and/or characters.
5. Allow the user access to the keyboard to privately enter their User PIN.
6. Select "Change PIN."

! *For security purposes the Enrollment Administrator should not know the User PIN. Should the user forget their PIN, the Enrollment Authority can reset it to a default value without having the original User PIN.*

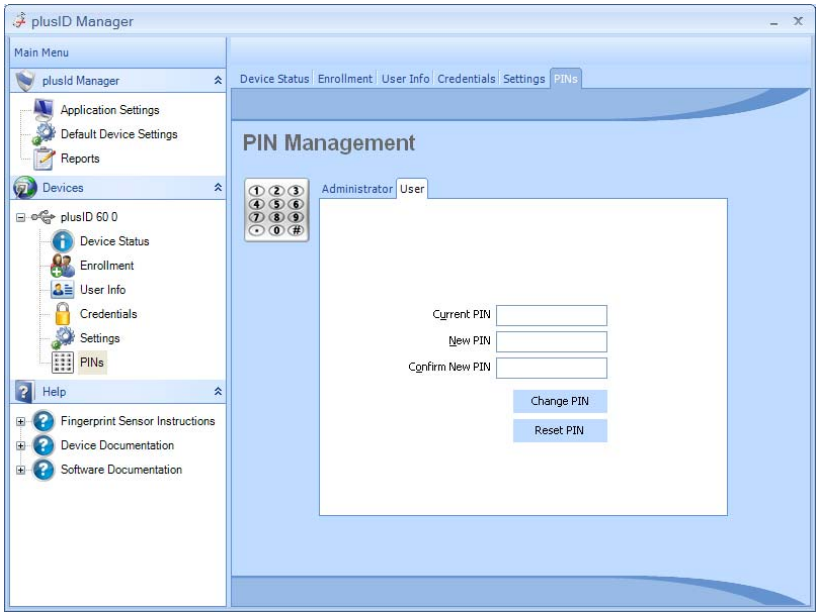


Figure 12
User PIN Screen

d. **Resetting the User PIN**

Unlike the Administrative PIN on the device, the User PIN can be reset to its factory default value in the event a user forgets their logon/User PIN. To reset the User PIN:

1. Select “PINs” from the main menu tree
2. Select the ‘User” tab
3. Select “Reset PIN."
4. Enter the Administrator PIN
5. The User PIN will be reset to its original default value: 1234.

Section IV: HELP

The “Help” branch of the main menu tree contains documentation for quick reference in lieu of referring to hard copies. There are three main categories of documentation. Click the “plus” arrow next to each category to see the expanded list of files contained therein.

The Help categories and documentation files include:

Fingerprint Sensor Instructions
- “How to Swipe” sensor instruction pictorial
- Troubleshooting guidelines (abbreviated)

Device Documentation
- plusID60 Quick Start Guide for device usage

Software Documentation
- plusID Manager software Quick Start Guide for device issuance
- plusID Manager Operators Manual

Viewing Help Documentation

All of the documentation is in PDF format and can be viewed simply by double-clicking the file name. The file will open within the application window.

To view a file in an external window, full size, click the “Launch in External Browser” text link at the bottom of the application window (Figure 1).

Printing Help Documentation

1. Double-click on the file name to open the document in the application window.
2. Click the “Launch in External Browser” text link at the bottom of the application window (Figure 1).
3. Print the document from the PDF viewer application used to open the file

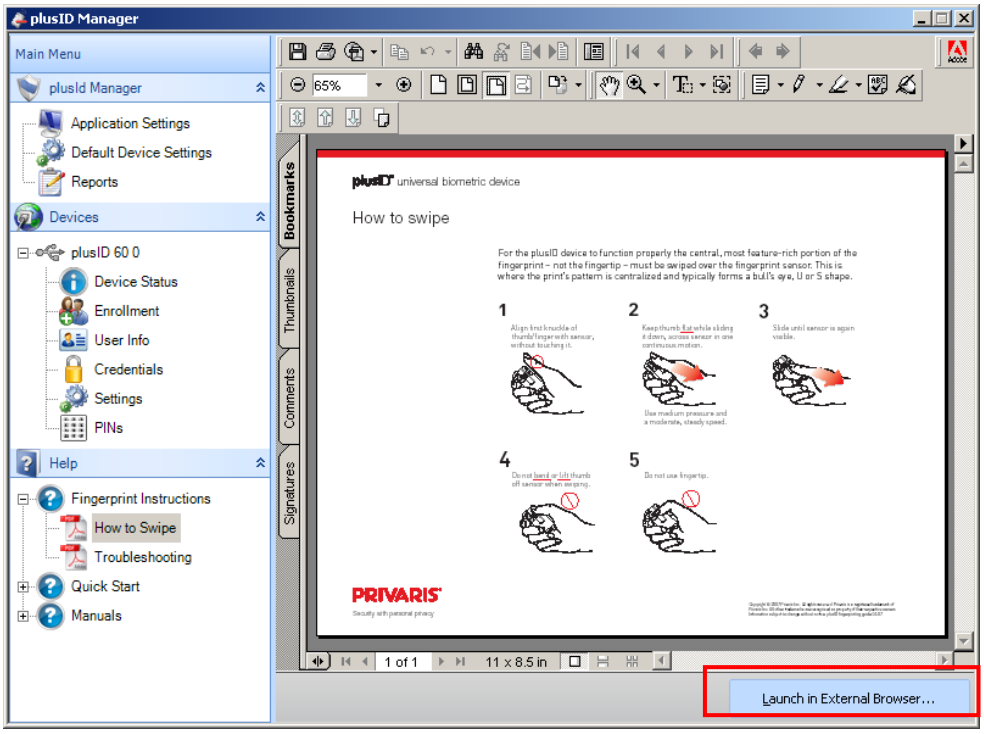


Figure 1
External Browser Button

Appendix A

Troubleshooting - Expanded

If any of the following three bullet points apply, refer to the troubleshooting levels below, starting with Level 1 and progressing through Level 5, as necessary, and erasing and re- enrolling fingers as necessary.

- Verification or enrollment failed
- Verifications are sluggish (two seconds or more)
- The user cannot could not quickly and repeatedly verify

Troubleshooting Level 1

- Make sure that the user is holding the device with only one hand, or as it was held during enrollment
- Wipe-off any excess dirt or grease from finger using a tissue or article of clothing

Troubleshooting Level 2

Review the following list of common swipe sensor errors and correct the user's behavior(s) accordingly.

Common Errors

- Accidentally touching the sensor before beginning to swipe

  Do not place/rest finger on sensor *before* swiping, it triggers the device's red light. Place finger on sensor and swipe in one continuous motion.

- Bending the finger during a swipe

  Always keep thumb flat and level with the device while swiping. Even a slightly bent finger lifts the central, most feature-rich portion of the fingerprint off of the sensor and exposes the fingertip (the least feature-rich portion of the print).

- Not following through

  Do not stop swiping until the fingerprint sensor is clearly visible above the thumb.

- Pressing too hard

  Do not squeeze the device. Use medium pressure. On a scale of 1 to 5, with 1 being very light and 5 being hard, pressure should equal about a 3.

- Not pressing hard enough

  Lightly dragging thumb over the sensor is not sufficient for the sensor to see the print. The finger must make solid contact, which requires medium pressure. On a scale of 1 to 5, with 1 being very light and 5 being hard, pressure should equal about a 3.

- Starting a swipe too high or too low

  With thumb hovering over top the sensor, align the first knuckle with the sensor as the starting point for swiping. This exposes only the central and most feature-rich portion of the fingerprint to the sensor during a swipe.

- Swiping too fast or too slow

  Use a moderate, steady speed. Swiping too fast or too slow prevents the sensor from collecting the necessary data for processing.

- Keep thumb level while swiping, do not tilt or rock thumb to the left or right.

Troubleshooting Level 3

Approximately 10% of all users have a fingerprint that is not centrally located. So the area that is swiped over the sensor is not very feature-rich and results in a low quality fingerprint template:

- Examine the user's fingerprint in bright light to determine if its pattern (typically a bull's eye, U shape, or S shape) is off-center and closer to the left or right side of their finger.

- If their print is off-center, coach the user to roll their finger to the left or right accordingly when swiping such that the main pattern of their fingerprint is fully exposed to the sensor. They will always have to use the same swiping technique (during enrollment and day-to-day device use).

Troubleshooting Level 4

If enrollment of the thumbs is still failing or verification is sluggish, try enrolling other fingers, starting with the primary index finger. If index fingers cannot be enrolled, attempt to enroll any other finger, with the goal of having any two fingers enrolled, one as a primary and one as a back-up.

The device is designed for thumbs so that is can be operated with one hand, but any finger can technically be enrolled.

Troubleshooting Level 5

Approximately 1 % of the population is unable to use fingerprint biometric technologies. If enrollment and verification is failing for all fingers after trying Troubleshooting steps 1 - 5, then the user should be issued a non-biometric means for access.

Appendix B
Overview of plusID Device Light Behavior

The plusID device has four indicator lights: green (top left), yellow (bottom left), red (top right), and blue (bottom right).

Green, Yellow, Red and Blue…appear all at once for an instant.
The device is powering on.

Green, Yellow, Red and Blue…blink four times
The device is powering off.

Green, Yellow, Red and Blue….then solid red and device powers off
Indicates a non-enrolled device. If the device is enrolled, it indicates a function button that has not been programmed with an access credential.

Blinking Green
The device is requesting a verification (fingerprint swipe).

Solid Yellow
The fingerprint sensor is processing a verification (fingerprint swipe).

Solid Green
Any successful fingerprint operation. During verification, solid green indicates a successful fingerprint match. During enrollment, solid green indicates a completed enrollment.

Solid Red
A failed fingerprint operation or a dead battery. During verification, solid red indicates that the device cannot match the live fingerprint placed on the sensor with the authorized users' stored fingerprint template. During enrollment, solid red indicates that the device was not able to capture enough data to successfully complete enrollment.

A solid red light after powering on the device, followed by the device automatically shutting off, indicates that the battery has been depleted and needs recharged immediately.

Brief solid red…then blinking Green
During enrollment, the sensor did not get sufficient information from the fingerprint to process the swipe. This often happens if the sensor is touched before a swipe is begun, as opposed to placing the finger and swiping in one continuous motion. When the device blinks green, try again.

Blinking Yellow
When disconnected from a computer, blinking yellow indicates a low battery (below 15%). The device needs recharged. When connected to a computer, blinking yellow indicates that a device with a low battery (below 15%) is being recharged. The blinking yellow will turn off when the battery is fully charged.

Blinking Red
Battery level is critically low (below 8%). Recharge device immediately.

Blinking Blue
Indicates device is connected via USB to a power source other than a computer (a wall or car outlet). If connected to a computer, a brief blinking blue light indicates device is attempting to establish a connection. A continuously blinking blue light when connected to a computer indicates a USB driver problem.

Solid Blue
Indicates that device has successfully established a connection to a computer via USB. The blue light will stay on as long as the device is connected.

Cycling Green, Red, Yellow, and Blue
The device's software is being upgraded. Wait until the cycling stops before turning off or unplugging the device from your computer.

Appendix C
plusID Battery Recharge Instructions

The plusID device is powered by a rechargeable battery. A single battery charge is good for approximately 1,000 uses/verifications.

How to Charge

The battery is rechargeable using any mini-USB cable. A mini-USB cable is included with each plusID device for charging via a computer (a PC with a USB port is required). Insert the smallest end of the USB cable into the base of the plusID device and the largest end into a computer's USB port. The device will begin charging as soon as it is connected. Connecting to a computer's USB port is the preferred method of charging.

! *A high power USB port is required for charging. Some hub and keyboard USB ports are incapable of charging plusID devices.*

plusID can also be charged with many (but not all) wall chargers and car chargers that provide a mini-USB connector output. For assurance that a charger will effectively and safely charge your plusID device, it is strongly recommended that you use a Privaris approved wall outlet or car charger.

How Long to Charge

If the device's yellow or red light is blinking (less than 15% or 8% charge, respectively) a recharge of approximately 90 minutes is required to completely recharge the battery. In either case, the yellow light will continue to blink while the device is charging, and will turn off to indicate a full charge.

If the battery is too low for the device to function properly, it may simply not power on, or it may turn on, display a solid red light and then immediately power off. In this state, a recharge of two hours or more may be required and the device may not exhibit any signs of life for the first 20 – 30 minutes of charging.

Note: A dead battery has no affect on the data that is stored on the plusID device

Appendix D
plusID Button Operation

The plusID has four function buttons on the face of the device that during enrollment can be programmed with physical access credentials (card formats) for various doors and facilities.

Power On

Press any button that is programmed with an access credential. All four lights will appear for an instant and then blink green to request a verification (fingerprint swipe). If a solid red light appears instead of a blinking green light, the button does not have an associated access credential.

Restart

With the device powered on, pressing any other button with an access credential will restart the device.

Power Off

Press the same button used to turn on the device, or any button without an access credential. All four lights will blink four times as the device powers off. The device will turn off automatically after a pre-determined number of seconds (as configured under “Default Device Settings” in the plusID Manager).

Appendix E
Using plusID Devices for Logon in a Microsoft® Domain Environment

Introduction

plusID biometric devices can be used to log users onto a domain, via two or three-factor authentication. The plusID device is ISO 7816 Part 3 smart card compliant, and as such enumerates itself to a computer exactly like a smart card, allowing for rapid enterprise integration of plusID devices across Microsoft® systems that support smart cards.

System requirements

The following are the smart card related system requirements for deploying Privaris plusID biometric devices into a Microsoft® environment for user authentication/logon:

1. **Microsoft Windows domain environment**

   Microsoft Windows 2000 Server, and later, natively support smart card authentication as a means of logging users onto a domain environment. In a domain environment, users and their access permissions are stored and managed in a central location, referred to as the Active Directory.

   Once a server is configured to act as a domain controller, smart card authentication via plusID biometric devices is automatically enabled on all client machines that are a member of the domain. For details on server configuration, see “Additional Information” below.

2. **Microsoft certificate services**

   Smart card authentication relies on the public key infrastructure (PKI) to authenticate users to the domain. The Microsoft Certificate Services are the server component that provides the infrastructure to support PKI and is responsible for issuing credentials (certificates) that can be used for a variety of purposes, including secure email and user authentication.

   In security-conscious environments, these credentials are stored on a secure device such as the Privaris plusID so that they may not be tampered with or used without authorization. The Microsoft Certificate Services include a web-based interface through which an administrator can generate credentials for a user and securely store them on the user’s plusID. For details on downloading certificates, see “Additional Information” below.

3. **USB port**

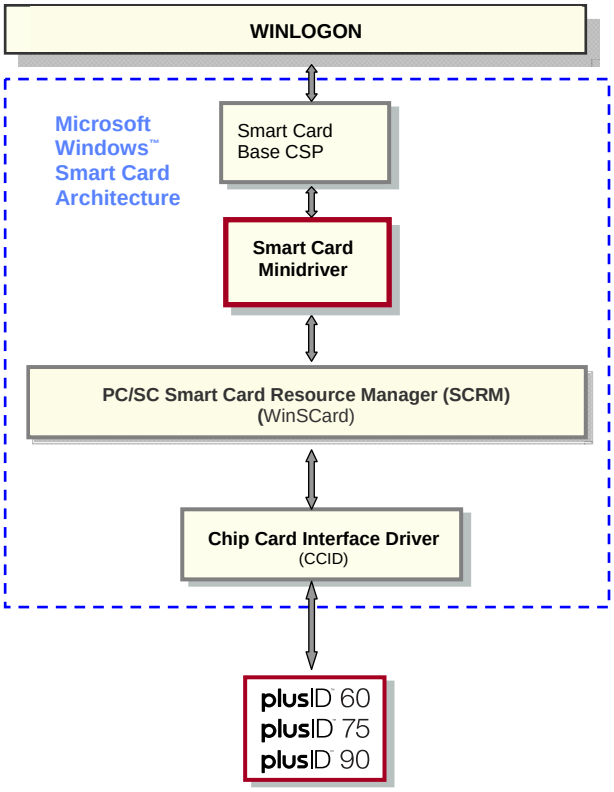
   The plusID device connects to the client machine using the Universal Serial Bus (USB). Each client machine must have at least one USB port available in order to connect to the device. The plusID device works with both high-power and low-power USB ports, though a high-power port is recommended in order to recharge the plusID’s internal battery.

4. Device Driver Software

Client machines must be configured before they are able to make use of a plusID. This includes the installation of device driver software, which consists of a CCID driver and a plusID device minidriver. The CCID driver is a standard driver provided by Microsoft for working with smart card devices such as the plusID and can be obtained via Windows Update when the plusID is first connected to the client. The device minidriver is a small software library provided by Privaris that allows Windows to interact with the plusID. The minidriver is included on the same CD-ROM as “plusID Manager” (the device enrollment and configuration software) and must be installed on each client machine.

How plusID Interfaces with Microsoft’s Smart Card Architecture for Logon

Blocks in red supplied by Privaris. Yellow = Microsoft software White = hardware



Additional information

Microsoft’s “Smart Card Deployment Cookbook” is an excellent resource covering all aspects of smart card deployment, from general information to detailed installation and configuration information. It can be accessed online at:

http://www.microsoft.com/technet/security/guidance/identitymanagement/smrtcdcb/default.mspx.

Appendix F
Licensing Agreement

READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT (“AGREEMENT”) CAREFULLY BEFORE SELECTING THE “I ACCEPT” BUTTON BELOW. THE SOFTWARE APPLICATIONS AND THE ACCOMPANYING USER DOCUMENTATION CONTAINED ON THIS MEDIA ARE COPYRIGHTED AND ARE LICENSED (NOT SOLD) TO YOU IN ACCORDANCE WITH THE TERMS OF THIS AGREEMENT. BY SELECTING THE “I ACCEPT” BUTTON BELOW, YOU MANIFEST YOUR ASSENT TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT ASSENT TO BE BOUND BY THE TERMS OF THIS AGREEMENT, THEN YOU MUST SELECT THE “I DO NOT ACCEPT” BUTTON BELOW AND PROMPTLY RETURN THIS MEDIA, IN UNALTERED FORM, AND YOU WILL RECEIVE A REFUND OF YOUR MONEY.

1. Generally. This Agreement represents the entire agreement between you, the end user (either in your individual capacity or as an authorized agent of an otherwise legally-recognized organization), and Privaris, Inc. (“Licensor”) relating to the software that is made available to you on this media by Licensor and intended for installation on certain hardware product(s) (“Hardware”) sold to you by Licensor or its authorized resellers and/or authorized licensees, as well as all documentation related thereto (collectively, the “Software”). This Agreement supersedes any prior proposal, representation, or understanding between you and Licensor related to the Software. This is a legally-binding agreement and governs the conditions under which you and/or your organization may use the Software.

2. Term. This Agreement is effective on your selecting the “I Accept” button below and shall continue until terminated as set forth in this Agreement. You may terminate this Agreement at any time by uninstalling the Software and returning the Software and all copies of the Software to Licensor. Licensor may terminate this Agreement on the breach by you of any term of this Agreement, including without limitation your failure to pay any applicable fees described in this Agreement. On any such termination, you shall uninstall the Software and return to Licensor the Software and all copies of the Software.

3. Grant of Licenses. Licensor grants you the personal, nontransferable, nonsublicensable and nonexclusive right and license to install and execute the Software (in its executable, objectcode form only) on the Hardware for the sole purpose of serving your personal needs or the internal needs of your business. You shall not assign, sublicense, transfer, pledge, lease, rent, or share your rights under this Agreement, whether by contract, operation or law or otherwise. Any use, copying, or distribution of the Software not expressly authorized by this Agreement shall automatically terminate your right and license hereunder. This grant shall be limited to use of the Software with the Hardware in accordance with the terms of this Agreement.

4. Trade Secret Protection. The Software contains substantial trade secrets of Licensor, and you shall employ reasonable security precautions to maintain the confidentiality of such trade secrets. You shall not "unlock," decompile, or reverse-assemble the binary or object code portions or versions of the Software, as the terms are generally used in the computer industry.

5. Fees. The fees for the use of the Software in accordance with this Agreement consist of the periodic license fees that are based on the number of devices purchased by you as such periodic license fees may be modified from time to time by Licensor. The dollar amount of such fees and the terms of payment are specified in the product invoice separately furnished to you. You shall pay such fees to Licensor in accordance with the terms of such product invoice.

6. Limited Warranty. Licensor warrants that the Software will, for a period of one (1) year following its delivery to you, be in good working order and will conform in all material respects to Licensor's published specifications. Licensor does not warrant that the operation of the Software will be uninterrupted or error-free, or that the functionality of the Software will meet your individualized requirements. The foregoing warranty does not cover repair for damages, malfunctions, or service

failures caused by (1) actions of any non-Licensor personnel, your failure to follow Licensor's installation, operation, or maintenance instructions, (3) attachment to or incorporation in the Software of non-Licensor products not supported or otherwise authorized by Licensor, or (4) or any factor beyond Licensor's control, including fire, explosion, lightning, pest damage, power surges or failures, strikes or labor disputes, water, acts of God, the elements, war, terrorism, civil disturbances, acts of civil or military authorities or the public enemy, transportation facilities, fuel or energy shortages, or acts or omissions of communications carriers.

EXCEPT FOR THE WARRANTIES SET FORTH IN THIS SECTION 6, THE SOFTWARE IS LICENSED "AS IS," AND LICENSOR DISCLAIMS ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, OR INTERFERENCE WITH YOUR ENJOYMENT OF THE SOFTWARE OR OF NON-INFRINGEMENT. YOUR SOLE REMEDY AGAINST LICENSOR, ITS AFFILIATES, SUBCONTRACTORS, AND REPRESENTATIVES FOR LOSS OR DAMAGE CAUSED BY ANY FAILURE OF THE SOFTWARE TO OPERATE IN CONFORMITY WITH THIS WARRANTY, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT OR TORT, INCLUDING NEGLIGENCE, STRICT LIABILITY OR OTHERWISE, SHALL BE (1) THE REPAIR OR REPLACEMENT OF THE SOFTWARE, PROVIDED THAT SUCH SOFTWARE IS RETURNED IN ACCORDANCE WITH THE CONDITIONS PROVIDED HEREIN OR (2) IF SUCH REPAIR CANNOT BE MADE OR AN EQUIVALENT REPLACEMENT CANNOT BE PROVIDED, THE REFUND OF AMOUNTS PREVIOUSLY PAID BY YOU BETWEEN DISCOVERY OF THE FAILURE OF THE SOFTWARE TO OPERATE IN CONFORMITY WITH THIS WARRANTY AND THE RETURN OF THE SOFTWARE AS REQUIRED BY THIS AGREEMENT.

7. Limitations on Liability. IN NO EVENT SHALL LICENSOR BE LIABLE FOR INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES, OR FOR LOST PROFITS, SAVINGS, OR REVENUES OF ANY KIND, OR FOR LOST DATA OR DOWNTIME, REGARDLESS OF WHETHER LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE CUMULATIVE LIABILITY OF LICENSOR TO YOUR ORGANIZATION FOR ALL CLAIMS RELATING TO THE SOFTWARE OR THIS AGREEMENT, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT OR TORT, INCLUDING NEGLIGENCE, STRICT LIABILITY, OR OTHERWISE, SHALL NOT EXCEED THE TOTAL AMOUNT OF ALL FEES PAID TO LICENSOR HEREUNDER.

8. Miscellaneous. The provisions of Sections 4, 6, 7 and this Section 8 shall continue to apply in accordance with their terms, notwithstanding the termination of this Agreement. References to "your organization" or "you" herein, for purposes of establishing the permitted use of the Software, shall include the operations of any direct or indirect parent or subsidiary company or of any direct or indirect subsidiary company of any such parent company. This Agreement and the rights and obligations of the parties with respect to the Software shall be governed by Virginia law, as it applies to a contract negotiated, executed, and performed in that state and without giving effect to principles of conflicts of law. Any legal action or proceeding arising under this Agreement shall only be initiated in the courts of the Commonwealth of Virginia. Execution and delivery of this Agreement by the parties indicates their intent to submit their disputes, their persons and their property, generally and unconditionally, to the jurisdiction of such courts. Venue shall be proper in any such court. If any action is brought by either party to this Agreement against the other party regarding the subject matter of this Agreement, the prevailing party shall be entitled to recover, in addition to any other relief granted, reasonable attorney fees and expenses of litigation.

YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT AND UNDERSTAND THIS AGREEMENT AND THAT BY OPENING THIS PACKAGE, YOU MANIFEST YOUR ASSENT TO BE BOUND BY ITS TERMS AND CONDITIONS.

[ ] I ACCEPT
[ ] I DO NOT ACCEPT

This product includes software developed by XHEO INC (http://www.xheo.com).

(c) 2000 - 2007 The Legion Of The Bouncy Castle (http://www.bouncycastle.org)

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

The Privaris plusID device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.