PRECISE™ BIOMETRICS

User's Guide

for Precise 100 A

Precise 100 Logon 2.1
Windows NT/2000

Fingerprint Identification System

Precise 100 A

Notice

Electromagnetic Compatibility (EMC) Notices

For Europe: CE

This digital equipment fulfils the requirements for radiated emission according to limit B of EN55022: 1994 and the requirements for immunity according to EN55024: 1998 residential, commercial and light industry.

For the U.S.A.: FCC

For Precise 100 SC reader:

This 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.

For Precise 100 A reader:

This device complies with part 15, subpart B, class B of the FCC Rules demonstrated by compliance with EN55022: 1994, class B. 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.

info@precisebiometrics.com
www.precisebiometrics.com
Phone +46 (0)46 31 11 00
Fax +46 (0)46 31 11 01
Address: Dag Hammarskjölds v 2
SE-224 64 Lund
Sweden

P/N: AM010005 R3B

Content

Chapter 1
Introduction

Congratulations on selecting Precise Biometrics' Fingerprint Identification System! Using your fingerprint for identification is an easy and secure way to prove your identity. Please read this chapter before you install and use the system.

This chapter includes the following information:

- What's new in Precise Logon 2.1
- The fingerprint reader
- The fingerprint identification process
- Why use fingerprint technology?
- The Precise 100 family
- Icons and conventions

What's New in Precise Logon 2.1

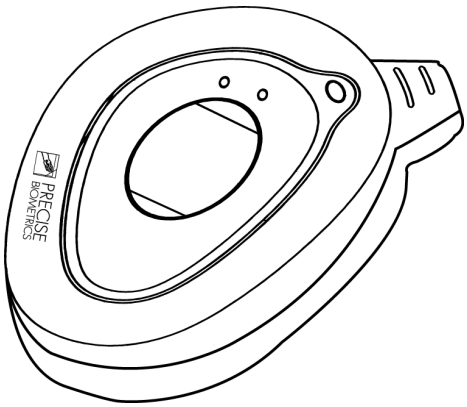
Three new main features are introduced with the Precise 100 Logon 2.1 software:

1. To enable biometric logon to a network, the installation of Precise 100 Logon 2.1 software is **only** needed on the client PCs. **There is no need for any additional software installation on the domain server.**
2. The domain administrator has the possibility to remotely administrate user accounts on the domain server by using the BioManager for Domains application, i.e. administration can be done from any workstation in the network having the Precise 100 Logon 2.1 installed. The BioManager for Domains application is included in the Precise 100 Logon 2.1 software.
3. The user has the possibility to remotely (i.e. from his own PC) enrol and re-enrol fingerprints, changing primary logon finger etc. for his own user account, called personal enrolment.

Precise 100 A

The Fingerprint Reader

The fingerprint reader includes a sensor for reading fingerprints. When you place your finger on the fingerprint reader, the part of the finger that touches the sensor is read. The sensor measures the capacitance in the finger pad, which reveals the pattern of the fingerprint. Thus, a paper copy with a picture of a fingerprint can not grant access to the system.



The Precise 100 A fingerprint reader

The Fingerprint Identification Process

When logging into a system, your fingerprint is compared to a fingerprint template, i.e. a data file containing information about the fingerprint, stored on a hard disk.

The fingerprint template is a set of characteristics which are unique for one specific fingerprint and not an image of your fingerprint. Your actual fingerprints cannot be recreated using the data from the fingerprint template.

If your fingerprint matches the fingerprint template, the system will grant you access. If the match is not successful, the system will deny access. It takes less than one second for the system to compare a read fingerprint with the information in the database. All information sent between the fingerprint reader and computer is encrypted for maximum security.

At logon, you simply enter your username and place your finger on the fingerprint reader to log into the system!

Why Use Fingerprint Technology?

In modern society, there is a vast need for secure identification, for instance when logging into computer network. An unauthorised person who obtains access to computer files constitutes a major risk to many companies. In order to prevent unauthorised access, network users have previously identified themselves with a password entered together with the username when logging into a network.

The disadvantages of passwords:

- Unreliable identification. An unauthorised person who knows your password can easily access your user account.
- A complicated system. In order to increase security, users are regularly asked to change their passwords. This makes it difficult to remember a password.
- Users forget their passwords, this increase the administration workload.
- Users write down their passwords on notes and store them close to their applications. This can be a serious security hazard.

The advantages of fingerprint identification:

- Secure identification. By identifying yourself with your fingerprint, you use a unique "key" to access your user account. All your fingerprints are unique – no person has identical fingerprints.
- Simplicity. It is simple to use fingerprints for identification. You do not have to worry about changing or memorising passwords anymore – your fingerprint provides secure identification, year after year.

Simply put, with Precise 100 A, you are identified by who you are, not by what you know!

About the Precise 100 Family

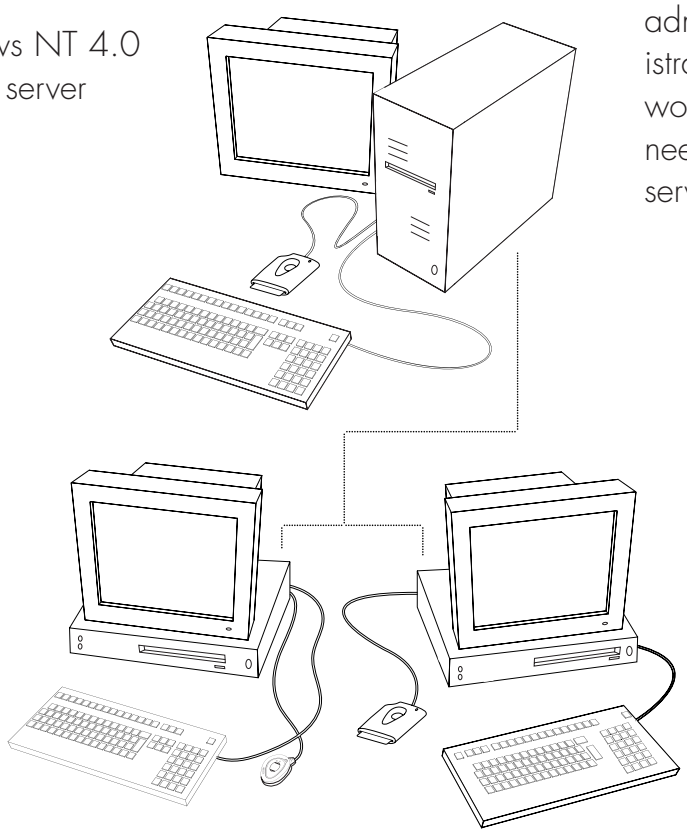
Precise 100 A Logon – For Windows NT/2000, local or in an NT domain. Fingerprint data is stored on the local hard drive, or server hard drive. For logon to local accounts and/or domain server accounts.

Precise 100 SC Logon – For Windows NT/2000, local or in an NT domain. For maximum security, fingerprint data can be stored on smart cards, as well as on the local hard drive. For logon to local accounts and/or domain server accounts.

Precise 100 SC SDK – Precise Biometrics' Software Development Kit, for OEM-customers and system integrators who want to integrate Precise Biometrics' software and hardware into their own system. It contains documentation, tools, API, and examples.

Possible configuration

Windows NT 4.0
Domain server



With the Precise 100 Logon 2.1 software an administrator can administrate all users from any workstation, without the need for additional server software.

With Precise 100 SC and the Precise 100 Logon 2.1 software installed, users can log on to local accounts and/or domain server accounts. For maximum security, fingerprint data can be saved on smart cards.

Local workstation, with Precise 100 A installed

Local workstation, with Precise 100 SC installed

Icons and Conventions

- Key names on the keyboard appear in italics, for example *Caps Lock*, *Ctrl*, *Enter*.
- Names of fields, text boxes and buttons appear in bold type, for example **Username**, **User**, **OK**.
- Keys that you should press and hold down together appear as the key names and the plus (+) sign, for example *Ctrl* + *Alt* + *Delete*.
- An arrow is used to separate icons or menu options that should be selected in succession, for example **Start > Settings > Control Panel**.

Chapter 2
Installation

The installation consists of two parts. Start by following the instructions in the Preparing Installation section. Then continue with the Installing the Fingerprint Identification Software section.

NOTE: If you are using a Precise 100 A with parallel port connector, it is very important that the parallel port of the PC is set to ECP mode before using the fingerprint reader. Otherwise, the fingerprint reader will not function properly. See Setting the Parallel Port in this chapter.

This chapter includes the following information:

- Minimum system requirements
- Preparing installation
- Setting the parallel port
- Connecting the fingerprint reader
- Installing the fingerprint identification software
- Attaching the fingerprint reader

NOTE: In order to log into your domain server account using your fingerprint:

- the Precise 100 A must be installed on your workstation
- your fingerprints must be registered on the domain server by a **domain server administrator** using the **Biomanager for Domains** or by **Personal Enrolment**.

Minimum System Requirements

In order to install the software included on the enclosed CD-ROM, your computer must meet the following system requirements:

- PC with 200 MHz Pentium processor or equivalent
- 10 MB hard disk space available
- USB port *or* Parallel port with ECP support and PS/2 keyboard/mouse port

NOTE: If you wish to connect the Precise 100 A PAR reader to a secondary parallel port, this port has to be on the ISA-bus and not the PCI-bus.

- One of the following operating systems:
  1. Windows NT 4 Workstation with Service Pack 6
  2. Windows NT 4 Server with Service Pack 6
  3. Windows 2000 Professional
- Mouse or compatible pointing device
- CD-ROM drive (unless you are installing the software from a network)
- VGA resolution graphics card or higher

NOTE: To logon to a domain server using Precise 100 Logon 2.1, the server must be running Windows NT 4.0 Server operating system with Service Pack 6.

Preparing Installation

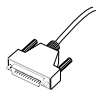
The Precise 100 A fingerprint reader comes in two versions: Precise 100 A PAR and Precise 100 A USB. The Precise 100 A PAR communicates with the computer through the computer's parallel port, and the keyboard port or mouse port is used to power the fingerprint reader. The Precise 100 A USB communicates with the computer through the computer's USB port and does not need additional power.

Parallel

USB

In the following a picture of a parallel connector indicates a section relevant only to Precise 100 A PAR readers while a picture of a USB connector indicates a section relevant only to Precise 100 A USB readers.

If you are a using a Precise 100 A USB reader you should skip the following two sections and continue with the Installing the Fingerprint Identification Software section. However, if you are using a Precise 100 A PAR reader, follow the instruction below prior to starting the installation.



Setting the Parallel Port

Before connecting the fingerprint reader, ensure that the parallel port is set to ECP mode. It is very important that the parallel port is set to ECP mode before using the fingerprint reader. Otherwise, the fingerprint reader will not function properly. If you do not know whether your computer is in ECP mode (most new computers are), please see the computer manual for additional information, or follow the instructions below.

1. Access the system setup utility. On most computers, this is done by pressing the F1, F10, Delete or Esc key during system booting – i.e. immediately after the power switch on your computer has been turned on. Keep pressing the key until the system setup, sometimes called the BIOS, appears.

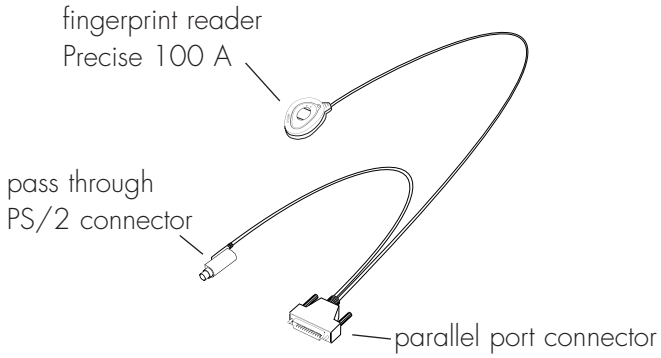
2. Find the parallel port mode. Set the port mode to ECP (sometimes called Flexible mode). If you are unable to find the port mode, your computer is probably already in ECP mode.

3. Save your changes and exit the system setup utility. If you have problems with the ECP settings, please contact your computer retailer.

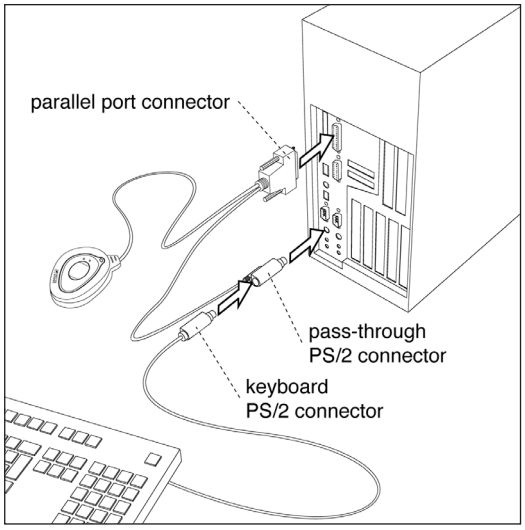
Connecting the Fingerprint Reader to the Computer

1. Make sure that the parallel port is set to ECP mode.

2. Turn off the computer.



3. Connect the fingerprint reader to the parallel port at the back of the computer by using the connector. Make sure that the connector is secured, so that it can not be disconnected by mistake.



4. Unplug the keyboard/mouse PS/2 connector from the keyboard or mouse port at the back of the computer. Plug the pass-through PS/2 connector from the fingerprint reader into the keyboard/mouse port instead.

5. Connect the keyboard/mouse PS/2 connector to the pass-through PS/2 connector.

6. Power on the computer.

Continue with the next step – Installing the Fingerprint Identification Software.

Installing the Fingerprint Identification Software

NOTE: Only users with administrator rights can install the software.

The fingerprint identification software, Precise 100 Logon 2.1, is needed to read your fingerprints and to save and retrieve information about your fingerprints, accessible domains, etc.

During installation you may be instructed to restart your computer before continuing to the next step in the installation procedure. If the Master Setup screen does not appear automatically after restart, start the CD from your desktop by double-clicking **My Computer > CD > MasterSetup.exe** icon.

NOTE: Once the software is installed, you will be able to register fingerprints using the BioManager for Domains (see The BioManager for Domains chapter for details) and store them locally if you log on as administrator on your local workstation. However, that will not grant access to domain server accounts. To be able to log into a domain server account using your fingerprint, your fingerprint will have to be registered and stored on the domain server.

When the fingerprint identification software is installed on your local computer, you can use Personal Enrolment to register your fingerprints on the domain server. See the Personal Enrolment chapter for details.

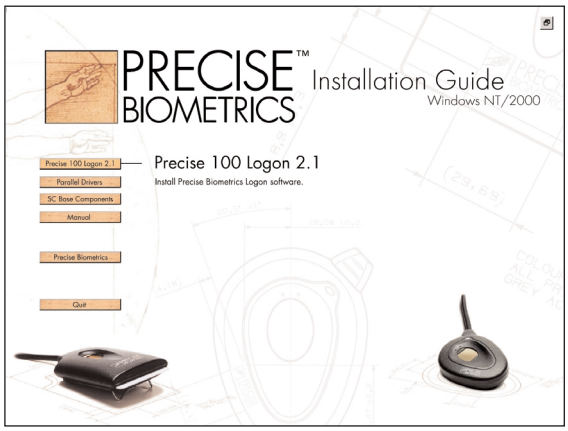
Installing the Precise 100 Logon 2.1 Software

NOTE: If you have a previous release of Precise Biometrics fingerprint identification software installed on your computer, please do the following before you install the Precise 100 Logon 2.1 software: 1) Make sure you have a backup password (see the chapter BioManager). 2) To uninstall the old software, read carefully the chapter Uninstalling in your Precise Biometrics manual and follow the instructions.

NOTE: After installation, the computer has to be restarted before you can use the software.

1. Log into your local computer as administrator. It is strongly recommended that all Windows programs are closed and no disk is in the disk driver.

2. Insert the enclosed Precise 100 Logon 2.1 software CD into your computer's CD-ROM drive. The Master Setup screen appears.



Master Setup screen

NOTE: If the CD does not start automatically, start the CD by clicking **Start > Run**. Enter D:\MasterSetup.exe, where "D" is the name of your CD drive. Click **OK**.

3a. If you have a Precise 100 A USB reader, connect the fingerprint reader to your computer. Windows 2000 will detect the new hardware and install the necessary drivers from the CD.

3b. If you have Precise 100 A PAR reader, click the Parallel Driver button to install the necessary parallel port drivers.

4. If you are using Windows NT you must install the *updated* Microsoft Smart Card Base Components, if not previously installed. **Do not install the Smart Card Base Components if you are using Windows 2000, the system may crash**.

   To install the Smart Card Base Components
   a) Click the **SC Base Components** button, a submenu appears.
   b) Click the **Base Components** button in the submenu. You don't need to reboot your computer after this step if you continue directly with the next step.
   c) Click the **Update** button in the submenu and follow the instructions.

5. To install the Precise 100 Logon 2.1 software, click the **Precise Logon 100 2.1** button and follow the instructions.

The software will guide you through the installation. Use the *Back* and *Next* buttons to navigate through the screens.

6. Click **Finish** to complete the installation. The computer has to be restarted after the installation is completed. Remove the software CD from the CD-ROM drive before restarting the computer.

The software is now installed on your hard drive.

7. When the fingerprint identification software is installed on your local computer, you can use Personal Enrolment to register your fingerprints on the domain server. See the Personal Enrolment chapter for details.

Precise Demo

It is recommended that you practice registering and verifying fingerprints for a few minutes using the Precise Demo. This will help you to practice finger positioning which will make it easier to log on using the fingerprint reader. When you are using the Demo, none of your operations will affect your system.

Start the Precise Demo by clicking **Start > Programs > Precise Biometrics > Demo**.

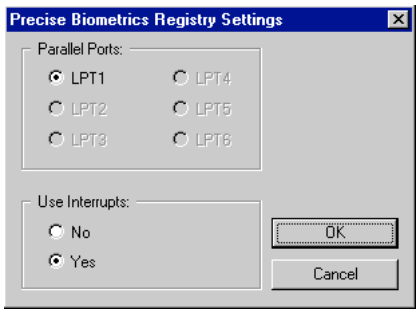
Port Configuration

If you are using Windows NT (only) and your system is equipped with multiple parallel ports, you can specify which parallel port the fingerprint reader is connected to. This is done in the Precise Biometrics Registry Settings. In the rare case you should experience compatibility problems with other software, you may also need to turn interrupts on or off.

1. Click **Start > Settings > Control Panel**. The Control Panel screen appears.

2. Double-click on the Precise Biometrics logo. The Precise Biometrics Registry Settings screen appears.

3. Make the desired changes and click **OK**.



Attaching the Fingerprint Reader

If preferable, the fingerprint reader can be attached to, for example the side of your monitor. Simply use the adhesive tape at the back of the fingerprint reader. The adhesive tape is very durable and will keep the fingerprint reader attached for many years. The fingerprint reader can be removed and attached again. If the adhesive tape loses its stickiness, replace it with one of the enclosed adhesive tapes.

Before attaching the fingerprint reader, make sure that it will be comfortable for you to use the fingerprint reader in its new place. Try some different positions to find out which is the best before removing the adhesive tape cover strip. If you are right-handed, the right side of your monitor will probably work best, and vice versa.

1. Make sure the surface on which you want to attach the fingerprint reader is perfectly clean.

2. Remove the cover strip from the adhesive tape at the back of the fingerprint reader.

3. Attach the fingerprint reader by pressing it to the surface.

Replacing the Adhesive Tape

If the adhesive tape has lost its stickiness, use the enclosed adhesive tapes. The enclosed adhesive tapes have a cover strip on both sides.

1. Remove the old tape from the fingerprint reader before attaching the new adhesive tape.

2. Remove one cover strip from the new tape and press the sticky side to the fingerprint reader.

3. Finally remove the remaining cover strip and attach the fingerprint reader to the desired surface.

Chapter 3

Using the Fingerprint Reader

As with most new technology, it might take some training to feel at home logging on using your fingerprint. When you log on and verify your fingerprint, it is important that you place your finger on the fingerprint reader in a proper way. The following chapter contains some examples of good and bad ways of placing your finger on the fingerprint reader.

It is highly recommended that you practice by using the Precise Demo for a few minutes (see Precise Demo in the previous chapter for details).

This chapter includes the following information:

- Placing your finger correctly on the fingerprint reader
- Fingerprint reader maintenance

Placing Your Finger Correctly on the Fingerprint Reader

When you place your finger on the fingerprint reader sensor to identify yourself, please remember two things:

1. It is important that you use the correct finger. For example, if you place your left index finger on the sensor, you will not be granted access if the system expects you to use your left middle finger. When logging on, a screen shows you which finger you are expected to use – it is marked with a dot.

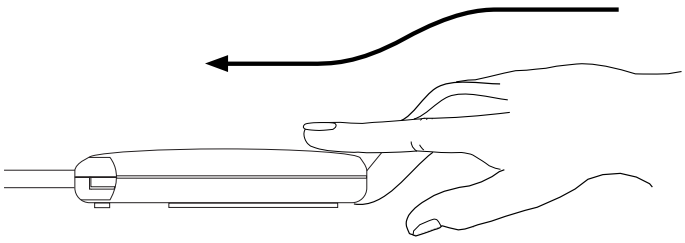
2. Your finger should be properly positioned on the sensor. Poor positioning and too much or too little pressure could result in an erroneous reading – which may prevent you from gaining access to the system.

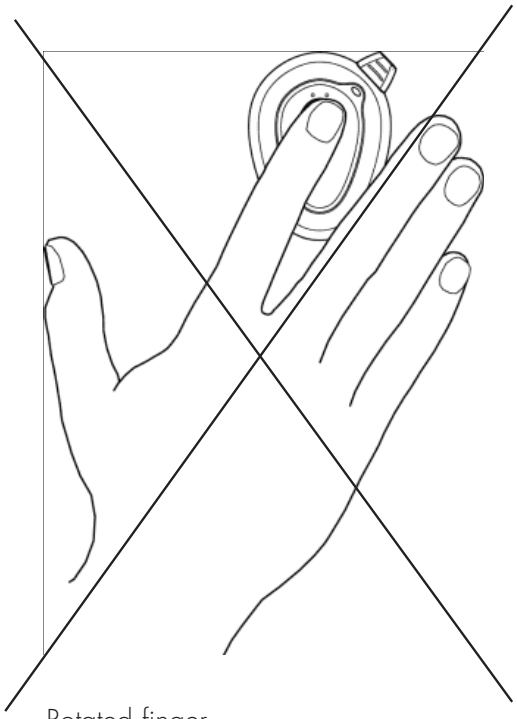
Correct Finger Placement

Most of the information in a fingerprint is located in the middle of the finger pad. Therefore, it is important that the middle of the finger pad is placed in the sensor centre at enrolment and logon.

- Press your finger pad flat to the sensor.
- Let the top of your finger pad touch the top of the sensor on your fingerprint reader.
- Use medium pressure and avoid rotating your finger.

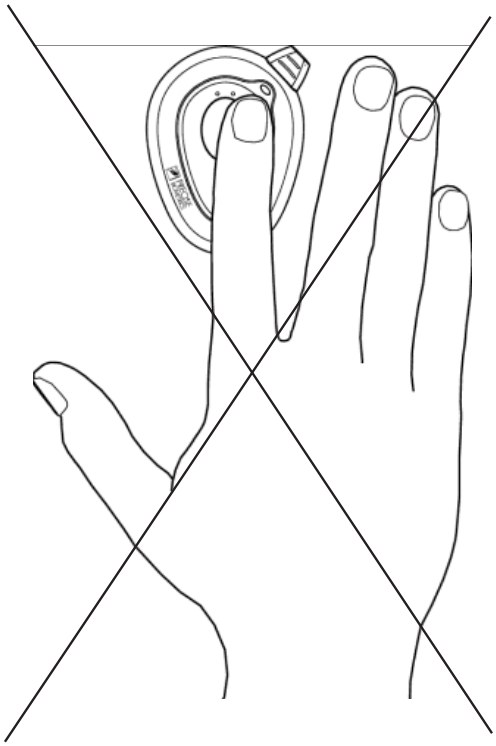
The following graphics show some examples of different fingerprint images:





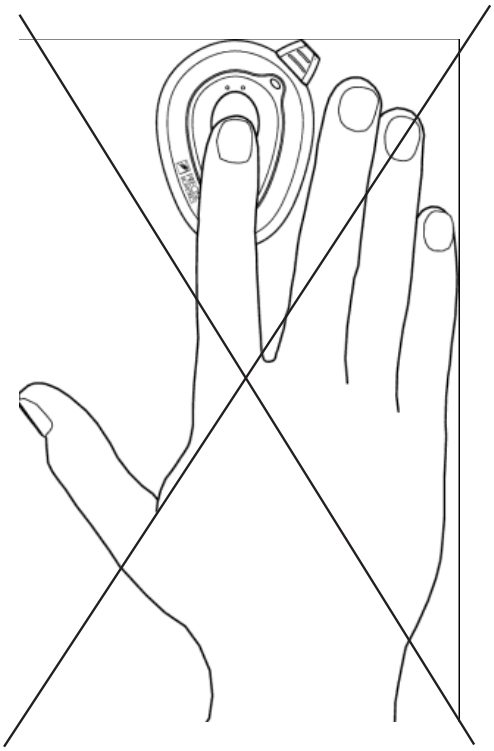
Rotated finger

Poor image:
rotated fingerprint.



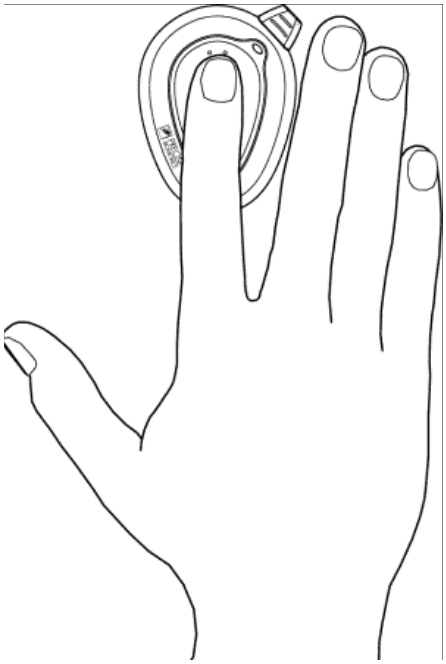
Skew finger
– too far to the right.

Poor image:
off-centre fingerprint.



Finger placed too far down on the sensor

Poor image:
off-centre fingerprint.



Perfectly placed finger

Good image:
fingerprint in the middle,
medium pressure to the sensor.

If the placement is correct, but too much or too little pressure is used, the images will look like this:

Poor image:
too dark fingerprint caused by excessive pressure. The finger may also be wet.

Poor image:
faint fingerprint caused by insufficient pressure. The finger may also be very dry.

When you are placing your finger on the fingerprint reader sensor, it is important that you use the finger marked in the Verify Fingerprint window.

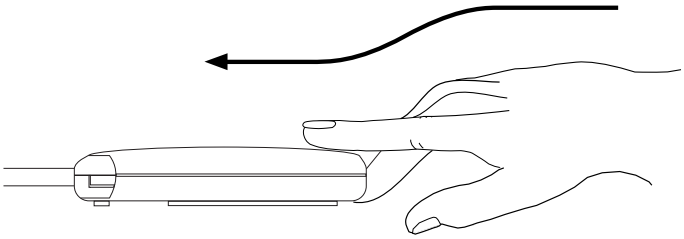
Good image from the sensor

Above is a good fingerprint, which will result in a perfect match and system access.

Above is a good fingerprint, which will not result in a match since the fingerprint is not matched with its corresponding template. You may have placed the wrong finger on the sensor, or it could be an unauthorised person trying to log into your account. The system will deny access.

To learn more about how to position your finger on the fingerprint reader, use the Precise Demo. To start the Precise Demo, click **Start > Programs > Precise Biometrics > Demo**.

High electrostatic discharges might damage the fingerprint sensor. If your Precise 100 Reader is used in an environment where there is a high risk of electrostatic discharges when putting the finger on the sensor, it is important to follow the instructions below.



We recommended to always use the Precise 100 Reader as described here. When putting the finger on the sensor, let your finger slide via the finger guide towards the sensor (see picture).

When putting the finger on the sensor multiple times in a short time period, e.g. during enrolment, you only have to slide via the finger guide the first time you put your finger on the sensor.

Fingerprint Reader Maintenance

It is very important that the sensor surface is kept clean. If the sensor is dirty or scratched, there is an increased risk that a fingerprint can not be successfully matched with its corresponding template stored in the database.

- Protect the fingerprint reader from any kind of physical damage.
- If necessary, clean the surface with a clean cotton cloth. You can dampen the cloth slightly with a cleaner.
- Do not use paper tissue for cleaning purposes, since it may scratch the surface.
- Do not spray cleaner directly onto the fingerprint reader.

Chapter 4
Personal Enrolment
– Administrating Your Own User Account

This chapter addresses the process of remotely enrolling a user into the fingerprint database system and registering a user's fingerprint data.

This chapter includes the following information:

- Administrating your own user account.
- Biometric and non-biometric users.
- Enrolment via the Windows Security screen.

Administrating Your Own User Account

A user can remotely administrate user accounts on a domain server. This includes enrolling and re-enrolling fingerprints, changing the password and changing the primary logon finger. Administration of the currently logged-on user is initiated via the Windows Security screen (or by an administrator using the BioManager for Domains – see The BioManager for Domains chapter for details).

Biometric and Non-Biometric Users

There are two types of user. A biometric user is a user who has been enrolled into the system and who can log on using fingerprints. A non-biometric user is a user who has not been enrolled into the system and can not use fingerprint logon.

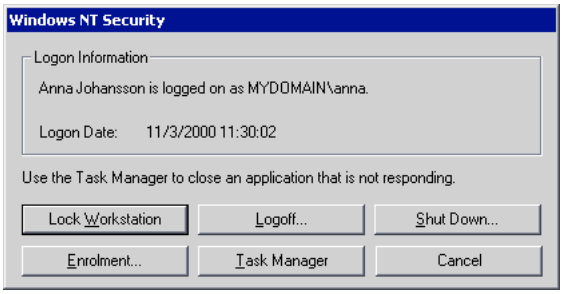
Enrolment via the Windows Security Screen

When the enrolment wizard is started via the Windows Security screen, the user account of the currently logged-on user is pre-selected.

To start the enrolment wizard via the Windows Security screen:

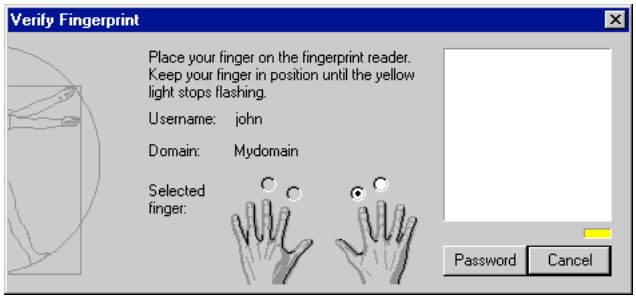
1. Press *Ctrl* + *Alt* + *Delete*.

The Windows Security screen appears.



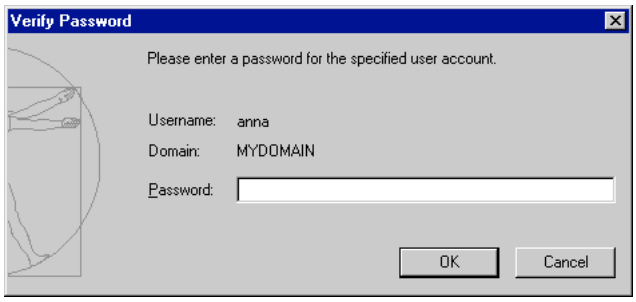
2. Click **Enrolment**.

If you are a biometric user the Verify Fingerprint screen appears (see 2.1 below). Otherwise the Verify Password screen appears (see 2.2 below).



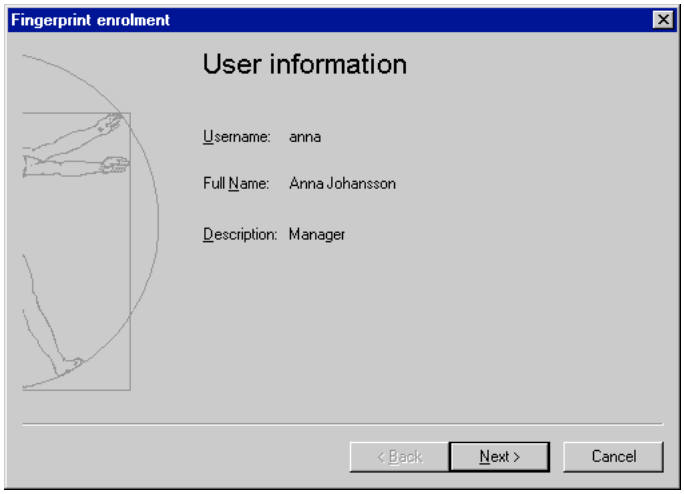
2.1. Place your finger on the fingerprint reader.

2.1.1 If you have a password you can choose to log on using this password even if you are a biometric user. Click **Password** and the Verify Password screen appears.



2.2. Enter your password and click **OK**.

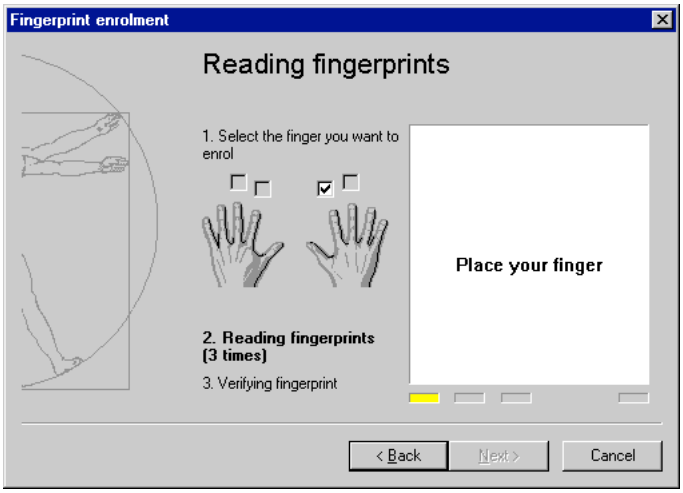
The enrolment wizard starts and the User information screen appears.



3. Here you can view your username, your full name and your description.

4. Click **Next**.

The Reading fingerprints dialog appears.



In the Reading fingerprints dialog you can register your fingerprints.

6. To register a fingerprint, follow the instructions below:

6.1. Select the finger to register by clicking in one of the checkboxes. Follow the instructions on the screen. Make sure the selected finger is placed on the fingerprint reader sensor.

NOTE: Place the middle of the finger pad on the sensor, to ensure an image rich in fingerprint information.

6.2. After collecting three images of the fingerprint, the best image is automati cally selected and verified against a fourth image. This is done to ensure that the best image is of sufficient quality. Registered fingers will be marked with grey check boxes containing a checkmark.

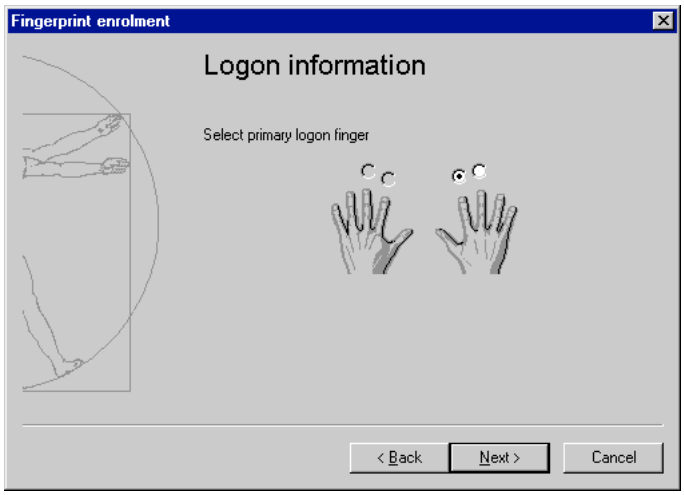
NOTE: It is recommended that more than one fingerprint is registered, in case a finger gets scratched, etc. To register additional fingerprints, just click in a new checkbox.

7. Click **Next** when as many fingers as desired have been registered.

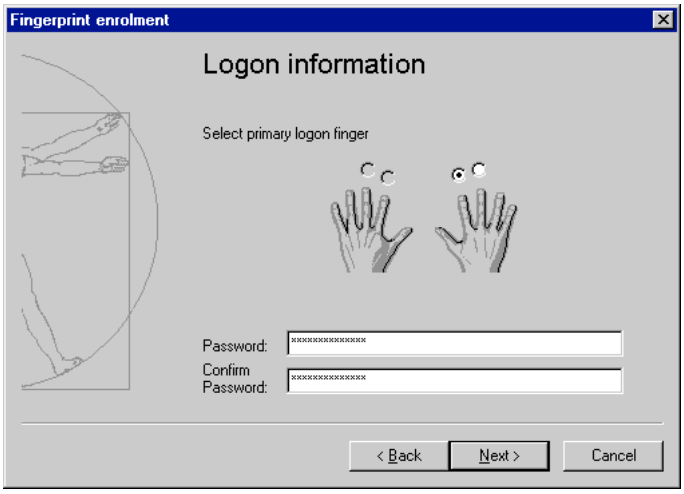
The Logon information dialog appears.

In the Logon information dialog you select the primary logon finger. The primary logon finger is the finger that usually will be used to log on or unlock a workstation.

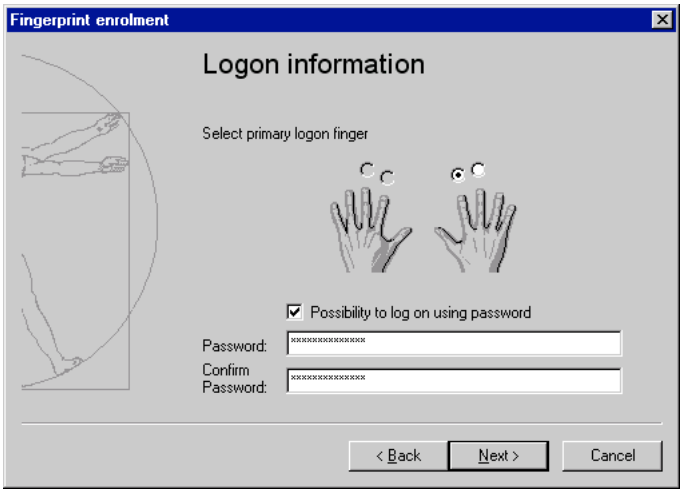
Depending on the administrator's settings for your account (see The Biomanager for Domains chapter for details), there will also be one of the following choices for the use of passwords:



7.1 If the administrator has turned off the possibility for users to change pass words in the Windows User Manager, the dialog will look like the one above and there will be no further choices.



7.2 If users are allowed to change passwords, you can enter your new pass word in the **Password** and **Confirm Password** fields.



7.3 If the checkbox **Possibility to log on using password** appears, you can leave it unchecked to get a random, auto-generated password, which will not be available to you. This means that the only way you can log on is to use your fingerprint.

7.4 If you check the **Possibility to log on using password** checkbox you will be able to choose your own new password which you will then have to enter twice.

NOTE: Fore more information on passwords see section About Passwords in The BioManager for Domains chapter.

8. Click **Next**.

The saving screen appears.

9. Click **Finish**

Until you click **Finish** you can go back to step 4 above using the **Back** button. No changes will be saved until you click **Finish**.

The information is encrypted and saved on the hard drive.

You can abort the enrolment process at any time by clicking **Cancel**. In that case no changes will be saved.

NOTE: Due to the need for synchronisation between the PDC and the BDC, it may sometimes take a couple of minutes before it is possible to logon to the system when User Data has been updated or changed using the enrolment wizard.

Chapter 5
The BioManager for Domains

NOTE: Chapter 5 is for administrators. Users without administrator rights do not have access to the BioManager for Domains.

The BioManager for Domains (henceforth referred to as the BioManager) is used for administrating biometric user accounts (see Biometric and Non-Biometric Users later in this chapter). This chapter addresses the process of enrolling a user into the fingerprint database system and registering a user's fingerprint data.

This chapter includes the following information:

- The BioManager for Domains
- Biometric and Non-Biometric Users
- Primary logon fingers
- Passwords
- Security level
- Registering fingerprints
- Adding a new user
- Enrolling an existing user
- Checking and changing a user's properties
- Deleting a user

Introduction to the BioManager for Domains

Using the Biomanager Administrators can:

- Choose which domain and user account to administrate
- Add and delete users
- Register fingerprints
- Turn password users into biometric users
- Decide whether a biometric user is allowed to use a password as backup
- Change properties for users
- Set the security level for the system

Biometric and Non-Biometric Users

There are two types of user. A biometric user is a user who has been enrolled into the system and who can log on using fingerprints. A non-biometric user is a user who has not been enrolled into the system and can not use fingerprint logon

Users are listed in the BioManager with a symbol next to each username. The following symbols are used to define a user's current status:

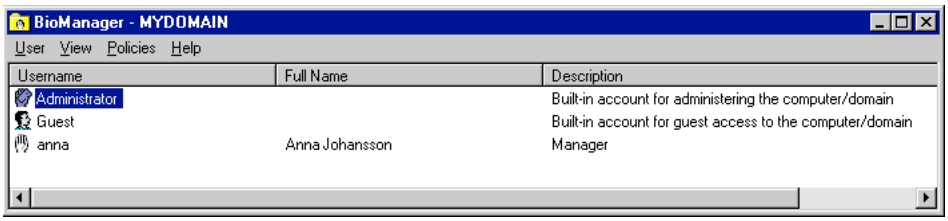
 Biometric user, with fingerprint information stored on the hard drive.

 Biometric user with fingerprint information stored on smart card.

 Non-biometric user. Can not log on using a fingerprint yet, must use a password

Accessing the BioManager

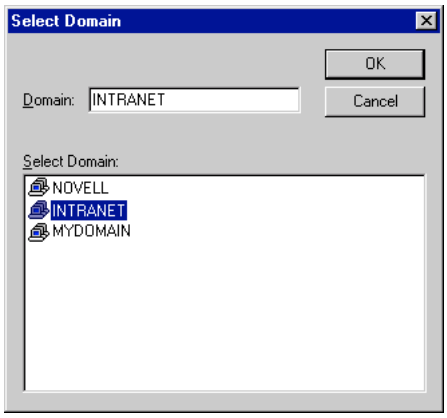
Click **Start > Programs > Precise Biometrics > BioManager for Domains**. The BioManager screen appears.



Changing Domain

When the BioManager is started, the domain of the local computer is selected. Change to another domain by clicking **User** > **Select Domain**.

The Select Domain screen appears.



Select the domain you wish to administer and click **OK**.

About Primary Logon Fingers

The primary logon finger is the finger normally used to log on. The system assumes that the selected primary logon finger is placed on the fingerprint reader when a user logs into or unlocks a workstation. The fingerprint on the sensor is then compared to the primary logon fingerprint template in the database. The user can choose to verify another registered finger when logging on.

The primary logon finger is chosen during enrolment, in the Fingerprint registration wizard. The wizard is accessed by clicking **User > New User** or **User > Properties** at the BioManager screen. Any registered finger can be chosen as primary logon finger. To change the primary logon finger, see Checking and Changing a User's Properties at the end of this chapter.

NOTE: The user can change the primary logon finger using Personal Enrolment. See the Personal Enrolment chapter for details.

About Passwords

It is possible to let a fingerprint user log on with a backup password, if this option is chosen during enrolment. It is not recommended, however, as passwords make it easier for an unauthorised person to log into the user's account.

NOTE: Only use the password option if the user really needs an alternative to fingerprints for logon.

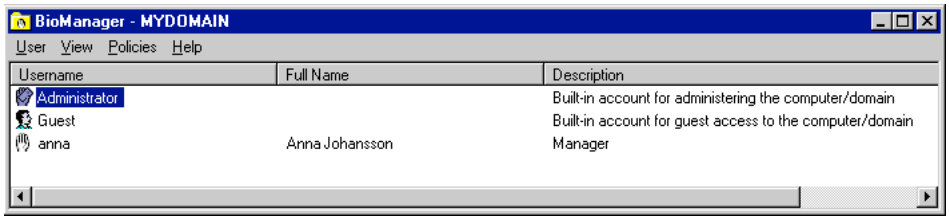
If the user uses a laptop computer at work and uses the same laptop at home or when travelling, a password could be very useful. At logon, the user can choose to log on using a fingerprint reader or by writing a password.

NOTE: If the password logon possibility is *not* chosen, the user can only log on using a fingerprint. If a current password user is enrolled into the fingerprint database system, the current password will no longer be valid.

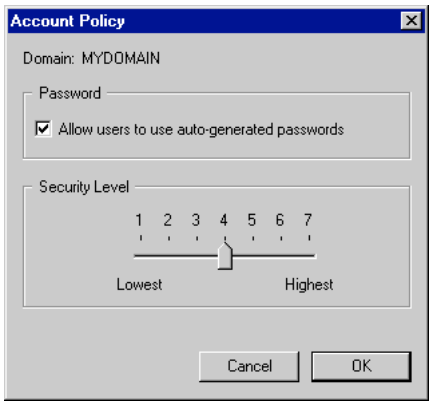
Auto-generated Passwords

You can specify whether or not users should be allowed to choose to use passwords.

1. Click **Start** > **Programs** > **Precise Biometrics** > **BioManager for Domains**. The BioManager screen appears.



2. Click **Policies** > **Account**. The Account Policy screen appears.



If **Allow users to use auto-generated passwords** is checked (default) users will have the possibility to choose whether or not they want to have a random auto-generated password. If the user chooses to use an auto-generated password he will not to be able to log on using a password.

If you uncheck **Allow users to use auto-generated passwords** users cannot choose to use auto-generated passwords. The user may however still type in a password that can be used for logon.

About the Security Level

The security level is an important part of the identification system. A higher security level reduces the risk of an unauthorised person logging into an account. An administrator can set the security level for biometric users. The security level is set globally; i.e. the set security level affects all biometric users in the domain.

The False Acceptance Rate, FAR, is a parameter used to indicate the probability that an unauthorised user is given access to an account. The False Rejection Rate, FRR, indicates the probability that an authorised user is denied access to an account.

A secure system, i.e. a system with a high security level, means a low false acceptance rate.

- Higher security levels = an excellent match between the fingerprint on the sensor and the fingerprint template in the database is required. The FAR is very low; the FRR is comparatively high.
- Lower security levels = a less perfect match between the fingerprint on the sensor and the equivalent fingerprint template in the database is required. The FAR is comparatively high; the FRR is low.

Higher security levels (level 6 or 7) result in:

- A very secure system. It will be virtually impossible for an unauthorised person to log into a user account.
- A system which sometimes rejects an authorised user trying to log into an account. A small scratch, a distorted fingerprint or poor finger positioning on the fingerprint reader may produce a fingerprint that the system does not accept as a satisfactory match to the fingerprint template stored in the database.

Lower security levels (level 1or 2) result in:

- A less secure system. At lower security levels, the risk of an unauthorised user logging into an account increases.
- A system which very rarely rejects an authorised user who wants to log into an account.

Security level 4 is recommended to guarantee a reliable system that grants easy access to authorised users while barring unauthorised users.

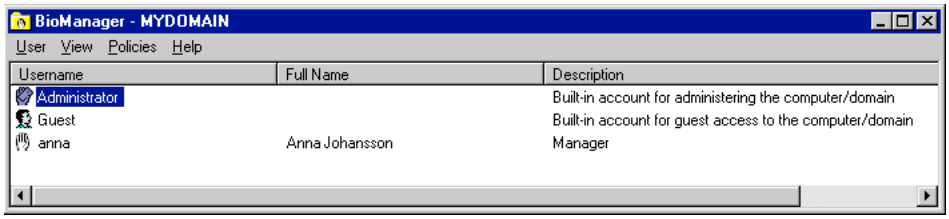
When should the higher and lower levels be selected? A lower security level is selected when there is little risk of an unauthorised user attempting to log on, and a very fast verification process is desirable. A higher security level is selected when security is the main concern. In this case, the verification process may take a little longer.

NOTE: An experienced biometric user is less likely to be falsely rejected than a novice biometric user. The FRR decreases as a user gets more used to biometric logon and learns a proper finger placement.

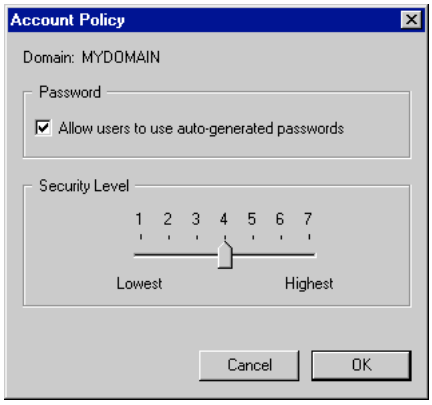
Setting the Security Level

The security level is accessed from the BioManager.

1. Click **Start > Programs > Precise Biometrics > BioManager for Domains**. The BioManager screen appears.



2. Click **Policies > Account.** The Account Policy screen appears.



Set the security level and click **OK**. Security level 4 is recommended for most purposes.

Passwords and Security Level

If an administrator allows users to log on with a password, a high security level loses part of its function. Even if the system is very restrictive when fingerprints are verified, the security might suffer from users who write down passwords on notepads or choose a very simple password, which can easily be cracked.

Fingerprint Registration

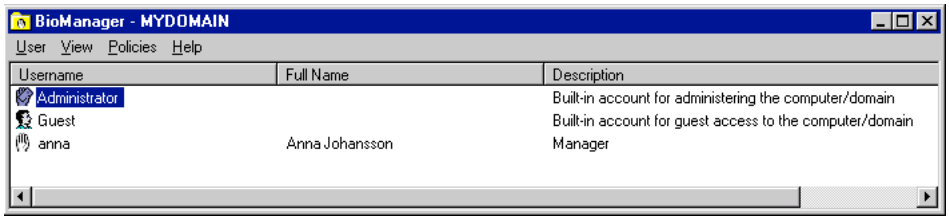
In order for a user to use a fingerprint to log on, the fingerprint must be read and stored in a database – i.e. it has to be registered. The fingerprint data will be stored on a hard drive.

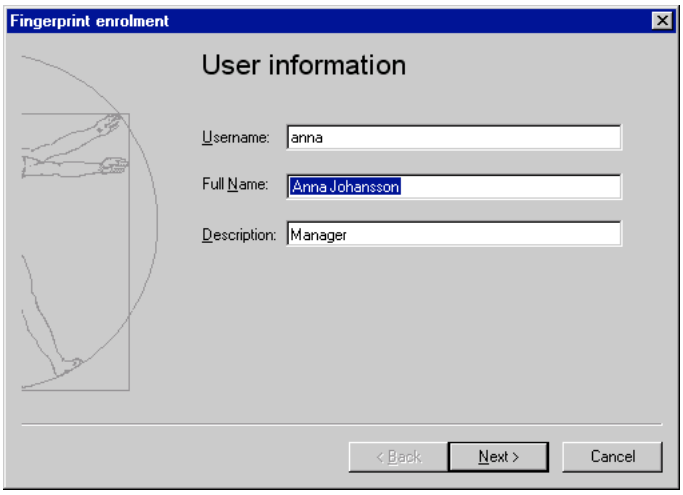
Only an administrator can register fingerprints using the BioManager. To enrol a user, whose username is not on the username list, see Beginning Fingerprint Registration of a New User in this chapter. To enrol a user listed in the BioManager, see Beginning Fingerprint Registration of an Existing User in this chapter.

Beginning Fingerprint Registration of a New User

Log on as administrator.

1. Click **Start > Programs > Precise Biometrics > BioManager for Domains**.
   The BioManager screen appears.





2. Click **User > New User**. The User information screen appears.

3. Type the user's name in the **Username** field.

4. Type the user's complete name in the **Full Name** field.

5. Type the user description in the **Description** field.

6. Click **Next**.

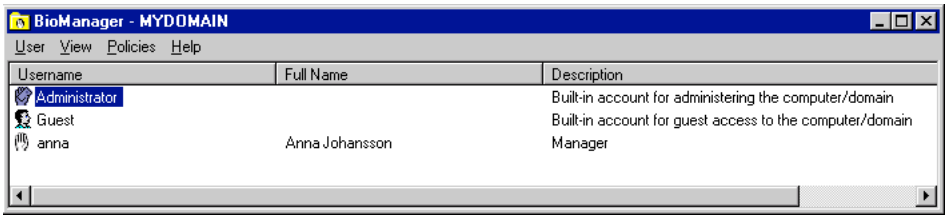
See Continue Fingerprint Registration in this chapter for information on how to continue.

Beginning Fingerprint Registration of an Existing User

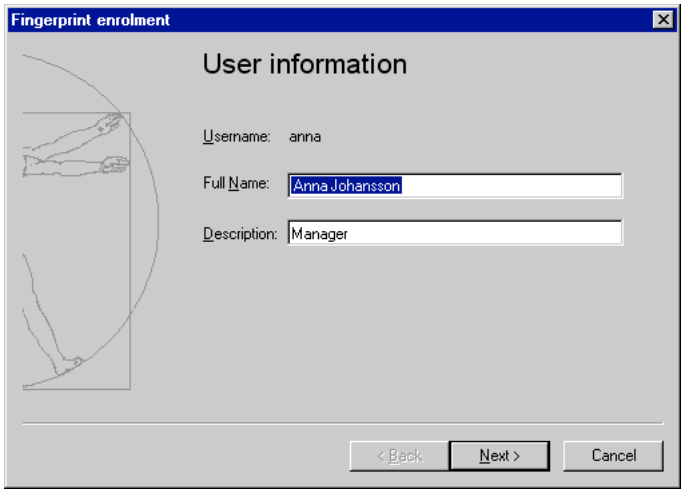
If a user has an account registered, his or her username is listed in the BioManager. An administrator can register, or re-register, the fingerprints of both password users and current biometric users.

1. Log on as administrator.

2. Click **Start > Programs > Precise Biometrics > BioManager**.
   The BioManager screen appears.



3. Double-click on a username. You can also click on a username and then click **User > Properties**. The User information screen appears.



4. Type the full name in the **Full Name** field.

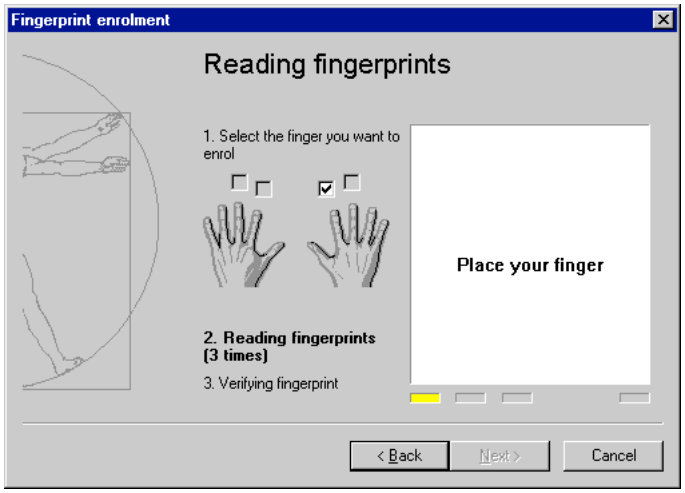
5. Type the description in the **Description** field.

6. Click **Next**.

See Continue Fingerprint Registration in this chapter for information on how to continue.

Continue Fingerprint Registration

When you click **Next** in the User information screen, the Reading fingerprints dialog appears:



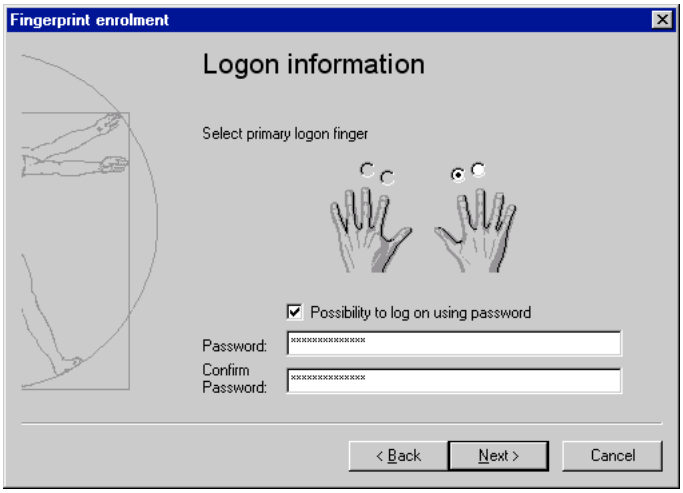
1. Select the finger to register by clicking in one of the checkboxes. Let the user follow the instructions on the screen. Make sure the selected finger is placed on the fingerprint reader sensor.

NOTE: Instruct the user to place the middle of the finger pad on the sensor, to ensure an image rich in fingerprint information.

2. After collecting three images of the fingerprint, the best image is automatically selected and verified against a fourth image. This is done to ensure that the best image is of sufficient quality. Registered fingers will be marked with grey check boxes containing a checkmark.

NOTE: It is recommended that more than one fingerprint is registered, in case a finger gets scratched, etc. To register additional fingerprints, just click in a new checkbox.

3. Click **Next** when as many fingers as desired have been registered. The Logon information screen appears.



4. Select the primary logon finger. The primary logon finger is the finger that usually will be used to log on or unlock a workstation.

5. If desired, select the **Possibility to log on using password** checkbox. This enables the user to log on using either a password or a fingerprint. Type the password in the **Password** field. Confirm the chosen password in the **Confirm** field.

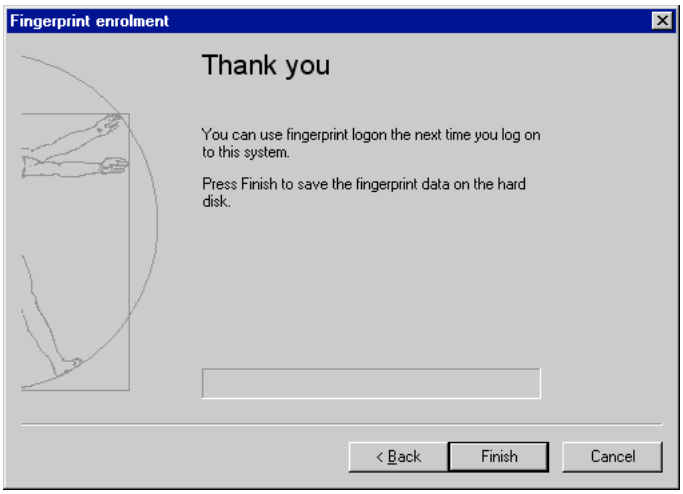
NOTE: Before you allow users to log on using a password, be sure to read the information in Passwords and Security Level earlier in this chapter.

6. If you leave the Possibility to log on using password checkbox unchecked, a random password will be auto-generated. This password will not be available to the user, which means that the only way the user can log on is using his/her fingerprint.

NOTE: To keep the user from checking the **Possibility to log on using password** checkbox during Personal Enrolment, the **User cannot change password** checkbox must be checked in the Windows User Manager.

NOTE: If a current password user is enrolled, the current password will no longer be valid. A new password must be typed, in order for the user to log on with a password as a backup.

7. Click **Next**. The saving screen appears.



8. Click **Finish**.

Until you click Finish you can go back as far as the User information screen using the **Back** button. No changes will be saved until you click **Finish**.

The information is encrypted and saved on the hard drive.

NOTE: Due to the need for synchronisation between the PDC and the BDC, it may sometimes take a couple of minutes before it is possible to logon to the system when User Data has been updated or changed using the BioManager for Domains.

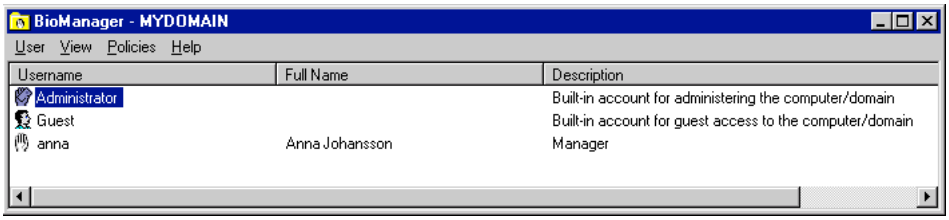
Checking and Changing a User's Properties

An administrator can check and change the set properties for an enrolled user:

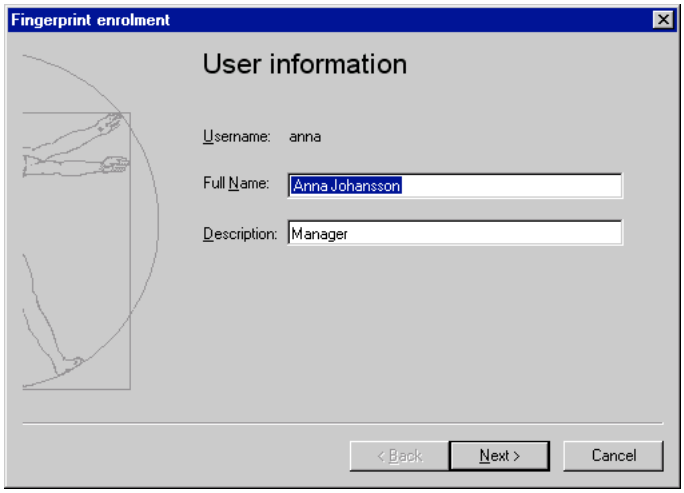
- Full name
- Description
- Register fingerprints
- Primary logon finger
- Possibility to log on using a password

1. Log on as administrator.

2. Click **Start > Programs > Precise Biometrics > BioManager for Domains**. The BioManager screen appears.



3. Double-click on a username. You can also click on a username and then click **User > Properties**. The User information screen appears.



4. Navigate through the screens using the **Back** and **Next** buttons.

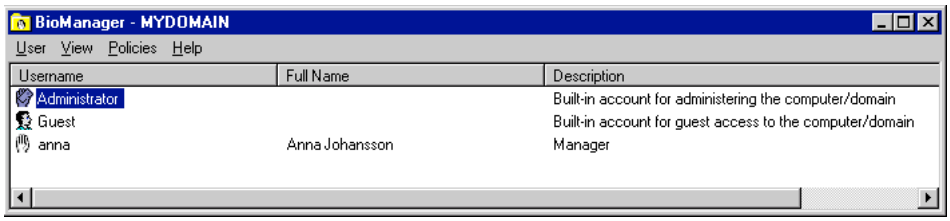
5. Make the desired changes and save the data by clicking **Finish** on the last screen.

See Continue Fingerprint Registration in this chapter for information on how to register fingerprints.

Deleting a User

When a user is removed from the username list, he or she cannot log into the associated account anymore.

1. Click **Start > Programs > Precise Biometrics > BioManager for Domains**.
   The BioManager screen appears.



2. Click on the username that you want to delete from the list.

3. Click **User > Delete**.

4. Click **OK** to delete the user.

5. Click **OK** to confirm operation.

The user is now deleted and can no longer log into the system.

Chapter 6
Logging on

When you have registered your fingerprints, you can log into the system using the fingerprint reader. Fingerprint logon is a very secure and simple way to log on. If you want detailed information on how to place a finger on the fingerprint reader, please see Placing Your Finger Correctly on the Fingerprint Reader in the Using the Fingerprint Reader chapter.

NOTE: In order to log into your domain server account using your fingerprint:

- the Precise 100 A must be installed on your workstation
- your fingerprints must be registered on the **domain server.** See the chapters Personal Enrolment and The BioManager for Domains for more information.

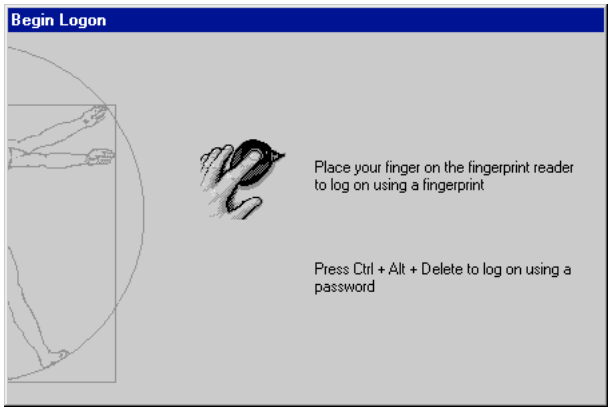
This chapter includes the following information:

- Logging on with fingerprint
- Logging on with a password

Logging on with a Fingerprint

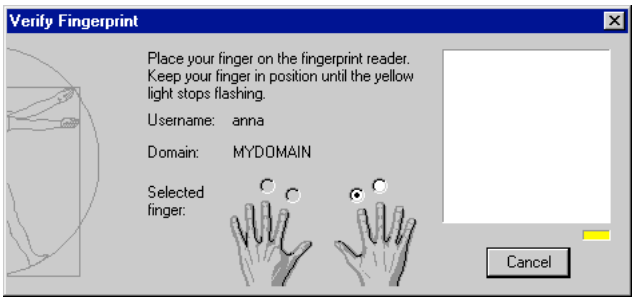
NOTE: You can only log into a domain account using the fingerprint reader once you have enrolled your fingerprints on the domain server. You can only log on with a fingerprint that has been enrolled and stored on the hard disk or on a smart card.

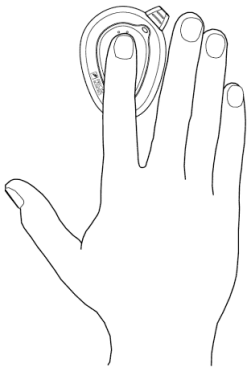
To log on from the Begin Logon screen:



1. Place your primary logon finger on the fingerprint reader sensor.

The Verify Fingerprint screen appears.

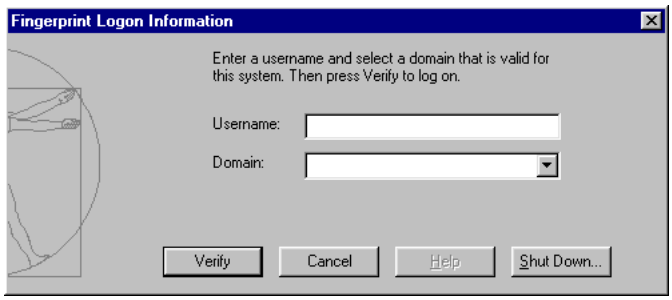




2. Keep your finger placed on the sensor as long as the yellow light is flashing. The system verifies your fingerprint and access rights for the selected domain and displays the Windows desktop.

NOTE: The system will try to identify you as the most recent user. If you are not the most recent user, follow the instructions below:

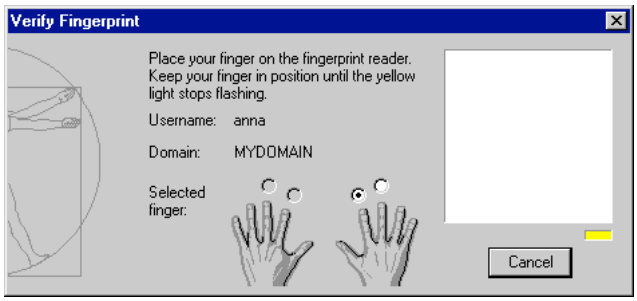
1. Click **Cancel** on the Verify Fingerprint screen.
   The Fingerprint Logon Information screen will appear.



2. Type your username in the **Username** field.

3. Select your domain from the **Domain** pull-down list.

4. Click **Verify**. The Verify Fingerprint screen appears.



5. Place your primary logon finger on the sensor. The yellow light starts flashing.

NOTE: To use another finger on the sensor, select that finger on the Verify Fingerprint screen – assuming that the fingerprint is previously registered.

6. Keep the finger placed on the sensor until the yellow light ceases to flash.

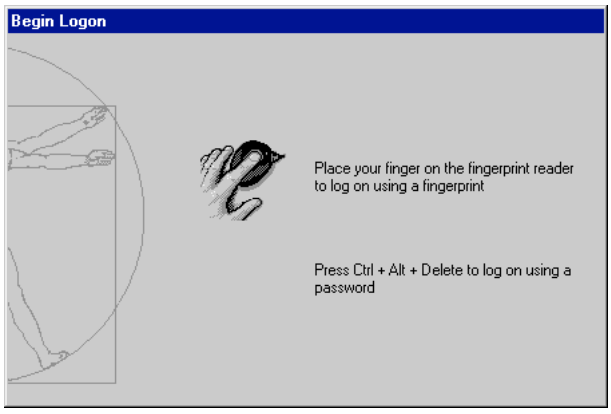
The system verifies your fingerprint and access rights for the selected domain and displays the Windows desktop.

If logon fails, try lifting your finger and putting it back on the sensor again. Try adjusting the position of your finger. If you still can not log on, see Fingerprint Troubleshooting in the Troubleshooting chapter.

Logging on with a Password

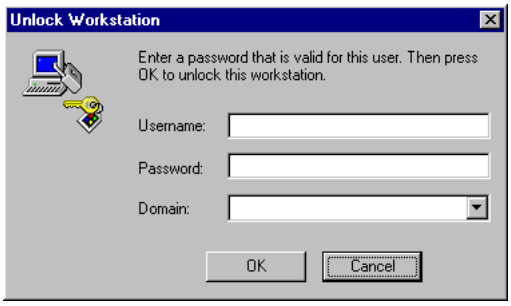
NOTE: You can only log on using a password if you entered a password when you enrolled and registered your fingerprints. See the chapter Personal Enrolment for details. Once your fingerprints have been registered, any previous password vill no longer be valid.

To begin logon from the Begin Logon screen:



1. Press *Ctrl* + *Alt* + *Delete*.

The Logon Information screen appears.



2. Type your username in the **Username** field.

3. Type your password in the **Password** field.

4. Select your domain from the **Domain** pull-down list.

5. Click **OK**.

The system verifies your password and access rights for the selected domain and displays the Windows desktop.

If logon failed, please check the spelling of your username and password.

Chapter 7

Locking and Unlocking

When you leave your workstation temporarily, it is recommended that you lock it to prevent others from using it and accessing your files. The screen saver function can be used to automatically lock the computer. See your Windows documentation for more information about screen savers.

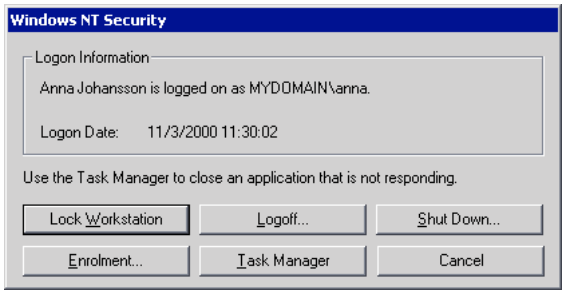
This chapter includes the following information:

- Locking your workstation
- Unlocking your workstation with a fingerprint
- Unlocking your workstation by typing a password

Locking a Workstation

To lock the workstation you are working on:

1. Press *Ctrl* + *Alt* + *Delete*.
   The Windows Security screen appears.



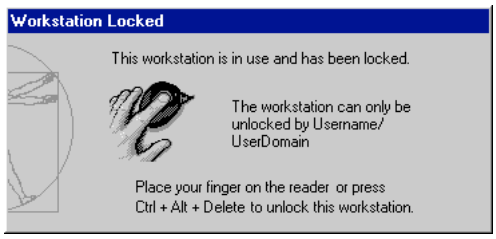
2. Click **Lock Workstation**.

The system locks the workstation. You are the only one who can unlock your workstation. An administrator can log you off.

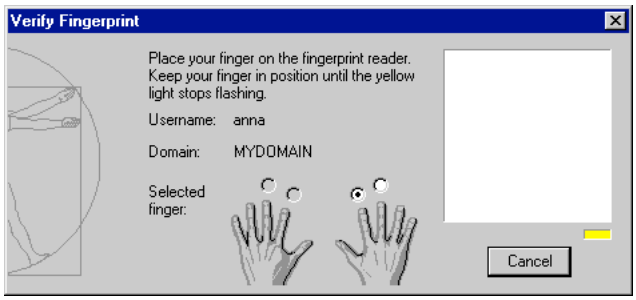
Unlocking a Workstation

Unlocking with a Fingerprint

To unlock a workstation from the Workstation Locked screen:



1. Place your primary logon finger on the fingerprint reader sensor. The Verify Fingerprint screen appears. Your primary logon finger will be selected.



2. Keep your finger placed on the sensor as long as the yellow light is flashing. The system verifies your fingerprint and displays the Windows desktop.

NOTE: To logon with another finger on the sensor, select that finger on the Verify Fingerprint screen – assuming that the fingerprint is previously registered.

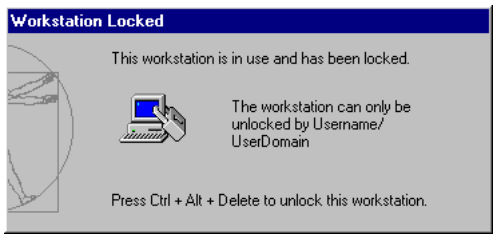
If the unlocking fails, try lifting your finger and putting it back on the sensor again. Try adjusting the position of your finger. If you still can not unlock, see Fingerprint Troubleshooting in the Troubleshooting chapter.

If you have the possibility to use a password, you can press *Ctrl* + *Alt* + *Delete* at the Workstation Locked screen to unlock the workstation using your password.

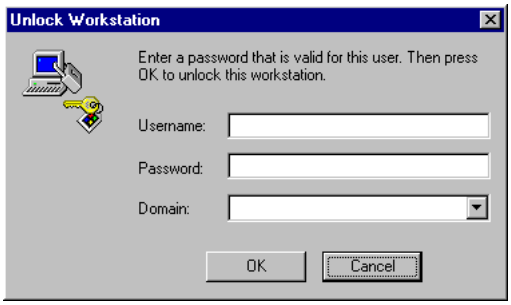
Unlocking with a Password

NOTE: You can only unlock a workstation using a password if you entered a password when you enrolled and registered your fingerprints. See the chapter Personal Enrolment for details.

To unlock a workstation from the Workstation Locked screen:



1. Press *Ctrl* + *Alt* + *Delete*.
   The Unlock Workstation screen appears.



2. Type your password in the **Password** field. Click **OK** and your Windows desktop will be displayed.

If the unlocking fails, please check the spelling of the password.

Chapter 8
Troubleshooting

This chapter includes the following information:

- Fingerprint troubleshooting
- Password troubleshooting

Fingerprint Troubleshooting

If the fingerprint verification fails, the red light on the fingerprint reader is turned on.

- Lift your finger and put it back on the sensor. Try to slightly adjust the positioning of your finger.
- Make sure you placed the right finger on the sensor, i.e. the finger marked with a dot on the Verify Fingerprint screen.
- Try to log on using another registered fingerprint.
- Place your finger flat on the sensor – not rotated in any direction. See Placing Your Finger Correctly on the Fingerprint Reader in the Using the Fingerprint Reader chapter for more information.
- Place the centre of your finger pad in the sensor centre.
- Apply enough pressure – the fingerprint reader must be able to detect the fingerprint contours.
- Your finger must not be wet.
- If your finger pad is too dry try breathing on your finger before verification.
- The sensor must be clean. If necessary, gently wipe the sensor with a soft cotton cloth dampened with a mild ammonia-based cleaner.
- If using the parallel port, the parallel port must be set to ECP mode. See Setting the Parallel Port in the Installation chapter for more information.
- Check that the computer and fingerprint readers are properly connected. See Connecting the Fingerprint Reader in the Installation chapter for more information.

If you are still unable to log on, please contact an administrator:

- You might need to register your troublesome fingerprint one more time, or register a new fingerprint.
- Your user account might have been deleted.

Password Troubleshooting

NOTE: You can only log on using a password if you entered a password when you enrolled and registered your fingerprints. See the chapter Personal Enrolment for details. Once your fingerprints have been registered, any previous password will no longer be valid.

1. Make sure the username, domain and password are valid.

2. Make sure the spelling is correct and that Caps Lock is not active. Windows is case sensitive.

If you are still unable to log on, please contact an administrator. Your user account might have been deleted.

Chapter 9
Uninstalling

Only users with administrator rights can uninstall the Precise Biometrics software.

The consequences of uninstalling are:

1. No user accounts will be affected in any way.
2. Users without a backup password will have to get a password to access their user account. The password used before biometric conversion is no longer valid.
3. Backup passwords registered in the BioManager can be used as standard Windows passwords.
4. If the precise 100 A is reinstalled, the biometric user accounts can be accessed as before.

NOTE: The installed Precise 100 Logon 2.1 software is good for use with both Precise 100 A and Precise 100 SC fingerprint readers. If the system is changed from Precise 100 A to Precise 100 SC, the existing software should not be uninstalled.

Uninstalling the Precise 100 Logon 2.1 Software on Windows NT

1. Click **Start > Settings > Control Panel**.
   The Control Panel screen appears.
2. Double-click **Add/Remove** Programs.
   The Add/Remove Programs Properties screen appears.
3. Click **Precise 100 Logon**.
4. Click **Add/Remove**...
5. Follow the instructions in the wizard, selecting **Remove** on the **Program Maintenance** page.
6. Click **Yes** to restart the computer

The Precise 100 Logon 2.1 software is uninstalled.

Uninstalling the Precise 100 Logon 2.1 Software on Windows 2000

1. Click **Start > Settings > Control Panel**.
   The Control Panel screen appears.
2. Double-click **Add/Remove Programs**.
   The Add/Remove Programs screen appears.
3. Click **Precise 100 Logon**.
4. Click **Remove**.
5. Confirm by clicking **Yes**.
6. Click **Yes** to restart the computer.

The Precise 100 Logon 2.1 software is uninstalled.

Uninstalling the Precise 100 Parallel Drivers

1. Double-click **uninstall.exe**. This program can be found in the directory **../Program Files/Precise Biometrics/Parallel Drivers**.
2. Restart the computer.

The Parallel drivers are uninstalled.

Glossary

Biometric
A biometric is a measurable, unique, physical characteristic. For example, the patterns on your retinas and your fingerprints are biometrics.

Biometric/Non-Biometric User
There are two types of user. A biometric user is a user who has been enrolled into the system and who can log on using fingerprints. A non-biometric user is a user who has not been enrolled into the system and can not use fingerprint logon.

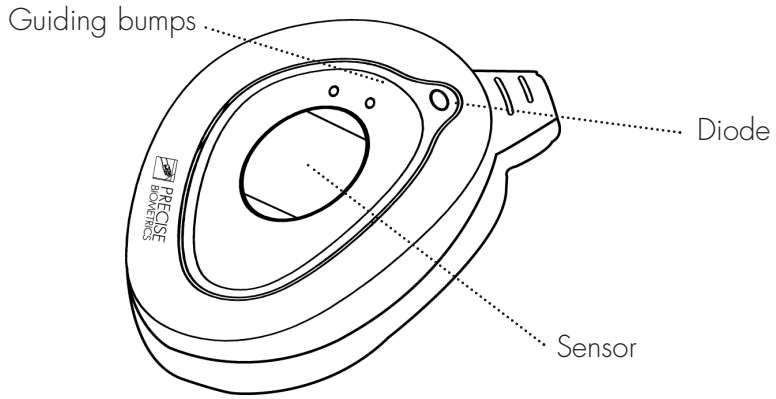
ECP/Enhanced Capabilities Port
The Precise 100 A PAR and Precise 100 SC PAR readers communicates with the computer via the computer's parallel port. To make the fingerprint reader and computer communicate properly via the parallel port, the parallel port must be set to a mode called ECP – Enhanced Capabilities Port. Most new computers are set to ECP by default, but not all. See the Installation chapter for details. This does not apply for USB readers.

Enrolment
The process of registering your fingerprints is sometimes referred to as enrolment, as you are enrolled into the system as a biometric user. See Registration for more details.

Finger Pad
The finger pad is the part of your finger containing the fingerprint. If you take a closer look on your finger pad, you will find that most of the information in the fingerprint comes from the middle of the finger pad. That is the part, which should be placed in the middle of the sensor when you register or log on.

Fingerprint Reader

The fingerprint reader is used to read a finger placed on the sensor. The sensor measures the capacitance of the finger pad, which reveals the pattern of the fingerprint. Thus, a paper copy with a picture of a fingerprint can not grant access to the system.



The fingerprint reader is used both to enrol a fingerprint to store it in a database, and to verify a fingerprint during logon.

Fingerprint Registration

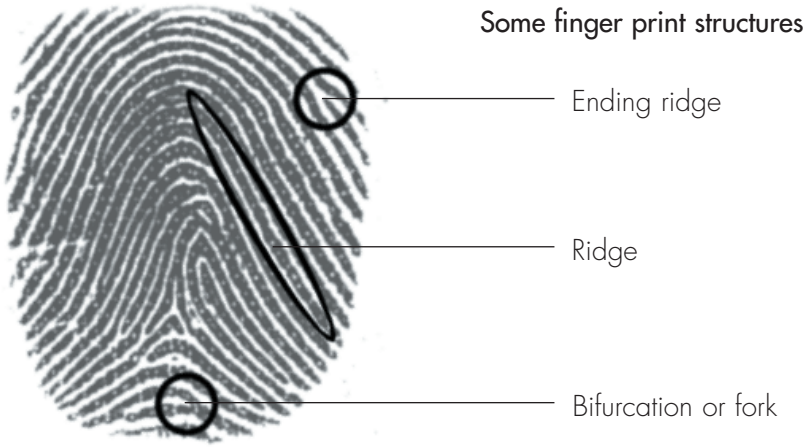
See **Registration**

Fingerprint Template

A fingerprint template is a data file containing information about the fingerprint. The fingerprint template is a set of characteristics which are unique for one specific fingerprint and is not an image of your fingerprint. Your actual fingerprints cannot be recreated using the data from the fingerprint template.

Fingerprints

Your fingerprint can be described as a pattern of lines or ridges with valleys in between. The lines form specific patterns that are observable to the naked eye. Loops, arches and whirls are examples of patterns found in a fingerprint.



The fingerprints also include so-called minutiae points. Minutiae points are the points, where a ridge begins, ends or splits. Precise Biometrics' system identifies a person by looking at loops, arches, whirls and minutiae points, and by measuring global features such as line thickness and curve. These features make every fingerprint unique.

Plug-n-Play

Plug and Play is a technology that supports automatic configuration of PC hardware and external devices. A user can just attach a new device such as sound card or peripheral devices ("plug it in") and start working ("begin playing") without having to configure the device manually. Plug and Play technology is implemented in hardware, in operating systems, and in supporting software such as drivers and BIOS.

Primary Logon finger

The primary logon finger is the finger normally used when logging into the system. The system assumes that you place your selected primary logon finger on the fingerprint reader when you log on or unlock a workstation. The fingerprint on the sensor is then compared to the primary logon fingerprint template in the database. For example, if your right index finger has been selected as the primary logon finger, the right index finger is marked on the Verify Fingerprint screen, which appears when you log on or unlock a workstation.

Reader

See **Fingerprint Reader**

Registration

When you are enrolled into the fingerprint database system, your fingerprints will be registered. You will have to place each finger pad on the fingerprint reader sensor four times. The best image will be saved in a database. Registered fingerprints are used when you log into the system. For example, if your right index finger has been registered, you can place your right finger on the fingerprint reader sensor to verify your identity when you log on. The fingerprint on the sensor will be compared to the registered fingerprint. If your fingerprint on the sensor matches the fingerprint in the database, you are granted access to the system.

Sensor
The sensor is the black window on the fingerprint reader. The sensor is used to read your fingerprint. Do not "roll" your finger pad when you log on or register a fingerprint. Just press it flat to the sensor.

Template
See Fingerprint Template

Verification
When you register a fingerprint, log on or unlock a system, your fingerprint is verified. During verification, the finger on the sensor is compared to a template of a registered fingerprint from the fingerprint database. In other words, you verify that you indeed are who you claim you are and that the fingerprint on the sensor matches the fingerprint template in the database.