Cross Match Technologies, Inc

Verifier E

Administrator's Manual

Version 3.1

Third Edition (October 2003)

Please refer to:
http://www.crossmatch.com/support_software.html
for a list of software license declarations.

Table of Contents

List of Figures

Conventions

Bold UPPER/lower Case indicates function buttons to select.

Italic indicates functions or menu items.

Throughout this manual are boxes that contain notices and warnings. They are defined as follows:


NOTICE
Used to make a procedure easier. To disregard this notice may cause inconvenience, but not mechanical damage or personal injury.


CAUTION
Used to prevent equipment damage or data loss. To disregard the caution may cause mechanical damage or data loss; however, personal injury is not likely.


WARNING
Used when an action or circumstance may potentially cause injury or loss of life. Mechanical damage may also result.


DANGER
Used whenever an action or circumstance is likely to or will cause injury or loss of life. Mechanical damage may also result.

1 Introduction

Congratulations on your purchase of the Verifier™ E fingerprint verifying device. Before you install and operate this device, please read the warranty information in Chapter 12 of this manual.

The Administrator's Manual is a procedural guide intended to assist Administrators in setting up and operating Verifier E.

Cross Match Technologies, Inc. is a premier designer and manufacturer of durable fingerprint readers that output high-definition, forensic-quality and distortion-free fingerprint images.

1.1 The Verifier E

The Cross Match Verifier E is the latest technology in fingerprint readers. The Verifier E is the most sophisticated, durable high-quality fingerprint reader in the marketplace today.

Designed to fit on a desktop, its rugged construction makes it ideal for a large daily volume of trouble-free enrollments, verifications and identifications. The Verifier E connects to existing Ethernet networks and can be viewed through any web-browser software or custom applications using standard TCP/IP protocol. The device comes standard with Finger Detection that detects that a finger is present, analyzes ridge counts and captures the print in a fraction of a second automatically. The unit is also equipped with a platen heater to help prevent halo effects caused by temperature differences between the platen and finger. Cross Match Technologies prides itself on being a leader in the forensic-quality fingerprint scanner marketplace.

Cross Match Technologies is known for superior image quality, consistency from device to device, durability and low maintenance requirements. The Verifier E is built around Cross Match Technologies' forensic quality images. The Verifier series is ideal for demanding commercial applications such as:

- National ID Programs
- Border Patrol
- Passport Projects
- Jail Systems
- Driver's License Projects
- Social Security Projects

1.2 Features

- Generous Platen Area
- Ethernet Operation
- Finger Detect
- Heated Platen
- Smart Finger Print Recognition
- Web Browser Interface
- ANSI-NIST Compliant
- Rugged, Durable and Portable
- Consistent High-Quality Forensic Flat Finger Images
- Low Maintenance Requirements
- PNG and BMP images (512 x 480)
- Optional use of Silicone Pad

2 System Requirements

2.1 Operating Systems

- Any operating system that supports TCP/IP

2.2 Hardware

- A computer with an Ethernet port is needed to interface with the Verifier E

2.3 Software

- Web Browser
- OPTIONAL: Java (Version 1.3 or higher) runtime environment for “Live Image” display (downloadable, see section 3.5.2 on page 3-11)

2.4 Cable

- A standard Network Ethernet Standard Category 5 -Twisted Pair Cable, either straight-through or crossover. The cable is required but not supplied. See Chapter 9 for ordering information.

3 Operation

This chapter outlines the steps necessary for the proper installation and operation of the Verifier E fingerprint verifier.

3.1 Packing List

Item	Part Number
Verifier E	900085
Power adapter (120 VAC to 12VDC, 800 mA)	113001
OR	
Power adapter (Universal Switcher 90VAC-260VAC to regulated 15VDC@ 1A).	113003
Silicone Pad Demo Kit	800436
Operator's Manual	870061

Parts of the Verifier E

3.1.1 Top of Verifier E

Figure 1 - Top of Verifier E

The top of the Verifier E contains a status light and a finger detector.

- Status light – Flashes red every few seconds during "idle" conditions and has a solid green illumination during image capture
- Finger detector – Senses when a finger is placed on the platen.

3.1.2 Bottom of Verifier E

The bottom of the Verifier E contains a label with information on Part Number, Serial Number, Manufacture Date, UL Listing, FCC compliance and CE Compliance. See Figure 2 for a representation of the label.

Figure 2 - Bottom of Verifier E

3.1.3 Back of Verifier E

The back of the Verifier E has four connectors:

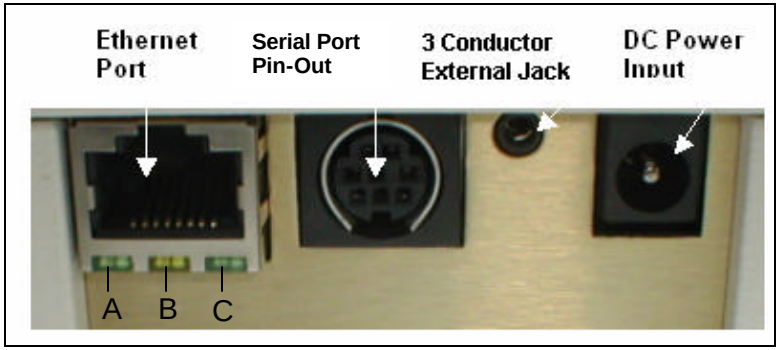


Figure 3 – Connectors

1. **The Ethernet Port with three LEDs** - The Ethernet port connects the Verifier E to a hub connected to a Network.

Light	Color	Significance
A. Link LED	Green	Connected properly, the link is good
B. Speed LED	Yellow	Off - 10 Megabits per second (Mbps) On - 100 Mbps
C. Activity LED	Green	Lets you know when there is activity

2. **Serial Port Pin-Out** - The serial port on the back of the Verifier E device is available through an 8-pin DIN connector. The serial port uses three of these pins for Ground, Transmit, and Receive. No handshake lines are available so handshaking should be disabled in your application. A standard PC serial port has Receive (data in) on pin-2, Transmit (data out) on pin-3 and Ground on pin-5**.** Figure 4 shows the corresponding pins required on the Verifier E DIN connector.

Arrow = direction of data flow to PC Serial port.

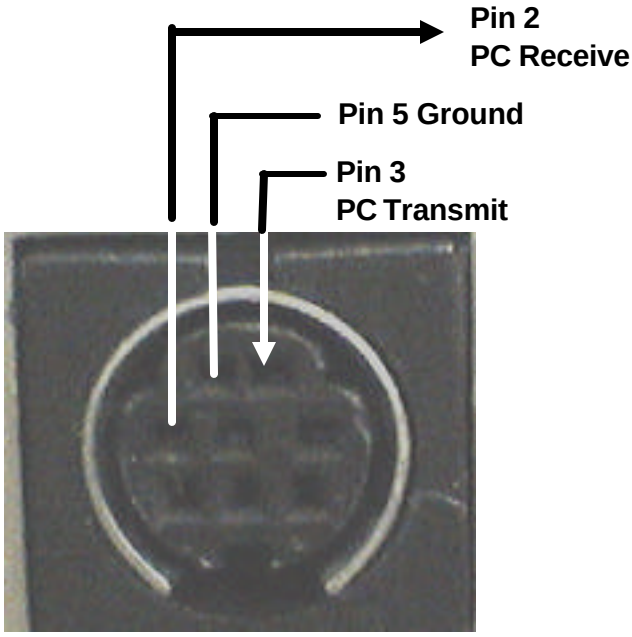


Figure 4 - Serial Port Pin-Out

3. **Three Conductor External Jack** – Is a tripper relay contact, i.e., will open a door.
   - Tip = Normally Closed (NC)
   - Ring = Normally Open (NO)
   - Shield = Common

Output Relay Rating	
Rating	**Value**
Nominal Switching Capacity (resistive load)	1A @ 30VDC
Max. Switching Power (resistive load)	30W

4. **DC Power Input** – 12 - 15 VDC – Maximum 500 mA.

   This product is intended to be supplied by a Listed Direct Plug-In Power Unit marked "Class 2 or LPS" and rated from 12-15 VDC and at least 800 mA.

3.2 Connecting to a Computer

The Verifier E needs a functioning TCP/IP network connection in order to operate. The Verifier E, as shipped from the factory, is configured to use Dynamic Host Configuration Protocol (DHCP) to obtain all the necessary network settings to function. The Verifier E can also be manually configured using a static IP Address.

3.2.1 DHCP Connection

The default network environment assumes a functioning DHCP server along with a Domain Name System (DNS) server that supports dynamic DNS updates from the DHCP records. The DHCP server supplies the IP address and other network settings to the Verifier E. The DNS server maps names to the IP address to allow the device to be referenced by the name rather than IP address. The dynamic update procedure of the DHCP protocol allows for the device to request a network name that should be used to access this device. The DHCP server will then forward this request to the DNS server which will update the IP – name mapping. The Verifier E, as shipped from the factory,

will request a name based on the serial number listed on the bottom of the device. This can be changed in Network Configuration. See Section 3.8.

1. Connect the Network Ethernet cable to the Verifier E.
2. Connect the DC power cord to the rear of the Verifier E. Plug the power adaptor into an electrical outlet.
3. If connected to a functioning network, in 18-20 seconds a status tone will emit from the Verifier E and the status light will start to blink.

3.2.2 Static Connection

If the TCP/IP network the Verifier E is connected to does not support DHCP/DNS services, it will be necessary to manually configure the network settings for the device.

The easiest way to do this is to take advantage of a static IP address alias that is also programmed into the unit. This address is 169.254.5.33. This address is in a range of private network addresses set aside for Automatic Private IP Addressing (APIPA).

With APIPA, DHCP clients can automatically self-configure an IP address and subnet masks when a DHCP server is not available. Computers running Microsoft® Windows® (Windows 98® and above) support this feature automatically.

The easiest way to manually configure the network settings is:

1. Configure another computer to operate on this private network.
2. Connect the computer and the Verifier E, to each other (i.e., a single cable between the two).

3. If the computer is running Microsoft Windows 98 or later, and it is configured for DHCP operation itself, it will try to obtain an IP address from the DHCP server. Since there is no DHCP server (it is only connected to the Verifier E), it will eventually time out and assign itself an address from the range for APIPA as described above. This will allow communications with the Verifier E by specifying the IP address alias of the Verifier E directly from the web browser (http://169.254.5.33) for further configuration as described in section 3.8.
4. If another operating system is used that does not support APIPA, then it will be necessary to configure a computer with the following static IP address information:
    - IP Address: 169.254.5.30
    - Subnet Mask: 255.255.0.0
    - Broadcast Address: 169.254.5.255
    - Network Address: 169.254.5.0
    - Gateway: 169.254.5.1

5. The computer and the Verifier E are then connected directly to each other where further configuration of the Verifier E can take place via the 169.254.5.33 IP address.

NOTICE

If the Verifier E and the computer are configured for DHCP operation (the default for both), but there is no DHCP server present, it will take some time before both devices time-out and give up on finding a DHCP server. For the Verifier E this time-out value is 60-seconds. On the Verifier E it is possible to know when this time-out period ends by waiting to access the device until the start-up tones are heard.

3.3 Device Communication

Go to http:// 300E-XXXXXXX (X being the serial number listed on the bottom of the Verifier E).

3.4 Operations from the Network

All operations for the Verifier E are performed from the Network Graphical User Interface (GUI).

Figure 5 - Main GUI Page

3.5 Auto-Refresh Display

This will enable the display to refresh every second.

NOTICE
If using Windows Explorer, Version 5.5 or above is required.

3.5.1 Live Image Display

NOTICE
Requires Java 1.3.0 or higher. See section 3.5.2

1. Place the subject's finger on the platen on the front of the Verifier E. The LEDs under the platen will illuminate, a beeping tone will emit and the status light will turn green.

2. The fingerprint image will display. There will be a message indicating if it is a new picture or if it is idle.

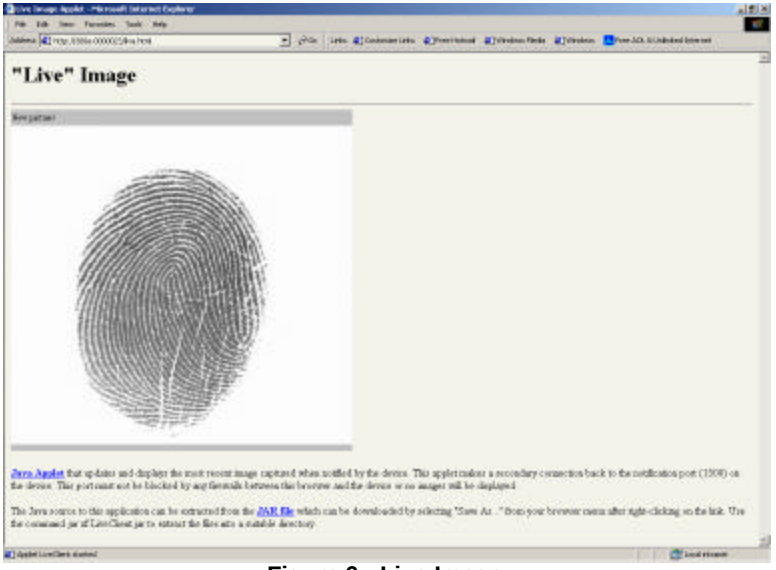


Figure 6 - Live Image

A Java Applet updates and displays the most recent image captured when notified by the device. This applet makes a secondary connection back to the notification port (1500) on the device. This port must not be blocked by firewalls between the browser and the device or the images will not display.

The Java source to this application can be extracted from the Java Archive (JAR file) which can be downloaded by selecting "Save As" from your browser menu after right-clicking on the link. Use the command "*jar xf LiveClient.jar*" to extract the files into a suitable directory.

3.5.2 Installing Java

Installing Java™ J2SE is optional and only required to support the "Live Image" display operation.

1. Go to http://java.sun.com/
2. Click Downloads.
3. Click J2SE under Technologies.
4. Click J2SE Downloads.
5. Click JS2SE 1.3.0 (or the most current version).
6. Choose the download under JRE for the appropriate operating system.

3.5.3 Output Relay Control

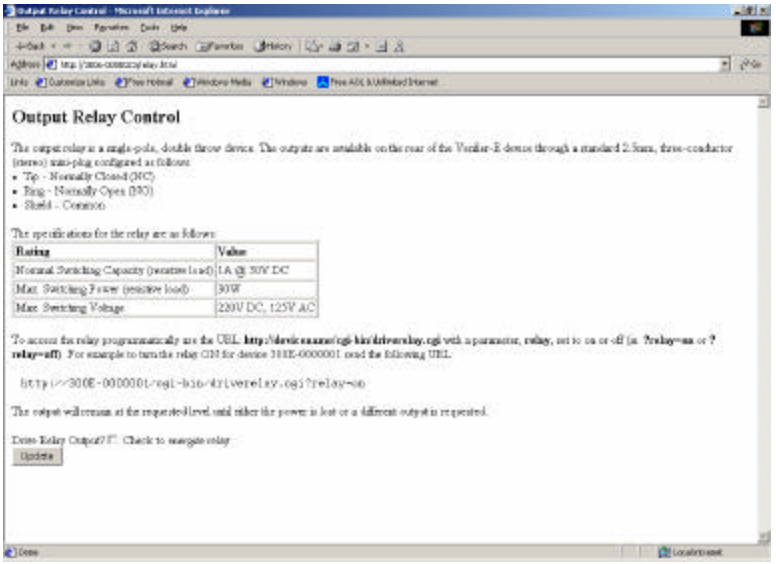


Figure 7 - Output Relay Control

The output relay is a single-pole, double throw device. The outputs are available on the rear of the Verifier-E device through a standard 2.5mm, three-conductor (stereo) mini-plug configured as follows:

- Tip - Normally Closed (NC)
- Ring - Normally Open (NO)
- Shield - Common

The specifications for the relay are as follows:

Output Relay Rating	
Rating	**Value**
Nominal Switching Capacity (resistive load)	1A @ 30V DC
Max. Switching Power (resistive load)	30W

To access the relay programmatically use the URL: **http://devicename/cgi-bin/driverelay.cgi** with a parameter, **relay**, set to on or off (such as **?relay=on** or **?relay=off**).

Example: to turn the relay ON for device 300E-0000001 send the following URL:

http://300E-0000001/cgi-bin/driverelay.cgi?relay=on

3.5.4 Return BMP Image to You

Save bitmap (BMP) must be enabled (see Section 3.7.1.2) for this function.

1. Click the "**Return BMP image to you"** button. The image in bitmap format will display.

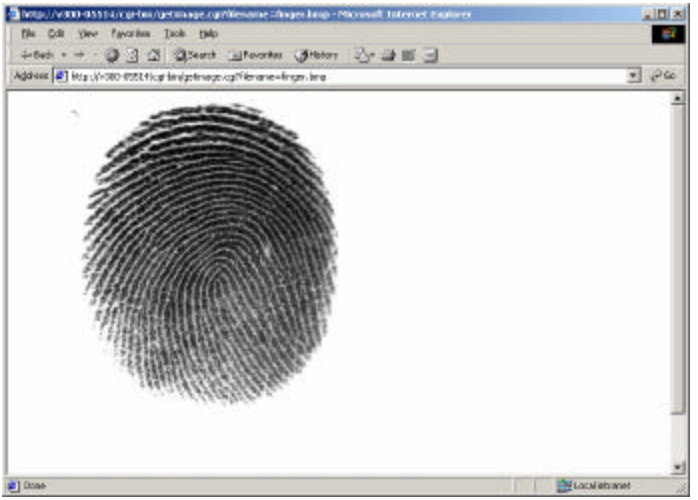


Figure 8 - Return BMP Image

NOTICE

BMP sizes are 512W x 480H.

3.5.5 Return PNG Images to You

Save Portable Network Graphics (PNG) must be enabled (see Section 3.7.1.2) for this function.

1. Click the "**Return PNG image to you"** button. The image in Portable Network Graphics format will display.

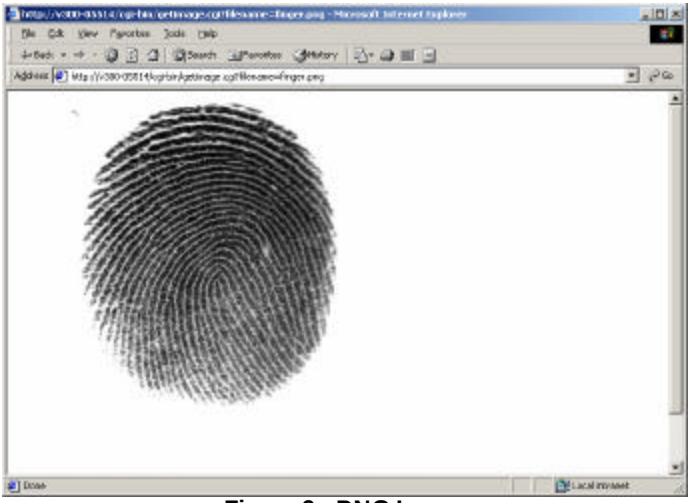


Figure 9 - PNG Image

NOTICE
PNG sizes are 512W x 480H.

3.6 Configure Device

The Verifier E is flexible enough to be configured for your own specifications to suit your specific needs and for ease of use. This section is under a security area that needs a password for entry.

1. Click **Configure Device** to access the Configure Device menu. This feature will need a password for entry. The Security Device Access window will display:

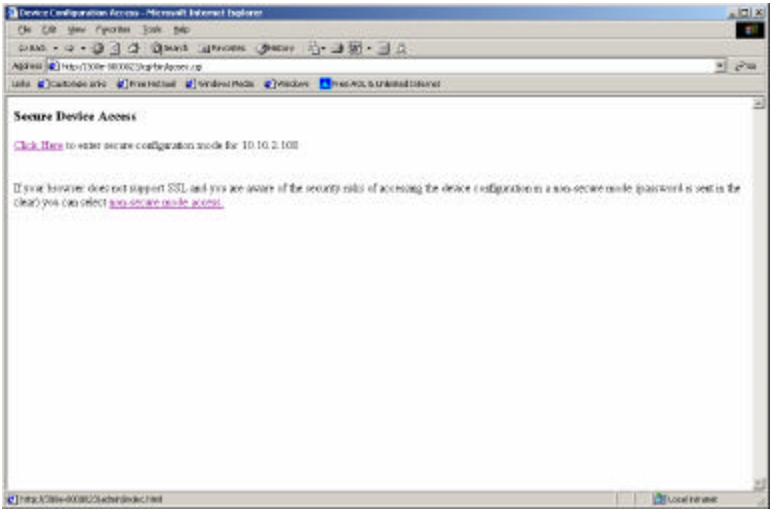


Figure 10 - Secure Device Access

2. Click **Click Here**. The Security Alert window will display. OR, if your browser does not support SSL and you are aware of security risks, click **non-secure mode access**.

Figure 11 - Security Alert

3. Click **Yes** to proceed. The Enter Network Password window will display.

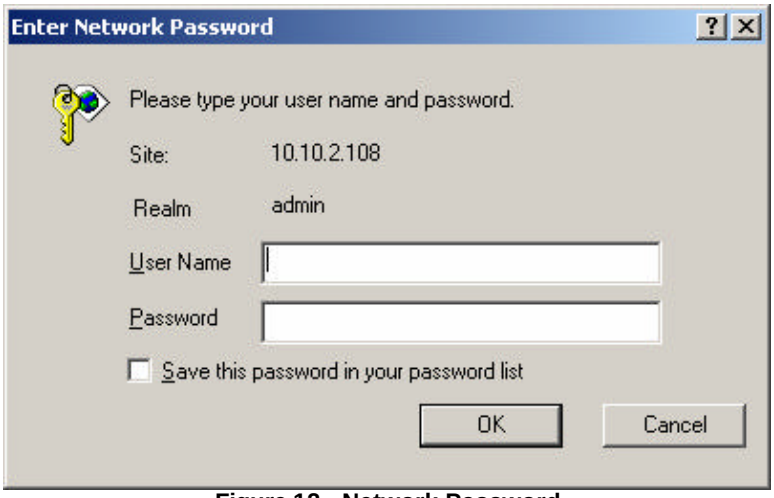


Figure 12 - Network Password

4. Type your user name in the User Name field and your password in the Password field. The default settings are:

   - User Name: admin
   - Password: nimda

5. If you wish to save this user name and password, click the check box next to *Save this password in your password list*.

6. Click **OK**. The device configuration window will display.


NOTICE

It is recommended that the Administrator change the default password.

3.7 Configuring the Verifier E

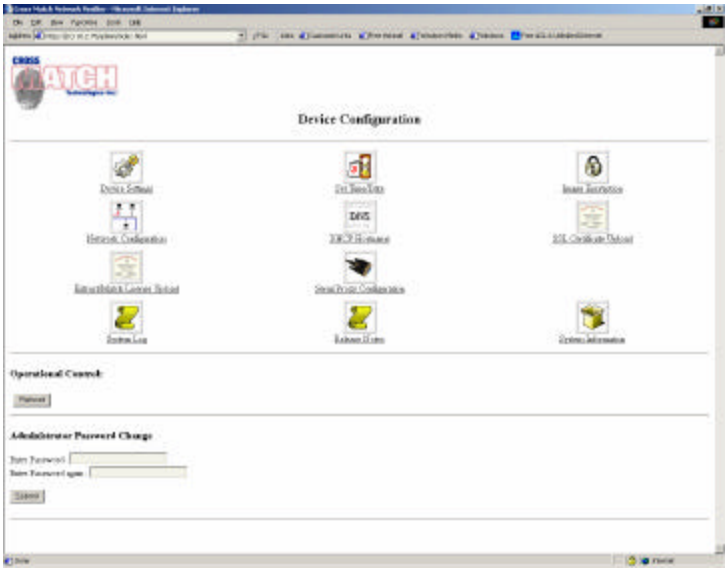


Figure 13 - Device Configuration

NOTICE
All settings are set to default configurations.

NOTICE
It is recommended that the Administrator change the default password. This password should be kept in a safe place.

3.7.1 Device Settings


NOTICE

A check in a check box ☑ indicates a procedure that is enabled

A check box ☐ that is blank indicates a procedure that is disabled.

3.7.1.1 User Interface (UI)

☑ Sound alert on Good fingerprint scan

☑ Sound alert on Bad fingerprint scan

☑ Play Sound at Startup

3.7.1.2 Camera

10 The number of fingerprint ridges required before a fingerprint is captured.

10 Bad image count threshold.

0 Contrast (-31-31).

160 Gain (100x) (100-200).

91 Integration time (msec) (20-150).

160 Illumination level (0-255).

☑ Flip image horizontally

☐ Flip image vertically

☐ Invert image

☑ Use Finger Sensor

☑ Save BMP (.bmp bitmap file) Format

☐ Save PNG (Portable Network Graphics) Format

3.7.1.3 Application Interface

1500 Port for Remote Notification.

1501 Port for Remote Configuration.

1. Click **Update** if you have changes and want to save them.
2. Click **Reset** if you want to go back to the current settings.

3.8 Network Configuration

This screen displays the current configuration of your network. If the IP address is DHCP, these values are ignored.

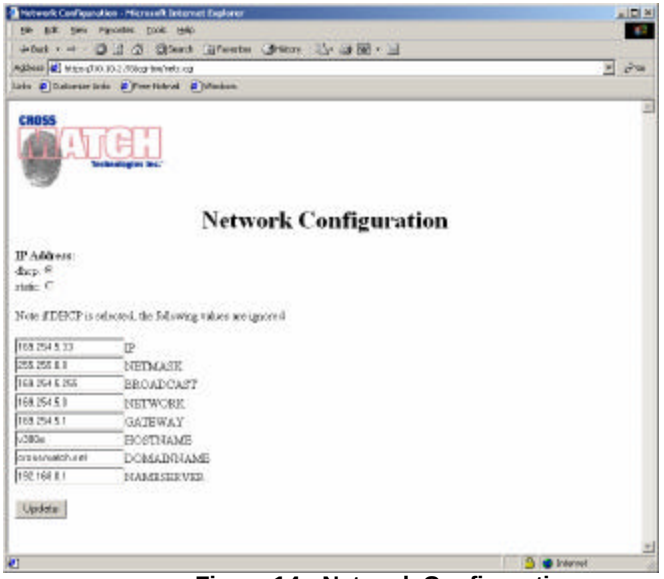


Figure 14 - Network Configuration

1. If the IP Address is static, all values must be input.
2. Click **Update** when the input is complete.

3.8.1 Extract and Match License Upload

The Extract and Match license is used to verify that this unit has been enabled for use with the Cross Match Extract and Match software. This software is optional and is delivered separately from the device. For further information on the Extract and Match software please consult with your Cross Match Technologies salesperson.

The license file that is delivered from Cross Match for uploading with this utility is matched to the serial number of the device and will only work with that device. Please make sure that the license file you are using matches the serial number of the unit you are updating. The serial number can be found on the label on the bottom on the unit.

If the unit was ordered with this capability from the factory, a valid license file will already be in place. Uploading a license file should only be required if the unit is being upgraded to enable this feature.

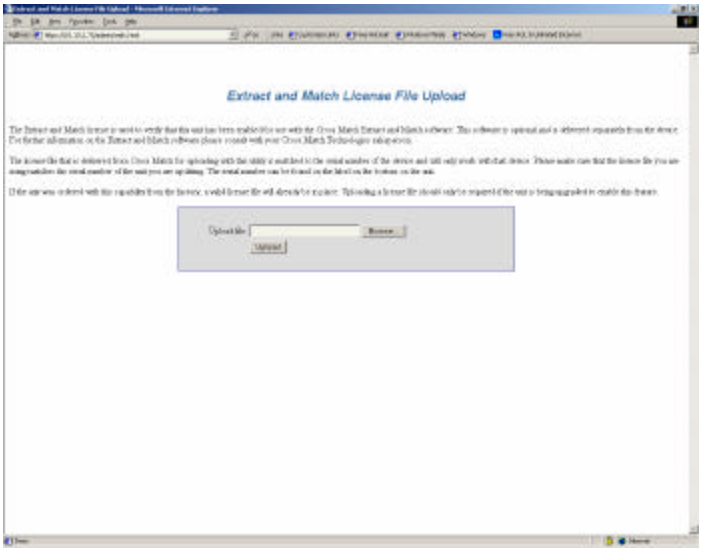


Figure 15 - Extract and Match License Upload

3.8.2 System Log

This screen displays a log of events for the current day.

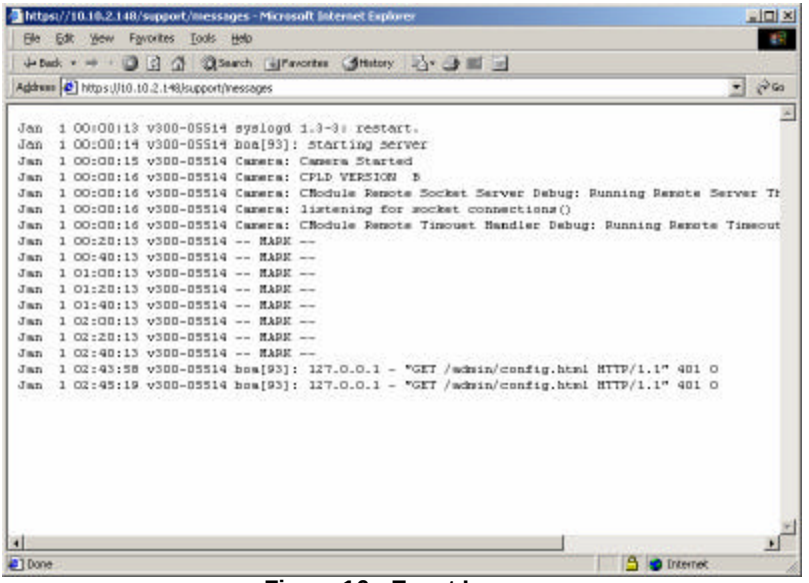


Figure 16 - Event Log

3.8.3 Set Date/Time

Set the time and date according to Coordinated Universal Time (UTC).

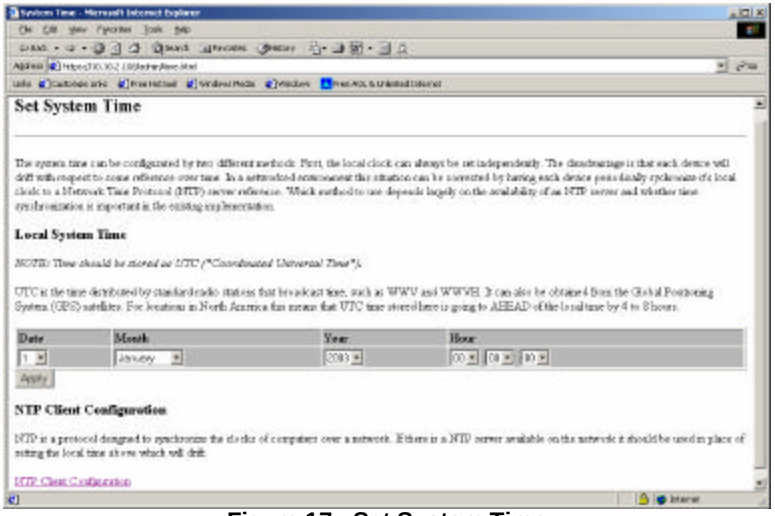


Figure 17 - Set System Time

3.8.3.1 NTP Client Configuration

Configures the optional network time protocol (NTP) support.

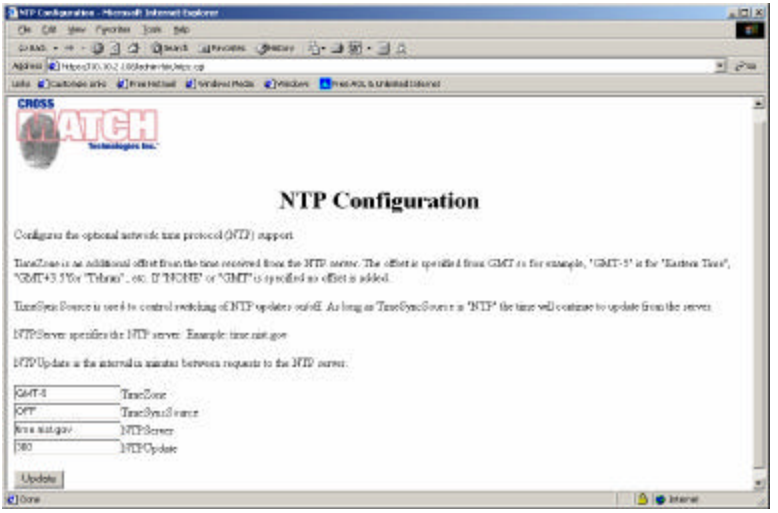


Figure 18 - NTP Configuration

TimeZone is an additional offset from the time received from the NTP server. The offset is specified from GMT so for example, "GMT-5" is for "Eastern Time", "GMT+3.5"for "Tehran" , etc. If "NONE" or "GMT" is specified no offset is added.

TimeSyncSource is used to control switching of NTP updates on/off. As long as TimeSyncSource is "NTP" the time will continue to update from the server.

NTPServer specifies the NTP server. Example: time.nist.gov

NTPUpdate is the interval in minutes between requests to the NTP server.

3.8.4 DHCP Hostname

This device supports DHCP. DHCP is a client-server protocol that allows devices on an IP network (the DHCP clients) to request configuration information from a DHCP server. DHCP allocates network addresses from a central pool on an as-needed basis. You can specify the hostname the device should request during DHCP configuration. This allows an application to refer to this device by name rather than IP address.

NOTICE

Please note that not all DHCP servers support dynamic updates of the DNS tables. Consult your system administrator for further information.

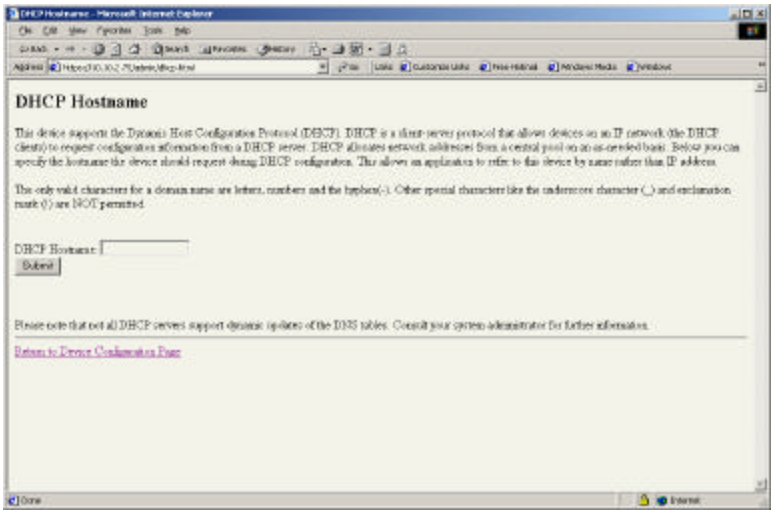


Figure 19 - DHCP Hostname

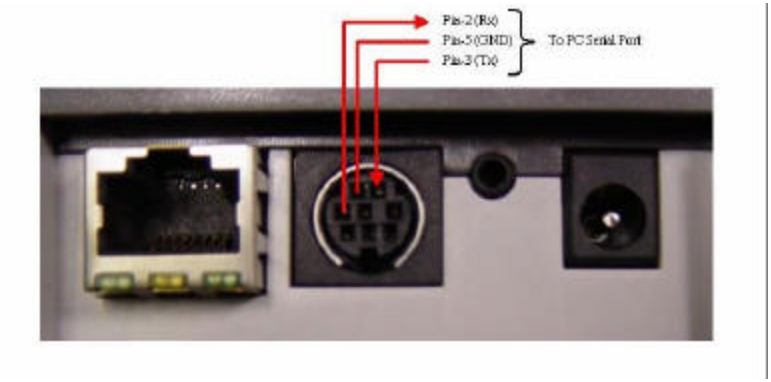
3.8.5 Serial Proxy Configuration

The Serial Proxy service allows for redirecting a network socket connection to/from the RS-232 serial port on the rear of the device. The proxy service listens for incoming network connections on the port specified below and proxies the data to and from the serial port configured according to the settings below.

You can easily test this by connecting the serial I/O lines to a computer serial port, running a terminal program to use that serial port (e.g. HyperTerm, minicom, etc.) and then opening a Telnet connection to the port specified below (such as "$ telnet 300E-xxxx 5334"). Now, any data you type in the serial terminal will show up in the Telnet window and vice versa.

The serial port on the back of the Verifier-E device is available through an 8-pin DIN connector. The serial port uses three of these pins for Transmit, Receive, and Ground. No handshake lines are available and flow control should be disabled in your application.

A standard RS-232 serial port has Receive (data-in) on pin-2, Transmit (data-out) on pin-3, and Ground on pin-5. The following diagram shows the corresponding pins on the Verifier-E DIN connector:



Baud Rate:

1200: ○

2400: ○

4800: ○

9600: ○

19200: ◉

38400: ○

57600: ○

115200: ○

Number of Data Bits:

5:

6:

7:

8:

Number of Stop Bits:

1:

2:

Parity:

none:

even:

odd:

300 Client Timeout (secs)

5334 Proxy Port Number (default is 5334)

Update

3.9 Release Notes

Indicates the releases and builds of the software for the Verifier E.

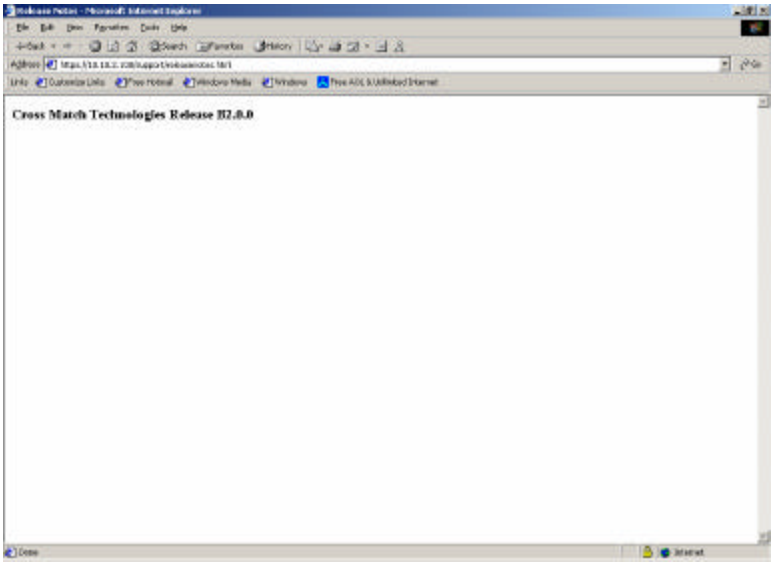


Figure 20 - Release Notes

3.9.1 Image Encryption

This is the key used to perform the optional encryption of the image when requested from the device. Encryption is performed using 128-bit RC4.

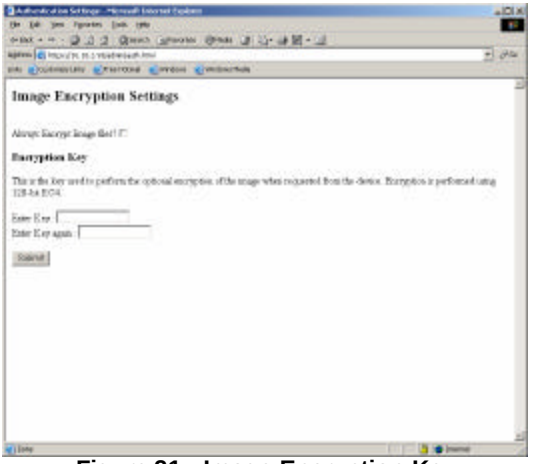


Figure 21 - Image Encryption Key

1. Enable the check box if you want to always encrypt image files.

2. Enter the key used to perform the optional encryption of the image when requested from the device. Encryption is performed using 128-bit RC4.

3. Reenter the key.

4. Click **Submit** to submit your entry.

3.9.2 SSL Certificate Upload

The Secure Sockets Layer (SSL) certificate is used to secure communications between a client and this device. The SSL certificate is a digital document that has a unique code to identify the holder of the certificate to the system accessing this device.

Certificates are available in a number of different file formats. The Verifier E requires files in Privacy Enhanced Mail (PEM) format. If your certificate is not in PEM format, then it must be converted before uploading to this device. There are a number of utilities available on the Internet for converting certificates between various formats.

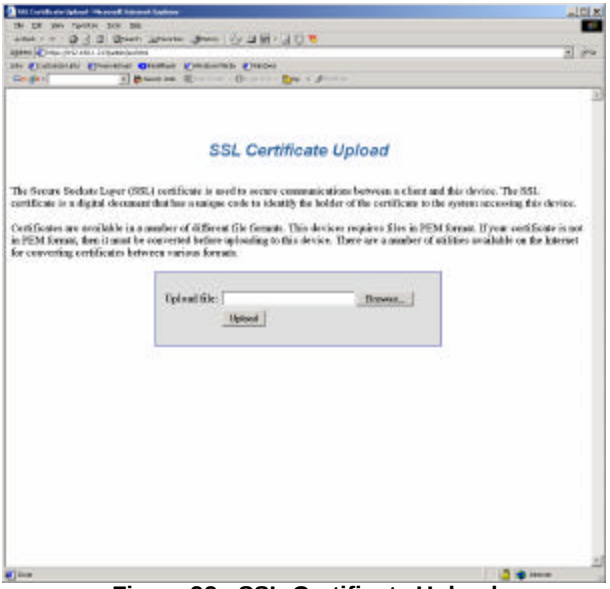


Figure 22 - SSL Certificate Upload

3.9.3 System Information

Information is given on Hardware Identification, Brand, Date, MAC Address, Serial Number and Part Number.

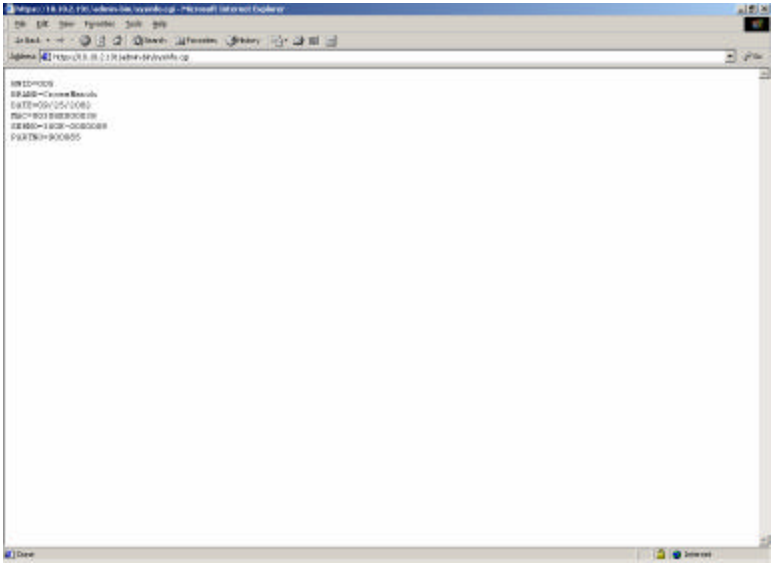


Figure 23 - System Information

3.9.4 Operational Control

In event the Verifier E needs to be rebooted, Click **Reboot**. A reboot would be necessary if changes were made that affected the current operation of the device, such as changing the network settings.

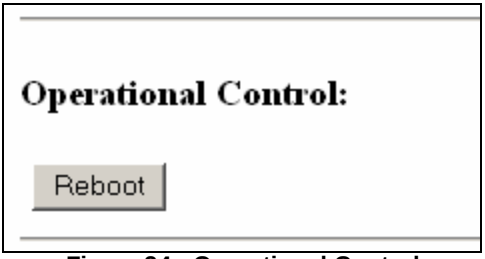


Figure 24 - Operational Control

3.9.5 Administrator's Password Change

1. Enter the password in the *Enter Password* field.
2. Re-enter the current password in the *Enter Password Again* field.
3. Click **Submit**.

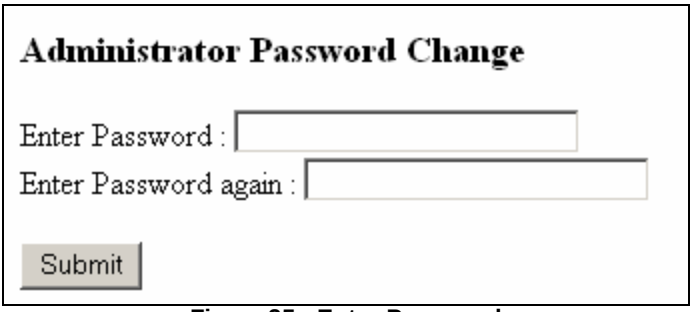


Figure 25 - Enter Password


NOTICE
It is recommended that the Administrator change the password.

3.10 Help

This section displays help given for configuration of the Verifier E.

3.10.1 Overview

All device communication takes place using standard TCP/IP protocols over ports 80 (HTTP), 443 (HTTPS), and 1500 (Notification Port). Configuration and image retrieval are performed using standard HTTP or if encrypted communications are required, HTTPS.

For further information on HTTP consult the HTTP Protocol Description.

3.10.2 Image Retrieval

Image retrieval is accomplished via standard HTTP using the URL:
http://devicename/cgi-bin/getimage.cgi.


NOTICE
A fingerprint image is not stored on the device indefinitely. After approximately 10 seconds the last image that was captured will be removed.

3.10.3 Encryption (Optional)

The device supports two different modes of data encryption: HTTPS and image encryption.
HTTPS uses Secure Sockets Layer (SSL) for encryption. SSL, in turn, requires that a suitable certificate be installed on the device. In order to simplify device management, all verifier devices are shipped with and share a common certificate rather than being locked to the particular device name or IP address as is normally required. In practice, this means that SSL access will require special handling in order to allow encrypted communications to proceed. If using a browser, a warning box is normally displayed saying in effect that the name does not match the certificate. By accepting this warning and continuing, encrypted communications will still take place and all data will be secure.

Image encryption only is also available as an alternate method of encrypting just the fingerprint image files during communications. This method does not have the overhead of setting up an SSL connection each time data is to be transferred. This method is normally disabled and must be enabled via the "Image Encryption" link on the "Device Configuration" page. Images are encrypted with a shared-secret using 128-bit RC4 encryption. The shared-secret is also configured on the "Image Encryption" page.

3.10.4 The Notification Port

The Notification Port allows external applications to monitor and be notified of certain events as they occur on the device. The device will function without using the notification port, but certain operations, such as when a new image is available, will require a continuous connection with the device that is not possible using HTTP.

The notification port uses a very simple ASCII-based protocol running over TCP/IP on port 1500. The protocol consists of the following ASCII text commands:

Commands sent by the Verifier-E:

```
Notify
Idle
```

Commands understood (received) by the Verifier-E:

```
Subscribe
Ack
Suspend
Resume
Quit
```

All commands must be followed by a LF or CR/LF pair to delimit each command.

The procedure for an application is to open a TCP/IP socket to port 1500 and send the following (ASCII Text):

```
Subscribe
```

followed by a LF character.

From this point on the unit will send one of two messages: "Idle" or "Notify". Both messages require an "Ack" reply message to be sent back to the Verifier-E within several seconds or the unit will drop the connection. The "Idle" message is sent approximately every 10 seconds as a hearbeat message.

"Notify" is sent when a new image is available. The new image may be retrieved from the device via the URL described. Again, an "Ack" reply message must be sent for the Notify command but it should be sent AFTER the image has been retrieved (this tells the camera it's OK to take a new picture).

Image acquisition can be application controlled through the use of the "Suspend" and "Resume" commands. These commands may be sent at any time but are only active while the finger sensor is active (i.e., a finger is on the platen). A "Suspend" will cause the Verifier-E to stop updating the image until *EITHER* the finger is removed from the platen *OR* a "Resume" command is received.

The following ladder diagram shows the message flow from host to Verifier E and back for typical operation:

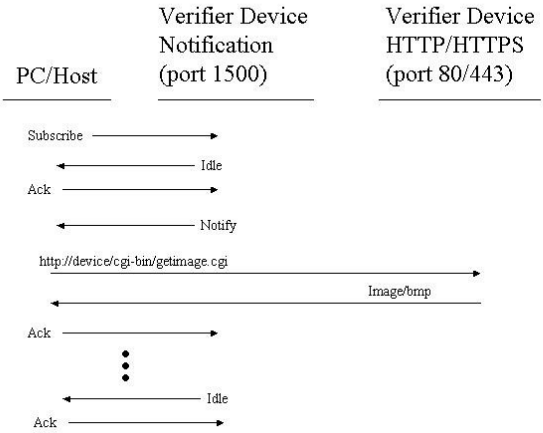


Figure 26 - Message Flow

An application can be simulated using telnet as shown in the following transcript:

```
$ telnet cmec-p6 1500
Trying 192.168.1.218...
Connected to cmec-p6.
Escape character is '^]'.
Subscribe
Idle
```

```
Ack
Idle
Ack
Notify
Ack
Idle
Ack
Notify
Ack
Quit
Connection closed by foreign host.
$
```

Notice that after a "Quit" is received, the unit drops the connection.

3.10.5 Advanced Help

Further information on advanced image control operations can be found in Advanced Control Port Commands.

3.10.6 Advanced Control Port Commands

The device supports a further port, 1501, which can be used to control the image produced by the device if required. Under normal circumstances, these controls are unnecessary as the device has intelligent software that will adjust the settings to obtain a satisfactory image. However, there may be some situations in which it is necessary to adjust the image quality manually.
Like the notification port, the control port uses a standard TCP/IP-based ASCII communications protocol. It is **NOT** necessary to send a "Subscribe" command before using this port. Simply connect, send the data, wait for responses, and finally send "Ack" commands.
The Control command set is:
Commands sent by the Verifier-E:

```
  Idle
```



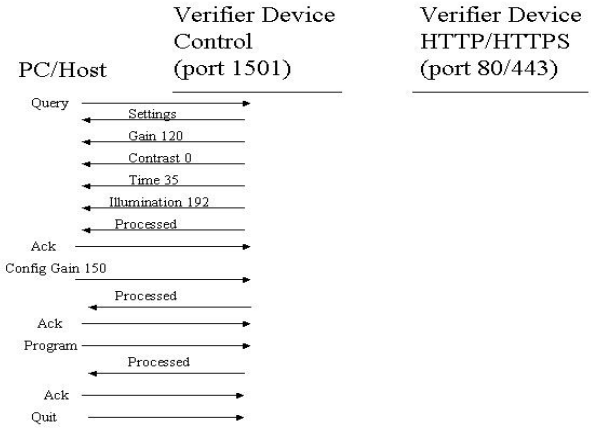
```
  Settings
  Processed
```

Commands understood (received) by the Verifier-E:

```
  Ack
  Query
  Config [Gain|Contrast|Time|Illumination]
value
  Program
  Quit
```

As before, all commands must be followed by a LF or CR/LF pair to delimit each command.

The control commands Query, Config, and Program, are designed to allow an application to adjust the image setting in almost "real time" if required by a particular application. The correct procedure is to issue a "Query" command to get the current settings, change the desired settings with a "Config" command, and then make the new settings take effect with a "Program" command. The device will issue a "Processed" response to each command that must be replied in turn with an "Ack" command. This is illustrated in the following example message flow that shows how the image gain value is changed from 120 to 150.



A Quit command is sent to close the control port connection.

4 Technical Support

During the initial set-up, installation and operation of your Verifier E, you may require some technical assistance. Cross Match Technologies, Inc., committed to quality products and services, provides a variety of sources for technical support.

4.1 Electronic Mail

Free technical support by e-mail is available for the duration of the warranty period and is provided on a first-come, first-serve basis at support@crossmatch.com. Depending on the information requested, you may be directed to call Cross Match Technologies Customer Care for additional assistance. If the warranty has expired, please contact Cross Match Technologies Customer Care by telephone or facsimile.

4.2 Telephone/Facsimile

Free technical support is available through Customer Care via telephone and/or facsimile for the Verifier E under warranty (see page 12-1 for Warranty Terms). After the warranty has expired, technical support will be provided at a specified cost per hour. Contact Customer Care for further information.

Technical support of software products and/or services purchased from Cross Match Technologies, Inc. or of third party products is not covered under warranty and will be provided at a cost to the purchaser.

When contacting Customer Care, please be prepared to provide the following information:

- Company name

- Contact person
- Verifier E serial number (located on the bottom of product)
- Information on the configuration of your PC workstation or laptop
- Error messages appearing on the screen

Cross Match Technologies thanks and congratulates you on your purchase of our fingerprint capture product. Now that your system is installed and operating, if you experience any difficulties or have any questions, Cross Match Technologies **Customer Care is available Monday through Friday from 8:00 to 5:00 EST** at the following toll-free phone number:

1-877-474-0228

At times, we may be assisting other customers and your call may be routed to an automated attendant. Please leave your name, the name of your company and your telephone number and a technician will call you back.

If you are not satisfied with Cross Match's Customer Care, please feel free to escalate the situation to management in the following ways.

Escalation Level 1
Customer Care Manager
E-mail: CustomerServiceManager@CrossMatch.com
Office: (561) 622-3704

Escalation Level 2
Director of Customer Care
E-mail: DirectorCustomerService@CrossMatch.com
Office: (561) 493-7370

Facsimile: (561) 622-9938

5 Maintenance

Routine maintenance procedures will prolong, not only the life of the glass platen that the finger is placed upon, but also the life of the entire product itself. Regular cleaning of the platen and the surrounding metallic fingerplate area should be scheduled once a month. The optional silicone pad should also be inspected.


NOTICE

Although the silicone pad is optional, it is highly recommended to use, as it enhances fingerprint quality.

5.1 Verifier E

5.1.1 Platen (Glass Surface)

Regular cleaning of the platen and the surrounding fingerplate area should be scheduled at least once a month.


NOTICE

Water, 70 - 91% isopropyl alcohol or mixture of water and isopropyl alcohol is acceptable to clean the platen surface. Use the liquids very sparingly so as not to soak the unit.


CAUTION

DO NOT use harsh abrasives or soaps on the platen. This may damage the platen and render the unit inoperable. Utilization of unapproved cleaning solutions will void the warranty.

5.1.2 Fingerplate

The fingerplate is the area around the platen, therefore, keeping it clean protects the platen from dirt and grime. To remove dirt, grime, and oil, take a soft, damp, lint free cloth (i.e., cheesecloth or lens tissue) with a small amount of non-abrasive hand soap and carefully wipe the fingerplate AWAY from the platen area.


NOTICE

DO NOT use harsh abrasives or soaps. This may damage the platen and the barcode scanner window and render the unit inoperable. Utilization of unapproved cleaning solutions will void the warranty.

5.1.3 Case

Maintaining the exterior of the case will ensure product longevity. To clean the case put a small amount of non-abrasive hand soap on a damp, clean, soft towel and rub gently. Be careful to keep the cleaning solution away from the platen and connectors.

5.2 Optional Silicone Pad

5.2.1 Cleaning

1. To properly clean the silicone pad, you will need to assemble the following materials:
   - 70-91% Isopropyl Alcohol Spray
   - Kimwipes®
2. Spray pad sparingly with the Isopropyl alcohol solution.
3. Wipe the silicone pad from top to bottom with a light amount of pressure.

4. Turn the Kimwipe over between wipes or discard and use a new one.


NOTICE

Never rub the pad in a back and forth motion, or apply heavy pressure when cleaning. This may cause the pad to become damaged.

5.2.2 Changing the Optional Silicone Pad

The silicone pads on the finger platen should be changed regularly.

Signs that the silicone pad needs to be changed could be:

- Air bubbles
- Inability to remove streaks from the pad
- Tearing
- Corners peeling up

To properly replace the silicone pad, you will need to assemble the following materials:

- Alcohol Spray
- Kimwipes®
- New silicone pad
- Adhesive tape

5.2.3 Removing an Old Silicone Pad

1. With the edge of your nail, carefully pry up one corner of the used silicone pad. A non-metal object such as a toothpick can also be used.

Figure 27 - Removing Silicone Pad

2. Once the silicone pad has been removed use the alcohol spray to clean the platen. With Kimwipes or a lint-free cloth, wipe off the surface until clean and dry.

5.3 Attaching a New Silicone Pad

There are thin Mylar protective sheets on each side of the silicone pad that MUST be removed.

1. While holding the replacement silicone pad only by the edges, apply adhesive tape to one side of the silicone pad. Pull to remove the Mylar protective sheet.

Figure 28 - Remove Mylar

2. Angle one edge of the pad toward the front of the platen.
3. With the unprotected side down, drop the silicone pad on the platen. It is best to put one end of the silicone pad against the front edge of the platen and let it drop down as shown in Figure 29.

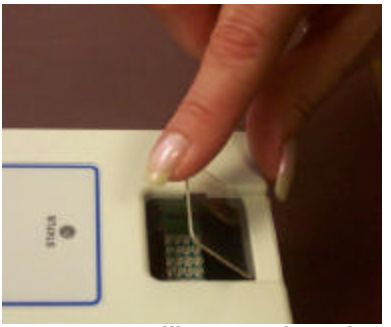


Figure 29 - Drop Silicone Pad on Platen

4. Rub your finger around the silicone pad to remove any air bubbles.
5. Place a piece of adhesive tape on the silicone pad and pull to remove the second Mylar protective sheet.

Figure 30 - Removing the 2nd Mylar

6 Troubleshooting

This section describes some common problems and possible solutions concerning the Verifier E. Please try suggestions below before contacting Cross Match Technologies Customer Care.

PROBLEM: CANNOT ACCESS THE UNIT ON THE NETWORK
Possible Error Messages Displayed: **None**
Primary Steps to Resolution
1. Verify that the unit is powered on and a network cable is attached. Remove power, reapply and wait for unit to power up. After a few seconds, the Link LED should illuminate.
2. Verify that the hostname is correct. The default hostname is the serial number printed on the bottom of the unit. The default URL would be http://300E-xxxxxxx (x being the serial number).
3. Open a command shell and ping the hostname (i.e., ping 300e-xxxxxxx). If you cannot ping the device, see the next troubleshooting section, "Cannot Ping Device". If you can ping the device, go to Secondary Steps to Resolution.
Secondary Steps to Resolution (if Primary unsuccessful)
Please contact Cross Match Technologies Customer Care

PROBLEM: CANNOT PING DEVICE
Possible Error Messages Displayed: **None**
Primary Steps to Resolution
1. Check the Ethernet port lights on the back of the unit. If the unit is powered on with an active connection, the Link (A) LED light should be illuminated. Ideally the unit will be operation on a 100 Mbps network and the Speed (B) LED should be illuminated as well. If there is any activity on the network, the Activity (C) LED will be illuminated.
Secondary Steps to Resolution (if Primary unsuccessful)
1. If no Ethernet LEDs are on, verify that the unit is powered on.
Tertiary Steps to Resolution (if Secondary unsuccessful)
Please contact Cross Match Technologies Customer Care

PROBLEM: "LIVE" IMAGE DISPLAY NOT WORKING
Possible Error Messages Displayed: **None**:
Primary Steps to Resolution
The "Live Image" display applet will not function correctly with the default Microsoft Internet Explorer JVM (Java Virtual Machine).
1. Install Sun Microsystem's JVM (http://Java.sun.com).
2. Check to see which JVM is active in Internet Explorer by clicking on: **Tools > Internet Options > Advanced**

3. Scroll down to Java (Sun) (if you do not see this section, you will need to install Sun JVM – See Section 3.5.2 on page 3-11.
4. Ensure that the box “Use Java 2v 1.4.1 for <applet> (requires restart)” is checked.
Secondary Steps to Resolution (if Primary steps were unsuccessful)
Please contact Cross Match Technologies Customer Care

PROBLEM: NO ETHERNET LINK LED
Possible Error Messages Displayed: **None**
Primary Steps to Resolution
1. Ensure that the unit has power. Is the status light active (blinking or solid)? The status light is a dim red when the unit is first powered on.
2. Ensure that the network is active. Can you access the network with this cable using a different unit or another computer?
3. Try a different network cable.
Secondary Steps to Resolution (if Primary steps were unsuccessful)
Please contact Cross Match Technologies Customer Care.

PROBLEM: AUTO REFRESH DISPLAY NOT WORKING
Possible Error Messages Displayed: **None**
Primary Steps to Resolution
1. If you are using Microsoft Internet Explorer, upgrade to version 5.5 or greater.
Secondary Steps to Resolution (if Primary steps were unsuccessful)
Please contact Cross Match Technologies' Customer Care.

PROBLEM: UNIT WILL NOT TAKE IMAGES
Possible Error Messages Displayed:
None
Primary Steps to Resolution
1. Verify that the finger sensor is enabled in Device Configuration (see section 3.7 on page 3-19).
2. Ensure that the setting for "number of ridges required before a fingerprint is captured" is not set too high. A typical value is between 7 and 20.
Secondary Steps to Resolution (if Primary steps were unsuccessful)
Please contact Cross Match Technologies Customer Care.

PROBLEM: CANNOT SAVE IMAGES IN BMP OR PNG FORMAT
Possible Error Messages Displayed:
Not Found **Sorry that file does not exist**.
Primary Steps to Resolution
1. Verify that Save BMP (.bmp bitmap file) Format and/or Save PNG (Portable Network Graphics) is checked in Device Configuration (see section 3.7.1 on page 3-20).
Secondary Steps to Resolution (if Primary steps were unsuccessful)
Please contact Cross Match Technologies Customer Care.

7 Returns and Repairs

To return a Verifier E for repair or replacement, contact Customer Care via e-mail or telephone for a Return Material Authorization (RMA) number.

E-Mail:	**support@crossmatch.com**
Telephone (voice):	(877) 474-0228 (toll-free)
Facsimile:	(561) 622-8769

The RMA number should be marked clearly on the outside of the box as well as on the shipping label, as shown below. Any product shipped to Cross Match Technologies without an RMA number will be returned to sender.

CROSS MATCH TECHNOLOGIES, INC.
3960 RCA Boulevard, Suite 6001
Palm Beach Gardens, FL USA 33410
Attn: RXXXX.XXXX

When a package with an RMA number arrives at Cross Match Technologies, the corresponding paperwork (describing the reason for the return) is pulled, and the product is routed to the appropriate department for applicable servicing/replacement. Once completed, the product is then shipped back to the sender.


NOTICE

All configurations (User Password, HostName, etc) will be reset to factory settings when returned and may need to be reconfigured to your settings.

If the product is under warranty, the following freight guidelines will apply:

- The purchaser is responsible for all freight charges incurred in sending product for servicing.
- Cross Match Technologies, Inc. will be responsible for all freight charges incurred in the return of that product back to the purchaser.

If the product is not under warranty, all freight charges will be the responsibility of the purchaser.


NOTICE

ALL RMA's MUST be shipped back in original packaging (i.e., all boxes, plastic bags and Styrofoam ends). If original packaging is not available, call Cross Match Technologies' Customer Care for instructions.

8 Contact Information

Below is contact information for Cross Match Technologies, Inc. For more information on technical support, see **Chapter 4**. For more information on returning your Verifier E see **Chapter 7**.

CORPORATE ADDRESS
Cross Match Technologies, Inc.
3950 RCA Boulevard, Suite 5001
Palm Beach Gardens, Florida USA 33410

PRODUCT RETURN ADDRESS
Cross Match Technologies, Inc.
3960 RCA Boulevard, Suite 6001
Palm Beach Gardens, Florida USA 33410
RMA#:

COMPANY TELEPHONE NUMBER - Corporate, Customer Care, Sales/Extended Warranty
(561) 622-1650 - Main Corporate Number
(877) 474-0228 - Customer Care (toll-free)
(866) 725-3926 - Sales (toll-free)

COMPANY FACSIMILE NUMBER
(561) 622-9938 - Corporate
(561) 622-8769 - Technical, Customer Care

WEB PAGE
Corporate: www.crossmatch.com

E-MAIL
General Mailbox: info@crossmatch.com
Sales Department: sales@crossmatch.com
Technical: support@crossmatch.com

9 Supplies and Accessories

If you should need to order any supplies or additional peripherals for your Verifier E you can call or e-mail us for information or pricing.

Part Number	Item
122091	Cable, Network, Patch, CAT5E - 7 Ft.
122092	Cable, Network, Patch, CAT5E - 12 Ft.
122093	Cable, Network, Patch, CAT5E - 50 Ft.
900091	Kit, Supplies, Standard - Verifier 300 Series Includes: ▪ 1 box Kimwipes ▪ 10 Silicone Pads ▪ 1 Spray bottle for Isopropyl Alcohol*
900092	Kit, Supplies, Large - Verifier 300 Series Includes: ▪ 10 boxes Kimwipes ▪ 30 Silicone Pads ▪ 4 Spray bottles for Isopropyl Alcohol*
900093	Kit, Silicone Pad, Standard - Verifier 300 Series - Includes: ▪ 10 Silicone Pads
900094	Kit, Silicone Pad, Large - Verifier 300 Series - Includes: ▪ 30 Silicone Pads
930032	12 Month Extended Warranty

* The Isopropyl Alcohol is not supplied, and must be purchased by the user.

COMPANY SALES NUMBER

(561) 622-1650
(866) 725-3926 (toll-free)

E-MAIL
sales@crossmatch.com

10 Verifier E Specifications

Dimension	Height: 2.27” Width: 3.21” Length 6.33”
Weight	2.8 lbs
Scanner	• Platen Area: 1.2” x 1.2” • Gray Scale: 256 levels of gray • Resolution: 500 dpi +/- 5 pixels in X and Y axis • Linearity: < 1 pixel (average)
Image Types	BMP, PNG (512W x 480H)
Electrical	Voltage: 12 – 15 VDC
Communication	Ethernet 10/100 BASE-T
Environment	Temperature range: 0° F to 122° F
Humidity Range	10-95% non-condensing; splash resistant
Regulatory	FCC, UL, CE

10.1 FCC Statement

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/television technician for help

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.

10.2 UL Listing

This device is listed by, and bears the mark of, Underwriters Laboratories, Inc.

10.3 CE Compliance

This device complies with the mandatory European marking to indicate conformity with the essential health and safety requirements set out in European Directives.

11 Glossary

Term or Acronym	Definition
APIPA	Automatic Private IP - With APIPA, DHCP Clients can automatically self-configure an IP Address and subnet mask when a DHCP server isn't available.
BMP	The standard bit-mapped graphics format used in the Windows environment. By convention, graphics files in the BMP format end with a .BMP extension.
Broadcast	A transmission to multiple, unspecified recipients.
DHCP	Dynamic Host Configuration Protocol - a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.
DNS	Domain Name System - An Internet service that translates domain names into IP addresses.
Domain Name	A name that identifies one or more IP addresses. Example: Crossmatch.com.
Encryption	The translation of data into a secret code. Encryption is the most

Term or Acronym	Definition
	effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decode it.
Gateway	A node on a network that serves as an entrance to another network.
Host Name	The unique name that identifies a computer on a network. Example: Verifier E could be a Host Name.
HTTPS	A protocol for transmitting data securely over the World Wide Web.
IP Address	The unique numerical identifier for a computer or device on a TCP/IP network. Example: 128.121.221.78 could be an IP address.
JAR Files	Short for Java Archive, a file format used to bundle components required by a Java Applet.
MAC Address	Media Access Control address – A hardware address that uniquely identifies each node of a network.
Name Server	A program that translates names from one form into another. For example, the Internet relies on the DNS to translate domain names into IP Addresses

Term or Acronym	Definition
Netmask	A 32-bit bit mask which shows how an Internet address is to be divided into network, subnet and host parts. The netmask has ones in the bit positions in the 32-bit address that are to be used for the network and subnet parts, and zeros for the host part. The mask should contain at least the standard network portion (as determined by the address's class), and the subnet field should be contiguous with the network portion.
PEM	PEM (.pem) is an abbreviation for Privacy Enhanced Mail (RFC 1421 - RFC 1424), an early standard for securing electronic mail (IRTF, IETF). The PEM format often is used for representing a certificate, certificate request, by base64 encoding it and putting the encoding between the typical PEM delimiters.
PNG	Portable Network Graphics - bit-mapped graphics format similar to GIF.
SSL	Secure Sockets Layer. A protocol for transmitting private documents via the Internet.
Subnet Mask	A mask used to determine what subnet an IP belongs to. An IP address has two components, the network address and the host address.

12 Standard Warranty & Remedy

Limited Warranty:

Cross Match Technologies, Inc. ("CMT") warrants that the CMT product you have purchased will be free from defects in material and workmanship in normal service and under normal conditions for a period of 1 year from the date of shipment. Normal service and normal conditions are defined in the product documentation. This limited warranty is subject to the terms and conditions set forth below.

Repair or Replacement:

The sole obligation of CMT and your exclusive remedy and recourse under this limited warranty is for CMT, at your election, to either (i) repair the suspected defective product and return the same to you or (ii) replace the suspected defective product, all on the terms set forth below. The repair or replacement will provide you with a product which, in CMT's opinion, performs consistently with its age and usage.

If you become aware that your CMT product is defective in material or workmanship in normal service and under normal conditions during its one year warranty period, then you must promptly contact CMT's Customer Care Center, describe the suspected defect in detail and request a Return Merchandise Authorization ("RMA") number prior to sending the affected product for repair or requesting a replacement product. Please see your product manual for more information on RMAs.

If you elect to have CMT replace your suspected defective product during the one year warranty period, CMT will ship a refurbished replacement product to you, and you will

return your suspected defective product to CMT upon your receipt of the replacement product. The original returned product will become the property of CMT and will not be returned to you. CMT will pay the freight to send the replacement product to you, and you will pay the freight to return the suspected defective product to CMT's designated Service Center.

Alternatively, during the one year warranty period, you may return your suspected defective product to CMT's designated Service Center for repair. You will pay the freight to send the product to CMT's designated Service Center, and CMT will pay the freight to return the repaired product to you.

Each repaired or replacement product is warranted (as set forth herein) for the remaining portion of the original one year product warranty.

THE FOREGOING CONSTITUTES YOUR SOLE AND EXCLUSIVE REMEDY AND CMT'S SOLE AND EXCLUSIVE LIABILITY IN CONNECTION WITH YOUR CMT PRODUCT, AND IS IN LIEU OF ANY AND ALL OTHER REMEDIES WHICH MAY BE AVAILABLE TO YOU.

Limitations:

This limited warranty does not cover visits to repair the CMT product at your premises, or the commissioning of the product on site. This limited warranty is only a promise by CMT, to you the customer, that CMT will repair certain faults. It is not a warranty, guarantee or promise that your CMT product will conform to its specification or will not fail. Some defects and failures are not covered. CMT will not provide warranty repair or replacement if in CMT's opinion the problem resulted from externally caused damage or use outside the product's specifications, or from the use of

options, parts, equipment, software or consumables which are not CMT approved. This limited warranty does not cover the replacement of used consumables or of parts which need replacement during the life of the product as a result of the use made of them. Cross Match Technologies reserves the right to improve/modify products at any time, at its sole discretion, as it deems necessary.

CMT shall incur no liability under this limited warranty and this limited warranty is void able by CMT if in CMT's opinion (a) the product is used other than under normal use and under proper environmental and/or electrical conditions, as specified in the product manual; (b) the product is not maintained as specified in the product manual; (c) the product is subject to abuse, misuse, neglect, accident, flooding, storm, lightning, power surges, dirty power, third-party errors or omissions, or acts of God; (d) the product is modified or altered (unless expressly authorized in writing by CMT); (e) the product is installed or used in combination or in assembly with products not supplied or authorized by CMT; (f) there is a failure to follow specific restrictions or operating instructions; or (g) payment for the product has not been timely made.

CMT's obligations hereunder are contingent upon your providing the product serial number as proof-of-purchase, and upon CMT's determination that the suspected malfunction is actually due to defects in material or workmanship.

THIS LIMITED WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES RELATED TO THE CMT PRODUCT, WHETHER EXPRESSED, IMPLIED, OR STATUTORY, INCLUDING THE WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ALL OF WHICH ARE EXPRESSLY DISCLAIMED BY CMT. THIS LIMITED WARRANTY IS FOR THE SOLE BENEFIT OF, AND

APPLIES ONLY TO, THE ORIGINAL PURCHASER OF THE CMT PRODUCT. THIS WARRANTY IS NOT ASSIGNABLE BY SAID PURCHASER.

Out-of-Warranty Repairs:

When warranty coverage for your CMT product lapses, or for repairs or replacements not covered by CMT's warranty, (i) you will pay for all repairs at CMT's then-prevailing hourly labor rate (with a one hour minimum) plus parts and shipping, (ii) you will pay CMT's then-current price for all replacement products plus shipping, and (iii) you will pay CMT's then-prevailing hourly labor rate (with a one hour minimum after the first 15 minutes) for telephone support in 15 minute increments.

To obtain out-of-warranty service, you must obtain an RMA number and send the affected product, at your expense, to the designated CMT Service Center for inspection. You will be contacted with an estimated price and time of repair or replacement after analysis. No repairs or replacements will be made until CMT receives a Purchase Order or credit card number from you. You shall pay return freight charges, which will be added to the invoice, for the return of the repaired product or replacement product.

In the event you decide not to have a unit repaired or replaced after receiving a repair estimate, there will be a one hour labor charge at the prevailing hourly rate for evaluation plus return freight charges.

At your request, CMT will, for a premium, ship a refurbished unit to you in exchange for the failed unit. CMT will contact you with a price for the exchange after receipt of the failed unit. The shipment will be made when CMT receives a Purchase Order or credit card number from you. You will pay return freight charges, which will be

added to the invoice, for the exchange unit. The original returned product will become the property of CMT and will not be returned to you. The refurbished unit will be warranted as set forth above [one year] from the date of shipment.

Extended Warranty:

An Extended Warranty is available for this product. For Extended Warranty terms, pricing, or requirements, please contact CMT Sales at toll free: (866) 725-3926 [(1) (561) 622-2146] or visit us on the web at http://www.crossmatch.net/contact_us.html.

13 Index