



ViiSAGE iA-thenticate® 5.3

Administrator's Guide

Viisage iA-thenticate 5.3

Administrator's Guide

Copyright ©2007 by Viisage Technology, Inc.
296 Concord Road, Billerica, MA 01821 USA
Phone 978-932-2200, fax 978-932-2225, web www.viisage.com

Customer support:

support-ia@l1id.com
+1 978-932-2200
+1 800-555-8784 toll-free (North America)

All rights reserved.

Unpublished rights reserved under the copyright laws of the United States.

Viisage, the Viisage logo, iA-thenticate, BorderGuard, ID-Guard, ID-Passport, iA-DataPort, iA-Examiner, ID-License, TextWatch, and iA-Administrator are trademarks or registered trademarks of Viisage Technology, Inc., an L-1 Identity Solutions Company. All other brand and product names are trademarks or registered trademarks of their respective companies or organizations.

Covered by one or more U.S. and foreign patents including U.S. Patent No. 6,269,169.

RADIO AND TELEVISION INTERFERENCE

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

In order to maintain compliance with FCC regulations shielded cables must be used with this equipment. Operation with non-approved equipment or unshielded cables is likely to result in interference to radio & television reception.

Changes or modifications not expressly approved by Viisage could void the users' authority to operate the equipment.

Safety Guidelines: Follow these safety guidelines to protect your iA-thenticate system from damage and to ensure your own safety.



WARNING: Do not attempt to disassemble the iA-thenticate unit or to operate it with any parts removed. The unit contains no user-serviceable parts.

Operate iA-thenticate only in an area where the temperature is between 50° F and 105° F (between 10° C and 40° C).

Do not spill food or liquids on the iA-thenticate unit. If the unit gets wet, immediately shut down the system and contact Viisage. Do *not* attempt to open the unit. Only a qualified iA-thenticate technician should perform service and repair work.

Do not set anything on top of the iA-thenticate unit or cables. Route all cables so that people will not step or trip on them.

Use a surge-protection power strip to protect iA-thenticate against electrical damage, as you would with any computer.

The information contained in this document is subject to change without notice. Viisage assumes no responsibility for technical or editorial errors or omissions, or for the use of this material. Nor does Viisage make any commitment to update the information contained in this document. This document contains proprietary information that is protected by copyright. All rights reserved. No part of this document may be photocopied or reproduced in any form without the prior written consent of Viisage.

Edition IA-ADMIN-5.3, 12/07
Publication PUB-00052-A-15

Table of Contents

Part One Setting Up a New iA-thenticate Unit

1	Introduction to iA-thenticate	1-1
	BorderGuard and ID-Guard	1-1
	BorderGuard	1-1
	ID-Guard	1-2
	Setting Up Your System	1-2
2	Setting Up a Color BorderGuard Unit	2-1
	PC System Requirements	2-1
	Installing Software	2-2
	Setting the PC's Taskbar and Display Properties	2-2
	Installing DirectX	2-3
	Installing the iA-thenticate Security Software	2-3
	Installing iA-Examiner	2-4
	Installing DL-Alert	2-4
	Installing the Custom Calibration File	2-4
	Installing Other Optional Software	2-4
	Restarting	2-4
	Connecting Hardware and Installing Drivers	2-5
	Connecting Hardware	2-5
	Installing Drivers	2-5
	Configuring Hardware and Software	2-6
	Configuring a Smart-Card Unit	2-6
	Configuring Internet Explorer	2-6
	Configuring a Non-English Version of Windows	2-6
	Running the Software for the First Time	2-7
	Testing the B4500/5000 Smart Card Reader	2-8
	Controlling Access	2-9
	Creating Local User Groups and Users	2-9
	Assigning File and Folder Permissions	2-10
	Installing an Optional Reader or Scanner	2-11
	What's Next?	2-12

3	Setting Up an ID-Guard Unit	3-1
	PC System Requirements	3-1
	Installing Software	3-2
	Setting the PC's Taskbar and Display Properties	3-2
	Installing DirectX	3-3
	Uninstalling Regula software	3-3
	Installing the Regula SDK	3-3
	Installing the iA-thenticate Security Software	3-4
	Installing iA-Examiner	3-4
	Installing DL-Alert	3-4
	Installing Other Optional Software	3-4
	Restarting	3-4
	Connecting Hardware and Installing Drivers	3-5
	Connecting Hardware	3-5
	Installing Drivers	3-5
	Configuring Hardware and Software	3-7
	Configuring Internet Explorer	3-7
	Configuring a Non-English Version of Windows	3-8
	Controlling Access	3-8
	Creating Local User Groups and Users	3-9
	Assigning File and Folder Permissions	3-9
	Installing an Optional Reader or Scanner	3-11
	What's Next?	3-11

4	Installing an Optional Reader or Scanner	4-1
	Installing the E-Seek Intelli-Check Reader	4-1
	Serial Model	4-1
	USB Model	4-2
	Installing a Flatbed Scanner	4-3

Part Two

Configuring and Managing iA-thenticate

5	Using the Administration Tools	5-1
	iA-Administrator	5-2
	iA-Examiner	5-3
	What's Next?	5-5

6	Quick Configuration Guide	6-1
----------	--	------------

7	Configuring iA-thenticate	7-1
	Viewing Unit Information	7-2

Setting Options for Basic Operation	7-3
ICAO Expiration Test	7-3
Signals and Alerts	7-4
Startup	7-4
Restoring Normal Logon	7-4
Hardware	7-5
Software	7-5
Advanced	7-6
Setting Options for Saving Images and Logs	7-7
Two Ways to Save Images and Logs	7-7
Captured Images	7-10
Document Results Log	7-10
Saving Based on Test Results	7-11
JPEG Image Quality	7-11
Temporary Images and Logs	7-12

8	
Configuring iA-Examiner	8-1
System Configuration Screens	8-1
Configuring Peripherals	8-2
Configuring Printing	8-4
Configuring Data Saving	8-5
Data Saving Options	8-5
Using a Networked Database	8-8
Configuring Tests	8-9
Configuring Document Processing	8-12
Configuring Verification Databases	8-14
About VerifyME	8-14
Configuring VerifyME	8-15
Configuring Data Entry	8-17
Configuring a Custom ID Type	8-18
Configuring Static Database Information	8-18
Configuring Debugging	8-19
Configuring Processing of Unidentified Documents	8-19
Configuring System Directories	8-21
Configuring Display Options	8-21
Configuring Smart Card Options	8-24
About Basic Access Control	8-24
Smart Card Options	8-24
Configuring Bar Code and Magstripe Options	8-25
Configuring Reference Database Options	8-25
Configuring Test Suppression	8-26
Configuring Test Override Options	8-26
Configuring Alerts for Indeterminate Tests	8-27
Configuring Credit Card Options	8-27
Configuring Data Transmission Options	8-28
Configuring iA-Examiner Doc Log Options	8-28
Configuring Miscellaneous Options	8-29

9	Managing iA-Examiner	9-1
	Purging Saved Data	9-2
	Backing Up Saved Data	9-3

Part Three

Using Optional Features

10	Using iA-DataPort	10-1
	Preparing to Use iA-DataPort	10-2
	Choosing Where to Send Data	10-2
	Using the Optional Keyboard Filter	10-3
	Starting iA-DataPort	10-4
	Starting the iA-DataPort Utility	10-4
	Running the Utility Minimized	10-4
	Viewing Captured Data	10-5
	Configuring Settings	10-6
	Configuring General Settings	10-6
	Configuring Communication Port Settings	10-8
	Configuring Data Format Settings	10-8
	Configuring MRZ Data Format Settings	10-10
	Configuring Data Transmit Settings	10-12
	Configuring Display Settings	10-12
	Configuring Startup Settings	10-14

Appendices

A	Setting Up a Monochrome BorderGuard Unit	A-1
	PC System Requirements	A-1
	Installing Software	A-2
	Setting the PC's Taskbar and Display Properties	A-2
	Installing the iA-thenticate Security Software	A-3
	Installing iA-Examiner	A-3
	Installing DL-Alert	A-3
	Installing the Custom Calibration File	A-3
	Installing Other Optional Software	A-4
	Restarting	A-4
	Installing Hardware	A-4
	Installing the PCI Card	A-4
	Connecting the BorderGuard Cables	A-5
	Finishing Installation	A-6
	Starting Up and Checking Installation	A-6
	Configuring Internet Explorer	A-6

Configuring a Non-English Version of Windows	A-6
Controlling Access	A-8
Creating Local User Groups and Users	A-8
Assigning File and Folder Permissions	A-9
Installing an Optional Reader or Scanner	A-10
What's Next?	A-10
B	
Solving Problems	B-1
Color BorderGuard	B-2
Drivers Do Not Install As Expected	B-2
Camera Driver Installation Problems	B-3
iA-Examiner Reports a COM Port Error	B-3
Color BorderGuard B4500/5000	B-4
Drivers Do Not Install As Expected	B-4
Camera Driver Installation Problems	B-5
iA-Examiner Reports a COM Port Error	B-5
Smart Card Driver Installation Problems	B-6
ID-Guard	B-9
Scanning Produces Unexpected Behavior	B-9
Camera Driver Installation Problems	B-9
Monochrome BorderGuard	B-12
iA-Examiner Reports an IACOMO Error	B-12
E-Seek Intelli-Check Magstripe and Bar Code Reader	B-13
Scanning a Magstripe or Bar Code Produces an Error	B-13
Flatbed Scanner	B-14
Scanning Produces an Error or Unexpected Behavior	B-14
C	
Periodic Maintenance	C-1
Cleaning the Glass Platform	C-1
Cleaning the BorderGuard Sensor Switch	C-2
Defragmenting the Hard Drive	C-2

Part One

Setting Up a New iA-thenticate Unit

Introduction to iA-thenticate

iA-thenticate® is a hardware and software system for testing the authenticity of travel and ID documents and for checking the identity of document owners.

Basic document testing includes verifying the checksum digits in a document's machine-readable zone (MRZ), checking its expiration date, and confirming the proper use of IR-absorbent (B900) ink.

With optional software and hardware, the system can test documents in additional ways and also check a document owner's identity. For example:

- With ID-Passport® software, the system can verify additional features such as UV patterns and security laminate.
- With ID-License™ and DL-Alert™ software and a magnetic stripe and bar code reader, the system can read and verify driver's licenses and non-driver IDs.
- With TextWatch® software, the system can compare information read from the document against a custom database of names, stolen document numbers, or other important data.
- With an integrated smart card reader, the system can read, verify, and cross-check information from an embedded smart chip.

BorderGuard and ID-Guard

Note

The *BorderGuard* unit has also been called an *iA-thenticate* unit. Your unit may have either label.

Note

Some older *BorderGuard* units have a monochrome camera.

The system includes a *BorderGuard*® or *ID-Guard*® unit and a PC running *iA-thenticate* software.

BorderGuard

BorderGuard processes passport-size documents as well as smaller wallet-size cards. It captures document images using a color camera, and often uses an attached reader to read magnetic stripes (magstripes) and two-dimensional (2D) bar codes. Some units

have an integrated smart-card reader for reading chips embedded in the front and back pages (covers) of documents.



Color BorderGuard with
Smart Chip Reader



Color BorderGuard B4500/5000

ID-Guard

ID-Guard processes standard wallet-size cards such as driver's licenses and IDs. It captures document images using a color camera, and has an integrated magstripe reader. It can also read 2D bar codes directly from the captured document images without additional hardware.



ID-Guard

Setting Up Your System

Note

If you have an older BorderGuard unit with a monochrome camera, see Appendix A, "Setting Up a Monochrome BorderGuard Unit."

To set up your iA-thenticate system, carefully follow the instructions in the appropriate chapter:

- Chapter 2, "Setting Up a Color BorderGuard Unit"
- Chapter 3, "Setting Up an ID-Guard Unit"

Part Two of this guide explains how to configure and manage your system, and Part Three explains how to use optional features.

Setting Up a Color BorderGuard Unit

Note

If you have an older BorderGuard unit with a **mono-chrome** camera, see Appendix A, "Setting Up a Monochrome BorderGuard Unit."

This chapter explains how to set up your iA-thenticate system if you have a BorderGuard (iA-thenticate) unit with a color camera. This includes:

- Color BorderGuard* units, which have a text panel above the document platform
- Color BorderGuard B4500/5000* units, which have indicator lights instead

Before you proceed with installation, check the *Release Notes* for new information. If you are upgrading from a previous version, you may need to follow additional steps.

IMPORTANT

Although setting up this system is similar to setting up a PC, there are important differences. Follow the instructions in this chapter carefully, or your system may not work properly.

If you are not experienced in setting up and managing PCs in a networked environment, you should not attempt to do the setup yourself.

PC System Requirements

You install the iA-thenticate software on a Windows PC, and you connect the BorderGuard unit to the PC through a USB cable. Some units also connect using a standard serial cable. Your PC must meet these requirements:

Hardware

Note

For BorderGuard color units with USB ports, adding USB devices may increase the minimum system requirements. Viisage recommends using the USB ports on your computer before using any ports that may be on the back of the BorderGuard unit.

- Processor: 1.6 GHz Pentium 4 or better recommended; 2.8 GHz or better for a smart-card unit
- RAM: 256 MB minimum; 512 MB minimum for a smart-card unit
- Free disk space: 300 MB minimum; 1 GB or more recommended when saving captured images and data
- Video display: 1024x768 resolution, 65536 colors, or better
- An available USB 2.0 port (high speed, 480 Mbps)
- An available standard serial port (for units that require it)

Configuration

- Swap file: Recommended 768 MB minimum and 1024 MB maximum for drive C and for the data drive (where you store captured images)

Supported operating systems

- Windows 2000 Service Pack 4 or higher with updates 823980 (Microsoft Security Bulletin MS03-026) and 828028 (Bulletin MS04-007)
- Windows XP Professional Service Pack 2

Other software requirements

- Internet Explorer 6.0 Service Pack 1 or higher with update 832894 (Microsoft Security Bulletin MS04-004)
- Current Microsoft USB driver recommended; third-party USB drivers may also perform well

Installing Software

Do not connect the BorderGuard hardware yet.

Setting the PC's Taskbar and Display Properties

Your system should be configured so the taskbar displays on top of other windows and the font size is small (Windows 2000) or normal (XP). These are the default Windows settings. If you have changed these settings, follow these steps to restore the defaults:

Windows 2000	Windows XP
<ol style="list-style-type: none">1. Start the PC, log on as an administrator, and exit from all programs.2. Right-click the taskbar and choose Properties.3. On the Taskbar Properties screen, deselect Always on top and click OK.4. Right-click the Windows desktop and choose Properties.5. On the Settings tab, click Advanced.6. In the Font Size drop-down list, select Small Fonts if it is not already selected.7. Follow any further on-screen instructions for confirming your choice and installing fonts. You do <i>not</i> need to restart the system at this point unless Windows requires you to do so.	<ol style="list-style-type: none">1. Start the PC, log on as an administrator, and exit from all programs.2. Right-click the taskbar and choose Properties.3. On the Taskbar Properties screen, deselect Keep the taskbar on top of other windows and click OK.4. Right-click the Windows desktop and choose Properties.5. On the Appearance tab, in the Font Size drop-down list, select Normal if it is not already selected.6. Follow any further on-screen instructions for confirming your choice and installing fonts. You do <i>not</i> need to restart the system at this point unless Windows requires you to do so.

Note

This release has been tested with DirectX 9.0c. Later versions of DirectX may also be compatible.

Note

The CD's folder names include the name of the software plus version information—for example, *iA-thenticate 5.3 Install (SFW-00099-A-00)*. For simplicity, these instructions use just the first part of the name—for example, *iA-thenticate....*

Note

If you are upgrading, the screens you see may differ slightly from the ones listed. Just follow the on-screen instructions.

Installing DirectX

This software requires that DirectX 9.0c End-User Runtime be installed on your PC. To find out whether you already have this software installed:

1. Select Start→Run, type `dxdiag`, and click OK.
2. Find the DirectX version listed under System Information on the System tab.

If the version is not 9.0c or later, you must install DirectX 9.0c:

Installer	Instructions
<i>iA-thenticate CD:</i> <i>iA-thenticate... \</i> <i>iA-thenticate... \</i> DirectX \ <i>directx_9c_oct05sdk_</i> <i>redist.exe</i>	Follow the on-screen instructions.

Installing the iA-thenticate Security Software

Installer	Screen	Instructions
<i>iA-thenticate CD:</i>	Intro	Click Next.
<i>iA-thenticate... \</i> <i>iA-thenticate... \</i> 1_iA-thenticate \ <i>Setup.exe</i>	License	Click Yes to agree.
	Setup Type	If you have a BorderGuard Color unit, with a <i>text panel</i> above the document platform, select BorderGuard - color unit. If you have a BorderGuard B4500/5000 unit, with <i>indicator lights</i> rather than a text panel, select BorderGuard - B4500
	Data Drive	<i>If</i> you want to change the drive for storing data, click Browse and choose any mapped drive. Click Next.
	Summary	Click Next to proceed with installation.
	Complete	Accept No, I will restart my computer later. Click Finish.

Installing iA-Examiner

Installer	Screen	Instructions
<i>iA-thenticate CD: iA-thenticate... \ iA-thenticate... \ 2_iA-Examiner \ Setup.exe</i>	Intro	Click Next.
	Data Drive	<i>If you want to change the drive for storing iA-Examiner data, click Browse and choose a location.</i> Click Next to proceed with installation.
	Complete	Click Finish.

Installing DL-Alert

If you have optional DL-Alert™ software—either the Intelli-Check or Positive Access® version—install it now.

Installer	Screen	Instructions
<i>iA-thenticate CD: iA-thenticate... \ DL-Alert-IC... \ DL-AlertIntelli-Check.exe or iA-thenticate... \ DL-Alert-PA... \ DL-Alert-PositiveAccess.exe</i>	Intro	Click Next to proceed with installation.
	Warning	<i>Note the message and click OK. You will find instructions later in this document for configuring iA-Examiner.</i>
	Complete	Click Finish.

Installing the Custom Calibration File

Note

Older BorderGuard units have a SampleScan diskette rather than a CD.

1. Insert the SampleScan CD.
2. On the CD, find the folder that matches the serial number on the BorderGuard unit.
For reliable operation, you must use the correct calibration file for each unit.
3. Copy the SampleScan.cfg file from the folder to this directory:
C:\BorderGuard\Config
4. Right-click the copied SampleScan.cfg file and choose Properties. Deselect Read-only and click OK.

Installing Other Optional Software

If you have other optional software such as ID-Passport or ID-License, install it now. Follow the instructions included with the optional software.

Restarting

After you finish installing software, restart your PC.

Connecting Hardware and Installing Drivers

Connect the BorderGuard hardware *only after you have installed the software* as described starting on page 2-2.

Connecting Hardware

Note

The included power supply might not have a power cord suitable for your country. In this case you must obtain and use a 3-conductor grounded supply cord with a plug cap suitable for your country. It must have a minimum internal conductor area of 0.75 mm² and have a standard IEC 320 female connector.

Each BorderGuard unit ships with a USB cable and a power supply and cord. Some units also include a standard serial cable.

To connect the BorderGuard hardware:

1. Restart the PC after installing the software, and log on as an administrator.
2. Plug the BorderGuard power cable into the connector on the back of the BorderGuard unit, and plug the line cord into a surge-protected power source (100–240 VAC, 47–63 Hz, 170 W).
3. Turn *on* the power switch on the BorderGuard unit, and wait for the Welcome message to appear on its text panel.
4. *If* your unit includes a serial cable, connect it from the serial port on the back of the unit to the appropriate COM port on your PC (the one you selected during installation, page 2-3).
5. Connect the USB cable from the USB port on the back of the BorderGuard unit to an available USB 2.0 port (high-speed, 480 Mbps) on your PC. When you do this, Windows automatically starts installing drivers.

Installing Drivers

Driver installation varies with the version of Windows and the type of BorderGuard unit. Follow the appropriate instructions below. *If the drivers do not install as described here*, follow the problem-solving instructions on page B-2 for a color BorderGuard unit or B-4 for a color BorderGuard B4500/5000.

Note

If you see the following error message during installation with a B4500/5000 unit, refer to "Repairing the OmniKey Registration Settings" on page B-8:

Cannot import C:\Program Files\OmniKey\55x3 Driver V2.1.0.8\settings.reg

Windows XP

To install all drivers:

- ❖ Just wait. Windows XP should install all drivers automatically.

Windows 2000

To install drivers for BorderGuard B4500/5000:

Just wait. Windows 2000 should install all drivers automatically.

To install drivers for BorderGuard Color units:

1. When the new hardware wizard runs, confirm that the small window showing the device name says USB 2.0 Camera or Color Camera 01. Sometimes you have to move the wizard window to see this small window.
2. On the first wizard screen, click Next.

3. Select Display a list of known drivers for this device so that I can choose a specific driver, and click Next.
4. Click Have Disk and select C:\BorderGuard\Tools\BorderGuard Camera. (If there is no Have Disk button, first click Next and then click Have Disk.)
5. When the wizard displays the driver, click Next.
6. If you see a message about the digital signature, click Yes to continue. If you are asked whether you want to overwrite a newer file, click Yes.
7. Click Finish.

Configuring Hardware and Software

After installation, you may need to set some basic configuration options.

Configuring a Smart-Card Unit

If you have a smart-card unit, follow these steps to configure it:

1. Run iA-Administrator by choosing Start→Programs→iA-thenticate→iA-Administrator.
2. On the Configuration tab, under Signals and Alerts, deselect both of the Beep when... options. (These are currently incompatible with smart-card processing.)
3. Click Apply, then exit iA-Administrator.
4. Run iA-Examiner using the desktop shortcut or by choosing Start→Programs→iA-thenticate→iA-Examiner.
5. Click Mgmt Funcs and then System Config.
6. On System Configuration Page 1, select Smart Card Reader.
7. Click Apply and Done, then exit iA-Examiner.

Configuring Internet Explorer

If you use the VerifyMe verification database, follow these steps to configure Internet Explorer:

1. Start Internet Explorer.
2. Select Tools→Internet Options.
3. On the Advanced tab, under the Security heading, deselect Warn if changing between secure and not secure mode.

Configuring a Non-English Version of Windows

If you install this software on a unit running a non-English version of Windows, you may need to follow some additional steps.

To configure Windows 2000—Dutch, French, or Portuguese:

1. Select Start→Run, type DCOMCNFG, and click OK.
2. On the Default Security tab, under Default Access Permissions, click Edit Default.
3. In the displayed list, look for an entry for SYSTEM and also for INTERACTIEF (Dutch), INTERACTIF (French), or INTERATIVO (Portuguese).

If either name is missing, follow these steps to add the missing name or names:

- a. Click Add.
- b. In the drop-down List Frames From list, select the name of your unit.
- c. In the Names list, select the missing name or names and click Add.
- d. Click OK several times to accept the changes.

To configure Windows XP—Dutch, French, or Portuguese:

1. Select Start→Run, type DCOMCNFG, and click OK.
2. Open Component Services, then Computers, then My Computer, and then DCOM Config.
3. Right-click BGServer and choose Properties.
4. On the Security tab, under Launch and Activation Preferences, select Customize and click Edit.
5. If the displayed list does not include INTERACTIEF (Dutch), INTERACTIF (French), or INTERATIVO (Portuguese), add the appropriate name and select all the Allow permissions.
6. In the same list, select all the Allow permissions for SYSTEM. Then click OK.
7. Back on the Security tab of the BGServer Properties window, under Access Permissions, select Customize and click Edit.
8. In the displayed list, select both of the Allow permissions for SYSTEM and for INTERACTIF, INTERATIVO, or INTERACTIEF. Then click OK.
9. In the BGServer Properties window, click OK. Then close the Component Services window.

Running the Software for the First Time

After you finish installation:

1. Restart the system and log on as an *administrator*.
2. Run iA-Examiner using the desktop shortcut or by choosing Start→Programs→iA-thenticate→iA-Examiner.

If you see an error message about a COM port when you start iA-Examiner, follow the instructions on page B-3 (for color BorderGuard) or B-5 (for color BorderGuard B4500/5000) to correct the problem.

This ensures that all settings are properly registered. After that, you can run the software using non-administrator accounts.

Testing the B4500/5000 Smart Card Reader

If you have a smart-card reader on a BorderGuard B4500/5000 unit, verify that it is functioning correctly. The following two procedures will check the smart card reader functionality. You can use either the iA-Examiner test or the OMNIKEY applet test.

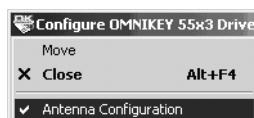
To test the smart card reader using iA-Examiner:

1. In iA-Examiner, process a smart card document that has its chip in the front cover side of the document (on the glass).
2. Process a smart card document that has its chip in the back cover side of the document (on the platform in front of the glass).
3. Check the smart card test results for both documents.

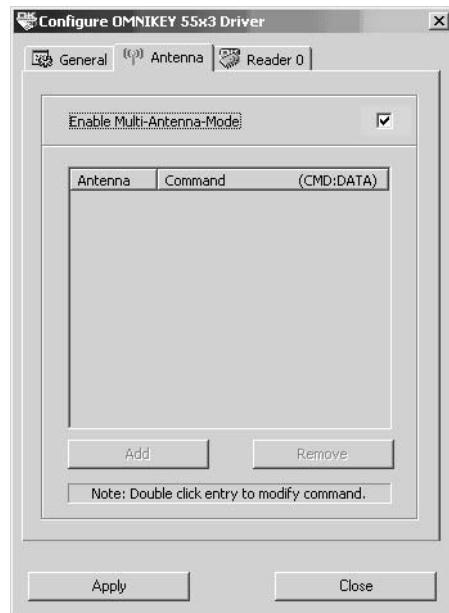
If iA-Examiner displays smart card test results for both documents, the unit is operating correctly. If iA-Examiner fails to recognize the smart card, follow the instructions for fixing the problem in “Repairing the OmniKey Registration Settings” on page B-8.

To test the smart card OMNIKEY applet:

1. In Control Panel, run the OMNIKEY 55x3 Driver Applet.
2. Right-click in the title bar of the applet and select Antenna Configuration.



3. On the Antenna tab, verify that “Enable Multi-Antenna Mode” is checked.



If “Enable Multi-Antenna Mode” is not checked, follow the instructions for fixing the problem in “Repairing the OmniKey Registration Settings” on page B-8.

Controlling Access

This section explains how to create local user groups and set file permissions for your system so that different users have just the access they need.

Creating Local User Groups and Users

First, create two local user groups and assign users to these groups as needed.

1. Create these two local user groups:

iA-thenticate Users
iA-thenticate Administrators

2. Create as many users as you need for the people who will use the system, and make each one a member of the appropriate user group:

Local User Group	Users Who Should Belong to This Group	Access Allowed
iA-thenticate Users	Personnel who use iA-Examiner to test and examine documents	iA-Examiner: user functions
iA-thenticate Administrators	Technical administrators, security managers, and operations managers	iA-Examiner: user and management functions iA-Administrator All Users startup folder (C:\Documents and Settings\All Users\Start Menu\Programs\Startup)

Assigning File and Folder Permissions

Assigning file and folder permissions ensures that each group of users can run the appropriate programs.

To assign file and folder permissions:

1. Follow steps a-c for each file in the table below:
 - a. Right-click the file and choose Properties.
 - b. Select the Security tab.
 - c. In the Name list, remove the entries for Everyone and Users (if listed). Then add Read & Execute permissions for user groups as indicated in the table.

For this file in C:\BorderGuard\Bin\	Assign Read & Execute permissions for these groups
iA-Administrator.exe (iA-Administrator)	iA-thenticate Administrators
BGDataPort.exe (iA-DataPort)	iA-thenticate Users iA-thenticate Administrators
BGExaminer.exe (iA-Examiner)	iA-thenticate Users iA-thenticate Administrators
BGServer.exe (ID-Server)	iA-thenticate Users iA-thenticate Administrators
ExaminerConfiguration (iA-Examiner configuration)	iA-thenticate Administrators
ExaminerManager (iA-Examiner management)	iA-thenticate Administrators
ExaminerReport (iA-Examiner reporting)	iA-thenticate Administrators
ExaminerViewer (iA-Examiner document review)	iA-thenticate Administrators
iA-SecondaryStation.exe (Secondary Station)	iA-thenticate Users iA-thenticate Administrators

2. *iA-thenticate* Administrators must be able to change startup settings for All Users. Follow these steps to assign the needed permissions to C:\Documents and Settings\All Users\Start Menu\Programs\Startup:

- a. Right-click folder C:\Documents and Settings and choose Properties.
- b. Select the Security tab.
- c. Add Full Control permissions for the *iA-thenticate* Administrators group.
- d. Repeat steps a-c for each successive folder in the path:

All Users (inside Documents and Settings)
Start Menu (inside All Users)
Programs (inside Start Menu)
Startup (inside Programs)

3. If you use Windows security to limit users' access to various folders on your system, *all iA-thenticate users* must have these permissions:

- Full control to the work folder, normally C:\BorderGuard\Working
- Read and execute access to C:\BorderGuard and all of its sub-folders
- Read, write, and execute access to:
 - C:\BorderGuard\Config\SampleScan.cfg
 - The folder for storing captured images—for example, E:\BorderGuard\Images
 - The folder containing the *iA-Examiner* database BGExaminer.mdb, normally C:\BorderGuard\Bin
 - If you use TextWatch, the folder containing the TextWatch database iAT.sys, normally C:\BorderGuard\Bin

In addition, *iA-thenticate administrators* must have these permissions:

- Write access to:
 - The folder containing the *iA-Administrator* database Administrator.mdb, normally C:\BorderGuard\Bin
 - The Windows registry
- Read, write, and execute access to:
 - The configuration folder, C:\BorderGuard\Config and all sub-folders

Installing an Optional Reader or Scanner

If your system includes a bar code and magstripe reader or a flatbed scanner, install it now by following the instructions in chapter 4.

What's Next?

Your iA-thenticate system is now set up to work using factory-default settings. Probably you will want to change some of those settings. Part Two of this guide explains how.

Setting Up an ID-Guard Unit

This chapter explains how to set up your iA-thenticate system if you have an ID-Guard unit, which processes standard wallet-size cards such as driver's licenses and IDs. ID-Guard has an integrated magstripe reader and can read 2D bar codes directly from the captured document images without additional hardware.

Before you proceed with installation, check the *Release Notes* for new information. If you are upgrading from a previous version, you may need to follow additional steps.

IMPORTANT

Although setting up this system is similar to setting up a PC, there are important differences. Follow the instructions in this chapter carefully, or your system may not work properly.

If you are not experienced in setting up and managing PCs in a networked environment, you should not attempt to do the setup yourself.

PC System Requirements

You install the iA-thenticate software on a Windows PC, and you connect the ID-Guard unit to the PC through a USB cable. Your PC must meet these requirements:

Hardware

- Processor: 2.4 GHz Pentium 4 or better recommended
- RAM: 512 MB minimum
- Free disk space: 300 MB minimum; 1 GB or more recommended when saving captured images and data
- Video display: True color mode (24 or 32 bit)
- An available USB 2.0 port (high speed, 480 Mbps) with adequate power
- For computers that do not supply adequate power through a single USB port (especially laptops running on batteries), a second USB port is required

Configuration

- Swap file: Recommended 768 MB minimum and 1024 MB maximum for drive C and for the data drive (where you store captured images)

Supported operating systems

- Windows 2000 Service Pack 4 or higher with updates 823980 (Microsoft Security Bulletin MS03-026) and 828028 (Bulletin MS04-007)
- Windows XP Professional Service Pack 2

Other software requirements

- Internet Explorer 6.0 Service Pack 1 or higher with update 832894 (Microsoft Security Bulletin MS04-004)
- Current Microsoft USB driver recommended; third-party USB drivers may also perform well

Installing Software

Do not connect the ID-Guard hardware yet.

Setting the PC's Taskbar and Display Properties

Your system should be configured so the taskbar displays on top of other windows and the font size is small (Windows 2000) or normal (XP). These are the default Windows settings. If you have changed these settings, follow these steps to restore the defaults:

Windows 2000	Windows XP
<ol style="list-style-type: none">1. Start the PC, log on as an administrator, and exit from all programs.2. Right-click the taskbar and choose Properties.3. On the Taskbar Properties screen, deselect Always on top and click OK.4. Right-click the Windows desktop and choose Properties.5. On the Settings tab, click Advanced.6. In the Font Size drop-down list, select Small Fonts if it is not already selected.7. Follow any further on-screen instructions for confirming your choice and installing fonts. You do <i>not</i> need to restart the system at this point unless Windows requires you to do so.	<ol style="list-style-type: none">1. Start the PC, log on as an administrator, and exit from all programs.2. Right-click the taskbar and choose Properties.3. On the Taskbar Properties screen, deselect Keep the taskbar on top of other windows and click OK.4. Right-click the Windows desktop and choose Properties.5. On the Appearance tab, in the Font Size drop-down list, select Normal if it is not already selected.6. Follow any further on-screen instructions for confirming your choice and installing fonts. You do <i>not</i> need to restart the system at this point unless Windows requires you to do so.

Note

This release has been tested with DirectX 9.0c. Later versions may also be compatible.

Note

The CD's folder names include the name of the software plus version information—for example, *iA-thenticate 5.3 Install (SFW-00099-A-00)*. For simplicity, these instructions use just the first part of the name—for example, *iA-thenticate*....

Note

If you are upgrading, the screens you see may differ slightly from the ones listed. Just follow the on-screen instructions.

Installing DirectX

This software requires that DirectX 9.0c End-User Runtime be installed on your PC. To find out whether you already have this software installed:

1. Select Start→Run, type `dxdiag`, and click OK.
2. Under the systems tab, find the DirectX Version listed under System Information.

If the version is not 9.0c or later, you must install DirectX 9.0c:

Installer	Instructions
<i>iA-thenticate CD:</i> <i>iA-thenticate... \</i> <i>iA-thenticate... \</i> DirectX \ <i>directx_9c_oct05sdk_</i> <i>redist.exe</i>	Follow the on-screen instructions.

Uninstalling Regula software

Before installing the Regula SDK version 4.10, you must uninstall any previous versions. To find out whether you already have this software installed and uninstall any previous versions:

1. Select Start→Settings→Control Panel→Add/Remove Programs.
2. Look for Regula programs (for example, Regula Document Reader SDK or Regula Document Reader Core Components).
3. Select each program and click Remove.

Installing the Regula SDK

To install Regula SDK version 4.10:

Installer	Instructions
<i>iA-thenticate CD:</i> <i>iA-thenticate... \</i> <i>iA-thenticate... \</i> Regula_SDK-4.10 \ <i>setup.exe</i>	Follow the on-screen instructions in the InstallShield Wizard.

Installing the iA-thenticate Security Software

Installer	Screen	Instructions
<i>iA-thenticate CD: iA-thenticate... \ iA-thenticate... \ 1_iA-thenticate \ Setup.exe</i>	Intro	Click Next.
	License	Click Yes to agree.
	Setup Type	Select ID-Guard.
	Data Drive	<i>If you want to change the drive for storing data, click Browse and choose any mapped drive.</i> Click Next.
	Summary	Click Next to proceed with installation.
	Complete	Accept No, I will restart my computer later. Click Finish.

Installing iA-Examiner

Installer	Screen	Instructions
<i>iA-thenticate CD: iA-thenticate... \ iA-thenticate... \ 2_iA-Examiner \ Setup.exe</i>	Intro	Click Next.
	Data Drive	<i>If you want to change the drive for storing iA-Examiner data, click Browse and choose a location.</i> Click Next to proceed with installation.
	Complete	Click Finish.

Installing DL-Alert

If you have optional DL-Alert™ software—either the Intelli-Check or Positive Access® version—install it now.

Installer	Screen	Instructions
<i>iA-thenticate CD: iA-thenticate... \ DL-Alert-IC... \ DL-AlertIntelli-Check.exe or iA-thenticate... \ DL-Alert-PA... \ DL-Alert-PositiveAccess.exe</i>	Intro	Click Next to proceed with installation.
	Warning	Note the message and click OK. You will find instructions later in this document for configuring iA-Examiner.
	Complete	Click Finish.

Installing Other Optional Software

If you have other optional software such as ID-Passport, ID-License, or Global-ID, install it now. Follow the instructions included with the optional software.

Restarting

After you finish installing software, restart your PC.

Connecting Hardware and Installing Drivers

Connect the ID-Guard hardware *only after you have installed the software* as described starting on page 3-2.

Connecting Hardware

Note

You may not need to use the second USB connector on the Y cable. This is included to help users who experience power issues. If you do not need the extra connector, simply leave it disconnected.

Your ID-Guard unit may have a Y-shaped USB cable for use with computers that do not supply adequate power through a single USB port. For additional power (especially with a laptop running on batteries), you can plug the extra USB connector into a second USB 2.0 port on the computer.

See page B-9 for problem-solving instructions.

To connect the ID-Guard hardware:

1. Restart the PC after installing the software, and log on as an administrator.
2. Connect the USB cable from the USB port on the back of the ID-Guard unit to an available USB 2.0 port (high-speed, 480 Mbps) on your PC. When you do this, Windows starts automatically installing drivers.

Installing Drivers

Installation of additional drivers varies with the version of Windows. Follow the appropriate instructions below. *If the drivers do not install as described here*, follow the problem-solving instructions on page B-9.

Notes

- Make sure you note the name of the hardware device on the first page of the installation wizard. You will need the name of the device to select the correct driver in step 4. This is especially important in Windows 2000 because the first screen closes when you click Next.
- On some Windows 2000 systems, the Crescentec camera driver will be found automatically. If this happens, accept the “Digital signature not found” warning. If prompted for any additional files (such as CsMini20.sys), browse to C:\BorderGuard\Tools\Crescentec. See page B-9 for additional information.

To install each device driver (repeat as needed):

Windows 2000	Windows XP
<ol style="list-style-type: none"> 1. Make sure you can see the small window that shows the name of the hardware device; this is sometimes hidden behind the wizard. 2. On the first wizard screen, click Next. 3. Select Search for a suitable driver for my device (recommended) and click Next. 4. Select Specify a location and click Next. 5. Browse to the folder shown in the table below and click Next. 6. If the message Digital signature, not found displays, click Yes to continue. 7. If you are asked whether you want to overwrite a newer file, click Yes. 8. Click Finish. 	<ol style="list-style-type: none"> 1. Make sure you can see the small window that shows the name of the hardware device; this is sometimes hidden behind the wizard. 2. If the first wizard screen asks about connecting to Windows Update to search for software, select No, not this time and click Next. 3. Select Install from a list or specific location (Advanced) and click Next. 4. Select Don't search. I will choose the driver to install. Click Next. 5. Click Have Disk and browse to the folder shown in the table below. (If there is no Have Disk button, first click Next and then click Have Disk.) 6. If you see a warning about the digital signature, click Continue Anyway. If you are asked whether you want to overwrite a newer file, click Yes. 7. Click Finish.

Driver files and locations:

For this hardware device:	Browse to this file:
ID Tech USB Serial Converter	C:\BorderGuard\Tools\ID-Tech USB\FTDIBUS.INF
USB 2.0 Camera or Crescentec DC-1100	C:\BorderGuard\Tools\Crescentec\dc1100.inf
ID Tech USB Serial Port or USB Serial Port	C:\BorderGuard\Tools\ID-TechUSB\FTDIPORT.INF

To calibrate the reader:

1. Select Start→Programs→Regula→Document Reader SDK 4.1→Test40.
2. Click Load Library.
3. Click Initialize.
A status message displays the progress.
4. Click Connect.
(You may see a message stating that the firmware does not support device ID storage; this is not an error.)
5. Click Calibrate.

Note

If you connect a different ID-Guard hardware unit, you must re-calibrate.

6. Capture the Test Object side 1 by placing the blank side down on the glass and clicking OK.
7. Capture the Test Object side 2 by placing the checkerboard side down on the glass and clicking OK.
8. When the message displays Verify: Device_Calibration return=0x00000000, calibration is successful.
9. Click Disconnect.
10. Click Free Library.
11. Close the Test40 application.

To configure the Magnetic Stripe Reader:

1. Open Device Manager. (Right-click My Computer, choose Manage, and click Device Manager.)
2. Expand the Ports (COM & LPT) item and find the COM port number assigned to the IDTech USB Serial Port (for example, COM3).
3. Record the port number for use in step 8.
4. Select Start→Programs→iA-thenticate→iA-Examiner.
5. In iA-Examiner, select Mgmt Funcs→System Config.
6. Select Magnetic Stripe Reader.
7. Select Serial.
8. Verify that the Comm Port setting is the number assigned to the IDTech USB Serial Port in Device Manager. If necessary, enter the correct port.
9. Click Apply.

Configuring Hardware and Software

After installation, you may need to set some basic configuration options.

Configuring Internet Explorer

If you use the VerifyMe verification database, follow these steps to configure Internet Explorer:

1. Start Internet Explorer.
2. Select Tools→Internet Options.
3. On the Advanced tab, under the Security heading, deselect Warn if changing between secure and not secure mode.

Configuring a Non-English Version of Windows

If you install this software on a unit running a non-English version of Windows, you may need to follow some additional steps.

To configure Windows 2000—Dutch, French, or Portuguese:

1. Select Start→Run, type DCOMCNFG, and click OK.
2. On the Default Security tab, under Default Access Permissions, click Edit Default.
3. In the displayed list, look for an entry for SYSTEM and also for INTERACTIEF (Dutch), INTERACTIF (French), or INTERATIVO (Portuguese).

If either name is missing, follow these steps to add the missing name or names:

- a. Click Add.
- b. In the drop-down List Frames From list, select the name of your unit.
- c. In the Names list, select the missing name or names and click Add.
- d. Click OK several times to accept the changes.

To configure Windows XP—Dutch, French, or Portuguese:

1. Select Start→Run, type DCOMCNFG, and click OK.
2. Open Component Services, then Computers, then My Computer, and then DCOM Config.
3. Right-click BGServer and choose Properties.
4. On the Security tab, under Launch and Activation Preferences, select Customize and click Edit.
5. If the displayed list does not include INTERACTIEF (Dutch), INTERACTIF (French), or INTERATIVO (Portuguese), add the appropriate name and select all the Allow permissions.
6. In the same list, select all the Allow permissions for SYSTEM. Then click OK.
7. Back on the Security tab of the BGServer Properties window, under Access Permissions, select Customize and click Edit.
8. In the displayed list, select both of the Allow permissions for SYSTEM and for INTERACTIF, INTERATIVO, or INTERACTIEF. Then click OK.
9. In the BGServer Properties window, click OK. Then close the Component Services window.

Controlling Access

This section explains how to create local user groups and set file permissions for your system so that different users have just the access they need.

Creating Local User Groups and Users

First, create two local user groups and assign users to these groups as needed.

1. Create these two local user groups:

iA-thenticate Users
iA-thenticate Administrators

2. Create as many users as you need for the people who will use the system, and make each one a member of the appropriate user group:

Local User Group	Users Who Should Belong to This Group	Access Allowed
iA-thenticate Users	Personnel who use iA-Examiner to test and examine documents	iA-Examiner: user functions
iA-thenticate Administrators	Technical administrators, security managers, and operations managers	iA-Examiner: user and management functions iA-Administrator All Users startup folder (C:\Documents and Settings\All Users\Start Menu\Programs\Startup)

Assigning File and Folder Permissions

Assigning file and folder permissions ensures that each group of users can run the appropriate programs.

To assign file and folder permissions:

1. Follow steps a–c for each file in the table below:
 - a. Right-click the file and choose Properties.
 - b. Select the Security tab.
 - c. In the Name list, remove the entries for Everyone and Users (if listed). Then add Read & Execute permissions for user groups as indicated in the table.

For this file in C:\BorderGuard\Bin\	Assign Read & Execute permissions for these groups
iA-Administrator.exe (iA-Administrator)	iA-thenticate Administrators
BGDataPort.exe (iA-DataPort)	iA-thenticate Users iA-thenticate Administrators
BGExaminer.exe (iA-Examiner)	iA-thenticate Users iA-thenticate Administrators
BGServer.exe (ID-Server)	iA-thenticate Users iA-thenticate Administrators
ExaminerConfiguration (iA-Examiner configuration)	iA-thenticate Administrators
ExaminerManager (iA-Examiner management)	iA-thenticate Administrators

For this file in C:\BorderGuard\Bin\	Assign Read & Execute permissions for these groups
ExaminerReport (iA-Examiner reporting)	iA-thenticate Administrators
ExaminerViewer (iA-Examiner document review)	iA-thenticate Administrators
iA-SecondaryStation.exe (Secondary Station)	iA-thenticate Users iA-thenticate Administrators

2. iA-thenticate Administrators must be able to change startup settings for All Users. Follow these steps to assign the needed permissions to C:\Documents and Settings\All Users\Start Menu\Programs\Startup:

- Right-click folder C:\Documents and Settings and choose Properties.
- Select the Security tab.
- Add Full Control permissions for the iA-thenticate Administrators group.
- Repeat steps a-c for each successive folder in the path:

All Users (inside Documents and Settings)
Start Menu (inside All Users)
Programs (inside Start Menu)
Startup (inside Programs)

3. If you use Windows security to limit users' access to various folders on your system, *all iA-thenticate users* must have these permissions:

- Full control to the work folder, normally C:\BorderGuard\Working
- Read and execute access to C:\BorderGuard and all of its sub-folders
- Read, write, and execute access to:
 - C:\BorderGuard\Config\SampleScan.cfg
 - The folder for storing captured images—for example, C:\BorderGuard\Images
 - The folder containing the iA-Examiner database BGExaminer.mdb, normally C:\BorderGuard\Bin
 - If you use TextWatch, the folder containing the TextWatch database iAT.sys, normally C:\BorderGuard\Bin

In addition, *iA-thenticate administrators* must have these permissions:

- Write access to:
 - The folder containing the iA-Administrator database Administrator.mdb, normally C:\BorderGuard\Bin
 - The Windows registry
- Read, write, and execute access to:
 - The configuration folder, C:\BorderGuard\Config and all sub-folders

Installing an Optional Reader or Scanner

If your system includes a flatbed scanner, install it now by following the instructions in chapter. See “Installing an Optional Reader or Scanner” on page 4-1.

What's Next?

Your iA-thenticate system is now set up to work using factory-default settings. Probably you will want to change some of those settings. Part Two of this guide explains how.

Setting Up an ID-Guard Unit

Installing an Optional Reader or Scanner

You can add bar code and magstripe readers to your system for processing documents that have 2D bar codes and magnetic stripes. You can also add a flatbed scanner for capturing images of documents that are larger than the glass platform on your BorderGuard or ID-Guard unit.

Installing the E-Seek Intelli-Check Reader

Viisage recommends and supplies the E-Seek Intelli-Check combination bar code and magstripe reader for your BorderGuard unit. It is available in *serial* and *USB* models. The reader is preconfigured to work with your iA-thenticate system. However, if it should lose its settings, you can restore them as explained on page B-13.

Serial Model

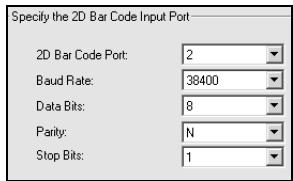
Follow these instructions if your reader has a *serial* connection.

To install the E-Seek Intelli-Check serial reader:

1. Locate the longer serial cable supplied with the reader. Plug its 9-pin D connector into a serial port on your PC.
2. Plug the other end of the cable into the E-Seek Intelli-Check reader.
3. Plug the cable from the supplied power adapter into the reader. Then plug the power adapter into a surge-protected power source that meets the requirements printed on the adapter. The reader beeps three times when you connect the power.
4. *If you are using iA-Examiner*, configure it to use the reader:
 - a. Start iA-Examiner by double-clicking its icon on the desktop or by selecting Start→Programs→iA-thenticate→iA-Examiner.
 - b. In iA-Examiner, click Mgmt Funcs and then System Config.
 - c. On System Configuration Page 1, under Peripherals, select E-Seek Reader.
 - d. Click Apply and then Done.



5. If you are using *iA-DataPort*, configure it to use the reader:



- Start *iA-DataPort* by double-clicking its icon on the desktop or by selecting Start→Programs→*iA-authenticate*→*iA-DataPort*.
- Choose **Settings**→**Comm Ports Settings**.
- For 2D Bar Code Port, select the port you chose in step 1.
- Click **OK**.

This completes the installation of the serial reader.

USB Model

Note

When you plug in the USB cable, the system *should* install drivers automatically. But if the new-hardware wizard runs, follow the steps listed on page B-2 (for color BorderGuard) or B-4 (for color BorderGuard B4500/5000) to install the drivers.

Follow these instructions if your reader has a *USB* connection.

To install the E-Seek Intelli-Check USB reader:

- If you are using *iA-Examiner*, configure it to use the reader:
 - Plug the reader's USB cable into an available USB port and wait while the system automatically installs drivers. (If this doesn't happen, and the new hardware wizard runs instead, refer to Appendix B for troubleshooting instructions.)
 - Start *iA-Examiner* by double-clicking its icon on the desktop or by selecting Start→Programs→*iA-authenticate*→*iA-Examiner*.
 - In *iA-Examiner*, click **Mgmt Funcs** and then **System Config**.
 - On System Configuration Page 1, under **Peripherals**, select **E-Seek Reader**.
 - Click **Apply** and then **Done**.
- If you are using *iA-DataPort*, configure it to use the reader:
 - If you have already followed step 1 to configure *iA-Examiner*, find the reader's port number by going back to System Configuration Page 1 and noting the **Comm Port Number** assigned to the E-Seek reader. Then *skip to step e*.
 - Otherwise, with the system running, open the Device Manager. (Right-click **My Computer**, choose **Manage**, and click **Device Manager**.)
 - Expand the **Ports (COM & LPT)** item so you can see any entries under it. The list may already contain an entry named **USB Serial Port**. In the next step an *additional* entry named **USB Serial Port** will appear with a different COM number.
 - Plug the reader's USB cable into an available USB port. As you do, watch for the new **USB Serial Port** entry to appear. Note the COM number assigned to the new entry. For example, it might be listed as **USB Serial Port (COM4)**.
 - Start *iA-DataPort* by double-clicking its icon on the desktop or by selecting Start→Programs→*iA-authenticate*→*iA-DataPort*.
 - Choose **Settings**→**Comm Ports Settings**.
 - For 2D Bar Code Port, select the number you found in step c. Click **OK**.

This completes the installation of the USB reader. If you later unplug the reader and plug it into a different USB port, your system may want to reinstall USB drivers and assign a different COM port number. In this case you must reconfigure *iA-DataPort* for the new port number.

Installing a Flatbed Scanner

Note

The automatic cropping option does not currently work properly with the Canon model.

The iA-thenticate system is designed to work with any TWAIN-compliant USB flatbed scanner. Viisage has tested and qualified two models: *Canon CanoScan LiDE 500F* and *Epson Perfection 3490 Photo*.

To install the flatbed scanner:

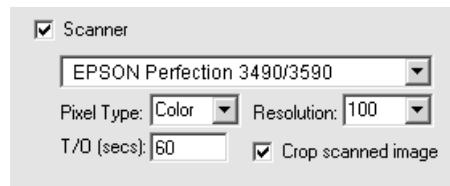
- ♦ Follow the manufacturer's instructions for installing the scanner software and hardware.

To configure the system to use the scanner:

1. Run iA-Examiner (Start→Programs→iA-thenticate→iA-Examiner). Click Mgmt Funcs, and then System Config.

2. On System Configuration Page 1, under Peripherals, select Scanner.

3. From the drop-down list, select the scanner you have installed. If you see two similar entries for your scanner, select the one that does *not* start with WIA.



Be careful not to select the iA-thenticate camera, listed as OVT SuperCam.

4. For Pixel Type, select either Color or Grayscale to choose the type of image you want to scan, display, and store. Because of JPEG compression, color images take only slightly more disk space than grayscale.

5. For Resolution, select a value that provides the readability and detail you need. The default value of 100 dpi gives decent readability, small files, and quick scanning. Higher resolutions give better detail but also larger files and slower scans. The system stores scans in JPEG format using the Image Quality setting specified under Saving Data. Here are some sample file sizes for an 8.5x11-inch document with Image Quality set to Medium:

Resolution	Pixel Type	File Size
100 dpi	Grayscale	38 KB
	Color	40 KB
200 dpi	Grayscale	152 KB
	Color	167 KB
300 dpi	Grayscale	314 KB
	Color	349 KB

6. For T/O (timeout), use the default value of 60 seconds unless you have a reason to change it. This is the amount of time the system will wait for a scan to finish before it cancels the scan.

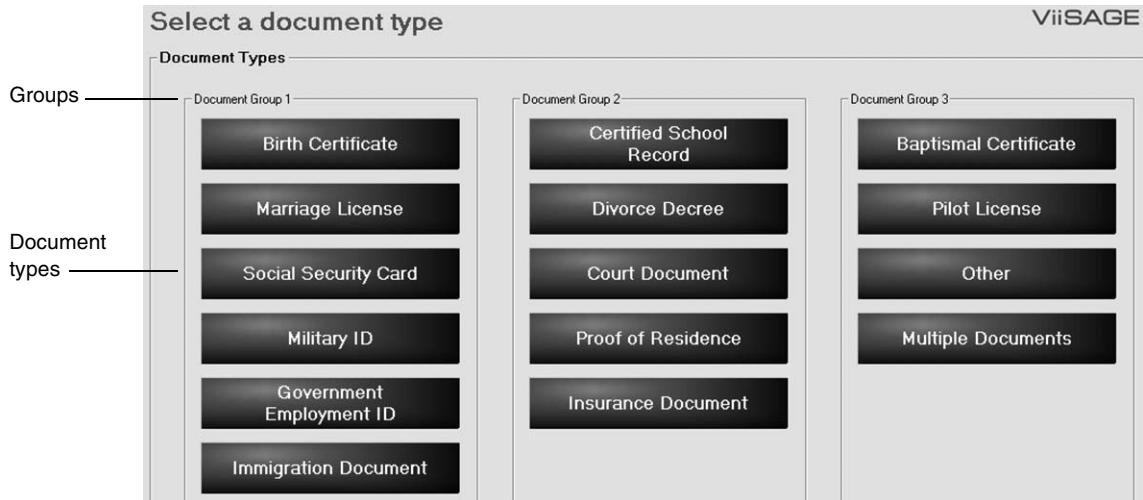
7. Select Crop Scanned Image unless you always want to display and save the scanner's entire platform area.

Note

If you see an error message or unexpected behavior when using the scanner, refer to the problem-solving section on page B-14.

8. Under Saving Data, be sure to select Save Document Images and Visible, or the scanned images will not be saved. Whether you select Convert Images to JPEG or not, scanned images are always saved as JPEGs using the Image Quality setting.
9. Click **Apply**. Restart iA-Examiner to put the changes into effect.

You can also change the scanned-document types and how they are grouped, if necessary. When scanning a document, the operator sees these types displayed on the screen and chooses one:



You can change the name above each group of buttons, the number of buttons in each group, and the document type that appears on each button.

This procedure requires you to directly edit an important configuration file. Do not proceed unless you are comfortable editing such files. Make no changes other than to the indicated text, and be sure to keep all quotation marks as they are.

To change the scanned-document types and groups:

1. In My Computer or Windows Explorer, find C:\BorderGuard\Config\BGExaminerLanguage.cfg and make a backup copy of it for safekeeping.
2. Open BGExaminerLanguage.cfg in a Unicode text editor such as Notepad, and find this section (about halfway through the file):

```

; Document Types Control
; Document Types Frame
DOC_TYPES_FRAME"Document Types"

; Document Group Frames
DOC_TYPES_GROUP_1"Document Group 1"
DOC_TYPES_GROUP_2"Document Group 2"
DOC_TYPES_GROUP_3"Document Group 3"

; Document Types
DOC_TYPES_DOCUMENT_1"Birth Certificate"
DOC_TYPES_DOCUMENT_2"Marriage License"
DOC_TYPES_DOCUMENT_3"Social Security Card"
DOC_TYPES_DOCUMENT_4"Military ID"
DOC_TYPES_DOCUMENT_5"Government Employment ID"
DOC_TYPES_DOCUMENT_6"Immigration Document"

```

```
DOC_TYPES_DOCUMENT_7""
DOC_TYPES_DOCUMENT_8"Certified School Record"
DOC_TYPES_DOCUMENT_9"Divorce Decree"
DOC_TYPES_DOCUMENT_10"Court Document"
DOC_TYPES_DOCUMENT_11"Proof of Residence"
DOC_TYPES_DOCUMENT_12"Insurance Document"
DOC_TYPES_DOCUMENT_13""
DOC_TYPES_DOCUMENT_14""
DOC_TYPES_DOCUMENT_15"Baptismal Certificate"
DOC_TYPES_DOCUMENT_16"Pilot License"
DOC_TYPES_DOCUMENT_17"Other"
DOC_TYPES_DOCUMENT_18"Multiple Documents"
DOC_TYPES_DOCUMENT_19""
DOC_TYPES_DOCUMENT_20""
DOC_TYPES_DOCUMENT_21""
```

3. To change the names above the button groups, replace Document Group 1, Document Group 2, and Document Group 3 with the names you want displayed.
4. To change the document types, replace Birth Certificate and so on with the names you want on the buttons. Types 1–7 belong to the first group, 8–14 to the second group, and 9–21 to the third group. If you leave a type blank (""), no button will be displayed in that position.
5. Save the changed file and test iA-Examiner for proper operation. If anything goes wrong, replace the changed file with the backup copy you made of the original file.

Installing an Optional Reader or Scanner

Part Two

Configuring and Managing iA-thenticate

5

Using the

Administration Tools

You use two administration tools to configure iA-thenticate:

- iA-Administrator
- iA-Examiner (Management Functions)

This chapter introduces these tools, and the following chapters explain how to use them to configure your iA-thenticate system.

iA-Administrator

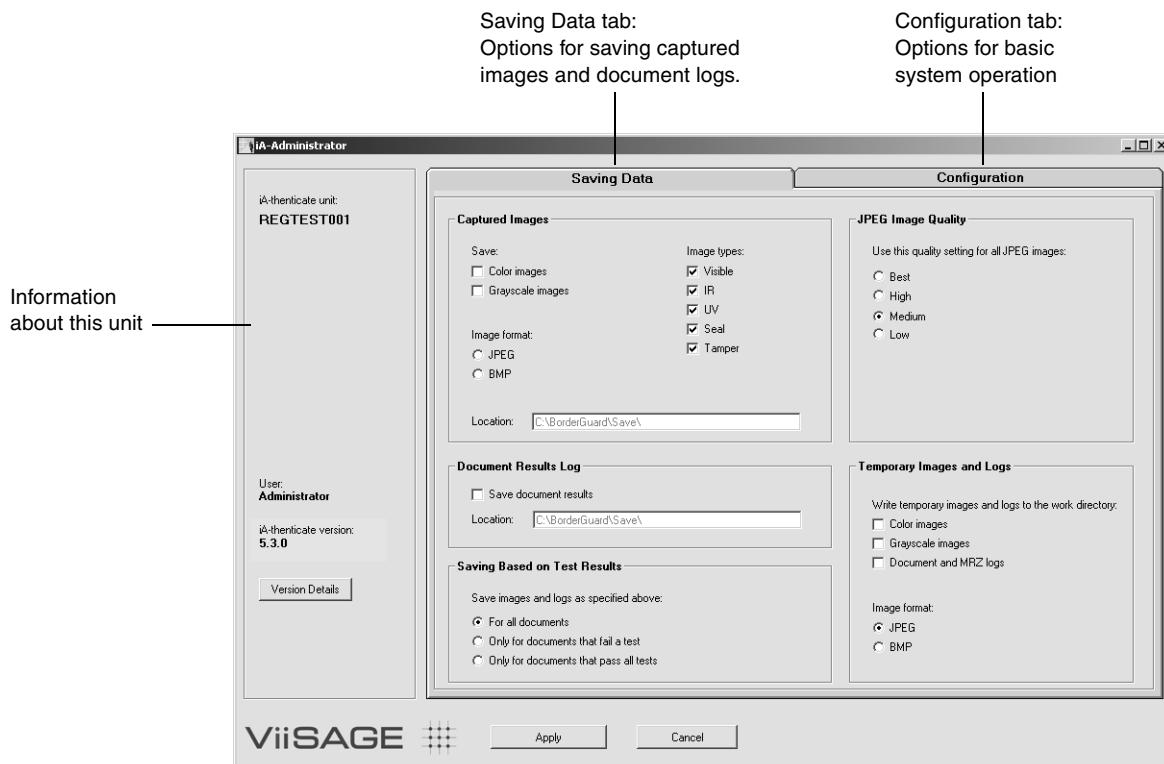
You use iA-Administrator to:

- View information about your system
- Set options for basic system operation
- Set options for saving captured images and document logs—if you do *not* use iA-Examiner to save images and logs

To run iA-Administrator:

1. Log on as a local administrator or member of the iA-thenticate Administrators user group.
2. Select Start→Programs→iA-thenticate→iA-Administrator.

The iA-Administrator screen looks like this:



iA-Examiner

iA-Examiner is the primary program that operators use for processing documents. In addition to its operator screens, it has a section of Management Functions screens that let you set options beyond those you set with iA-Administrator.

You use the iA-Examiner management screens to:

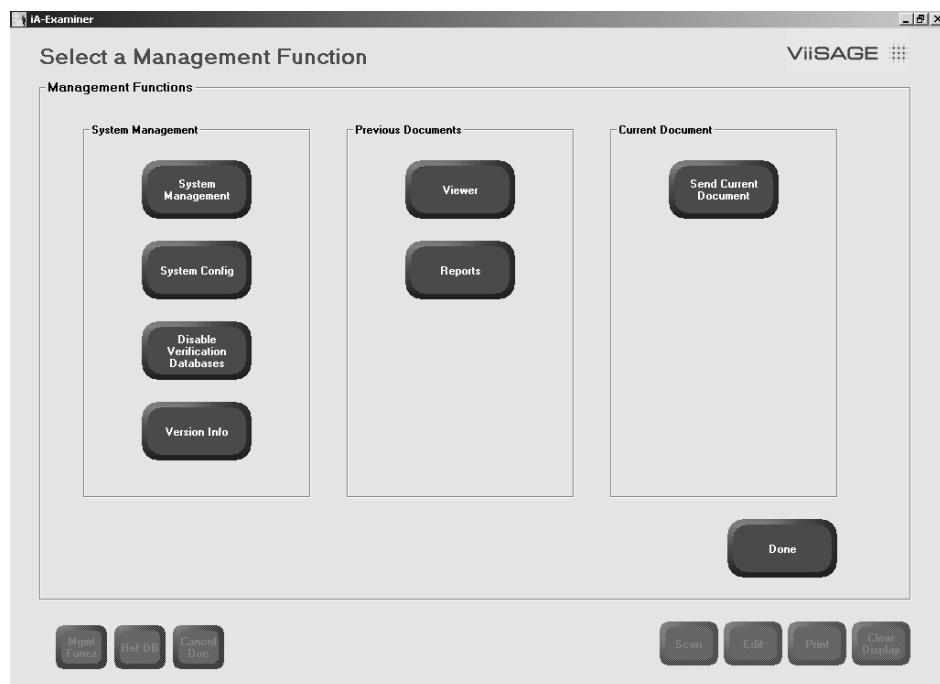
- Set options for saving captured images and document logs
- Control details of iA-Examiner appearance and behavior
- Choose document testing options
- Enable optional iA-Examiner features
- Configure a magstripe and bar code reader and a printer

Note

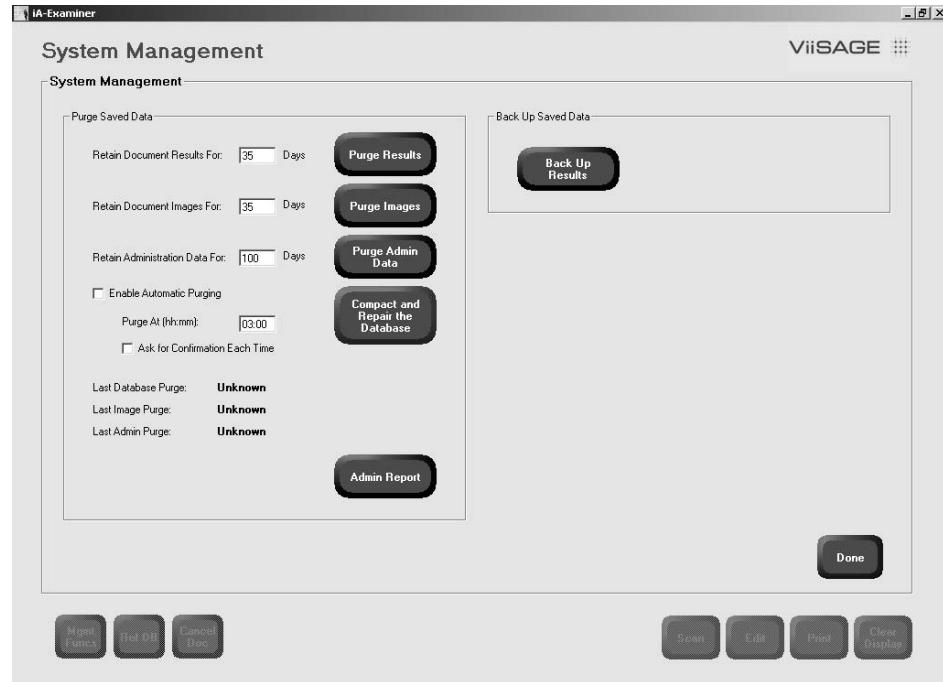
Access to the management screens is restricted when you use the recommended security setup described on page 2-9 for BorderGuard units or 3-8 for ID-Guard units.

To use iA-Examiner's management functions:

1. Log on as a local administrator or member of the iA-thenticate Administrators user group.
2. Run iA-Examiner by double-clicking the iA-Examiner icon on your desktop or by selecting Start→Programs→iA-thenticate→iA-Examiner.
3. On the main iA-Examiner screen, click Mgmt Funcs. You can then click System Management or System Config to accomplish various management and configuration tasks.



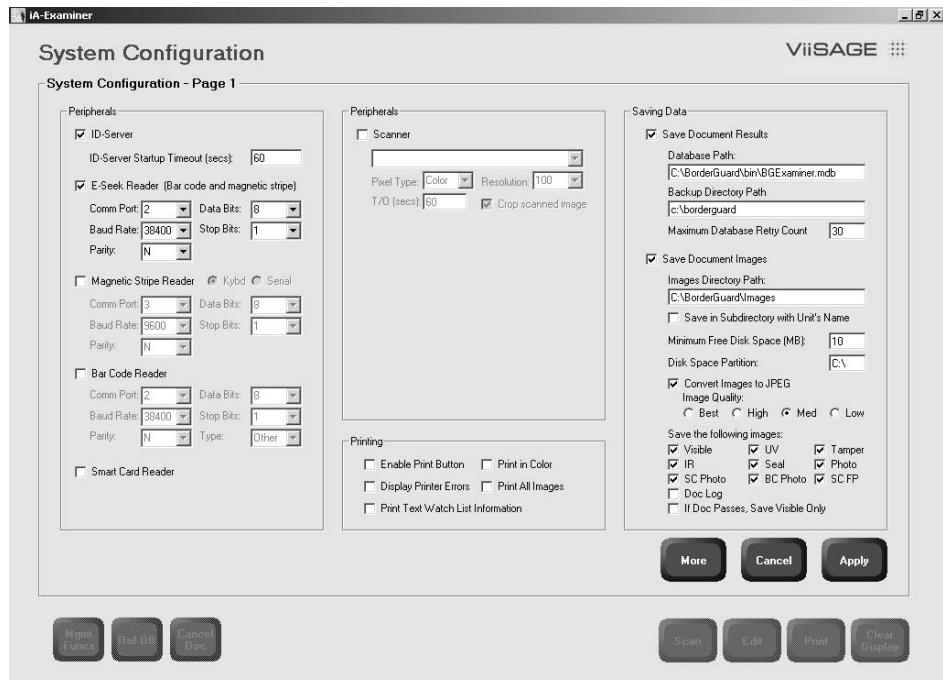
The System Management screen mostly lets you manage saved data:



Note

Use the More and Back button to move between the System Configuration pages in iA-Examiner.

The System Configuration screen lets you set a variety of options (on multiple pages) for peripheral configurations, driver's license and ID processing, printing, data saving, document testing, screen display, and other features:



What's Next?

Use the following chapters to learn how to use iA-Administrator and iA-Examiner to configure your system's operation:

- ❑ Chapter 6, “Quick Configuration Guide”

This is a compact guide for configuring the settings and options that are most important for most installations. It may be all you need to configure your system.

If you need more-detailed information, see the following chapters.

- ❑ Chapter 7, “Configuring iA-thenticate”
(using iA-Administrator)
- ❑ Chapter 8, “Configuring iA-Examiner”
(using the iA-Examiner configuration screens)
- ❑ Chapter 9, “Managing iA-Examiner”
(using iA-Examiner management functions)

6

Quick Configuration Guide

The next two pages are a compact guide for configuring the settings and options that are most important for most installations. The Quick Configuration Guide assumes you are using iA-Examiner and not iA-DataPort.

For detailed information about all the available options, see chapters 7–9.

Quick Configuration Guide

Configuring Data Saving and Purging

iA-Examiner: System Configuration Page 1

The screenshot shows the 'Saving Data' section of the configuration page. It includes fields for 'Save Document Results' (checked), 'Database Path' (C:\BorderGuard\bin\BGEExaminer.mdb), 'Backup Directory Path' (c:\borderguard), 'Maximum Database Retry Count' (30), 'Save Document Images' (checked), 'Images Directory Path' (C:\BorderGuard\Images), 'Save in Subdirectory with Unit's Name' (unchecked), 'Minimum Free Disk Space (MB)' (100), 'Disk Space Partition' (D:\), 'Convert Images to JPEG' (checked), 'Image Quality' (Med), and 'Save the following images' (checkboxes for Visible, UV, Tamper, IR, Seal, Photo, SC Photo, BC Photo, SC FP, Doc Log, and 'If Doc Passes, Save Visible Only' checked).

- Select Save Document Results, Save Document Images.
- Specify Database Path, Backup Directory Path. (To share one database, see page 8-8.)
- Specify Images Directory Path, and the same drive letter for Disk Space Partition.
- Optional: Select Save in Subdirectory.
- Specify 100 MB or more for Minimum Free Disk Space.
- Select Convert Images to JPEG and Med.
- Under Save the following images: Select all image types, deselect Doc Log, and optionally select If Doc Passes.

iA-Examiner: System Management

The screenshot shows the 'Purge Saved Data' section. It includes fields for 'Retain Document Results For' (35 Days), 'Retain Document Images For' (35 Days), 'Retain Administration Data For' (100 Days), 'Enable Automatic Purging' (checked), 'Purge At (hh:mm)' (03:00), and 'Ask for Confirmation Each Time' (unchecked).

- Specify the purging options you want to use.

Configuring Printing

Start→Settings→Printers

- Select the printer you want to use and select it as the default (File→Set As Default Printer).

iA-Examiner: System Configuration Page 1

The screenshot shows the 'Printing' section. It includes checkboxes for 'Enable Print Button' (checked), 'Print in Color' (unchecked), 'Display Printer Errors' (unchecked), 'Print All Images' (unchecked), and 'Print Text Watch List Information' (unchecked).

- Select Enable Print Button.
- Select any other options you want to use.

Configuring an Optional Reader

Do this only if you are using a magstripe or bar code reader other than the E-Seek Intelli-Check model.

iA-Examiner: System Configuration Page 1

The screenshot shows the 'Reader' section. It includes two sections: 'Magnetic Stripe Reader' (checked) with options for Comm Port (3), Data Bits (8), Baud Rate (9600), Stop Bits (1), and Parity (N); and 'Bar Code Reader' (checked) with options for Comm Port (2), Data Bits (8), Baud Rate (38400), Stop Bits (1), and Parity (N).

- Select Magnetic Stripe Reader if you are using one, and choose the appropriate options for your reader.
- Select Bar Code Reader if you are using one, and choose the appropriate options for your reader.

For more information, see page 8-2.

Configuring Testing

iA-Examiner: System Configuration Page 2

Tests

Checksum Test

- Max. Questionable Characters:
- Hide Expected Checksum
- Hide Questionable Character Count
- Enable MRZ Data Edit
- MRZ Edits Affect All Data and Tests
- Display Checksum Correct. Screen On Alert

TextWatch Test

- Enable TextWatch
- TextWatch Database Path:
- Display a match on any of the following:
 - Match By Name
 - Match By Document Number

Document Watch Test

- Enable Document Watch
- Document Watch Database Path:

Pattern Tests

- Display Pattern Confidence

Legal Age Test

- Enable Legal Age Test
- Minimum Legal Age:

Document Cross-CheckTest

- Enable Document Cross-Check Test

Smart Card Test

- Enable Smart Card Cross-Check Test

Identification Test

- Enable Identification Test

- For typical operation, accept the defaults for your system (which may differ from the ones shown).
- Otherwise see page 8-9.

Configuring a Smart-Card Unit

iA-Administrator: Configuration tab

Signals and Alerts

- Beep when the operator may remove the document
- Warn when the operator removes a document too soon
- Beep when the operator removes a document too soon:
 - 1/4 second
 - 1/2 second
 - 350 Hz
 - 440 Hz

- Deselect both Beep when options.

iA-Examiner: System Configuration Page 1

Peripherals

- ID-Server
- ID-Server Startup Timeout (secs):
- Comm Port: Baud Rate: Parity:
- Smart Card Reader

- Select Smart Card Reader.

iA-Examiner: System Configuration Page 2

Tests

Checksum Test

- Max. Questionable Characters:
- Hide Expected Checksum
- Hide Questionable Character Count
- Enable MRZ Data Edit
- MRZ Edits Affect All Data and Tests
- Display Checksum Correct. Screen On Alert

TextWatch Test

- Enable TextWatch
- TextWatch Database Path:

Pattern Tests

- Display Pattern Confidence

Legal Age Test

- Enable Legal Age Test
- Minimum Legal Age:

Document Cross-CheckTest

- Enable Document Cross-Check Test

Smart Card Test

- Enable Smart Card Cross-Check Test

- Select Display Checksum Correct. Screen On Alert.
- Optional: Select Enable Smart Card Cross-Check Test.

iA-Examiner: System Configuration Page 5

Smart Card Options

- Smart Card Timeout (secs):
- Placement Timeout (secs):
- Placement Timeout Action:
 - Fail Smart Card Test
 - Ignore Smart Card
- Prompt for Smart Card:
 - By Document Profile
 - Always
- Automatically Display MRZ Edit Screen For BAC
- Country Signing Certificate Folder Path:

Disable Reading of These Optional Data Groups:

- DG3 - Fingerprint
- DG11 - Personal
- DG4 - Iris
- DG12 - Document
- DG5 - Portrait
- DG13 - Optional
- DG6 - Signature
- DG7 - Signature

- Select Fail Smart Card Test.
- Deselect Prompt for Smart Card.
- If you process Basic Access Control cards, select Automatically Display MRZ Edit Screen for BAC.
- Optional: Select data groups not to read.

Configuring Document Processing

iA-Examiner: System Configuration Page 3

iA-Examiner is the Primary Program

- iA-Examiner is the Primary Program
- Don't Use Document Sets
- Let Operator Add Documents to Set

- For typical operation, select iA-Examiner Is the Primary Program and select the Document Sets option you want to use.

Otherwise see page 8-12.

Configuring iA-thenticate

Note

Before you read this chapter, see chapter 6, “Quick Configuration Guide.” It may contain all the information you need to get your system up and running.

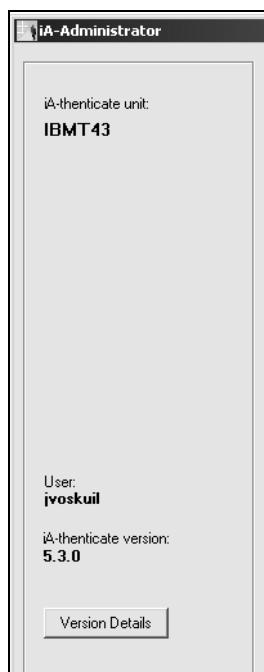
This chapter explains how you use iA-Administrator to:

- View information about your system
- Set options for basic system operation
- Set options for saving captured images and document logs—if you do *not* use iA-Examiner to save images and logs

Chapter 5, “Using the Administration Tools,” introduces iA-Administrator, tells how to start it, and gives an overview of its screen.

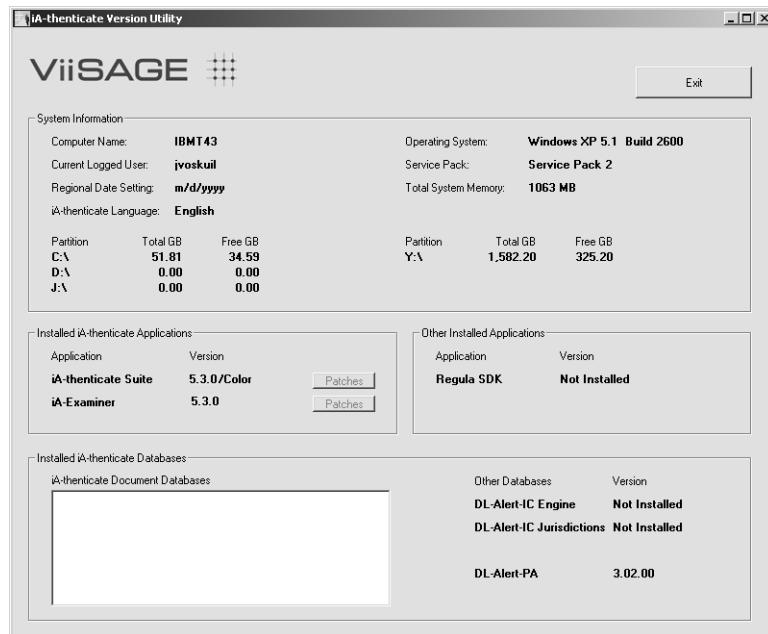
Chapter 8, “Configuring iA-Examiner,” describes additional ways to control and configure your system using iA-Examiner.

Viewing Unit Information



The left side of the iA-Administrator screen shows your system's computer name, the name of the logged-on user, and the iA-thenticate software version. It also includes a button for viewing detailed version information.

Clicking Version Details runs the iA-thenticate Version Utility, which shows detailed information about the installed software:

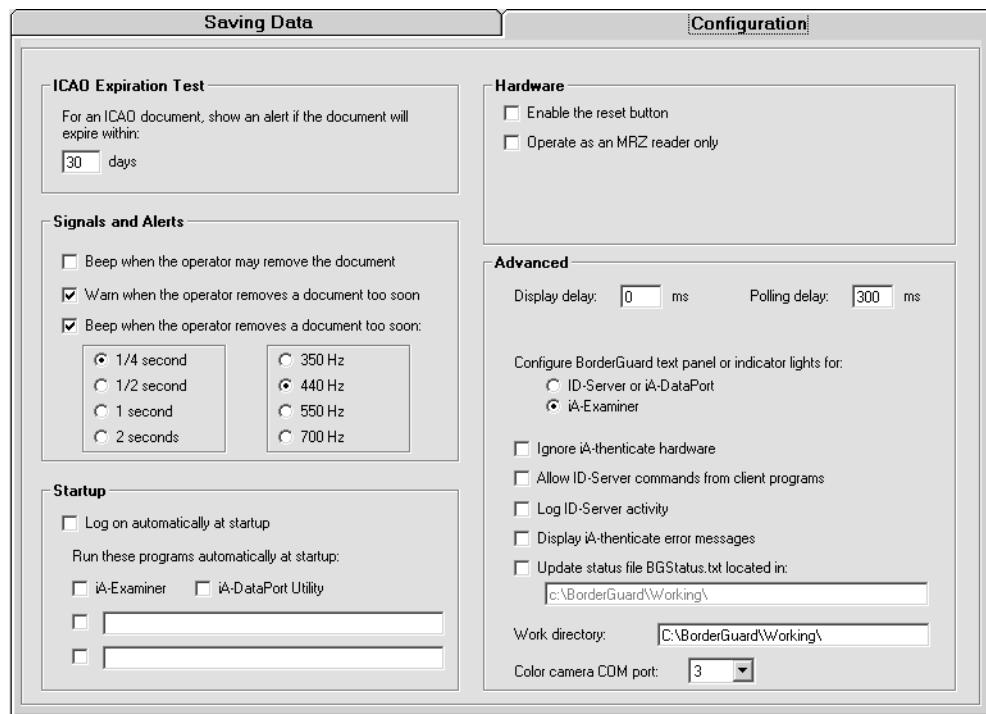


Note

You can also run the iA-thenticate Version Utility by choosing *Start→Programs→iA-thenticate→iA-VersionUtility*.

Setting Options for Basic Operation

To set options for basic operation, run iA-Administrator (Start→Programs→iA-thenticate→iA-Administrator) and click the Configuration tab. In each section of the screen, set the options according to the following descriptions and recommendations.



Note

Some options appear only for certain hardware configurations, as noted in the descriptions.

ICAO Expiration Test

Option	Description	Recommendations
For an ICAO document, show an alert if the document will expire within __ days	Displays an alert for an <i>ICAO</i> document if it expires within this number of days. (When iA-Examiner tests the expiration date of a <i>non-ICAO</i> license or ID by reading the magstripe or bar code, it displays an alert only if the document has already expired.)	Use the default value of 30 days unless you want the alert displayed farther in advance or not as far.

Signals and Alerts

You can use audio signals and alerts with an iA-thenticate Plus unit (which has a small built-in speaker) and with a standard iA-thenticate unit attached to a PC with a sound card and speaker.

Option	Description	Recommendations
Beep when the operator may remove the document	Beeps (using the standard system beep) when testing is complete and the operator may safely remove the document.	Deselect this if you are using a smart card reader. Otherwise, select it if you want this feature.
Warn when the operator removes a document too soon	Displays a message when the operator removes a document before testing is complete.	
Beep when the operator removes a document too soon	Beeps at the selected frequency and for the selected time when the operator removes a document before testing is complete. (This option does not apply to ID-Guard units.)	Deselect this if you are using a smart card reader. Otherwise, select it if you want this feature. If several systems are located near each other, you can choose different beep frequencies to make them distinctive.

Startup

You can set up your system to log on and run programs automatically at startup.

Option	Description	Recommendations
Log on automatically at startup	Bypasses the Windows logon screen at startup and logs on as user autologon. You can change this setting only if your user account allows you to edit the Windows registry.	<i>We do not recommend using this option in a production environment, because it bypasses normal Windows logon security.</i>
Run these programs automatically at startup	After Windows starts, runs the selected programs automatically. To add a program, type its full pathname. Selected programs are added to the Startup program group for All Users: C:\Documents and Settings\All Users\Start Menu\Programs\Startup\	Select the programs you want to run at startup. If you select more than one program, one may hide another after startup. If you select no programs, the Windows desktop appears after startup.

Restoring Normal Logon

If you select Log on automatically at startup, Windows never displays the logon screen. To temporarily bypass automatic logon and disable automatic logon, you must follow special procedures.

To bypass automatic logon temporarily:

1. While starting or restarting the system, press and hold the Shift key until the Logon dialog box appears.
2. Log on in the usual way.

To disable automatic logon:

1. Log on as a local administrator or using another account that allows you to edit the Windows registry.
2. Run iA-Administrator.
3. Deselect Log on automatically at startup and click **Apply**.

Hardware

These settings may vary depending on your hardware unit.

Option	Description	Recommendations
Enable the reset button	Activates the reset button on the back of some older BorderGuard units, so that pressing it shuts down the unit. This works only when the iA-thenticate software is running.	Select this <i>only</i> if you have a BorderGuard Plus unit (with built-in PC) that you are using as a compact, self-contained unit without monitor or keyboard, as explained in the <i>iA-Administrator's Guide</i> that came with your unit. The reset button lets you properly shut down such a unit.
Operate as an MRZ reader only	Captures and tests only visible and IR images and skips all pattern and brightness tests.	Select this only if you need maximum processing speed and you do not need the excluded images and test results.

Software

These settings apply only to the B4500/5000.

Option	Description	Recommendations
Best Quality Mode	Default setting.	Keep this setting for most applications.
Fast Mode	Not recommended.	Contact Viisage technical support before switching to this mode. Reboot after switching modes.

Advanced

You will probably never need to change any of the following advanced options. You should leave them alone unless you have a specific reason to change them.

Option	Description	Recommendations
Display delay	How long the system displays the test results from the last document processed before it starts looking for a new document to process. After it starts looking, it keeps polling according the Polling delay value (next).	Use the default value of 0 ms.
Capture delay	Adjusts capture timing. (Appears only if you have an ID-GUARD unit.)	<p>Do not change unless needed for troubleshooting.</p> <p>You may need to increase the capture delay if the system fails to identify documents and the visible image looks like an IR image, or if you experience other problems associated with underpowered PC. See “ID-Guard” in Appendix B for troubleshooting instructions.</p>
Polling delay	How long the system waits between checks to see if a new document has been placed on the document platform.	Use the default value.
Configure BorderGuard text panel or indicator lights for	Which program controls the messages on the built-in text panel, or the indicator lights, on a BorderGuard unit.	<p>If you use iA-Examiner as your primary application, select iA-Examiner. If you use iA-DataPort as your primary application, select ID-Server or iA-DataPort.</p> <p>If you use a custom program as your primary application, and it is designed to write information to the text display, select iA-Examiner. Otherwise select ID-Server or iA-DataPort.</p>
Ignore iA-thenticate hardware	Operates as if the hardware components (camera, lights, and so on) are not connected.	Do not select this except for testing purposes.
Allow ID-Server commands from client programs	Not currently used.	Leave this deselected.
Log ID-Server activity	Records ID-Server activity in a log file named <code>iaT_Log.txt</code> . This file is saved in the work directory (see below).	Do not select this except for troubleshooting purposes.
Display iA-thenticate error messages	Displays extra error messages that do not normally affect operation and are not normally displayed.	Do not select this except for troubleshooting purposes.

Option	Description	Recommendations
Update status file BGStatus.txt located in	Constantly updates a file named BGStatus.txt in the specified directory with the system's current status. Other programs can then monitor the status by reading this file.	Do not select this unless you are running a custom program that needs to read this file.
Work directory	The directory used for storing various work files.	Use the default directory (C:\BorderGuard\Working\ unless you have a reason to change it.
Color camera COM port	The COM port where the color camera is connected, set during installation. Appears only if you have a color BorderGuard or color BorderGuard B4500/5000 unit.	For further information, see pages 2-3 and 2-5. A value of INV (invalid) means the port number is greater than 255. Contact Viisage Customer Support if you need help resolving this issue.

Setting Options for Saving Images and Logs

You can configure the system to save captured document images as well as text logs containing document information and test results. You may want to save these files for various reasons related to security, operations, and record-keeping.

Two Ways to Save Images and Logs

You can set options for saving images and logs here in iA-Administrator or in iA-Examiner. The two ways are independent of each other, and you can use either one.

- If you use iA-Examiner to process documents, it's generally easiest to use iA-Examiner to save images and logs as well. And it offers more options than iA-Administrator.
- Unless you have a special reason to do so, you should not save images and logs using *both* iA-Administrator and iA-Examiner.

This table compares the two ways.

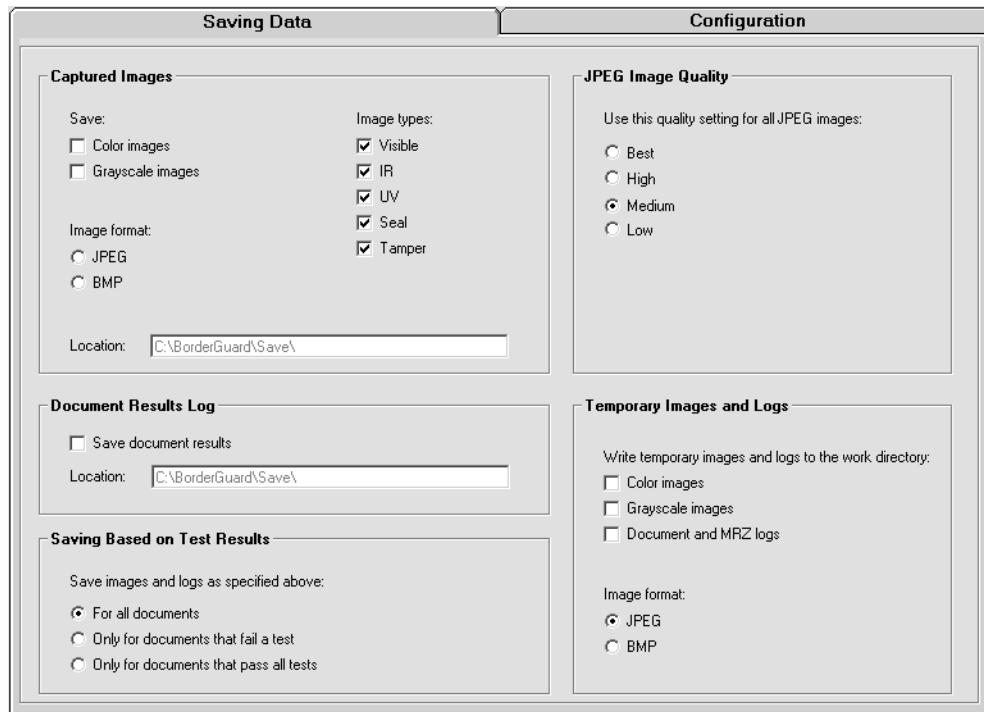
Using iA-Administrator...	Using iA-Examiner...
You can save images in JPEG (.jpg) format with several levels of compression, or in uncompressed Bitmap (.bmp) format.	The same.
You can select the image types you want to save—any combination of visible, IR, UV, seal, and tamper.	In addition to the visible, IR, UV, seal, and tamper images, you can save the ID photo from the visible image, the ID photo from a 2D bar code, and the ID photo and finger-print image from a smart card.

Note

ID-Guard does not capture UV, seal, or tamper images.

Using iA-Administrator...	Using iA-Examiner...
On monochrome BorderGuard systems you can save grayscale images. On color BorderGuard, color BorderGuard B4500/5000, and ID-Guard systems you can save color images, grayscale images, or both.	On monochrome BorderGuard systems you can save grayscale images. On color BorderGuard, color BorderGuard B4500/5000, and ID-Guard systems you can save only color images.
You can save the selected images and logs for all documents, or only for those that pass all tests, or only for those that fail a test.	You can save the selected images and data for all documents. Or, for documents that pass all tests, you can save the visible image alone.
You save document results in an individual plain-text (.txt) log file for each document.	You save document results in a single database (.mdb) file for all documents. You can also save individual XML log files for custom processing.
The document results lack some of the information that iA-Examiner is able to record.	The document results contain additional information, including details about licenses and IDs, data retrieved from verification databases, data the operator enters manually, data from smart cards, and more.
Administrator includes no facility for viewing previously captured images and linking them to saved document information and test results.	You can use the Viewer feature in iA-Examiner to view prior documents processed by the system and see their captured images, extracted information, and test results (as explained in the <i>Viisage iA-Examiner User's Guide</i>).

To set data-saving options here in iA-Administrator, click the Saving Data tab, and use the descriptions and recommendations in the following tables. Or, to set data-saving options in iA-Examiner, see “Configuring Data Saving” on page 8-5.



Captured Images

Option	Description	Recommendations
Save	<p>Saves color or grayscale images, or both, to the location specified.</p> <p>Names each file using the document type and number (if known), date and time processed (if needed to make the name unique), and image type. For example, for a typical ICAO document:</p> <p style="text-align: center;">USA_P_12345678_VC.jpg</p> <p>where USA is the country code, P is the ICAO document type, 12345678 is the document number, and VC is the image type (can be I, S, T, U, or V, plus C if the image is color).</p>	<p>Set these options to suit your needs. Be sure the location you use for saving images has enough disk space. <i>If the disk fills up, the system will no longer operate properly.</i></p> <p>To reduce file sizes, use the JPEG format rather than BMP. See JPEG Image Quality, below, for more information.</p>
Image format	The graphics file format for saving images, JPEG or BMP. JPEG files are compressed according to the JPEG Image Quality setting (below).	
Location	The full pathname of the directory for saving images, on a local drive or mapped network drive.	
Image types	The types of images to save—Visible (white light), IR, UV, Seal, Tamper. Only Visible and IR appear for ID-GUARD units.	

Document Results Log

Option	Description	Recommendations
Save document results	Saves an individual text file of test results for each document processed.	Select this if you want a record of document information and test results for each document.
Location	The full pathname of the directory for saving the logs, on a local drive or mapped network drive.	Usually it's most convenient to use the same directory you use for saving images (above).

Saving Based on Test Results

Option	Description	Recommendations
Save images and logs as specified above	<p>Saves images and logs based on whether they pass or fail <i>these tests only</i>: checksum, expiration, B900 ink, patterns (visible, IR, UV, seal), brightness (IR, UV), and tamper.</p> <p>For all documents: Saves all images and logs regardless of test results.</p> <p>Only for documents that fail a test: Saves images and logs only for documents that fail one of these tests.</p> <p>Only for documents that pass all tests: Saves images and logs only for documents that pass all these tests.</p>	<p>Select the option that meets your needs.</p> <p>Note: You must also select the kinds of images you want to save (above): Color images, Grayscale images, or both.</p>

JPEG Image Quality

Option	Description			Recommendations
Use this quality setting for all JPEG images	<p>The quality setting to use when saving JPEG images, from Best (highest image quality, largest file) to Low (lowest image quality, smallest file).</p> <p>The list below shows the approximate file size of a single saved image. (JPEG sizes vary with the document and image type.)</p>			<p>Use Medium for decent quality and relatively small files. For better quality, use High or Best.</p> <p>Do not use Low if you want to be able to analyze images later for authenticity.</p>
	Format	Grayscale	Color B4500/5000	
	BMP	430 KB	3800 KB	9200 KB
	JPEG Best	170 KB	460 KB	700 KB
	JPEG High	110 KB	220 KB	400 KB
	JPEG Medium	50 KB	100 KB	200 KB
	JPEG Low	15 KB	30 KB	100 KB

Temporary Images and Logs

As the system captures images and creates logs, it holds them in memory while it processes the document. As explained above, you can have the system preserve these images and logs by saving them to a disk directory; otherwise they are discarded.

In addition, you can have the system write the images and logs from memory to the work directory, where they stay only until the next document is processed. Because this takes extra time, you should not use this option unless you have a reason to do so.

Option	Description	Recommendations
Write temporary images and logs to the work directory	<p>Writes the selected images and logs from the system's memory to the work directory (page 7-7).</p> <p>The images and logs from each document overwrite those from the previous document.</p>	<p>Do not select any of these except for a specific purpose, such as collecting the images and logs using a custom program.</p> <p>Note: If you want to use the Doc Log option described on page 8-7, you must select Document and MRZ Logs here.</p>
Image format	<p>The graphics file format for saving the temporary images, JPEG or BMP. JPEG files are compressed according to the JPEG Image Quality setting (above).</p>	Select the format you want to use.

Configuring iA-Examiner

Note

Before you read this chapter, see chapter 6, “Quick Configuration Guide.” It may contain all the information you need to get your system up and running.

iA-Examiner is the primary software interface an operator uses for viewing and analyzing the results of the system’s document testing. Using iA-Examiner’s configuration screens, you can customize many details about the way it works. This chapter explains how.

Before you do so, you should first configure the basic operation of your system using the iA-Administrator program as explained in chapter 7, “Configuring iA-thenticate.”

System Configuration Screens

You set configuration options for iA-Examiner from several System Configuration screens.

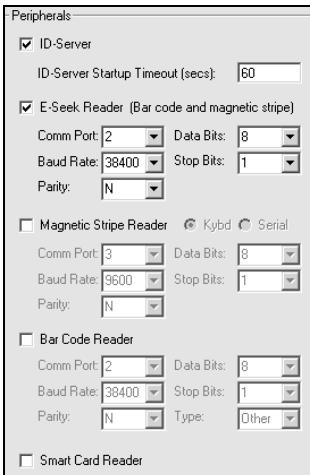
To display the System Configuration screens:

1. Run iA-Examiner (Start→Programs→iA-thenticate→iA-Examiner).
2. On the iA-Examiner screen, click Mgmt Funcs.
3. On the Management Functions screen, click System Config.
4. To display additional System Configuration pages, click More (and Back, when appropriate).

This chapter describes the options on these screens and recommends appropriate settings.

Configuring Peripherals

System Configuration Page 1: Peripherals

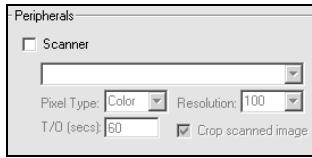


Option	Description	Recommendations
ID-Server	Automatically starts ID-Server when iA-Examiner starts. ID-Server is the authentication “engine” that must be running to process documents. When running, its icon appears in the Windows taskbar: 	Leave this selected for normal operation.
ID-Server Startup Timeout	The time allowed for ID-Server startup and hardware calibration when starting iA-Examiner.	Leave this set at its default value of 60 seconds.
E-Seek Reader (Bar code and magnetic stripe)	Enables the E-Seek Intelli-Check combination bar code and magstripe reader (either serial or USB).	Select this if you use one of the E-Seek readers; otherwise deselect it. (See note at left.)
Comm. Port	The COM port used for communicating with the reader.	Do not change this setting; the system sets it automatically.
Baud Rate Parity Data Bits Stop Bits	Details of the communication protocol between the PC and the E-Seek bar code reader.	Leave these set at their default values: 38400, N, 8, 1
Magnetic Stripe Reader	Enables an optional magstripe reader other than an E-Seek reader.	Select this if you have an ID-GUARD unit or if you are using an add-on magstripe reader other than E-Seek. Otherwise deselect it.
Kybd Serial	The type of magstripe reader: one that connects between the keyboard and the PC or one that connects to a serial port.	Select the correct type for your reader. For the ID-Guard’s built-in reader, select Serial. If you select Kybd and you also use iA-DataPort, you must deselect both Mag Stripe Reader and Keyboard Filter in iA-DataPort (page 10-7). Otherwise iA-Examiner will not receive magstripe data.
Comm. Port	The COM port used for communicating with the reader.	For an ID-Guard unit, follow the setup instructions in chapter 3.
Baud Rate Parity Data Bits Stop Bits	Details of the communication protocol between the PC and a serial magstripe reader.	Leave these set at their default values (38400, N, 8, 1) unless your reader requires different settings.
Bar Code Reader	Enables an optional 2D bar code reader other than an E-Seek reader.	Select this if you are using a bar code reader other than E-Seek; otherwise deselect it. (See note at left.)
Comm. Port	The COM port used for communicating with the reader.	Select the reader’s port number.

Note

Examiner and iA-DataPort cannot both use the same reader at the same time. If you use iA-DataPort and you select a reader here, you must deselect it in iA-DataPort (page 10-6).

Option	Description	Recommendations
Baud Rate Parity Data Bits Stop Bits	Details of the communication protocol between the PC and the bar code reader.	Leave these set at their default values (38400, N, 8, 1) unless your reader requires different settings.
Smart Card Reader	Enables an optional smart card reader (for reading embedded chips).	Select this if your unit has a smart card reader. Otherwise deselect it.



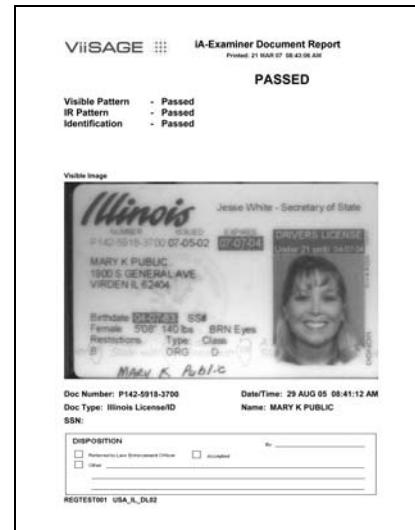
Option	Description	Recommendations
Scanner Pixel Type Resolution T/O Crop scanned image	Enables an optional flatbed scanner and sets options for its use.	For instructions about installing and configuring a flatbed scanner, see chapter 4, “Installing an Optional Reader or Scanner.”

Configuring Printing

System Configuration Page 1: Printing

You can configure iA-Examiner so the operator can print document results to the system's default printer. (See example on right.)

Before this feature will work, you must set up your default printer in the usual way using the Printers control panel (Start→Settings→Printers).



- Printing	
<input type="checkbox"/> Enable Print Button	<input type="checkbox"/> Print in Color
<input type="checkbox"/> Display Printer Errors	<input type="checkbox"/> Print All Images
<input type="checkbox"/> Print Text Watch List Information	

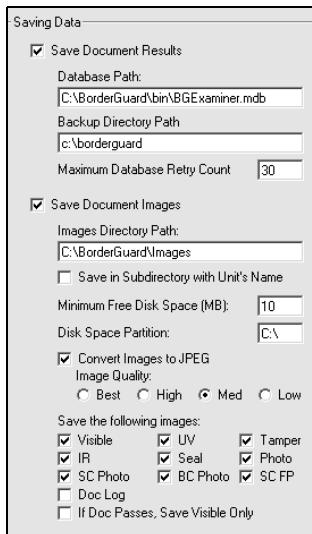
Option	Description	Recommendations
Enable Print Button	Activates the Print button on the iA-Examiner screen.	Select this if you want operators to be able to print document results.
Print in Color	Sends color information when printing, including green and red text to mark passed and failed tests. On a color unit, document images print in color.	Select this if you are using a color printer and want the printout in color.
Display Printer Errors	Displays any printer error messages on the iA-Examiner screen.	Select this if you want the operator to see printer error messages.
Print All Images	Prints all captured images on a second page (in addition to the visible image on the main page).	Select this if you want all the images included in the printout.
Print Text Watch List Information	Prints the detailed results of the TextWatch test.	Select this if you have the optional TextWatch feature and want the detailed results included in the printout.

Configuring Data Saving

System Configuration Page 1: Saving Data

You can set data-saving options here in iA-Examiner or in iA-Administrator. See “Two Ways to Save Images and Logs” on page 7-7 to compare the two methods and decide which options you want to use.

Data Saving Options



Option	Description	Recommendations
Save Document Results	Saves information and test results for each processed document in the document-results database (.mdb) file you specify.	Select this if you want a text record of each document you process.
Database Path	The full pathname of the database file, on a local or mapped network drive. This file, BGEaminer.mdb, is in BorderGuard\Bin\ on the drive designated for storing data.	Use the default directory or one that suits your needs. If you use a directory other than the default, copy the BGEaminer.mdb file from the BorderGuard\Bin directory on the data drive to the directory you specify. iA-Examiner will not create a new file from scratch. You can also specify the same file for several networked units, as explained on page 8-8.
Backup Directory Path	The full pathname of the directory for saving a backup copy of the current database, on a local drive or mapped network drive.	Specify the directory you want to use for backing up the database, as explained on page 9-3.
Maximum Database Retry Count	If the database is on a network drive, a network or server problem could break your connection to it. The Retry Count tells the system how many times to try reconnecting when this happens. For more information, see page 8-8.	Depending on your network and the type of problem, the default 30 tries could take from 15 seconds to several minutes. You may want to experiment by disconnecting the network cable or shutting down the file server, and then adjust the number for a reasonable delay under those conditions.

Option	Description	Recommendations
Save Document Images	<p>Saves the images you specify for each document you process, in either Windows Bitmap (.bmp) or JPEG (.jpg) format.</p> <p>Gives each file a unique name based on the document type and number (if known), date and time processed, and image type.</p> <p>For example, a Rhode Island, USA driver's license #987654321, processed 2007-March-18 at 11:55:33, IR image:</p> <p style="text-align: center;">DL_USA_RI_987654321_070318115533_I.jpg</p> <p>Image type can be I (infrared), S (seal), T (tamper), U (ultraviolet), or V (visible), plus C if the image is color. Other image types are SCP for smart card photo and BCP for bar code photo.</p>	<p>Select this if you want to save some or all of the images for later reference.</p> <p><i>Color images take a lot of disk storage space. To avoid problems, your drive should have plenty of free space.</i></p> <p>To reduce file sizes (but also reduce image quality), use JPEG compression (below).</p> <p>To avoid saving unnecessary images, select only the types you want using Save the following images, below.</p>
Images Directory Path	<p>The full pathname of the directory for saving images, on a local drive or mapped network drive.</p> <p>If you specify the same directory for several networked units, you can then view reports that include all the units, as explained on page 8-8.</p>	<p>If you set data-saving options in iA-Administrator as well as here—<i>not recommended</i>—be sure to specify different directory paths to avoid file naming conflicts.</p> <p>Also see the next item, Save in Subdirectory with Unit's Name.</p>
Save in Subdirectory with Unit's Name	<p>Saves each unit's images in a subdirectory of the images directory (previous item) rather than in the images directory itself. The subdirectory's name is the unit's computer name.</p>	<p>Select this if you want to keep the saved images from different units separate.</p> <p>Important: Do not select this if you want to be able to review prior documents as described in the <i>Viisage iA-Examiner User's Guide</i>. That feature does not work with images saved in separate directories.</p>
Minimum Free Disk Space	<p>The amount of disk space (on the specified drive partition) that must be available for iA-Examiner to continue saving images. If the space falls below this amount, iA-Examiner displays a message and stops saving images.</p>	<p>The default value of 10 MB is an absolute minimum.</p> <p>If you are saving images on your C: drive, you should increase this to 100 MB or more to avoid problems with the operating system.</p>
Disk Space Partition	<p>The drive partition to monitor for free disk space.</p>	<p>Set this to the same drive you use for the Images Directory Path.</p>
Convert Images to JPEG	<p>Saves the images in JPEG (.jpg) format rather than Windows Bitmap (.bmp) using the Image Quality setting you specify (below).</p>	<p>Select this if you want to reduce file sizes at the cost of some image quality.</p>

Option	Description			Recommendations																								
Image Quality	<p>The quality setting to use when saving JPEG images, from Best (highest image quality, largest file) to Low (lowest image quality, smallest file). The list below shows the approximate file size of a single saved image. (JPEG sizes vary with the document and image type.)</p> <table> <thead> <tr> <th>Format</th> <th>Grayscale</th> <th>Color</th> <th>B4500/5000</th> </tr> </thead> <tbody> <tr> <td>BMP</td> <td>430 KB</td> <td>3800 KB</td> <td>9200 KB</td> </tr> <tr> <td>JPEG Best</td> <td>170 KB</td> <td>460 KB</td> <td>700 KB</td> </tr> <tr> <td>JPEG High</td> <td>110 KB</td> <td>220 KB</td> <td>400 KB</td> </tr> <tr> <td>JPEG Medium</td> <td>50 KB</td> <td>100 KB</td> <td>200 KB</td> </tr> <tr> <td>JPEG Low</td> <td>15 KB</td> <td>30 KB</td> <td>100 KB</td> </tr> </tbody> </table>			Format	Grayscale	Color	B4500/5000	BMP	430 KB	3800 KB	9200 KB	JPEG Best	170 KB	460 KB	700 KB	JPEG High	110 KB	220 KB	400 KB	JPEG Medium	50 KB	100 KB	200 KB	JPEG Low	15 KB	30 KB	100 KB	<p>Use Medium for decent quality and relatively small files. For better quality, use High or Best.</p> <p>Do not use Low if you want to be able to analyze images later for authenticity.</p>
Format	Grayscale	Color	B4500/5000																									
BMP	430 KB	3800 KB	9200 KB																									
JPEG Best	170 KB	460 KB	700 KB																									
JPEG High	110 KB	220 KB	400 KB																									
JPEG Medium	50 KB	100 KB	200 KB																									
JPEG Low	15 KB	30 KB	100 KB																									
Note ID-Guard does not capture UV, seal, or tamper images.	Save the following images	<p>The types of images and logs to save. In addition to Visible (white light), IR, UV, Seal, and Tamper images, you can also save:</p> <p>Photo: ID photo from visible image SC Photo: ID photo from smart card BC Photo: ID photo from bar code SC FP: Fingerprint from smart card</p> <p>Doc Log: Log detailing how the system initially read and analyzed the document—the same as the Extended Doc Log Data listed on System Configuration Page 5 (page 8-28).</p>	<p>Select each image type you want to save.</p> <p>To save the document log:</p> <ol style="list-style-type: none"> 1. Select Doc Log here. 2. Also select Document and MRZ Logs using iA-Administrator, as described on page 7-12. <p>Also see the next item.</p>																									
	If Doc Passes, Save Visible Only	<p>For documents that <i>pass</i> all tests, save only the visible image. For documents that <i>fail</i> any test, save all the selected images.</p> <p>This does not affect saving the document results log.</p>		Select this if you need only a simple “photocopy” of documents that pass all tests. This lets you save disk space while keeping important forensic information about documents that cause alerts.																								

Using a Networked Database

Examiner saves document data and test results in the BGExaminer.mdb database, located by default in directory \BorderGuard\Bin on the drive designated for storing data.

If you have several networked iA-thenticate systems, you can save their data in a single database on a mapped network drive. You can then review the combined data and generate reports from it, as explained in chapters 3 and 4 of the *Viisage iA-Examiner User's Guide*.

If you want to review captured images along with the combined data, you can also save the images from all the units to a common network location.

Performance and Reliability

Before you decide to use a networked database, you should consider performance and reliability.

- ❑ Saving data on a network takes longer than on a local disk, especially if you save images as well. Be sure your network is fast enough for your application. Instead of saving uncompressed Bitmap images, use JPEG compression to reduce file size.
- ❑ A problem with the network or the file server can disrupt your operations.

If a system loses its connection to the database, it tries several times to reconnect, as specified by the Maximum Database Retry Count (page 8-5). During this time it displays a progress bar and prevents any operator actions.



If it cannot reconnect, it lets you proceed but displays **No database connection** in red. As long as this message appears, the system is *not working normally*. You should not continue using it for production work until the connection is restored.

When the network or server problem is resolved, the system reconnects automatically within 10 seconds, the red message disappears, and normal operation resumes.

Setting Up a Networked Database

To set up a networked database:

1. Copy BGExaminer.mdb from its default location on one of your iA-thenticate systems to a network-accessible folder.
2. On each iA-thenticate system:
 - a. Map the database folder or its drive as a network drive.
 - b. Run iA-Examiner. Click Mgmt Funcs then System Config.
 - c. On System Configuration Page 1, under Saving Data, select Save Document Results.
 - d. In the Database Path field, fill in the complete pathname of the networked database—for example, G:\Data\BGExaminer.mdb.
 - e. Specify the Maximum Database Retry Count as explained on page 8-5.

f. To save images to the network folder as well:

- Select **Save Document Images**.
- In the **Images Directory Path** field, fill in the pathname of a network folder—for example, G:\Data.
- In the **Disk Space Partition** field, fill in just the drive letter associated with the network folder—for example, G:\.
- To keep images from different systems in different subfolders, select **Save in Subdirectory with Unit's Name**.
- To make image saving faster, select **Convert Images to JPEG** and select only the image types you need to save. To review document data and images, you must select at least the **Visible** image.

Configuring Tests

System Configuration Page 2: Tests

Note: The *Viisage iA-Examiner User's Guide* has more information about each test.

The screenshot shows the 'Tests' configuration page with three main sections: 'Checksum Test', 'TextWatch Test', and 'Document Watch Test'. The 'Checksum Test' section includes fields for 'Max. Questionable Characters' (set to 5), checkboxes for 'Hide Expected Checksum' and 'Hide Questionable Character Count', and checkboxes for 'Enable MRZ Data Edit' (checked), 'MRZ Edits Affect All Data and Tests' (checked), and 'Display Checksum Correct. Screen On Alert' (unchecked). The 'TextWatch Test' section includes a checkbox for 'Enable TextWatch', a 'TextWatch Database Path' field containing 'c:\borderguard\bin\AT.sys', and checkboxes for 'Match By Name' (checked) and 'Match By Document Number' (unchecked). The 'Document Watch Test' section includes a checkbox for 'Enable Document Watch', a 'Document Watch Database Path' field containing 'c:\borderguard\bin\AT.sys', and a checkbox for 'Match By Document Number' (unchecked).

Option	Description	Recommendations
Checksum Test		
Max. Questionable Characters	When a document fails the checksum test, iA-Examiner shows the MRZ and highlights any characters it had trouble reading. But if there are more questionable characters than the number you specify here, iA-Examiner won't highlight any at all.	Use the default value of 5 to avoid overwhelming the operator with too much information when many of the MRZ characters are questionable.
Hide Expected Checksum	Suppresses display of the checksum that the system expected to find.	Select this if you do not want the operator to have access to the expected checksum.
Hide Questionable Character Count	Suppresses display of the total number of questionable characters.	Select this if you think displaying the number would not help the operator.
Enable MRZ Data Edit	Allows the operator to change the captured MRZ data onscreen to correct reading errors.	Select this option only if your operators are equipped to do such detailed analysis of test results.

Option	Description	Recommendations
MRZ Edits Affect All Data and Tests	<p>Accepts the operator's MRZ edits as permanent corrections, and changes the results of any affected tests. Otherwise the original data and test results are retained.</p> <p><i>Note:</i> If the operator changes MRZ characters to remedy a <i>smart card BAC failure</i> (see page 8-24), those changes are never permanent and do not affect other tests.</p>	Select this if you want the operator's edits to become permanent, overriding the captured data.
Display Checksum Correct. Screen on Alert	<p>Automatically displays the MRZ editing screen when there is a problem with the checksum.</p>	<p>Select this if you want the editing screen displayed automatically. Otherwise the operator must click Edit MRZ to display it.</p> <p>If you have a smart-card unit and you process any cards that use Basic Access Control, select this to ensure that the operator will not be asked to correct the same MRZ read error twice.</p>
TextWatch Test	<p>Enable TextWatch Activates the TextWatch test, which checks a watch list for matching names and document numbers.</p> <p>TextWatch Database Path The full pathname of the TextWatch database. The default is C:\BorderGuard\Bin\iAT.sys.</p> <p>Match By Name Searches the watch list for a matching name.</p> <p>Match By Document Number Searches the watch list for a matching document number.</p>	<p>Select this if you have the optional TextWatch feature and want to use it.</p> <p>Use the default pathname, or a different one if you have customized it.</p> <p>Select the matching options you want to use. If you select both Match By Name and Match By Document Number, you will see an alert if <i>either one</i> matches.</p>
Document Watch Test	<p>Enable Document Watch Activates the Document Watch test, which checks to see if the document number falls within specified ranges.</p> <p>Document Watch Database Path The full pathname of the Document Watch database. The default is C:\BorderGuard\Bin\iAT.sys.</p>	<p>Select this if you have the optional TextWatch and want to use its Document Watch feature.</p> <p>Use the default pathname, or a different one if you have customized it.</p>

Option	Description	Recommendations
Pattern Tests		
Legal Age Test		
Display Pattern Confidence	Reserved for future use	—
Enable Legal Age Test	Activates the legal age test, which checks to make sure the document owner is at least a certain age.	Select this if you want to test for legal age.
Minimum Legal Age	Defines the legal age you are testing for.	Set this to the legal age you want to test for, such as 21.
Document Cross-Check Test		
Enable Document Cross-Check Test	Activates the document cross-check test, which compares information across the documents in a set.	Select this if you have enabled document sets (page 8-14) and want to use this cross-check test.
Smart Card Test		
Enable Smart Card Cross-Check Test	Activates the smart card cross-check test, which compares MRZ information read from the smart chip and the document image.	Select this if you have a smart card reader and want to use this cross-check test.
Identification Test		
Enable Identification Test	Tells the system to report, along with the other test results, whether it was able to automatically identify the document. Note: The system <i>always</i> tries to identify the document automatically. This option only affects whether Identification is <i>listed</i> as a separate test.	Keep this selected unless you do not want to display Identification as a separate test.
Custom Tests (1-3)	Controls additional tests designed for custom applications. For further information, contact Viisage Customer Support and request the Tech Note titled <i>Information for iA-thenticate Integrators</i> .	Leave all the Enable Custom Test options deselected unless you know they apply to your application.
Custom Tests		
Enable Custom Test 1		
Result File Path:		
Executable File Path:		
Treat Result Timeout as:		
<input type="radio"/> Pass <input type="radio"/> Fail <input type="radio"/> Indeterm <input checked="" type="radio"/> Ignor		

Configuring Document Processing

System Configuration Page 3: Document Processing

Option	Description	Recommendations
<p>Another Program Opens iA-Examiner</p> <p><input type="checkbox"/> Automatically Return to Primary Program</p> <p><input type="checkbox"/> Minimize iA-Examiner When Returning</p> <p><input type="checkbox"/> Maximize on Alert</p> <p><input type="checkbox"/> Don't Auto Maximize for User Input</p> <p><input type="checkbox"/> Automatically Print Alerts</p> <p><input type="checkbox"/> Alert Warning on Return</p> <p><input type="checkbox"/> Supervisor Finish Only</p> <p><input type="checkbox"/> Send User Messages</p> <p><input type="checkbox"/> Send Examiner Status</p> <p>Primary App Window Name: <input type="text"/></p> <p>Primary App Name (for button): <input type="text"/></p> <p><input checked="" type="radio"/> iA-Examiner is the Primary Program</p> <p><input type="radio"/> Don't Use Document Sets</p> <p><input type="radio"/> Let Operator Add Documents to Set</p> <p><input type="checkbox"/> Require Clear Key Prior to a New Document</p>	<p>Used when the operator works primarily with a program other than iA-Examiner, and works with iA-Examiner only as a supplement to the primary program.</p>	<p>Select the appropriate option for your work environment—either this one or iA-Examiner is the Primary Program (below).</p> <p>If you select this, you must <i>deselect</i> Display Doc Info Screen on Alert on System Configuration Page 5 (see page 8-22).</p> <p><i>Note:</i> For a few kinds of documents, iA-Examiner prompts you to capture the reverse side after you capture the front side. Depending on how you use your system, some of the choices available with this option may not be compatible with the reverse-capture feature. Contact Viisage Customer Support for assistance.</p>
Automatically Return to Primary Program	Causes the primary program to come to the front automatically when the operator finishes reviewing a document. iA-Examiner finishes processing the document if the document had no alerts.	Select this if you want to return to the primary program automatically without having to click Clear, Cancel, or the program's button (below).
Minimize iA-Examiner When Returning	Causes the iA-Examiner screen to be minimized (rather than simply hidden behind the primary program screen) when returning to the primary program.	Select this if you want the iA-Examiner screen out of the way when it isn't in use.
Maximize on Alert	<p>Causes the iA-Examiner screen to come to the front automatically whenever a document requires review.</p> <p><i>Note:</i> iA-Examiner normally maximizes if it requires some <i>action</i> by the operator (but see the next item). It then minimizes automatically if Minimize iA-Examiner When Returning is selected (below).</p>	If you want iA-Examiner to appear automatically, select this. If you want the operator to see iA-Examiner only after manually selecting it from the primary program, deselect this.
Don't Auto Maximize for User Input	Prevents iA-Examiner from maximizing <i>automatically</i> when it requires some action by the operator. Instead, the primary program controls whether iA-Examiner maximizes or not.	If you want to control maximizing behavior through your primary program, select this. Otherwise deselect it.

Option	Description	Recommendations
Automatically Print Alerts	Automatically sends a report to the default printer when the operator leaves one or more problems unresolved during a review.	Select this if you want a paper record of unresolved document problems.
Alert Warning on Return	When the operator returns from the primary program, iA-Examiner displays an alert if any of the document's possible problems were not resolved during the iA-Examiner review.	Select this if you want an extra warning for the operator that the document has unresolved problems.
Supervisor Finish Only	A special-purpose option that works only with the settings shown at left.	Select this only in consultation with Viisage Customer Support.
Send User Messages	Sends to the primary program the messages iA-Examiner displays on its screen about what is happening and what the operator should do next.	Select this only if your primary program is set up to process these messages.
Send Examiner Status	Sends to the primary program certain indicators about iA-Examiner's status, such as "document inserted" and "document removed too soon."	Select this only if your primary program is set up to process these status indicators.
Primary App Window Name	The name that appears in the title bar of the primary program. Specifying this name ensures that iA-Examiner properly returns control to the primary program.	Enter the name exactly as it appears in the program's title bar.
Primary App Name (for button)	The program name to display on the Return to button that takes the operator back to the primary program. For example, if you type Master here, the button will say Return to Master.	Specify the program name for the button. (This does not need to match the name in the program's title bar.)
iA-Examiner Is the Primary Program	Used when the operator works primarily with iA-Examiner (rather than with another program).	Select the appropriate option for your work environment—either this one or Another Program Opens iA-Examiner (above).

Required settings for *Supervisor Finish Only*:

Document Processing:

- Another Program Opens iA-Examiner
 - Automatically Return to Primary Program
 - Minimize iA-Examiner When Returning
 - Maximize on Alert
 - Don't Auto Maximize for User Input
 - Automatically Print Alerts
 - Alert Warning on Return
 - Supervisor Finish Only
 - Send User Messages
 - Send Examiner Status

Primary App Window Name: **[Required]**

Primary App Name (for button): **[Req'd]**

Disallow Test Overrides:

Do not let the operator override results for these tests:

Checksum Doc Watch
 VIZ Match Credit Card
 Expiration Custom Test 1
 B900 Ink Custom Test 2
 Visible Pattern Custom Test 3
 IR Pattern Smart Card
 UV Pattern SCardXCheck
 Seal Pattern Identification
 Tamper Text Watch
 [All selected]

Option	Description	Recommendations
Don't Use Document Sets	Store each document's results independently of other documents.	If you want to be able to group several related documents together in a set, select Let Operator Add Documents to Set. In addition, on System Configuration Page 1, you must: <ul style="list-style-type: none"> • Select Save Document Results. • Select Save Document Images, and select at least the Visible image. If you don't want to group documents in sets, select Don't Use Document Sets.
Let Operator Add Documents to Set	Let the operator group 2–4 documents together in a set so their results are linked and can be compared.	
Require Clear Key Prior to a New Document	Requires the operator to take the extra step of clicking Clear Display before iA-Examiner will process the next document.	Select this only if you want to require this extra step.

Configuring Verification Databases

System Configuration Page 3: Verification Databases

A verification database is an external database that the system can reach through an Internet connection to verify certain information about documents and their owners. To use a verification database, you must be a registered subscriber.

Currently the system supports the VerifyME™ verification database.

About VerifyME

The VerifyME database includes information from U.S. states and Canadian provinces for verifying driver's licenses and nondriver IDs. It also includes information from countries worldwide for verifying the format of passport numbers.

U.S. and Canadian Driver's Licenses and IDs

When you process a U.S. or Canadian driver's license or nondriver ID, the system typically reads information from its 2D bar code or magstripe. (Information can also come from other sources such as operator entry.) The system uses this information to consult the VerifyME database. It can then display information retrieved from the database and point out certain kinds of discrepancies.

U.S. and Canadian information comes from departments of motor vehicles (DMVs) and voter registration offices. The sources vary by state and province. In general, DMV data tends to be more detailed and helpful for verifying documents and identifying their owners.

Examiner lets you specify, for each state and province, whether you want to consult the VerifyME database. If you find that you rarely get useful information from a certain jurisdiction, you can turn off database lookups for documents issued by that jurisdiction.

tion. This saves you the processing time needed for the lookup, any fee associated with it, and the bother of retrieving and possibly correcting unhelpful data.

When iA-Examiner shows you the results of a database lookup, it lists the source of the data as either DMV or Voter. This information can help you make decisions about which jurisdictions to include in your database lookups.

Passport Number Format

When you process a passport, the system typically reads information from its MRZ. (As with driver's licenses and IDs, the information can also come from other sources.) The system then checks the format of the document number against the VerifyME database and reports any problems.

This test is more limited than with driver's licenses and IDs but does help detect forged or altered document numbers.

Configuring VerifyME

Set these options on System Configuration Page 3:

Option	Description	Recommendations
Verification Database		
Jurisdictions	The jurisdictions for which you want to consult this database when processing U.S. and Canadian driver's licenses and IDs. Select Jurisdictions to see the list, select or deselect individual jurisdictions, and click OK.	Start with the default selections, which are all the jurisdictions covered by this database. If experience proves some to be unhelpful, deselect them.
Database	The name of the verification database you subscribe to.	Select VerifyMe.
Timeout	The maximum time you are willing to wait for a response from this database before iA-Examiner cancels the lookup request (in seconds).	Use the default value of 30 seconds unless this is unacceptably long in your work environment or you are willing to wait longer for results. <i>The operator cannot proceed with document processing until the lookup either succeeds or times out.</i>
Do Lookup For These Document Types: Licenses and IDs Passports	The types of documents for which you want to do lookups.	Select the types you want to be able to look up using VerifyME.

Option	Description	Recommendations
Do Lookup If This Field Exists: Document Number Soc. Sec. Number Full Name	Tells the system what information is required before it can do a lookup. For example, if you select Document Number, the system requires the document number before it does a lookup. If you select more than one, the system can do a lookup whenever it knows <i>any</i> of them.	For the VerifyME database, select Document Number and Full Name. Do not select Soc. Sec. Number.
Display Additional Retrieved Information: Always Never On Alert	Tells iA-Examiner when to display additional information after a lookup, which can include phone number, Social Security number, current address, and previous addresses.	Select one of the options.
Maximum Hits to Display	Not used for VerifyME.	—
Manual Lookup Only	Disables automatic database lookups, so that the operator must click the Issuer DB button to do a lookup.	Leave this deselected if you want the system to do a lookup automatically for any document that meets the requirements set up for this database. Select this if you want <i>no</i> automatic lookups. The operator must then click Issuer DB to do a lookup.

In addition, you must set up data entry fields so that the system can prompt the operator for any missing information that is required for the lookup.

- ◆ On System Configuration Page 4, under Data Entry, select these for four of the listed fields: First Name, Last Name, Document Number, and Postal Code. You can leave the Required checkboxes deselected unless you have a reason to select them.

For general information about configuring data entry, see the next section.

Configuring Data Entry

System Configuration Page 4: Data Entry

Data Entry		Required
Field #1:	Last Name	<input checked="" type="checkbox"/>
Field #2:	Soc Sec Number	<input type="checkbox"/>
Field #3:		<input type="checkbox"/>
Field #4:		<input type="checkbox"/>
Field #5:		<input type="checkbox"/>
Field #6:		<input type="checkbox"/>
Field #7:		<input type="checkbox"/>
Field #8:		<input type="checkbox"/>
Field #9:		<input type="checkbox"/>
Comment:	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input type="checkbox"/>
<input checked="" type="checkbox"/> Enable Previous Doc Info Button		

Option	Description	Recommendations
Field #1 ... Field #9	<p>A list of fields for the data entry screen, which allows the operator to enter any missing information. The data entry fields appear in the same order you select here.</p> <p>If you mark a field as Required, then the system automatically displays the data entry screen whenever it can't find the required information.</p>	<p>From the drop-down lists, select each field you want to appear on the data entry screen. If you want the data entry screen to appear automatically whenever the system can't find the information for a certain field, select Required.</p> <p>To include a custom field, select User Field #1, #2, or #3 and see "Configuring Static Database Information" on page 8-18. If you select Required for one of these fields, the system will <i>always</i> display the data entry screen.</p> <p>Note: To also let the operator display the data entry screen <i>manually</i>, select Enable Edit Button (page 8-21).</p>
Comment	Specifies whether the data entry screen includes a Comment field where the operator can type additional information.	<p>Select Yes or No to include the Comment field or not.</p> <p>To include the Comment field and <i>always</i> display the data entry screen, select both Yes and Required.</p>
Enable Previous Doc Info Button	Enables or disables the Use Previous Doc Info button on iA-Examiner's data entry screen, which lets the operator copy information from the previous document processed. (See "Processing a Document Using BorderGuard" in chapter 1 of the <i>iA-Examiner User's Guide</i> .)	Select or deselect to enable or disable this function.

Configuring a Custom ID Type

System Configuration Page 4: Custom ID Type

Custom ID Type
<input checked="" type="checkbox"/> Enable Custom ID Button
Custom ID Type <input type="button" value="Badge"/>
Default Image Display: <input type="radio"/> Visible <input checked="" type="radio"/> IR
<input checked="" type="checkbox"/> Don't Save Custom ID Images

Option	Description	Recommendations
Enable Custom ID Button	Displays an additional button on the document selection screen for processing a custom type of ID—or any other kind of document, such as a ticket or boarding pass.	Select this if you want the operator to be able to use this button.
Custom ID Type	The name to display on the button.	Use a name no more than about 30 characters long. After you configure the custom ID button, check the document selection screen to make sure the text fits on the button.
Default Image Display	The image to display by default on the test results screen, either Visible or IR.	Select the image that shows the most relevant information for the operator. The operator can also display the other images as usual.
Don't Save Custom ID Images	Tells iA-Examiner not to save document images whenever the operator uses the custom ID button. This prevents saving images if you have selected Save Document Images in iA-Examiner (page 8-5). <i>However, it does not prevent saving images if you have enabled image saving using iA-Administrator (page 7-10).</i>	Select this if you don't want the images of this custom document type saved for any reason, such as privacy or security. <i>Note the important condition in the description.</i>

Configuring Static Database Information

System Configuration Page 4: Static Database Information

Static Database Information
Customer Name: <input type="text" value="Customer Name"/>
Site Name: <input type="text" value="Site Name"/>
User Field #1: <input type="text" value="User Field 1"/>
User Field #2: <input type="text" value="User Field 2"/>
User Field #3: <input type="text" value="User Field 3"/>

Option	Description	Recommendations
Customer Name	Names stored in the document results database (page 8-5), intended for use in custom reports that you might generate from the database.	Fill in any suitable names.
Site Name	Names for custom fields, to hold any kind of information you want collected along with the documents you process. For example, you might name two fields Spouse's Name and Child's Name so the operator can enter this information as needed.	Assign suitable names for up to three custom fields. To make these fields appear on the data entry screen so the operator can fill them in, see the earlier section "Configuring Data Entry." To fit more characters into the name, avoid using lots of capital letters.

Configuring Debugging

System Configuration Page 4: Debugging

Debugging
<input type="checkbox"/> Log Debugging Information
<input checked="" type="radio"/> Log Level 1 (Initialization and errors only)
<input checked="" type="radio"/> Log Level 2 (Normal logging)
<input type="radio"/> Log Level 3 (Detailed logging)
<input type="checkbox"/> Log Debug Timing Information
Max Debug Log Size: <input type="text" value="5000"/> KBytes

Option	Description	Recommendations
Log Debugging Information	Creates a log of information useful for diagnosing problems.	Do not select this unless Viisage Customer Support asks you to do so for troubleshooting purposes.

Configuring Processing of Unidentified Documents

System Configuration Page 4: Processing Unidentified Documents

Note

For information about creating and using a custom document database, contact Viisage Customer Support.

The system can automatically identify ICAO documents and, with optional document databases, many non-ICAO documents as well. But what should happen if the operator processes a document that the system cannot automatically identify?

If you have an optional document database such as ID-License, iA-Examiner can display selection screens that let the operator manually identify the document. Or, iA-Examiner can process every unidentified document in a predetermined way.

The following table explains the four available options. In most cases, either the first or last option is most suitable:

- If you have an optional document database such as ID-License:
 - Use the first option (Go to the document selection screen) for the most flexibility in identifying and testing documents.
 - Use the last option (Process as a nonstandard document) if you usually want to simply capture unidentified documents without trying to identify or test them.
- If you do *not* have an optional document database, always use the last option (Process as a nonstandard document).

Processing Unidentified Documents

Go to the document selection screen

Go to the following document selection screen:

Country:

Jurisdiction:

Process as category:

Process as a nonstandard document

Option	Description	Recommendations
Go to the document selection screen	For an unidentified document, display the document selection screen, for selecting the document type using an Explorer-like list of countries, issuers, and types.	If you have an optional document database such as ID-License, this is the most flexible option.
Go to the following document selection screen	For an unidentified document, display the document selection screen, with the list already open to the country and jurisdiction you choose. For example, if you choose USA and Alabama, the list will open like this:	<p>Consider this option if:</p> <ul style="list-style-type: none"> • You have an optional document database such as ID-License, but you regularly process documents that the system doesn't identify, all from the same jurisdiction. • You have a custom document database for a certain jurisdiction, but the database does not include automatic document identification.  <p>You must make a choice for Country. You may make a choice for Jurisdiction or leave it blank.</p>
Process as category	Always process an unidentified document as a certain exact type. To use this, you must know the document's type code—for example, USA_AL_DL01 for a USA Alabama (AL) driver's license (DL) of a certain series (01).	Consider this option if most of the unidentified documents you process are of the same type. The operator can still use the Retest button (if enabled) to retest a document as a different type.
Process as a nonstandard document	For an unidentified document, don't display the document selection screen. Simply display the document's image without testing it.	Use this option if you don't have an optional document database such as ID-License. Also consider it if you want the system to simply capture unidentified documents without testing them, or you only occasionally want to test unidentified documents (using the Retest button).

Configuring System Directories

System Configuration Page 4: System Directories

System Directories
Document Summaries Directory: c:\borderguard\summaries

Option	Description	Recommendations
Document Summaries Directory	<p>The directory used for:</p> <ul style="list-style-type: none"> The results of searches you perform using the Document Viewer (<i>Viisage iA-Examiner User's Guide</i>, chapter 3) Temporary files for the data transmission feature (page 8-27). 	Use the default pathname: C:\BorderGuard\Summaries

Configuring Display Options

System Configuration Page 5: Display Options

Main Screen

Display Options
Main Screen
<input checked="" type="checkbox"/> Enable Cancel Button
<input checked="" type="checkbox"/> Enable Edit Button
<input checked="" type="checkbox"/> Enable Retest Button
<input type="checkbox"/> Display Security Level
<input type="checkbox"/> Display Doc Info Screen on Alert

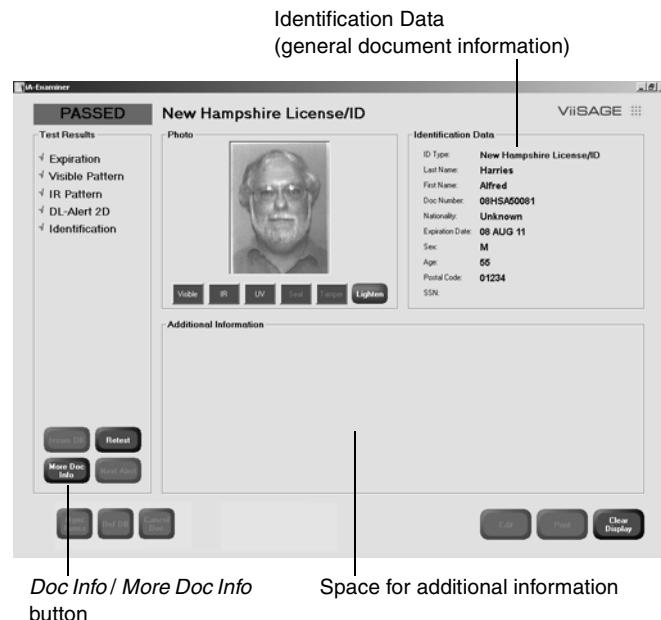
Option	Description	Recommendations
Enable Cancel Button	<p>Adds a Cancel Document button that lets the operator cancel evaluation of a document after capturing it.</p> <p>This button does <i>not</i> delete any saved test results or captured images, but it does exclude the canceled document from reports.</p>	Select this if you want the operator to be able to cancel evaluation of documents.
Enable Edit Button	<p>Adds an Edit button that lets the operator display the data entry screen for manually entering information.</p> <p>This option applies only if you have selected fields to appear on the data entry screen as described under “Configuring Data Entry,” page 8-16.</p>	Select this if you want the operator to be able to display the data entry screen even when the system doesn’t display it automatically.
Enable Retest Button	<p>Adds a Retest button that lets the operator retest the document (usually without having to recapture it) as a <i>different type</i> of document. This is used when the system doesn’t identify the document type correctly the first time. It requires an optional document database such as ID-License.</p>	Select this if you have ID-License or a custom document database and want to enable this feature.

Option	Description	Recommendations
Display Security Level	Used with ID-Passport, displays a number after the word REVIEW indicating the level of security testing done—for example, REVIEW 2. See the <i>ID-Passport Database Reference</i> (on the ID-Passport CD) for security level information.	Select this if you have ID-Passport and you want the operator to see and consider this information.
Display Doc Info Screen on Alert	When a document causes an alert, iA-Examiner normally displays information about the first alert. Selecting this option causes iA-Examiner to display general document information instead—as it does when a document passes all tests. The screen still lists all passed and failed tests, and the operator can click any one for more information.	If you select Another Program Opens iA-Examiner (page 8-12), you must deselect this. Otherwise, select the behavior you prefer.

Additional Information Display

When the iA-Examiner screen is not displaying the results of a selected test, it displays Identification Data—general document information including ID type, last and first names, document number, and so on. The operator sees this information:

- When a document passes all tests
- When a document causes an alert and the Display Doc Info Screen on Alert option (above) is selected
- By clicking Doc Info anytime



You can use the following options to let the operator see several kinds of additional information. The Doc Info button then becomes More Doc Info, and clicking it displays each kind of information in turn.

You can also tell iA-Examiner which kind of additional information to display first.

Additional Information Display	Primary
<input checked="" type="checkbox"/> Display Reference Image	<input checked="" type="radio"/>
<input type="checkbox"/> Display Raw MRZ Data	<input type="radio"/>
<input checked="" type="checkbox"/> Display Document Images	<input type="radio"/>
Img 1: <input type="button" value="Visible"/>	Img 2: <input type="button" value="UV"/>

Option	Description	Recommendations
Display Reference Image	Shows the sample or reference image for the processed document, if there is one.	Select each kind of information you want to let the operator see.
Display Raw MRZ Data	Shows the captured MRZ and the system's reading of it (ICAO documents only)	Under Primary, select the kind of information you want to appear first (even if you've selected only one kind of information).
Display Document Images Img 1 Img 2	Shows two of the captured document images side-by-side for comparison. You select the two images from the Img1 and Img2 lists.	

Selectable Display Fields

By default, iA-Examiner displays this information under Identification Data:

ID Type	Expiration Date
Last Name	Sex
First Name	* Age
Doc Number	* Postal Code
Nationality	* (blank field)

You can customize the last three fields (marked with *). For each one you can choose Age, Postal Code, SSN (Social Security Number), Birth Date, or one of three custom fields.

Selectable Display Fields
Display Field #1: <input type="button" value="Age"/>
Display Field #2: <input type="button" value="PostalCode"/>
Display Field #3: <input type="button" value=""/>

Option	Description	Recommendations
Display Field #1	The last three fields to display under Identification Data (shown when the operator clicks Doc Info).	Choose the information you want displayed.
Display Field #2		
Display Field #3	UserField1, UserField2, and UserField3 correspond to the matching entries for Static Database Information (page 8-18).	

Document Viewer

Document Viewer
<input type="checkbox"/> Display Viewer Image Path

Option	Description	Recommendations
Display Viewer Image Path	When using the document viewer (Mgmt Funcs→Viewer), show the full pathname of the displayed document image.	Select this if you want to be able to easily locate the saved image file while using the document viewer.

Configuring Smart Card Options

System Configuration Page 5: Smart Card Options

If your unit has a smart card reader, you can use the options in this section to adjust the way it operates.

About Basic Access Control

Some smart cards use *Basic Access Control* (BAC). To read information from the chip, the system must supply codes based on information it has already read from the document's printed MRZ. If iA-thenticate misreads the MRZ, access to the chip may be blocked. In this case the operator must correct the information manually before the chip can be read.

Smart Card Options

Smart Card Options

Smart Card Timeout (secs):	20
Placement Timeout (secs):	5
Placement Timeout Action:	<input checked="" type="radio"/> Fail Smart Card Test <input type="radio"/> Ignore Smart Card
<input type="checkbox"/> Prompt for Smart Card	<input checked="" type="checkbox"/> By Document Profile <input type="checkbox"/> Always
<input checked="" type="checkbox"/> Automatically Display MRZ Edit Screen For BAC	
Country Signing Certificate Folder Path:	
Disable Reading of These Optional Data Groups:	
<input checked="" type="checkbox"/> DG3 - Fingerprint	<input type="checkbox"/> DG11 - Personal
<input checked="" type="checkbox"/> DG4 - Iris	<input type="checkbox"/> DG12 - Document
<input checked="" type="checkbox"/> DG5 - Portrait	<input checked="" type="checkbox"/> DG13 - Optional
<input checked="" type="checkbox"/> DG7 - Signature	

Option	Description	Recommendations
Smart Card Timeout (sec)	The amount of time allowed to read the information from the smart card.	Use the default value of 20 seconds.
Placement Timeout (sec)	The amount of time allowed to detect a smart card after the system prompts the operator to place the document on the platform.	Use the default value of 5 seconds—long enough to let the operator place the document but short enough to time out quickly if no chip is present.
Placement Timeout Action	<p>The test result to record if the system does not detect a smart card before the Placement Timeout expires.</p> <p>Fail Smart Card Test: Records the smart card test as failed</p> <p>Ignore Smart Card: Records no result for the smart card test, just as if the document had no smart card</p>	Choose Fail Smart Card Test unless you have a specific reason to choose the other option.
Prompt for Smart Card	No longer supported.	Do not select this option.
Automatically Display MRZ Edit Screen for BAC	If access to the card is blocked because the system has misread the MRZ, automatically displays the screen that lets the operator correct misread MRZ characters.	Select this to display the edit screen automatically as needed. Otherwise the operator must click Retry to display the edit screen when needed.
Country Signing Certificate Folder Path	The folder where you keep country signing certificate files that you have obtained from issuing authorities.	You can specify any folder on a local or mapped drive.
Disable Reading of These Optional Data Groups	Ignores the selected data groups when reading a smart card. These groups may or may not be present on the cards you process.	Select any data groups that you do not care about, that are never present on the cards you process, or that cause too many reading errors to make them worthwhile.

Configuring Bar Code and Magstripe Options

System Configuration Page 5: Bar Code and Magnetic Stripe Options

Option	Description	Recommendations
Bar Code and Magnetic Stripe Analyzer	Enables validation of the magstripe or bar code on a license or ID card using optional software.	This selection is made automatically during DL-Alert installation—ID Check for the Intelli-Check version or ID Code for the Positive Access version. You should not change it unless you are asked to do so by Viisage Customer Support.
Prompt for Bar Code or Magnetic Stripe	If the operator captures a license or ID without first scanning its bar code or magstripe, the system asks the operator to either do the scan or click the Skip Scan button. The prompt appears only when the document has a bar code or magstripe.	Select this if you want to give the operator a second chance to scan a document's bar code or magstripe.

Configuring Reference Database Options

System Configuration Page 5: Reference Database Options

Option	Description	Recommendations
Enable Reference Database	Reserved for future use.	
Reference Database config files Path	Reserved for future use.	

Configuring Test Suppression

System Configuration Page 6: Suppressed Test Results

Suppressed Test Results	
Ignore the results of these tests and do not display them on the screen:	
<input type="checkbox"/> Checksum	<input type="checkbox"/> Doc Watch
<input type="checkbox"/> VIZ Match	<input type="checkbox"/> Credit Card
<input type="checkbox"/> Expiration	<input type="checkbox"/> Custom Test 1
<input type="checkbox"/> B900 Ink	<input type="checkbox"/> Custom Test 2
<input type="checkbox"/> Visible Pattern	<input type="checkbox"/> Custom Test 3
<input type="checkbox"/> IR Pattern	<input type="checkbox"/> Smart Card
<input type="checkbox"/> UV Pattern	<input type="checkbox"/> SCard XCheck
<input type="checkbox"/> Seal Pattern	<input type="checkbox"/> Identification
<input type="checkbox"/> Tamper	<input type="checkbox"/> 2D XCheck
<input type="checkbox"/> Text Watch	
<input type="checkbox"/> Facial Watch	
<input type="checkbox"/> DL-Alert 2D	
<input type="checkbox"/> DL-Alert MSR	
<input type="checkbox"/> Verif. DB 1	
<input type="checkbox"/> Verif. DB 2	
<input type="checkbox"/> Legal Age	
<input type="checkbox"/> Doc XCheck	
<input type="checkbox"/> MRZ Quality	
<input type="checkbox"/> IR Brightness	
<input type="checkbox"/> UV Brightness	

Option	Description	Recommendations
Checksum	Ignores the selected test when evaluating a document for problems and does not display its results for the operator.	Leave all the tests deselected so they are not suppressed.
VIZ Match		Do not select any tests to suppress except for troubleshooting or other special purposes.
Expiration		
...		
	(Your list of tests may differ slightly from the one shown.)	
	However, if the test is included in the document profile, the system still performs the test and records its results in the document-results database as usual.	

Configuring Test Override Options

System Configuration Page 6: Disallowed Test Overrides

Do not let the operator override results for these tests:	
<input type="checkbox"/> Checksum	<input type="checkbox"/> Doc Watch
<input type="checkbox"/> VIZ Match	<input type="checkbox"/> Credit Card
<input type="checkbox"/> Expiration	<input type="checkbox"/> Custom Test 1
<input type="checkbox"/> B900 Ink	<input type="checkbox"/> Custom Test 2
<input type="checkbox"/> Visible Pattern	<input type="checkbox"/> Custom Test 3
<input type="checkbox"/> IR Pattern	<input type="checkbox"/> Smart Card
<input type="checkbox"/> UV Pattern	<input type="checkbox"/> SCard XCheck
<input type="checkbox"/> Seal Pattern	<input type="checkbox"/> Identification
<input type="checkbox"/> Tamper	<input type="checkbox"/> 2D XCheck
<input type="checkbox"/> Text Watch	
<input type="checkbox"/> Facial Watch	
<input type="checkbox"/> DL-Alert 2D	
<input type="checkbox"/> DL-Alert MSR	
<input type="checkbox"/> Verif. DB 1	
<input type="checkbox"/> Verif. DB 2	
<input type="checkbox"/> Legal Age	
<input type="checkbox"/> Doc XCheck	
<input type="checkbox"/> MRZ Quality	
<input type="checkbox"/> IR Brightness	
<input type="checkbox"/> UV Brightness	

Option	Description	Recommendations
Checksum	Prevents the operator from overriding the results of the selected type of test.	Select any tests the operator is not allowed to override because of security or operational policies.
VIZ Match		
Expiration		
...		
	(Your list of tests may differ slightly from the one shown.)	If you select Supervisor Finish Only (page 8-13), you must select <i>all</i> the tests.
		Note: Even if you select Checksum here, the operator may still be able to change the results of the checksum test. To prevent that, you must deselect Enable MRZ Data Edit, as explained on page 8-9.

Configuring Alerts for Indeterminate Tests

System Configuration Page 6: Fail Tests on Indeterminate

Fail Tests on Indeterminate	
Fail these tests if the result is indeterminate:	
<input type="checkbox"/> DL-Alert 2D	<input type="checkbox"/> NDL VIS
<input type="checkbox"/> DL-Alert MSR	<input type="checkbox"/> Custom Test 1
<input type="checkbox"/> Verif. DB 1	<input type="checkbox"/> Custom Test 2
<input type="checkbox"/> Verif. DB 2	<input type="checkbox"/> Custom Test 3
<input type="checkbox"/> Smart Card	

Option	Description	Recommendations
Fail Tests If Results Are Indeterminate	<p>Some tests can show an indeterminate result if their results are incomplete or inconclusive. These include Verification Database, DL Alert 2D, DL Parser 2D, DL Alert MSR, DL Parser MSR, and custom tests.</p> <p>(Your list of tests may differ slightly from the one shown.)</p> <p>This option tells the system to treat such a result as a failure so that it causes an alert.</p>	Select this if you want indeterminate results to cause an alert.

Configuring Credit Card Options

System Configuration Page 6: Credit Card Options

Credit Card Options	
Display the Card Number As:	
<input type="radio"/> Full Number	<input checked="" type="radio"/> Last 4 Digits
Save the Card Number in the Database As:	
<input checked="" type="radio"/> Full Number	<input type="radio"/> Last 4 Digits
Default Image Display for Credit Cards:	
<input type="radio"/> Visible	<input checked="" type="radio"/> UV
<input checked="" type="checkbox"/> Don't Save Credit Card Images	

Option	Description	Recommendations
Display the Card Number As	Displays either all or part of the credit card number (read from the magstripe) onscreen. Also affects the number saved when you use the Create Results button (Mgmt Funcs→Viewer→Create Results).	If the operator needs to see the full number, select Full Number. Otherwise select Last 4 Digits.
Save the Card Number in the Database As	Saves either all or part of the credit card number in the document results database and in the iA-Examiner Doc Logs (page 8-28).	If you need to save the full number, select Full Number. Otherwise select Last 4 Digits.
Default Image Display for Credit Cards	The image to display by default on the test results screen, either Visible or IR.	Select the image that shows the most relevant information for the operator. The operator can also display the other images as usual.
Don't Save Credit Card Images	Tells iA-Examiner not to save document images for credit cards (if you have selected Save Document Images in iA-Examiner as explained on page 8-5).	Select this if you don't want iA-Examiner to save credit card images because of privacy or security concerns.
	<i>Important: Selecting this does not prevent saving credit card images if you have enabled image saving using iA-Administrator (page 7-10).</i>	You may also need to disable image saving using iA-Administrator (page 7-10).

Configuring Data Transmission Options

System Configuration Page 7: Data Transmission Options

Data Transmission Options	
<input type="checkbox"/> Enable Document Transmit Button	
<input type="checkbox"/> Enable Results Transmit Button	
Response File Timeout (secs):	30
Batch File Path:	c:\borderguard\working\DocTransmitBatch.bat
Response File Path:	c:\borderguard\working\DocTransmitResponse.txt

Option	Description	Recommendations
Enable Document Transmit Button	Activates the Send Current Document button on the Management Functions screen.	Select this if you want to be able to transmit document images and test results to another computer on your network for archiving or further analysis.
Enable Results Transmit Button	Reserved for future use.	—
Response File Timeout	For information about using the data transmission feature, contact Viisage Customer Support.	
Batch File Path		
Response File Path		

Configuring iA-Examiner Doc Log Options

System Configuration Page 7: iA-Examiner Doc Log Options

As explained under Configuring Data Saving (page 8-5), iA-Examiner can save document information and test results in the document-results database.

In addition, iA-Examiner can create XML log files containing document information and test results. In general, these log files are useful only if you have custom software that reads information from them as they are created. If you have no specific use for such files, you should leave all of the following Doc Log options deselected.

You can preserve the *final* document logs if you like. All the others are temporary files, overwritten with each new document.

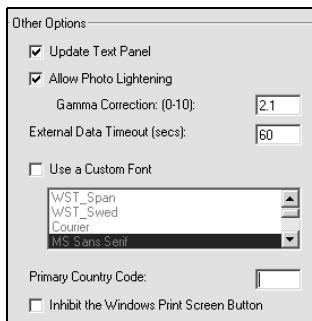
Examiner Doc Log Options	
Examiner Doc Log Directory:	
c:\borderguard\working	
<input type="checkbox"/> Save in Subdirectory with Unit's Name	
<input type="checkbox"/> Save Extended Doc Log Data	
<input type="checkbox"/> Create Smart Card MRZ Log	
<input type="checkbox"/> Create Preliminary Doc Log	
<input type="checkbox"/> Create Initial Doc Log	
<input type="checkbox"/> Create Final Doc Log	
<input type="checkbox"/> Save Final Doc Logs with Unique Names	

Option	Description	Recommendations
Examiner Doc Log Directory	The directory for creating iA-Examiner document logs.	Use C:\BorderGuard\Working unless you have a reason to use a different directory. You might want to use a network directory accessible to a number of iA-thenticate units.
Save in Subdirectory with Unit's Name	Creates each unit's logs in a subdirectory of the log directory rather than in the log directory itself. The subdirectory's name is the unit's computer name.	Select this if you want to create the logs from different units in a common location but in separate subdirectories.

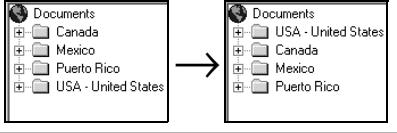
Option	Description	Recommendations
Save Extended Doc Log Data	Includes additional information in the initial and final document logs detailing how iA-thenticate read and analyzed the document.	Do not select this unless you need the additional details.
Create Smart Card MRZ Log	Creates a file containing MRZ information from the smart card: ExaminerSmartCardMRZLog.xml. This same information is included in the initial and final document logs.	Select these options only if you use software that reads and processes this information.
Create Preliminary Doc Log	Creates a file containing preliminary document information and test results—after the operator has finished entering any data and before the system has checked the results of any custom tests: ExaminerPreliminaryDocLog.xml.	
Create Initial Doc Log	Creates a file containing initial document information and test results—before the operator takes any actions to correct or override test results: ExaminerInitialDocLog.xml.	
Create Final Doc Log	Creates a file containing final document information and test results—after the operator has finished with the document: ExaminerFinalDocLog.xml, unless you select the next option.	Select this if you use software that reads and processes the information, or if you want to preserve the final logs for later use.
Save Final Doc Logs with Unique Names	Gives the final document log a unique name rather than overwriting it with each new document.	Select this if you want to preserve a copy of each final document log.

Configuring Miscellaneous Options

System Configuration Page 7: Other Options



Option	Description	Recommendations
Update Text Panel	Displays document information on BorderGuard's built-in text panel.	Leave this selected.
Allow Photo Lightening	Adds Lighten and Restore buttons to let the operator adjust the appearance of the document's ID photo. If you are saving the photo image, it is saved <i>as displayed</i> on the screen.	Select this if you notice that ID photos tend to be too dark on the screen and when saved as images.

Option	Description	Recommendations
Gamma Correction	<p>The amount of lightening to apply to the displayed ID photo when the operator uses the Lighten button, from 1 to 10:</p> <p>1: No lightening at all 10: Extreme lightening (Values between 0 and 1 actually <i>darken</i> the image.)</p>	Try the default value of 2.1. If the lightened photo is still too dark, try a slightly higher value such as 2.5 or 3.0. If it's too light, try a slightly lower value such as 1.8 or 1.5.
External Data Timeout (secs)	The maximum total time you are willing to wait for responses from all external databases.	Use the default value of 60 seconds unless this is unacceptably long in your work environment or you are willing to wait longer for results.
Use a Custom Font	Displays screen text using the font you select from the list.	<p>Leave this deselected unless you have a special reason to use it. <i>Changing the font can make the screen hard to read or even unusable.</i></p> <p>To restore the default font, deselect this option.</p> <p><i>Restart iA-Examiner after making any font change.</i></p>
Primary Country Code	<p>Displays the specified country at the top of the country list on the document selection screen. For example, specifying USA would change the display order like this:</p> 	Leave this blank to display all countries in alphabetical order, or specify a country's ICAO code to move it to the top of the list.
Inhibit the Windows Print Screen Button	Disables the Print Screen key so the operator cannot use it to capture an image of the screen while iA-Examiner is running.	Select this if you want to disable this function for security, privacy, or other reasons.

Managing iA-Examiner

Note

Before you read this chapter, see chapter 6, “Quick Configuration Guide.” It may contain all the information you need to get your system up and running.

iA-Examiner includes management functions for purging and backing up saved data. You perform these tasks on the System Management screen.

- ◆ On the iA-Examiner screen, click Mgmt Funcs, then click System Management.

Purging Saved Data

(System Management: Purge Saved Data)

Purge Saved Data

Retain Document Results For: Days **Purge Results**

Retain Document Images For: Days **Purge Images**

Retain Administration Data For: Days **Purge Admin Data**

Enable Automatic Purging **Compact and Repair the Database**

Purge At [hh:mm]:

Ask for Confirmation Each Time

Last Database Purge: **Unknown**
 Last Image Purge: **Unknown**
 Last Admin Purge: **Unknown**

Admin Report

Option	Description	Recommendations
Retain Document Results For	Number of days' worth of document results to keep in the database when using either manual or automatic purging. For example: 0: Purge everything 1: Keep only today's data 2: Keep today's and yesterday's data 3, 4, 5, etc.: Keep data from the specified number of days	Set to suit your needs.
Purge Results	Purges document results now, retaining recent results as specified.	Use this for manual purging, or set up automatic purging (below).
Retain Document Images For	How many days' worth of document images to keep in the saved-images folder when purging.	Set to suit your needs.
Purge Images	Purges images now, retaining recent images as specified.	Use this for manual purging, or set up automatic purging (below).
Retain Administration Data For	How many days' worth of actions to keep in the administration report when purging. (See Admin Report, below.)	Set to suit your needs.
Purge Admin Data	Purges the administration report now, retaining recent actions as specified.	Use this for manual purging, or set up automatic purging (below).

Option	Description	Recommendations
Enable Automatic Purging	Purges document results, images, and administration data automatically each day, retaining recent results, and data as specified.	Use this if you want to purge data automatically. <i>The system does not back up files automatically, so be sure to do regular backups (page 9-3) if you need to keep files and data beyond the retention period you set.</i>
Purge At (hh:mm)	Sets the time of day for automatic purging, using 24-hour time (0:00–23:59).	Specify a time when the system is running but not in heavy use.
Ask for Confirmation Each Time	Requires the operator to confirm each automatic purge before it happens.	Select or deselect this to suit your needs.
Compact and Repair the Database	Runs the Compact and Repair Database utility within Microsoft Access, which optimizes performance and repairs damage.	Periodically use this option to improve performance and prevent problems.
Admin Report	Displays a report of administration actions, including manual and automatic purges and database maintenance.	Use this to see the report anytime.

Backing Up Saved Data

(System Management: Back Up Saved Data)



Option	Description	Recommendations
Back Up Results	Copies the document results database from the database directory to the backup directory. You specify these directories on System Configuration Page 1, as explained in the table on page 8-5. Note: Each backup copy <i>overwrites</i> the previous backup copy.	Periodically use this option to preserve a backup copy of the database in a safe location.

Part Three

Using Optional Features

10

Using iA-DataPort

Note

At this time iA-DataPort does not work with ID-GUARD or with smart card units.

iA-thenticate includes a data transmission feature called iA-DataPort™. It can route data captured from a document's MRZ, magstripe, and 2D bar code to:

- A program running on the iA-thenticate PC
- Another PC through a standard serial port
- A virtual serial port (using third-party software)

Your own software can then process and store the data to meet your needs.

Preparing to Use iA-DataPort

Choosing Where to Send Data

iA-DataPort can send captured data to a program, a standard serial port, or a virtual port.

Sending Data to a Program

If you want to send data to a program running on the iA-thenticate PC, select the Simulated Keyboard option and choose related options as explained on page 10-7.

Sending Data Through a Serial Port

If you want to send data to another PC through a standard serial port, you need:

- An available serial port on your iA-thenticate PC
- An available serial port on the other PC
- A null-modem serial cable

To use the serial port connection:

1. Attach the null-modem cable between the serial ports on the iA-thenticate PC and the other PC.
2. Select the Communications Port option as explained on page 10-7.

By default, iA-DataPort sends data through the COM 1 port. If your BorderGuard unit is already using this port, you must change the port settings accordingly.

Sending Data Through a Virtual Port

Sending data through a virtual serial port allows another program running on the iA-thenticate PC to receive and process the data as if it were coming in through a standard serial port.

To use a virtual serial port:

- ❖ Install and configure appropriate third-party software for setting up a virtual serial port on your iA-thenticate PC.
- ❖ Select the Communications Port option as explained on page 10-7.

Note

On a BorderGuard unit with built-in PC, COM 1 is the lower serial connector.

Using the Optional Keyboard Filter

Note

If you use the E-Seek Intelli-Check reader, you do *not* need this filter.

If you want to transmit data from a magstripe reader *other than* the E-Seek Intelli-Check combined magstripe and bar code reader, you may want to install and use the optional keyboard filter provided with iA-DataPort.

A magstripe reader sends data as if it were typed on a keyboard. Depending on how you use your unit, magstripe and keyboard data can sometimes be sent to the wrong program. The keyboard filter can prevent this problem by recognizing magstripe data and sending it to iA-DataPort, no matter which other programs are running.

After installing the filter, you can enable or disable it anytime as explained on page 10-7.

To install the optional keyboard filter:

Windows 2000	Windows XP
<ol style="list-style-type: none"> 1. Open the System control panel. On the Hardware tab, click Device Manager. 2. In the Device Manager window, expand the Keyboards item. Then right-click the current keyboard and select Properties. 3. On the Driver tab, click Update Driver. 4. On the Welcome to the Upgrade Device Driver Wizard screen, click Next. 5. On the Install Hardware Device Drivers screen, select Display a list of the known drivers for this device so that I can choose a specific driver, and click Next. 6. On the Select a Device Driver screen, click Have Disk. 7. On the Install from Disk screen, click Browse and select the file <code>C:\BorderGuard\Tools\MagStripeFilter\IAMSFilter.inf</code> 8. On the Install from Disk screen, click OK. 9. On the Select a Device Driver screen, click Next. 10. On the Upgrade Driver Warning screen, click Yes. 11. On the Start Device Driver Installation screen, click Next. 12. On the Digital Signature Not Found screen, click Yes. 13. On the Completing the Upgrade Device Driver Wizard screen, click Finish. 14. Close the IAI Magstripe Filter Driver Properties window. In the System Settings Change window, click Yes to restart. 	<ol style="list-style-type: none"> 1. Open the System control panel. On the Hardware tab, click Device Manager. 2. In the Device Manager window, expand the Keyboards item. Then right-click the current keyboard and select Properties. 3. On the Driver tab, click Update Driver. 4. On the Welcome to the Hardware Update Wizard screen, select Install from a list or specific location and click Next. 5. On the next screen, select Don't search. I will choose the driver to install. Then click Next. 6. On the next screen, click Have Disk. 7. On the Install from Disk screen, click Browse and select the file <code>C:\BorderGuard\Tools\MagStripeFilter\IAMSFilter.inf</code> 8. On the Install from Disk screen, click OK. 9. On the next screen, when you see the message This driver is not digitally signed, click Next. 10. On the Upgrade Driver Warning screen, click Yes. 11. On the next warning screen, click Continue Anyway. 12. On the Completing the Hardware Update Wizard screen, click Finish. 13. Close the IAI Magstripe Filter Driver Properties window. In the System Settings Change window, click Yes to restart.

Starting iA-DataPort

You start iA-DataPort by running the iA-DataPort Utility. As explained in the rest of this chapter, the utility lets you:

- View data as it is captured from the MRZ, magstripe, and 2D bar code
- Configure various settings for capturing, displaying, formatting, and transmitting the captured data
- Test the operation of each information-capture device

Starting the iA-DataPort Utility

To run the iA-DataPort Utility and start iA-DataPort:

- ❖ Double-click the iA-DataPort Utility icon on your desktop.
Or, select Start→Programs→iA-thenticate→iA-DataPort.

Running the Utility Minimized

In most cases you can run the iA-DataPort Utility minimized (if you want to do so) while you process documents. See “Configuring Startup Settings” on page 10-14.

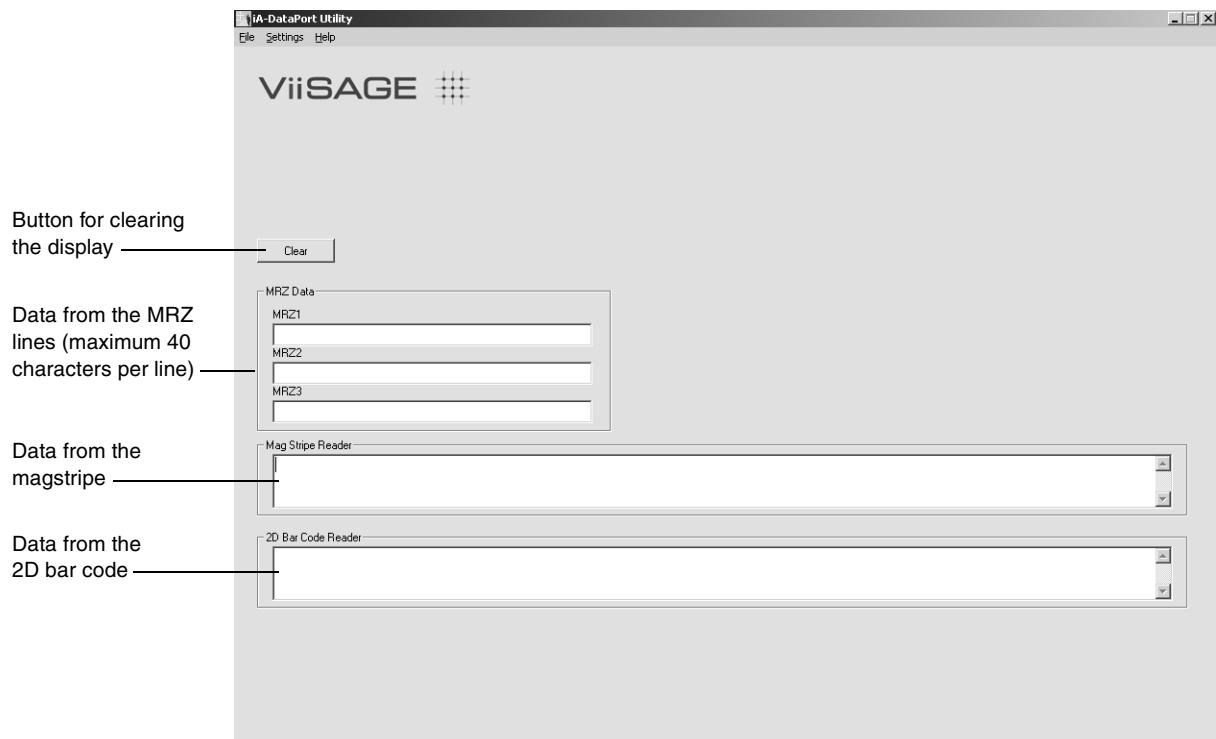
However, you *cannot* run the utility minimized if you are using a “keyboard wedge” magstripe reader *without* using the optional keyboard filter described on page 10-3.

In addition, selecting this option will prevent the application from being maximized. The menus will not be available and you will only be able to close the application via a Windows shutdown or using the Windows Task Manager.

If you are running iA-DataPort minimized and need to disable this option, open the config file C:/BorderGuard/Config/BGDataPort.cfg. Under Startup Settings, edit the setting to RunMinimizedOnly=No.

Viewing Captured Data

The iA-DataPort Utility window shows the data captured from the MRZ lines, magstripe, and 2D bar code, highlighted in yellow. You can clear the displayed data by clicking Clear.



Configuring Settings

Using the Settings menu, you can configure:

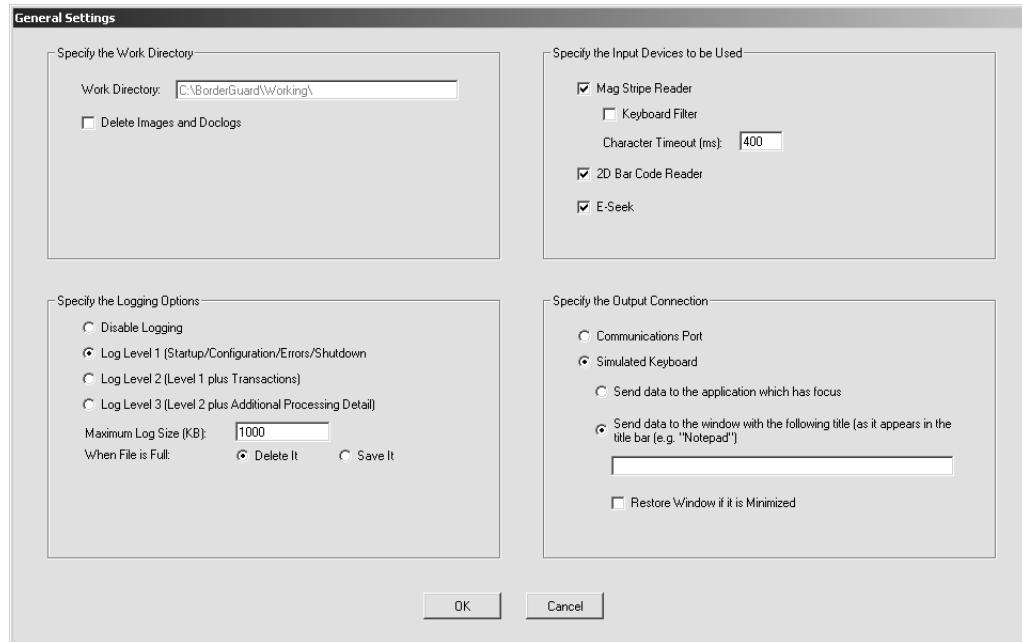
General settings	Data transmit settings
Communication port settings	Display settings
Data format settings	Startup settings
MRZ data format settings	

Configuring General Settings

General settings let you configure your input devices, specify how you want iA-DataPort to handle the data they capture, and set up logging.

To configure general settings:

1. Select Settings→General Settings.



2. If you want iA-DataPort to delete images and document logs from the work directory after processing each document, select **Delete Images and Doclogs**. (You set the location of the work directory using iA-Administrator, as explained on page 7-7.)
3. Specify the logging options you want to use:
 - Select one of the options for logging iA-DataPort activity: **Disable Logging** or **Logging Level 1, 2, or 3**, as described on the screen.
 - If you enable logging, specify the maximum size for the log file and what you want done with the file when it reaches that size:
 - To discard the existing file and start a new one, select **Delete It**.
 - To retain the existing file and start a new one, select **Save It**.

Note

iA-DataPort and iA-Examiner cannot both use the same reader at the same time. If you select the magstripe reader or the bar code reader here, you must deselect that reader in iA-Examiner (page 8-2).

Do not select a reader if you don't have the device attached.

4. Select each input device you are using:

- If you are using a magstripe reader (see note at left):
 - Select Mag Stripe Reader.
 - To use the optional keyboard filter to route magstripe data to iA-DataPort, select Keyboard Filter. See page 10-3 for installation instructions and more information about the filter.
 - Important:* If you want magstripe data routed to a different program, such as iA-Examiner, be sure to *deselect* both Keyboard Filter and Mag Stripe Reader.
 - For Character Timeout, use the default value of 400 ms.
- If you are using a 2D bar code reader, select 2D Bar Code Reader. (See note at left.)
- If you are using the E-Seek Intelli-Check combined magstripe and bar code reader, select E-Seek.

5. Select one of the output connections:

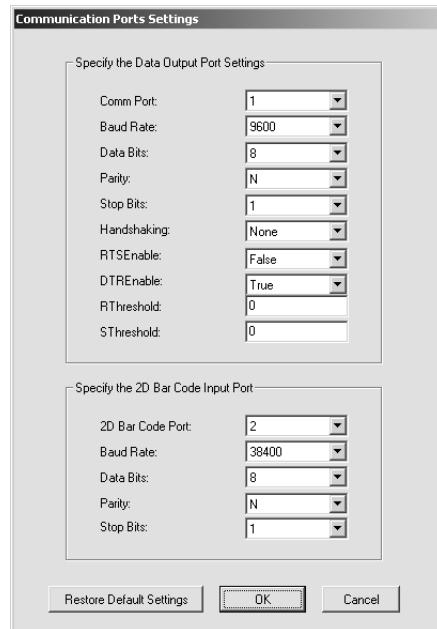
- To send output to a serial communications port, select Communications Port.
- To send output to an application, as if the data were being typed using an ordinary keyboard, select Simulated Keyboard and choose the options you want to use:
 - To send the output to the front program window, select Send data to the application which has focus.
 - To send the output to a specific program window, select Send data to the window with the following title. Enter the window's full title (exactly as it appears in the title bar), or enter enough characters from the *beginning or end* of the window's title to identify it uniquely. For example, if the window's title is Log0001.txt - Notepad, you might enter either Log or Notepad.
 - To restore the specified program window after each read (if it's minimized), select Restore Window if it is Minimized.

Configuring Communication Port Settings

You must configure the port settings so that they match those of your BorderGuard unit and your bar code reader.

To configure communication port settings:

1. Select Settings→Comm Ports Settings.



2. If you want to send data to another PC through the PC serial port as described on page 10-2, select the appropriate values under Data Output Port Settings. The Comm Port number must match the port to which the null modem cable is attached.
3. For the 2D Bar Code Input Port settings, select values that match those set for your bar code reader. The default values for the E-Seek Intelli-Check reader are 2, 38400, 8, N, 1.
4. Click OK.

Configuring Data Format Settings

You can format the data that the system sends to your application by specifying the characters used for starting, ending, and delineating each group of data.

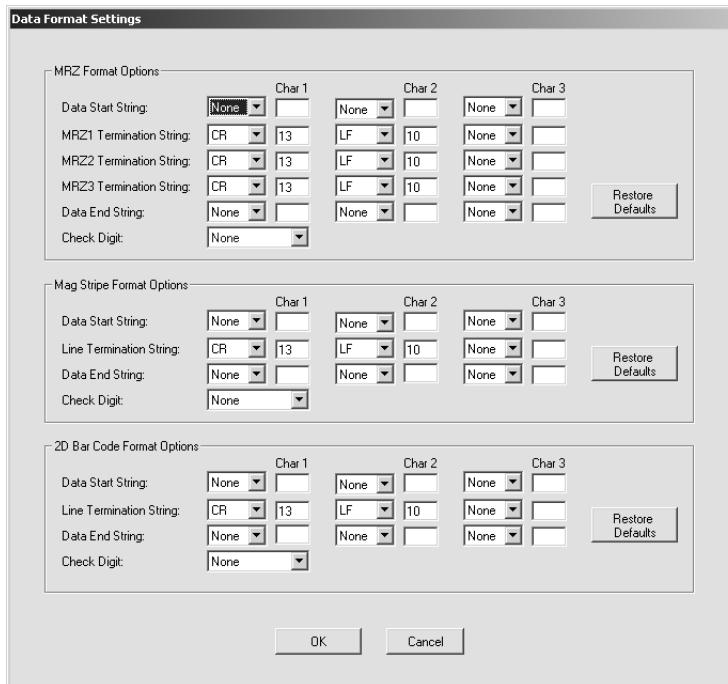
For MRZ data, you can specify as many as three characters to start the block of data, three characters to end the block of data, and three characters to insert after each line of the MRZ within the block of data, as well as a calculated check digit. Similarly, you can specify starting, ending, delineating, and check digit characters separately for magstripe data and 2D bar code data.

Note

To restore the factory-set values, click Restore Default Settings.

To configure data format settings:

1. Select Settings→Data Format Settings.



2. Under MRZ Format Options:

- Specify as many as three characters to send at the start of the MRZ data. To specify a character, you can:
 - Select it from the drop-down list of special characters, including NUL, STX, ETX, EOT, ENQ, ACK, HT, LF, VT, FF, CR, and ESC.
 - Or, select Other from the drop-down list and type the character's decimal ASCII value in the box to the right of the list
- Specify as many as three characters to insert at the end of the first line of MRZ data. Do the same for the second line and third line of MRZ data.
- Specify as many as three characters to send at the end of the entire block of MRZ data.
- Specify that a check digit be sent at the end of the data, calculated using the CRC16-ARINC algorithm.

3. Similarly, specify starting, delineating, and ending characters under Mag Stripe Format Options and 2D Bar Code Format Options. You can also select the check digit option for each.

4. Click OK.

Note

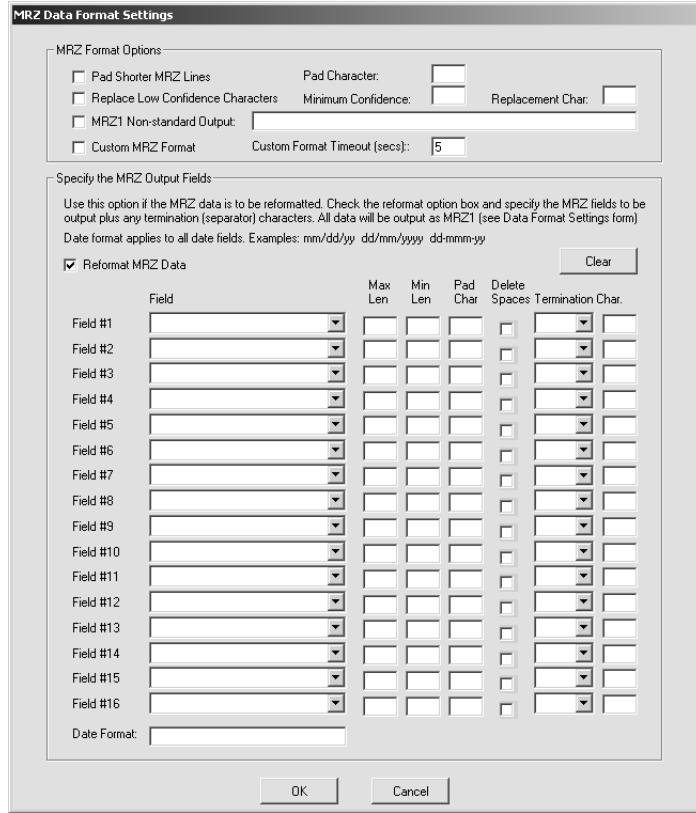
To restore the default settings for one of the kinds of data, click the matching Restore Defaults button.

Configuring MRZ Data Format Settings

In addition to the MRZ formatting options you set on the Data Format Settings screen, you can also format the MRZ data in other ways.

To configure MRZ data format settings:

1. Select Settings→MRZ Format Settings.



2. To make the data length the same for each MRZ line in a document, filling out shorter lines with extra characters to be the same length as the longest line, select **Pad Shorter MRZ Lines**. Specify the pad character you want to use.
3. To replace any character that the system has trouble reading with a different character:
 - a. Select **Replace Low Confidence Characters**.
 - b. For **Minimum Confidence**, specify how low the system's confidence must be before it replaces a character. The range is 0.0 to 1.0, and the default is 0.8.
 - Lowering the value tells the system to allow lower confidence in its readings, so it replaces fewer characters.
 - Raising the value tells the system to require higher confidence in its readings, so it replaces more characters.

- c. For Replacement Character, specify which character you want substituted for each doubtful character. For example, you might want to use a question mark (?) or underscore (_).
- 4. To send a notation or other text when the system is unable to automatically identify the document as a specific type (whether ICAO or non-ICAO), select MRZ1 Non-standard Output and enter the text you want to send. For example, you might want to send a notation such as [Unknown document].
- 5. Leave Custom MRZ Format *deselected* unless you have created a custom MRZ-processing application in consultation with Viisage Customer Support.
- 6. To process the captured MRZ data and send it in a different format, select Reformat MRZ Data and then choose how you want to format each field, in order. For each field:

Notes

- One field you can select is *Pass/Fail*. This is not MRZ data but an extra field for sending overall test results. Select this to send **P** when a document passes all tests, **E** when it fails only the expiration test, or **F** when it fails any other test.
- Setting *Max Len* and *Min Len* to the same number results in a fixed-length field.
- If you select *Delete Spaces*, iA-DataPort removes the embedded spaces before adjusting the field's length using the *Max Len* and *Min Len* settings.

- a. Under Field, select the name of the field—for example, Surname.
- b. If you want the field to be no longer than a certain length when iA-DataPort sends it, specify that length under Max Len. iA-DataPort then truncates longer fields to this length. If you don't want a long field truncated, leave Max Len blank.
- c. If you want the field to be *at least* a certain length when iA-DataPort sends it:
 - Under Min Len, specify the minimum number of characters the field should contain.
 - Under Pad Character, type the character you want to use to fill out a short field to the minimum length. The default is a space.
 If you don't want the field padded to any minimum length, leave Min Len blank or enter 0 (zero).
- d. If you want all spaces in the field removed, select *Delete Spaces*. For example, VAN LIND would become VANLIND.
- e. Under Termination Char, specify the character to insert immediately after a variable-length field to mark its end. You can select various untypeable characters (such as NUL) from the drop-down list, or you can enter any typeable character (such as >) in the second box.

Finally, specify the Date Format you want to use for sending dates. This determines the day-month-year order, the punctuation used between elements, the month format (number or abbreviation), and the year format (2 or 4 digits). For example, for August 14, 2003:

This date format...	Sends this data...
mm/dd/yy	08/14/03
yyyy-mm-dd	2003-08-14
dd mmm yyyy	14 Aug 2003

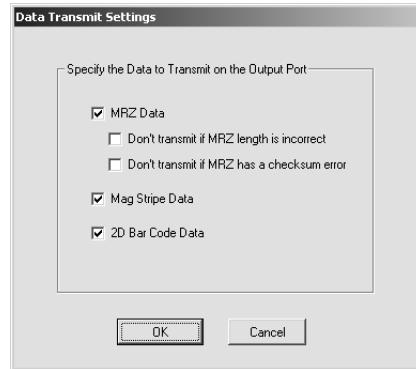
- 7. Click OK.

Configuring Data Transmit Settings

You can select which kinds of data you want the system to transmit—any combination of MRZ data, magstripe data, and 2D bar code data.

To configure data transmit settings:

1. Select Settings→Data Transmit Settings.



2. Select all the kinds of data you want the system to transmit to your application.
3. If you select MRZ Data, you can also select either or both of these options, to prevent transmission of faulty or questionable data:
 - Don't transmit if MRZ length is incorrect
 - Don't transmit if MRZ has a checksum error

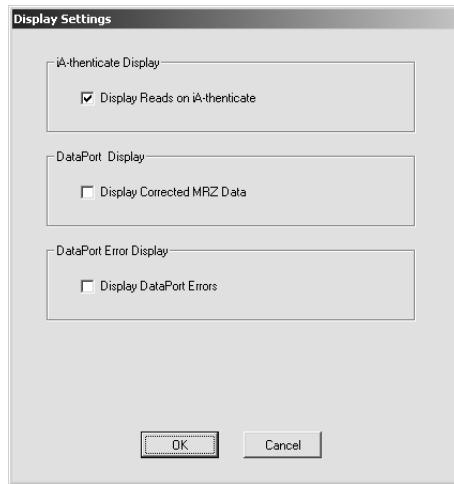
Configuring Display Settings

You can make several choices about:

- What kinds of information the iA-DataPort Utility displays on its main screen
- What additional kinds of information the system displays during operation (apart from the iA-DataPort Utility screen)

To configure display settings:

1. Select Settings→Display Settings.



2. Under iA-thenticate Display:

- If you have a BorderGuard unit with a text panel and you want DataPort to show extra messages there about magstripe and bar code processing, select Display Reads on iA-thenticate.

3. Under DataPort Display:

- If you select Replace Low Confidence Characters (page 10-10) and you want the displayed MRZ to show the replacement characters (rather than the original, doubtful ones), select Display Corrected MRZ Data.

4. Under DataPort Error Display:

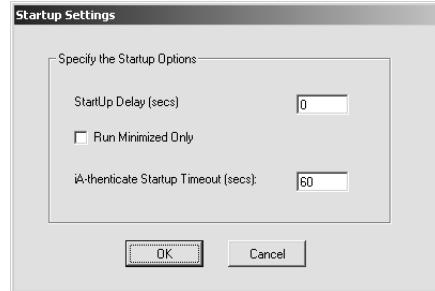
- If you want data port error messages to appear onscreen and on BorderGuard's built-in text panel whenever they occur, select Display DataPort Errors. You may want to do this when you first set up iA-DataPort and to troubleshoot any problems.
- To suppress such error messages so that the operator does not see them, deselect this option.

Configuring Startup Settings

iA-DataPort includes settings to set startup delays and to run the utility minimized so the operator doesn't see its screen.

To configure startup settings:

1. Select Settings→Startup Settings.



2. For Startup Delay, use the default value of 0 seconds. But if your unit is set up to run iA-DataPort automatically at startup, and you see error messages during startup, try increasing this value.
3. If you want the iA-DataPort utility to run minimized each time you start it, select Run Minimized Only. Do *not* select this option unless you have determined that you *can* run the utility minimized, as explained under "Running the Utility Minimized" on page 10-4.
4. For iAuthenticate Startup Timeout, use the default value of 60 seconds.
5. Click OK.

Appendices

A

Setting Up a Monochrome BorderGuard Unit

Note

If you have a monochrome BorderGuard *Plus* system (with built-in CPU), see the *Administrator's Guide* that came with your system for hardware setup information. For software upgrade instructions, see the *Release Notes* that came with the new software.

This chapter explains how to set up your iA-thenticate system if you have a BorderGuard (iA-thenticate) unit with a *monochrome* camera.

Before you proceed with installation, check the *Release Notes* for new information. If you are upgrading from a previous version, you may need to follow additional steps.

IMPORTANT

Although setting up this system is similar to setting up a PC, there are important differences. Follow the instructions in this chapter carefully, or your system may not work properly.

If you are not experienced in setting up and managing PCs in a networked environment, you should not attempt to do the setup yourself.

PC System Requirements

You install the iA-thenticate software on a Windows PC, and you connect the monochrome BorderGuard unit to the PC through a plug-in PCI interface card. Your PC must meet these requirements:

Hardware

- Processor: 800 MHz Pentium 4 or better recommended
- RAM: 256 MB minimum
- Free disk space: 300 MB minimum; 1 GB or more recommended when saving captured images and data
- Video display: 1024x768 resolution, 65536 colors, or better
- An available PCI-bus master slot, 2.0-compliant, capable of supplying 1.2 A at 12 VDC

Configuration

- Swap file: Recommended 768 MB minimum and 1024 MB maximum for drive C and for the data drive (where you store captured images)

Supported operating systems

- Windows 2000 Service Pack 4 or higher with updates 823980 (Microsoft Security Bulletin MS03-026) and 828028 (Bulletin MS04-007)
- Windows XP Professional Service Pack 2

Other software requirements

- Internet Explorer 6.0 Service Pack 1 or higher with update 832894 (Microsoft Security Bulletin MS04-004)

Installing Software

Do not connect the BorderGuard hardware yet.

Setting the PC's Taskbar and Display Properties

Your system should be configured so the taskbar displays on top of other windows and the font size is small (Windows 2000) or normal (XP). These are the default Windows settings. If you have changed these settings, follow these steps to restore the defaults:

Windows 2000	Windows XP
<ol style="list-style-type: none">1. Start the PC, log on as an administrator, and exit from all programs.2. Right-click the taskbar and choose Properties.3. On the Taskbar Properties screen, deselect Always on top and click OK.4. Right-click the Windows desktop and choose Properties.5. On the Settings tab, click Advanced.6. In the Font Size drop-down list, select Small Fonts if it is not already selected.7. Follow any further on-screen instructions for confirming your choice and installing fonts. You do <i>not</i> need to restart the system at this point unless Windows requires you to do so.	<ol style="list-style-type: none">1. Start the PC, log on as an administrator, and exit from all programs.2. Right-click the taskbar and choose Properties.3. On the Taskbar Properties screen, deselect Keep the taskbar on top of other windows and click OK.4. Right-click the Windows desktop and choose Properties.5. On the Appearance tab, in the Font Size drop-down list, select Normal if it is not already selected.6. Follow any further on-screen instructions for confirming your choice and installing fonts. You do <i>not</i> need to restart the system at this point unless Windows requires you to do so.

Note

The CD's folder names include the name of the software plus version information—for example, *iA-thenticate 5.3 Install (SFW-00099-A-00)*. For simplicity, these instructions use just the first part of the name—for example, *iA-thenticate....*

Note

If you are upgrading, the screens you see may differ slightly from the ones listed. Just follow the on-screen instructions.

Installing the iA-thenticate Security Software

Installer	Screen	Instructions
<i>iA-thenticate CD:</i> <i>iA-thenticate... \</i> <i>iA-thenticate... \</i> 1_iA-thenticate \ <i>Setup.exe</i>	Intro	Click Next.
	License	Click Yes to agree.
	Setup Type	Select BorderGuard - monochrome unit.
	Data Drive	<i>If</i> you want to change the drive for storing data, click Browse and choose any mapped drive. Click Next.
	Summary	Click Next to proceed with installation.
	Complete	Accept No, I will restart my computer later. Click Finish.

Installing iA-Examiner

Installer	Screen	Instructions
<i>iA-thenticate CD:</i> <i>iA-thenticate... \</i> <i>iA-thenticate... \</i> 2_iA-Examiner \ <i>Setup.exe</i>	Intro	Click Next.
	Data Drive	<i>If</i> you want to change the drive for storing iA-Examiner data, click Browse and choose a location. Click Next to proceed with installation.
	Complete	Click Finish.

Installing DL-Alert

If you have optional DL-Alert™ software—either the Intelli-Check or Positive Access® version—install it now.

Installer	Screen	Instructions
<i>iA-thenticate CD:</i> <i>iA-thenticate... \</i> <i>DL-Alert-IC... \</i> <i>DL-AlertIntelli-Check.exe</i> <i>or</i> <i>iA-thenticate... \</i> <i>DL-Alert-PA... \</i> <i>DL-Alert-PositiveAccess.exe</i>	Intro	Click Next to proceed with installation.
	Warning	Note the message and click OK. You will find instructions later in this document for configuring iA-Examiner.
	Complete	Click Finish.

Installing the Custom Calibration File

Note

Older BorderGuard units have a SampleScan diskette rather than a CD.

Each BorderGuard unit comes with a custom calibration file, supplied on a CD labeled SampleScan. One SampleScan CD may contain calibration files for several units.

1. Insert the SampleScan CD.
2. On the CD, find the folder that matches the serial number on the BorderGuard unit.
For reliable operation, you must use the correct calibration file for each unit.

3. Copy the SampleScan.cfg file from the folder to this directory:
C:\BorderGuard\Config\
4. Right-click the copied SampleScan.cfg file and choose Properties. Deselect Read-only and click OK.

Installing Other Optional Software

If you have other optional software such as ID-Passport or ID-License, install it now. Follow the instructions included with the optional software.

Restarting

After you finish installing software, restart your PC.

Installing Hardware

Install the BorderGuard hardware *only after you have installed the software* as described starting on page A-2.

Use proper antistatic procedures for the following steps, grounding yourself with a wrist strap or carefully discharging static by touching the metal case of the power supply.

Installing the PCI Card

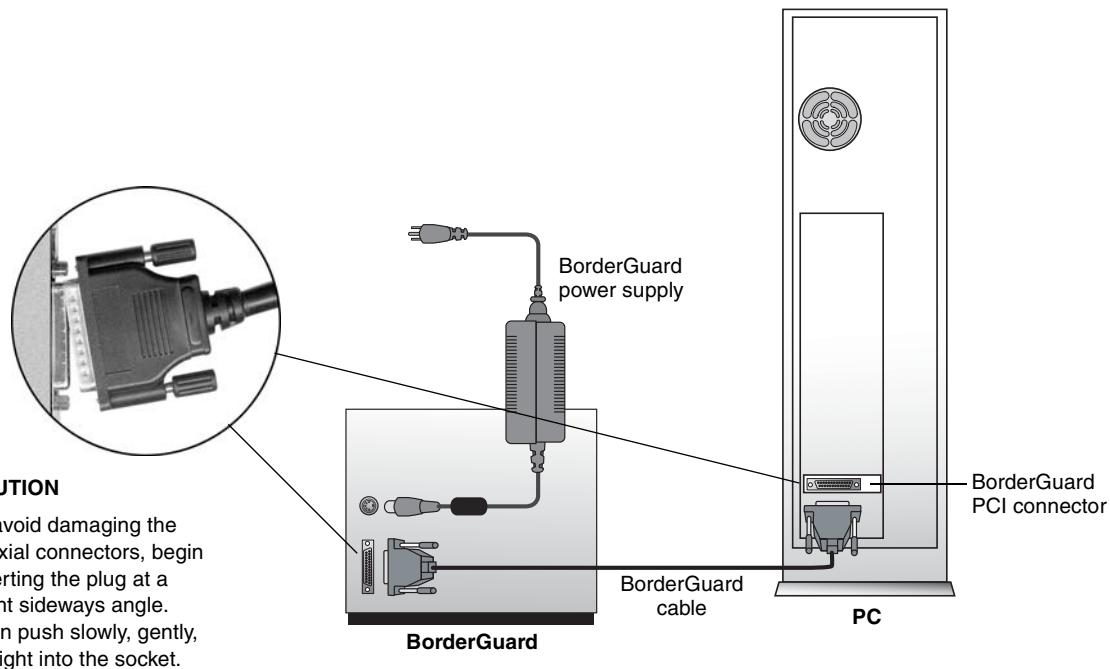
To install the PCI card into your PC:

1. Shut down the PC and disconnect the power and other cables.
2. Remove the PC's case to gain access to the PCI slots, following the instructions supplied by the PC manufacturer.
3. Remove the slot cover from an available PCI master slot.
4. Carefully align and insert the BorderGuard PCI card into the slot, applying just enough pressure to seat it fully.
5. Replace the screw from the removed slot cover to secure the PCI card.
6. Replace the PC's case and reattach its cables. *Do not start the PC* until you connect the BorderGuard cables as explained next.

Connecting the BorderGuard Cables

BorderGuard comes with a cable for connecting it to the PCI card you installed in your PC. It also comes with its own power supply and cord.

To connect the BorderGuard cables:



1. Plug one end of the BorderGuard cable into the connector on the PCI card you installed in your PC.
2. Plug the other end of this cable into the matching connector on the back of the BorderGuard unit.
3. Make sure the power switch on the BorderGuard unit is off.
4. Plug the cable from the BorderGuard power supply into the power connector on the back of the BorderGuard unit.
5. Plug the line cord from the power supply into a surge-protected power source that can supply 170 W at 100–240 VAC, 47–63 Hz.

Note

The included power supply might not have a power cord suitable for your country. In this case you must obtain and use a 3-conductor grounded supply cord with a plug cap suitable for your country. It must have a minimum internal conductor area of 0.75 mm² and have a standard IEC 320 female connector.

Finishing Installation

Starting Up and Checking Installation

1. Turn on the BorderGuard unit using its power switch.
2. Start the PC and log in as an administrator. You will see a message saying that the system has found new hardware.
3. When you see a message about the digital signature (Windows 2000) or Windows Logo testing (XP), click Yes or Continue Anyway.
4. Double-click the iA-Examiner icon on your desktop. After an initialization process, you should see the iA-Examiner screen.
If you see an error message instead, you must reinstall the driver as described on page B-12.
5. Exit by clicking the close button or selecting File→Exit.

Configuring Internet Explorer

If you use the VerifyMe verification database, follow these steps to configure Internet Explorer. Otherwise you can skip these steps.

1. Start Internet Explorer.
2. Select Tools→Internet Options.
3. On the Advanced tab, under the Security heading, deselect Warn if changing between secure and not secure mode.

Configuring a Non-English Version of Windows

If you install this software on a unit running a non-English version of Windows, you may need to follow some additional steps.

To configure Windows 2000—Dutch, French, or Portuguese:

1. Select Start→Run, type DCOMCNFG, and click OK.
2. On the Default Security tab, under Default Access Permissions, click Edit Default.
3. In the displayed list, look for an entry for SYSTEM and also for INTERACTIEF (Dutch), INTERACTIF (French), or INTERATIVO (Portuguese).

If either name is missing, follow these steps to add the missing name or names:

- a. Click Add.
- b. In the drop-down List Frames From list, select the name of your unit.
- c. In the Names list, select the missing name or names and click Add.
- d. Click OK several times to accept the changes.

To configure Windows XP—Dutch, French, or Portuguese:

1. Select Start→Run, type DCOMCNFG, and click OK.
2. Open Component Services, then Computers, then My Computer, and then DCOM Config.
3. Right-click BGServer and choose Properties.
4. On the Security tab, under Launch and Activation Preferences, select Customize and click Edit.
5. If the displayed list does not include INTERACTIEF (Dutch), INTERACTIF (French), or INTERATIVO (Portuguese), add the appropriate name and select all the Allow permissions.
6. In the same list, select all the Allow permissions for SYSTEM. Then click OK.
7. Back on the Security tab of the BGServer Properties window, under Access Permissions, select Customize and click Edit.
8. In the displayed list, select both of the Allow permissions for SYSTEM and for INTERACTIF, INTERATIVO, or INTERACTIEF. Then click OK.
9. In the BGServer Properties window, click OK. Then close the Component Services window.

Controlling Access

This section explains how to create local user groups and set file permissions for your system so that different users have just the access they need.

Creating Local User Groups and Users

First, create two local user groups and assign users to these groups as needed.

1. Create these two local user groups:

iA-thenticate Users
iA-thenticate Administrators

2. Create as many users as you need for the people who will use the system, and make each one a member of the appropriate user group:

Local User Group	Users Who Should Belong to This Group	Access Allowed
iA-thenticate Users	Personnel who use iA-Examiner to test and examine documents	iA-Examiner: user functions
iA-thenticate Administrators	Technical administrators, security managers, and operations managers	iA-Examiner: user and management functions iA-Administrator All Users startup folder (C:\Documents and Settings\All Users\Start Menu\Programs\Startup)

Assigning File and Folder Permissions

Assigning file and folder permissions ensures that each group of users can run the appropriate programs.

To assign file and folder permissions:

1. Follow steps a–c for each file in the table below:
 - a. Right-click the file and choose Properties.
 - b. Select the Security tab.
 - c. In the Name list, remove the entries for Everyone and Users (if listed). Then add Read & Execute permissions for user groups as indicated in the table.

For this file in C:\BorderGuard\Bin\	Assign Read & Execute permissions for these groups
iA-Administrator.exe (iA-Administrator)	iA-thenticate Administrators
BGDataPort.exe (iA-DataPort)	iA-thenticate Users iA-thenticate Administrators
BGExaminer.exe (iA-Examiner)	iA-thenticate Users iA-thenticate Administrators
BGServer.exe (ID-Server)	iA-thenticate Users iA-thenticate Administrators
ExaminerConfiguration (iA-Examiner configuration)	iA-thenticate Administrators
ExaminerManager (iA-Examiner management)	iA-thenticate Administrators
ExaminerReport (iA-Examiner reporting)	iA-thenticate Administrators
ExaminerViewer (iA-Examiner document review)	iA-thenticate Administrators
iA-SecondaryStation.exe (Secondary Station)	iA-thenticate Users iA-thenticate Administrators

2. iA-thenticate Administrators must be able to change startup settings for All Users. Follow these steps to assign the needed permissions to C:\Documents and Settings\All Users\Start Menu\Programs\Startup:

- a. Right-click folder C:\Documents and Settings and choose Properties.
- b. Select the Security tab.
- c. Add Full Control permissions for the iA-thenticate Administrators group.
- d. Repeat steps a–c for each successive folder in the path:

All Users (inside Documents and Settings)
 Start Menu (inside All Users)
 Programs (inside Start Menu)
 Startup (inside Programs)

3. If you use Windows security to limit users' access to various folders on your system, *all iA-thenticate users* must have these permissions:

- Full control to the work folder, normally C:\BorderGuard\Working
- Read and execute access to C:\BorderGuard and all of its sub-folders
- Read, write, and execute access to:
 - C:\BorderGuard\Config\SampleScan.cfg
 - The folder for storing captured images—for example, E:\BorderGuard\Images
 - The folder containing the iA-Examiner database BGExaminer.mdb, normally C:\BorderGuard\Bin
 - If you use TextWatch, the folder containing the TextWatch database iAT.sys, normally C:\BorderGuard\Bin

In addition, *iA-thenticate administrators* must have these permissions:

- Write access to:
 - The folder containing the iA-Administrator database Administrator.mdb, normally C:\BorderGuard\Bin
 - The Windows registry
- Read, write, and execute access to:
 - The configuration folder, C:\BorderGuard\Config and all sub-folders

Installing an Optional Reader or Scanner

If your system includes a bar code and magstripe reader or a flatbed scanner, install it now by following the instructions in chapter 4.

What's Next?

Your iA-thenticate system is now set up to work using factory-default settings. Probably you will want to change some of those settings. Part Two of this guide explains how.

B

Solving Problems

This appendix has instructions for solving specific problems mentioned elsewhere in this guide. For additional help, please contact Visage Customer Support:

support-ia@l1id.com
+1 978-932-2200
+1 800-555-8784 toll-free (North America)

Color BorderGuard

Drivers Do Not Install As Expected

Important!

During driver installation, never allow the new-hardware wizard to search for drivers by connecting to Windows Update. Installing drivers other than the ones supplied by Viisage can cause software malfunctions and system instability.

After you install software and then start color BorderGuard for the first time, Windows should install several drivers, as described on page 2-5. Windows XP should install all of them automatically, and Windows 2000 should install all but one automatically.

If this automatic process fails, and the new hardware wizard runs to ask for your help installing additional drivers, follow these instructions each time the wizard runs. You may also need to follow these steps if the drivers for an E-Seek Intelli-Check USB reader do not install as expected.

To install each device driver (repeat as needed):

Notes

- For a smart-card unit, you may need to install each of the SCR331-DI drivers twice.
- During driver installation, you may also be asked to locate the file ftser2k.sys. If so, browse to C:\BorderGuard\Tools\USB Serial.
- Whether you are installing in Windows 2000 or XP, clicking “Have Disk” and manually selecting the device driver will ensure that the correct driver is installed.

Windows 2000	Windows XP
<ol style="list-style-type: none"> 1. Make sure you can see the small window that shows the name of the hardware device; this is sometimes hidden behind the wizard. 2. On the first wizard screen, click Next. 3. Select Display a list of known drivers for this device so that I can choose a specific driver, and click Next. 4. Click Have Disk and browse to the file shown in the table below. (If there is no Have Disk button, first click Next and then click Have Disk.) 5. When the wizard displays the driver, click Next. 6. If you see a message about the digital signature, click Yes to continue. If you are asked whether you want to overwrite a newer file, click Yes. 7. Click Finish. 	<ol style="list-style-type: none"> 1. Make sure you can see the small window that shows the name of the hardware device; this is sometimes hidden behind the wizard. 2. If the first wizard screen asks about connecting to Windows Update to search for software, select No, not this time and click Next. 3. Select Install from a list or specific location (Advanced) and click Next. 4. Select Don’t search. I will choose the driver to install. Click Next. 5. Click Have Disk and browse to the folder shown in the table below. (If there is no Have Disk button, first click Next and then click Have Disk.) 6. If you see a warning about the digital signature, click Continue Anyway. If you are asked whether you want to overwrite a newer file, click Yes. 7. Click Finish.

Driver files and locations:

For this hardware device:	Browse to this file:
USB 2.0 Camera or Color Camera 01	C:\Borderguard\Tools\BorderGuard Camera\OVtcam2.inf
USB Fast Serial Adapter	C:\Borderguard\Tools\USB Serial\FTDIBUS.INF
USB Serial Port	C:\Borderguard\Tools\USB Serial\FTDIPORT.INF
SCR331-DI USB Smart Card Reader	C:\Borderguard\Tools\SCM SCR331-DI Reader\S331DI2K.INF
SCR331-DI Contactless Reader	C:\Borderguard\Tools\SCM SCR331-DI Reader\S331DICL.INF

Camera Driver Installation Problems

If you have followed the steps in the table above and still experience problems, you may need to uninstall and reinstall the camera driver.

To uninstall and reinstall the camera driver:

1. In Add/Remove Programs, select Uninstall OmniVision SuperCAM and remove the program.
2. Open Device Manager (Right-click My Computer, choose Manage, and click Device Manager).
3. In the imaging devices section, look for an OmniVision camera entry with a yellow exclamation point. If the OmniVision entry is there, right-click the entry and choose Uninstall.
4. Right-click the computer name at the top of the list and select Scan for Hardware Changes.
5. When prompted for the camera driver, follow the steps in the table above to install.

iA-Examiner Reports a COM Port Error

With a color BorderGuard unit that has no serial cable, when you start iA-Examiner after installing software as described on page 2-7, you should see the main iA-Examiner screen. If you see an error message about a COM port, you must follow these steps to find the port number assigned to the camera and configure the system to use it.

1. Open Device Manager. (Right-click My Computer, choose Manage, and click Device Manager.)
2. Expand the Ports (COM & LPT) item and find any USB Serial Port listings.
 - If there is only one entry, note the COM port number assigned to it. For example, it might be listed as USB Serial Port (COM3).
 - If you have an E-Seek magstripe and bar code reader, you will see two USB Serial Port listings. To determine which one belongs to the color camera, unplug the E-Seek reader and watch to see which entry disappears. Note the COM port number assigned to the *remaining* entry. Then reconnect the E-Seek reader.
3. Run iA-Administrator by choosing Start→Programs→iA-thenticate→iA-Administrator.
4. On the Configuration tab, under Advanced, select the number for Color camera COM port that matches the one you found in Device Manager.
5. Click Apply, then exit iA-Administrator.

If the problem persists when you run iA-Examiner again, contact Viisage Customer Support.

Color BorderGuard B4500/5000

Drivers Do Not Install As Expected

Important!

During driver installation, never allow the new hardware wizard to search for drivers by connecting to Windows Update. Installing drivers other than the ones supplied by Viisage can cause software malfunctions and system instability.

Notes

- During driver installation, you may also be asked to locate the file ftser2k.sys. If so, browse to C:\BorderGuard\Tools\USB Serial.
- Whether you are installing in Windows 2000 or XP, clicking "Have Disk" and manually selecting the device driver will ensure that the correct driver is installed

After you install software and then start the B4500/5000 for the first time, Windows should install several drivers automatically, as described on page 2-5.

If this automatic process fails, and the new hardware wizard runs to ask for your help installing additional drivers, follow these instructions each time the wizard runs. You may also need to follow these steps if the drivers for an E-Seek Intelli-Check USB reader do not install as expected.

To install each device driver (repeat as needed):

Windows 2000	Windows XP
<ol style="list-style-type: none"> 1. Make sure you can see the small window that shows the name of the hardware device; this is sometimes hidden behind the wizard. 2. On the first wizard screen, click Next. 3. Select Display a list of known drivers for this device so that I can choose a specific driver, and click Next. 4. Click Have Disk and browse to the file shown in the table below. (If there is no Have Disk button, first click Next and then click Have Disk.) 5. When the wizard displays the driver, click Next. 6. If you see a message about the digital signature, click Yes to continue. If you are asked whether you want to overwrite a newer file, click Yes. 7. Click Finish. 	<ol style="list-style-type: none"> 1. Make sure you can see the small window that shows the name of the hardware device; this is sometimes hidden behind the wizard. 2. If the first wizard screen asks about connecting to Windows Update to search for software, select No, not this time and click Next. 3. Select Install from a list or specific location (Advanced) and click Next. 4. Select Don't search. I will choose the driver to install. Click Next. 5. Click Have Disk and browse to the folder shown in the table below. (If there is no Have Disk button, first click Next and then click Have Disk.) 6. If you see a warning about the digital signature, click Continue Anyway. If you are asked whether you want to overwrite a newer file, click Yes. 7. Click Finish.

Driver files and locations:

For this hardware device:	Browse to this file:
USB 2.0 Camera or Color Camera 01	C:\Borderguard\Tools\BorderGuard Camera\OVUSB2.inf
USB Fast Serial Adapter	C:\Borderguard\Tools\USB Serial\FTDIBUS.INF
USB Serial Port	C:\Borderguard\Tools\USB Serial\FTDIPORT.INF

Camera Driver Installation Problems

In some cases, the camera driver may try to load automatically during installation. A digital signal warning may appear and you may be prompted for a file you cannot find in the C:\Borderguard\Tools\BorderGuard Camera directory. If this happens, exit the wizard and use the following steps to update the drivers using Device Manager.

Also use this procedure if any of the following problems occur:

- Error message “No Camera Found” at startup
- Images are upside down
- Documents inserted in B4500/5000 are not recognized

To update drivers using Device Manager:

1. Open Device Manager (Right-click My Computer, choose Manage, and click Device Manager).
2. In the Imaging Devices folder, right-click OmniVision SuperCam and select Properties.
3. On the Drivers tab, verify that the Driver Version is 2.1.0.1 and the Driver Date is 10/15/2007.
4. If the driver has the wrong version or date stamp, or if an exclamation point or question mark appears next to the icon in Device Manager, click Update Driver. Use the “Have Disk” path and locate the driver file specified on page B-4.

Uninstalling and Reinstalling the Camera Drivers

If you have followed the steps above and still experience problems, you may need to uninstall and reinstall the camera driver.

To uninstall and reinstall the camera driver:

1. In Add/Remove Programs, select Uninstall OmniVision SuperCAM and remove the program.
2. Open Device Manager (Right-click My Computer, choose Manage, and click Device Manager).
3. In the imaging devices section, look for an OmniVision camera entry with a yellow exclamation point. If the OmniVision entry is there, right-click the entry and choose Uninstall.
4. Right-click the computer name at the top of the list and select Scan for Hardware Changes.
5. When prompted for the camera driver, follow the steps in the table above to install.

iA-Examiner Reports a COM Port Error

With a color BorderGuard unit that has no serial cable, when you start iA-Examiner after installing software as described on page 2-7, you should see the main iA-Examiner screen. If you see an error message about a COM port, you must follow these steps to find the port number assigned to the camera and configure the system to use it.

1. Open the Device Manager. (Right-click My Computer, choose Manage, and click Device Manager.)
2. Expand the Ports (COM & LPT) item and find any USB Serial Port listings.
 - If there is only one entry, note the COM port number assigned to it. For example, it might be listed as USB Serial Port (COM3).
 - If you have an E-Seek magstripe and bar code reader, you will see two USB Serial Port listings. To determine which one belongs to the color camera, unplug the E-Seek reader and watch to see which entry disappears. Note the COM port number assigned to the *remaining* entry. Then reconnect the E-Seek reader.
3. Run iA-Administrator by choosing Start→Programs→iA-thenticate→iA-Administrator.
4. On the Configuration tab, under Advanced, select the number for Color camera COM port that matches the one you found in Device Manager.
5. Click Apply, then exit iA-Administrator.

If the problem persists when you run iA-Examiner again, contact Viisage Customer Support.

Smart Card Driver Installation Problems

To check and reinstall the smart card drivers if necessary:

1. Open Device Manager (Right-click My Computer, choose Manage, and click Device Manager).
2. Look for OmniKey55x3 or USB Converter in the SmartCard Devices folder or the Other Devices folder.
3. If an exclamation point appears next to the icon, close Device Manager and browse to the file C:\BorderGuard\Tools\ACG\Ominkey55x3_v2_1_DualAntenna_x86.msi to start the installation wizard.
4. On the first screen of the wizard, click Next.
5. On the End User Agreement screen, check the “I accept” box and click Next.
6. On the Custom Setup screen, accept the default and click Next.
7. On the next screen, click Install.
8. If you see a message about the digital signature, click Yes to continue. If you are asked whether to overwrite a newer file, click Yes.

The final screen of the installation wizard indicates if the driver setup has been successful. If driver setup is *not* successful, or if you see an OmniKey error message during installation, proceed to “Repairing the OmniKey Registration Settings” on page B-8.

Smart Card Error on iA-Examiner Startup

If you try to start iA-Examiner and get a smart card device error on a Windows 2000 system, this may have been caused by turning the B4500/5000 off and on again, or unplugging the USB cable and then plugging it in again. To correct the error, reboot the system.

Testing the Smart Card Reader

The following two procedures will check the smart card reader functionality. You can use *either* the iA-Examiner test or the OMNIKEY applet test.

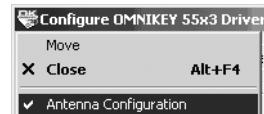
To test the smart card reader using iA-Examiner:

1. In iA-Examiner, process a smart card document that has its chip in the front cover side of the document (on the glass).
2. Process a smart card document that has its chip in the back cover side of the document (on the platform in front of the glass).
3. Check the smart card test results for both documents.

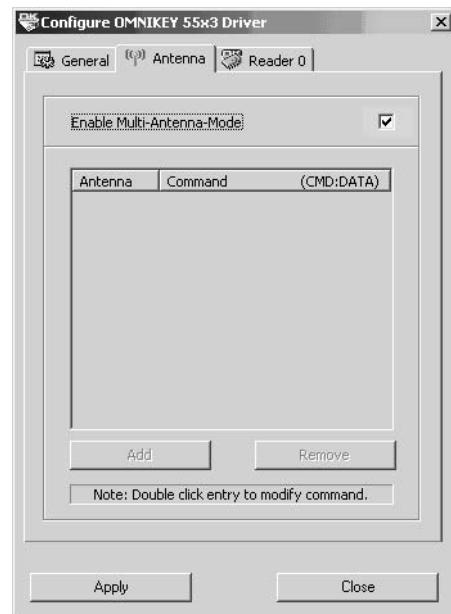
If iA-Examiner displays smart card test results for both documents, the unit is operating correctly. If iA-Examiner fails to recognize the smart card, follow the instructions for fixing the problem in “Repairing the OmniKey Registration Settings” on page B-8.

To test the OMNIKEY applet:

1. In Control Panel, run the OMNIKEY 55x3 Driver Applet.
2. Right-click in the title bar of the applet and select Antenna Configuration.



3. On the Antenna tab, verify that “Enable Multi-Antenna Mode” is checked.

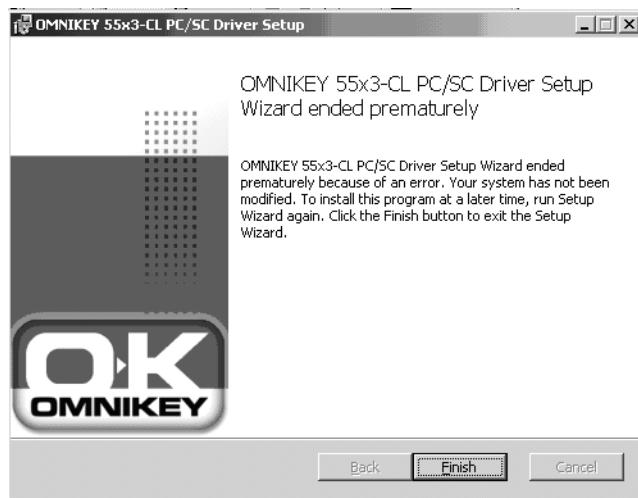


If “Enable Multi-Antenna Mode” is not checked, proceed to the next section, “Repairing the OmniKey Registration Settings.”

Repairing the OmniKey Registration Settings

Follow this procedure if any of the following occurs:

- iA-Examiner fails to recognize a smart card after you configured the smart card unit (see “Testing the B4500/5000 Smart Card Reader” on page 2-8).
- The OmniKey applet test on page B-7 shows that “Enable Multi-Antenna Mode” is not checked.
- The following error appears during installation:
“Cannot import C:\Program Files\OmniKey\55x3 Driver V2.1.0.8\settings.reg”
- Driver setup is *not* successful or you receive the following OmniKey error message when you follow the procedure in “Smart Card Driver Installation Problems” on page B-6.



To repair the registration settings:

1. In the folder C:\Program Files\OmniKey\55x3 Driver V2.1.0.8, double-click the file **settings.reg**.
2. Click **Yes** to add the information in the file to the registry.
3. In the dialog box that confirms the information was entered, click **OK**.
4. Reboot the system.

ID-Guard

Scanning Produces Unexpected Behavior

If this happens...	The problem may be:	To solve the problem:
Images display incorrectly and the system fails to identify documents. The visible image may look like an IR image.	This problem is usually due to an underpowered PC, especially if running a laptop on batteries.	<p>Each ID-Guard unit ships with a Y-shaped USB cable for use with computers that do not supply adequate power through a single USB port. For additional power, plug the extra USB connector into a second USB 2.0 port on the computer.</p> <p>You may be also able to increase laptop power changing the default battery setting for higher performance.</p> <p>Additionally, you may be able to resolve the problem by adjusting the capture timing for the ID-Guard unit (the default value for Capture Delay is 100). In iA-Administrator, click the Configurations tab. Change the Capture Delay to 200 and reboot the PC. If the problem persists, increase the value in increments of 100, restarting each time, until the problem stops.</p>
ID-Guard system fails to read bar codes after installation.	Previous version of Regula software was not properly uninstalled before installing the ID-Guard software.	<p>In Add/Remove programs, look for two instances of Regula Document Reader SDK. (Note that Regula Document Reader Core Components may be present and is not related to this problem.) Uninstall both instances of Regula Document Reader SDK.</p> <p>Reinstall Regula Document Reader SDK 4.10.</p>

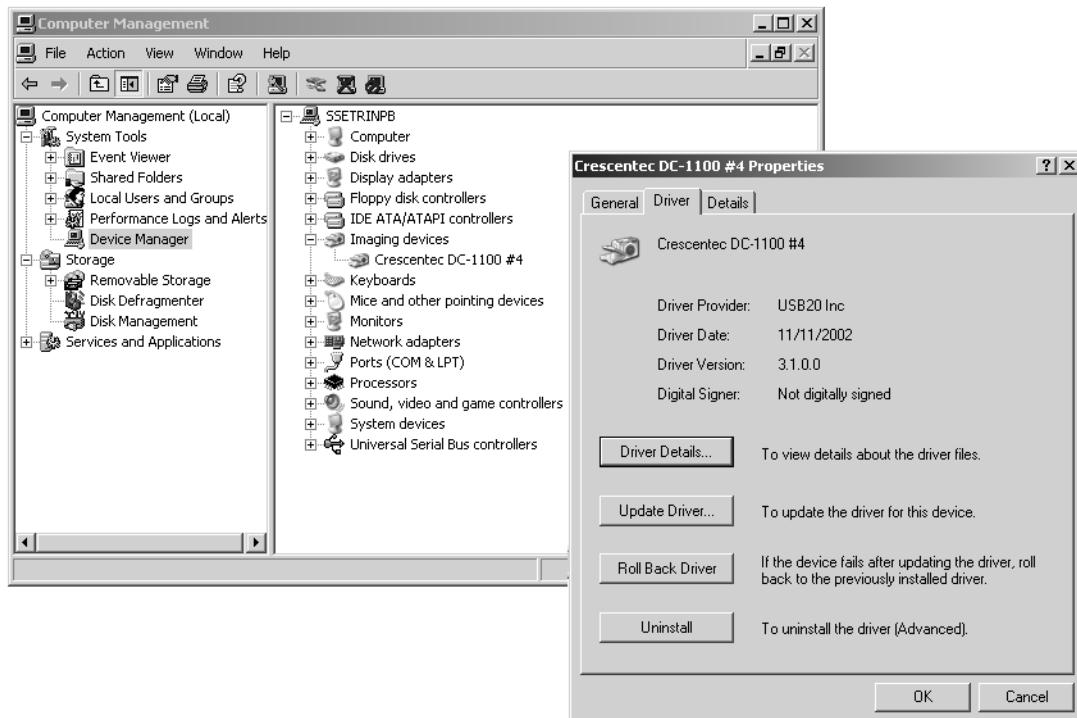
Camera Driver Installation Problems

In some cases, the camera driver may try to load automatically during installation. A digital signal warning may appear and you may be prompted for a file you cannot find in the C:\BorderGuard\Tools\BorderGuard Camera directory. If this happens, exit the wizard and use the following steps to update the drivers using Device Manager.

Also use this procedure as a troubleshooting tool if any problems with camera operation occurs.

To update drivers using Device Manager:

1. Open Device Manager (Right-click My Computer, choose Manage, and click Device Manager).
2. In the Imaging Devices folder, right-click Crescentec DC-1100, and select Properties. Select the Driver tab and verify that the driver version is correct (Windows XP shown):



Windows XP:

Provider = USB20 Inc.
Version = 3.1.0.0
Date = 11/11/2002

Windows 2000:

Provider = USB20 Inc.
Version = 3.1.0.0
Date = Not available

3. If the wrong driver version is installed or if an exclamation point or question mark appears next to the icon in Device Manager, click Update Driver, and install the device driver using the following instructions:

Windows 2000	Windows XP
<ol style="list-style-type: none"> 1. Make sure you can see the small window that shows the name of the hardware device; this is sometimes hidden behind the wizard. 2. On the first wizard screen, click Next. 3. Select Search for a suitable driver for my device (recommended) and click Next. 4. Select Specify a location and click Next. 5. Browse to the folder shown in the table below and click Next. 6. If you see the message “Digital signature, not found” displays, click Yes to continue. 7. If you are asked whether you want to overwrite a newer file, click Yes. 8. Click Finish. 	<ol style="list-style-type: none"> 1. Make sure you can see the small window that shows the name of the hardware device; this is sometimes hidden behind the wizard. 2. If the first wizard screen asks about connecting to Windows Update to search for software, select No, not this time and click Next. 3. Select Install from a list or specific location (Advanced) and click Next. 4. Select Don't search. I will choose the driver to install. Click Next. 5. Click Have Disk and browse to the folder shown in the table below. (If there is no Have Disk button, first click Next and then click Have Disk.) 6. If you see a warning about the digital signature, click Continue Anyway. If you are asked whether you want to overwrite a newer file, click Yes. 7. Click Finish.

Driver files and locations:

For this hardware device:	Browse to this file:
ID Tech USB Serial Converter	C:\Borderguard\Tools\ID-Tech USB\FTDIBUS.INF
USB 2.0 Camera or Crescentec DC-1100	C:\Borderguard\Tools\Crescentec\dc1100.inf
ID Tech USB Serial Port or USB Serial Port	C:\Borderguard\Tools\ID-TechUSB\FTDIPORT.INF

Monochrome BorderGuard

iA-Examiner Reports an IACOM0 Error

With a monochrome BorderGuard unit, when you start iA-Examiner after installing software as described on page A-6, you should see the main iA-Examiner screen. If the driver for the PCI card was not properly installed for some reason, you see one of these error messages instead:

IACOM0: The system cannot find the file specified.

IACOM0: The port does not exist. Please check for its availability.

In this case you must follow these steps to reinstall the driver:

Windows 2000	Windows XP
<ol style="list-style-type: none">1. Open the System control panel. On the Hardware tab, click Device Manager.2. Under Imaging Devices (or possibly Other Devices) find the item named Multimedia Controller, displayed with an exclamation point. Right-click it and select Properties.3. On the Driver tab, click Update Driver.4. On the first screen of the wizard, click Next.5. On the next screen, select Search for a suitable driver... and click Next.6. On the next screen, deselect all the checkboxes and click Next.7. On the next screen, click Next.8. On the Digital Signature Not Found screen, click Yes.9. On the final screen, click Finish.	<ol style="list-style-type: none">1. Open the System control panel. On the Hardware tab, click Device Manager.2. Under Imaging Devices (or possibly Other Devices) find the item named Multimedia Controller, displayed with an exclamation point. Right-click it and select Properties.3. On the Driver tab, click Update Driver.4. On the first screen of the wizard, select Install the software automatically... and click Next.5. When you see a message about Windows Logo testing, click Continue Anyway.6. On the final screen, click Finish.

Now try starting iA-Examiner again. If you still get an error message, contact Viisage Customer Support.

E-Seek Intelli-Check Magstripe and Bar Code Reader

Scanning a Magstripe or Bar Code Produces an Error

Note

iA-DataPort displays errors only if *Display DataPort Errors* is selected as described on page 10-13).

If you have the E-Seek Intelli-Check magstripe and bar code reader, and iA-Examiner or iA-DataPort keeps displaying an error message when you scan a magstripe or bar code, the reader may have lost its correct settings. Typical error messages:

- iA-Examiner: E-Seek identifier code not found
- iA-DataPort: E-Seek header is not enabled or an extra beep after reading a document

To reset the E-Seek Intelli-Check reader to its correct settings:

- Find the setup card supplied with the reader.

If you can't find the supplied card, make a clean photocopy of this page on heavy, stiff paper, and cut out the card. (Or use ordinary paper and tape the photocopied bar code onto a blank ID card.)

- With the E-Seek Intelli-Check reader powered on, scan the bar code by briskly inserting and removing the card. The reader should respond with a warbling beep indicating that the settings have been accepted.



Flatbed Scanner

Scanning Produces an Error or Unexpected Behavior

If this happens...	The problem may be:	To solve the problem:
When you start iA-Examiner, you see the message Component VSTwain.dll or one of its dependencies not correctly registered.	The scanner software is not correctly installed.	Follow the scanner manufacturer's instructions for installing the scanner software.
When you start iA-Examiner, you see the message Warning! The flatbed scanner is off-line.	The scanner is turned off or its USB cable is disconnected.	Check the scanner's power source, power switch, and USB cable. If that doesn't work, restart iA-Examiner.
When you click Scan, you see the message Scanner error. Ready for new document. You may also see a message about the scanner driver.	The scanner has lost communication with the computer.	Wait a few moments and click Scan again. If that doesn't work, restart iA-Examiner.
While the scanner is scanning, you see the message Scanner error. Ready for new document.	The scanner timeout is too short.	On System Configuration Page 1, enter a longer time for T/O (timeout).
After you replace one scanner with a different model, you see the message Warning! The flatbed scanner is off-line.	iA-Examiner is still expecting the previous scanner.	On System Configuration Page 1, first deselect Scanner. Then select Scanner again, and choose your new scanner model from the list.
After you properly install and configure a scanner, and try to use it to scan a document, it always times out without scanning.	Previously installed scanner software may be interfering with the current scanner.	Exit iA-Examiner. Run the software provided by the scanner manufacturer for capturing images. If it displays a list of scanners to use, be sure to choose your current model. Use it to scan a test document, and then exit. Run iA-Examiner and try scanning again.
When you try to configure the scanner options on System Configuration Page 1, iA-Examiner seems unresponsive.	An error may have occurred that is preventing you from selecting the options.	Minimize iA-Examiner and look for a window with a system error message.

If this happens...	The problem may be:	To solve the problem:
Even though you have selected the Crop Scanned Image option, images are not correctly cropped.	The scanner's glass platform may be dirty or dusty.	Clean the scanner's glass according to the manufacturer's instructions.
	The cropping software may be malfunctioning.	If you have chosen a resolution higher than 100 dpi, try returning to the default resolution of 100 dpi.
	Cropping does not currently work properly with the Canon CanoScan LiDE 500F.	Use a different scanner.
The system takes a long time to process a document placed on the iA-thenticcate unit (as much as a minute or more), or the captured image is black.	The scanner may have disrupted communication with the iA-thenticcate unit.	Disconnect the USB cable from the scanner, wait a few seconds, and reconnect it.

C Periodic Maintenance

Follow these procedures to keep your BorderGuard or ID-Guard unit working accurately and efficiently.

Cleaning the Glass Platform

During normal use, the glass document platform becomes dusty and smudged with fingerprints. It can also become sticky with adhesives from the documents you process.

To keep the unit working properly, you must keep the glass clean. You should clean the glass routinely at least once a week, and immediately if it becomes sticky.

We strongly recommend using pre-moistened optical wipes to clean the glass. They are effective, safe, convenient, and inexpensive.

Warnings:

- Never spray liquid onto the glass or any other part of the unit.*
- Never use an abrasive cleaner or pad of any kind.*
- Use only wipes that are specifically for cleaning optical surfaces.*

To clean the glass platform:

❖ Gently wipe the glass with a pre-moistened optical wipe.

As an alternative, you can use a clean, soft, lint-free cloth slightly moistened with denatured alcohol or a nonabrasive glass cleaner.

Cleaning the BorderGuard Sensor Switch

Some BorderGuard units use a mechanical sensor switch to detect an inserted document. Dirt and bits of paper can slip underneath this switch and interfere with its operation, so that the unit doesn't always respond when you place a document on the platform.

About once a month, or whenever a unit has problems responding to a document, you should check and clean the sensor switch.

To clean the sensor switch:

1. Raise the light shield and locate the sensor switch lever, at the back left corner of the platform.
2. Gently vacuum the switch area, being careful not to mar the glass.
3. Carefully remove any bits of paper stuck under the lever.

Defragmenting the Hard Drive

During normal use, the files and free space on your PC's hard drive become fragmented. As fragmentation becomes worse, your system runs less efficiently.

About once a month, you should use Disk Defragmenter to check your hard drive for fragmentation and to defragment it as necessary. The check takes just a few moments; defragmentation can take 15 minutes or more.

To check and defragment the hard drive:

1. Log on as an administrator.
2. Run Disk Defragmenter (Start→Programs→Accessories→System Tools→Disk Defragmenter).
3. Select the C drive and click **Analyze**.
4. If Disk Analyzer reports that the volume needs defragmenting, click **Defragment** to proceed.

Note: Even if Disk Analyzer reports that the volume does not need defragmenting, you can defragment it as a preventive measure.

5. If your system has additional drives, check and defragment them in the same way.



An L-1 Identity Solutions Company

ViiSAGE Technology, Inc.
296 Concord Road, Billerica, MA 01821 USA
T 978.932.2200 F 978.932.2225
www.viisage.com

PUB-00052-A-15