iA-thenticate Administrator's Guide

5.5

Document Number PUB-00052-B-00

L-1 Identity Solutions Technology

Confidential Information

Notice

RADIO AND TELEVISION INTERFERENCE

NOTE: 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 and Modifications not expressly approved by **L1 Identity Solutions** can void your authority to operate this equipment under Federal Communications Commissions rules.

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

About this Guide

The *iA-thenticate Administrators Guide* describes how to install, configure, and manage the L-1 iA-thenticate applications.

Who Should Read this Guide

This guide is intended for technical personnel and system administrators responsible for installing, configuring and managing the iA-thenticate system. Personnel should be familiar with Microsoft Windows applications.

Related Documents

PUB-00051-A-14	iA-thenticate 5.4 User Guide
PUB-00008-B-00	iA-thenticate 5.5 Release Notes
PUB-00190-A-00	iA-thenticate 5.5 Quick Configuration Guide

Revision History

Rev	Date	Comments
0.1		Preliminary review draft.
0.2	8/4/2010	First Technical Review
0.3	8/17/2010	Second Technical Review
1.0	9/1/2010	5.5 Release
1.1	5/6/2011	Added FCC/IC statements

Table of Contents

L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION

Chapter 1. Introduction

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

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.

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.

Figure 1.   Color BorderGuard with Smart Chip Reader

Figure 2.   Color Border Guard B4500/B5000

ID-Guard/J1000

ID-Guard/J1000 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.

Figure 3.   ID-Guard/J1000

L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION

Setting Up Your System

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

- See Chapter 2 to setup a Color BorderGuard unit.

- See Appendix A to setup a Monochrome BorderGuard unit.

- See Chapter 3 to set up an ID-Guard/J1000 unit.

- See Chapter 4 to setup additional hardware

- See Chapter 5 to familiarize yourself with the administrative tools you need to configure your system.

- See Chapters 6 and 7 to Configure your system.

- See Chapters 8 and 9 to Manage your system.

L-1 IDENTITY SOLUTIONS
    SECURE CREDENTIALING DIVISION

Chapter 2. Setting Up a Color 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. Refer to the *iA-thenticate 5.5 Release Notes* for additional information.

Note: 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.

L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION

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 the following requirements:

Hardware

For Windows XP

- 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)

Note: For Color BorderGuard units with USB ports, adding USB devices may increase the minimum system requirements. L-1 recommends using the USB ports on your computer before using any ports that may be on the back of the BorderGuard unit.

For Windows Vista and Windows 7

- Processor: 2.8 GHz Pentium 4 or better
- RAM: 512 MB minimum
- Free disk space: 16 GB
- 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: L-1 recommends 768 MB minimum and 1024 MB maximum for drive C and for the data drive (where you store captured images).

L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION

Supported Operating Systems

- Windows XP Professional Service Pack 2

- Windows Vista

- Windows 7

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.

L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION

Installing Software

Note: Do **not** connect the BorderGuard hardware yet.

Setting the PC's Power Scheme (Windows XP)

For optimal performance, the Power Scheme for the host computer should be set to **Always on**. This setting applies to laptops and PCs running Windows XP.

1. From the Windows **Start** button, select **Control Panel > Power Options**.
2. Click the **Power Schemes tab**.
3. In the **Power schemes** drop down list, select the **Always on** option.

Setting the PC's Power Scheme (Vista)

1. From the Windows **Control Panel,** select **Power Options**.
2. Select **Adjust Power Settings**.
3. Select the **High Performance** power plan.
4. Make sure that the **Put the Computer to Sleep** option is set to **Never**.

Setting the PC's Power Scheme (Windows 7)

1. From the Windows **Control Panel,** select **System and Security.**
2. Select **Power Options**.
3. Select the **Balanced** Power Plan and then click on **Change plan settings.** The **Edit plan settings** screen appears. Change both dropdown items (**Turn off Display** and **Put the computer to sleep**) to **Never**.
4. Expand the **Sleep** option and select **Change Advanced power settings**. The **Advanced Power settings** screen appears.
5. Set both the **Sleep after** and **Hibernate after** settings to **Never.**
6. Click **OK** and **Save Changes** on both this screen and the **Edit plan settings** screen**.**

Installing DirectX (Windows XP)

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
iA-thenticate CD: *iA-thenticate… * *iA-thenticate… * **DirectX** \ *directx_9c_oct05sdk_redist.exe*	Follow the on-screen instructions.

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, **iA-thenticate….**, for example.

Installing the iA-thenticate Security Software

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

Installer	Screen	Instructions
iA-thenticate CD: *iA-thenticate… * *iA-thenticate… * **1_iA-thenticate** \ *Setup.exe*	Intro	Click **Next**.
	License	Click **Yes** to agree.
	Setup Type	**For Windows XP only:** If you have a Color BorderGuard unit with a text panel above the document platform, select **BorderGuard - color unit**. If you have a Color BorderGuard B4500/5000 unit with indicator lights rather than a text panel, select **BorderGuard - B4500/B5000** **For Windows Vista and Windows 7:** **For** BorderGuard – B4500/B5000**,** click **Next**.
	Data Drive	If 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
iA-thenticate CD: *iA-thenticate… * *iA-thenticate… * **2_iA-Examiner** \ *Setup.exe*	Intro	Click **Next**.
	Data Drive	If 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 the optional **DL-Alert™** software, either the **Intelli-Check** or **Positive Access®** version, install it now.

Installer	Screen	Instructions
iA-thenticate CD: *iA-thenticate… \ DL-Alert-IC… \ DL-AlertIntelli-Check.exe* **or** *iA-thenticate… \ DL-Alert-PA… \ DL-Alert-PositiveAccess.exe*	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** or **ID-License** or **Global-ID**, install it now. Follow the instructions included with the optional software.

Restart your PC

After installing all your software, restart your PC.

L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION

Connecting Hardware and Installing Drivers

Connect the BorderGuard hardware only after you have installed the software as described in the previous section.

Connecting Hardware

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

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.

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 Border-Guard 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.
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. When the unit is connected and powered on, the drivers should install automatically. If Windows indicates that there was a problem with the installation, follow the problem-solving instructions in the *Drivers Do Not Install As Expected* section of Appendix B for color BorderGuard units.

Installing the Custom Calibration File

Each BorderGuard unit comes with custom calibration files. For reliable operation, you must install the correct calibration file for each unit.

To install the custom calibration file on Color BorderGuard B4500/5000 units:

1. Insert the SampleScan CD.
2. Double-click the file **DistributeSampleScan.exe** to start the *DistributeSampleScan* utility. The utility scans your system to identify your hardware unit and displays the serial number along with the default installation path.

3. Click **Copy Files**. The utility installs the correct calibration files for your hardware unit.
4. Verify that at least three files are copied.

5. Close the utility.

L-1 IDENTITY SOLUTIONS
    SECURE CREDENTIALING DIVISION

Note: If the utility does not detect a BorderGuard B4500/B5000 unit, a **Hardware Not Found** message appears.

To restart the initialization, click **OK** to close the message, connect the iA-thenticate unit, and click **Reset**.

To continue the installation without connecting hardware, click **OK** to close the message and then manually enter the serial number. You can also change the installation path. Use this procedure if you are installing the calibration file for multiple units over a network.

To install the custom calibration file on Color BorderGuard units:

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

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** and 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**.
8. Exit iA-Examiner.

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 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 *INTER-ACTIF, INTERATIVO,* or *INTERACTIEF*. Then click **OK**.
9. In the BGServer **Properties** window, click **OK**. Then close the Component Services window.

To configure Windows Vista and Windows 7—Dutch, French, or Portuguese:

1. Select **Start** and type *DCOMCNFG* into the edit box. 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 *INTER-ACTIF, 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 in Appendix B to correct the problem.

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

L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION

Testing the Smart Card Reader (B4500/B5000)

If you have a smart-card reader on a Color 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 172.

To test the smart card reader using 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, follow the instructions for fixing the problem in *Repairing the OmniKey Registration Settings* on page 172.

Enabling Automatic Logon and Application Start

For Windows Vista and Windows 7 systems, the iA-Administrator application must run with elevated privileges in order to enable automatic logon and to configure the applications to automatically start.

To configure the application to run elevated for a single instance

1. Click the **Start** button.
2. Select **All Programs** and select the **iA-thenticate** group.
3. Right click the application and select **Run as administrator**.

To configure the application to always run elevated

1. Click the **Start** button.
2. Select **All Programs** and select the **iA-thenticate** group.
3. Right-click **iA-Administrator** and click **Properties**.
4. Select the **Compatibility** tab.
5. Click the **Change settings for all users** button.
6. Under **Privilege Level**, select **Run this program as an administrator**,
7. Click **OK** twice to leave the configuration screens.

Note: If the **Run this program as an administrator** option is unavailable, it means that the application is blocked from always running elevated, the application does not require administrative credentials to run, the application is part of the current version of Windows Vista, or you are not logged into the computer as an administrator.

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

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:

Note: For Windows Vista and Windows 7 systems, a local user group for iA-thenticate Administrators must be created as described below as the PC's existing local Administrator group cannot be used.

L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION

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

Assigning File and Folder Permissions

Assigning file and folder permissions insures 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, Users** (if listed) and **Authenticated 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

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

2. Set permissions for your system, as follows:

For Windows XP

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**)

For Windows Vista and Windows 7

Before you can see the folders in the steps below you must first enable the viewing of system/hidden files.

- Open Windows Explorer. Select **Organize>Folder** and **Search Options**.

- From the **View** tab select **Show hidden files**, **folders**, or **drives**.

- Select **Apply to Folders** at the top of the window and then **Apply** at the bottom of the window to exit.

Follow these steps to assign the needed permissions to **C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup:**

a. Right-click folder **C:\ProgramData** 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:

> **Microsoft** (inside **Program Data**)
> **Windows** (inside **Microsoft**)
> **Start Menu** (inside **Windows**)
> **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 the following 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 also 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, *Installing an Optional Reader or Scanner*.

Hardware Startup and Shutdown

Follow these shutdown and startup procedures to avoid problems with communication between the PC and the camera.

To shut down the system:

1. Shut down the PC. If it has a mechanical power switch, turn it off.
2. Turn off the power switch on the BorderGuard unit.

To restart the system:

1. If you have just shut down the system, wait 30 seconds before restarting.
2. Turn on the power switch on the BorderGuard unit.
3. Start the PC.

To turn a Color BorderGuard unit off and on again, without rebooting the PC, eject both smart card readers before turning off the Color BorderGuard unit. Double-click the **Safely Remove Hardware** icon in the Windows task bar at the bottom of the screen, select the smart card readers from the list of devices and click **Stop.**

Chapter 3. Setting up An ID-Guard/J1000 Unit

This chapter explains how to set up your iA-thenticate system if you have an ID-Guard/J1000 unit, which processes standard wallet-size cards such as driver's licenses and IDs. ID-Guard/J1000 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. Refer to the *iA-thenticate 5.5 Release Notes* for additional information.

Note: 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.

L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION

PC System Requirements

You install the iA-thenticate software on a Windows PC, and you connect the ID-Guard/J1000 unit to the PC through a USB cable. Your PC must meet the following 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 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

**L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION**

Installing Software

Note:	Do not connect the ID-Guard/J1000 hardware yet.

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
iA-thenticate CD: *iA-thenticate…* *iA-thenticate… * **DirectX ** *directx_9c_oct05sdk_r edist.exe*	Follow the on-screen instructions

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, **iA-thenticate….**, for example.
Note:	If you are upgrading, the screens you see may differ slightly from the ones listed. Just follow the on-screen instructions.

L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION

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
iA-thenticate CD: *iA-thenticate… * *iA-thenticate… * **Regula_SDK-4.10** *setup.exe*	Follow the on-screen instructions in the Installshield Wizard.

Installing the iA-thenticate Security Software

Installer	Screen	Instructions
iA-thenticate CD: *iA-thenticate… * *iA-thenticate… * *1_iA-thenticate * *Setup.exe*	Intro	Click **Next**.
	License	Click **Yes** to agree.
	Setup Type	Select ID-Guard/J1000.
	Data Drive	If 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	Screens	Instructions
iA-thenticate CD: *iA-thenticate… \ iA-thenticate… \ 2_iA-Examiner \ Setup.exe*	Intro	Click **Next**.
	Data Drive	If 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 the optional DL-Alert™ software, either the Intelli-Check or Positive Access® version, install it now.

Installer	Screen	Instructions
iA-thenticate CD: *iA-thenticate… \ DL-Alert-IC… \ DL-AlertIntelli-Check.exe* **or** *iA-thenticate… \ DL-Alert-PA… \ DL-Alert-PositiveAccess.exe*	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, D-License, or Global-ID, install it now. Follow the instructions included with the optional software.

Restarting

After you finish installing software, restart your PC.

L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION

Connecting Hardware and Installing Drivers

Note: Connect the ID-Guard/J1000 hardware only after you have installed the software as described in the previous section.

Connecting Hardware

Your ID-Guard/J1000 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 Appendix B for problem-solving instructions.

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.

To connect the ID-Guard/J1000 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/J1000 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 in Appendix B.

Note: 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.

To install each device driver (repeat as needed):

For Windows XP:

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:

Note: If you connect to a different ID-Guard/J1000 hardware unit, you must re-calibrate.

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**.
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=0x000000000**, 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 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 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 following 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 (*C:\BorderGuard\Images* for example)

     – 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, *Installing an Optional Reader or Scanner.*

Chapter 4. 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.

L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION

Installing the E-Seek or Intelli-Check Reader
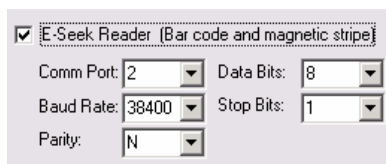
L-1 recommends and supplies the E-Seek or Intelli-Check combination bar code and magstripe reader for your BorderGuard unit. It is available in serial and USB models. The reader is preconfigured to work with your iA-thenticate system. However, if it should lose its settings, you can restore them as explained in Appendix B.

Serial Model
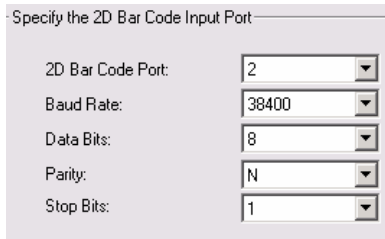
Follow these instructions if your reader has a serial connection.

To install the E-Seek or 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 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:
   a. Start iA-DataPort by double-clicking its icon on the desktop or by selecting **Start>Programs>iA-thenticate>iA-DataPort**.
   b. Choose **Settings>Comm Ports Settings**.
   c. For 2D Bar Code Port, select the port you chose in step 1.
   d. Click **OK**.
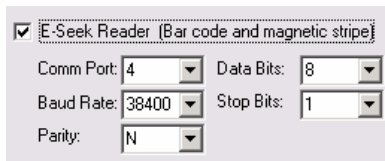
This completes the installation of the serial reader.

USB Model

Follow these instructions if your reader has a USB connection.

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

1. If you are using iA-Examiner, configure it to use the reader:
   a. 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.)
   b. Start iA-Examiner by double-clicking its icon on the desktop or by selecting **Start>Programs>iA-thenticate>iA-Examiner**.
   c. In iA-Examiner, click **Mgmt Funcs** and then **System Config**.
   d. On System Configuration Page 1, under **Peripherals**, select **E-Seek Reader**.
   e. Click **Apply** and then **Done**.
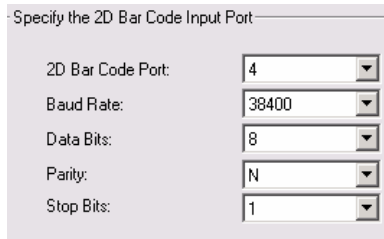
2. If you are using iA-DataPort, configure it to use the reader:
   a. If you have already followed step 1 to configure iA-Examiner, find the reader's port number by going back to System Configuration Page 1 and noting the Comm Port Number assigned to the E-Seek reader. Then skip to step e.
   b. Otherwise, with the system running, open the **Device Manager**. (Right-click **My Computer**, choose **Manage**, and click **Device Manager**.)
   c. 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.
   d. 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).
   e. Start **iA-DataPort** by double-clicking its icon on the desktop or by selecting **Start>Programs>iA-thenticate>iA-DataPort**.
   f. Choose **Settings>Comm Ports Settings**.
   g. For 2D Bar Code Port, select the number you found in step c. Click **OK**.

L-1 IDENTITY SOLUTIONS
    SECURE CREDENTIALING DIVISION

Specify the 2D Bar Code Input Port

2D Bar Code Port:	4
Baud Rate:	38400
Data Bits:	8
Parity:	N
Stop Bits:	1

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.

L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION

Installing a Flatbed Scanner

The iA-thenticate system is designed to work with any TWAIN-compliant USB flatbed scanner. L-1 has tested and qualified two models: Canon CanoScan LiDE 500F and Epson Perfection 3490 Photo.

To install the flatbed scanner:

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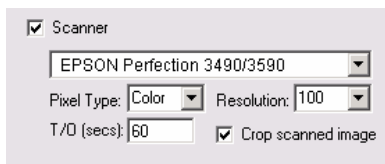
Note: Be careful not to select the iA-thenticate camera, listed as **OVT SuperCam**.

Note: If your scanner does not appear in the list, make sure it is properly installed. Test it using the software provided by the manufacturer.

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

---

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.

Note: If you see an error message or unexpected behavior when using the scanner, refer to the problem-solving section in Appendix B.

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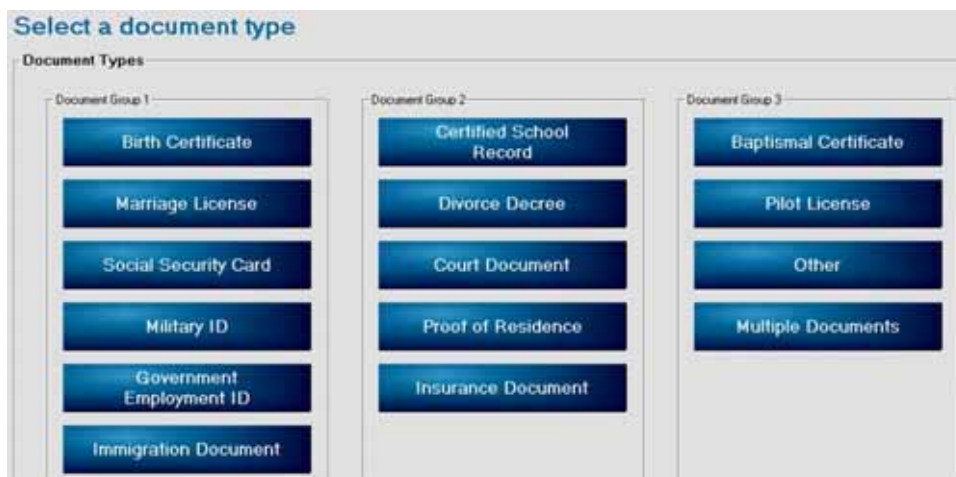
You can change the name above each group of buttons, the number of buttons in each group, and the document type that appears on each button.

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.

L-1 IDENTITY SOLUTIONS
    SECURE CREDENTIALING DIVISION

Chapter 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.

L-1 IDENTITY SOLUTIONS
    SECURE CREDENTIALING DIVISION

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:

Note: iA-Administrator has to be run with elevated privileges on Vista and Windows 7 systems.

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 appears:

L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION

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

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.

Note: Access to the management screens is restricted when you use the recommended security setup described on page 22 for BorderGuard units or 38 for ID-Guard/J1000 units.
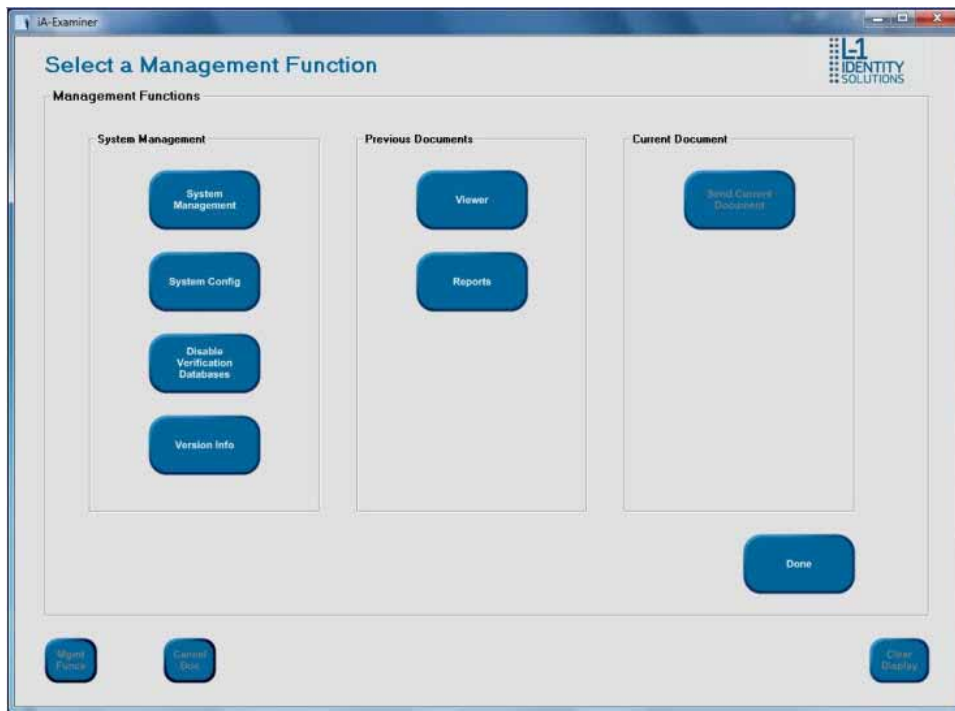
The System Management screen mostly lets you manage saved data:
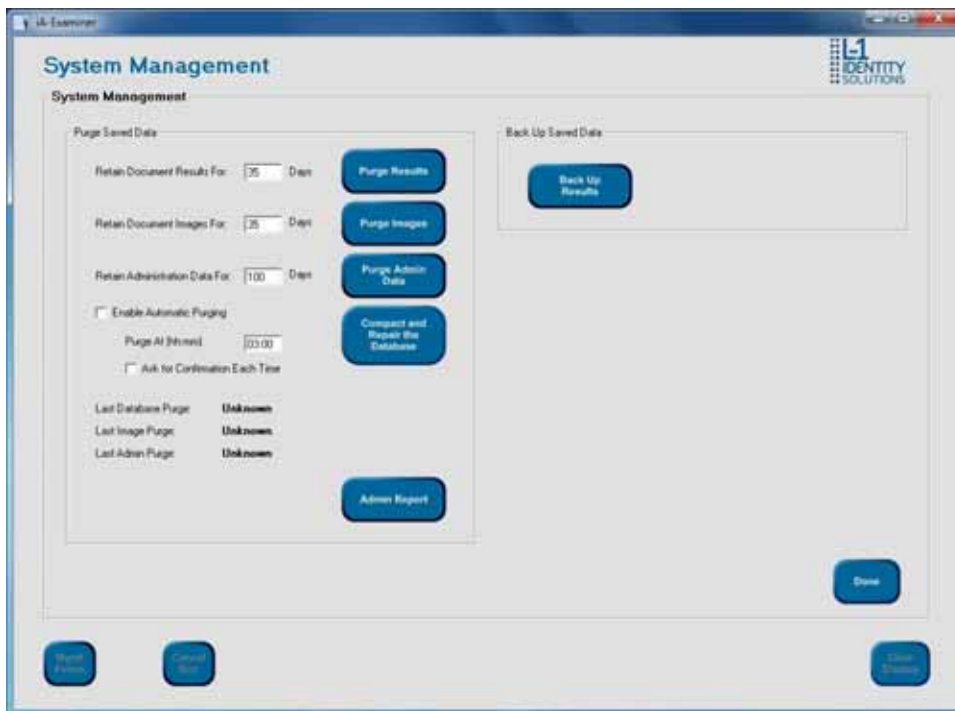
The System Configuration screen lets you set a variety of options (on multiple pages) for peripheral configurations, driver's license and ID processing, printing, data saving, document testing, screen display, and other features:

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

L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION

Chapter 6. Configuring iA-thenticate

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)

Refer to the *iA-thenticate Quick Configuration Guide* as it may contain all the information you need to get your system up and running.

Refer to Chapter 5 *Using the Administration Tools*, for an introduction to iA-Administrator.

Refer to Chapter 7, *Configuring iA-Examiner,* for additional information on 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 the **Version Details** button runs the iA-thenticate Version Utility, which shows detailed information about the installed software:
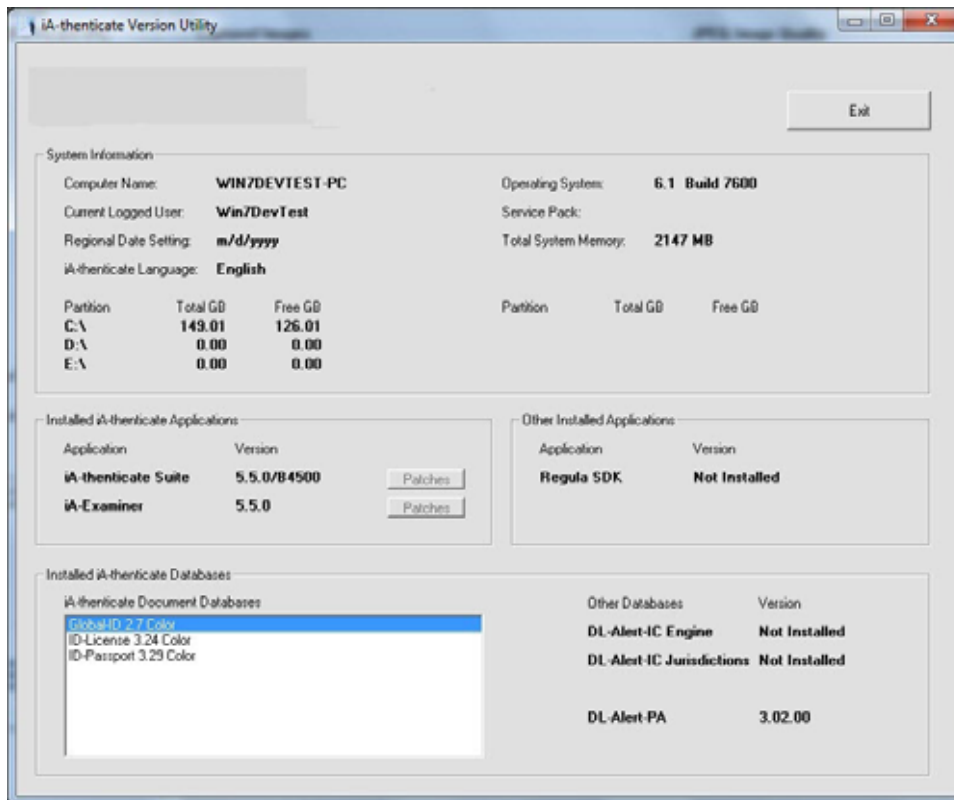
Note: You can also run the iA-thenticate Version Utility by choosing **Start> Programs> iA-thenticate> iA-VersionUtility**

L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION

Setting Options for Basic Operations

To set options for basic operation, run iA-Administrator (**Start>Programs>iA-thenticate>iA-Administrator**) and click the **Configuration** tab.

Note: iA-Administrator has to be run with elevated privileges on Vista and Windows 7 systems.
Refer to the *Enable Automatic Logon and Application Start* section on page 31 for details.

In each section of the screen, set the options according to the following descriptions and recommendations.
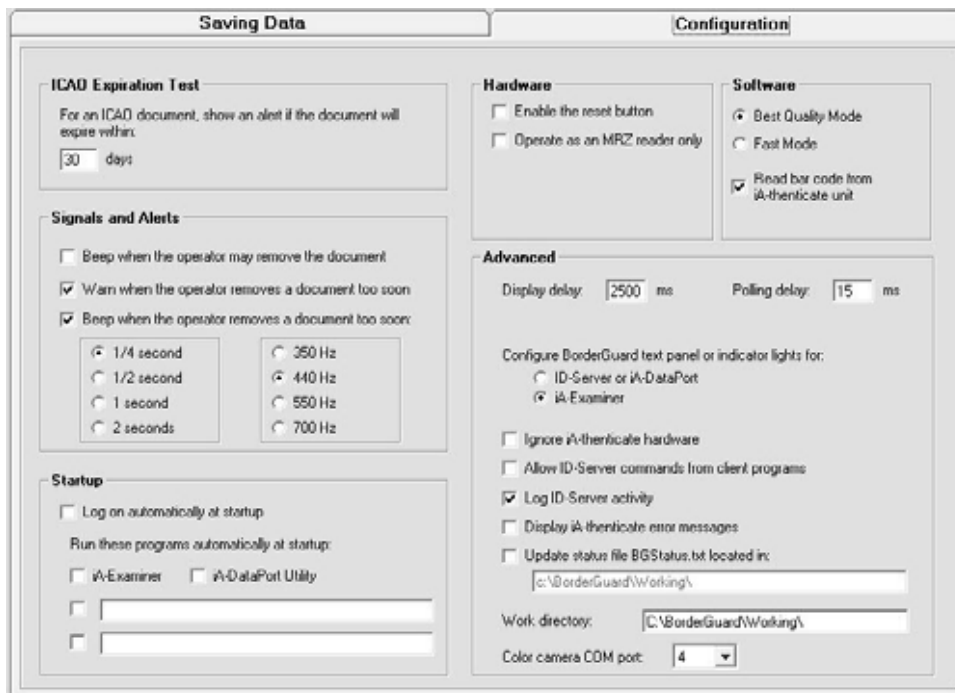
Note: Some options appear only for certain hardware configurations, as noted in the descriptions.

ICAO Expiration Test

Option	Description	Recommendations
For an ICAO document, show an alert if the document will expire within: (a configurable number of) days (30 days shown)	Displays an alert for an ICAO document if it expires within this number of days. (When iA-Examiner tests the expiration date of a non-ICAO 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	Recommendation
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/J1000 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.	We do not recommend using this option in a production environment, because it bypasses normal Windows logon security.
Run these programs automatically at startup	After Windows starts, runs the selected programs automatically. To add a program, type its full path name. Selected programs are added to the Startup program group for All Users: *C:\Documents and Settings\All Users\ Start Menu\Programs\Startup* (for XP) *C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup* (for Vista and Windows 7)	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, as follows:

Note: It has been reported that this process does not work for certain systems. You should

verify autologon processing in your environment before proceeding.

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 only 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 *iA-Administrator's Guide* 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 Color BorderGuard B4500/B5000.

Option	Description	Recommendations
Best Quality Mode	Default setting; provides highest image quality.	Keep this setting for most document authentication environments. You must use this setting to read bar codes on the B4500/B5000.
Fast Mode	Increases processing speed but reduces image quality.	Use only if processing speed is more important than image quality. Do *not* use if reading bar codes on the B4500/5000. Reboot after switching modes.
Read bar code from iA-thenticate unit	Enables bar code reading when capturing documents on the B4500/B5000 (as opposed to using an external reader).	Disable if you do not want to read bar codes on the B4500/B5000 (for example, if processing passports only and no licenses). Disable if running in Fast Mode.

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 to 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/J1000 unit.)	Do not change unless needed for troubleshooting. 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/J1000* in Appendix B for troubleshooting instructions.
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.	Configure for which program controls the messages on the built-in text panel, or the indicator lights, on a BorderGuard unit.	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. 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.
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.

Option	Description	Recommendations
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 iaT_Log.txt. 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.
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/B5000 unit.	For further information refer to the *Installing Software* section of Chapter 2. A value of INV (invalid) means the port number is greater than 255. Contact 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.

The following 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 fingerprint image from a smart card.
On monochrome BorderGuard systems you can save grayscale images. On Color BorderGuard, Color BorderGuard B4500/B5000, and ID-Guard/J1000 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/B5000, and ID-Guard/J1000 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.

Using iA-Administrator…	Using iA-Examiner…
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 iA-Examiner User's Guide).

Note: ID-Guard/J1000 does not capture UV, seal, or tamper images.

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 *87*.

Captured Images

Option	Description	Recommendations
Save	Saves color or grayscale images, or both, to the location specified. 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: USA_P_12345678_VC.jpg 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).	Set these options to suit your needs. Be sure the location you use for saving images has enough disk space. If the disk fills up, the system will no longer operate properly. To reduce file sizes, use the JPEG format rather than BMP. See JPEG Image Quality, below, for more information.
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	Saves images and logs based on whether they pass or fail these tests only: checksum, expiration, B900 ink, patterns (visible, IR, UV, seal), brightness (IR, UV), and tamper. **For all documents**: Saves all images and logs regardless of test results. **Only for documents that fail a test:** Saves images and logs only for documents that fail one of these tests. **Only for documents that pass all tests:** Saves images and logs only for documents that pass all these tests.	Select the option that meets your needs. **Note**: You must also select the kinds of images you want to save (above): Color images, Grayscale images, or both.

Jpeg Image Quality

Option	Description	Recommendations	
Use this quality setting for all JPEG images	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.)	Use **Medium** for decent quality and relatively small files. For better quality, use **High** or **Best**. Do not use **Low** if you want to be able to analyze images later for authenticity.	

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

L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION

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	Writes the selected images and logs from the system's memory to the work directory (see the *Advanced* table, page 73). The images and logs from each document overwrite those from the previous document.	Do not select any of these except for a specific purpose, such as collecting the images and logs using a custom program. **Note**: If you want to use the Doc Log option described in the *Configuring iA-Examiner Document Log Options* section (page 125), you must select Document and MRZ Logs here.
Image format	The graphics file format for saving the temporary images, JPEG or BMP. JPEG files are compressed according to the JPEG Image Quality setting (above).	Select the format you want to use.

Chapter 7. Configuring iA-Examiner

Note: Before you read this chapter, see the *iA-thenticate Quick Configuration Guide* as 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 6. *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


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. Refer to the *Sending Data Through a Serial Port* section on page 134.

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 or Intelli-Check combination bar code and magstripe reader (either serial or USB).	Select this if you use one of the readers; otherwise deselect it. (See note)
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 or Intelli-Check reader.	Select this if you have an ID-GUARD unit or if you are using an add-on magstripe reader other than E-Seek or Intelli-Check. 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/J1000'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 (page139). Otherwise iA-Examiner will not receive magstripe data.
Comm. Port	The COM port used for communicating with the reader	For an ID-Guard/J1000 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.

Option	Description	Recommendations
Bar Code Reader	Enables an optional 2D bar code reader other than an E-Seek or Intelli-Check reader.	Select this if you are using a bar code reader other than E-Seek or Intelli-Check; otherwise deselect it. (See the note at the beginning of this table).
Comm Port	The COM port used for communicating with the reader	Select the reader's port number
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.
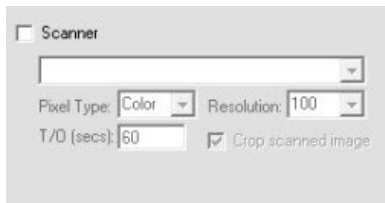
Option	Description	Recommendations
Scanner Pixel Type Resolution T/O Crop scanned image	Enables an optional flatbed scanner and sets options for its use.	For instructions about installing and configuring a flatbed scanner, see Chapter 4, *Installing an Optional Reader or Scanner*

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 as shown in the following figure:
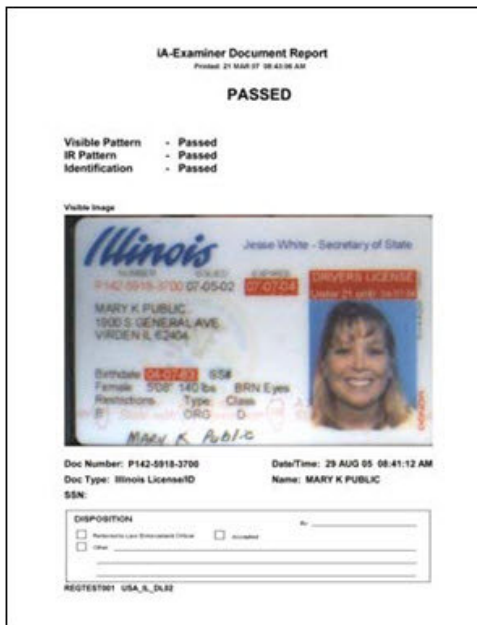
Before this feature will work, you must set up your default printer in the usual way using the Printers control panel.

L-1 IDENTITY SOLUTIONS
    SECURE CREDENTIALING DIVISION

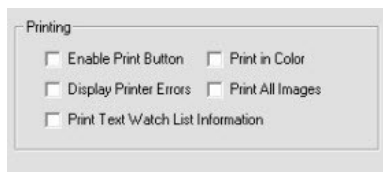| Option	Description	Recommendations
Enable Print Button	Activates the Print button on the iA-Examiner screen.	Select this if you want operators to be able to print document results.
Print in Color	Sends color information when printing, including green and red text to mark passed and failed tests. On 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* (page 75) 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, *BGExaminer.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 BGExaminer.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 in the *Using a Networked Database* section on page 91.
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 in the *Backing-up Saved Data* section on page 132.
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 the *Using a Networked Database* section on page 91	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	Saves the images you specify for each document you process, in either Windows Bitmap (.bmp) or JPEG (.jpg) format. Gives each file a unique name based on the document type and number (if known), date and time processed, and image type. For example, a Rhode Island, USA driver's license #987654321, processed 2007-March-18 at 11:55:33, IR image: DL_USA_RI_987654321_070318115533_I.jpg 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.	Select this if you want to save some or all of the images for later reference. Color images take a lot of disk storage space. To avoid problems, your drive should have plenty of free space. To reduce file sizes (but also reduce image quality), use JPEG compression (below). To avoid saving unnecessary images, select only the types you want using Save the following images, below.
Images Directory Path	The full pathname of the directory for saving images, on a local drive or mapped network drive. If you specify the same directory for several networked units, you can then view reports that include all the units, as explained on page 91.	If you set data-saving options in iA-Administrator as well as here (not recommended) be sure to specify different directory paths to avoid file naming conflicts. Also see the next item, *Save in Subdirectory with Unit's Name*.
Save in Subdirectory with Unit's Name	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.	Select this if you want to keep the saved images from different units separate. **Important:** Do not select this if you want to be able to review prior documents as described in the iA-Examiner User's Guide. That feature does not work with images saved in separate directories.
Minimum Free Disk Space	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.	If you are saving images on your C: drive, a setting of at least 100 MB is recommended in order to avoid problems with the operating system.
Disk Space Partition	The drive partition to monitor for free disk space.	Set this to the same drive you use for the Images Directory Path.

Option	Description	Recommendations
Convert Images to JPEG	Saves the images in JPEG (.jpg) format rather than Windows Bitmap (.bmp) using the Image Quality setting you specify (below).	Select this if you want to reduce file sizes at the cost of some image quality.
Image Quality	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.)	Use **Medium** for decent quality and relatively small files. For better quality, use **High** or **Best**. Do not use **Low** if you want to be able to analyze images later for authenticity.

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

Option	Description	Recommendations
Save the following images	The types of images and logs to save. In addition to **Visible** (white light),**IR**, **UV**, **Seal**, and **Tamper** images, you can also save: **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 **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 7 (page 125) in the *Configuring iA-Examiner Document Log Options* section).	Select each image type you want to save. To save the document log: 1. Select **Doc Log** here. 2. Also select **Document and MRZ Logs** using iA-Administrator, as described in the *Temporary Images and Logs* section on page 80. Also, see the next item.
If Doc Passes, Save Visible Only	For documents that pass all tests, save only the visible image. For documents that fail any test, save all the selected images. This does not affect saving the document results log.	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.

Note: ID-Guard/J1000 does not capture UV, seal, or tamper images.

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 *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** (see the table in the *Configuring Data Saving* section on page 87). During this time it displays a progress bar and prevents any operator actions.

The database connection has been lost. Attempting to reconnect.

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 older 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*.

L-1 IDENTITY SOLUTIONS
    SECURE CREDENTIALING DIVISION

    e.   Specify the **Maximum Database Retry Count** as explained in the table in the *Configuring Data Saving* section on page 87.

    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 *G:\Data*, for example.

– In the **Disk Space Partition** field, fill in just the drive letter associated with the network folder, *G:*, for example.

– To keep images from different systems in different subfolders, Select **Save in Subdirectory** with the 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 *iA-Examiner User's Guide* has more information about each test.

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

Option	Description	Recommendations
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.
MRZ Edits Affect All Data and Tests	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. **Note:** If the operator changes MRZ characters to remedy a smart card BAC failure (see the table in the *Smart Card Options* section on page 116), those changes are never permanent and do not affect other tests.	Select this if you want the operator's edits to become permanent, overriding the captured data.
Display Checksum Correct. Screen on Alert	Automatically displays the MRZ editing screen when there is a problem with the checksum	Select this if you want the editing screen displayed automatically. Otherwise the operator must click Edit MRZ to display it. 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.
TextWatch Test Enable TextWatch	Activates the TextWatch test, which checks a watch list for matching names and document numbers.	Select this if you have the optional TextWatch feature and want to use it.
TextWatch Database Path	The full pathname of the TextWatch database. The default is *C:\BorderGuard\Bin\iAT.sys*.	Use the default pathname, or a different one if you have customized it.
Match by Name	Searches the watch list for a matching name.	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 either one matches.
Match by Document Number	Searches the watch list for a matching document number.	

Option	Description	Recommendations
Document Watch Test		
Enable Document Watch	Activates the Document Watch test, which checks to see if the document number falls within specified ranges.	Select this if you have the optional TextWatch feature and want to use its Document Watch feature.
Document Watch Database Path	The full pathname of the Document Watch database. The default is *C:\BorderGuard\Bin\iAT.sys*.	Use the default path name, or a different one if you have customized it.

Pattern Test

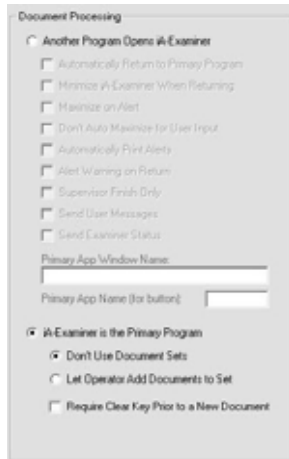| Option	Description	Recommendations
Pattern Test		
Display Pattern Confidence	Reserved for future use.	
Legal Age Test		
Enable Legal Age Test	Activates the Legal Age test, which checks to make sure the document owner is at least a certain age.	Select this if you want to test for legal age.
Minimum 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 (see the table in the *Configuring Document Processing* section on page 98) and want to use this cross-check test.
Smart Card Cross-Check 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.

Option	Description	Recommendations
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 always tries to identify the document automatically. This option only affects whether Identification is listed as a separate test.	Keep this selected unless you do not want to display Identification as a separate test.
Reverse Side Test Enable Reverse Side Test	Activates the reverse side test. This test is performed on the second side of a two-sided document and verifies that the document captured is the proper back for the front that was captured.	Select this if you want to check the reverse side of documents.
Custom Tests 1-3 (see figure, below)	Controls additional tests designed for custom applications. For further information, contact Customer Support and request the Tech Note titled *Information for iA-thenticate Integrators*.	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:
 ○ Pass ○ Fail ○ Indeterm ◉ Ignore

☐ Enable Custom Test 2
 Result File Path:

 Executable File Path:

 Treat Result Timeout as:
 ○ Pass ○ Fail ○ Indeterm ◉ Ignore

☐ Enable Custom Test 3
 Result File Path:

 Executable File Path:

 Treat Result Timeout as:
 ○ Pass ○ Fail ○ Indeterm ◉ Ignore
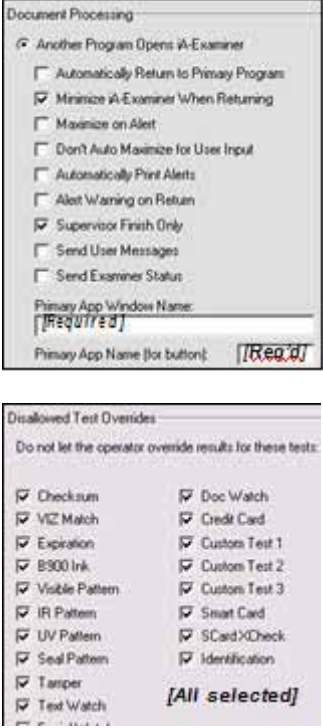
L-1 IDENTITY SOLUTIONS
    SECURE CREDENTIALING DIVISION

Configuring Document Processing

System Configuration Page 3: Document Processing

Option	Description	Recommendations
Another Program Opens iA-Examiner	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.	Select the appropriate option for your work environment, either this one or **iA-Examiner as the Primary Program** (below). If you select this, you must deselect **Display Doc Info Screen on Alert** (see the table in the *Configuring Display Options* section on page111. **Note**: 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 Customer Support for assistance.

Option	Description	Recommendations
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	Causes the iA-Examiner screen to come to the front automatically whenever a document requires review. **Note**: iA-Examiner normally maximizes if it requires some action by the operator (but see the next item). It then minimizes automatically if Minimize iA-Examiner When Returning is selected (below).	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 automatically 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.
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.

Option	Description	Recommendations
Supervisor Finish Only 	A special-purpose option that works only with the settings shown at left.	Select this only in consultation with 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.)

Option	Description	Recommendations
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).
Don't Use Document Sets Let Operator Add Documents to Set	Store each document's results independently of other documents. Let the operator group 2–4 documents together in a set so their results are linked and can be compared.	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: • 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**.
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.

L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION

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.

For more information about using iA-Examiner with verification databases, please contact L-1.

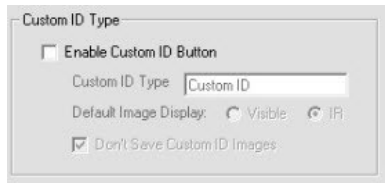# Configuring Data Entry

System Configuration Page 4: Data Entry

Option	Description	Recommendations
Field #1 thru Field #9	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. If you mark a field as **Required**, then the system automatically displays the data entry screen whenever it can't find the required information.	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**. To include a custom field, select **User Field #1, #2, or #3** and see *Configuring Static Database Information* (page 106). If you select **Required** for one of these fields, the system will always display the data entry screen. **Note**: To also let the operator display the data entry screen manually, select **Enable Edit Button** (page 111).
Comment	Specifies whether the data entry screen includes a Comment field where the operator can type additional information.	Select **Yes** or **No** to include the Comment field or not. To include the Comment field and always display the data entry screen, select both **Yes** and **Required**.

Option	Description	Recommendations
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 iA-Examiner User's Guide.)	Select or deselect to enable or disable this function.

Configuring a Custom ID Type

System Configuration Page 4: Custom ID Type

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 87). However, it does not prevent saving images if you have enabled image saving using iA-Administrator (page 77).	Select this if you don't want the images of this custom document type saved for any reason, such as privacy or security. Note the important condition in the description.

Configuring Static Database Information

System Configuration Page 4: Static Database Information

Option	Description	Recommendations
Customer Name Site Name	Names stored in the document results database (page 87), intended for use in custom reports that you might generate from the database.	Fill in any suitable names.
User Field #1 User Field #2 User Field #3	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* on page 103. To fit more characters into the name, avoid using lots of capital letters.

Configuring Debugging

System Configuration Page 4: Debugging

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

Configuring the Processing of Unidentified Documents

System Configuration Page 4: Processing Unidentified Documents

Note: For information about creating and using a custom document database, contact 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?
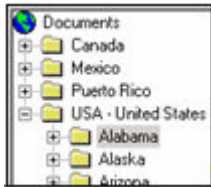
If you have an optional document database such as ID-License or Global-ID, iA-Examiner can display selection screens that let the operator manually identify the document, or iA-Examiner can process every unidentified document in a predetermined way.

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).

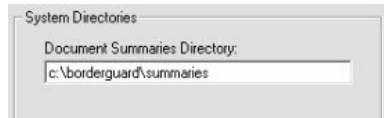| Option	Description	Recommendations
Go to the document selection screen	For an unidentified document, display the document selection screen, for selecting the document type using an Explorer-like list of countries, issuers, and types.	If you have an optional document database such as ID-License or Global-ID, 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: You must make a choice for **Country**. You may make a choice for **Jurisdiction** or leave it blank.	Consider this option if: • You have an optional document database such as ID-License or Global-ID, 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.
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 or Global-ID. 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

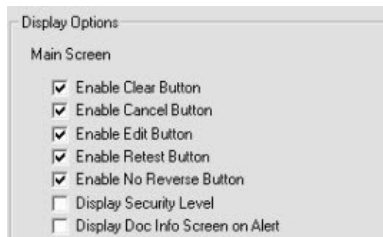| Option	Description	Recommendations
Document Summaries Directory	The directory used for: • The results of searches you perform using the Document Viewer (iA-Examiner User's Guide, chapter 3) • Temporary files for the data transmission feature (see the Configuring Data Transmission Options section on page 124).	Use the default pathname: *C:\BorderGuard\Summaries*

L-1 IDENTITY SOLUTIONS
    SECURE CREDENTIALING DIVISION

Configuring Display Options

System Configuration Page 5: Display Options

Main Screen

Option	Description	Recommendations
Enable Clear Button	Adds a **Clear** button that lets the operator clear out the data shown on the main Examiner screen. This may be done for privacy reasons, for example.	Select this if you want the operator to be able to clear the data from the Examiner screen when processing of a document is complete.
Enable Cancel Button	Adds a **Cancel Document** button that lets the operator cancel evaluation of a document after capturing it.

This button does not delete any saved test results or captured images, but it does exclude the canceled document from reports. | Select this if you want the operator to be able to cancel evaluation of documents. |
| Enable Edit Button | Adds an **Edit** button that lets the operator display the data entry screen for manually entering information.

This option applies only if you have selected fields to appear on the data entry screen as described under *Configuring Data Entry* (page 103). | 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. |

Option	Description	Recommendations
Enable Retest Button	Adds a **Retest** button that lets the operator retest the document (usually without having to recapture it) as a different type 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 or Global-ID.	Select this if you have ID-License, Global-ID, or a custom document database and want to enable this feature. See *Configuring Processing of Unidentified Documents* (page 108) for more information.
Enable No Reverse Button	Adds a **No Reverse** button that becomes available once the operator captures the first side of a two sided document and is being prompted to capture the second side. The button allows the operator to skip processing of the 2nd side.	Select this if you want the operator to be able to complete processing of a two sided document by capturing the first side only.
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 ID-Passport Database Reference (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 98), you must deselect this. Otherwise, select the behavior you prefer.

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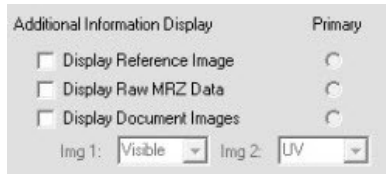
When the iA-Examiner screen is not displaying the results of a selected test, it displays Identification Data—general document information including ID type, last and first names, document number, and so on. The operator sees this information,

- When a document passes all tests

- When a document causes an alert and the **Display Doc Info Screen on Alert** option (above) is selected, or,

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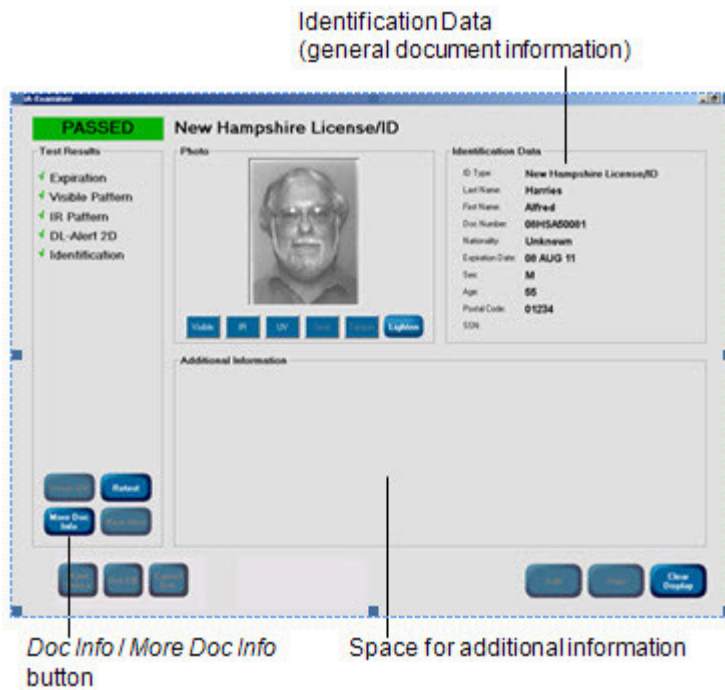
You can use the following options to let the operator see several kinds of additional information. The **Doc Info** button then becomes **More Doc Info**, and clicking it displays each kind of information in turn.

L-1 IDENTITY SOLUTIONS
   SECURE CREDENTIALING DIVISION

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

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. Under **Primary**, select the kind of information you want to appear first (even if you've selected only one kind of information).
Display Raw MRZ Data	Shows the captured MRZ and the system's reading of it (ICAO documents only)	
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

Selectable Display Fields

Display Field #1: Age
Display Field #2: PostalCode
Display Field #3:

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.

Option	Description	Recommendations
Display Field #1 Display Field #2 Display Field #3	The last three fields to display under **Identification Data** (shown when the operator clicks **Doc Info**). **UserField1**, **UserField2**, and **UserField3** correspond to the matching entries for **Static Database Information** (page 106).	Choose the information you want displayed.

Document Viewer

Document Viewer

☐ 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.
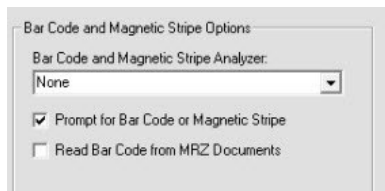
Smart Card Options

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.

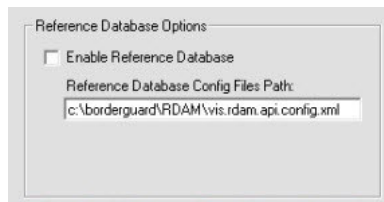| Option	Description	Recommendations
Placement Timeout Action	The test result to record if the system does not detect a smart card before the Placement Timeout expires. **Fail Smart Card Test:** Records the smart card test as failed **Ignore Smart Card:** Records no result for the smart card test, just as if the document had no smart card	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.

L-1 IDENTITY SOLUTIONS
   SECURE CREDENTIALING DIVISION

Configuring Bar Code and Mag Stripe Options

System Configuration Page 5: Bar Code and Magnetic Stripe Options

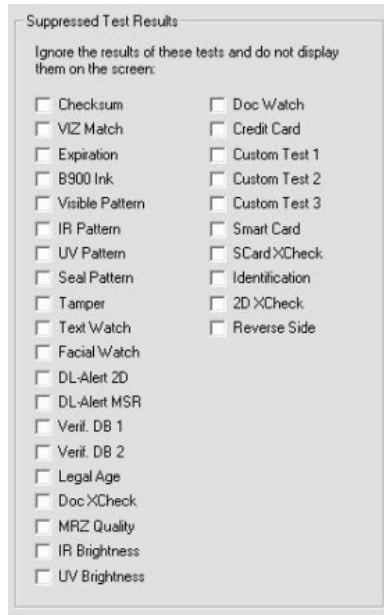| Option	Description	Recommendations
Bar Code and Magnetic Stripe Analyzer	Enables validation of the magstripe or bar code on a license or ID card using optional software.	This selection is made automatically during DL-Alert installation—**ID Check** for the Intelli-Check version or **ID Code** for the Positive Access version. You should not change it unless you are asked to do so by Customer Support.
Prompt for Bar Code or Magnetic Stripe	If the system is configured to process magstripes and bar codes, and the bar code or magstripe has not been scanned when a document is finished processing, the system asks the operator to either do the scan or click the **Skip Scan** button. The operator should process the bar code or magstripe using either the B4500/5000 or an external reader, or click **Skip Scan**.	Select this if you want to give the operator a second chance to scan a document's bar code or magstripe.
Read Bar Code from MRZ documents	Examiner will read the bar code from MRZ documents such as passports.	Select this if you want to read bar codes from passports or other documents with MRZ.

L-1 IDENTITY SOLUTIONS
  SECURE CREDENTIALING DIVISION

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.	

L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION

Configuring Test Suppression

System Configuration Page 6: Suppressed Test Results

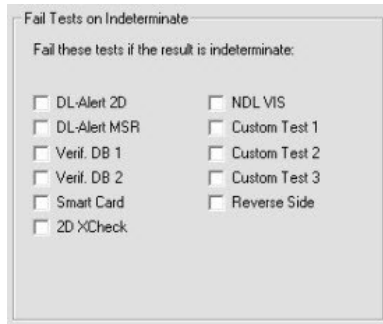| Option	Description	Recommendations
Checksum VIZ Match Expiration …	Ignores the selected test when evaluating a document for problems and does not display its results for the operator. (Your list of tests may differ slightly from the one shown.) However, if the test is included in the document profile,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

Configuring Test Override Options

System Configuration Page 6: Disallowed Test Overrides

Option	Description	Recommendations
Checksum VIZ Match Expiration …	Prevents the operator from overriding the results of the selected type of test. (Your list of tests may differ slightly from the one shown.)	Select any tests the operator is not allowed to override because of security or operational policies. If you select **Supervisor Finish Only** (see the *System Configuration Page 3 Document Processing* table starting on page98), you must select all 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 93.

L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION

Configuring Alerts for Indeterminate Tests

System Configuration Page 6: Fail Tests on Indeterminate

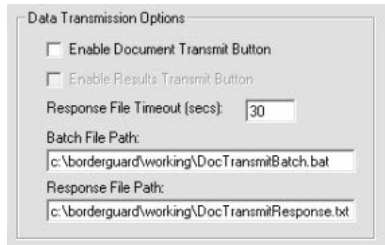| Option	Description	Recommendations
Fail Tests If Results Are Indeterminate	Some tests can show an indeterminate result if their results are incomplete or inconclusive. These include **Verification Database**, **DL Alert 2D**, **DL Parser 2D**, **DL Alert MSR**, **DL Parser MSR**, and **custom tests**.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

L-1 IDENTITY SOLUTIONS
    SECURE CREDENTIALING DIVISION

Configuring Credit Card Options

System Configuration Page 6: Credit Card Options

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 125).	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 87). **Important**: Selecting this does not prevent saving credit card images if you have enabled image saving using iA-Administrator (page 77).	Select this if you don't want iA-Examiner to save credit card images because of privacy or security concerns. You may also need to disable image saving using iA-Administrator (page 77).

L-1 IDENTITY SOLUTIONS
    SECURE CREDENTIALING DIVISION

Configuring Data Transmission Options

System Configuration Page 7: Data Transmission Options

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 Customer Support	
Batch File Path		
Response File Path		

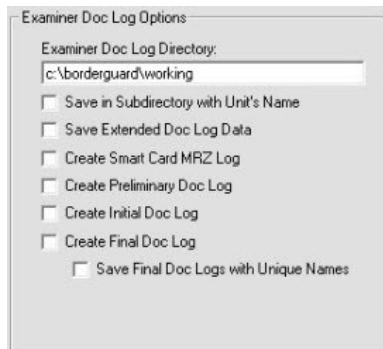**L-1 IDENTITY SOLUTIONS**
SECURE CREDENTIALING DIVISION

Configuring iA-Examiner Document Log Options

System Configuration Page 7: iA-Examiner Doc Log Options

As explained under *Configuring Data Saving* (page 87), 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.
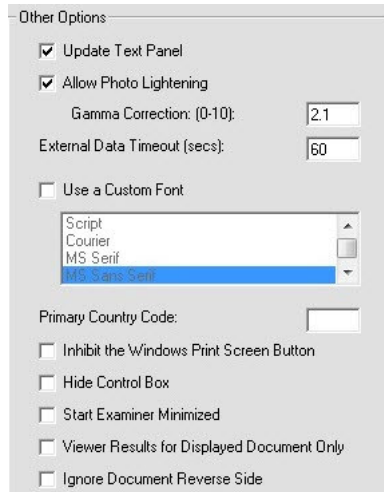

Option	Description	Recommendations
Examiner Doc Log Directory	The directory for creating iA-Examiner document logs.	Use *C:\BorderGuard\Working* unless you have a reason to use a different directory. You might want to use a network directory accessible to a number of iA-thenticate units.
Save in Subdirectory 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.
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.

Option	Description	Recommendations
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.

L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION

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 as displayed on the screen.	Select this if you notice that ID photos tend to be too dark on the screen and when saved as images.
Gamma Correction	The amount of lightening to apply to the displayed ID photo when the operator uses the **Lighten** button, from 1 to 10: 1: No lightening at all 10: Extreme lightening (Values between 0 and 1 actually darken the image.)	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.

Option	Description	Recommendations
Use a Custom Font	Displays screen text using the font you select from the list.	Leave this deselected unless you have a special reason to use it. Changing the font can make the screen hard to read or even unusable. To restore the default font, deselect this option. Restart iA-Examiner after making any font change.
Primary Country Code	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: 	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.
Hide Control Box	Hides the shutdown/maximize/minimize control box for the iA-Examiner window.	Select this if you want to prohibit the operator from performing those functions with this control box and plan to control those functions in some other way.
Start Examiner Minimized	Causes iA-Examiner to stay minimized in the task bar upon starting up.	Select this if you are using a program other than Examiner as the primary application and want iA-Examiner to start minimized.
Viewer Results for Displayed Document only	When selecting **Create Results** on the iA-Examiner Viewer Screen, only the document showing will be included in the summary file instead of all of the documents that met the search criteria.	Select this if you want the iA-Examiner summaries to only include the doc currently being viewed.
Ignore Document Reverse Side	If this option is selected, the operator will not be prompted to capture the 2nd side of a document that has test features on both sides. The subsequent capture will not be treated as the 2nd side of the document and the Reverse Side Test will not be run if enabled.	Select this if you only want to process one side of documents that have test features on both sides.

Chapter 8. Managing iA-Examiner

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

Note: Before you read this chapter, refer to the *iA-thenticate Quick Configuration Guide,* as it

may contain all the information you need to get your system up and running

---

To access the System Management Screen:

1. On the iA-Examiner screen, click **Mgmt Funcs**, followed by **System Management**.

Purging Saved Data

Option	Description	Recommendations
Retain Document Results For	Number of day's 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.

Option	Description	Recommendations
Purge Admin Data	Purges the administration report now, retaining recent actions as specified.	Use this for manual purging, or set up automatic purging (below).
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. The system does not back up files automatically, so be sure to do regular backups (page 132) if you need to keep files and data beyond the retention period you set.
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.

L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION

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 87. **Note**: Each backup copy overwrites the previous backup copy.	Periodically use this option to preserve a backup copy of the database in a safe location.

Chapter 9. Using iA-DataPort

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.

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

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 in the *Configuring General Settings* section on page 139.

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 *Configuring General Settings* section on page 139. 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.

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

L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION

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:

1. Install and configure appropriate third-party software for setting up a virtual serial port on your iA-thenticate PC.
2. Select the **Communications Port** option as explained *Configuring General Settings* section on page 139.

Using the Optional Keyboard Filter

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

If you want to transmit data from a magstripe reader *other than* the E-Seek or 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 139.

L-1 IDENTITY SOLUTIONS
    SECURE CREDENTIALING DIVISION

Windows XP

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 *C:\BorderGuard\Tools\MagStripeFilter\IAMSFilter.inf*
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.

L-1 IDENTITY SOLUTIONS
    SECURE CREDENTIALING DIVISION

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:

1. 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 147.

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 135.

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**.

L-1 IDENTITY SOLUTIONS
SECURE CREDENTIALING DIVISION

Viewing Captured Data

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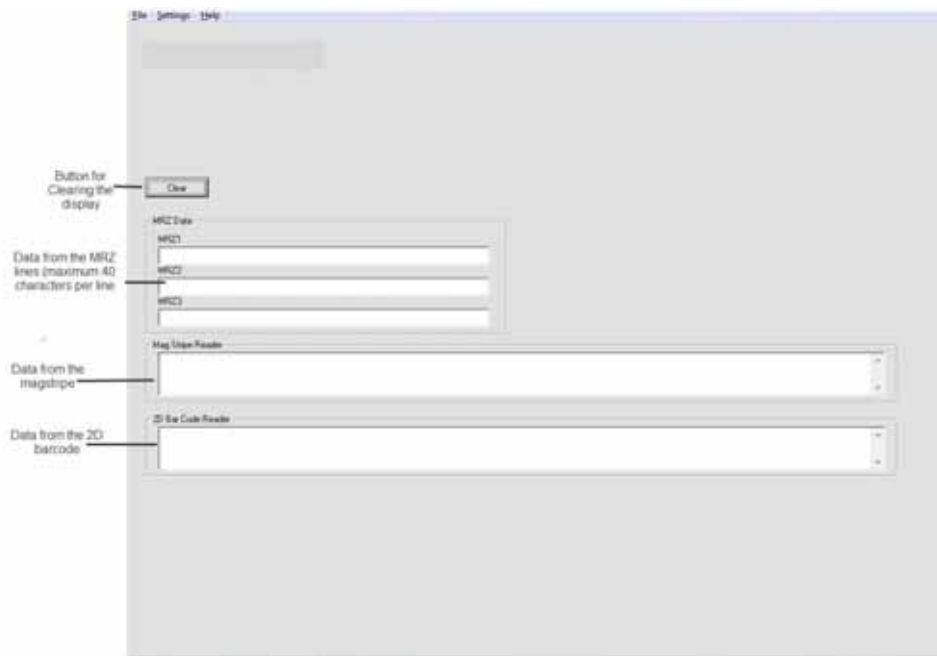
Configuring Settings

Using the Settings menu, you can configure:

- General Settings

- Communication Port Settings

- Data Format Settings

- MRZ Data Format Settings

- Data Transmit Settings

- Display Settings

- Startup 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**
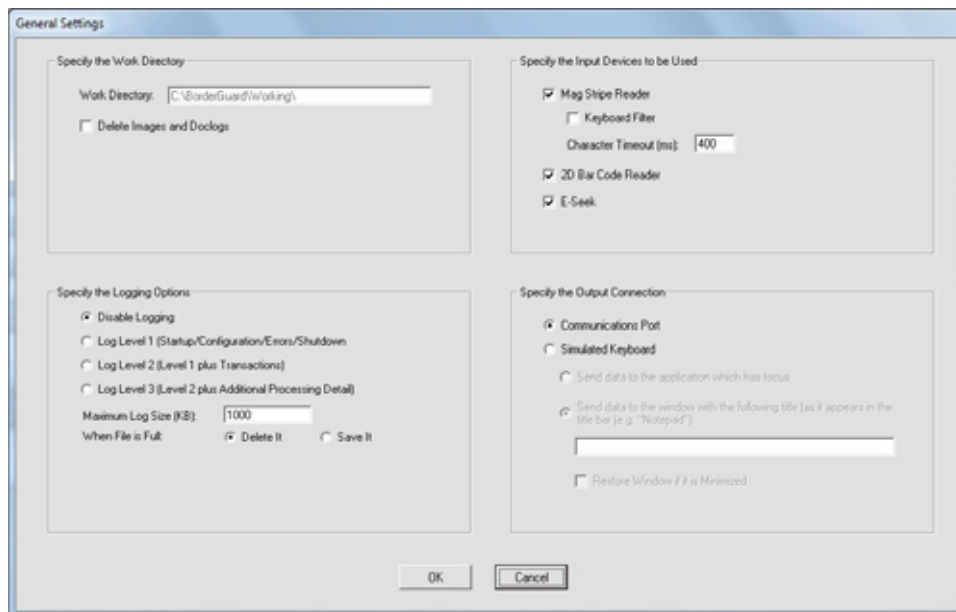
2. If you want iA-DataPort to delete images and document logs from the work directory after processing each document, select **Delete Images and Doclogs**. (You set the location of the work directory using iA-Administrator, as explained in the *Advanced* table on page 73).

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**.

4. Select each input device you are using:

Note: For magstripe readers, 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 82).

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

   – Select **Mag Stripe Reader**.

   – To use the optional keyboard filter to route magstripe data to iA-DataPort, select **Keyboard Filter**. See page 135 for installation instructions and more information about the filter.

Note: 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 above.)
   • If you are using the E-Seek or 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 134, 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 or Intelli-Check reader are 2, 38400, 8, N, 1.
4. Click **OK**.

Note: To restore factory set values, click **Restore Default Settings**.

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.

To configure data format settings:

1. Select **Settings**>**Data Format Settings**.

2. Under **MRZ Format Options**:
   a. 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.
   b. 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.
   c. Specify as many as three characters to send at the end of the entire block of MRZ data.
   d. 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 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:

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**.

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.

L-1 IDENTITY SOLUTIONS
  SECURE CREDENTIALING DIVISION

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.**
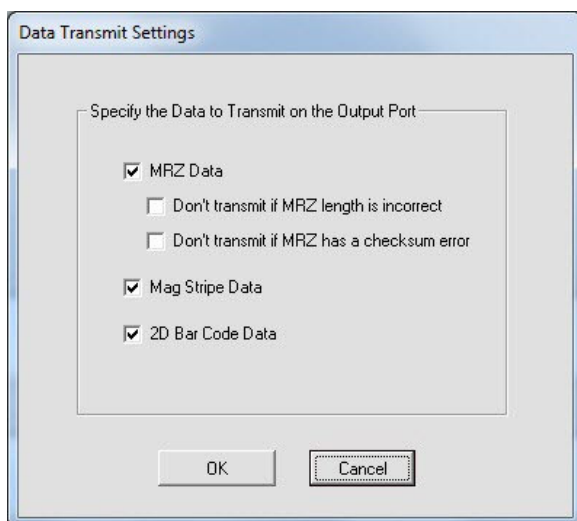
2. Select all the kinds of data you want the system to transmit to your application.
3. If you select **MRZ Data**, you can also select either or both of these options, to prevent transmission of faulty or questionable data:

   • 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**.
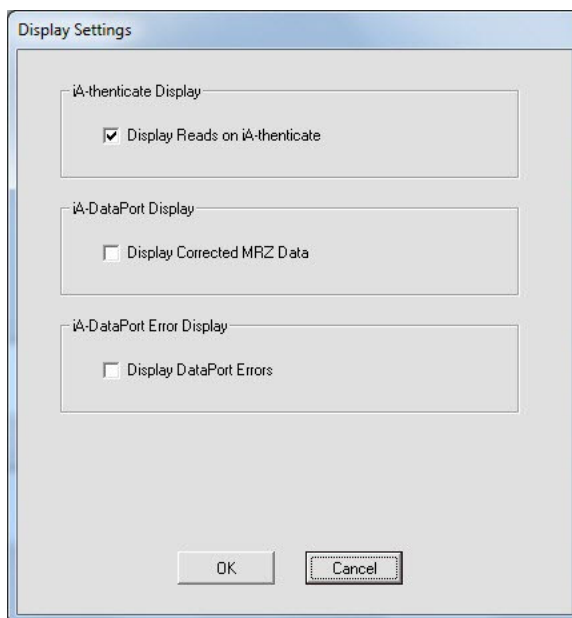
2. Under iA-thenticate Display:

- 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 140) 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 DataPort 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**.
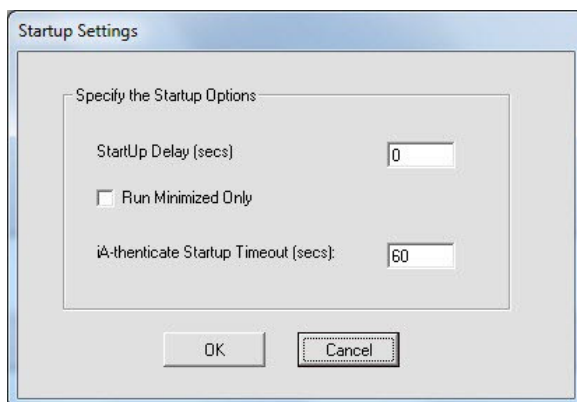
2. For **Startup Delay**, use the default value of **0** seconds. But if your unit is set up to run iA-DataPort automatically at startup, and you see error messages during startup, try increasing this value.
3. If you want the iA-DataPort utility to run minimized each time you start it, select **Run 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 137.
4. For **iA-thenticate Startup Timeout**, use the default value of **60** seconds.
5. Click **OK.**

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 *monochrome* camera.

Before You Begin

• Check the Release Notes for new information.

• If you are upgrading from a previous version, you may need to follow additional steps.

• 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.

• 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.

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 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

Note: 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 **Normal**. These are the default Windows settings. If you have changed these settings, follow these steps to restore the defaults:

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 not need to restart the system at this point unless Windows requires you to do so.

Installing the iA-thenticate Security Software

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.

Installer	Screen	Instructions
iA-thenticate CD: *iA-thenticate… * *iA-thenticate… * **1_iA-thenticate** \ *Setup.exe*	Intro	Click **Next**.
	License	Click **Yes** to agree.
	Setup Type	Select **BorderGuard - monochrome unit**.
	Data Drive	*If* 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
iA-thenticate CD: *iA-thenticate… * *iA-thenticate… * **2_iA-Examiner** \ *Setup.exe*	Intro	Click **Next**.
	Data Drive	If 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
iA-thenticate CD: *iA-thenticate… \ DL-Alert-IC… \ DL-AlertIntelli-Check.exe* **or** *iA-thenticate… \ DL-Alert-PA… \ DL-Alert-PositiveAccess.exe*	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

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 the following directory: *C:\BorderGuard\Config*
4. Right-click the copied *SampleScan.cfg* file and choose **Properties**. Deselect **Read-only** and click **OK.**

Note: Older BorderGuard units have a SampleScan diskette rather than a CD

Installing Other Optional Software

If you have other optional software such as ID-Passport, Global-ID, 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 151.

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:

BorderGuard power supply

BorderGuard PCI connector

BorderGuard cable

PC

BorderGuard

CAUTION

To avoid damaging the coaxial connectors, begin inserting the plug at a slight sideways angle. Then push slowly, gently, straight into the socket.
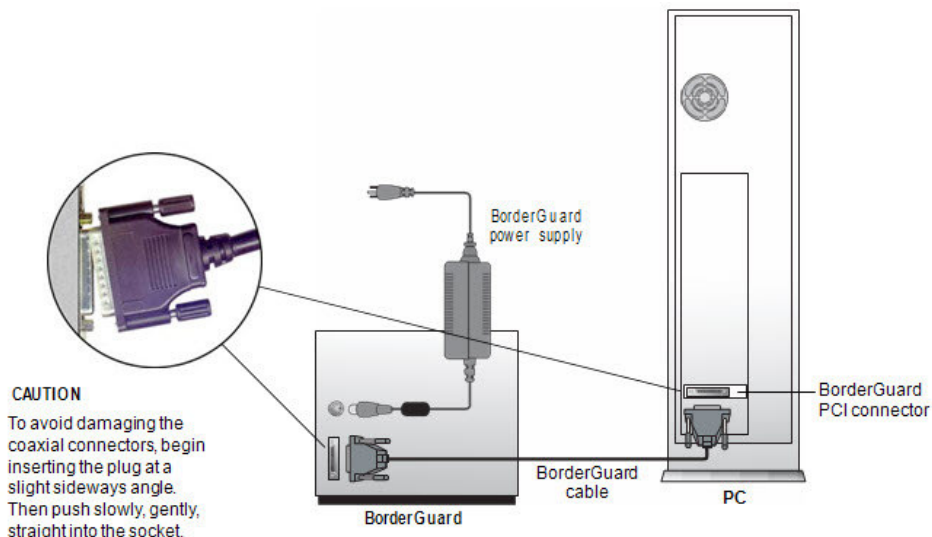
1. Plug one end of the BorderGuard cable into the connector on the PCI card you installed in your PC.
2. Plug the other end of this cable into the matching connector on the back of the BorderGuard unit.
3. Make sure the power switch on the BorderGuard unit is off.
4. Plug the cable from the BorderGuard 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 the 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 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 177.
5. Exit by clicking the **Close** button or selecting **File>Exit**.

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 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.

L-1 IDENTITY SOLUTIONS
    SECURE CREDENTIALING DIVISION

Appendix B. Solving Problems

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

support-ia@l1id.com

+1 978-932-2200

+1 800-555-8784 toll-free (North America

Color BorderGuard

The first step in troubleshooting any problem should be to completely shut down and turn off the system, including any attached PC. Wait 30 second and restart. In many cases, restarting will resolve the problem. If not, follow the troubleshooting procedures in this section.

Capture Timeout Errors

If you see a *Capture Timeout* error at startup, or if you start up successfully but see *Error01* and the VFD (two-line text panel) reads *Capture Timeout* when attempting to capture a document, follow these troubleshooting steps:

1. Verify that the **Power Scheme** setting on the host computer is set to **Always on.** From the Windows **Start** button, select **Control Panel > Power Options** and click the **Power Schemes** tab. In the Power schemes drop down list, the **Always on** option should be selected.
2. Verify that the computer meets minimum requirements.
3. Check for any unnecessary USB devices attached (even a memory stick or USB drive can contribute to bandwidth issues).
4. Contact Customer Support.

Drivers Do Not Install As Expected

Note: 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 L-1 can cause software malfunctions and system instability.

After you install software and then start Color BorderGuard for the first time, Windows should automatically install several drivers, as described on page 24.

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 or Intelli-Check USB reader do not install as expected.

To install each device driver (repeat as needed):

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**.

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*.

Clicking **Have Disk** and manually selecting the device driver will ensure that the correct driver is installed.

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 2-8, you should see the main iA-Examiner screen. If you see an error message about a COM port, use the following 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 or Intelli-Check 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 or Intelli-Check 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 t**hat matches the one you found in Device Manager.

5. Click **Apply** and exit iA-Administrator.

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

USB Device Errors

For Color BorderGuard or Color BorderGuard B4500/5000 systems, follow this shutdown and startup procedure to avoid problems with communication between the PC and the camera.

To shut down the system:

1. Shut down the PC. If it has a mechanical power switch, turn it off.
2. Turn off the power switch on the BorderGuard unit.

To restart the system:

1. If you have just shut down the system, wait 30 seconds before restarting.
2. Turn on the power switch on the BorderGuard unit.
3. Start the PC.

If you need to turn a Color BorderGuard unit off and on again without rebooting the PC, eject both smart card readers before turning off the unit.

To eject a smart card reader:

1. Double-click the **Safely Remove Hardware** icon in the Windows task bar at the bottom of the screen.
2. Select the smart card readers from the list of devices and click **Stop.**

Color BorderGuard B4500/B5000

The first step in troubleshooting any problem should be to completely shut down and turn off the system, including any attached PC. Wait 30 seconds and restart. In many cases, restarting will resolve the problem. If not, follow the troubleshooting procedures in this section.

Capture Timeout Errors

If you see a *Capture Timeout* error at startup, or if you start up successfully but get an *Error01* or see a red blinking light when attempting to capture a document, follow these troubleshooting steps:

1. Check that the PC's Power Scheme is set properly:

    For Windows XP

    For optimal performance, the Power Scheme for the host computer should be set to **Always on**. This setting applies to laptops and PCs running Windows XP.

    a. From the Windows **Start** button, select **Control Panel > Power Options**.
    b. Click the **Power Schemes tab**.
    c. In the **Power schemes** drop down list, select the **Always on** option.

    For Windows Vista

    a. From the Windows **Control Panel,** select **Power Options**.
    b. Select **Adjust Power Settings**.
    c. Select the **High Performance** power plan.
    d. Make sure that the **Put the Computer to Sleep** option is set to **Never**.

    For Windows 7

    a. From the Windows **Control Panel,** select **System and Security.**
    b. Select **Power Options**.
    c. Select the **Balanced** Power Plan and then click on **Change plan settings.** The **Edit plan settings** screen appears. Change both dropdown items (**Turn off Display** and **Put the computer to sleep**) to **Never**.
    d. Expand the **Sleep** option and select **Change Advanced power settings**. The **Advanced Power settings** screen appears.
    e. Set both the **Sleep after** and **Hibernate after** settings to **Never.**
    f. Click **OK** and **Save Changes** on both this screen and the **Edit plan settings** screen**.**

2. Verify that the computer meets minimum requirements.
3. Check for any unnecessary USB devices attached (even a memory stick or USB drive can contribute to bandwidth issues).
4. Contact Customer Support.

Drivers Do Not Install As Expected

After you install software and then start the B4500/5000 for the first time, Windows should install several drivers automatically, as described on page 24.

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 or Intelli-Check USB reader 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 L-1 can cause software malfunctions and system instability.

Note: Cicking **Have Disk** and manually selecting the device driver will ensure that the correct driver is installed

To install each device driver for Windows XP (repeat as needed):

Note: During driver installation, you may also be asked to locate the file ftser2k.sys. If so, browse to *C:\BorderGuard\Tools\ USB Serial*.

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**.

Windows XP 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
USB Converter or OMNIKEY 55x3	C:\Borderguard\Tools\ACG\ACG2.inf

To install each device driver for Windows Vista and Windows 7 (repeat as needed):

1. Right-click on any instances of **Unknown Device** or any instance of a device with an *exclamation mark* or *question mark* on it.
2. Click **Update Driver Software**.
3. Select **Browse my computer for driver software**.
4. Select **Let me pick from a list of device drivers on my computer**.
5. Click **Have Disk** (If there is no **Have Disk** button, click **Show all devices** and **Next).**
6. Browse to the file location (see the following table), select the file and click **OK** and **Next**.

Vista and Windows 7 Driver Files and Locations

For this hardware device:	Browse to this file:
Color Camera 01 or B5000 Camera	Try *C:\Borderguard\Tools\BorderGuard Camera\x86\b5000_device.inf*. If you get a message that the driver is not right for your hardware, try: *C:\Borderguard\Tools\BorderGuard Camera\x86\b5000_driver.inf*
USB Fast Serial Adapter	*C:\Borderguard\Tools\USB Serial\FTDIBUS.INF*
USB Serial Port	*C:\Borderguard\Tools\USB Serial\FTDIPORT.INF*
USB Converter or OMNIKEY 55x3 Reader (USB)	*C:\Borderguard\Tools\ACG\ACG2.inf*

Note: After the process is run for every instance of **Unknown Device** and any device with an exclamation mark or question mark on it, reboot the PC and look for any new instances of **Unknown Device** or any device with an exclamation mark or question mark on it. Repeat the entire process until no more of these instances exist after a reboot.

Note: If you need to manually load the camera drivers, see the *Windows Vista and Windows 7* paragraph of the *Camera Driver Installation Problems* section below for additional steps.

# Camera Driver Installation Problems (Windows XP)

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 for Windows XP:

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 in the table above.

Uninstalling and Reinstalling the Camera Drivers (Windows XP)

If you have followed the steps above and still experience problems, you may need 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 in Chapter 2, you should see the main iA-Examiner screen. If you see an error message about a COM port, 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 or Intelli-Check 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 or Intelli-Check 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 Customer Support.

USB Device Errors

Follow these shutdown and startup procedures to avoid problems with communication between the PC and the camera.

To shut down a BorderGuard 4500/5000 system:

1. Shut down the PC. If it has a mechanical power switch, turn it off.
2. Turn off the power switch on the BorderGuard unit.

To restart a BorderGuard 4500/5000 system:

1. If you have just shut down the system, wait 30 seconds before restarting.
2. Turn on the power switch on the BorderGuard unit.
3. Start the PC.

Document on the Platform Error

If you get the startup error message *There is a document on the platform. Please remove it and restart the application* but there is definitely no document on the glass, this may be a hardware issue. Please contact Customer Support to return the unit for repair.

For emergency purposes, the following temporary step can be taken to use the unit, but this is not a supported operating mode.

1. Open c:\BorderGuard\Config\BGScan.cfg.
2. In the [Document Detection] section, edit the *DetectionModule* parameter.

   Change from: **DetectionModule=6**

   To: **DetectionModule=4**
3. Save the file.

Smart Card Reader Errors

Smart Card Driver Installation Problems (Windows XP)

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, right-click the icon, select **Properties**, and select the **Drivers tab**. Click **Update Driver** and use the **Have Disk** path to locate the driver file specified in the table on page 168.

Smart Card Driver Installation Problems (Vista and Windows 7)

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 Reader (USB)** *or* **USB Converter** in either the **SmartCard Readers** *or* **Other Devices** folder.
3. If an exclamation point appears next to the icon, right-click the icon, select **Properties**, and select the **Drivers tab**. Click **Update Driver Software** and use the **Have Disk** path to locate the driver file specified in the table on page 168.

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 172.

To test the smart card reader using 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 Smart Card Reader (B4500/B5000) on page 30).

- The OmniKey applet test on the previous page shows that **Enable Multi-Antenna Mode** is not checked.

To repair the registration settings:

1. In the folder *C:\BorderGuard\Tools\ACG*, double-click the file **settings_L1ID.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.
5. Retest the smart card reader.

ID Guard/J1000

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.	Each ID-Guard/J1000 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. You may be also able to increase laptop power changing the default battery setting for higher performance. Additionally, you may be able to resolve the problem by adjusting the capture timing for the ID-Guard/J1000 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.
ID-Guard/J1000 system fails to read bar codes after installation.	Previous version of Regula software was not properly uninstalled before installing the ID-Guard/J1000 software.	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*. Reinstall *Regula Document Reader SDK 4.10*.

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.

You can also use this procedure as a troubleshooting tool if you encounter any problems with camera operation.

To update drivers using the **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):
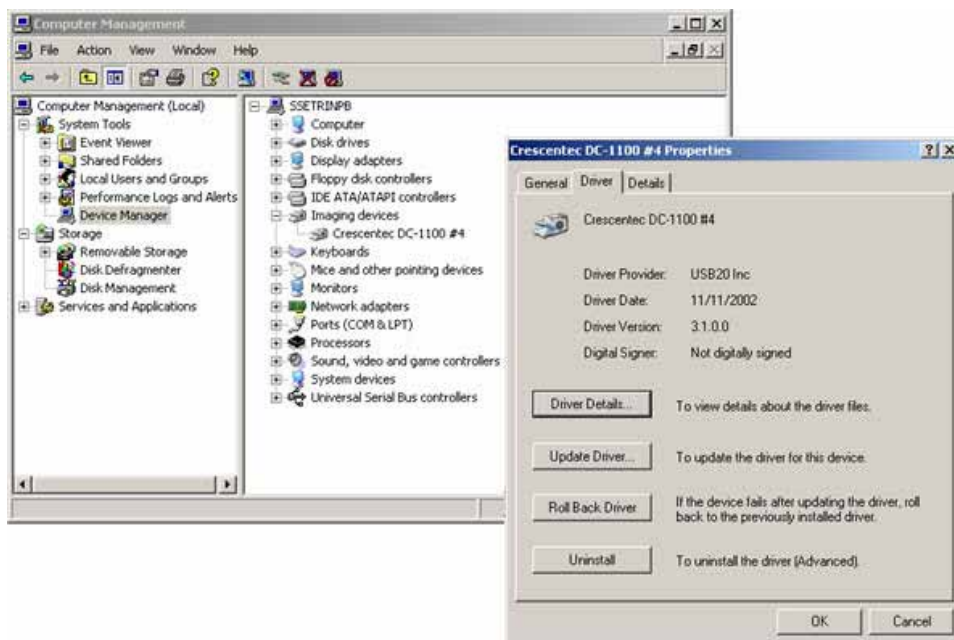
3. If the wrong driver version is installed or if an exclamation point or question mark appears next to the icon in **Device Manager**, click **Update Driver**, and install the device driver using the following instructions:
   a. Make sure you can see the small window that shows the name of the hardware device; this is sometimes hidden behind the wizard.
   b. If the first wizard screen asks about connecting to **Windows Update** to search for software, elect **No, not this time** and click **Next**.
   c. Select **Install from a list or specific location** (**Advanced**) and click **Next**.
   d. Select **Don't search. I will choose the driver to install**. Click **Next**.
   e. 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**.)

f. 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**.

g. 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 in Appendix A, you should see the main iA-Examiner screen. If the driver for the PCI card was not properly installed for some reason, you will 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.

If you encounter either message follow the steps below to reinstall the driver:

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 Customer Support.

E-Seek or 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 146).

If you have an E-Seek or 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 include:

- 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 or 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 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.

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-thenticate unit (as much as a minute or more), or the captured image is black.	The scanner may have disrupted communication with the iA-thenticate unit.	Disconnect the USB cable from the scanner, wait a few seconds, and reconnect it.

L-1 IDENTITY SOLUTIONS
    SECURE CREDENTIALING DIVISION

Appendix 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

Index