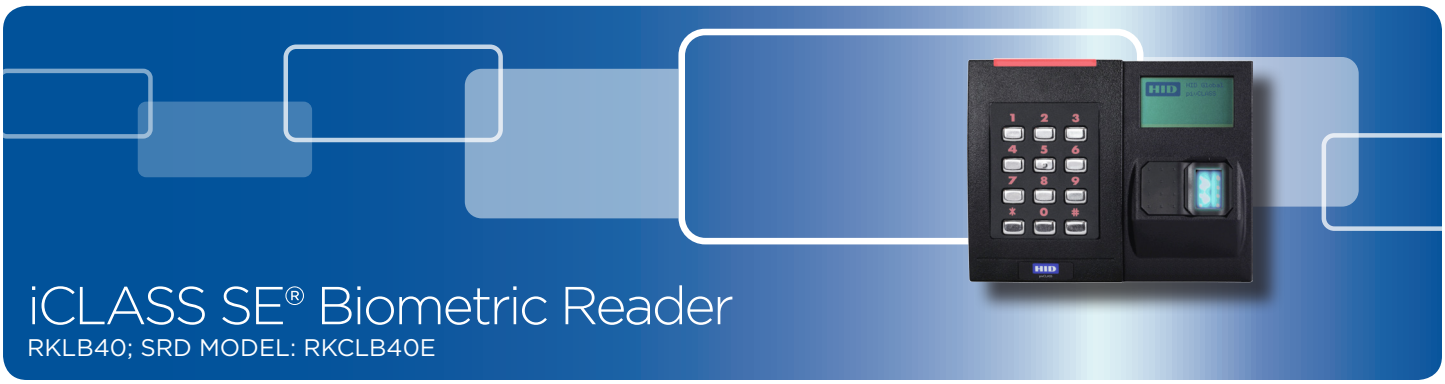
USER GUIDE



iCLASS SE® Biometric Reader

RKLB40; SRD MODEL: RKCLB40E

PLT-02550, Rev A.1

www.hidglobal.com/PLT-03342

- Lisez le code QR ou suivez le lien pour consulter la version française de ce document.
- Escanee el código QR o visite el vínculo para consultar la versión en Español de este documento.
- Scannen Sie den QR-Code oder öffnen Sie den Link für die deutsche Version dieses Dokuments.
- Faça a leitura do código QR ou acesse o link da versão em português deste documento.
- Scansiona il codice QR o visita il link della versione Italiana di questo documento.
- Отсканируйте QR-код или пройдите по ссылке, чтобы получить версию этого документа на русском языке.
- 扫描 QR 码或访问此 文档的中文版本的链接。
- この文書の日本語版を表示するには、QR コードをスキャンするか、リンクを クリックします。
- QR 코드를 스캔하거나 링크를 방문하면 이 문서의 한국어 버전을 볼 수 있습니다.

1. Introduction

The iCLASS SE® Biometric Reader is a multi-functional reader and enroller that can be used in a variety of locations. It is highly configurable and allows the user to access a wide range of different operational parameters which are outlined in this document.

The Reader has three Operational Modes. The Operational Mode chosen is configured in the **Initial Setup** and will reflect how the Reader will be used and where it will be located. The Mode can be changed via the **Administration** menu (see *Section 2.1.4: Operational Mode*).

- **Reader/Enroller Mode:** Both Reader and Enroller Modes are available.
- **Enroller Only Mode:** Enrolls user and administration cards. It does not process credentials to allow access control. The Reader will typically be located in an office with secure access.
- **Reader Only Mode:** Processes credentials. The Reader will typically be located at a building entrance or door.

Notes:

- All enrollment actions are performed locally to the Reader.
- After **Initial Setup**, additional functionality for the chosen Operational Mode can be accessed via the **Administration** menu (see *Section 2.1.4: Operational Mode*).
- The triangle on the display menu indicates the current default value.

2. Initial Setup

When the Reader is first switched on, the **Initial Setup** menu is displayed which will take you through the following stages:

1. Select Language, Credential Type and Operational Mode (all card types).
2. Choose Site Key (Seos® cards only).
3. Verify Admin (all card types).

Note: Two configuration cards are included with the Reader to complete Initial Setup reset if Initial Setup needs to be modified. To complete Initial Setup reset:

1. Power cycle the Reader.
2. Within the first 15 seconds of power on, present and hold “SE BIO Initial Setup Reset Card 1” to the face of the Reader keypad until the Reader stops beeping and the LED is solid red or flashing blue/red.
3. Present and hold “SE BIO Initial Setup Reset Card 2” to the face of the Reader keypad until the Reader stops beeping and the LED is solid red or flashing blue/red.

2.1 Initial Setup – Functional Selections

2.1.1 Select Language

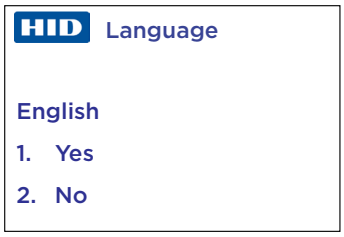
HID Language
1. ▸ English
2. Francais
3. Español
4. < more >

1. Power on the Reader.
2. Use the keypad to select the language. **Example:** For English, select **1**.

Note: To see additional languages select **4. < more >**.

• English	• Italiano (Italian)
• Français (French)	• Русский (Russian)
• Español (Spanish)	• 中文 (Chinese)
• Deutsch (German	• 日本語 (Japanese)
• Português (Portuguese)	• 한국어 (Korean)

3. The selected language will appear on the screen.
   - Choose **1. Yes** to confirm or **2. No** to cancel and go back to the language selection dialog.



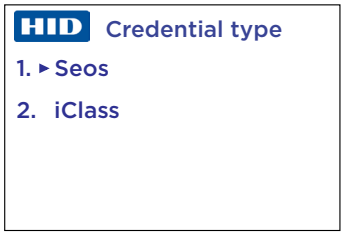
Note: The menu will wrap to the beginning until a language is chosen.

4. From this point on, all screens will display in the selected language.

Note: To change the language after the Initial Setup, go to the **Administration** menu and select **Configuration** (see *Section 4.2.3: Configuration menu functions*).

2.1.2 Select Credential Type

Once the language is chosen, Initial Setup advances to the **Credential Type** menu. This configures the card types that the Reader will enroll.



1. To select the Credential Type:
   - Select **1. Seos**. This Mode enrolls Seos cards but will *not* enroll iCLASS or iCLASS SR cards.
   - Select **2. iCLASS**. This Mode enrolls *only* iCLASS or iCLASS SR cards.
2. Once you make your choice a confirmation dialog appears. Choose **1. Yes** to confirm or **2. No** to cancel and return to the **Credential Type** menu.

2.1.3 PIN Requirement

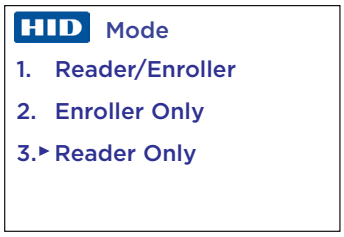
Note: When in reader mode, PIN data entered on the keypad will also be sent to the door controller for verification unless local PIN verify keypad part number option has been ordered.

This configures whether a PIN enrolled to the card by the reader must be verified locally by the reader before the card data is sent to the door controller. If **Required** is chosen, a PIN number will be asked for when Users and Admins are enrolled, and also when cards are presented to a Reader to gain access. (For more information on PINs, see *Second page of Configuration options* in *Section 4.2.3: Configuration menu functions*).

- Select **1. Required** or **2. Not Required**.
- When you make your choice a confirmation dialog appears. Choose **1. Yes** to confirm or **2. No** to cancel.

2.1.4 Operational Mode

Once the Credential Type and PIN Requirement choices are made, Initial Setup advances to the **Operational Mode** menu.



1. To select the Operational Mode:
   - Select **1** for **Reader/Enroller:** The **Present Card** menu will be the main interface thereafter. This mode allows the reader to act as either a reader or enroller.
   - Select **2** for **Enroller Only:** The **Administration** menu will be the main interface thereafter.
   - Select **3** for **Reader Only:** The **Present Card** menu will be the main interface thereafter.
2. Confirm the choice:
   - Select **1. Yes** to confirm.
   - Select **2. No** to cancel and return to the **Operational Mode** menu.
   - If you select **1. Yes**, a confirmation dialog appears. Choose **1. Yes** to confirm or **2. No** to cancel.

This ends the Initial Setup – Functional Selections stage. The next stage differs, depending on the Credential Type chosen.

Note: If the Reader is switched off at this point in the Initial Setup process it will return to this stage when it is switched back on.

2.2 Initial Setup – Site Key

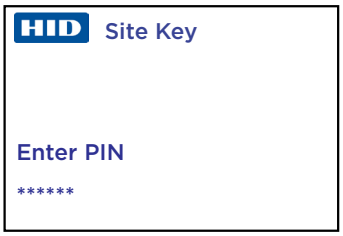
Note: This stage applies only when the credential type is set to Seos.

The Site Key setup follows the Operational Mode setup.

The Site Key encrypts the biometric credentials onto the card so they are unique to each site. The Site Key must be between 6 and 11 characters and must be entered identically onto all readers on that particular site.

To choose the Site Key:

1. Enter the Site Key and press **#**.
2. The reader will display **Verify**. Enter the Site Key number again and press **#**.

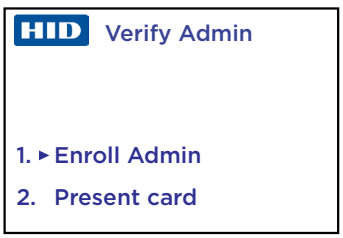


Note: If the Site Key number is not entered within the timeout period the Reader will display **Enrollment Failed** and return to the **Site Key** menu.

3. Once the Site Key value has been successfully entered and verified, the Reader displays **Success** and advances to the next stage.

2.3 Initial Setup – Verify Admin

The final stage of Initial Setup registers the **Admin card**. The Reader presents two choices: **Enroll Admin** or **Present Card** in order to verify an existing Admin card.



Note: The following Enrollment dialog is the same for Initial Setup, Add Admin, and Add User. The main title at the top of the display changes to indicate the current function.

2.3.1 Enrollment Dialog

Example: "Enroll Admin" choice in the "Verify Admin" step

The Reader displays:

1. Enroll Admin

2. Present Card

Note: The user should chose **2. Present Card** if they already have an Admin card. When an Admin card is successfully presented to the Reader (it will ask for a finger to be presented and a PIN, if required) this choice will succeed. If there is a failure to present an Admin card, then an error message is shown and the **Verify Admin** menu is re-presented.

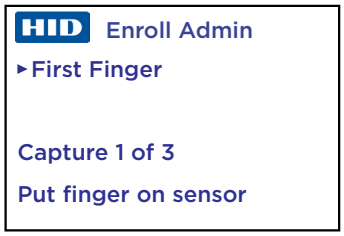
1. Select **1. Enroll Admin**. The Reader displays:

   First Finger

   Capture 1 of 3

   Put finger on sensor

   The Reader will request to capture the first finger three times.



Note: The second line on the display will give instructions to the user, such as **Put finger on sensor**, **Press harder**, **Move right**, **Remove finger**, and so on. Also, for each of the three captures it is recommended that the user fully removes their finger and repositions it slightly differently on the sensor (e.g., more pressure, to one side a little) as this allows the sensor to collect more/different information.

The Reader then asks for the second finger to be captured three times.

When the operation is complete the Reader displays **Success**.

Note: If there is an error, if the fingerprint is not captured, or if the Reader times out, the Reader displays **Authentication Failed** and the sequence returns to the **Enroll Admin** screen. After three failed attempts the display reverts to the main menu. In the case of Initial Setup the display returns to the **Verify Admin** menu, as you must successfully enroll a new Admin (or prove that you have already done so) to exit that step.

2. If a PIN number is required, the Reader then displays:

   Keypad pin

   Enter the PIN number and press **#**. The PIN number can be from 1 to 12 digits. You must the end entry with the **#** key, unless you use a 12-digit PIN in which case the Reader accepts the PIN when the 12th digit is entered and the **#** key is not required.

   The Reader will display **Verify**. Enter the PIN again and press **#**.

   Note: If the PIN is not entered within the timeout period the Reader will display **Enrollment Failed** and will prompt the user to try again. After three attempts the sequence returns to the **Enroll Admin** screen.

3. The Reader then displays:

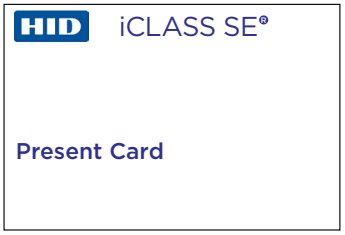
   Write to card

   Present card

   Present the card to the reader. If successful, the Reader will reboot into the Operational Mode you have chosen for it and is ready for normal use.

3. Operation – Reader

In Reader Mode, the display shows the **Present Card** screen.



1. Present the card to the Reader.
2. Follow the on-screen prompts to present a finger to the Reader, if required.
3. Enter your PIN number, if required.

   Note: These requirements can be changed via the **Configuration** menu.

4. When successful, the Reader will:
   - Beep and flash green (LED).
   - Display **Success!**
   - Transmit the access information that is stored on the card to an attached panel.

   Note: If the information provided does not match what is stored on the presented card, the iCLASS SE Biometric Reader will prompt the user to try again. After three unsuccessful attempts at verification the display reverts to **Present Card** and the user must start over.

4. Operation – Administration

4.1 Access the Administration Menu

If the Reader is configured to be a Reader/Enroller and the user wishes to access Administration mode, follow this procedure:

1. The Reader that is configured to be a Reader/Enroller displays the **Present Card** menu as its main screen.
2. Before you present a card, select **1** on the keypad.
3. ~~Present an Admin card and follow the on-screen prompts to verify biometric information and PIN number as required.~~

4.2 Administration Menu Functions

From the **Administration** menu, access the functions below.

Note: Each menu will return to the main menu if it times out.

4.2.1 Manage Users

This presents the choice of enrolling or verifying a User: the standard Enrollment dialog is used (see *Section 2.3.1: Enrollment Dialog*).

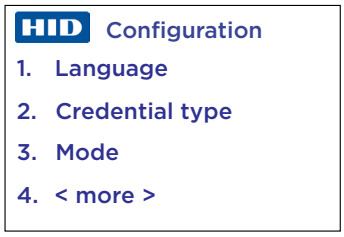
4.2.2 Manage Admins

This presents the choice of enrolling an Admin or verifying an existing Admin card. Each option follows the standard Enrollment dialog (see *Section 2.3.1: Enrollment Dialog*). The other choice is to revoke an Admin. If this option is chosen the user must present an existing Admin card to the reader. Users need to ensure they always have at least one Admin card on the site as the only way to get a replacement Admin card is to reset the reader to the factory setup and go through the initial setup process.

4.2.3 Configuration menu functions

To access the **Configuration** menu, select **3** from the **Administration** menu.

Note: The options in the **Configuration** menu will differ, depending on how the Reader has been set up. For example, If the Reader has been set up for iCLASS or iCLASS SR cards, then non-relevant menus (e.g., Site Key) will not be displayed.



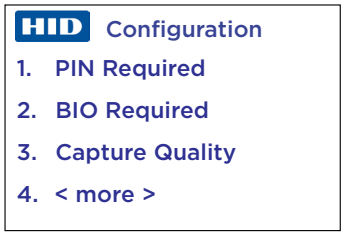
1. **Language:** Changes the language.
2. **Credential Type:** Changes the Credential Type.

Notes:

- If the user changes the Credential Type from **iCLASS** cards to **Seos** cards, then the Reader will reboot into Initial Setup – Site Key mode. The Site Key can then be set up and an Admin card re-created so that it is enabled for all those credential types.
  Note: If the Credential Type is changed in this way, *all* readers on a site must be reconfigured so they all have the same Site Key.
- If the user changes the Credential Type from **Seos** cards to **iCLASS** cards, then the Reader will reboot into Initial Setup – Verify Admin mode. The confirmation Yes/No dialog will display (because the Site Key is not required for iCLASS or iCLASS SR cards).

3. **Mode:** Changes the Operational Mode.
4. Select **4 < more >** to see the next page of Configuration options.

Second page of Configuration options



1. **PIN Required:**

   Yes: To require a PIN for access.

   No: Does not require a PIN for access (Default).

   Note: If the user changes from **PIN Not Required** to **PIN Required** *all* cards on site may need to be re-enrolled, because they may have been previously enrolled when no PIN was required. To facilitate this migration process, It is suggested that the user sets up one or more separate, dedicated enrollers that require a PIN and use these enrollers to add PINs to users' cards, including Admin cards. The site Readers are set to ignore PIN numbers so they will be able to accept the re-enrolled cards. Once all of the user cards have been re-enrolled then the rest of the Readers on the site can be reset to require PINs.

2. **BIO Required:**

   Yes: To require a fingerprint for access (Default).

   No: Does not require a fingerprint for access.

3. **Capture Quality:**

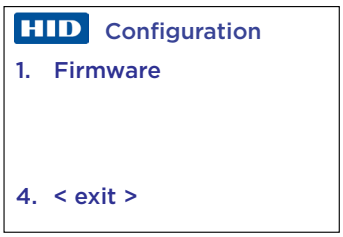
   Low Quality: Only one scan is required when capturing each fingerprint.

   High Quality: Three scans are required when capturing each fingerprint. This is the recommend mode as the likelihood of success when a user presents a finger to gain access is increased.

4. Select **4 < more >** to see the next page of Configuration options.

Third page of Configuration options

- **Firmware:** Displays the Firmware information, if needed, when working with Technical Support.



Note: Press **#** to bring up a page with the Site Key number (option only appropriate when the **Credential Type** is set to **Seos**).

- **Visitor Card Enabled:** This option is only available if the **Credential Type** is set to **iCLASS or iCLASS SR**.

  Yes: To allow visitor cards to be used in this environment.

  No: Do not allow visitor cards in this environment (Default).

If you select **Yes** and go to **Manage Users** there will now be a third choice in the Enrollment dialog: **Enroll Visitor**. Visitor cards are prepared ahead of time, are generic, and can be given to visitors without requiring them to enroll their biometric information. No fingerprint information will be processed by the reader. If **PIN Required** is set, visitors will need to be told what the PIN value is to permit access.

Select **4 < exit >** to return to the first screen of Configuration options.