1743 S Grand Ave | Glendora, CA 91740
Support: 800.883.8822

PALIDIN Application
&
ID-150 Scanner
System
Manual

1743 S Grand Ave | Glendora, CA 91740
Support: 800.883.8822

Version Control Table

Version	Date	Author	Version Description
2018.1.0	May 14, 2018	David Roman-Rodriguez	Initial release
2018.1.1	August 21, 2018	David Roman-Rodriguez	**Added**: troubleshooting examples 6.8 to 6.17, and 7.5. **Updated**: section 7.4
2018.1.2	November 14, 2018	David Roman-Rodriguez	**Added:** troubleshooting example 6.18. **Updated**: sections: 4.3.1, 4.4.7, 4.4.8, 6.7.2, and 6.15. Incorporated software changes from PALIDIN v0.8.0: larger portrait image in main result page, larger document images in transaction report, sample file and transaction report are saved with the same file name, app resolution issue on Surface Pro 3 devices, print transaction report from main result page, expiration field will have a red font is document is expired, etc.

1743 S Grand Ave | Glendora, CA 91740
Support: 800.883.8822

Table of Contents

1743 S Grand Ave | Glendora, CA 91740
Support: 800.883.8822

1 - Introduction

Welcome to the FraudFighter family! We are excited to have you onboard. This system manual will be your source of information for all software and hardware related topics. Your new identity document (ID) authentication system will aid in minimizing the risk of ID document fraud and all of its negative business impacts. Let's start with a quick introduction to the AssureID software and how it works as well as the PALIDIN application.

The AssureID document authentication software utilizes machine-enabled forensic examination processes to verify authenticity of identity documents. Techniques that previously required a document expert, whose skills and knowledge were developed over decades of practice, have been automated and built around a comprehensive library of global document templates.

The various scanners from different manufacturers that are integrated for use with the AssureID document library each share some common attributes. First and foremost is the ability to capture high-resolution images of the ID document, both front and back, typically under more than one wavelength of light (e.g. visible white light, Infra-Red light and/or Ultraviolet light).

Depending on document type and scanner chosen, data may be captured from the document that is stored in various digital formats. This might include Radio Frequency Identification chips (RFID), magnetic stripe, B900 security printing, barcodes and digital watermarks. Also, the software is equipped with an Optical Character Recognition (OCR) engine capable of recognizing the printed information on the document. There is also software available for translating non-English character printing to English.

With the images and the data captured from the document, the AssureID software is then able to conduct dozens of tests to ensure that (1) the design and document printing techniques meet the specifications of the issuing jurisdiction, (2) the visible and non-visible security features are present, as expected, (3) the digital data is formatted properly, and (4) the data from all different sources (barcode, OCR, RFID chips, etc.) matches and crosschecks properly. Depending on the identity document being examined, as many as three dozen or more tests may be conducted on any given ID verification.

The PALIDIN application (powered by AssureID), on the other hand, gives you more features and functionalities. For instance, it gives you the ability to choose the name of the file when saving a transaction report. It gives you the ability to export historical data and much more. PALIDIN has been developed by FraudFighter and we'll be responsible for maintaining the user interface and its feature roadmap.

2 - Software Download & Installation

Please refer to our software installation guide for step by step instructions on how to download and install the i-Dentify driver, AssureID software, AssureID document library, and PALIDIN programs.

Please note the computer device needs to meet the following minimum system requirements:

- 2GHz Intel® Pentium® 4 CPU minimum (Intel® Core™ 2 Duo or higher recommended)
- 2 GB RAM minimum (4 GB or higher recommended)
- 10GB available hard disk space minimum (20GB or higher recommended)
- USB 2.0 port
- Supported Windows operating systems:

Operating system version	Type	Release
Microsoft Windows 10	64-bit	
Microsoft Windows 8.1	32- and 64-bit	
Microsoft Windows 8	32- and 64-bit	
Microsoft Windows 7	32- and 64-bit	
Microsoft Vista	32- and 64-bit	Service Pack 2 or later
Microsoft Windows XP	32-bit	Service Pack 3 or later
Microsoft Windows XP	64-bit	Service Pack 2 or later

Note: In order to install and update software components, the user needs to have administrative rights on the computer. If a non-administrative user attempts to install or upgrade the software, the installation won't be successful (which may results in older versions of the software being deleted or corrupted).

3 - i-Dentify ID-150 Scanner Info & Installation

3.1 - Features

The ID-150 Desktop Document Scanner has the following features:

- High resolution (600 dpi) double-sided color card scanner
- High-speed scan and transfer of images within 5 seconds
- Plug-and-play connectivity with high speed USB 2.0 interface
- Patented card transport mechanism for jitter-free image and reliable scanning
- Compact and user-friendly design
- Clamshell type cover mechanism for easy maintenance
- 870 nm IR image for front side of ID card authentication (ID-150 only)
- Scanning modes:
    - 24-bit color, black and white, and grayscale for visible images
    - Black and white, and grayscale for 870nm near-infrared image (ID-150 only)
- One-pass magnetic stripe reader for ISO 7811 and AAMVA specification (ID-150 only)

Figure 1 - ID-150 device

3.2 - Specifications

The hardware specifications for the ID-100 and ID-150 Document Scanners are listed below:

Specification	ID-150
ID Card Size	
Width	53.5 – 54.9mm (ISO specification 53.92 - 54.18)
Length	85 – 86mm (ISO specification 85.47 - 85.90)
Thickness	0.4 – 1.0mm (ISO specification 0.68 - 0.84)
Scanner	
Scanning Side	Duplex
Illumination	Front: RGB (470/530/620nm) Rear: RGB (465/520/630nm) Near-Infrared (880nm)
Sensor	Front: Color CIS Rear: Color CIS
Scan Width	54mm
Resolution	300/600 dots per inch (DPI)
Color	8-bit grayscale; 1 bit B/W; 24-bit RGB color
Scan Speed	42mm/sec @ 600dpi; 84mm/sec @ 300dpi
Magnetic Stripe Reader	
Tracks	ISO7811 3 Track, US/Canada AAMVA Driver License
Interface	
Type	USB 2.0 High Speed (480Mbps)
Physical Dimensions	
Size	118W x 169D x 71H (mm)
Weight	750g
Power	
Input	DC12V, 1.0A
Active Current	900Ma
Idle Current	300Ma
Environment	
Operating	0 - 50 °C; 10 - 90% RH, non-condensing
Storage	-20 - 70 °C; 5 - 95% RH, non-condensing
Reliabillity	
MTBF*	26,280 hours
MCBF**	1,095,000 cycles (scans)
Compliance	
Radio Frequency Interference	This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: - This device may not cause harmful interference, and - This device must accept any interference received, including interference that may cause undesired operation.
RoHS Compliant	Yes
Certifications	CUL , CE, C-Tick

* Mean Time Between Failure

** Mean Cycles Between Failure

3.3 - Rear Panel

The rear panel of the document scanner is shown below (ID-100 is shown):

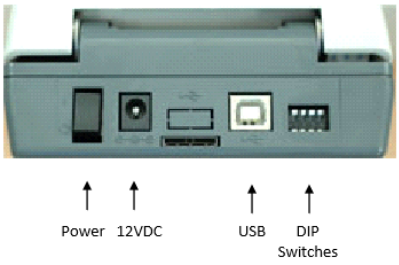


Figure 2 - ID-150 rear panel

The table below describes the purposes of the DIP switches. DIP switches should not be changed from the default position except for cleaning (#3) or if instructed by FraudFighter Support personnel.

DIP Switch #	Default	Purpose
1	Off (Up)	Reserved
2	Off (Up)	Reserved
3	Off (Up)	Enable feed roller spin motion for cleaning when On (Down)
4	Off (Up)	Upgrade firmware when On (Down)

Figure 3 - Dip switch function and state

3.4 - Status Indicators

The ID-150 document scanner has two LED status indicators on the front left surface. LED1 reports the USB status and scan ready state. LED2 reports the power supply status.

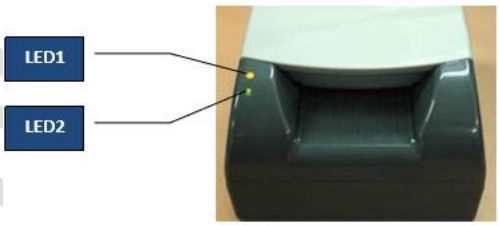


Figure 4 - LED designation

The state of these LEDs will indicate the current status and assist in troubleshooting problems. See the table below for interpreting the state of the indicators:

LED1	LED2	Meaning
Off	Off	Power is off. Check the power cable and switch.
Blinking Red	Green	USB is not connected. Check the USB cable and connectivity.
Red	Green	Device is in an error state. Restart device or reinstall drivers.
Blinking Yellow	Green	Scanning a card.
Stable Yellow	Green	Ready to scan.

Figure 5 - LED status indicators

3.5 - Installation

The ID-150 document scanner package includes the following pieces, see figure “x” for reference:

- ID-150 document scanner unit
- USB cable with ferrite core
- External power supply

Figure 6 - Items included with ID-150 device

Note: DO NOT connect the scanner to the computer until you have downloaded and installed the I-Dentify drivers, AssureID software, and Document Library files.

To install the scanner, follow these steps:

1. Plug the USB cable to the computer (USB 2.0 port) and the back of the scanner
2. Connect the power cable to the scanner and connect to power supply.
3. Turn ON the device by using the switch in the back on the scanner (I=ON; O=OFF)

4 - PALIDIN Application Guide

4.1 - AssureID Ready for Use

By clicking on the system tray, you can find the AssureID software icon. If the icon shows a red "x," this means the AssureID service is not active. To start the service, right-click the AssureID icon and select the "Start Service" option, see figure 7.

If the application has been working properly but suddenly it stops working, shutting down the service ("shutdown service") then restarting the service should be the first step to resolve a non-working application.

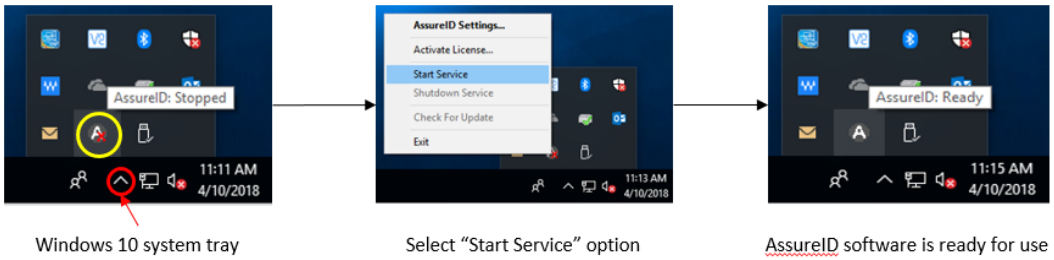


Figure 7 - AssureID status

4.2 - PALIDIN Home Screen

Once you open the PALIDIN application, you'll see the main home screen, see figure 8. If the application is ready for use, you should see the "Online" scanner status, on the bottom right corner of the window. It make take a few minutes for the software to recognize and connect to the ID scanner (this is true on older computer devices). If you see a "No scanner detected" status, wait until the status changes to "Scanner Status: Online" and the "Insert a document to begin scanning" message is displayed.

The document scan status will change from "Connect a scanner to begin checking documents," to "Insert a document to begin scanning," to "Now scanning a document…," to finally "Remove Document. Processing results."

The app checks for a new update every time the application is opened (internet connection required). If an update is available, the app will display a message, in the bottom left corner of the screen, letting you need to install the latest version of the software.

At the bottom of the screen, you will see the current software version of the three main software components: AssureID, Document Library, and PALIDIN.

At the top of the screen you'll find the main navigation tabs: Home, Results, Settings, and Exports.

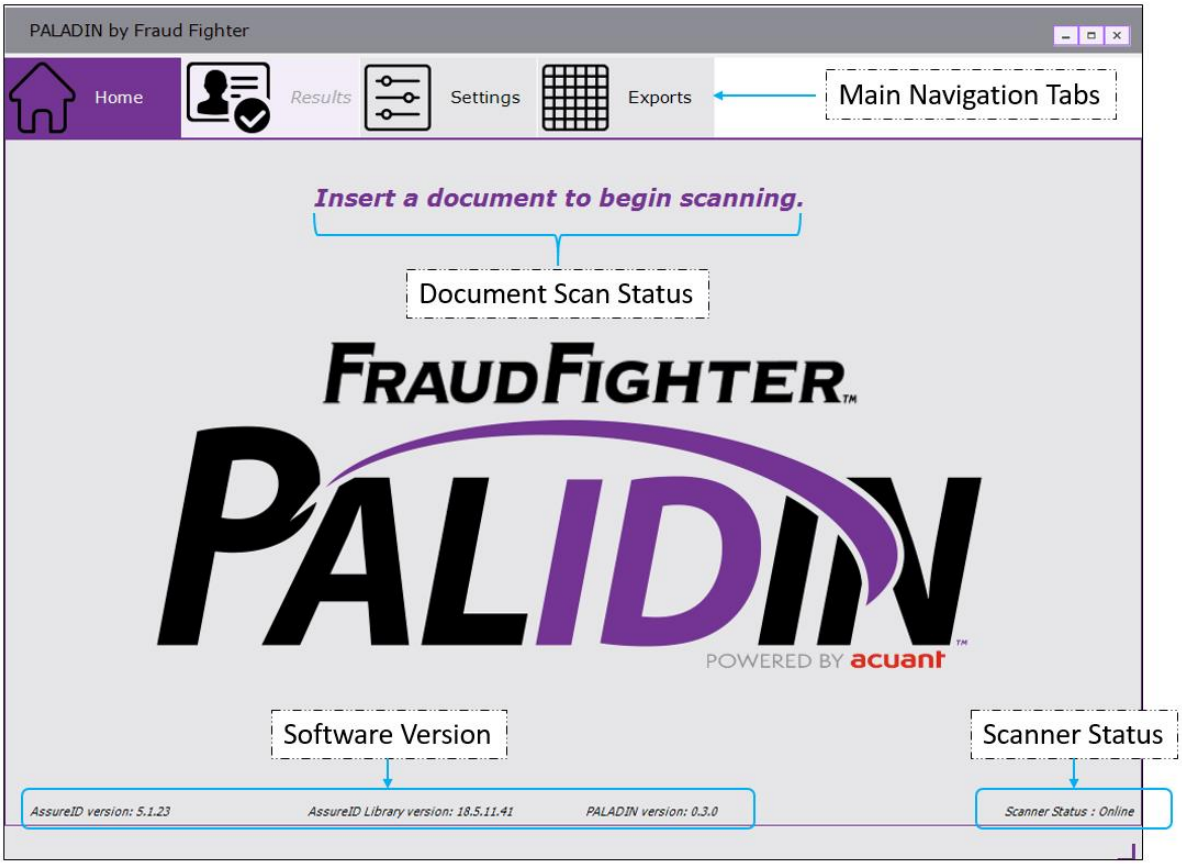


Figure 8 - RevealID Home Screen

4.2.1 – Inserting a document into the scanner

Insert the ID1 type document with the front of the document facing up and the magnetic stripe to the right (as shown below). This is important because the magnetic stripe reader is situated on the right side of the scanner.

4.3 – Results

The results tab contains all information related to the scanned document: authentication results, images, biographic data, authentication tests, and transaction report. Collectively known as the "inspection result options."

4.3.1 Main

When an ID document is inspected and authenticated by the PALIDIN application, the main result screen will be displayed, see figure 9. Please note that once the system displays the result screen, clicking on the home, settings, or export tab will automatically discard the current transaction information. The main result screen displays the following information:

- The document authentication result (i.e. Passed, Failed, Attention, or Unknown)
- The inspection result detail section will list the individual tests that received an "attention" or "failed" result, or any other system configuration parameter (i.e. age verification).
- A large portrait image, and a smaller image of the front of the document. The larger portrait image is designed to ensure the bearer presenting the document is in fact the person shown in the ID document. You can customize whether these images should display or not.
- The left-hand inspection navigation options give you the ability to look closely at the inspection results (i.e. authentication tests) and to see the images and data captured by the scanner.
- The document type and personal information section will display detail information about the document and Personally Identifiable Information (PII). The main result screen can be customized to display little to no PII information.
- The inspection result actions will allow you to: (1) save a transaction report, (2) save a sample, or (3) print a transaction report.
    - Transaction Report: is a PDF file that includes a summary of the inspection result, document images, and personal information. This is the manual approach to saving a transaction report. The transaction report can be customized to include all or no PII information and/or document images.
    - Sample: a sample file is a collection of data and images stored in a proprietary and encrypted file format (i.e. .sample). A sample file is used for troubleshooting and doing forensic work on software and hardware issues. Using special software the FraudFighter team can review the results of a specific document to determine what may have caused a certain result. For instance, we can see whether the document was misfed or if there was a malfunction with any of the scanner hardware sensors. Customers should only save a sample report when asked by a FraudFighter team member.
- The status bar will let you know when a scan is completed, and when a transaction report or sample report is saved. If there's an error when saving a file, the status bar message will let you know.

There are four possible authentication results:

1. Passed: the software recognizes the document and was successful in verifying physical security features and data content sufficient to enable a "pass" grade to be rendered.

2. Failed: the software recognizes what type of document it is supposed to be but cannot verify some physical security features and/or data content sufficient to enable a “pass” grade.
3. ! Attention + reason: this result implies that the software was able to recognize and validate the authenticity of the document, but the document has an issue(s). For instance, it may be expired, the magnetic strip might be damaged, or dirt on the document has obscured some visible features.
4. Unknown Document: this result implies one of two things (1) the document is not a part of the library (the document is “untrained”), or (2) the document is of poor quality forgery.

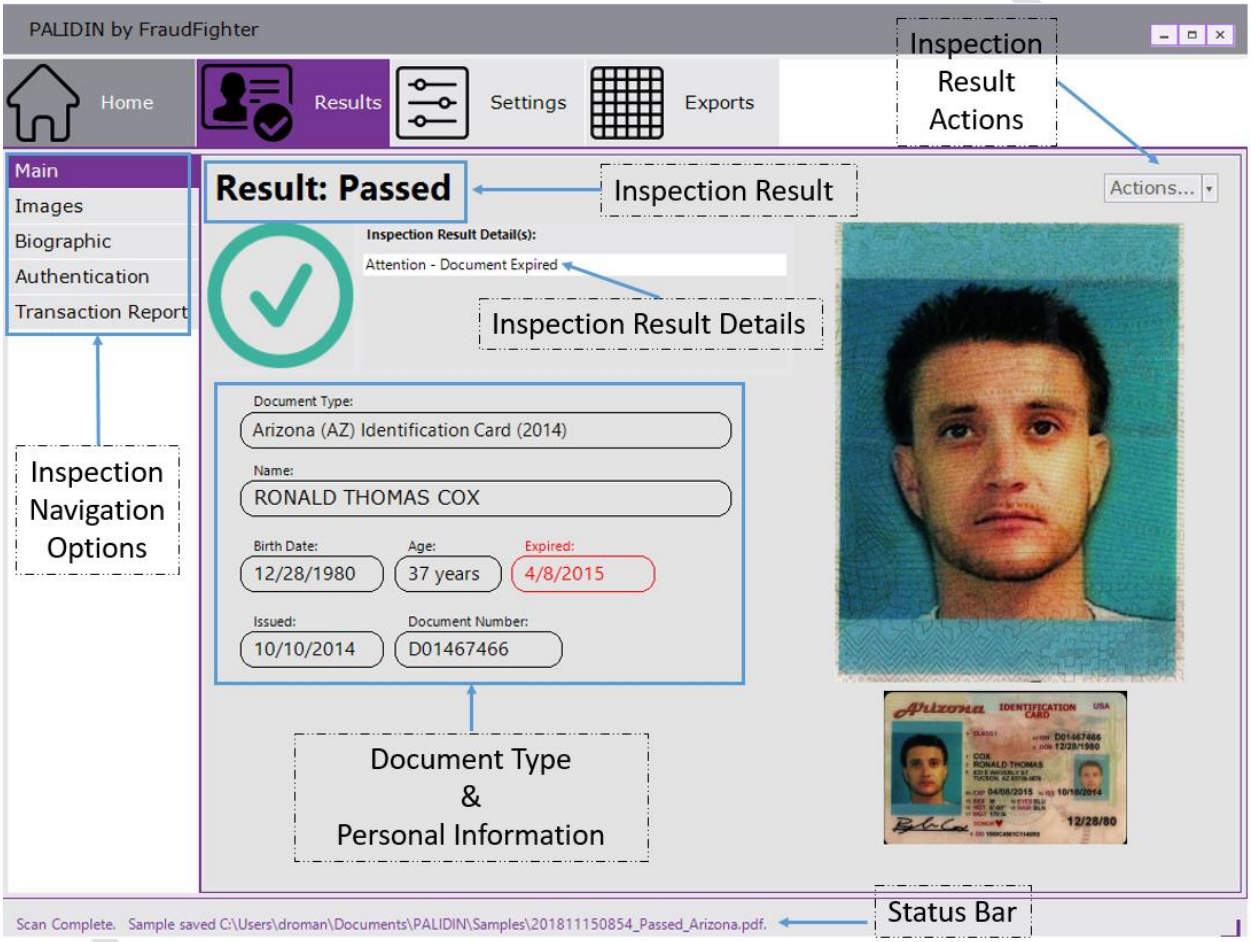


Figure 9 - Inspection Results screen

4.3.2 - Images

This screen displays the high-resolution images captured by the scanner. You’ll see both the front and back of the ID document as well as an infrared version of the front of the ID document, see figure 10. Depending on which scanner device you use, you may see ultraviolet versions of both the front and the back of the document (e.g. Desko Penta scanner). Select a thumbnail to inspect the document image in more detail. Use the left slider or +/- buttons to increase/decrease the image size. You can also use the mouse wheel to adjust the image size.

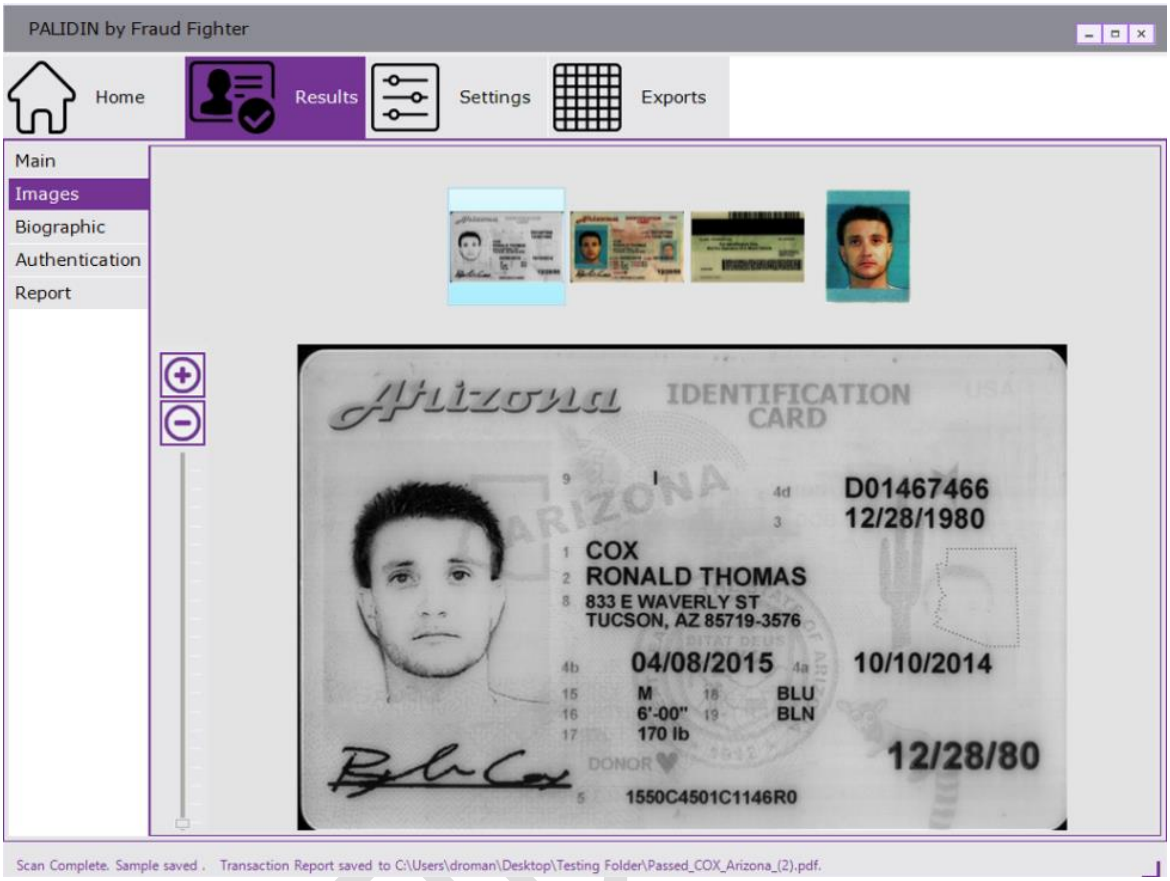


Figure 10 - Images screen

4.3.3 - Biographic

This screen displays the various personal data information extracted from the document, see figure 11. It also displays the personal data stored on the multiple security mechanisms in the document (e.g. magnetic strip, 1D barcode, 2D barcode, chip, etc.). The biographic information will vary depending on the document type (e.g. ID document versus passport).

4.3.4 - Authentication

This screen displays the individual authentication tests performed on the document and their respective result (e.g. birth date crosscheck, 2D barcode read, 2D barcode content, etc.), see figure 12. This page can be configured to display: (1) only authentication tests that failed, or (2) to display all authentication tests (including those tests that received a pass result).

The authentication engine performs a weighted average on all of the individual authentication test results in order to give the document the overall authentication result. This means that it is possible for a document to fail one test but still receive a pass overall result.

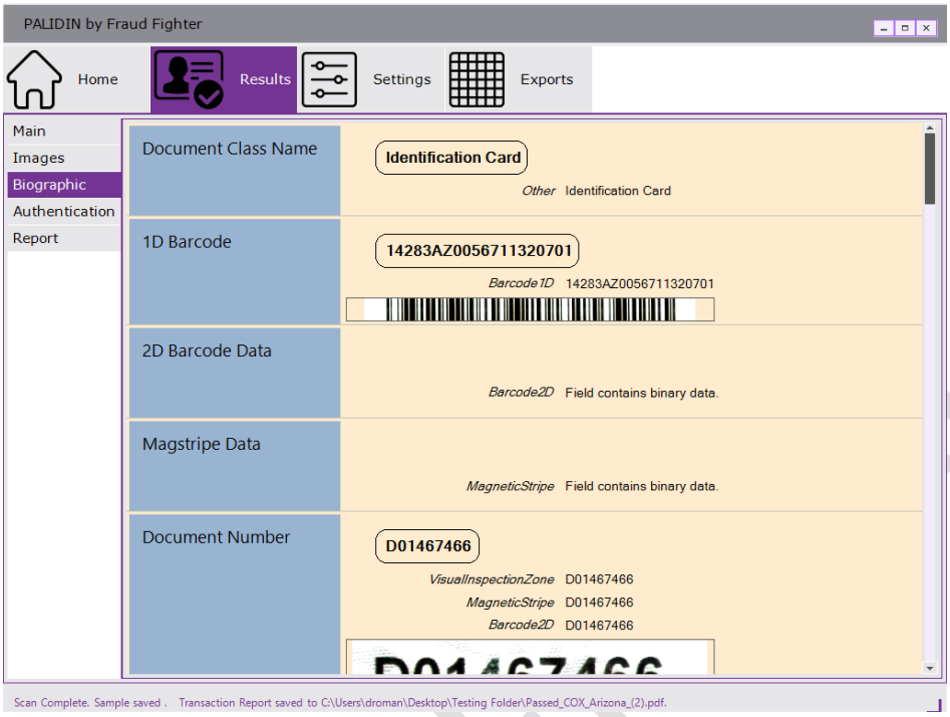


Figure 11 - Biographic Information screen

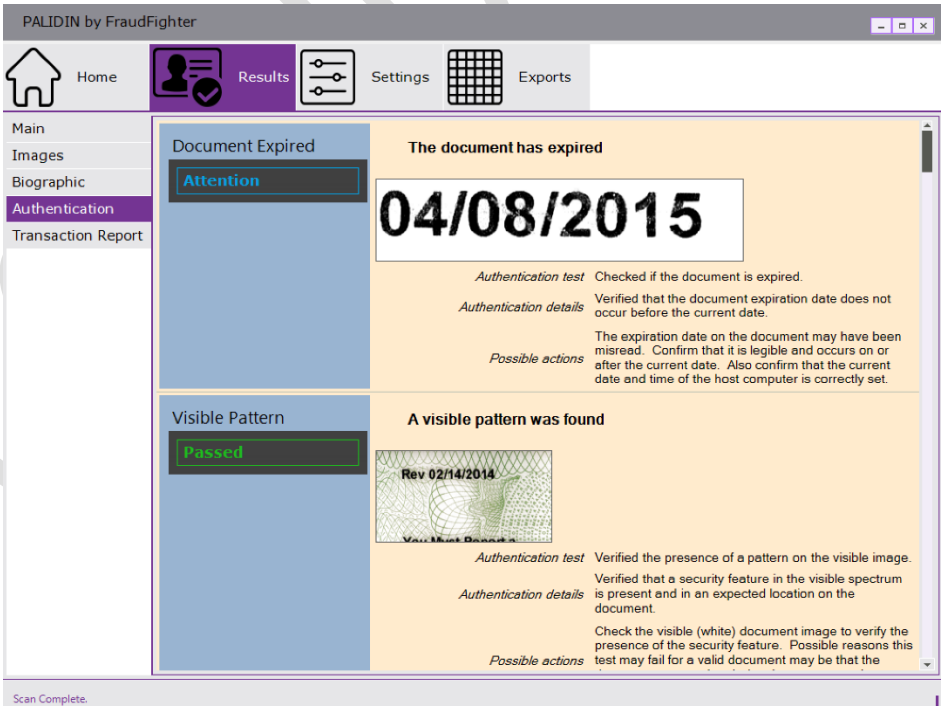


Figure 12 - Authentication Test Results screen

4.3.5 – Transaction Report

This page will display a summary inspection report that can include high-definition images, document info and personal data collected by the scanner, see figure 13 (depending on system configuration). It also includes the date/time stamp and the computer name that processed the document scan. The data shown on the report can be customized to not include PII data or document images.

The transaction report page has a save report and print report option (floppy disk icon and printer icon, respectively). Please note that this is the manual way of saving reports. The automatic option will be covered in a later section. Use the "+/-" icons to adjust the report size.

If the "alerts" section on the transaction report needs to list various failed test results, the system will generate the report into two pages.

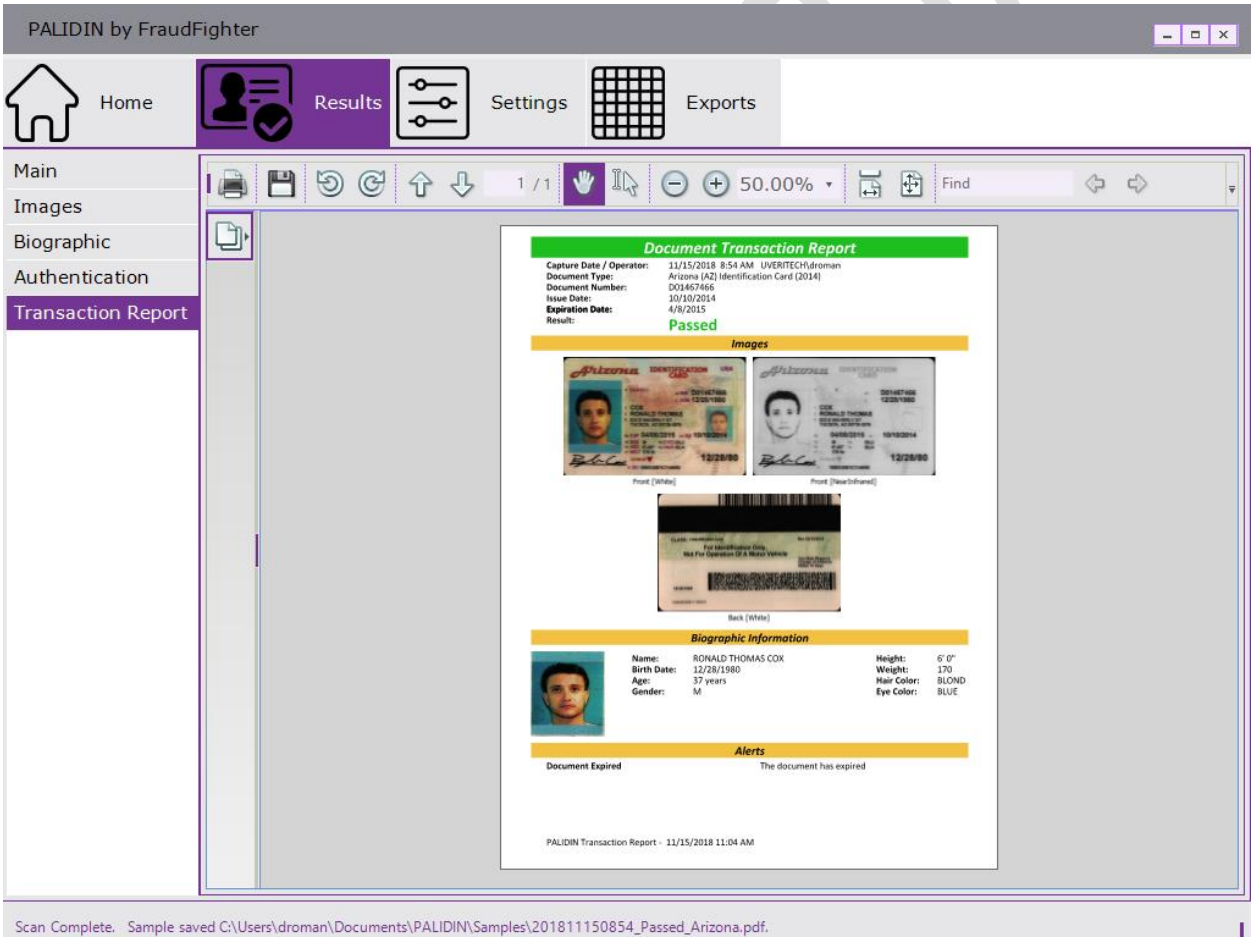


Figure 13 – Transaction Report screen

4.4 - Settings

There are multiple settings that can be enabled or disabled in order to better fit your business needs. Some of these will affect the way the user interacts with the software, as such, we recommend that you go through these options before you start using the application. From the home screen, click on "settings" to see the different options.

Enabling and disabling the settings:

- A greyed out toggle switch means the option is disabled; and conversely, a purple colored toggle switch means the option is enabled. Click on the toggle switch to enable/disable the option.
- An unchecked box means the option is disabled; and conversely, a checked box means the option is enabled. Click the box to enable/disable the option.
- For numerical options, you can use the "▲/▼" to increase/decrease a number. You can also type the desired number.
- For timeline options, you can use the provided options: days, weeks, months, years.
- There is no "save" button so settings will enable or disable as soon as a toggle or box is checked/unchecked.
- Hoovering your mouse over each setting component will display a "help" bubble with more information about the specific setting.

4.4.1 - General

See figure 14. This page covers the following settings:

- Ability for administrators to grant access to non-administrative users to view and change system configurations. This option is disabled by default.
- Allows you to set whether the app should automatically clear the current transaction information (configured in seconds). Once this time has elapsed, the system will go back to the home screen and discard the current transaction information. This option is disabled by default.
- Contactless chip capture and duplex capture should always be enabled. These options are enabled be default.
- Ability to set an automatic prompt for the transaction level user to try scanning the document again whenever a scan is not successful. We recommend that customers using a flatbed scanner device enable this feature. This option is disabled by default.

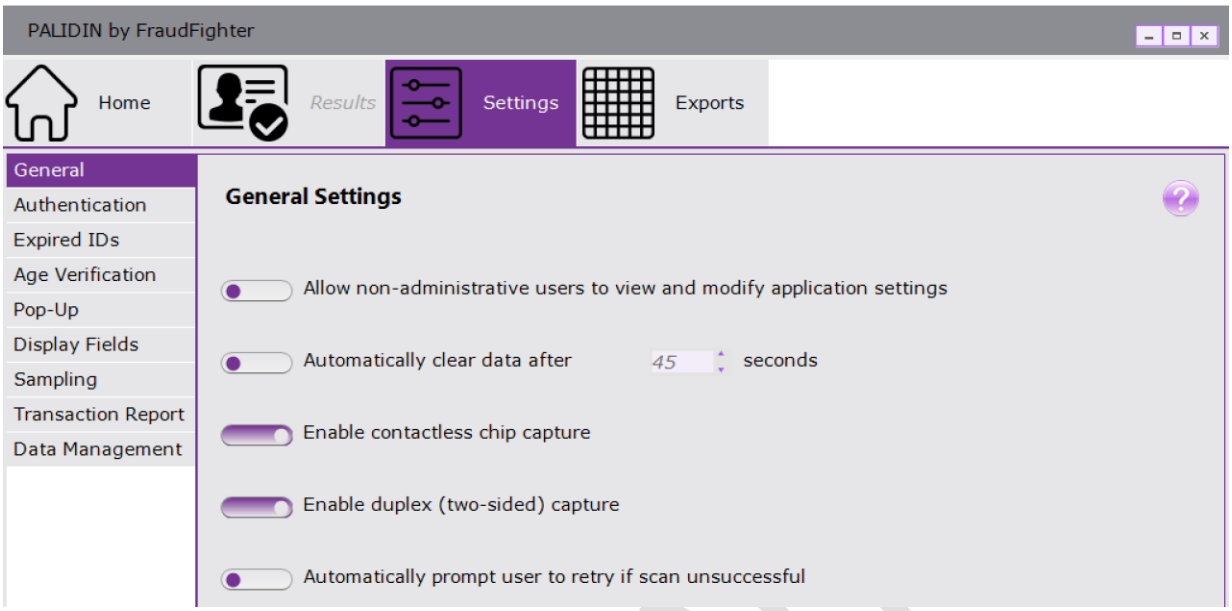


Figure 14 - General Settings

4.4.2 - Authentication

See figure 15. This page covers the following settings:

- Ability to set whether an “attention” inspection result should be displayed as passed or failed. By default, this option is disabled. As a reminder, Attention = Pass. Attention means the system was able to classify the document and authenticate it but the user should be aware or make note of something (most commonly an expired ID or a damaged magnetic strip).
- Ability to set whether “passed” individual authentication test results are displayed in the authentication details page. See figure 12. This image shows both passed and attention authentication results. This option is disabled by default.
- Ability to adjust authentication sensitivity. We strongly recommend to keep the sensitivity on the “normal” option. The normal option provides the optimal balance between fraudulent document detection, and genuine document rejection rates.
    - Low authentication setting: Provides a lower fraudulent document detection rate, while possibly resulting in lower genuine document rejection rates. This is not recommended for use in applications where fraudulent document detection is crucial.
    - High authentication setting: Provides a higher fraudulent document detection rate, while possibly resulting in a higher genuine rejection rate. This is recommended for use in high-security applications.

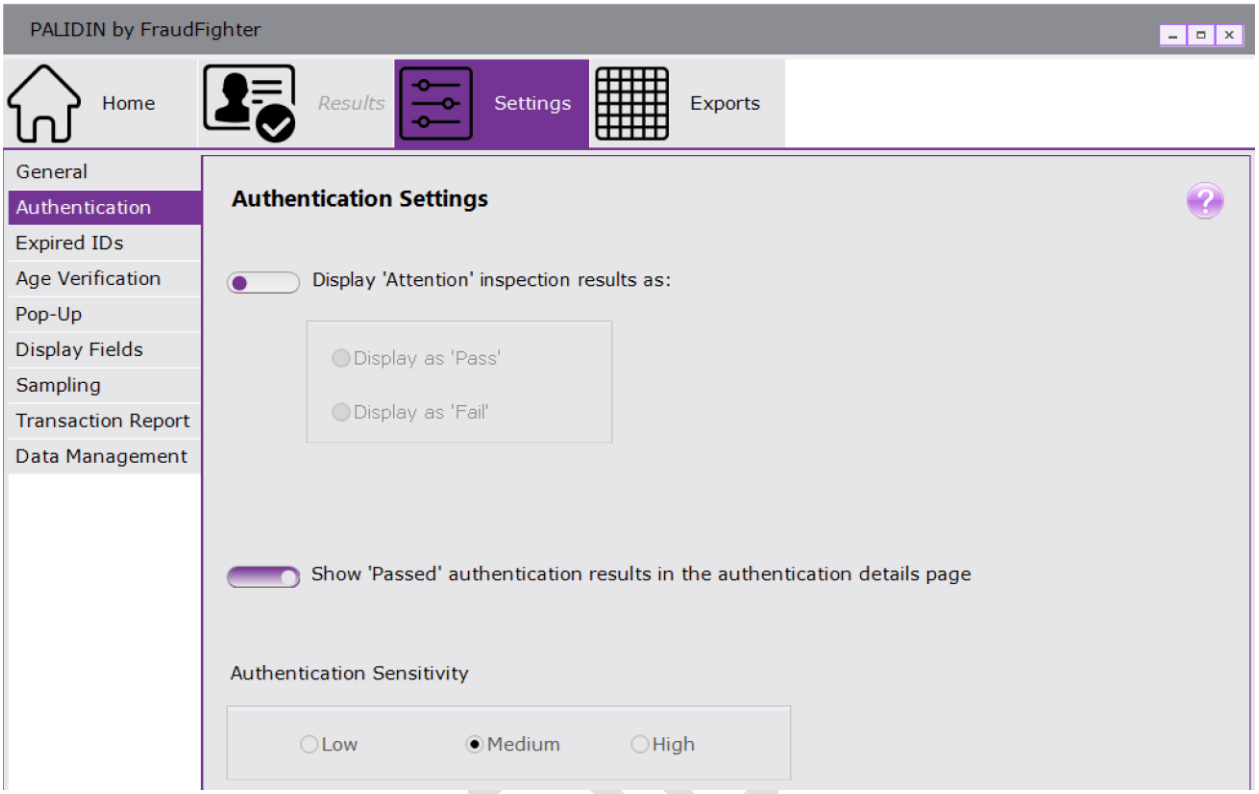


Figure 15 - Authentication Settings

4.4.3 - Expired IDs

This page allows you to set whether you want to accept expired ID's or ID's that will expire within "x" numbers of days from expiration date. These options are disabled by default. You'll have the following options:

- The first toggle switch allows you to set whether to accept expired ID's or not. By default, an expired ID will have an "attention" inspection result. If you enable this setting, expired documents will receive a pass result. You have two configuration options:
    1. To accept all expired ID's. This option will give an expired document a "pass" inspection result.
    2. To accept ID's that have expired within "x" number of days from expiration date. To set this configuration, select the option then use the "+/-" buttons to set the desired number of days. This options will give a "failed" inspection result if the document is outside of the set parameter. If the document is within the set parameter, the application will give it a "pass" result.
- Ability to set whether a document that will be expiring within "x" number of days (from expiration date) should be flagged as "attention" or "failed."
    1. To set this configuration, click the toggle switch, select the desired number of days until expiration date, then whether to flag it as attention or failed.

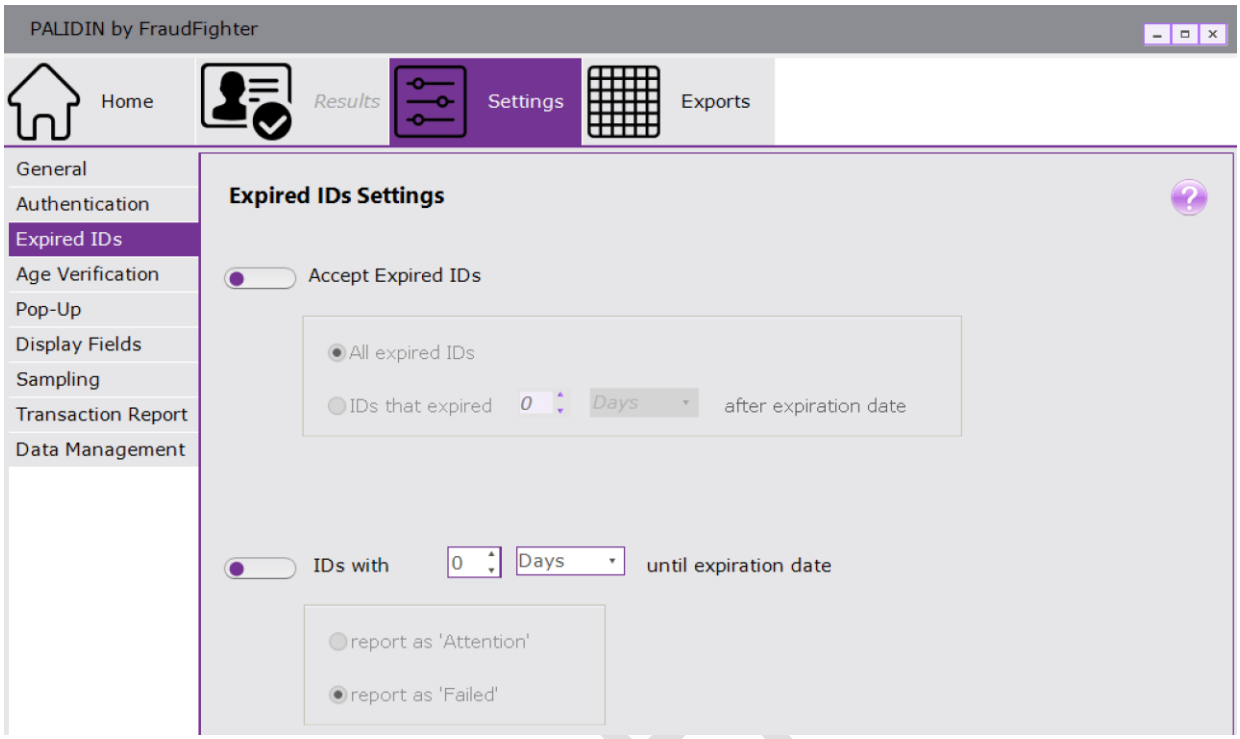


Figure 16 - Expired IDs Settings

4.4.4 - Age Verification

This page allows you to set an age verification parameter with a minimum age requirement (e.g. 21 years of age to buy alcohol) and whether to set the inspection result as “attention” or “failed.” This option is disabled by default.

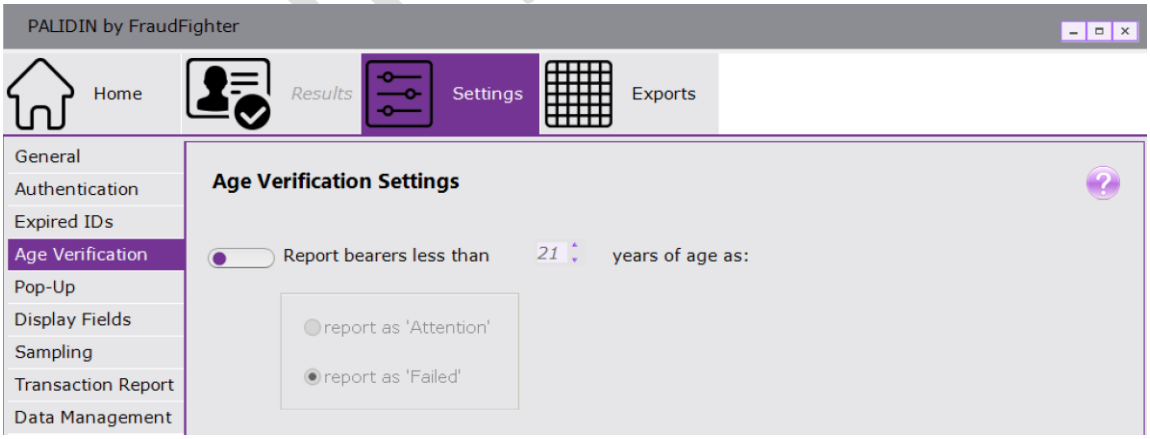


Figure 17 - Age Verification Setting

4.4.5 - Pop-Up

When the PALIDIN application is minimized, the application will continue running in the background. When this option is enabled, the PALIDIN app window will pop-up automatically whenever a document is being scanned. After the screen reaches the “duration” parameter, the app window will be automatically minimized and pop-up on the next scan. This option is disabled by default.

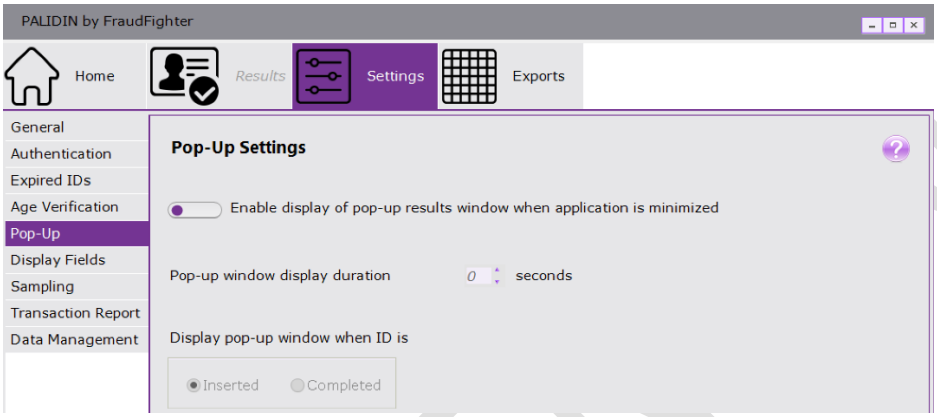


Figure 18 - Pop-up Settings

4.4.6 - Display Fields

This page will allow you to select which personal data fields you want to see in the inspection results page (see figure 9 under “document type and personal information”) and on the transaction PDF report. Adjust these settings based on state and federal laws governing the collection and recording of PII.

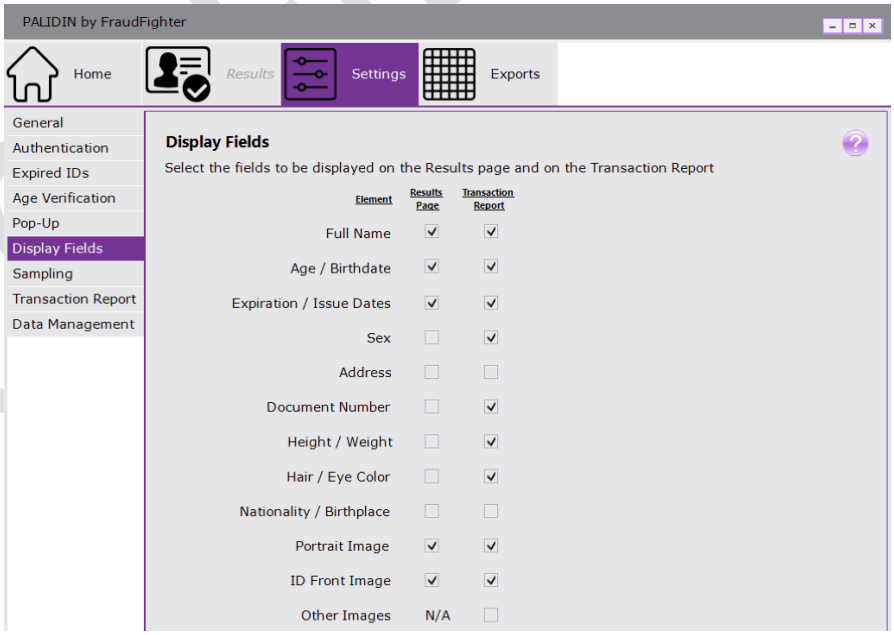


Figure 19 - Display Fields Settings

4.4.7 - Sampling

As a reminder, a sample file is a collection of data and images in a proprietary and encrypted file format (see page 14 for more details on sample reports). On this page you can control whether sample reports can be saved manually or automatically, see figure 20a. FraudFighter does not recommend that you automatically collect sample reports unless you are instructed to do so by one of our Customer Support team members. We use sample files to review particular document authentication results or to train the software and develop new document design templates.

To allow users to manually save a sample report, follow these steps:

- Click the toggle switch for "allow ID samples to be saved"
- Select the desired local folder location (this can be a networked folder too) by clicking the "…" button and navigating the "browse for folder" window.
    - Make sure the folder has been to set to allow the system to "write" to it otherwise the system won't be able to save the sample reports to the folder.
- Once you enable this feature, the "Edit File Name Pattern" option will be available. Click this button to tell the system what name to use while saving the file, see figure 20b.
    - Three field sections can be used to create the file name pattern.
    - Choose the desired data set for each of the three fields then click the "save pattern" button.
    - PALIDIN supports a "custom text" option, which allows you to type a desired data set (e.g. POS113, Store113A4, FinanceSystem, etc.). A custom text designation will be used on every file that is saved by the system.
    - Please note that this file name pattern will be used for both sample files and transaction reports.
- The user will have access to the "save sample" option in the inspection result actions drop-down menu.

To allow the system to automatically save sample reports, follow these steps:

- Click the toggle switch for "automatically collect ID samples"
- Under the "allow ID samples to be saved" section, select the desired local folder location (this can be a networked folder too) by clicking the "…" button and navigating the "browse for folder" window.
    - Make sure the folder has been to set to allow the system to "write" to it otherwise the system won't be able to save the sample reports to the folder.
- Once you enable this feature, the "Edit File Name Pattern" option will be available. Click this button to tell the system what name to use while saving the file, see figure 20b.
    - Three field sections can be used to create the file name pattern.
    - Choose the desired data set for each of the three fields then click the "save pattern" button.

- PALIDIN supports a “custom text” option, which allows you to type a desired data set (e.g. POS113, Store113A4, FinanceSystem, etc.). A custom text designation will be used on every file that is saved by the system.
- Please note that this file name pattern will be used for both sample files and transaction reports.

- You’ll have the ability to tell the system whether to save sample reports for all transactions or for specific transactions only.

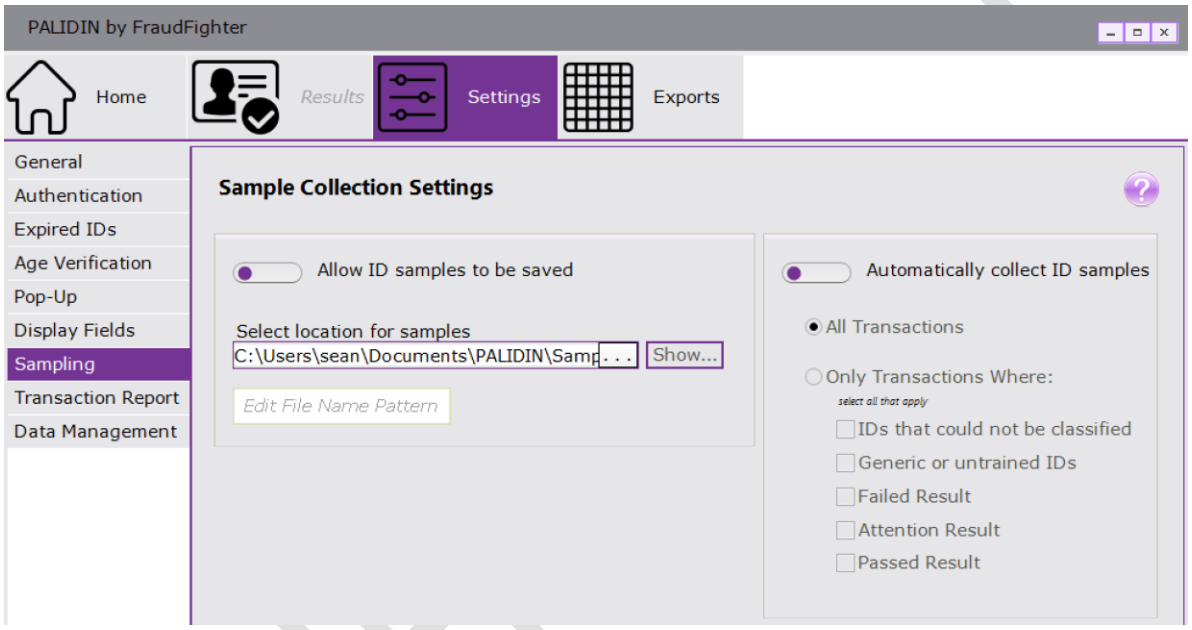


Figure 20a – Sampling Settings

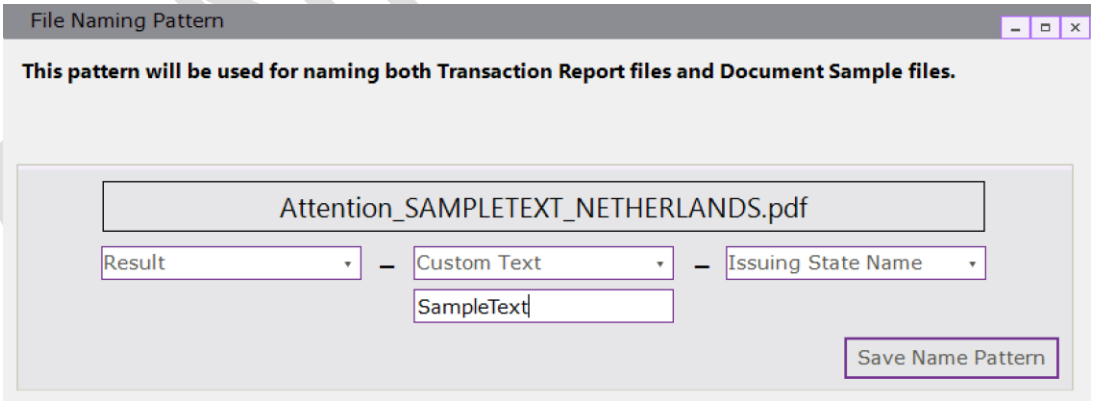


Figure 21b – Sampling Settings

4.4.8 – Transaction Report

A transaction report is a PDF document that can contain high-resolution images of the ID document, the results of the authentication test, and personal information as stored in the document. As a reminder, both the main result page and the transaction report can be customized via the "Display Fields" screen, see page 23 for instruction on how to customize the transaction report.

The transaction report is one method to maintain a record of the authentication test conducted on the ID document, see figure 21.

To allow users to manually save a transaction report, follow these steps:

- Click the toggle switch for "Allow Transaction Reports to be viewed, printed & saved"
- Select the desired local folder or networked folder by clicking the "…" button and navigating the "browse for folder" window.
    - If you select a folder other than the default, make sure the folder has been to set to allow the system to "write" to it otherwise the system won't be able to save the sample reports to the folder.
- Once you enable this feature, the "Edit File Name Pattern" option will be available. Click this button to tell the system what name to use while saving the file, see figure 20b.
    - Three field sections can be used to create the file name pattern.
    - Choose the desired data set for each of the three fields then click the "save pattern" button.
    - PALIDIN supports a "custom text" option, which allows you to type a desired data set (e.g. POS113, Store113A4, FinanceSystem, etc.). A custom text designation will be used on every file that is saved by the system.
    - Please note that this file name pattern will be used for both sample files and transaction reports.

To allow the system to automatically save transaction reports, follow these steps:

- Click the toggle switch for "Automatically save Transaction Reports"
- Under the "allow transaction reports to be viewed, printed & saved" section, select the desired local folder or networked folder by clicking the "…" button and navigating the "browse for folder" window.
    - If you select a folder other than the default, make sure the folder has been to set to allow the system to "write" to it otherwise the system won't be able to save the sample reports to the folder.
- You'll have the ability to tell the system whether to save all transaction reports or only specific transactions.
- Once you enable this feature, the "Edit File Name Pattern" option will be available. Click this button to tell the system what name to use while saving the file, see figure 20b.
    - Three field sections can be used to create the file name pattern.

- Choose the desired data set for each of the three fields then click the “save pattern” button.
- PALIDIN supports a “custom text” option, which allows you to type a desired data set (e.g. POS113, Store113A4, FinanceSystem, etc.). A custom text designation will be used on every file that is saved by the system.
- Please note that this file name pattern will be used for both sample files and transaction reports.

To set a password protection for transaction reports, follow these steps:

- Click the toggle switch for “Password protect saved report PDFs”
- Type the desired password in the “PDF protection password” section
- The system will require users to enter the password before they can view the PDF transaction report

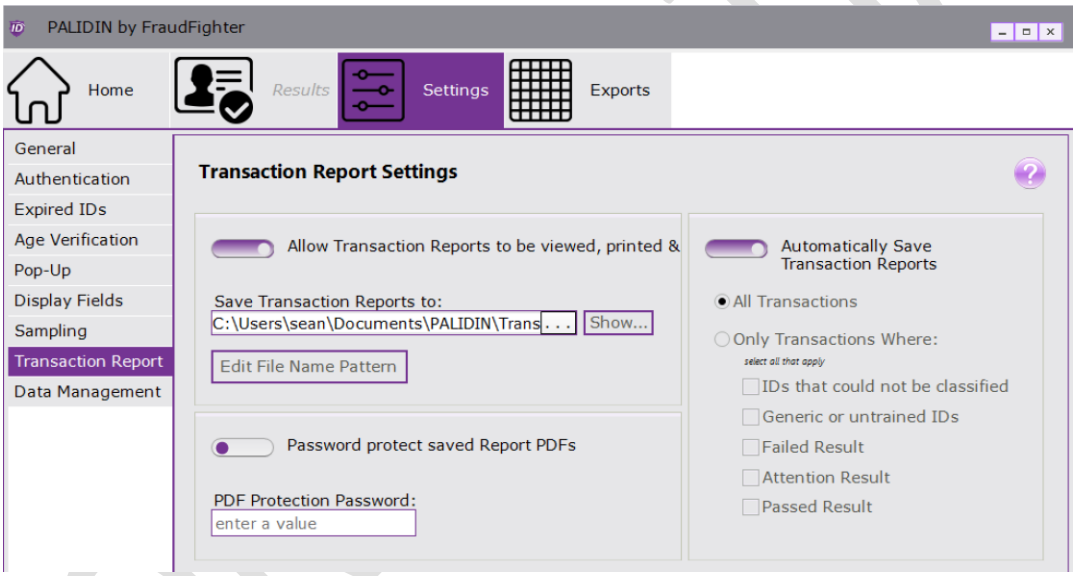


Figure 22 - Transaction Reports Settings

4.4.9 – Data Management

The second method to maintain a record of the transaction is to save the historical data only (without images). The system maintains a local database of each transaction and saves the information defined by the user.

To enable the recording and storing of the historical data, follow these steps:

- Select the desire option’s button. There are three options:
  - No Information – the system will not store any information, at all.
  - Status Only, no Identifiers – the system will save general transaction information only, to include: result, issuing state name/code, document class name, etc.

- Full Details – the system will save all information collected from the document, to include: surname, first name, middle name, address, birth date, etc.

<u>Note:</u> the system uses the current settings for storing the historical data. If you had the save "full details" selected last week, but this week you changed it to "status only," the system will export the transaction information according to the settings at the time of the transaction.

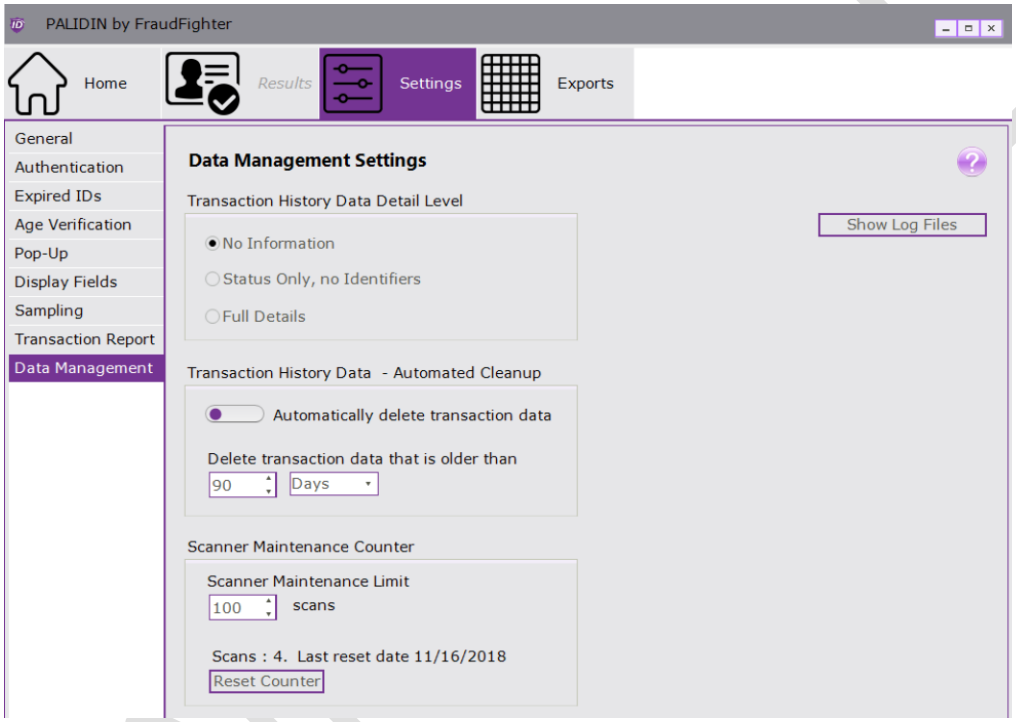


Figure 23 – Data Management Settings

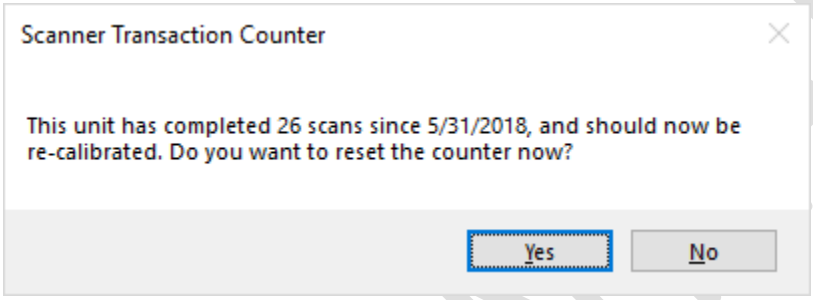
To set the time parameter that historical data will be stored, follow these steps:

- Click the toggle switch for "Automatically delete transaction data"
- Select the desired timeline in days, weeks, months or years.
- If you want to store the transaction data indefinitely, leave this feature disabled.

To set a reminder to clean your scanner, follow these steps:

- Under the "scanner maintenance counter" section, select or type the desired threshold for the reminder.
  - For the ID150 scanner, the manufacturer recommends to clean the scanner every 10,000 scans or once per month.
  - The minimum number of scans the system will accept is 100 scans.

  - You should adjust this setting to your particular environment. For instance, if you consistently scan dirty documents, the dirt will transfer to the rollers and this may affect the device's ability to scan the document properly.
- When the system reaches the threshold parameter, it will display the following message. If you click "yes", the counter will reset. If you click "no" the system will continue the prior scan count. If you are not ready to click "yes" when this message comes up, click "no," then clean your device. Once the scanner is cleaned, you can come to the data management page and click the "reset counter" option.



Note: Only click "yes" when you have cleaned the scanner. Resetting the counter implies that the scanner has been cleaned.

To locate the log files, follow these steps:

- Click "show log files" and the system will open a folder with debug, error and other info logs.
- From time to time, our customer support team may request these files in order to further assist you in troubleshooting a problem.

4.5 – Exports

See figure 23. The system will allow you to export historical transaction data in three formats: CSV (which can be opened with Excel), XML, and JSON. You'll have the ability to save multiple "templates" for exporting the data. Please note that in order for this feature to work, you need to save at least the "status only" information from the transaction.

To save a new export template, follow these steps:

- Click the "new template" button
- Type the desired template name in the "name" field
- Select the desired data format (CSV, XML or JSON)
- Select the desired folder location by clicking the "…" button and navigating the "browse for folder" window.
  - Make sure the folder has been to set to allow the system to "write" to it otherwise the system won't be able to save the sample reports to the folder.
  - Templates don't need to be saved to the same location. You have the option to save each template to a different folder location.

- Now, it's time to select the different data points to include in the export file. Click the desired field under the "Include Fields" section (left box) then click the ">" button. This will move the field to the box on the right. Continue to move fields from the left box to the right box as needed.
    - If you select a field by mistake, you can move it back by selecting the field on the box to the right then clicking the "<" button.
    - Only fields on the box to the right will be used in the export.
- If you have a specific order to display the data, on the box to the right, select the desired field, then click the "▲/▼" until the field is in the desired location.
- Select whether you want to export data from all transactions or for specific transactions only (e.g. failed, passed, etc.).
- Once you have selection all of your desired parameters, click the "Save Template" button.
- A window will open up letting you know the template was saved. Click "Ok."

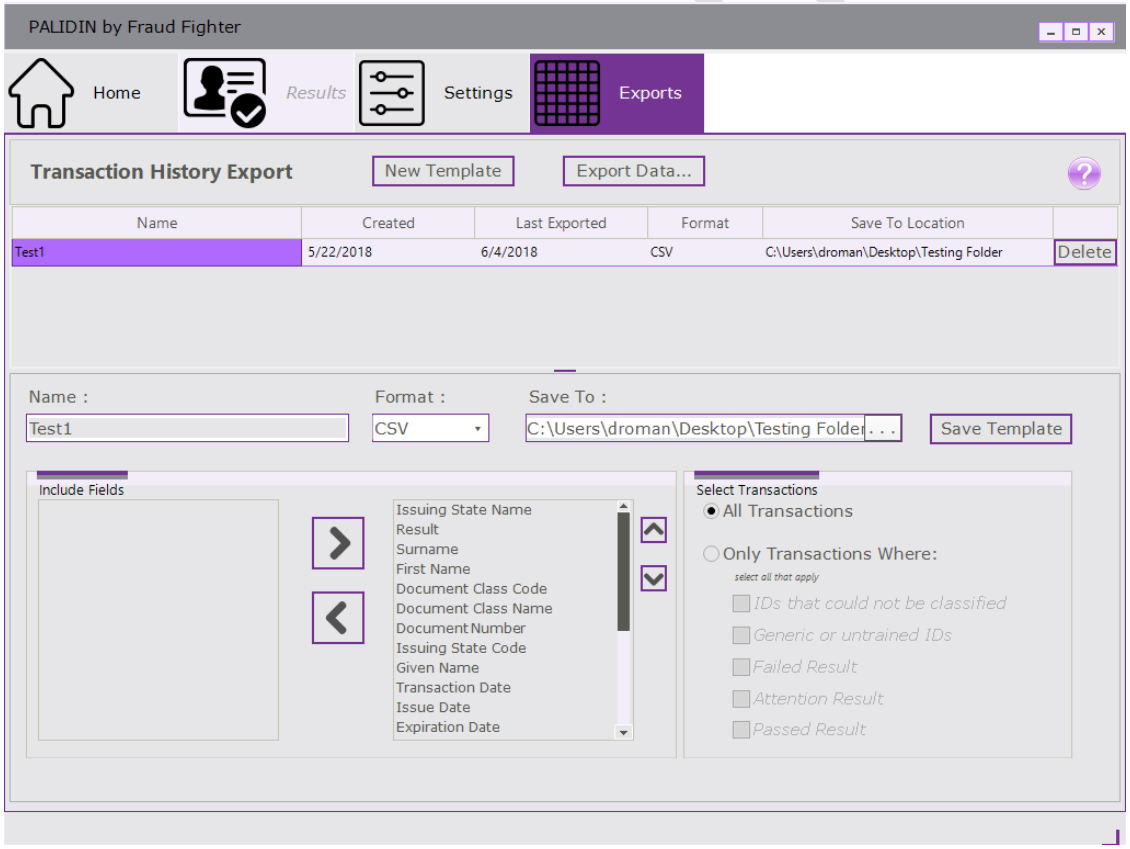


Figure 24 - Export Options

To export data, follow these steps:

- Click the “Export Data” button
- Using the drop-down menu option, select which template to use (this is at the top of the window “Export data using template:”)
- Select a date range or export data “since last export”
- Click the “export data” button
- A window will open up letting you the export was completed and that it includes “x” number of rows + the folder location that it saved to. Click “Ok”
- You can click on the “show” option in order to get to the folder location to open the file.

To edit a template, follow these steps:

- From the list of available export templates, select the desired template.
- Make the necessary changes then click the “Save Template” button.

To delete a template, follow these steps:

- From the list of available export templates, select the desired template.
- Click the “Delete” button, the system will ask you to confirm that you want to delete the template, click “Yes”
- A window will open up letting you know the template was deleted. Click “Ok”

5 - Scanner Maintenance

5.1 - Cleaning Schedule

Regularly scheduled cleaning of the scanner is recommended to ensure that the device feeds documents smoothly and delivers good quality images. The following components require cleaning according to the specified maintenance schedule:

Component	Recommended Maintenance Interval
Feed Rollers	10,000 scans or once per month
CIS	10,000 scans or once per month
Magnetic Stripe Reader (ID-150 only)	10,000 scans or once per month
Document Sensors	As required

Figure 25 - Cleaning Schedule

The instructions for cleaning these components are described separately for clarity. In general, it is recommended to clean all of the components that require cleaning at one time.

5.2 - Cleaning the Feed Rollers

Over time, the feed rollers in the scanner will accumulate dirt from the documents being scanned, necessitating that they be cleaned regularly, see figure 24. When dirty, the feed rollers have a greater tendency to slip, misfeed, or jam, resulting in poor quality images.

To clean the feed rollers, an alcohol or water-based solution should be used. "Card Reader Cleaning Cards, CR80," notebook screen cleaning wipes, or alcohol prep wipes/swabs are recommended, as long as they are water or alcohol-based.

Note: Do NOT use an ammonia-based cleaner.

There are a series of DIP switches on the rear of the scanner. By default, all ID-1xx scanners are shipped with their service DIP switches set to the OFF (UP) position. DIP switch #3 will put the rollers into a repetitive back and forth spin mode that is useful for cleaning the rollers.

Figure 26 - Cleaning the feed rollers

To clean the feed rollers, follow the steps below:

1. Power off the scanner.
2. Lift the cover to expose the feed rollers.
3. Carefully modify DIP switch #3, moving it to the ON position (to the DOWN position).
4. Power on the scanner. The rollers should begin moving back and forth.
5. Using a cleaning wipe or alcohol prep, hold it against the roller, cleaning them as they spin. Discard the prep/wipe when done (do not use it to clean another component).
6. Power off the scanner.
7. Carefully restore DIP switch #3 to its default setting of OFF (UP).
8. Close the cover.

5.3 - Cleaning the CMOS Image Sensor (CIS)

If irregular stripe patterns or artifacts appear in the scanned images, the CIS (CMOS image sensor) may be dirty. In this case, the CIS should be cleaned to ensure the scanned images are of good quality. The CIS can be accessed by opening the scanner.

To clean the CIS, an alcohol and/or water-based solution should be used. "Card Reader Cleaning Cards, CR80," notebook screen cleaning wipes, or alcohol prep wipes/swabs are recommended, as long as they are water or alcohol-based.

Note: Do NOT use an ammonia-based cleaner.

Figure 27 - Cleaning the CIS

To clean the CIS, follow the steps below:

1. Power off the scanner.
2. Lift the cover to expose the CIS.
3. Using a cleaning wipe or alcohol prep, clean the CIS (scan head) bars then discard the wipe when done. There are two CIS bars on the ID-150.
4. Close the cover.

5.4 - Cleaning the Magnetic Stripe Reader

Over time, the magnetic stripe reader will require cleaning to remove buildup and to ensure proper operation and accurate reads of magnetic stripes.

To clean the magnetic stripe reader, follow these steps:

1. Power off the scanner.
2. Lift the cover to expose the magnetic stripe reader.
3. Using a cleaning wipe or alcohol prep, clean the magnetic stripe reader.
4. Discard the wipe when done.
5. Close the cover.

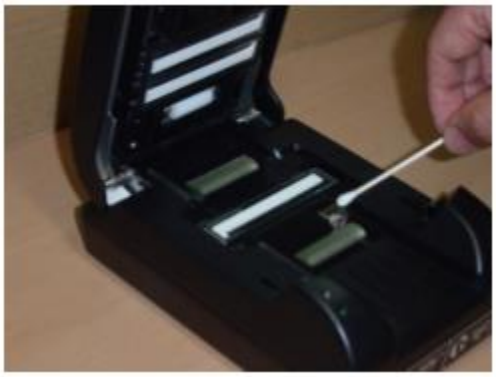


Figure 28 - Cleaning the magnetic stripe reader

5.5 - Cleaning the Document Sensors

The document sensors are utilized to detect the presence of a document in the feed path. They are visible when the scanner is opened as small holes before and after the first roller on both the top and bottom surfaces. There are two pairs of sensors, the first pair (top/bottom) is before the first feed roller, and the second pair (top/bottom) is immediately after the first feed roller. Documents are detected by breaking the light path between the two sensors.

Dust or dirt may collect in these holes over time resulting in the scanner not properly detecting when a document is present. To avoid issues, these sensors should be cleaned to ensure the sensor path is free of dirt.

To clean the document sensors, follow these steps:

1. Power off the scanner.
2. Lift the cover to expose the document sensors.
3. Using compressed air or an air gun, blow air into the document sensor holes to remove any dust or dirt buildup. When using a compressed air can, ensure that it remains upright to avoid getting any residue on the CIS.
4. Close the cover.

6 - RevealID Application Troubleshooting

6.1 - AssureID icon has an "x" on it

This means the service has stopped and needs to be restarted. From your system tray, right-click on the AssureID "A" icon, select the "start service" option. Once the "x" goes away, this means the service has started and you should be able to use the RevealID application again.

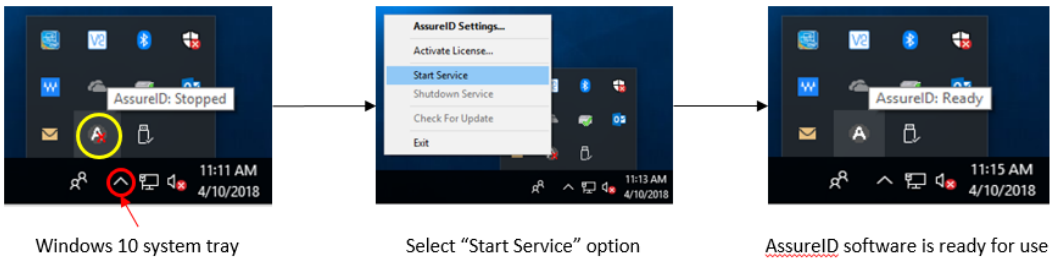


Figure 29 - AssureID state

6.2 - How do I check the current version of my drivers, software, and document library?

To check the current version of your drivers, software, and document library; follow these steps:

1. Navigate to your control panel screen then select the programs and features option
2. Sort the programs by "publisher"
3. You should see the AssureID Sentinel, AssureID Document Library, and i-Dentify Document Reader Driver programs.
4. To the far right of the screen, you will see a column for "version." This column will list the current version of the different programs, see figure 28.

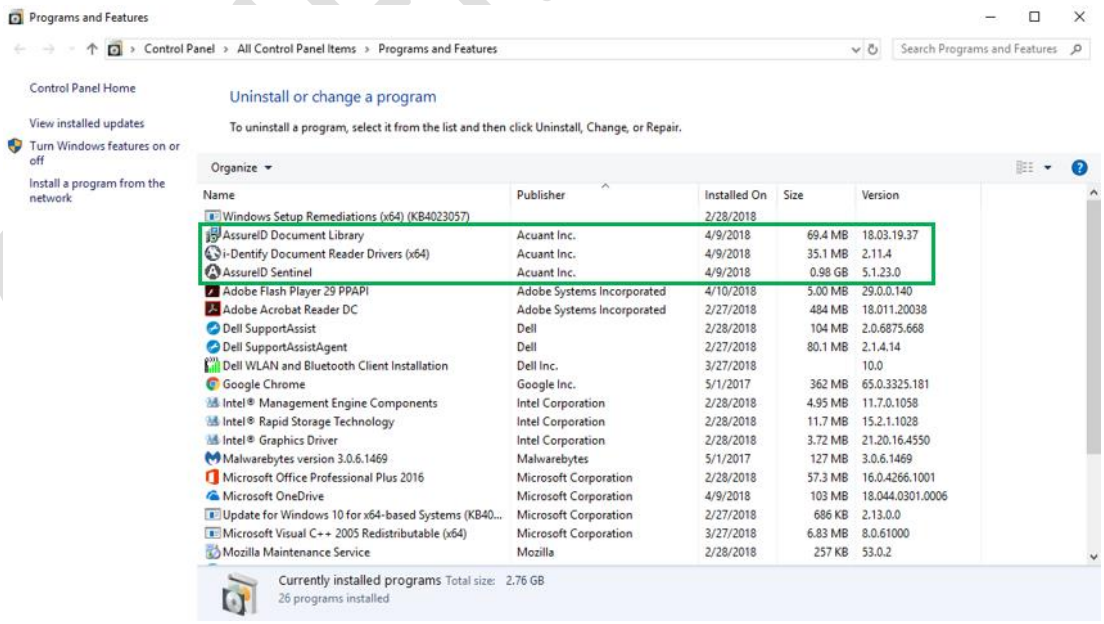


Figure 30 - Checking the current versions of drivers, software and document library

To check the version of your software and document library only, follow these steps:

1. From the PALIDIN home screen, look at the bottom left corner of the window. This section will display the version of the AssureID software, AssureID Document Library, and PALIDIN application.
2. Similarly, you can follow these steps:
    a. From your system tray, right-click on the AssureID "A" icon, select the "AssureID Settings" option
    b. Click on the "About" tab
    c. This page will list the version for engine (i.e. AssureID software) and the document library.

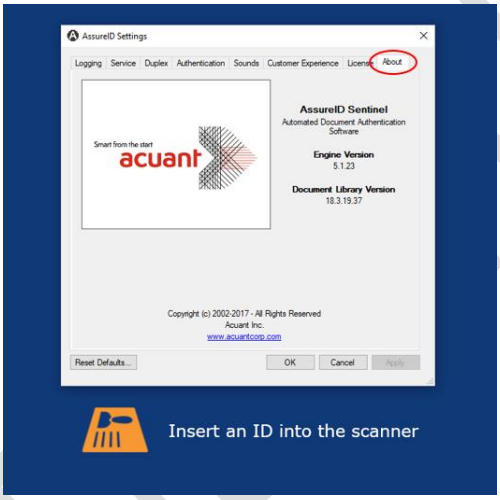


Figure 31 - Checking the current version of software and document library (only) in AssureID

6.3 – "No scanner detected" message

When the home screen displays the "no scanner detected" message, it means the application does not recognize there's a scanner connected to the computer. The scanner will have a blinking red light on LED1. Check the USB cable to make sure it is properly plugged on both the scanner and the computer. Once the application recognizes the scanner is connected (this may take a few minutes), the LED1 indicator will go back to its normal state (i.e. solid yellow) and the home screen will display the "scanner status: online" message.

You can also check the status of AssureID, from time to time, the AssureID software may stop working and may need to be restarted. See section 6.1 for details.

6.4 – Manually activating a license key

Whenever a computer device is not connected to the internet (most likely because the computer is part of a protected network system), you may need to manually activate the license key. To manually activate the license key, follow these steps:

1. Click Start > All Programs > AssureID > Tools > AssureID License Activation. The AssureID License Activator application window opens.
2. Enter the valid 26 alpha-numeric license key in the License Key text box.
3. For Activation Method, select Manual (Advanced).
4. Select the Create a license activation request file option.
5. Click Activate License.
6. An activation request file is created for the installed system. You will be prompted to specify a folder and file name for saving the activation request file. After the activation request file has been saved, you must include the generated activation request file as an attachment to an email and send that email to licensing@assuretec.com; CC: droman@uveritech.com
    a. Note: Manual license activation requires you to email the activation request file as an attachment to licensing@assuretec.com. The process of emailing the license request file to Acuant is not automatic.
7. After the activation request file has been received at Acuant, you will receive an email response that contains an activated license file. Activation requests via email are generally processed quickly and you should receive a response within 15 minutes. If you do not receive an email response within 24 hours, please contact FraudFighter so we can follow-up for you.
    a. Note: After you receive the email from Acuant that includes the activated license file, install the activated license file onto the exact system from which the request was generated.
8. Click Start > All Programs > AssureID > Tools > AssureID License Activation. The AssureID License Activator application window opens.
9. Enter the valid 26 alpha-numeric license key in the License Key text box.
10. For Activation Method, select Manual (Advanced) and select the Install an activated license file option.
11. Click Activate License.
12. At the prompt, browse to and select the activated license file received from Acuant and click Open. When the license is successfully activated, the License Activation application will display a confirmation and all software features authorized by the license will be enabled.

6.5 - Activating a license key using a local license server

If a direct Internet connection is not available from the computer where AssureID is installed, it is possible to activate via a locally-installed AssureID License Server, which acts as a proxy to connect to Acuant's centrally-hosted license activation server.

An AssureID License Server must be installed and accessible on the local network to activate AssureID using this method. For details on installing and configuring the AssureID License Server, please contact our FraudFighter support team.

6.6 - Moving software to another computer device

Whenever you need to move the software to another computer device, you'll need to deactivate the license on the current device then activate it on the new device. To complete this process, follow these steps:

1. Click Start > All Programs > AssureID > Tools > AssureID License Activation
2. Click Deactivate License.
3. Install the software on the new computer, the system will prompt you to enter the license key. Continue the installation process as normal.
4. You can also complete this process by going to: system tray, right-click on the AssureID "A" icon, select the "Activate License," then click "Deactivate License."

6.7 - Common license activation errors

6.7.1 - CodeReuseBlocked

There are no available seats on the license key. When you activate the software on a computer, a seat on the key is reserved by that computer. If you are moving the software to a new/replacement computer, you will first need to deactivate the prior computer that was using the license (see section 6.6). Also, if you have upgraded the operating system or reimaged the computer, it will be identified as a new computer on the licensing manager system. In this case, the seat will need to be deactivated from the old computer to free the seat.

There is a capability which allows you to perform a "self-deactivation." The only other requirement is that your computer can connect to the internet to reach the Acuant license server. When you launch the Activation tool, you will see one button for Activate License and another for Deactivate License. If you select to deactivate the license, it will release the computer from the license server and the seat on the license key will be available. You can then use the license key on the replacement computer and perform the activation.

6.7.2 – No License Servers

An Internet connection is required in order to activate a software license. This error message means the computer can't access the external internet. Start by checking two things:

1. Make sure you are logged-in as a full admin-right user when trying to activate the software license key.
2. Open your internet browser and try to load a website (any website like www.goggle.com). If you can access the internet continue to step a; if you cannot access the internet, continue to step b.
    a. Check to see if the computer can contact the license server. In your internet browser, copy and paste the following URL: http://licensing.assuretec.com/LicenseServer/Activator.asmx, you should receive a message that says "This web service is not open to the public." This means the computer is able to contact the license server. Try activating the license key one more time.

b. If you cannot access the internet, this means your IT department has the computer on lock-down and you'll need to follow the steps listed in section 6.4: manually activating a license key.

6.8 – Locating Installation & Activation Logs

At times, we may ask that you submit AssureID logs in order to assist in the troubleshooting of software installation problems. The logs can be found in the following locations:

- In the C:\ drive, you will find two logs "AssureID_Sentinel_Install" and "i-Dentify_Drivers_Install"
- In C:\Users\Public\Documents\My AssureID Data\logs, you will find a file called "AssureTec.AssureID.LicenseActivator"

6.9 – I need FraudFighter to double check the authenticity of a document for me

If you need us to double check the result of a particular document, we're more than happy to do so. However, in order for us to review the document and its authentication tests in detail, you need to submit a .sample file (this is different from the transaction report PDF file). A sample file is a collection of data and images in a proprietary format that allows us to review the document in detail.

You can set PALIDIN to either allow a user to manually save a sample file or set it to automatically collect sample files for you. To enable the sample collection, follow these steps:

- To give users the ability to manually save a .sample file, follow these steps:
  - From the home screen, go to Settings>Sampling
  - Enable the "Allow ID samples to be saved" option
  - Select the desired folder location by clicking the button with the three dots (can be a networked folder) or use the default location.
  - The "show" button will open up the folder so you can view the sample files.
  - When a document is scanned, the system will give the user the option to "save sample" under the "inspection result actions" dropdown menu.
- To automatically save a .sample file, follow these steps:
  - From the home screen, go to Settings>Sampling
  - Enable the "automatically collect ID samples" option
  - You can save a .sample file for all transaction or only certain transactions.
  - Select the desired folder location by clicking the button with the three dots (can be a networked folder) or use the default location.
  - The "show" button will open up the folder so you can view the sample files.
  - When a document is scanned, the system will automatically save the sample file.

6.10 – My state released a new document design and I get an "unknown" result

If a document design is not supported by the existing document library, an authentication template needs to be created for the new design. In order for the software company to create a template, you'll need to provide a .sample file of the document. A sample file is a collection of data and images in a proprietary format that allows the software company to review the design elements in detail in order to

create the template and add it to the document library. From the time a document design is released, it may take 3-6 weeks to be added to the document library.

For instructions on how to enable the collection of sample files, refer to section 6.9 above.

6.11 – How do I navigate the software update page?

The PALIDIN software update page is intended to be used as a flowchart that guides you through which specific software component you need to update. The software update page is located here: https://www.fraudfighter.com/software-update

The flowchart asks 2 main questions:

1. Are you installing AssureID for the first time on a computer? If the answer is yes, you'll need to install 4 software programs (i-Dentify driver, AssureID Sentinel, Document Library, and PALIDIN). You'll be re-directed to a step-by-step guide on how to install the software components.
    a. If the answer is no, and you have already installed the system, move to question #2.
2. Do you have an older version of AssureID Sentinel? If yes, you'll need to install 2 software programs (newer version of AssureID, and Document Library). You'll be re-directed to a step-by-step guide on how to install the software components.
    a. If the answer is no and you already have the current version, move to step# 3.
3. If you only need to update the document library file, click the "Click here to update your Document Library" box and you'll be re-directed to a step-by-step guide on how to install the new document library file.

Note: *The PALIDIN application includes an auto-update utility that will inform you whenever a new version of the application is available. A message will appear in the bottom left corner of the home screen and it will prompt you to update the application. Accept and install the update. You will need to close and restart PALIDIN in order for the changes to go into effect.*

6.12 – Same document returns different results

There is the possibility that the same document will return different results (when scanned in two different scanners/systems). In this case, the issue could be software or hardware. Let's explore both options:

- Software: the document template may need be modified in order to account for slight variations in image capture/cropping.
- Hardware: it's possible that one of the scanners is not working properly (i.e. not capturing image properly, magstripe reader not working, etc.).

Regardless of whether the issue is software or hardware, submitting a sample file of both transactions will provide us all the details that we need in order to confirm whether the root cause is software or hardware.

For instructions on how to enable the collection of sample files, refer to section 6.9 above.

6.13 – I know this is a good document but it gets a failed result

In cases in which a valid and legit document gets a fail result, it usually has to do with one of the following:

- The image captured by the scanner is not of good quality (hardware issue)
- The image was not cropped properly (hardware issue)
- The document is in very poor condition (e.g. document material is cracked, document laminate is peeling, inks have faded, etc.)

If the issue is due to scanner (hardware), the device can be sent back for repairs. If the document is in poor conditions, there's nothing that can be done in order for the system to return a different result. As a reminder, the system compares security features from the document to an existing template. If the images collected from the document show cracks, laminate peeling off, this will cause certain authentication tests to fail (or receive a caution result), in which case may result in an overall document fail result. If you need us to review a specific document result, please submit a .sample file.

For instructions on how to enable the collection of sample files, refer to section 6.9 above.

6.14 – My license expiration date is not correct

If you have activated your license key and the expiration date shown in the system is not correct, you can force the system to connect to the licensing manager server in order to pull the correct expiration date. To do this, follow these steps:

1. Open your file explorer window then navigate to the following location C:\ProgramData\AssureTec\AssureID.
    a. Note: the "program data" folder is usually hidden. You may need to enable the system to show hidden files. In the view options, there's a check box for "hidden files," make sure it is checked and you'll be able to see the program data folder.
2. In the "AssureID" folder, there's a file called "License.dlsc"
3. Delete the "license.dlsc" file by right-clicking on the file then choosing the delete option.
4. Go to the system tray, in the bottom right corner of the computer screen, right-click on the AssureID "A" icon then select the "Activate License" option
5. The license key should be listed already. Click the "activate license" button (if the computer is connected to the internet; otherwise, follow other activation procedures)
6. Once the activation is completed, you should see the message that says "The AssureID software has been activated. The maintenance on this license expires on <correct expiration date>."

6.15 – PALIDIN does not recognize that the scanner is connected (on a regular basis)

Depending on the computer performance (RAM, processor, etc.), the AssureID engine might stop working and disconnect from the scanner. Starting the AssureID engine again should establish a new connection to the scanner (see section 6.1 for instructions on how to re-start the engine).

More importantly, the computer device should be turned off (or restarted) at least once a week. This will ensure that unnecessary programs don't continue running in the background and cause the

computer's performance to decline (i.e. run out of RAM). This is particularly important if you are using the computer device to run other programs (like a POS system, CRM software, etc.)

If you are using a laptop or tablet device, it is important to ensure the device's display and sleep settings are set to "never" and that the "USB selective suspend setting" is disabled for both on battery and plugged in options. The steps required to change these settings will depend on the OS you are currently using. If you need any assistance checking these settings, please contact our support team.

6.16 - Error 1920 – Service AssureID Document Authentication Service failed to start.

Full message: Error 1920. Service AssureID Document Authentication Service (AssureID DAP Service) failed to start. Verify that you have sufficient privileges to start system services.

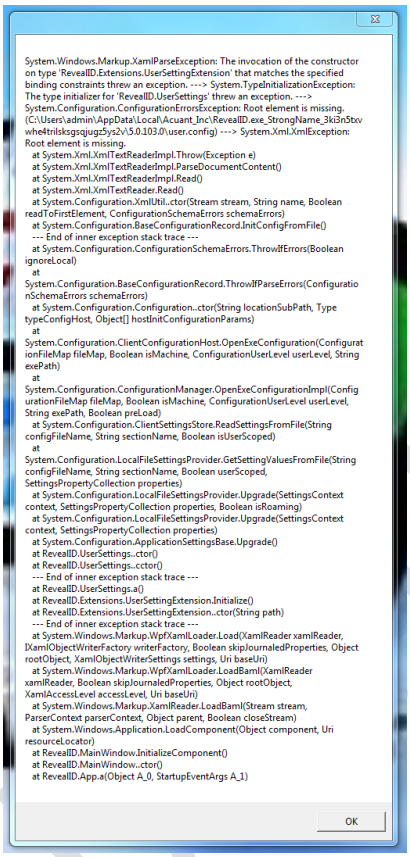
Generally speaking, this message comes up whenever a user has logged-in that doesn't have the sufficient privilege access (to certain system folders) in order to run AssureID.

6.17 – Error Message: "System.Windows.Markup.XamlParseException"

While upgrading the AssureID Sentinel software, you may encounter this error message. This error usually points to an issue with the "user.config" file. You can delete this file by following these steps:

1. Open your file explorer window then navigate to the following location C:\Users\<existing_Account>\AppData\Local\Acuant_Inc\RevealID.exe_StrongName_3ki3n5txvwhe4trilsksgsqjugz5ys2v\5.0.103.0
    a. Special Notes:
        i. The "existing account" refers to the user account logged-in to the computer
        ii. The "app data" folder is usually hidden. You may need to enable the system to show hidden files. In the view options, there's a check box for "hidden files," make sure it is checked and you'll be able to see the app data folder.
        iii. The "5.0.103.0" refers to the AssureID version. This folder name will match the AssureID version you have installed in your computer (e.g. 5.1.23, 5.1.10, etc.)
2. In the 5.0.103.0 folder you will see a file called "user.config"
3. Delete the "user.config" file by right-clicking on it then selecting the delete option.
4. After removing the file, restart the AssureID engine and open RevealID, the system should be functional now. The system will automatically generate a new version of the "user.config" file.

Here's an image of the full error message:



6.18 – Enabling “verbose details” logging and locating the DAPService log.

From time to time, we might request that you submit the DAPService log. This log contains information about each session that is initiated in the scanner (i.e. each document that is scanned).

To enable “verbose details,” which will allow our customer support team to view the details of the session, follow these steps:

- In the system tray, bottom right corner of your computer screen, right-click on the AssureID “A” icon
- Select “AssureID Settings…”
- In the Logging tab, locate the “filter” section. Check the “verbose details” box, then click “apply” then “OK”
- The system will start recording the verbose details.
- Scan a few documents as you would normally do in order for the system to record the session information.

To locate the DAPService log, follow these steps:

- In the system tray, bottom right corner of your computer screen, right-click on the AssureID “A” icon
- Select “AssureID Settings…”
- In the Logging tab, locate the “other” section, then click the “logs” button.
- This will open the folder where the logs are located.
- Sort the files by “date modified” to ensure you are looking at the newest files first (ascending order). You’ll be able to distinguish the different DAPService log files by the date and time they were last modified.

7 - i-Dentify ID-150 Scanner Troubleshooting

7.1 - Remove a jammed or stuck card

1. Lift the cover and slide the card out of the scanner.
2. After you remove the card, close the scanner cover and resume normal operations.

Figure 32 - Removing a jammed document from scanner

7.2 - LED1 is Blinking Red

This means the USB cable is not connected. Check the USB cable to make sure it is securely connected to both the scanner and computer. Once the scanner recognizes the USB interface, the LED1 light will go back to its normal stable yellow, which means the scanner is ready for use.

7.3 - LED1 is Solid Red

This means the scanner is in an "error state." Turn OFF the device then turn it back ON. The LED1 light should go back to its normal stable yellow, which means the scanner is ready for use.

7.4 - Scanner being recognized as "HP Printer" device

This usually happens whenever the scanner is connected to the computer before the i-Dentify software driver and AssureID Sentinel is installed. If the scanner does not get properly installed when connected to the computer, please follow these steps:

1. Power OFF the device and disconnect it from the computer
2. Go to Control Panel>Programs and Features
3. Uninstall the i-Dentify Document Reader Driver program
4. Go to Control Panel>Device Manager
5. Connect the scanner to the computer and power ON the device. Observe how the scanner is displayed in the device manager list. If it displays as "HP Printer," right-click on the entry then select "Uninstall" then check the "Delete the driver software for this device" box.
6. Power OFF the scanner and disconnect from the computer
7. Repeat step 4 & 5 until the device is unable to find a driver
8. Power OFF the scanner and disconnect from the computer
9. Install the i-Dentify Document Reader Driver then reboot the computer.
10. Once the reboot is complete, connect the scanner to the computer and power ON. In the lower right-hand corner of the computer screen you should see messages indicating the drivers are being installed and configured.

11. Open the PALIDIN application and you should see a message on the bottom right-corner of the home screen that says “Scanner Status: Online”

7.5 – Scanner does not power ON

In the event that the scanner does not power ON at all, follow these steps:

1. Plug the power cord to a different power outlet
2. Check the power cable for any damage, cuts, bents, etc.
3. Make sure the power cable is securely plugged into the back of the scanner
4. If you have a second scanner in your location, swap the scanners to see if the known “good” scanner turns on with the existing power cable. If it doesn’t turn ON, it means the power cable (or potentially power outlet) is not working. If it does turn ON, it means the scanner needs to be repaired.
5. Make sure all dip switches are set to the “up” position. Check the 3.3 – Rear Panel section, on page 8, for more details about dip switches.

If after all of these troubleshooting steps the scanner still doesn’t turn ON, it needs to be inspected by the manufacturer.

8 - Customer Support

8.1 - Contacting Customer Support

Our customer support team is available to answer any software or hardware questions you may have between normal business hours 7:00am to 5:00pm, U.S. Pacific Time, Monday through Friday. You can reach our support team by phone or email at:

- Phone: 800.883.8822
- Email: support@fraudfighter.com

We strongly recommend our customers to use the software and hardware troubleshooting steps provided in this document before calling our support team. This will aid in shortening the resolution time. If you decide that it is necessary to contact our support team, gather the following information before the call:

- An accurate, detailed description of the issue at hand.
- Version of AssureID, i-Dentify drivers, and Document Library in use.
- Workstation system specification (operating system, user security type, etc.)
- If the issue is regarding a scanner device, record and provide the model and serial number of the device.

8.2 - Software Warranty

With changes and updates constantly being made to documents such as driver's licenses and passports, it is imperative for FraudFighter customers to be using the most current version of the PALIDIN software and the AssureID Document Library. The original invoice date marks the start of a 12-month warranty period that can include software and Library updates and customer support, as well as access to special product updates and revisions. As your warranty period nears expiration, FraudFighter will contact you to renew these warranties. If renewed, you will receive an additional 12-months of these services; you may also choose to purchase additional years of renewals ahead of time. If you choose not to extend your software warranties, there is an increased risk for false positives (IDs that are flagged, but are authentic). In addition, running outdated versions of PALIDIN software and Document Library also jeopardizes your ability to classify new document types, as well as detect and stop counterfeit documents. Whenever you call us with a software question, please make sure you have the following information readily available:

1. PALIDIN version
2. AssureID version
3. AssureID Document Library version

8.2 - Hardware Warranty

There is a limited warranty that applies to all hardware supported by FraudFighter. From the initial invoice date, the purchase of a hardware device automatically comes with 12-months of hardware depot service. You will be responsible for paying one way shipping and FraudFighter will pay return shipping on repaired items. As your warranty period nears expiration, a FraudFighter sales

representative will contact you to renew these services for an additional year of coverage. Similar to software warranties, you may purchase multiple years of warranty coverage at any time during the warranty period, or at the time of your initial purchase. If you choose to forego hardware warranties, you will no longer be eligible to receive free repair services and you will be responsible for the repair cost of the scanner and/or replacement.

Whenever you call us with a hardware question, please make sure you have the following information readily available:

- Model number
- Serial number
- Date of Purchase (if available)

In the event that the issue cannot be resolved over the phone, we will process a returned merchandise authorization (RMA) number. Please be advised that we cannot accept product returns without a corresponding RMA number.

Units out of warranty can still be repaired but they will incur a $250 upfront examination fee (includes evaluation, cleaning, calibration and inspection labor). This fee cannot be waived and it is not refundable (if the unit cannot be repaired). Once a technician has examined the unit, a repair quote will be send to the customer. The manufacturer cannot perform any work on a scanner until the repair quote has been approved and paid. Customer has the right to decline the repair quote in which case the $250 examination final invoice will be processed and the unit will be returned to the customer.

Note: extended warranty options are available. Please contact your sales rep for more information.