PALIDIN Desktop Application
&
System Manual

PALIDIN User Manual - 2023

Table of Contents

Table of Contents

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 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 scanner drivers, authentication software, document library, and PALIDIN programs.

Please note the computer device should meet the following system requirements:

Component	Recommended
CPU: Intel Only	Intel Core i5 *(minimum 2 GHz)*
RAM	8GB
Disk Space	128GB
Operating System	Windows 10 Pro 64 bit or 11 Pro 64 bit

*NOTE: 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 result in older versions of the software being deleted or corrupted).*

3 - PALIDIN Application Guide

3.1 - 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.

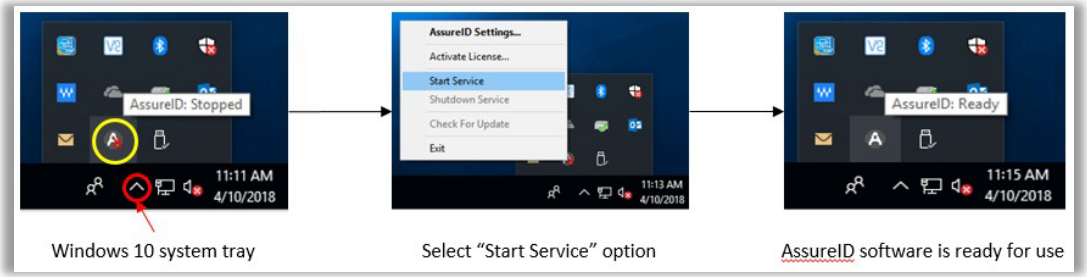


Figure 7 - AssureID status

3.2 - 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 may 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 *(see figure 8).*

As shown in figure 8, at the top of the screen you'll find the main navigation tabs: Home, Results, Support and Settings.

Figure 8 – PALIDIN Home Screen

3.3 - 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."

3.3.1 - 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 document library and is thus, unrecognized, or 2) that the forgery is of such low quality that it cannot be recognized.

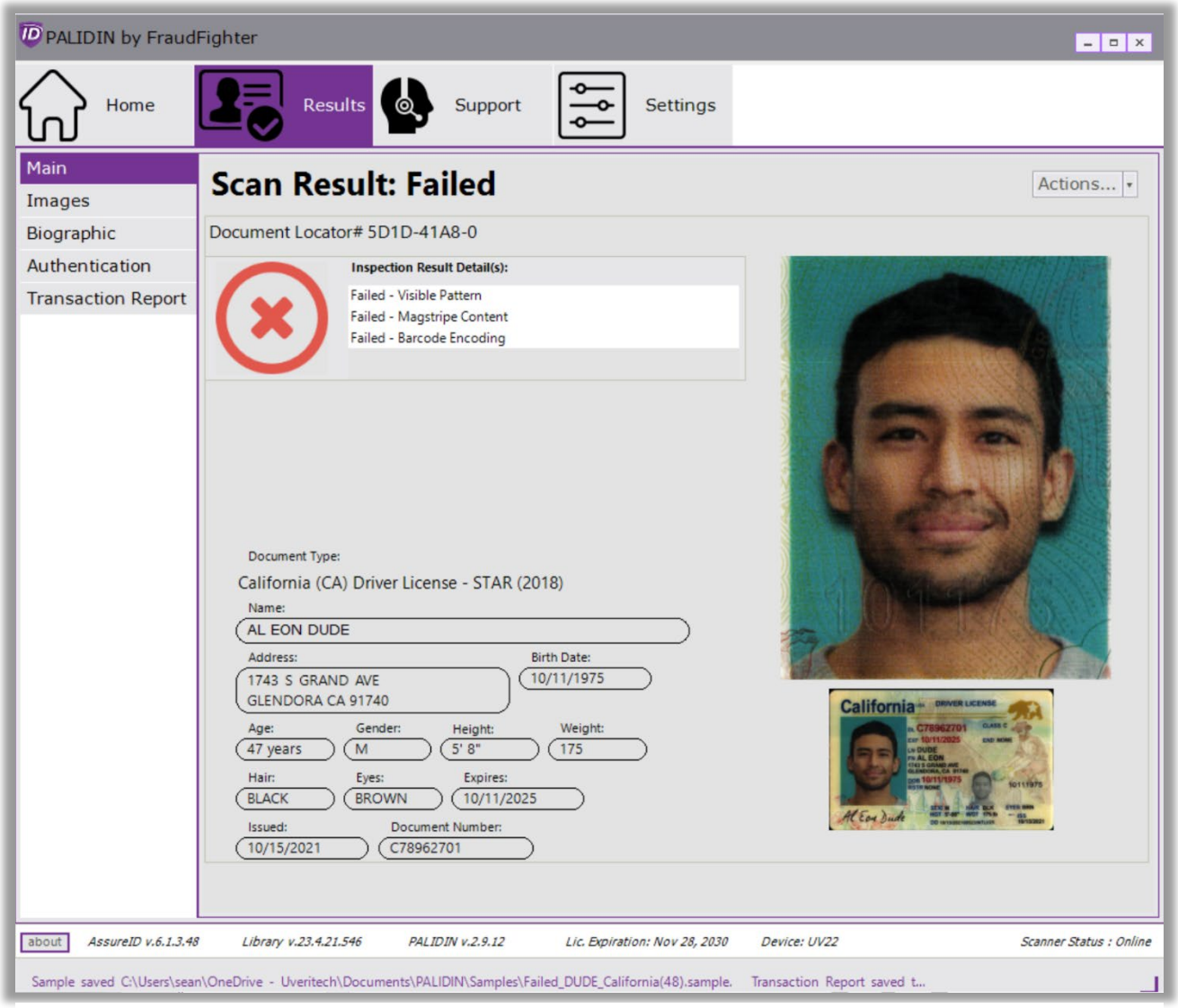


Figure 9 - Main Results Screen

3.3.2 - 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, additionally, see ultraviolet versions of both the front and the back of the document. 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.

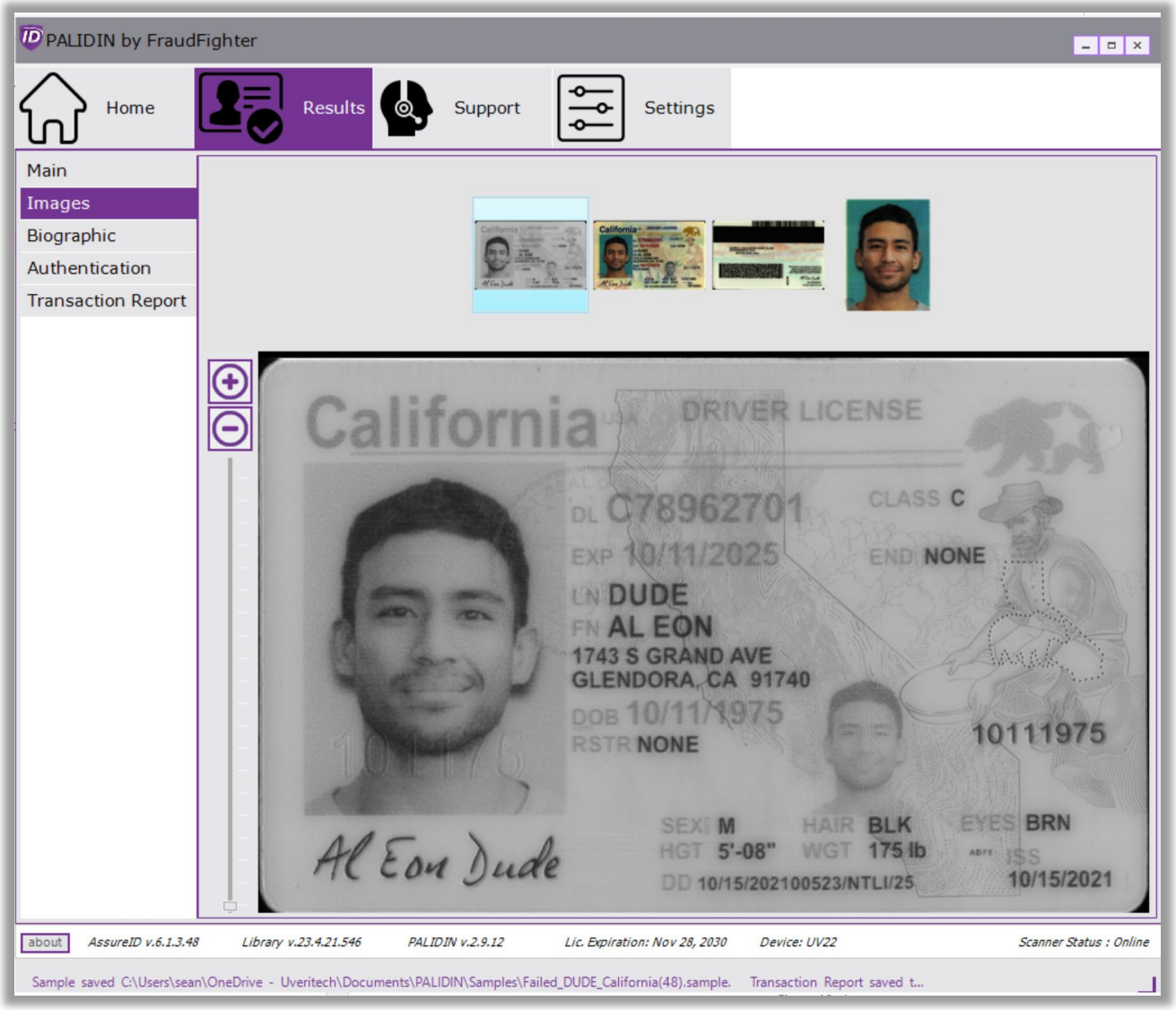


Figure 10 - Images screen

3.3.4 - 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).

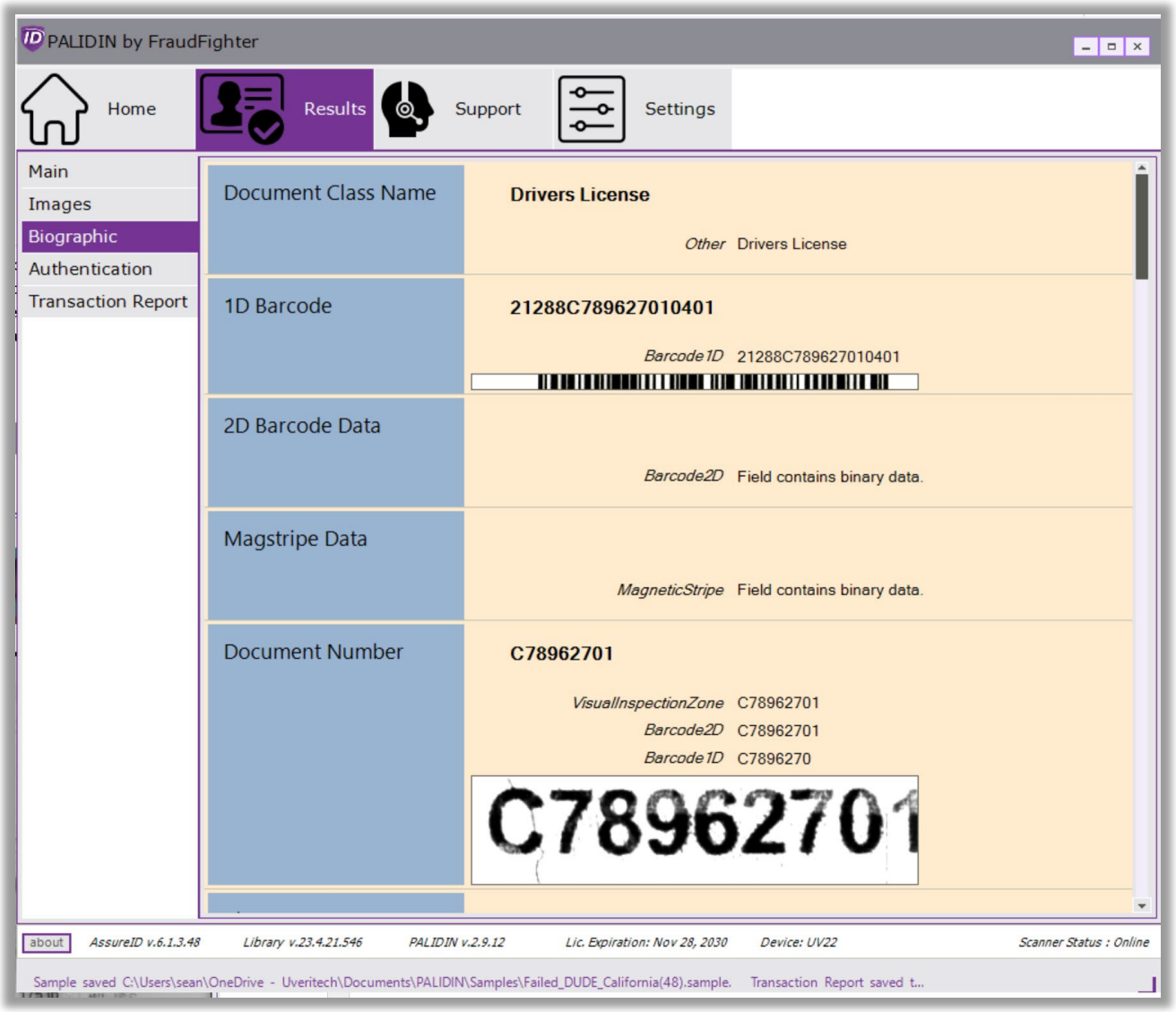


Figure 11 – Biometric Data Capture Screen

3.3.5 - 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).

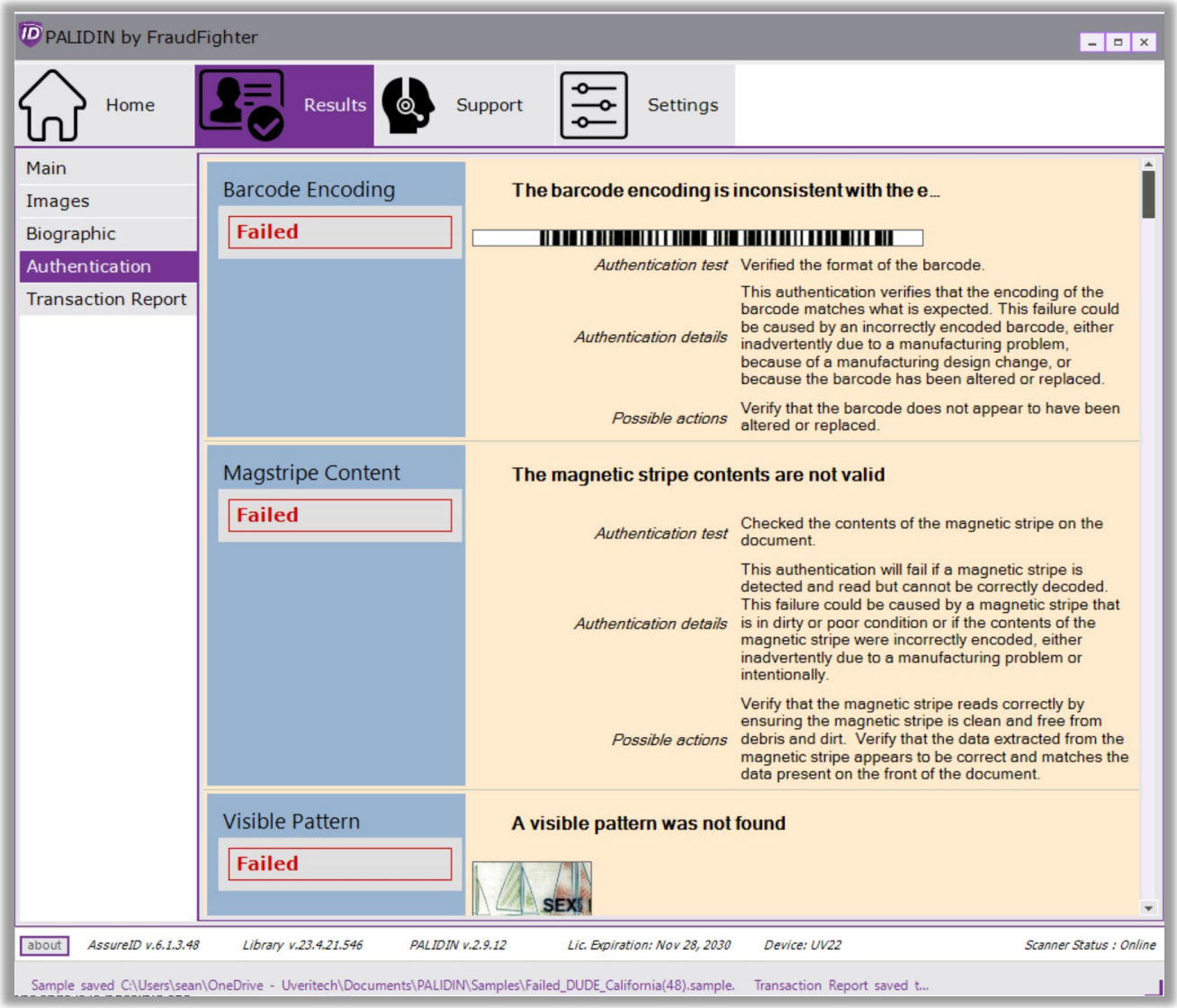


Figure 12 - Authentication Test Results screen

The authentication engine performs a weighted average on all the individual authentication test results 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.

3.3.6 - 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.

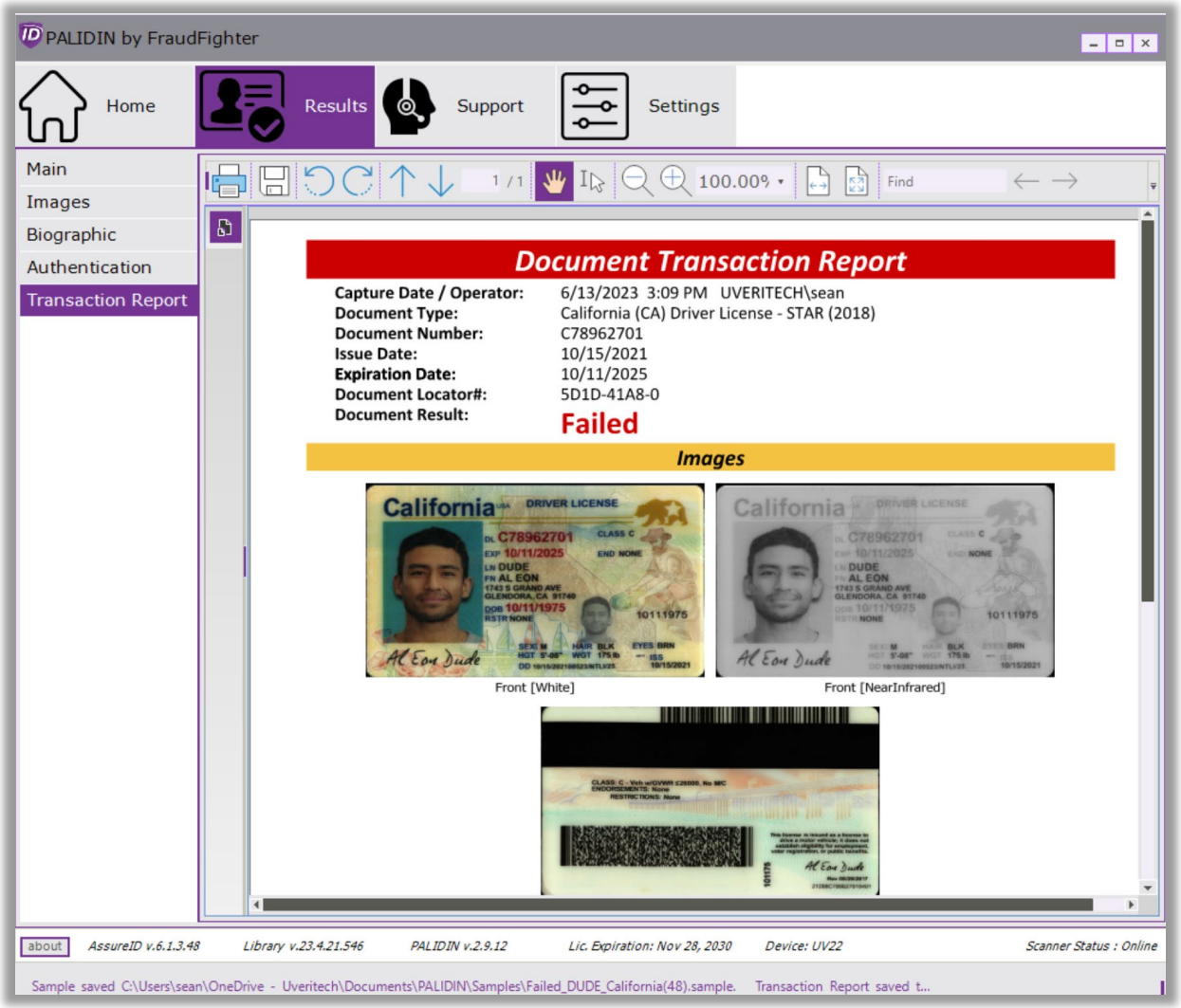


Figure 13 – Transaction Report screen

3.4 - Settings

There are multiple settings that can be enabled or disabled 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.
- Hovering your mouse over each setting component will display a "help" bubble with more information about the specific setting.

3.4.1 - 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 by 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.
- Military ID's legally may NOT have images saved, so this configuration setting is permanently disabled.
- Option to launch PALIDIN upon PC boot-up.
- Option to turn "on" automatic ("silent") updates.
- A counter that displays the number scans and which allows configuration of a scan-count threshold to trigger a maintenance warning or your scanning hardware.
- A button that will navigate the user to the folder where application log files may be found.

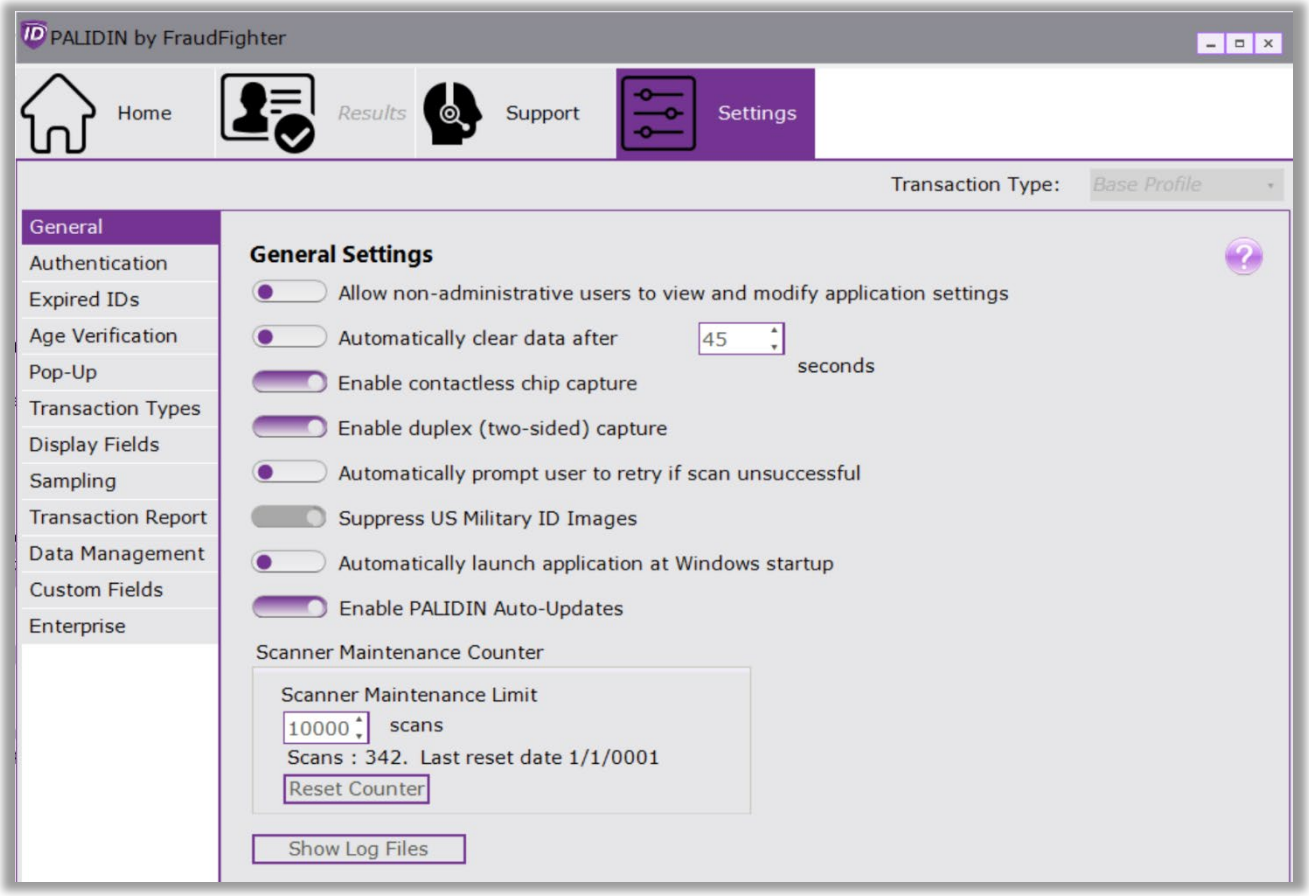


Figure 14 - General Settings

3.4.2 - 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 determine that it is authentic, however, 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 keeping 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.

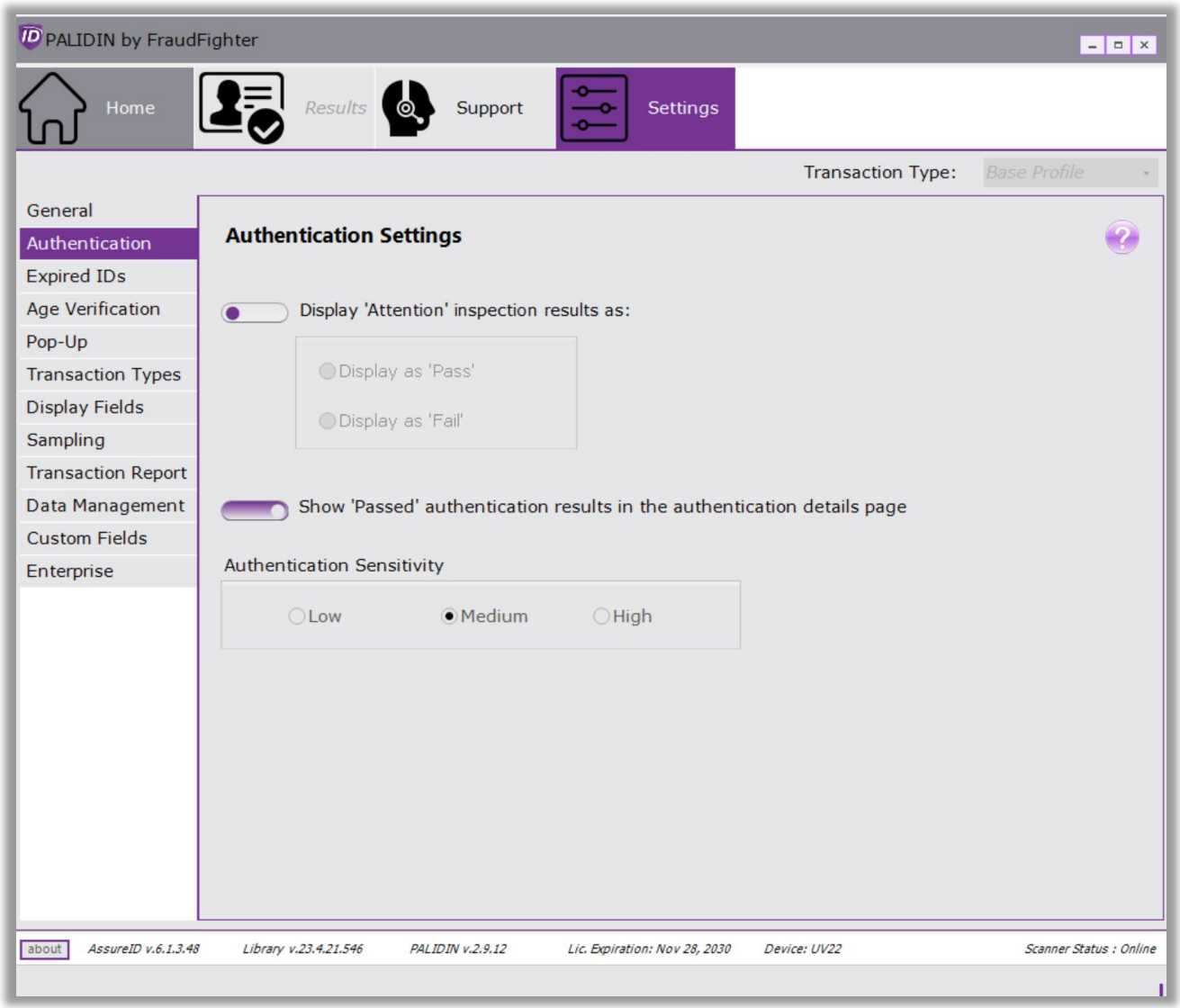


Figure 15 – Authentication Settings

3.4.3 - 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:

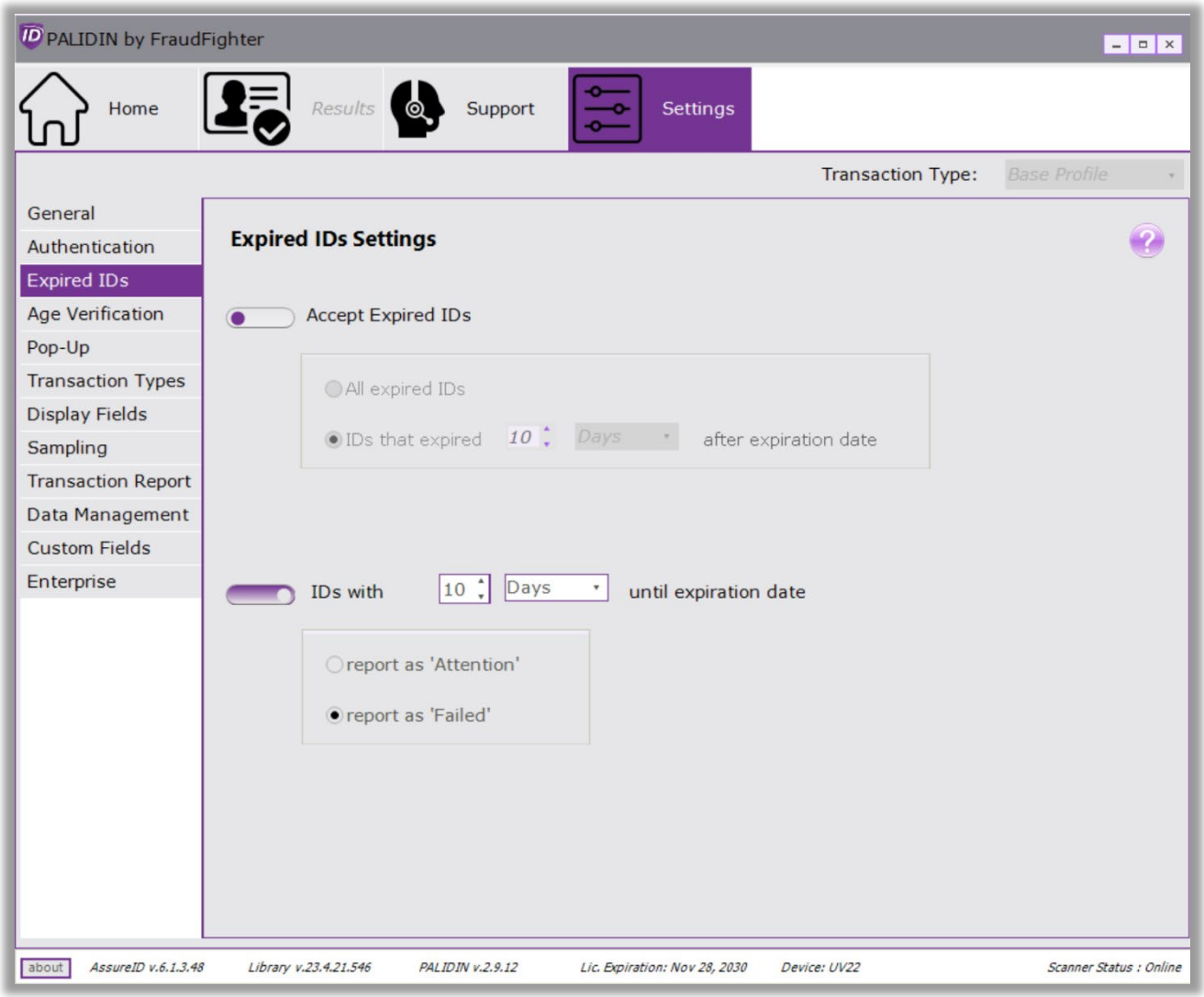


Figure 16 – Expired ID Settings

- 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 option 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.

3.4.4 - 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.

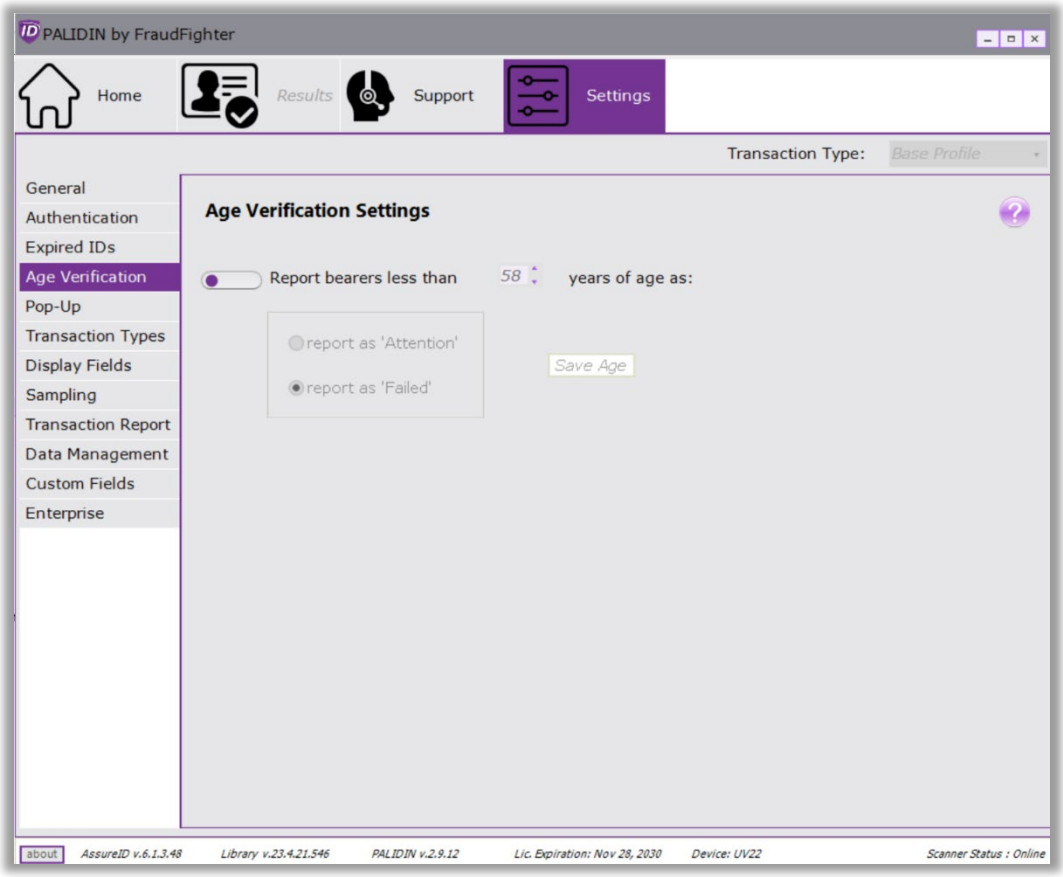


Figure 17 - Age Verification Setting

3.4.5 - 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.

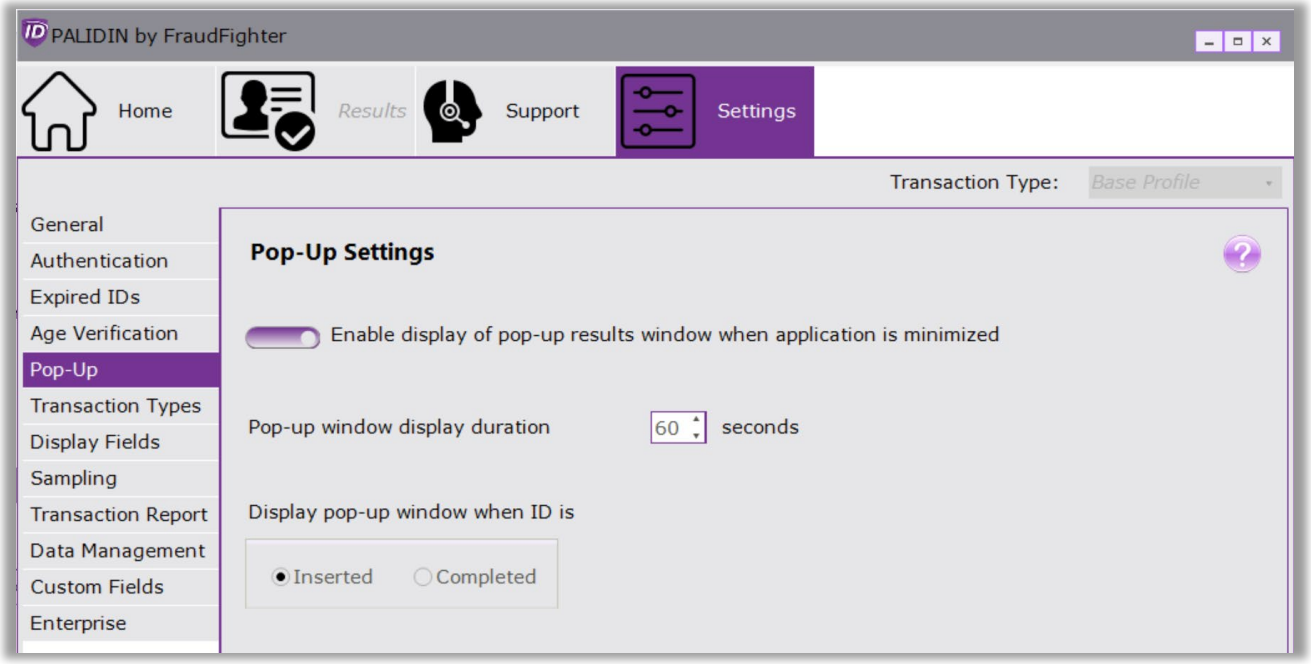


Figure 18 - Pop-up Settings

3.4.6 - Transaction Types

The Transaction Types function allows the user to create different types of transactions. When utilized, during document authentication process, the user will be prompted via a pop-up window to select the "type" of transaction being conducted. Depending on how you choose to configure the transaction type(s) this may require the user to enter/type data that will be directly associated to the transaction, and it can also cause different, unique sets of data and information to be displayed and/or stored from the transaction.

For example, an auto dealer may wish to scan a driver license prior to allowing a test drive of the vehicle. For this transaction, the company only wishes to store basic information including the name, date, time, location and document number along with the authentication result. So, the dealership could create transaction type: "TestDrive", and then configure the settings so that only the basic information with no PII is stored. See *figure 19*, which shows the screen where different transaction types can be created.

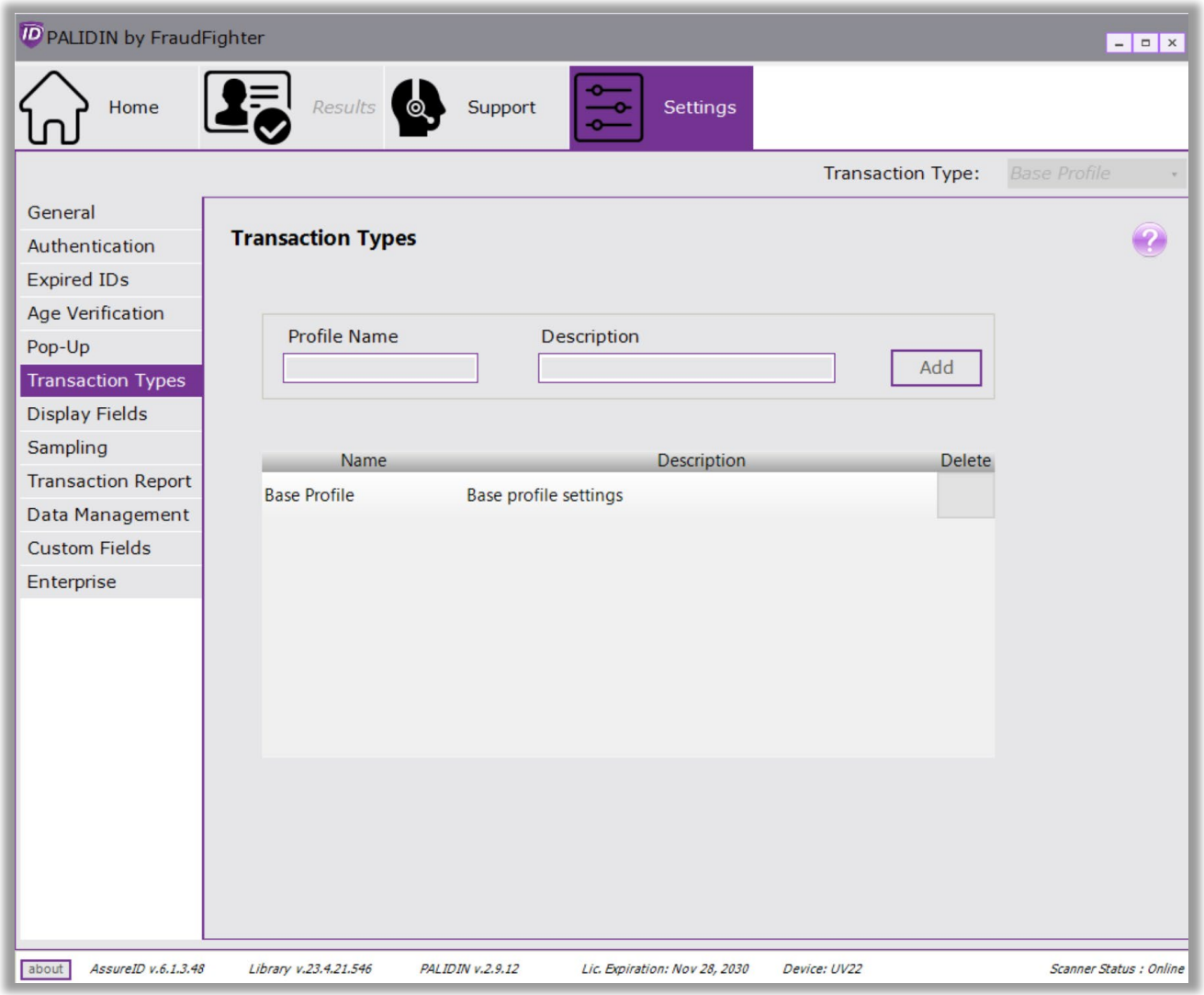


Figure 19 – transaction types screen

Later, the same customer may be ready to apply for financing. A second Document Authentication may be done at this time. Creating a "Finance Manager" transaction type, which would save a different set of data as may be required to satisfy finance department ID authentication record keeping requirements.

In section *3.4.8 -Display Fields*, we will discuss how the data saving protocols can be configured for different record types.

3.4.7 - PALIDIN Custom Field Feature

Organizations may at times need to associate a data point like a driver#, employee name, or employee# to a particular transaction. PALIDIN's custom field feature allows you to configure up to two custom fields, which are then associated with the record related to a specific identity document authentication transaction.

The custom field feature provides two setup options: (1) Validation, (2) Regular Expression. The validation option allows you to configure the custom field using common validation tests like field type, field length, support for special characters, etc. The Regular Expression (RegEx) option allows you to configure the custom field using more advanced validation processes.

Once the feature is enabled and configured, the user will be prompted to enter the data point and it will be associated with the historical record. The following screenshots summarize the process from setup, user prompt display, to displaying the custom field in the transaction report.

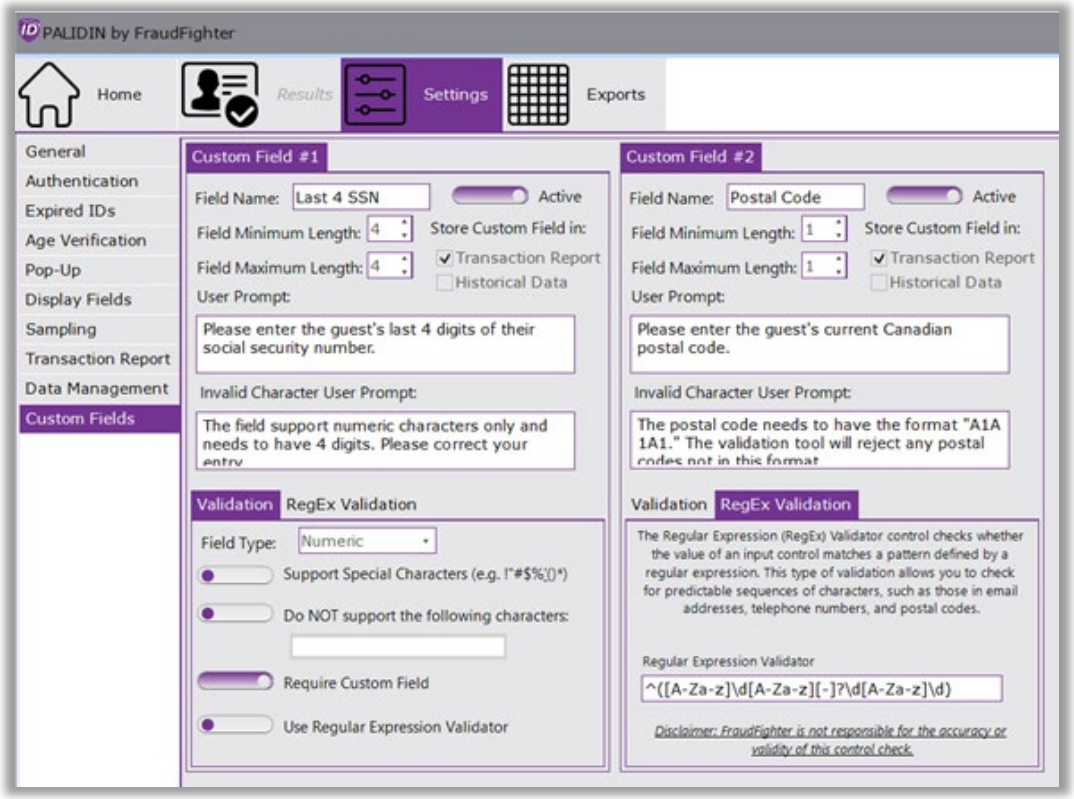


Figure 20 – Two custom fields setup in the PALIDIN app

In *figure 20*, "Custom Field #1" uses the validation approach and "Custom Field #2" uses the RegEx approach.

Figure 21 – custom field approach samples

User is presented with prompt to enter guest's last 4 digits of SSN and the current Canadian postal code.

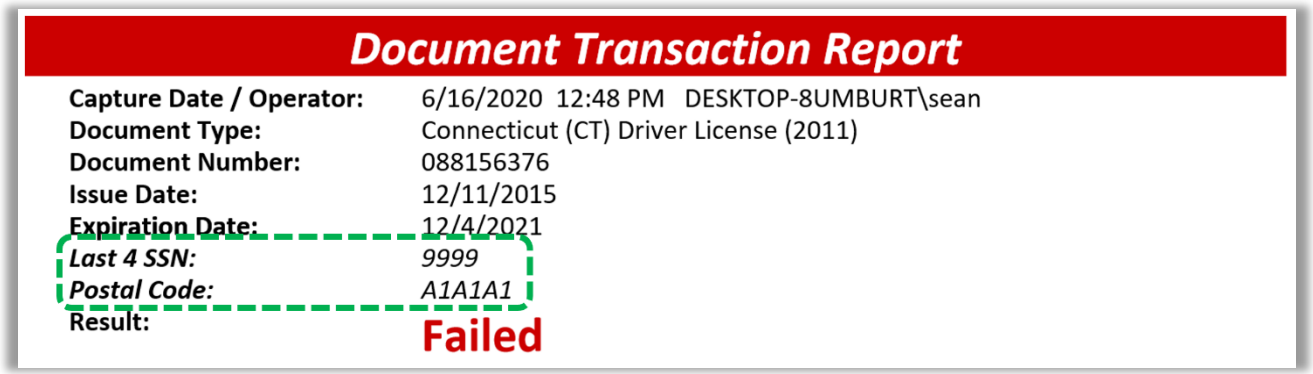


Figure 22 – Transaction Report displaying the two custom fields setup in the system.

3.4.8 - 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.

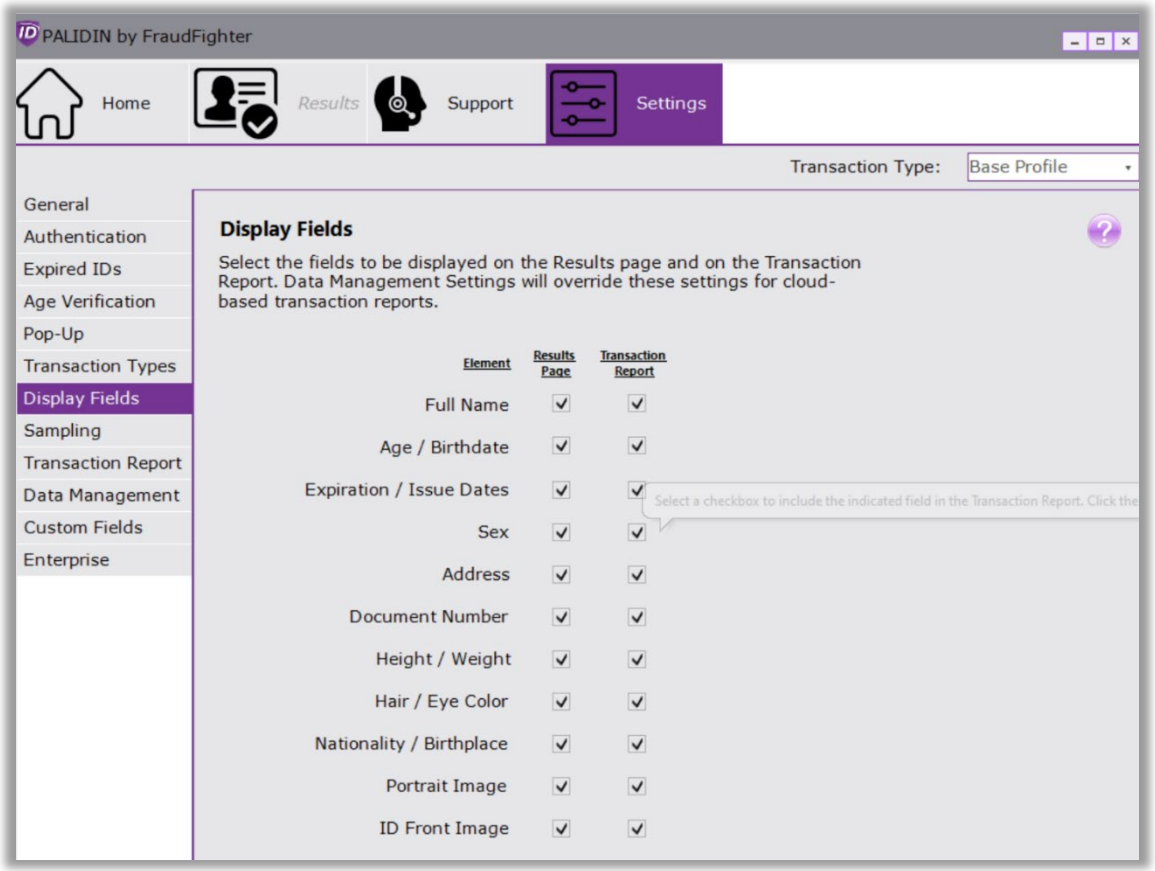


Figure 23 - Display Fields Settings

In the upper right corner of the display field configuration settings screen there is a "Transaction Type" drop down menu. *If* your organization has created unique transaction types, this is where you would select which information to save for each different transaction type.

3.4.9 - Sampling

As a reminder, a sample file is a collection of data and images in a proprietary and encrypted file format. On this page you can control whether sample reports can be saved manually or automatically, see *figure 24a*. 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 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 21b.
    - 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.

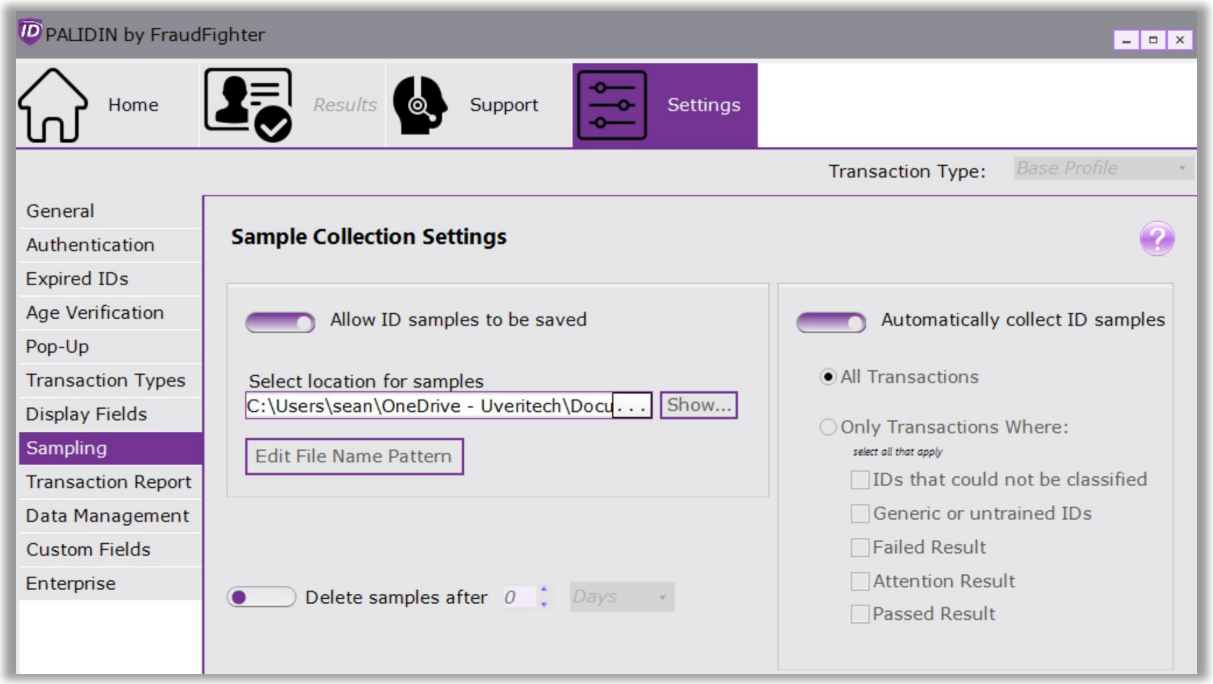


Figure 24a – Sampling Settings

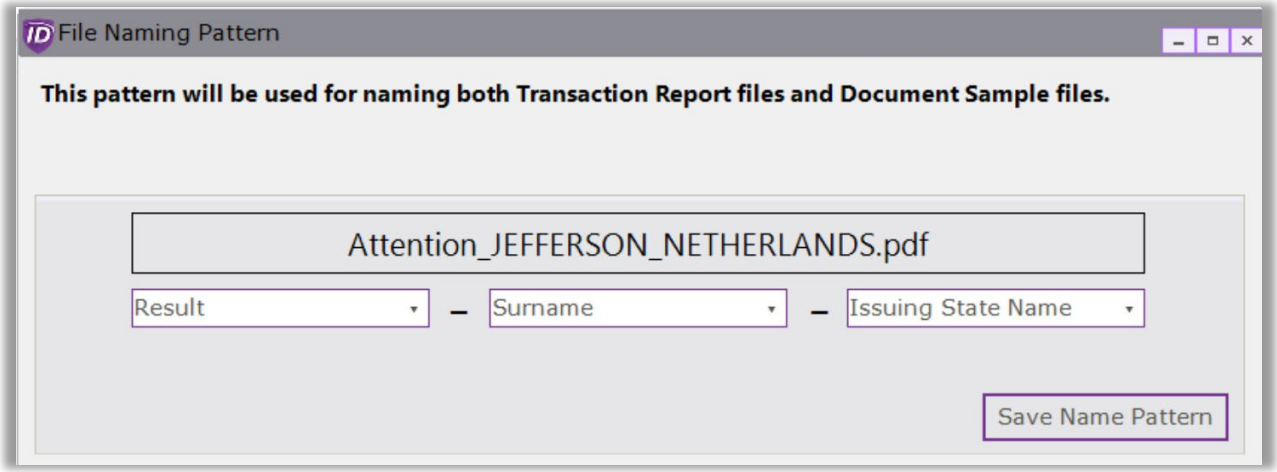


Figure 24b – Sampling Settings

3.4.10 - 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 section 3.4.8 for instructions 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 25*.

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 21b.
    - 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 23b*.
    - 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

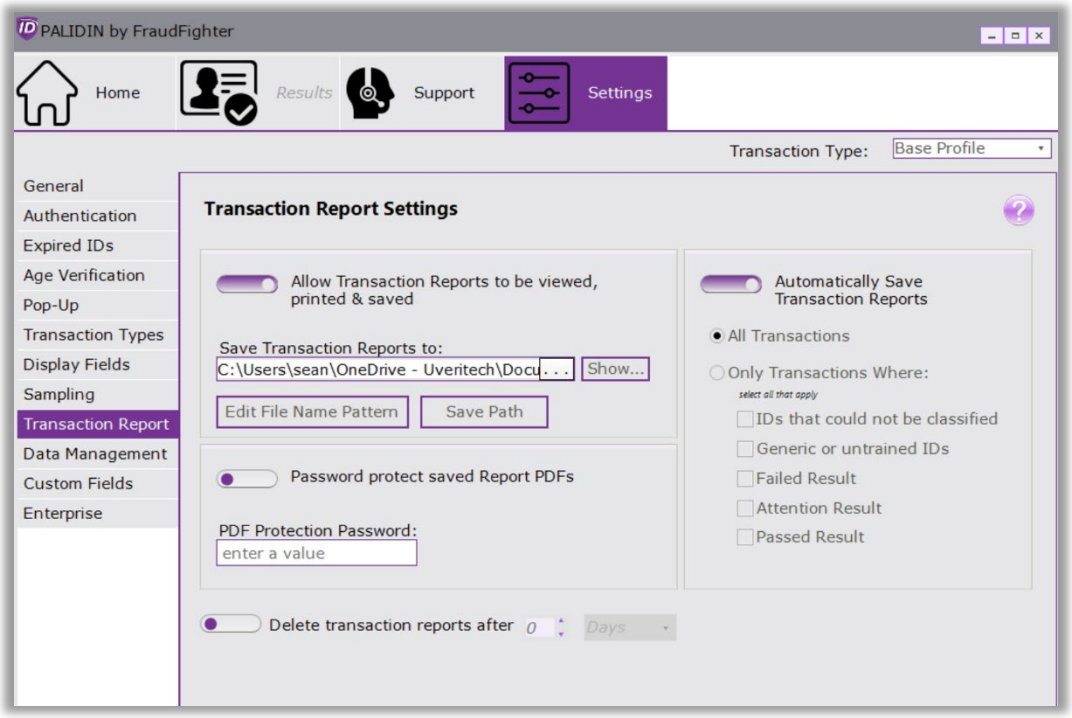


Figure 25 - Transaction Reports Settings

3.4.11 - 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.

NOTE: 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.

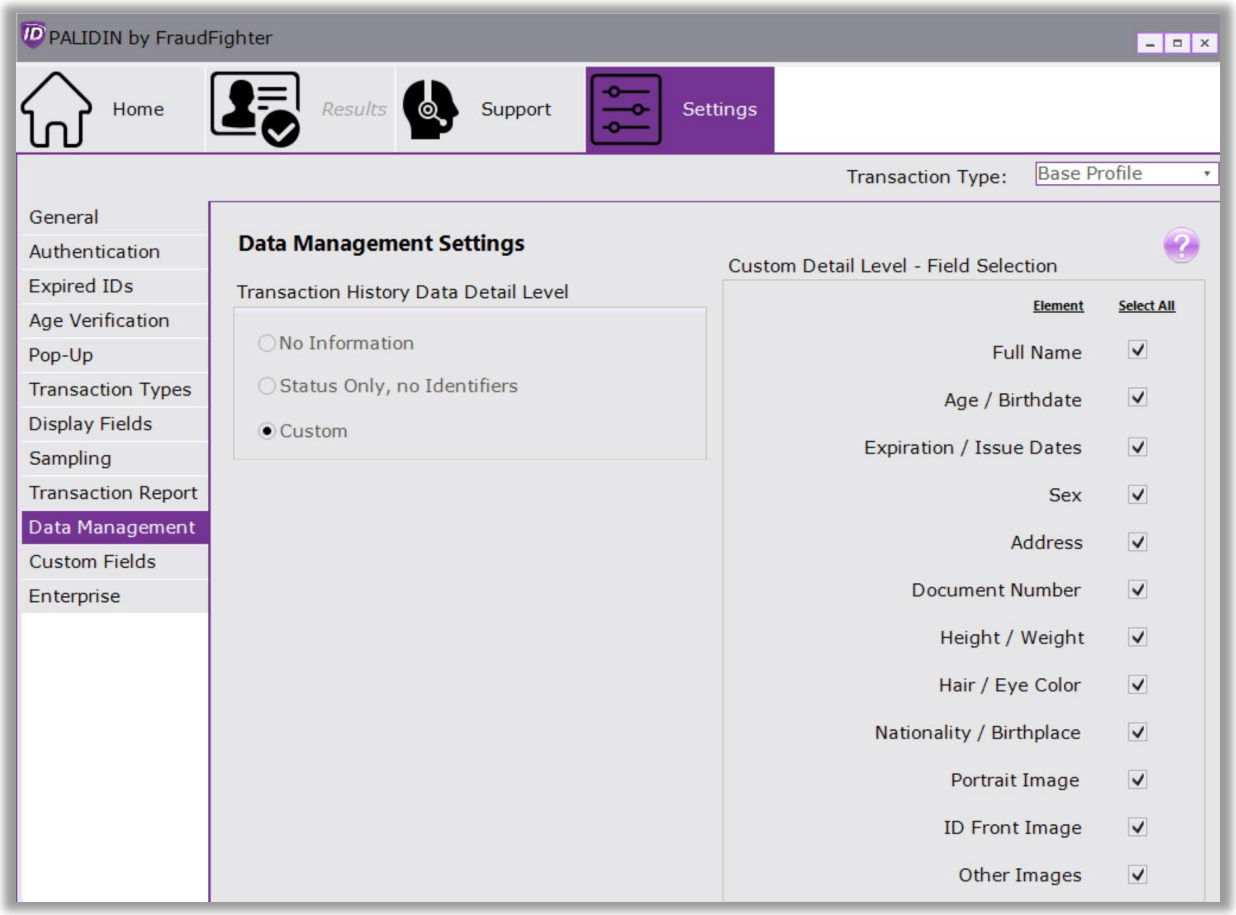


Figure 26 – Data Management Settings

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.

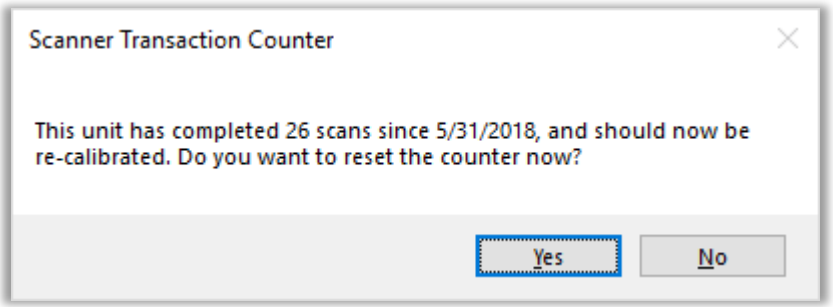
To set a reminder to clean your scanner, follow these steps:

- Under the "scanner maintenance counter" section, select or type the desired threshold for the

reminder.

- For the ID150 scanner, the manufacturer recommends cleaning 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 to further assist you in troubleshooting a problem.

3.5 - Exports

See *figure 27.* 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 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.

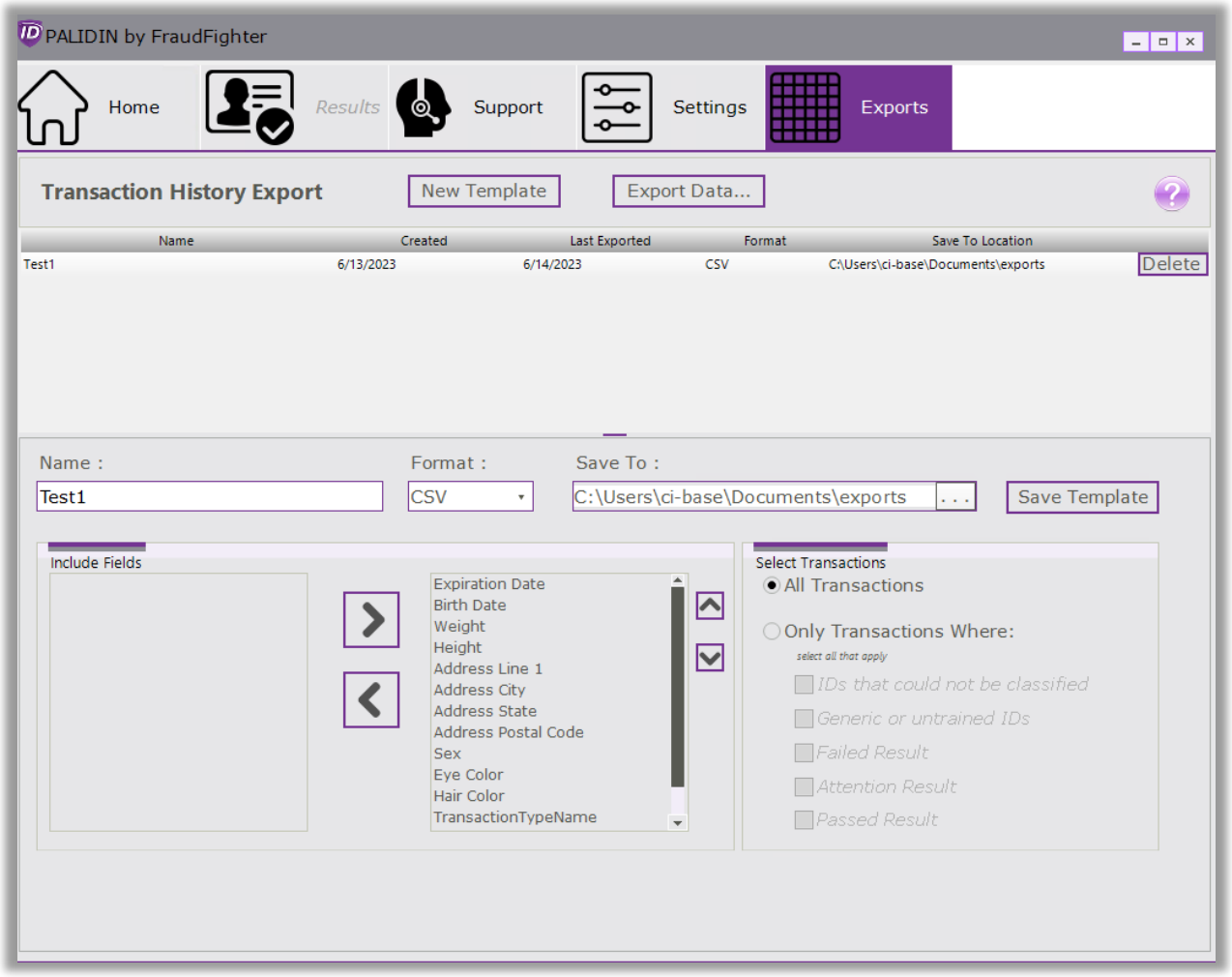


Figure 27 - Exports

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."

3.6 - Support Tab

Users may submit a support ticket by using the “Support” tab in the top navigation. When submitting a ticket through the desktop application, the appropriate logs required for technical/customer service evaluations will be automatically attached to your ticket. This. information will also include your software license key and device information.

All the fields in the form are required, and we highly recommend writing a detailed description of the problem you are experiencing so that our reps may be best prepared to assist you when they respond.

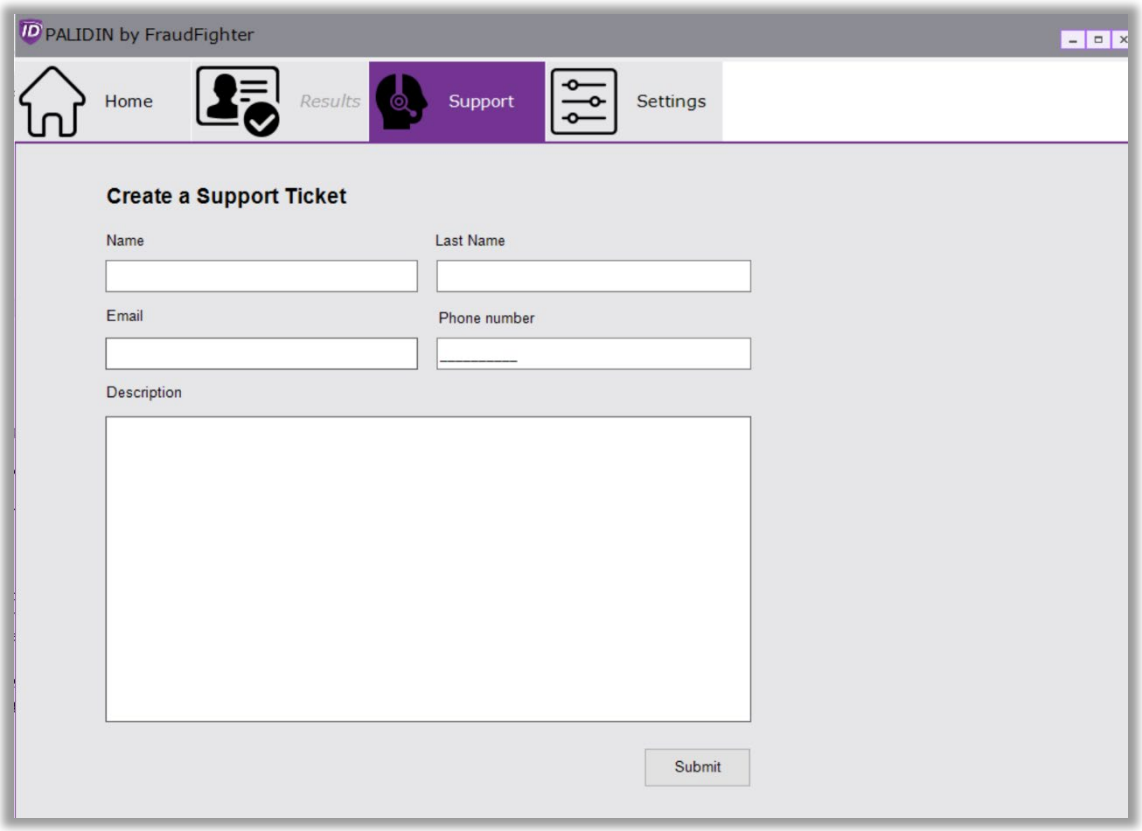


Figure 28 – Support Tab

4 - Customer Support

Our customer support team is available via phone, chat, or email. Customers can also take advantage of our dedicated customer support portal, where you'll be able to find helpful articles to FAQs, submit support tickets, track ticket status, as well as chat with our support team.

Live technicians are available M-F, 7:00am to 5:00pm PST
Phone: (800) 883-8822
Email: support@fraudfighter.com
TeamViewer Remote Support

Customer support can also be offered through a remote-computer session.
End-user required to allow Fraud Fighter to remotely control computer for necessary troubleshooting.

After Hours & Weekend support is available via our customer support ticketing system

4.1 - Customer Support Portal

Our dedicated customer support portal is available to all our customers. The portal allows you to access system manuals, troubleshooting guides and articles, submit a support ticket, as well as track its progress. The portal also includes a chat feature, where customers can chat with one of our customer support technicians.

Customer support portal: https://palidinsupport.fraudfighter.com/

Chat with our support technician (during business hours) M-F 7:00 AM – 5:00 PM Pacific

4.2 - Training

Upon deployment of the project, there are multiple training strategies to fit your organization's needs which include training videos (custom training videos can be provided upon request), live webinar training sessions, and/or quick starter guides.

Video# 1 - PALIDIN Basics
Video# 2 - How to use the system
Video# 3 - System Settings