2. REFLECTION REMOVAL (RR)

OPTIONS > CAPTURE > REFLECTION REMOVAL

Improve OCR processing by eliminating glare on the scanned image of the document. By enabling **RR**, the device takes two pictures of the document from two different angles.

> **Note**
>
> Using **RR** is increasing total processing time, because the device takes more pictures.

- White

OPTIONS > CAPTURE > REFLECTION REMOVAL > WHITE

Enable **RR** on white images by filling in the checkbox.

- Infra

OPTIONS > CAPTURE > REFLECTION REMOVAL > INFRA

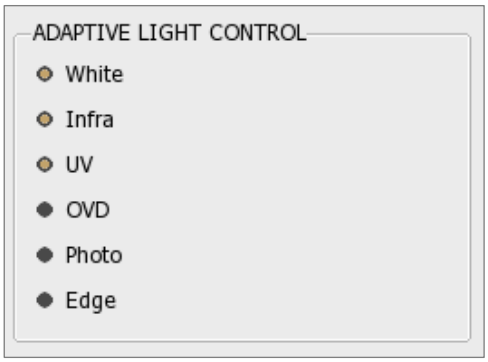
Enable **RR** on infra images by filling in the checkbox.

3. ADAPTIVE LIGHT CONTROL

OPTIONS > CAPTURE > ADAPTIVE LIGHT CONTROL

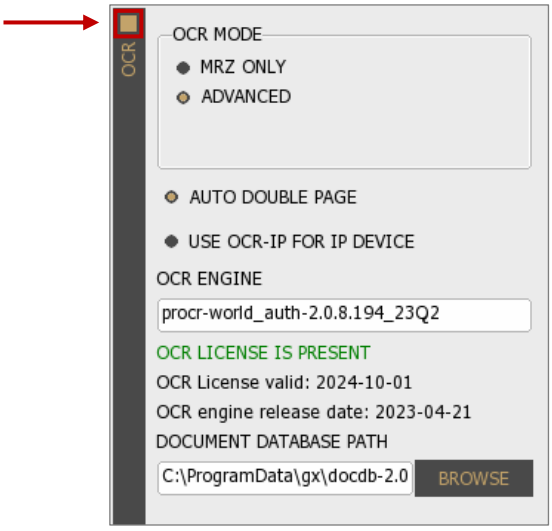
ADAPTIVE RECOGNITION's **ADAPTIVE LIGHT CONTROL** feature compensates for external light interference and make routine operation independent of the environment. In order to use this feature, fill in the checkbox(es) you wish to apply before starting the illumination process.

> **Note**
>
> Using **ADAPTIVE LIGHT CONTROL** is increasing total processing time, because the device takes more pictures.



5.6.3. OCR

Enable **OCR** process by filling in the checkbox on top-left corner of the layer.



1. OCR MODE

OPTIONS > OCR > OCR MODE

Select between two OCR modes to configure the OCR tasks to be performed.

- MRZ ONLY

OPTIONS > OCR > OCR MODE > MRZ ONLY

Select **MRZ ONLY** mode to get the data of the MRZ field from any ICAO-9303 standard document. When using this filter, no other OCR-related task is performed in order to ensure the fastest processing time. This option does not return any data from the Visual Inspection Zone (VIZ).

- ADVANCED

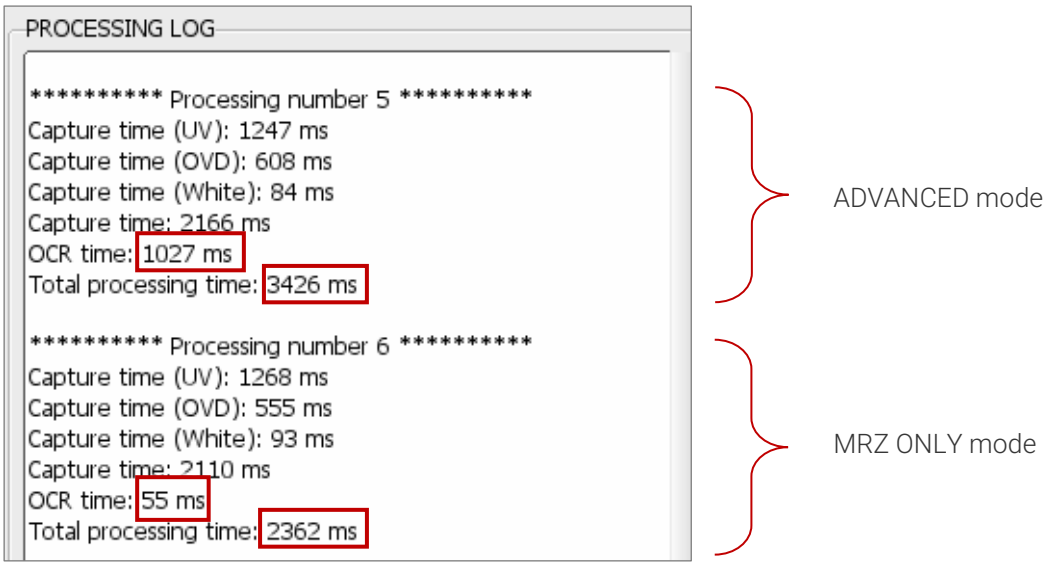
OPTIONS > OCR > OCR MODE > ADVANCED

Select **ADVANCED** mode to enable (if you have installed before) VIZ (or VIZ+Auth) engine besides MRZ to read document-specific data from the Visual Inspection Zone of different national documents. When using the device in **ADVANCED** mode, the following OCR-related functionalities are performed automatically:

  - UV dull paper check (if the device has a built-in UV illumination source)
  - B900 ink check
  - Automatic document cropping and rotation
  - Face photo cropping and face comparison

Note

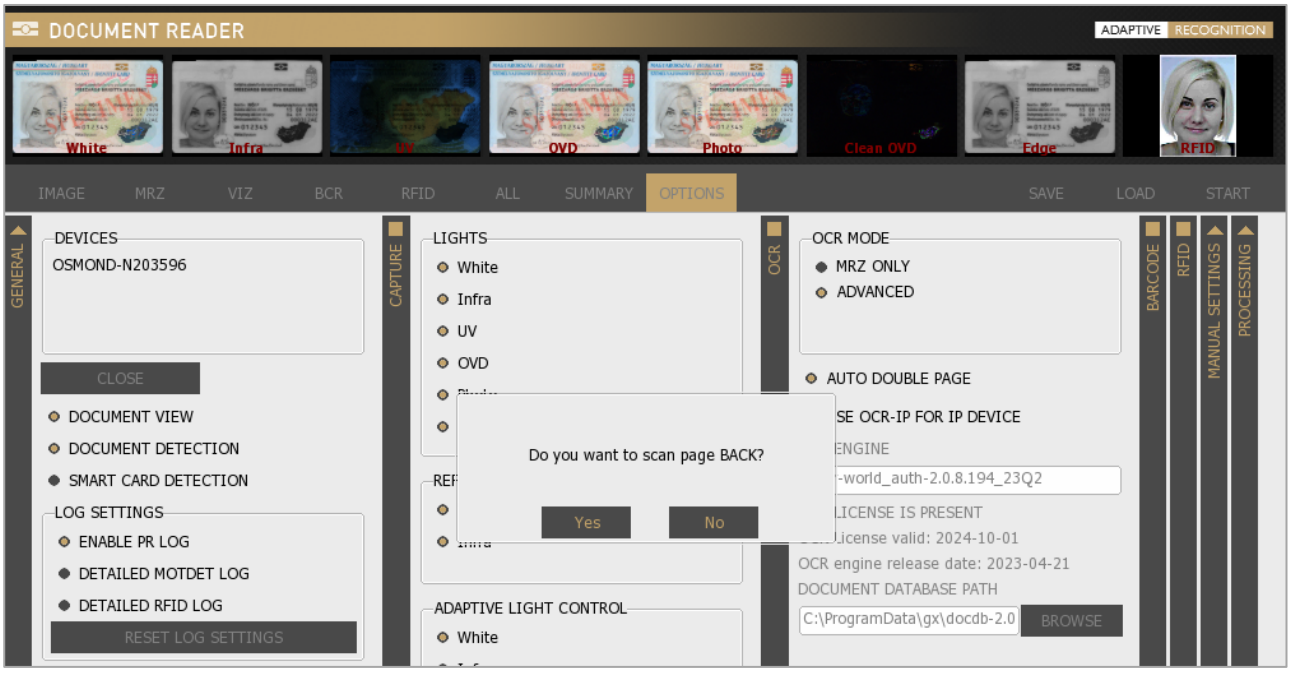
ADVANCED mode is increasing processing time.



2. AUTO DOUBLE PAGE

OPTIONS > OCR > AUTO DOUBLE PAGE

Enable AUTO DOUBLE PAGE to read double paged documents automatically. When this option is enabled, after scanning the front side of the document, the application asks the user if the back side of the document is needed. In case of clicking on the [Yes] button, FPR waits 10 seconds for the second side of the document.



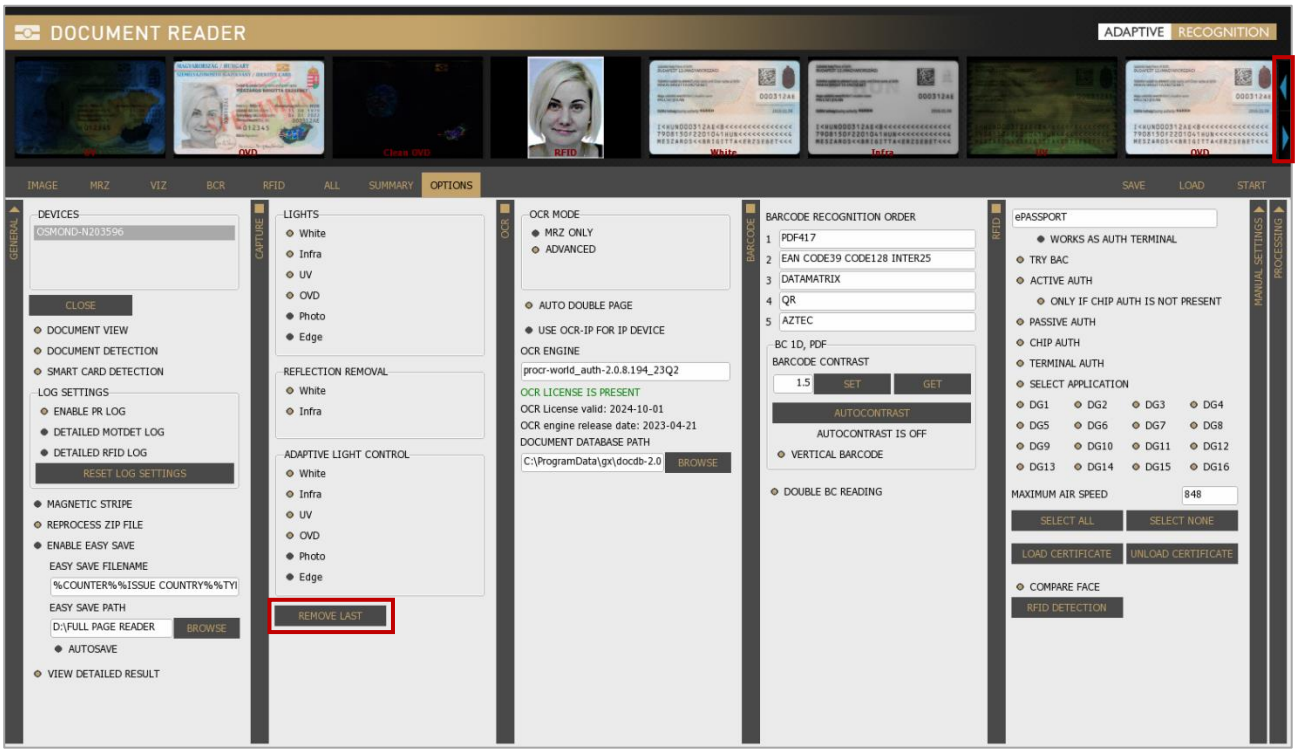
When the scanning of both sides is finished, use the blue colored left and right arrows to navigate among the scanned images.

Note

Left and right arrows are displayed, when more than 8 images are scanned from a document.

Note

The images from the last scanning can be removed by clicking on the [REMOVE LAST] button located at CAPTURE layer.



3. USE OCR-IP FOR IP DEVICE

OPTIONS > OCR > USE OCR-IP FOR IP DEVICE

When enabling **USE OCR-IP FOR IP DEVICE** option, for performing OCR, the FPR application uses the OCR engine that can be found on the remote network device.

> **Note**
>
> The "**procr-ip**" engine can be selected from the **OCR ENGINE** list, but if selected the document reading will **not be performed with local USB devices**. Therefore, in case of a locally run prwebsrv, do not select the "**procr-ip**" engine from the **OCR ENGINE** list.

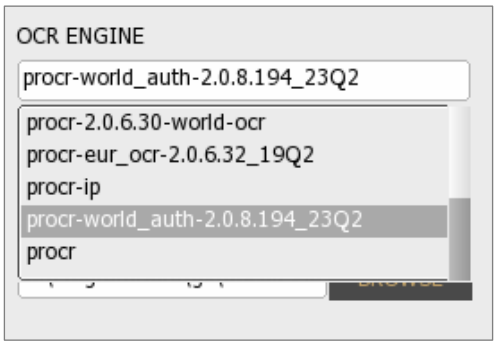
4. OCR ENGINE

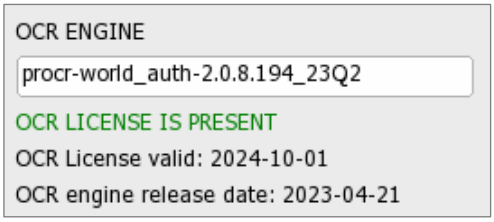
OPTIONS > OCR > OCR ENGINE

The Optical Character Recognition process of each document is performed by the **OCR ENGINE**. The default package contains the PR OCR engine, which reads the MRZ field from any ICAO 9303 standard document.

In some cases, OCR engines are trained for specific documents in order to provide additional information for authentication and/or VIZ reading (e.g., on ID type). Using such engines involves changing the PR OCR engine.

Select among **installed OCR engines on your computer**, if you have several installed engines. A dropdown list shows your available engine(s). With a left-click you can select your appropriate one. After selection, the software displays a status message about the availability as well as validity and release date of the given engine license.





> **Note**
>
> In the case of getting the "**NO OCR ENGINE INSTALLED**" message, please install your OCR engine package.

The passport reader software package and OCR engine are protected by software license. You need valid license to use PR Software features (Image capturing, RFID reading), as well as for performing MRZ OCR+Barcode Reading. Optionally, you also need license to use any specific OCR engine trained to perform VIZ reading and Authentication of certain documents. Licenses are stored on the document scanner device.

The green status message (displayed under OCR engine) indicates valid license.

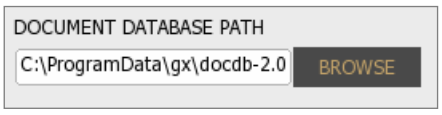
Possible error messages in processing log, referring to licenses:

- `(3:ERRO) [prapi] > (cmd:2008006f) (1012) - Hardware key does not work properly [prapi] (license).`
  → It is referring to the missing PR software license.
  Please, contact your ADAPTIVE RECOGNITION sales representative to ask for license update.
- `(3:ERRO) [prdoc] > Ocr read: FAILED: Hardware key does not work properly [gxmodule].`
  → It is referring to the missing VIZ OCR and/or MRZ OCR+Barcode Reading license.
  Please, contact your ADAPTIVE RECOGNITION sales representative to update your licenses.

5. DOCUMENT DATABASE PATH

OPTIONS > OCR > DOCUMENT DATABASE PATH

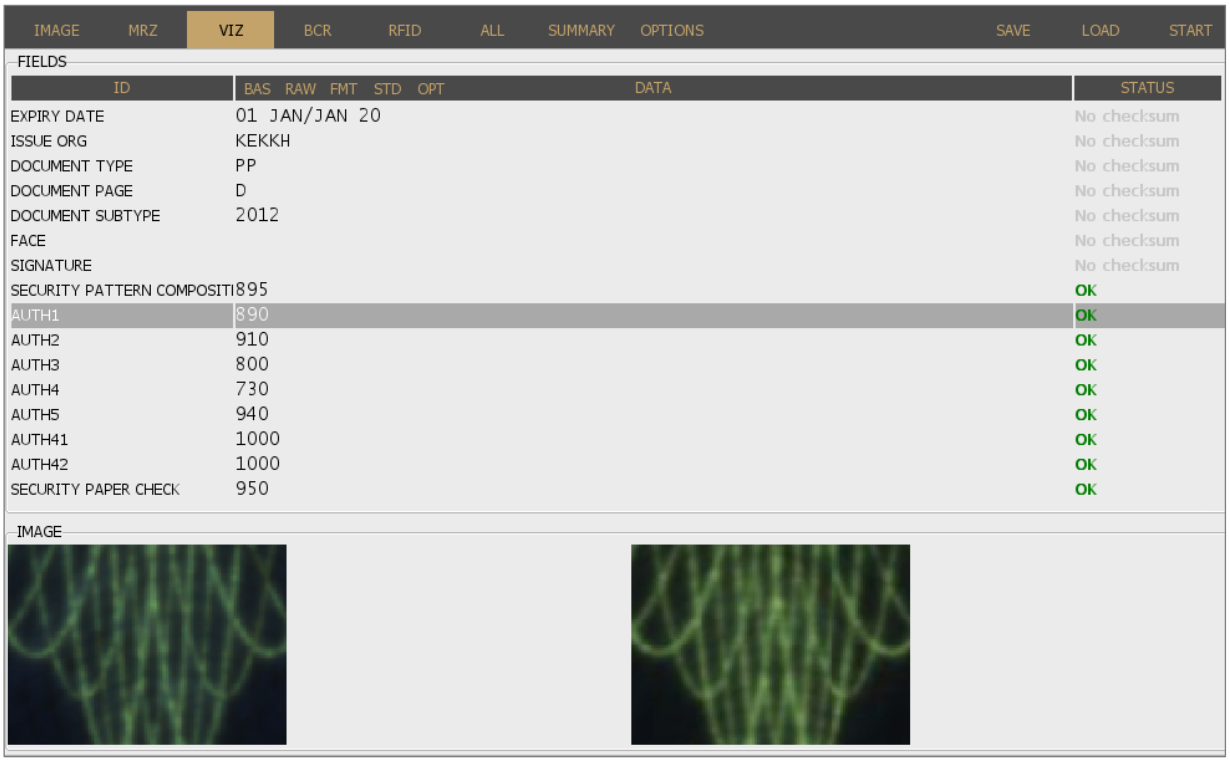
Define the path for reference image database for authentication purposes. The reference images are displayed in the AUTH check fields at VIZ tab. This path is set by default as you install VIZ OCR+Auth engine to your computer. The purpose of this function is to allow visual comparison of authenticated document sections with images stored in a reference database. If document database is not set or installed, the authentication feature still operates and its results are returned.



The values of the AUTH fields are in thousandths.
The limits are the following:

- 0-329: ERROR
- 330-659: WARNING
- 660-1000: OK

> **Note**
>
> These limits are ADAPTIVE RECOGNITION standard values.



Scanned image

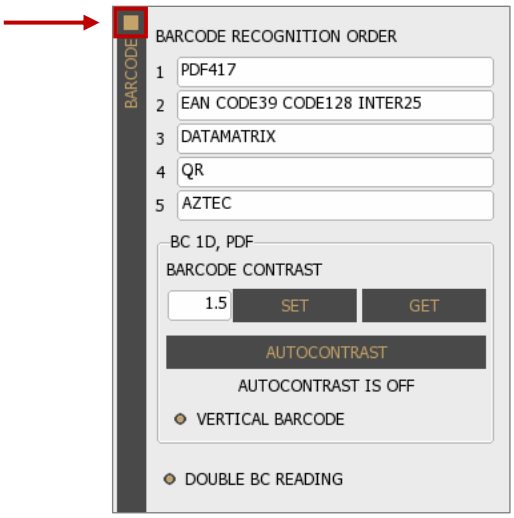
Reference image

Hint

By double clicking on the corresponding AUTH field, the accurate place of the image fragment will be shown in the complete image.

5.6.4. BARCODE

Enable **BARCODE** recognition by filling in the checkbox on top left corner of the layer.

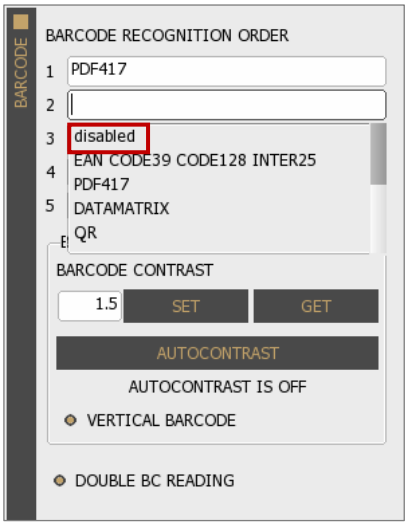


> **Note**
>
> If you do not need barcode recognition, disable this option to speed up processing.

1. BARCODE RECOGNITION ORDER

OPTIONS > BARCODE > BARCODE RECOGNITION ORDER

Set the order of tries in recognizing barcodes. Different types of barcodes are available to read. You can select your appropriate ones from the dropdown lists. Use **disabled** value for not needed types.



> **Note**
>
> Unnecessary barcode detection increases processing time. Select only necessary/possible types.

2. BARCODE CONTRAST

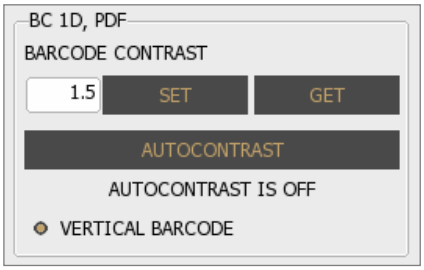
OPTIONS > BARCODE > BARCODE CONTRAST

Note

The following properties affect only 1D-type (EAN, CODE39, CODE128, INTER25) and PDF417 barcodes.

Set **BARCODE CONTRAST** to improve the accuracy of reading of low quality or damaged barcodes.

- Possible values: **0.3 – 7.0**
- Default value: **1.5**
- Recommended value: **1.2**
- Autocontrast values: **-1**, **-2** and **-3**



Hint

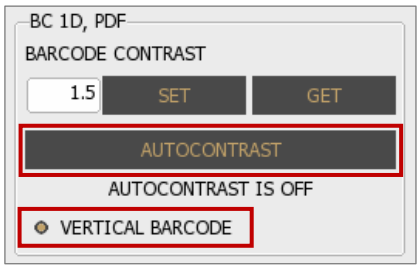
By clicking on the **[GET]** button you will get the current value.

Note

For more information on **BARCODE CONTRAST**, please contact ADAPTIVE RECOGNITION support team.

AUTOCONTRAST

It is recommended to use instead of manual settings. To utilize this function, click on the button. During operation the automation may turn off, thus the current status of the function is displayed below the **AUTOCONTRAST** button.



VERTICAL BARCODE

Enable/Disable recognition of barcodes that are positioned on the document in vertical orientation.

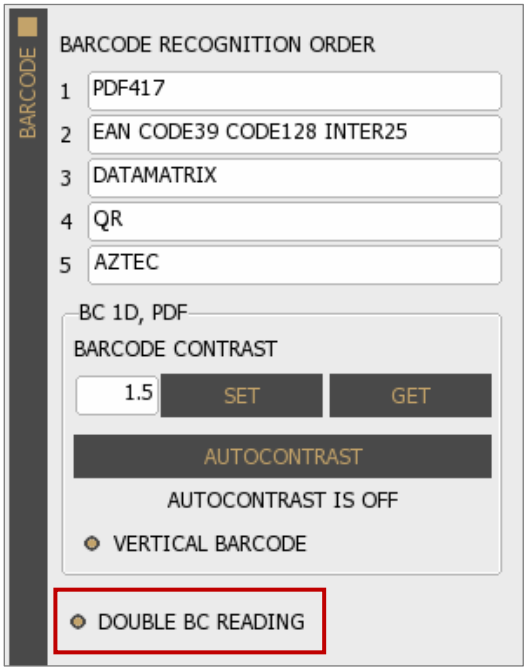
Note

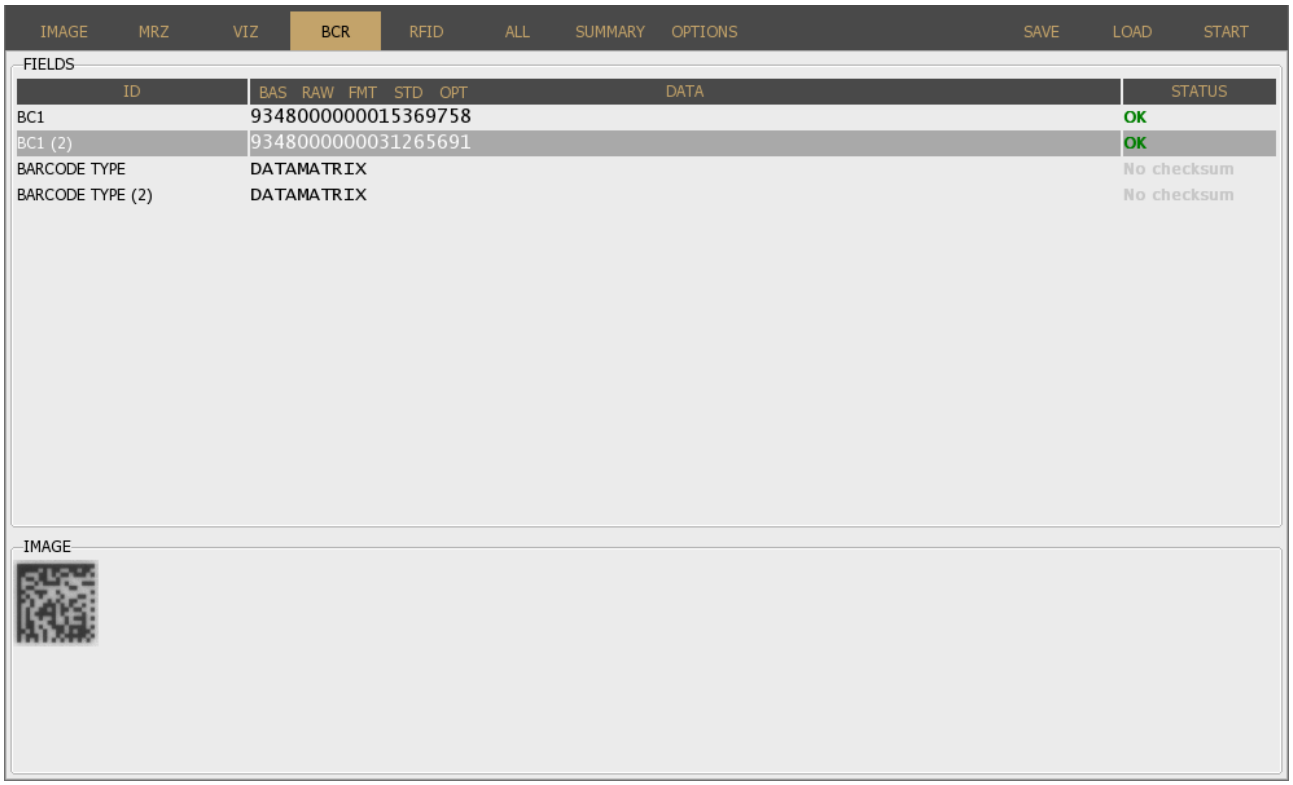
Enable this function to maximize the efficiency of barcode reading.

3. DOUBLE BC READING

OPTIONS > BARCODE > DOUBLE BC READING

Enable the **DOUBLE BC READING** function in order to scan multiple barcodes from the same document page in a single scanning attempt.



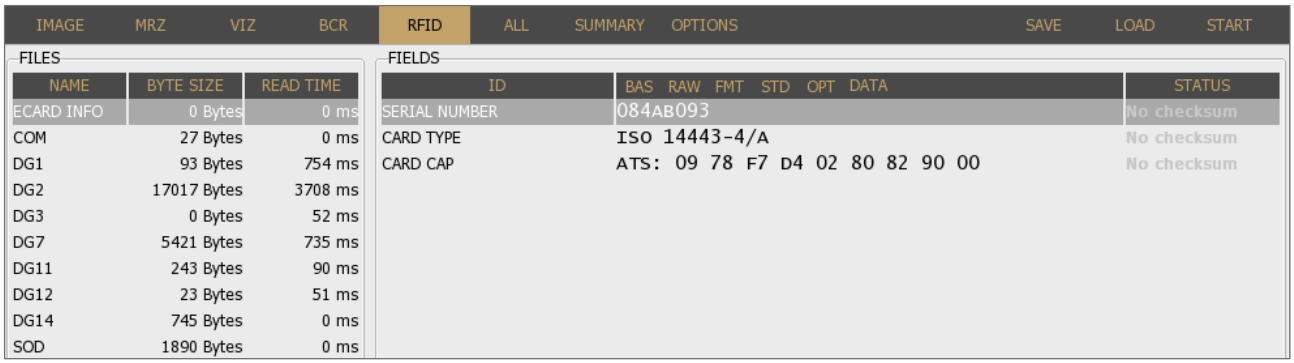


5.6.5. RFID

View the **RFID** layer in the **OPTIONS** tab to customize the parameters of RFID chip reading: authentications to perform and data groups to read.

RFID Authentication is a process that validates claimed identity of a participant in an electronic transaction. RFID chips may support different types of authentication methods.

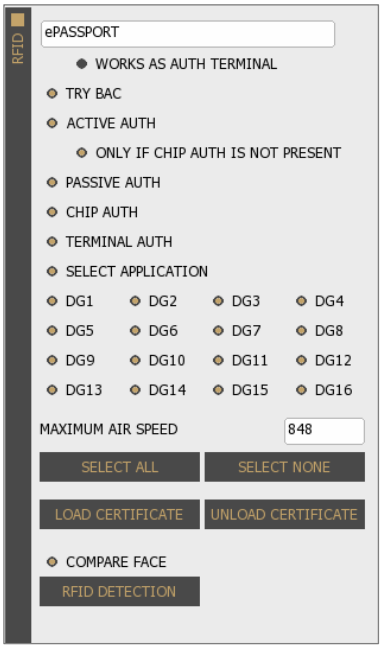
> **Note**
>
> In the case of **contact chip reading**, the extracted data is displayed in the **RFID** tab.



1. ePassport / eID

OPTIONS > RFID > ePassport / eID

Select the application to be read which can be eID or ePassport.



2. TRY BAC

OPTIONS > RFID > TRY BAC

Enable/Disable **TRY BAC** authentication.

TRY BAC forces the Basic Access Control (BAC) in case of appropriate and also inappropriate messages received by the document. The protocol for Basic Access Control is specified by ICAO. When performing Basic Access Control, the terminal authenticates the user by confirming they have physical access to the MRTD's data page. Such confirmation is done by requesting MRZ data (document number, birth date and expiry date) from user to start the BAC process.

3. ACTIVE AUTH

OPTIONS > RFID > ACTIVE AUTH

Enable/Disable **ACTIVE AUTHENTICATION**.

Active Authentication protects against chip cloning by verifying if DG15 is not a copy. It is basically a two-way interaction between the reader and the document that involves communication with the non-accessible memory of the chip. AA result is valid only after the Passive Authentication has been executed successfully.

4. PASSIVE AUTH

OPTIONS > RFID > PASSIVE AUTH

Enable/Disable **PASSIVE AUTHENTICATION**.

Passive Authentication is used to check if the data on the RF chip of the electronic document is authentic and unforged.

The authentication process includes two main steps:

- Authenticating the SOD
- Verifying the hashes of each DG file by comparing them to the hashes stored in SOD

For authenticating the SOD, the CSCA certificate of the document is required. Such certificate should be downloaded from the website of the document issuing authority, from ICAO PKD or via other trustworthy source. Once downloaded, it should be copied to: **C:\ProgramData\gx\pr\certs** (Windows) or **/var/gx/pr/certs** (Linux) or loaded manually with the **[LOAD CERTIFICATE]** button.

Supported certificate formats:

- .cer
- .crt
- .crl
- .cvcert
- .der
- .ldif
- .ml
- .pem

> **Note**
>
> The corresponding private key must have the same name as the cvcert it belongs to, only with pkcs8 extension.

Hint

The Passport Reader software package is implemented with German Master List that includes CSCA certificates of hundreds of documents.
You may download and use the latest version of this Master List from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/CSCA/GermanMasterList.html

5. CHIP AUTH

OPTIONS > RFID > CHIP AUTH

Enable/Disable **CHIP AUTHENTICATION**.

Chip Authentication is used to uncover cloned RF chips: it is a more advanced alternative to Active Authentication. Similarly to AA, CA also involves communication with the secure memory of the chip. CA is obligatory in EU passports.

6. TERMINAL AUTH

OPTIONS > RFID > TERMINAL AUTH

Enable/Disable **TERMINAL AUTHENTICATION**.

TA is designed to provide additional protection to sensitive data (fingerprint (DG3) and iris (DG4)) stored in the RFID chip. Without performing TA, the passport denies access to such biometric information as TA requires the inspection system to prove that it is authorized to access the sensitive information within the RFID chip.

TA consists of two major phases:

1. Building the certificate chain of public keys
2. Verifying if the terminal has the private key using the certificate chain

In order to perform both phases, the DV public and IS public certificates as well as the IS private key are required. These files can be loaded in the same way as PA certificates (see above). If all certificates are loaded, TA is performed automatically by the FPR and the sensitive data is displayed in the **RFID** and **SUMMARY** tabs.

Note

FPR is only able to perform TA if the private key is available and loadable in file format.

7. SELECT APPLICATION

OPTIONS > RFID > SELECT APPLICATION

Enable/Disable **SELECT APPLICATION** function. If it is selected, the Passport Reader software automatically selects a supported application on the RFID chip: ePassport, eID, eDL or IDL.

8. DG1-16

OPTIONS > RFID > DG1-16

Enable/Disable document's RFID data groups to read.

Some of the data groups need to have certificate to access its data. Required certificates can be obtained from the authority of the local national government.

9. MAXIMUM AIR SPEED

OPTIONS > RFID > MAXIMUM AIR SPEED

Set the maximum baud-rate for communication with the RFID chip.

10. LOAD/UNLOAD CERTIFICATE

OPTIONS > RFID > LOAD/UNLOAD CERTIFICATE

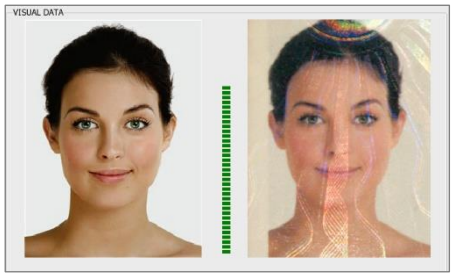
Browse and select your certification file that enables you to run RFID security mechanisms (PA and TA).

> **Note**
>
> Private keys (.pkcs8) cannot be loaded with **[LOAD CERTIFICATE]** button.

11. COMPARE FACE

OPTIONS > RFID > COMPARE FACE

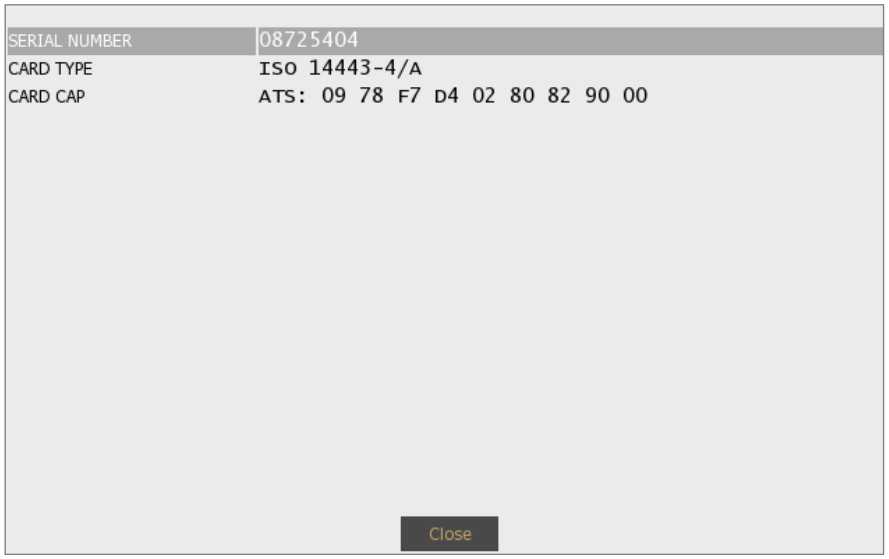
Enable/Disable comparing the face photo stored in chip against the one printed on the data page.



12. RFID DETECTION

OPTIONS > RFID > RFID DETECTION

Use the **RFID DETECTION** feature to determine if there is an eDocument positioned onto the document reader device. If you click on this button, a window will pop up with the fundamental data of the document/chip.



Note

This feature works only when the document is within 10 mm from the RFID antenna of the device.

5.6.6. MANUAL SETTINGS

Fine-tune your software by changing default system property values to customize operation according to your preferences.

> **Note**
>
> Changing parameters may have negative effect on system performance and operation. If in doubt with the proper value, please consult with ADAPTIVE RECOGNITION support team.

1. PROPERTY NAME

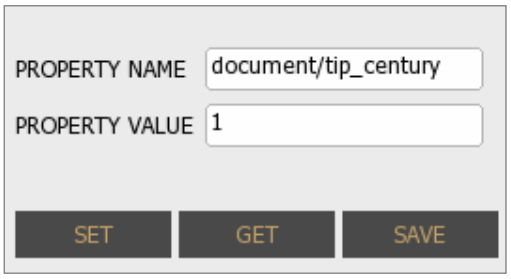
OPTIONS > MANUAL SETTINGS > PROPERTY NAME

Every property has a name and most properties have path as well. When referring to a property (e.g., in the FPR application) the path must be specified as well.

2. PROPERTY VALUE

OPTIONS > MANUAL SETTINGS > PROPERTY VALUE

The property value is a number or text that determines the effect of the property.



> **Note**
>
> For more information on possible property values, please check the Passport Reader Property List chapter.

5.6.7. PROCESSING

1. PROCESSING TIME

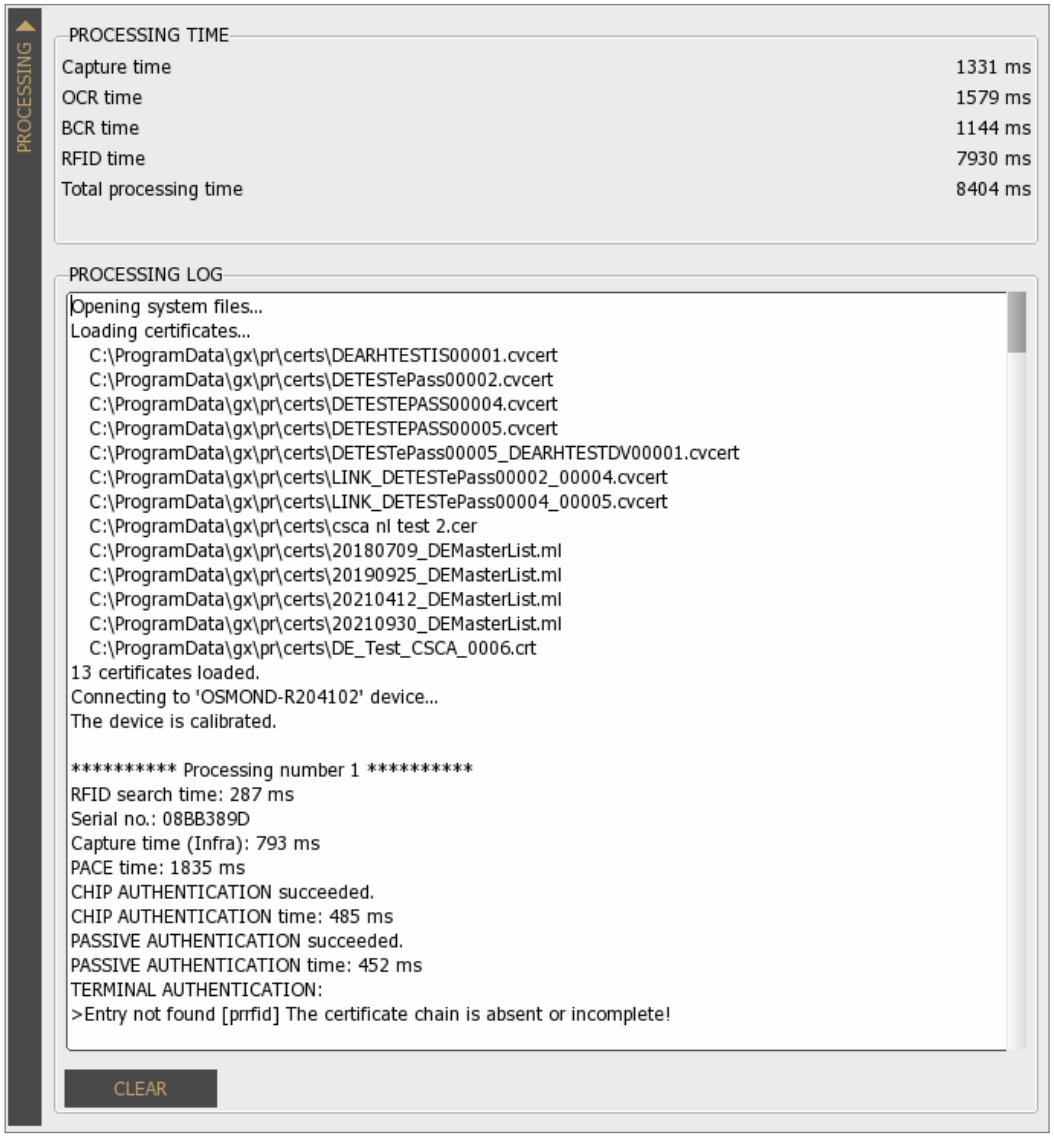
OPTIONS > PROCESSING > PROCESSING TIME

Brief summary of the **PROCESSING TIME** of each processing phase.

2. PROCESSING LOG

OPTIONS > PROCESSING > PROCESSING LOG

The **PROCESSING LOG** displays the main events of each document reading process.

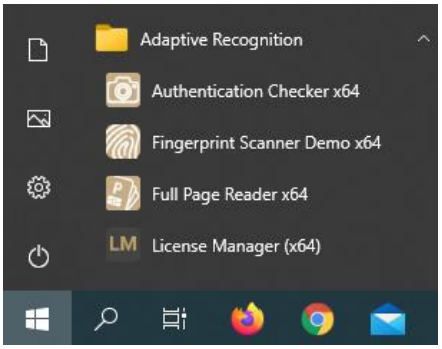


5.7. FAQ

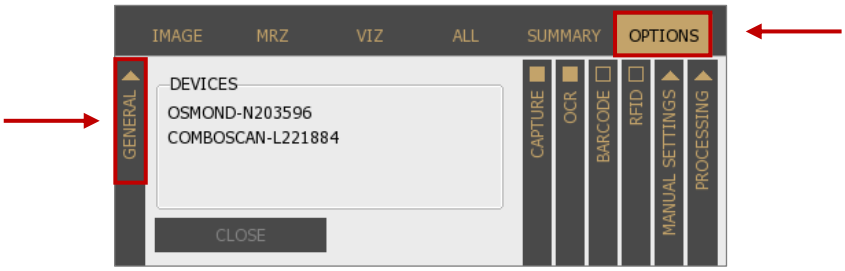
5.7.1. BASICS

How to connect reader before scanning?

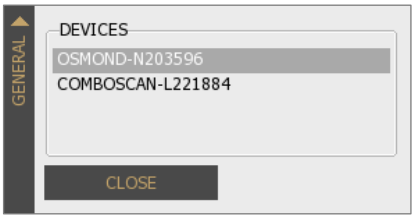
1. Open Full Page Reader (FPR) app.



2. View **GENERAL** layer in **OPTIONS** tab to see available reader(s).

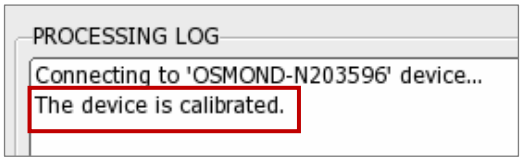


3. Connect reader to your system to gain access its features by
   a. clicking on the **[CONNECT]** button or
   b. clicking on the selected reader in the **DEVICES** list.



4. Check the status of the reader in the **PROCESSING LOG**

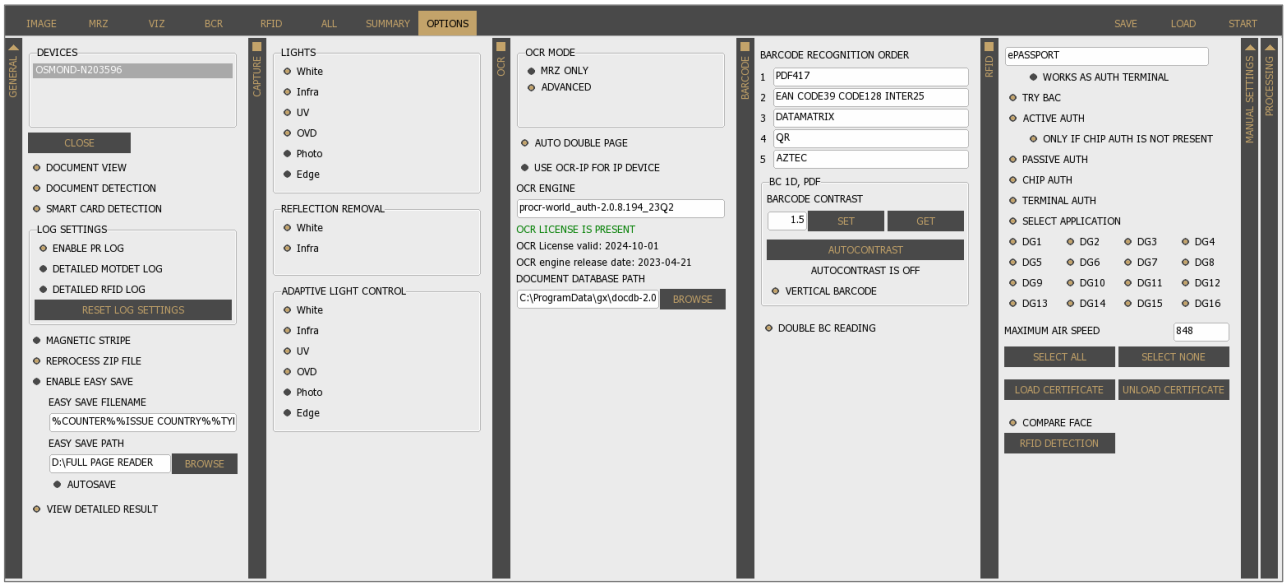
   If you get the "**The device is calibrated**." message, your reader is ready to use.



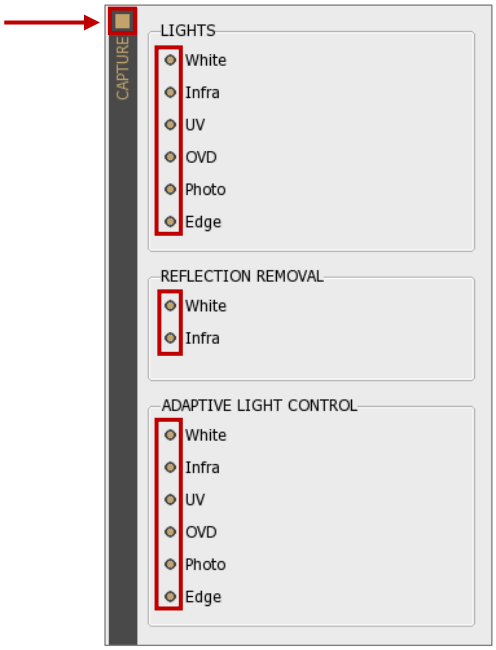
5.7.2. SCANNING

How to scan?

1. Connect reader.
2. Open vertical layers in **OPTIONS** tab and enable/disable filters to customize the FPR's operation according to your needs.

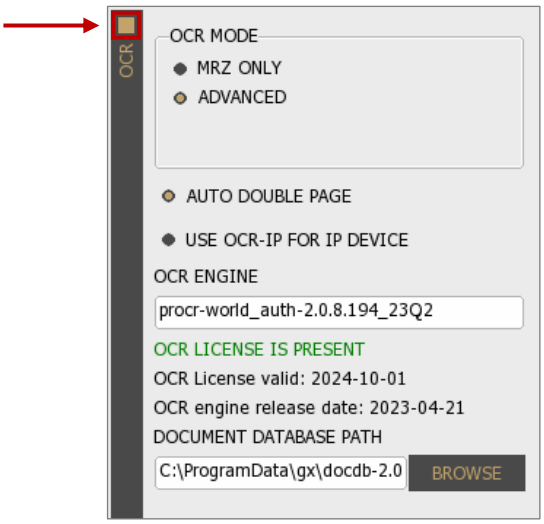


a. Activate **CAPTURE** layer for scanning documents by filling in the checkbox and set the illumination types you wish to apply.

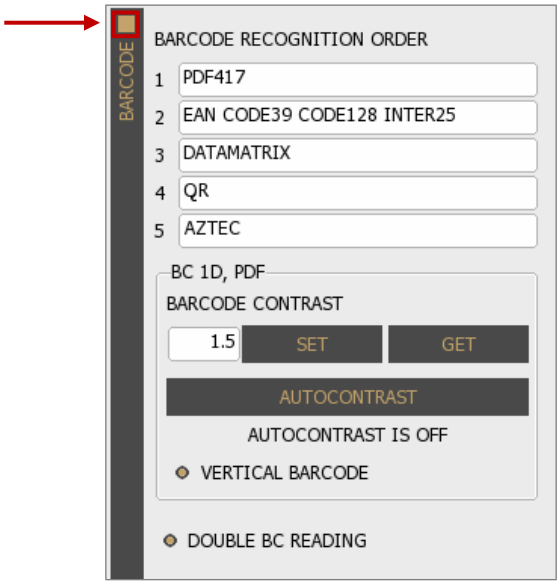


b. Activate **OCR** layer by filling in the checkbox and select your **OCR ENGINE** for performing character recognition.

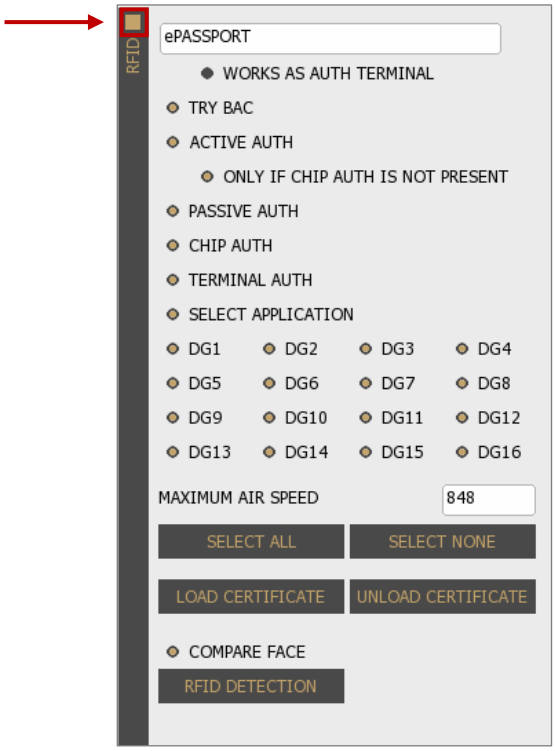
> **Note**
>
> Select **ADVANCED** mode to read data from **MRZ and VIZ fields** as well.



c. Activate **BARCODE** layer by filling in the checkbox to read barcode(s) from documents. If you expect different barcode types, you can set an order for faster process time.



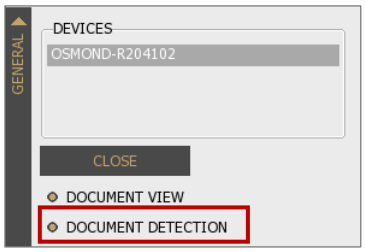
d. Activate RFID layer by filling in the checkbox to read RFID chip data from e-documents. Select the data groups to read and the authentication mechanisms to execute.



3. Start scanning by pressing the [START] button or use DOCUMENT DETECTION.

How to enable document presence detection (aka Motion Detection, Freerun Mode, Auto-scan)?

Select **DOCUMENT DETECTION** option on **OPTIONS / GENERAL** layer to enable document presence detection. This feature automatically scans images using the selected filters whenever a document is available on the surface of the reader.

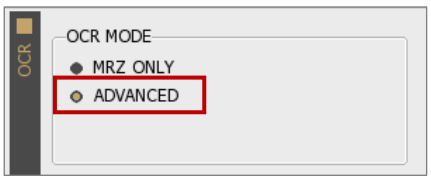


How to crop and rotate document?

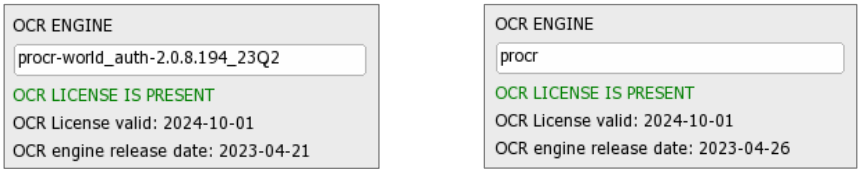
Select **DOCUMENT VIEW** option before the starting of the scanning process on **OPTIONS / GENERAL** layer to crop and rotate documents into upright position.

How to read VIZ fields?

- Select **ADVANCED** mode on **OPTIONS / OCR** layer to read data from **VIZ**.



- Select your **VIZ-OCR** engine to use.



- Check the processed VIZ data of a given document on the **VIZ** tab.

> **Note**
>
> **VIZ** tab is only visible if you have activated on the **OCR** layer.

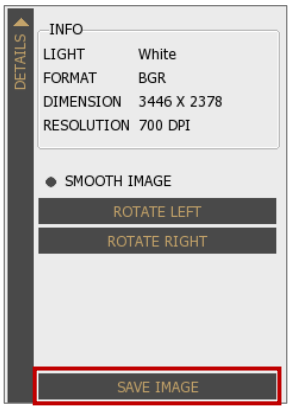
5.7.3. SAVE, LOAD, REPROCESS

How to save a scanning?

1. Select filters and scan a document.
2. Choose from the following saving methods:

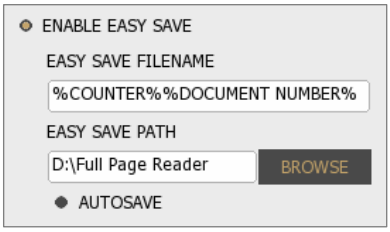
   a. Click on [SAVE] and browse the path as well as specify the filename to finish the saving process.

   b. Click on [SAVE IMAGE] on IMAGE / DETAILS layer to save the selected image. Browse the path and specify the filename to finish the saving process.



> **Note**
>
> SAVE IMAGE function is only able to save into image format.
> ZIP, PDF, XML or CSV formats are not available options.

   c. Select ENABLE EASY SAVE and click on [SAVE] to preserve the selected scanning.

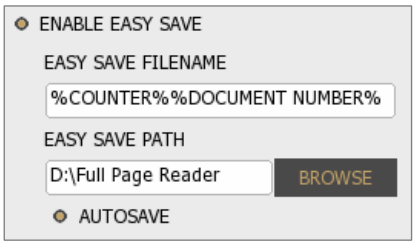


> **Note**
>
> At the first saving, you have to browse the path and define the filename, if the EASY SAVE PATH is not specified.

d. Select **ENABLE EASY SAVE** and turn on **AUTOSAVE** to perform automatic saving.

Important!

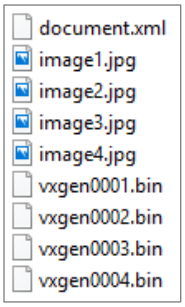
If the **EASY SAVE PATH** is not specified, the automatic saving is not performed.



3. If you have selected **ENABLE EASY SAVE**, you will find the images of the scanned document in the folder that you have selected at **OPTIONS / GENERAL / EASY SAVE PATH.**

What is included in the saved file?

- All **images** scanned by different light sources are available in original view.
- XML file with the **processed data** from document.
- Corresponding **binary data** for each image in .bin files.
- Copy of the **face photo** from RFID chip (if available).
- Copy of the **biometric data** from RFID chip (if RFID and CVCA certificate is available).



Note

If the following properties are enabled, the **cleanovd**, **cleanuv** and certain **field images** are also saved in the ZIP file:

- save_cleanovd – save cleanovd image,
- save_cleanuv – save cleanuv image,
- save_fieldimage – save field image.

For more information on these properties, see Passport Reader Property List chapter.

How to load or reprocess a previous scanning? What is the difference?

- LOAD

1. Click on the [LOAD] button.
2. Browse for your .zip file and click on it.
3. Open the selected file.
4. You get the original data and images in the app as it was processed earlier.

- REPROCESS

1. Select REPROCESS ZIP FILE option on GENERAL layer in OPTIONS tab.

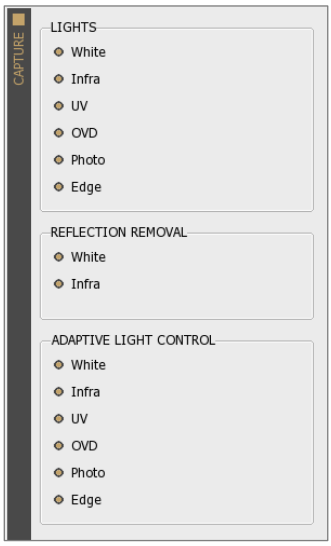
2. Set different filters to review same document in different conditions.
   I.e.: Select different OCR engine or barcode setting.
3. Click on the [LOAD] button.
4. Browse for your .zip file and click on it.
5. You get the reprocessed data as it was modified with new filters.

The difference between the two is that with the LOAD you get the original saved data in the app (you do not have to check the ZIP file) and with the REPROCESS ZIP FILE the saved data is processed again according to the actual or selected engine.

How to make a collection of sample documents to send to ADAPTIVE RECOGNITION?

1. Open Full Page Reader.
2. Select **all available illumination types** for both **LIGHTS** and **REFLECTION REMOVAL**.

> **Note**
>
> **REFLECTION REMOVAL** ensures glare-free images that provides higher OCR accuracy.



3. Scan the document based on the following:
   - Make sure that the document is in standstill position while scanning is performed.
   - Protect the scanning window from direct sunlight or strong ambient light from the environment.
   - Scan both sides of the document.
   - In case of ID-1 and ID-2 size documents:
     For the best OCR quality, please make scans with rotating the cards by 90°and 180° or positioning them randomly.
4. Save document(s) by clicking on the **[SAVE]** button – for training purposes, minimum 15 different scans needed from the same document type.

> **Hint**
>
> If you wish to scan more documents, using of **ENABLE EASY SAVE** and **AUTOSAVE** options are recommended to use to minimize the saving time.

VI. OSMOND N (NETWORK DEVICE)

Osmond N device operates as a network device. It could be connected to any internal network with DHCP, and the reader could be controlled via Web GUI.

> **Note**
>
> Osmond N model is able to operate in USB and Network mode as well. For more information see Devices Capable of Dual Operational Mode chapter.

1. ACCESSING THE DEVICE

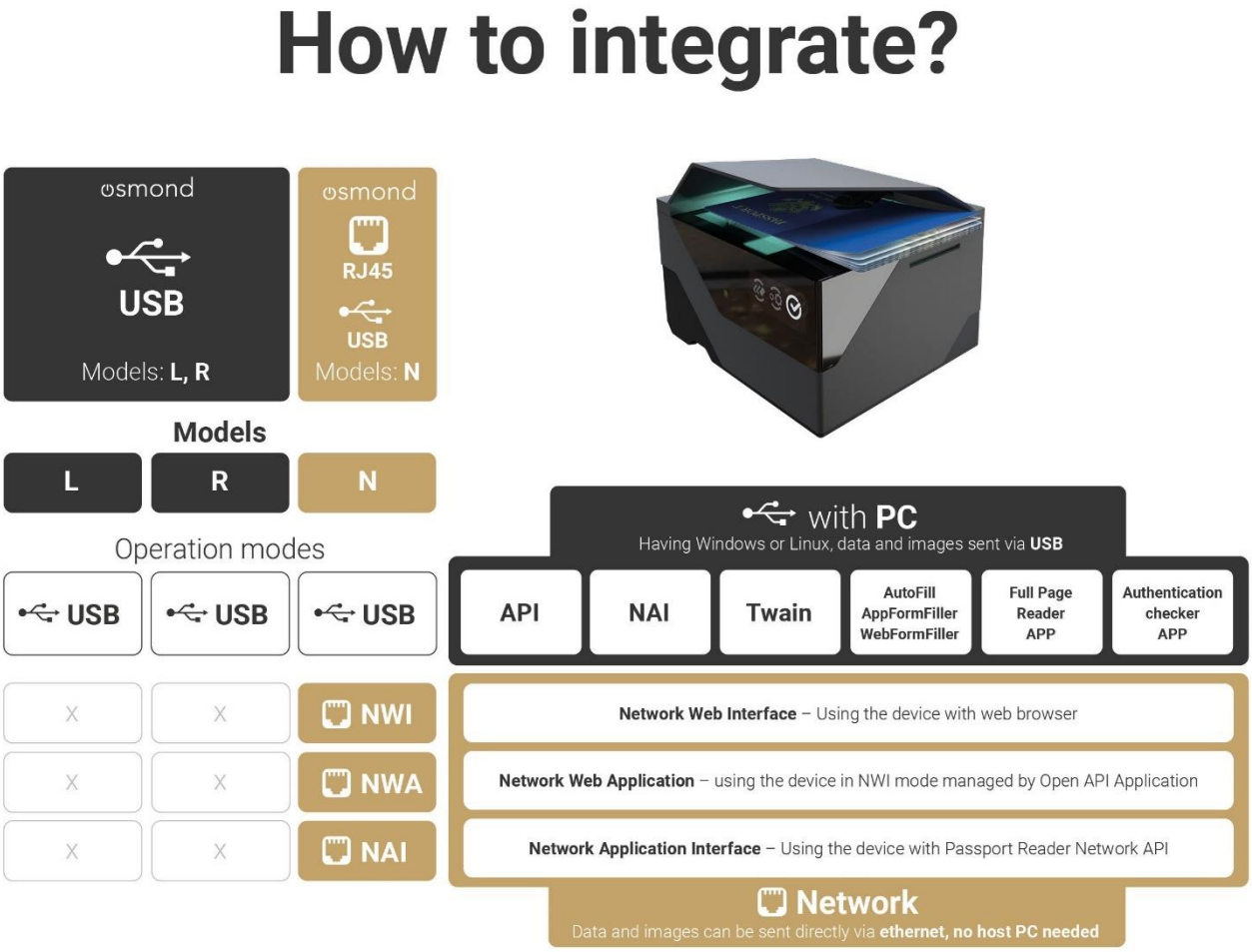
The Osmond operates without any kind of special software. All processes are running on the the device. The web server running on the scanner can be accessed with any other device (e.g., a laptop, tablet) that can log on to the network that the scanner is connected to.

SOFTWARE REQUIREMENTS

- For network setup, administrator (root) privileges are required.
- Web browser: We recommend using the latest versions of Chrome or Firefox.

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

1.1. INTEGRATION OPTIONS



1.2. ACCESSING THE WEB INTERFACE OF THE DEVICE FROM A BROWSER (NWI MODE)

Note

Follow the steps described in the Hardware Installation chapter to connect the network device to the PC.

1. Once the device is connected to the PC and turned on, the status LEDs on the Ethernet port switches to green and orange as well as the status LED on the power touch button switches to green.
2. A few seconds later the ADAPTIVE RECOGNITION logo is displayed on the OLED display (the booting is in progress).
3. After the boot process, the status display appears on the screen:

In case of Ethernet connection, the WebGUI is also loaded, when the device is ready for operation, the OLED display shows the following icon:

Important!

When using the device for the first time, the device must be connected to the Internet due to the time synchronization. This process only takes a few seconds after the check mark being displayed (see the icon above). If the interface disconnects the user instantly, use the Ctrl + F5 keyboard shortcut and try signing in again.

4. Please make sure that your network has a DHCP server in order to operate your document reader device.

5. If the network infrastructure provides support for DHCP and DNS services, start a browser and enter the following into the browser's address bar in order to access the web interface of the device/launch the WebGUI interface:

`{hostname and port}`

`OSMOND-N{serial number* and port}`

E.g., http://`OSMOND-N204203:3000`

*Type the serial number without the very first character. E.g., 204203 instead of 2204203.

> **Note**
>
> The hostname of your device is OSMOND-N{serialnumber*}. The serial number of your device is printed to the sticker located at the bottom of your scanner.
>
> *Type the serial number without the very first character.

6. If the DHCP server is not available for any reason, but the default gateway is set, the device is accessible on 192.0.2.3.

> **Note**
>
> For more information on setting the default gateway, see Direct Ethernet Connection chapter.

6.1. If the device is not accessible via domain name nor via 192.0.2.3:3000, make sure that you:

- check the Ethernet LEDs on the PC or the switch and device,
- check whether the assigned IP address of the device can be pinged,
- check proxy settings,
- check that your browser is not set to offline mode.

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

7. If all information was entered correctly, the following screen should come up in your browser window.

Important!

If login fails due to invalid username/password, delete the browser cache (Ctrl + F5), then retry login.

Note

When there is a time difference between device and host PC, the web interface allows the login, but only the DATE AND TIME menu will be available.

8. The default user account is the following:

   Login name: owner

   Password: Owner123*

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

Note

When the device is not in network mode, but e.g., in USB mode, and the user signs in the web interface, the interface directs the user to the MAINTENANCE / OPERATING MODE menu, where one of the following options must be selected:

- NWI (Network Web Interface): Using the device with web browser. This is the default mode, when logging in to the web interface.
- USB: Using the device with PC application, connected via USB.
- NAI (Network Application Interface - NetAPI): Using the device with Passport Reader Network API.
- NWA (Network Web Application): Using the device in NWI mode, managed by Open API application.

After selecting the operating mode, the device restarts immediately.

Note

After signing in, the user account and the user profile can be edited in the ADMINISTRATION / USERS menu.

The minimum length of the username is 5 characters and it can contain the following characters:

- a-z
- A-Z
- 0-9
- _
- .
- @
- -

The minimum length of the password is 8 characters.

After logging in, each user is granted a 10-minute-long session that is signaled by a counter at the bottom right corner of the browser window. This counter is constantly reset upon changing menu, saving a form and after each scanning process. The length of session can be adjusted at ADMINISTRATION / USERS / GENERAL SETTINGS / Session timeout.

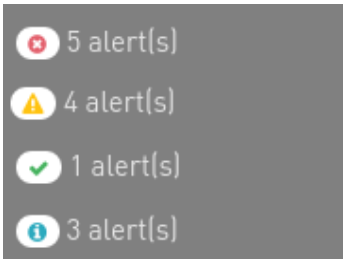
Important!

Closing the browser does not terminate the session. Make sure to log out (Main menu / QUIT) in order to allow other users from the same role to log in.

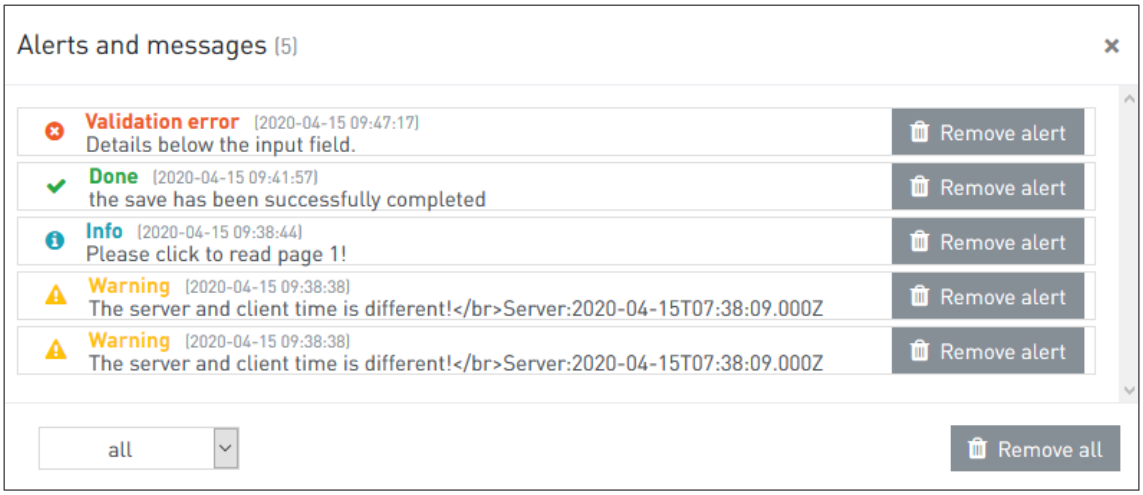
The system sends notifications about events which may concern the user. Such event can be for example the success or failure of saving a data sheet as well as if the document is to be changed in the document reader after scanning a page. Information about the number of the notifications is displayed on the left side of the status bar located at the bottom of the screen (if there is at least one notification).

The following notification types can be distinguished:

- Error
- Warning
- Notification about a successful execution of operation
- Information

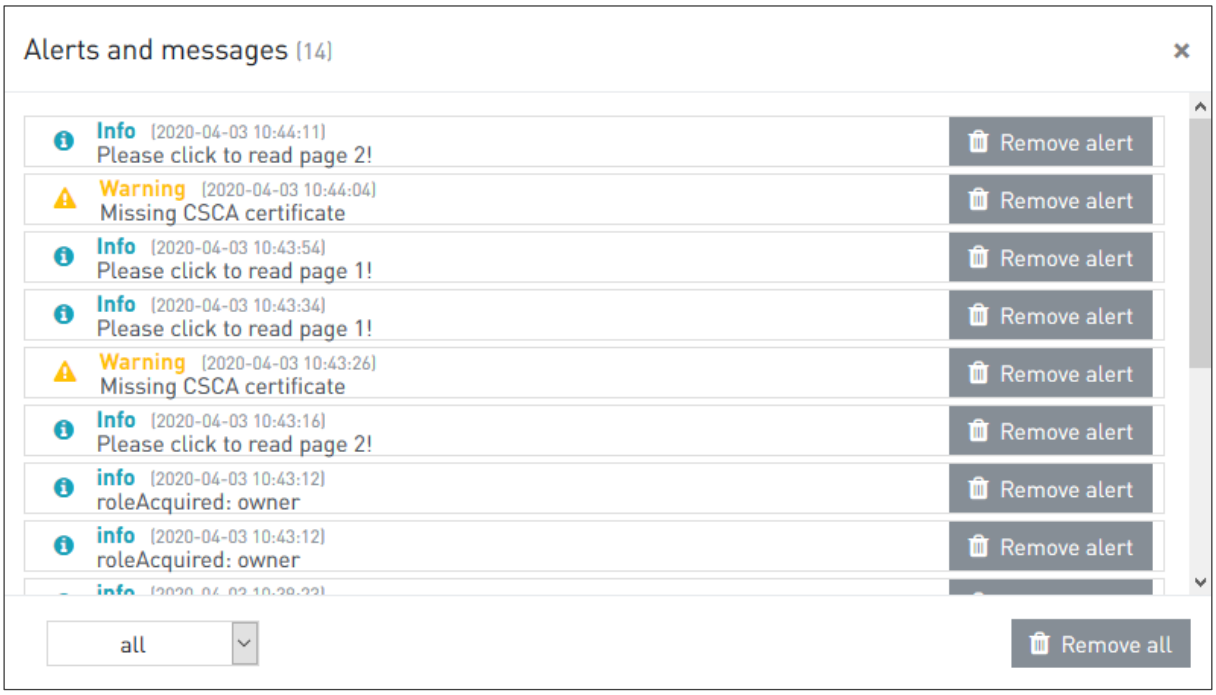


In the list the notification types are displayed with increasing priority. Thereby in the status bar the icon of the highest priority notification can always be seen with the number of the notifications. By clicking on the notification icon, the notifications can be viewed (in descending order by date).

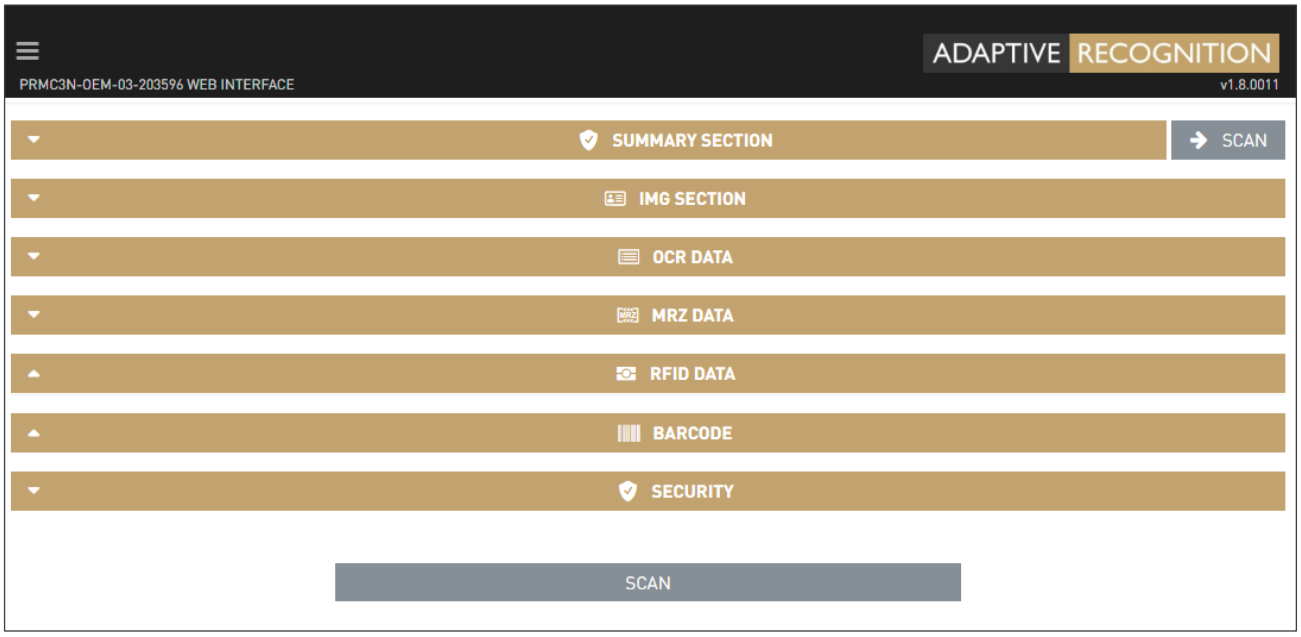


On the notification panel it can be selected that every or just the chosen notification type should be listed. The notifications can be deleted one by one or all at once.

In the case of a two-sided document the application indicates to the user which page is missing and should be inserted to the scanner.



If you are signed in, you will find the following screen in your browser window:



This is the home page, the START APP menu, where you can scan identity documents. Before scanning, it is important to check the Main menu (the three horizontal stripes; at the top left corner of the webpage) and perform the required settings.

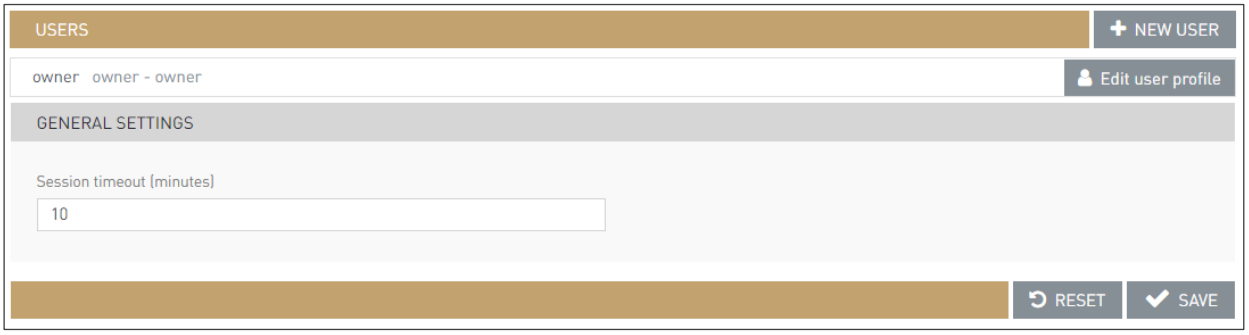
Further on the elements of the Main menu will be explained.

2. WEB INTERFACE

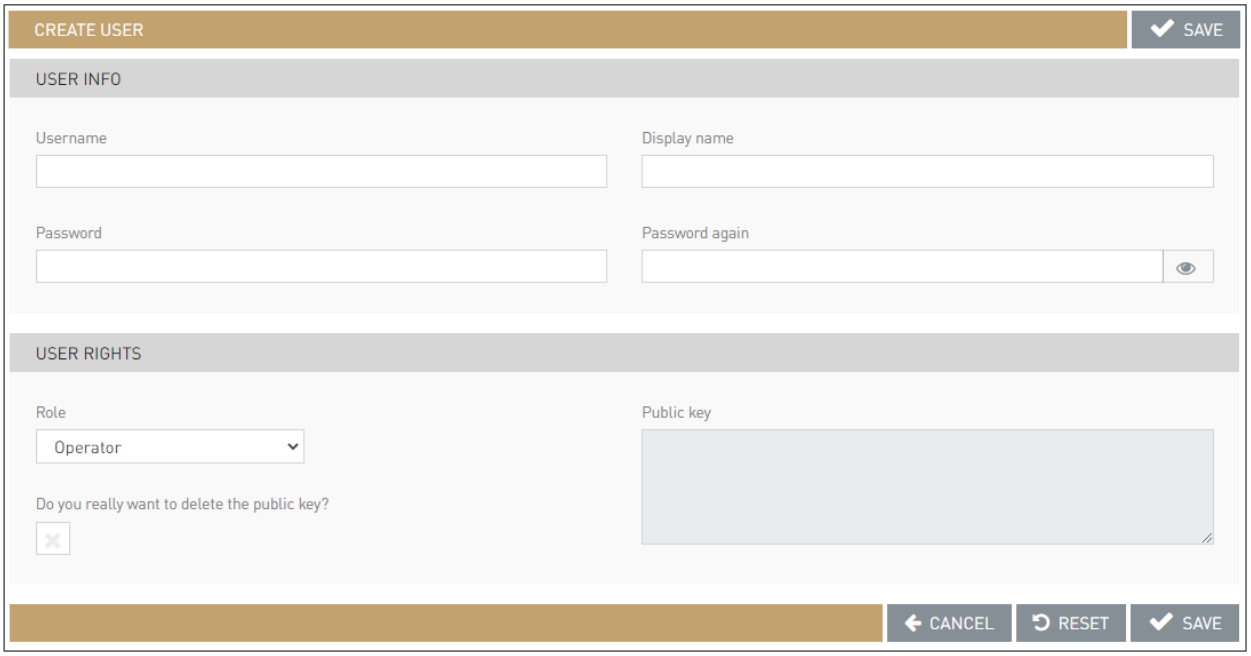
2.1. ADMINISTRATION

2.1.1. USERS

In the **USERS** menu, you can create and delete users, you can also change the passwords and the roles of the users. Click on the **[+NEW USER]** button to add a user.



The following window will appear.



Fill out the **Username** and **Password** fields and select the **Role** of the user. By clicking the **Eye** (👁) icon, you can either show or hide the password.

Display name is a nickname or alternative name that is displayed at the bottom right corner of the webpage.

When selecting **Role** for the user, choose from the following options:

	Start scanning process	Scan process menu	Admin menu	Network menu	Reboot and Restart	Application menu	Maintenance (except for reboot and restart)	Maintenance menu
Operator	✓							
Network admin			✓	✓			✓	
App admin		✓			✓			
Owner	✓	✓	✓	✓	✓	✓	✓	✓

Note

In the menu only those menu items are displayed to which the user has rights.

In addition to the fundamental user roles, the following roles are available as well:

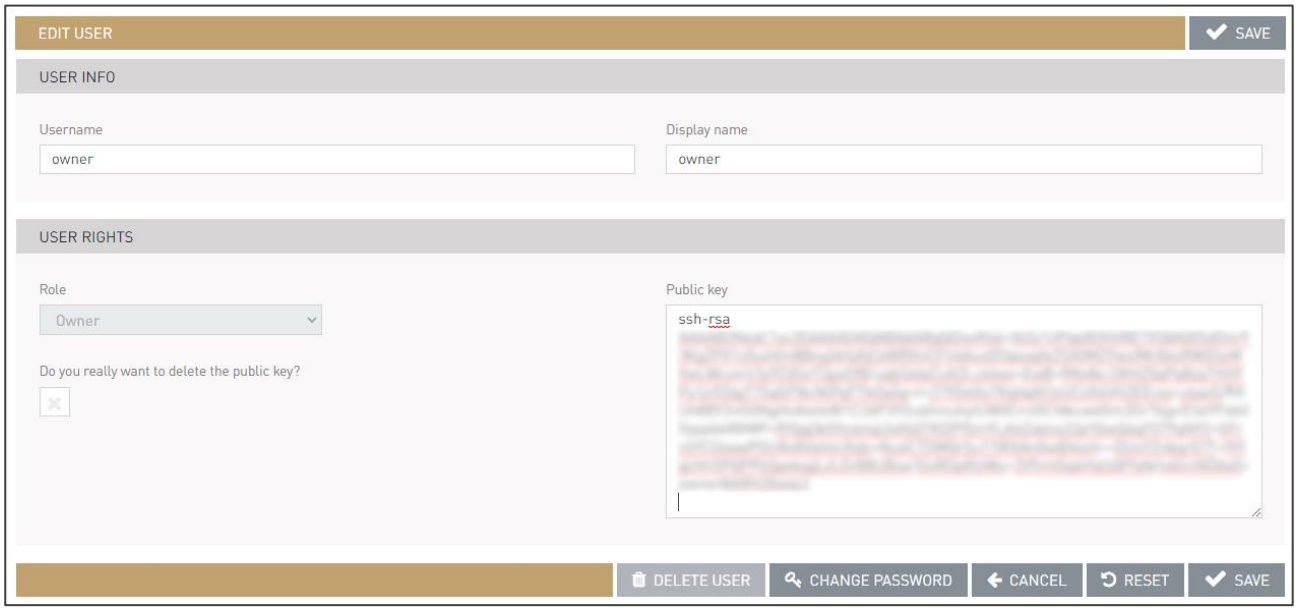
- **NAI**: This user role belongs to the NetAPI operating mode. NetAPI user is required to operate the Osmond N device via Passport Reader NetAPI.
- **NWA**: This user role belongs to the Network API operating mode and can only be used in Network API operating mode.

Note

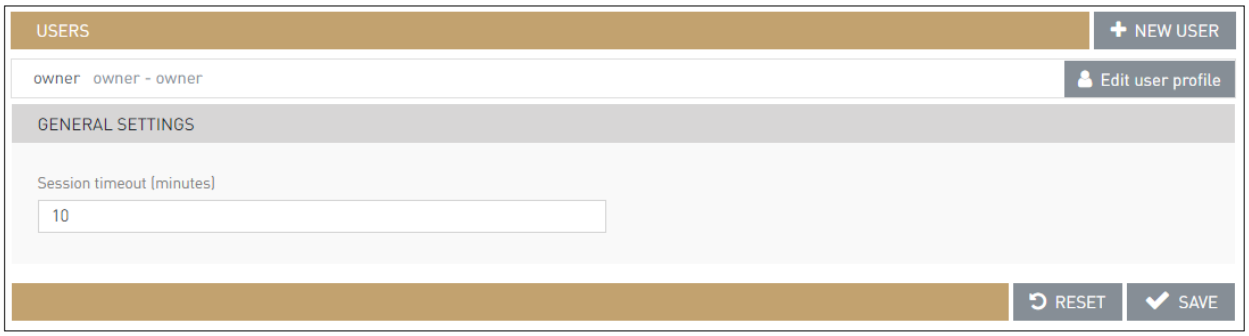
During NetAPI and Network API communication **only one user** can be connected to the device.

Once all the information has been entered, click on the **[SAVE]** button to create the new user. The created user will appear in the **USERS** menu.

Providing **Public key** is required only for establishing SSH connection to the device upon remote troubleshooting sessions. The **Owner** users can upload public key to the device: in the possession of the private key belonging to this public key, the device is accessible through SSH with a user named "baas" with limited rights. In order to use this function, the public key is to be copied to the **Public key** text field at the **EDIT USER** option. After a successful upload, SSH key based connection can be established (in the possession of the private key of the uploaded public key) with the "baas" user. The "baas" user has limited rights, the allowed operations for "baas" user can be listed with the "help" command.



Using the **Session timeout** option, owners may specify the length of user sessions. Session timeout value is applied for each user.

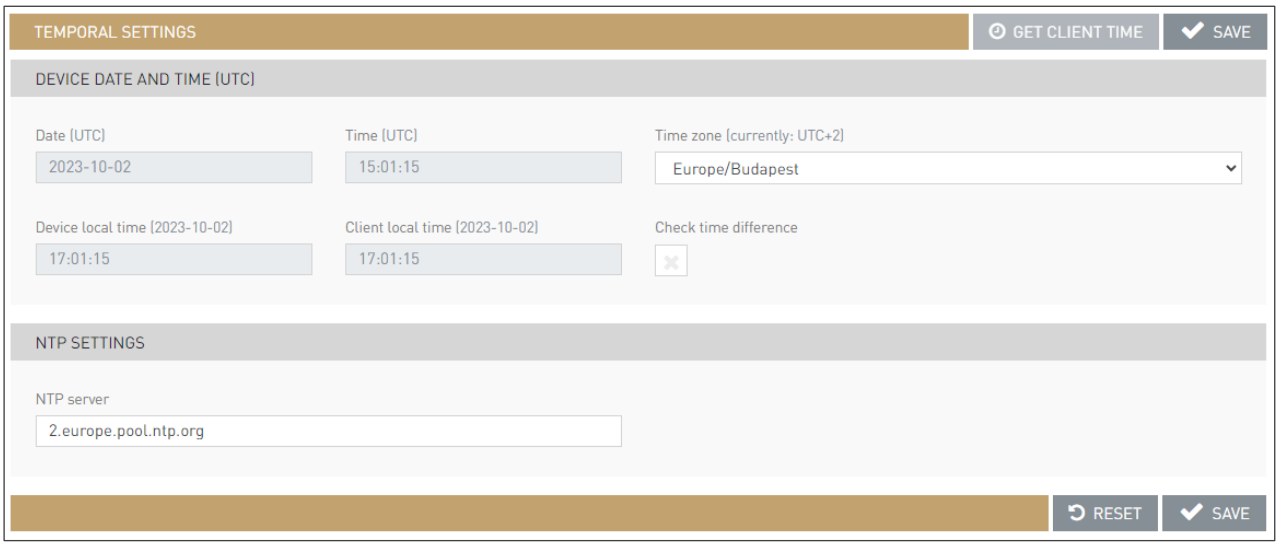


Note

From each role, only one user can be logged in, at the same time. The only exception is the **Owner** that can be logged in together with other, non-owner users.

2.1.2. DATE AND TIME

In the DATE AND TIME menu, you can set the server/device time and select a time zone.



To configure the server/device time, simply type the Date and Time into the corresponding textboxes. As an alternative, click on [GET CLIENT TIME] to adjust date and time to what is set on your computer, tablet or phone. Once the time has been set, click on the [SAVE] button to save the changes.

You can configure the time zone by selecting one of the available options from the dropdown menu under Time zone.

The Device local time and the Client local time are displayed, which thereby can be checked. The Device local time indicates the accurate time of the Osmond N device used by the client while the Client local time indicates the accurate time of the computer, tablet or phone used by the client. In order to enable the time difference checking between Device local time and Client local time, tick the box of the Check time difference option. If there is a low time difference (few seconds) between the document reader and the device connecting to the web interface, then it is indicated on the sign-in window (warning marked in orange). If the time difference is higher, then the color of the notification is marked in red (danger).

In order to ensure constant accurate time on your device, the Osmond supports time synchronization with NTP servers. Enter a valid IP address or a fully qualified domain name of an NTP server to activate NTP sync.

> **Note**
>
> If the NTP server is set, the date and time cannot be specified manually on the interface.

Note

Setting the correct time is necessary for the appropriate operation of the device.

The Osmond device has a built-in protection to prevent access to its web interface when time difference between the scanner and the client device is greater than 30 seconds.

Note

If access to the device fails on the first login attempt, wait 30 seconds then re-try login after pressing Ctrl + F5 in your browser.

The Osmond device is configured to synchronize time via remote time server. When using the device offline, automatic time setting is not performed.

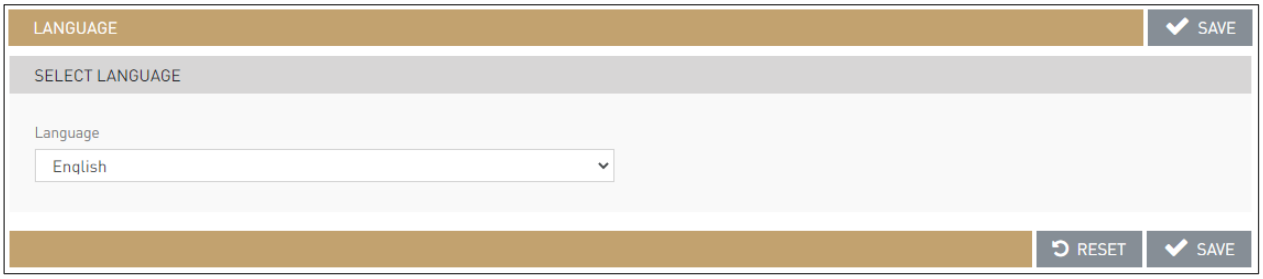
Time-delay information is also visible in the App:

The value of 127 is the time difference to the NTP server in milliseconds. Such low delay is normal; it depends on network speed.

2.1.3. LANGUAGE

In the LANGUAGE menu, you can select the language of your Osmond device web interface.

After language is selected, click [SAVE] to apply changes.



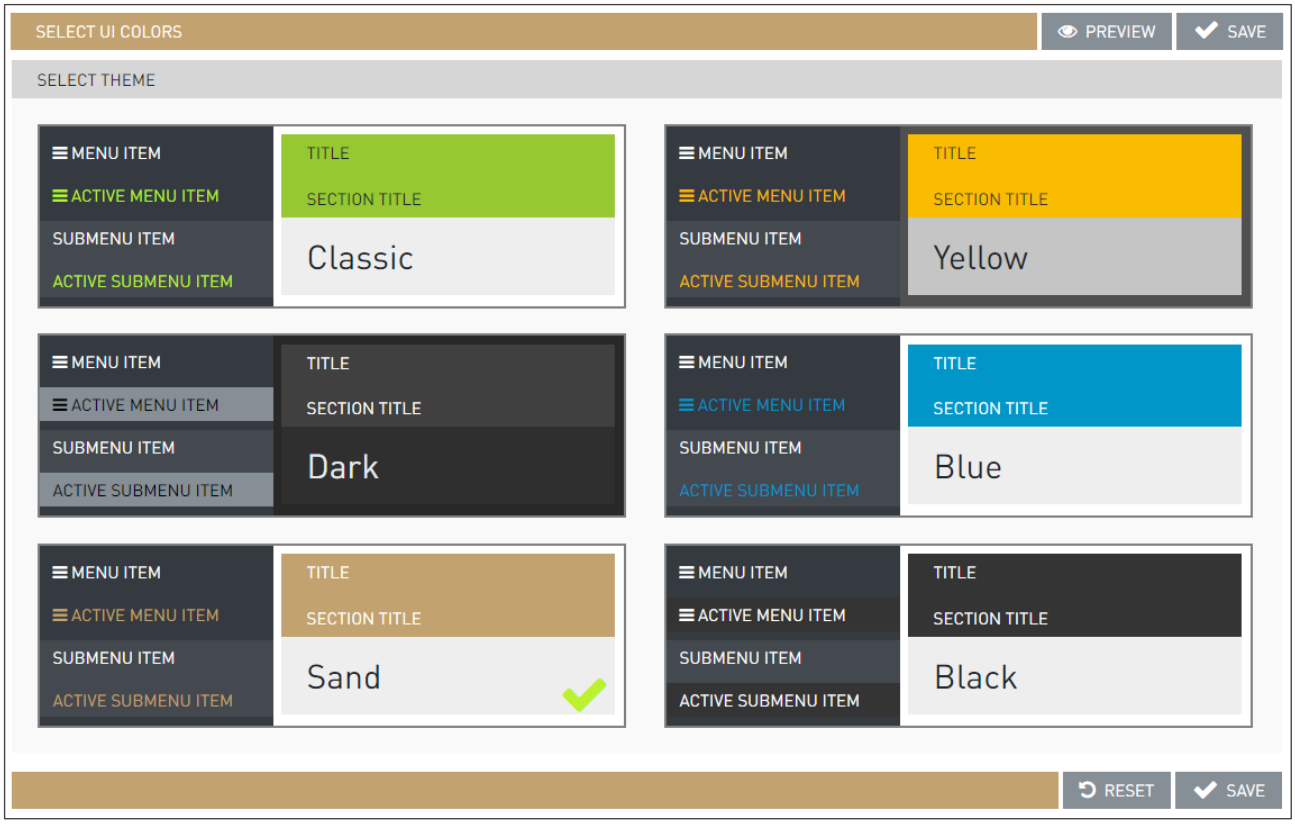
Note

English and Hungarian languages are currently available.

2.1.4. UI COLORS

In the **UI COLORS** menu, the color theme of the user interface can be customized. The selected theme can be viewed by clicking on the **[PREVIEW]** button.

After color theme is selected, click on the **[SAVE]** button to preserve the changes.



2.1.5. ENGINES AND LICENSES

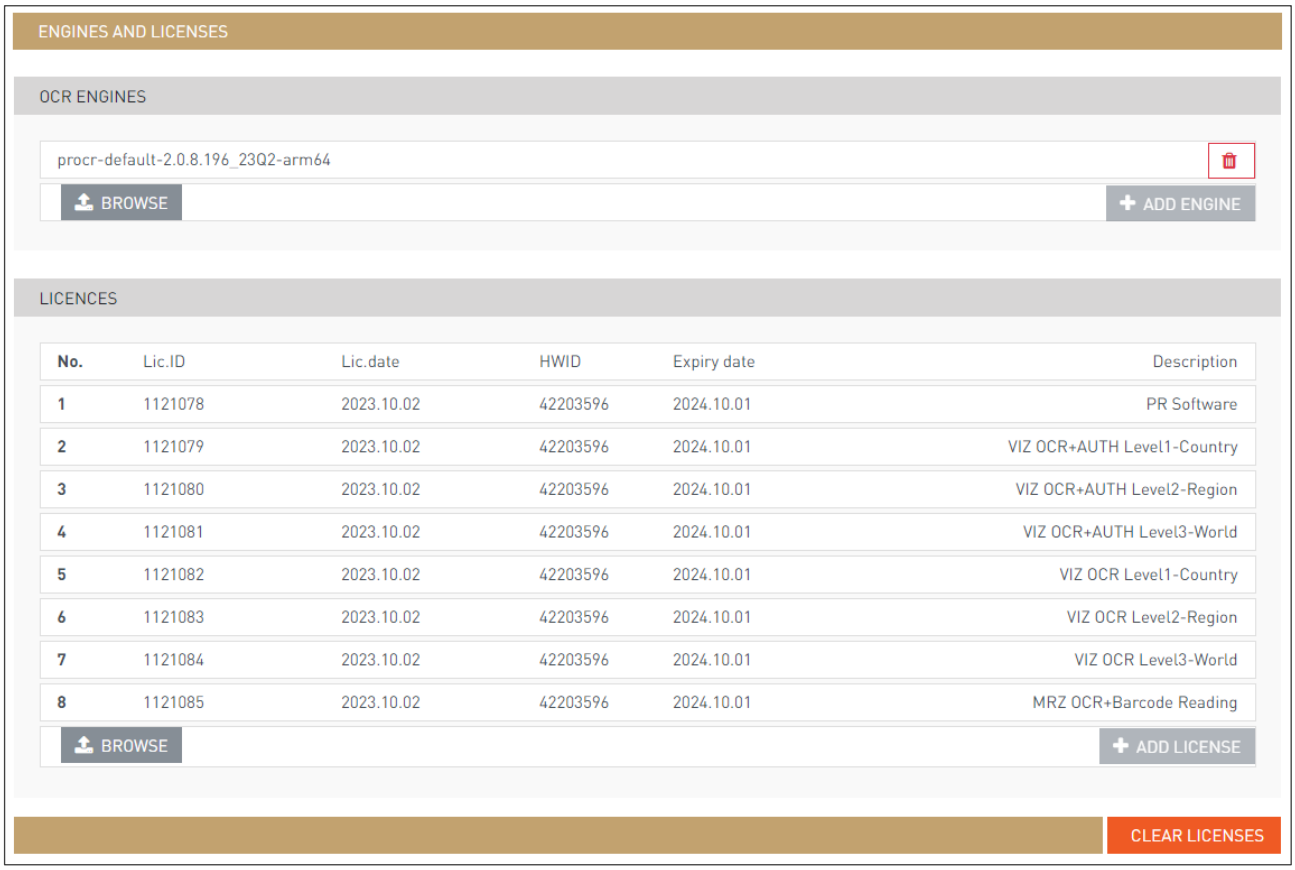
The ENGINES AND LICENSES menu is designed to manage OCR engines and software licenses on the Osmond device.

The selected OCR engine defines:

- what data can be extracted
- if authentication feature is available
- those documents that are supported for the above features

The licenses are listed with the following data under the LICENSES section:

- License ID
- License date
- Hardware ID
- Expiry date
- Description



Note

For availability and more information on OCR engines and software licenses, please contact your ADAPTIVE RECOGNITION sales representative.

Note

For more information on uploading OCR engines, see OCR Engine Management appendix.

Note

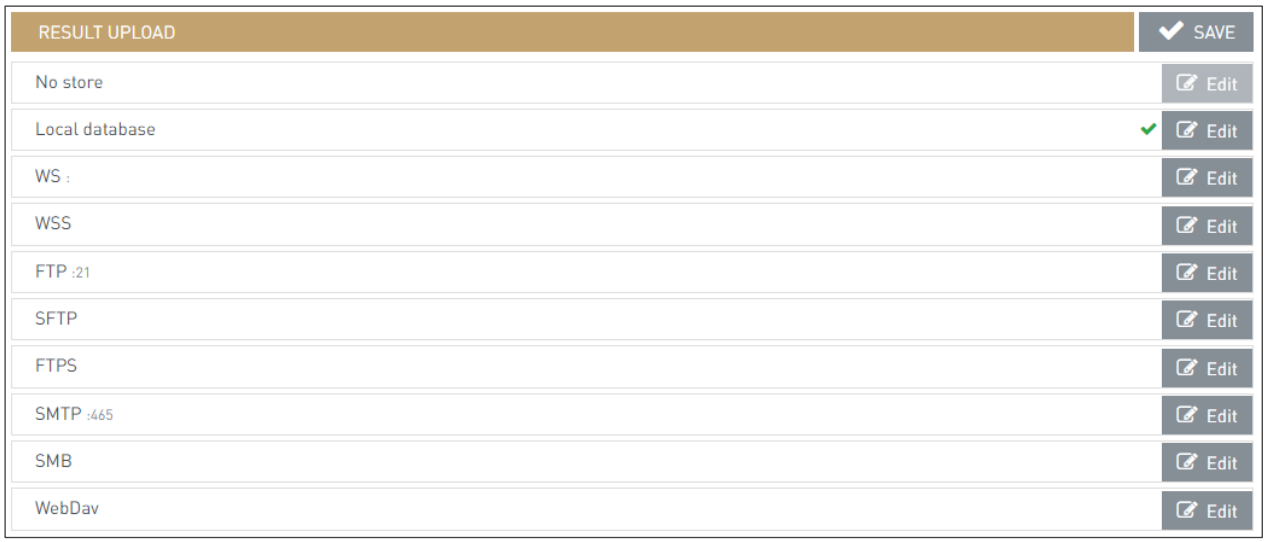
For more information and detail on the Passport Reader licenses and license handling, see License Management appendix.

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

2.1.6. RESULT UPLOAD

The Osmond supports numerous saving options and communication protocols for uploading document images and data to remote targets. Configuration of each protocol can be performed in this menu.

> **Note**
>
> For setting up communication protocols, please contact your IT department or system integrator.

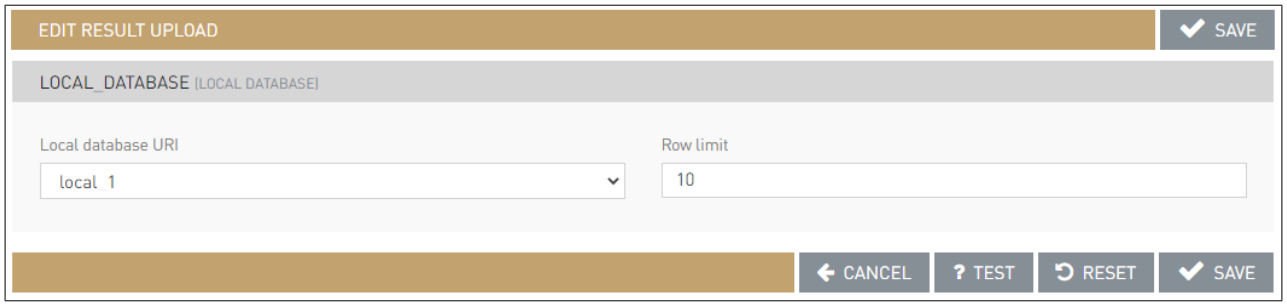


When the only purpose is the scanning, select the No store option. In this case the scanning results can be seen in the START APP menu, but when starting a new scanning, the results of the previous document disappear and cannot be reload from the device. The scanned data is not stored.

> **Note**
>
> In case of devices with firmware version 1.8.x, the No store option is the default setting at RESULT UPLOAD. However, in case of devices with firmware version 1.7.24 and below, the No store option is not going to be the default setting after firmware update either.
>
> No store option is available from 1.8.x version.

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

The Osmond built-in storage offers a feature to save scanned information to the device directly. In order to configure this function, click on **[Edit]** in the line of the **local_database**, then just select "local_1", "local_2" or "local_3" in the **Local database URI** field. Specify a **Row limit** for your database (one scanning corresponds to one row) as well. Once **Row limit** is reached, records in the database are overwritten, starting with the first one. After completing the changes, click on the **[SAVE]** button. Also, make sure to select **Local database** at **Communication protocol** option (MAIN CONFIGURATION).

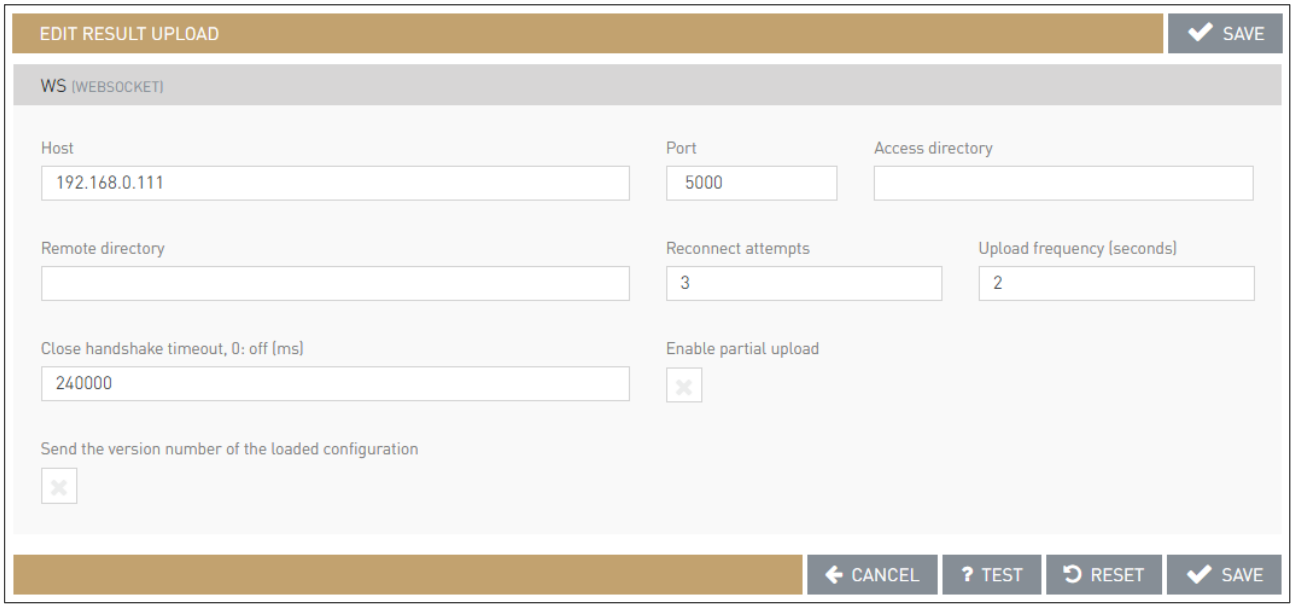


Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

The supported communication protocols:

– WS (WebSocket)

The WS protocol can be customized on the **EDIT RESULT-UPLOAD** window appearing by clicking on the **[Edit]** button in the line of **WS**.



Host, **Port** and **Access directory** can be set in the corresponding text fields by simply typing the desired values. You can specify the name of the folder accessible from the server's root directory with the **Remote directory** field. Enter the number of the **Reconnect attempts** in order to set the maximum number of the connections without error message. The set value of the **Close handshake timeout** defines the period during which the handshake is to be successfully established and fulfilled. The device attempts to upload the data at specified intervals, if the **Upload frequency** field is defined.

> **Note**
>
> The **Enable partial upload** function is currently not supported for Osmond devices.

The device sends the configuration file version in WS header if the box of the **Send the version number of the loaded configuration** is ticked.

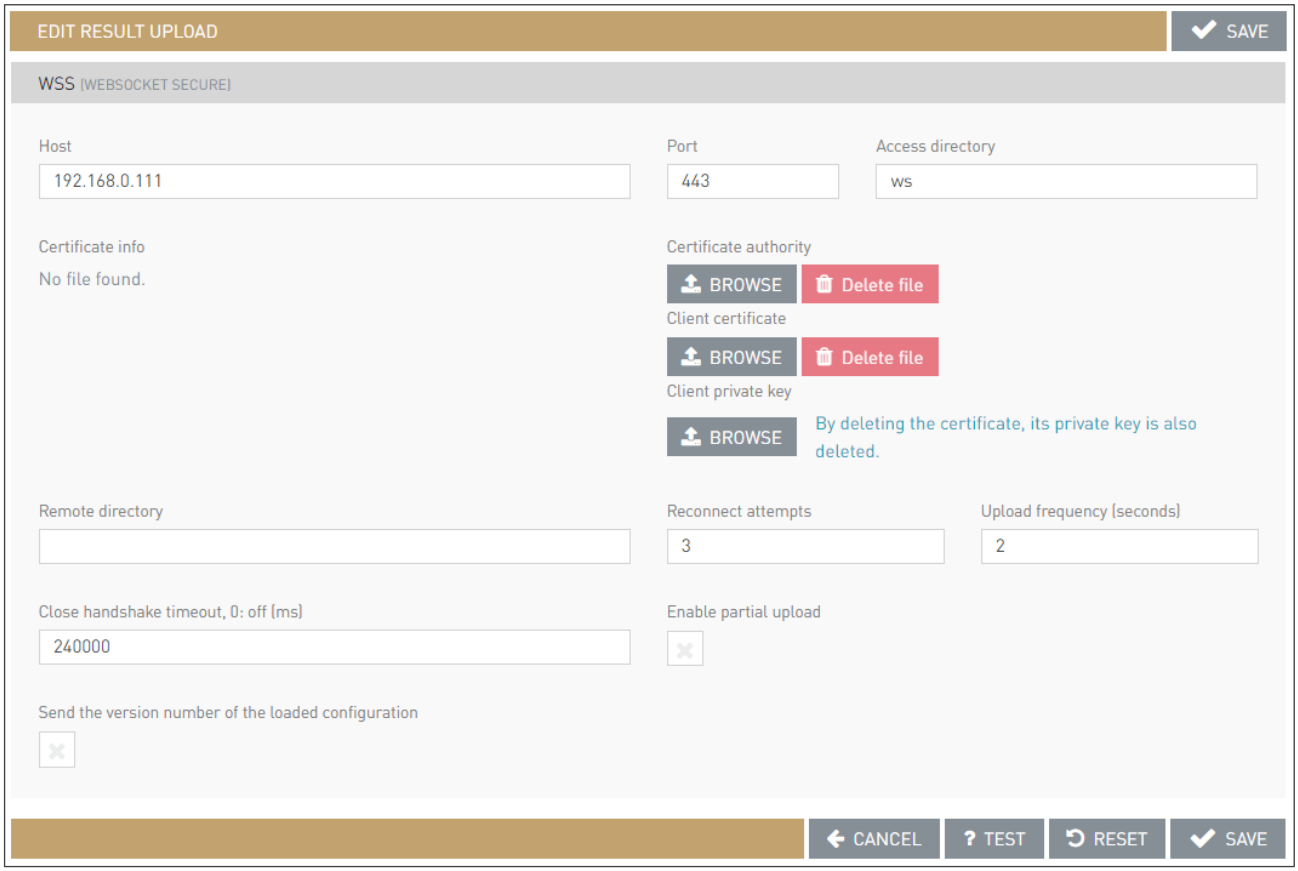
> **Note**
>
> The configuration version can be checked at MAINTENANCE / SYSTEM INFORMATION.

Click **[SAVE]** to apply changes.

Finally, make sure to select **WS** at **Communication protocol** option (MAIN CONFIGURATION).

– WSS (WebSocket Secure)

The WSS protocol can be customized on the **EDIT RESULT-UPLOAD** window appearing by clicking on the **[Edit]** button in the line of **WSS**.



Host, **Port** and **Access directory** can be set in the corresponding text fields by simply typing the desired addresses. Upload **Certificate authority**, **Client certificate** and **Client private key**. To upload the given certificate, click on the **[BROWSE]** button and select the certificate by clicking on the required one and clicking **[Choose file]**. After uploading the certificate files, their details are visible in the **Certificate info** field.

> **Note**
>
> If certificates are uploaded via configuration update from remote server, the "From config update" text is displayed instead of certificate filename in the **Certificate info** box.

You can specify the name of the folder accessible from the server's root directory with the **Remote directory** field. Enter the number of the **Reconnect attempts** in order to set the maximum number of the connections without error message. The set value of the **Close handshake timeout** defines the period during which the handshake is to be successfully established and fulfilled. The device attempts to upload the data at specified intervals, if the **Upload frequency** field is defined.

> **Note**
>
> The **Enable partial upload** function is currently not supported for Osmond devices.

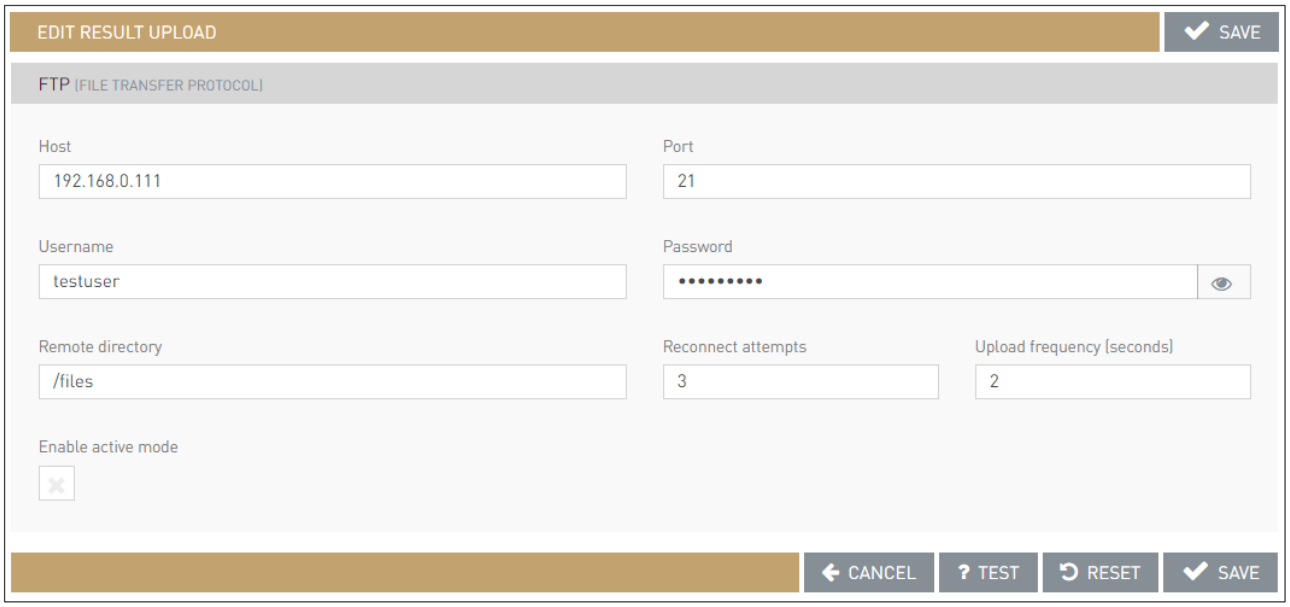
The device sends the configuration file version in WSS header if the box of the **Send the version number of the loaded configuration** is ticked.

> **Note**
>
> The configuration version can be checked at MAINTENANCE / SYSTEM INFORMATION.

Click **[SAVE]** to apply changes. Finally, make sure to select **WSS** at **Communication protocol** option (MAIN CONFIGURATION).

– FTP (File Transfer Protocol)

The FTP protocol can be customized on the EDIT RESULT-UPLOAD window appearing by clicking on the [Edit] button in the line of FTP.



Host and Port can be set in the corresponding text fields by simply typing the desired values. Fill out Username and Password fields.

You can specify the name of the folder accessible from the server's root directory with the Remote directory field. Enter the number of the Reconnect attempts in order to set the maximum number of the connections without error message. The device attempts to upload the data at specified intervals, if the Upload frequency field is defined.

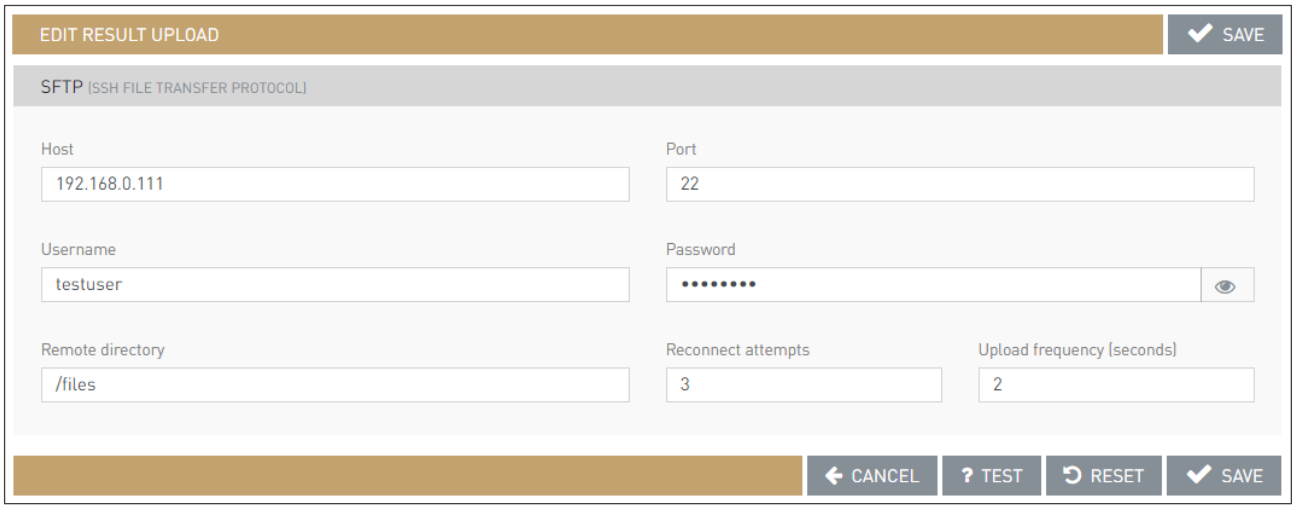
Tick the box in order to Enable active mode.

Click [SAVE] to apply changes.

Finally, make sure to select FTP at Communication protocol option (MAIN CONFIGURATION).

– SFTP (SSH File Transfer Protocol)

The SFTP protocol can be customized on the **EDIT RESULT-UPLOAD** window appearing by clicking on the **[Edit]** button in the line of **SFTP**.



Host and **Port** can be set in the corresponding text fields by simply typing the desired values. Fill out **Username** and **Password** fields.

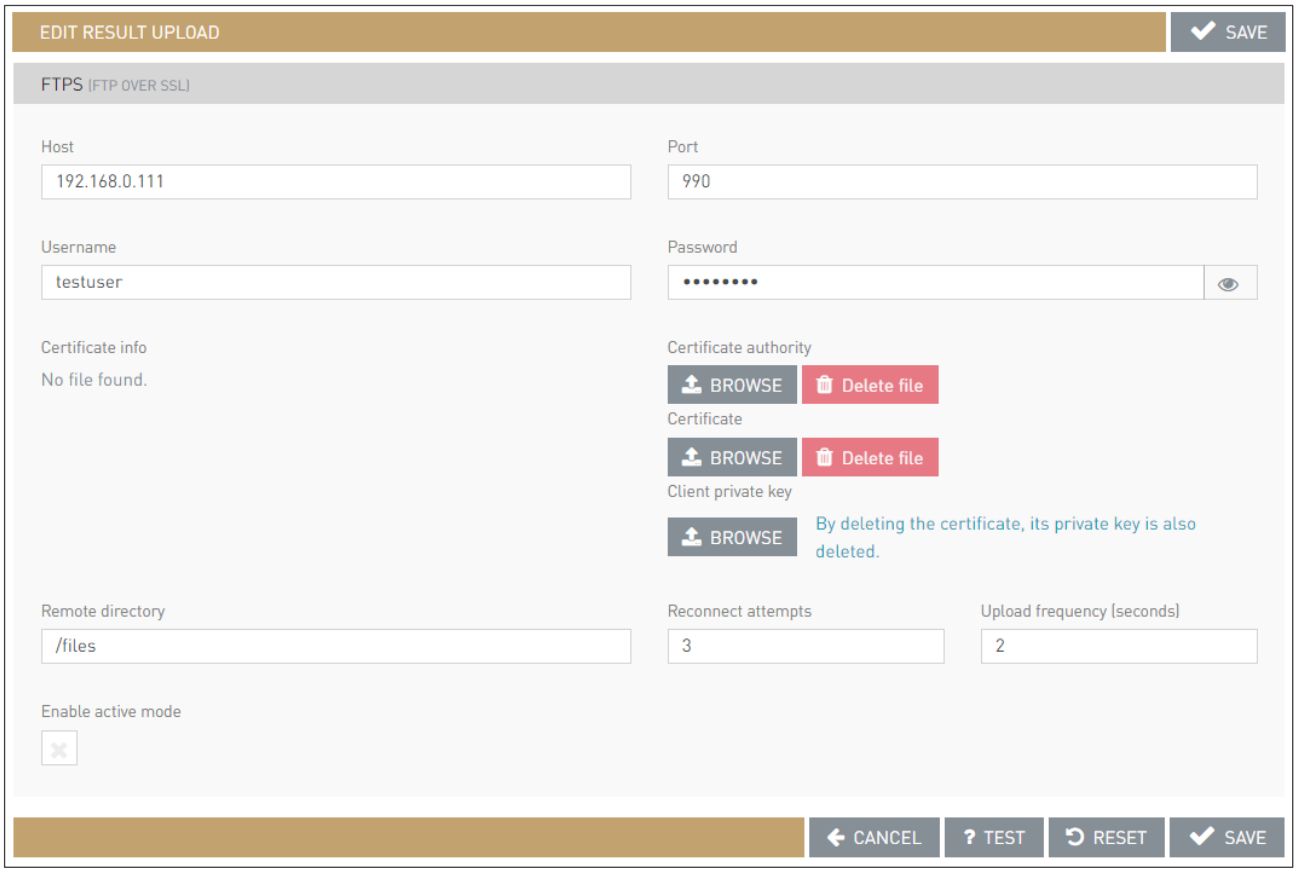
You can specify the name of the folder accessible from the server's root directory with the **Remote directory** field. Enter the number of the **Reconnect attempts** in order to set the maximum number of the connections without error message. The device attempts to upload the data at specified intervals, if the **Upload frequency** field is defined.

Click **[SAVE]** to apply changes.

Finally, make sure to select **SFTP** at **Communication protocol** option (MAIN CONFIGURATION).

– FTPS (FTP over SSL)

The FTPS protocol can be customized on the **EDIT RESULT-UPLOAD** window appearing by clicking on the **[Edit]** button in the line of **FTPS**.



Host and **Port** can be set in the corresponding text fields by simply typing the desired values. Fill out **Username** and **Password** fields.

Upload a **Certificate** by clicking on the **[BROWSE]** button and selecting the corresponding one by clicking on it and clicking **[Choose file]**.

Note

If certificates are uploaded via configuration update from remote server, the "From config update" text is displayed instead of certificate filename in the **Certificate info** box.

You can specify the name of the folder accessible from the server's root directory with the **Remote directory** field. Enter the number of the **Reconnect attempts** in order to set the maximum number of the connections without error message. The device attempts to upload the data at specified intervals, if the **Upload frequency** field is defined.

Tick the box in order to **Enable active mode**.

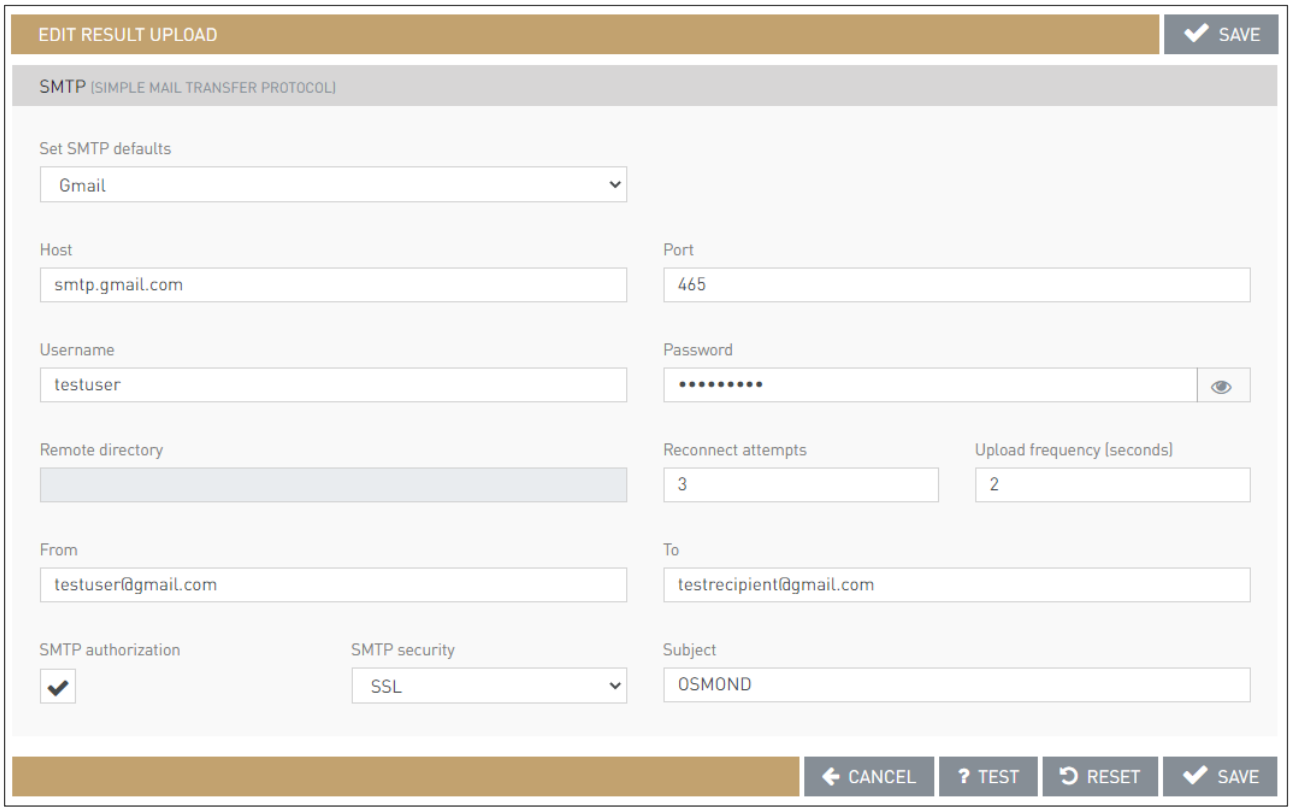
Click **[SAVE]** to apply changes.

Finally, make sure to select **FTPS** at **Communication protocol** option (MAIN CONFIGURATION).

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

– SMTP (Simple Mail Transfer Protocol)

The SMTP protocol can be customized on the **EDIT RESULT-UPLOAD** window appearing by clicking on the **[Edit]** button in the line of **SMTP**.



Select a service from the **Set SMTP defaults** list.

Host and **Port** can be set in the corresponding text fields by simply typing the desired values. Fill out **Username** and **Password** fields.

Enter the number of the **Reconnect attempts** in order to set the maximum number of the connections without error message. The device attempts to upload the data at specified intervals, if the **Upload frequency** field is defined.

Specify the sender's e-mail address in the **From** field and the recipient's e-mail address in the **To** field. Define the **Subject** of the mail to easily identify the mail containing the scan results. Tick the box in order to enable **SMTP authorization**.

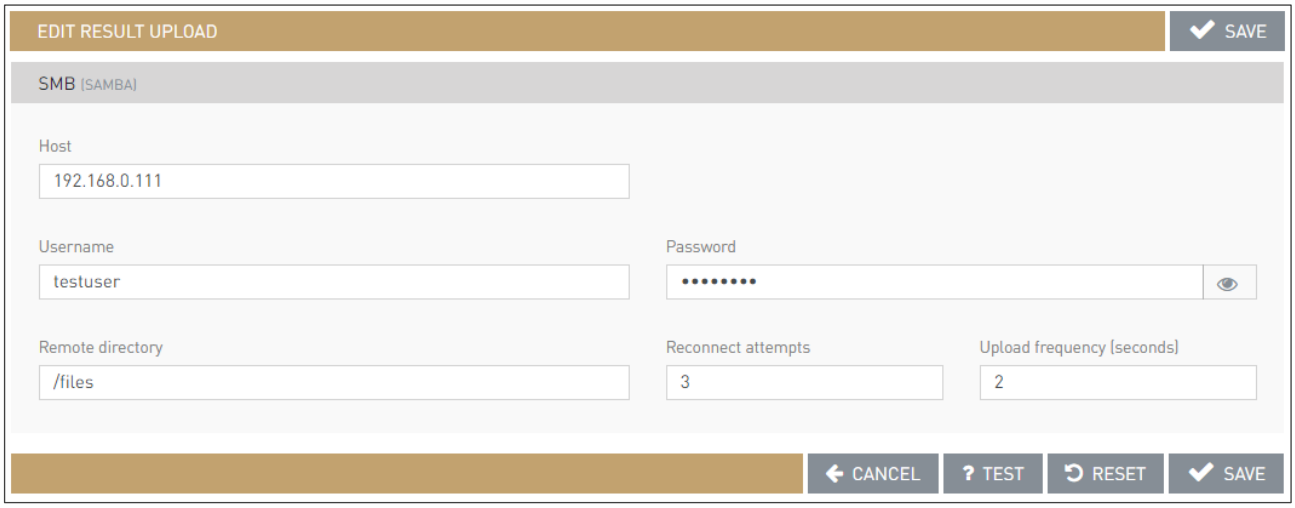
In order to secure the SMTP mail, select a cryptographic protocol from the **SMTP security**.

Click **[SAVE]** to apply changes.

Finally, make sure to select **SMTP** at **Communication protocol** option (MAIN CONFIGURATION).

– SMB (Server Message Block)

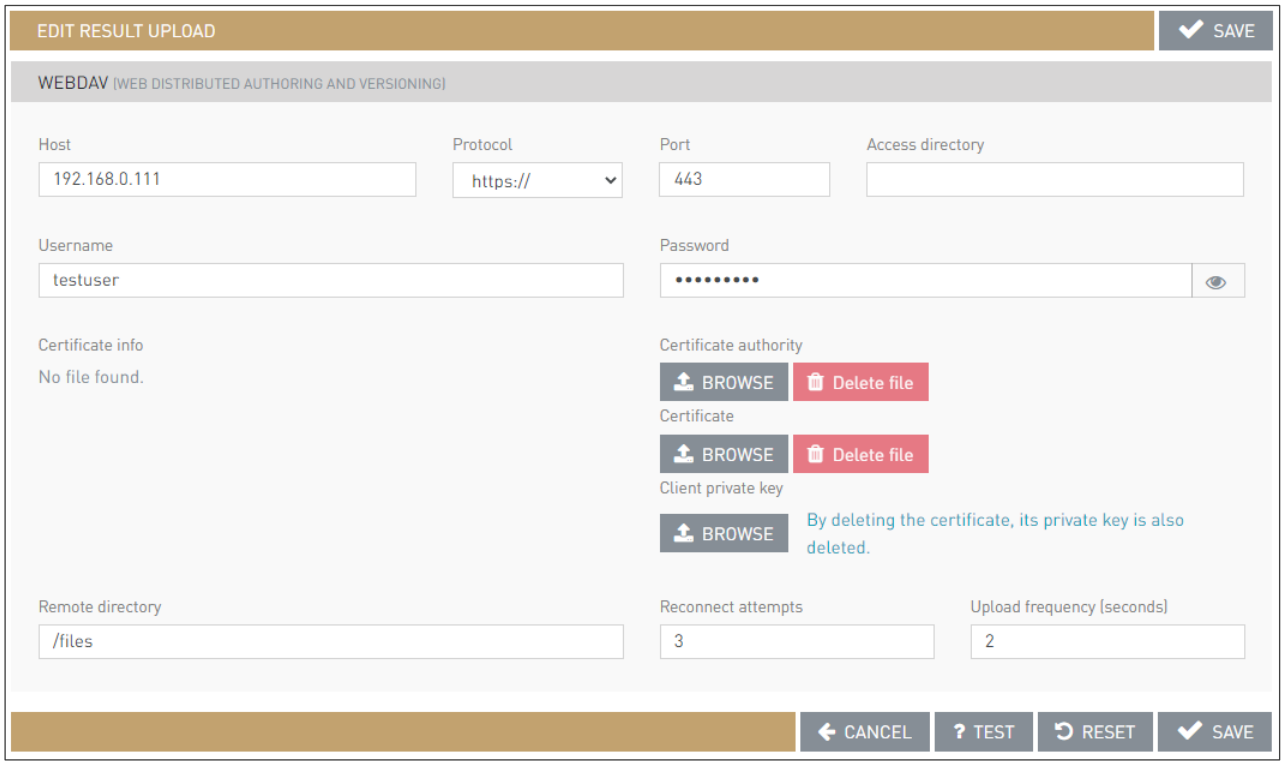
The SMB protocol can be customized on the EDIT RESULT-UPLOAD window appearing by clicking on the [Edit] button in the line of SMB.



Host can be set in the corresponding text field by simply typing the desired value.
Fill out Username and Password fields.
You can specify the name of the folder accessible from the server's root directory with the Remote directory field. Enter the number of the Reconnect attempts in order to set the maximum number of the connections without error message. The device attempts to upload the data at specified intervals, if the Upload frequency field is defined.
Click [SAVE] to apply changes.
Finally, make sure to select SMB at Communication protocol option (MAIN CONFIGURATION).

– WebDAV (Web Distributed Authoring and Versioning)

The WebDAV protocol can be customized on the EDIT RESULT-UPLOAD window appearing by clicking on the [Edit] button in the line of WebDAV.



Host, Port and Access directory can be set in the corresponding text fields by simply typing the desired values. Select a Protocol from the drop-down list. Fill out Username and Password fields. Upload Certificate authority, Certificate and Client private key. To upload the given certificate, click on the [BROWSE] button and select the certificate by clicking on the required one and clicking [Choose file]. After uploading the certificate files, their details are visible in the Certificate info field.

Note

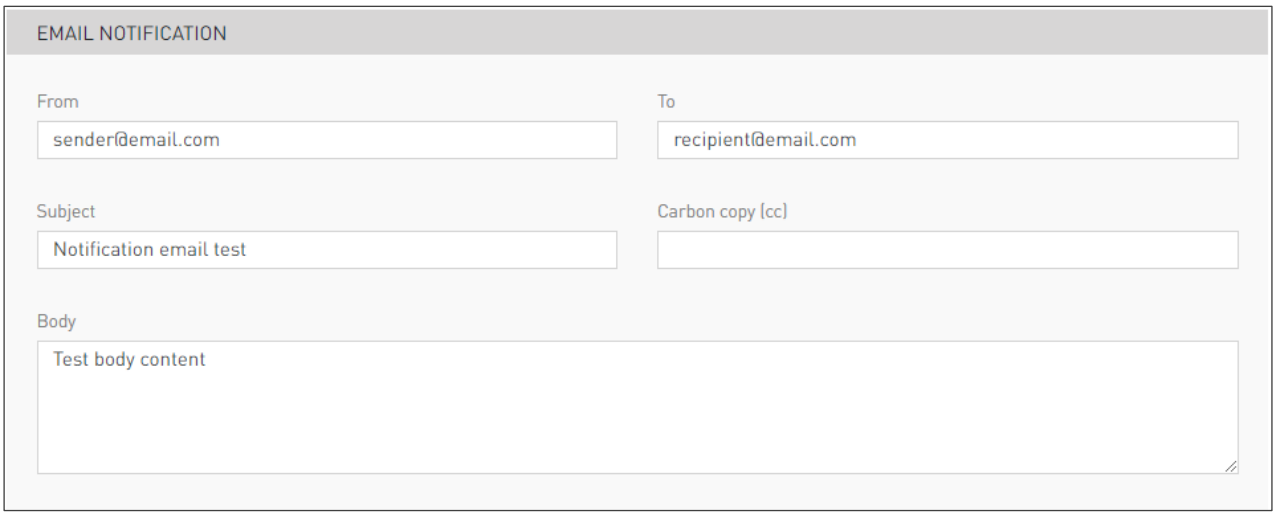
If certificates are uploaded via configuration update from remote server, the "From config update" text is displayed instead of certificate filename in the Certificate info box.

You can specify the name of the folder accessible from the server's root directory with the Remote directory field. Enter the number of the Reconnect attempts in order to set the maximum number of the connections without error message. The device attempts to upload the data at specified intervals, if the Upload frequency field is defined.

Click [SAVE] to apply changes.

Finally, make sure to select WebDAV at Communication protocol option (MAIN CONFIGURATION).

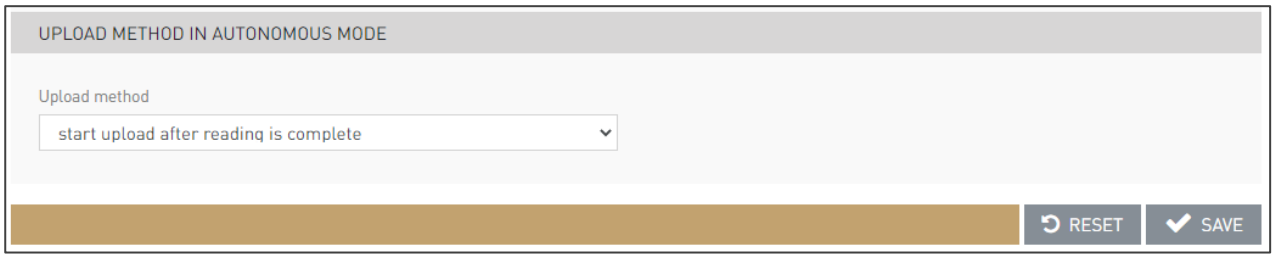
Besides uploading data to remote hosts, the Osmond also supports sending automatic e-mail notifications on scanned documents.



Just fill in the standard e-mail parameters and configure SMTP settings in ADMINISTRATION / RESULT UPLOAD / SMTP menu as well as make sure to enable the EMAIL NOTIFICATION option in the MAIN CONFIGURATION menu.

Under the RESULT UPLOAD menu can be selected the UPLOAD METHOD IN AUTONOMOUS MODE. The owners may choose between the following options:

- start upload after removing a document: the document upload should start right after the document has been removed from the scanner
- start upload after reading is complete: the document upload should start right after the document processing is finished



2.1.7. LOG UPLOAD

The **LOG UPLOAD** menu is designed to upload operation log files to remote log servers. The **LOG UPLOAD** menu can be configured by entering the parameters of one of the following protocols:

- SFTP
- FTPS
- SMB
- WebDav

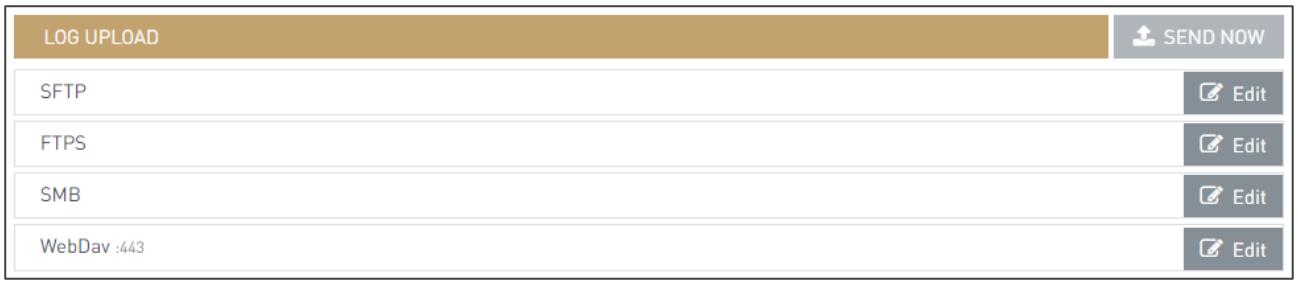
> **Note**
>
> It is recommended to select one of the protocols including encryption (SFTP, FTPS, Webdav).

Only those protocols can be selected from the list, that have the following parameters specified:

- Host
- Username
- Password

These parameters can be specified by clicking on the **[Edit]** button.

> **Note**
>
> Modification of the upload parameters restarts the ongoing upload process.



> **Note**
>
> Log files (syslog and API log) can be downloaded under **MAINTENANCE / SYSTEM INFORMATION / LOG MANAGEMENT**.

ARCHIVE LOG UPLOAD

When rotating the log file, this mode uploads the log file and the system starts a new one.

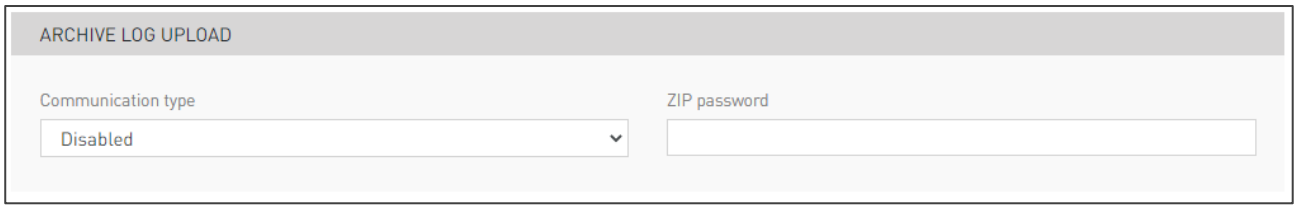
There is a system level logrotate which is performed every day at 00:00. At this time the syslog is saved as zip file, which is automatic. The syslog includes the log written by the software running in the system, with the exception of the API. API writes separately its log.

Under **Communication type** the preferred protocol can be selected from the following options.

- Disabled
- SFTP
- FTPS
- SMB
- WebDav

> **Note**
>
> If the Disabled option is selected, the upload is not performed.

In case of specifying the **ZIP password** field, the compressed file is password protected. If the field is left blank, there is no password protection on the zip file. The recommended minimum password length is 13 characters.



The immediate upload of the current log file (SEND NOW button):

There is a possibility to upload the already collected log manually. By clicking on the **[SEND NOW]** button located in the upper right corner, the current log file is zipped and sent to the location with a method as specified in the settings (see above). When using the **SEND NOW** function, the syslog generated between 00:00 and the time of the button press is saved as zip file.

REAL TIME LOG SENDING

The syslog can be transmitted in real-time. In order to enable the **Real time sending** function, tick the appropriate box. This function transmits the log line by line when it is generated. Thus, only single lines are sent not the entire syslog zipped.

The connection can be secured by ticking the **Use secure connection** box.

> **Note**
>
> When the **Use secure connection** function is enabled, the **TCP** protocol will be used for communication and the **FQDN** must be typed to the **IP address or FQDN** field.

Under **Protocol** select the preferred one, which can be TCP or UDP.

IP address or FQDN field can be set in the corresponding text field by typing the required value.

To the **Port** field enter the number of the port where the log server is waiting for the data.

The Osmond requires certificates for secure connection. Upload the:

- **Certificate authority:** the authority with which they signed the certificate
- **Certificate**: the certificate with which the client identifies themselves (used for encryption)
- **Client private key**: the private key of the client

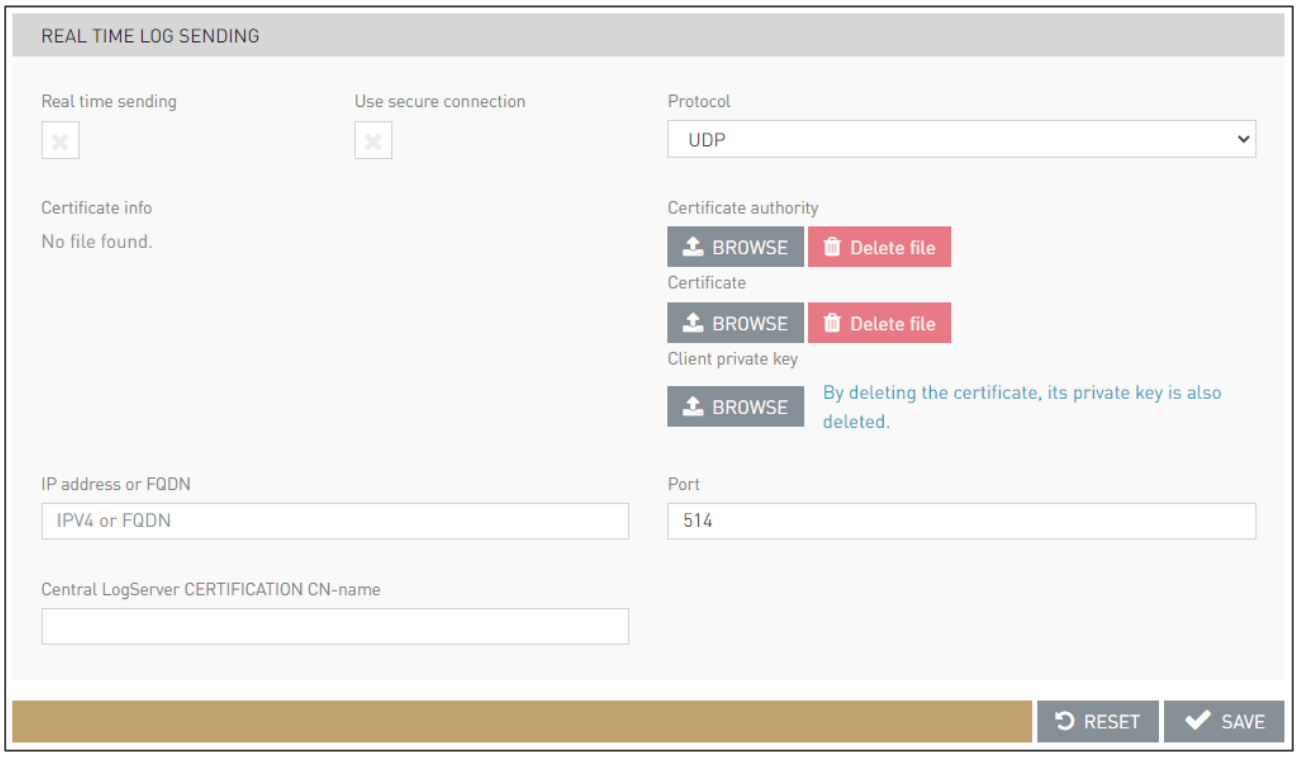
To upload the given certificate, click on the **[BROWSE]** button and select the certificate by clicking on the required one and clicking **[Choose file]**. After uploading the certificate files, their details are visible in the **Certificate info** field.

> **Note**
>
> If certificates are uploaded via configuration update from remote server, the "From config update" text is displayed instead of certificate filename in the **Certificate info** box.

> **Note**
>
> The upload of the **Certificate authority** is optional. It is required when the certificate is e.g., self-signed. If the authority is generally accepted, e.g., it is known by the OS too, the upload of it is not required.
> The format of the **Certificate**, **Certificate authority** and the **Client private key** must be PEM.

> **Note**
>
> The device can also use certificate or key towards the log server.

Enter the Log server common name into the **Central LogServer CERTIFICATION CN-name** field. This is an optional field. In case of specifying it, the connection is only established when the server corresponds to this. The identification is performed based on the CN-name.



2.1.8. DATABASE UPLOAD

In case of storing the reading in local database, the upload of the stored database can be set by defining the parameters of one of the following protocols:

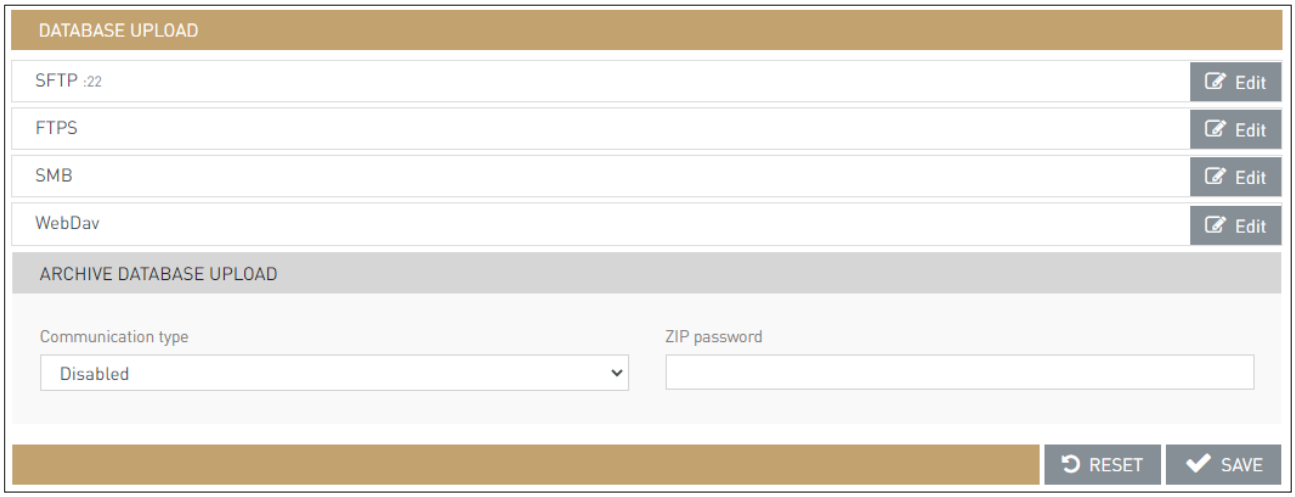
- SFTP
- FTPS
- SMB
- WebDav

Only those protocols can be selected from the list, that have the following parameters specified:

- Host
- Username
- Password

> **Note**
>
> Modification of the upload parameters restarts the ongoing upload process.

Under **Communication type** the preferred protocol can be selected. In case of specifying the **ZIP password** field the compressed file is password protected.



2.1.9. CONFIG UPLOAD

Important!

Only those configuration files can be uploaded to the device which are signed by ADAPTIVE RECOGNITION or possibly by the client. In both cases contact our Support Team.

The device is able to download automatically the configuration files. The operation of the device can be affected by the parameters included in these configuration files. This requires the operation of a HTTP/HTTPS server and the creation of an environment ideal for device configuration.

Note

For more information, please refer to the Setting the Configuration and Software Update on Osmond Device through Network chapter of the Osmond User Manual.

The configuration values can be uploaded in j_on file format. The j_on extension configuration file is **not JSON**, because it consists of two concatenated JSON structure and contains notes. Its field names can be formatted from the names of the properties included in the table in such way that the name-sections separated by slash symbols (/) give the levels of the JSON structure.

Example

ResultUpload/FTP/access_directory property in JSON format:

```
{ "ResultUpload/FTP/access_directory": "access_directory":
"/tmp/wss/" }
```

The **two-valued fields** can take '1' (meaning yes/true) or 'void string' (meaning no/false) values.

In the following section the j_on file structure and its formal requirements will be explained.

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

J_on file structure and formal requirements:

Each block begins with a comment depending on which table you want to insert it into.

These can be (without quotation marks):

- "//Properties"
- "//Doc_fields"

After that, the aforementioned values follow per blocks separated by comma in square brackets ([...]).

Only one "//Properties []" and one "//Doc_fields []" can be included: either "//Properties []" or "//Doc_fields []" or both.

The "//End" comment closes the structure at the end, after which the Enter key must be pressed.

A double table j_on file example:

```
//Properties
[
    {
        "app/summary_isText" : "1"
    },
    {
        "net/0/prefix" : "lan"
    }
]
//Doc_fields
[
  {
        "category" : "RFID",
        "customName" : "",
        "customOrder" : "",
        "defaultName" : "AuthTerminal",
        "defaultOrder" : "1",
        "isShowInOcr" : "",
        "isShowInRfid" : "",
        "isShowInSummary" : "",
        "label" : "AuthTerminal"
    },
    {
        "category" : "Additional data",
        "customName" : "",
        "customOrder" : "",
        "defaultName" : "Composite47",
        "defaultOrder" : "1",
        "isShowInOcr" : "",
        "isShowInRfid" : "",
        "isShowInSummary" : "",
        "label" : "Composite47"
    }
]
//End
```

Currently supported values:

- UpdateServerMain/update_time
- UpdateServer/1/host:
- UpdateServer/1/remote_directory
- UpdateServer/1/protocol
- UpdateServer/1/password
- ResultUpload/WSS/access_directory
- ResultUpload/WSS/host
- ResultUpload/WSS/authority/RawData
- ResultUpload/WSS/authority/UploadName
- ResultUpload/WSS/certificate/RawData
- ResultUpload/WSS/certificate/UploadName
- ResultUpload/WSS/private_key/RawData
- ResultUpload/WSS/private_key/UploadName
- ResultUpload/WSS/reconnect_attempts
- ResultUpload/WSS/upload_frequency
- UpdateServer/1/username
- LogUpload/ipAddress
- LogUpload/port
- LogUpload/protocol
- LogUpload/isRealtimeUpload
- queue/check_interval
- queue/minimal_available_space
- queue/package_limit
- queue/corrupted_package_limit
- queue/queue_warning_interval
- queue/should_send_queue_warning
- queue/is_delete_deferred_uploads
- queue/is_delete_corrupted_uploads
- run/configVersion
- ResultUpload/WSS/close_handshake_timeout

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

For remote device management, the upload of the J_on configuration file can be set by defining the parameters of one of the following protocols:

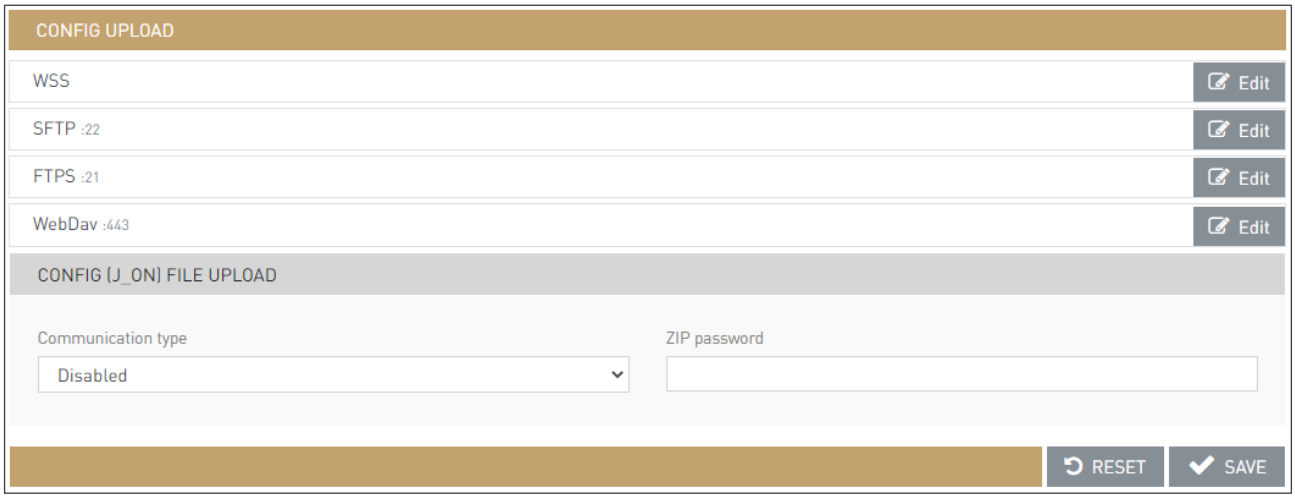
- SFTP
- FTPS
- SMB
- WebDav

Only those protocols can be selected from the list, that have the following parameters specified:

- Host
- Username
- Password

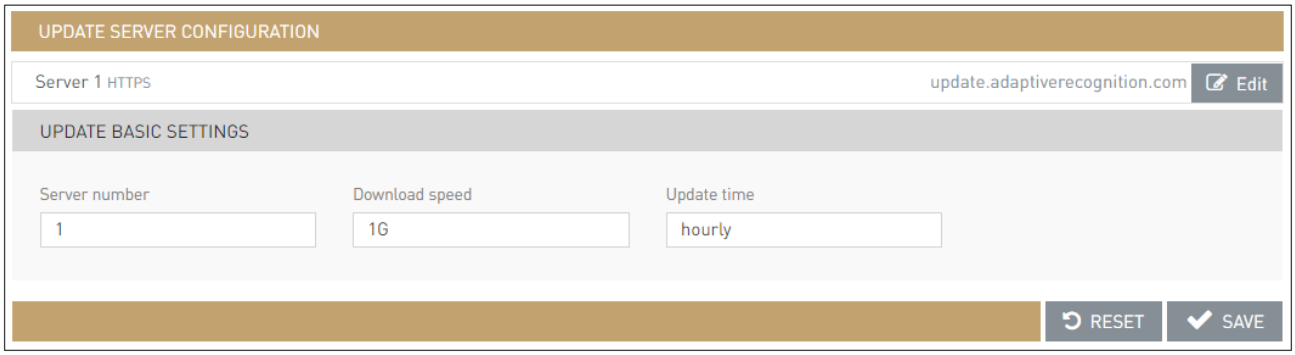
> **Note**
>
> Modification of the upload parameters restarts the ongoing upload process.

Under **Communication type** the preferred protocol can be selected. In case of specifying the **ZIP password** field the compressed file is password protected.



2.1.10. UPDATE SERVER

The Osmond device is capable of downloading and installing device firmware and configuration updates automatically, from remote servers.

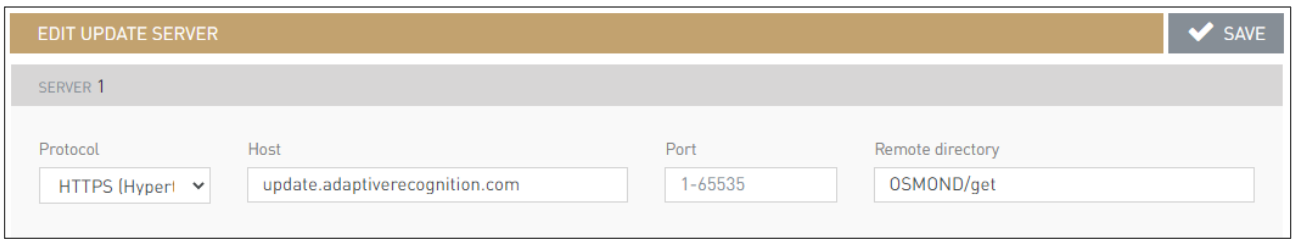


The device supports max. 9 remote servers (**Server number**) with **Download speed** and **Update time** configuration.

The **Download speed** can be specified in second/byte but the 'k', 'M' and 'G' letters can also be used. E.g., 1G stands for 1 Gigabyte. When set to 0, there is no speed limit.

Update time can be expressed using the 'daily', 'hourly' and 'weekly' expressions. For advanced setting, use 'cron' time expression. E.g., "0 */2 * * *" to check for updates in every two hours.

Upon clicking **Edit**, you may specify access details to the remote server. By default, it is configured to ADAPTIVE RECOGNITION update server.

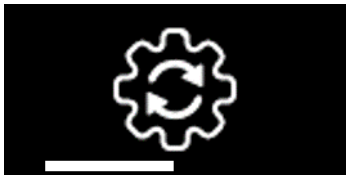


The Osmond device searches for updates at every start up. If new firmware or configuration file is available, it is downloaded automatically. Depending on the update, the device is either restated automatically after software download or not. In either way, installation of the update is performed at the next device start-up.

Note

The default update server is "update.adaptiverecognition.com". For more information on it, contact ADAPTIVE RECOGNITION support or sales team.

The update process is marked by a cogwheel icon with a progress bar on the device display:



When the installation of the new software is finished, a cogwheel with the tick is displayed:

If updating fails for any reason, that is also signaled on the device display:

Note

Username and Password protection is not yet supported for update servers.

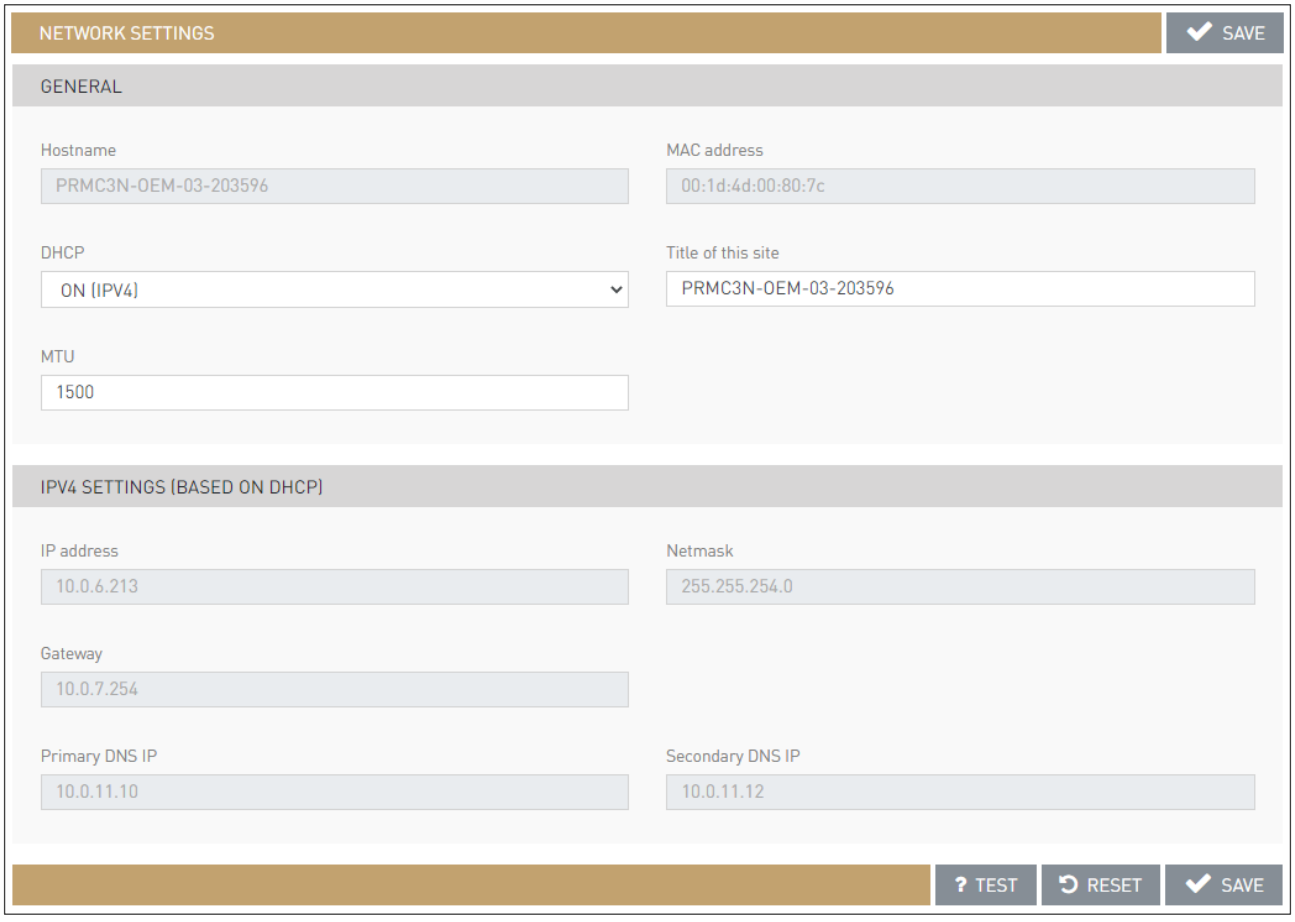
Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

2.2. NETWORK

2.2.1. LAN

In the NETWORK menu, the local network connection of the device can be set. This setting is required to enable local network availability and upload results to an external network.
In this menu, you can inspect the Hostname and MAC address. You can also change Netmask, DNS IP as well as IP addresses of the Osmond device. In special cases MTU field can be specified.

> **Note**
>
> Network parameters can be modified by users with owner or network admin privileges.

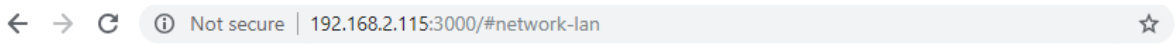


Once all the necessary changes have been made, click on [SAVE] to preserve the changes.

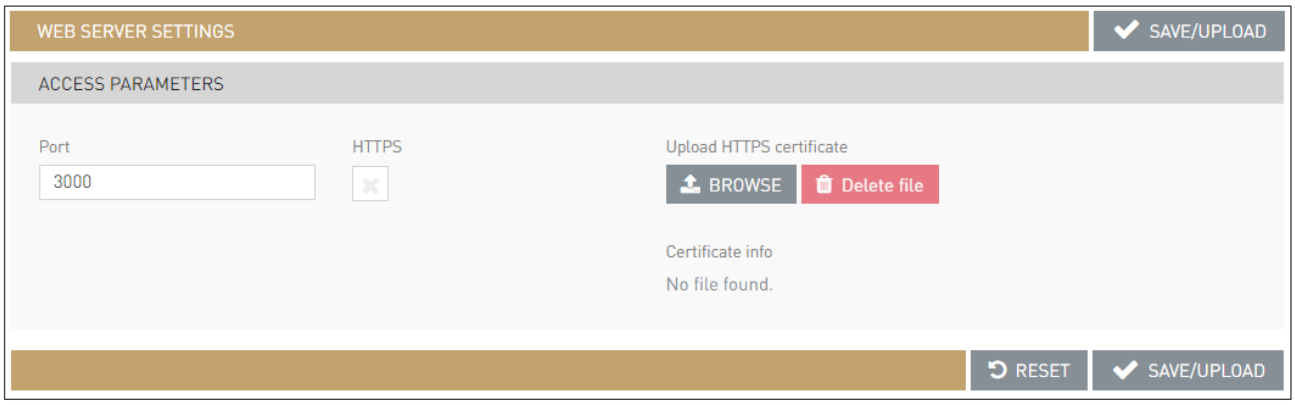
2.2.2. WEB SERVER

In the WEB SERVER menu, you can configure the parameters of accessing the web interface of the device. Such parameters include the following:

- set the port of the web server - this port value is present in the browser address bar:



- enable or disable HTTPS (requires HTTPS cert. for both the web browser and web interface)
- upload a HTTPS certificate for accessing the web interface of the device



The Osmond device requires SSL certificate for HTTPS connection. This certificate should be uploaded in the NETWORK / WEB SERVER menu (using the Upload HTTPS certificate button) and must have .pem format that includes both the public certificate and the private key.

> **Note**
>
> Keys protected by passwords are not supported by the device.

Port

To change the port number simply click into the **Port** text field and enter a desired port number. Make sure to click **[SAVE]** to apply any modified value.

> **Note**
>
> Port value cannot be lower or equal to 1024.

HTTPS

To enable or disable the use of HTTPS protocol for device communication, simply check or uncheck the checkbox next to **HTTPS**.

HTTPS Certificate

To upload a HTTPS certificate, click on the **[BROWSE]** button and select the certificate by clicking on that you want to upload by clicking on **[Choose file]**.

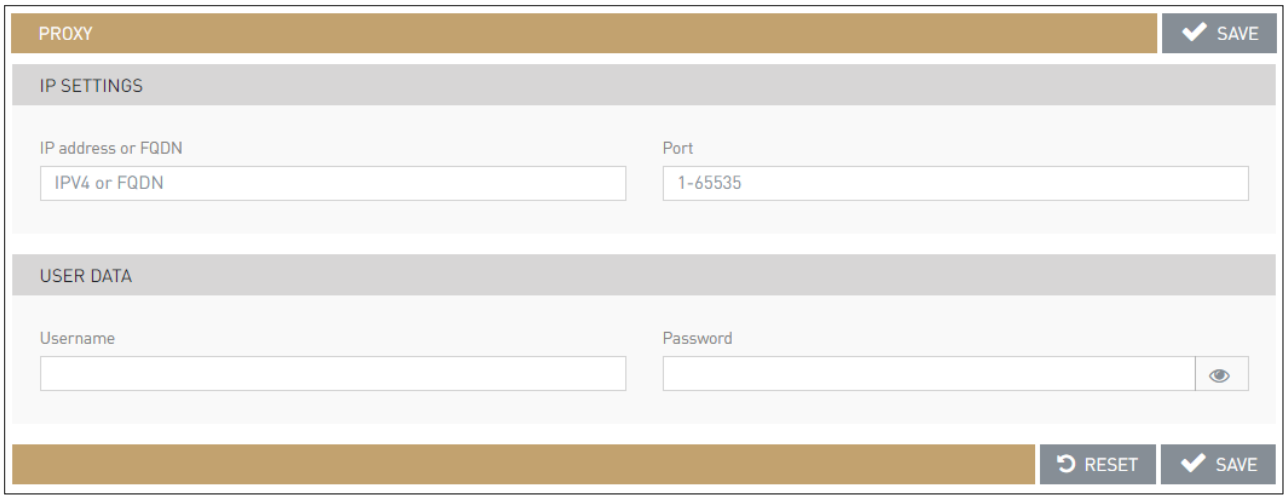
> **Note**
>
> In order to appear admin interface of the device as trusted website, your certificate must be installed to your web browser manually.

> **Note**
>
> For successful HTTPS connection, the rootCA of the uploaded certificate must be added to the browser trusted publishers list.

> **Note**
>
> For more information on the steps of establishing HTTPS connection, see Using HTTPS Protocol with Osmond Devices chapter.

2.2.3. PROXY

When uploading any image or data to a remote server, there might be a need to configure a proxy server – if such server is used to establish connection between the device and the target network then its parameters can be set in the PROXY menu:



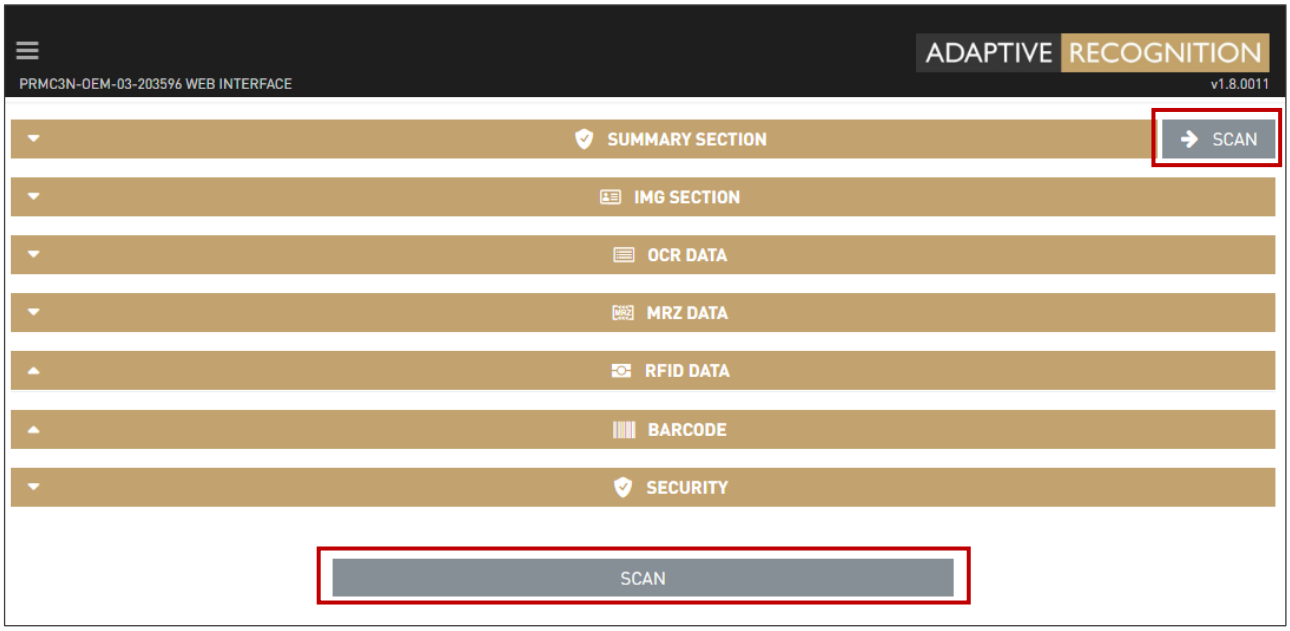
IP address or FQDN and Port of the Proxy server can be set in the corresponding text fields by simply typing the desired values. If the Proxy server requires authentication, set the Username and Password in the USER DATA section. Make sure to click [SAVE] to apply any new values.

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

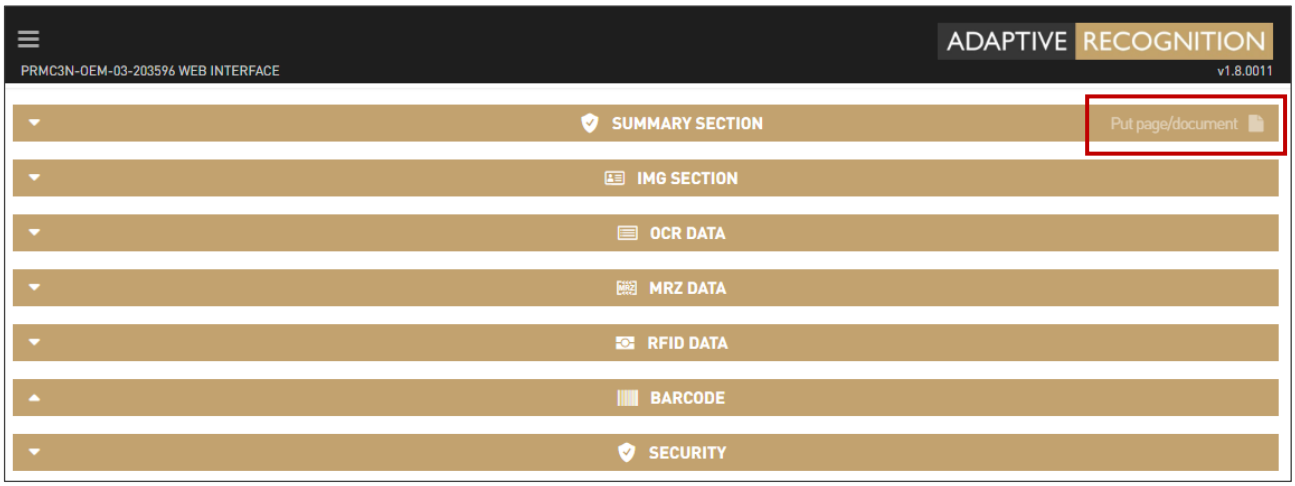
2.3. APPLICATION

2.3.1. START APP

The Osmond device includes a built-in application to scan document images, perform OCR and authentication, read barcodes and RFID chip information and to send the results to a specific target. In **Interactive** scan mode (see MAIN CONFIGURATION) just click **[SCAN]** to scan & process a document.



In **Autonomous** mode (see MAIN CONFIGURATION) just wait until **Put page/document** can be seen on the screen (in the line of **SUMMARY SECTION**).



Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

Note

The pictograms appearing in the upper right corner indicate the phases of the reading process depending on the given scanning mode. For more details on the pictograms and their meanings see Web Interface Reading Phases – Icon Description appendix.

Note

The icons appearing on the OLED display indicate the status of the reading process regardless of the scanning mode. For more details on the display icons and their meanings see OLED Display Status Icons of Osmond Network Devices appendix.

Acquired information from a document scan is organized into different sections, based on the content of the read data. By default, the **Application** displays the following sections:

1. SUMMARY SECTION

The **SUMMARY SECTION** reflects the overall status of document validity. Here you can inspect the image of the document as well as segmented MRZ data and RFID image (if available).

Note

The **SUMMARY SECTION** shows data fields that are configured in the **EDIT APP / FIELD SETUP** menu.

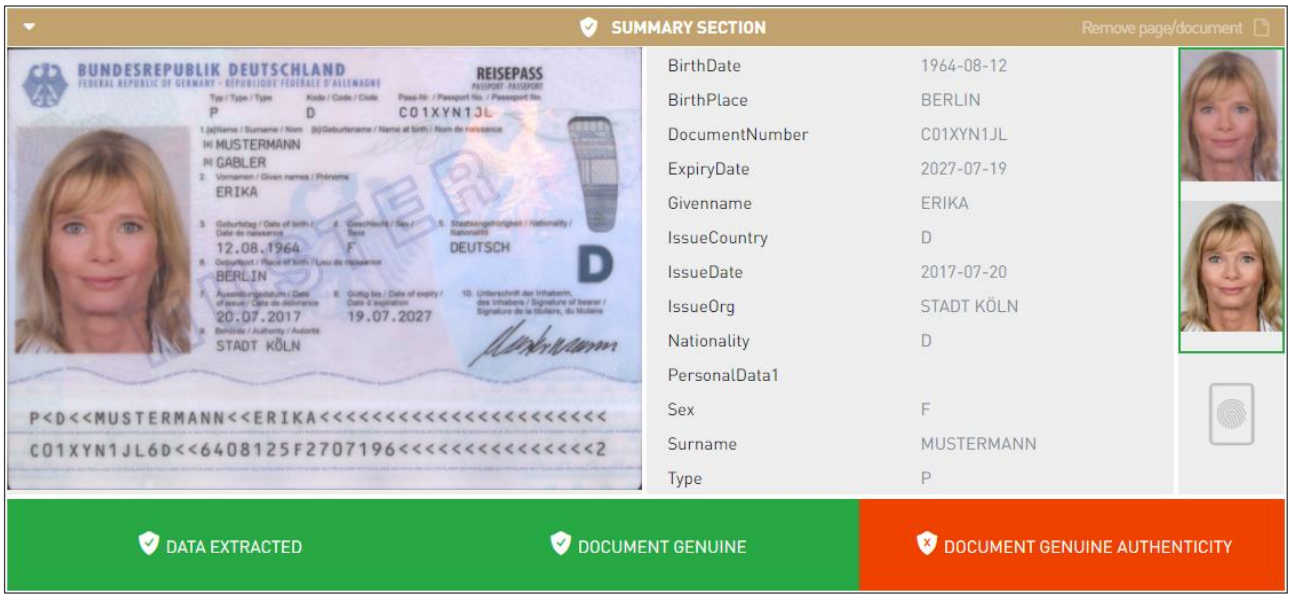
The **Data extracted** and **Document genuine** sections provide feedback on whether the read data is correct (valid values with correct checksum) and genuine (result of security checks including RFID authentications).

1. **Data extracted**: Processing data
   - Error (red), if there is an error in the **RFID** and/or **MRZ** sections
   - Warning (orange), if no MRZ line has been read
2. **Document genuine**: Checking the document
   - Error (red), if the **SECURITY**, **OCR** and/or **Face Compare** are incorrect
   - Warning (orange), if the document type is unknown (i.e., not passport, ID card, driving license) and/or the result of the **Face Compare** is uncertain

If any of the checks fails, the **Data extracted** and/or **Document genuine** sections turn to red. If either the **Data extracted** or **Document genuine** or both sections are red, the color of the **SUMMARY SECTION** tab also turns to red. If the scanning process has not started yet both fields (**Data extracted** and **Document genuine**) are grey.

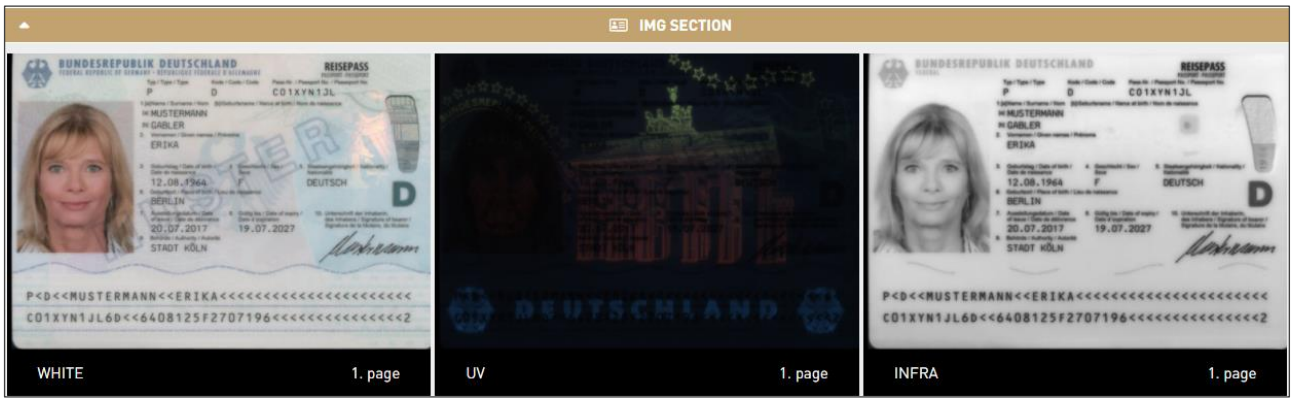
Colored frame appears around the first two images located on the right side (below in mobile view) if **Face Compare** has taken place (between the visually detected and stored in the RFID chip). The color of the frame alters according to the result of the face comparison. The interval limits of the results are the following:

- **60-100%: OK** (green) - No error message; the rate of the similarity is greater than 60%
- **30-60%: WARNING** (orange) - The two images are similar; the rate of the similarity is between 30% and 60%
- **0-30%: ERROR** (red) - The two images differ from each other; the rate of the similarity is less than 30%



2. IMG SECTION

Here you can inspect the scanned document under different illuminations. The available lights depend on your Osmond model as well as on the configuration set under the SCAN PROCESS / LIGHT SETTINGS menu.



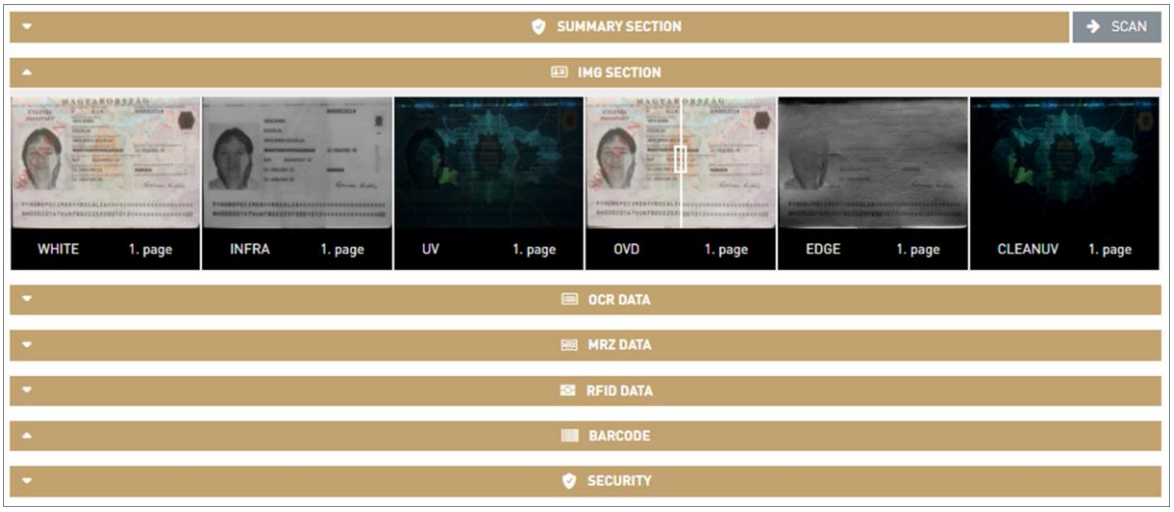
Note

Only those image types can be seen which have been enabled in the APPLICATION / EDIT APP / Img Section menu and the corresponding illumination type has been selected in the SCAN PROCESS / SCAN LIGHT menu.

Note

The scanned images are displayed in columns at IMG SECTION. The number of columns can be configured at APPLICATION / EDIT APP / Img section / Number of columns (on large display).

For example, if the selected number is 6:



3. OCR DATA

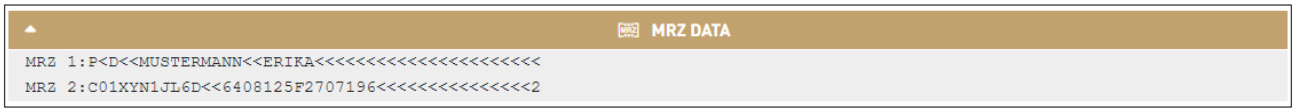
In the **OCR DATA** section, the processed MRZ and VIZ data can be examined.

> **Note**
>
> The **OCR DATA** section shows data fields that are configured in the **EDIT APP / FIELD SETUP** menu.

OCR DATA		
	MRZ	VIZ
BirthDate	1984-06-07	
Composite1	P<AUSCITIZEN<<JANE<<<<<<<<<<<<<<<<<<<<<<<<	
Composite2	PE0914748 6AUS8406077F1903267<40103503K<<<<00	
DocType	PP	
DocumentNumber	PE0914748	
DullCheck		540
ExpiryDate	2019-03-26	
Givenname	JANE	
IssueCountry	AUS	
Name	CITIZEN JANE	
Nationality	AUS	
PersonalData1	40103503K	
Sex	F	
Surname	CITIZEN	
Type	P	

4. MRZ DATA

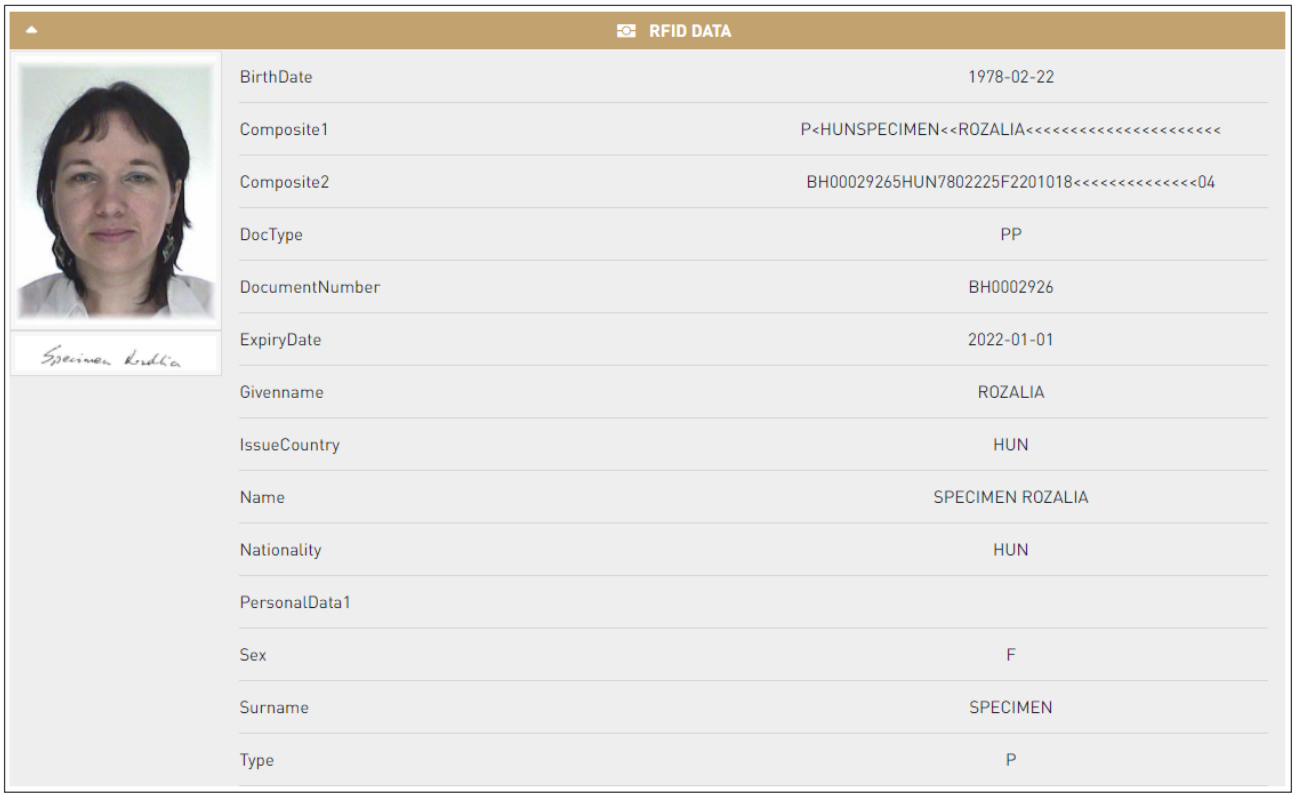
If the scanned document has printed MRZ lines, those are displayed in this section.



5. RFID DATA

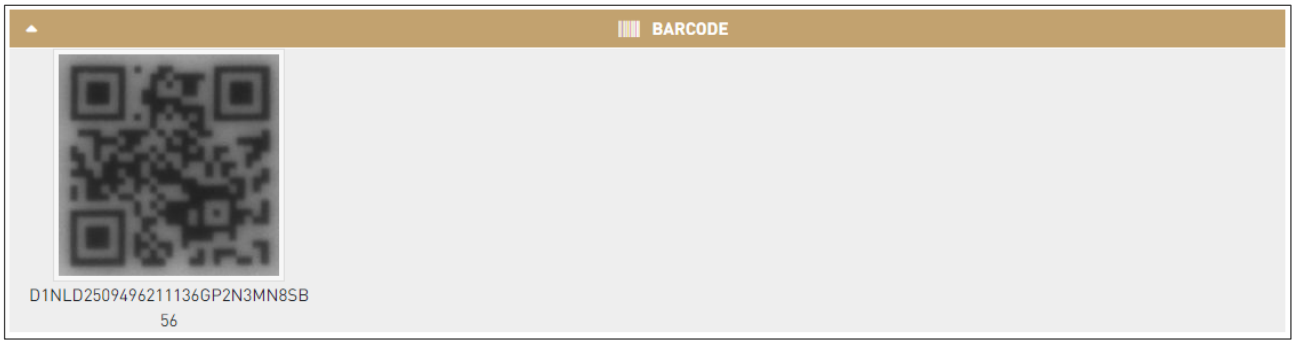
In the **RFID DATA** section, data read from the RFID chip of the document is displayed. These data include segmented MRZ line information (DG1 in ePassports) as well as RFID face image (DG2 in ePassports).

> **Note**
>
> The **RFID DATA** section shows data fields that are configured in the **EDIT APP / FIELD SETUP** menu.



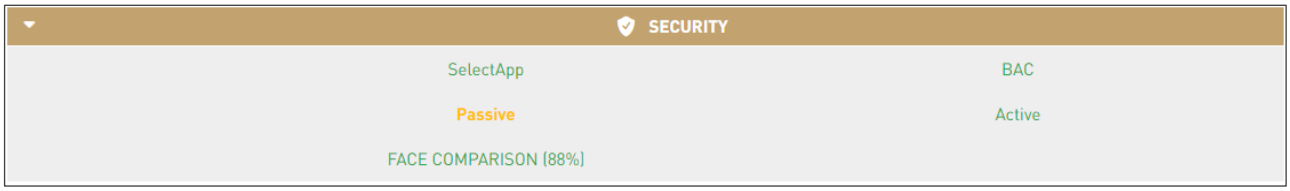
6. BARCODE

If you scan a document with barcode on it, image of the barcode and its decoded data are displayed in this section. Make sure to configure which barcodes would you like to read in the SCAN PROCESS / BARCODE SETTINGS menu before scanning a document with barcodes.



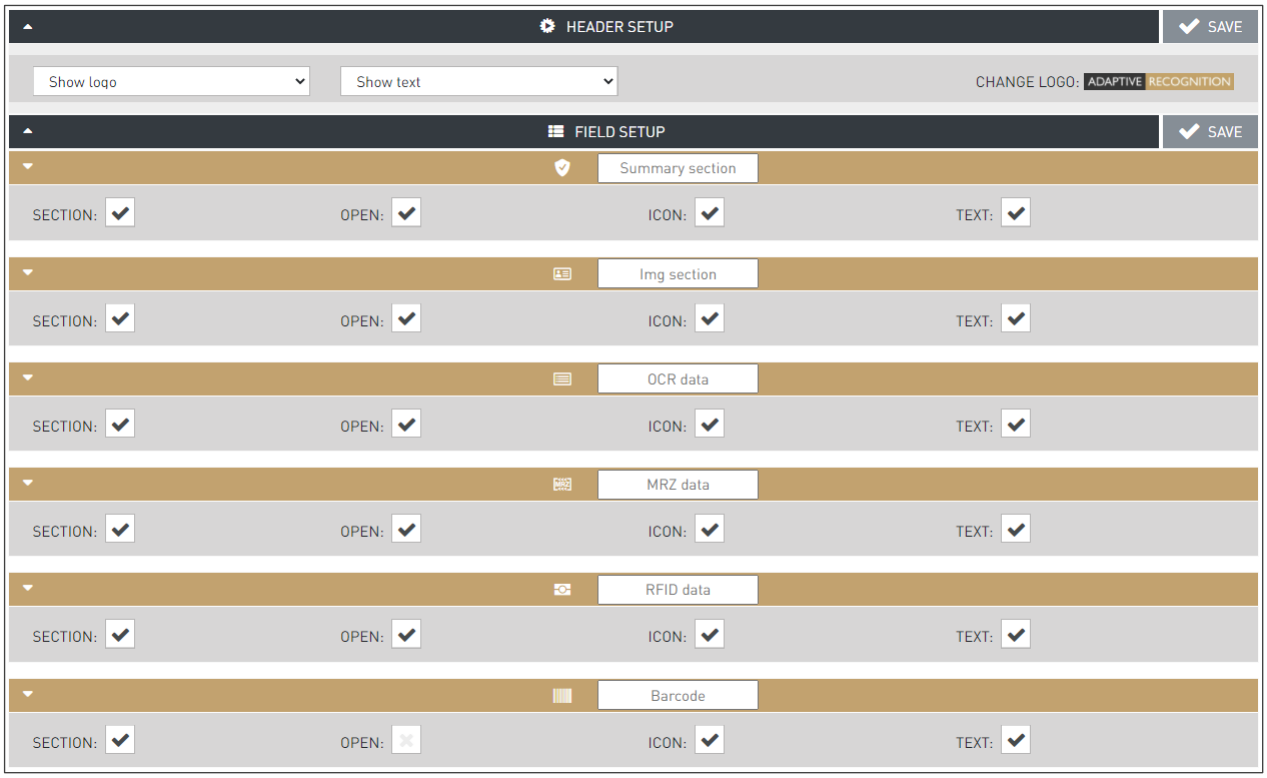
7. SECURITY

The SECURITY tab displays the result of all security checks performed on the document. If any of them fails, it is displayed in red. Orange values (typically Passive Authentication) mean that the authentication could not be performed.



2.3.2. EDIT APP

In order to meet different user requirements, the reader Application can be fully customized using the EDIT APP option.



The interface of the document reader device is divided into sections. At every section it is possible to perform the following settings:

- Full section is visible/hidden
- The section by default is in open/closed position

Note

In those web browsers in which the interface is already in use, the program notes the user activity thereby the sections will be displayed as last used (opened or closed). The function is not working in incognito mode.

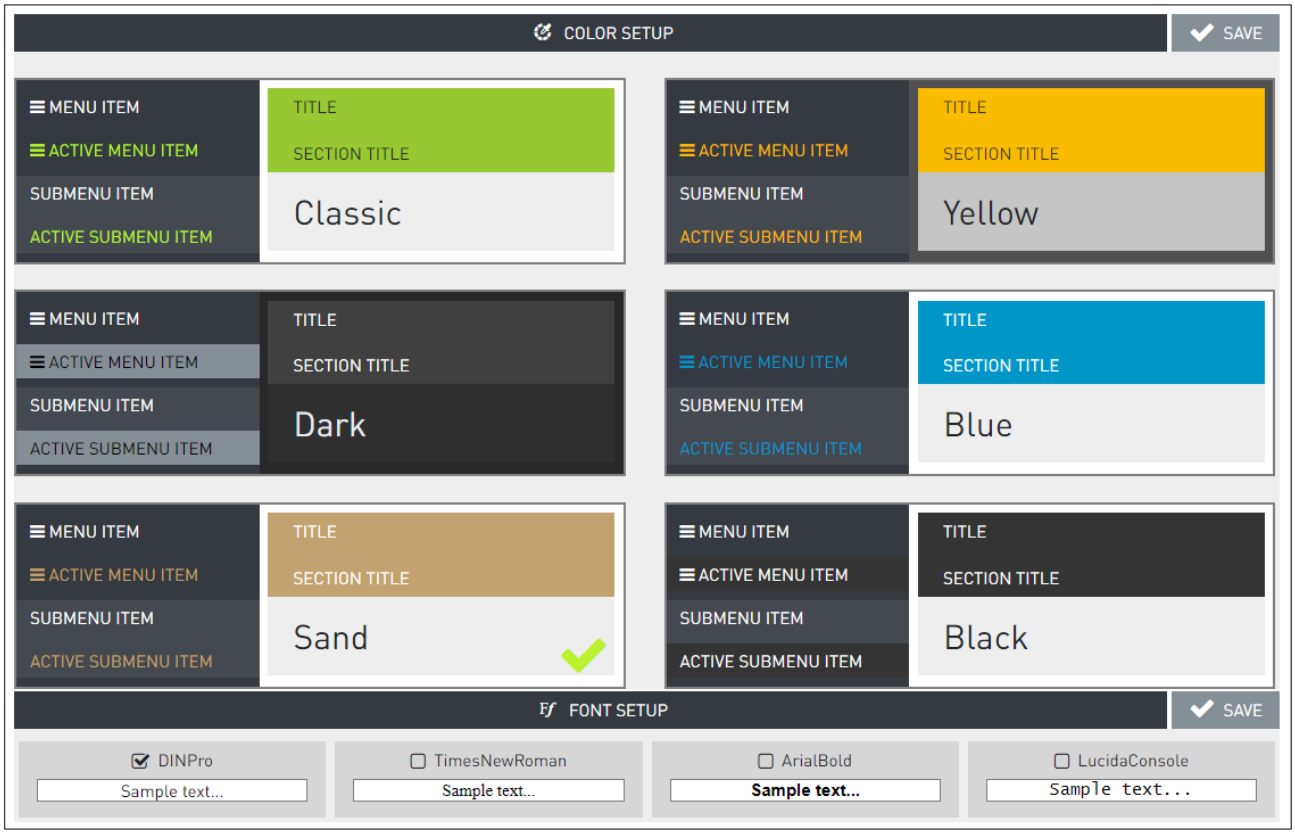
- The icon of the section is visible/hidden
- The name of the section is visible/hidden
- Modifying the name of the section

Starting with the header of the Application (Show logo, Show text and CHANGE LOGO options), each section can be customized in the following aspects:

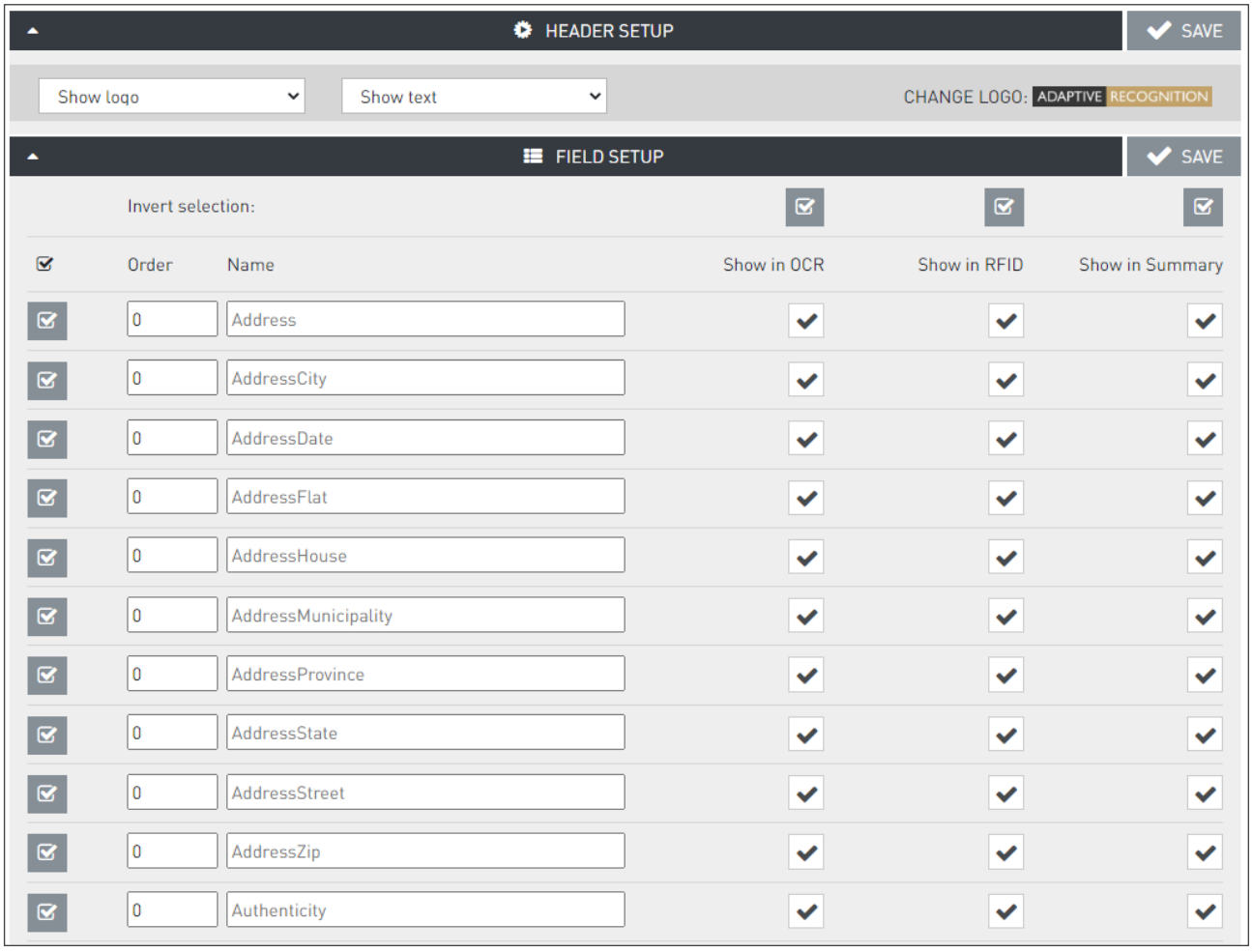
SECTION: If selected, the section is present in the Application.
OPEN: If selected, the Application shows the contents of the section by default.
ICON: If selected, the icon - next to the title of the section – is displayed in the Application.
TEXT: If selected, the title of the section is displayed.

The "UPLOAD" and "SCAN" phrases appearing on the web interface can be customized by entering the preferred values.

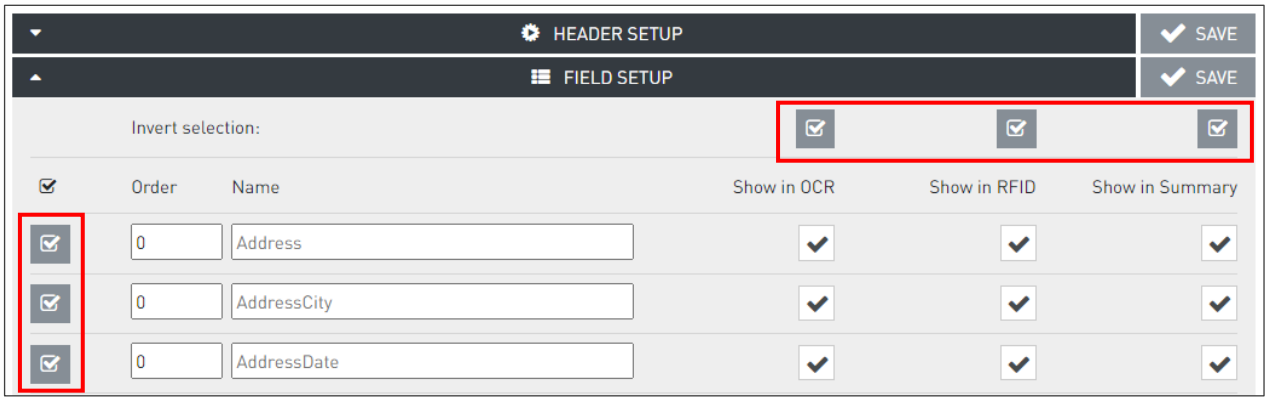
Besides the above options, the fonts and colors used in the Application can also be customized at the COLOR SETUP and FONT SETUP sections.



Using the **FIELD SETUP** menu, all data appearing in the application can be customized. Every field can be displayed in the APP Summary (**Show in Summary**), RFID (**Show in RFID**) and OCR (**Show in OCR**) sections.



When selecting multiple fields for the same APP section, use the  icon to select all fields in the same column or line.



2.3.3. CONFIG BACKUP

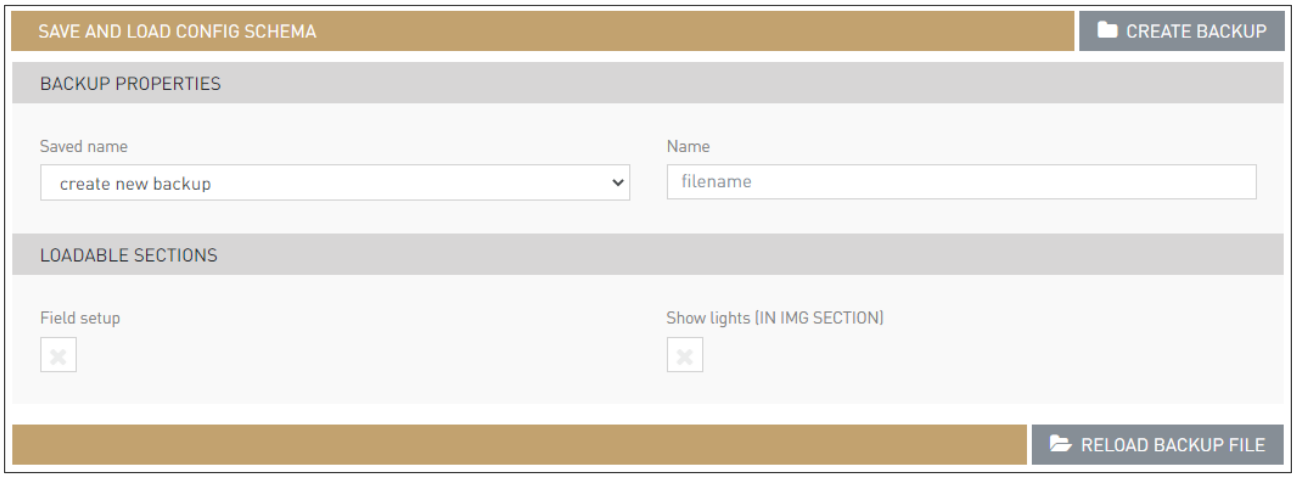
In the CONFIG BACKUP menu, the configuration schemes relating to the reading interface can be saved and reloaded as well.

In order to save a backup file, first, under the Saved name field, select a new or a former backup option. In case of creating a new backup, the filename can be entered to the Name field. Last, by clicking on the CREATE BACKUP button, the former backup file is overwritten or a new one is created.

In order to reload a former backup, click on the RELOAD BACKUP FILE button. When reloading the file, the configuration settings chosen under LOADABLE SECTIONS are loaded according to the selected backup from Saved name field.

The following sections can be saved:

- Field setup: Settings of the fields to be displayed during reading
- Show lights: Settings applied to the displayed images during reading



Note

APPLICATION / CONFIG BACKUP and MAINTENANCE / BACKUP is not the same.
Under APPLICATION / CONFIG BACKUP the Field setup and Show lights sections can be saved. Under MAINTENANCE / BACKUP the User settings and Configuration data can be saved.

2.3.4. HISTORY

The Osmond device is equipped with internal storage space to save images and data of scanned documents. This feature can be activated by selecting the "local database" option in the ADMINISTRATION / RESULT UPLOAD menu and together with zip format (PACKAGE FORMAT menu).

> **Note**
>
> The available storage space highly depends on the number of installed OCR engines. Refer to the SYSTEM INFORMATION / DISK section on detailed information on used disk space.

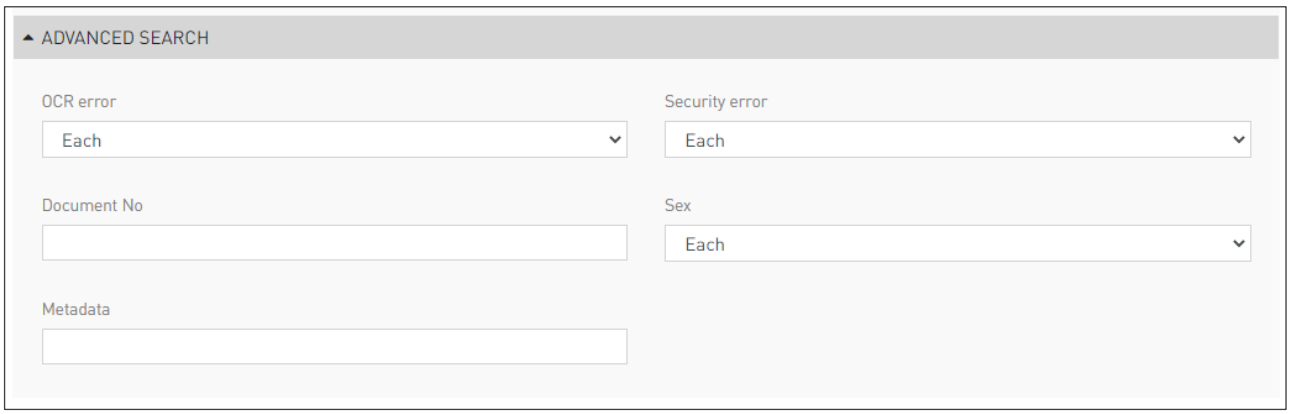
The fields can come from different sources (e.g., MRZ, RFID) therefore the values from all available sources will be stored in the database but in the search interface these values appear as merged.

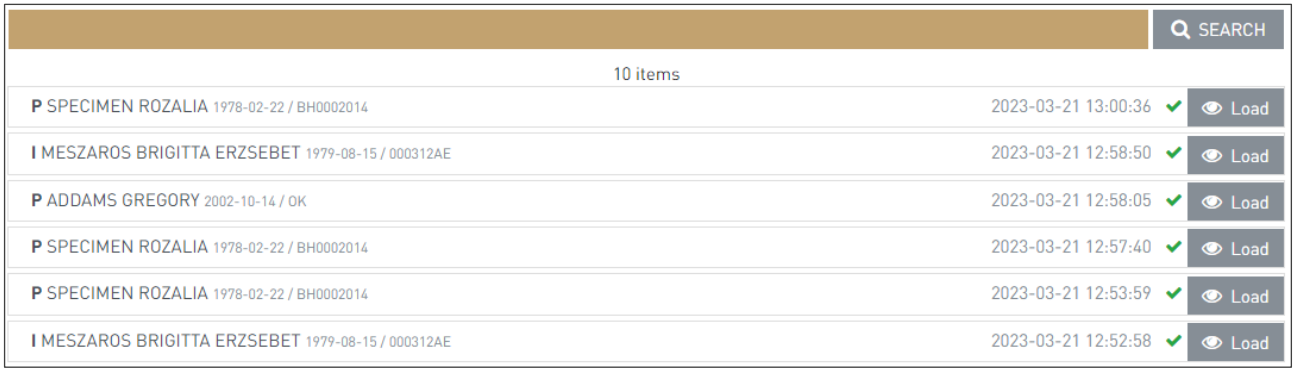
Once documents are saved, they can be browsed in the HISTORY by using multiple filter criteria. For filtering time periods, use the date format of the MRZ lines (e.g., 210919 stands for 2021 September 19).

> **Note**
>
> The barcode and RFID data cannot be reloaded at HISTORY / Load.

Besides document fields like **Surname**, **Given names**, **Period**, **Type**, **Nationality** and **Date of birth**, advanced searches can also be performed to list documents according to the following criteria:

- Documents with OCR error
- Documents with security issue
- Documents belonging to male and female bearers
- Documents having a specific document number



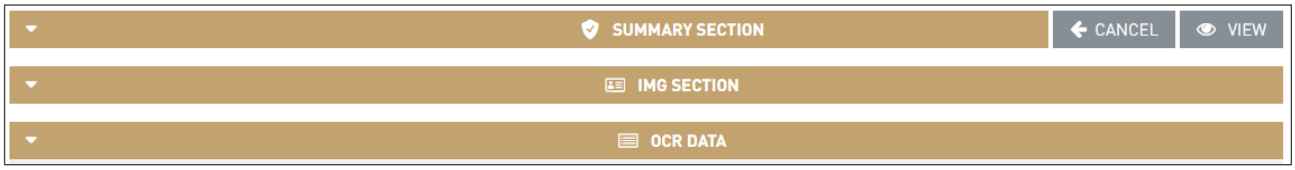


2.3.5. FILE UPLOAD

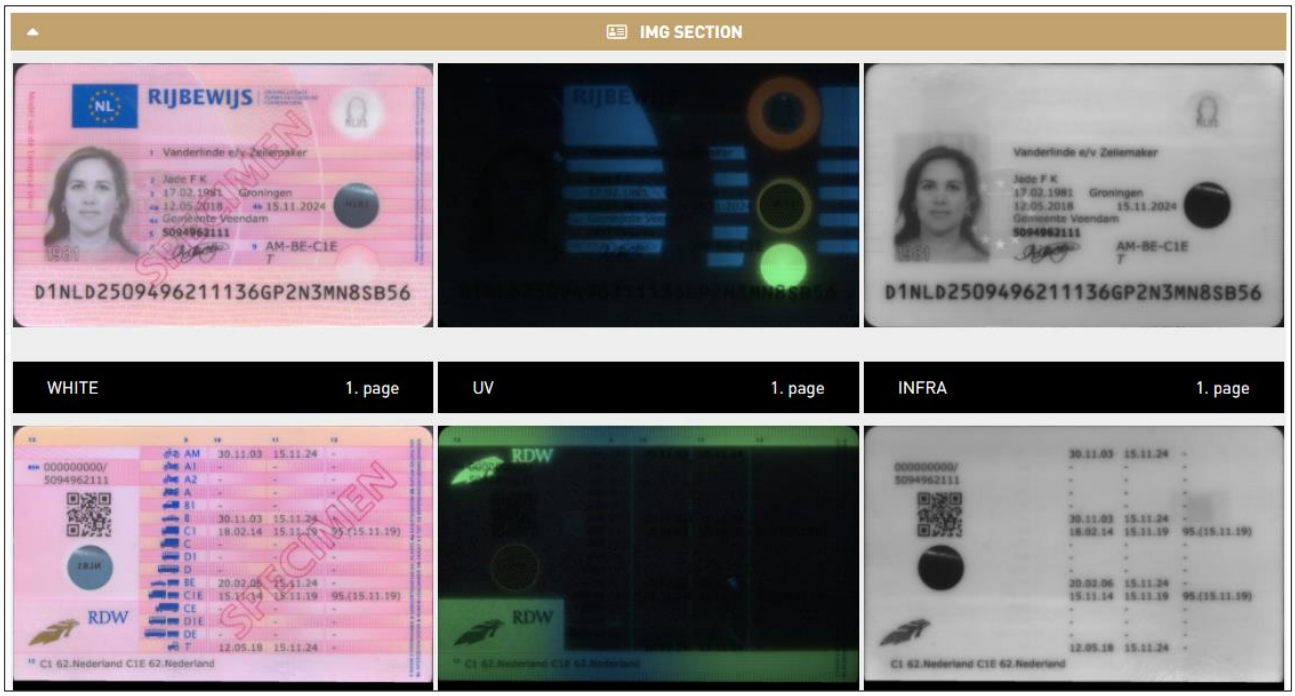
The Osmond device provides support to upload and process document packages that have been created earlier, using zip format (SCAN PROCESS / PACKAGE FORMAT).
The zip format includes document images, OCR-, and RFID data as well.

> **Note**
>
> Only those zip files can be loaded that have been saved by Osmond devices.

Just browse a .zip file that was saved before and click [UPLOAD]. After that, click on [VIEW] to display the results in the Application:

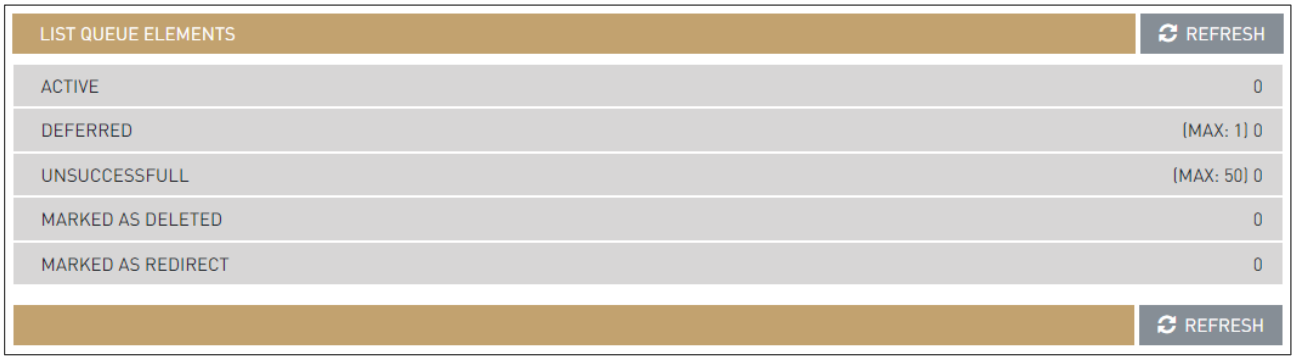


After clicking [VIEW], the images and data from the .zip file is displayed as if it were a result of a live scanning process:

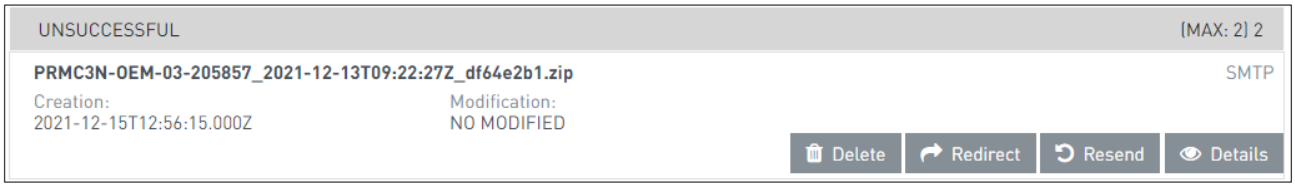


2.3.6. LIST QUEUE

The Osmond device uses upload queue for uploading documents into remote servers. Using such queue, it is not necessary to wait for a document until it is uploaded but the next scanning process can be started immediately.



- ACTIVE: Number of documents currently in queue (waiting for uploading).
- DEFERRED: First upload attempt failed, waiting for the next attempt.
- UNSUCCESSFUL: Upload has failed multiple times. No more upload attempt is performed.
  For any document in unsuccessful status, the following actions can be performed:
  - Delete: See below at "MARKED AS DELETED".
  - Redirect: See below at "MARKED AS REDIRECT".
  - Resend: Attempt to upload document as configured at RESULT UPLOAD protocol, as many times as set at "Connect attempts".
  - Details: Loading document data into the APP – Same as APPLICATION / HISTORY / LOAD option.



- MARKED AS DELETED: In order to remove any document from queue:
  Initiate the deletion, and then confirm the removal from queue as an Owner user.
- MARKED AS REDIRECT: In order to redirect any document from queue:
  Initiate the re-direction and specify the alternate protocol. Then, confirm the redirection as an Owner user.

> **Note**
>
> The maximum number of the DEFERRED and UNSUCCESSFUL uploads can be modified at SCAN PROCESS / QUEUE OPTIONS.

2.4. SCAN PROCESS

2.4.1. MAIN CONFIGURATION

Under the **MAIN CONFIGURATION** menu, users can set the following:

1. SCAN OPTIONS

   - When **Interactive** scanning mode is selected, capturing a document is triggered manually by the user, upon click on **[SCAN]** (**START APP** menu). See reading phase icon description in Appendix.
   - When **Autonomous** mode is selected, reading of a document is automatic, based on the built-in motion detection feature of Osmond. See reading phase icon description in Appendix.
   - Switch on/off automatic **Document cropping and rotation** and **Face comparison**.
   - **Image resolution** can be selected, the following options are available:
     - **Low** with a resolution of 300 DPI
     - **Medium** with a resolution of 500 DPI
     - **High** with a resolution of 700 DPI

> **Note**
>
> In case of devices with **firmware version 1.8.x**, the value of the **Image resolution** is set to **High** by default. If the user requirements need lower resolution in order to reduce the stored file size or due to time-critical applications, change the default value.

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

– **Logging** should be used for troubleshooting purposes involving ADAPTIVE RECOGNITION support team.

  The value of the **Log level** consists of 2 digits:

  1. value: 0-2

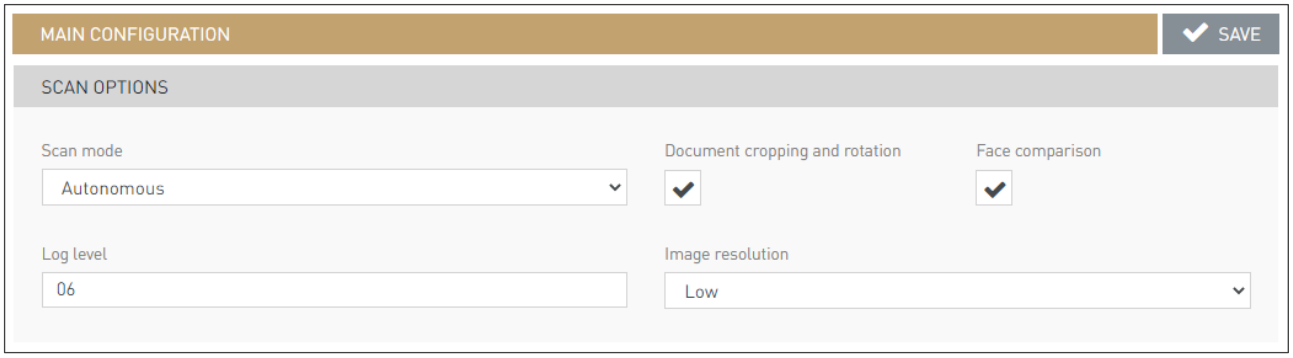
  This is the log level of the interface and the operation of the webserver and modules behind it. In the case of sending troubleshooting related log files, set this value to 2.

  2. value: 0-9

  This is the log level of the operation of the document scanner. In the case of sending troubleshooting related log files, set this value to 9. The value 0 or maximum the value 6 are recommended for normal operation, because the levels between 7 and 9 can already affect the performance.

Note

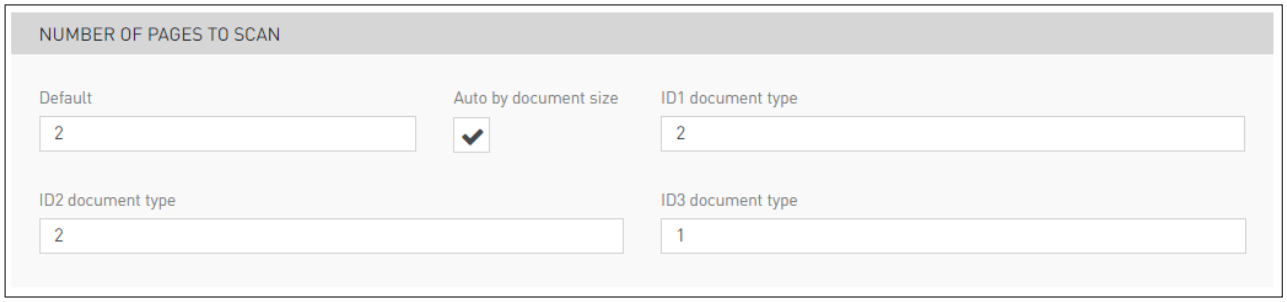
Changing log level value involves automatic device restart. Save any changes before editing this field.



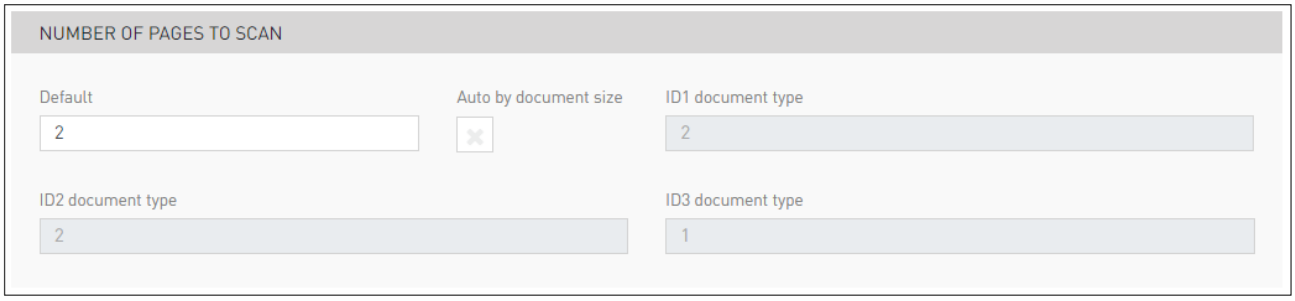
2. NUMBER OF PAGES TO SCAN

The NUMBER OF PAGES TO SCAN option specifies the number of pages to be scanned from the same document.

- The Default value must be specified. If the document size cannot be determined, upon using the Auto by document size mode, the Default value will be applied. As many pages can be displayed in the App as the Default value.
- Tick the box in order to enable Auto by document size mode. When Auto by document size is in use, the device automatically determines the document size.
  The default number of pages for the following document types are:
  ID1 document type: 2 (ID-1 size cards: like national ID cards, driver licenses or any other 85.60 mm x 53.98 mm = 3 ⅜ in x 2 ⅛ in sized or smaller printed documents)
  ID2 document type: 2 (ID-2 size cards: like French and Romanian ID cards, visas or any other 105 mm x 74 mm = 4 ⅛ in x 2 15⁄16 in sized printed documents)
  ID3 document type: 1 (ID-3 size cards: like passports or any other 125 mm x 88 mm = 4 15⁄16 in x 3 7⁄16 in sized printed documents)



Auto by document size is enabled



Default value is applied, **Auto by document size** is disabled

Note

In the case of documents with 2 pages you must choose the illumination types of the 2nd page too.

Note

If the reading process is interrupted then the scanning will go on with reading the first page when returning to the reading process – regardless of the scanning mode.

3. PACKAGE UPLOAD OPTIONS

- By using the **Auto** mode at **AutoSend**, every scanned document is automatically uploaded via the protocol selected at **Communication type**, in a format selected at **Package Type**. If **Approve** mode is selected, document is uploaded only upon user confirmation, by clicking on the **[Approve]** button, at the bottom of the App.

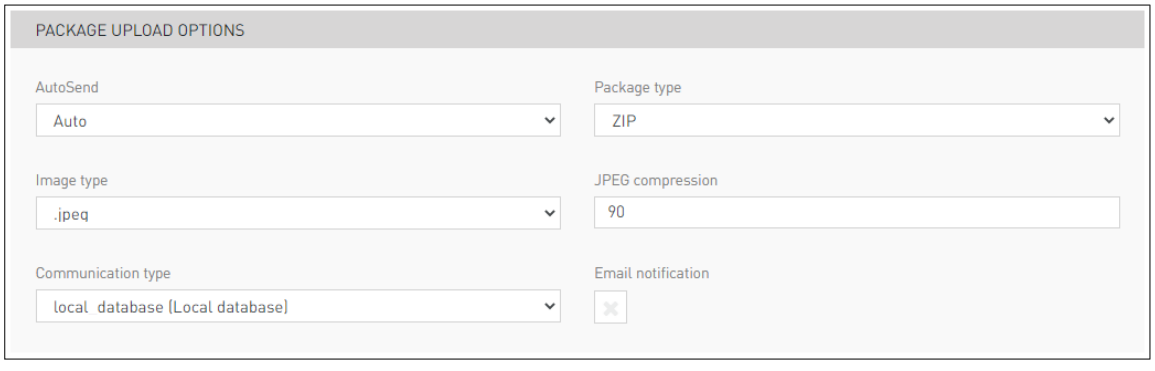
> **Note**
>
> Configuration of any upload protocol can be done in the **RESULT UPLOAD** menu, by clicking on the corresponding **[Edit]** button.

> **Note**
>
> For more information on the selectable package type formats (ZIP, CSV, PDF), see Package Format chapter.

- The uploaded package contains **Image type** elements as specified in the corresponding field. The following options can be selected from the drop-down menu:
  - .jpeg
  - .bmp
  - .png
  - .jp2k

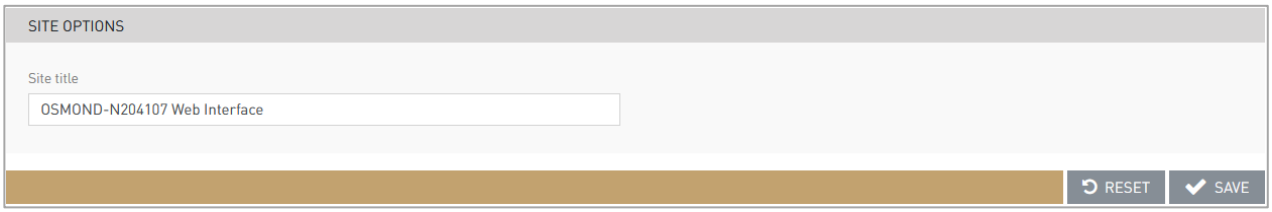
  If ".jpeg" is selected, its compression is configured as specified at **Jpeg compression**.

- The **Email notification** option is designed to send automatic e-mails upon scanning a document. Make sure to configure parameters of **EMAIL NOTIFICATION** at **ADMINISTRATION / RESULT UPLOAD** in order to use this function.



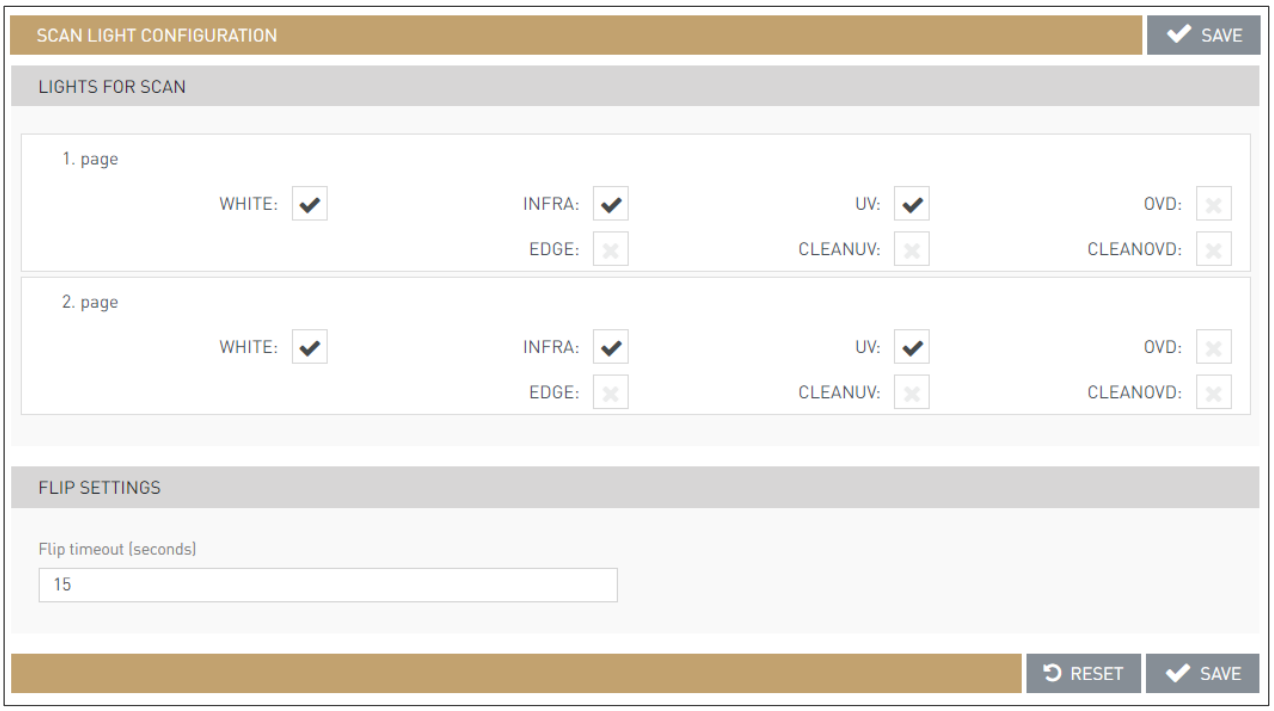
4. SITE OPTIONS

Users can also change the **Site title** of Osmond web interface website in browsers. The text displayed in the header of the browser can be customized in the **Site title** field, if the application is on the reading interface (**START APP** menu). In case of other menu items, the displayed address can be specified in **NETWORK / LAN**.



2.4.2. SCAN LIGHT

In the SCAN LIGHT menu, users can select the illumination types of the image capturing process.



Note

Only those image types can be seen which have been enabled in the APPLICATION / EDIT APP / Img Section menu and the corresponding illumination type has been selected in the SCAN PROCESS / SCAN LIGHT menu.

Note

In order to perform complete OCR and authentication tasks, images should be scanned under INFRA, WHITE and UV lights as well.

IMAGE TYPES:

- WHITE: visible white illumination (with reflection removal)

  Enable/Disable WHITE illumination by right-clicking on its button.

  An image scanned in white light is a simple photo of the document – as it can be seen by the human eye. It is usable for human inspection and for examination of background pattern or face photo.

- INFRA: B900 infrared illumination

  Enable/Disable INFRA illumination by right-clicking on its button.

  In this illumination, the background patterns are not visible, so optical recognition algorithms provide better results.

- UV: ultraviolet (UV-A) illumination

  Enable/Disable UV illumination by right-clicking on its button.

  Images scanned in ultraviolet illumination can be used to check authenticity features (graphics and text printed with special fluorescent ink) which are only visible under UV light. These authenticity features can be observed by viewing the UV image or the UV pattern (clean UV) image. In the case of the latter one, the background is darker so the authenticity features can be seen more clearly.

UV

UV pattern

- OVD

  Enable/Disable OVD illumination by right-clicking on its button.

  The Passport Reader system is capable of visualizing and removing simple holograms and most types of OVI patterns. Holograms can be observed by viewing the OVD image or the OVD pattern (clean OVD) image. In the case of the latter one, just the hologram can be seen from the document.

OVD

OVD pattern

- PHOTO

> **Note**
>
> The **Photo** light is only available for Osmond USB models manufactured from December 2022.

Enable/Disable the **PHOTO** light by right-clicking on its button.

Photo light is optimized for scanning photos with very high image details and color accuracy. **Photo** image is similar to an image scanned in white light with more sharpness and contrast.

Image scanned in White light

Image scanned in Photo light

> **Note**
>
> Using **Photo** light is increasing processing time. Use only when it is needed.

- EDGE

  Enable/Disable **EDGE** light by right-clicking on its button.

  When using Edge light, the document is illuminated at a flat angle in order to make the protruding objects located on the document cast a shadow.

The Flip timeout value specifies a time interval between capturing two sides of the same document. If the time specified here is up before entering the second page of a document, then scanning is performed automatically. This feature is designed to avoid endless waiting if second page of a document is not scanned for some reason.

> Note
>
> Flip timeout is only in force when the Autonomous mode is selected.

In Autonomous mode, the device waits for a number of seconds (specified at Flip timeout) between scanning two sides/pages of the same document. When time runs out, the device goes to the next side/page of the document by all means.

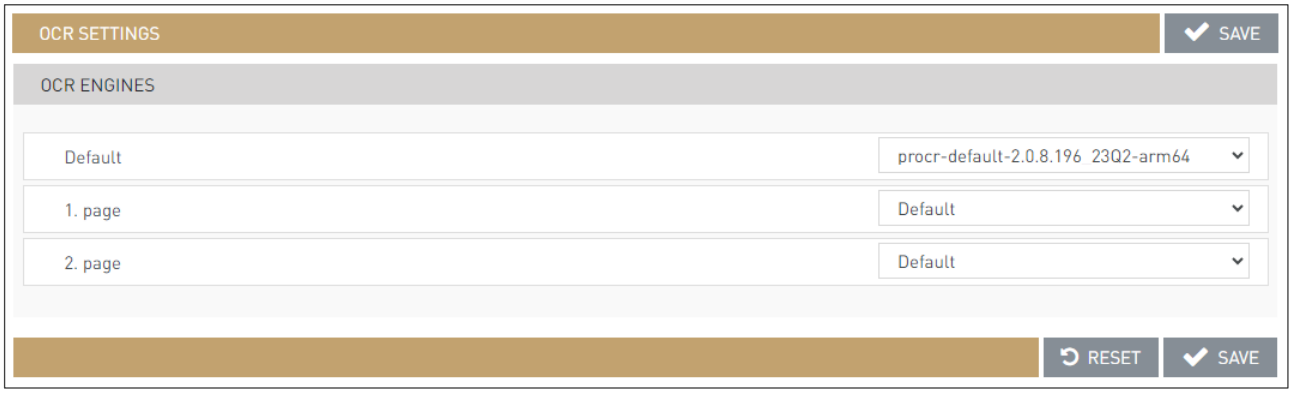
In case of a two-sided document:

1. The device is empty, waits for the document
2. Detects the inserted document
3. Reading
4. Waits for the removing of the document (there is currently no timeout here)
5. Detects that the document has been removed
6. Waits for the second side of the document until the specified time at Flip timeout
7. Reading is in progress, if before Flip timeout the document has been inserted or if the Flip timeout takes place
8. If the document is removed or due to the Flip timeout a blank reading has taken place, then the device uploads the data

The primary role of the Flip timeout setting is that in case of reading multiple-page documents, the reading process is even continued when fewer pages have been inserted after a given timeout based on the number of missing pages the session is terminated.

2.4.3. OCR SETTINGS

Using the **OCR SETTINGS** menu, users can configure which OCR engine is used for scanning the 1st and the 2nd page (front side & back side) of the document.

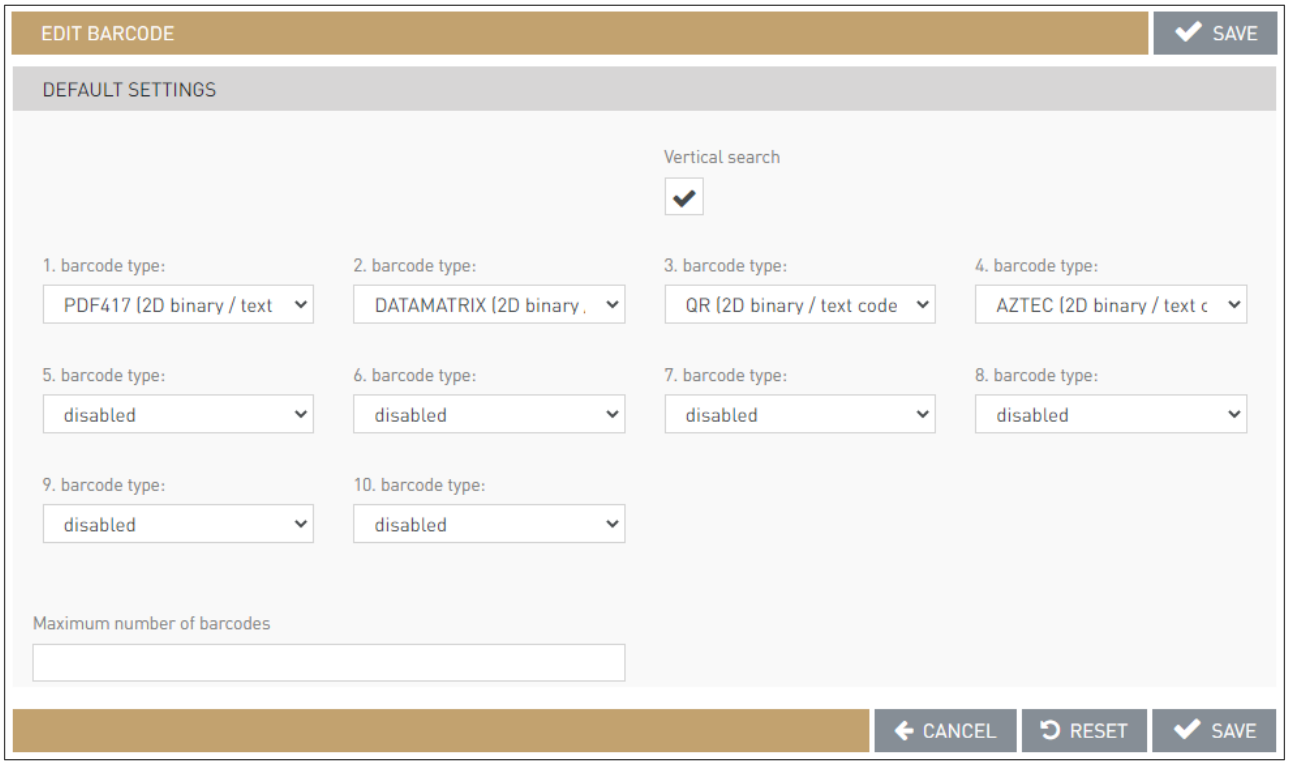


> **Note**
>
> For more information on OCR engines, please contact our technical support team.

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

2.4.4. BARCODE SETTINGS

In the **BARCODE SETTINGS** menu, users can also specify which barcode types should be searched for on the first and second pages of the scanned documents. Just click on **[Edit]** to customize the settings of the **1. page**, **2. page** or both (**Default:**).



If the **Vertical search** option is disabled, barcodes are read only if positioned on the document window in horizontal direction. Such settings enable very fast barcode reading option e.g., for boarding passes.

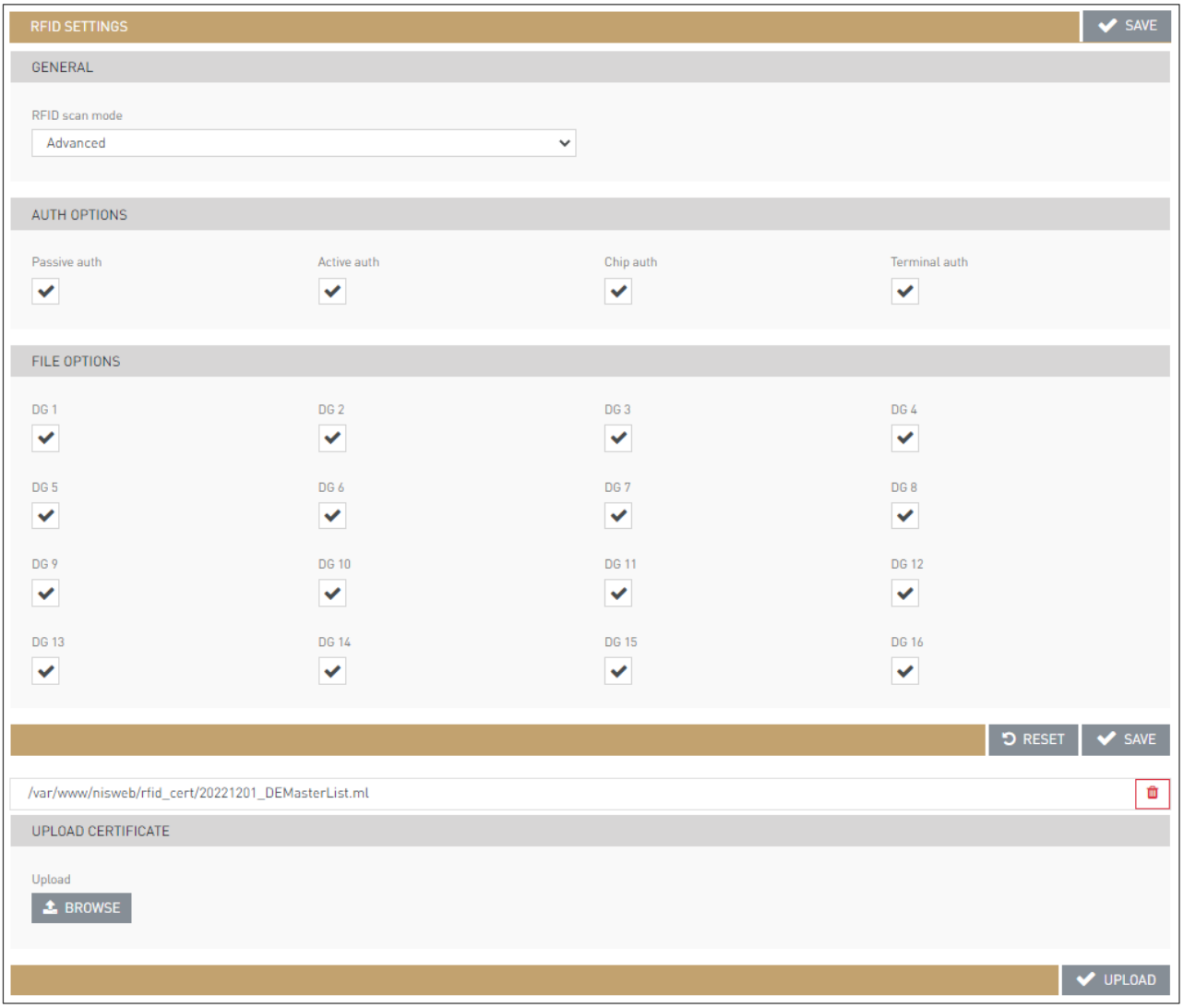
In order to configure the Application to read any barcode, all the available types should be selected in the **barcode type** textboxes. The barcode reading algorithm first searches for barcodes specified in **1. barcode type** then for ones specified in **2. barcode type** and so on.

The value specified in the **Maximum number of barcodes** field defines the maximum number of the barcodes that the device searches for on one document page.

2.4.5. RFID SETTINGS

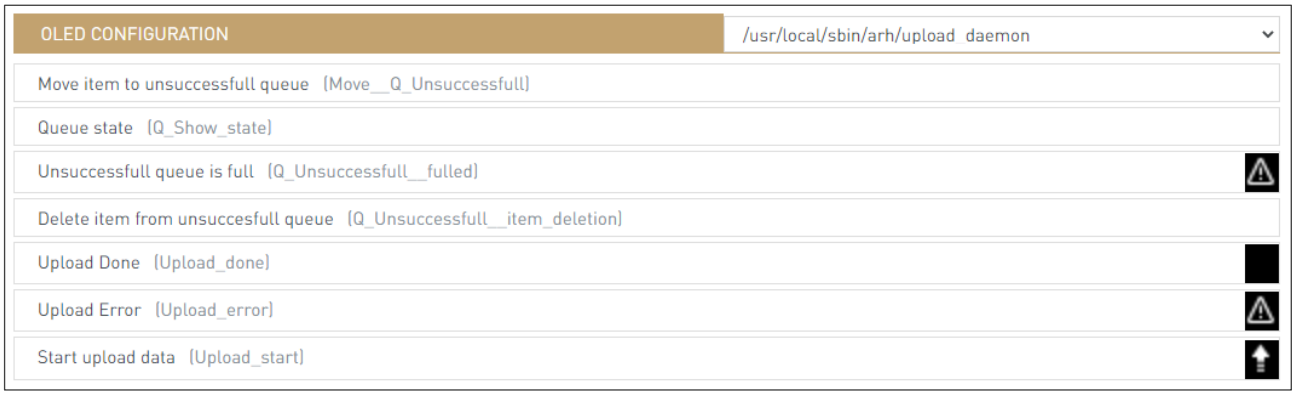
In the **RFID SETTINGS** menu, users can

- Select the RFID scanning mode (**Off/Default/Advanced**)
- Select which RFID authentication should be performed (**PA, AA, CA, TA**)
- Which RFID files should be read from eDocuments (**DG1…DG16**)
- Upload RFID **certificate** usable for Passive Authentication (PA)



2.4.6. DISPLAY

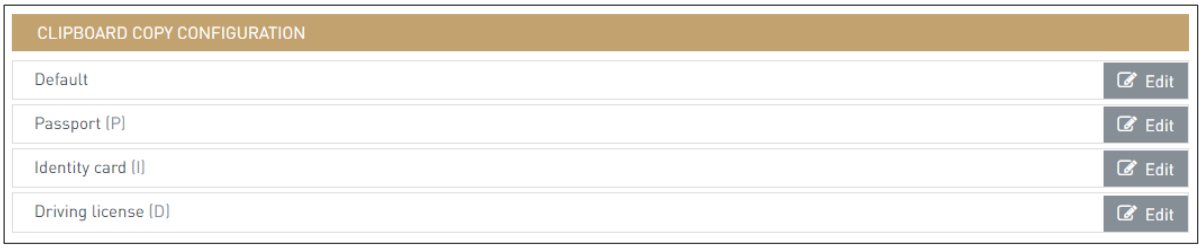
The **DISPLAY** menu lists the device statuses displayed on the OLED screen. For the various device states, the App can display an image, a text or blank screen which can be checked and viewed in this menu.



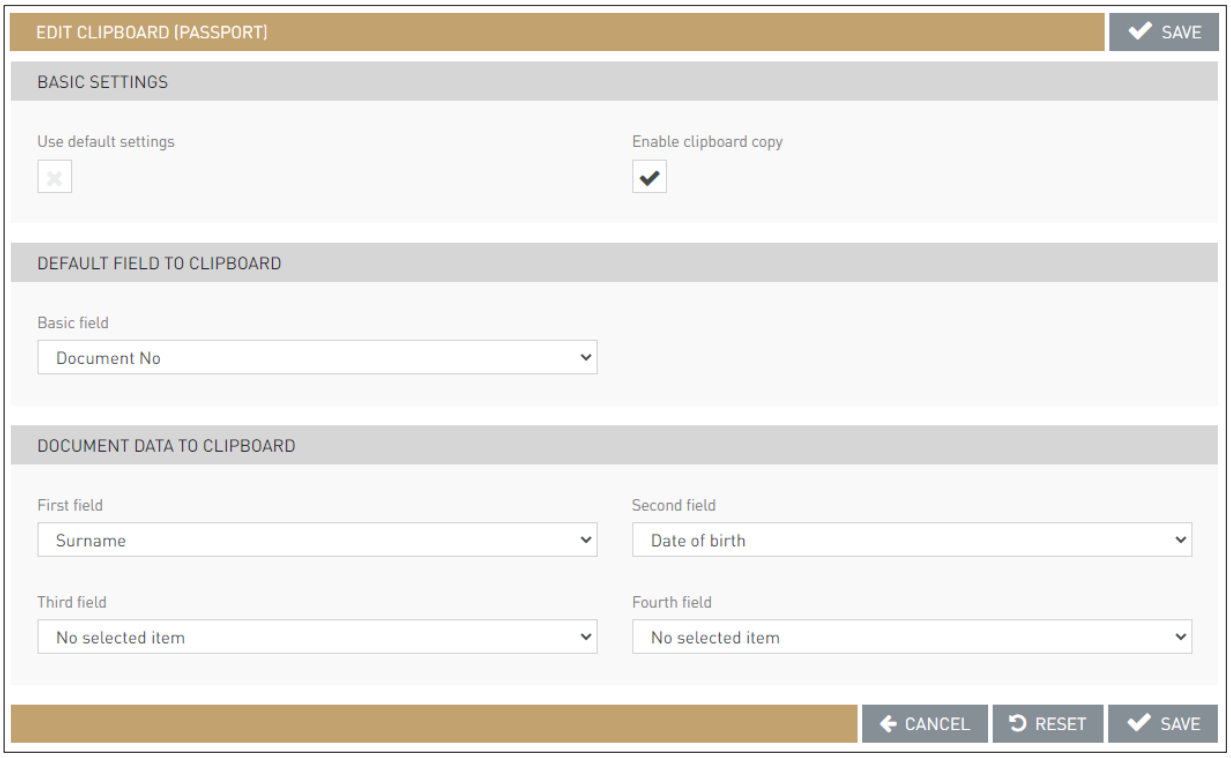
Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

2.4.7. CLIPBOARD COPY

The **CLIPBOARD COPY** feature is designed to copy OCR-ed fields to the clipboard automatically, after scanning a document. This function can be customized for different document types:



Upon clicking **[Edit]**, the feature can be activated by selecting the **Enable clipboard copy** option and the document fields to be copied to clipboard can be selected (**Basic field** – if only one field is required, **First**…**Fourth field** – if more than one field is required).



2.4.8. PACKAGE FORMAT

The Osmond device can upload images and data to remote targets packed into different formats:

- The Osmond-specific **zip** includes images, OCR-, and RFID data as well, packed into a single zip file. This kind of package can also be uploaded to the Application and displayed like results of any live scan.

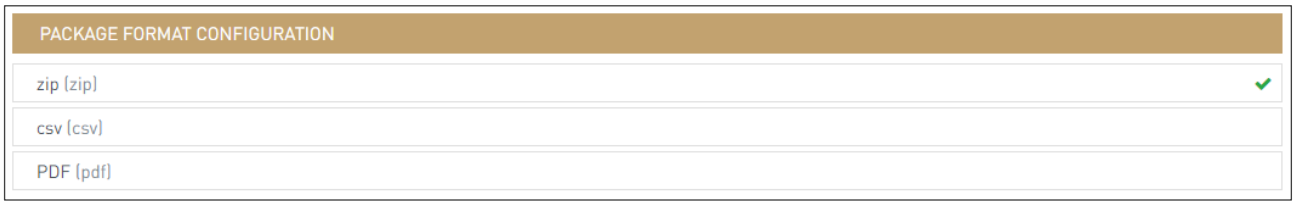
Note

For saving documents into local database, only .zip format is supported.

- The **csv** format contains RFID and OCR data (text) only as a comma separated list.
- The **PDF** format includes OCR, RFID information as well as document images including cropped face photo. This format is optimized for printing.

Important!

Please select the package format at **SCAN PROCESS / MAIN CONFIGURATION / PACKAGE UPLOAD OPTIONS**.



2.4.9. PDF TEMPLATE

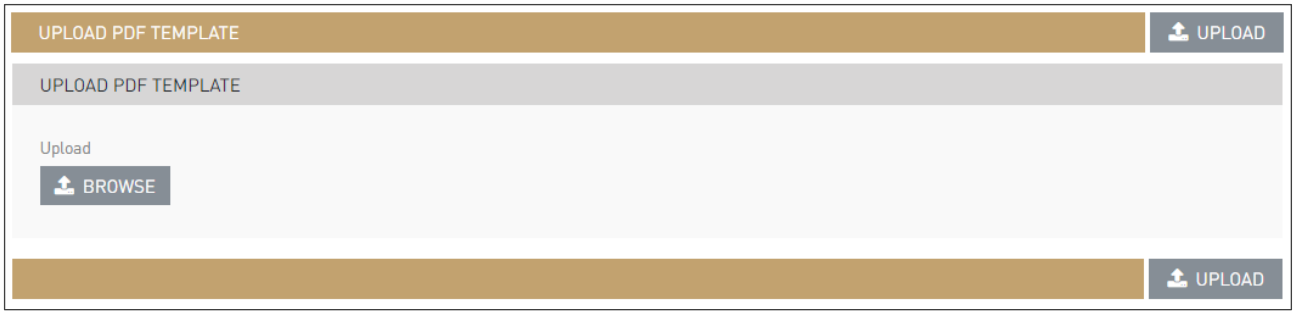
In the **PDF TEMPLATE** menu, you can upload your customized PDF template file. The template defines the appearance of the file containing OCR, RFID data as well as document images packed into PDF package format.

Note

For more information, please contact our support team.

Important!

Please select **PDF** package format at SCAN PROCESS / MAIN CONFIGURATION / PACKAGE UPLOAD OPTIONS in order to utilize this function.



2.4.10. QUEUE OPTIONS

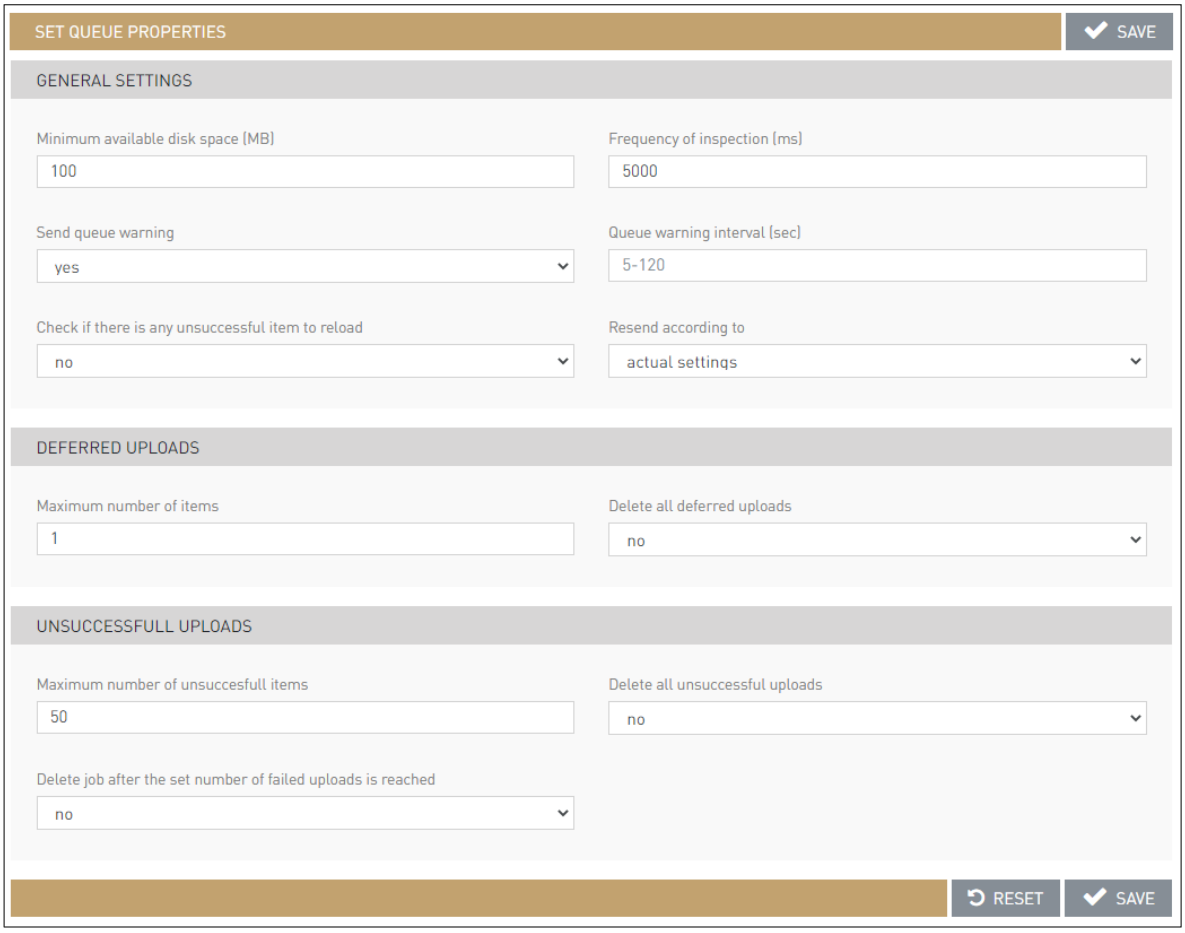
In this menu, owners may configure different queue settings.

The **Minimum available disc space** option specifies a minimal amount of free space that should always be present on the device. If this limit is hit for any reason, it may have effect on queue sizes. The value of 100MB is a factory default setting that should not be altered.

The **Frequency of inspection** specifies the frequency of checking if there is any document in the upload queue. **Queue warning interval** specifies the frequency of sending queue update notifications. Such notifications can be turned on/off by using the **Send queue warning** option.

It is possible to resend the content of the unsuccessful items if you select "yes" under **Check if there is any unsuccessful item to reload**. The location of the reupload can be set under **Resend according to**, where the following options are available:

- **original settings**: the reupload is performed to the original location,
- **actual settings**: the reupload is performed to the currently set location.



The **Maximum number of items** specifies that how many documents can be waiting for uploading at the same time. In order to delete all these documents, use the **Delete all deferred uploads** option.
For any documents failed to upload, owners may limit the number of such items (**Maximum number of unsuccessful items**) and can also delete all of them permanently by using the **Delete all unsuccessful uploads** option. Furthermore, such documents can also be deleted automatically - after all upload attempts have been performed – if the **Delete job after the set number of failed uploads is reached** menu item is set to "yes".

Note

When setting **Delete all unsuccessful uploads** or **Delete all deferred uploads** to „yes", this value is automatically switched back to „no" after deleting items is finished.

Note

When **UNSUCCESFUL** limit is reached, the oldest element in queue is overwritten by the result of the latest scan.

When **DEFERRED** limit is hit, scanning any new document is not possible until the number of deferred elements is decreased.

Important!

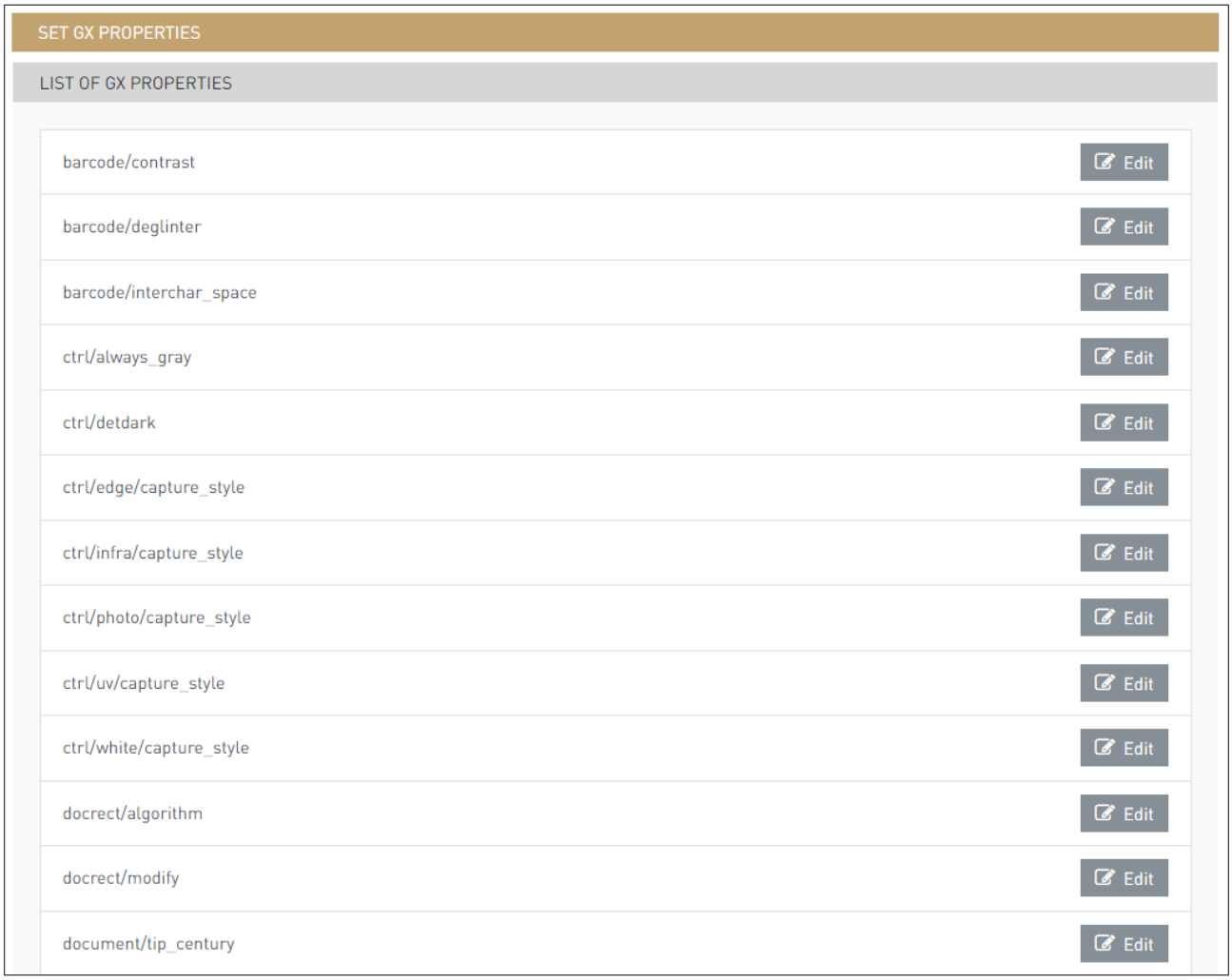
When setting the **Maximum number of items** or **Maximum number of unsuccessful items** to any value that is lower than the current number of items in queue, oldest items are deleted to meet new queue limit. E.g., if there are 5 documents in the **Unsuccessful queue** when **Maximum number of unsuccessful items** is set to 3, the two oldest documents in the queue are deleted. Every occurrence of deleting is logged into the device syslog (delete_queue).

2.4.11. GX PROPERTY

GX PROPERTY menu is designed to customize certain properties, which belong to one of the following categories:

1. Barcode
2. Capture
3. Document
4. RFID
5. Result
6. MotDet
7. Image Cropping

In the followings section these properties will be listed and explained.



1. Barcode

- barcode/contrast
  - **Value type**: Float
  - **Default value**: 1.5
    min: -3.0
    max: 10.0
  - **Description**: Barcode reading fine-tuning. Usable for barcodes with poor printing quality.

    Possible settings:

    -2: Automatic adaptation for barcode quality. Recommended if the same type and quality of barcodes are read.

    -3: Readjusting algorithm for every single barcode. Use if various barcode types and qualities are scanned.

- barcode/deglinter
  - **Value type**: Boolean
  - **Default value**: 0
  - **Description**: Special barcode reading algorithm optimization for barcodes covered with damaged foil.

- barcode/interchar_space
  - **Value type**: Boolean
  - **Default value**: 0
  - **Description**: Special barcode reading algorithm, specifically designed to read code 39 barcodes available on Mexican documents (printed with large gap between characters).

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

2. Capture
   - ctrl/always_gray
     - Value type: Boolean
     - Default value: 0
     - Description: If 1, it provides gray output images. Recommended for time critical applications.
   - ctrl/white/capture_style
     - Value type: Integer
     - Default value: 899
   - ctrl/infra/capture_style
     - Value type: Integer
     - Default value: 4739
   - ctrl/uv/capture_style
     - Value type: Integer
     - Default value: 4864
   - ctrl/edge/capture_style
     - Value type: Integer
     - Default value: 643
   - ctrl/photo/capture_style
     - Value type: Integer
     - Default value: 903

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

3. Document

- document/tip_century
  - **Value type**: Integer
  - **Default value**: 0
    min: 0
    max: 1
  - **Description**: It has effect on dates that do not contain the century, the algorithm tries to figure it out from the year and current date.

- document/tip_names
  - **Value type**: Integer
  - **Default value**: 0
    min: 0
    max: 3
  - **Description**: Name parsing algorithm for Australian documents.

    Possible settings:

    0 – Turned off.
    1 – Division of the name parts.
    2 – Transformation of lowercase/uppercase.
    3 – 1 and 2 can be combined if value is set to 3.

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

4. RFID

- rfid/air_speed
  - Value type: Integer
  - Default value: 848
    min: 106
    max: 848
  - Description: Speed of communication with the RFID chip (106, 212, 424, 848).

- rfid/pref_ext_ds
  - Value type: Integer
  - Default value: 0
    min: -1
    max: 2
  - Description: It controls the priority of document signer certificates (Cert.DS) during the checking process. The checking process is executed with:
    0: the file in the RFID chip first.
    1: the external certificate first.
    -1: the file in the RFID chip only.
    2: the external certificate only.

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

5. Result
   - save_cleanovd
     - Value type: Boolean
     - Default value: 0
     - Description: Black OVD image is saved in the ZIP file.
   - save_cleanuv
     - Value type: Boolean
     - Default value: 0
     - Description: Enhanced UV image is saved in the ZIP file.
   - save_fieldimage
     - Value type: String
     - Default value: ""
     - Description: Usable for saving image snippets of corresponding document fields, e.g., name, date etc.

6. MotDet
   - ctrl/detdark
     - Value type: Boolean
     - Default value: 0
     - Description: This property is specially developed for capturing dark documents (e.g., front cover of certain passports). If set to 1, motion is triggered on inserting dark documents as well.

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

7. Image Cropping

- docrect/algorithm

  - Value type: Integer

  - Default value: 0
    min: 0
    max: 2

  - Description: It configures the document cropping algorithm.

    Possible settings:
    0 – Standard algorithm
    1 – OCR engine-specific algorithm
    2 – First use the standard algorithm, then – if the first was unsuccessful – the OCR engine-specific one.

- docrect/modify

  - Value type: Integer
  - Description: Advanced document cropping configuration, based on OCR results.
    Possible settings:
    0 – No document frame modification
    1 – New document frame is applied
    2 – Modify upside down orientation only

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

2.5. MAINTENANCE

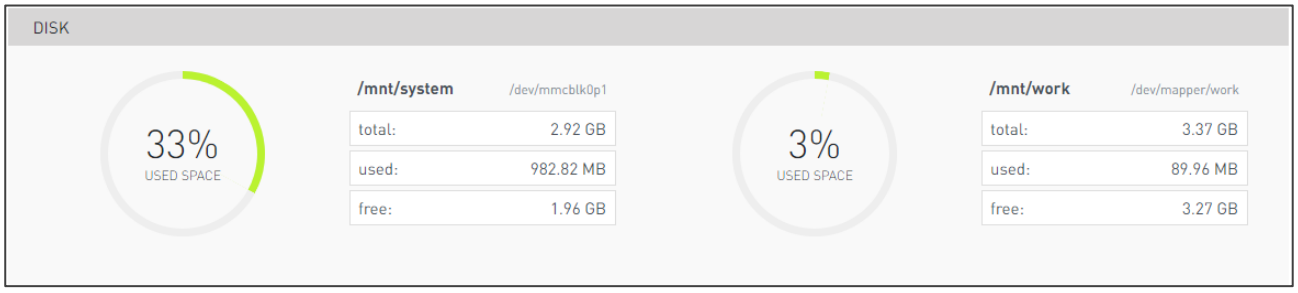
The MAINTENANCE section provides device information for support team and engineers upon any troubleshooting process.

2.5.1. SYSTEM INFORMATION

The Osmond N is equipped with a built-in OS (no other installation is needed). Current status of different elements of this PC can be observed here.
Under SYSTEM INFORMATION among others, you can check or perform the following:

- App version under SYSTEM INFORMATION / ABOUT
- Config version under SYSTEM INFORMATION / ABOUT

- Disk usage under SYSTEM INFORMATION / DISK



- Create logpack and operation log under SYSTEM INFORMATION / LOG MANAGEMENT.

Note

The following description of LOG MANAGEMENT is valid from version 1.8.x.
These functions are available from 1.8.x version.

The log files, mainly used for troubleshooting, can be downloaded in the LOG MANAGEMENT section. Use the following buttons in order to save the log files:

- Create logpack

  A diagnostic file named "systeminfo" (system-information_{timestamp}-UTC.zip) can be created with the Create logpack button. This file contains useful information for the support team to fix the possibly experienced errors. It is important to mention that there is always only one "systeminfo" file: by clicking on the [Create logpack] button the previous "systeminfo" file is automatically overwritten.

- Prepare download

  After generating the logpack (by clicking on the [Create logpack] button), click on the [Prepare download] button, and then the logpack can be downloaded directly from a link.

- Create operation log

  The "pr.log" file can be originated by clicking on the [Create operation log] button. This file contains the log of the API.

- Save operation log

  After generating the Create operation log, click on the [Save operation log] button.

Note

When specifying the log level at SCAN PROCESS / MAIN CONFIGURATION / Logging, take into consideration that the first digit with value between 0-2, is the level of the log originated under Create logpack button, and the second digit with value between 0-9, is the level of the log originated under Create operation log.

2.5.2. OPERATING MODE

In the OPERATING MODE menu select one of the following options which meets the requirements:

- NWI (Network Web Interface): Using the device with web browser. This is the default mode, when logging in to the web interface.
- USB: Using the device with PC application, connected via USB.
- NAI (Network Application Interface – NetAPI): Using the device with Passport Reader Network API.
- NWA (Network Web Application): Using the device in NWI mode, managed by Open API application.

> **Note**
>
> After selecting the operating mode, the device restarts immediately.

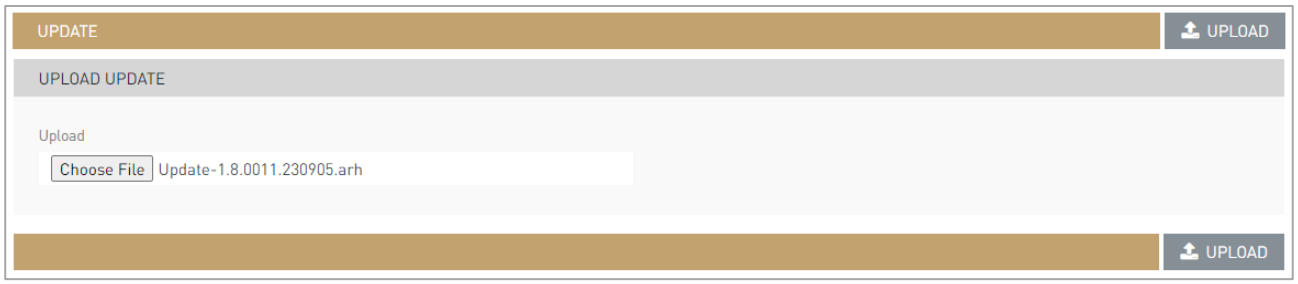
> **Note**
>
> The selecting field is only available, if the network webserver is in HTTPS mode.

2.5.3. UPDATE

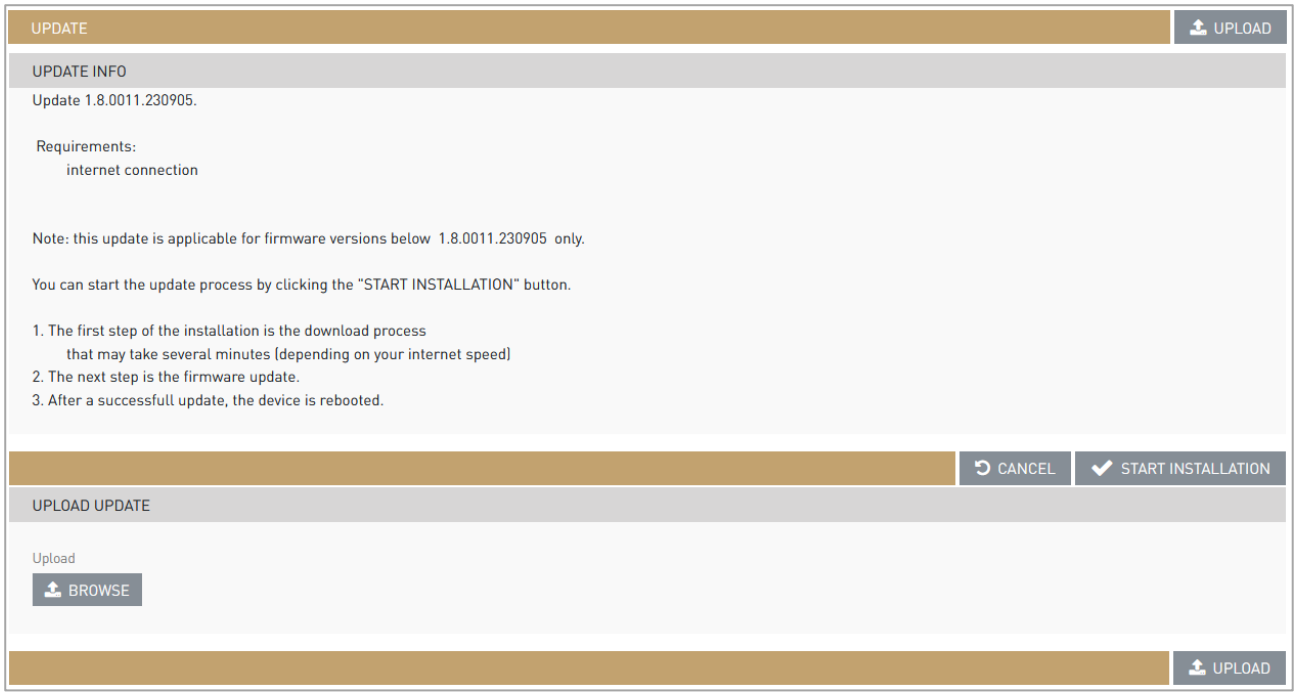
The purpose of the **UPDATE** menu is to provide an easy-to-use device firmware update feature for users with **Owner** privileges. Update files can be browsed and uploaded after clicking on the corresponding buttons.

The device updates are available and can be downloaded from the ADAPTIVE RECOGNITION website.

1. On the website click on **Firmware** and download the **WebGUI based** firmware update.
2. Then, in the **MAINTENANCE / UPDATE** menu click on the **[BROWSE]** button and select the downloaded update file.



3. Click on the **[UPLOAD]** button, and the following instructions appear:



4. Check the details in the **UPDATE INFO** field.

5. Then, click on the [START INSTALLATION] button to initiate the update process.

Important!

Internet connection is required during the update.

Important!

After updating the device, when opening the web interface, it is important to delete the browser cache (in most Windows and Linux browsers: Ctrl + F5 keyboard shortcut), because the features in the new firmware may not be appeared on the interface.

Note

Osmond N devices can be updated with MSI installer as well. For more information on firmware installation with MSI, see the Firmware Installation for Osmond with Updater MSI chapter.

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

2.5.4. BACKUP

The BACKUP option is designed to offer a feature to save all device settings and to load it back in the future, at any time. Backup option helps to avoid data loss upon any mayor software or hardware damage.
Only those sections can be saved under BACKUP, data of which can be modified by users during using the web interface. These are the following:

- Users
- Configuration data

The backup file (.zip) is password protected, thus the zip file can only be reuploaded to the same device.

Important!

It can cause malfunction if after version update, a backup file belonging to previous version is reuploaded to the device. If you are not sure that the previous backup will not cause any problem, then without version downgrade do not reupload such file.

2.5.5. RESTART

Use the RESTART option to apply any new network-, or operation related change in device configuration. On restart, all application of the device is restarted but its operating system remains fully operable.

2.5.6. REBOOT

Reboots the operating system of the device together with all its application. After REBOOT, all modules and programs are started automatically.

2.6. QUIT

Use the QUIT option to log out from the device.

VII. MAINTENANCE

The device has no moving parts – except for the motorized, auto-focus module – which ensures maximum reliability and low maintenance. However, in order to ensure that the device remains in a satisfactory operating condition, the following actions should be performed regularly.

1. CLEANING THE DEVICE

ADAPTIVE RECOGNITION document reader devices generally do not need any kind of special maintenance; however, they should be regularly cleaned in order to ensure that they are fully operational and are able to extract data from the IDs properly.

Important!

The devices are to be used indoors, in an office environment only (SOHO).

Osmond document reader package includes:

- 1 piece of **Passport Reader Glass Wet Wipe (alcoholic virucide wipe)**,
- 1 piece of **Passport Reader Glass Dry Wipe**.

Note

However, any kind of soft cleaning wipe and **standard mild glass cleaner liquid** can be used to clean the devices.

The glass window (the ID reading surface) should be cleaned regularly with mild glass cleaner and a soft cloth. Lint-free microfiber cloth is recommended for the best results.

Cleaning the reading surface **frequently** is of utmost importance, as contamination and stains on the glass surface could negatively impact the accuracy of the optical data reading, and shorten the lifespan of the glass itself.

Important!

Abrasive materials (e.g., sand) are to be avoided by any means.

Hard materials can also shorten the lifespan of the reading surface (for example metal objects (e.g., rings) touching the window glass). This kind of contact with the scanning window should be avoided.

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

1.1.1. DISINFECTION

Isopropyl alcohol (70%) can be used to safely clean and disinfect the surface of the document reader devices, both the scanning window glass and plastic parts. For the exact concentration of isopropyl alcohol which is sufficient to eliminate COVID19, please consult WHO and other trusted sources.

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

VIII. APPENDIX

1. CORRECT DOCUMENT PLACEMENT

The following section provides a short guide on how different types of documents should be placed on the scanning surface of the Osmond device in order to acquire the best OCR and authorization results.

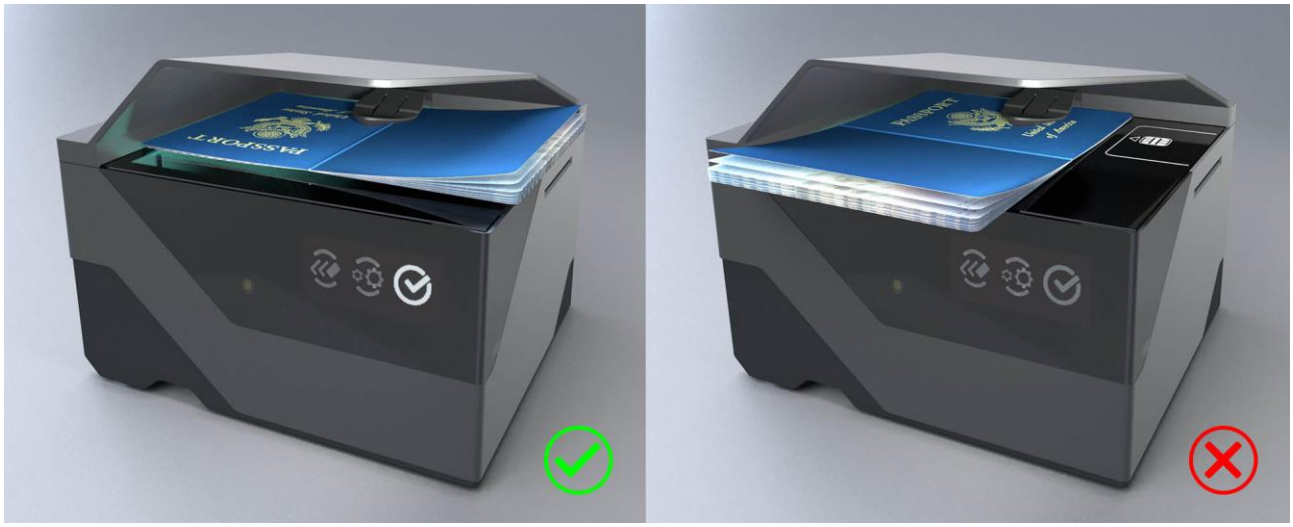
In case of ID1 and ID2 size cards (like national ID cards, driver licenses, EHIC – European Health Insurance Card, name/business cards or any other 86x54mm = 3.4"x2.1" sized (or smaller) printed document), place them in the middle of the scanning surface. The correct positioning must be performed according to the following images.

As it can be seen on the first two sample images, the cards can be placed vertically and horizontally as well. However, please avoid placing the card at close to the angle of 45 degrees (as it is shown in the third image).

Note

In most cases the optimal position of the ID is not necessarily in the corner of the scanning surface. However, certain authentication or reflection elements can make an exception to this.

In case of **passports**, place them horizontally in the upper left corner of the scanning surface according to the following images.



In case of **contact smart cards with chip,** use the smart card slot on the side of the device according to the following image.

Note

Please pay attention that the contact chip of the smart card must be facing up when inserting it to the slot.

2. OLED DISPLAY STATUS ICONS

2.1. OLED DISPLAY STATUS ICONS OF OSMOND NETWORK DEVICES

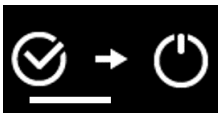
Unlike previous document scanner models, the Osmond device is equipped with OLED display. This screen is able to display the following status icons on Osmond network devices.

DISPLAY ICON	STATUS NAME	STATUS DESCRIPTION
	Ready to scan	The device is ready to scan. Insert document, then wait (Autonomous mode) or click on the SCAN button (Interactive mode).
	Scanning	Scanning images and performing OCR.
	RFID reading	Performing RFID chip reading.
	Remove / Flip document	Remove the document. In case of reading multiple-page document, insert the next document page onto the device.
	Moving	The document is moving on the glass.
	Waiting for the next page	Insert the next document page onto the device.
	Create ZIP package	Document images and data are packed and prepared for uploading to remote server or local database.
	Store data to queue	The document data is inserted into the upload queue. Upload is performed as soon as possible.

	Starting data upload	The data package upload is started.
	Upload done	The data package upload is successfully done.
	Upload error / Unsuccessful queue is full	The upload is failed or the documents in unsuccessful status have reached the maximum number of the unsuccessful queue.

2.2. OLED DISPLAY STATUS ICONS OF OSMOND USB DEVICES

Unlike previous document scanner models, the Osmond device is equipped with OLED display. This screen is able to display the following status icons on **Osmond USB devices**.

DISPLAY ICON	STATUS NAME	STATUS DESCRIPTION
	USB disconnected	The device is ready but USB disconnected
	USB connected	The device connected via USB
	Ready	The device is ready to scan
	Moving	The document is moving on the glass
	Moving ready	The document has stopped, and ready to scan
	RFID reading	RFID reading is in progress
	Working	Document reading is in progress
	File transfer	Firmware file is transferring
	Update in progress	Firmware update is in progress
	Update OK	Firmware update finished successfully
	Update error	Firmware update failed
	Power off	The device is turning off

Note

If you see the "Update error" icon during the update process, this indicates that the update has failed for some reason. In this case, the device automatically rollbacks to the original firmware version.

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

3. WEB INTERFACE READING PHASES – ICON DESCRIPTION

3.1. ICONS OF THE READING PHASES IN INTERACTIVE MODE

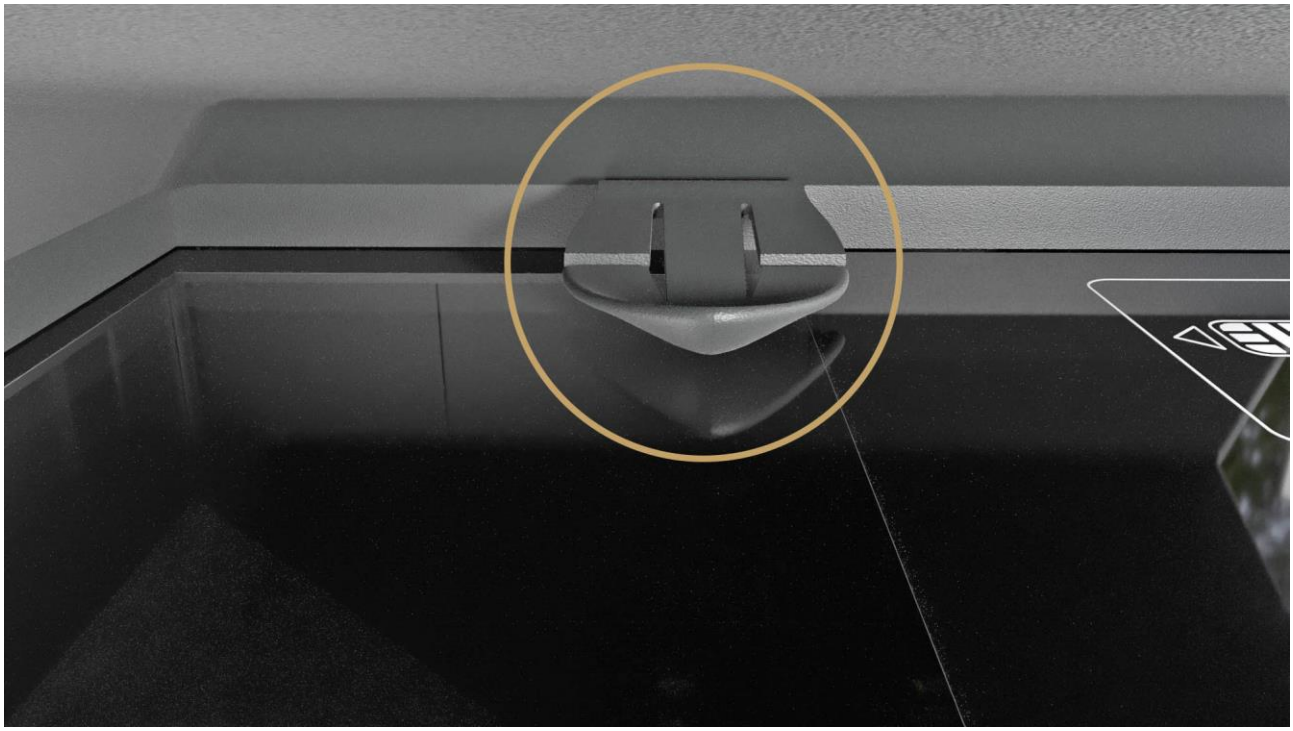
- Arrow icon: the SCAN button is clickable, by clicking on it the reading process begins
- Card icon: the document reading is in progress
- Plug icon: waiting for standby status
- Transmission tower icon: placing the result of the reading in upload queue
- Upload icon: upload is in progress

3.2. ICONS OF THE READING PHASES IN AUTONOMOUS MODE

- Plug icon: waiting for standby status
- Transmission tower icon: placing the result of the reading in upload queue
- "Remove page/document": waiting for the removal of the document
- "Put page/document": waiting for the insertion of the document
- Card icon: the document reading is in progress
- Upload icon: upload is in progress

4. REMOVING THE OSMOND DOCUMENT HOLDER

The Osmond device is designed with a removable document holder built in the shield.

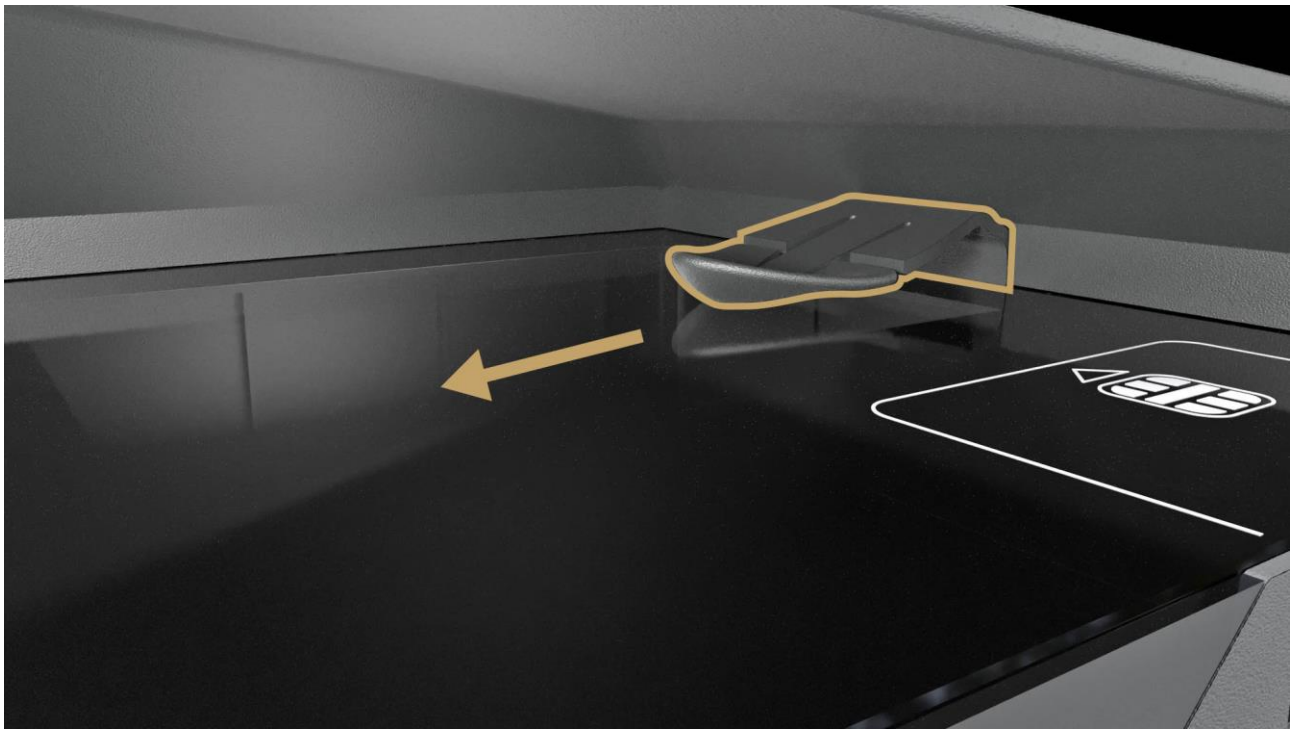


Document holder under the shield

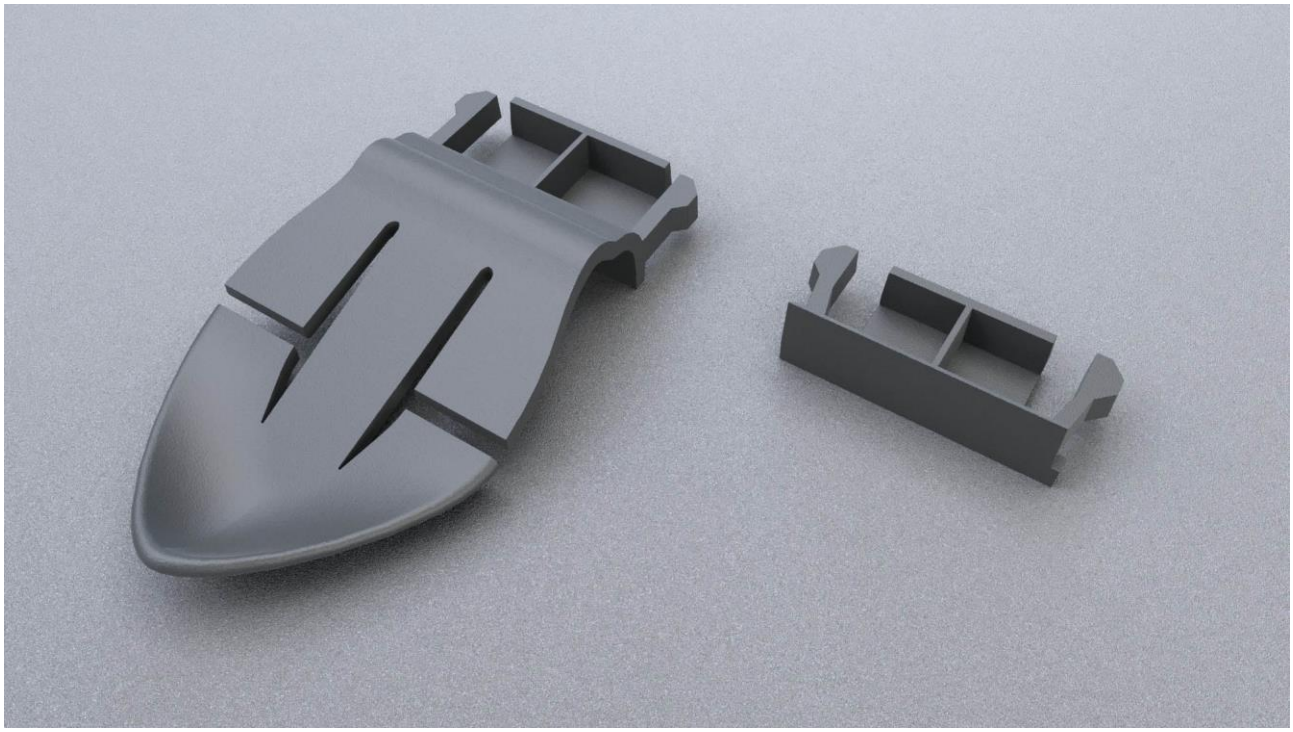
This feature can be vital in special cases e.g., scanning extremely thick documents which cannot fit to the device due to their size being incompatible with the document holder.

The process is simple and easy to perform in which the following steps will guide the user:

1. Hold firmly the document holder and carefully pull it towards the front side of the device (OLED display, ON/OFF touch button) to remove it.

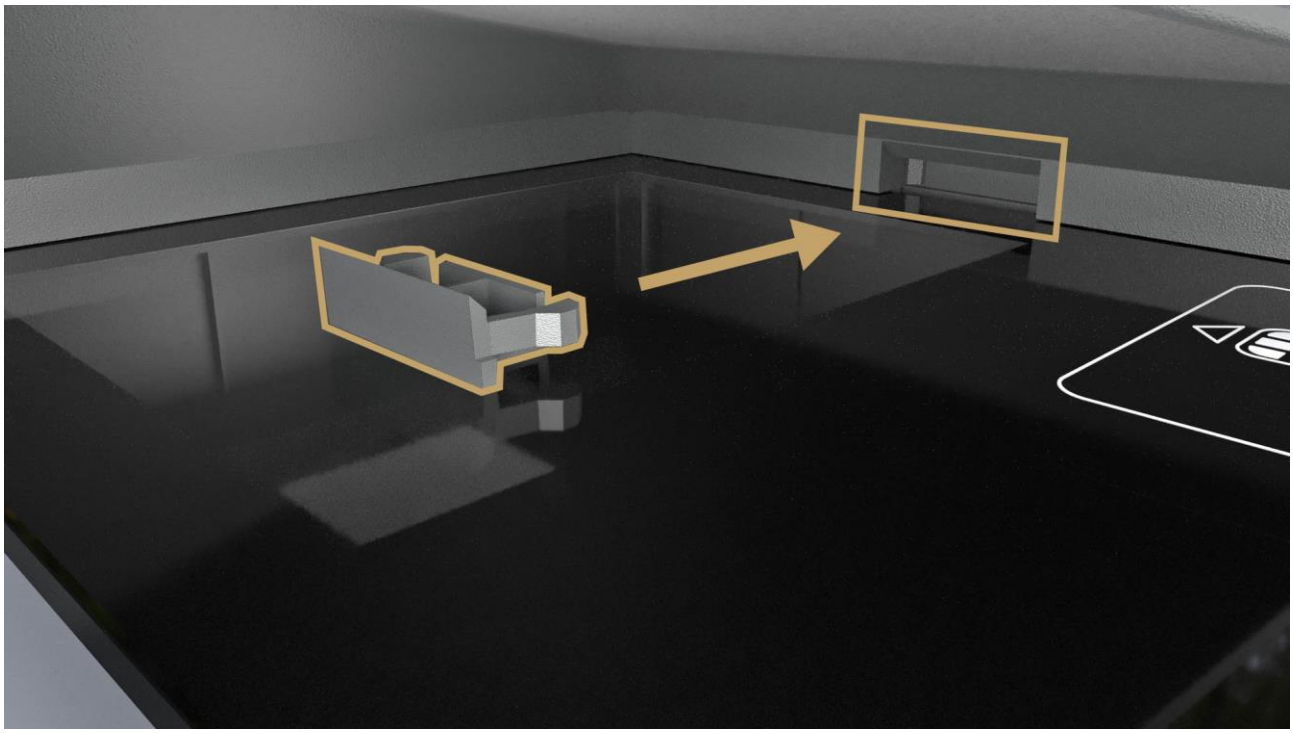


2. Look for the blind plug which is provided with the device in the box.

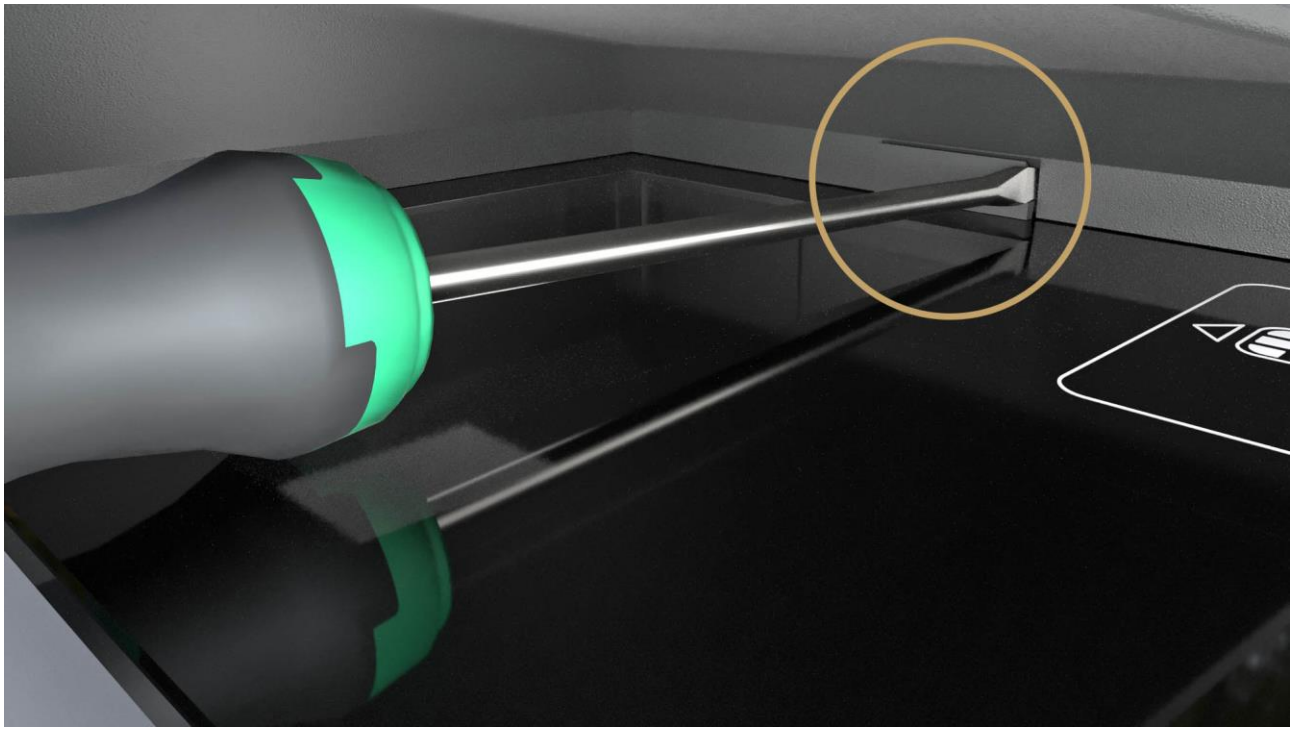


The document holder (left) and the blind plug (right)

3. Gently push the blind plug into the slot of the document holder.



4. If the document holder is to be put back to the device later on, then the blind plug can be removed by using a long and flat screwdriver.



Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

5. OLED STANDBY MODE

In order to protect the lifetime of the OLED display, the OLED screen enters idle mode.

> **Note**
>
> The OLED display switches to standby state after 15 minutes of inactivity. The blinking green LED with the black OLED screen indicates this state.

By using the **ctrl/screen_standby** property a time interval can be specified, after which the OLED screen of the device enters idle mode (sleep mode). This function can be activated by:

1. specifying **Screen standby** function in the PRDTool utility tool,
2. specifying it on the **OPTIONS / MANUAL SETTINGS** tab in the Full Page Reader application,
3. modifying the gxsd.dat file.

> **Note**
>
> In the device firmware a fixed 3600 sec timer is set. Following this the OLED brightness is reduced to 20%, but it is not turned off.
> In the case of modifying the gxsd.dat file (see below), the customized value will be valid in the given environment and the OLED display operates as explained in the following section.

1. In the PRDTool utility tool:

In the PRDTool click on the cogwheel icon in the **Settings** column to open the additional features menu. Enable the **Screen standby** option and specify a time period. In order to save the changes, click on the **[Apply]** button.

> **Note**
>
> When the screen standby mode is activated, the OLED fades for 3 seconds, then it goes dark completely. At this point, the power button LED starts blinking green.

> **Note**
>
> For more information on setting the standby mode in PRDTool, see PRDTool appendix.

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

2. In the Full Page Reader application:

> **Note**
>
> This method is currently available only in USB mode.

In the Full Page Reader application navigate to the **OPTIONS / MANUAL SETTINGS** tab, and type "**ctrl/screen_standby**" (without apostrophes) into the "**PROPERTY NAME**" field and specify any decimal value as "**PROPERTY VALUE**".
The decimal value is in seconds (example: if you specify the decimal value as "5", the OLED screen fades after 5 seconds of the device being idle). The OLED screen fades after the specified time has passed. After the fade out and an additional 3 seconds the OLED screen turns off.

> **Note**
>
> By default, a 3-second period is between the fade out and the off state.

> **Note**
>
> If you specify this setting in Full Page Reader App exclusively, it is only active until closing the application and the property must be set again after startup.

3. In the gxsd.dat file:

> Note
>
> This method is currently available only in USB mode.

In the gxsd.dat file, add the following:

```
<ctrl>
      <screen_standby value="X"/>
</ctrl>
```

This is to be pasted anywhere into the <pr> section. The value "X" must be a decimal value in seconds. The OLED screen fades after the specified time has passed. After the fade out and an additional 3 seconds the OLED screen turns off.

> Note
>
> By default, a 3-second period is between the fade out and the off state.

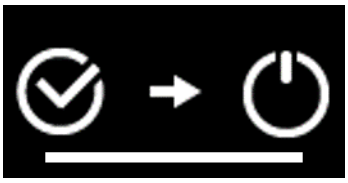
However, if you modify the gxsd.dat file as mentioned, the setting will be default which will be reflected in the application as well. This only needs to set once in the gxsd.dat file.

> Note
>
> This setting only goes live after the scanner is connected in the application. If the scanner is turned on, but it is not connected in the application, the device operates as set in its own gxsd.dat file. However, after connecting the scanner in the app, the setting goes live and the display enters sleep mode after the time specified.

6. SHUTDOWN PROCESS

To turn off the device, perform the following steps:

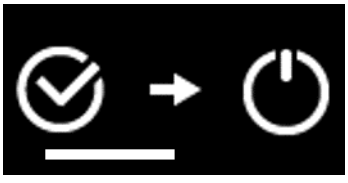
1. Press and hold the power touch button until the shutdown process starts. Hold the power touch button for another 5 seconds. The progress bar on the OLED screen shows the remaining time.



2. Release the button.

3. Press and hold the power touch button again in order to approve the process.

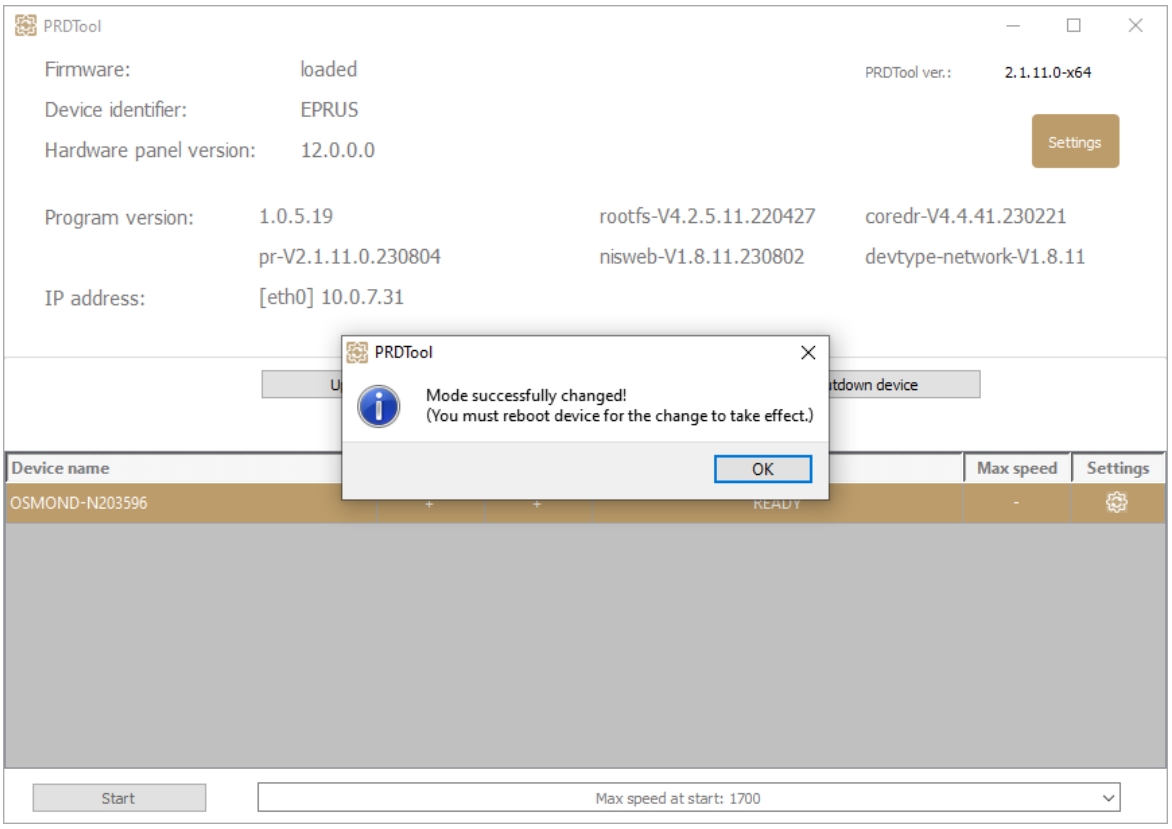
Hold the power touch button for a few seconds. The progress bar on the OLED screen shows the remaining time.



4. The shutdown process is finished, the device turns off.

7. DEVICES CAPABLE OF DUAL OPERATIONAL MODE

Osmond N model is able to operate in both USB and Network mode. On this device you can easily switch between modes by using a small utility tool called PRDTool.



PRDTool is part of the PR software packages from version 2.1.9.1 and above, so in order to use it you need to install the software which was discussed in USB DEVICES section.

The PRDTool is usually located in „C:\Program Files\Adaptive Recognition\utils\PRDTool\" or „C:\Program Files (x86)\Adaptive Recognition\utils\PRDTool\" folder depending on the architecture of the installed PR software.

The tool's purpose is to gather various information from passport reader devices, such as firmware version, network information, etc.

The tool is also providing the user with an interface to carry out various tasks on the device, like switching mode, firmware update or device reset.

Note

For more information regarding the PRDTool and switching between modes, see PRDTool appendix which describes the whole process in detail.

8. LICENSE MANAGEMENT

This short description will guide you through the steps of uploading ADAPTIVE RECOGNITION Passport Reader licenses to your document reader device.
In case of a new order, license upload is required only when the ordered software license was supplied separately (not pre-installed on the scanner).

Purpose of licenses

Each software module has its own related license file, storing:

- Issuing date
- Expiry date
- Device serial number

The update service period of the given software module is controlled by the expiry date. All software versions that are issued prior to this date, will run on the device.

License storage

In case of all scanner models that were manufactured in 2014 or later, the licenses are stored on the scanners.

Ways of uploading licenses

- In case of USB devices: For uploading licenses to a small number of specific scanners, our suggestion is using the License Manager application. If you have a larger quantity of scanners and licenses to be copied, we offer an automated license upload feature as well.
- In case of Network devices: Licenses can only be uploaded to network devices via web interface. For more information see License Upload via Web Interface chapter.

Migrating licenses between devices

License migration is not possible, as all issued licenses are linked to one scanner, based on its serial number.

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

8.1. LICENSE UPLOAD USING LICENSE MANAGER

The License Manager application is designed to upload ADAPTIVE RECOGNITION passport reader license files to a specific document reader device.

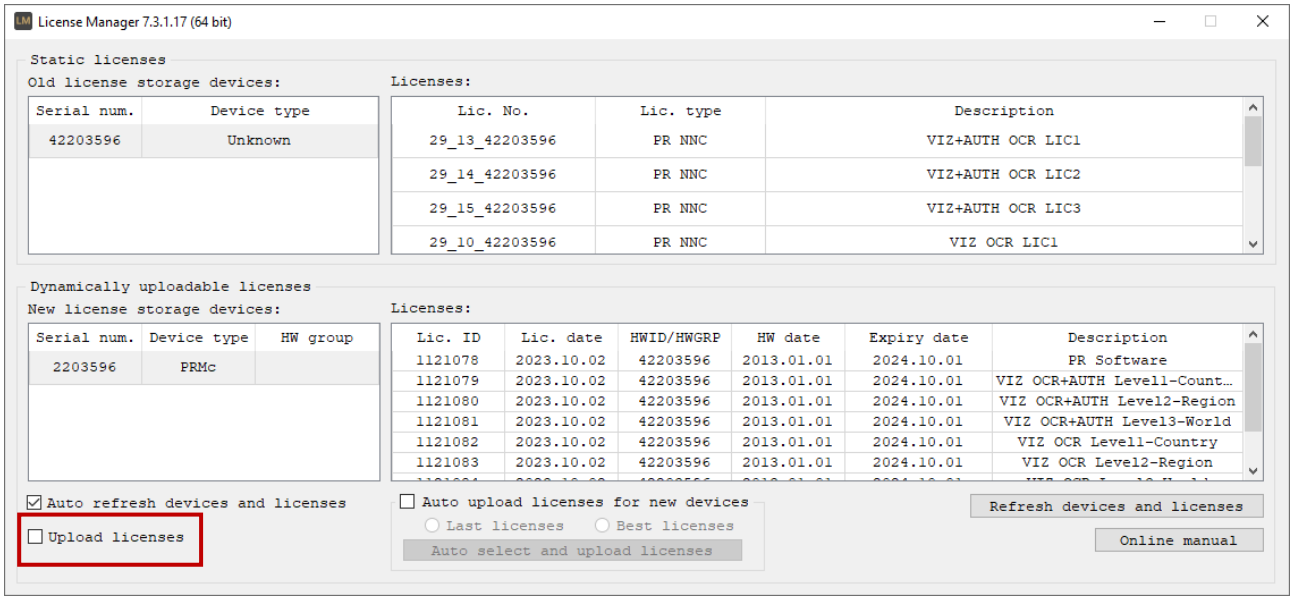
8.1.1. INSTALLATION

The application gets automatically installed by installing Passport Reader version 2.1.7. and above versions.

8.1.2. STEPS OF LICENSE UPLOAD

1. Enable the "Upload licenses" option to view functions for uploading licenses.

> **Note**
>
> If "Auto upload licenses for new devices" is enabled, the function is greyed out.



2. Make sure that the new license files are copied under the path specified at "License directory".

3. **Select the license(s) to upload** to your device. In order to select more licenses at the same time, please use the Ctrl + left click.

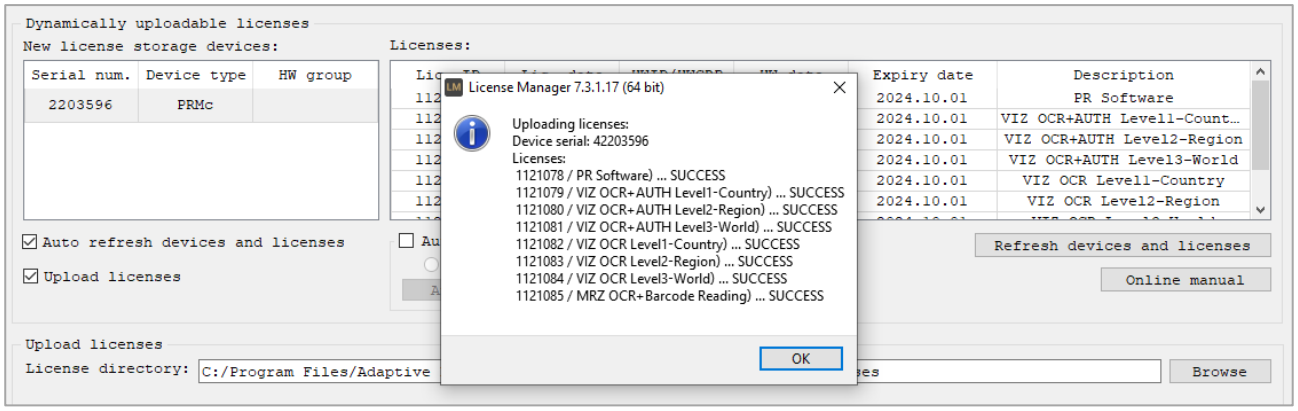
Hint

By enabling the "**Auto upload licenses for new devices**" option, licenses can be uploaded automatically, according to one of the following logics:

a. Last licenses: Automatically upload the latest license file for the connected device (license update).

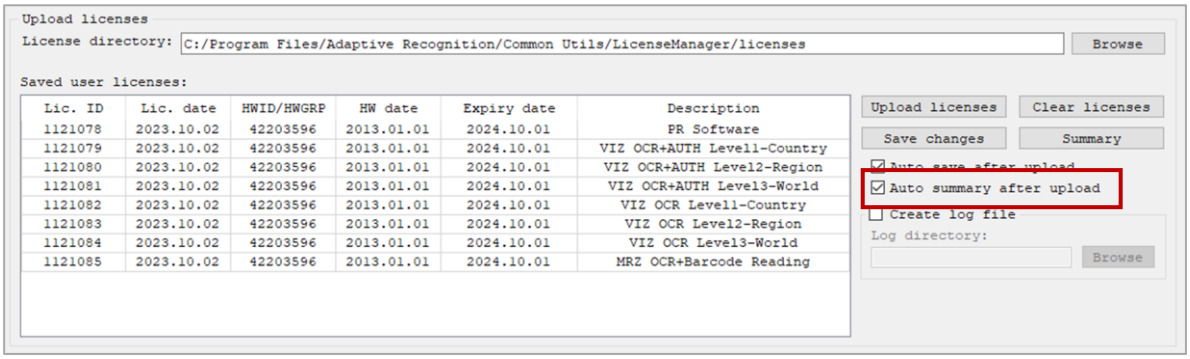
b. Best licenses: Automatically upload licenses that provide support the maximal number of documents/region (license upgrade).

4. **Click** "**Upload licenses**" to copy the selected license(s) to your device and check their presence in the "Licenses" textbox.

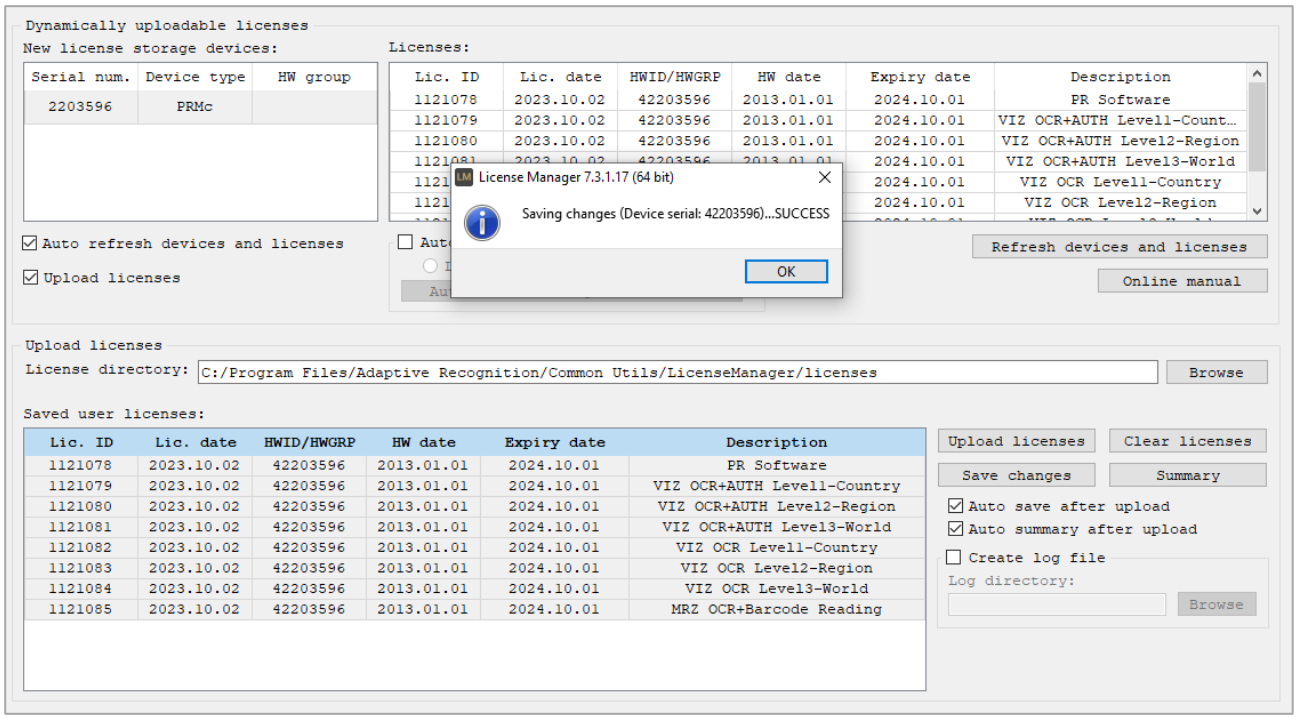


Hint

Enable "**Auto summary after upload**" to have an instant pop-up feedback after successful upload.

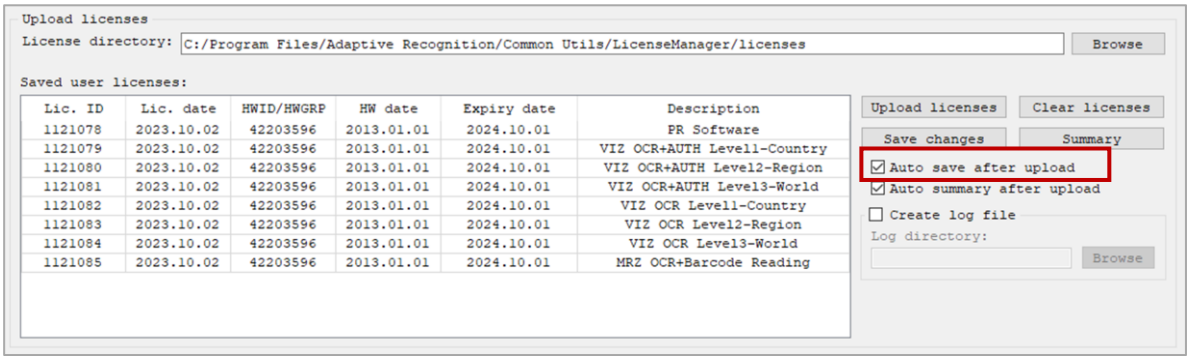


5. Click on "Save changes" and exit the application.



Hint

Enable "Auto save after upload" to skip using "Save changes" after each license upload.



8.2. AUTOMATED WAYS FOR LICENSE UPLOAD

For uploading licenses to multiple devices, we offer automated methods instead of using License Manager one-by-one with each scanner.

8.2.1. STEPS

Automated upload can be activated in the following way:

1. Set the update_licenses property to 1. This can be done via gxsd.dat (within the <pr> and </pr> nods) or by using the SetProperty() function.
2. Move the license files to ProgramData\GX\pr folder.
3. Once that is completed, upload will be performed automatically, by the UseDevice() function. In practice, it happens when the scanner is started by either ADAPTIVE RECOGNITION Full Page Reader or any end user application.

More information about update_licenses property

- 0: automatic license update is disabled
- 1: automatic license update is enabled
- 2: automatic license update is enabled but only once. After a successful update, the value of update_licenses property is automatically changed to 0. This value is designed to skip checking hundreds of licenses upon each UseDevice() function that may require few seconds.

8.2.2. USING MSI PACKAGE

The above logic can be implemented in a special MSI package that performs exactly the same automated license upload tasks on your passport reader devices. This special MSI package is available on request from ADAPTIVE RECOGNITION Support Team.

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

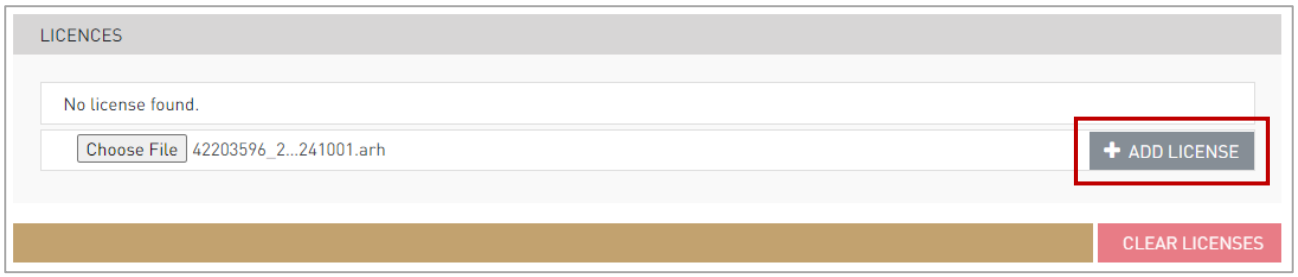
8.3. LICENSE UPLOAD VIA WEB INTERFACE

1. First you need to sign in on the web interface of your document reader.

> **Note**
>
> In order to access the web interface of the device, please follow the steps of the following chapter: Accessing the Web Interface of the Device from a Browser.

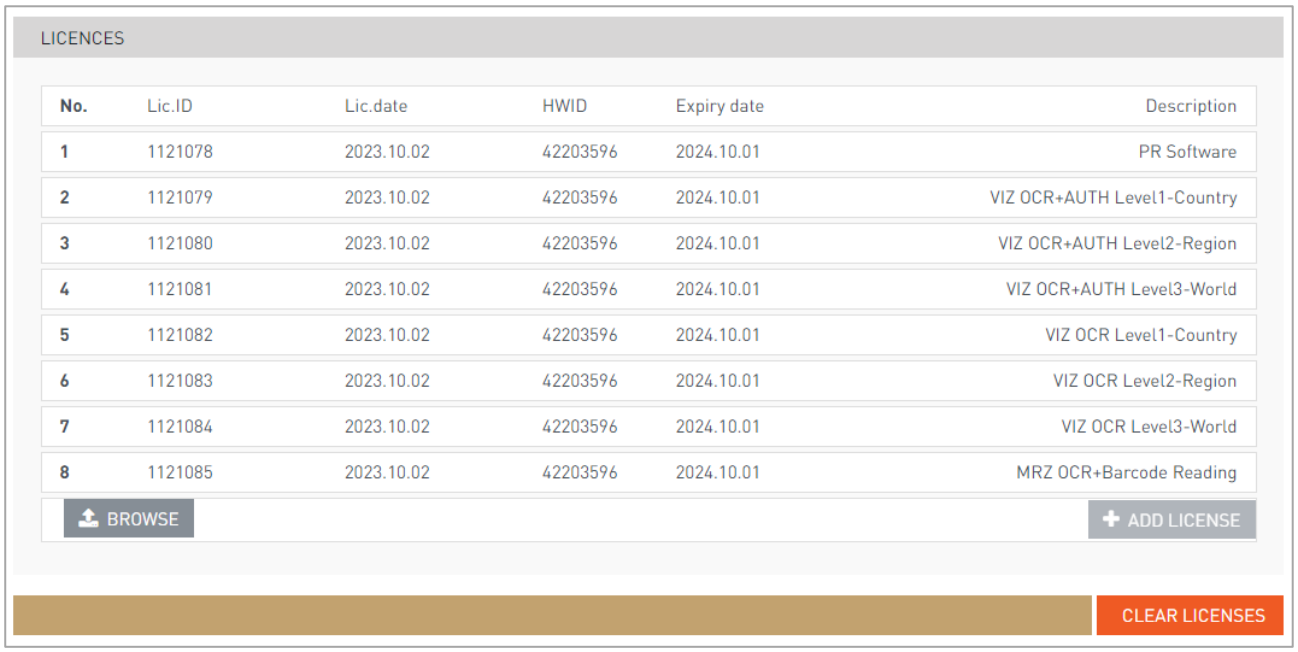
2. After logging in, click on the **Main menu** (the three horizontal stripes; at the top left corner of the webpage) and locate **ADMINISTRATION / ENGINES AND LICENSES / LICENSES** submenu.

3. In order to upload a license, click on the **[BROWSE]** button and select the corresponding one. Afterwards, click on the **[ADD LICENSE]** button.



> **Note**
>
> The extension of the license file is ".arh" and the license file name begins with the serial number of the device.

4. When you have added the required license file, press F5 in order to refresh the page. Then, the uploaded license is listed under LICENSES.



Note

The system also sends a notification about the success or failure of the saving. Check the notification panel by clicking on the notification icon displayed on the left side of the status bar located at the bottom of the screen.

9. VIZ OCR AND VIZ AUTH OCR ENGINE MANAGEMENT

This short description will guide you through the steps of uploading ADAPTIVE RECOGNITION Passport Reader engines to your document reader device.

OCR engines are add-on modules of the Passport Reader software. They are required for reading and identifying the VIZ (Visual Inspection Zone) fields of the documents.

The following types can be distinguished based on zone coverage:

- country (L1 / Level 1 Single Country)
- region (L2 / Level 2 Region)
- world (L3 / Level 3 World)

> **Note**
>
> The use of OCR engine is license-bound.

Ways of uploading OCR engines

1. In case of **USB** devices: OCR engines can be uploaded with MSI installer.
   OCR engines are available and can be downloaded from the ADAPTIVE RECOGNITION website.

2. In case of **Network** devices: OCR engines can be uploaded to network devices via web interface.

Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

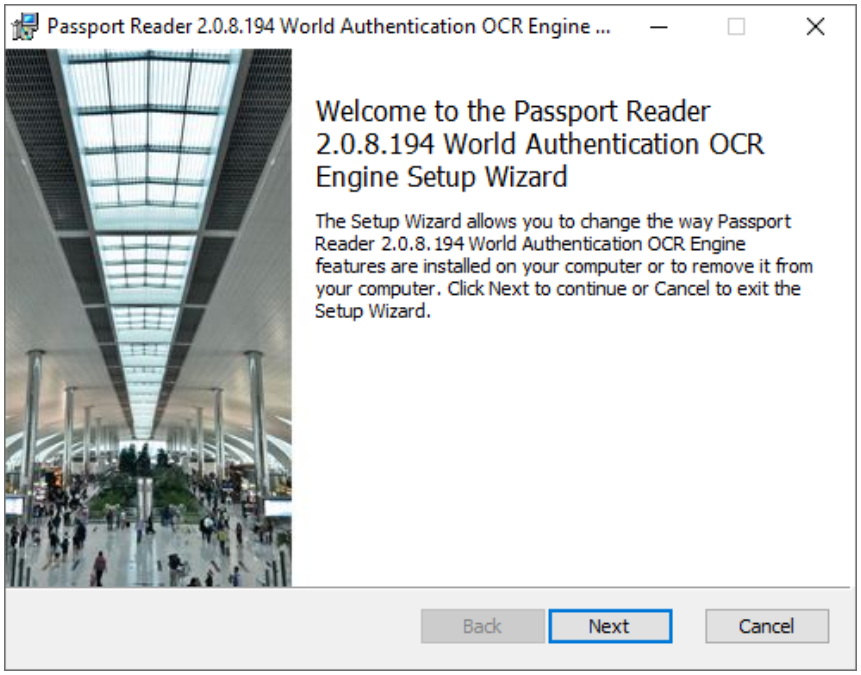
9.1. UPLOADING OCR ENGINES TO USB DEVICES

Important!

Administrator rights are needed for installation.

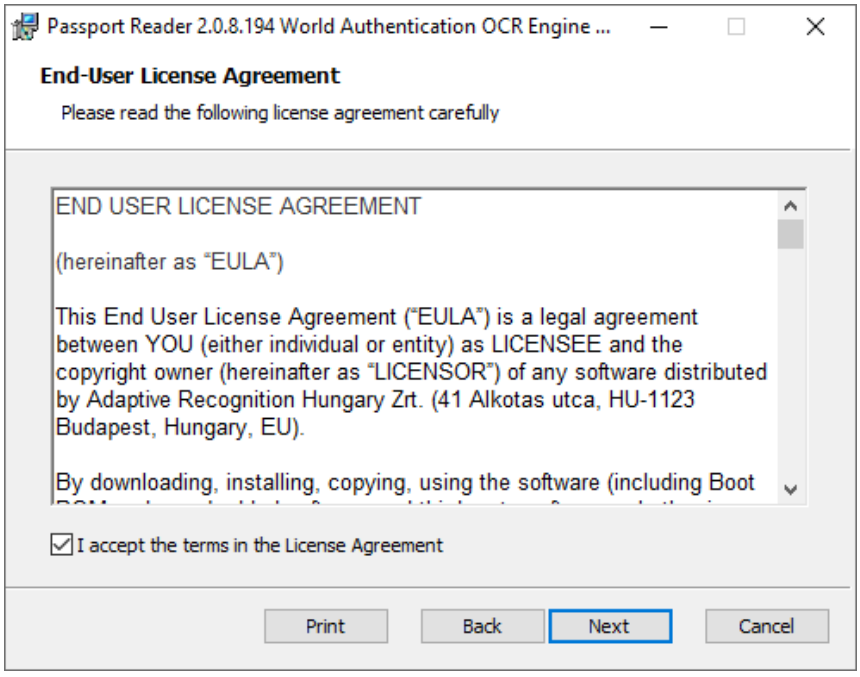
OCR engines are available and can be downloaded from the ADAPTIVE RECOGNITION website.

1. On the website click on **Engines** and click on the **[Download]** button belonging to the selected OCR engine (VIZ OCR or VIZ AUTH OCR).
2. By clicking on the **[Download]** button the webpage redirects you to the **VIZ OCR Software Add-On for VIZ reading** page.
3. Under **Engines** select the required version and click on its **[Download]** button.
4. Open the downloaded package and select the appropriate folder depending on the OS and device.
5. Run the **procr-XXX_ocr-2.0.X.XX.msi** installer.
6. The installation starts with the following window:

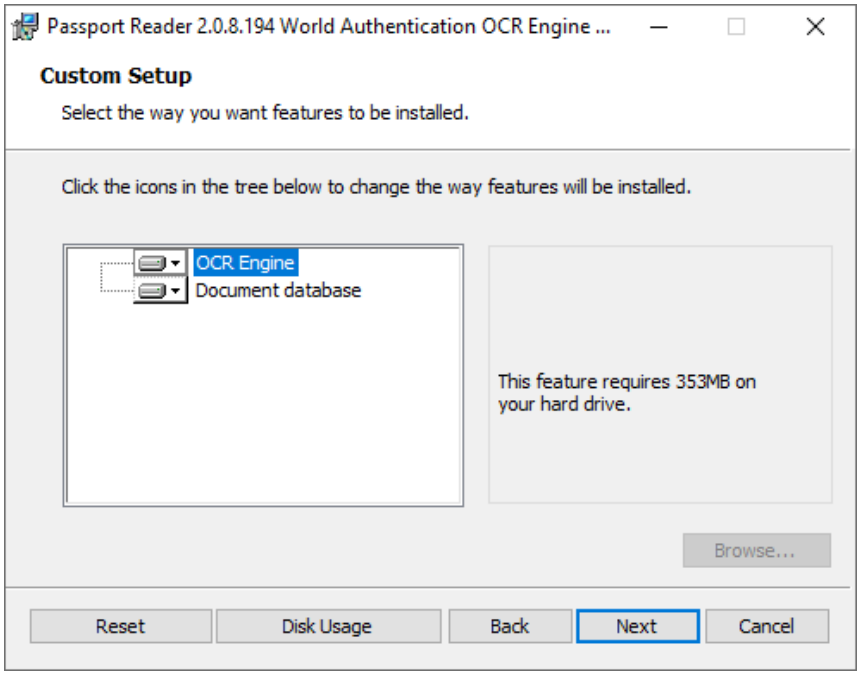


7. Click **[Next]** to launch installation.

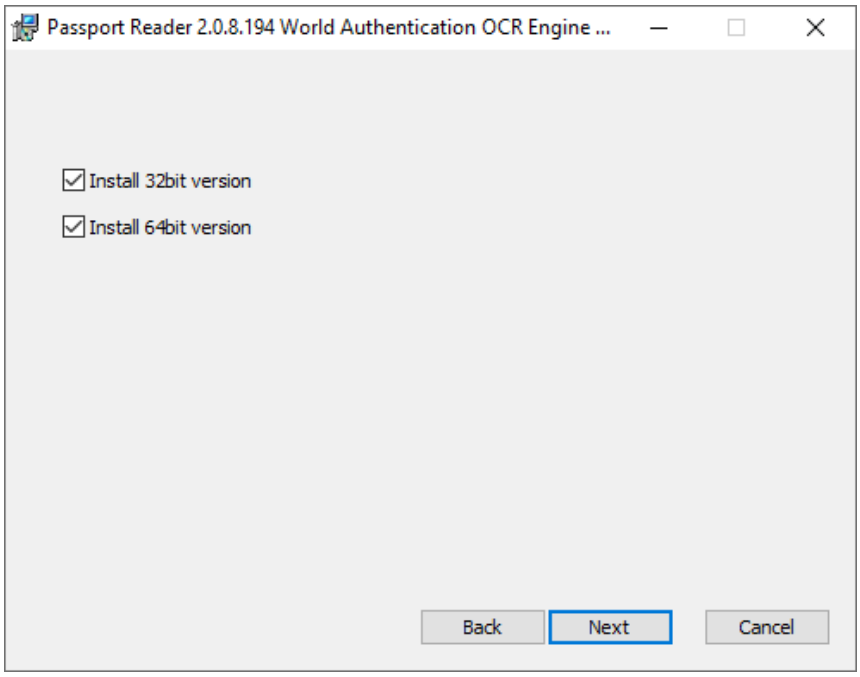
8. Accept the EULA (by ticking the checkbox above) and start the custom installation process by clicking on [Next].



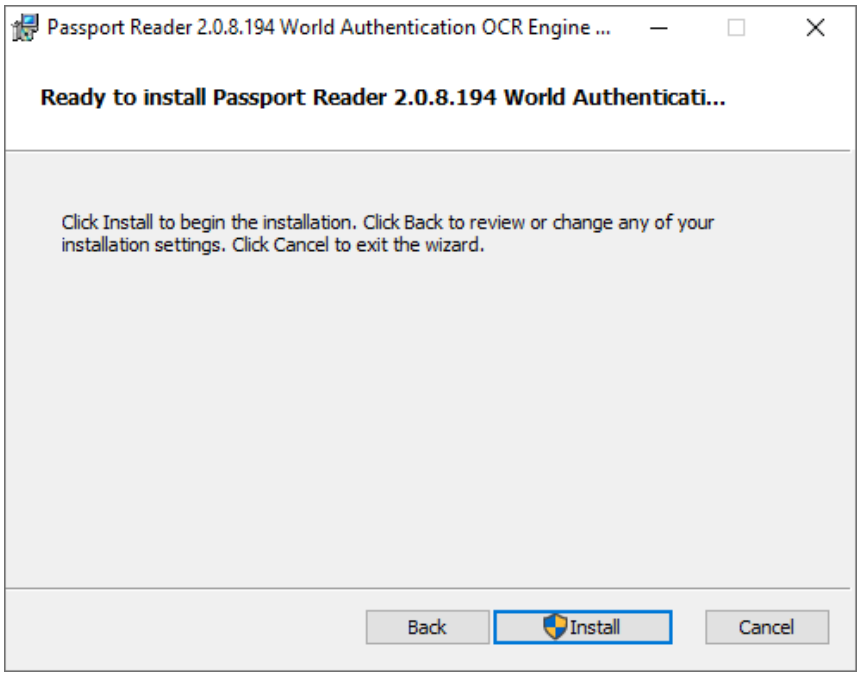
9. In the Custom Setup window, select the modules to be installed according to your preferences.

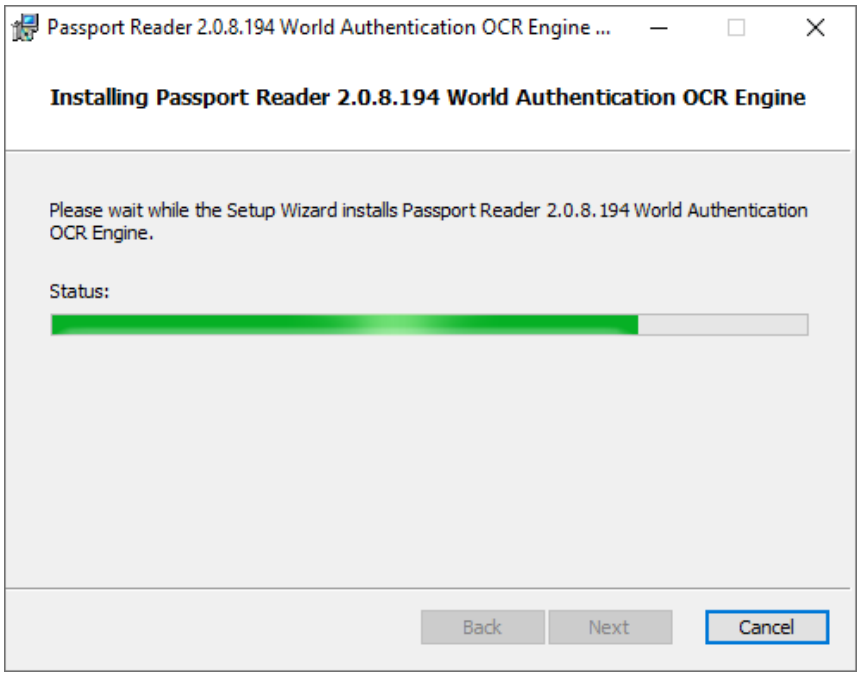


10. Select the bit version of the engine to be installed according to your system architecture.

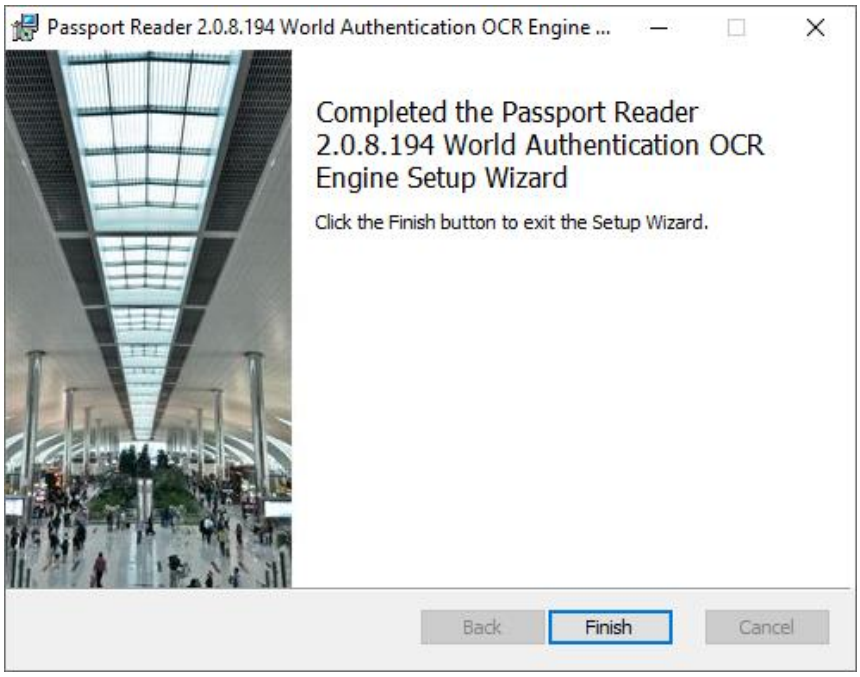


11. Clicking on [Install] will begin installation.

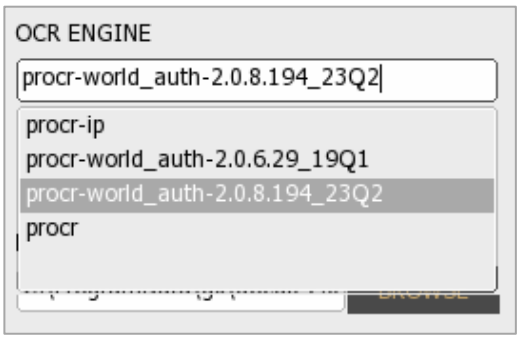




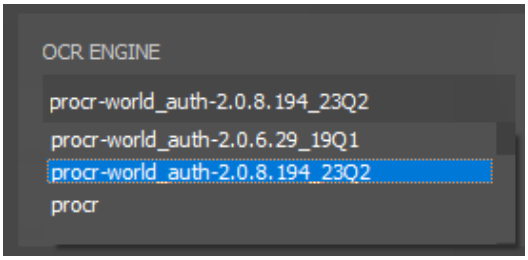
12. Click [Finish] to complete the installation.



13. After finishing the installation, select the installed OCR engine in the Full Page Reader or Authentication Checker application.



In case of Full Page Reader



In case of Authentication Checker

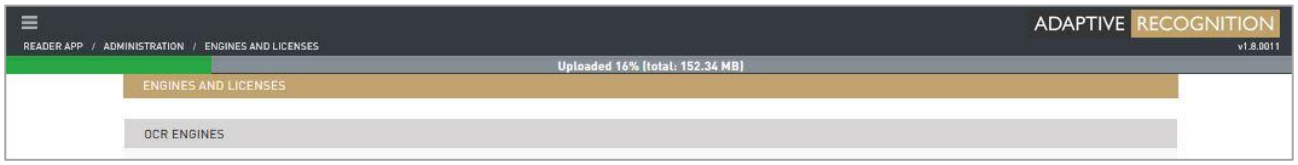
9.2. UPLOADING OCR ENGINES TO NETWORK DEVICES

OCR engines are available and can be downloaded from the ADAPTIVE RECOGNITION website.

1. On the website click on **Engines** and click on the **[Download]** button belonging to the selected OCR engine (VIZ OCR or VIZ AUTH OCR).
2. By clicking on the **[Download]** button the webpage redirects you to the **VIZ OCR Software Add-On for VIZ reading** page.
3. Under **Engines** select the required version and click on its **[Download]** button.
4. Then, sign in on the web interface of your document reader.

> **Note**
>
> In order to access the web interface of the device, please follow the steps of the following chapter: Accessing the Web Interface of the Device from a Browser.

5. After logging in, click on the **Main menu** (the three horizontal stripes; at the top left corner of the webpage) and locate **ADMINISTRATION / ENGINES AND LICENSES / OCR ENGINES** submenu.
6. In order to upload the engine, click on the **[BROWSE]** button and select the procr-XXX_ocr-2.0.X.XX.arh file from the "**network**" folder of the downloaded OCR package.
7. Afterwards, click on the **[ADD ENGINE]** button. A progress bar will indicate the status of the uploading process.



8. After a few seconds, the uploaded engine is listed under the **OCR ENGINES** section. If the given engine is not displayed, press Ctrl + F5.