ADAPTIVE **RECOGNITION**

Osmond
User Manual

This manual contains instructions on accessing the web interface, system settings and setup guidelines, as well as usage and maintenance.

RELEASE DATE
07.11.2024.

OSMOND

USER MANUAL

Passport Reader Software Package v. 2.1.11.1
Firmware v. 1.8.0011

Document version: 07.11.2024.

Table of Contents

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

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

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

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

I. QUICKSTART GUIDE OF OSMOND L, R AND N

1. WHAT'S IN THE BOX

1 Osmond Passport Reader

2 Power Cord Schuko CEE 7/7

3 Universal Power Supply
100-240 V AC, 50/60 Hz

4 Glass Cleaner Wet Wipe

5 Glass Cleaner Dry Wipe

6 USB 3.1 A-C
INCLUDED WITH R AND L MODELS

7 Ethernet RJ45
INCLUDED WITH N MODELS

8 USB 3.1-C
OPTIONAL WITH ALL MODELS

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

2. HOW TO GET STARTED

2.1. USB DEVICES – OSMOND R AND L

1. Connect the **USB cable** to the scanner (USB-C) and to the PC (USB-A).
2. Connect the **power supply** to the scanner.
3. Connect the **power cord** to the to the power supply and to the wall socket.
4. Turn the device on by covering the **power touch button** for 1-2 seconds.
5. After the button led turns **from red to green**, the device starts booting, which may take a few minutes. The status icon displayed on the OLED screen will indicate the current status of the process. For more information on it, see the OLED Display Status Icons chapter.
6. Install our latest **Passport Reader Software Package** on Windows or Linux. The Software Package is available from our portal. For more information on it, see Software Installation chapter.

> **Note**
>
> In case of **installation rollback**, reinstall the Passport Reader Software Package **as admin**. For more information on the installation process, see Software Installation chapter.

7. The **default PR OCR** engine is embedded to the **Passport Reader Software MSI**, there are no other tasks to perform. However, in case of purchasing **VIZ OCR** or **VIZ AUTH OCR engine**, download the required VIZ OCR or VIZ AUTH OCR engine from the ADAPTIVE RECOGNITION website and perform the installation. For more information on it, see VIZ OCR and VIZ AUTH OCR Engine Management chapter.
8. The **default license** valid for the basic software functions is **pre-installed** on the device. In this case the license is up to date, thus there are no other tasks to perform. However, **license upload is required**, when:
   - Purchasing **VIZ OCR** or **VIZ AUTH OCR** engine,
   - Purchasing **Autofill** application,
   - Purchasing **license update**,
   - Purchasing other **additional software**,
   - The ordered software license was **supplied separately**.

   For more information on license upload, see License Management chapter.

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

9. **Operating the device** according to application areas:

   9.1. **For end-user, or testing the software setup:**

   - Full Page Reader application (**default operation mode**) (included in the PR Software Package)
   - Authentication Checker application (included in the PR Software Package)

   9.2. **For quick integration:**

   - Autofill application (sold separately)

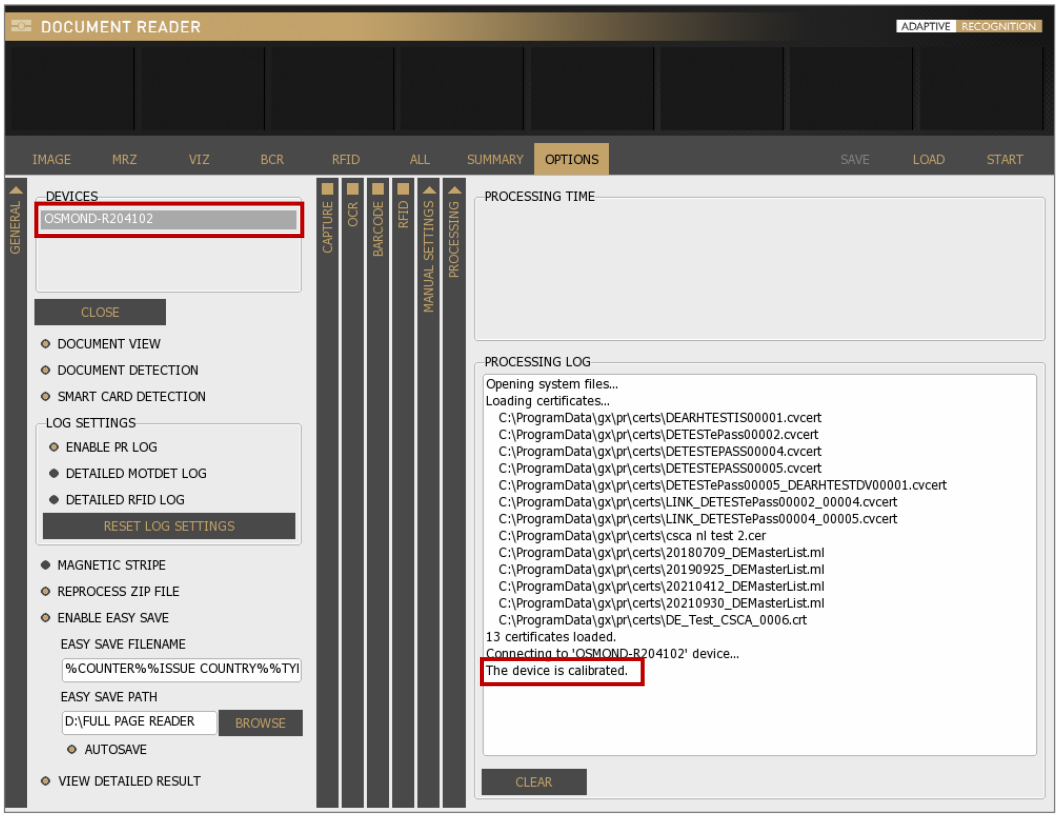
   9.3. **For solution developer:**

   - API
   - Twain
   - NAI

10. Check if the **setup was successful**:

    In case of the default application, **Full Page Reader (FPR)**, the steps are the following:

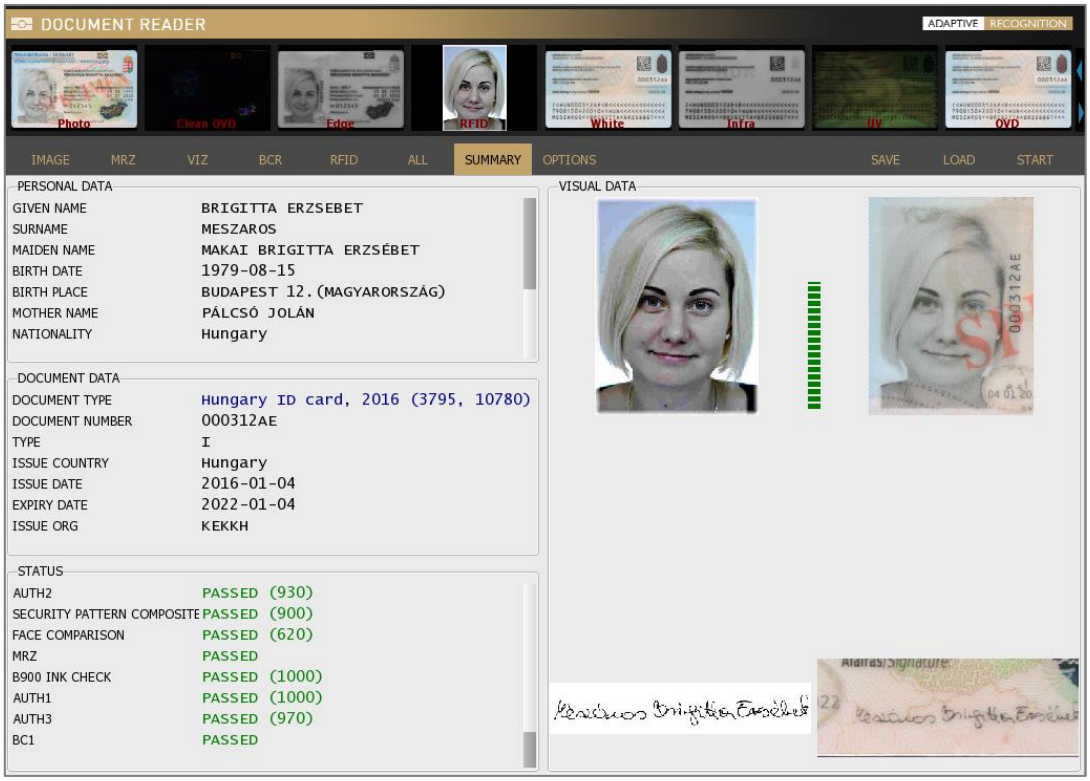
    - If in the opened FPR application the device is **displayed in the DEVICES list** and it is **highlighted in grey** as well as in the **PROCESSING LOG** field "**The device is calibrated.**" message appears, then the reader is **connected** and **ready to use**.



Note

If a **device is connected** to the computer, but it is **not displayed** in the **DEVICES** list, then try to **change the USB port** and/or **USB cable**. If the issue is not resolved after these changes, **reinstall** the Passport Reader Software Package **as admin**. For more information on the installation process, see Software Installation chapter.

- After the device is connected successfully, **place a document on the scanning surface** of the reader. The device starts the scanning process automatically.
- After the scanning process is finished, the **extracted data can be examined** in the application.



Note

For more information on **Osmond USB** devices, see Osmond R and L (USB Devices) chapter.

2.2. DUAL USB/NETWORK INTERFACE DEVICES – OSMOND N

Note

Osmond N model is able to **operate** in both **USB and Network** (default) mode. **Switching between modes** can be easily done by using PRDTool, which is part of the PR software packages from version 2.1.9.1 and above. In order to use this utility program, install the Passport Reader Software Package which is available from our portal. For more information on the installation, see Software Installation chapter.
In case of **using the device in USB mode**, follow the steps discussed in the USB Devices – Osmond R and L chapter. Note, that USB cable will be required.

1. Connect the **power supply** to the scanner.
2. Connect the **power cord** to the power supply and to the wall socket.

Note

Regardless of the operation mode (USB or network), the **Osmond N** device can be powered via PoE+ switch or PoE+ injector with standard 802.3.at-2009. In this case the maximum distance between the reader and the POE source is 100 m.

Note

If the given PC has an adequate PCI card with 20W PowerDelivery functionality and USB type-C slot, then the **Osmond N** device can be powered via USB regardless of the operation mode (USB or network).

3. Connect the **Ethernet cable** to the scanner and to the PC/router.
4. Turn the device on by covering the **power touch button** for 1-2 seconds.
5. After the button led turns **from red to green**, the device starts booting, which may take a few minutes. The status icon displayed on the OLED screen will indicate the current status of the process. For more information on it, see the OLED Display Status Icons chapter.

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

6. Access the **web interface** of the device (NWI mode):

   6.1. Start a browser and enter the following into the browser's address bar:

   a. If **DHCP and local DNS services** are available:

   `{hostname and port}`

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

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

   *Type the serial number without the very first character.

   b. **If the DHCP server is not available**, but the default gateway is set, the device is accessible on the **factory fallback IP address**:

   http://192.0.2.3:3000

   6.2. Log in to the web interface with the default user account:

   Login name: owner

   Password: Owner123*

7. The **default PR OCR** engine is **pre-installed** on the device, there are no other tasks to perform. However, in case of purchasing **VIZ OCR** or **VIZ AUTH OCR engine**, download the required VIZ OCR or VIZ AUTH OCR engine from the ADAPTIVE RECOGNITION website and perform the installation. For more information on it, see VIZ OCR and VIZ AUTH OCR Engine Management chapter.

8. The **default license** valid for the basic software functions is **pre-installed** on the device. In this case the license is up to date, thus there are no other tasks to perform. However, **license upload is required**, when:

   - Purchasing **VIZ OCR** or **VIZ AUTH OCR** engine,
   - Purchasing **Autofill** application,
   - Purchasing **license update**,
   - Purchasing other **additional software**,
   - The ordered software license was **supplied separately**.

   For more information on license upload, see License Management chapter.

9. **Operating the device**:

9.1. In **Network mode** according to application areas:

9.1.1. **For end-user**:

- Network Web Interface (NWI) **(default operation mode)**: Using the device with web browser

9.1.2. **For integration:**

- Network Web Application (NWA): Using the device in NWI mode managed by Open API Application
- Network Application Interface (NAI): Using the device with Passport Reader Network API

9.2. In **USB mode** according to application areas:

9.2.1. **For end-user, or testing the software setup:**

- Full Page Reader application (included in the PR Software Package)
- Authentication Checker application (included in the PR Software Package)

9.2.2. **For quick integration:**

- Autofill application (sold separately)

9.2.3. **For solution developer:**

- API
- Twain
- NAI

10. Check if the **setup was successful**:

In case of the default operation mode, **Network Web Interface (NWI)**, the steps are the following:

- **Connect** the device **to the PC** and the **Internet**. **Turn** the device **on**. The device is **ready for operation**, when the following icon appears on the OLED display:

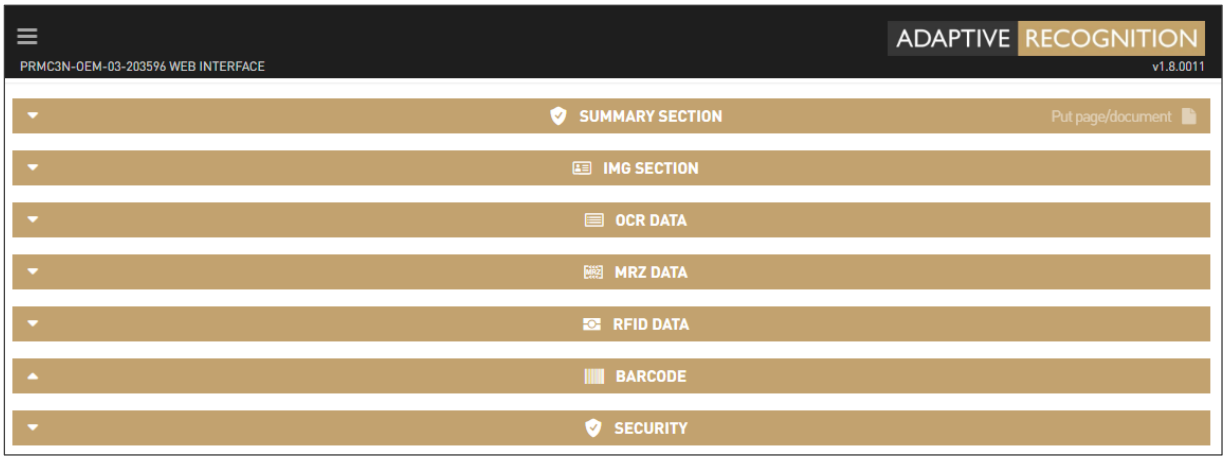
- **Start a browser** and **enter the following into the browser's address bar** in order to access the web interface:
  a. If **DHCP and local DNS services** are available:
     `{hostname and port}`
     `OSMOND-N{serial number* and port}`
     E.g., `http://OSMOND-N204203:3000`

     *Type the serial number without the very first character.

  b. If **DHCP is not available**, but the **default gateway is set**:
     192.0.2.3:3000

- If all information was entered correctly, the **following screen** should come up in your browser window:

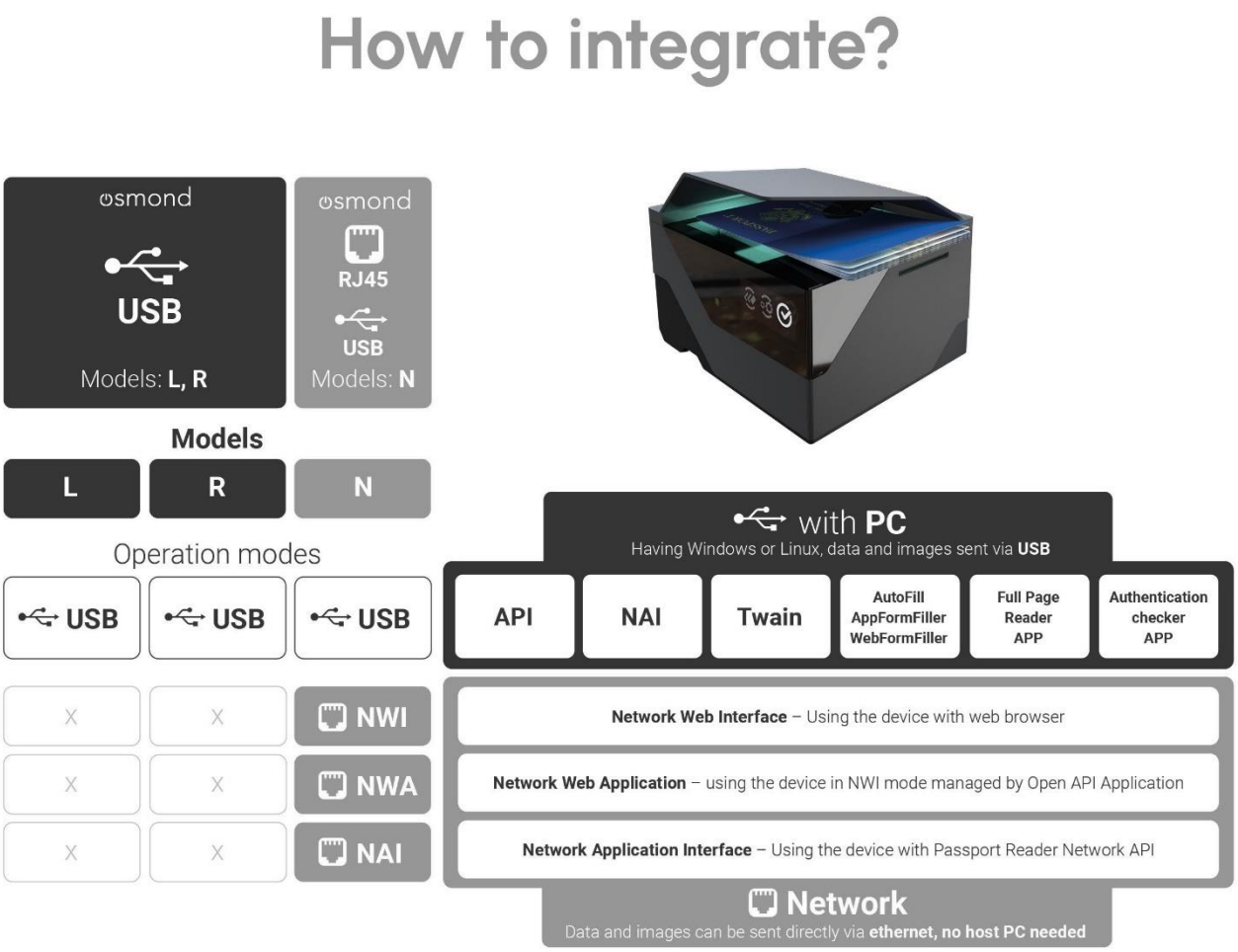
- **Log in** with the default user account.
- After signing in, the **START APP** menu (home page) will appear, where identity documents can be scanned:



- **Place a document on the scanning surface** of the reader. The device starts the scanning process automatically.
- After the scanning process is finished, the **extracted data can be examined** in the **START APP** menu of the web interface organized into different sections.

> Note
>
> For more information on **Osmond Network** device, see Osmond N (Network device) chapter.

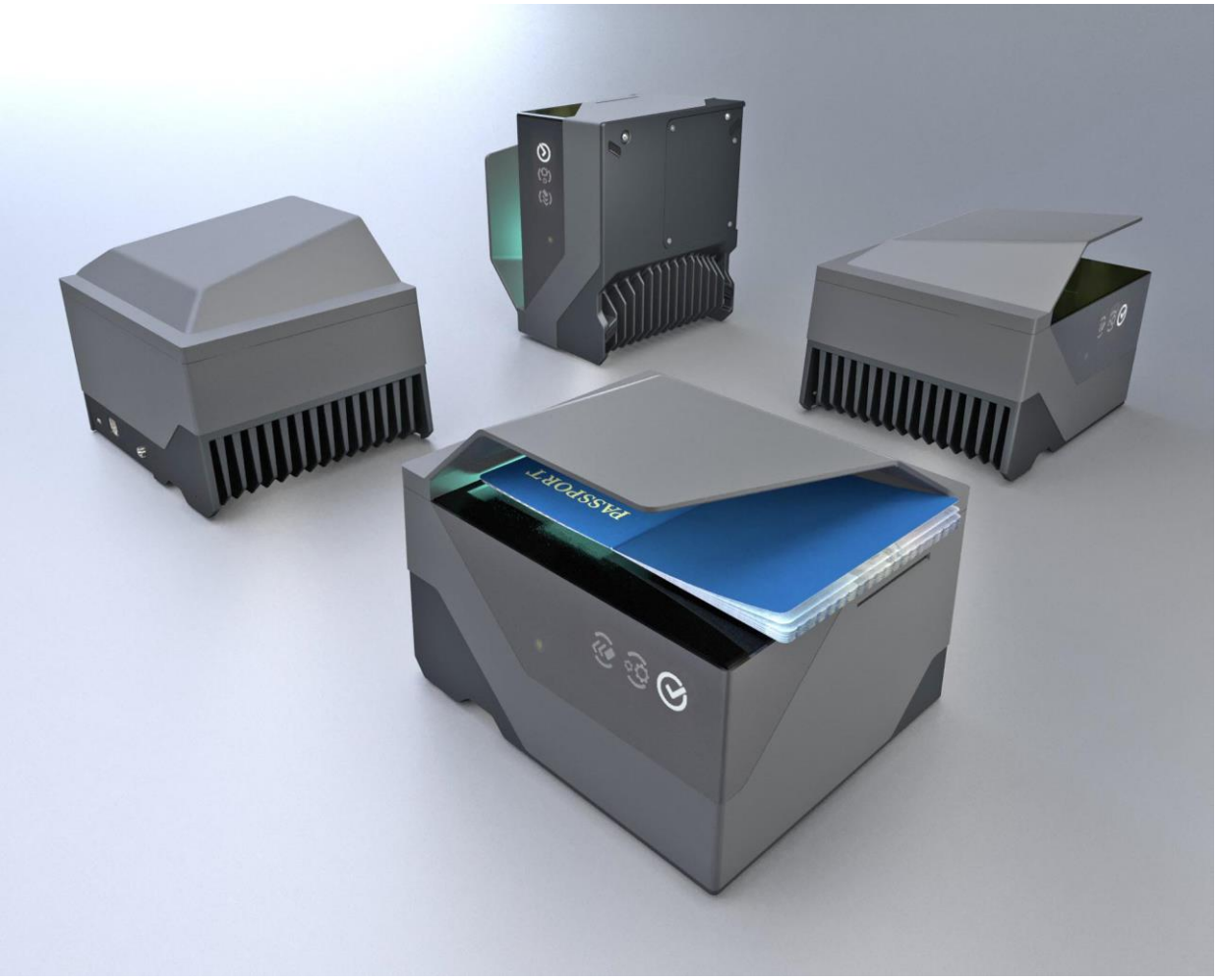
3. DEVICE INTEGRATION



II. INTRODUCTION

The Osmond is a full-page, multi-purpose passport and ID reader that provides automatic, accurate data extraction and verification with the ability to read multiple types of identity documents: **passports, e-passports, ID cards, visas** and **driver licenses**. The printed data is extracted from the entire page (MRZ, VIZ and 1D & 2D bar codes) while digital data is obtained from contactless (RFID) and contact smart chip (optional). The available multiple illumination sources are visible white, IR, UV, OVD and edge light. A special feature of the Osmond device (type N) is that it has a built-in OS (no other installation is needed) which runs a fully functional web server that is accessible virtually with any device once the reader is connected to a network. The recognized documents are processed by the device, no separate PC is needed to process the collected data. In addition, Osmond N model is able to operate in both USB and Network mode. You can easily switch between modes by using a small utility tool called PRDTool.

For more information on the technical specifications of the Osmond device, click on this link to access a comprehensive tech datasheet.

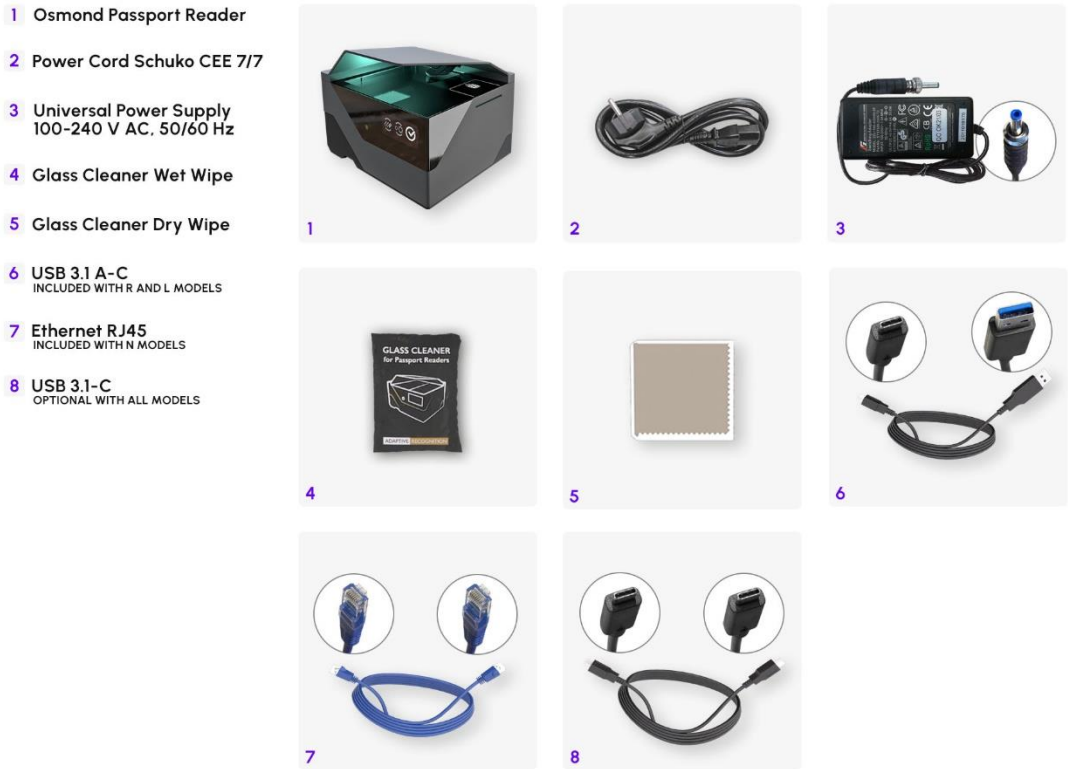


Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

III. DEVICE OVERVIEW

1. PACKAGE CONTENTS

	Passport Reader device	5V output power supply	Power cord (EU)	USB cable (USB3.0)	Ethernet cable	1 pc of glass cleaning wipe	Blind plug
Osmond L*	✓	✓	✓	✓	-	✓	✓
Osmond R**	✓	✓	✓	✓	-	✓	✓
Osmond N***	✓	✓	✓	-	✓	✓	✓



*Osmond L: USB base model with UV illumination

**Osmond R: USB device with UV illumination and built-in RFID module

***Osmond N: Network device with UV illumination, built-in RFID module and dual operational mode (USB and network mode)

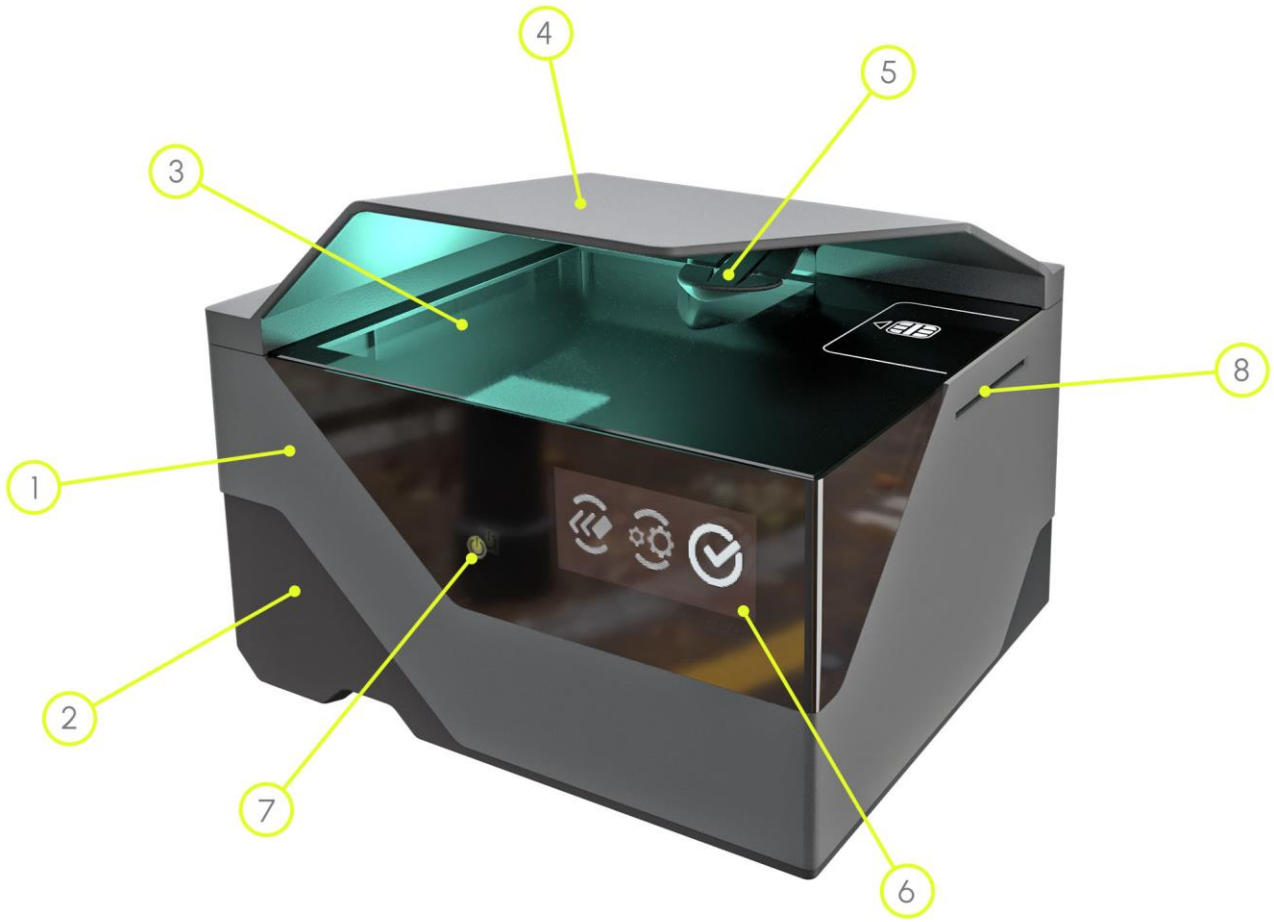
Note

For more information on the technical parameters and the comparison of the Osmond L, R and N models, click on this link.

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

2. PARTS AND COMPONENTS

The device is produced in a **plastic (ABS) housing** (**1**) and an **aluminum base plate** (**2**). The **object-plate** (**3**) is protected from the external light-striking by the **plastic (ABS) shield/cover** (**4**). The shield has a **document holder** (**5**) in order to facilitate the placing of the document. The **OLED display** (**6**), indicating the various phases of the device, and the **On/Off touch button** (**7**) are installed on the front of the body. Optionally, the device is equipped with a **smart card reader*** (**8**), located on the side of the device.

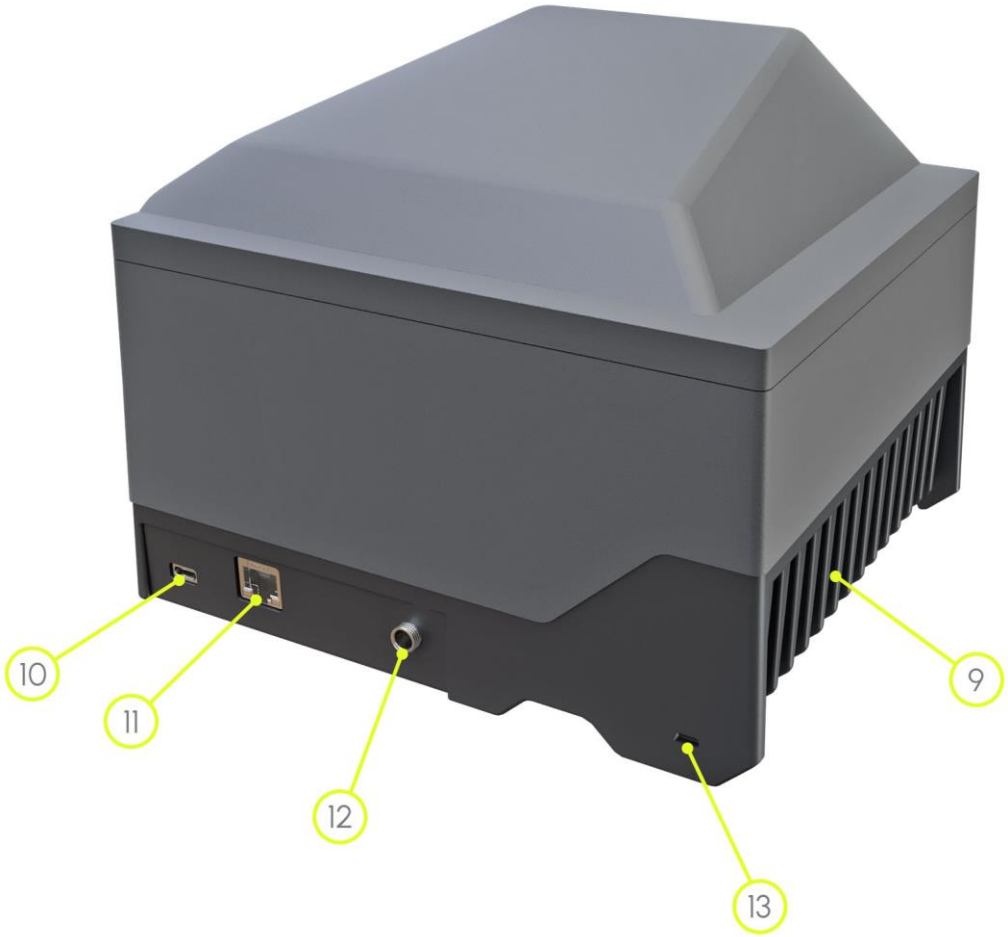


Note

*The smart card reading function is not available in network mode as for now.

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

The scanner is designed with an **aluminum heatsink** (**9**). The **USB socket** (**10**), the **Ethernet port*** (**11**), the **power supply socket** (**12**) and the **Kensington® security slot** (**13**) are located on the back of the device.

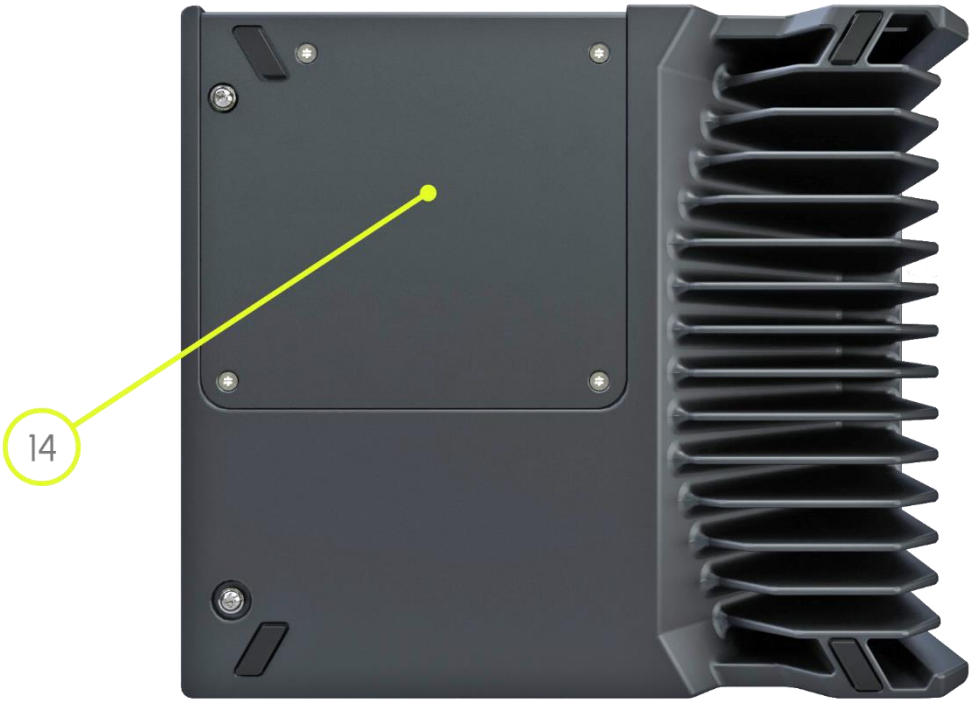


*Ethernet port is only available at **Osmond N** model.

Note

The Osmond device is designed with a removable document holder built in 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. In that case, this holder can be removed and replaced with the so called '**blind plug**'. For more information on how to perform the replacement, see Removing the Osmond Document Holder appendix.

The **cover plate for service functions** (**14**) is located at the bottom of the device.



Note

Service functions include the following operations:

- factory reset,
- auto power-up,
- buzz sound for power on.

Note

When placing the device on its side to access the cover plate, please look out for the aluminum heat sink.

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

IV. HARDWARE SETUP

In this section instructions and recommendations concerning the hardware integration are described, which are the following:

- The device should be on a stable surface, placed horizontally. Do not install the device to an unsteady place. The device has rubber footing, which ensure a solid grip.
- Do not throw or drop the device.
- Avoid bright, alternating lights, which can interfere with image capture. For example, do not illuminate the scanner surface with a lamp, especially when scanning ID-1 size documents.
- Avoid heavy dust in the ambience of the device. The devices are to be used indoors, in an office environment only (SOHO).
- It is recommended to maintain the device in certain intervals. Wipe the dust and grease off the glass with the wipes provided with the reader, see Maintenance appendix with its subchapters.
- The most efficient way to place the documents on the scanning surface is to put the ID in the left corner, and avoid placing the card at an angle close to 45 degrees. For more information, see Correct Document Placement chapter.
- You should avoid wearing rings and nail extensions. Avoid placing grainy documents on the surface of the reader. Pay attention to prevent getting grains of sand or other materials inside the device.

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

1. HARDWARE INSTALLATION

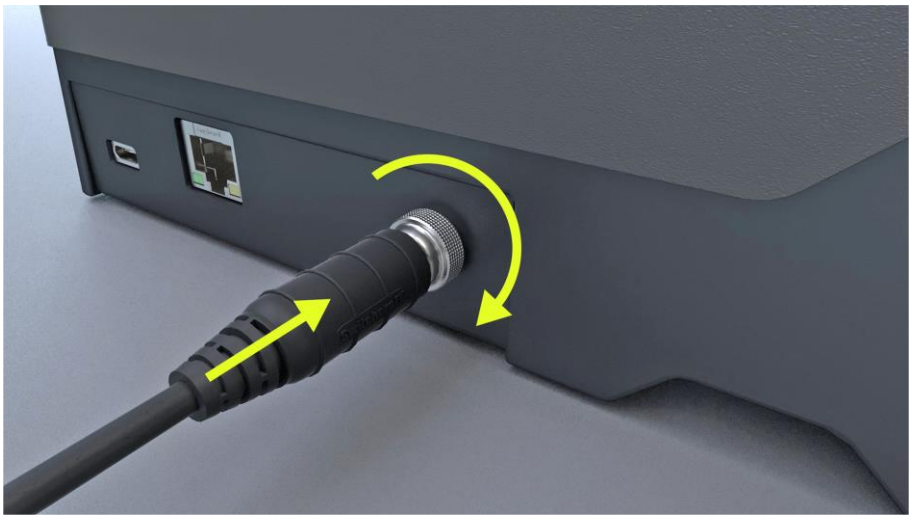
1.1. DEFAULT INSTALLATION

Follow the next steps to connect the Osmond USB (L, R) or network (N) device to the PC:

1. Connect the **power supply** to the unit.

Important!

Connect the power supply to the device by completely screwing on to the right the round, dotted part of the power supply closest to the housing.



Note

Only use the power supply that was shipped with the device.

Note

Regardless of the operation mode (USB or network), the **Osmond N** device can be powered via PoE+ switch or PoE+ injector with standard 802.3.at-2009. In this case the maximum distance between the reader and the POE source is 100 m.

Note

If the given PC has an adequate PCI card with PowerDelivery functionality and USB type-C slot, then the **Osmond N** device can be powered via USB regardless of the operation mode (USB or network).

2. Connect the reader to the PC or to your environment:

   - In case of **Osmond R and L (USB devices)**: Connect the device to one of the **USB 2.0 or 3.0 ports** of the PC with the supplied USB cable.

> **Note**
>
> It is strongly recommended to use the USB ports of the motherboard. When connecting the USB cable to the front panel USB port, use shielded cable between the motherboard and the USB panels.

   - In case of **Osmond N (network device)**: Connect the device directly to a computer or network switch with an **Ethernet cable**.

> **Note**
>
> For more information on connecting the device directly to the PC with an Ethernet cable, see Direct Ethernet Connection chapter.

3. Turn the device on by **covering the power touch button for 1-2 seconds** with your entire fingertip.

4. After the button led turns **from red to green**, the device starts booting. Please note that the boot sequence may take a few minutes. The status icon displayed on the OLED screen will indicate the current status of the process, see the OLED Display Status Icons chapter for more information on the icons and their descriptions.

> **Note**
>
> If the device is used with a laptop, please make sure that the output voltage of the USB ports is not less than 5V. For this reason, it is highly recommended that you use the laptop on AC power (with the power cord connected).

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

1.2. ADDITIONAL INSTALLATION

Note

The additional service functions (auto power-up and buzz sound) are only available on devices with specific serial number: **from serial number 1244012 Osmond V2**.
For more information on Osmond V2 device and its requirements, see Updated Software Requirements of the Osmond V2 chapter.

1.2.1. AUTO POWER-UP

Osmond R V2 devices can be switched to automatic start-up mode. There are jumpers below the service panel at the bottom. By changing the jumper settings, Osmond R V2 can be set to a mode in which it switches on automatically if it gets power. As a result, there is no need to push the power button. Thus, it can be integrated into KIOSKs where the power button is usually covered. If you need a version for KIOSK without the top cover, we offer a KIOSK version of Osmond.

Setting the auto power-up function:

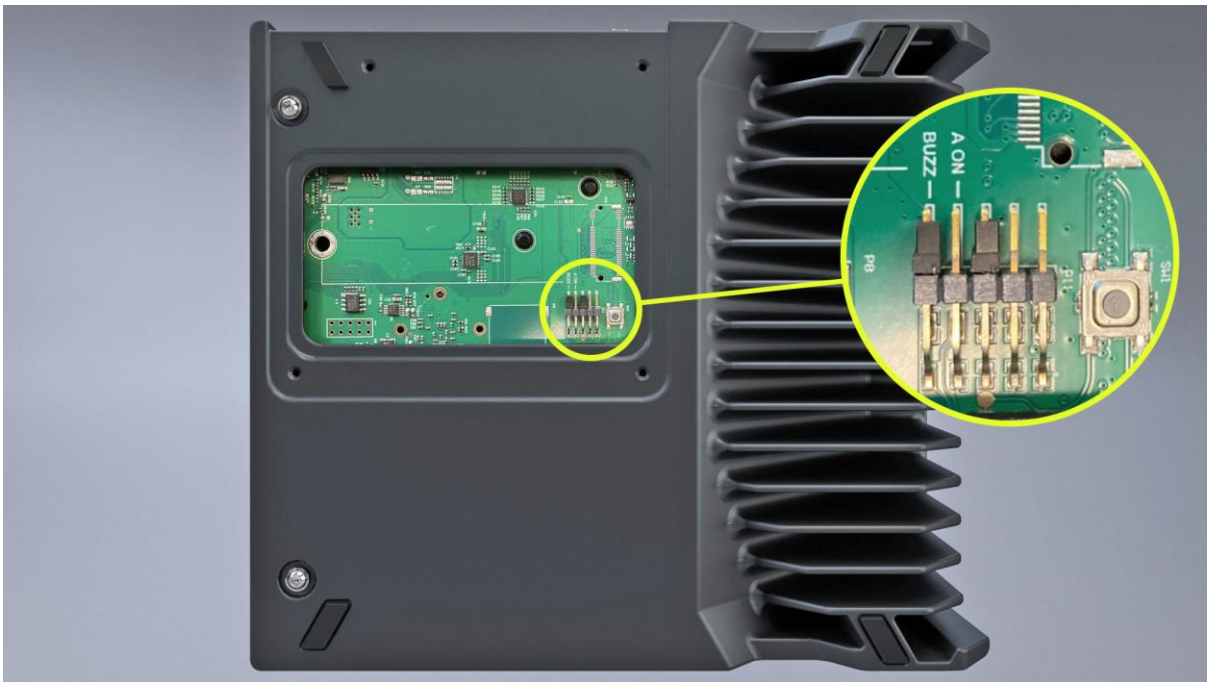
1. **Turn the reader off** with the On/Off touch button and **disconnect** the connected cables (power supply, USB cable).

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

2. Place the device on its side looking out for the aluminum heat sink and **unscrew** the 4 smaller screws in order to remove the service cover plate.

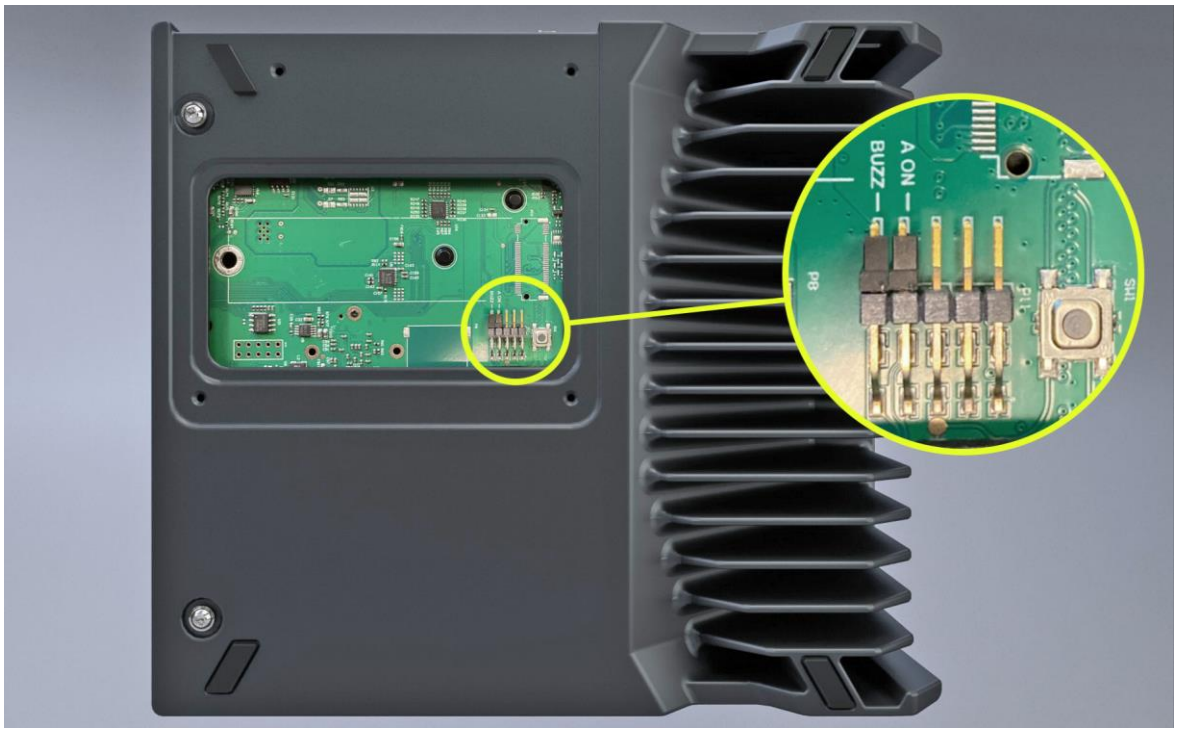
> **Note**
>
> Use an 8 TX screwdriver.

3. Search for the **jumper** pins located on the printed circuit board:



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

4. **Remove the black jumper** button from the third, center pin (empty pin). Then, **place it** to the pin with the "**A ON**" marking.



5. **Put the service panel back and retighten** the screws, being careful not to break the thread.

> **Note**
>
> Our recommendation is a tightening torque of 0.4 NM.

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

1.2.2. BUZZ SOUND FOR POWER ON

Osmond R V2 devices can be set to buzz when the device is connected to a power source. After being connected and waiting a few seconds, a buzzing sound can be heard. By default, this function is disabled. In order to enable it, follow the steps described below.

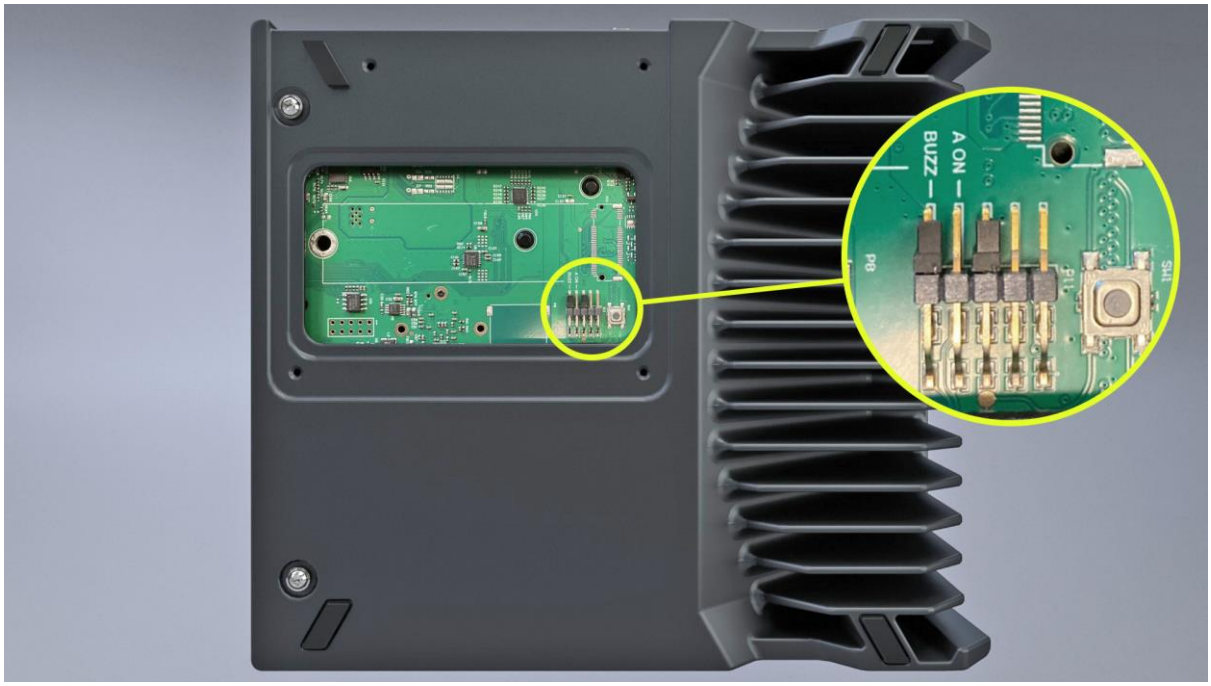
Setting the buzz sound function:

1. **Turn the reader off** with the On/Off touch button and **disconnect** the connected cables (power supply, USB cable).
2. Place the device on its side looking out for the aluminum heat sink and **unscrew** the 4 smaller screws in order to remove the service cover plate.

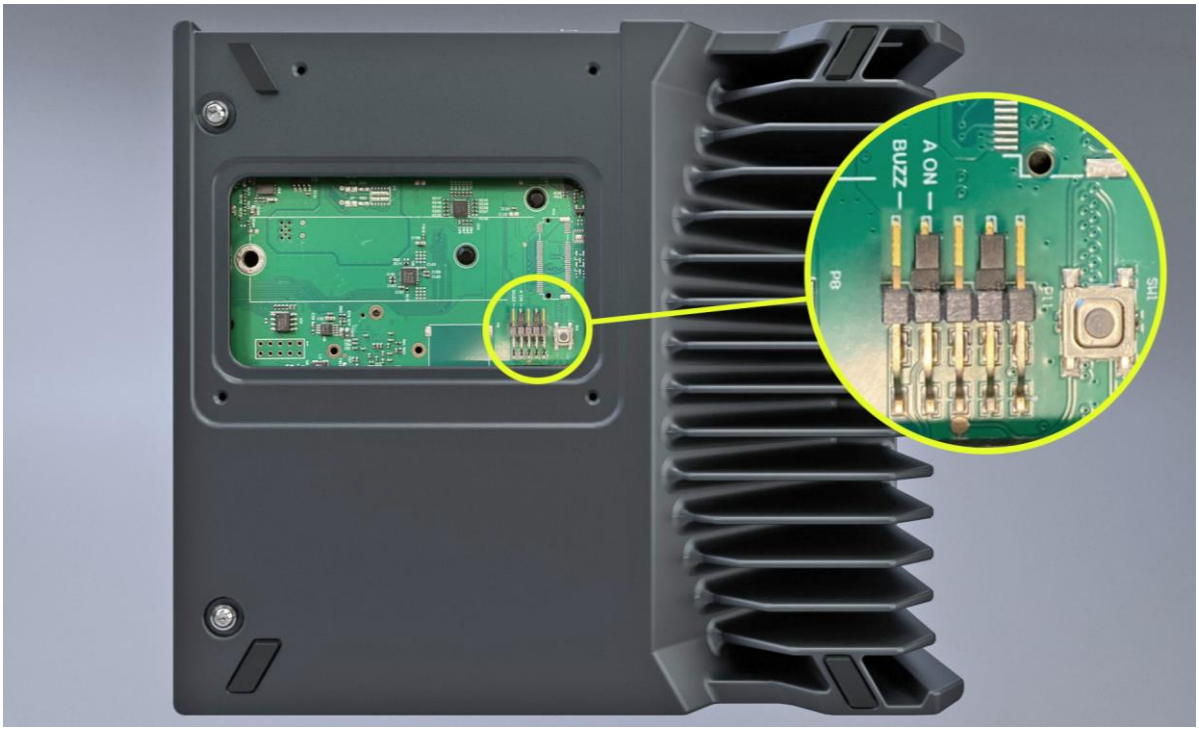
> Note
>
> Use an 8 TX screwdriver.

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

3. Search for the **jumper** pins located on the printed circuit board:



4. **Remove the black jumper** button from the first pin marked as "**BUZZ**". Then, **place it** to an empty pin without marking.



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

5. **Put the service panel back and retighten** the screws, being careful not to break the thread.

> **Note**
>
> Our recommendation is a tightening torque of 0.4 NM.

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

V. SAFETY

Important!

Equipment modifications:

This equipment must be installed and used according with the instructions given in its documentation. This equipment contains no serviceable components. Unauthorized equipment changes or modifications cause warranty to void.

Important!

Only operate the device with the power supply it was shipped with.

Important!

The device should not be operated with its object-plate exposed to direct sunlight.

Important!

Do not look directly into the UV-A and INFRA lights during scanning process. They may cause damage to the eye.

Important!

Do not use abrasive cleaners or solvents when cleaning the device. These may scratch the glass or damage the plastic.

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

VI. OSMOND R AND L (USB DEVICES)

Osmond R and L models are USB devices that operate as any other ADAPTIVE RECOGNITION passport reader. They can be used with the Full Page Reader or Authentication Checker application as well as our SDK.

> Note
>
> For more information on the Full Page Reader or Authentication Checker application, see the Full Page Reader Application or the Authentication Checker Application chapters.

1. SYSTEM REQUIREMENTS

Recommended minimum system requirements:

- Intel Pentium 2 GHz CPU or higher (or equivalent x86 compatible CPU),
- 1 GB RAM or more (depending on application),
- 32 or 64-bit Microsoft Windows 7/8.1/10/11/Vista operating system or Linux operating system (kernel version 3.2),
- Integrated USB 2.0 port (on motherboard).

> Note
>
> The speed of image processing highly depends on the type of hardware used. In general, the shorter recognition time is needed, the more powerful machine you are advised to use.

> Note
>
> In case of an **authentication engine**, the recommended system requirements are the following:
>
> - 64-bit system,
> - 4+ GB RAM.

> Note
>
> In case of purchasing **VIZ OCR engine**, it is strongly recommended to use 64-bit operating systems.

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

1.1. UPDATED SOFTWARE REQUIREMENTS OF THE OSMOND V2

The new generation of Osmond (**V2**) device is manufactured from August 2024 starting with serial number 1244012. It requires the **Passport Reader Software Package 2.1.11.3.o3** or higher version. Earlier software versions are not supported.

The **Passport Reader Software Package 2.1.11.3.o3** includes the following:

- The SDK and API is the same as in earlier versions.
- All applications written for earlier Osmond models will work, but this new package has updated drivers that are required for the hardware of the Osmond V2.
- **Windows 10 and 11** operating systems are fully supported.

Limitations if using Osmond R V2 on Windows 7/8 (legacy drivers):

- PC/SC interface for RFID and contact chip is not available on Windows 7/8 systems.
- 3rd party RFID / contact chip / smartcard software that would use PC/SC to control directly our RFID or contact chip hardware will not work on Windows 7/8 systems.

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

2. SOFTWARE INSTALLATION

Due to the fact that Osmond USB devices operate similar to any other ADAPTIVE RECOGNITION passport reader in order to use it, the ADAPTIVE RECOGNITION driver package is necessary. For Osmond devices, the Passport Reader software package **2.1.10.2 or higher version** is required.

The Passport Reader software package is available in the following ways:

- Check the automatic notification email which was sent on the day of the dispatch and use the link to download the latest passport reader software.
- Alternatively, check our portal (https://adaptiverecognition.com/doc/id-scanners-readers/passport-reader-software/#software/) to access our software modules.

The Passport Reader Software Package includes the following components:

- Drivers for Passport Reader devices and AFS510 Fingerprint Scanner devices
- Software Development Kit for C/C++, Visual Basic, Delphi, C#, VB.NET and Java programming languages:
  - Interface files
  - Sample programs
  - Manual in HTML and CHM format
- Full Page Reader Application
- Authentication Checker Application
- Passport Reader utility programs (License Manager, PRDTool)
- NetAPI SDK (from PR Software Package 2.1.11.1)

Note

Silent installation can also be performed. There is an example below, the actual command may differ.

For example:

```
msiexec.exe /i pr-2.1.11.2-x64.msi /qn
ADDLOCAL="certificates,gxsddriver,drivers,prddriver,fxmcusbdriver,
omnikeydriver,arhftdidriver,gx,pr,fullpagereader,apps,authchecker,
pcsc,tools,fpsdemo,license_tools,ocr,prdt,prwebsrv,qtgx,VCRedist8,
VCRedist8Policyx64,VCRedist10,VCRedist14"
```


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

2.1. INSTALLATION ON WINDOWS OPERATING SYSTEMS

Important!

Administrator rights are needed for installation.

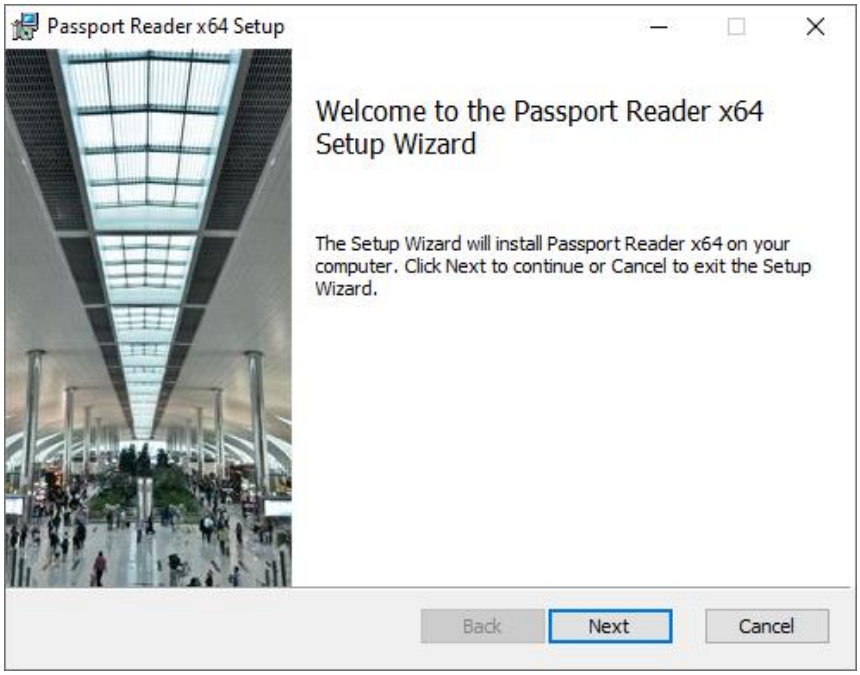
Important!

Upon installation of the 32-bit version to a 64-bit PC, the 64-bit device drivers are installed automatically. For 32-bit application development on 64-bit PCs, install the 32-bit version of the Passport Reader software as well.

1. Before installing the Passport Reader software, all previous versions of the software must be uninstalled from the system. This process differs depending on the version that is currently installed on the system.
   - For versions 2.1.5-26W or earlier, go to **Start Menu / Programs / GX / UNINSTALL** and run **– FULL UNINSTALL –** as well as **Start menu / Programs / GX / 32 bit version / – FULL UNINSTALL –** if applicable.
   - For versions 2.1.6 or later, go to **Control Panel / Add/Remove Programs** and remove all versions of the Passport Reader software.
2. Once all previous versions of the software have been uninstalled, restart the computer.
3. Next, locate the downloaded software package and run **pr-2.1.x-x86.msi** (in case of 32-bit operating systems) or **pr-2.1.x-x64.msi** (in case of 64-bit operating systems).

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

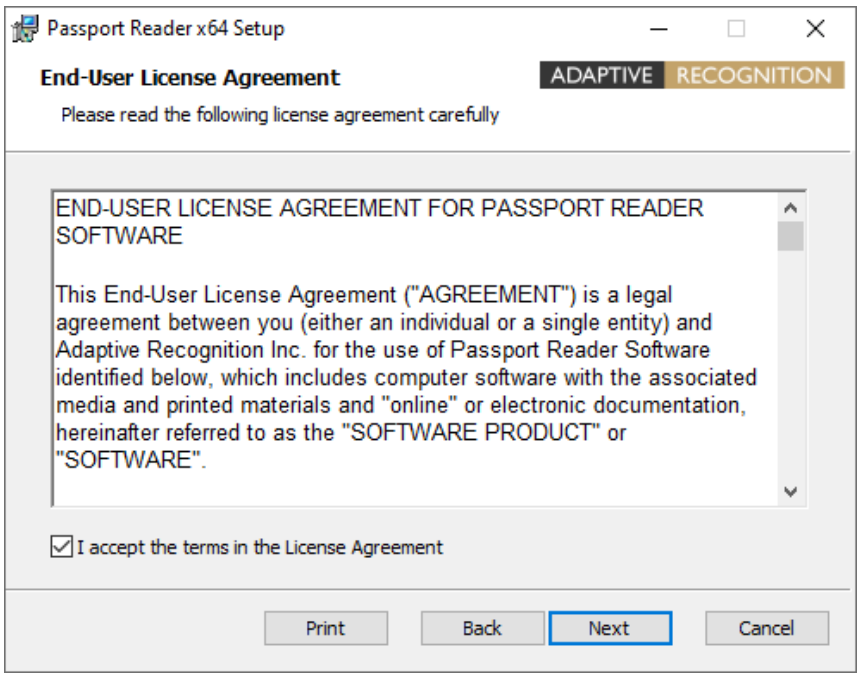
4. The installation starts with the following window:



Welcome Page of Passport Reader x64 setup

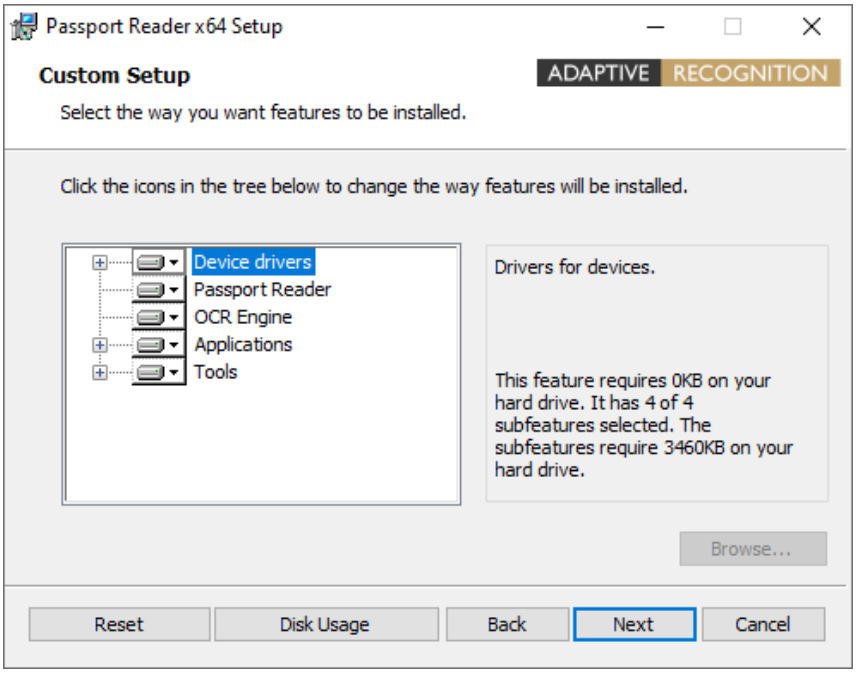
5. Click **[Next]** to launch installation.

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



End-User License Agreement (EULA)

7. In the **Custom Setup** window, select the modules you wish to install on the PC.
   Installing the **Device Drivers** and the **Passport Reader** modules are necessary for device operation, the installation of all other modules is optional.

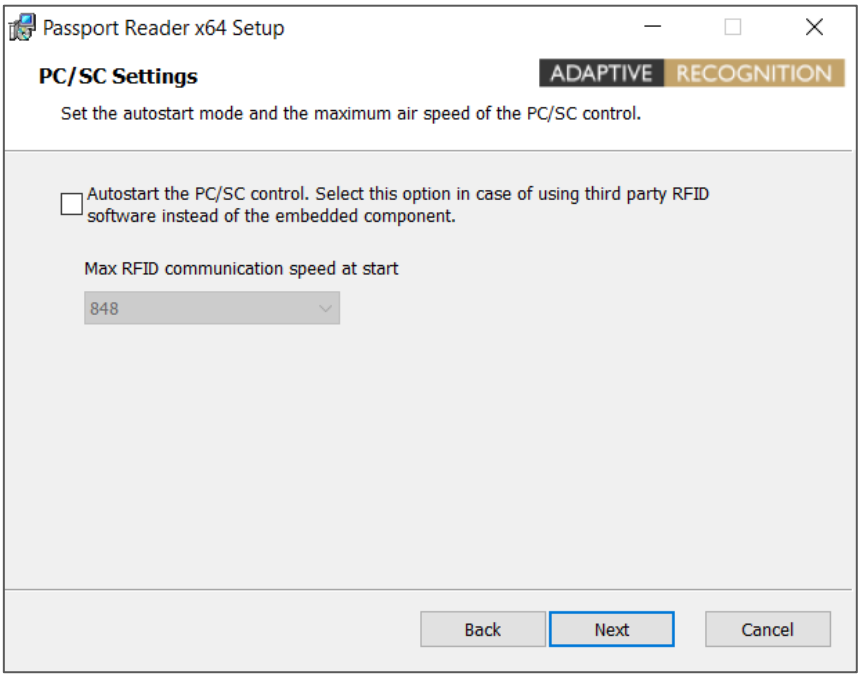


Custom Setup

Note

SDK and Documentation are available in the "sdk" folder of the PR Software Package.

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

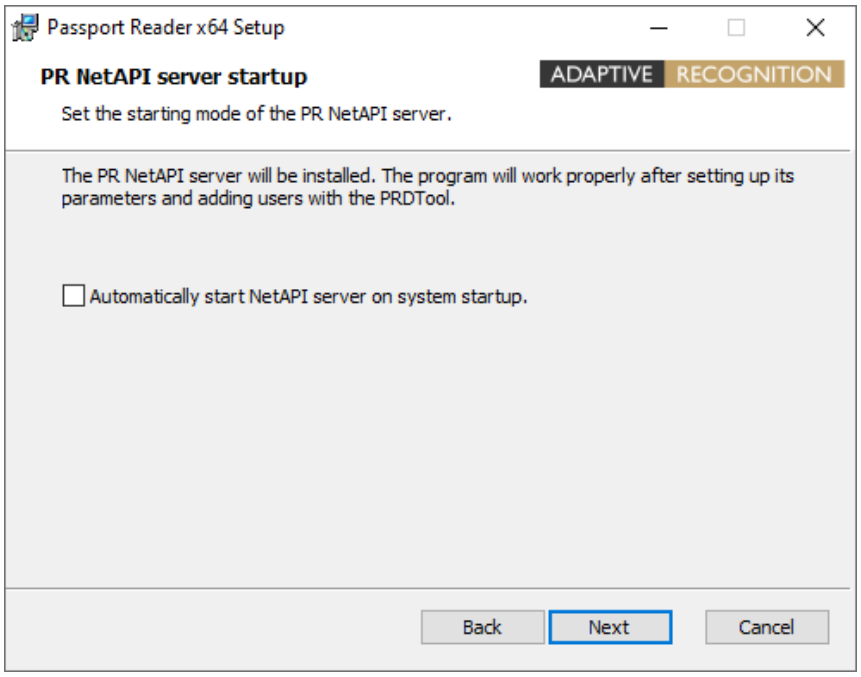


PCSC Settings

Important!

Please select the **Autostart** option only if you intend to use your document reader device via the PC/SC interface. This setting can also be modified after the installation is finished. For more information, please see the PC/SC section.

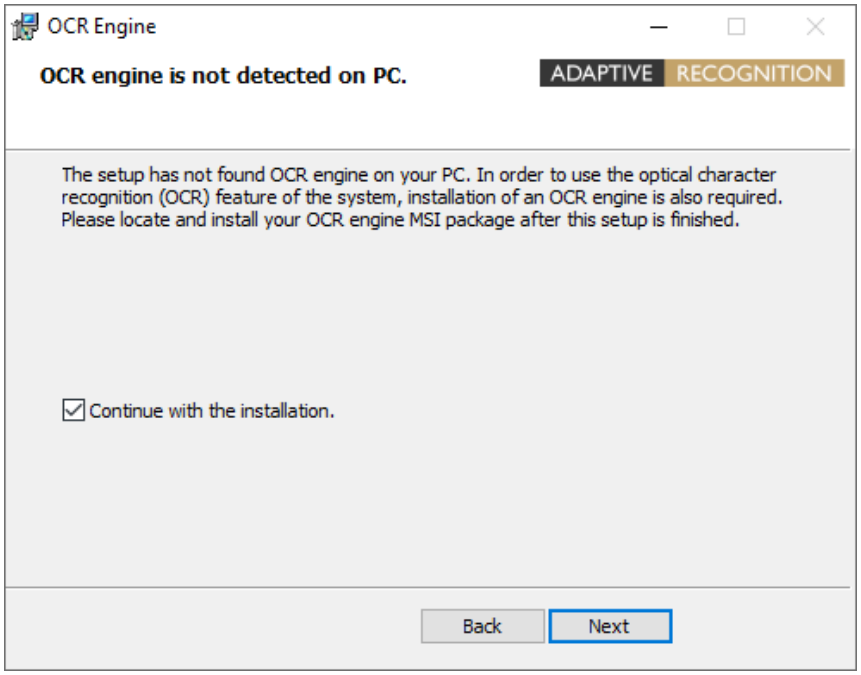
Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM



Important!

Please select the **Automatically start NetAPI server on system startup** option only if you intend to use your document reader device in NAI mode. In this mode the device is used with the Passport Reader Network API. This setting can also be modified after the installation is finished. For more information, please see the NetAPI (NAI mode) section.

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



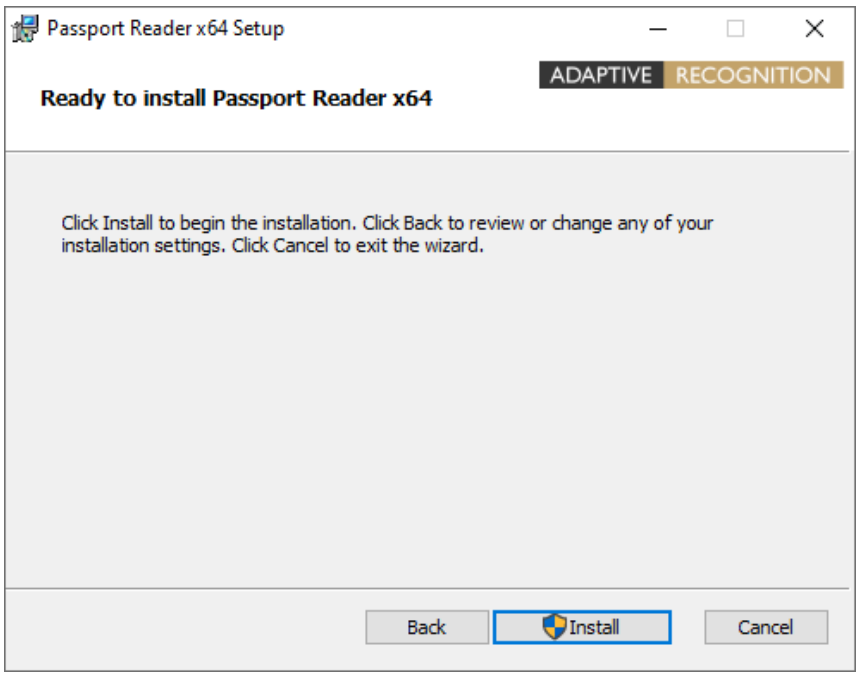
Important!

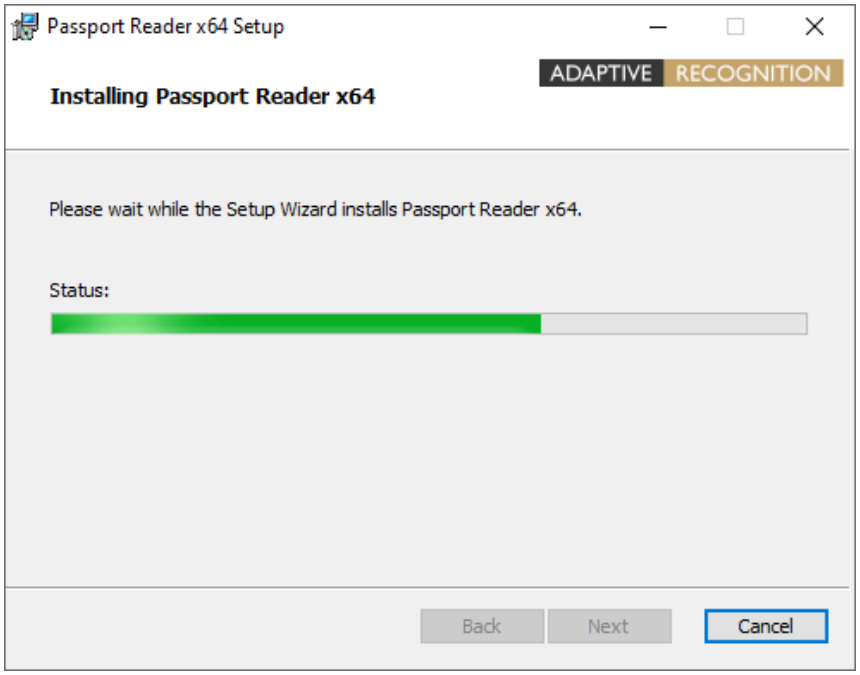
If the PR Software Package version is **below 2.1.11**, then in order to use the OCR functionality of your document reader device, please also install the **procr-2.0.x.xx.msi** package located in the **win** folder of the Passport Reader install package, after current installation is finished.

In the case of **version 2.1.11**, the OCR engine is embedded to the Passport Reader Software MSI. Therefore, when performing the software installation, the OCR engine is also installed.

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

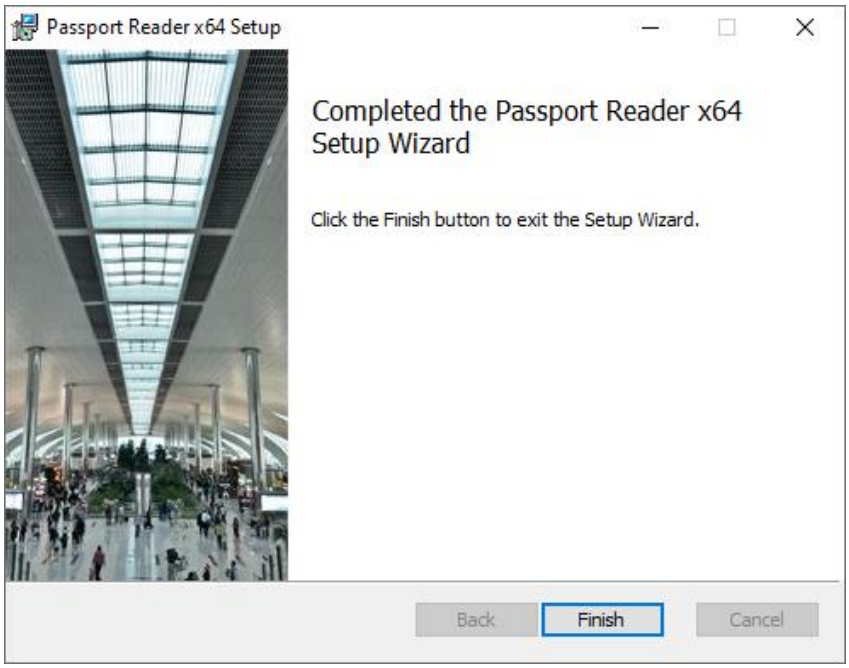
8. Clicking on **[Install]** will begin installation.



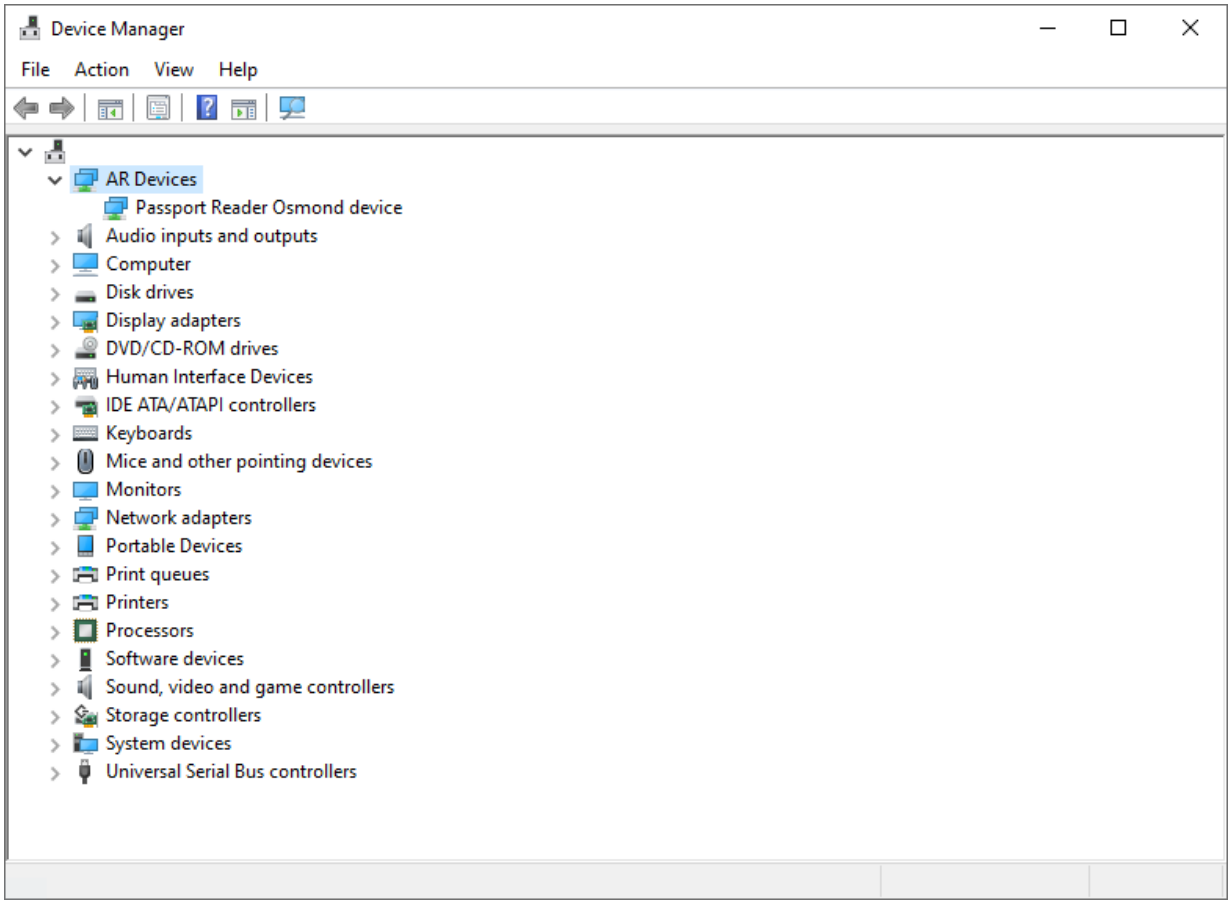


Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

9. Click **[Finish]** to complete the installation.



10. After the installation has finished, open the **Device Manager**. If the installation was successful, a group named **AR Devices** together with **Passport Reader Osmond device** (Osmond models) should be listed.



2.2. INSTALLATION ON LINUX OPERATING SYSTEM

Note

Please read through this manual carefully!

The Passport Reader is a travel document reader and analyzer system by AdaptiveRecognition Inc., which bases on the GX system and provides for software developers an easy-to-program interface through its Application Programming Interface.

2.2.1. BEFORE YOU INSTALL THE PACKAGES

The system was built under Ubuntu 20.04 and has been tested on:

- Ubuntu 22.04 LTS
- Ubuntu 20.04 LTS
- Fedora 36
- Debian 8

Note

Please read the license agreement before installing the packages.

For the installation you need "GNU Make", "GNU C/C++" compiler and the corresponding GLIBC. The kernel headers and configuration files must be installed as well.

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

2.2.2. CONTENTS OF THE INSTALL PACKAGE

GX

`gx-7.2.x-x.tar.gz`	GX system

Passport Reader

`pr-2.1.x-x.tar.gz`	Passport Reader system
`prd-2.1.x-x.tar.gz`	PRDDRV driver for Passport Reader devices
`procr-2.x.x-x.tar.gz`	OCR engine
`fxmcusb-7.x.x-x.tar.gz`	USB Neural Network Controller devices
`licutils-7.x.x-x.tar.gz`	License Manager
`pr-fullpagereader-2.x.x-x.tar.gz`	Full Page Reader application
`pr-authenticationchecker-2.x.x-x.tar.gz`	Authentication Checker application
`pr-certificates-x.tar.gz`	German master list certificate collection
`pr-udev-2.x.x-x.tar.gz`	Scripts and udev rules for automatic driver loading

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

2.2.3. THE INSTALLATION PROCEDURE

1. Unpack and copy all files into your system:

- use `_install.sh`

Dependencies:

Please install the following libraries with your distribution package manager or manually (these libraries are apart from services):

- SDL (A library for portable low-level access to a video framebuffer, audio output, mouse, and keyboard)
- SDL ttf (A library that enables using TrueType fonts in your SDL applications)
- SDL net
- SDL gfx (`libSDL-gfx1.2-4` if the `libSDL1.2-5` is available only then make a symbolic link in the `/usr/lib/x86_64-linux-gnu` folder with the following command `ln -s libSDL_gfx.so.15 libSDL_gfx.so.13`)
- SDL image
- FreeType (TrueType font rendering library)
- libpcsclite1
- pcscd
- Qt

GX: none

Passport Reader: GX

2. **Compile kernel modules:**

   - Download a kernel source from https://github.com/torvalds/linux and unpack into `/usr/src` directory.

     If you have an older GX version in the kernel tree, please remove it manually by using the script `_uninstall.sh`.

     You can use the kernel source package of your distribution (e.g., Ubuntu 10.04 → linux-kernel-headers).

   - Or make sure that the kernel config files are installed.
     Check the `/lib/modules/$(KERNEL_VERSION)/build` directory.

   - Compile the AdaptiveRecognition Inc. drivers:
     Compile the drivers with "make" command in the following order:
     - `/usr/src/gx/kernel/gxsd`
     - `/usr/src/gx/kernel/prddrv`
     - `/usr/src/gx/kernel/fxmc_usb`

     Note

     If you get a "No rule to make target..." error message by typing "make":
     If the output of "uname -i" is "unknown" and your system is either i386 or x86_64:
     Make a symbolic link to e.g., `b_prddrv.o` by typing:

     ```
     ln -s b_prddrv.o.x86_64 b_prddrv.o
     ```

     according to your system.

3. **Install new kernel modules:**

   For **PRDDRV**:

   ```
   /sbin/insmod /usr/src/gx/kernel/gxsd/gxsd.ko
   /sbin/insmod /usr/src/gx/kernel/prddrv/prddrv.ko
   ```

4. **Automatic driver loading is enabled by the pr-udev module.**

   This module enables the automatic installation of the driver modules upon connecting the reader to the PC. As a result, there is no need to start the driver manually.

   Note

   If this feature is unnecessary, then the user should remove the `98-ar.rules` from the `/etc/udev/rules.d` directory.

2.2.4. AFTER INSTALLATION

Once installation is complete, you can find the manual for the GX and PR systems under `/usr/share/doc/gx`. The header files can be found in the SDK, the library files in `/usr/lib64/gx`.

The basic GX library is in `/usr/lib64 (libgxsd.so.7)`. The file containing the property data is `/var/gx/gxsd.dat`.

After the kernel modules were started, you can check the state of the running drivers under `/proc/gx`.

2.2.5. INSTALLATION OF ANOTHER ENGINE

The engine comes in a `.tar.gz` file. Type the following command to start the installation:

```
tar xvfz engine.tar.gz -C /
```

2.2.6. UNINSTALLATION

If you want to uninstall the AdaptiveRecognition Inc. files simply type:

```
_unistall.sh.
```


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

3. READER CONFIGURATION

The Passport Reader device can be configured by those programs that are installed with the Passport Reader Software Package. These programs are the **PRDTool** and the **License Manager** utility programs.

PRDTool is part of the Passport Reader software packages from **version 2.1.9.1 and above**. This program is for querying device information and performing some low-level operations for Passport Reader USB devices, especially for the Osmond device.

License Manager is a license handling application which is designed to upload ADAPTIVE RECOGNITION passport reader license files to a specific document reader device. The application is installed with the Passport Reader software packages from **version 2.1.7. and above**.

For more information and detail on the PRDTool program or the Passport Reader licenses and license handling, see PRDTool or License Management appendices.

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

4. AUTHENTICATION CHECKER APPLICATION

ADAPTIVE RECOGNITION provides its Authentication Checker application included in the 2.1.9 and above Passport Reader (PR) software packages.
This software offers full-spectrum ID document authentication with a range of security checks and visualization features. After each scanning, the software informs the user about the authenticity of the scanned document in a comprehensive way, with 4 views on one display.
The app works with fixed values to facilitate its use.

It provides:

- images scanned by different illumination sources (white, infra, UV)
- OCR mode to reach MRZ and VIZ data
- optical and RFID authentications as well as comparison of their results

The main emphasis is on the authentications to maximize the result of the examination.

This chapter is going to show you the functions of the app and the methods of the use.
The structure of this section is the following:

- First, the app overview and its accessing will be discussed.
- Next, a closer look will be taken at the Dashboard of the application.
- Finally, the user will be guided through the Sections of the application.

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

4.1. REQUIREMENTS

- An ADAPTIVE RECOGNITION scanner connected to your PC
- ADAPTIVE RECOGNITION Passport Reader Software version 2.1.10.2 or later
- PC: min. 2GB RAM, full HD display resolution (1920 x 1080)
- OS: 32/64-bit Windows 7/8/8.1/10/11 or Linux

Note

To make the most of the ADAPTIVE RECOGNITION document reader device and the application, it is recommended to use the VIZ AUTH engine on 64-bit operating systems.

4.2. START AUTHENTICATION CHECKER

Windows

After installing ADAPTIVE RECOGNITION software package on your computer, you will be able to open Authentication Checker from **Windows Start menu > Adaptive Recognition > (Passport Reader) > Authentication Checker x86** or **x64** (based on your computer architecture and previous installation).

Linux

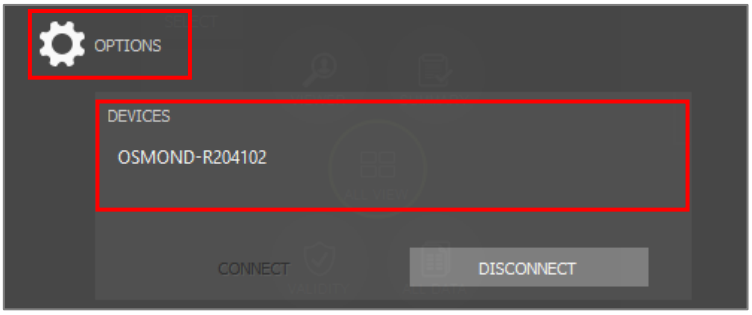
Depending on your distribution, you can open command terminal and insert: **AuthenticationChecker** or use dashboard search bar: **Linux Start menu > Applications > Adaptive Recognition Apps > Authentication Checker 64-bit version** (based on your computer architecture and previous installation).

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

4.3. CONNECTION

In order to scan with any ADAPTIVE RECOGNITION reader device, you have to make sure that there is an available reader connected to your computer and it is turned on.

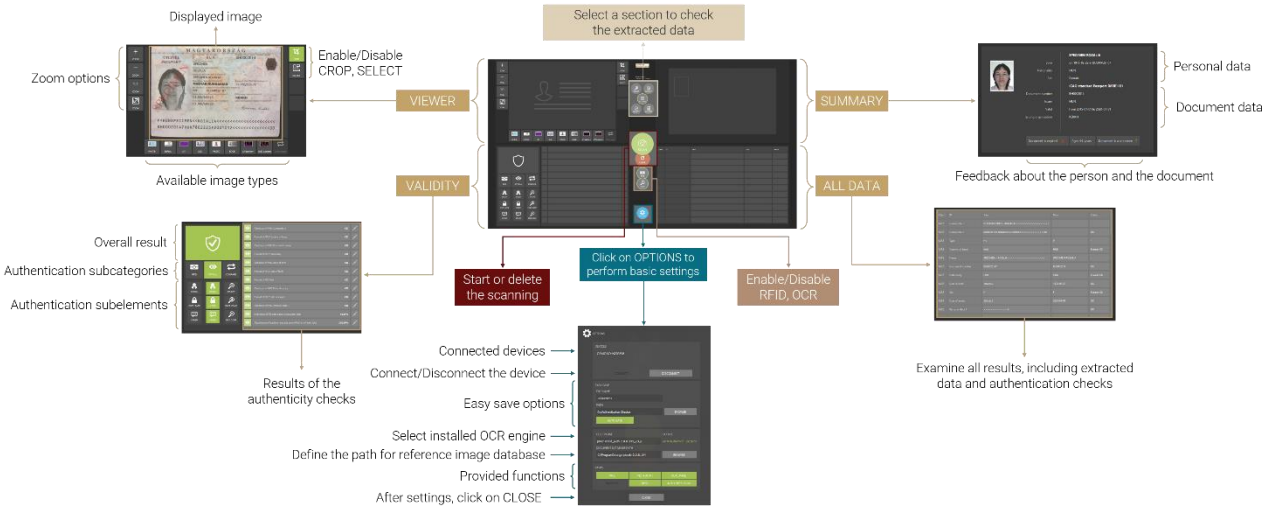
You can check the **DEVICES** list in the **OPTIONS** menu.



> **Note**
>
> By default, the app is connecting automatically to the document reader.

> **Note**
>
> If the device is connected properly, the **SCAN** button turns green. If the connection is unsuccessful, the **SCAN** button remains grey.

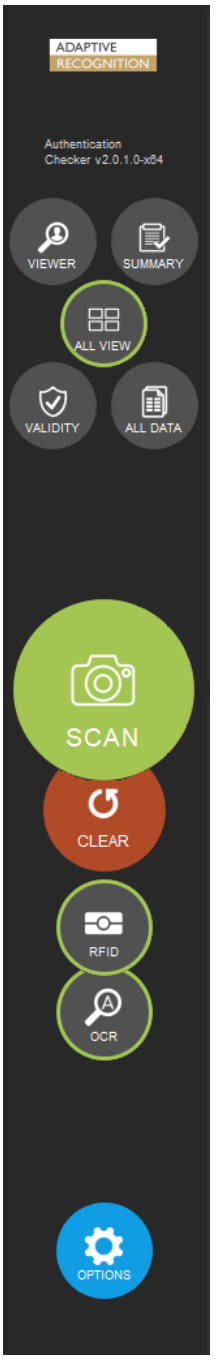
4.4. OVERVIEW



4.5. DASHBOARD

You can direct the operation of the program, change views, start or delete a scanning as well as perform some basic settings.

> **Note**
>
> In **ALL VIEW** mode the Dashboard is located in the middle of the opened window, while in the selected view (**VIEWER**, **VALIDITY**, **SUMMARY**, **ALL DATA**) on the right side of the window.



ALL VIEW

Use the **ALL VIEW** button to check all results (**VIEWER**, **VALIDITY**, **SUMMARY**, **ALL DATA**) on one display.

VIEWER

Select **VIEWER** to examine the scanned images under several illuminations on full screen.

VALIDITY

Select **VALIDITY** to view the results of the authenticity checks, including optical checks, digital data verification and comparison checks on full screen.

SUMMARY

Select **SUMMARY** to look at the selection of the extracted personal and document data on full screen.

ALL DATA

Select **ALL DATA** to examine all results, including extracted data and authentication checks on full screen.

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

SCAN

Click on the **[SCAN]** button to start the scanning process, if the **AUTO DETECTION** mode is not selected. The status signal around the **SCAN** button indicates the progression of the scanning process.

> Note
>
> **AUTO DETECTION** mode is switched on by default, thereby the scanning will start automatically.

CLEAR

Use the **[CLEAR]** button to delete the extracted data of the previously scanned document.

RFID

Click on the **[RFID]** button to enable/disable RFID reading.

> Note
>
> The green outline around the button indicates that the function is turned on.

> Note
>
> The MRZ reading is part of the OCR, but since it is needed for RFID reading in the most cases of the documents, the **RFID** and **OCR** buttons impact the enabling of MRZ reading. To turn on/off MRZ reading separately, click on **OPTIONS** and enable/disable **MRZ** by clicking on it at the **TASKS**.

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

OCR

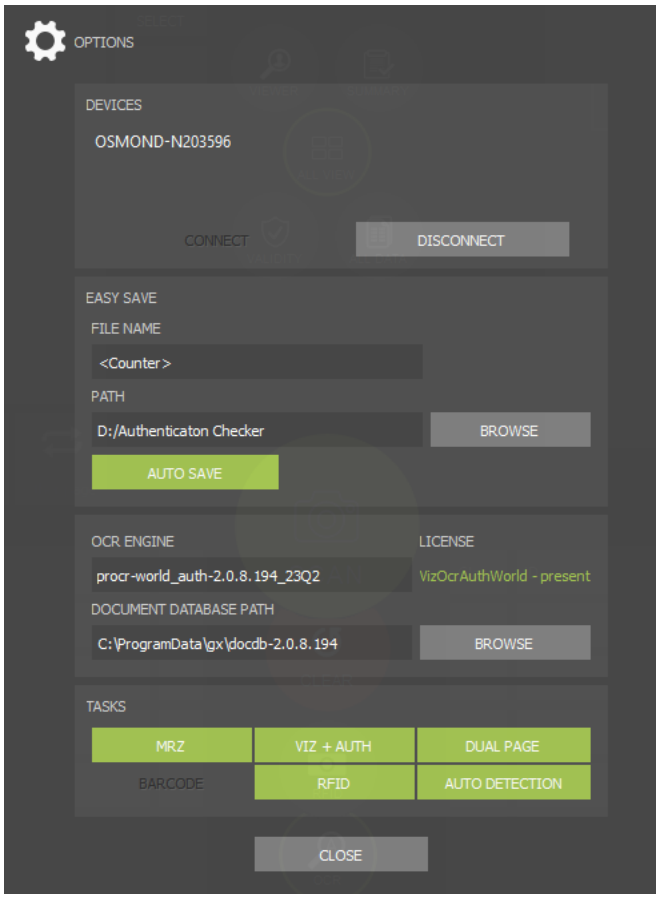
Click on the **[OCR]** button to enable/disable optical character recognition.

> **Note**
>
> The green outline around the button indicates that the function is turned on.

> **Note**
>
> The MRZ reading is part of the OCR, but since it is needed for RFID reading in the most cases of the documents, the **RFID** and **OCR** buttons impact the enabling of MRZ reading. To turn on/off MRZ reading separately, click on **OPTIONS** and enable/disable **MRZ** by clicking on it at the **TASKS**.

OPTIONS

Click on the **[OPTIONS]** button to perform some fundamental settings, customize the scanning process.



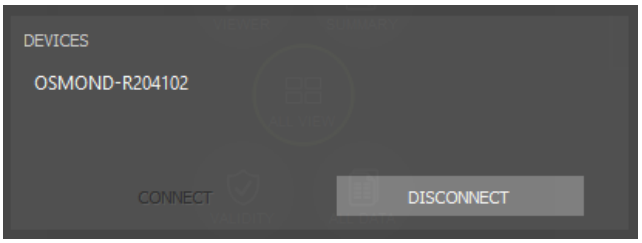
4.5.1. OPTIONS

1. DEVICES

You can see the list of the document scanners connected to your computer.

> **Note**
>
> By opening the app, the device is connected automatically.

> **Note**
>
> You can work with only one device at a time.



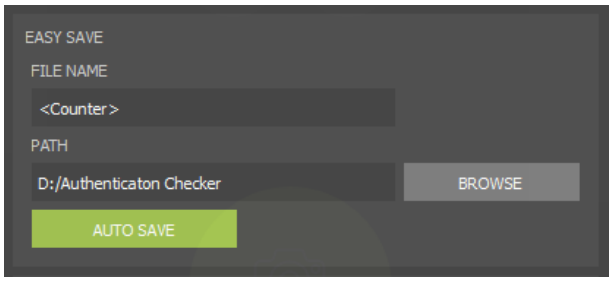
2. EASY SAVE

The **EASY SAVE** can make frequent document saving simpler. Turn **AUTOSAVE** on and set the **FILE NAME** and **PATH** to save the results of all scanning process automatically. After that, the software creates the filename automatically based on the configured template, then saves the .zip to the path specified.

> **Note**
>
> When using **EASY SAVE**, determine the filename syntax and path before first scanning. This option will save every scanning into the same path.

> **Important!**
>
> If the **AUTOSAVE** is not turned on, the saving process is skipped.

> **Note**
>
> If you want to save encrypted files which can only be decoded in ADAPTIVE RECOGNITION's network, then, when saving the file select **.ecz** extension.
> For more information on encrypted autosave, see the Encrypted Autosave in Authentication Checker chapter.



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

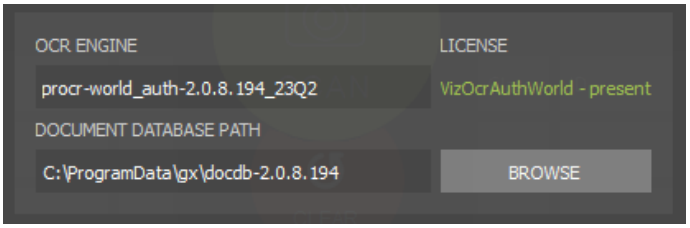
3. OCR ENGINE

The optical character recognition process of each document is performed by the **OCR ENGINE**. Select between **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 required engine-license and its availability.

The **DOCUMENT DATABASE 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 the authenticated document sections with images stored in a reference database. If the document database is not set or installed, the authentication feature still operates and its results are returned.

> **Note**
>
> The non-default settings of the **OCR ENGINE** and **DOCUMENT DATABASE PATH** are not saved. If you close and reopen the app, the default settings will be valid again.

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



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

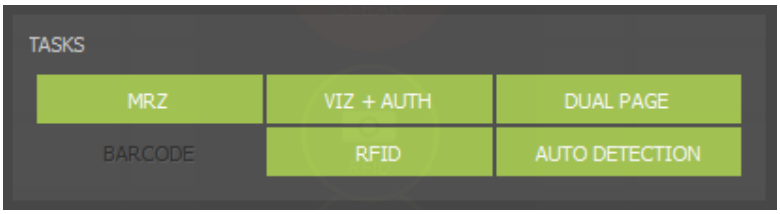
4. TASKS

Select between the provided functions: **MRZ, VIZ+AUTH, DUAL PAGE, RFID** reading and **AUTO DETECTION**.

- **MRZ**: Select this task to get the data of the Machine Readable Zone.
- **VIZ+AUTH**: Enable this task to read document-specific data and verify the optical authentications from the Visual Inspection Zone of different national documents.
- **DUAL PAGE**: Enable this task to read double paged documents automatically. When this function 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 **[OK]** button, Authentication Checker waits 10 seconds for the second side of the document.

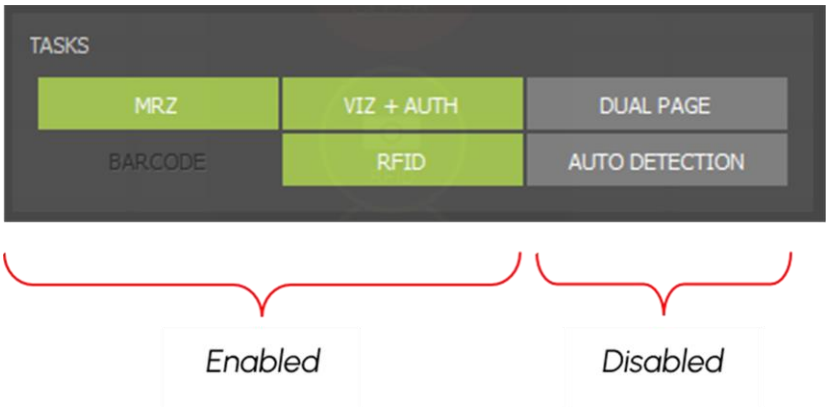
> **Note**
>
> **DUAL PAGE** function only operates automatically, on the condition of the document being recognized by the **VIZ OCR engine**. For more information on VIZ OCR engine, see ADAPTIVE RECOGNITION website.

- **RFID**: Choose this task to read the data from the document's built-in RFID chip.
- **AUTO DETECTION**: Enable/Disable the automatic document presence detection mode (motion detection). This feature senses documents placed on the scanner glass surface. Whenever a document is present, the software captures images of the document.



Note

Click on the button of the given task to enable (green background) or disable (grey background) it.



Note

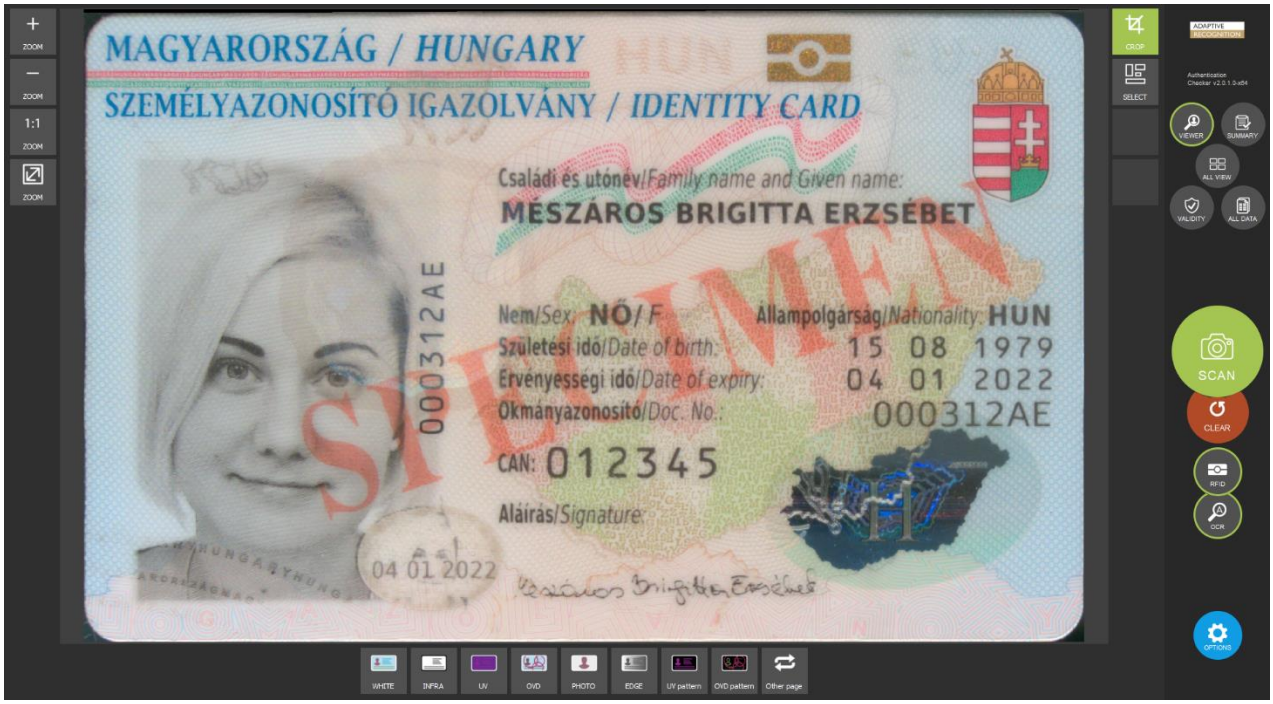
After performing settings, close the window with the **[CLOSE]** button to start document reading.

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

4.6. SECTIONS

4.6.1. VIEWER

In the **VIEWER** section the scanned and/or selected images are displayed. Observe the images under various illuminations, zoom in/out, crop and fit the image to screen as well as perform manual security feature checks.



1. **ZOOM OPTIONS**

- **Zoom in (+)**
- **Zoom out (-)**
- **1:1 Zoom**: shows scanned image in actual size
- **Fit Zoom**: fits scanned image to screen

Note

- You can zoom in by left-clicking inside the image and dragging your mouse over the area you wish to enlarge.
- You can use the scroll to zoom in and out.
- To return to the original (fit) view, double-click in the picture.
- When the image is zoomed in, drag the document with the right mouse button to observe the entire document.

2. CROP

Enable/Disable **CROP** by clicking on the button.

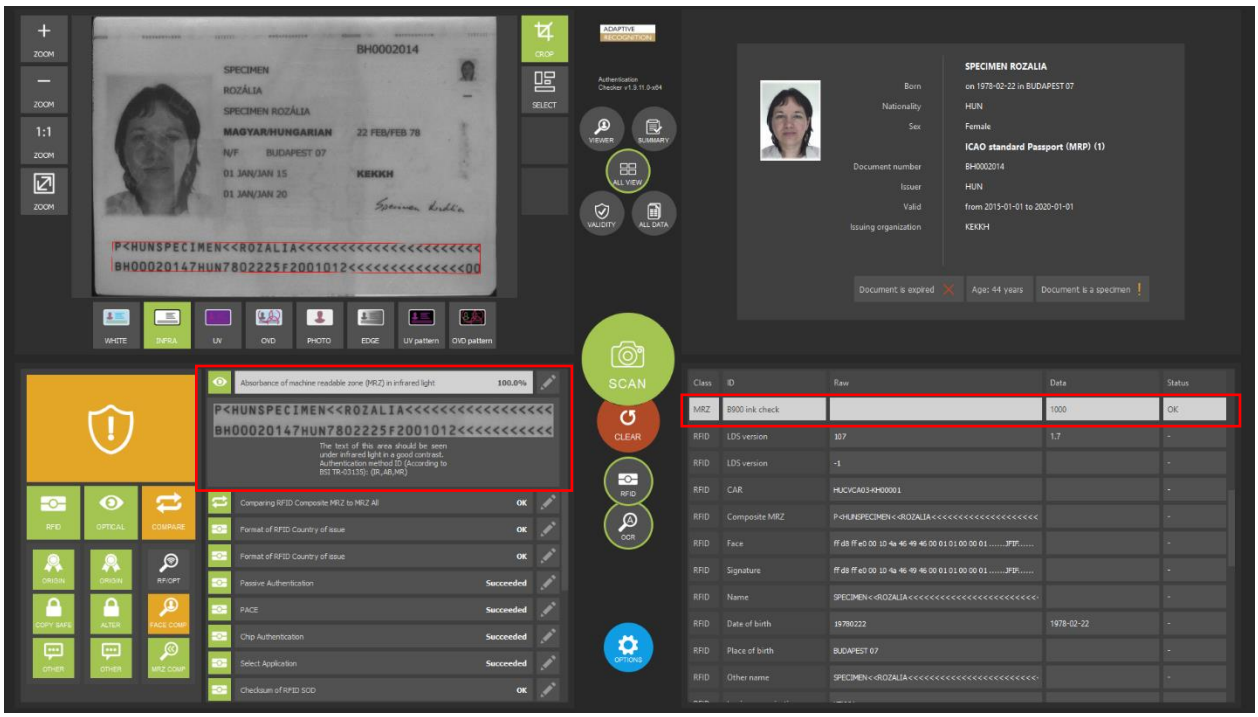
It crops and rotates documents into upright position.

3. SELECT

The **SELECT** function shows you the read authentication and OCR fields.

> **Hint**
>
> If **SELECT** is turned on and the cursor is over the **SELECT** button, at that time the frame of every read field will appear.
>
> If **SELECT** is turned on and the cursor is over the buttons of the different image types, at that time the frames of the read data by the given illumination will appear.

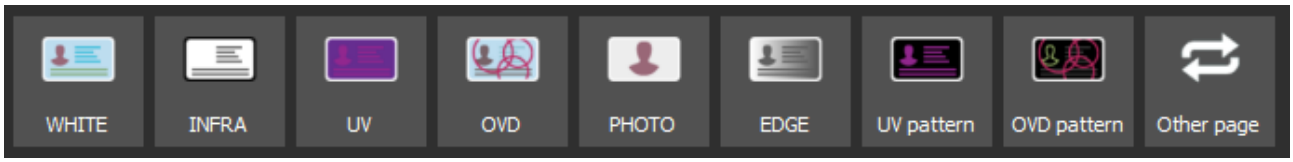
By moving the mouse inside the scanned picture, frames close to the cursor will appear around the read fields. If you click on one of them in **ALL VIEW** mode, in the **VALIDITY** and **ALL DATA** sections the related check(s) to the data in the frame will be highlighted in grey. In these sections you can check the meaning of the given data, how it has been read and the result of the reading.



> **Note**
>
> If you click on the **Dashboard**, the selection will be cancelled.

4. IMAGE TYPES

> **Note**
>
> The number of image types depends on the capabilities of the given scanner.



- **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

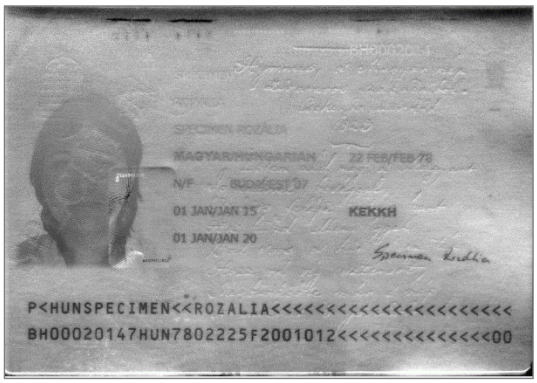
Image scanned in Photo light

> **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.

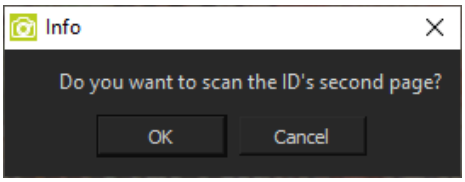
  When using Edge light, the document is illuminated at a flat angle in order to make the protruding objects located on the document cast a shadow.



- **Other page**

  Enable/Disable **Other page** by left-clicking on its button.

  Select this option to check the back side of the read double paged documents. When the **DUAL PAGE** function 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 **[OK]** button, Authentication Checker waits 10 seconds for the second side of the document.



When the scanning of both sides is finished, enable the **Other page** option and select the illumination source (e.g., white, infra, UV, OVD, photo, edge, UV pattern, OVD pattern) under which the back side of the scanned document is to be checked.

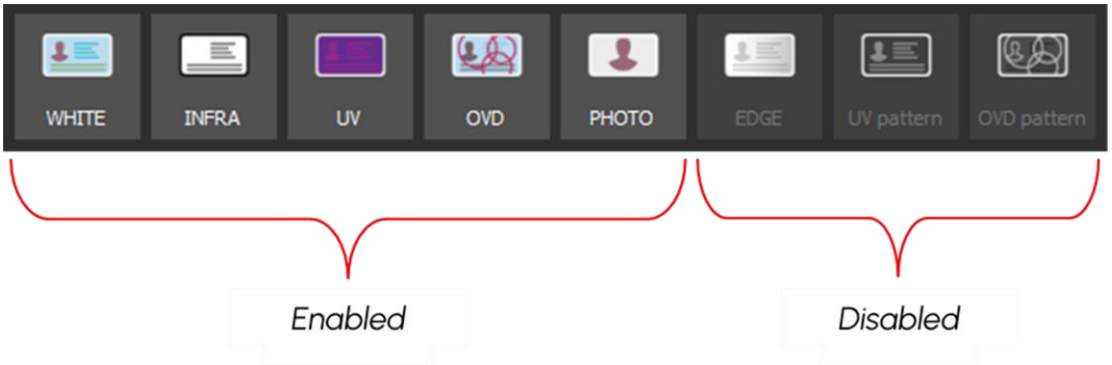
Note

DUAL PAGE function only operates automatically, on the condition of the document being recognized by the VIZ OCR engine. For more information on VIZ OCR engine, see ADAPTIVE RECOGNITION website.

In the **VIEWER** section two image types can be examined alternately. Select one of the required image types by clicking on its icon, then click on the other and continue clicking on it as long as it is necessary. Thereby the two selected images will alternate. This way both lights can be observed without diverting the attention of the operator or moving the mouse.

Note

Use the right mouse click to enable/disable the several illuminations of the application. When disabled, the icon is grey. When enabled, the icon is colored.



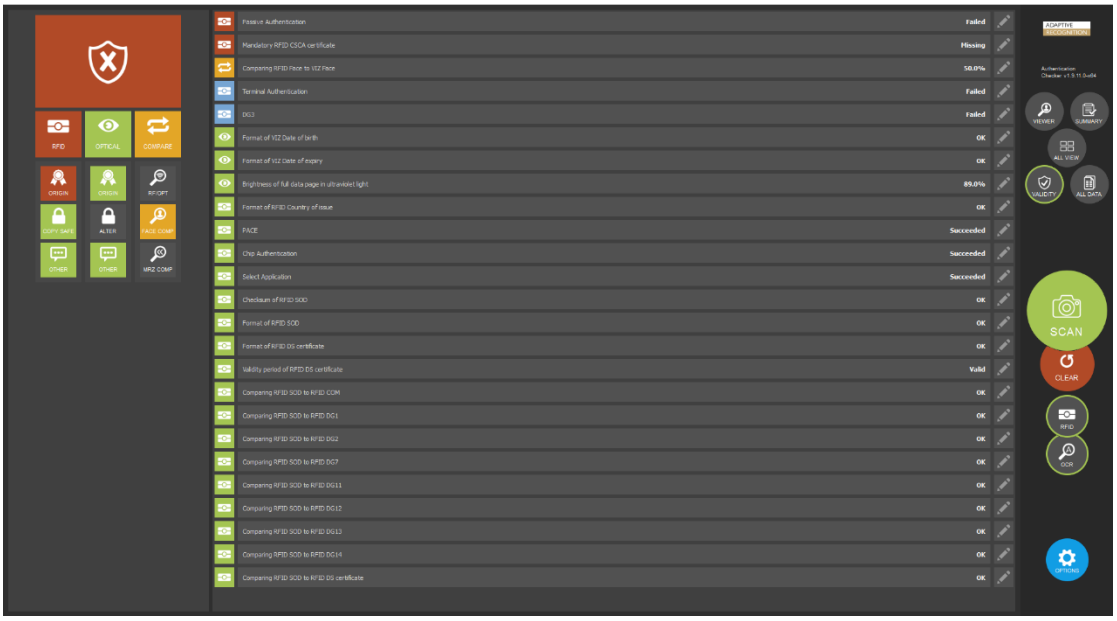
Note

If you click on the **ALL VIEW** button, you will get back to the divided view.

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

4.6.2. VALIDITY

In the **VALIDITY** section the results of the authenticity checks are displayed, including digital data verification (**RFID**), optical (**OPTICAL**) and comparison checks (**COMPARE**).



1. OVERALL RESULT

		
GENUINE	**WARNING**	**FAILED**
This document has been found genuine. See confidence rates in the chart.	Questionable authentication results or reading failures. See details in the chart. Manual inspection is recommended.	Unsatisfactory authentication results or reading failure of key data. In-depth manual inspection is recommended.

> **Note**
>
> If you click on the symbol, you will get the results of every extracted data in the chart.

> **Note**
>
> Some tests are not executed by the Passport Reader System, but by this program. The results of these tests currently do not count into the overall result and do not appear in this panel. They only appear in the **SUMMARY** section.

2. AUTHENTICATION CATEGORIES

- **RFID**: authentications in relation to e-documents (performing various access control functions and checking data integrity/genuineness of the chip)
- **OPTICAL**: security checks of optical security features, including ink, paper material, pattern matching using various illuminations, etc.
- **COMPARE**: printed vs. digital data comparison checks (including MRZ and face photo)

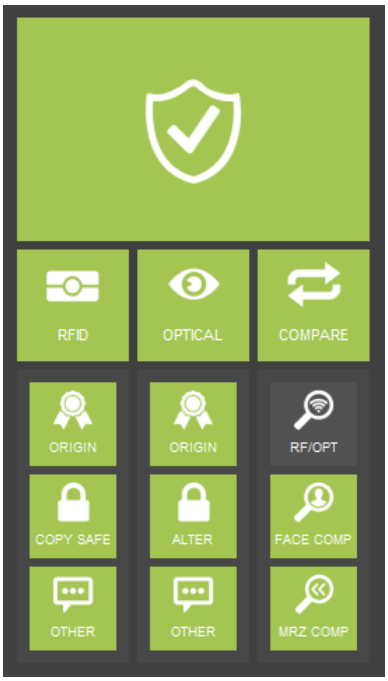
> Note
>
> If you click on one of the categories, you will get exclusively its results in the chart.

3. AUTHENTICATION ELEMENTS

Each category has 3 elements:

RFID

- **ORIGINALITY**: Checks if the data on the RF chip of the electronic document is authentic and unforged
- **COPY SAFE**: Uncovers cloned RF chips
- **OTHER**: Checks which do not belong to the previous two elements



OPTICAL

- **ORIGINALITY**: Checks if the physical document is authentic
- **ALTERATION**: Checks if the document data has been tampered with
- **OTHER**: Checks which do not belong to the previous two elements

COMPARE

- **RF/OPT**: –
- **FACE COMPARISON**: Compares the VIZ face (the printed face photo on the document) to the RFID face (stored in the chip)
- **MRZ COMPARISON**: Compares MRZ (on the document) to RFID MRZ (stored in the chip)

> Note
>
> If you click on one of the elements, you will get exclusively its results in the chart.

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

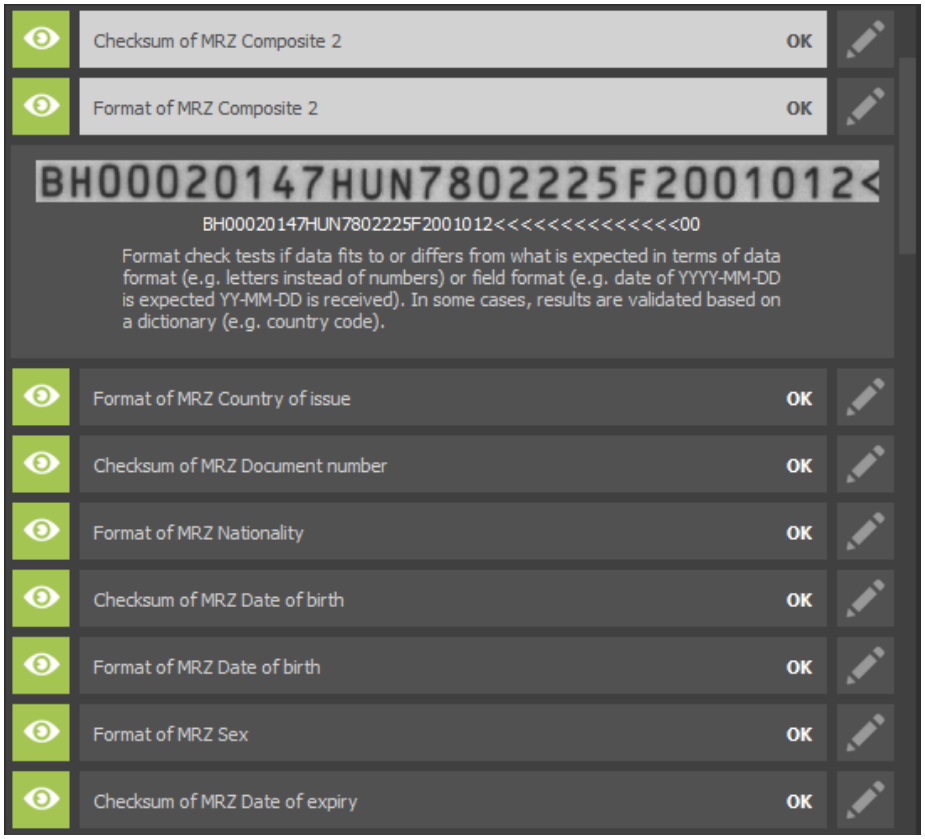
4. THE CHART

In the chart the different checks and their results are displayed. By clicking on a check, a short description about the given check as well as the interpretation of its result, image(s) from the reference database (if the **OCR ENGINE** and the **DOCUMENT DATABASE PATH** are set), picture(s) about the given data on the document (optional) and the read data (optional) can be seen.
On the left side of the chart the authentication categories' symbols can be seen, that shows you which category the given check belongs to. The background colors of the symbols indicate the given check's result, except blue, which means test results unrelated to document security. On the right side of the chart the given check's result can be seen.

The display of the results can be filtered by the following:

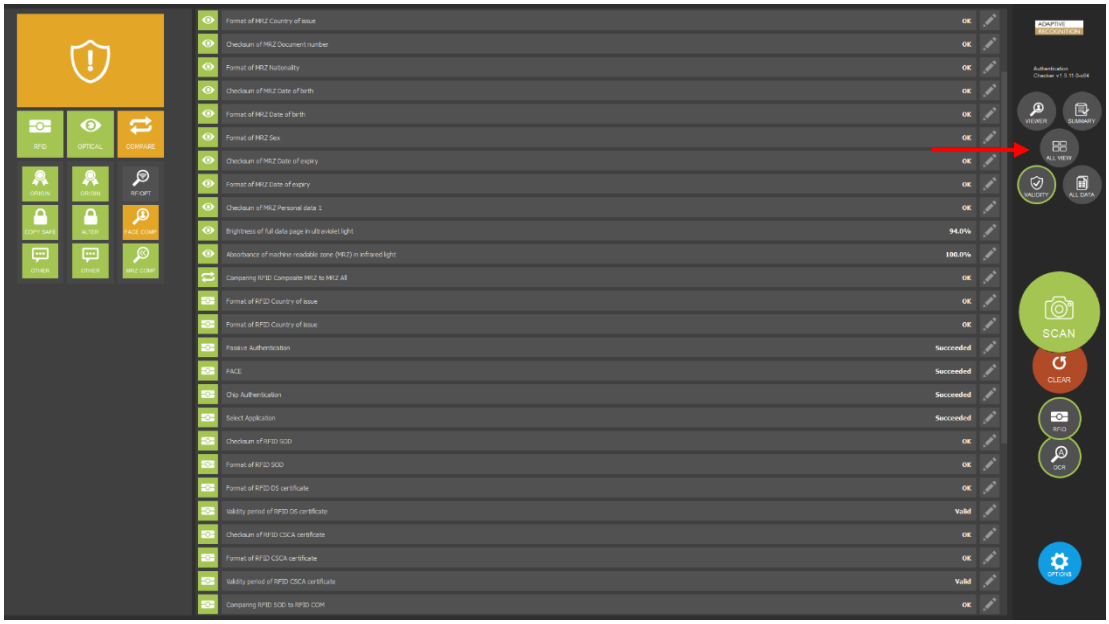
- displays the results of every extracted data (by clicking on the symbol of the overall result)
- displays just the results of a chosen category (by clicking on a category)
- displays just the results of a chosen element (by clicking on an element)

> **Note**
>
> More checks may be highlighted at the same time in the chart, if on the given data can be performed different inspectorial processes.



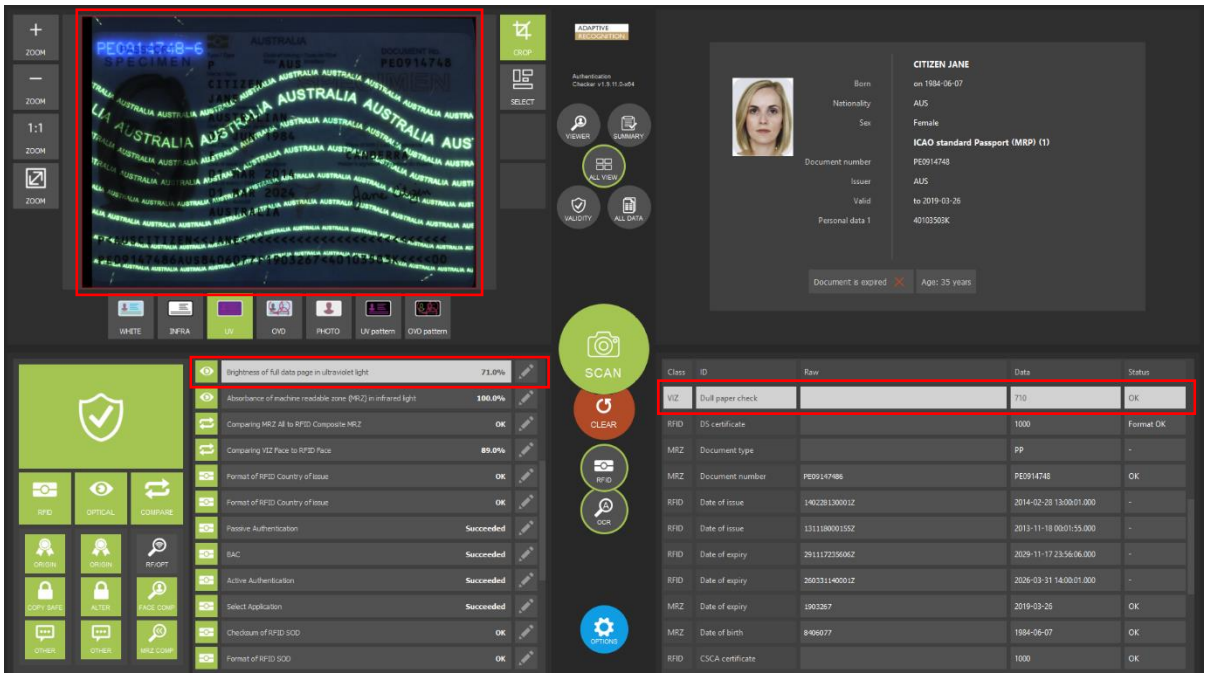
Note

If you click on the **ALL VIEW** button, you will get back to the divided view.



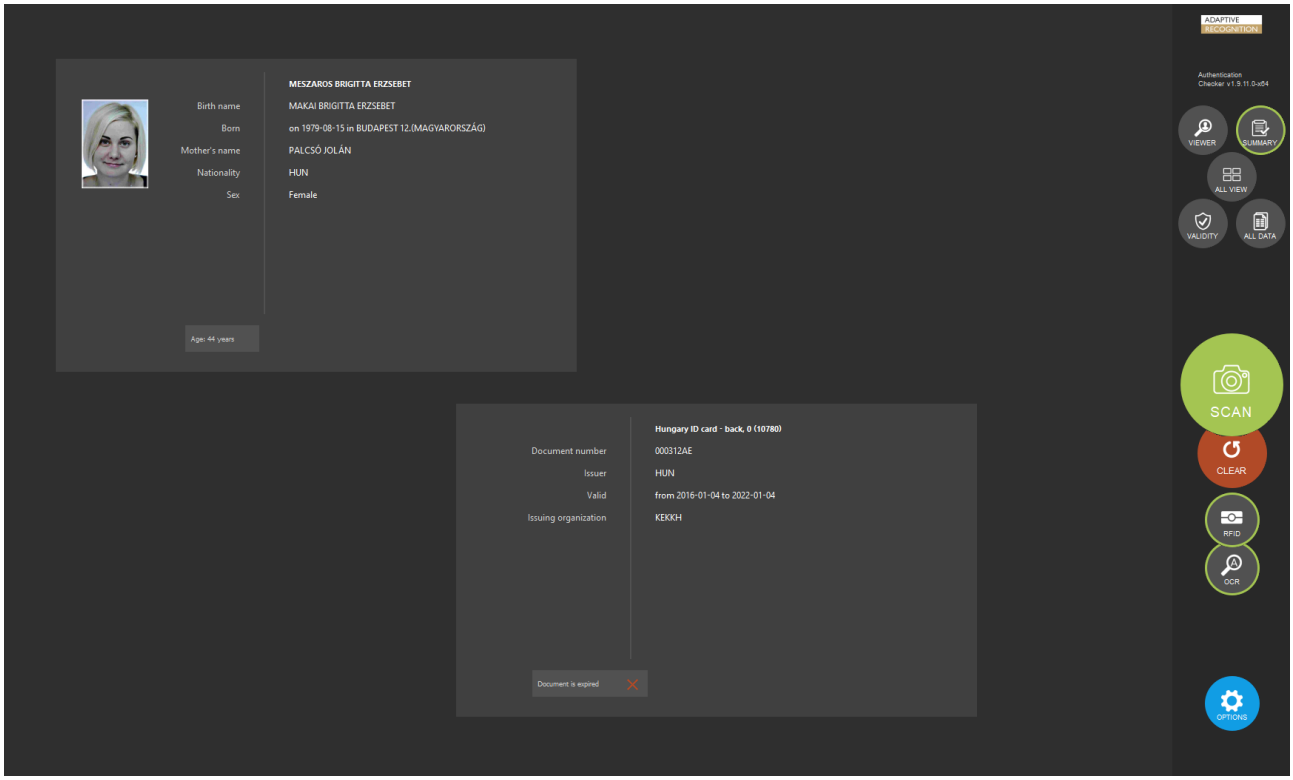
Note

If you click on a certain data in the **VALIDITY** section in **ALL VIEW** mode, a red frame will be displayed around the original location of the data in the **VIEWER** section as well as in the **ALL DATA** section the related check(s) to the data will be highlighted in grey. To cancel the selection, click on the **Dashboard**.



4.6.3. SUMMARY

In the **SUMMARY** section, selection of the essential personal and document data is displayed. The scanned data is displayed in two separate windows depending on the data type (personal or document data).



SUMMARY section summarizes the result of the scanning process.

It displays:

- essential personal information: name, birth name, date of birth, nationality, sex, face photo
- essential document information: document type, document number, document issuer country, document validity, issuing organization
- feedback:
  - document is expired/document is not expired/document with a close expiry date
  - age
  - document is a specimen
  - unknown document

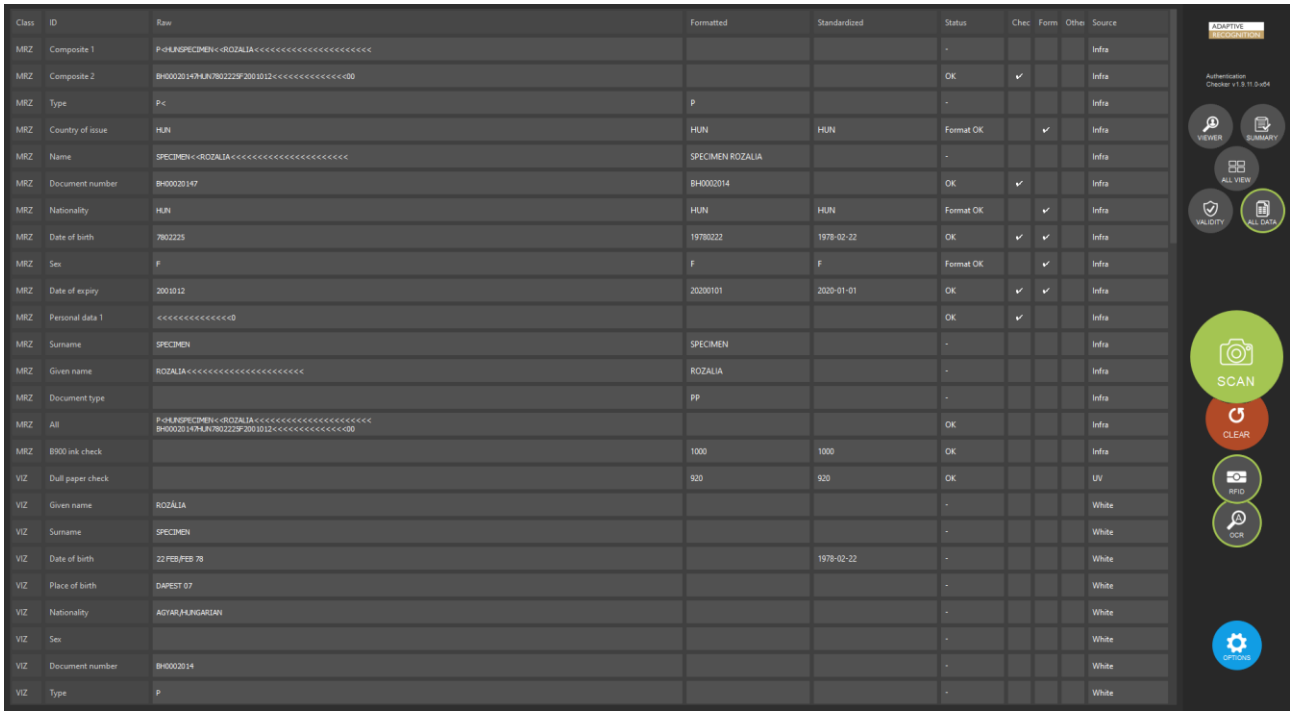
> **Note**
>
> If you click on the **ALL VIEW** button, you will get back to the divided view.

4.6.4. ALL DATA

The **ALL DATA** section displays all available data retrieved from the document.

Note

More details (e.g., more columns) can be found in the **ALL DATA** panel than in the **ALL VIEW** mode.



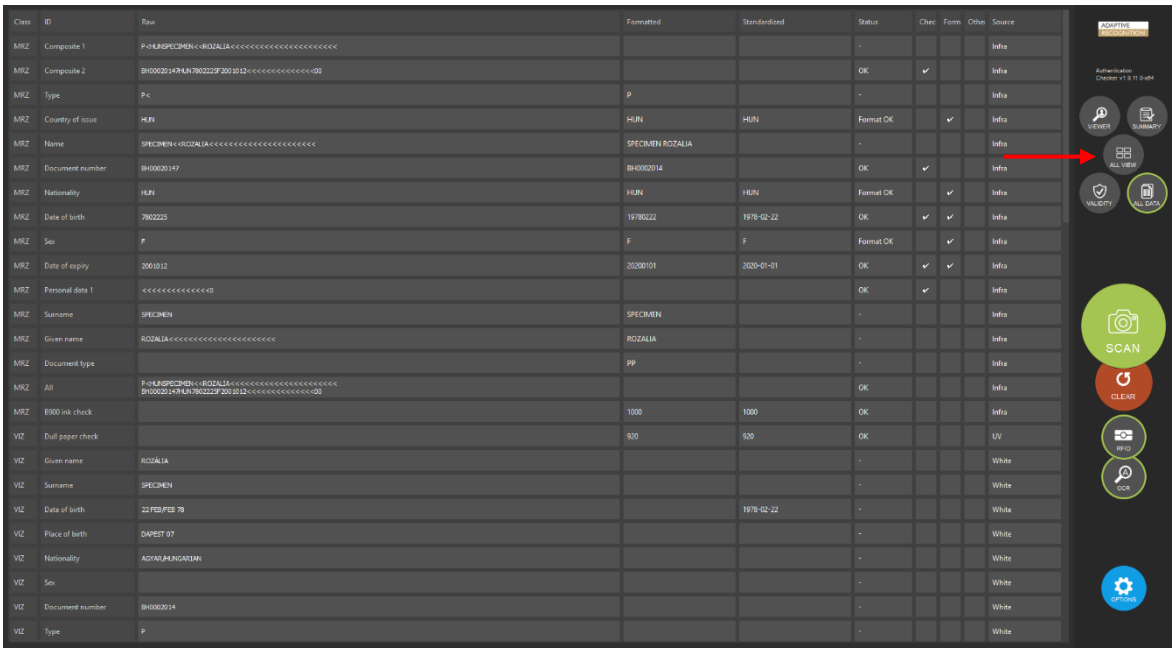
Class	ID	Raw	Formatted	Standardized	Status	Chec	Form	Other	Source
MRZ	Composite 1	P<HUNSPECIMEN<<ROZALIA<<<<<<<<<<<<<<<<<<<<<<			-				Infra
MRZ	Composite 2	BH00020147HUN7802225F2001012<<<<<<<<<<<<<<00			OK	✓			Infra
MRZ	Type	P<	P		-				Infra
MRZ	Country of issue	HUN	HUN	HUN	Format OK		✓		Infra
MRZ	Name	SPECIMEN<<ROZALIA<<<<<<<<<<<<<<<<<<<<<<	SPECIMEN ROZALIA		-				Infra
MRZ	Document number	BH00020147	BH0002014		OK	✓			Infra
MRZ	Nationality	HUN	HUN	HUN	Format OK		✓		Infra
MRZ	Date of birth	7802225	19780222	1978-02-22	OK	✓	✓		Infra
MRZ	Sex	F	F	F	Format OK		✓		Infra
MRZ	Date of expiry	2001012	20200101	2020-01-01	OK	✓	✓		Infra
MRZ	Personal data 1	<<<<<<<<<<<<<<0			OK	✓			Infra
MRZ	Surname	SPECIMEN	SPECIMEN		-				Infra
MRZ	Given name	ROZALIA<<<<<<<<<<<<<<<<<<<<<<	ROZALIA		-				Infra
MRZ	Document type		PP		-				Infra
MRZ	All	P<HUNSPECIMEN<<ROZALIA<<<<<<<<<<<<<<<<<<<<<< BH00020147HUN7802225F2001012<<<<<<<<<<<<<<00			OK				Infra
MRZ	B900 ink check		1000	1000	OK				Infra
VIZ	Dull paper check		920	920	OK				UV
VIZ	Given name	ROZÁLIA			-				White
VIZ	Surname	SPECIMEN			-				White
VIZ	Date of birth	22 FEB/FEB 78		1978-02-22	-				White
VIZ	Place of birth	DAPEST 07			-				White
VIZ	Nationality	AGYAR/HUNGARIAN			-				White
VIZ	Sex				-				White
VIZ	Document number	BH0002014			-				White
VIZ	Type	P			-				White

Note

If you click on the header of the columns, the data order will be reversed as well as the aspect of the order can be modified because the app categorizes the related ones.

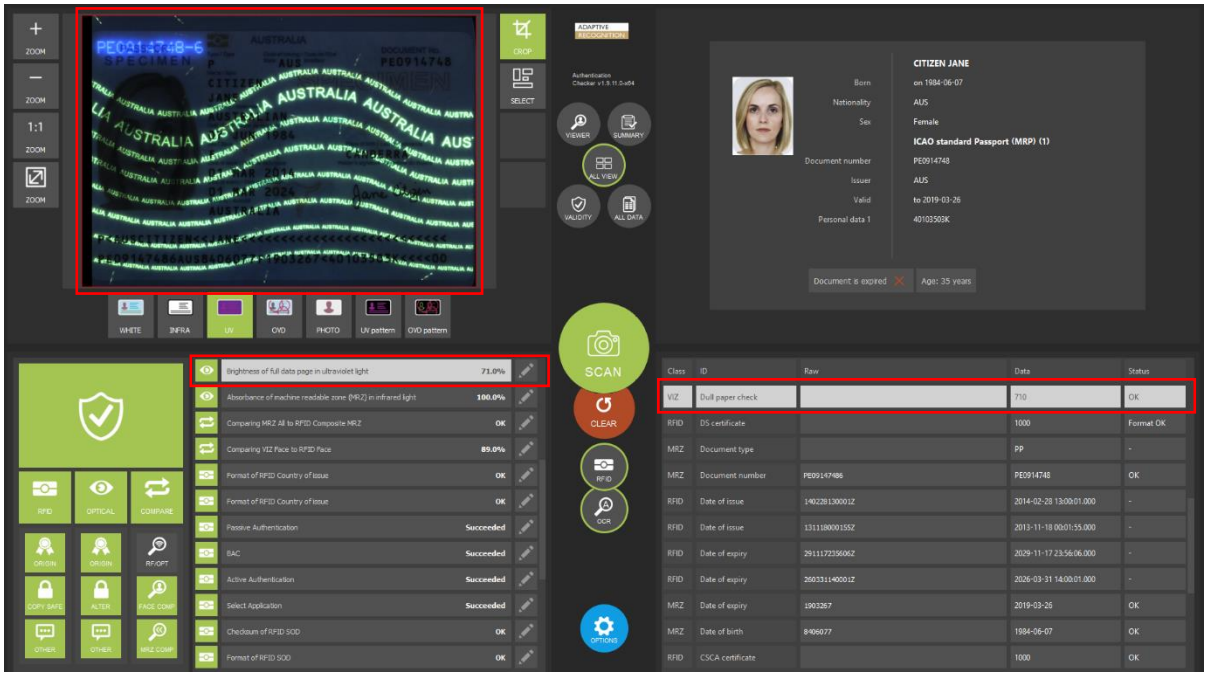
Note

If you click on the **ALL VIEW** button, you will get back to the divided view.



Note

If you click on a certain data in the **ALL DATA** section in **ALL VIEW** mode, a red frame will be displayed around the original location of the data in the **VIEWER** section as well as in the **VALIDITY** section the related check(s) to the data will be highlighted in grey. To cancel the selection, click on the **Dashboard**.



4.7. CERTIFICATES

For successful authentication, the reader needs digital certificates from the document issuer authorities. This software contains these certificates for currently used passports, but in order to support the latest documents, the certificates should be updated from time to time.

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. FULL PAGE READER APPLICATION

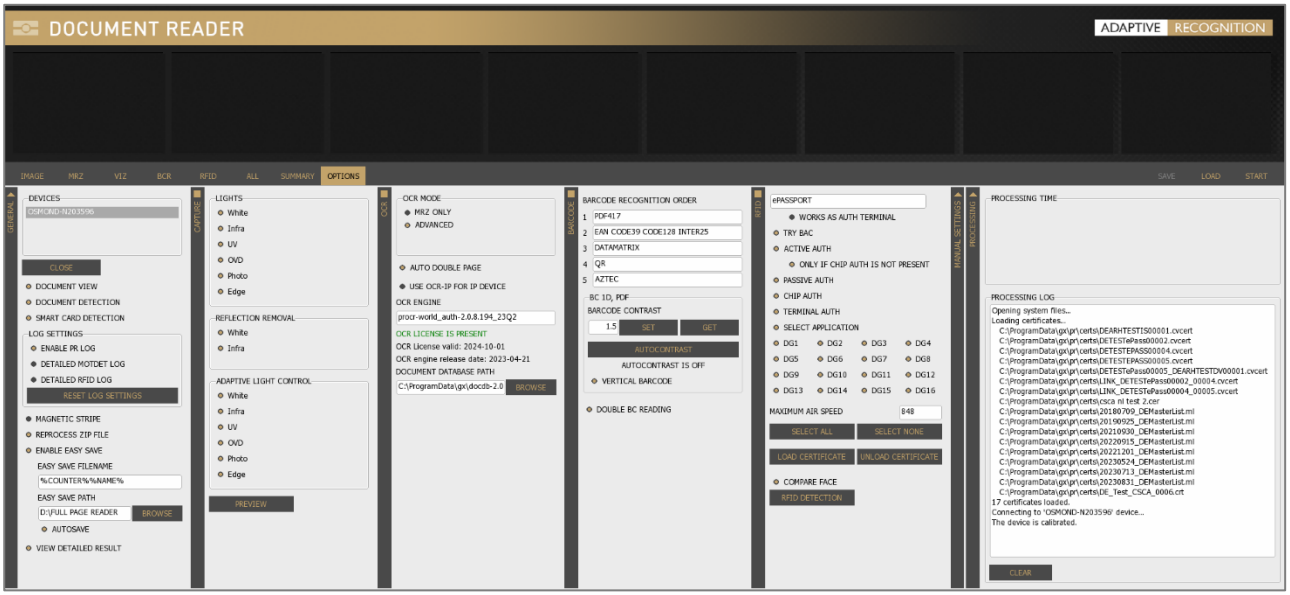
ADAPTIVE RECOGNITION provides its Full Page Reader (FPR) application included in the Passport Reader (PR) software package. Full Page Reader application is able to fully exploit the ADAPTIVE RECOGNITION document reader devices' capabilities on user level.

It provides:

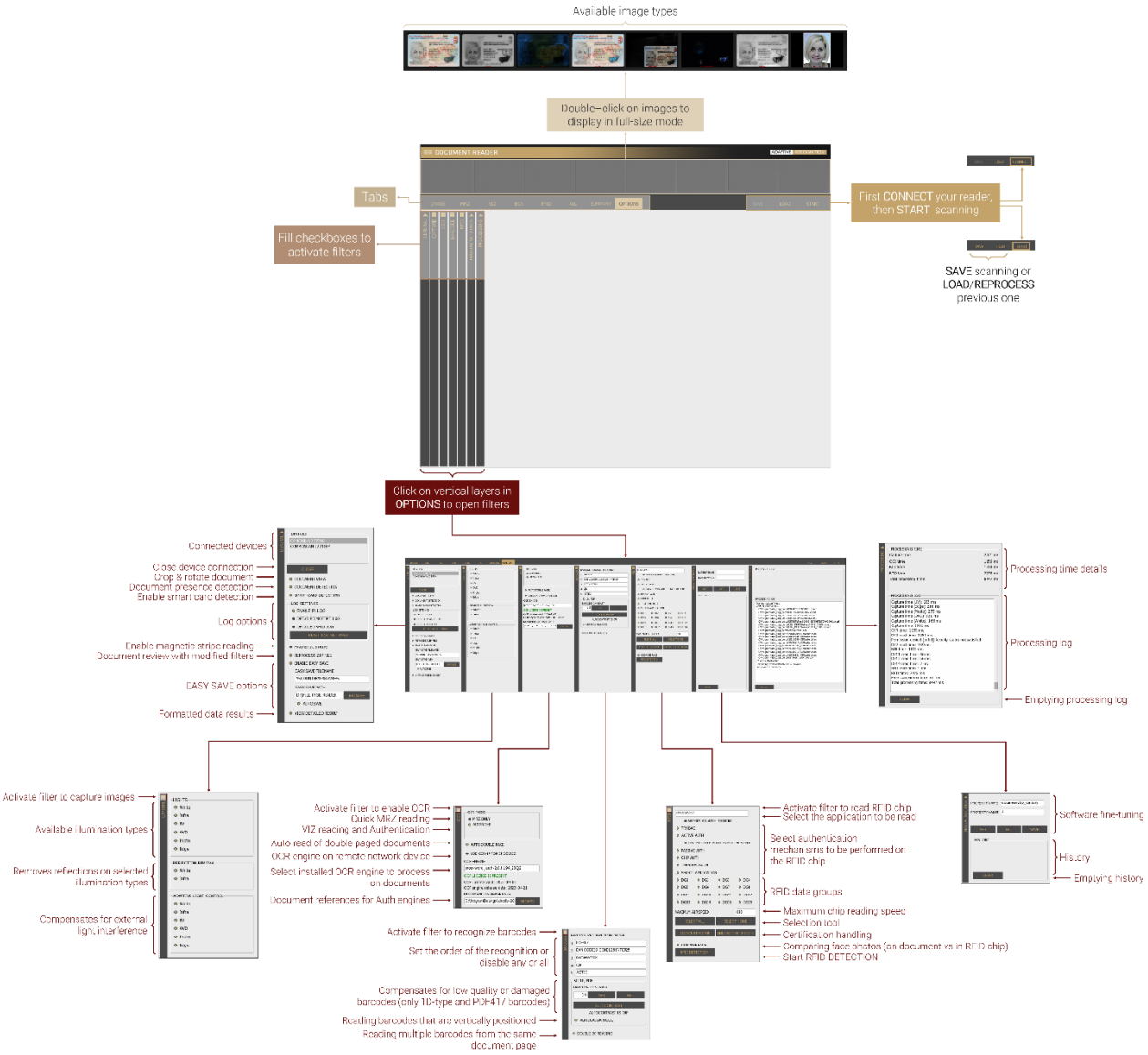
- images scanned by different illumination sources (white, infra, UV)
- OCR mode to reach MRZ, VIZ data and read different barcode types
- optical and RFID authentications

This chapter is going to show you the functions of the app and the methods of the use.
The structure of this section is the following:

- First, the device overview and its accessing will be discussed.
- Next, a closer look will be taken at the tabs of the application.
- Then, the user will be guided through the settings of the Options tab menu.
- Finally, a list of frequently asked questions is expounded.



5.1. OVERVIEW



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

5.2. REQUIREMENTS

- ADAPTIVE RECOGNITION ID/Passport Reader device(s) connected to the PC
- PC: minimum 2 GHz CPU and 1GB RAM
- OS: 32/64-bit Windows XP/Vista/7/8/8.1/10/11 or Linux

Note

To make the most of the ADAPTIVE RECOGNITION document reader device and the application, it is recommended to use the VIZ AUTH engine on 64-bit operating systems.

5.3. START FULL PAGE READER

- **Windows**

  After installing ADAPTIVE RECOGNITION software package on your computer, you will be able to open Full Page Reader from **Windows Start menu > Adaptive Recognition > (Passport Reader) > Full Page Reader x86 or x64** (based on your computer architecture and previous installation).

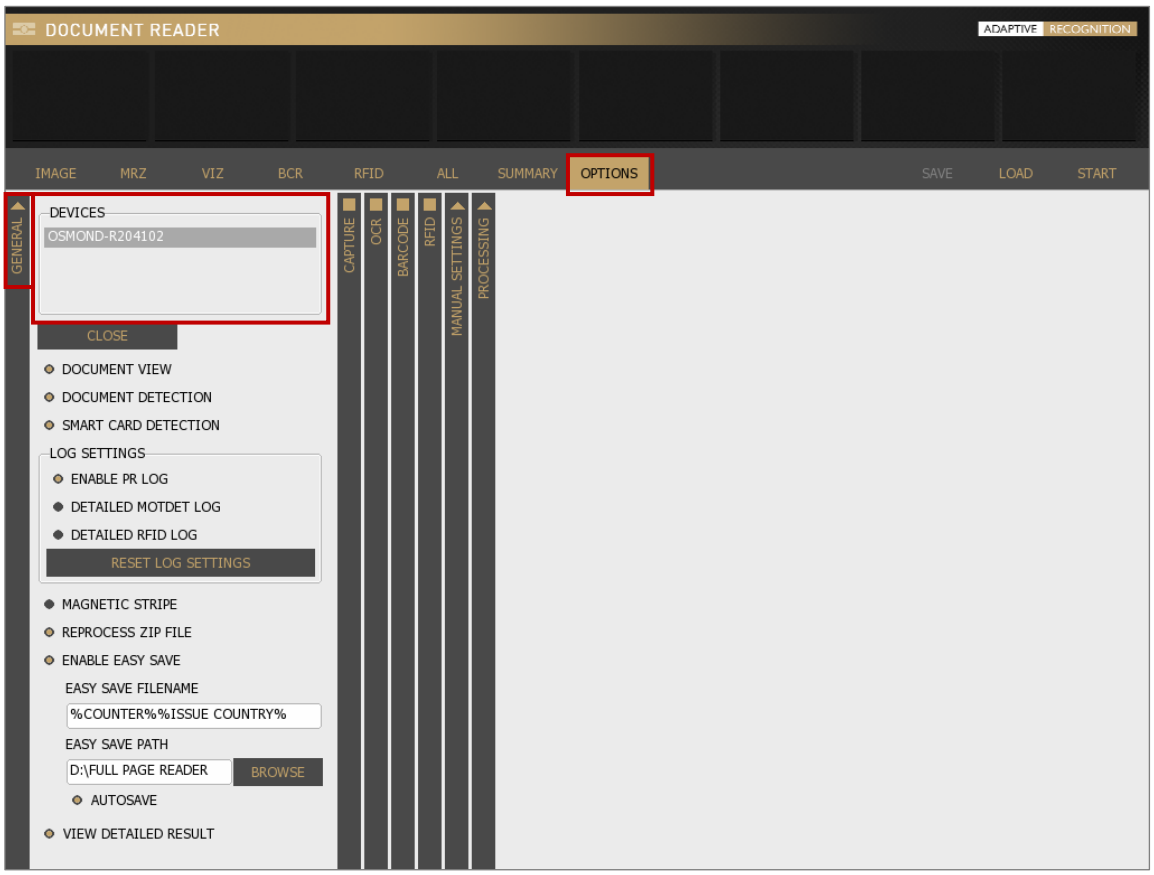
- **Linux**

  Depending on your distribution, you can open command terminal and insert: **FullPageReader** or use dashboard search bar: **Linux Start menu > Applications > Adaptive Recognition Apps > Full Page Reader 64-bit version** (based on your computer architecture and previous installation).

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

5.4. CONNECTION

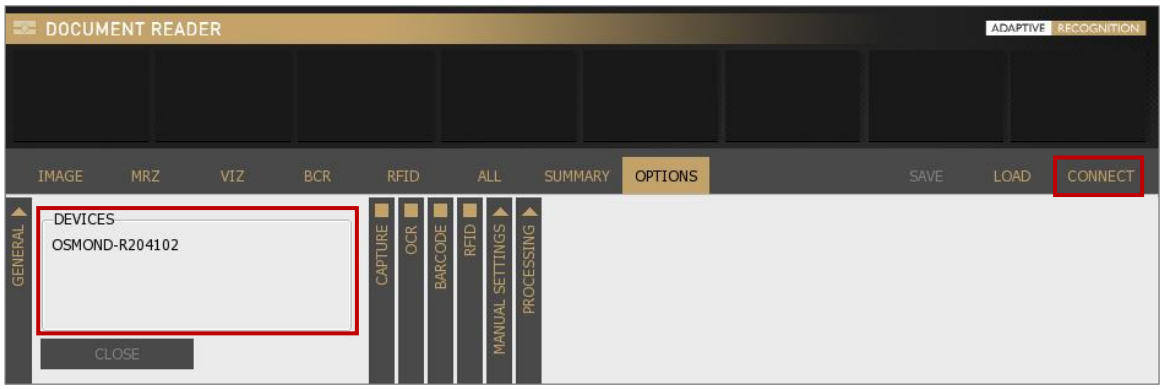
In order to scan with any ADAPTIVE RECOGNITION reader device, you have to make sure that there is an available reader connected to your computer and it is turned on. You can check the **DEVICES** list in the **OPTIONS** tab at **GENERAL** layer.



Note

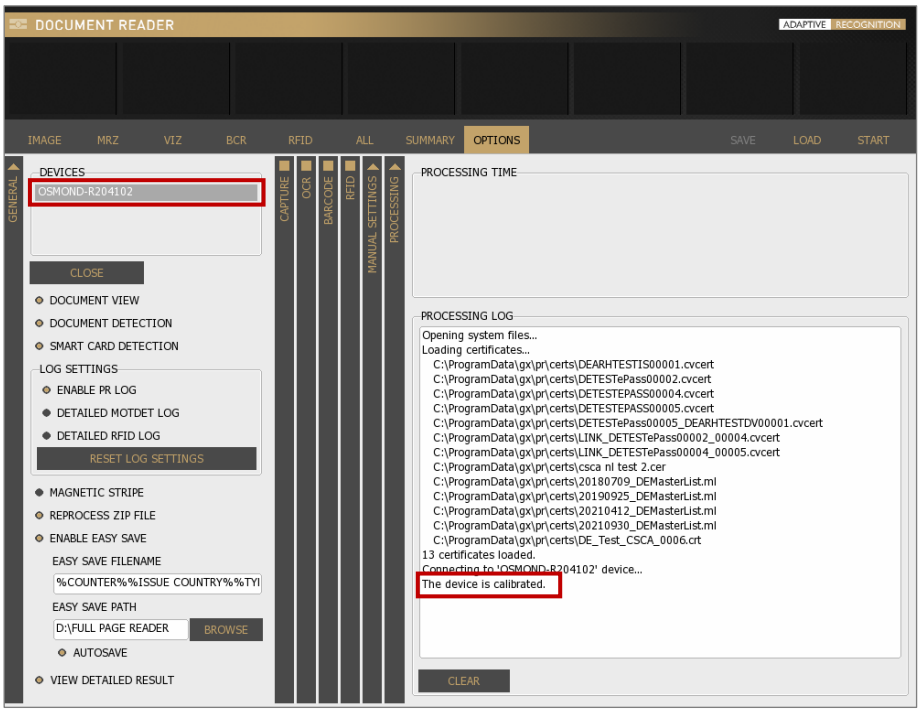
If a device is connected to the computer, but it is not displayed in the **DEVICES** list, then try to change the USB port and/or USB cable. If the issue is not resolved after these changes, reinstall the Passport Reader Software Package as admin. For more information on the installation process, see Software Installation chapter.

Connect your device by clicking on **[CONNECT]** or clicking on the selected reader in the **DEVICES** list.



Readers hold a factory default calibration file. Reading this file from the device for the first time may take some time, which consequently slows down the system startup. In order to save time, the file is automatically copied to the local file system on the first attempt of using the device to speed up communication. In this case "**Reading calibration file...**" message appears in the **PROCESSING LOG** field.

If your reader is displayed in the **DEVICES** list highlighted in grey and in the **PROCESSING LOG** field you get the "**The device is calibrated.**" message, your reader is connected and ready to use.



Note

The Product Name contains the following information: the device name, configuration (components) and serial number (without 1st digit).

E.g., OSMOND-R204102

5.5. TABS

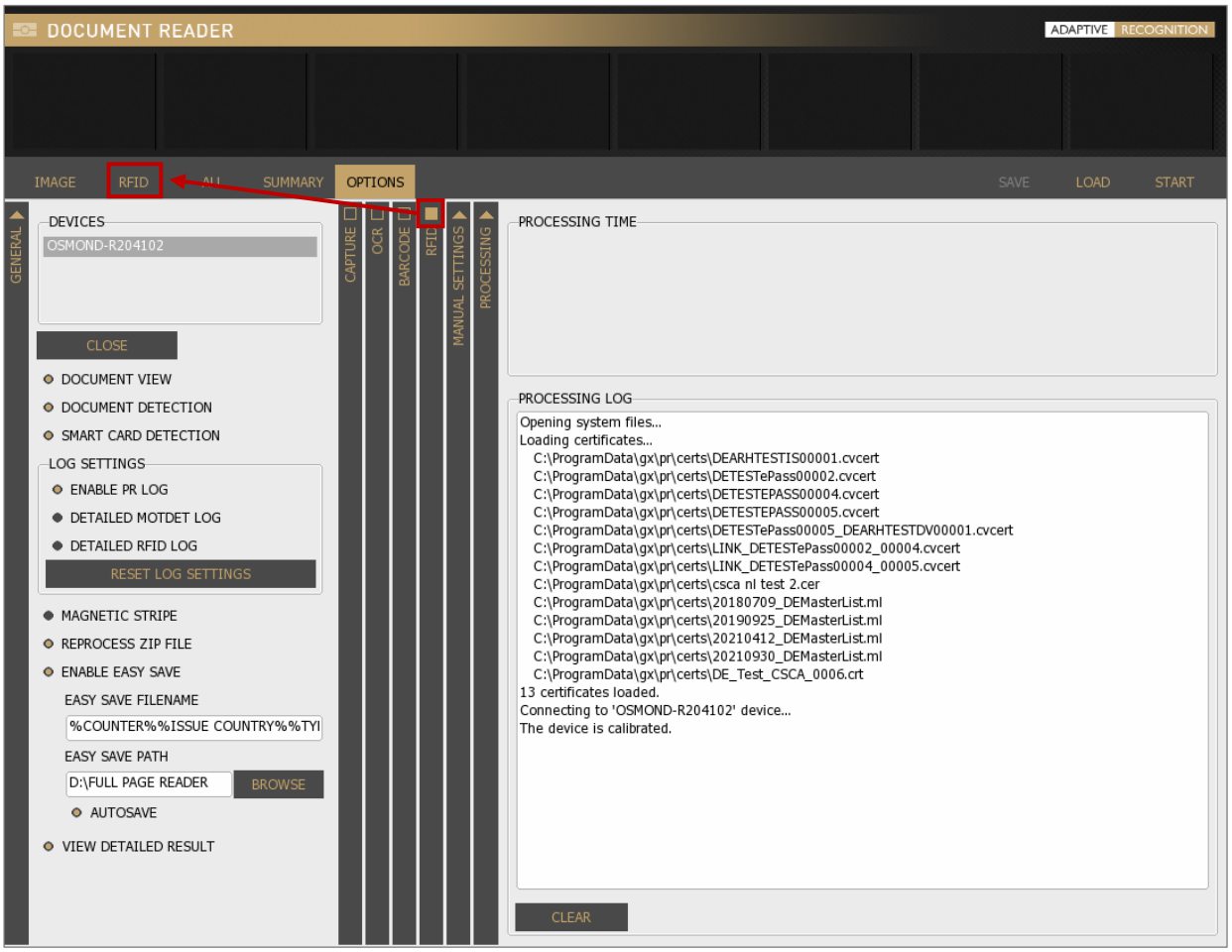
Enable/Disable any of the checkboxes on vertical layers (columns) in the **OPTIONS** tab. These checkboxes switch on/off software functions like image capturing, OCR, barcode and RFID reading. By switching on functions, you will make visible the corresponding tab menu and related data as well.

Note

These columns can open and close like a vertical accordion menu.

Example

Enable RFID reading by filling in the checkbox on the vertical grey layer in the **OPTIONS** tab. This also enables the **RFID** tab to display RFID data after a successful reading process.

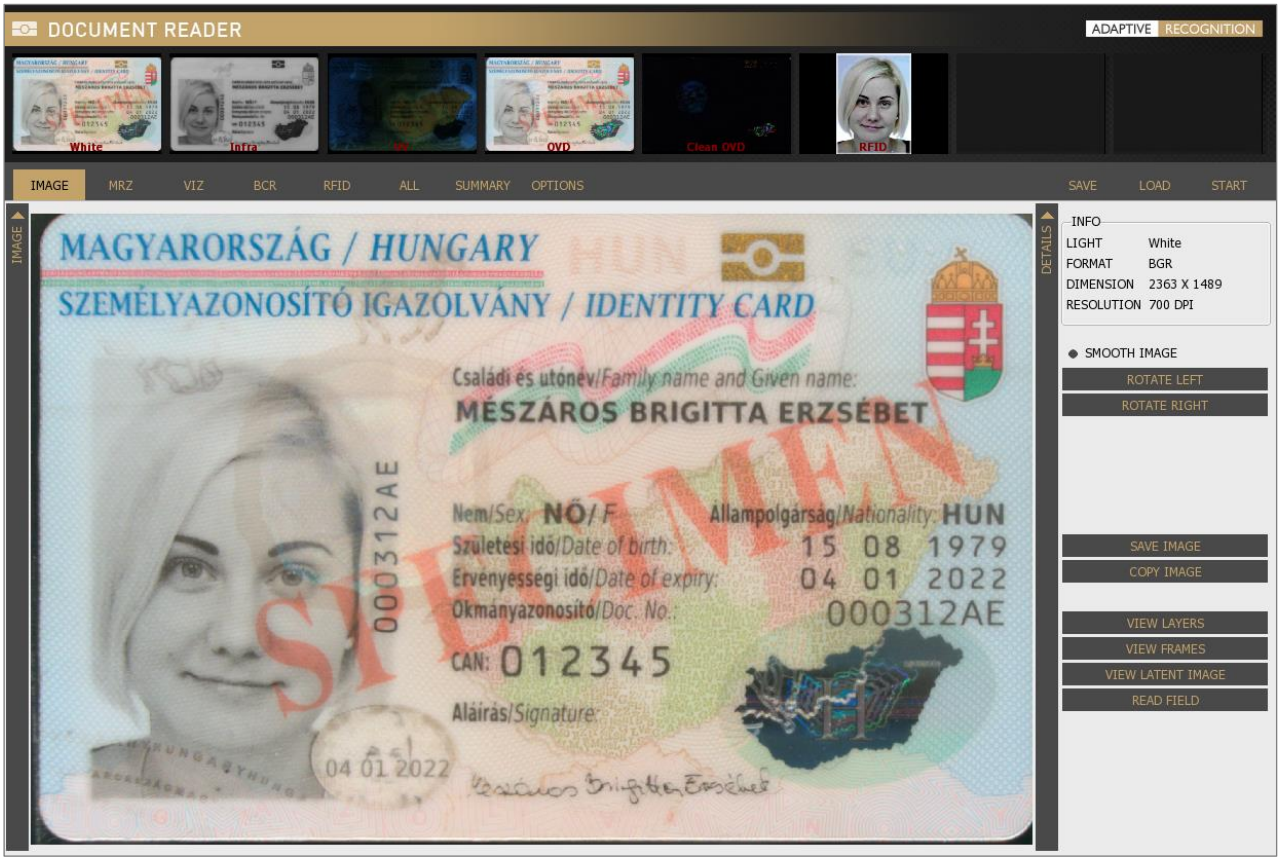


5.5.1. IMAGE

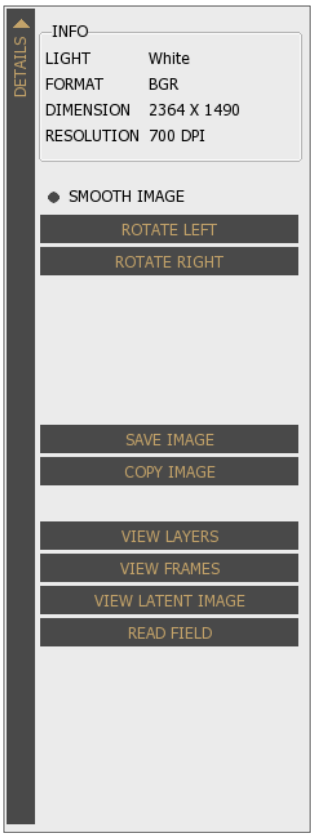
1. IMAGE

On the **IMAGE** layer, the scanned and/or selected images are displayed. Navigate among images by clicking on the thumbnail view on top or double clicking on the ones at details of the document field. Zoom in by left-clicking inside the image and dragging your mouse over the area you wish to enlarge.

> **Note**
>
> All images (even the ones at details of the document fields) can be zoomed out by double-clicking.



2. DETAILS



INFO

Light or field ID, format, dimension and resolution information about the selected image are displayed.

SMOOTH IMAGE

Use linear filtering for zooming by estimating intermediate points among end points automatically. This results a smooth image to display.

ROTATE LEFT/RIGHT

Rotate the image by pressing **[ROTATE LEFT]** or **[ROTATE RIGTH]** button. You can rotate the image by 90 degrees in one direction with one click.

SAVE IMAGE

Save the scanned image to your system by clicking on the **[SAVE IMAGE]** button.

COPY IMAGE

Copy the selected image to clipboard by clicking on the **[COPY IMAGE]** button.

> **Note**
>
> The **COPY IMAGE** function is available only for Windows OS.

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

VIEW LAYERS

By selecting between UV (**VIEW UV FLASHLIGHT**) and OVD flashlights (**VIEW OVD FLASHLIGHT**) on the right, you can check the document under these two illumination types separately. If you do not choose from these flashlights, you can grab the corner/edge of a given layer (except for infra) to optically remove each and every layer from the image of the scanned ID document by left-click. Check slider view too by holding-right-click.

> **Note**
>
> After optically removing the UV or OVD layer, the order of the remaining optically removable layers is fix following a natural order.

VIEW FRAMES

This function displays a frame of the selected reading field. **MRZ**, **VIZ**, **BARCODE** and **ERROR FRAMES** can be displayed around the original location of the data. Select the frame you wish to display from the available options.

VIEW LATENT IMAGE

Important!

VIEW LATENT IMAGE function works well on high-resolution images (e.g., images scanned by Osmond devices).

It displays the JURA IPI security feature. IPI is encrypted information in the face photo part of the document (passport or ID) that can be made visible either by special lenses or ADAPTIVE RECOGNITION document reader devices.

Note

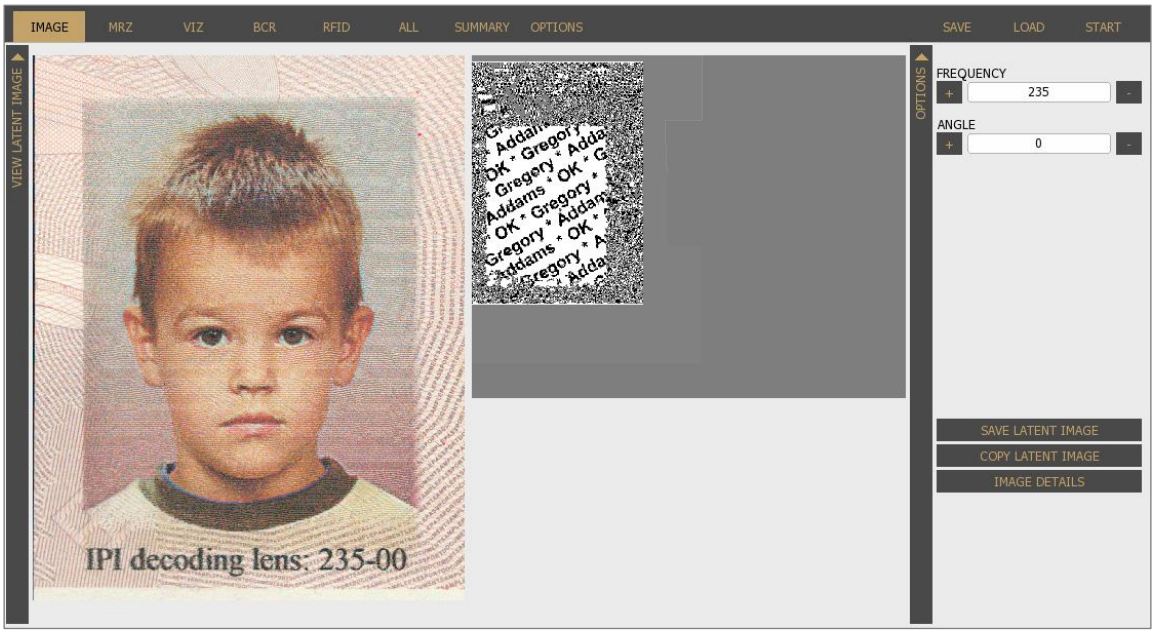
To check the JURA IPI security feature, enable **Photo** camera on **CAPTURE** layer in the **OPTIONS** tab and click on the **Photo** image from the thumbnail images.

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

Note

You need to specify the **FREQUENCY** and **ANGLE** values to make this security feature visible. These values can vary by documents.

Specify these values by filling out the corresponding fields.

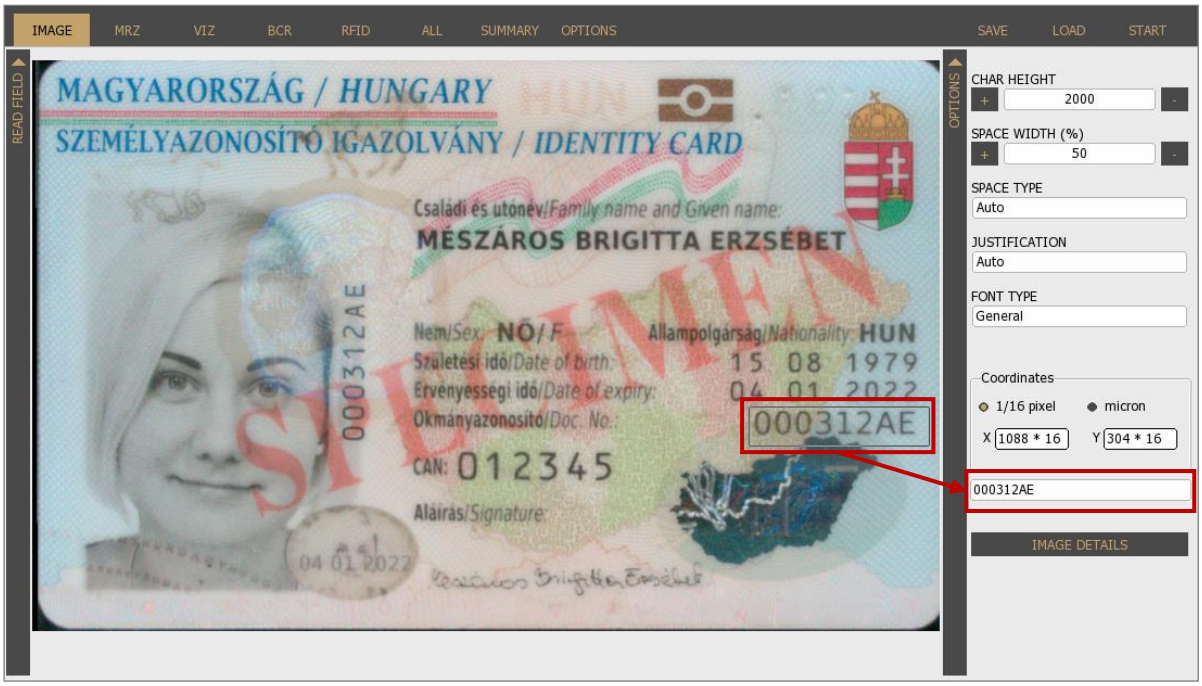


READ FIELD

> **Note**
>
> This function is only available with engines 2.0.6.xx.

The **READ FIELD** function is equivalent to manual OCR. It can be used on **White** and **Infrared** images. Draw a rectangle around any text or barcode and its content will be displayed in the field at the bottom-right corner of the window. Adjust height/width properties to optimize recognition rate.

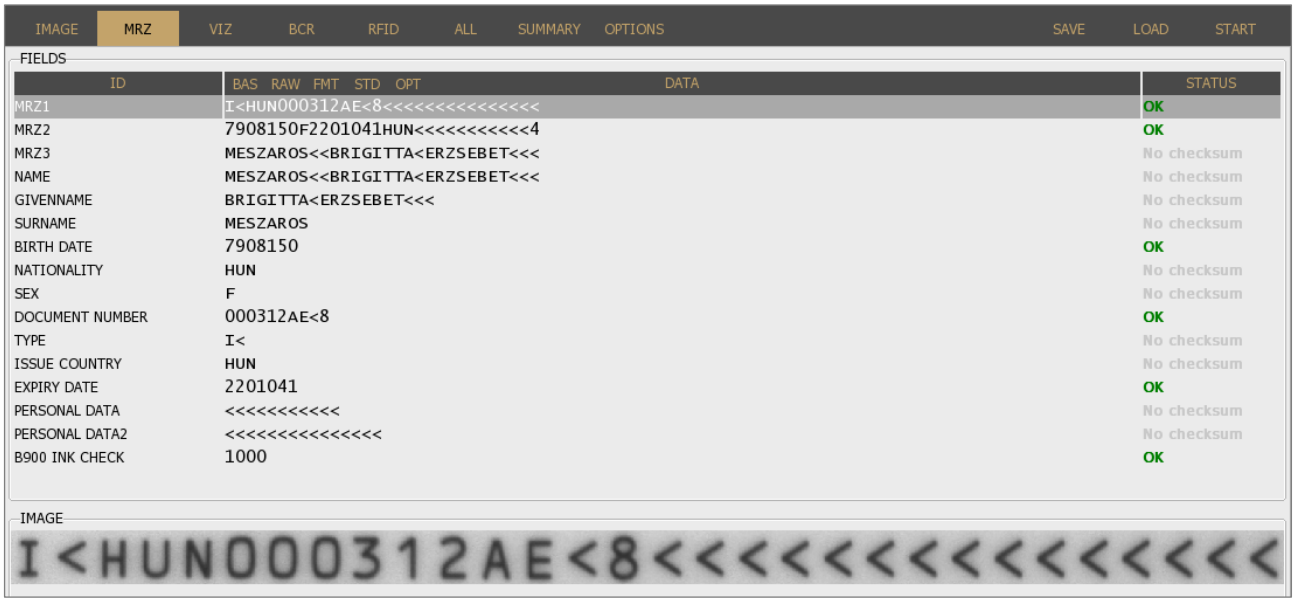
> **Note**
>
> It is suitable for trying out the manual OCR.
> This function has limited ability (only recognizes a few fonts).



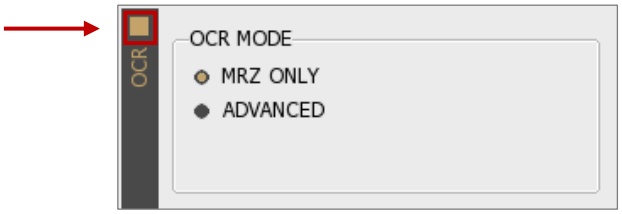
> **Note**
>
> In order to go back to the **DETAILS** layer, please click on the **IMAGE DETAILS** button.

5.5.2. MRZ

Displays processed MRZ data and a photo of each field.

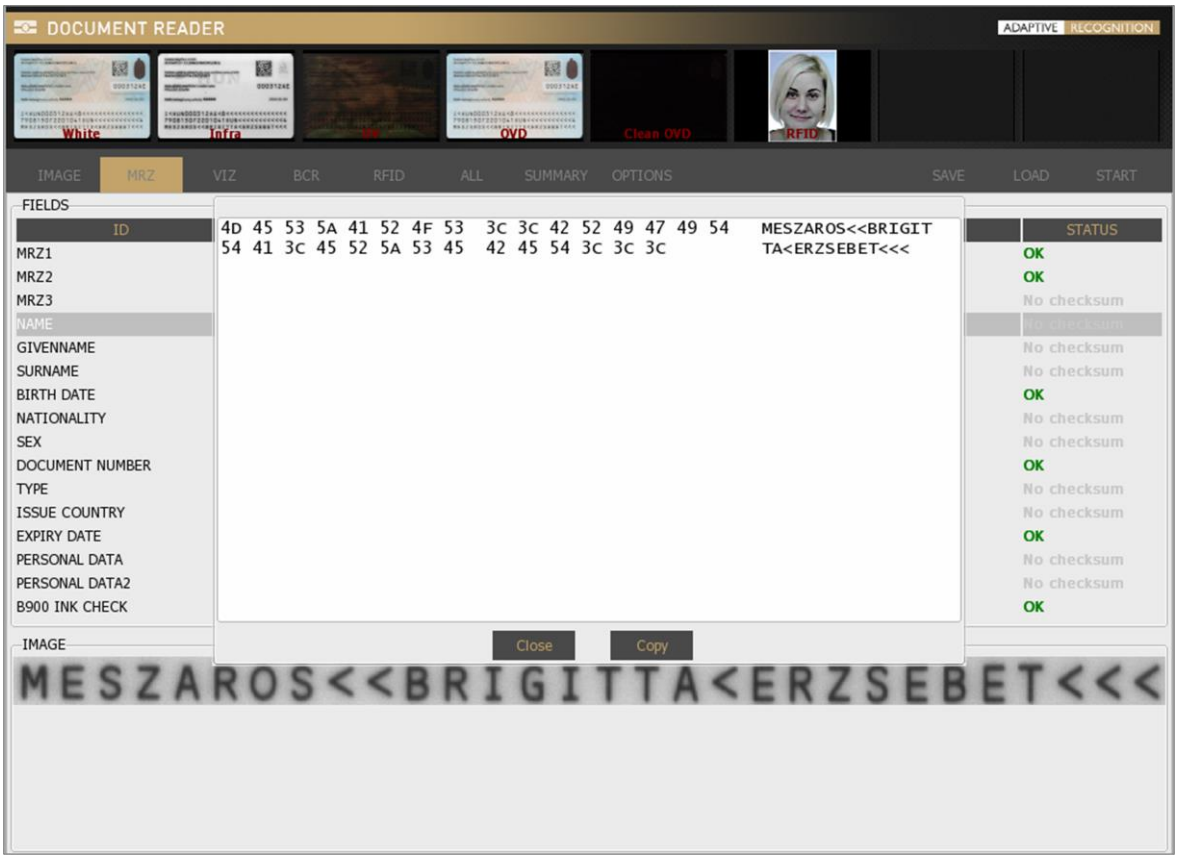


This tabulator option is displayed when OCR checkbox is filled in on the **OPTIONS / OCR** (vertical) layer and **MRZ ONLY** or **ADVANCED** mode is selected.



Note

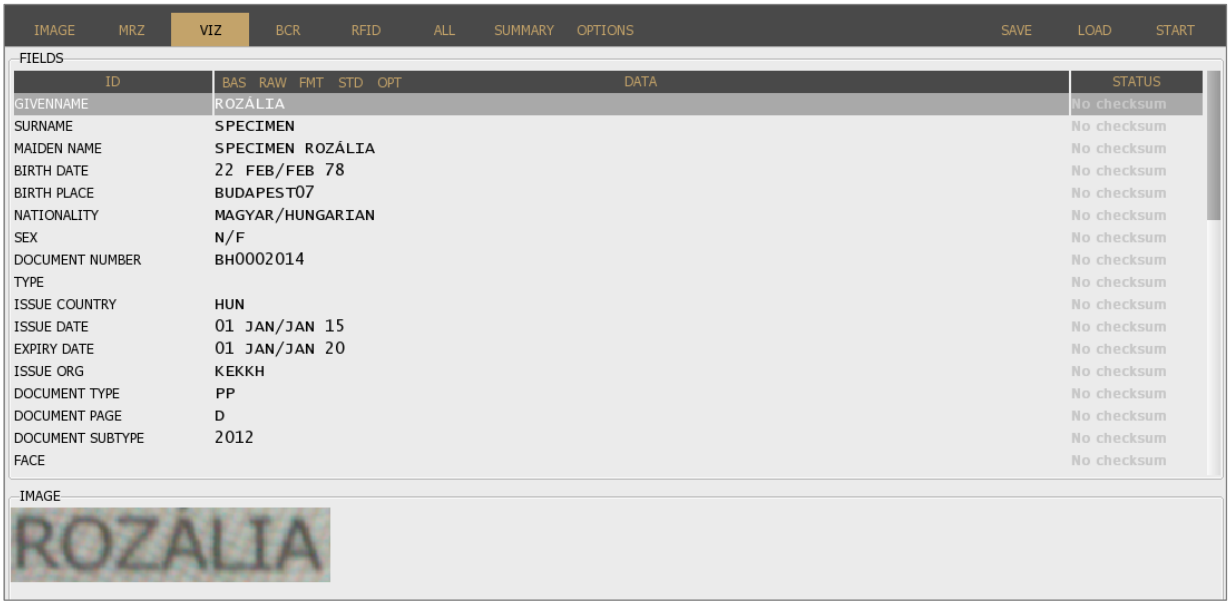
The extracted MRZ data fields can be copied to clipboard. Clipboard copy function can be activated by right clicking on any data line and in the pop-up window clicking on the **[Copy]** button.



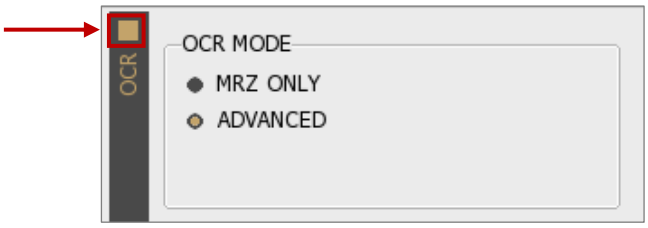
5.5.3. VIZ

Displays processed VIZ data and a photo of each field.

> **Note**
>
> The results of the authentication will be displayed in **VIZ** tab. The VIZ and AUTH results will be displayed only if you have special engine, that supports the scanned document.



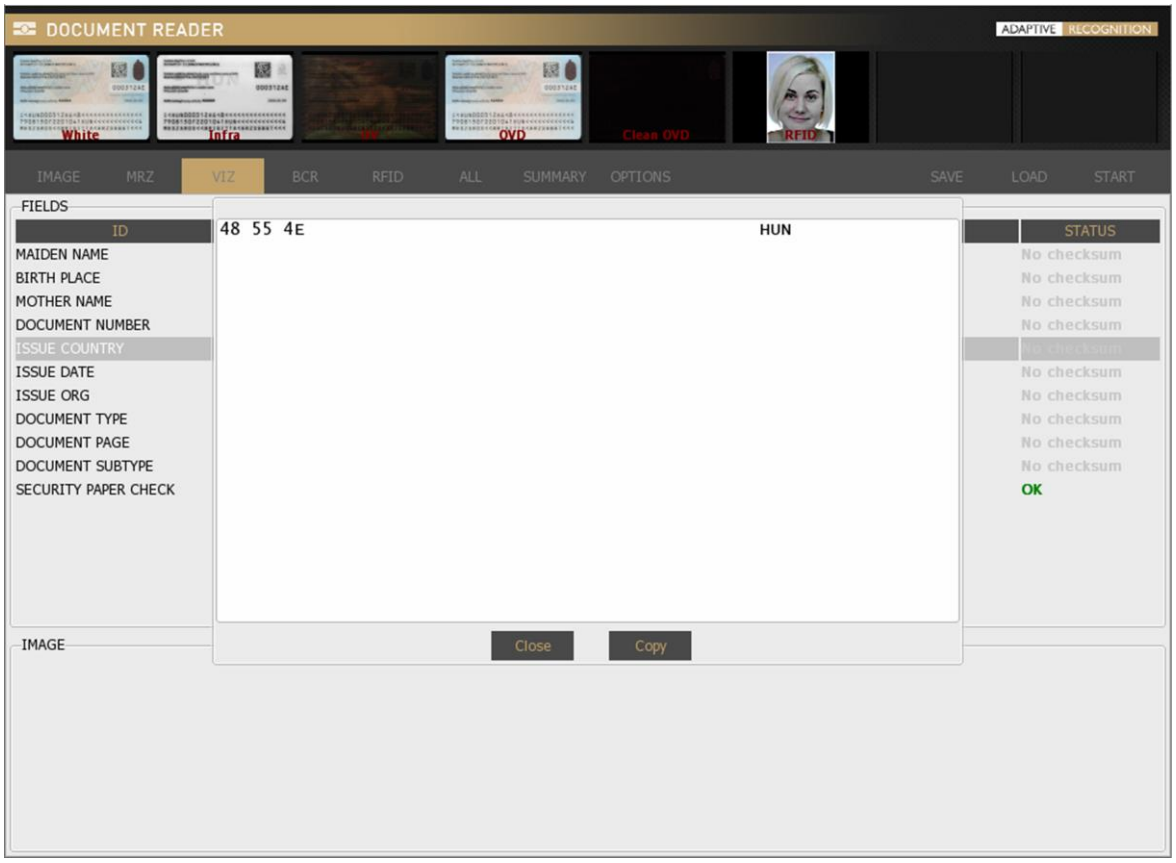
To see this tab, fill in OCR checkbox on the **OPTIONS / OCR** layer and select **ADVANCED** filter therefore MRZ and VIZ tabs are enabled.



Select VIEW DETAILED RESULT filter to review formatted data. Choose format in the header of the **DATA** column.

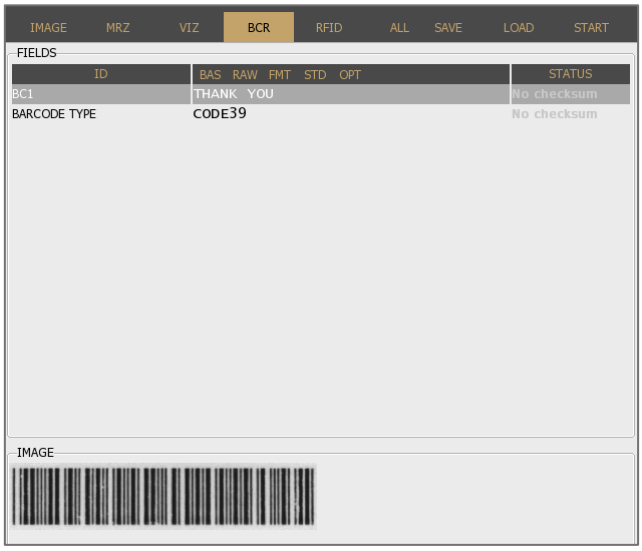
Note

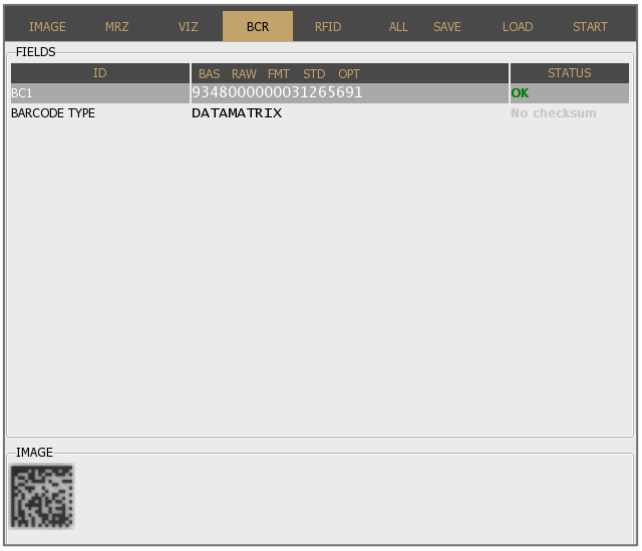
The extracted VIZ data fields can be copied to clipboard. Clipboard copy function can be activated by right clicking on any data line and in the pop-up window clicking on the **[Copy]** button.



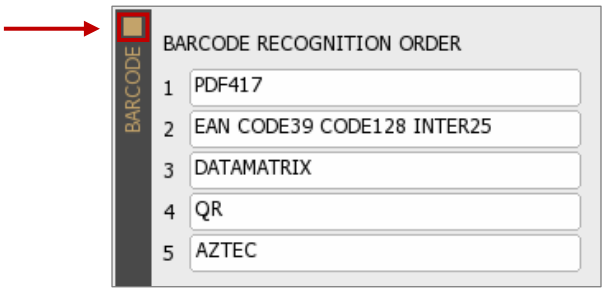
5.5.4. BCR

BCR displays barcode data and a photo of the barcode itself.





To see this option, enable barcode recognition on **OPTIONS / BARCODE** layer by filling in the checkbox on the vertical layer.

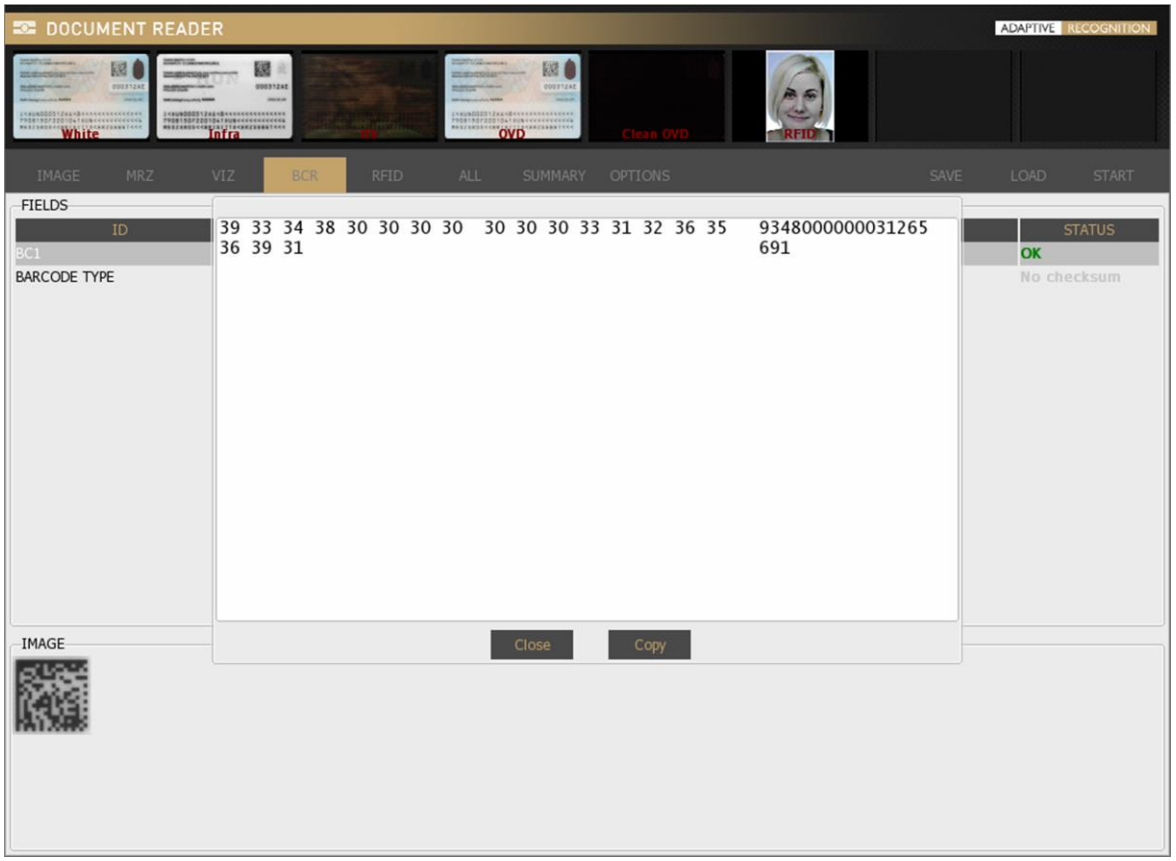


Note

For more information on customizing the barcode settings, see Barcode chapter.

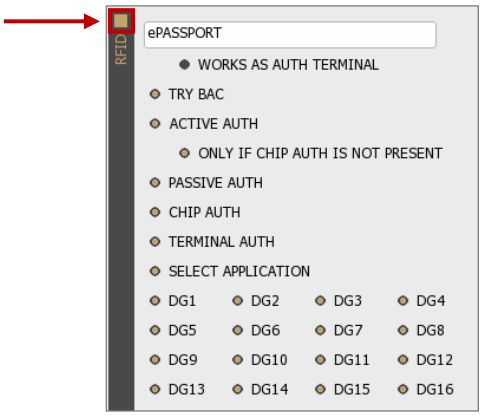
Note

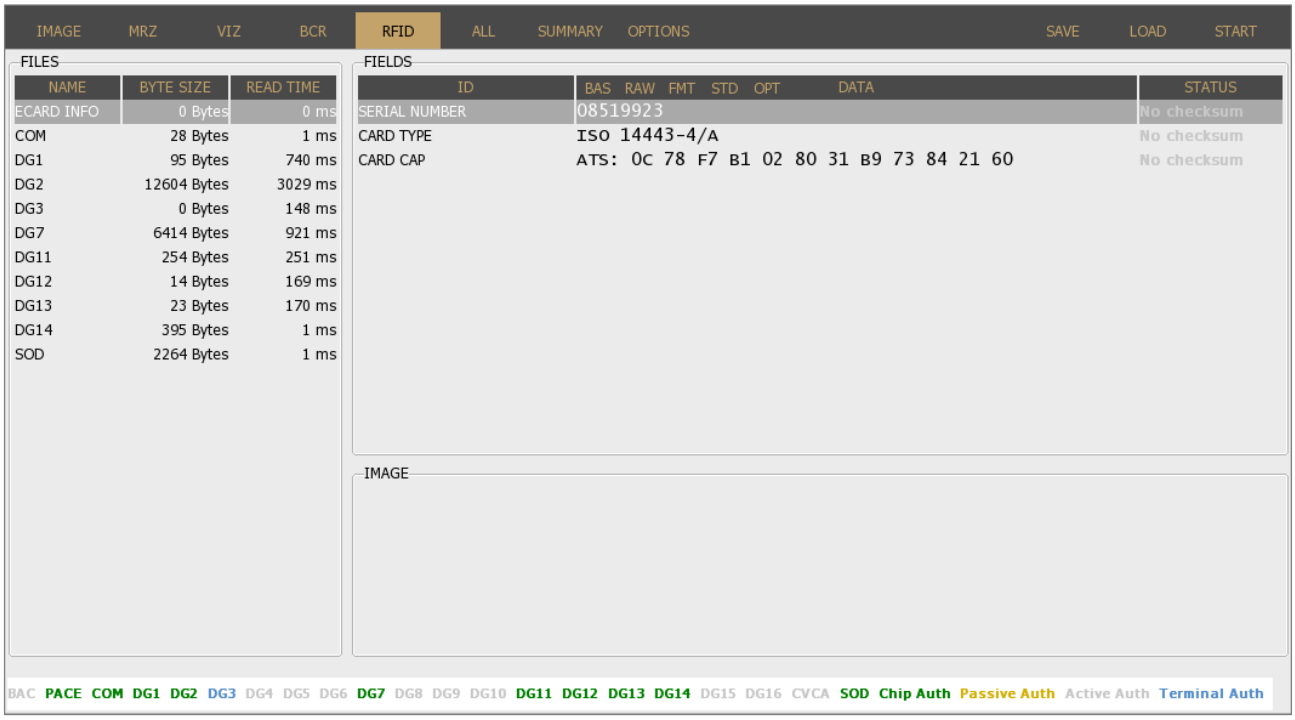
The extracted barcode data fields can be copied to clipboard. Clipboard copy function can be activated by right clicking on any data line and in the pop-up window clicking on the **[Copy]** button.



5.5.5. RFID

Displays RFID chip data. To see this option, enable RFID reading in **OPTIONS** by filling in the checkbox of the **RFID** vertical layer.



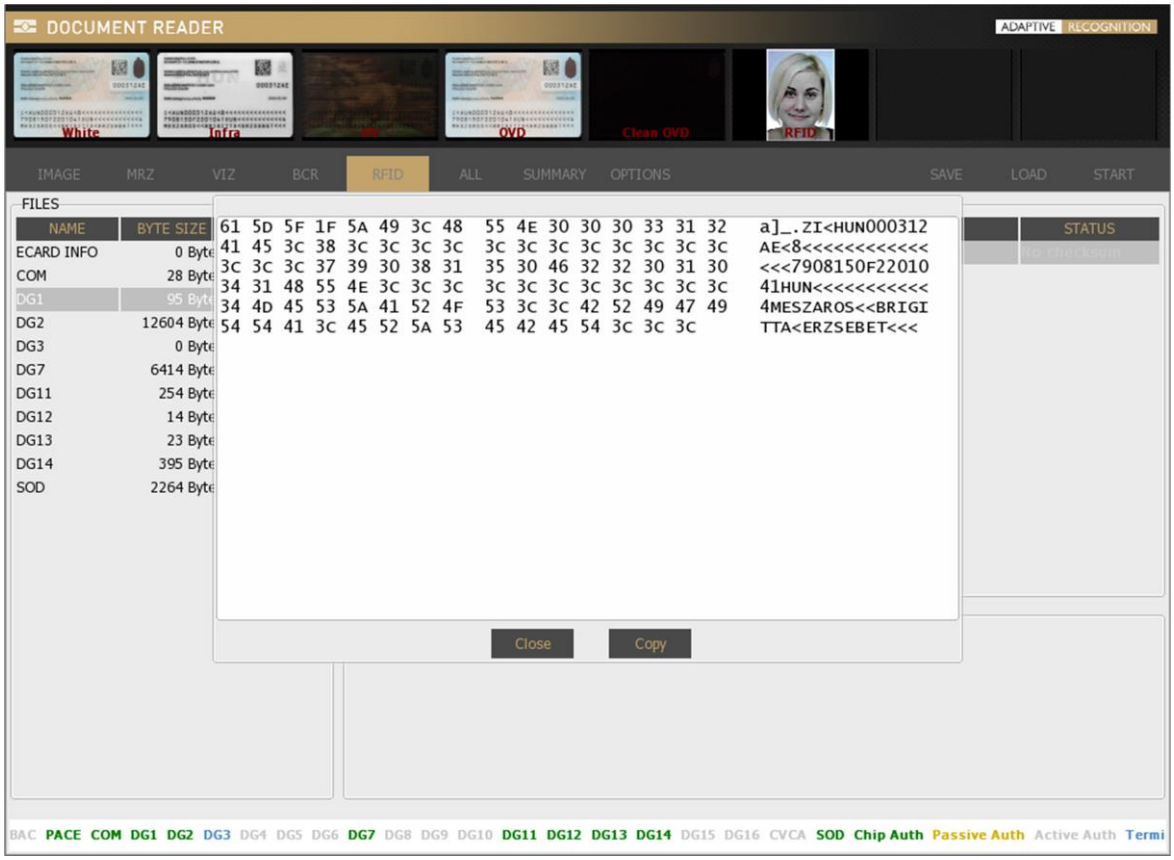


Note

RFID function turns off automatically, if there is no RFID reader module built in the device.

Note

The extracted RFID data fields can be copied to clipboard. Clipboard copy function can be activated by right clicking on any data line and in the pop-up window clicking on the **[Copy]** button.

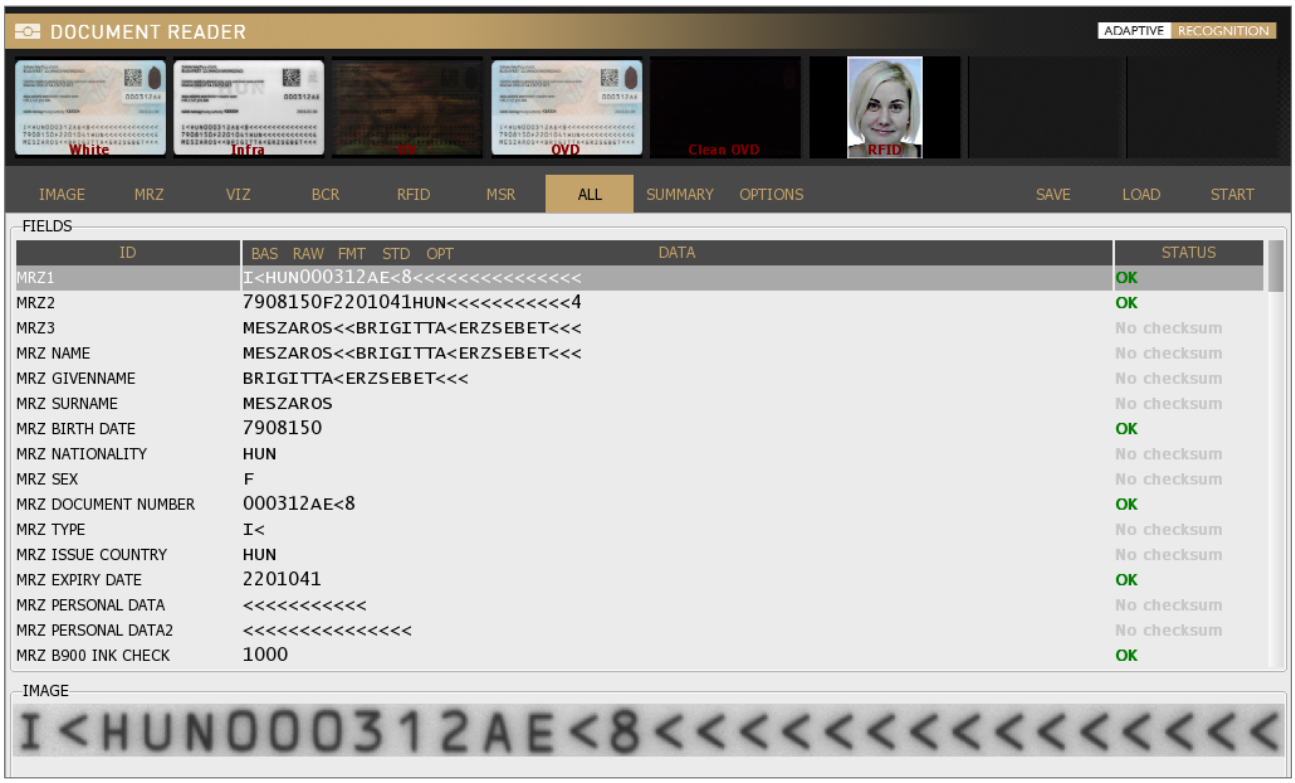


Note

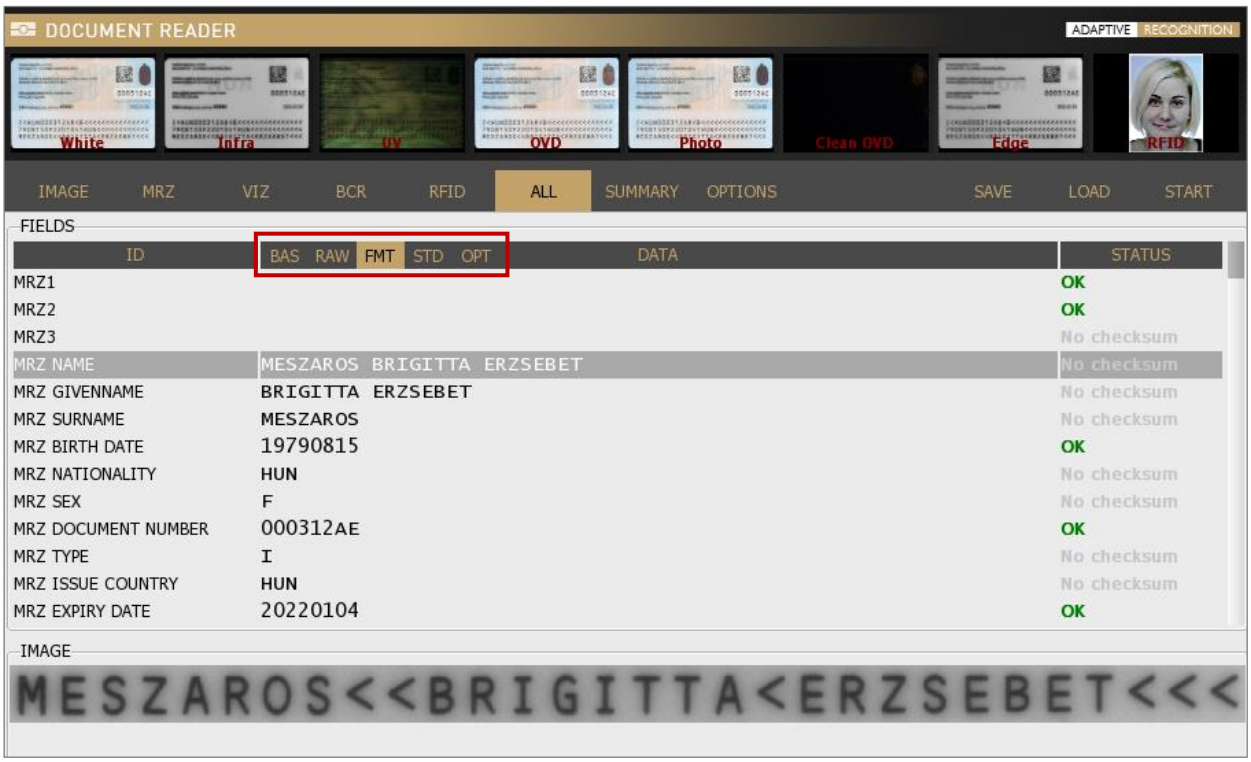
For more information on customizing the settings of the RFID reading, see RFID chapter.

5.5.6. ALL

Displays all available data retrieved from the document.

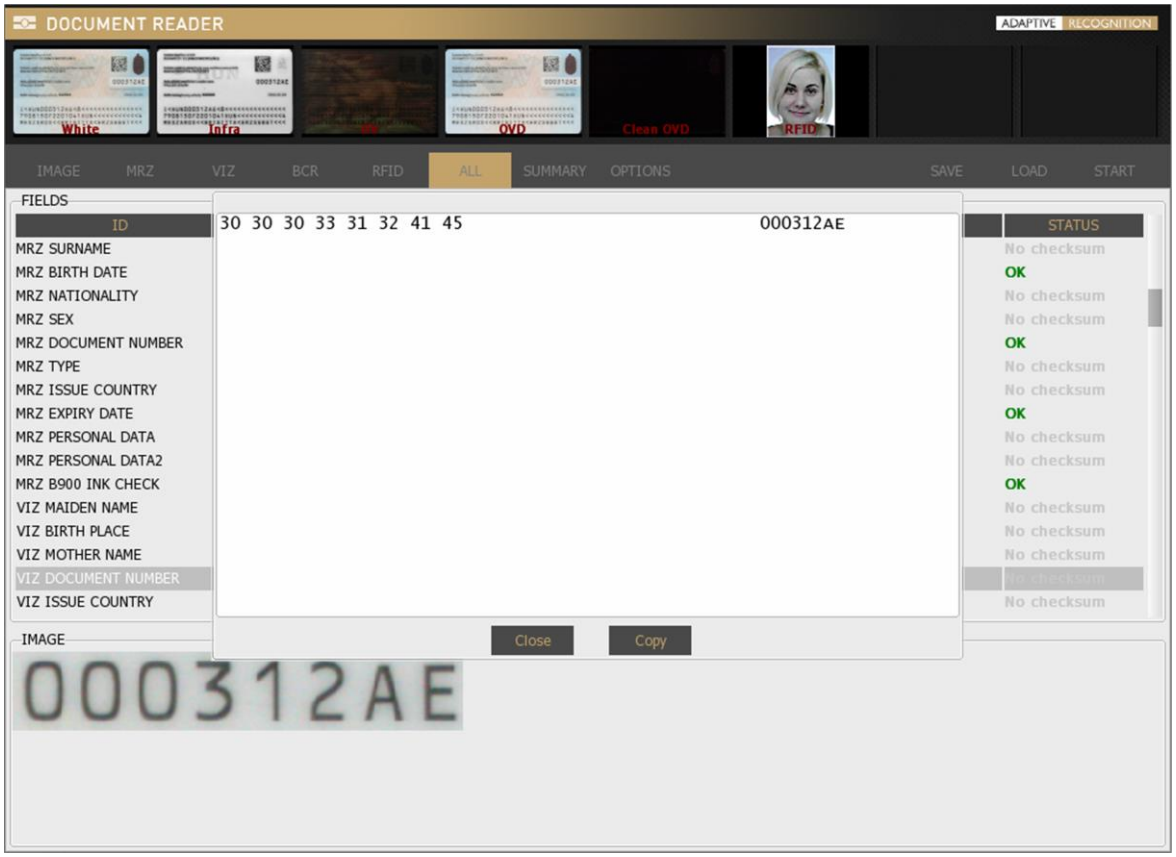


Select VIEW DETAILED RESULT filter to review formatted data. Choose format in the header of the **DATA** column.



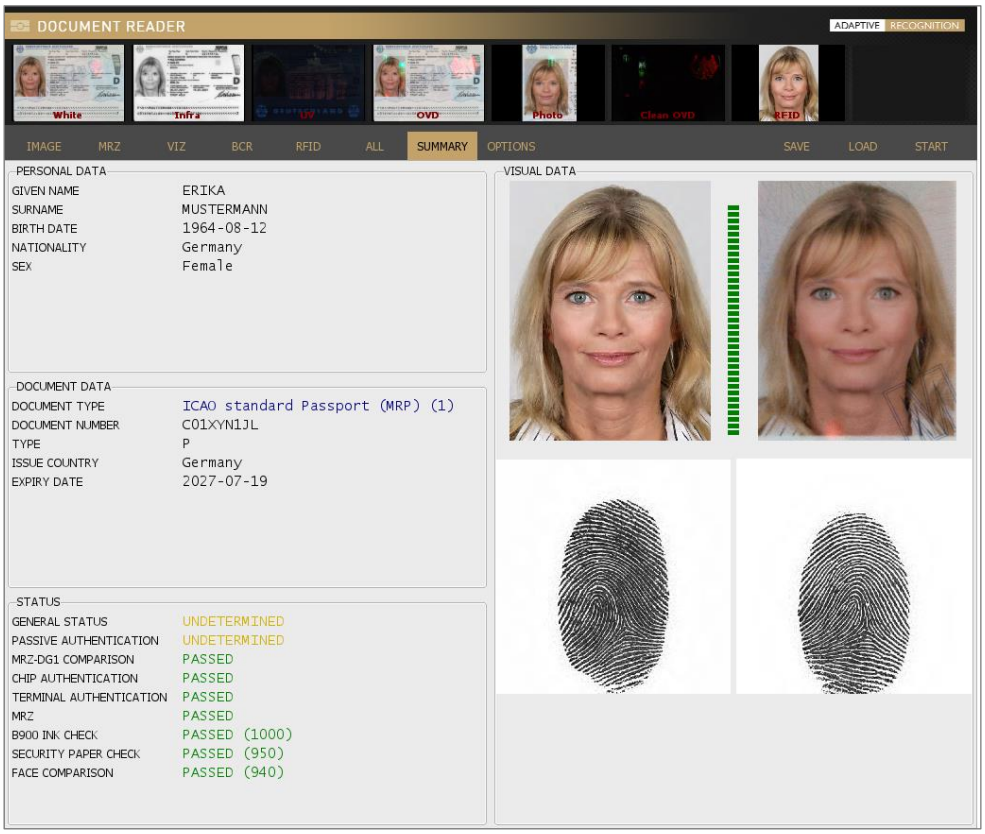
Note

The extracted data fields displayed in the **ALL** tab can be copied to clipboard. Clipboard copy function can be activated by right clicking on any data line and in the pop-up window clicking on the **[Copy]** button.



5.5.7. SUMMARY

Brief summary of the personal data, document data and the results of the security crosschecks. Face compare result is also displayed in the **SUMMARY** tab.



5.5.8. OPTIONS

Customize application properties, lights, logs and much more on the **OPTIONS** tab. For more details, please check the OPTIONS chapter.

5.5.9. SAVE

After a reading process, you have the option to save the given document. By default, the software compresses all available images and corresponding data into one **ZIP**, **PDF**, **XML**, **CSV** or **ECZ** file that can be saved to a custom location.

> **Note**
>
> The application is able to save encrypted ZIP (ECZ) file. Such files can be decrypted if the appropriate private key is available. Not recommended for personal use.
> For more information on encrypted save, see the Encrypted Saving chapter.

5.5.10. LOAD

Load scanned documents, including images illuminated by various light sources, as well as corresponding data.

> Note
>
> This functionality is supported only for **.zip files** that have been saved earlier by ADAPTIVE RECOGNITION passport reader software.

5.5.11. CONNECT/START

Use the **[CONNECT]** button to access the selected document reader device or click on **[START]** to begin the scanning process after the device is connected successfully.

> Note
>
> When reading contact chip card, click on **[START]** to begin the scanning process.

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

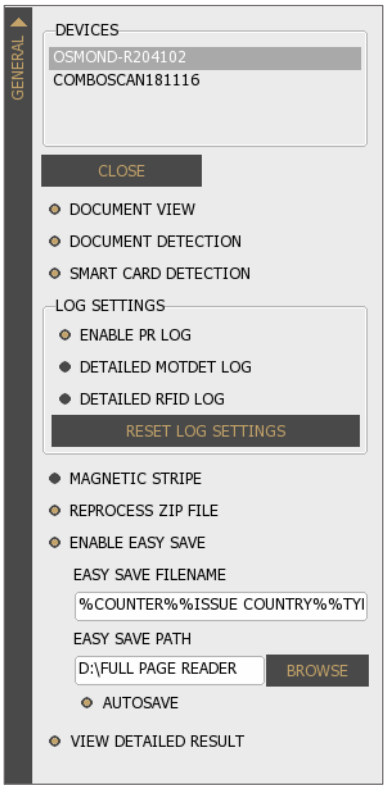
5.6. OPTIONS

5.6.1. GENERAL

DEVICES

OPTIONS > GENERAL > DEVICES

You can see the list of document scanners connected to your computer.



> **Note**
>
> You can work with only one device at a time. Also, you can navigate across devices by clicking on the chosen one.

DOCUMENT VIEW

OPTIONS > GENERAL > DOCUMENT VIEW

It crops and rotates documents into upright position.

> **Note**
>
> Automatic document rotation is performed properly if the **DOCUMENT VIEW** mode and **ADVANCED OCR MODE** are both selected before the starting of the scanning process.

DOCUMENT DETECTION

OPTIONS > GENERAL > DOCUMENT DETECTION

Enable/Disable the automatic document presence detection mode (motion detection). This feature senses documents placed on the scanner glass surface. Whenever a document is present, the software scans images of the document, as configured in **OPTIONS / CAPTURE**.

SMART CARD DETECTION

OPTIONS > GENERAL > SMART CARD DETECTION

Devices equipped with smart card reader can execute automatic detection of smart cards when they are inserted into the smart card reader by enabling the **SMART CARD DETECTION** option.

> Note
>
> **SMART CARD DETECTION** is not performed when RFID reading is disabled.

LOG SETTINGS

OPTIONS > GENERAL > LOG SETTINGS

The Full Page Reader application is equipped with a configurable logging feature to support any troubleshooting activities with ADAPTIVE RECOGNITION support team. By enabling different log options, you can include various events of the passport reader software in the log files.

> Note
>
> Enabling detailed RFID logging is increasing processing time.

- **ENABLE PR LOG**: Enable/Disable logging
- **DETAILED MOTDET LOG**: Enable/Disable detailed logs for motion detection
- **DETAILED RFID LOG**: Enable/Disable detailed logs for RFID communication

> Hint
>
> Your log file is located at:
>
> Windows: `c:\ProgramData\gx\pr\pr.log`
> Linux: `~/tmp/pr.log`

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

REPROCESS ZIP FILE

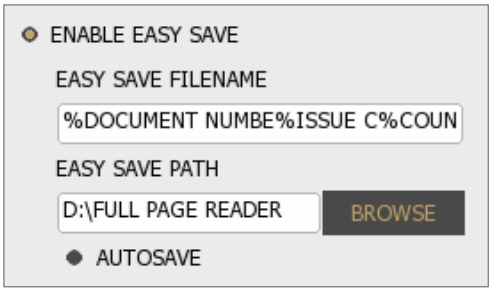
OPTIONS > GENERAL > REPROCESS ZIP FILE

When loading **.zip** files saved earlier, the program either process them again with your current software version (**REPROCESS ZIP FILE** is enabled) or displays the original saved data (**REPROCESS ZIP FILE** is disabled). This option enables to perform OCR process and optical authentications using the current FPR application setup.

ENABLE EASY SAVE

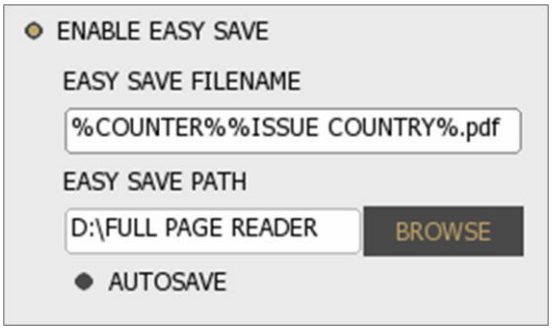
OPTIONS > GENERAL > ENABLE EASY SAVE

The easy save option is designed to make frequent document saving simpler. Just select **ENABLE EASY SAVE**, then set the **filename** and **path**. Afterwards there is no need to browse path and specify filename when saving **.zip** files: the software creates the filename automatically based on the configured template, then saves the .zip to the path specified.



Note

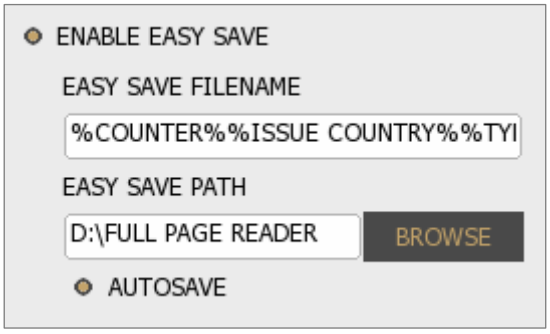
If the **filename** contains the extension, the program saves in the corresponding format (zip, pdf, xml, csv or ecz).



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

If you turn **AUTOSAVE** on, results of all scanning process will be saved automatically. By using this option, there is no need to click on the **[SAVE]** button anymore.

> **Note**
>
> When using easy save, determine the filename syntax and path before first scanning. This option will save every scanning into the same path.



Through easy save the ZIP files cannot only be saved to the local file system, but they can be sent to remote systems through **ftp**, **ftps**, **http**, **https**, **smtp** protocols. To use this option, the matching URL must be typed to the path (e.g., ftps://ftp.myserver.com/shares). Afterwards the user settings can be entered by pressing the settings button.

> **Note**
>
> The given password is not saved in the computer, you have to type it after every program launch.

> **Note**
>
> If you want to save encrypted files which can only be decoded in ADAPTIVE RECOGNITION's network, then, when saving the file select **.ecz** extension.
> For more information on encrypted autosave, see the Encrypted Autosave in Full Page Reader chapter.

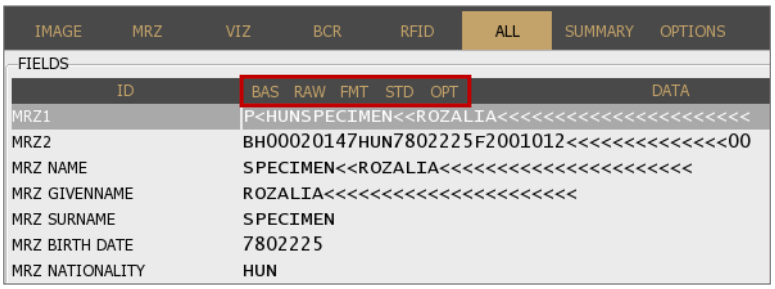
VIEW DETAILED RESULT

OPTIONS > GENERAL > VIEW DETAILED RESULT

Formatted data can be displayed on **MRZ**, **VIZ**, **BCR**, **RFID** and **ALL** tabs.

The following formatting types are available:

- Basic (**BAS**)
- Raw (**RAW**)
- Formatted (**FMT**)
- Standardized (**STD**)
- Optimal (**OPT**)

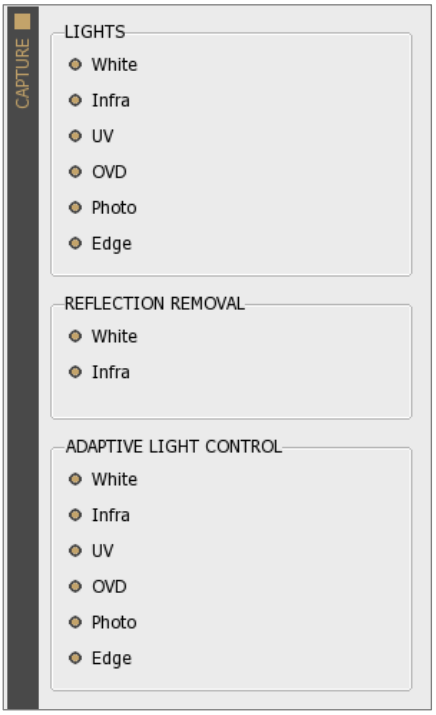


5.6.2. CAPTURE

1. LIGHTS

OPTIONS > CAPTURE > LIGHTS

The available lights can be checked at the **OPTIONS / CAPTURE / LIGHTS.**



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

- **White**

OPTIONS > CAPTURE > LIGHTS > WHITE

Enable **White** illumination by filling in the checkbox.

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**

OPTIONS > CAPTURE > LIGHTS > INFRA

Enable **Infra** illumination by filling in the checkbox.

The ICAO 9303 document specifies that for reading text and barcodes, images shall be scanned in infrared light (wavelength: 900 nm). In this illumination, the background patterns are not visible, so optical recognition algorithms provide better results.

- **UV**

OPTIONS > CAPTURE > LIGHTS > UV

Enable **UV** illumination by filling in the checkbox.

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.

- **OVD**

OPTIONS > CAPTURE > LIGHTS > OVD

Enable **OVD** illumination by filling in the checkbox.

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 **clean OVD** image. In the case of the latter one, just the hologram can be seen from the document.

OVD

Clean OVD

- **Photo**

OPTIONS > CAPTURE > LIGHTS > PHOTO

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

Enable **Photo** light by filling in the checkbox at **OPTIONS / CAPTURE / LIGHTS.**

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.

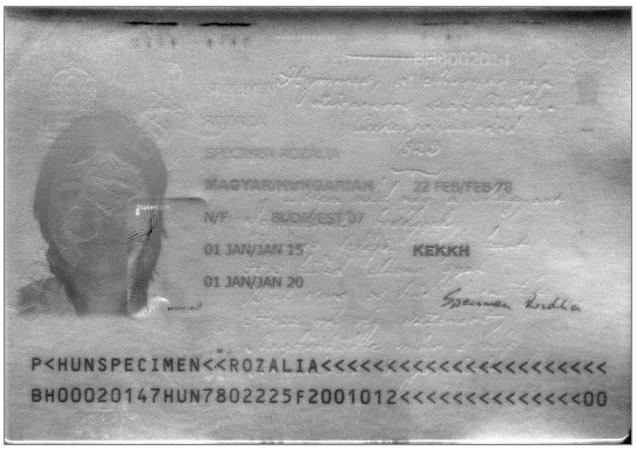
Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

- **Edge**

OPTIONS > CAPTURE > LIGHTS > EDGE LIGHT

Enable **Edge** light by filling in the checkbox at **OPTIONS / CAPTURE / LIGHTS.**

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.



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

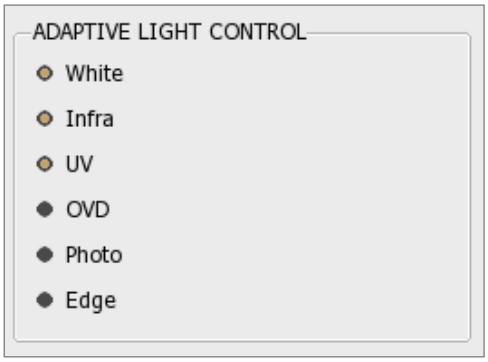
Enable **RR** on infra images by filling in the checkbox.

3. ADAPTIVE LIGHT CONTROL

OPTIONS > CAPTURE > ADAPTIVE LIGHT CONTROL

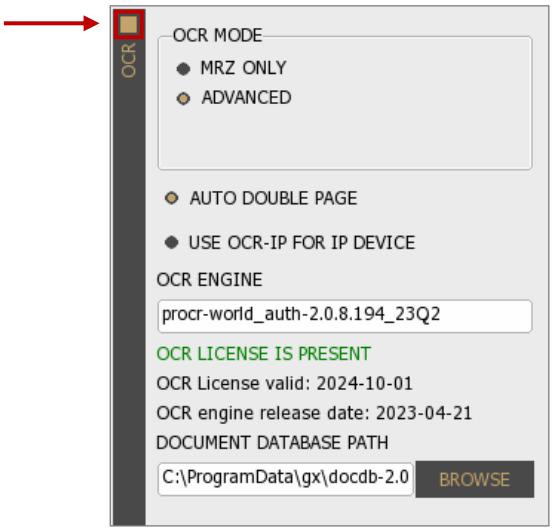
ADAPTIVE RECOGNITION's **ADAPTIVE LIGHT CONTROL** feature compensates for external light interference and make routine operation independent of the environment. In order to use this feature, fill in the checkbox(es) you wish to apply before starting the illumination process.

> **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).

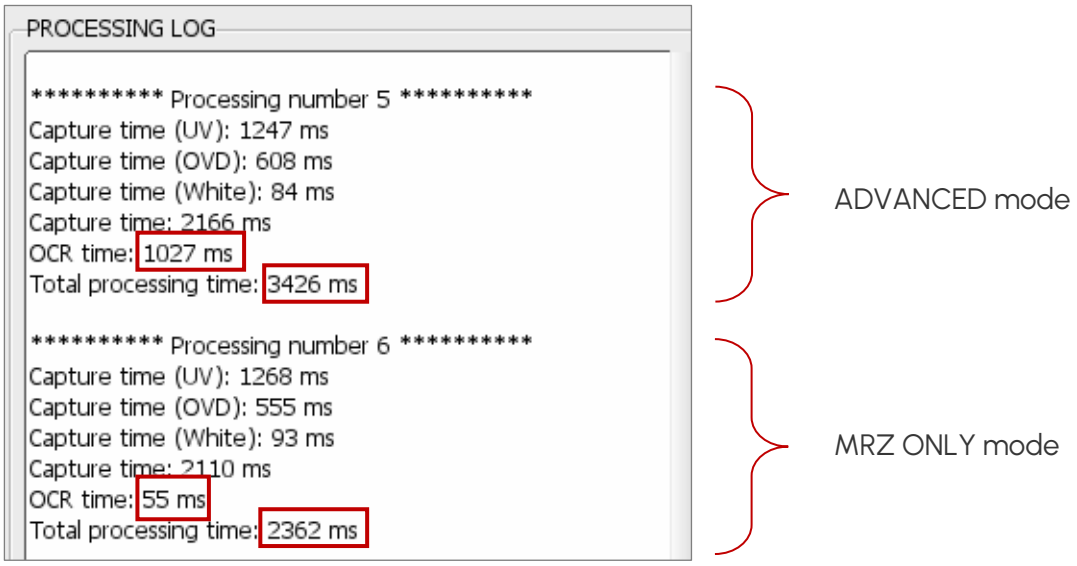
- **ADVANCED**

  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

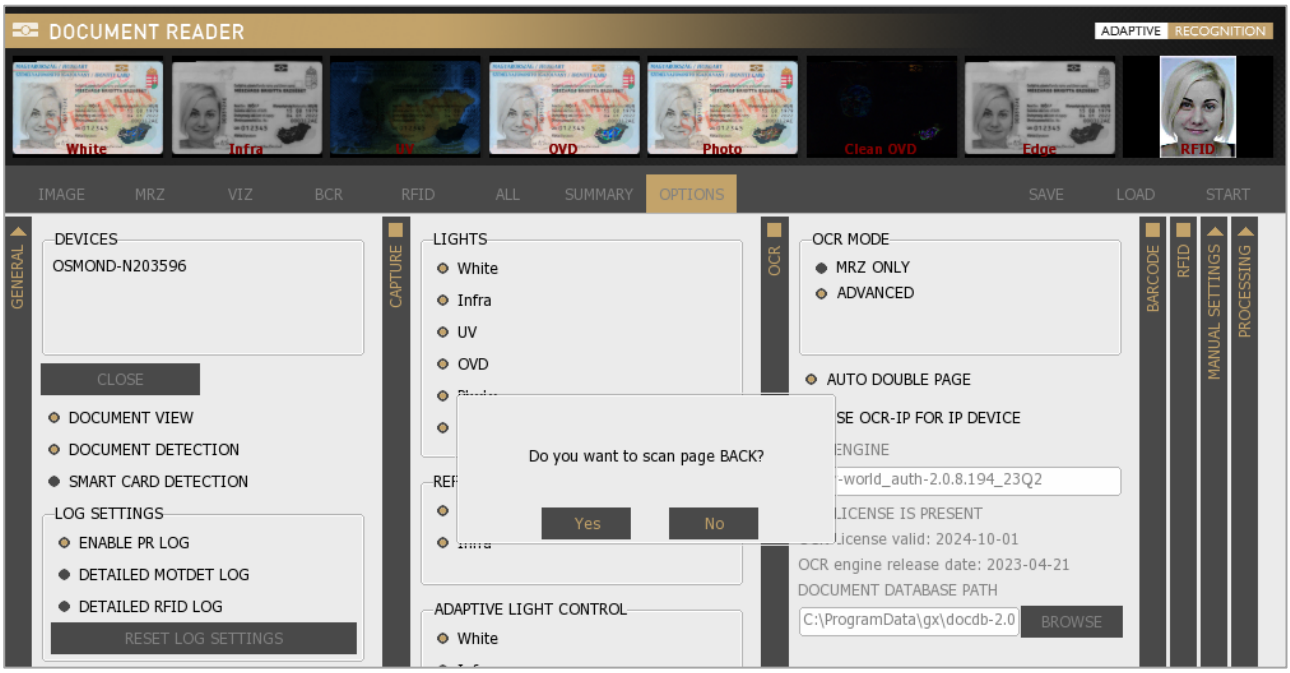
> **Note**
>
> **ADVANCED** mode is increasing processing time.



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.



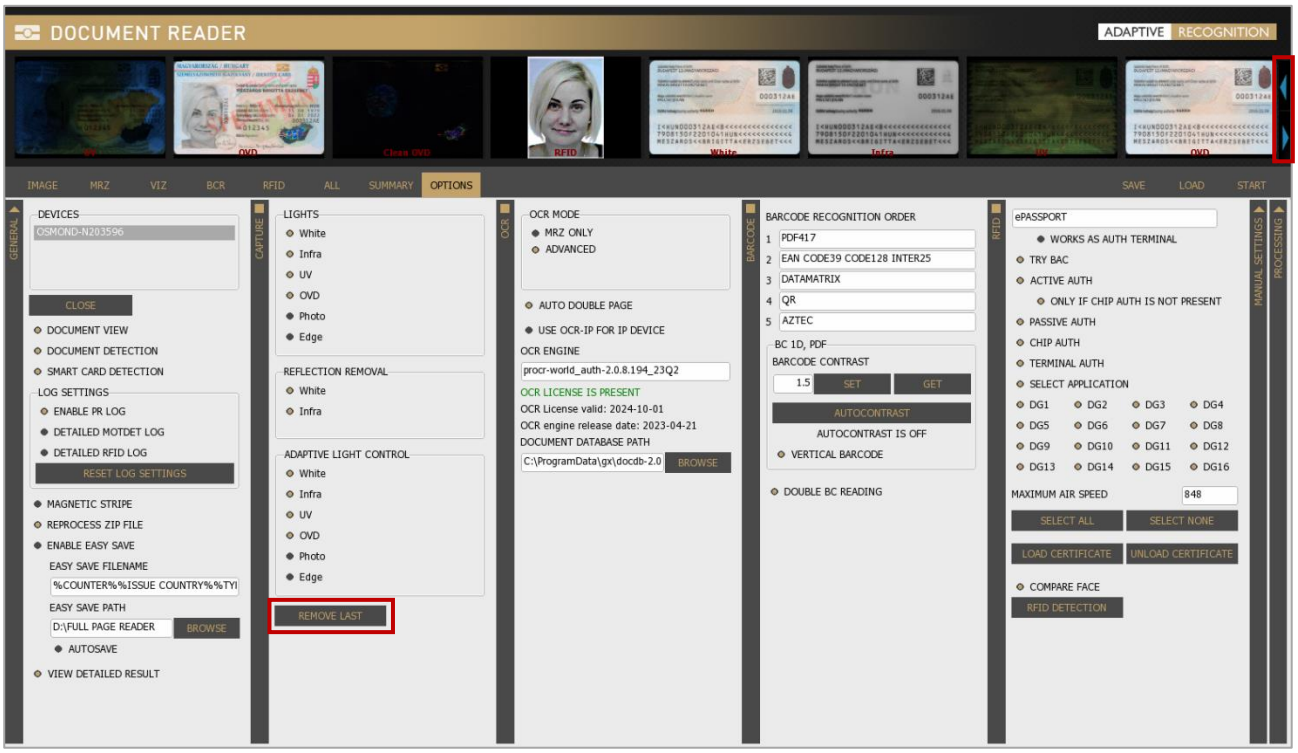
When the scanning of both sides is finished, use the blue colored left and right arrows to navigate among the scanned images.

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.



Note

AUTO DOUBLE PAGE function only operates automatically, on the condition of the document being recognized by the VIZ OCR engine. For more information on VIZ OCR engine, see ADAPTIVE RECOGNITION website.

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.

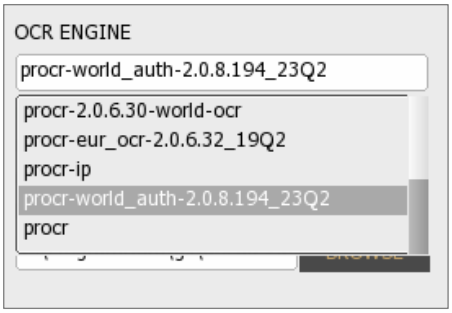
4. OCR ENGINE

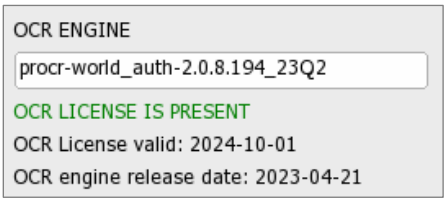
OPTIONS > OCR > OCR ENGINE

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.

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

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.

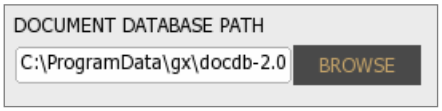
> **Note**
>
> For availability and more information on OCR engines and software licenses, please contact your ADAPTIVE RECOGNITION sales representative.

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

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.



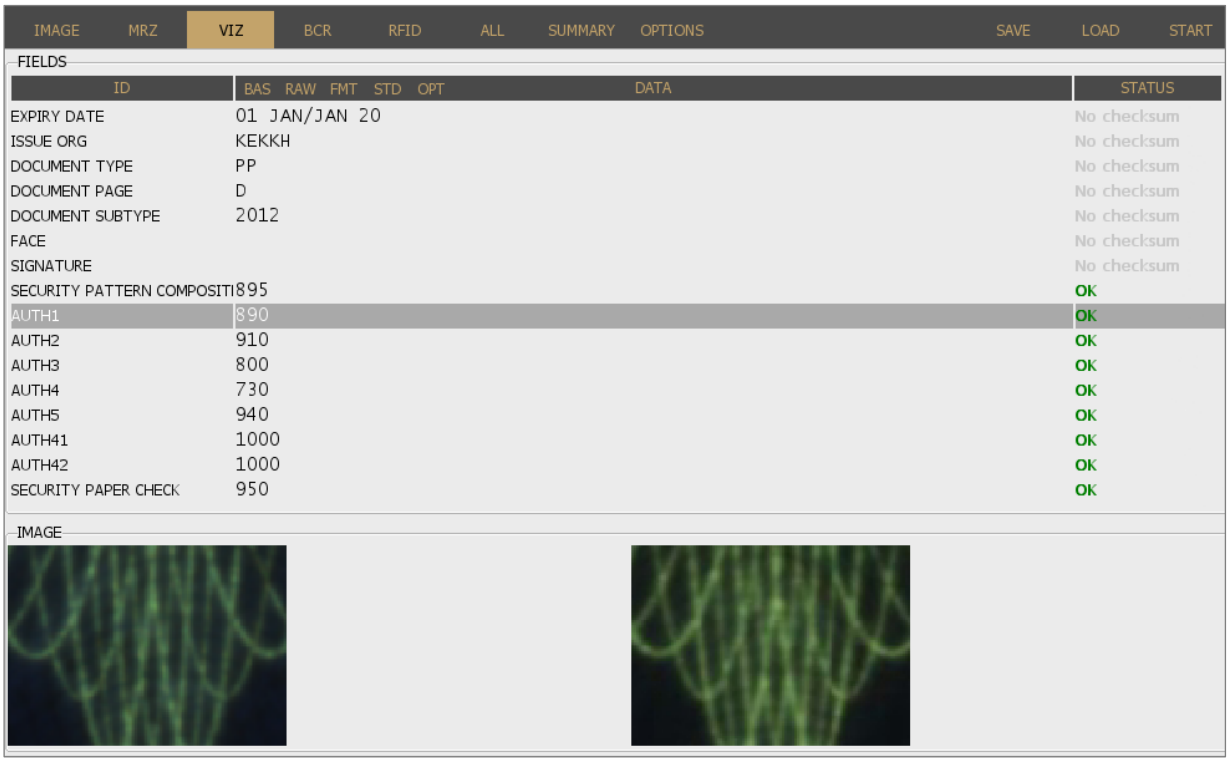
The values of the AUTH fields are in thousandths.

The limits are the following:

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

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

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



Scanned image

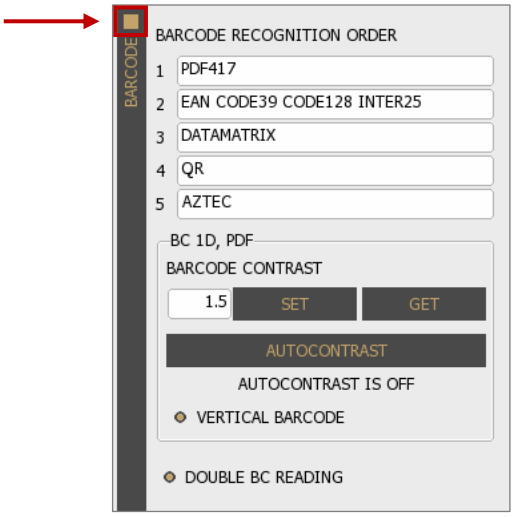
Reference image

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.

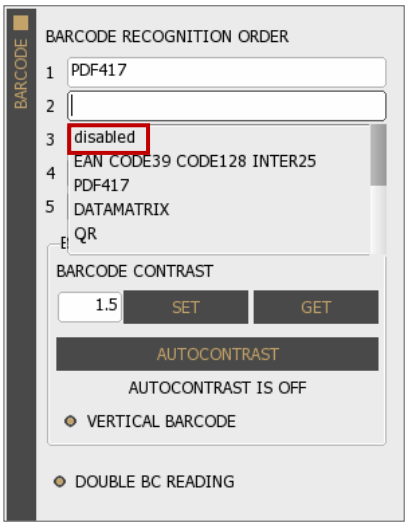


> **Note**
>
> If you do not need barcode recognition, disable this option to speed up processing.

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.

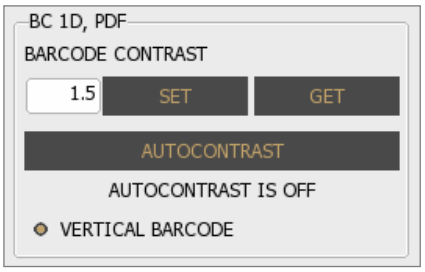
2. BARCODE CONTRAST

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**

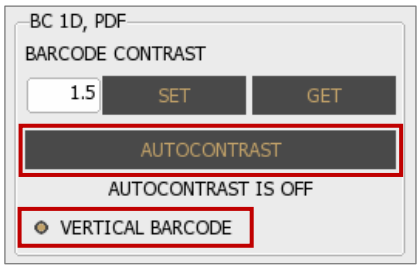


> **Hint**
>
> By clicking on the **[GET]** button, you will get the current value.

> **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.

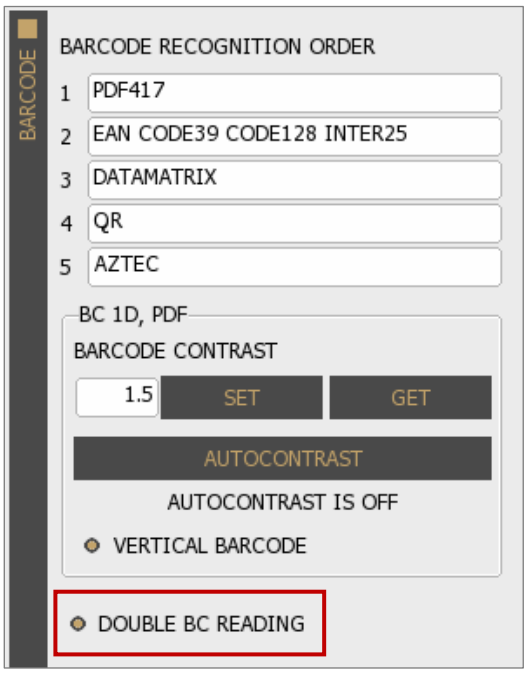
> **Note**
>
> Enable this function to maximize the efficiency of barcode reading.

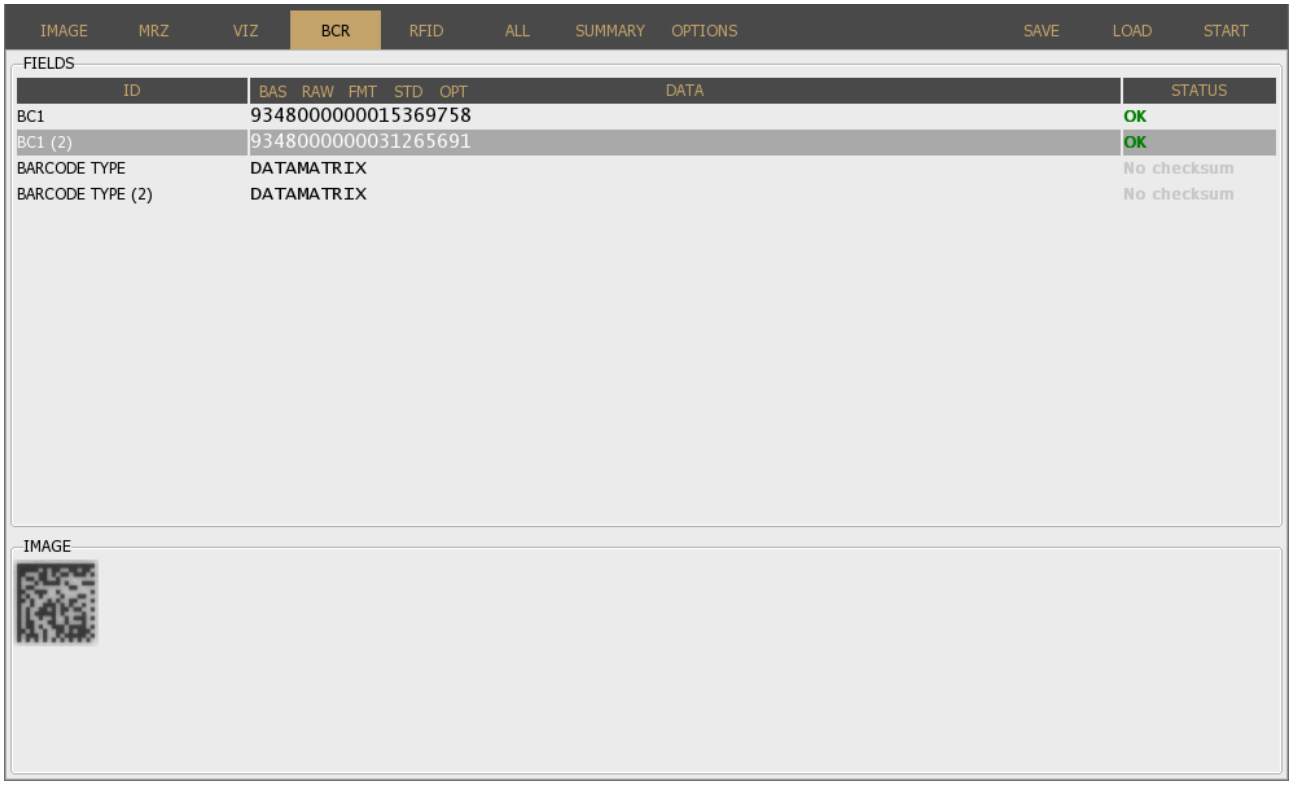
Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

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.



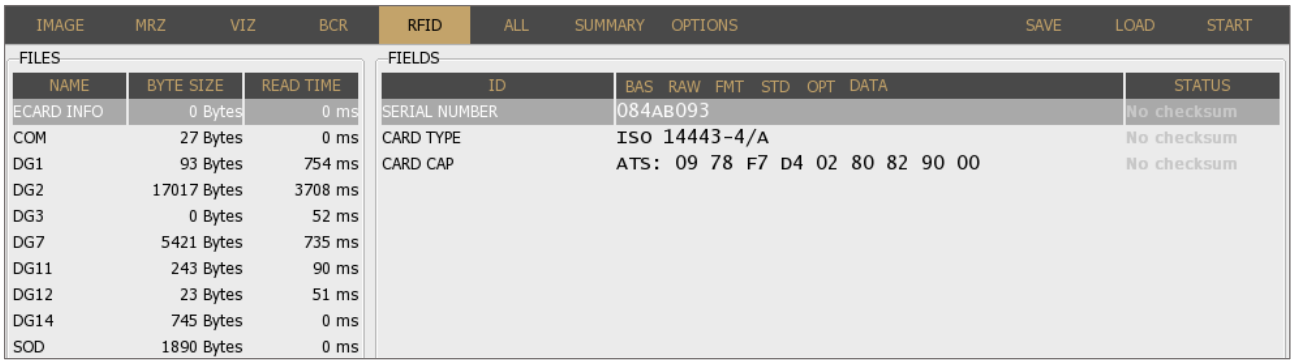


5.6.5. RFID

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.

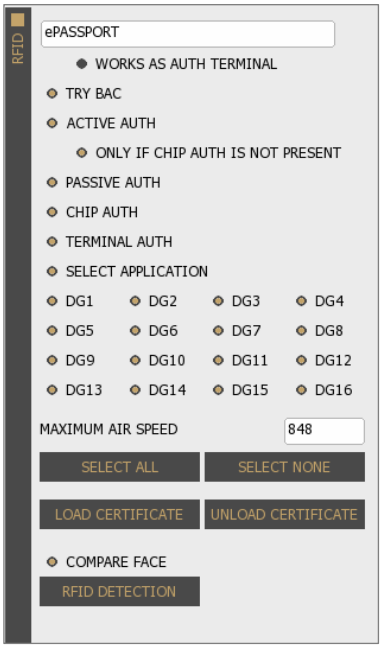
> **Note**
>
> In the case of **contact chip reading**, the extracted data is displayed in the **RFID** tab.



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

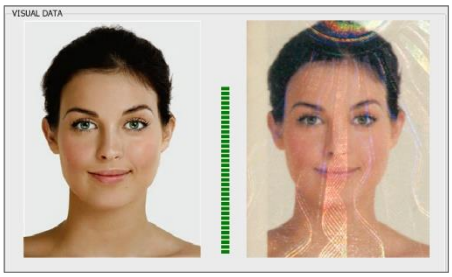
Browse and select your certification file that enables you to run RFID security mechanisms (PA and TA).

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

11. COMPARE FACE

OPTIONS > RFID > COMPARE FACE

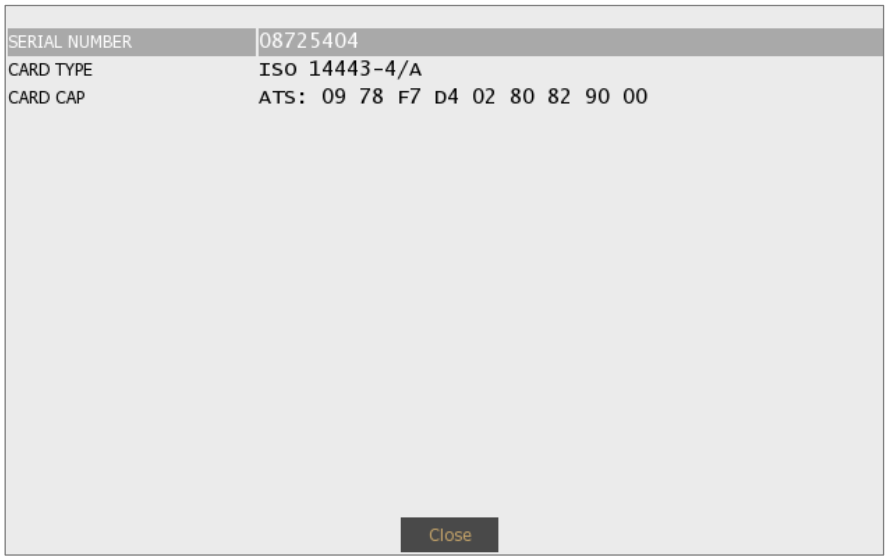
Enable/Disable comparing the face photo stored in chip against the one printed on the data page.



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

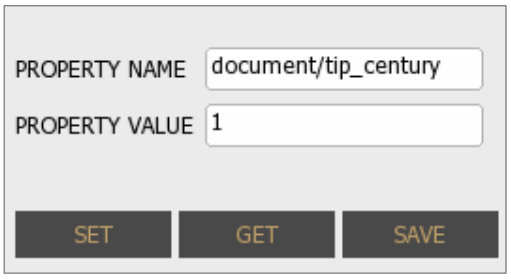
OPTIONS > MANUAL SETTINGS > PROPERTY NAME

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.

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

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

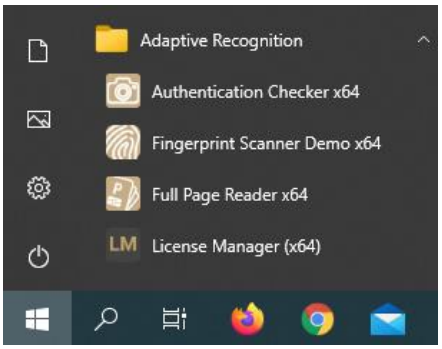
The **PROCESSING LOG** displays the main events of each document reading process.

5.7. FAQ

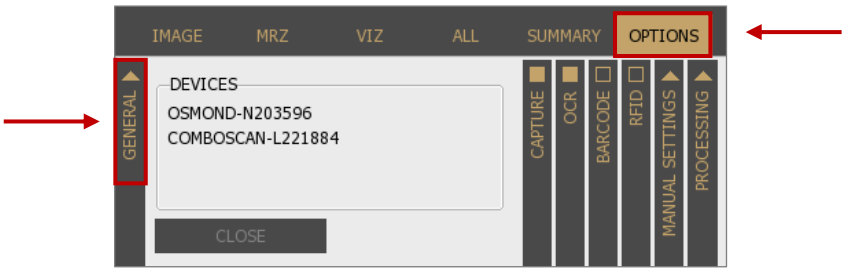
5.7.1. BASICS

How to connect reader before scanning?

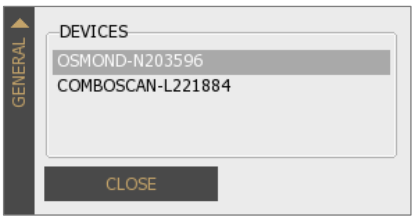
1. Open Full Page Reader (FPR) app.



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

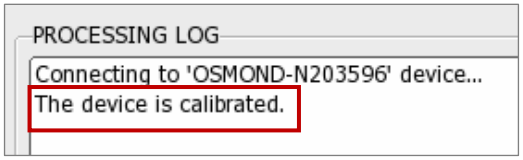


3. Connect reader to your system to gain access its features by
   a. clicking on the **[CONNECT]** button or
   b. clicking on the selected reader in the **DEVICES** list.



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

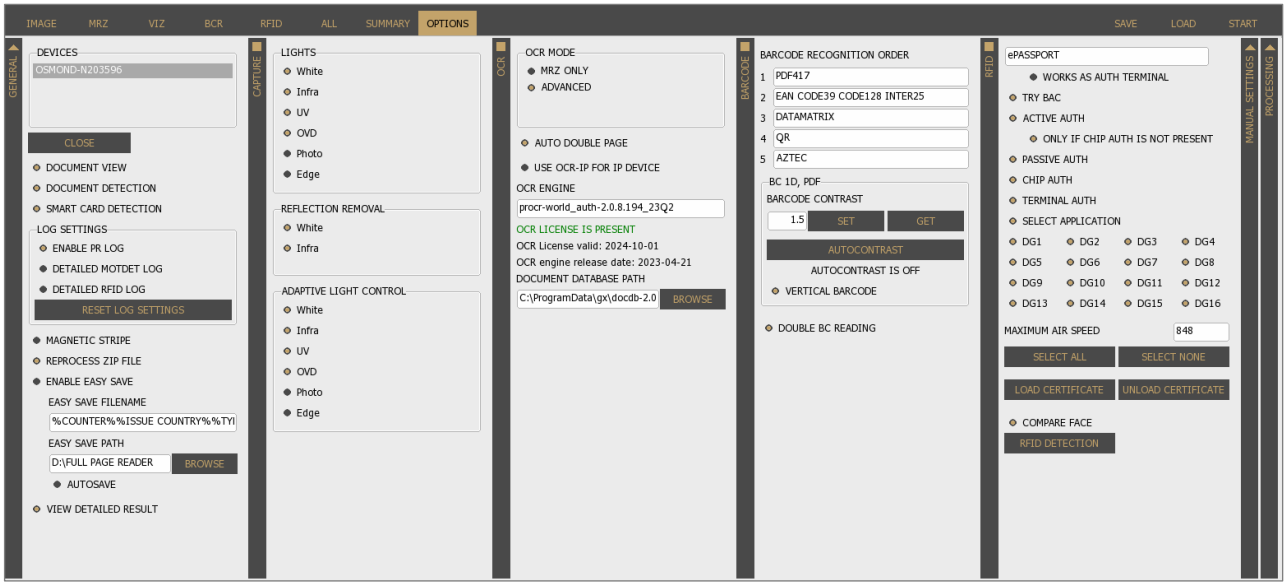
   If you get the "**The device is calibrated**." message, your reader is ready to use.



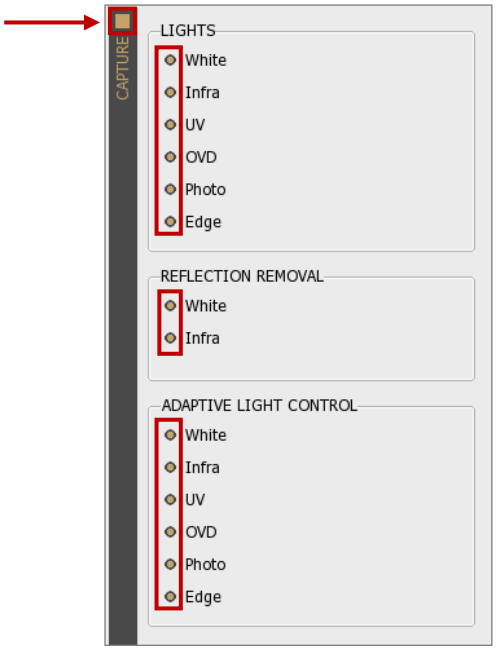
5.7.2. SCANNING

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.

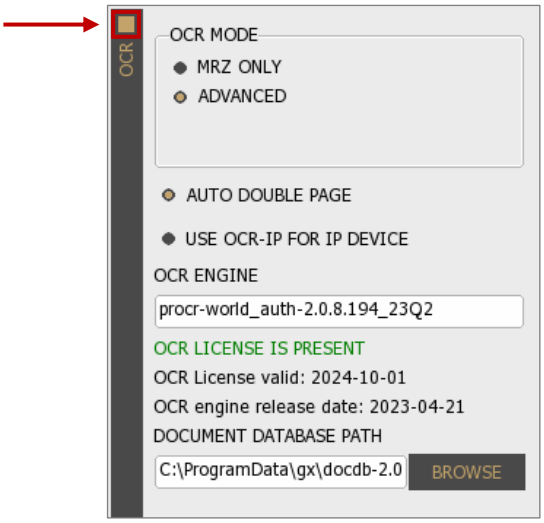


a. Activate **CAPTURE** layer for scanning documents by filling in the checkbox and set the illumination types you wish to apply.

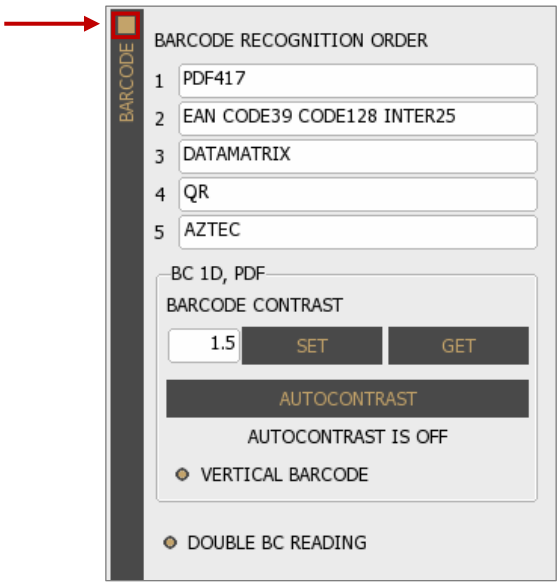


b. Activate **OCR** layer by filling in the checkbox and select your **OCR ENGINE** for performing character recognition.

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

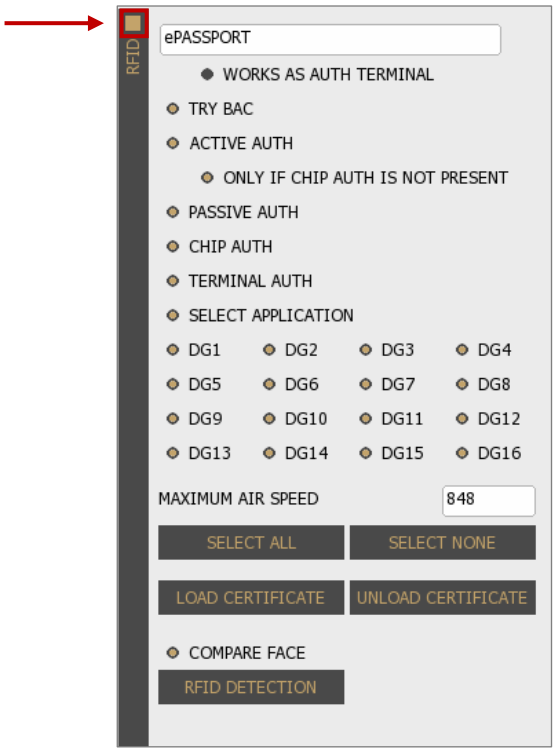


c. Activate **BARCODE** layer by filling in the checkbox to read barcode(s) from documents. If you expect different barcode types, you can set an order for faster process time.



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

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.

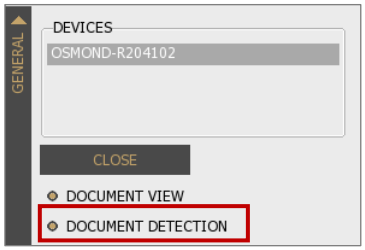


3. Start scanning by pressing the **[START]** button or use **DOCUMENT DETECTION**.

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

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.

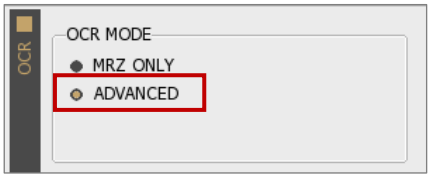


How to crop and rotate document?

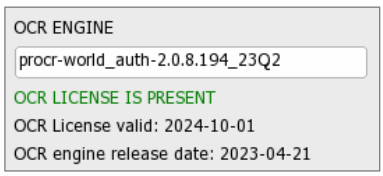
Select **DOCUMENT VIEW** option before the starting of the scanning process on **OPTIONS / GENERAL** layer to crop and rotate documents into upright position.

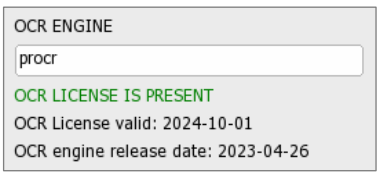
How to read VIZ fields?

- 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.

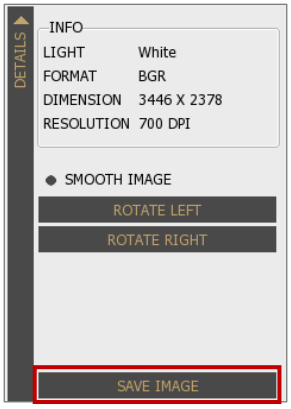
5.7.3. SAVE, LOAD, REPROCESS

How to save a scanning?

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

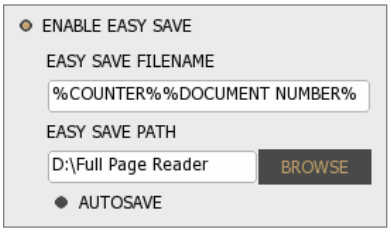
   a. Click on **[SAVE]** and browse the path as well as specify the filename to finish the saving process.

   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.

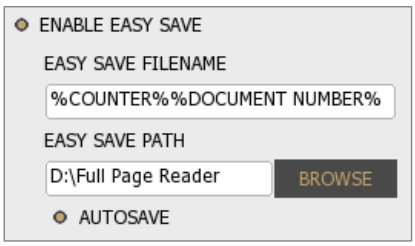


> **Note**
>
> At the first saving, you have to browse the path and define the filename, if the **EASY SAVE PATH** is not specified.

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

Important!

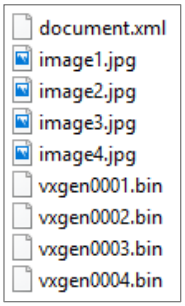
If the **EASY SAVE PATH** is not specified, the automatic saving is not performed.



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.

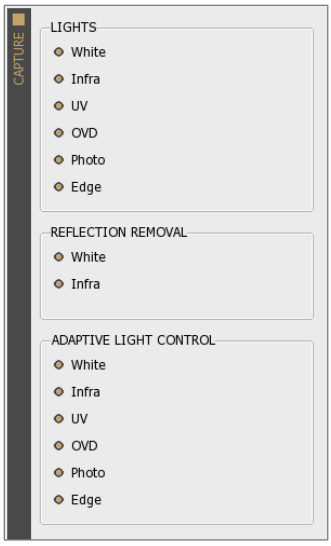
The difference between the two is that with the **LOAD** you get the original saved data in the app (you do not have to check the ZIP file) and with the **REPROCESS ZIP FILE** the saved data is processed again according to the actual or selected engine.

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

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.

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

VII. 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

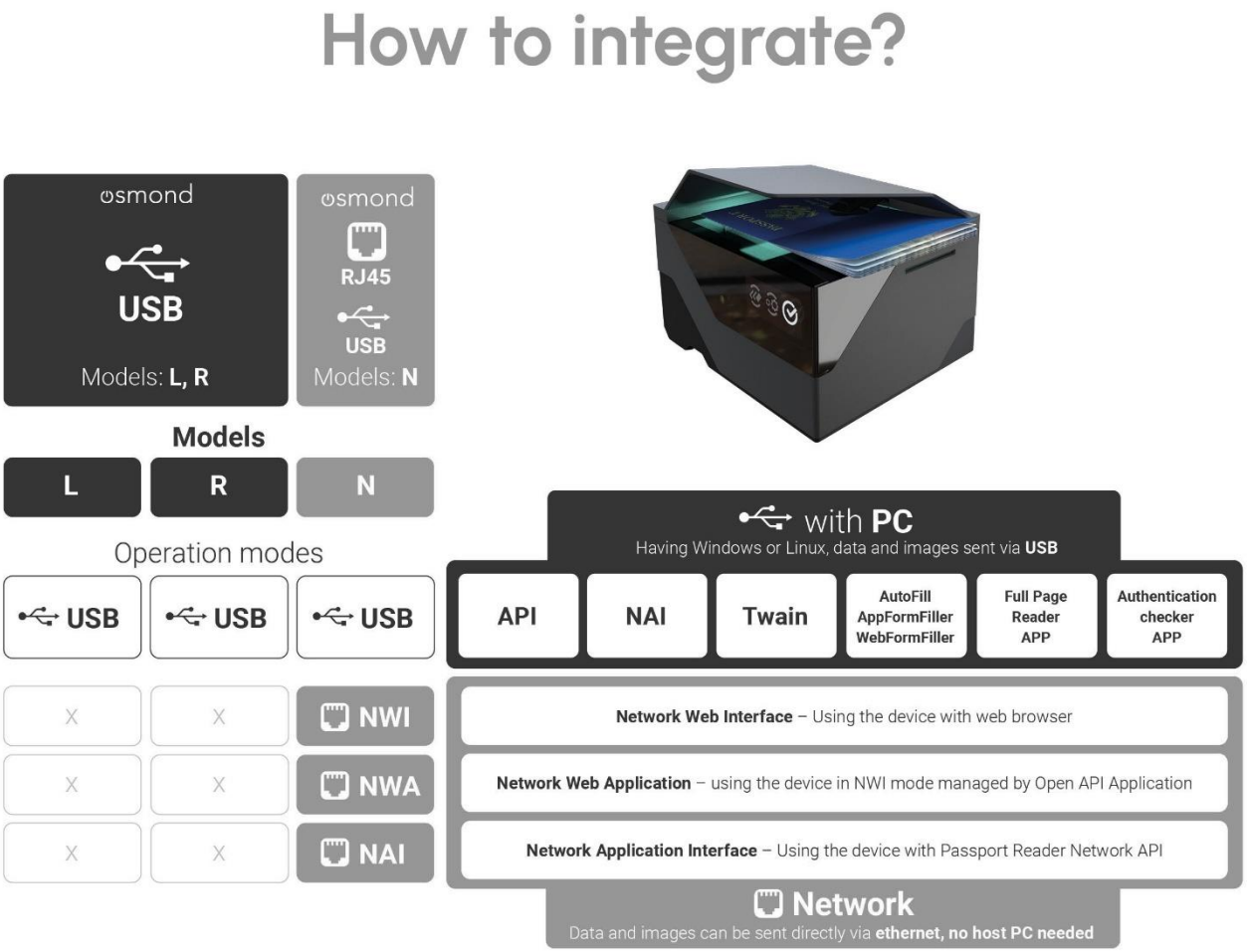
The Osmond operates without any kind of special software. All processes are running on the device. The web server running on the scanner can be accessed with any other device (e.g., a laptop, tablet) that can log on to the network that the scanner is connected to.

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



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

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 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*

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**.

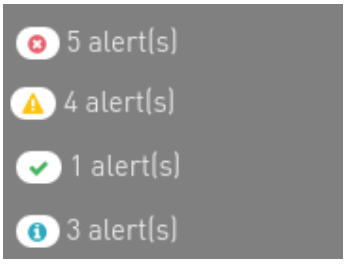
Important!

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.

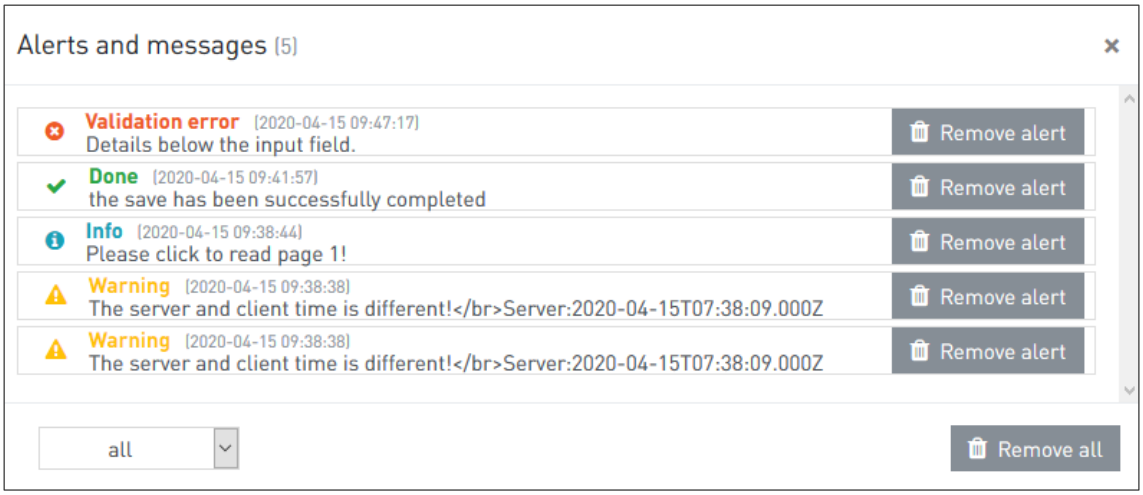
The system sends notifications about events which may concern the user. Such event can be for example the success or failure of saving a data sheet as well as if the document is to be changed in the document reader after scanning a page. Information about the number of the notifications is displayed 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

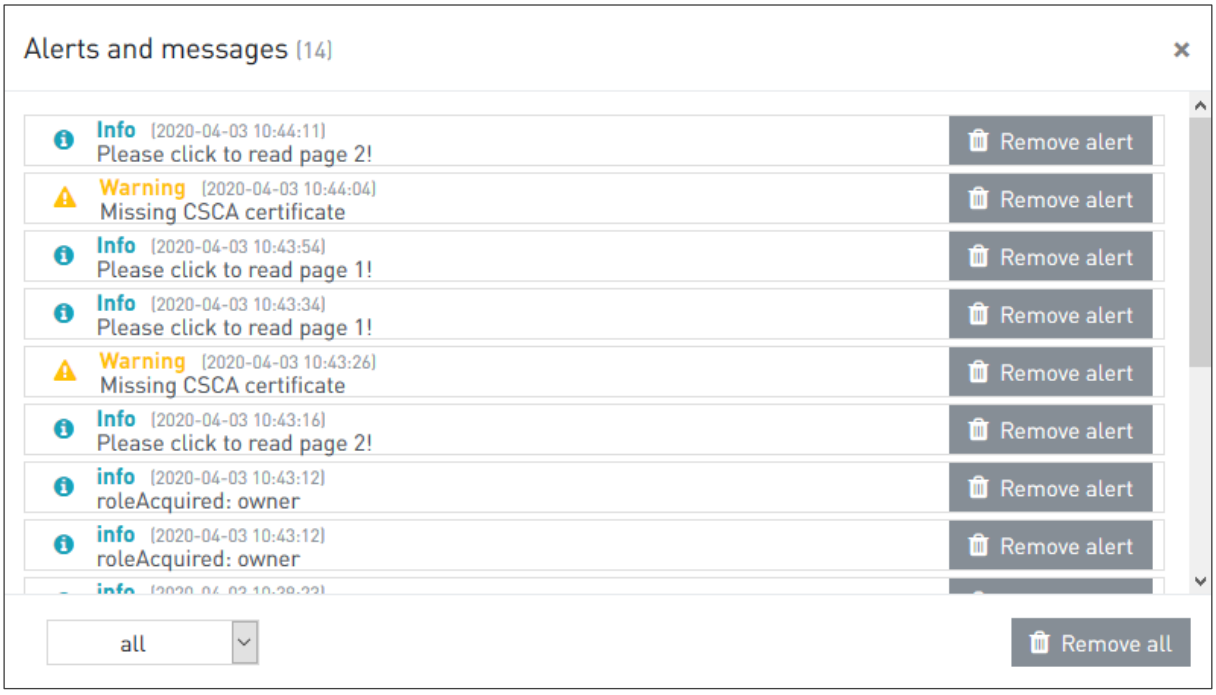


In the list the notification types are displayed with increasing priority. Thereby in the status bar the icon of the highest priority notification can always be seen with the number of the notifications. By clicking on the notification icon, the notifications can be viewed (in descending order by date).

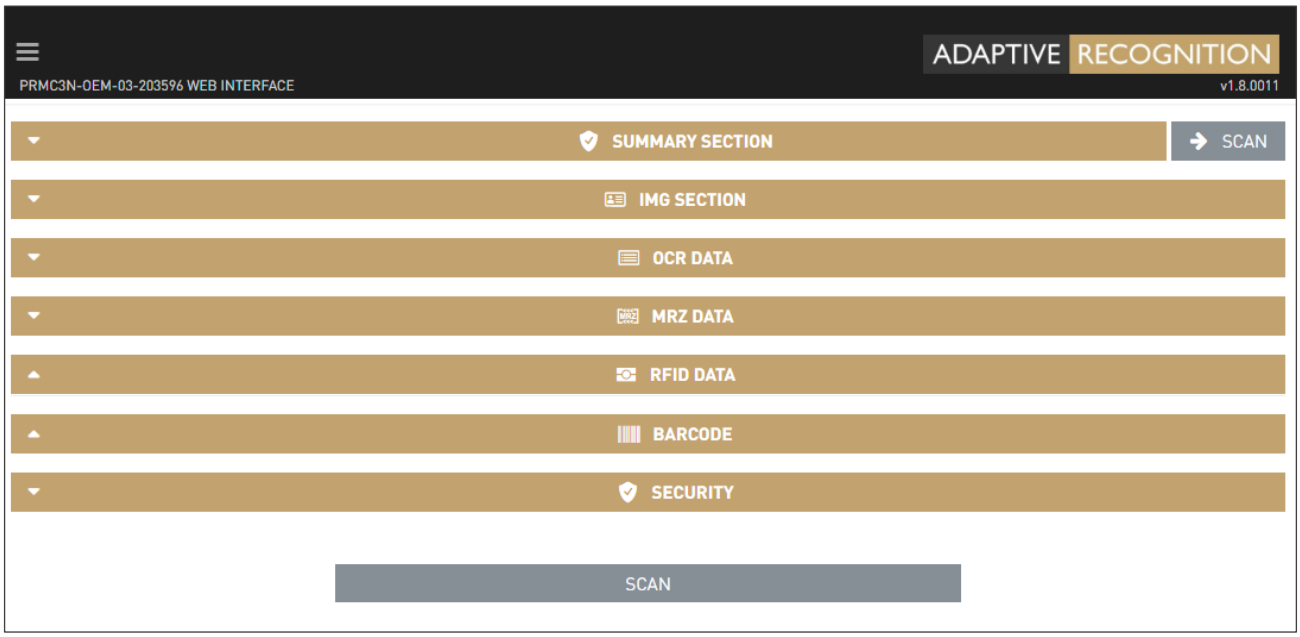


On the notification panel it can be selected that every or just the chosen notification type should be listed. The notifications can be deleted one by one or all at once.

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.

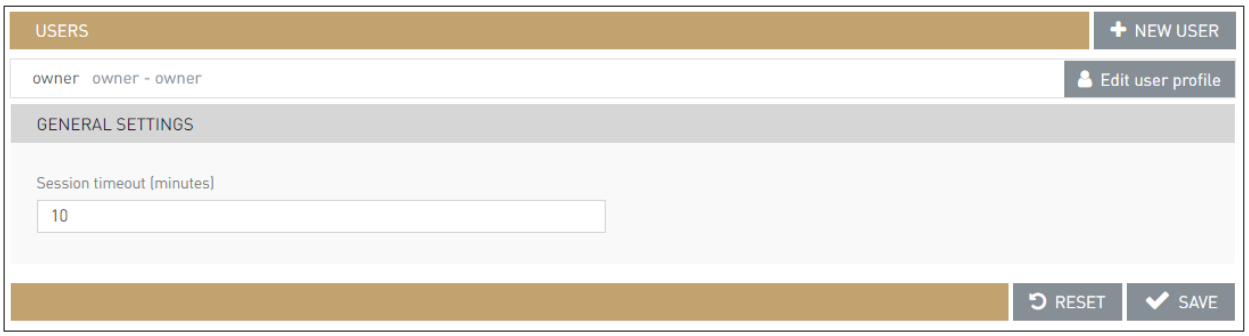
Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

2. WEB INTERFACE

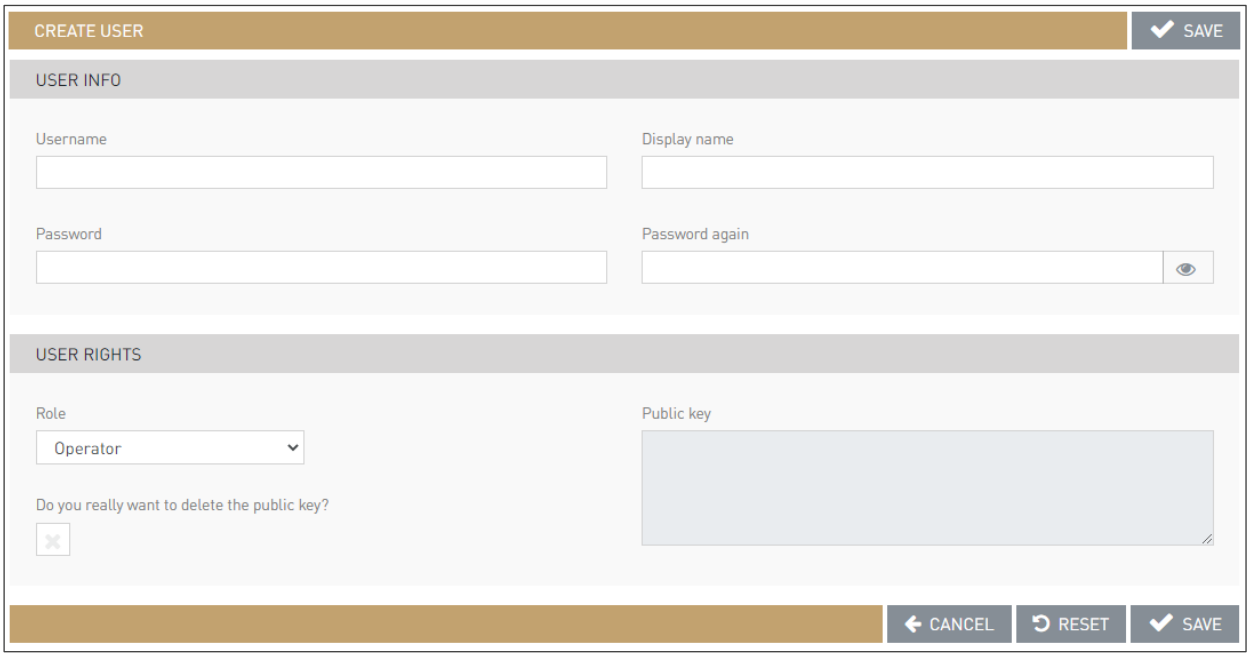
2.1. ADMINISTRATION

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:

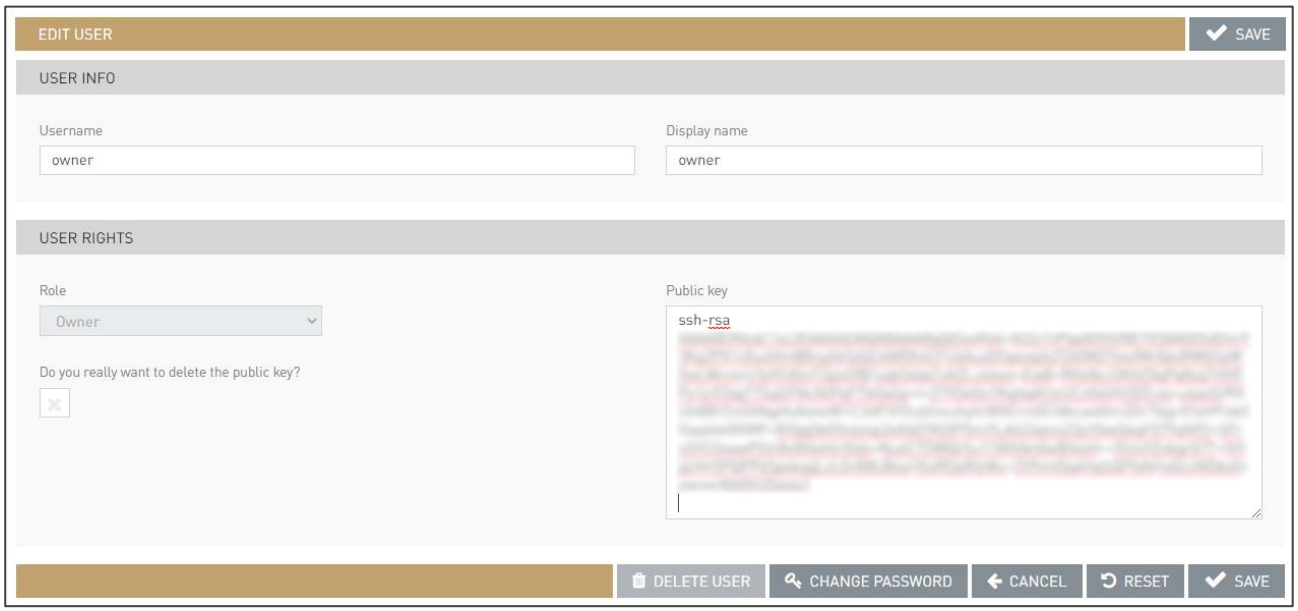
- **NAI**: This user role belongs to the NetAPI operating mode. NetAPI user is required to operate the Osmond N device via Passport Reader NetAPI.
- **NWA**: This user role belongs to the Network Web Application API operating mode and can only be used in Network Web Application API operating mode.

> **Note**
>
> During NetAPI and Network Web Application API communications **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.

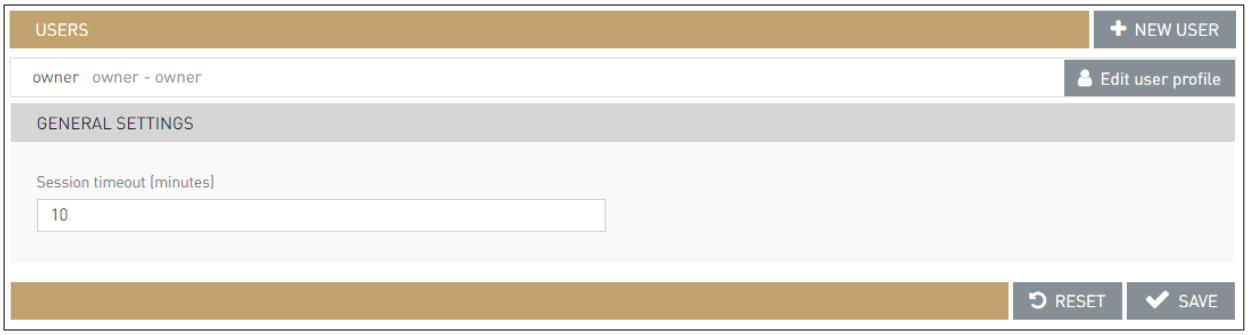
Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

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.



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

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

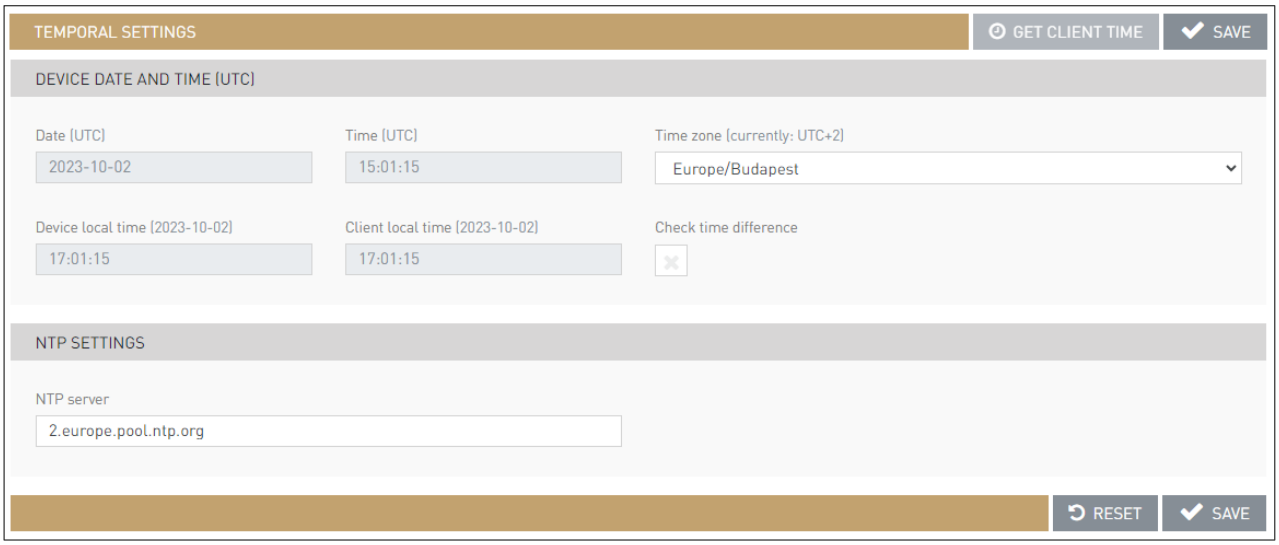


> **Note**
>
> From each role, only one user can be logged in, at the same time. The only exception is the **Owner** that can be logged in together with other, non-owner users.

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

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 server**s. 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.

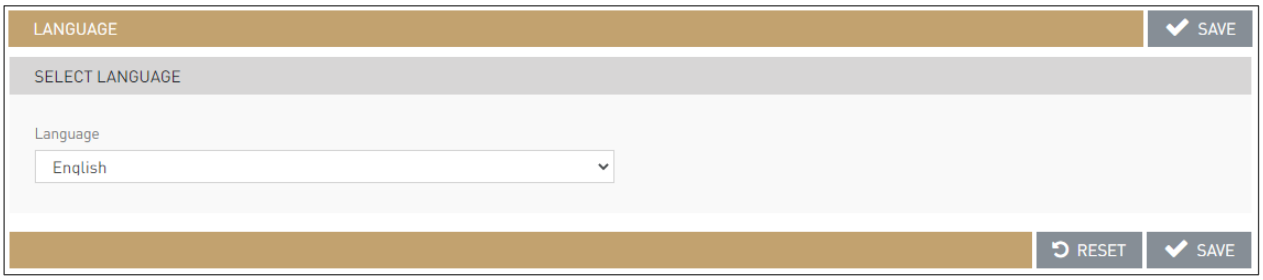
The Osmond device is configured to synchronize time via remote time server. When using the device offline, automatic time setting is not performed.

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.



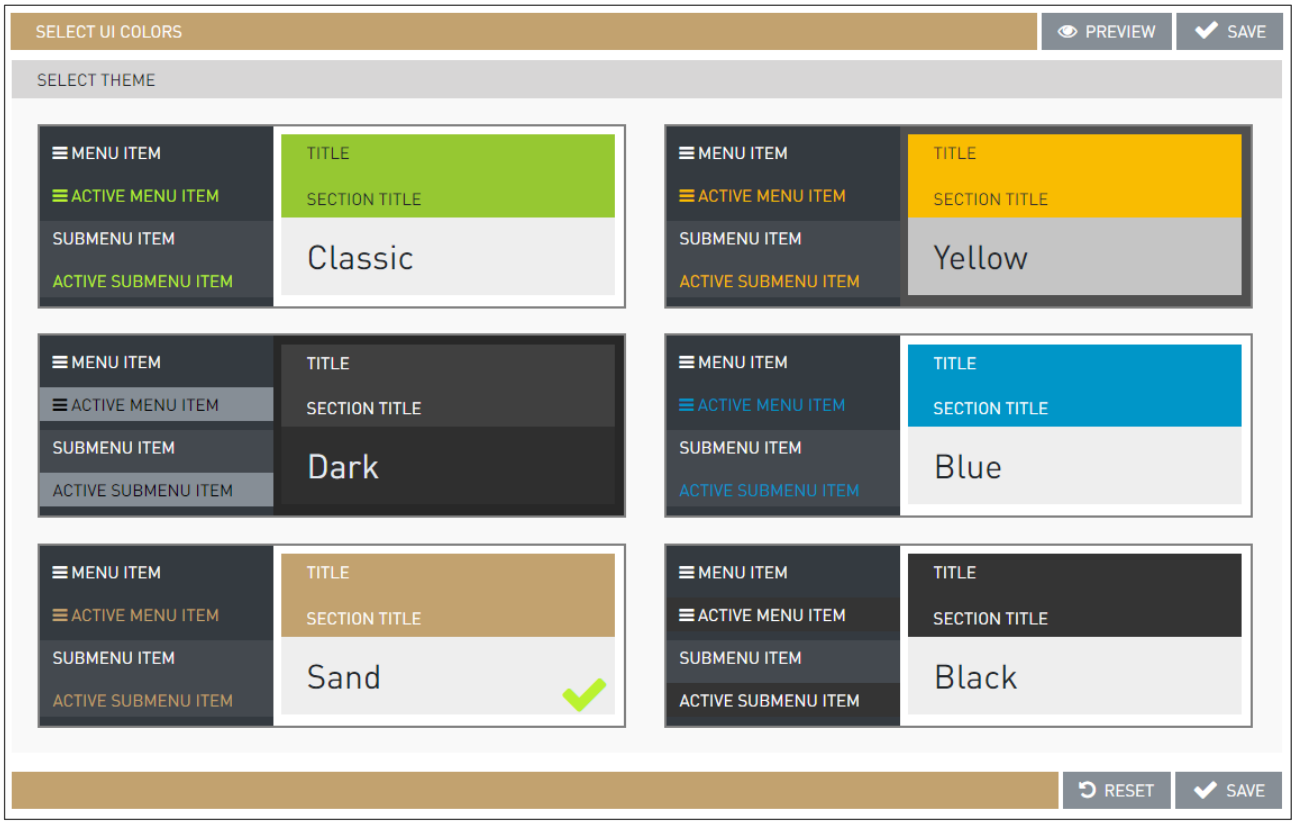
> **Note**
>
> English and Hungarian languages are currently available.

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

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.



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

2.1.5. ENGINES AND LICENSES

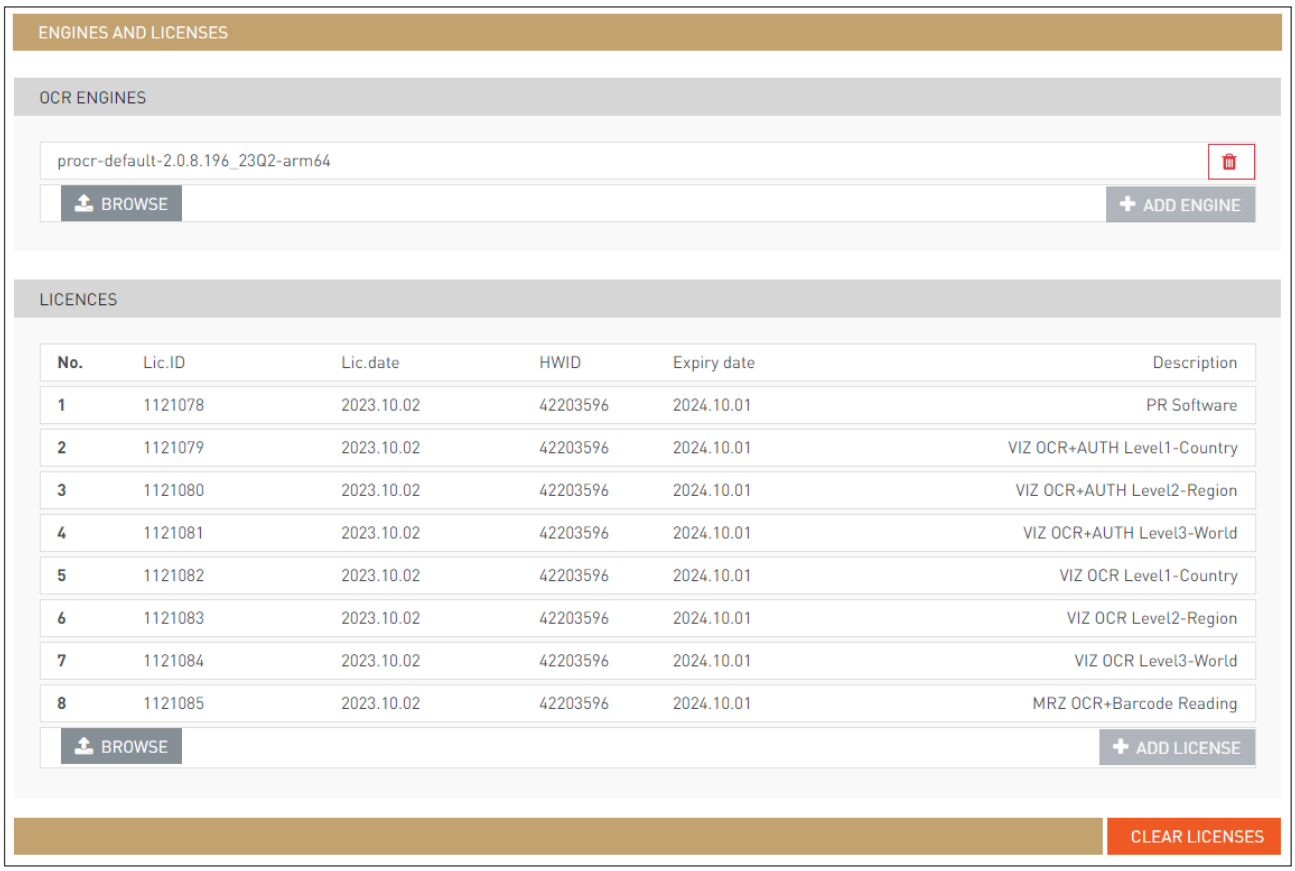
The **ENGINES AND LICENSES** menu is designed to manage OCR engines and software licenses on the Osmond device.

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



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

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 VIZ OCR and VIZ AUTH OCR Engine Management appendix.

Note

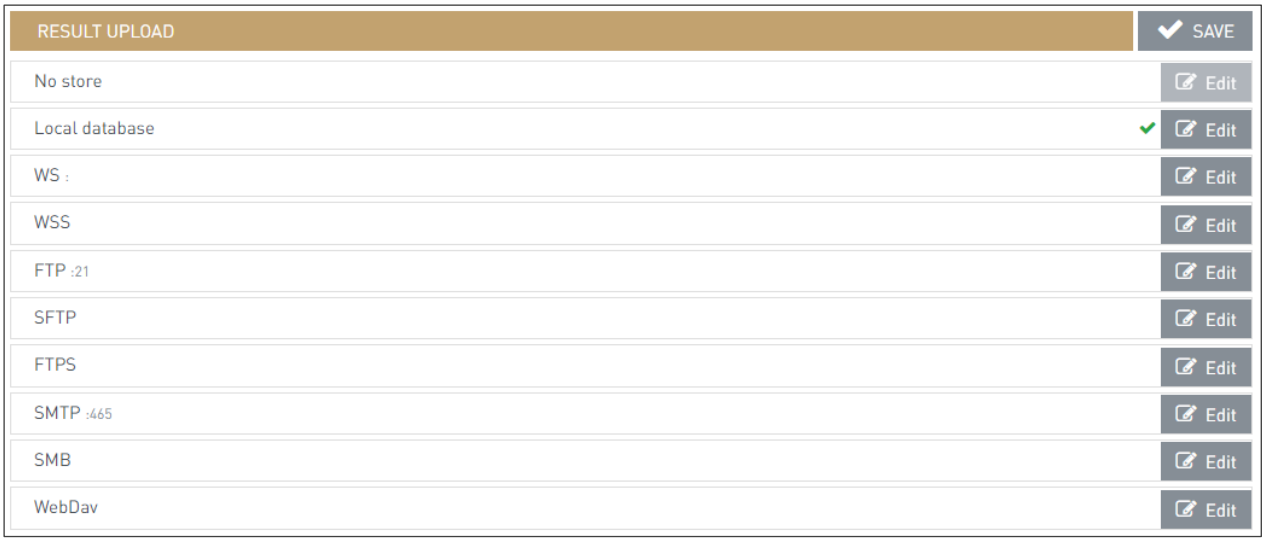
For more information and detail on the Passport Reader licenses and license handling, see License Management appendix.

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.

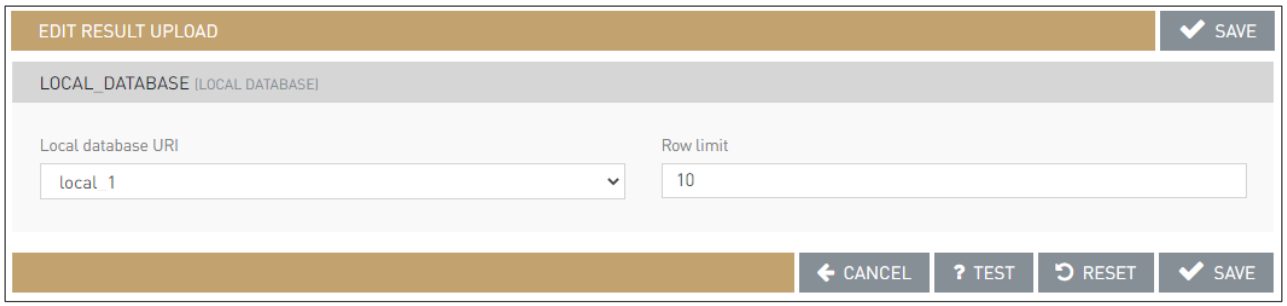


When the only purpose is the scanning, select the **No store** option. In this case the scanning results can be seen in the **START APP** menu, but when starting a new scanning, the results of the previous document disappear and cannot be reload from the device. The scanned data is not stored.

> **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

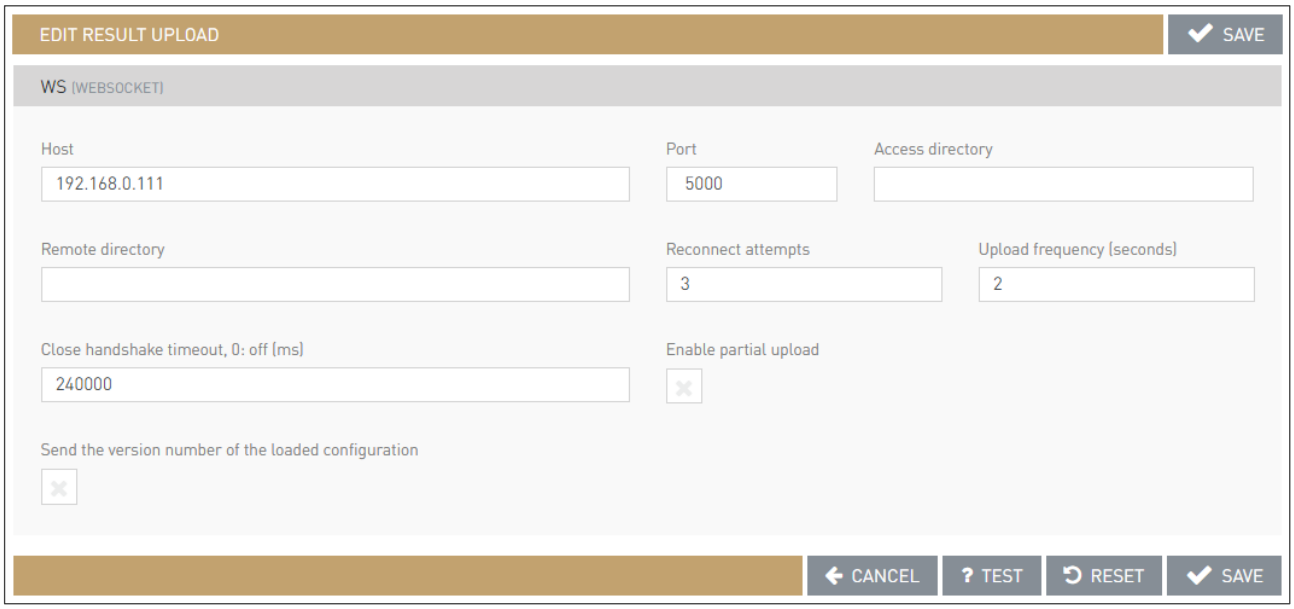
The Osmond built-in storage offers a feature to save scanned information to the device directly. In order to configure this function, click on **[Edit]** in the line of the **local_database**, then just select "local_1", "local_2" or "local_3" in the **Local database URI** field. Specify a **Row limit** 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).



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.

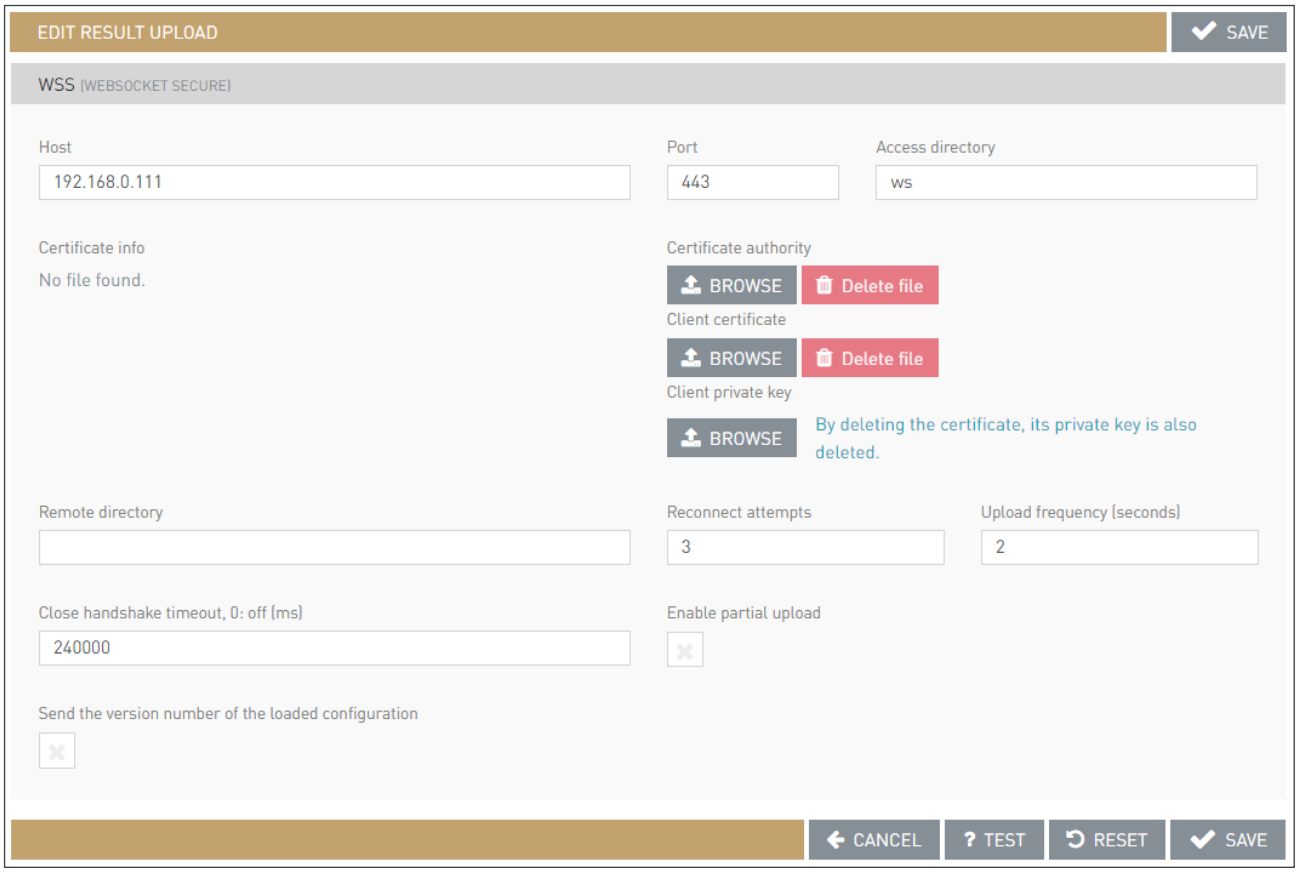
> Note
>
> The configuration version can be checked at MAINTENANCE / SYSTEM INFORMATION.

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.

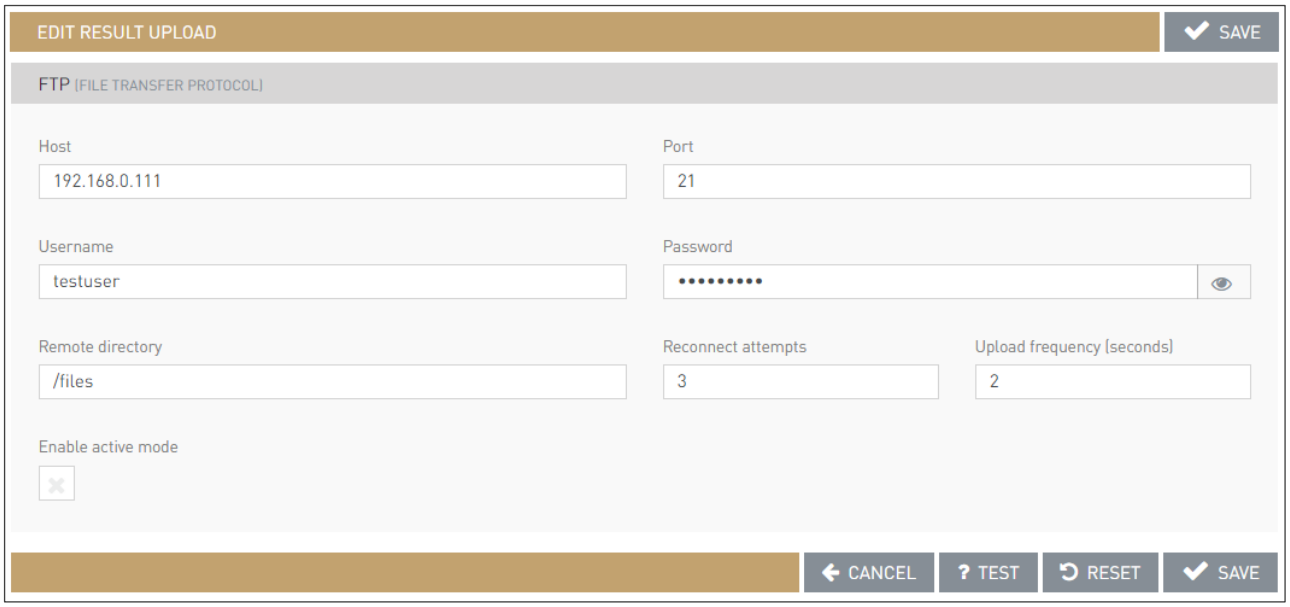
> Note
>
> The configuration version can be checked at MAINTENANCE / SYSTEM INFORMATION.

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

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

– **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.

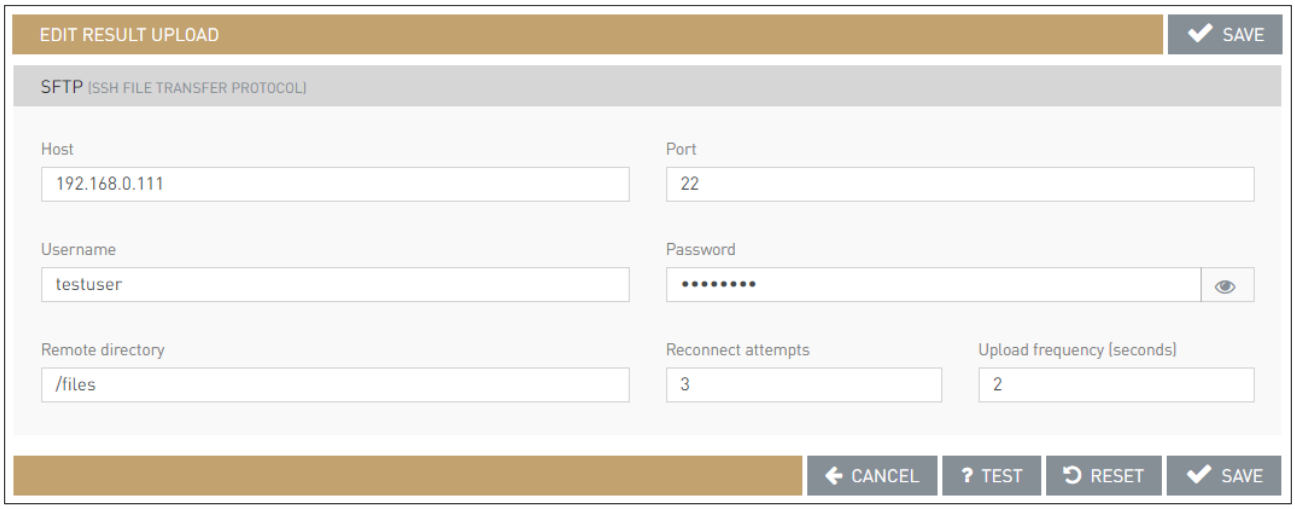
Tick the box in order to **Enable active mode**.

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.

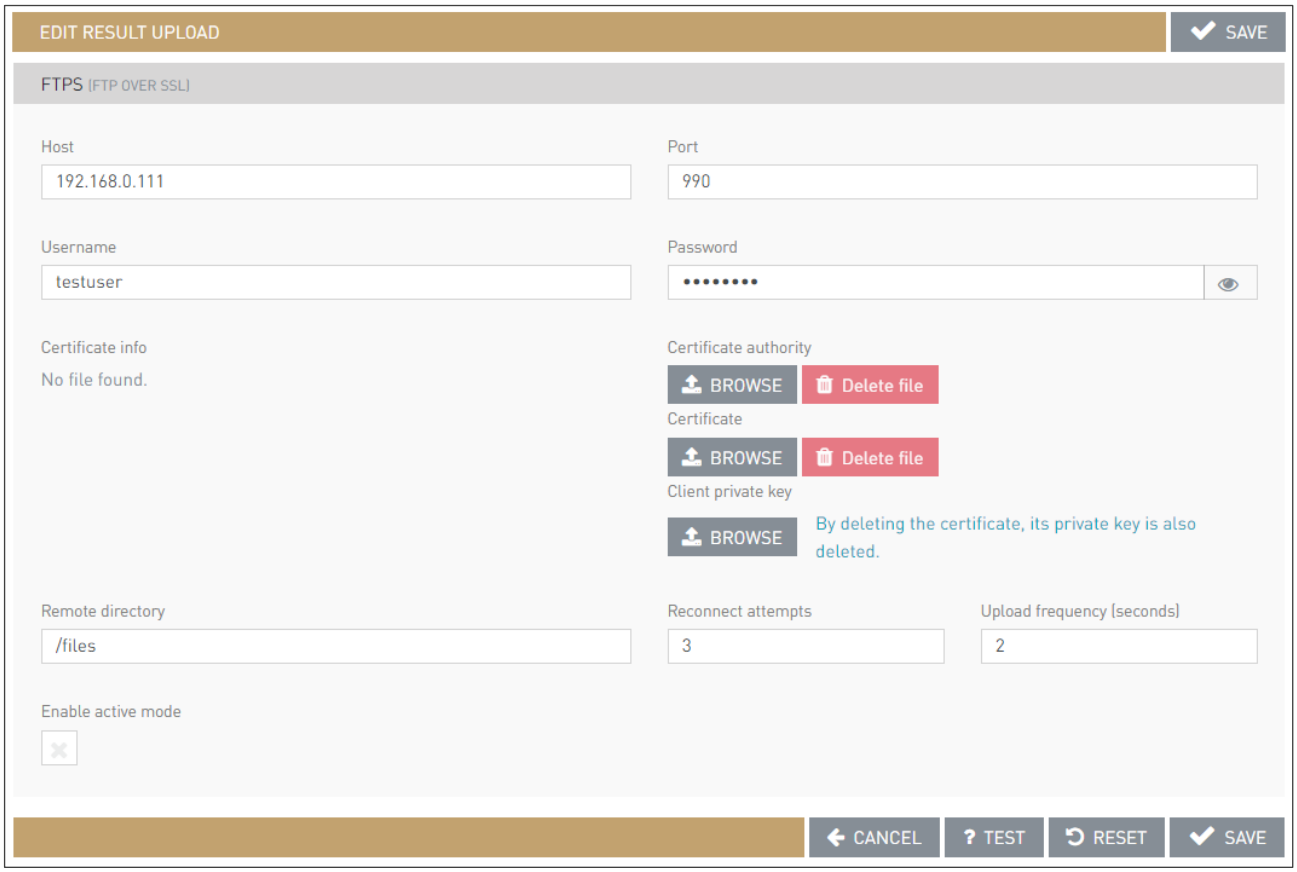
You can specify the name of the folder accessible from the server's root directory with the **Remote directory** field. Enter the number of the **Reconnect attempts** in order to set the maximum number of the connections without error message. The device attempts to upload the data at specified intervals,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

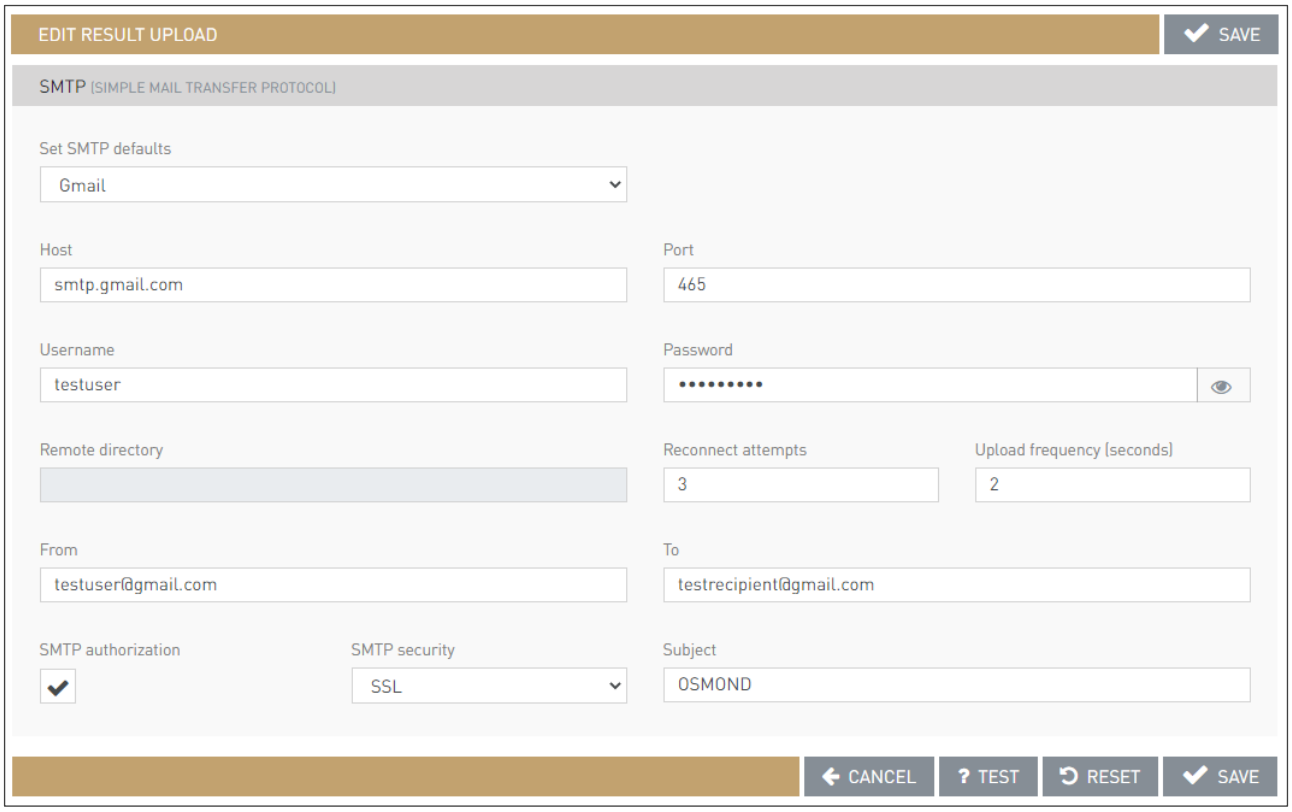
Click **[SAVE]** to apply changes.

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**.

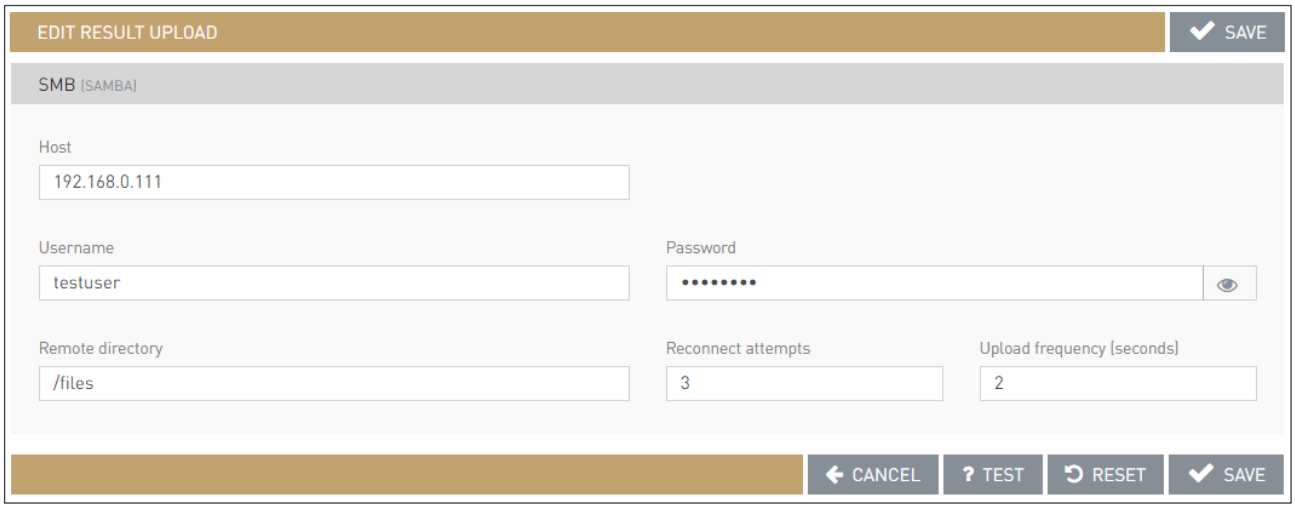
In order to secure the SMTP mail, select a cryptographic protocol from the **SMTP security**.

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.

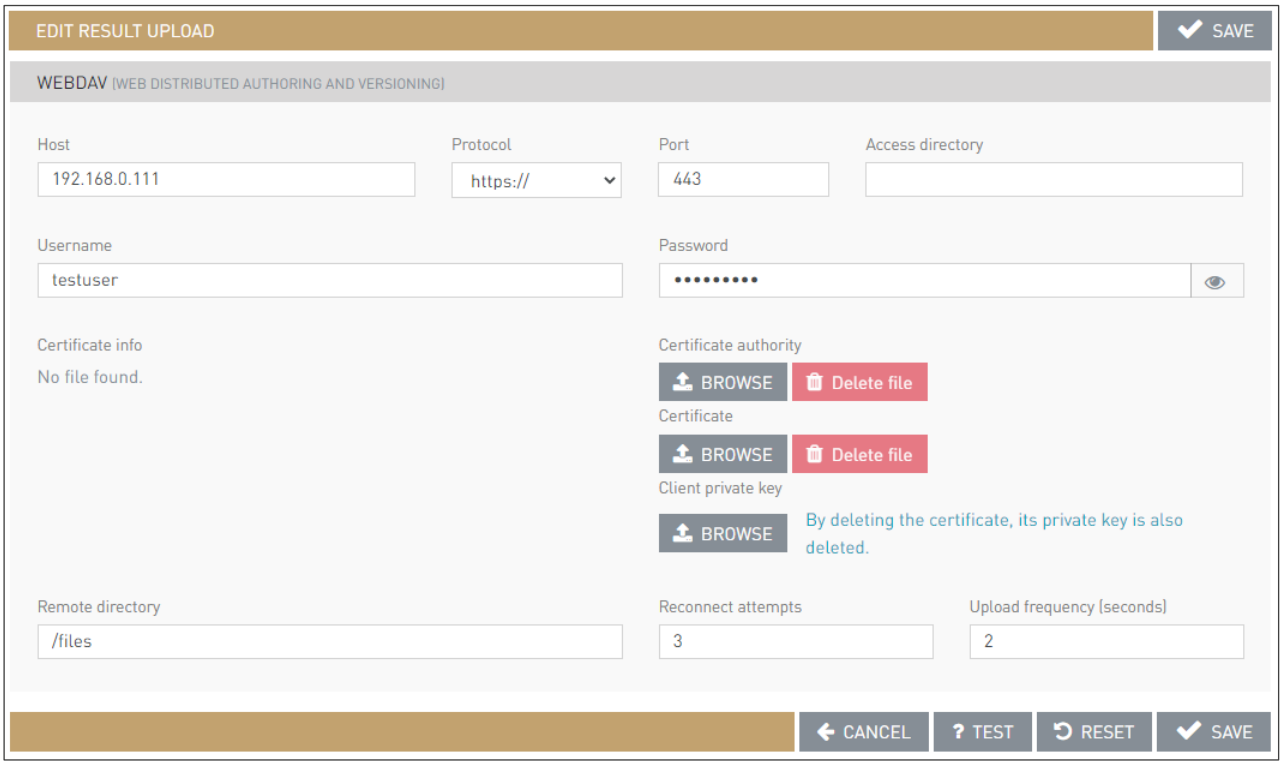
You can specify the name of the folder accessible from the server's root directory with the **Remote directory** field. Enter the number of the **Reconnect attempts** in order to set the maximum number of the connections without error message. The device attempts to upload the data at specified intervals,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

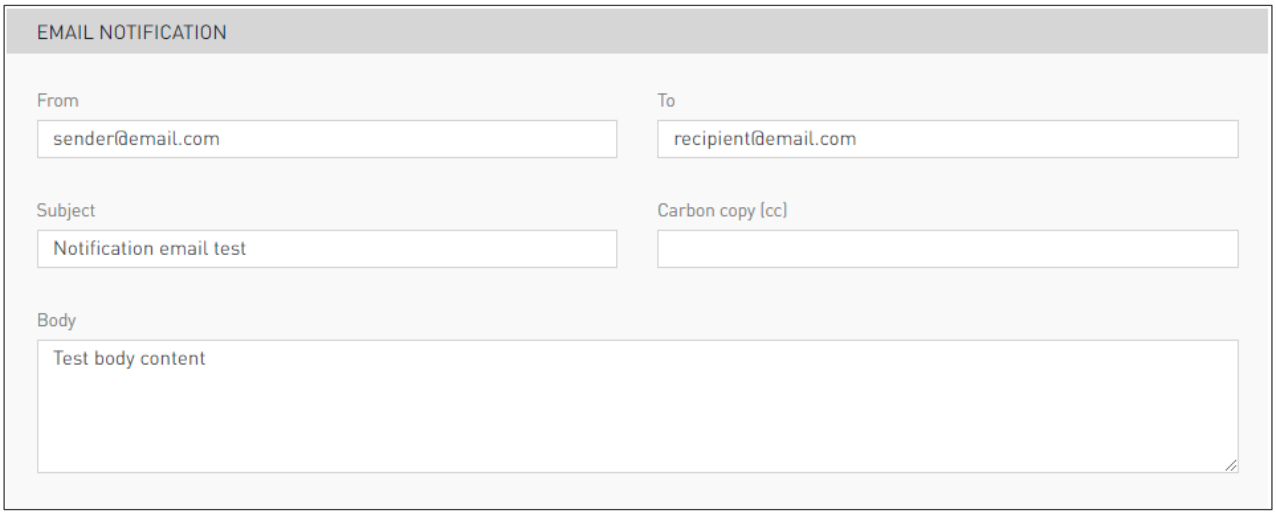
> **Note**
>
> If certificates are uploaded via configuration update from remote server, the "From config update" text is displayed instead of certificate filename in the **Certificate info** box.

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).

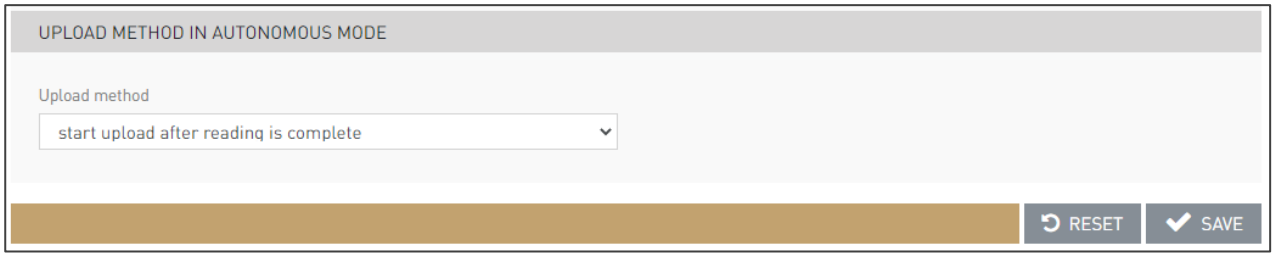
Besides uploading data to remote hosts, the Osmond also supports sending automatic e-mail notifications on scanned documents.



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

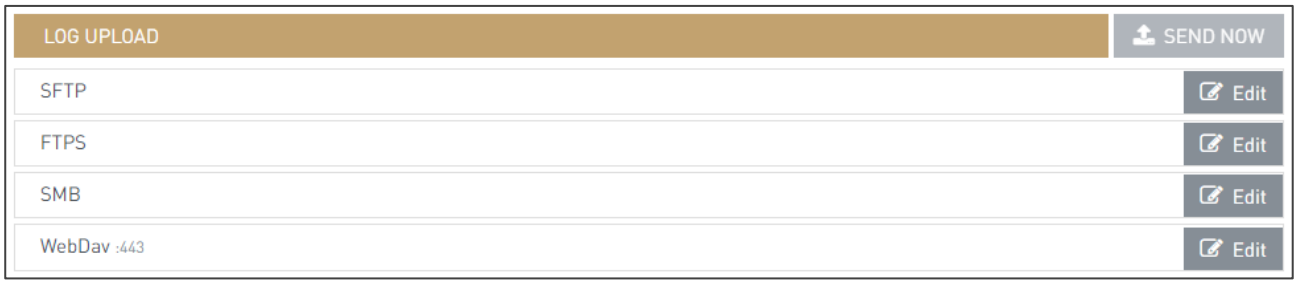
> Note
>
> It is recommended to select one of the protocols including encryption (SFTP, FTPS, Webdav).

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**.

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

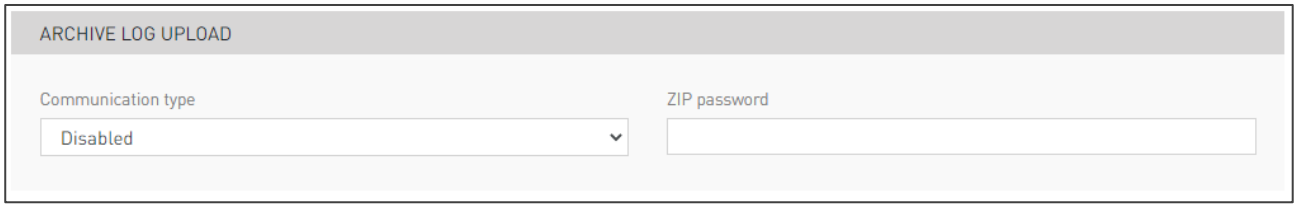
ARCHIVE LOG UPLOAD

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

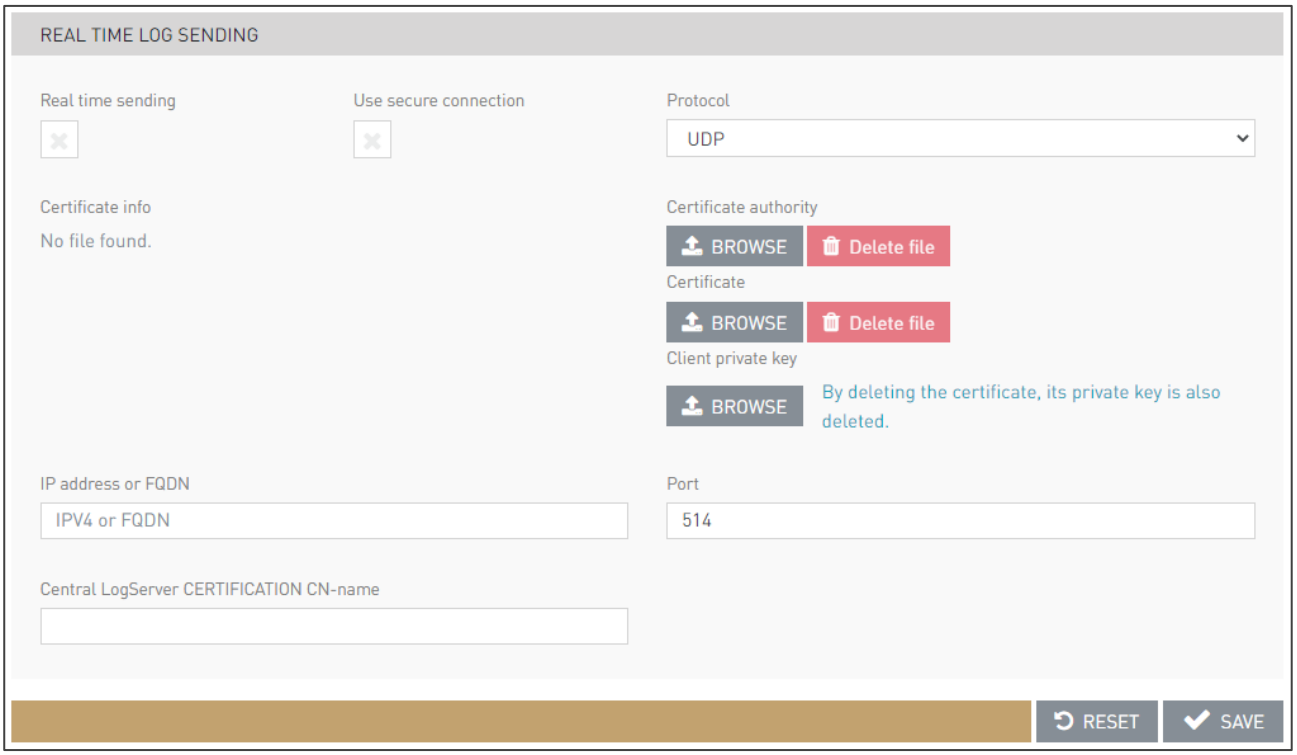
To upload the given certificate, click on the **[BROWSE]** button and select the certificate by clicking on the required one and clicking **[Choose file]**. After uploading the certificate files, their details are visible in the **Certificate info** field.

> 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:

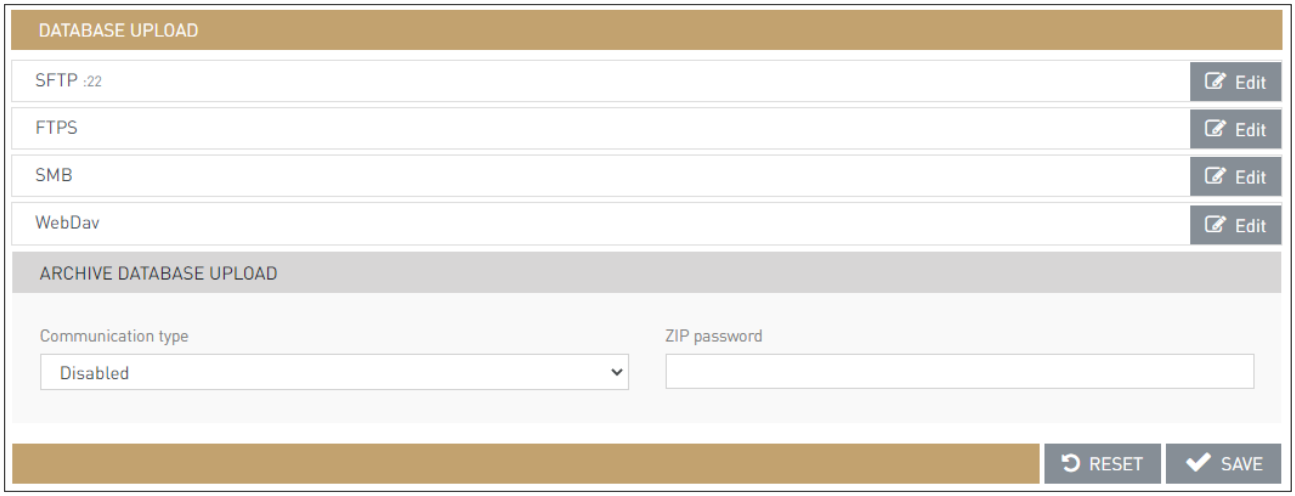
- SFTP
- FTPS
- SMB
- WebDav

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.



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

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.

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
```

The most commonly used values for the config file:

- 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:

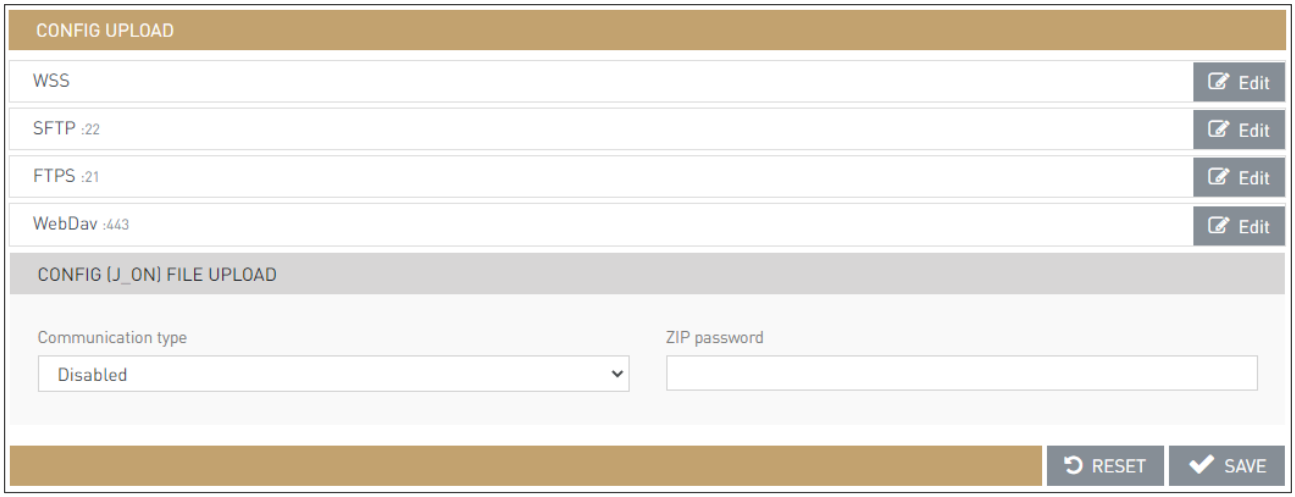
- SFTP
- FTPS
- SMB
- WebDav

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.

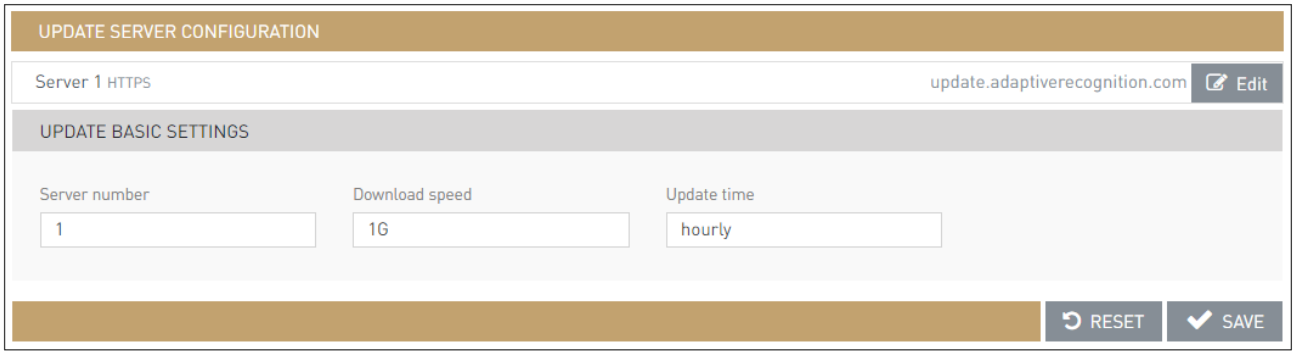
Under **Communication type** the preferred protocol can be selected. In case of specifying the **ZIP password** field the compressed file is password protected.



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

2.1.10. UPDATE SERVER

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

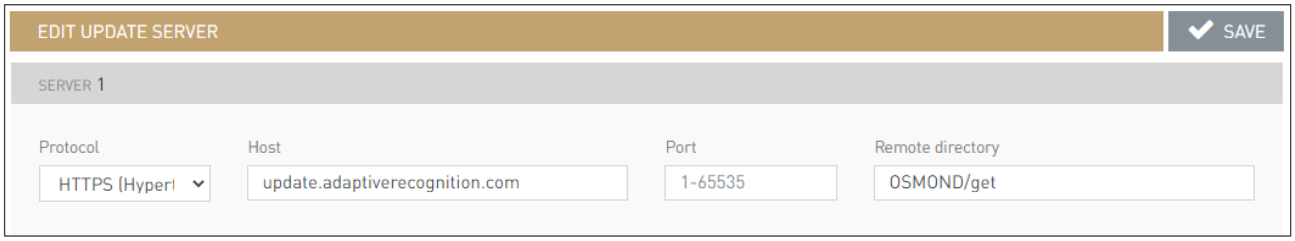


The device supports max. 9 remote servers (**Server number**) with **Download speed** and **Update time** configuration.

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 restarted automatically after software download or not. In either way, installation of the update is performed at the next device start-up.

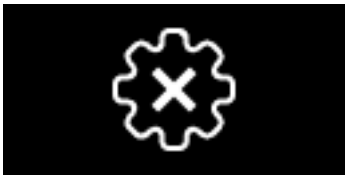
Note

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

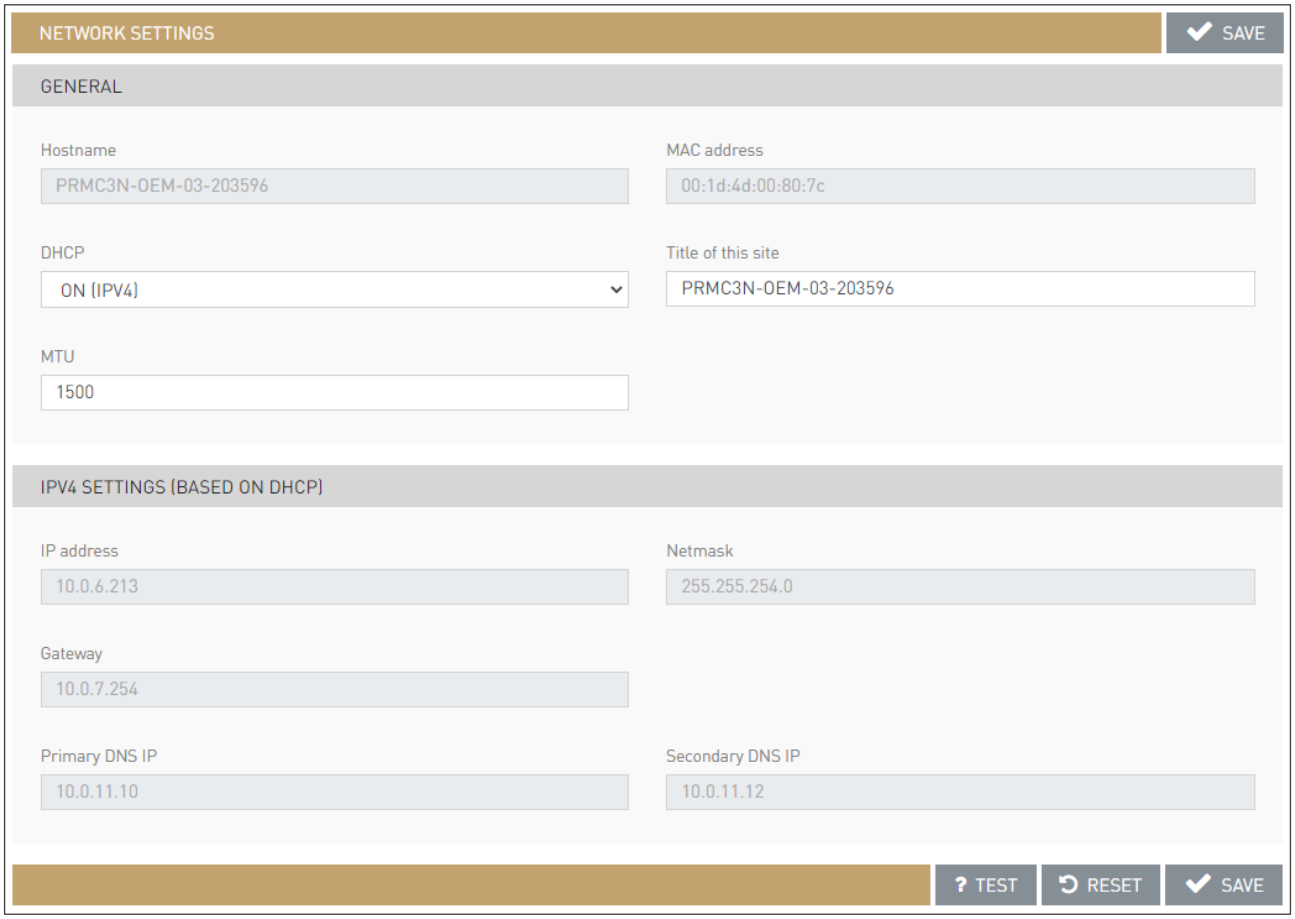
2.2. NETWORK

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.

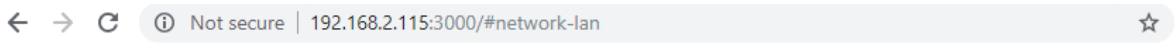


Once all the necessary changes have been made, click on **[SAVE]** to preserve the changes.

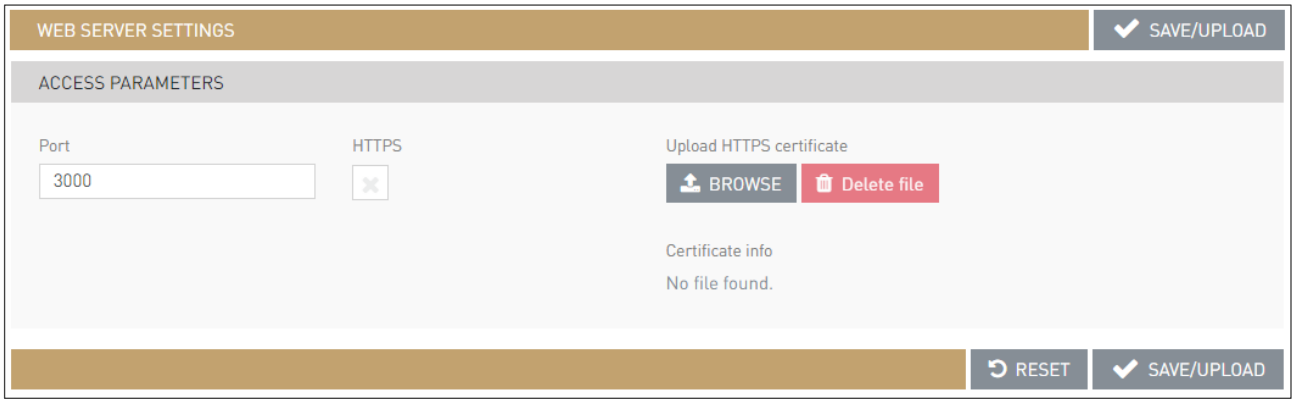
2.2.2. WEB SERVER

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.

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

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.

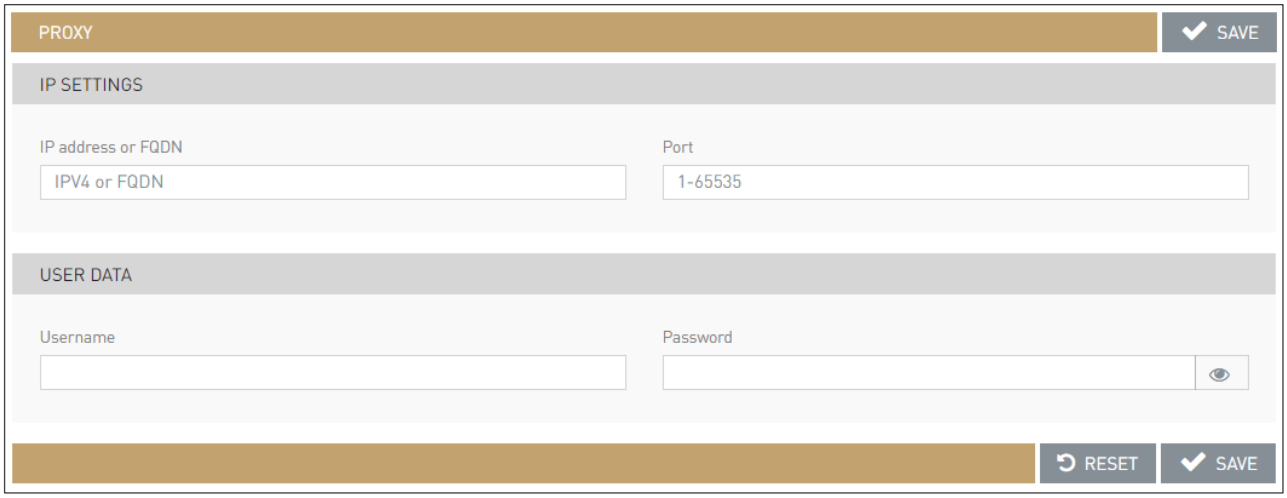
> Note
>
> For successful HTTPS connection, the rootCA of the uploaded certificate must be added to the browser trusted publishers list.

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

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

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:

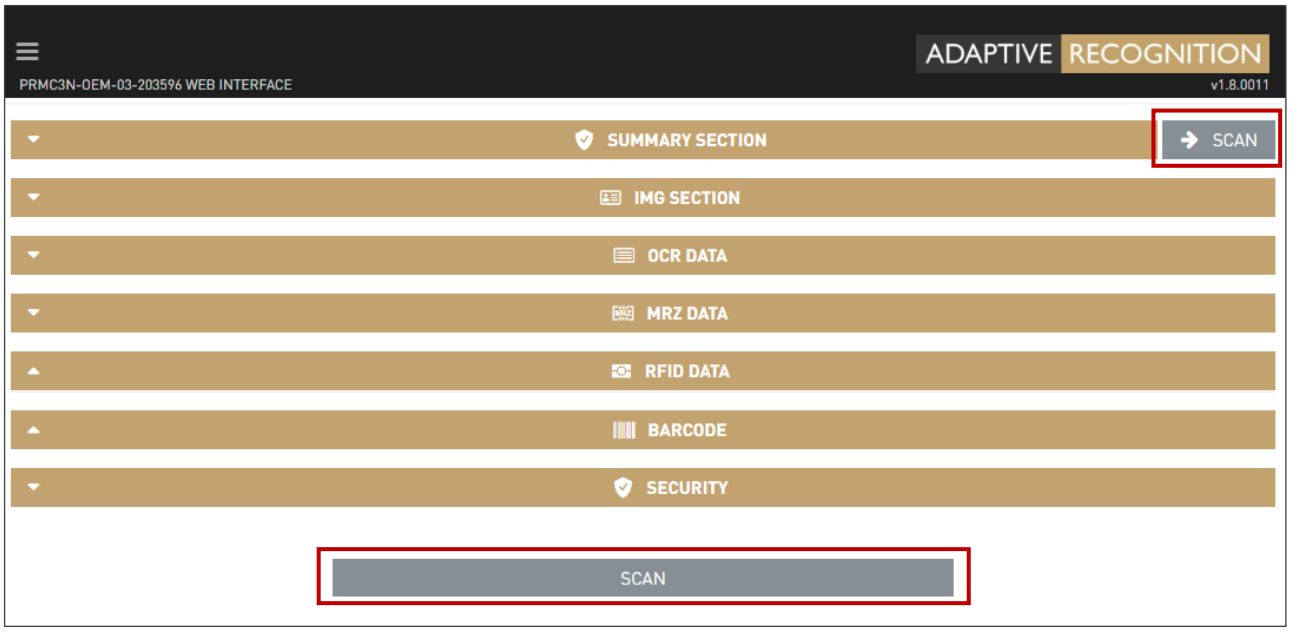


IP address or FQDN and **Port** of the Proxy server can be set in the corresponding text fields by simply typing the desired values. If the Proxy server requires authentication, set the **Username** and **Password** in the **USER DATA** section. Make sure to click **[SAVE]** to apply any new values.

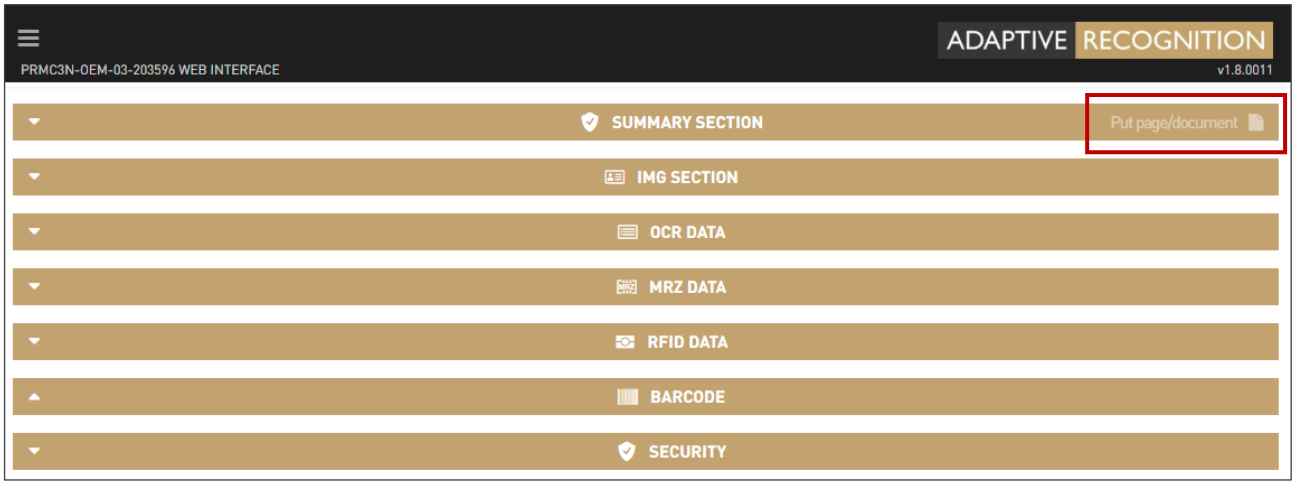
2.3. APPLICATION

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**).



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).

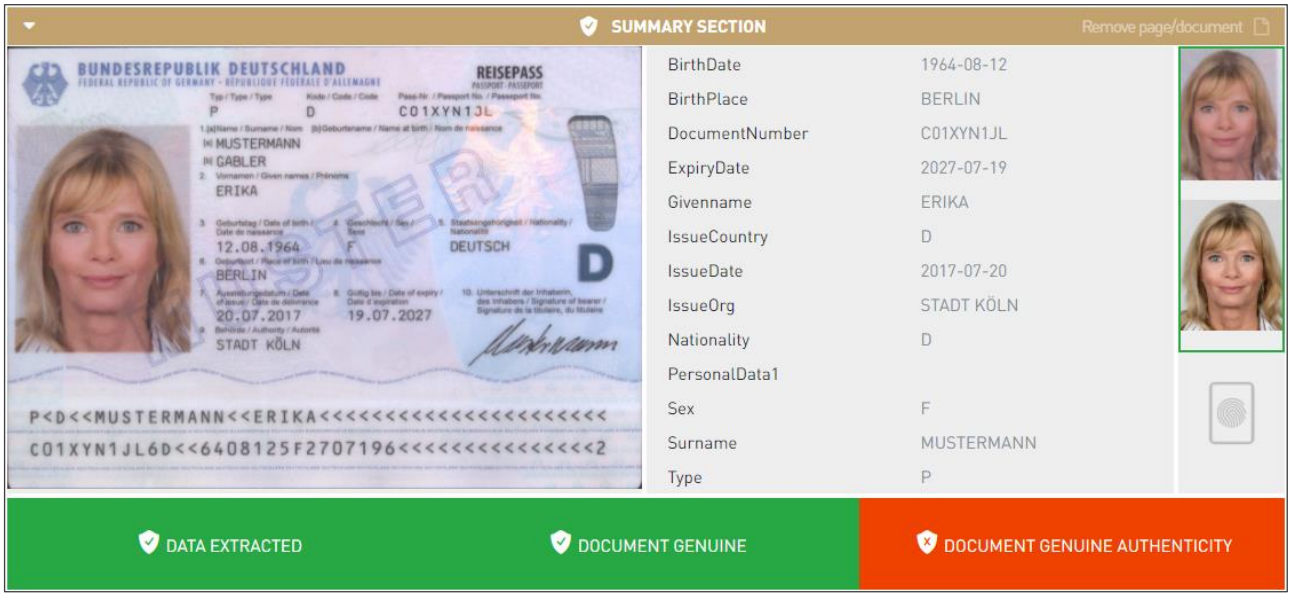
1. **Data extracted**: Processing data
   - **Error** (red), if there is an error in the **RFID** and/or **MRZ** sections
   - **Warning** (orange), if no MRZ line has been read
2. **Document genuine**: Checking the document
   - **Error** (red), if the **SECURITY**, **OCR** and/or **Face Compare** are 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:

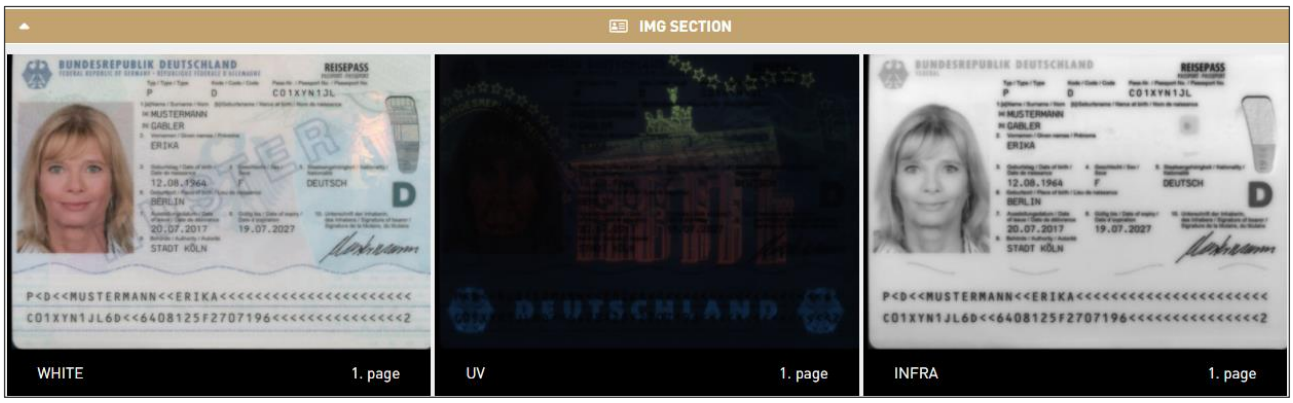
- **60-100%: OK** (green) - No error message; the rate of the similarity is greater than 60%
- **30-60%: WARNING** (orange) - The two images are similar; the rate of the similarity is between 30% and 60%
- **0-30%: ERROR** (red) - The two images differ from each other; the rate of the similarity is less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



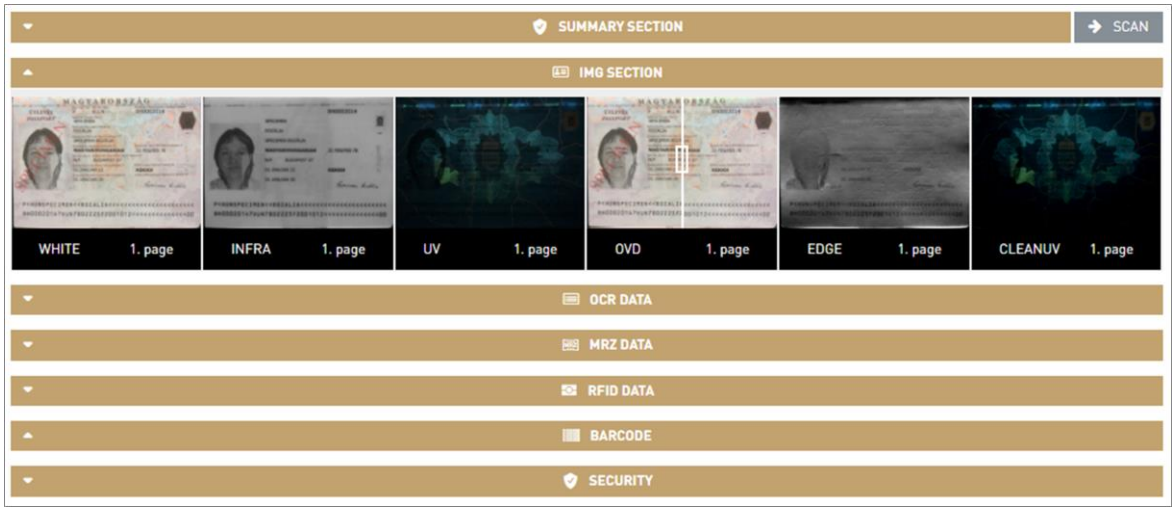
Note

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	PE09147486AUS8406077F1903267<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.

MRZ DATA

```
MRZ 1:P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<<
MRZ 2:C01XYN1JL6D<<6408125F2707196<<<<<<<<<<<<<<<2
```

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).

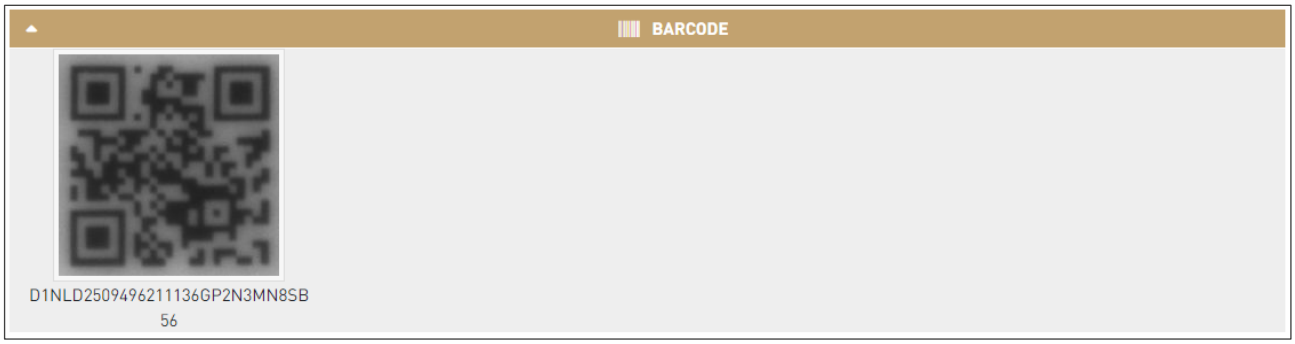
> **Note**
>
> The **RFID DATA** section shows data fields that are configured in the **EDIT APP / FIELD SETUP** menu.

RFID DATA

BirthDate	1978-02-22
Composite1	P<HUNSPECIMEN<<ROZALIA<<<<<<<<<<<<<<<<<<<<<<<
Composite2	BH00029265HUN7802225F2201018<<<<<<<<<<<<<<04
DocType	PP
DocumentNumber	BH0002926
ExpiryDate	2022-01-01
Givenname	ROZALIA
IssueCountry	HUN
Name	SPECIMEN ROZALIA
Nationality	HUN
PersonalData1	
Sex	F
Surname	SPECIMEN
Type	P

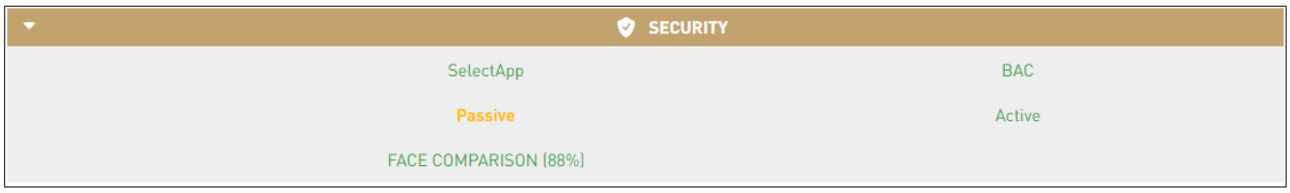
6. BARCODE

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.



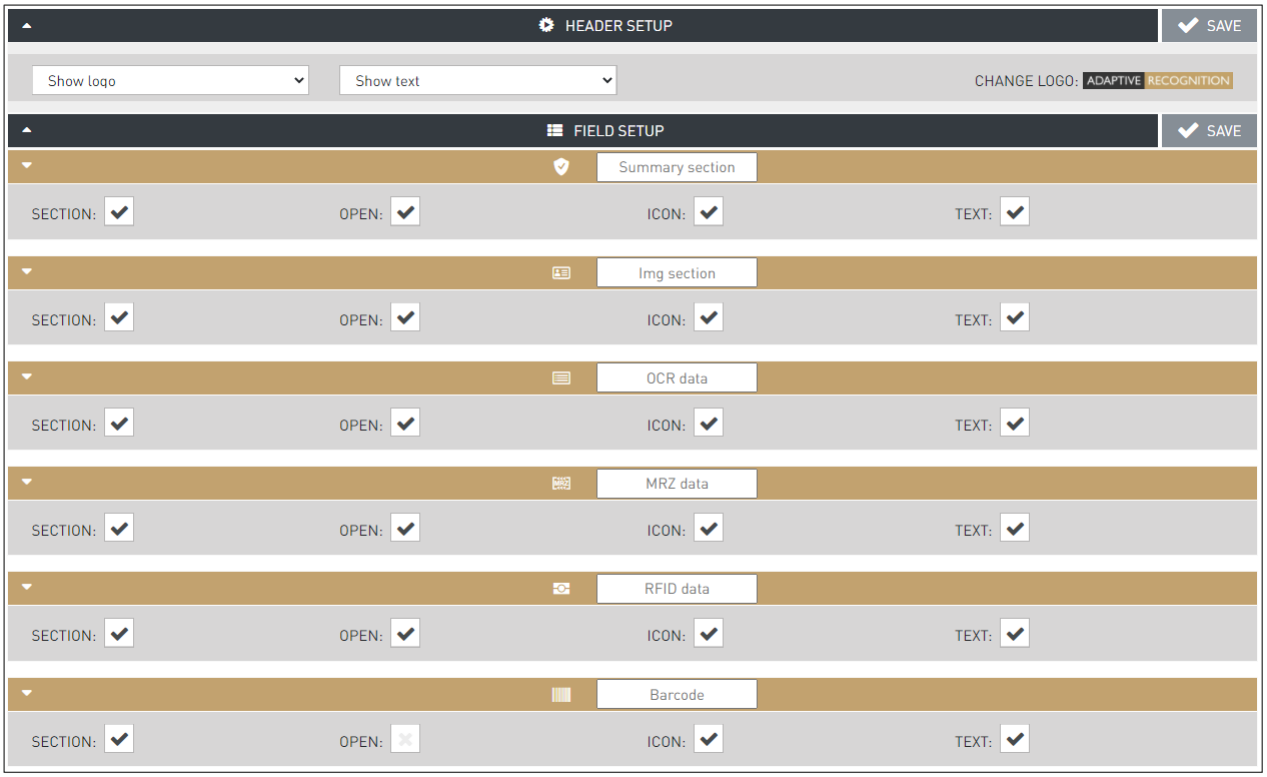
7. SECURITY

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.

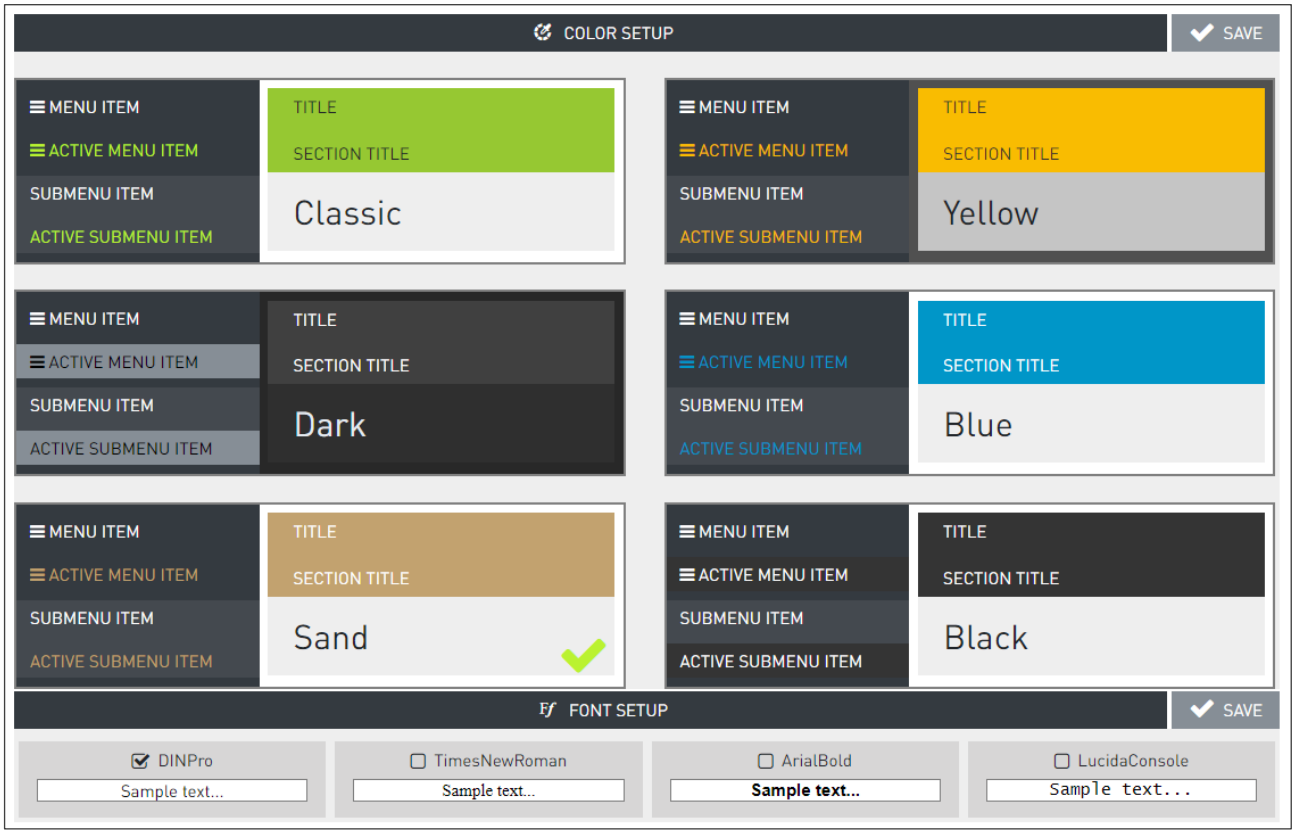
OPEN: If selected, the Application shows the contents of the section by default.

ICON: If selected, the icon - next to the title of the section – is displayed in the Application.

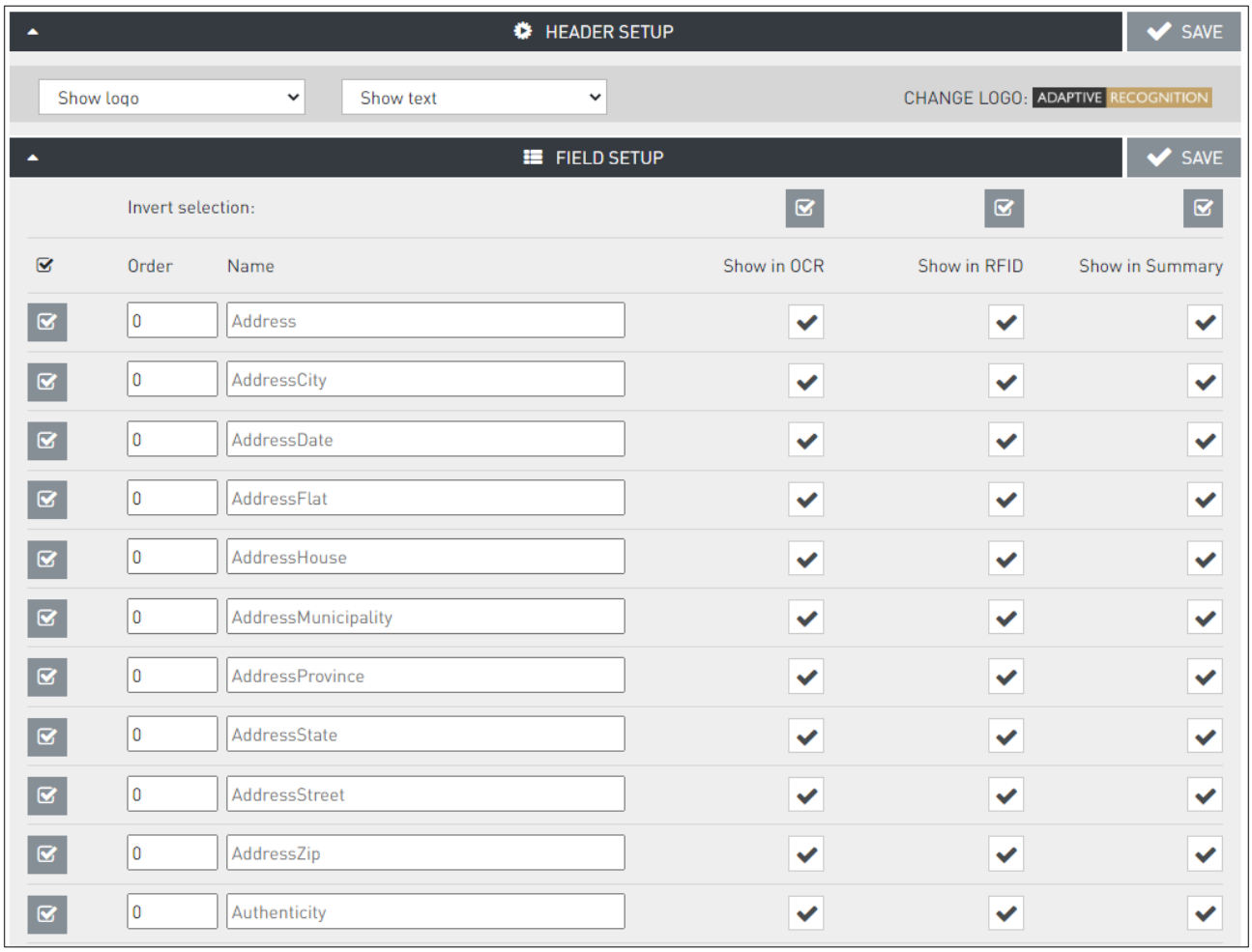
TEXT: If selected, the title of the section is displayed.

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

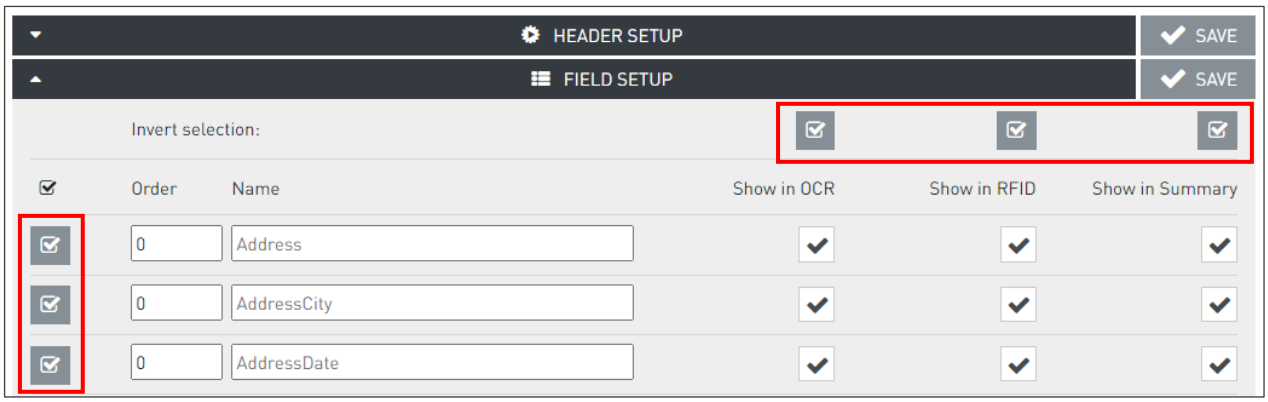
Besides the above options, the fonts and colors used in the Application can also be customized at the **COLOR SETUP** and **FONT SETUP** sections.



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.



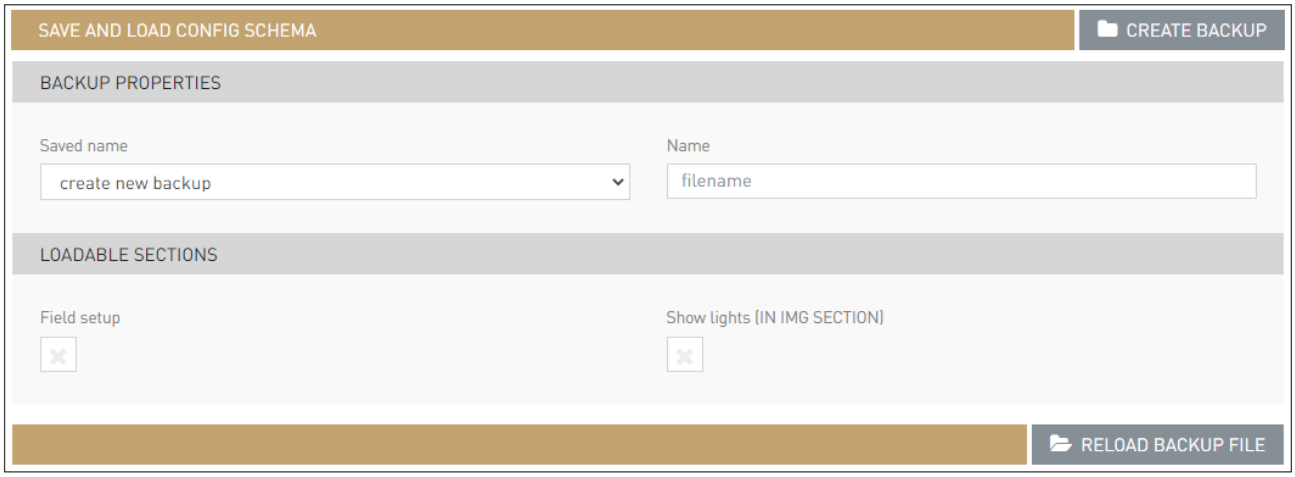
2.3.3. CONFIG BACKUP

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 **Users** settings and **Configuration data** can be saved.

2.3.4. HISTORY

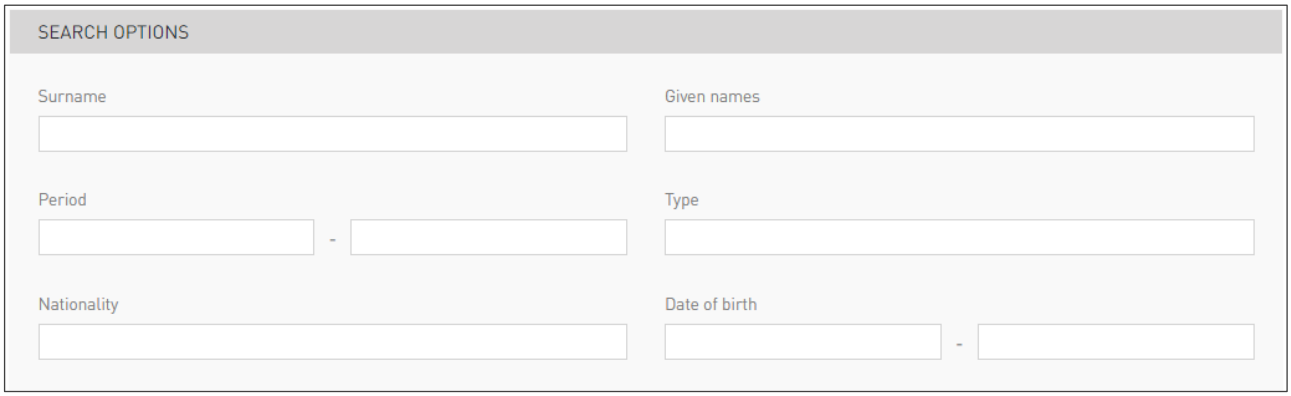
The Osmond device is equipped with internal storage space to save images and data of scanned documents. This feature can be activated by selecting the "local database" option in the **ADMINISTRATION / RESULT UPLOAD** menu and together with zip format (**PACKAGE FORMAT** menu).

> 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.

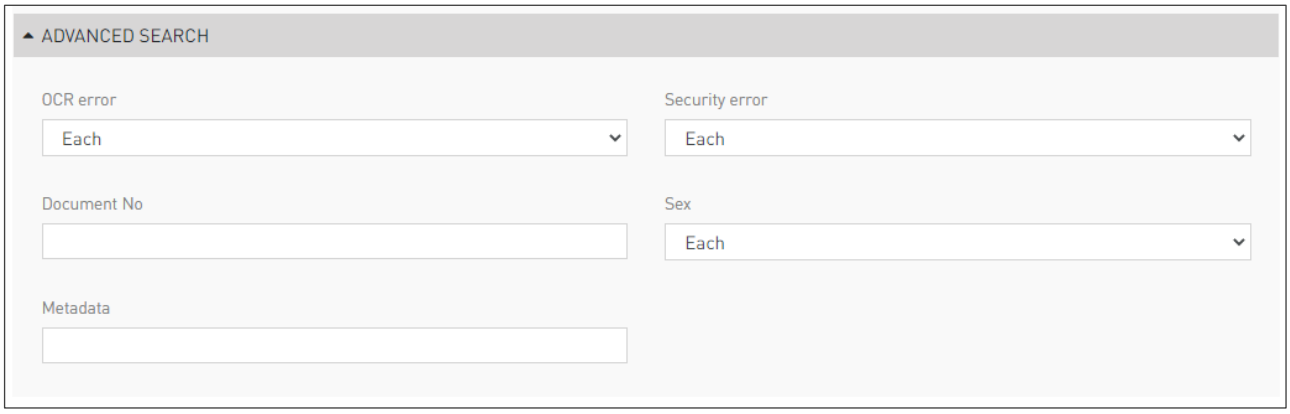
Once documents are saved, they can be browsed in the **HISTORY** by using multiple filter criteria. For filtering time periods, use the date format of the MRZ lines (e.g., 210919 stands for 2021 September 19).

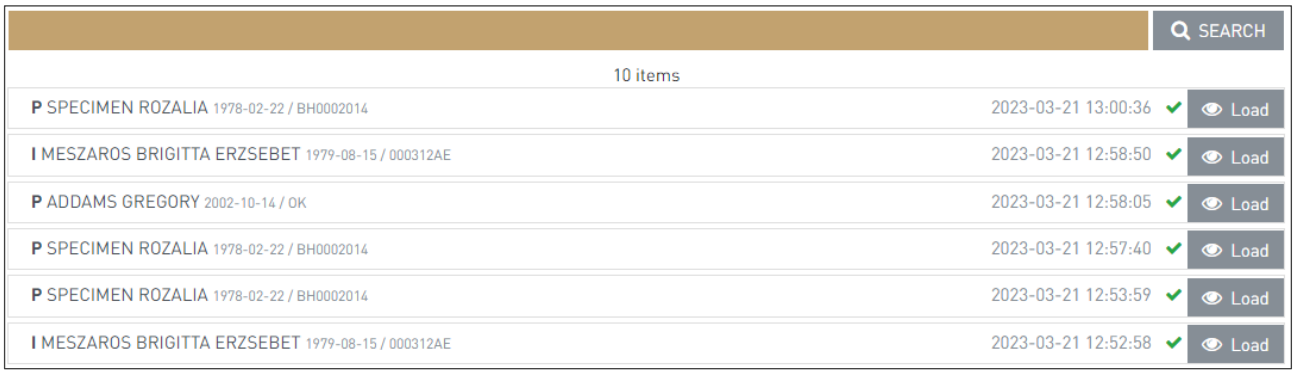
> Note
>
> The barcode and RFID data cannot be reloaded at **HISTORY / Load**.



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



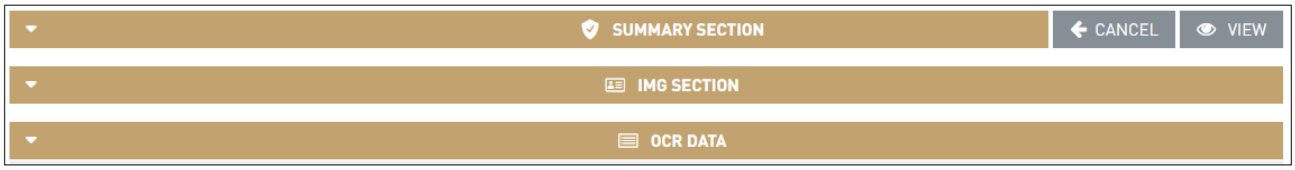


2.3.5. FILE UPLOAD

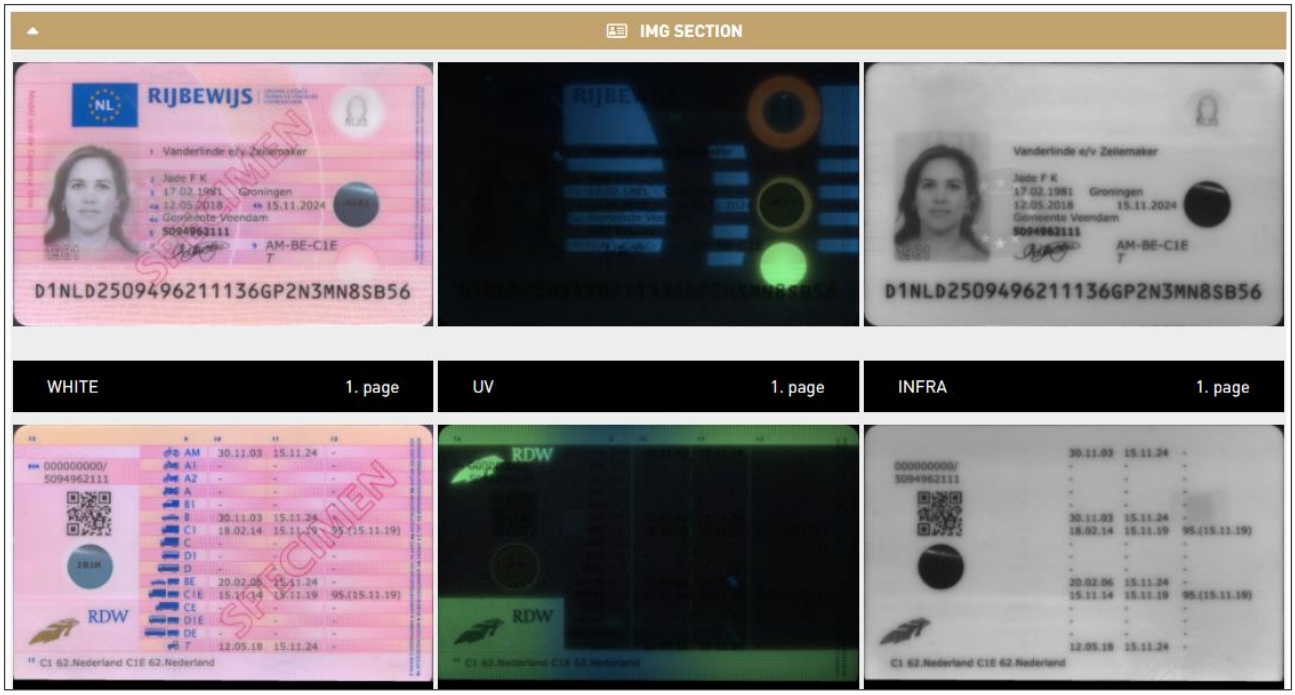
The Osmond device provides support to upload and process document packages that have been created earlier, using zip format (**SCAN PROCESS / PACKAGE FORMAT**).
The zip format includes document images, OCR-, and RFID data as well.

> **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:

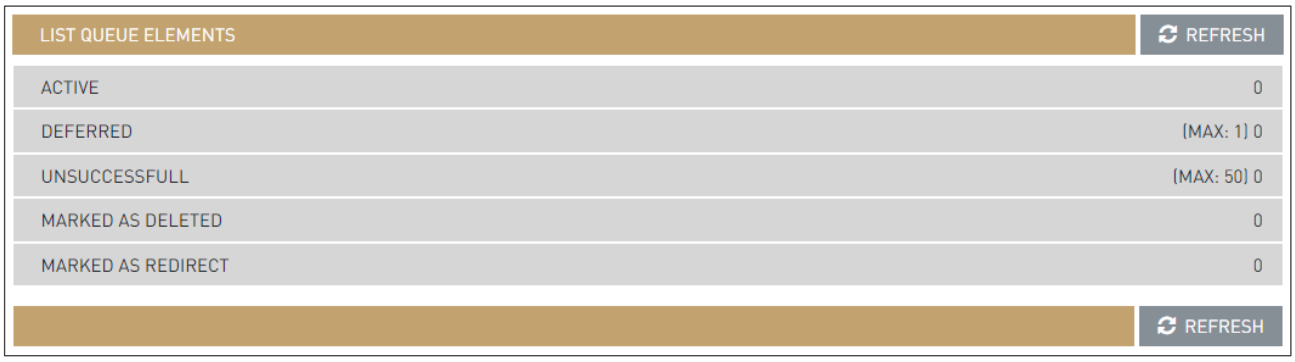


After clicking **[VIEW]**, the images and data from the .zip file is displayed as if it were a result of a live scanning process:



2.3.6. LIST QUEUE

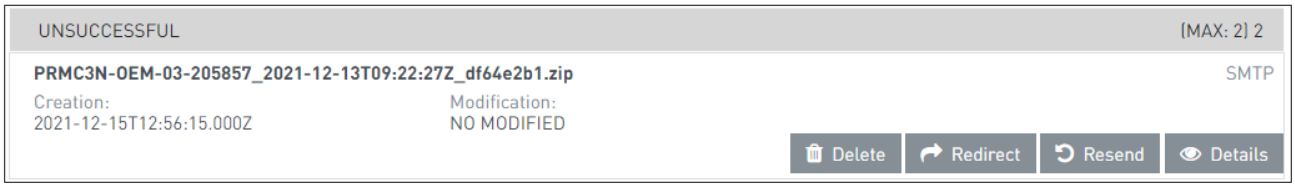
The Osmond device uses upload queue for uploading documents into remote servers. Using such queue, it is not necessary to wait for a document until it is uploaded but the next scanning process can be started immediately.



- **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.

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

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

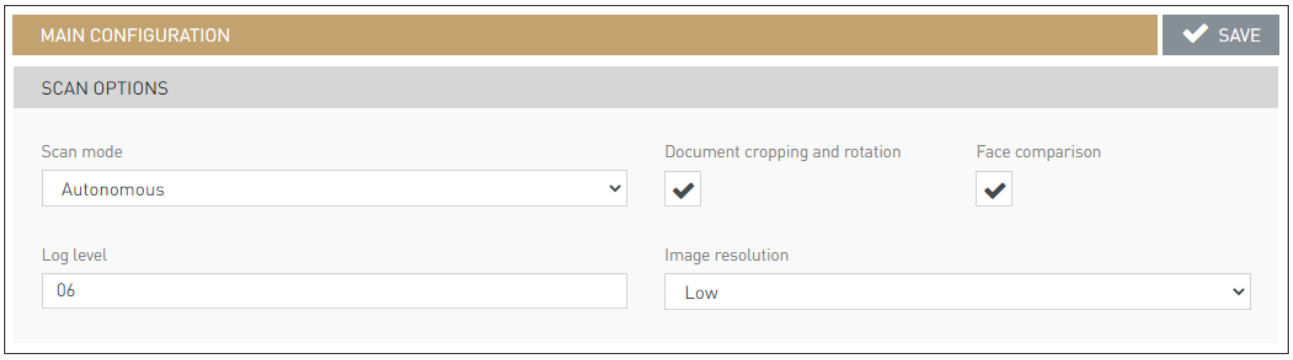
  1. value: 0-2

  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.

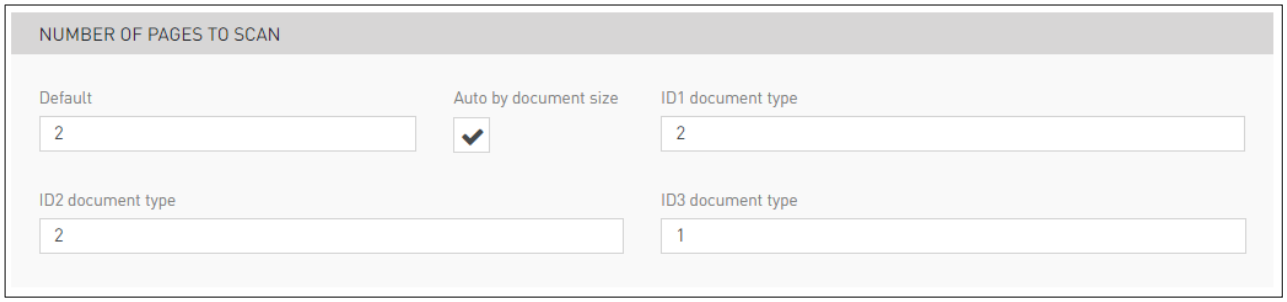


Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

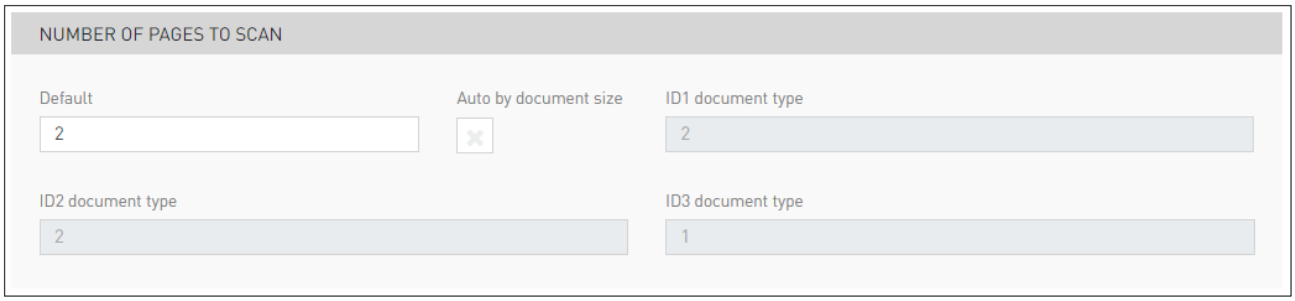
2. NUMBER OF PAGES TO SCAN

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 3/8 in x 2 1/8 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 1/8 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.

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

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.

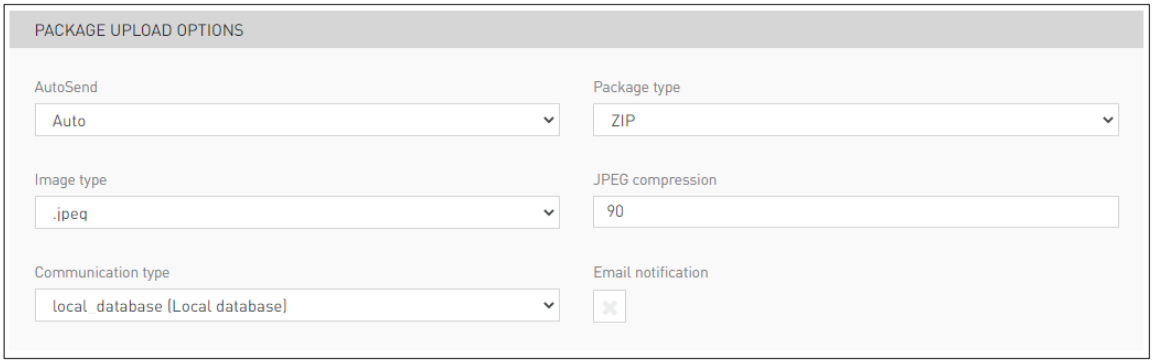
> Note
>
> Configuration of any upload protocol can be done in the **RESULT UPLOAD** menu, by clicking on the corresponding **[Edit]** button.

> 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

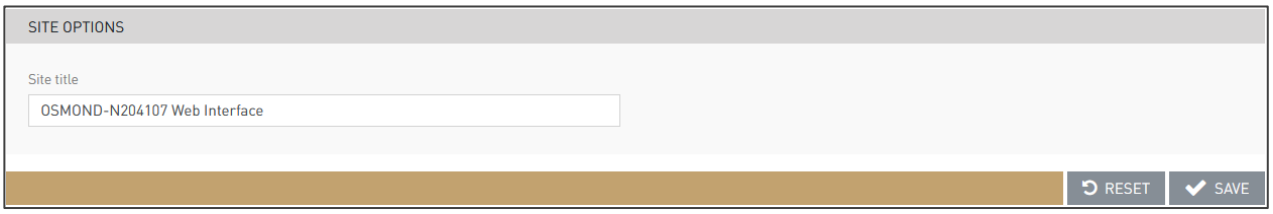
  If ".jpeg" is selected, its compression is configured as specified at **Jpeg compression**.

- 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

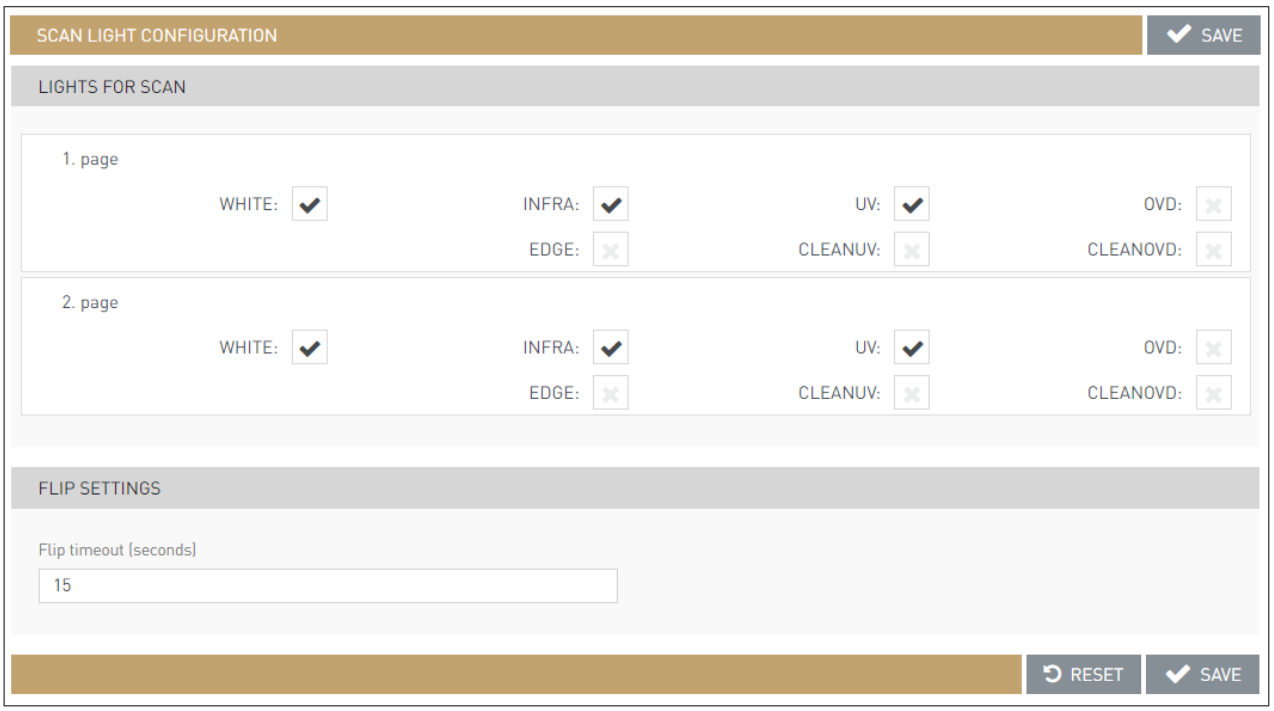
Users can also change the **Site title** of Osmond web interface website in browsers. The text displayed in the header of the browser can be customized in the **Site title** field, if the application is on the reading interface (**START APP** menu). In case of other menu items, the displayed address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



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

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

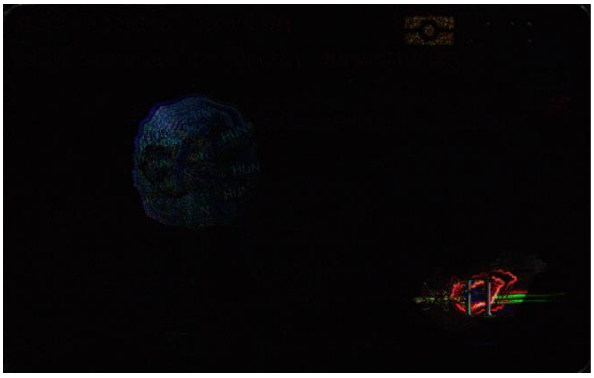
UV pattern

- **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

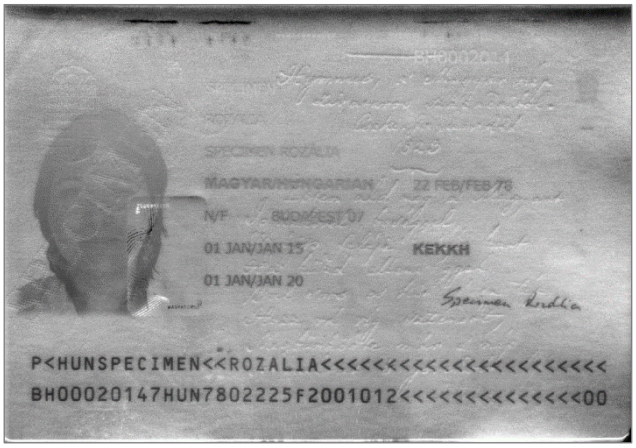
Image scanned in Photo light

> **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.

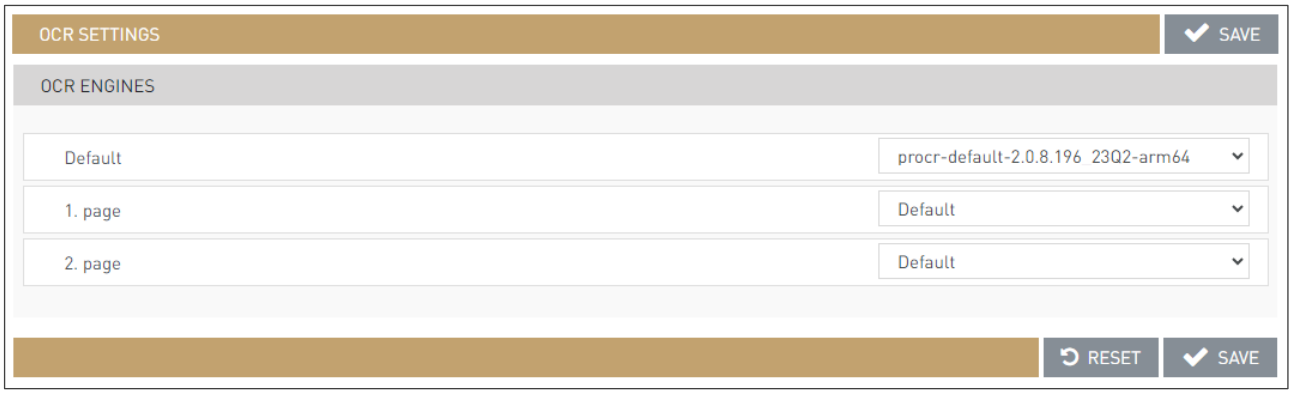
In case of a two-sided document:

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.



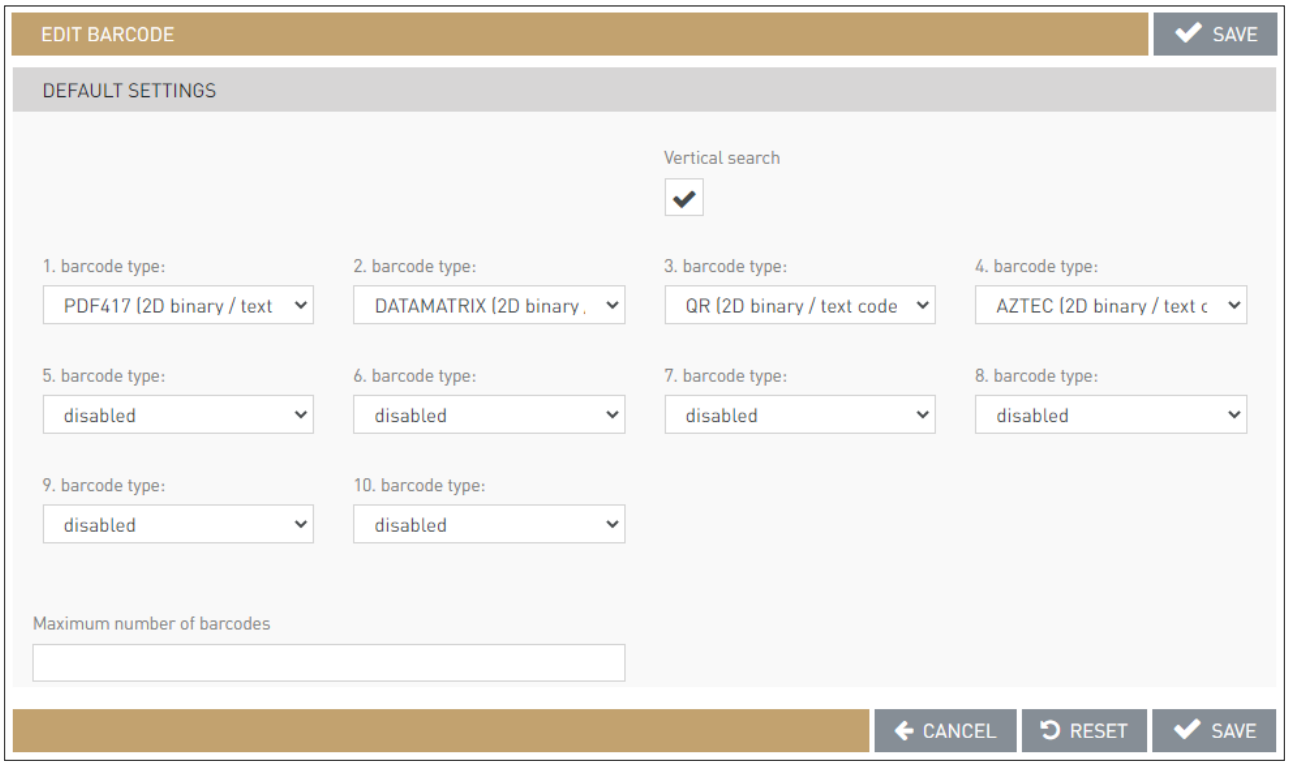
Note

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.

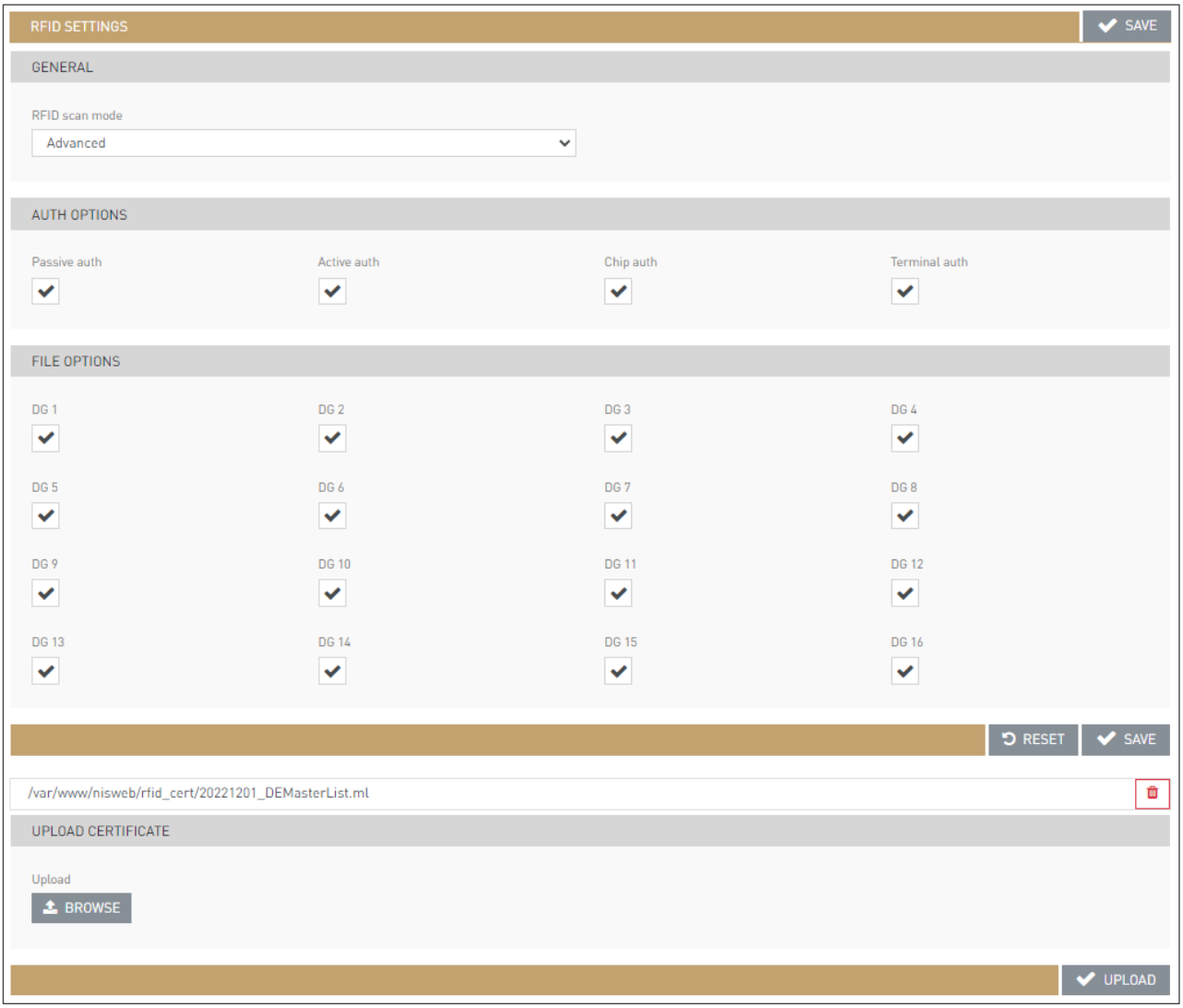
In order to configure the Application to read any barcode, all the available types should be selected in the **barcode type** textboxes. The barcode reading algorithm first searches for barcodes specified in **1. barcode type**, then for ones specified in **2. barcode type** and so on.

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

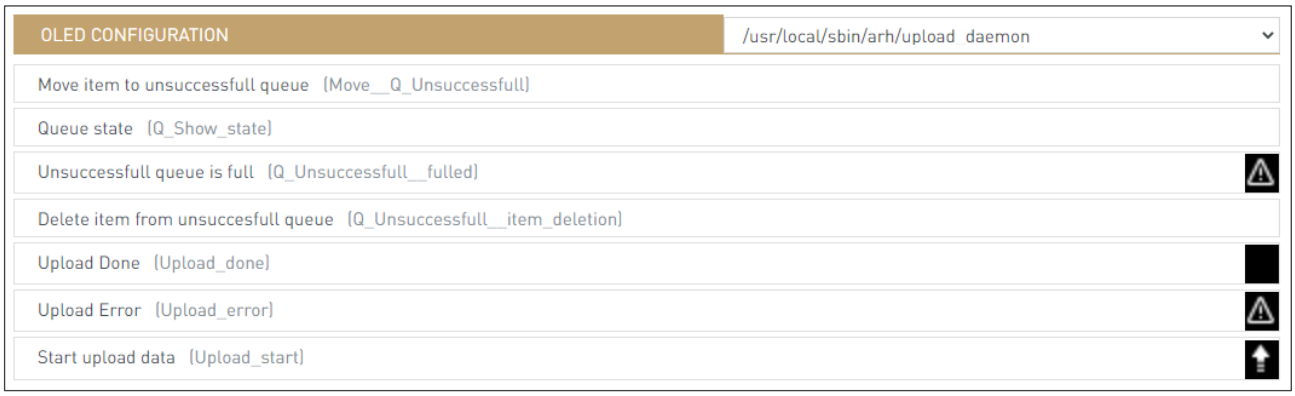
- Select the RFID scanning mode (**Off/Default/Advanced**)
- Select which RFID authentication should be performed (**PA, AA, CA, TA**)
- Which RFID files should be read from eDocuments (**DG1...DG16**)
- Upload **RFID certificate** usable for Passive Authentication (PA)



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

2.4.6. DISPLAY

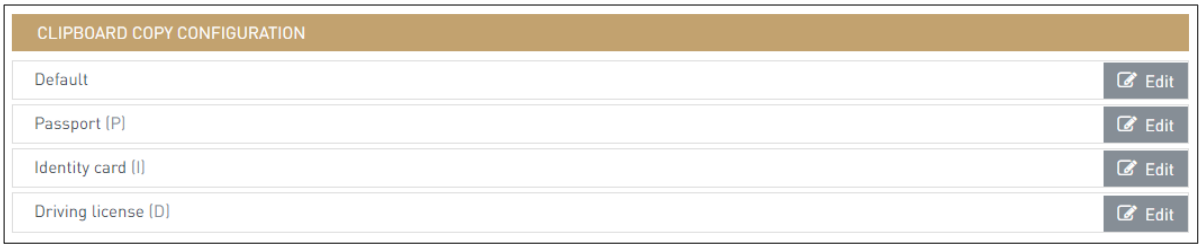
The **DISPLAY** menu lists the device statuses displayed on the OLED screen. For the various device states, the App can display an image, a text or blank screen which can be checked and viewed in this menu.



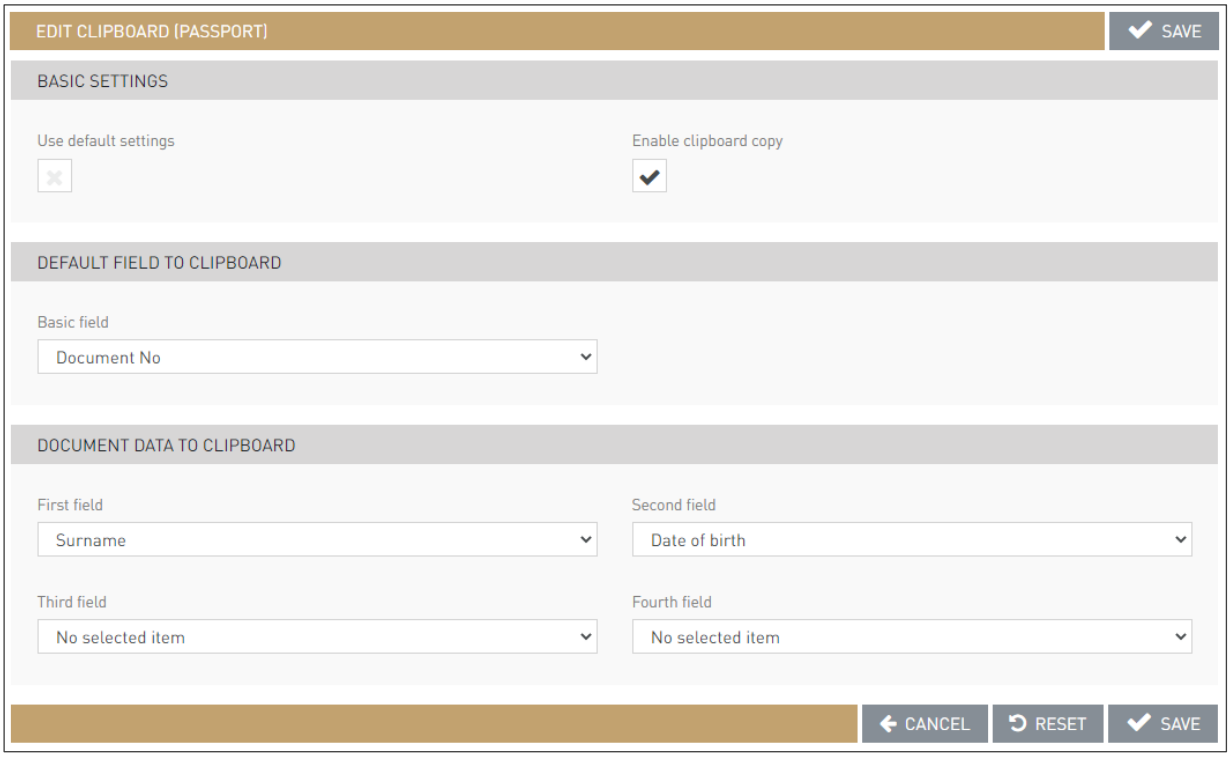
Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

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

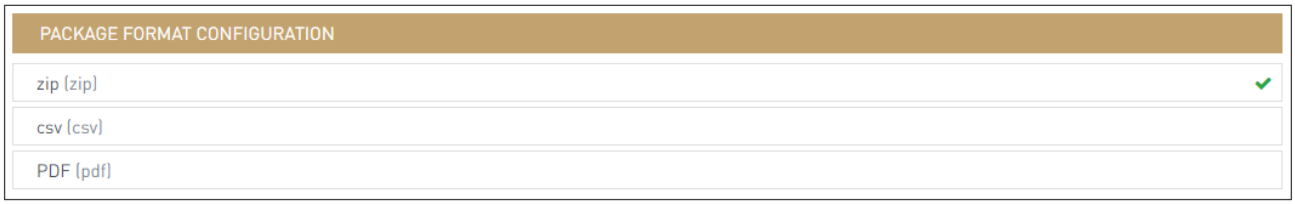
The Osmond device can upload images and data to remote targets packed into different formats:

- 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**.



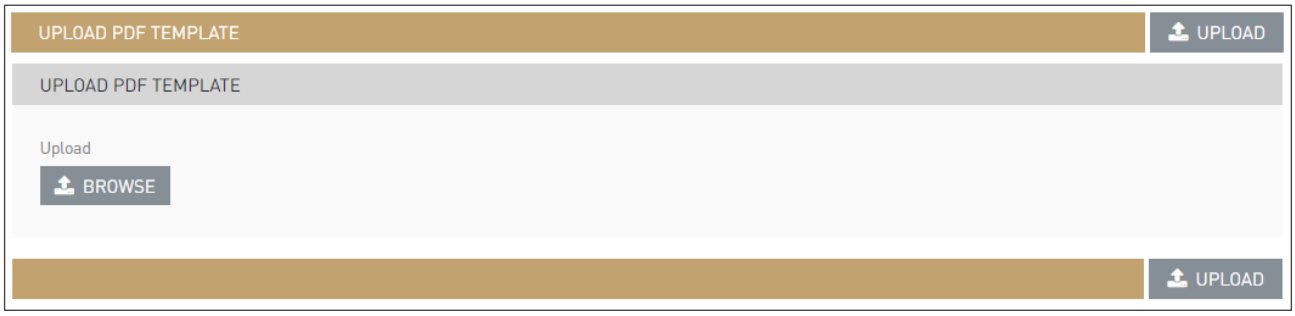
Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

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.



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

2.4.10. QUEUE OPTIONS

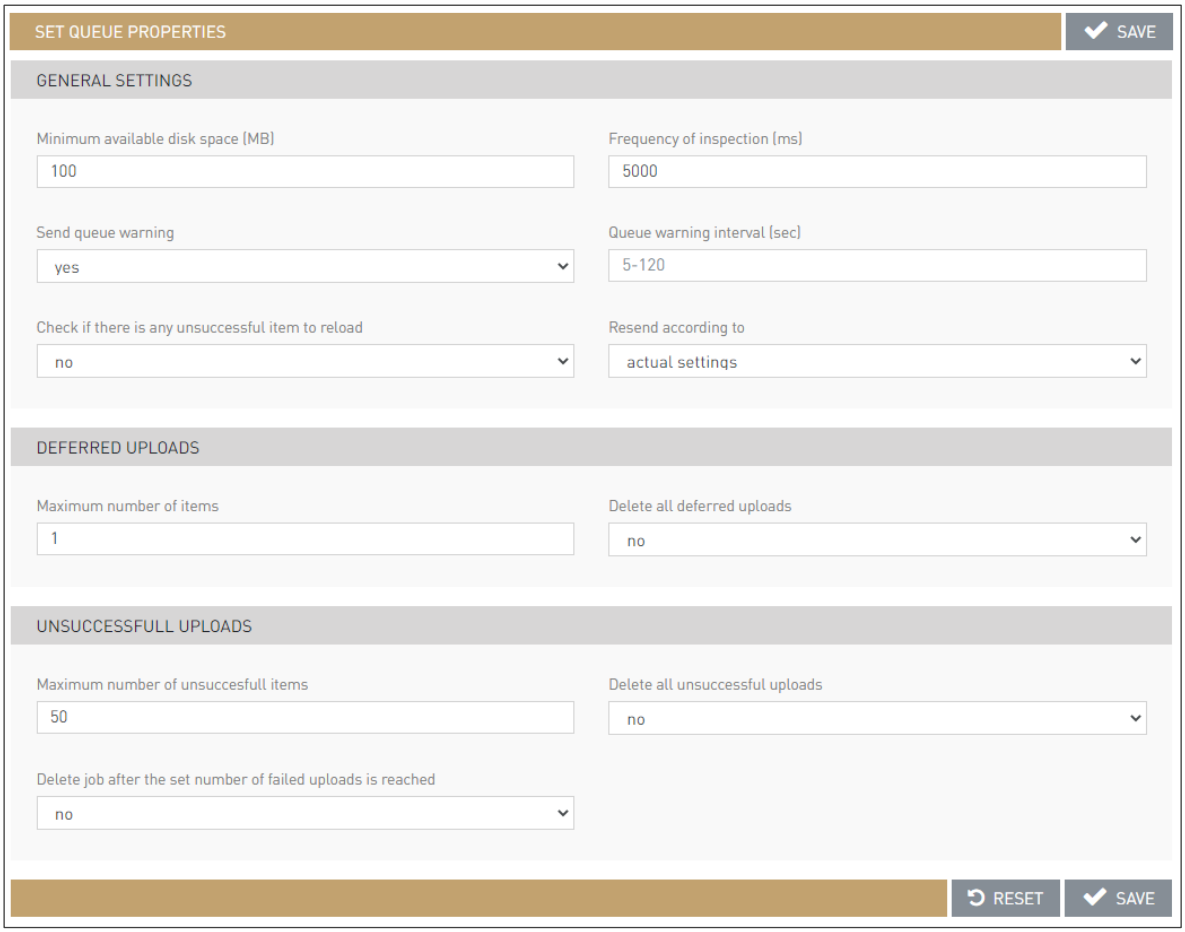
In this menu, owners may configure different queue settings.

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.



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

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!

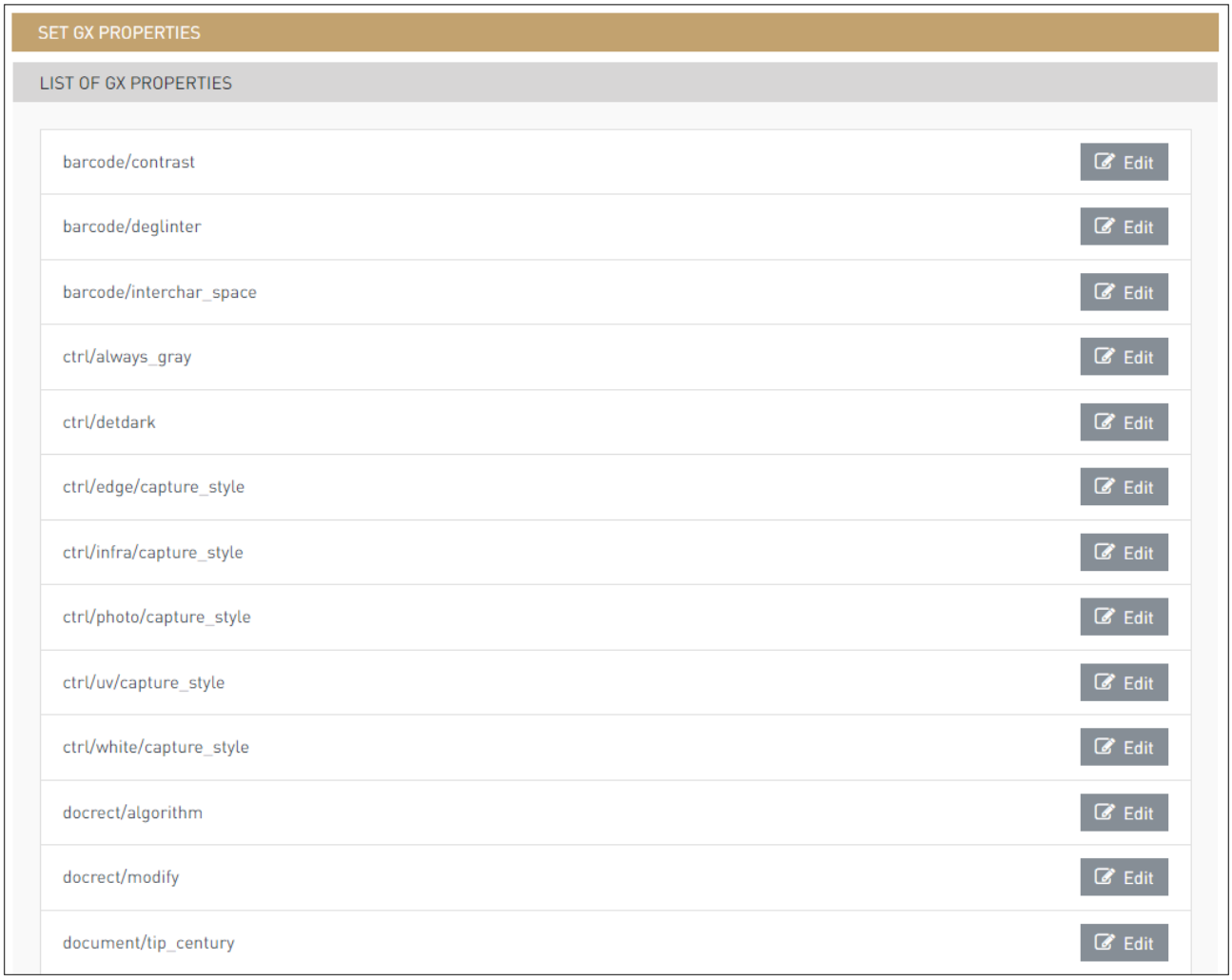
When setting the **Maximum number of items** or **Maximum number of unsuccessful items** to any value that is lower than the current number of items in queue, oldest items are deleted to meet new queue limit. E.g., if there are 5 documents in the **Unsuccessful queue** when **Maximum number of unsuccessful 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 **Nordic** REQUESTINFO@ADAPTIVERECOGNITION.COM
Adaptive Recognition **Hungary** Adaptive Recognition **Singapore** 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 **Nordic** REQUESTINFO@ADAPTIVERECOGNITION.COM
Adaptive Recognition **Hungary** Adaptive Recognition **Singapore** 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.

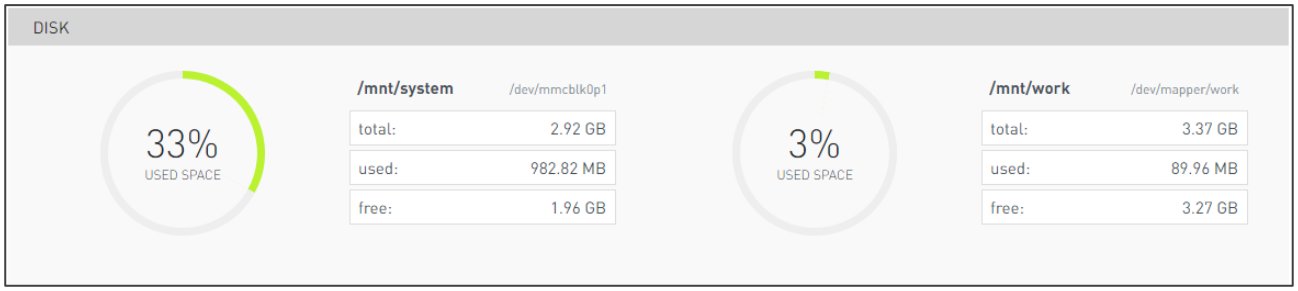
2.5.1. SYSTEM INFORMATION

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**



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

- 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.

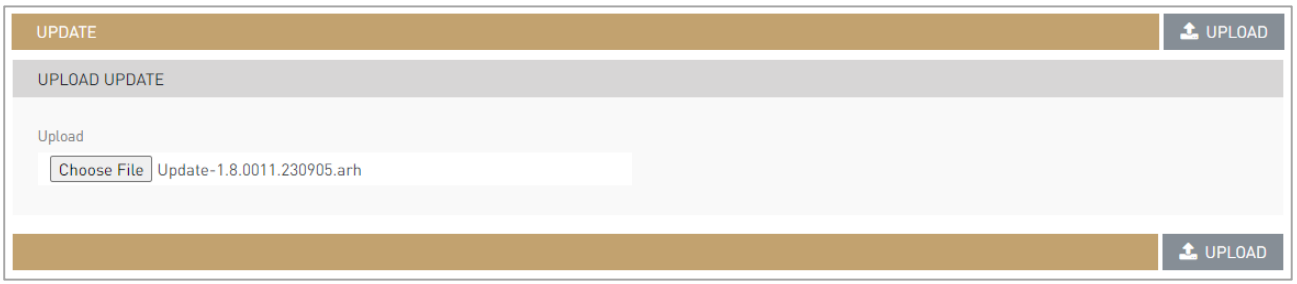
Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

2.5.3. UPDATE

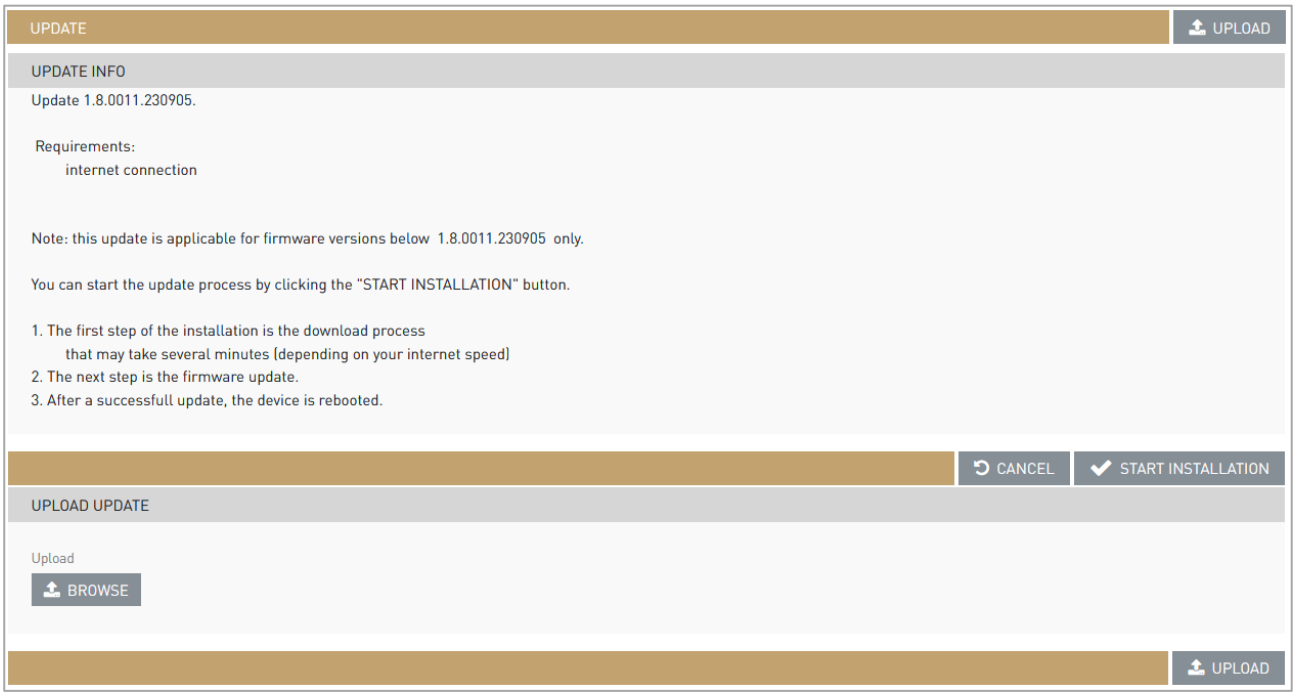
The purpose of the **UPDATE** menu is to provide an easy-to-use device firmware update feature for users with **Owner** privileges. Update files can be browsed and uploaded after clicking on the corresponding buttons.

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 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.

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

VIII. 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.

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

IX. 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.

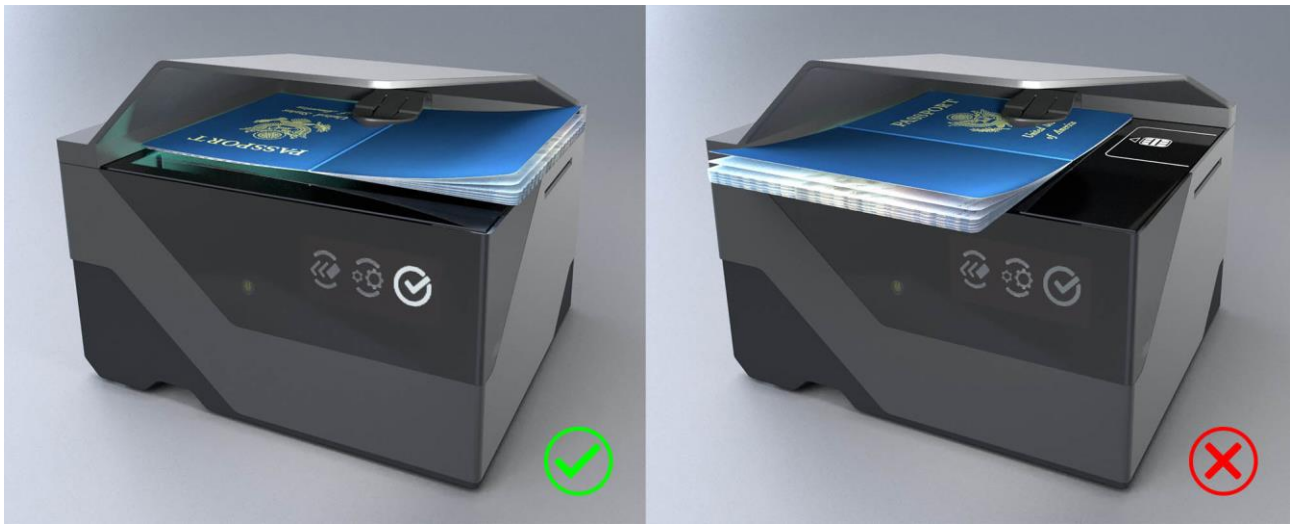
In case of **ID1** and **ID2 size cards** (like national ID cards, driver licenses, EHIC – European Health Insurance Card, name/business cards or any other 86x54mm = 3.4"x2.1" sized (or smaller) printed document), place them in the upper left corner of the scanning surface. The correct positioning must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

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

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.

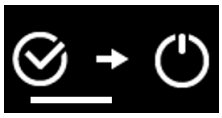
	Starting data upload	The data package upload is started.
	Upload done	The data package upload is successfully done.
	Upload error / Unsuccessful queue is full	The upload is failed or the documents in unsuccessful status have reached the maximum number of the unsuccessful queue.

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

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

	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

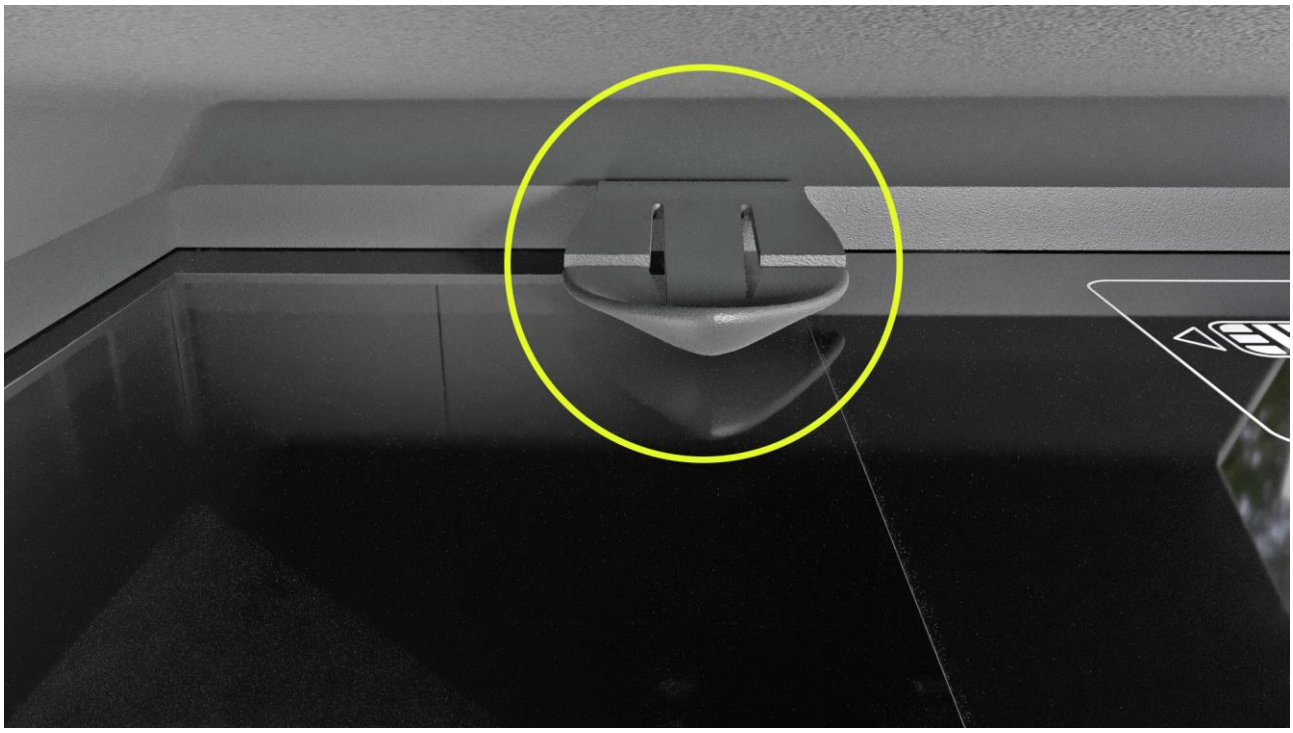
3.2. ICONS OF THE READING PHASES IN AUTONOMOUS MODE

- **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

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

4. REMOVING THE OSMOND DOCUMENT HOLDER

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



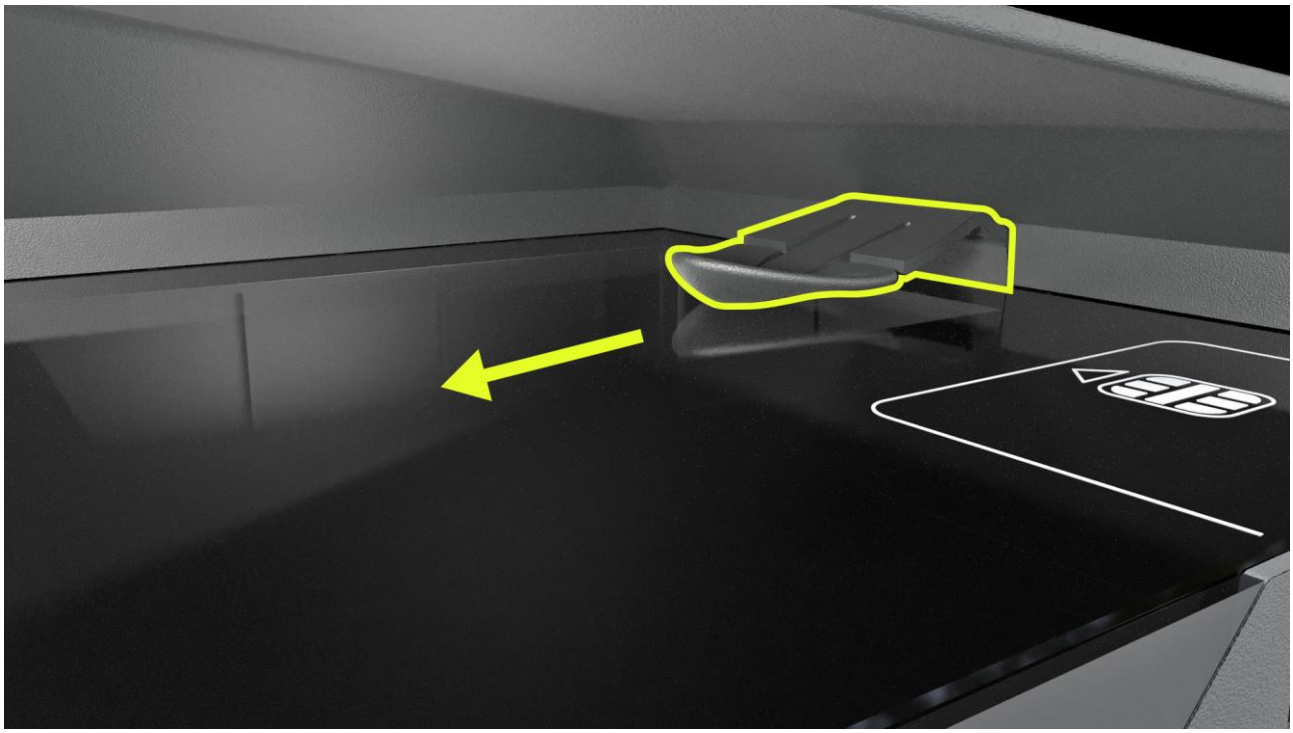
Document holder under the shield

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.

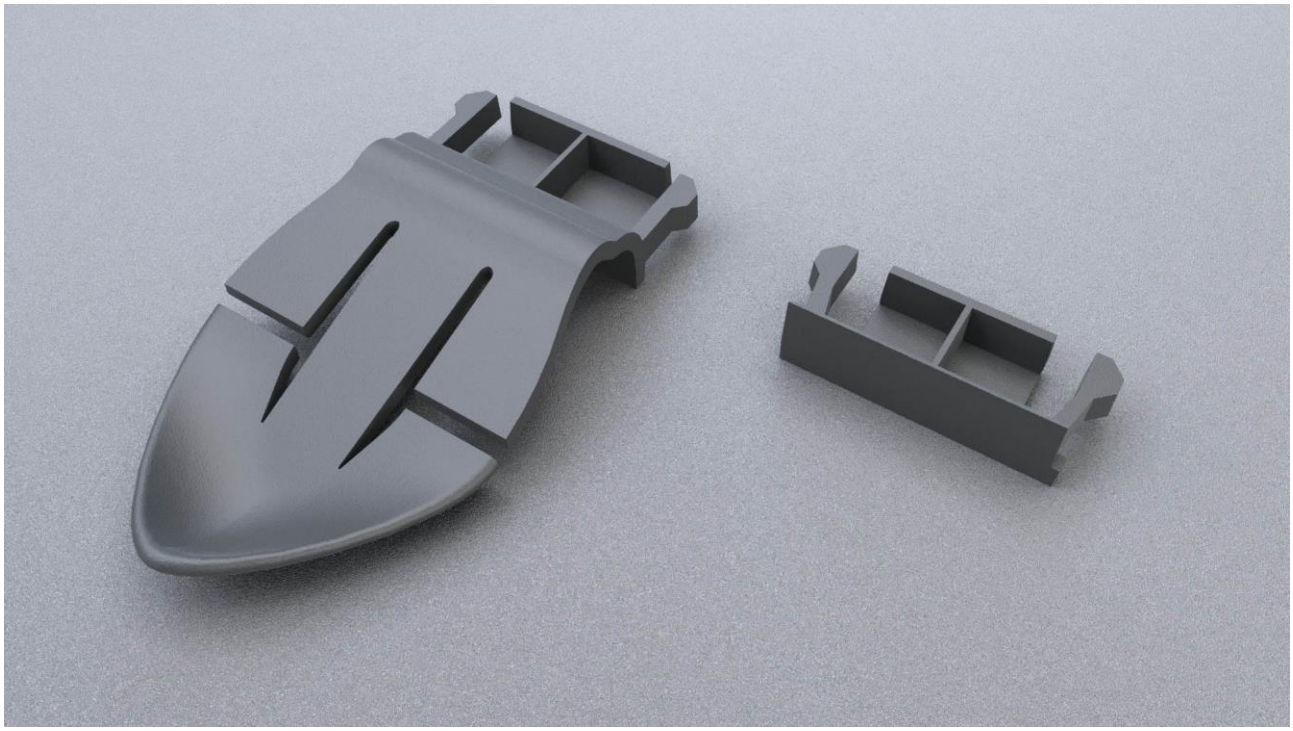
Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

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.



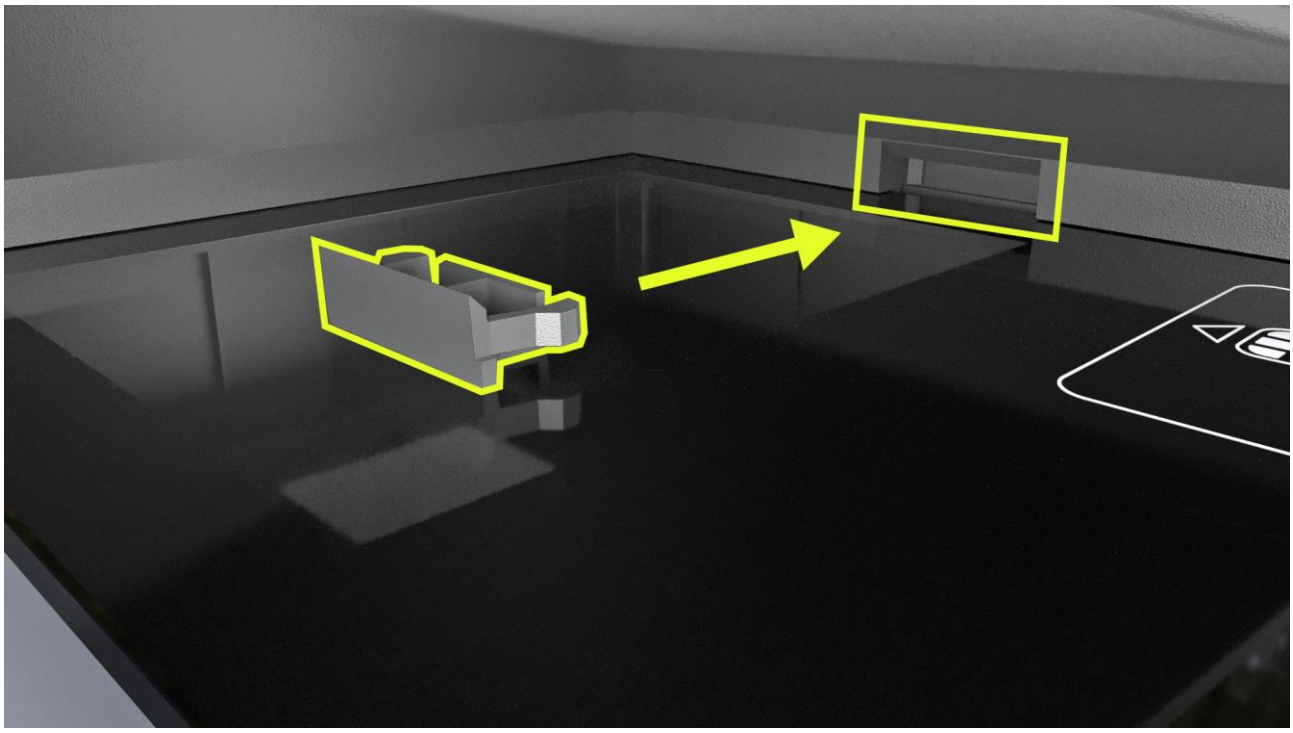
2. Look for the blind plug which is provided with the device in the box.



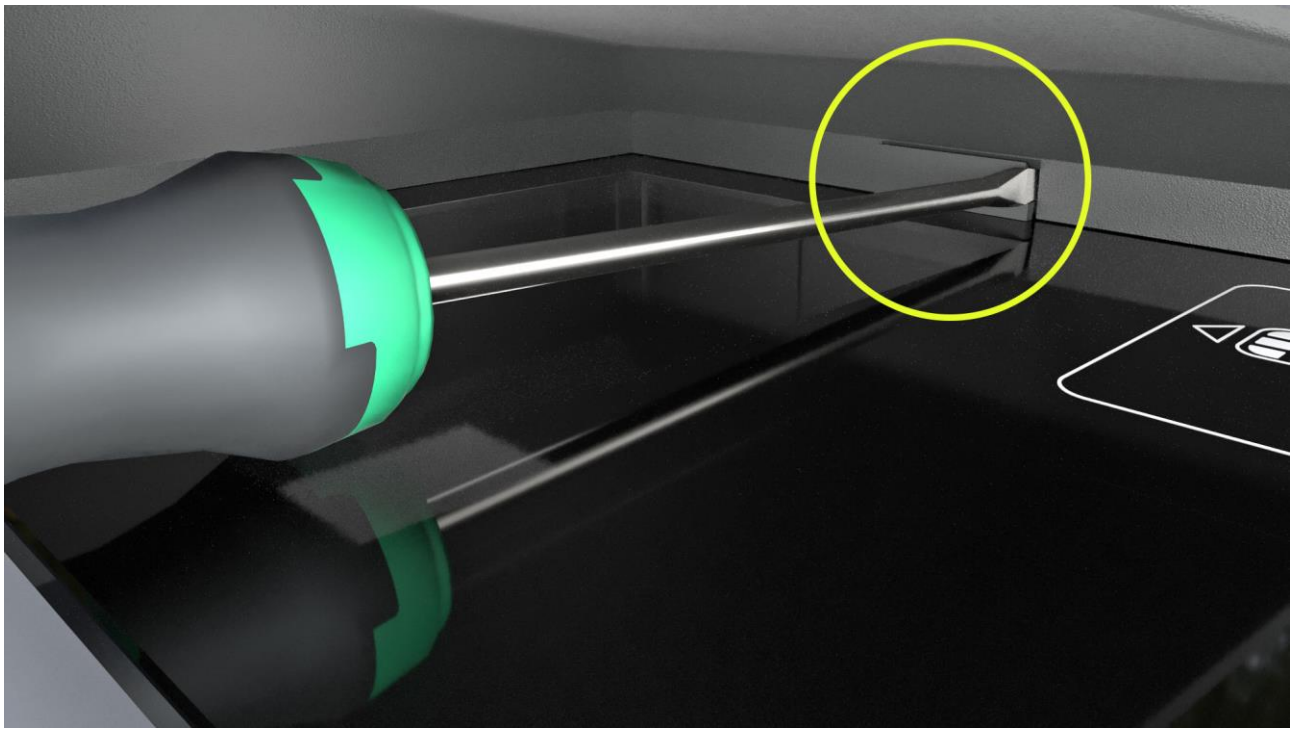
The document holder (left) and the blind plug (right)

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

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.

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

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.

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

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.

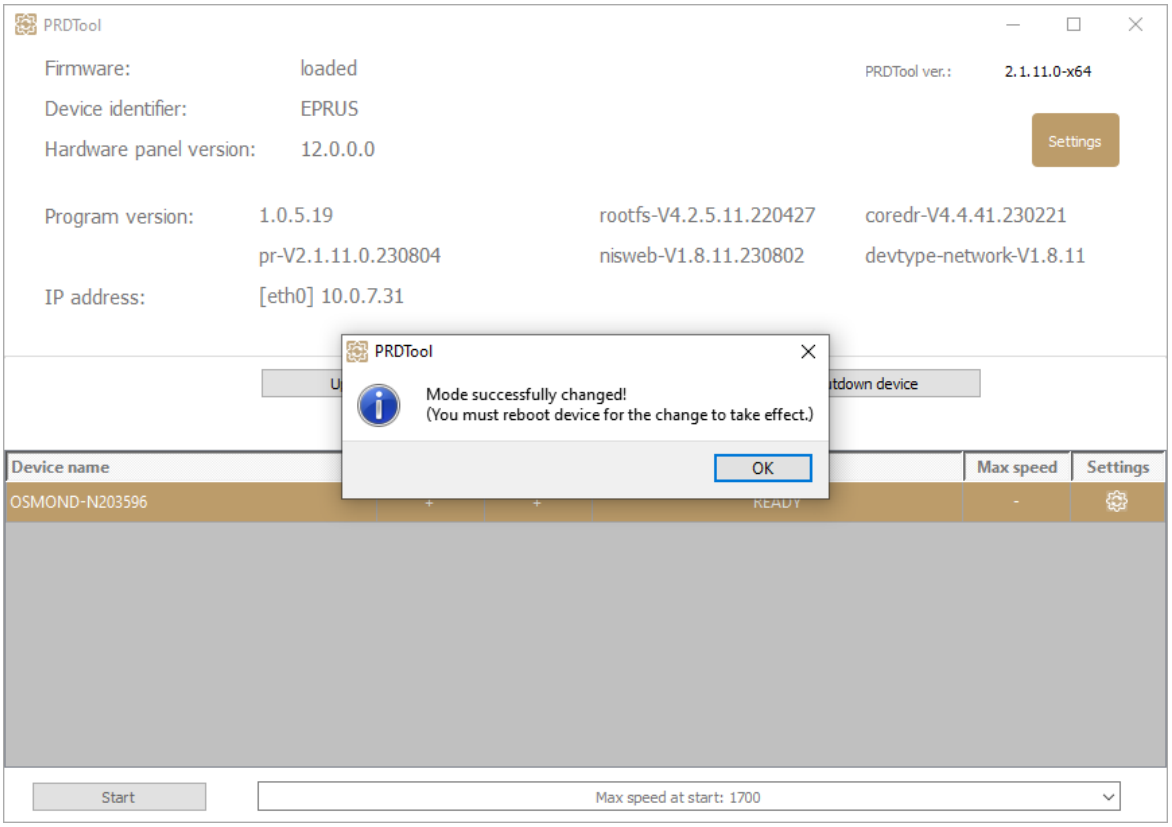
Hold the power touch button for a few seconds. The progress bar on the OLED screen shows the remaining time.

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

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

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.

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

Ways of uploading licenses

1. In case of **USB** devices:
   - For uploading licenses to a small number of specific scanners, our suggestion is using the License Manager application.
   - In case of uploading licenses to a larger quantity of scanners, we offer an automated license upload feature (MSI installer). For more information on it, see Automated Ways for License Upload chapter.
2. In case of **Network** devices:
   - Uploading licenses to a small number of scanners can be performed via web interface. For more information on this, see License Upload via Web Interface chapter.
   - In addition, license upload to one or more network devices can be performed in USB mode as well by using the License Manager application. Thereby, when operating the Osmond N in USB mode, there is no need to change the operation mode of the device.
   - In case of performing the license upload on a larger quantity of scanners and an operating update server owned by the customer is at disposal, we can provide the update package which can be sent to the given devices through the update server. For more information on it, contact ADAPTIVE RECOGNITION support team.
   - In case of a larger quantity of scanners without an operating update server, the device can download and install the update package automatically, from the default AdaptiveRecognition update server ("update.adaptiverecognition.com") via web interface. Note, that the given device(s) must have access to this update server. For more information on it, contact ADAPTIVE RECOGNITION support team.

Migrating licenses between devices

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

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.

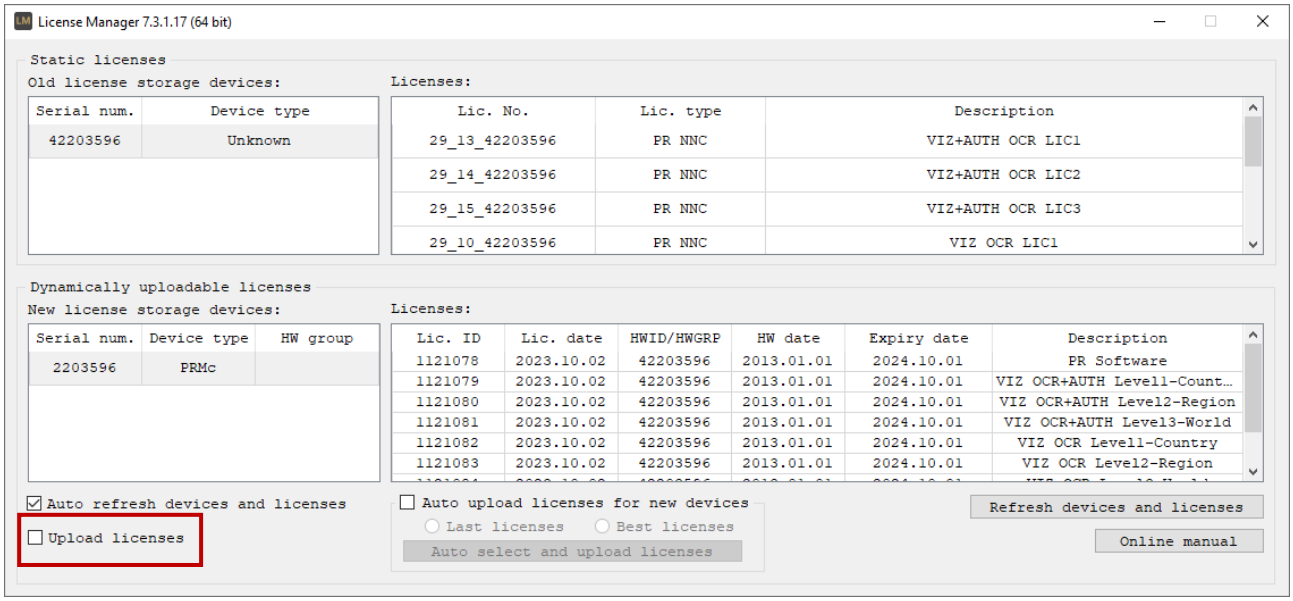
8.1.1. INSTALLATION

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.

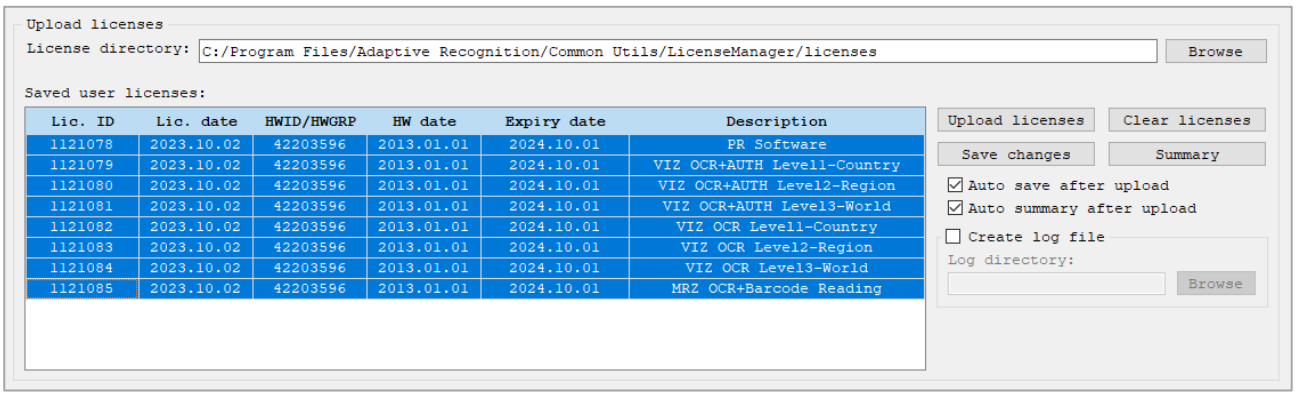
> **Note**
>
> If "**Auto upload licenses for new devices**" is enabled, the function is greyed out.



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

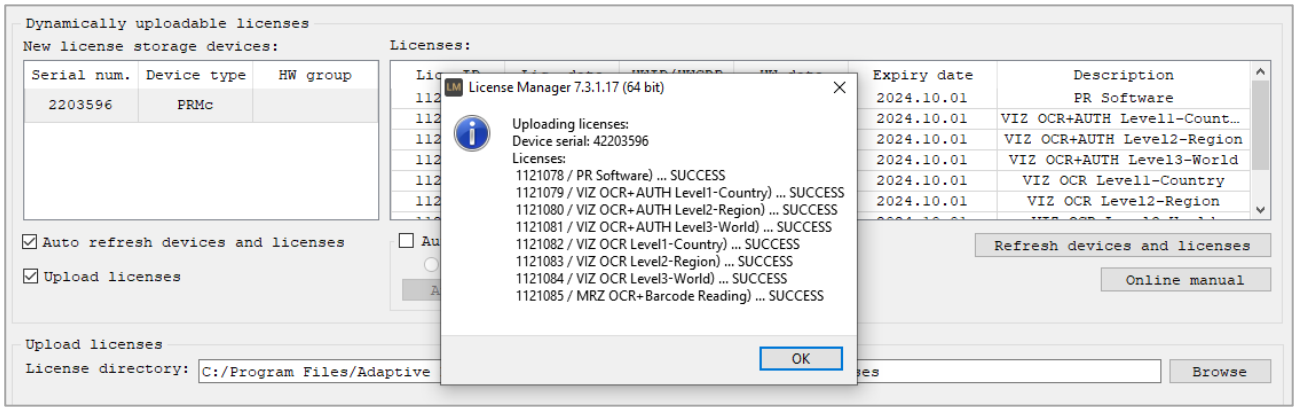
3. **Select the license(s) to upload** to your device.

> **Note**
>
> In order to select more licenses at the same time, use **Ctrl + left click**.
> In order to select all the licenses at the same time, use the **Ctrl + A** keyboard shortcut.



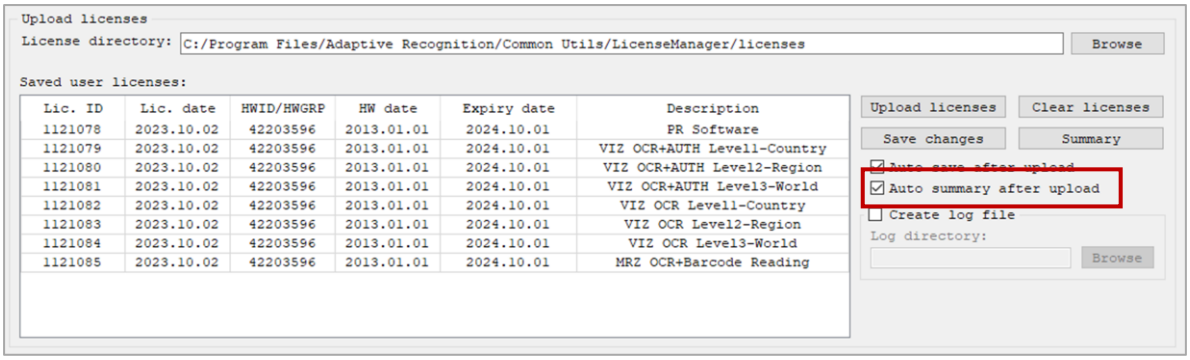
> **Hint**
>
> By enabling the "**Auto upload licenses for new devices**" option, licenses can be uploaded automatically, according to one of the following logics:
>
> a. **Last licenses**: Automatically upload the latest license file for the connected device (license update).
>
> b. **Best licenses**: 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.

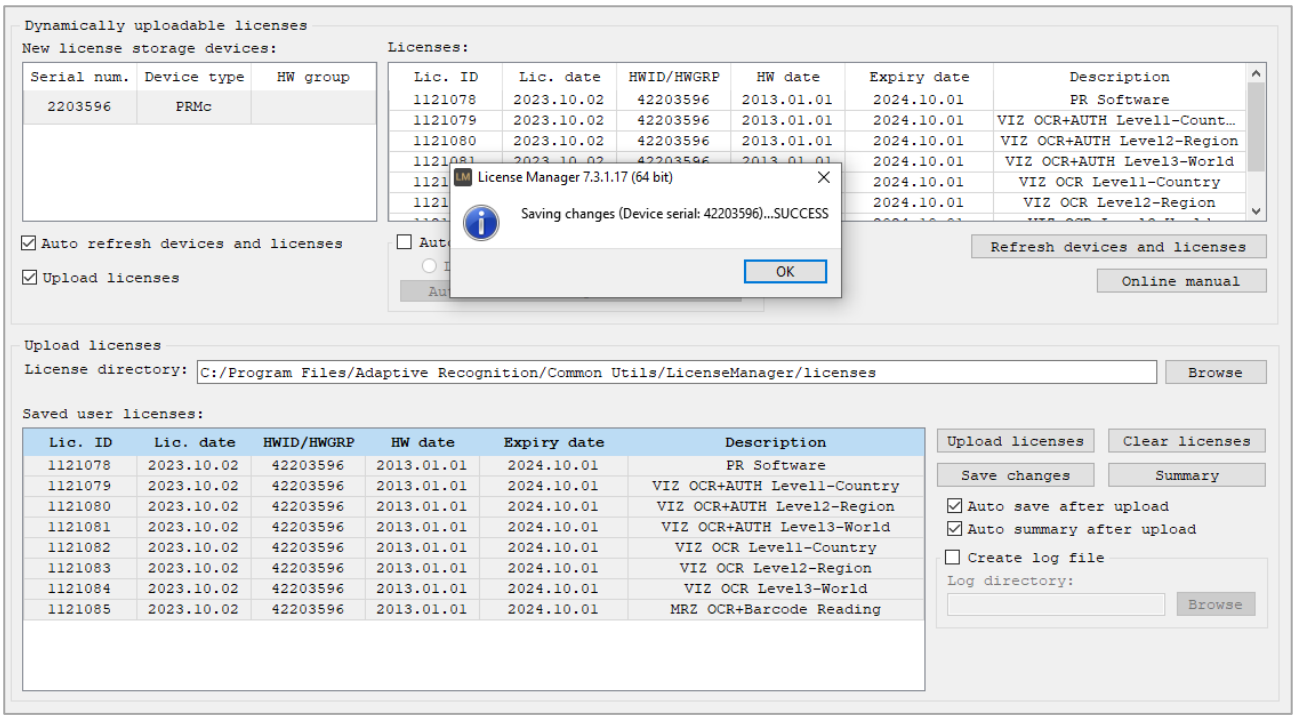


Hint

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

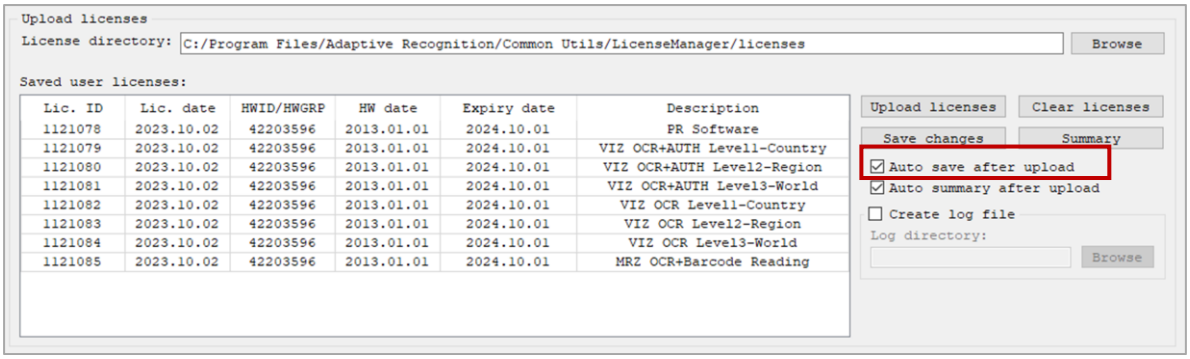


5. **Click on "Save changes"** and exit the application.



Hint

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



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

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.

> **Note**
>
> This functionality is only available for USB document scanners or devices operating in USB mode.

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

8.3. LICENSE UPLOAD VIA WEB INTERFACE

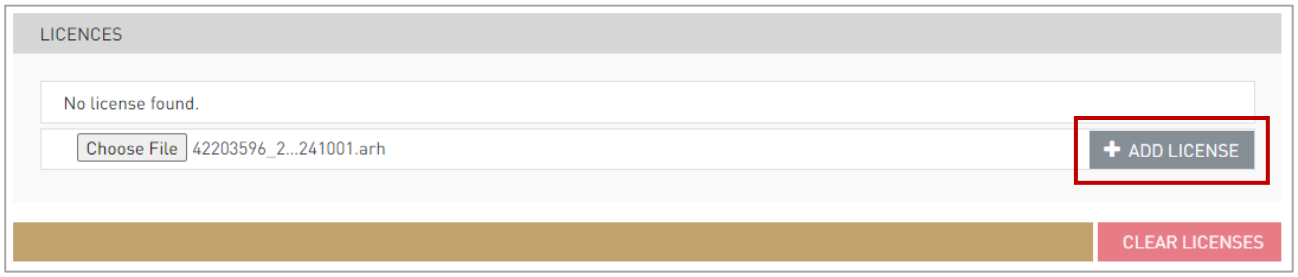
> **Note**
>
> This functionality is only available for Osmond N in network mode.

1. First you need to sign in on the web interface of the Osmond N reader.

> **Note**
>
> In order to access the web interface of the Osmond N 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.

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

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**.

LICENCES

No.	Lic.ID	Lic.date	HWID	Expiry date	Description
1	1121078	2023.10.02	42203596	2024.10.01	PR Software
2	1121079	2023.10.02	42203596	2024.10.01	VIZ OCR+AUTH Level1-Country
3	1121080	2023.10.02	42203596	2024.10.01	VIZ OCR+AUTH Level2-Region
4	1121081	2023.10.02	42203596	2024.10.01	VIZ OCR+AUTH Level3-World
5	1121082	2023.10.02	42203596	2024.10.01	VIZ OCR Level1-Country
6	1121083	2023.10.02	42203596	2024.10.01	VIZ OCR Level2-Region
7	1121084	2023.10.02	42203596	2024.10.01	VIZ OCR Level3-World
8	1121085	2023.10.02	42203596	2024.10.01	MRZ OCR+Barcode Reading

BROWSE ADD LICENSE

CLEAR 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.

Alerts and messages (2)

Done (2023-10-02 16:04:15) License Manager is uploaded — Remove alert

success (2023-10-02 16:01:09) Saving changes...OK — Remove alert

all — Remove all

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.

Note

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

Note

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

Note

In case of purchasing **VIZ OCR or VIZ AUTH OCR engine**, it is strongly recommended to use 64-bit operating systems.

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

Ways of uploading OCR engines

1. In case of **USB** devices:
   - OCR engines can be uploaded with MSI installer. For more information on this, see Uploading OCR Engines to USB Devices chapter.

2. In case of **Network** devices:
   - OCR engines can be uploaded to network devices via web interface. For more information on this, see Uploading OCR Engines to Network Devices chapter.
   - In addition, OCR engine upload to one or more network devices can be performed in USB mode as well, with MSI installer. Thereby, when operating the Osmond N in USB mode, there is no need to change the operation mode of the device. For more information on this, see Uploading OCR Engines to USB Devices chapter.
   - In case of uploading the OCR engines to a larger quantity of scanners and an operating update server owned by the customer is at disposal, we can provide the update package which can be sent to the given devices through the update server. For more information on it, contact ADAPTIVE RECOGNITION support team.
   - In case of a larger quantity of scanners without an operating update server, the device can download and install the update package automatically, from the default ADAPTIVE RECOGNITION update server ("update.adaptiverecognition.com") via web interface. Note, that the given device(s) must have access to this update server. For more information on it, contact ADAPTIVE RECOGNITION support team.

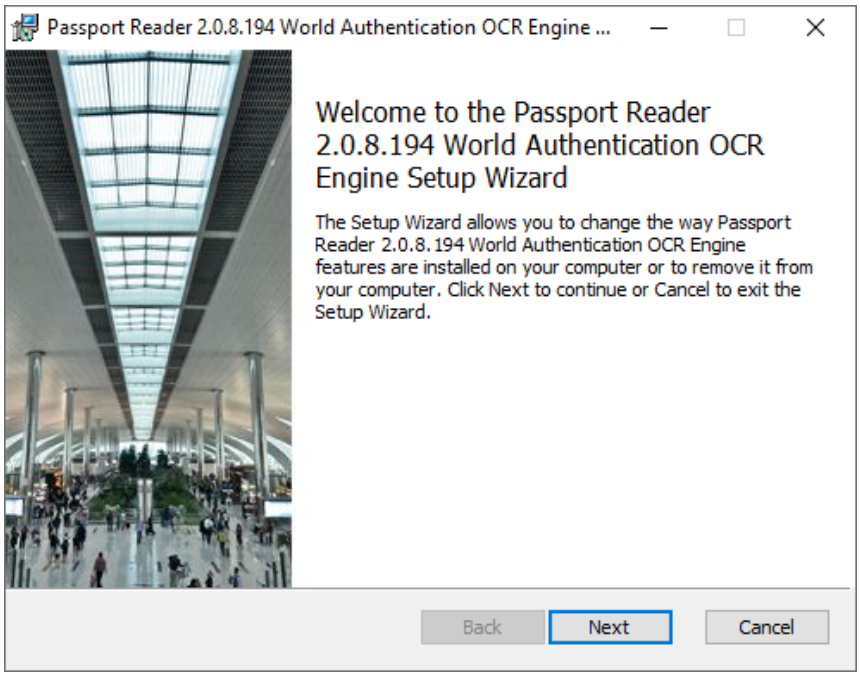
9.1. UPLOADING OCR ENGINES TO USB DEVICES

Important!

Administrator rights are needed for installation.

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

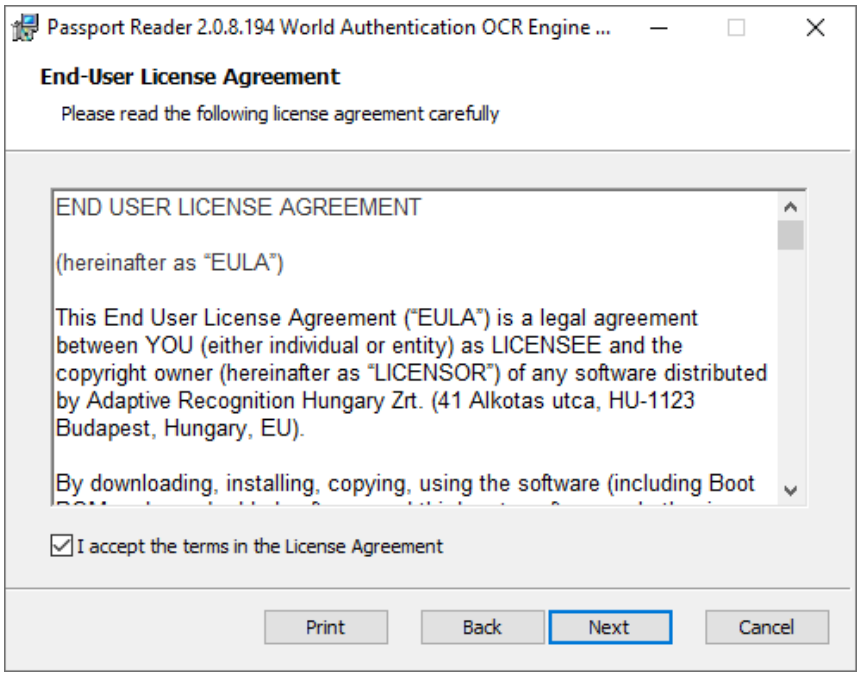
1. On the website click on **Engines** and click on the **[Download]** button belonging to the selected OCR engine (VIZ OCR or VIZ AUTH OCR).
2. By clicking on the **[Download]** button, the webpage redirects you to the **VIZ OCR Software Add-On for VIZ reading** (in case of VIZ OCR) or **Authentication Software Add-Ons for AR ID reading** (in case of VIZ AUTH OCR) 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** (in case of VIZ OCR) or **procr-XXX_auth-2.0.X.XX.msi** (in case of VIZ AUTH OCR) installer.
6. The installation starts with the following window:



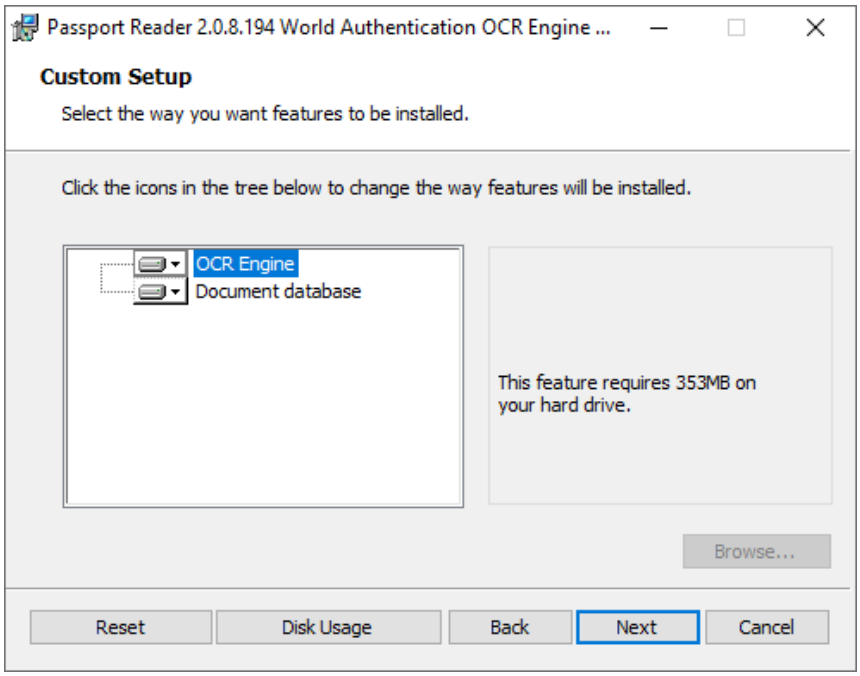
7. Click **[Next]** to launch installation.

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

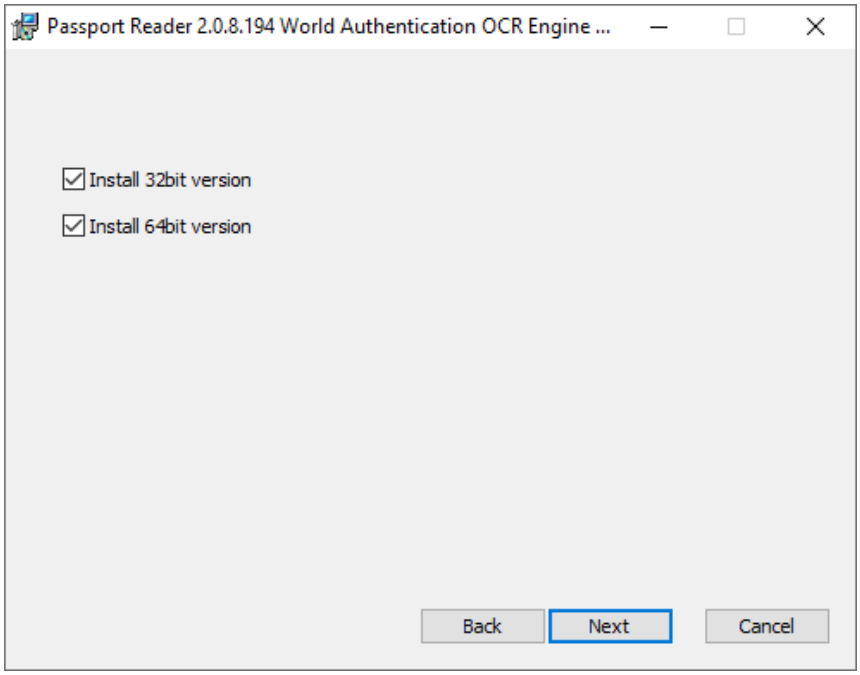
8. Accept the EULA (by ticking the checkbox) and start the custom installation process by clicking on **[Next]**.



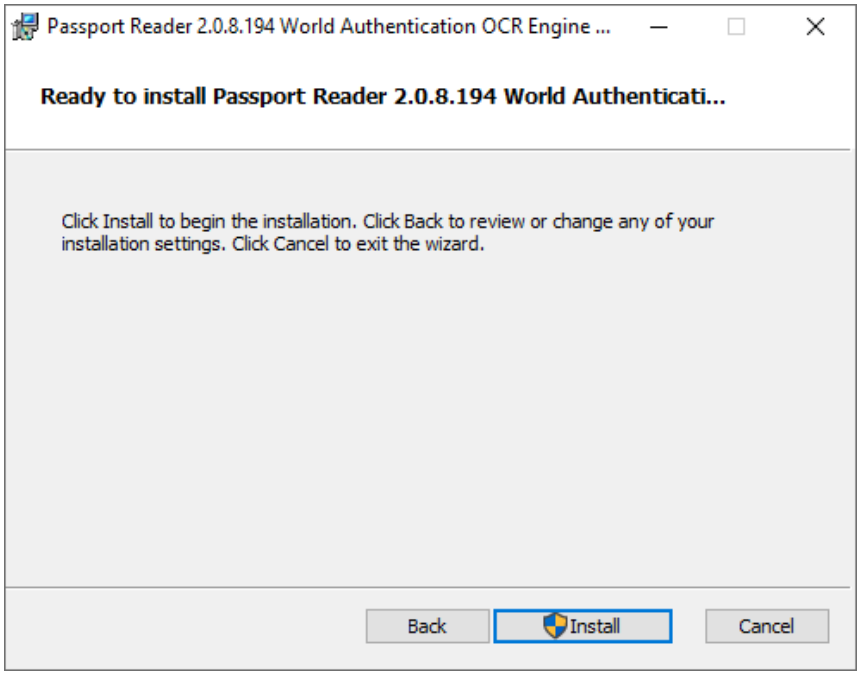
9. In the **Custom Setup** window, select the modules to be installed according to your preferences.

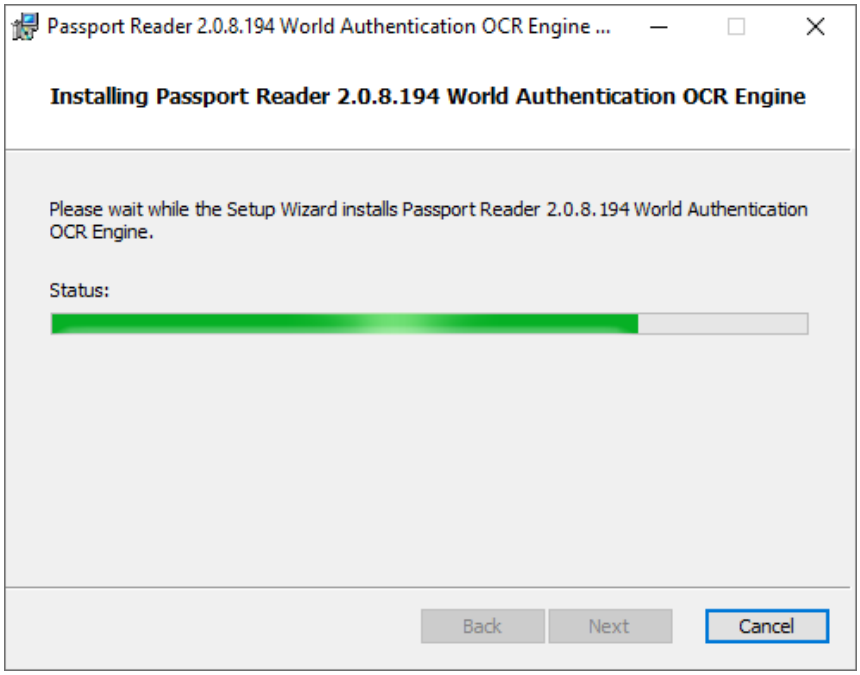


10. Select the bit version of the engine to be installed according to your system architecture.

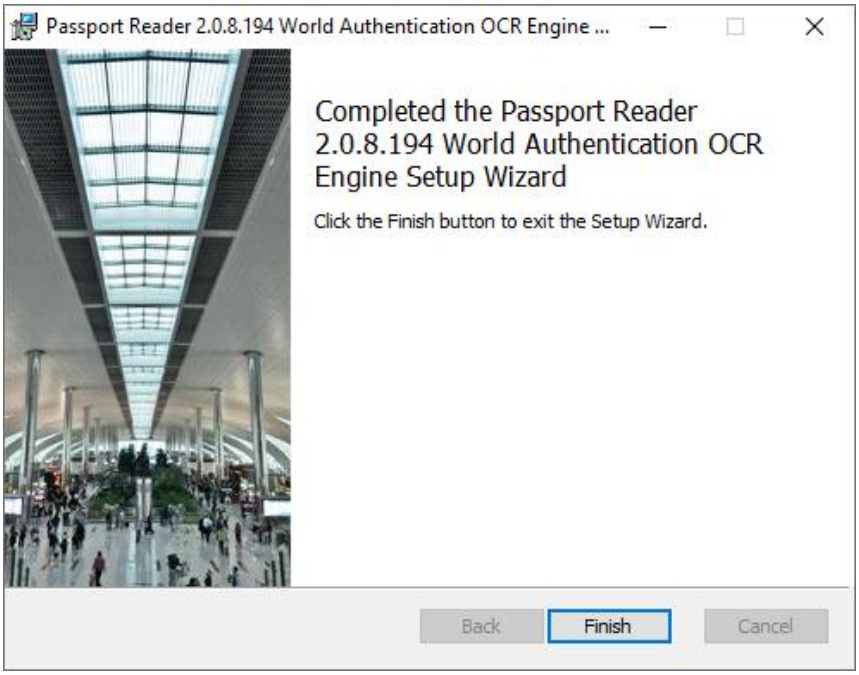


11. Clicking on **[Install]** will begin installation.

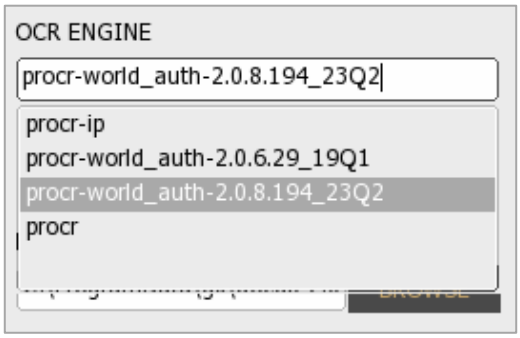




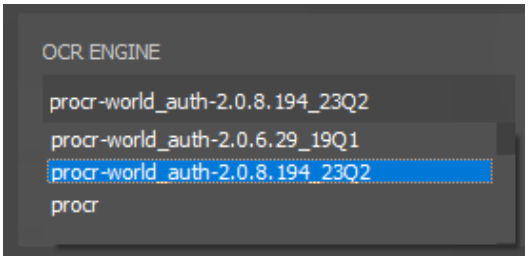
12. Click **[Finish]** to complete the installation.



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

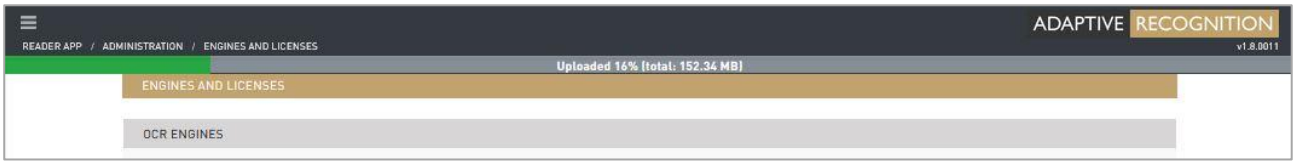
9.2. UPLOADING OCR ENGINES TO NETWORK DEVICES

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

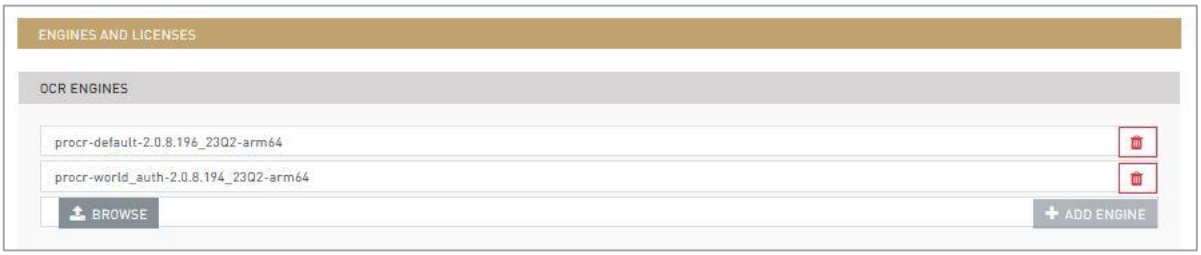
1. On the website click on **Engines** and click on the **[Download]** button belonging to the selected OCR engine (VIZ OCR or VIZ AUTH OCR).
2. By clicking on the **[Download]** button, the webpage redirects you to the **VIZ OCR Software Add-On for VIZ reading** page.
3. Under **Engines** select the 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.



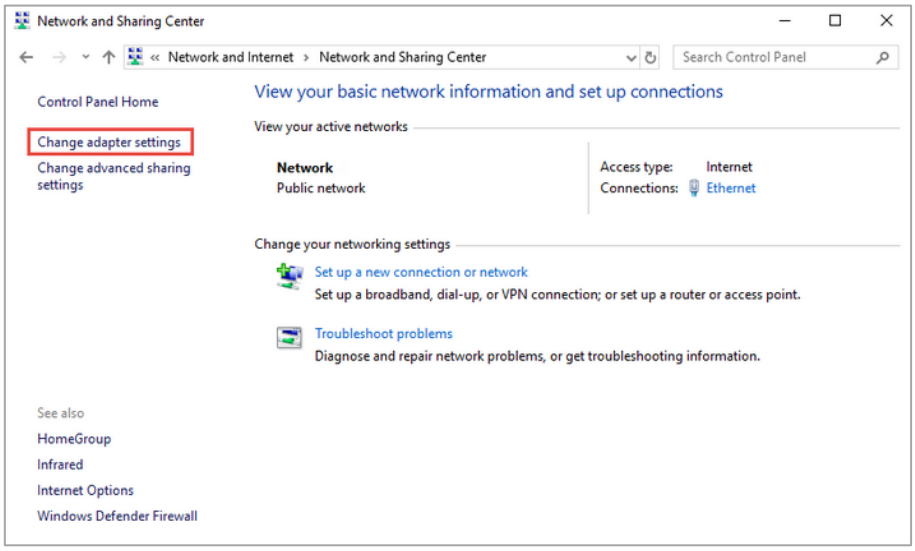
8. After a few seconds, the uploaded engine is listed under the **OCR ENGINES** section. If the given engine is not displayed, press Ctrl + F5.



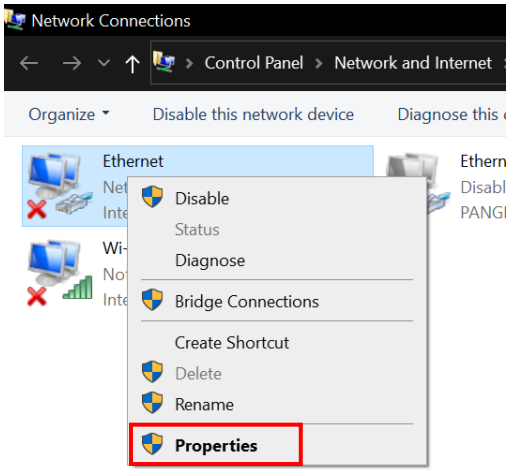
10. DIRECT ETHERNET CONNECTION

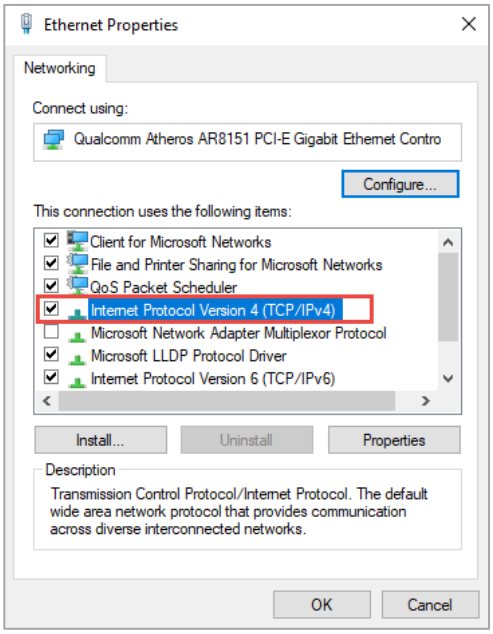
If you connect the device directly to the PC with an Ethernet cable, you can reach the device on its default IP 192.0.2.3, but you need to modify your Ethernet adapter settings manually.

1. In order to do so, please open "**Network and Sharing Center**" in **Windows Control Panel** and click on "**Change adapter settings**" located on the left side.

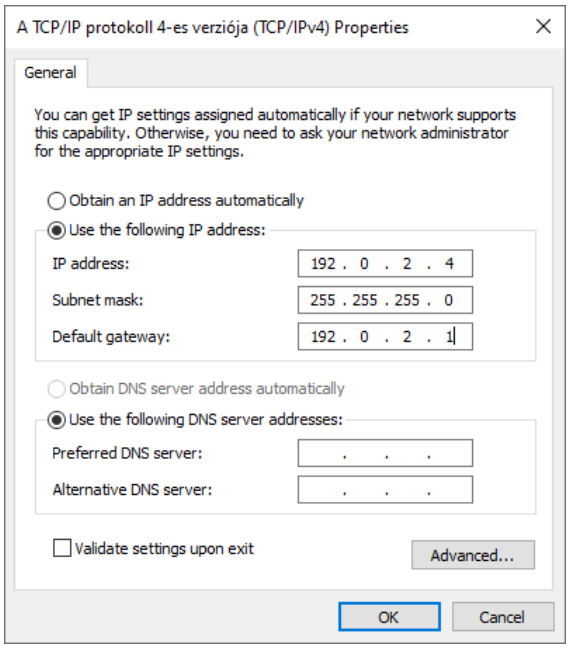


2. Right-click on **Ethernet**, then select **Properties**. In the appearing menu double-click "**Internet Protocol Version 4 (TCP/IPv4)**".





3. Select "**Use the Following IP address**", and set:
   - 192.0.2.4 as "**IP address**"
   - 255.255.255.0 as "**Subnet mask**"
   - 192.0.2.1 as "**Default gateway**"



4. Click on **[OK]** to apply changes.

11. USING HTTPS PROTOCOL WITH OSMOND DEVICES

The following procedure details the steps of establishing secure HTTP connection (HTTPS) when using the Osmond device web interface. The main focus of the method described below is to **avoid using certificates from any third-party publisher** for such purpose.

The entire process includes of three main steps:

1. Creating and managing certificates
2. Uploading certificate to Osmond devices and activating HTTPS
3. Importing root certificate to web browser

The procedure can be performed on both Linux and Windows operating systems as well. For both OS types, SSL library must be installed. For more information on installing SSL to Windows 10, you may refer to the following link: https://www.stechies.com/installing-openssl-windows-10-11/

1. Creating and managing certificates

1.1 Root CA certificate

Root-CA is used to sign device certificates. After importing to web browser as a trusted root certificate, other certificates signed by Root CA are also considered as trusted.

1.1.1 Generating Root CA

- At first, a private key should be generated that is necessary for generating the certificate:

```
openssl genrsa -out CA.key 4096
```

- Then, generate the CA certificate:

```
openssl req -x509 -new -nodes -key CA.key -sha256 -days 1826 -out
CA.crt -subj "/CN=CompanyName Root
CA/C=HU/ST=Budapest/L=Budapest/O=CompanyShortName"
```


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

1.2 Device Certificate

1.2.1 Generating device certificate (devicename.subdomain.company.hu)

The device private key and a 'certificate signing request' (devicename.key, devicename.csr)

```
openssl req -new -nodes -out devicename.csr -newkey rsa:4096 -
keyout n204109.key -subj
"/CN=devicename.subdomain.company.hu/C=HU/ST=Budapest/L=Budapest/O
=CompanyShortName"
```

Note

The "devicename" is the hostname of your device.

The hostname of your device is OSMOND-N{serialnumber*}, e.g., OSMOND-N204109. 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.

1.2.2 Signing the CSR with Root CA

- **Linux**:

```
cat > devicename.v3.ext << EOF
      authorityKeyIdentifier=keyid,issuer
      basicConstraints=CA:FALSE
      keyUsage = digitalSignature, nonRepudiation,
      keyEncipherment, dataEncipherment
      subjectAltName = @alt_names
      [alt_names]
      DNS.1 = devicename.subdomain.company.hu
EOF
```

- **Windows**:

```
copy con devicename.v3.ext
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment,
dataEncipherment
subjectAltName = @alt_names
[alt_names]
DNS.1 = devicename.subdomain.company.hu
^Z
```

```
openssl x509 -req -in devicename.csr -CA CA.crt -CAkey CA.key -
CAcreateserial -out devicename.crt -days 730 -sha256 -extfile
devicename.v3.ext
```

1.2.3 Creating the HTTPS certificate

The HTTPS certificate can be created by simply copying the device key and cert files together, as follows:

- **Linux:**

  ```
  cat devicename.crt devicename.key > devicename.ssl.pem
  ```

- **Windows:**

  ```
  Get-Content devicename.crt, devicename.key | Set-Content
  devicename.ssl.pem
  ```

Contents of the **devicename.ssl.pem** file:


```
-----BEGIN CERTIFICATE-----
MIIFwTCCA6mgAwIBAgIUe4wVn/akwZrNU5uh7NM+VNtiFQgwDQYJKoZIhvcNAQEL
BQAwVTETMBEGA1UEAwwTAPBgNVBAgM {MORE DATA} N94M/
Zh3RxAs1D45esm2KvJnYuzs0NQk+YPkVhBM5n37CFVjFRj6BsQ==
-----END CERTIFICATE-----
-----BEGIN PRIVATE KEY-----
MIIJQQIBADANBgkqhkiG9w0BAQEFAASCCSswggknAgEAAoICAQCWvJLgLjqYUuB1
Fhwh3peOGQg9/q {MORE DATA} k6eA0K1ZVA9FI4h/CBt1daOq4m
BtMaKi5j4QaIDWGefOZJEcs08NFJ
-----END PRIVATE KEY-----
```


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

2. Configuring HTTPS via Osmond device web interface

2.1 Uploading certificate and activating HTTPS via Osmond web interface

HTTPS can be activated and HTTPS cert can be uploaded via the NETWORK / WEB SERVER menu of the Osmond device web interface. For more information, please refer to the WEB SERVER chapter of the Osmond User Manual.

2.2 Uploading certificate via .json configuration file

For activating HTTPS and uploading HTTPS certificate via .json configuration file, please refer to the following sample:

```
        //Properties
[
{
"webserver/isHttps" : "1"
},
{
"webserver/certificate/RawData" : "-----BEGIN CERTIFICATE-----
MIIFwTCCA6mgAwIBAgIUe4wVn/akwZrNU5uh7NM+ wKQV {MORE DATA}
AkGA1UEBhMCSFUxETAPBgNVBAgM CEJ1ZGFwZXN0MREwDwYDVcNMjMw Q== -----END
CERTIFICATE----- -----BEGIN PRIVATE KEY----- MIIJQQIBADANBgkqhkiG
{MORE DATA}
AoICAQCWvJLgLjqYUuB1BFMZppLQCfkI/4TZcaHe1IcZ9uT2MlEzrNWVS
iH3OO9nOnwFAnM6I4OKgdC712Sy Fhwh3peOGQg9/ FJ -----END PRIVATE KEY---
--"
}
]
//End
```

Note

Mind \n (0x0A) line endings in .json file. Missing or invalid line endings cause update file to be ignored by the device.

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

3. Browser settings

In order to establish secure connection to Osmond device web interface via web browser, the root CA must be imported to browser so the device cert. can be trusted. The following steps should be performed once for any browser:

3.1 Firefox

Settings → → Privacy and Security → Certificates → View Certificates → Authorities → Import...

3.2 Google Chrome

Settings → Privacy and Security → Security → Manage Device Certificates → Trusted Root Certification Authorities → Import...

Note

For NetAPI use, the root CA must be added to the PC OS trusted source list on the PC running the NetAPI application.

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

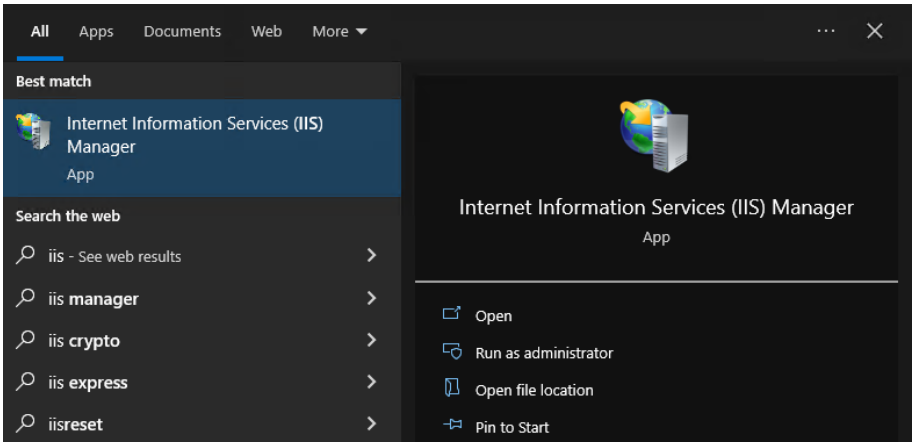
12. INSTALLATION OF THE SSL CERTIFICATE

In this section the installation of the SSL certificate on Windows and Linux operating systems will be discussed. The acquisition of the SSL certificate will not be detailed, but a website will be linked. By clicking on this link, a certificate valid for 90 days can be requested for free according to the web page, address of which is the following:

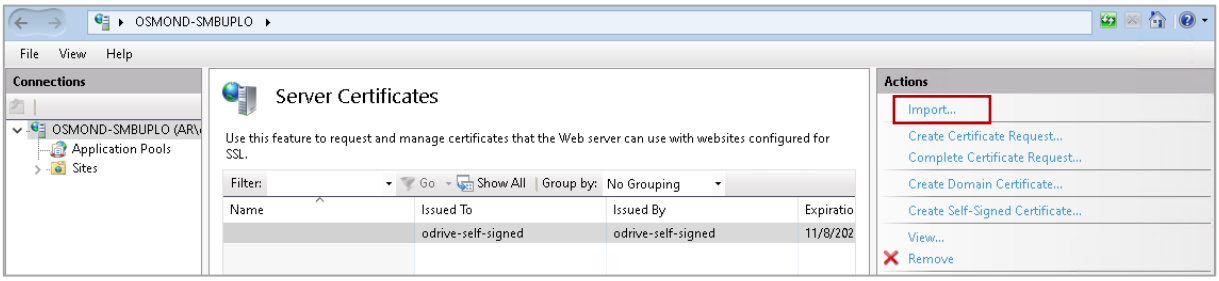
https://www.sslforfree.com/

12.1. INSTALLING THE SSL CERTIFICATE ON WINDOWS 10

1. Start the **Internet Information Services (IIS)** program:
   - Open Start menu
   - Enter: iis



2. Double-click on the **Server Certificates** icon located in the middle part of the window under the IIS bar.
3. Select "**Import...**" from the **Actions** menu located on the right side.

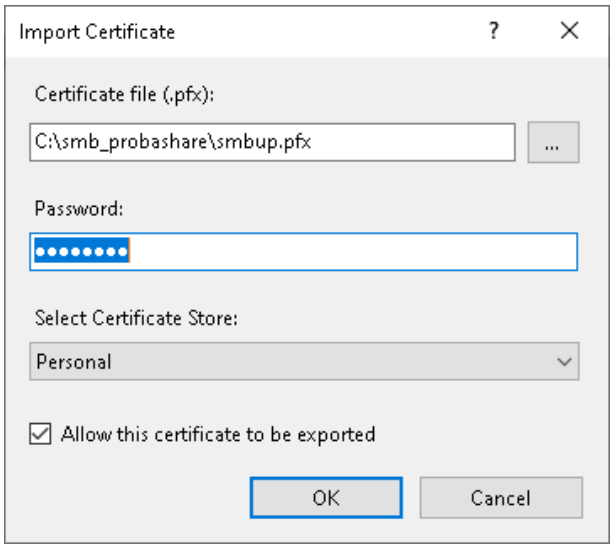


4. In the appearing window:
   - Enter the filename and the path of the certificate to the **Certificate file (.pfx)** field. Alternatively, browse the certificate file by clicking on the **[...]** button.
     - The file format must be **.pfx**. If the file has a different format, convert it to .pfx by using OpenSSL (or other utility program).

       For example:

       Converting a certificate with .pem format to pfx format:

       ```
       openssl pkcs12 -inkey privkey1.pem -in cert1.pem -export -out rootca.pfx
       ```
   - If the certificate is password protected, enter its password to the **Password** field.
   - Select "**Personal**" under **Select Certificate Store**.



5. After performing these settings, click on the **[OK]** button.
6. It is recommended to copy the certificate to the file system:
   - Open Command Prompt. Command Prompt can be accessed by entering "cmd" text to the search bar at Start menu and clicking on the appearing Command Prompt line.
   - Create the library structure:

     ```
     mkdir c:\Users\tesztg\ssl\certs\
     mkdir c:\Users\tesztg\ssl\private\
     ```
   - Navigate to the certificates:

     ```
     cd c:\smb_probashare
     ```
   - Copy the files of the certificate to the created library structure:

     ```
     copy cert1.pem c:\Users\tesztg\ssl\certs\
     copy privkey1.pem c:\Users\tesztg\ssl\certs\
     ```

12.2. INSTALLING THE SSL CERTIFICATE ON UBUNTU

The following commands apply to Ubuntu 22.04. However, the SSL certificate can be installed to other Linux versions with similar commands as well. The commands can be issued from a terminal. In the example the certificate consists of two pem files:

cert1.pem

privkey1.pem

The **cert1.pem** is the certificate. The **privkey1.pem** is the key. If the certificate is not in this format, it is recommended to convert it to pem format with e.g., OpenSSL program.

1. Update Ubuntu:

```
sudo apt update
sudo apt upgrade -y
```

2. Install OpenSSL:

```
sudo apt-get install openssl
```

3. It is recommended to navigate to the library containing the certificate.
   For example:

```
cd /home/tesztg
```

4. Check if the cert library already contains files with the **cert1.pem** and **privkey1.pem** names:

```
[ -e /etc/ssl/certs/cert1.pem ] && echo "exists"
[ -e /etc/ssl/private/privkey1.pem ] && echo "exists"
```

5. If the cert library already contains files with the **cert1.pem** and **privkey1.pem** names, then rename the new ones:

```
mv cert1.pem cert2.pem
mv privkey1.pem privkey2.pem
```

> **Note**
>
> In the further examples the original filenames will be used (**cert1.pem**, **privkey1.pem**).

6. Copy the cert and the key files to the OpenSSL library:

```
sudo cp cert1.pem /etc/ssl/certs
sudo cp privkey1.pem /etc/ssl/private
```

7. Set the rights:

```
sudo chmod 644 /etc/ssl/certs/cert1.pem
sudo chown root:ssl-cert /etc/ssl/private/privkey1.pem
sudo chmod 640 /etc/ssl/private/privkey1.pem
```

8. Add the user to the SSL cert group in order to read the private keys:

```
sudo usermod -a -G ssl-cert tesztg
```

where:

`ssl-cert` is the name of the group

`tesztg` is the name of the user

9. Restart the PC:

```
sudo reboot
```


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

12.3. QUERYING THE INTERMEDIATE CERTIFICATE

The two files mentioned before, can contain all keys (public, private) and certificates (root, intermediate, server).

1. The server – e.g., Apache2 server – can be tested with the following command:

   ```
   openssl s_client -connect test.example.com:443 -servername
   test.example.com
   ```

   where:

   `test.example.com` is the fully qualified domain name (FQDN) of the server

   `443` is the port through which the server is listening

2. If everything is OK, the following line is returned:

   ```
   Verify return code: 0 (ok)
   ```

3. But if the following line is returned, the intermediate certificate may be missing:

   ```
   Verify return code: 21 (unable to verify the first certificate)
   ```

4. In order to query the intermediate certificate, run the following command:

   ```
   openssl s_client -connect test.example.com:443 -servername
   test.example.com > logcertfile
   ```

   This command creates a file named `logcertfile`.

5. After this, run one of the following commands according to your operating system:

   - In case of Linux:

     ```
     openssl x509 -in logcertfile -noout -text | grep -i "issuer"
     ```

   - In case of Windows:

     ```
     openssl x509 -in logcertfile -noout -text | findstr /i "issuer"
     ```

   This command returns the URI through which the intermediate certificate can be downloaded. In the present example the output of the command above is the following:

   ```
   Issuer: C = US, O = Let's Encrypt, CN = R3
           CA Issuers - URI:http://r3.i.lencr.org/
   ```

   With this:

   ```
   curl --output intermediate.crt http://r3.i.lencr.org/
   ```


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

6. The created `intermediate.crt` certificate must be converted to PEM format:
   ```
   openssl x509 -inform DER -in intermediate.crt -out intermediate.pem -text
   ```

7. The resulting `intermediate.pem` file must be copy to the server. If the file is already on the server in another library, then the following commands can be issued from that given library:
   ```
   sudo cp intermediate.pem /etc/ssl/certs/
   sudo chmod 644 /etc/ssl/certs/intermediate.pem
   ```

8. Then, it must be set in the configuration file of the server. In case of Apache2 server, set in the conf extension file:
   ```
   SSLCertificateChainFile /etc/ssl/certs/intermediate.pem
   ```

9. At last, restart the Apache2 server:
   ```
   sudo systemctl restart apache2.service
   ```

12.4. MERGING THE INTERMEDIATE AND THE SERVER CERTIFICATES

If the several files of the same certificate are to be merged (e.g., merging the intermediate certificate with the server and root certificates), then enter the following command:

```
sudo cat cert1.pem intermediate.pem > cert1_full_chain.pem
```

If the newly created file (`cert1_full_chain.pem`) does not work, concatenate the files in a different order. For example:

```
sudo cat intermediate.pem cert1.pem > cert1_full_chain.pem
```

After that:

```
sudo chmod 644 /etc/ssl/certs/cert1_full_chain.pem
```

In this case just pass the generated file to the Apache2 server.

> **Note**
>
> WSS servers also use such full chain file, because only one certificate file and one key file can be passed.

13. SETTING THE WS PROTOCOL ON OSMOND

The current version (1.8) of the Osmond firmware is capable of uploading the scanned data to a server via multiple protocols.
In this section the settings of the WebSocket (WS) protocol will be explained.

The parameters are the following:

- IP address of the WS server: 192.168.1.2
- The shared folder on Windows (upload path): C:\ws_share
- The shared library on Linux: /home/tesztg/ws_share

13.1. WS SERVERS

In the Annex chapter three WS servers can be found. Their source codes are also available in the **ws_server_java**, **ws_server_python** and **ws_server_ruby** libraries. One is written in Ruby, the other in Python, and the third in Java. Each can be used for receiving and storing the compressed (zip) packages of Osmond via WebSocket.

It is recommended to save the source code as a file named **ws_server_ruby.rb**, **ws_server_python.py** or **ws_server_java.java**, because this description will refer to the servers by these names.

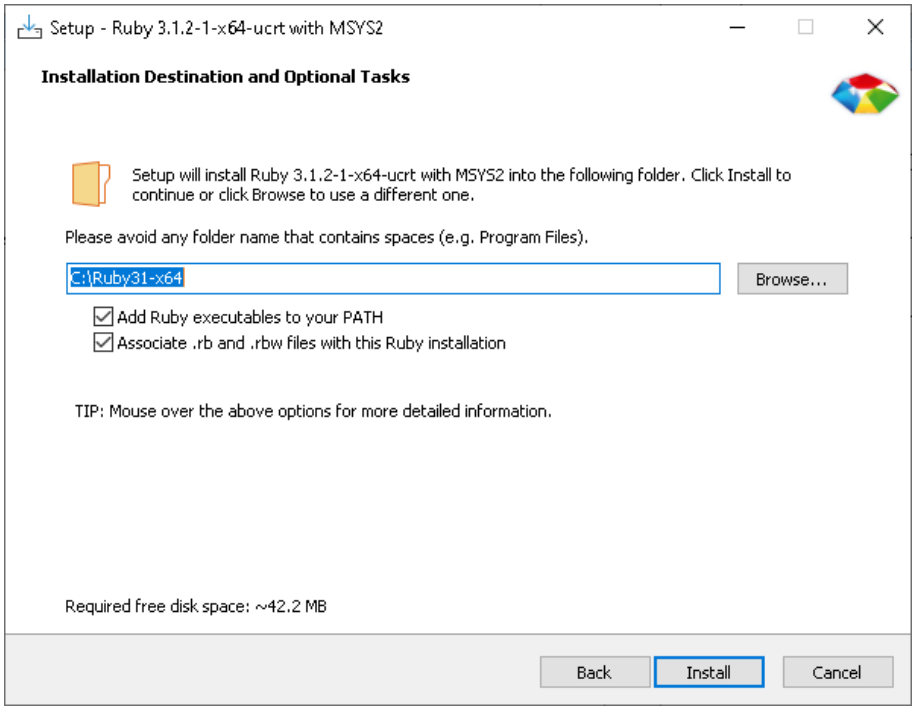
Each WS server has a configuration file. The names of these configuration files are the following: **ws_server_ruby.json**, **ws_server_python.json** and **ws_server_java.json**. They can be found in the Annex as well. Installing only one of the three servers to a PC is adequate.

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

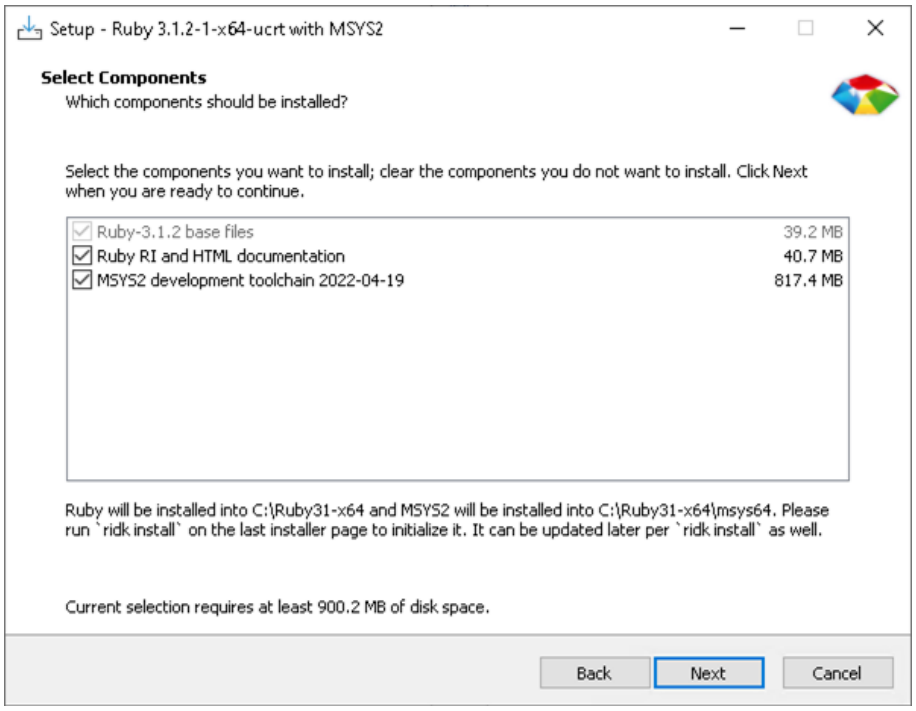
13.2. INSTALLING AND SETTING THE WS SERVER ON WINDOWS 10

13.2.1. INSTALLING RUBY

1. Download and install Ruby 3 or newer version with Devkit (currently Ruby+Devkit 3.1.2-1 (x64) can be accessed):
   - Navigate to https://rubyinstaller.org/downloads/.
   - Select "**Add Ruby executables to your PATH**" and "**Associate .rb and .rbw files with this Ruby installation**" by ticking the checkboxes.
   - Then, click on **[Install]**.



- Select "**Ruby RI and HTML documentation**" and "**MSYS2 and MINGW development toolchain**" by ticking the checkboxes.

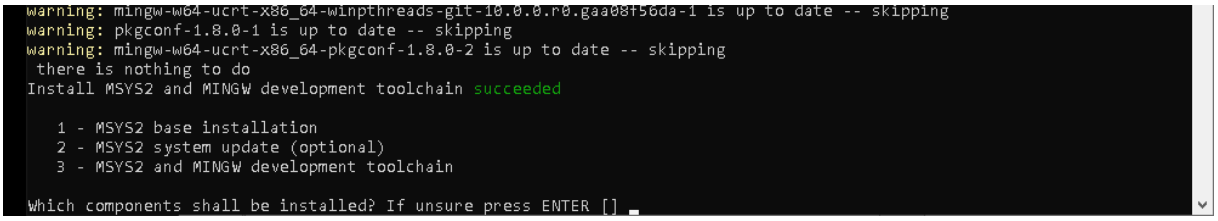


- After the installation is finished, run "ridk install" too by selecting the "**Run 'ridk install' to set up MSYS2 and development toolchain.**" option.

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

- In the appearing terminal select "**3 – MSYS2 and MINGW development toolchain**" by typing 3 and then pressing the **[Enter]** key.

- After it is executed, press **[Enter]**.



2. Restart the PC.
3. Open Command Prompt. Command Prompt can be accessed by entering "cmd" text to the search bar at Start menu and clicking on the appearing Command Prompt line.
4. Install the websocket-eventmachine-server ruby package in the Command Prompt:

```
gem install websocket-eventmachine-server
```


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

13.2.2. INSTALLING THE RUBY WS SERVER

1. Create a library which will receive the packages. For example, use the following command in the terminal:
   ```
   mkdir C:\ws_share
   ```

2. Create a library where the WS server files are to be copied. For example, use the following command in the terminal:
   ```
   mkdir C:\temp\ws_server_ruby
   ```

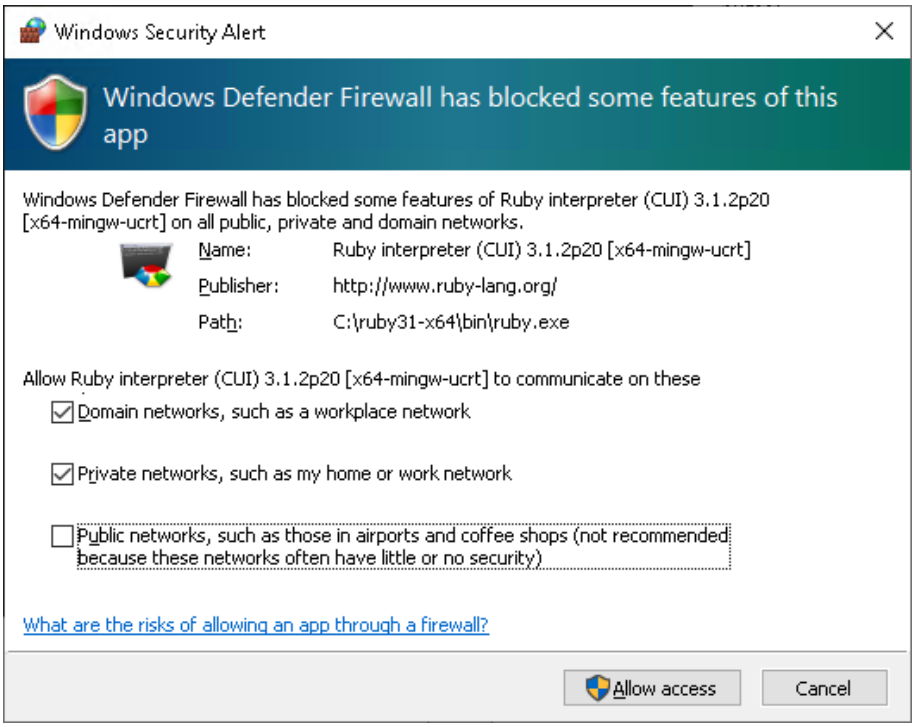
3. Copy the **ws_server_ruby.rb** and the **ws_server_ruby.json** files to the `C:\temp\ws_server_ruby` library. The **ws_server_ruby.rb** and the **ws_server_ruby.json** files can be found in the Annex chapter.

4. In the **ws_server_ruby.json** file set the port number through which the server will be listening, and the directory which will receive the uploaded zip files.
   - "ws_port": "2080"
     It is recommended to set the port number to 2080.
   - "upload_directory": "C:\\ws_share"
     On Windows, the upload_directory can be entered the following ways:
     - C:\\ws_share
     - C:/ws_share

5. Navigate to the WS server directory in command line:
   ```
   cd C:\temp\ws_server_ruby
   ```

6. Start the server:
   ```
   ruby ws_server_ruby.rb
   ```

7. If a window pops up indicating that Firewall has blocked Ruby, click on the **[Allow access]** button on this window. Thereby Ruby interpreter can accept the incoming connections.



8. In order to stop the server, use the Ctrl + C keyboard shortcut or simply close the terminal.

13.2.3. INSTALLING PYTHON

1. Download and install Python 3 or newer version (currently Python 3.11.3 can be accessed):
   - Navigate to https://www.python.org/downloads/.
   - Select "**Use admin privileges when installing py.exe**" and "**Add python.exe to PATH**" by ticking the checkboxes.
   - Then, click on **[Install Now]**.

   - After installation, it is recommended to restart the PC.

2. Open Command Prompt. Command Prompt can be accessed by entering "cmd" text to the search bar at Start menu and clicking on the appearing Command Prompt line.

3. Install the websockets python package in the Command Prompt:

```
pip install websockets
```

13.2.4. INSTALLING THE PYTHON WS SERVER

1. Create a library which will receive the packages. For example, use the following command in the terminal:
   ```
   mkdir C:\ws_share
   ```

2. Create a library where the WS server files are to be copied. For example, use the following command in the terminal:
   ```
   mkdir C:\temp\ws_server_python
   ```

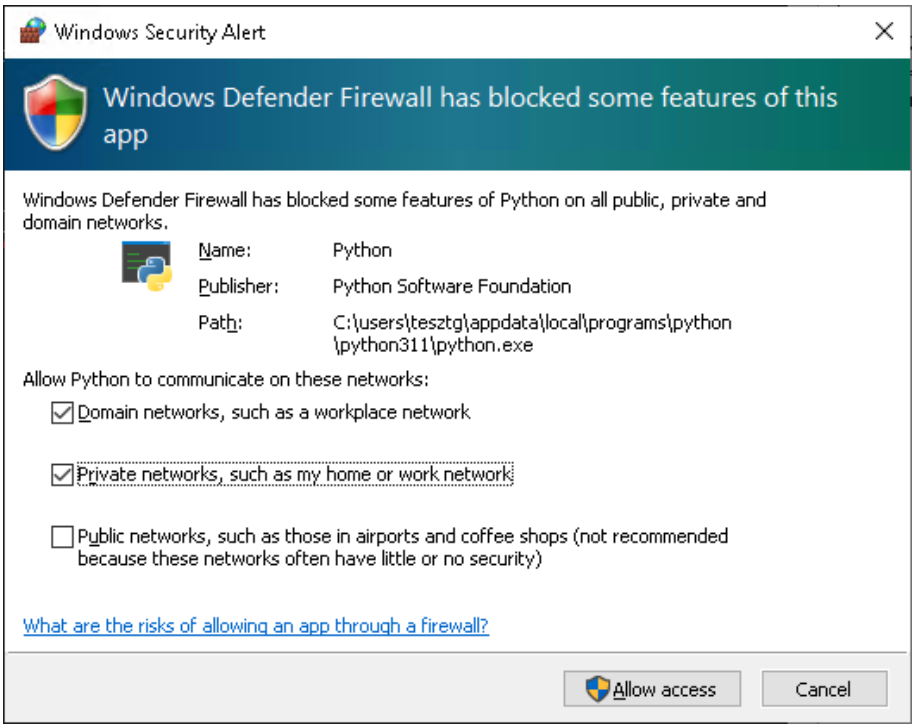
3. Copy the **ws_server_python.py** and the **ws_server_python.json** files to the `C:\temp\ws_server_python` library. The **ws_server_python.py** and the **ws_server_python.json** files can be found in the Annex chapter.

4. In the **ws_server_python.json** file set the port number through which the server will be listening, and the directory which will receive the uploaded zip files.
   - "ws_port": "2080"
     It is recommended to set the port number to 2080.
   - "upload_directory": "C:\\ws_share"
     On Windows the upload_directory can be entered in the following ways:
     - C:\\ws_share
     - C:/ws_share

5. Navigate to the WS server directory in command line:
   ```
   cd C:\temp\ws_server_python
   ```

6. Start the server:
   ```
   python ws_server_python.py
   ```

7. If a window pops up indicating that Firewall has blocked Python, click on the **[Allow access]** button on this window. Thereby Python interpreter can accept the incoming connections.



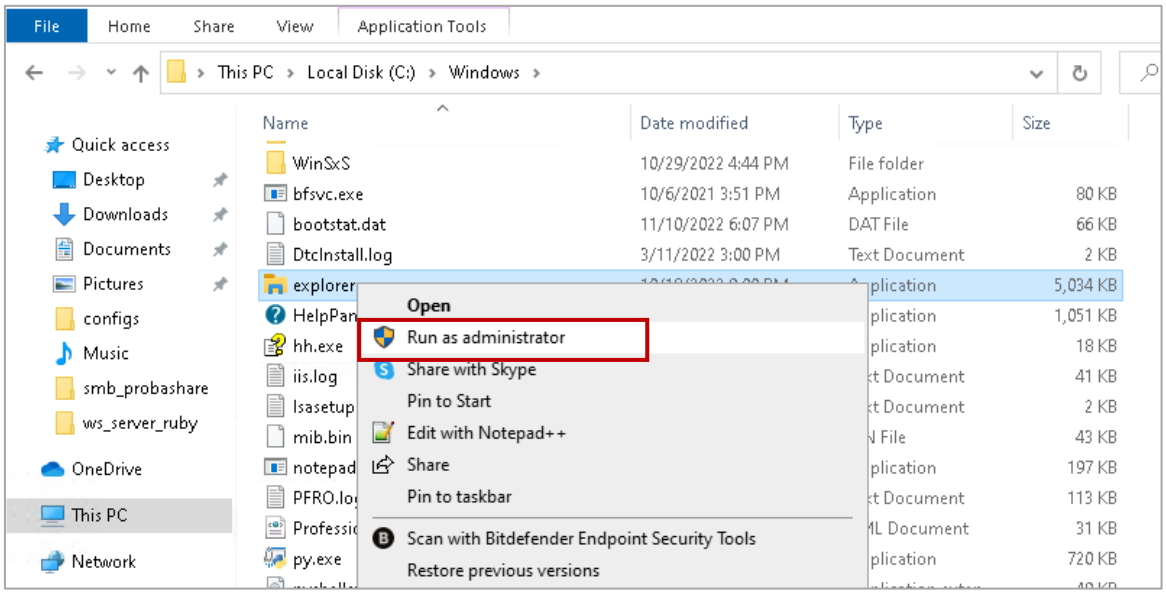
8. In order to stop the server, use the Ctrl + C keyboard shortcut or simply close the terminal.

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

13.2.5. INSTALLING JAVA

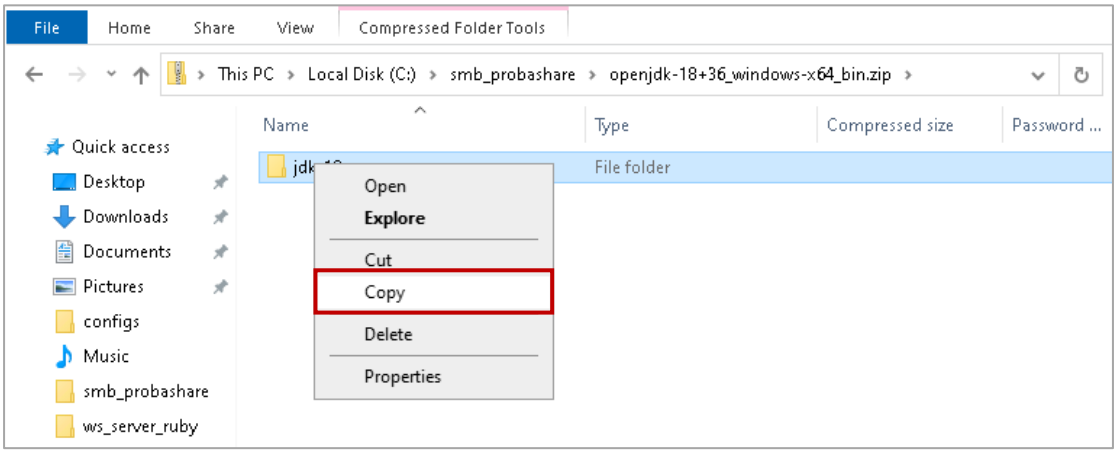
In the following section the installation of OpenJDK will be described. For running the WS server, any version of Java can be used. The testing on Windows has been performed with the version 18 of OpenJDK.

1. Navigate to https://jdk.java.net/java-se-ri/18.
2. Download the OpenJDK installer for Windows.
3. Decompress the zip file and copy its contents to the C:\Program Files\Java library:
   - Open File Explorer with administrator rights:
     - Open File Explorer by clicking on its icon on taskbar or from the Start menu.
     - Browse the **C:\Windows\explorer.exe** file.
     - Right click on the file.
     - In the appearing quick menu select the "**Run as administrator**" menu item.



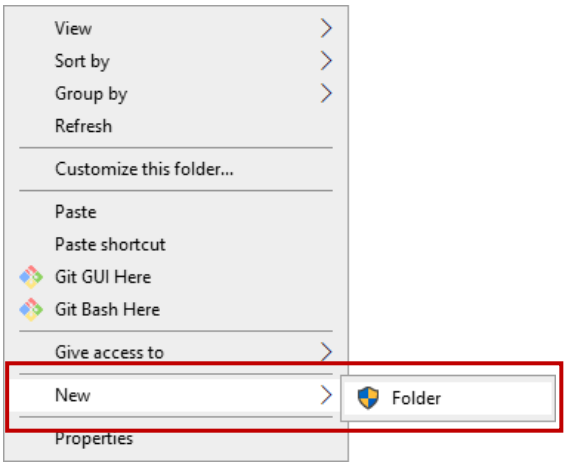
   - In the recently opened File Explorer browse the downloaded zip file. (The name of the current version is "openjdk-18+36_windows-x64_bin.zip".)
   - Double click on the zip file.

– Right click on it, then in the appearing quick menu select "**Copy**".



– Then, navigate to the **C:\Program Files** library.

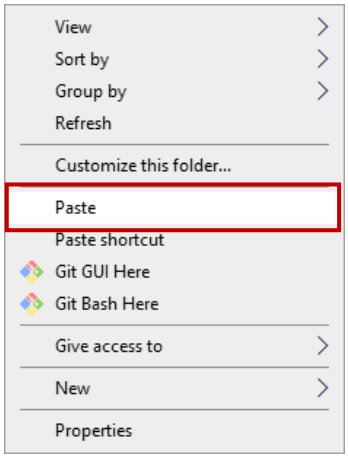
– Right click on a neutral area, then select **New / Folder** menu item from the pop-up quick menu.



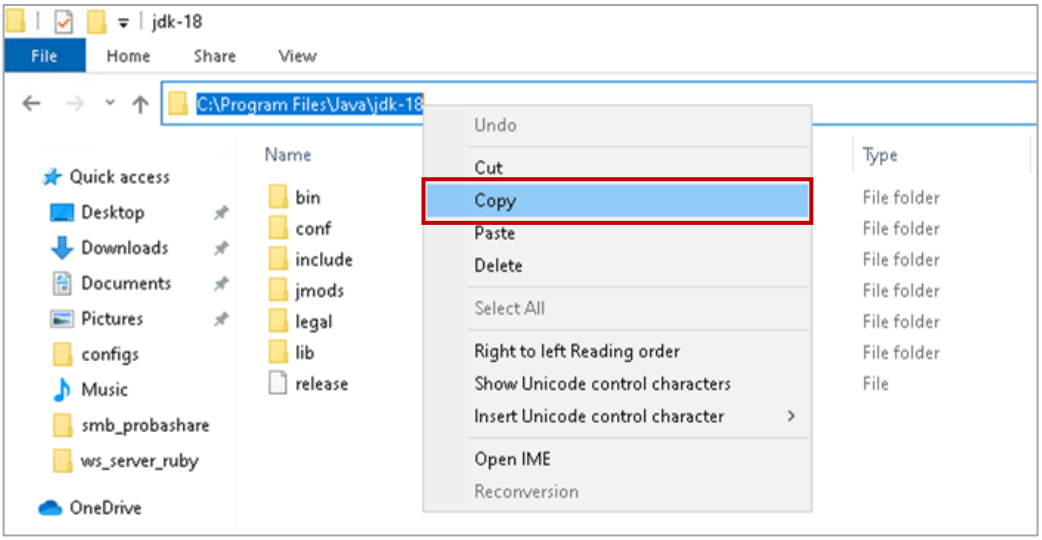
– After that, Windows creates a new directory. Rename it to "**Java**" and press **[Enter]**.

– Double click on **Java** directory to enter the holder.

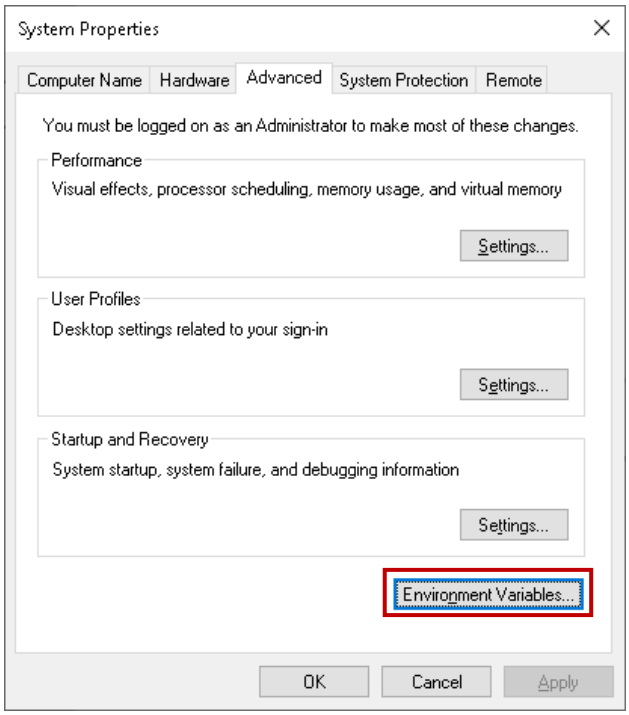
– Right click on a neutral area, then select **Paste**.



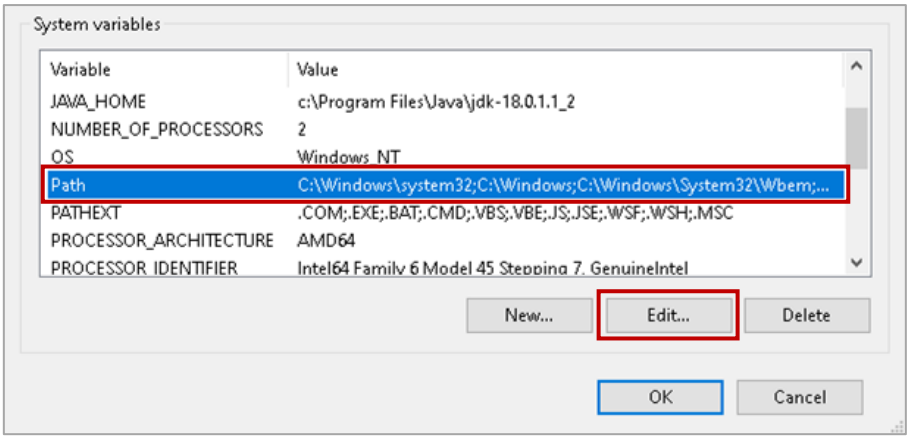
– After decompression, copy to clipboard the path of the **Java** directory:
  - Double click on the created directory (e.g., named jdk-18) to enter the holder.
  - Click on a neutral area of the address bar of the File Explorer (e.g., to the right of the path of the folder).
  - In the appearing quick menu select "**Copy**".



4. Open Control Panel. Control Panel can be accessed by entering its name to the search bar at Start menu and clicking on the appearing Control Panel line.
5. Navigate to **Control Panel / System and Security / System / Advanced system settings**.
6. In the appearing window click on the **[Environment Variables...]** button.



7. In the pop-up window under **System variables** select the **Path** variable. Then, click on the **[Edit...]** button.



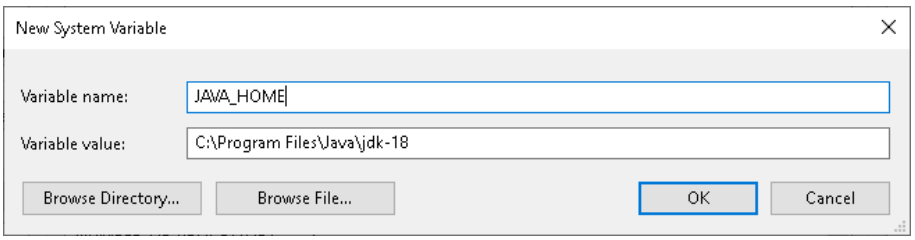
8. In the appearing window click on the **[New]** button.

9. Paste the path copied to clipboard into a new row. Complete the copied path with the **\bin** directory:
   `C:\Program Files\Java\jdk-18\bin`

10. Then, click on **[OK]**.

11. After that, in the **System variables** section select the **[New...]** button.

12. In the pop-up window enter the following values:
    - **Variable name:** JAVA_HOME
    - **Variable value:** C:\Program Files\Java\jdk-18

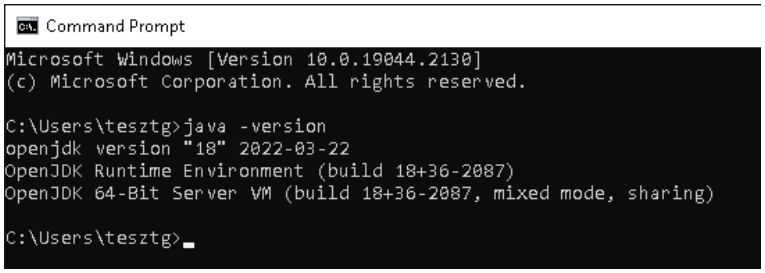


13. Then, click on **[OK]**.

14. After that, select the **[OK]** button again.

15. Close the window and restart Windows.

16. Check if the installation is properly performed:
    - Open Command Prompt. Command Prompt can be accessed by entering "cmd" text to the search bar at Start menu and pressing **[Enter]**.
    - In the Command Prompt enter the following command:
      `java -version`
    - If the returned value is **openjdk version "18"**, then Java is properly installed.



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

13.2.6. INSTALLING THE JAVA WS SERVER

1. Create a library which will receive the packages. For example, use the following command in the terminal:
   ```
   mkdir C:\ws_share
   ```

2. Create a library where the WS server files are to be copied. For example, use the following command in the terminal:
   ```
   mkdir C:\temp\ws_server_java
   ```

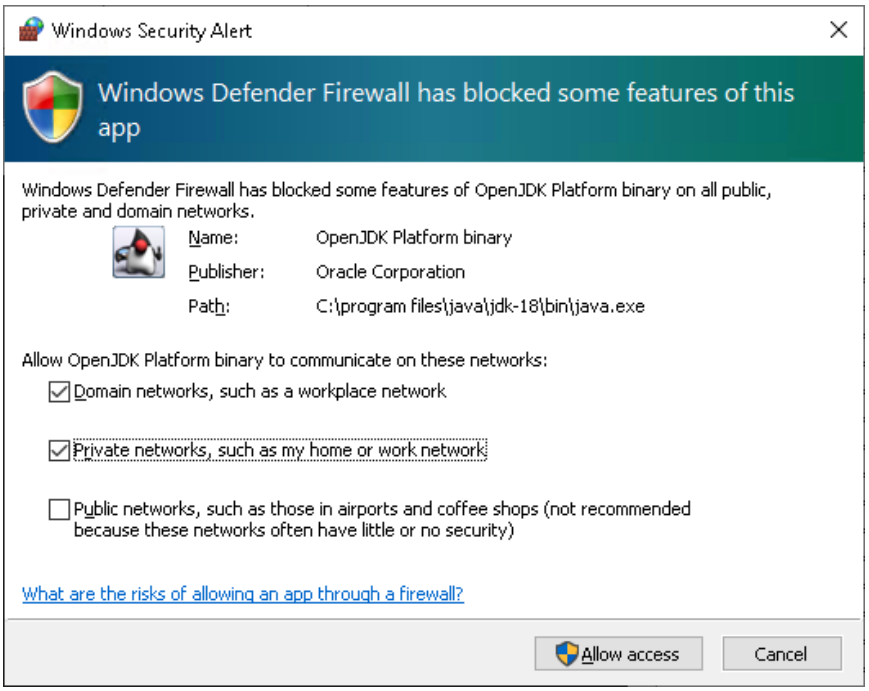
3. Copy the **ws_server_java.jar** and the **ws_server_java.json** files to the `C:\temp\ws_server_java` library. The **ws_server_java.jar** and the **ws_server_java.json** files can be found in the Annex chapter.

4. In the **ws_server_java.json** file set the port number through which the server will be listening, and the directory which will receive the uploaded zip files.
   - "ws_port": "2080"
     It is recommended to set the port number to 2080.
   - "upload_directory": "C:\\ws_share"
     On Windows the upload_directory can be entered in the following ways:
     - C:\\ws_share
     - C:/ws_share

5. Navigate to the WS server directory in command line:
   ```
   cd C:\temp\ws_server_java
   ```

6. Start the server:
   ```
   java -jar ws_server_java.jar
   ```

7. If a window pops up indicating that Firewall has blocked Java, click on the **[Allow access]** button on this window. Thereby Java interpreter can accept the incoming connections.



8. In order to stop the WS server, use the Ctrl + C keyboard shortcut or type "exit" in the running terminal.

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

13.3. INSTALLING AND SETTING THE WS SERVER ON LINUX

13.3.1. INSTALLING RUBY

Under Linux install Ruby from command line. The commands may depend on the distribution.

The following commands apply to Ubuntu 22.04.

1. Update Ubuntu:

```
sudo apt update
sudo apt upgrade -y
```

2. Install Ruby (it may have been already installed):

```
sudo apt install ruby-full
```

3. After installation, it is recommended to query the Ruby version:

```
ruby -version
```

4. If the returned value is 3 or greater, the version is correct.

5. Install the websocket-eventmachine-server ruby package in the command line:

```
sudo gem install websocket-eventmachine-server
```


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

13.3.2. INSTALLING RUBY WS SERVER

1. Create a library which will receive the packages. For example, use the following command in the terminal:

   ```
   mkdir /home/tesztg/ws_share
   ```

   The user running the WS server, is the "tesztg" Therefore create the package directory in the home directory of this user.

2. Create a library where the WS server files are to be copied. For example, use the following command in the terminal:

   ```
   mkdir /home/tesztg/ws_server_ruby
   ```

3. Copy the **ws_server_ruby.rb** and the **ws_server_ruby.json** files to the `/home/tesztg/ws_server_ruby` library. The **ws_server_ruby.rb** and the **ws_server_ruby.json** files can be found in the Annex chapter.

4. In the **ws_server_ruby.json** file set the port number through which the server will be listening, and the directory which will receive the uploaded zip files.
   - "ws_port": "**2080**"
     It is recommended to set the port number of the WS server to 2080.
   - "upload_directory": "**/home/tesztg/ws_share**"
     If the upload_directory is in the home directory of the user who runs the WS server, then the tilde (~) character can be used for substituting the home directory of the user. Therefore, the example above can be entered in the following way as well:
     ~/ws_share

5. Navigate to the WS server directory in command line:

   ```
   cd /home/tesztg/ws_server_ruby
   ```

6. Start the server:

   ```
   ruby ws_server_ruby.rb
   ```

13.3.3. INSTALLING PYTHON

Most Linux distributions, including Ubuntu 22.04, install one of the Python versions during its installation. In order to perform the following steps, open a terminal.

1. Before querying the version, it is recommended to update the operating system:

   ```
   sudo apt update
   sudo apt upgrade -y
   ```

2. Query the Python version:

   ```
   python3 -V
   ```

   This queries the version of Python 3.

   - If **no error** is returned, the Python version is correct.
   - If **error** is returned, install Python 3:

     ```
     sudo apt-get install python3
     ```

3. Install the websockets python package:

   ```
   pip install websockets
   ```


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

13.3.4. INSTALLING PYTHON WS SERVER

1. Create a library which will receive the packages. For example, use the following command in the terminal:

   ```
   mkdir /home/tesztg/ws_share
   ```

   The user running the WS server, is the "tesztg" Therefore create the package directory in the home directory of this user.

2. Create a library where the WS server files are to be copied. For example, use the following command in the terminal:

   ```
   mkdir /home/tesztg/ws_server_python
   ```

3. Copy the **ws_server_python.py** and the **ws_server_python.json** files to the `/home/tesztg/ws_server_python` library. The **ws_server_python.py** and the **ws_server_python.json** files can be found in the Annex chapter.

4. In the **ws_server_python.json** file set the port number through which the server will be listening, and the directory which will receive the uploaded zip files.

   - "ws_port": "**2080**"
     It is recommended to set the port number of the WS server to 2080.
   - "upload_directory": "**/home/tesztg/ws_share**"
     If the upload_directory is in the home directory of the user who runs the WS server, then the tilde (~) character can be used for substituting the home directory of the user. Therefore, the example above can be entered in the following way as well:
     ~/ws_share

5. Navigate to the WS server directory in command line:

   ```
   cd /home/tesztg/ws_server_python
   ```

6. Start the server:

   ```
   python3 ws_server_python.py
   ```

13.3.5. INSTALLING JAVA

Most Linux distributions, including Ubuntu 22.04, install one of the Java versions during its installation. Ubuntu 22.04 currently contains the OpenJDK 11.0.17 by default.

In order to perform the following steps, open a terminal.

1. Before querying the version, it is recommended to update the operating system:

   ```
   sudo apt update
   sudo apt upgrade -y
   ```

2. Query the Java version:

   ```
   java -version
   ```

   Result of this query can take the following values:

   - If the returned value is "Command 'java' not found", then Java is not installed.
   - If the returned value is a version number (e.g., 11.0.17), then Java is installed and no other steps are needed.

3. If Java is not installed, enter the following command in the terminal:

   ```
   sudo apt install default-jdk
   ```

4. After finishing the installation, check which version has been installed with the following command:

   ```
   java -version
   ```


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

13.3.6. INSTALLING JAVA WS SERVER

1. Create a library which will receive the packages. For example, use the following command in the terminal:

   ```
   mkdir /home/tesztg/ws_share
   ```

   The user running the WS server, is the "tesztg" Therefore create the package directory in the home directory of this user.

2. Create a library where the WS server files are to be copied. For example, use the following command in the terminal:

   ```
   mkdir /home/tesztg/ws_server_java
   ```

3. Copy the **ws_server_java.jar** and the **ws_server_java.json** files to the `/home/tesztg/ws_server_java` library. The **ws_server_java.jar** and the **ws_server_java.json** files can be found in the Annex chapter.

4. In the **ws_server_java.json** file set the port number through which the server will be listening, and the directory which will receive the uploaded zip files.
   - "ws_port": "**2080**"
     It is recommended to set the port number of the WS server to 2080.
   - "upload_directory": "**/home/tesztg/ws_share**"
     If the upload_directory is in the home directory of the user who runs the WS server, then the tilde (~) character can be used for substituting the home directory of the user. Therefore, the example above can be entered in the following way as well:
     ~/ws_share

5. Navigate to the WS server directory in command line:

   ```
   cd /home/tesztg/ws_server_java
   ```

6. Start the server:

   ```
   java -jar ws_server_java.jar
   ```

7. In order to stop the WS server, use the Ctrl + C keyboard shortcut or type "exit" in the running terminal.
    - The WS server may not shut down immediately. In this case the server throws an error message at the next startup:
      ```
      java.net.BindException: Address already in use
      ```
    - At this time query the running WS processes:
      ```
      ps ax | grep ws_ | grep -v grep
      ```
    - The first number is the process ID. The ongoing Java process can be shut down by knowing this number.
      For example:
      ```
      3630 pts/2    Sl+    0:00 java -jar ws_server_java.jar
      ```
    - Then, in this case:
      ```
      kill 3630
      ```


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

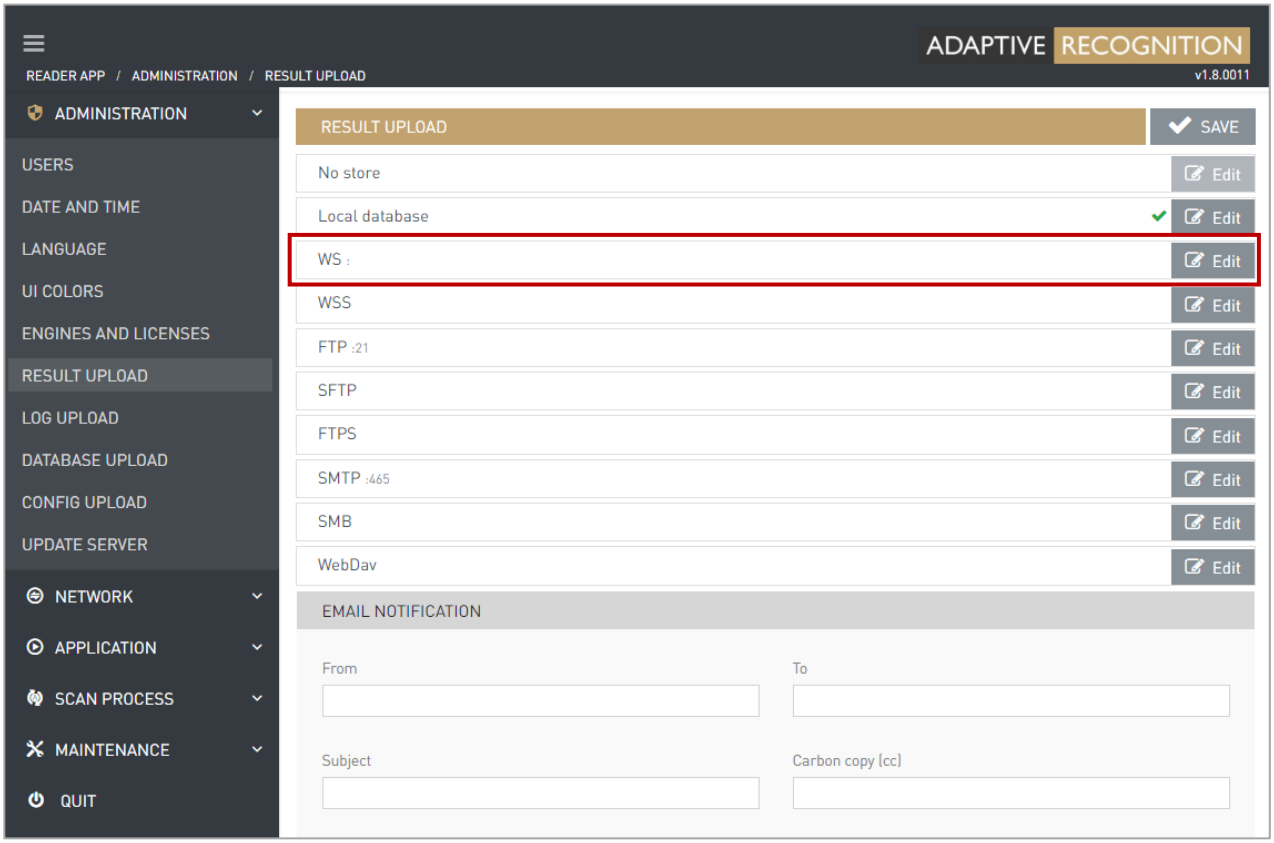
13.4. SETTING ON OSMOND

The parameters of the WS protocol can be set on the web interface of the Osmond device. By default, the web interface is accessible on 192.0.2.3:3000, but it can be set to another address as well. The IP address of the Osmond in the example is 192.168.6.244:3000.

1. After signing in to the web interface, click on the **Main menu** (the three horizontal stripes; at the top left corner of the webpage) in order to open the menu items.

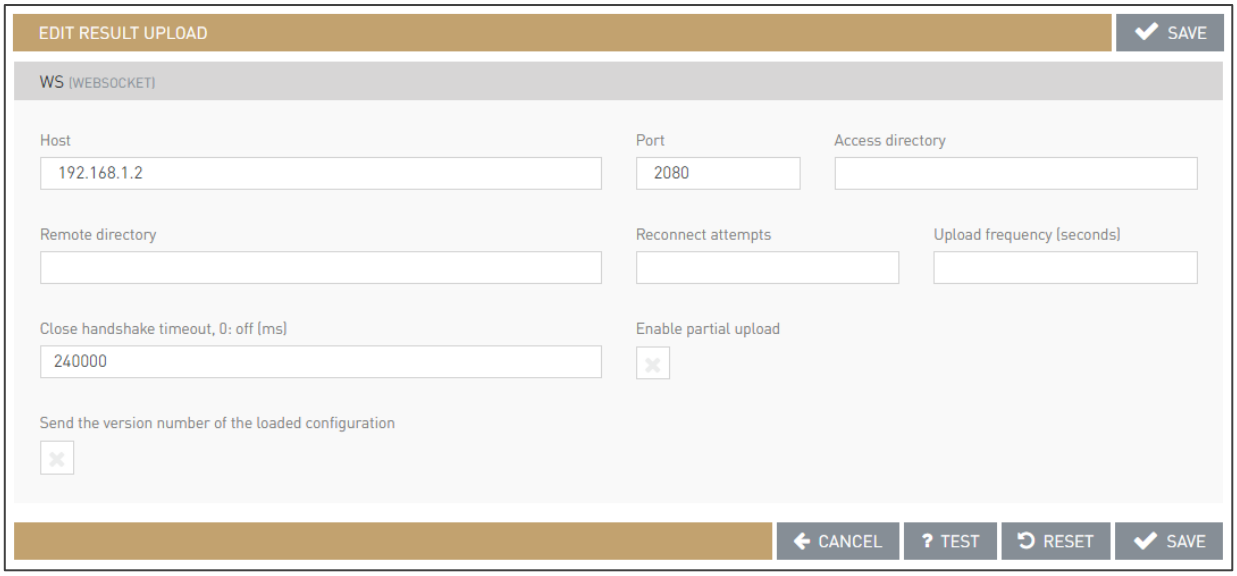
2. Navigate to **ADMINISTRATION / RESULT UPLOAD**.

3. Click on the **[Edit]** button belonging to **WS** protocol.



4. On the appearing menu set the following:
   - **Host**: IP address of the WS server, in this case: 192.168.1.2
   - **Port**: Port of the WS server: 2080

> **Note**
>
> Leave the other fields blank.



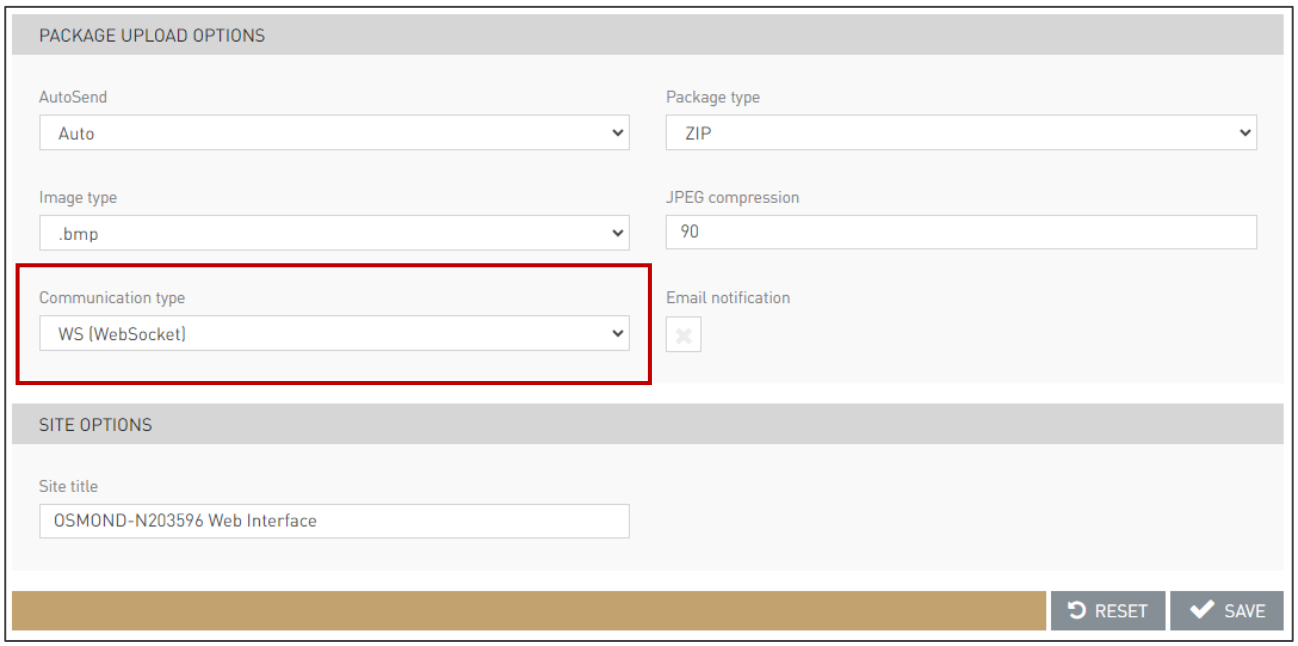
5. Check the correct settings are applied by clicking on the **[TEST]** button.
   Every test result must be passed (green).

6. If the test is passed, click on the **[SAVE]** button.

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

7. Then, navigate to **SCAN PROCESS / MAIN CONFIGURATION**. In this menu item, under **PACKAGE UPLOAD OPTIONS / Communication type** select **WS (WebSocket)** protocol.

8. Then, click on the **[SAVE]** button.



After performing these settings, the scanned documents are transferred to the upload server as a zip file.

13.5. ANNEX

13.5.1. WS_SERVER_RUBY.RB

```
require 'websocket-eventmachine-server'
require 'json'

ws_port = (JSON.parse File.read "ws_server_ruby.json")["ws_port"].to_i
upload_directory = File.expand_path (JSON.parse File.read "ws_server_ruby.json")["upload_directory"]
puts "WS server started (Ruby)"
puts "Upload directory: #{upload_directory}"

EM.run do
 file_name = ""
 WebSocket::EventMachine::Server.start(:host => "0.0.0.0", :port => ws_port) do |ws|
  ws.onopen do
   file_name = ""
  end

  ws.onmessage do |msg, type|
   if type.to_s == "text"
    if (JSON.parse msg.to_s)["params"].length > 0
     unless (JSON.parse msg.to_s)["params"].is_a?(Array)
      unless (JSON.parse msg.to_s)["params"]["packageReady"].nil?
       if (JSON.parse msg.to_s)["params"]["packageReady"].length > 0
        if (not file_name.nil?) and (file_name.length == 0)
         file_name = (JSON.parse msg.to_s)["params"]["packageReady"].gsub(/:/, ".")
        end
       end
      end
     end
    end
   elsif type.to_s == "binary"
    if (not file_name.nil?) and (file_name.length > 0)
     f2 = File.open("#{upload_directory}/#{file_name}","wb")
     f2.write(msg)
     f2.close
     puts "File was written into #{file_name}"
    end
   end
  end
```

```
  ws.onclose do
    file_name = ""
  end
 end
end
```

13.5.2. WS_SERVER_RUBY.JSON

```
{
 "ws_port": "2080",
 "upload_directory": "~/ws_share"
}
```

13.5.3. WS_SERVER_PYTHON.PY

```
#!/usr/bin/env python

import asyncio
import websockets
import json
import os

ws_server_ruby_json = json.loads(open("ws_server_python.json", "r").read())
ws_port = int(ws_server_ruby_json["ws_port"])
upload_directory = os.path.expanduser(ws_server_ruby_json["upload_directory"])
print("WS server started (Python)")
print("Upload directory: ", upload_directory)


async def echo(websocket):
    file_name = ""
    try:
        async for message in websocket:
            try:
                if isinstance( message, str):
                    data = json.loads(message)
                    if "params" in data.keys():
                        if isinstance(data["params"], dict):
                            if "packageReady" in data["params"].keys():
                                if len(data["params"]["packageReady"]) > 0:
                                    if (file_name is not None) and (len(file_name) == 0):
                                        file_name = data['params']['packageReady'].replace(':', '.')
                elif isinstance( message, bytes):
                    if len(file_name) > 0:
                        with open(upload_directory + "/" + file_name, 'wb') as file:
                            file.write(message)
                        print("File was written into ", file_name)
                        file_name = ""
            except Exception as e:
                print ("Error: ", e)
                print ("Error: ", e.with_traceback())
    except websockets.exceptions.ConnectionClosedError:
        pass
```

```
async def main():
    async with websockets.serve(echo, "0.0.0.0", ws_port, max_size=12*1024*1024, compression=None):
        await asyncio.Future()  # run forever

asyncio.run(main())
```

13.5.4. WS_SERVER_PYTHON.JSON

```
{
 "ws_port": "2080",
 "upload_directory": "~/ws_share"
}
```


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

13.5.5. WS_SERVER_JAVA.JAVA

```
package org.example;

import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStreamReader;
import java.net.InetSocketAddress;
import java.net.UnknownHostException;
import java.nio.ByteBuffer;
import java.nio.charset.StandardCharsets;
import java.nio.file.Files;
import java.nio.file.Path;
import java.nio.file.Paths;
import java.util.Collections;
import org.java_websocket.WebSocket;
import org.java_websocket.drafts.Draft;
import org.java_websocket.drafts.Draft_6455;
import org.java_websocket.handshake.ClientHandshake;
import org.java_websocket.server.WebSocketServer;
import org.json.JSONObject;
import java.io.*;

public class ws_server_java extends WebSocketServer {
  String  file_name = "";
  static int ws_port = 2080;
  static String upload_directory = "";

  public ws_server_java(int port) throws UnknownHostException {
    super(new InetSocketAddress(port));
  }

  public ws_server_java(InetSocketAddress address) {
    super(address);
  }

  public ws_server_java(int port, Draft_6455 draft) {
    super(new InetSocketAddress(port), Collections.<Draft>singletonList(draft));
  }

  @Override
  public void onOpen(WebSocket conn, ClientHandshake handshake) {
```

```
    /*
    System.out.println(
            conn.getRemoteSocketAddress().getAddress().getHostAddress() + " connected");
    */
}

@Override
public void onClose(WebSocket conn, int code, String reason, boolean remote) {
    file_name = "";
}

@Override
public void onMessage(WebSocket conn, String message) {
    JSONObject message_json = new JSONObject(message);
    if (message_json.has("params")) {
        if (message_json.get("params") instanceof JSONObject) {
            if (((JSONObject)message_json.get("params")).has("packageReady")) {
                if (((String)(((JSONObject)message_json.get("params")).get("packageReady"))).length() > 0) {
                    if (file_name == "") {
                        file_name = ((String)(((JSONObject)message_json.get("params")).get("packageReady"))).replace(":", ".");
                    }
                }
            }
        }
    }
}

@Override
public void onMessage(WebSocket conn, ByteBuffer message) {
    try {
        if (file_name.length() > 0) {
            OutputStream f2 = new FileOutputStream(upload_directory + "/" + file_name);
            f2.write(message.array());
            f2.flush();
            f2.close();
            System.out.println("File was written into " + file_name);
        }
    } catch (Exception ex) {
        System.out.println("Error: " + ex.getMessage());
        ex.printStackTrace();
        System.exit(1);
    }
```

```
}

private static String expand_path(String basic_path) {
    if (basic_path.startsWith("~" + File.separator)) {
        basic_path = System.getProperty("user.home") + basic_path.substring(1);
    }
    return basic_path;
}

public static void main(String[] args) throws InterruptedException, IOException {
    try {
        String full_json_path = System.getProperty("user.dir") + "/ws_server_java.json";
        Path path_full_json_path = Paths.get(full_json_path);
        if (!Files.exists(path_full_json_path)) {
            System.out.println("Error: the config file does not exist: " + full_json_path);
            System.out.println("Exiting...");
            System.exit(1);
        }
        String ws_server_java_str = new String(Files.readAllBytes(path_full_json_path), StandardCharsets.UTF_8);
        JSONObject ws_server_java_json = new JSONObject(ws_server_java_str);
        ws_port = Integer.parseInt((String)ws_server_java_json.get("ws_port"));
        upload_directory = expand_path((String)ws_server_java_json.get("upload_directory"));
        if (!Files.exists(Paths.get(upload_directory))) {
            System.out.println("Error: the given upload directory does not exist: " + upload_directory);
            System.out.println("Exiting...");
            System.exit(1);
        }
    } catch (Exception ex) {
        System.out.println(ex.getMessage());
        ex.printStackTrace();
        System.exit(1);
    }
    ws_server_java s = new ws_server_java(ws_port);
    s.start();
    System.out.println("Wserver started on port: " + s.getPort());

    BufferedReader sysin = new BufferedReader(new InputStreamReader(System.in));
    while (true) {
        String in = sysin.readLine();
        s.broadcast(in);
        if (in.equals("exit")) {
            System.out.println("Exiting from the app...");
```

```
            s.stop(10000);
            //System.exit(0);
            break;
        }
    }
  }

  @Override
  public void onError(WebSocket conn, Exception ex) {
    ex.printStackTrace();
    if (conn != null) {

    }
  }

  @Override
  public void onStart() {
    System.out.println("Server started!");
    setConnectionLostTimeout(0);
    setConnectionLostTimeout(100);
  }
}
```

13.5.6. WS_SERVER_JAVA.JSON

```
{
 "ws_port": "2080",
 "upload_directory": "~/ws_share"
}
```

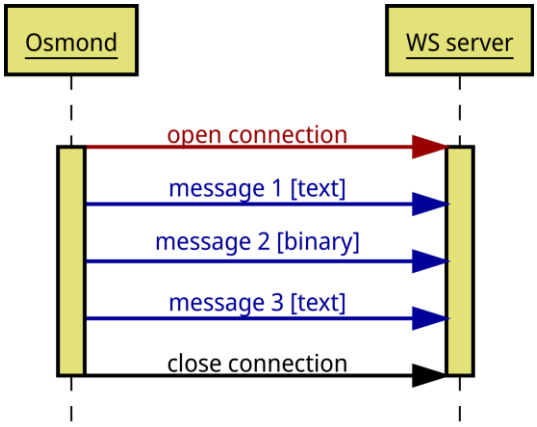
13.5.7. THE STRUCTURE OF THE WS COMMUNICATION DATA CONTENT

1. SENDING THE SETTINGS

In case of setting the "Config (j_on) file upload", the first upload sent at startup will be the configuration j_on file (it is not a JSON, however very similar). This is not a scanned data, but it is transferred in ZIP format.

2. SEND DATA THROUGH WS/WSS PROTOCOL

Data transmission is a communication at the end of which the connection is terminated.



Simplified sequence diagram of the WS/WSS protocol

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

3. MESSAGES OF WHICH THE COMMUNICATION CONSISTS

1. Message

TEXT message which can be of two types depending on the value of the "**Send the version number of the loaded configuration?**":

- If it is enabled:

```
{
"jsonrpc":"2.0",
"method":"notify",
"params":{
 "packageReady":"$remote_directory/$filename",
 "deviceName":"$deviceName",
 "serialNumber":"$serialNumber",
 "nwRelease":"$nwRelease",
 "configVersion":"$configVersion"
 }
}
```

- If it is not enabled:

```
{
"jsonrpc":"2.0",
"method":"notify",
"params":{
 "packageReady":"$remote_directory/$filename",
 "deviceName":"$deviceName",
 "serialNumber":"$serialNumber",
 "nwRelease":"$nwRelease"
 }
}
```

2. Message

BINARY type message which contains the file to be uploaded.

3. Message

TEXT message which can be of two types depending on the value of the "**Send the version number of the loaded configuration?**":

- If it is enabled:

```
{
"jsonrpc":"2.0",
"method":"notify",
"params":{
 "packageReady":"$remote_directory/$filename",
 "deviceName":"$deviceName",
 "serialNumber":"$serialNumber",
 "nwRelease":"$nwRelease",
 "configVersion":"$configVersion",
 "fileSent":"end_of_transmission"
 }
}
```

- If it is not enabled:

```
{
"jsonrpc":"2.0",
"method":"notify",
"params":{
 "packageReady":"$remote_directory/$filename",
 "deviceName":"$deviceName",
 "serialNumber":"$serialNumber",
 "nwRelease":"$nwRelease",
 "fileSent":"end_of_transmission"
 }
}
```

4. MEANING

- **$remote_directory** contains the value of the "remote directory" specified in the configuration.
- **$filename** is the name of the file to be uploaded.
- **$serialNumber** is the serial number of the document reader device.
- **$nwRelease** contains the release date of the firmware.
- **$configVersion** contains the version number of the current configuration. (It is handed over by the sender during transfer.)

5. EXAMPLES

- When "**Send the version number of the loaded configuration?**" is disabled:

1. {"jsonrpc":"2.0","method":"notify","params":{"packageReady":"dir/OSMOND-N211786_2022-11-04T12.24.18Z_bcda358e.zip","deviceName":"OSMOND-N","serialNumber":"211786","nwRelease":"8-RC-2022-11-03"}}
2. binary-data.
3. {"jsonrpc":"2.0","method":"notify","params":{"packageReady":"dir/OSMOND-N211786_2022-11-04T12.24.18Z_bcda358e.zip","deviceName":"OSMOND-N","serialNumber":"211786","nwRelease":"8-RC-2022-11-03","fileSent":"end_of_transmission"}}

- When "**Send the version number of the loaded configuration?**" is enabled:

1. {"jsonrpc":"2.0","method":"notify","params":{"packageReady":"dir/OSMOND-N211786_2022-11-04T13.24.18Z_ad1131c0.zip","deviceName":"OSMOND-N","serialNumber":"211786","nwRelease":"8-RC-2022-11-03","configVersion":"0.0.0.0"}}
2. binary-data.
3. {"jsonrpc":"2.0","method":"notify","params":{"packageReady":"dir/OSMOND-N211786_2022-11-04T13.24.18Z_ad1131c0.zip","deviceName":"OSMOND-N","serialNumber":"211786","nwRelease":"8-RC-2022-11-03","configVersion":"0.0.0.0","fileSent":"end_of_transmission"}}

6. FILENAME RULES

6.1. Meaning of the fields:

- **%READER** is the device ID
- **%YYYY** marks the year, which consists of 4 digits
- **%mm** marks the month, which consists of 2 digits
- **%dd** marks the day, which consists of 2 digits
- **%HH** marks the hour, which consists of 2 digits
- **%MM** marks the minutes, which consists of 2 digits
- **%SS** marks the seconds, which consists of 2 digits
- **%RANDOMHEXANUMBER** is an 8-character long random number in hexadecimal form.

Important!

The time is UTC-based.

6.2. File names:

- The structure of the read data file name:

  %READER_%YYYY-%mm-%ddT%HH.%MM.%SSZ_%RANDOMHEXANUMBER.zip

  Example

  OSMOND-N211786_2022-11-04T13.24.18Z_ad1131c0.zip

- The structure of the configuration file name:

  config_%READER_%YYYY%mm%dd-%HH%MM%SS.zip

  Example

  config_OSMOND-N211786_20221104-123446.zip

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

14. SETTING THE FTP PROTOCOL ON OSMOND

The current version (1.8) of the Osmond firmware is capable of uploading the scanned data to a server via multiple protocols.

In this section the settings of the FTP protocol will be explained.

The parameters are the following:

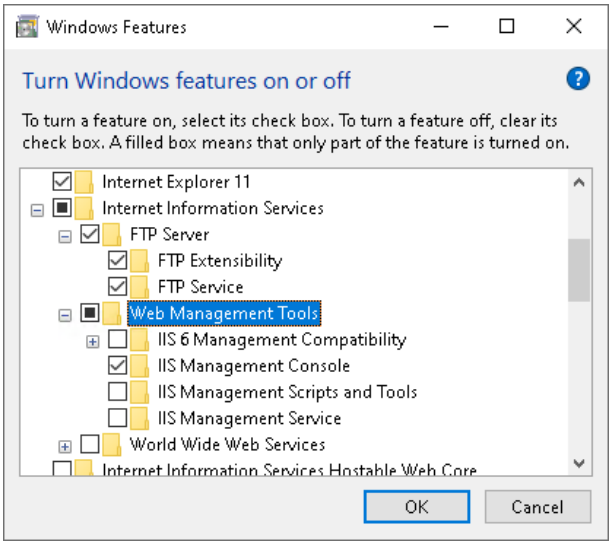
- IP address of the FTP server: 192.168.1.2
- IP address of the Osmond device: 192.168.6.244
- The user (registered Windows user with password): tesztg
- The password of the user: 123456
- The shared folder on Windows (upload path): C:\ftp_share

14.1. INSTALLING AND SETTING THE FTP SERVER ON WINDOWS 10

14.1.1. INSTALLING THE FTP SERVER

1. Navigate to **Start menu / Control Panel / Programs / Turn Windows features on or off**.

2. Select the following options by ticking their checkboxes:
   - **Internet Information Services / FTP Server / FTP Extensibility**
   - **Internet Information Services / FTP Server / FTP Service**
   - **Internet Information Services / FTP Server / Web Management Tools / IIS Management Console**



3. Click on the **[OK]** button.

14.1.2. SETTING FTP

1. Create the library, for example:
   C:\ftp_share

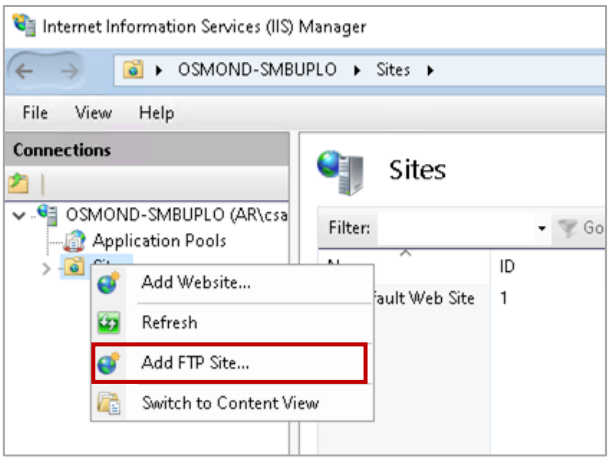
> **Note**
>
> If the library is created with the user, with which the FTP is used – in this case "tesztg" – then there is no need to share it.

2. Navigate to **Start menu / Internet Information Services (IIS) Manager**.

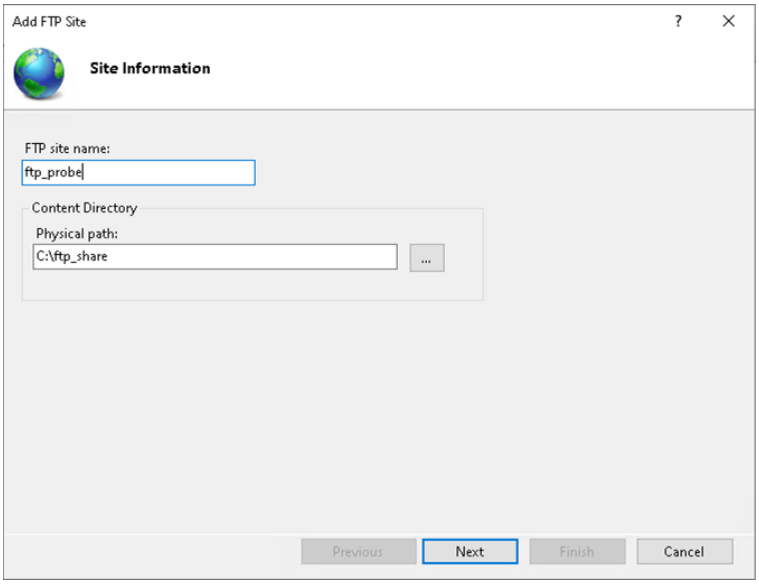
3. On the left panel click on the arrow to unfold additional items.

4. Right click on "**Sites**".

5. Select the "**Add FTP Site...**" option.

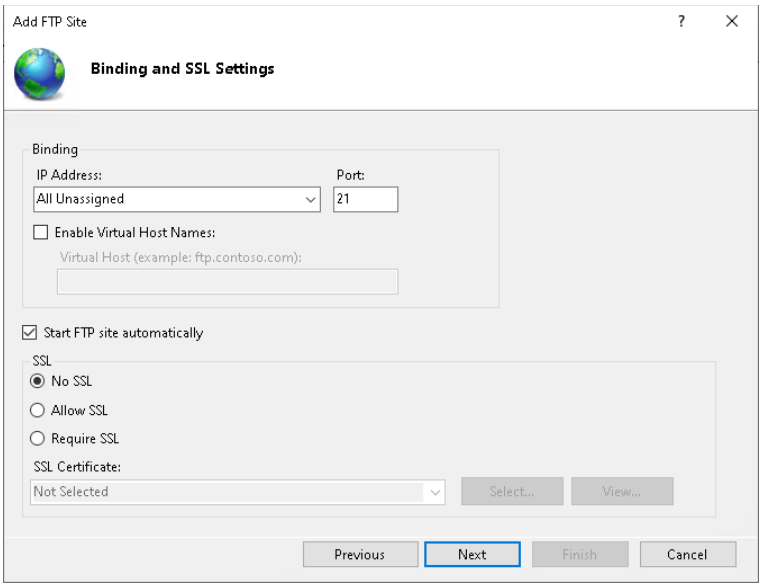


6. In the appearing window specify the following parameters:
   - **FTP site name**: in this case ftp_probe
   - **Physical path**: in this case C:\ftp_share



7. Then, click on the **[Next]** button.

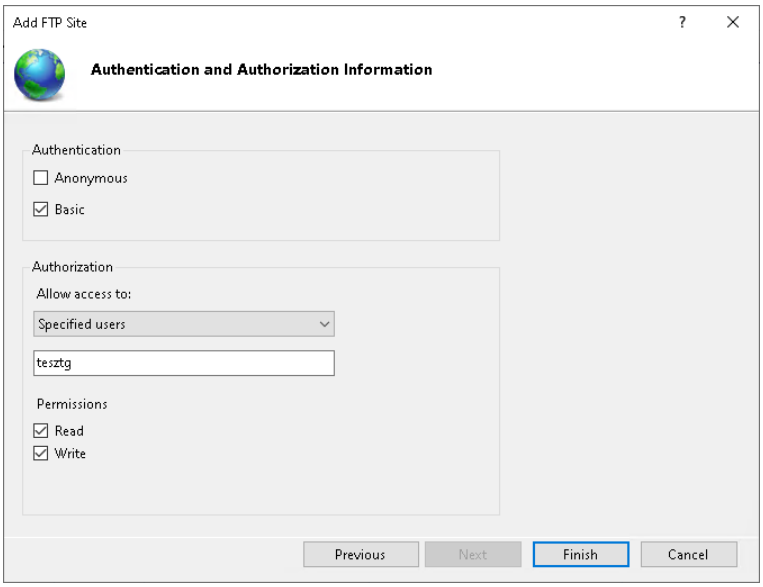
8. In the next window select "**No SSL**". Leave the rest of the settings as default:
   - **IP address**: "All Unassigned"
   - **Port**: "21"
   - Enabled "**Start FTP site automatically**"



9. Then, click on **[Next]**.

10. In the next window set the following values:
    - At **Authentication** select "**Basic**"
    - At **Authorization / Allow access to** select "**Specified users**".

      Under "**Specified users**" field, enter the username, in this case "tesztg"
    - At **Authorization / Permissions** select "**Read**" and "**Write**".



11. Then, click on **[Finish]**.

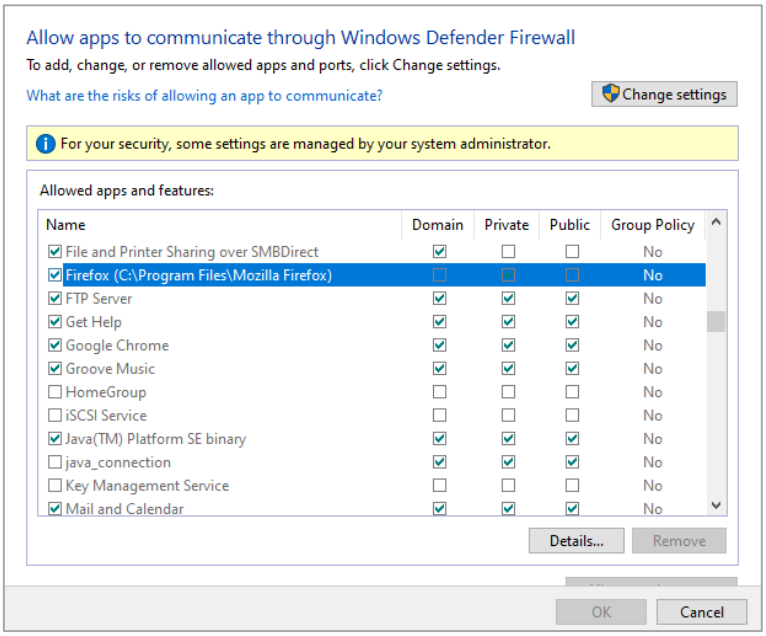
Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

14.1.3. SETTING THE FIREWALL

It is recommended to check the Windows Firewall settings:

1. Navigate to **Control Panel / System and Security / Windows Defender Firewall / Allow an app or feature through Windows Defender Firewall**.

2. Enable "**FTP server**" under the appropriate network type by ticking the box.



Note

In case of making any modification, restart the PC.

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

14.2. INSTALLING AND SETTING THE FTP SERVER ON LINUX

14.2.1. INSTALLING THE FTP SERVER

Under Linux install FTP server from command line. The commands may depend on the distribution. The following commands apply to Ubuntu 22.04.

1. Update Ubuntu:
   ```
   sudo apt update
   sudo apt upgrade -y
   ```

2. Install FTP Daemon (Vsftpd):
   ```
   sudo apt install vsftpd
   ```

3. After installation, it is recommended to check the daemon:
   ```
   systemctl status vsftpd
   ```

4. If the returned message is "Active: active (running)", then everything is OK.

5. Add a user to the system. This user will use the FTP server, thereby you can log in with this user:
   ```
   sudo adduser tesztg
   ```

   Specify the password of the user (e.g., 123456).
   In addition, other values (e.g., full name, phone number) can be entered as well. Entering these values is optional, they can be omitted.

6. Create the FTP library.
   ```
   sudo mkdir -p /home/tesztg/ftp_share
   sudo chmod -R 750 /home/tesztg/ftp_share
   sudo chown tesztg: /home/tesztg/ftp_share
   ```

7. The FTP user must be entered to the `vsftpd.user_list` file:
   ```
   sudo bash -c 'echo tesztg >> /etc/vsftpd.user_list'
   ```

14.2.2. SETTING THE FTP

1. Open the **/etc/vsftpd.conf** file:

   ```
   sudo vim /etc/vsftpd.conf
   ```

   In the **/etc/vsftpd.conf** file:

   ```
   anonymous_enable=NO
   local_enable=YES
   write_enable=YES
   chroot_local_user=YES
   pasv_min_port=30000
   pasv_max_port=31000
   userlist_enable=YES
   userlist_file=/etc/vsftpd.user_list
   userlist_deny=NO
   allow_writeable_chroot=YES
   user_sub_token=$USER
   local_root=/home/$USER/ftp_share
   ```

   After setting, save the file and quit:

   In case of Vim text editor:

   Press the **[Esc]** key and use the **:wq** command.

   Other text editor can be used as well.

2. Restart the FTP Daemon.

   ```
   sudo systemctl restart vsftpd
   ```

The FTP server can be tested from the server itself with the following command:

```
ftp 192.168.1.2
```

If it requires the username and password, and with these a log in is performed, then the FTP server operates.

14.2.3. SETTING THE FIREWALL

The ports used by FTP must be set in the firewall, then restart it, if the firewall is active. In general, the `ufw` runs on Ubuntu. Its state can be queried with the `sudo ufw status` command.

If it is active, then:

- `sudo ufw allow 20:21/tcp`
- `sudo ufw allow 30000:31000/tcp`
- `sudo ufw disable`
- `sudo ufw enable`

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

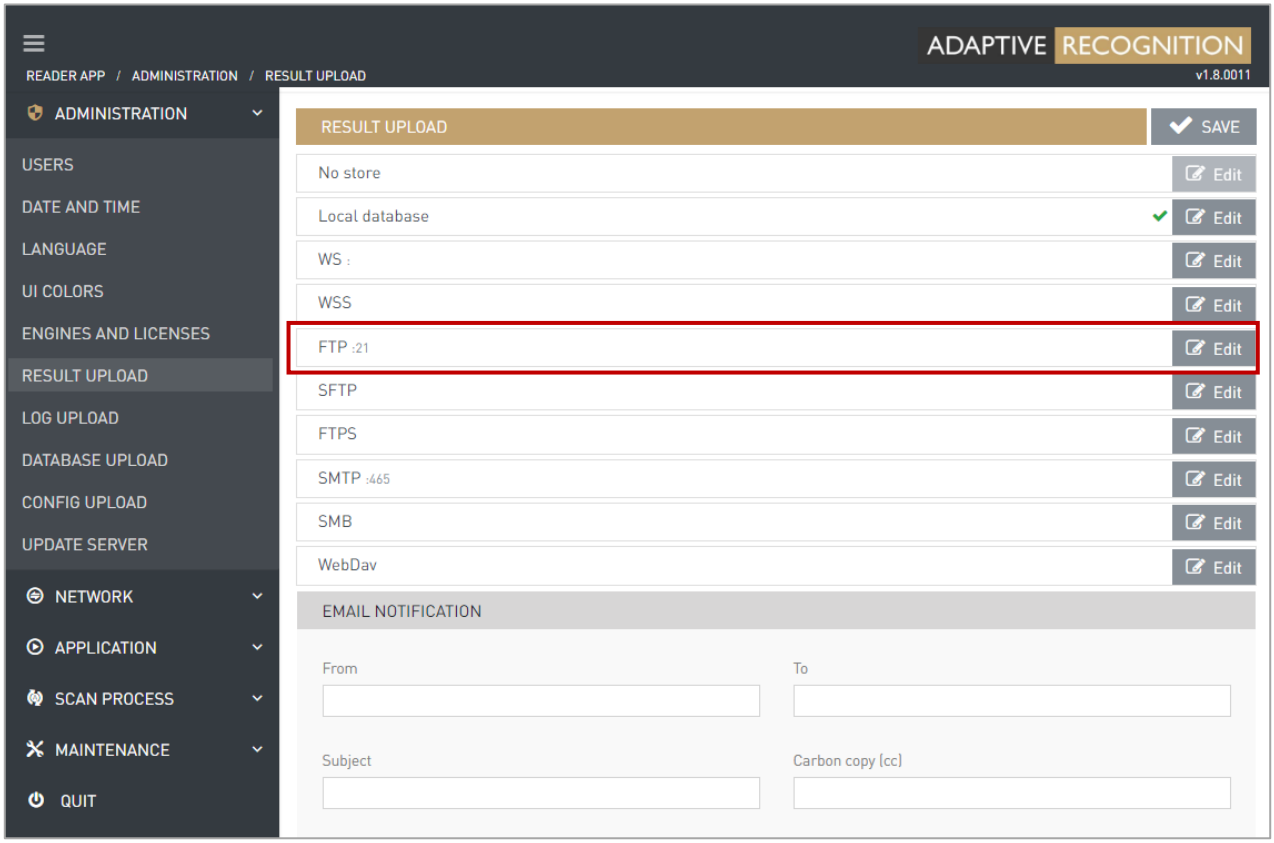
14.3. SETTING ON OSMOND

First, the parameters of the FTP protocol must be set on the web interface of the Osmond device. By default, the web interface is accessible on 192.0.2.3:3000, but it can be set to another address as well. The IP address of the Osmond in the example is 192.168.6.244:3000.

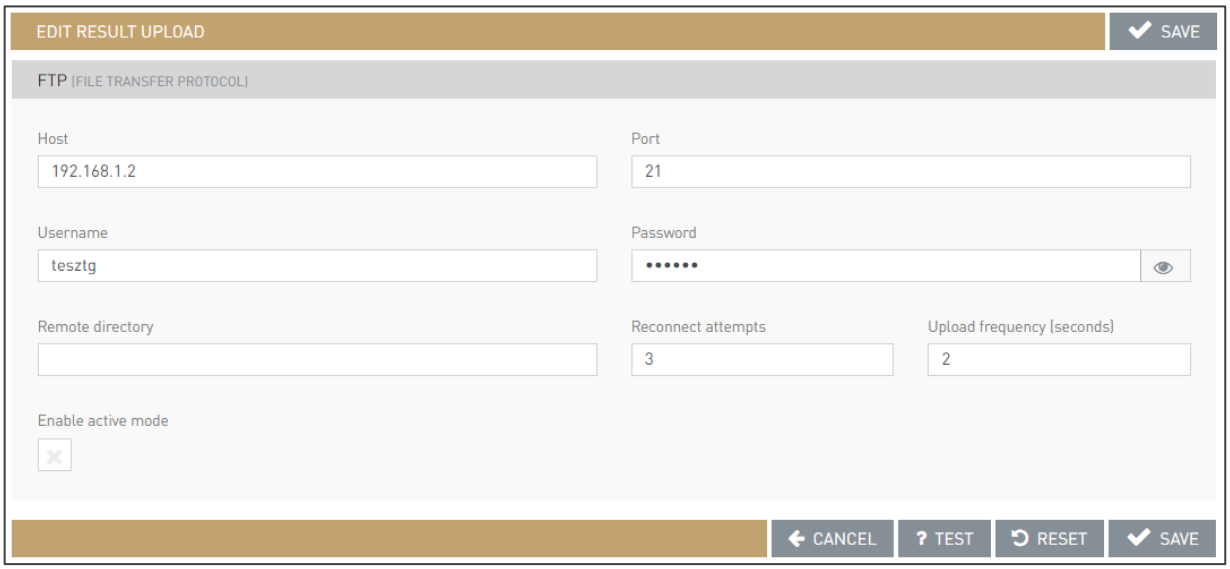
1. After signing in to the web interface, click on the **Main menu** (the three horizontal stripes; at the top left corner of the webpage) in order to open the menu items.

2. Navigate to **ADMINISTRATION / RESULT UPLOAD**.

3. Click on the **[Edit]** button belonging to **FTP** protocol.



4. On the appearing menu set the following:
   - **Host**: IP address of the FTP server, in this case: 192.168.1.2
   - **Port**: Port of the FTP server: 21
   - **Username**: Name of the user, in this case: tesztg
   - **Password**: Password of the user, in this case: 123456
   - **Remote directory**: Name of the folder accessible from the server's root directory. This field must be blank.
   - **Reconnect attempts**: The maximum number of the connections without error message, in this case: 3
   - **Upload frequency (seconds)**: The upload daemon checks if there is data to upload at specified intervals, in this case: 2



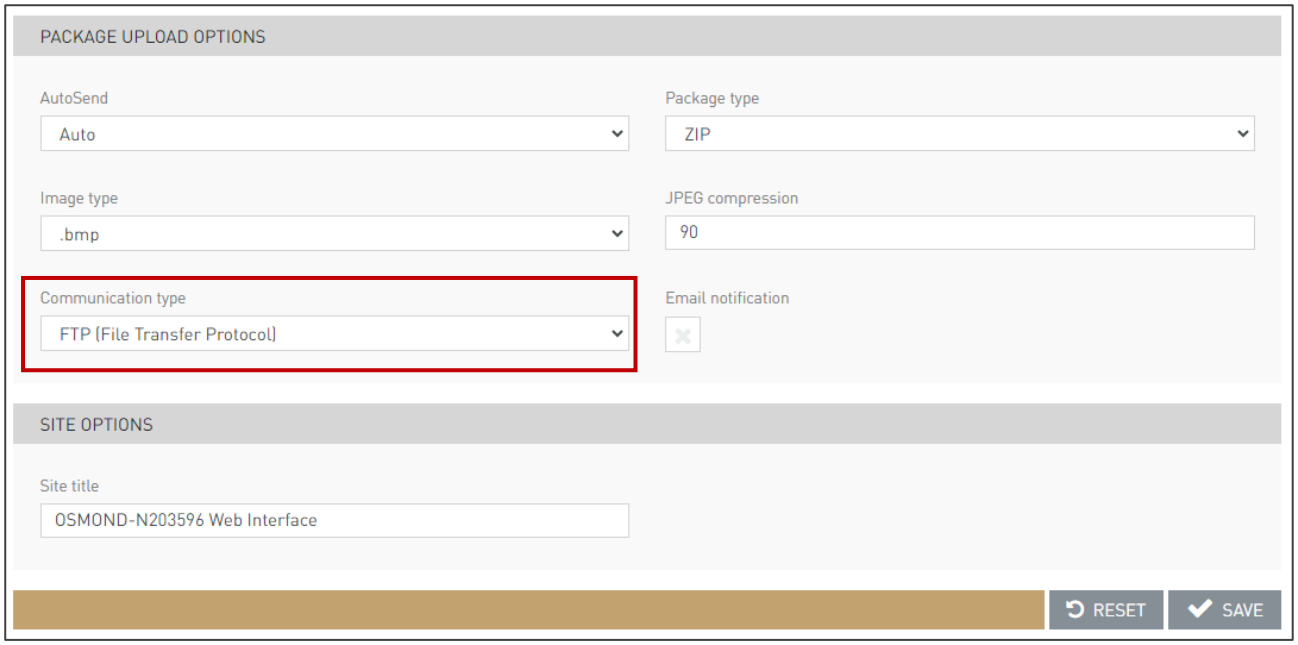
5. Check the correct settings are applied by clicking on the **[TEST]** button.
   Every test result must be passed (green).

6. If the test is passed, click on the **[SAVE]** button.

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

7. Then, navigate to **SCAN PROCESS / MAIN CONFIGURATION**. In this menu item, under **PACKAGE UPLOAD OPTIONS / Communication type** select **FTP (File Transfer Protocol)** protocol.

8. Then, click on the **[SAVE]** button.



After performing these settings, the scanned documents are transferred to the upload server as a zip file.

14.4. TESTING THE SETUP

In case of error, the FTP server can be tested from command line with the following command:

```
curl -T probe_file.txt ftp://tesztg:123456@192.168.1.2
```

where:

`probe_file.txt` is the name of the file which is to be uploaded. There is no format restriction, it can be any file type.

`tesztg` is the name of the user, used for signing in to Windows as well.

`123456` is the password belonging to the user.

`192.168.1.2` is the IP address of the FTP server.

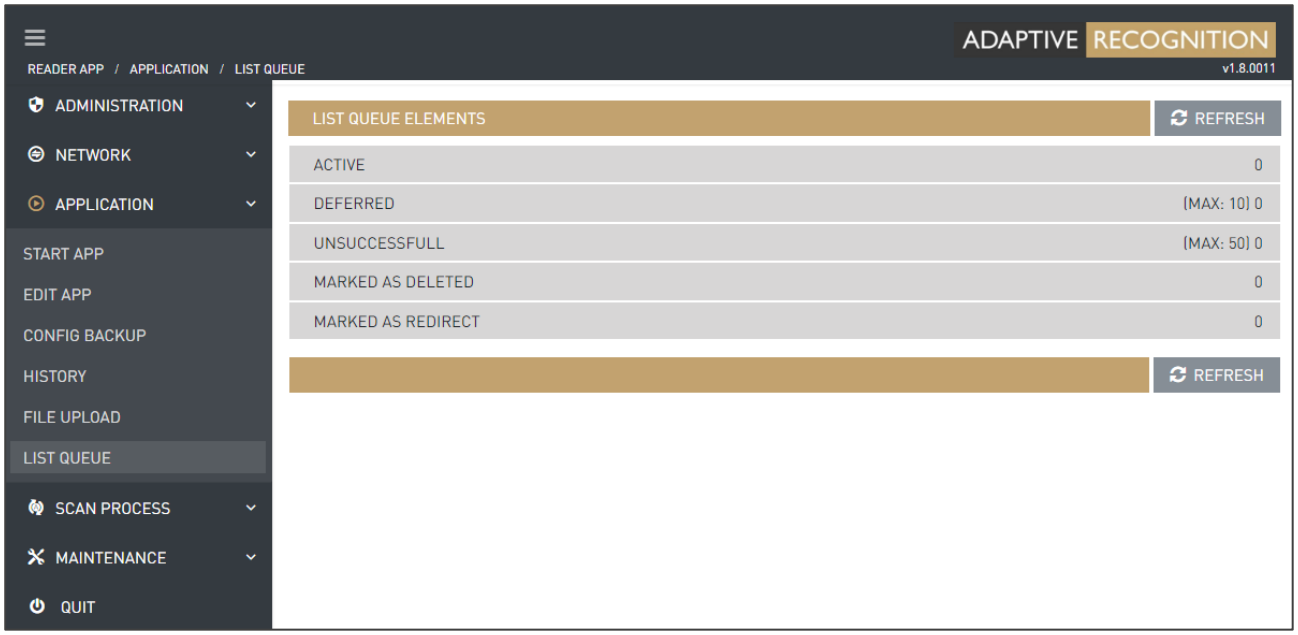
> **Note**
>
> In case of error, the `curl` command will give a more detailed description than the web interface of Osmond.

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

14.5. TROUBLESHOOTING

14.5.1. OSMOND

If upload is not working, Osmond will collect the unsuccessful documents to the **UNSUCCESSFUL queue** until its limit is not reached. When **UNSUCCESFUL** limit is reached, the oldest element in queue is overwritten by the result of the latest scan. Documents in unsuccessful status can be checked in the **APPLICATION / LIST QUEUE** menu. In case of correct operation this row is empty.



Note

If upload is not working, then the FTP server firewall (Windows or Linux) or another network device may be blocking it.

14.5.2. LINUX

If the FTP Daemon (**vsftpd**) is not running, its operation can be affected with the following commands:

- Start the Daemon:
  ```
  sudo systemctl start vsftpd
  ```
- Restart the Daemon:
  ```
  sudo systemctl restart vsftpd
  ```
- Stop the Daemon:
  ```
  sudo systemctl stop vsftpd
  ```
- Enable the Daemon to start automatically on startup (if it is not set, then it is recommended):
  ```
  sudo systemctl enable vsftpd
  ```
- Disable the Daemon to not start automatically on startup:
  ```
  sudo systemctl disable vsftpd
  ```
- Query the status of the Daemon:
  ```
  sudo systemctl status vsftpd
  ```


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

15. SETTING THE SMB (SMB1) PROTOCOL ON OSMOND

The current version (1.8) of the Osmond firmware uses the SMB1 protocol. By default, this protocol is disabled on the current Windows versions, but it is still available.
In this section the settings of the SMB1 protocol will be explained.

The parameters are the following:

- IP address of the SMB server: 192.168.1.2
- IP address of the Osmond device: 192.168.6.244
- The user (registered Windows user with password): tesztg
- The password of the user: 123456
- The shared folder on Windows (upload path): C:\smb_probashare

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

15.1. SETTING SMB ON WINDOWS 10

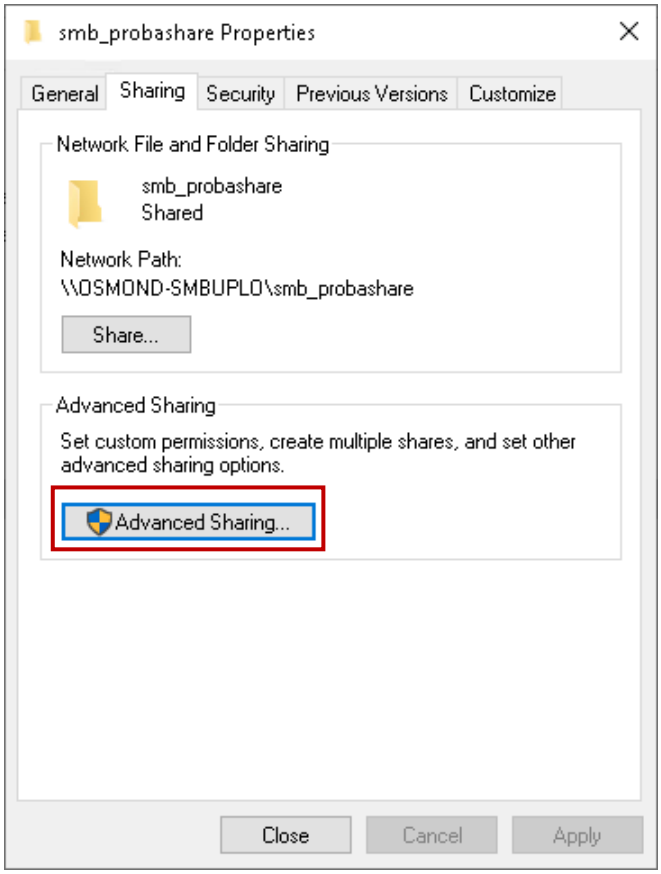
15.1.1. SHARING THE LIBRARY ON THE NETWORK

1. Create the library, for example:
   C:\smb_probashare

2. Right click on the library in the **File Explorer**, and from the appearing menu select "**Properties**".

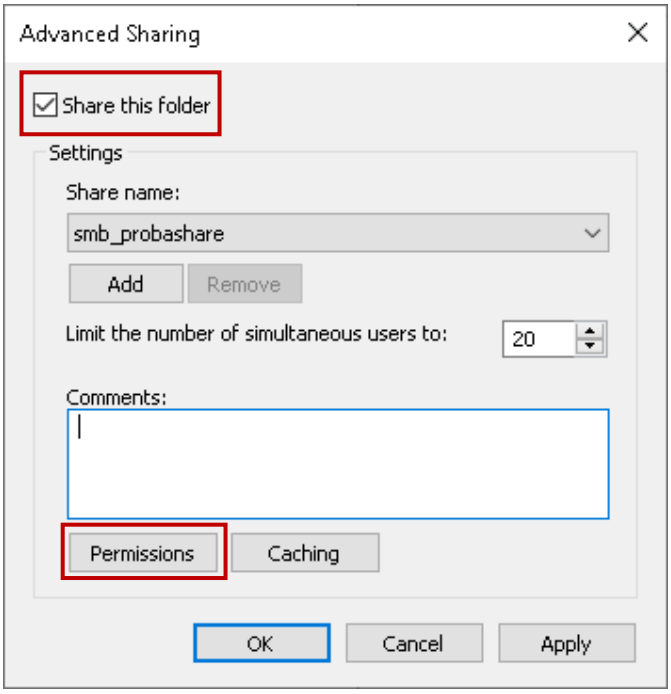
3. In the pop-up window select the "**Sharing**" tab.

4. On the "**Sharing**" tab click on the **[Advanced Sharing...]** button.

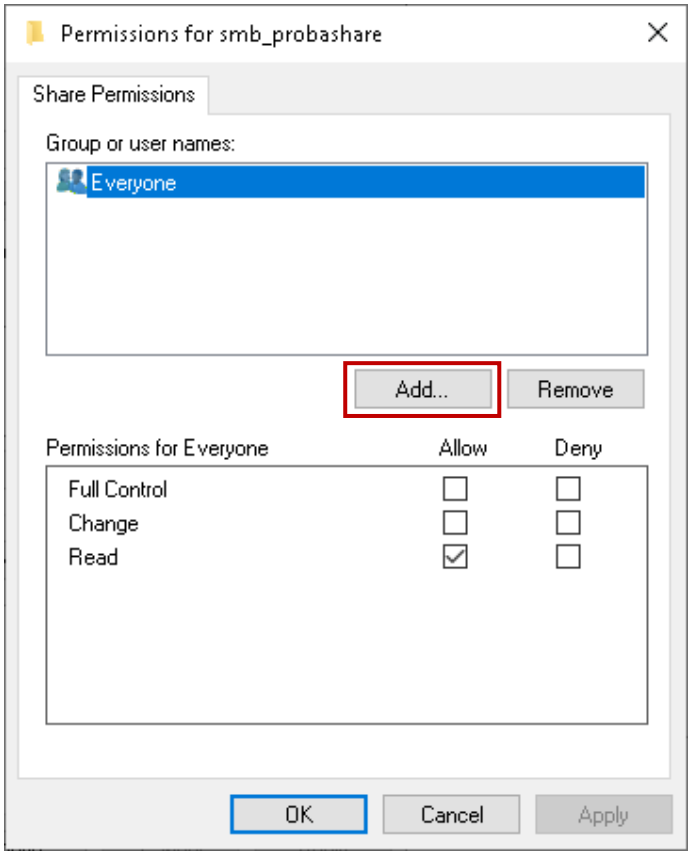


5. Enable "**Share this folder**" by ticking the box.

6. Click on the **[Permissions]** button.

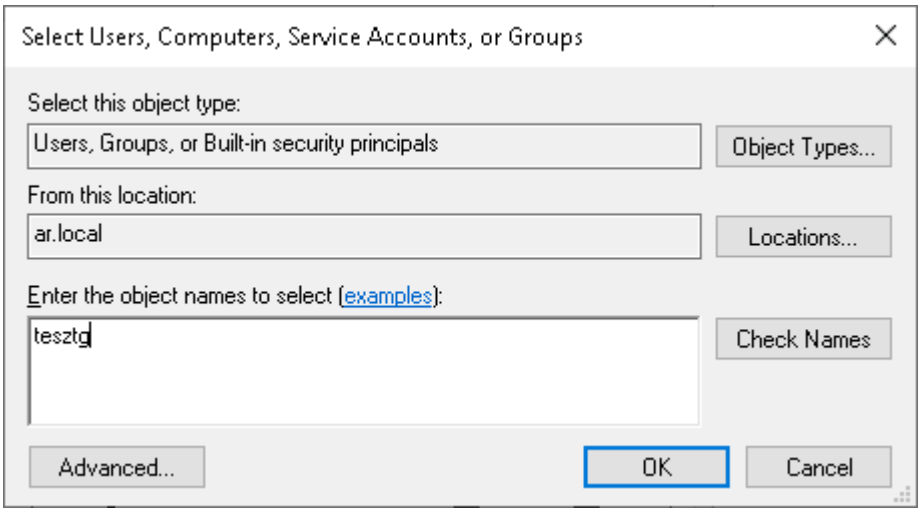


7. Then, click on the **[Add...]** button.

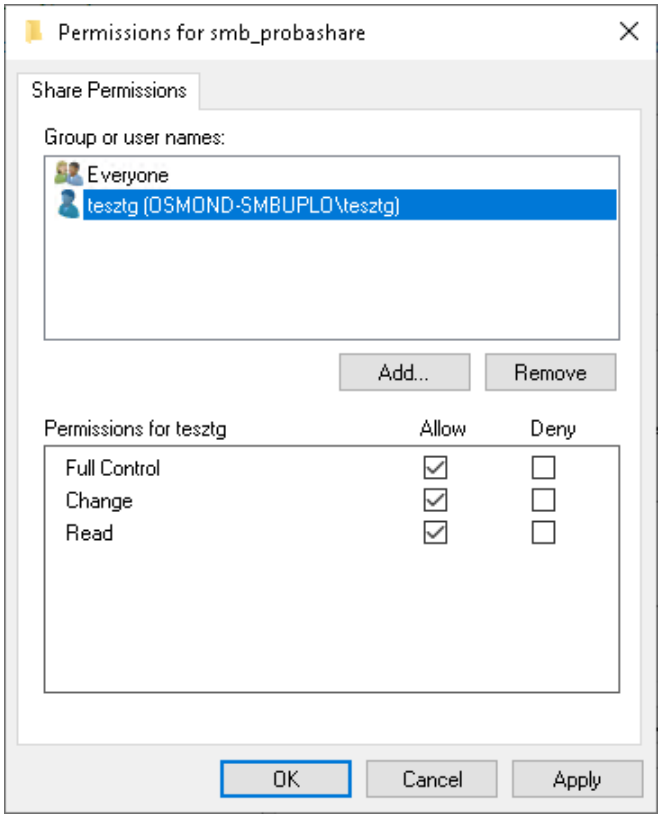


8. In the appearing window enter the name of the user on whose behalf the upload is performed. For example: tesztg

9. Click on the **[Check Names]** button to make sure the entered name is compatible.
   If the username cannot be found, then click on the **[Locations...]** button in order to select the location to search. This can be useful on PCs within domain.



10. Click on the **[OK]** button to return to **Permissions** window. Here, set the permissions of tesztg user to the given library. Checking the box for "**Full Controll**" is advised.



11. Afterwards click the **[Apply]**, then the **[OK]** buttons.

12. Click on the **[OK]** button again.

13. Then, click on the **[Close]** button.

The shared library appears on the network and can be accessed through SMB2 or SMB3 protocols.

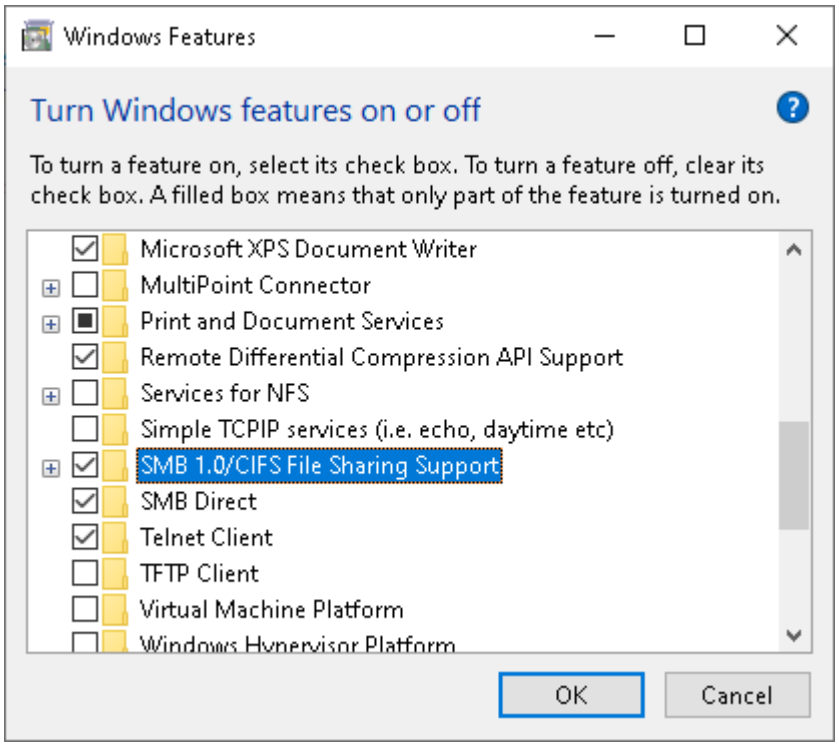
15.1.2. ENABLING SMB1 PROTOCOL ON WINDOWS 10

By default, the SMB1 protocol is disabled on Windows 10, thereby it must be enabled:

1. Navigate to **Start/Control Panel/Programs/Turn Windows features on or off**.

2. Enable "**SMB 1.0/CIFS File Sharing Support**" by ticking the box.

3. Then, click on the **[OK]** button.



4. Restart the PC.

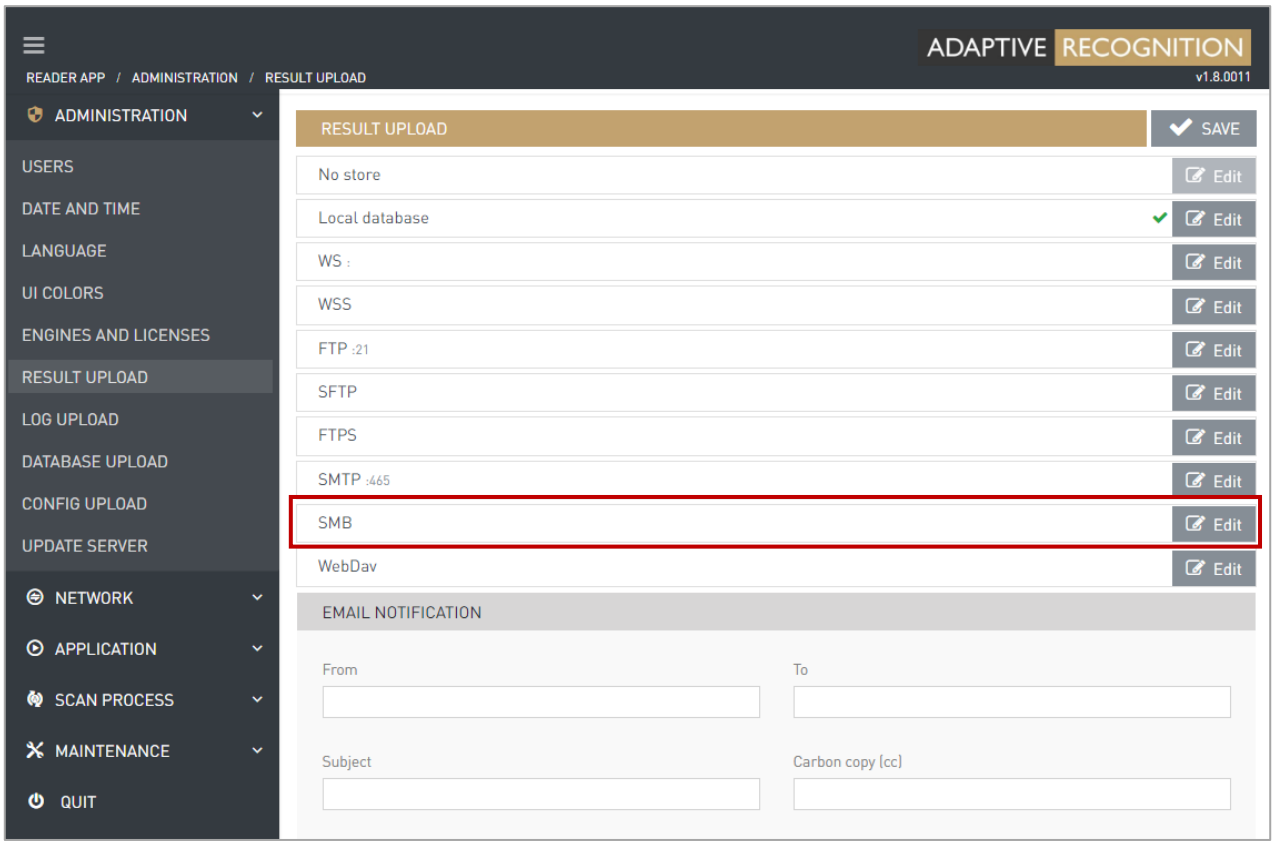
15.2. SETTING ON OSMOND

First, set the parameters of the SMB protocol on the web interface of the Osmond device. By default, the web interface is accessible on 192.0.2.3:3000, but it can be set to another address as well. The IP address of the Osmond in the example is 192.168.6.244:3000.

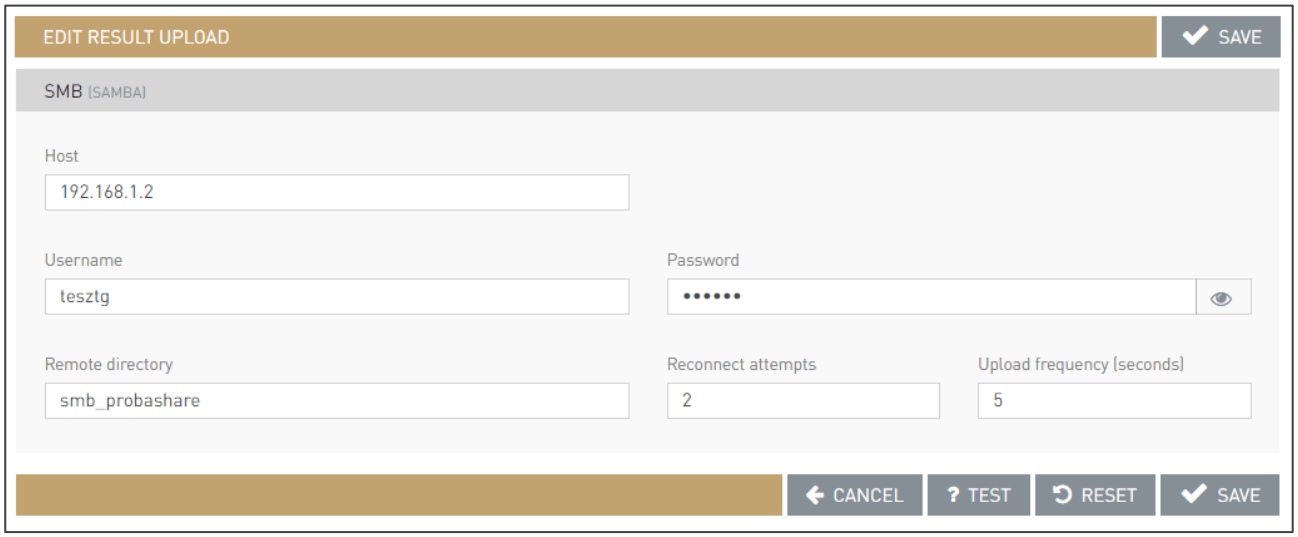
1. After signing in to the web interface, click on the **Main menu** (the three horizontal stripes; at the top left corner of the webpage) in order to open the menu items.

2. Navigate to **ADMINISTRATION / RESULT UPLOAD**.

3. Click on the **[Edit]** button belonging to **SMB** protocol.



4. On the appearing menu set the following:
   - **Host**: IP address of the SMB server, in this case: 192.168.1.2
   - **Username**: Name of the user, in this case: tesztg
   - **Password**: Password of the user, in this case: 123456 (This password is required for the tesztg user to sign in to Windows as well.)
   - **Remote directory**: The folder created on C: drive, in this case: smb_probashare
   - **Reconnect attempts**: The maximum number of the connections without error message, in this case: 2
   - **Upload frequency (seconds)**: The upload daemon checks if there is data to upload at specified intervals, in this case: 5

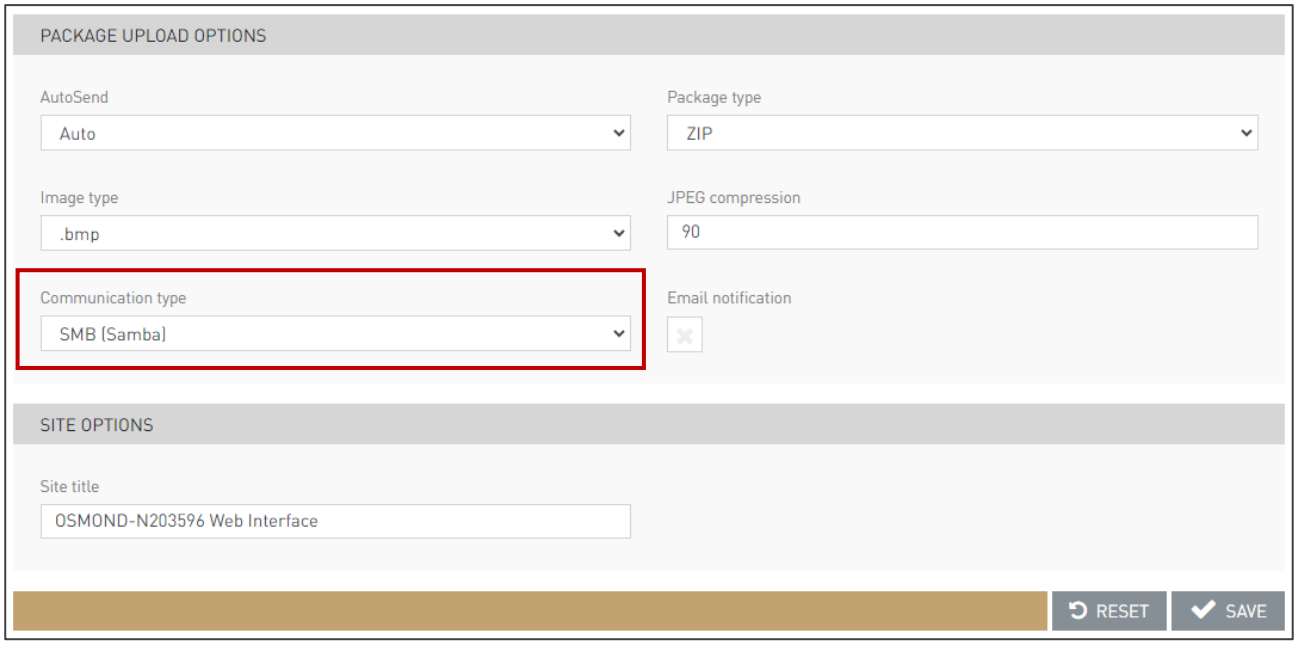


5. Check the correct settings are applied by clicking on the **[TEST]** button.
   Every test result must be passed (green), except for the last one, result of which can be the following: "Warning: The resource referenced in the URL does not exist. (78)". This message can be ignored.

6. If the test is passed, click on the **[SAVE]** button.

7. Then, navigate to **SCAN PROCESS / MAIN CONFIGURATION**. In this menu item, under **PACKAGE UPLOAD OPTIONS / Communication type** select **SMB (Samba)** protocol.

8. Then, click on the **[SAVE]** button.



After performing these settings, the scanned documents are transferred to the upload server as a zip file.

15.3. TESTING THE SETUP

In case of error, the SMB server can be tested from command line with the following command:

```
curl --upload-file probe_file.txt -u tesztg:123456
smb://192.168.1.2/smb_probashare/
```

where:

probe_file.txt is the name of the file which is to be uploaded. There is no format restriction, it can be any file type.

tesztg is the name of the user, used for signing in to Windows as well.

123456 is the password belonging to the user.

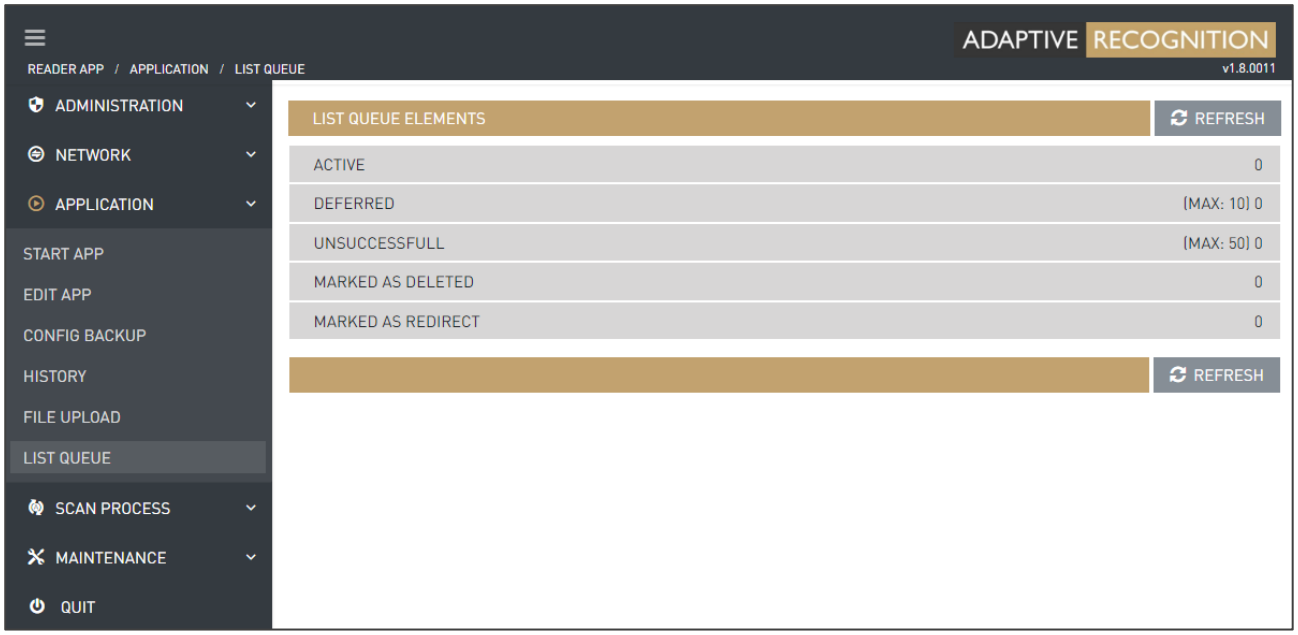
192.168.1.2 is the IP address of the SMB server.

smb_probashare is the shared folder, actually a path, without marking the C: drive.

> **Note**
>
> In case of error, the **curl** command will give a more detailed description than the web interface of Osmond.

15.4. TROUBLESHOOTING

If upload is not working, Osmond will collect the unsuccessful documents to the **UNSUCCESSFUL queue** until its limit is not reached. When **UNSUCCESFUL** limit is reached, the oldest element in queue is overwritten by the result of the latest scan. Documents in unsuccessful status can be checked in the **APPLICATION / LIST QUEUE** menu. In case of correct operation this row is empty.



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

If upload is not working, then the Windows Firewall or another network device may be blocking it.

Setting the Windows 10 Firewall:

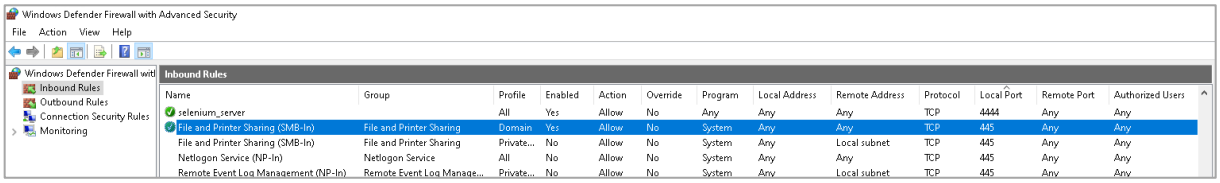
1. Navigate to **Control Panel/System and Security/Windows Defender Firewall**.

2. Click on **[Advanced settings]** located in the left section.

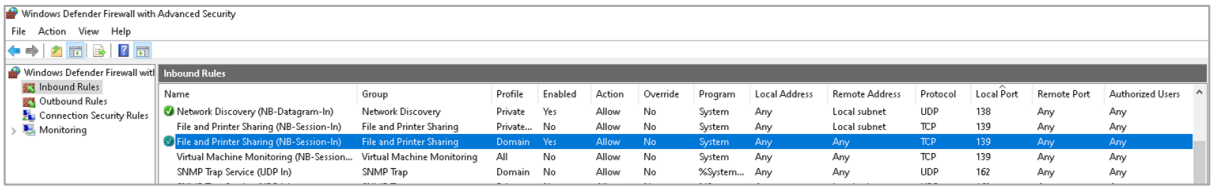
3. In the appearing window click on **[Inbound Rules]** located in the left section.

4. Enable the rules for the **ports 139 and 445** to the profile which the PC is belonging to:
   Right click on the given rule, then click on the **[Enable Rule]** option:

   - **File and Printer Sharing (SMB-In)**



   - **File and Printer Sharing (NB-Session-In)**



16. SETTING THE WEBDAV PROTOCOL ON OSMOND

The current version (1.8) of the Osmond firmware is capable of uploading the scanned data to a server via multiple protocols.
In this section the settings of the WebDav protocol will be explained.

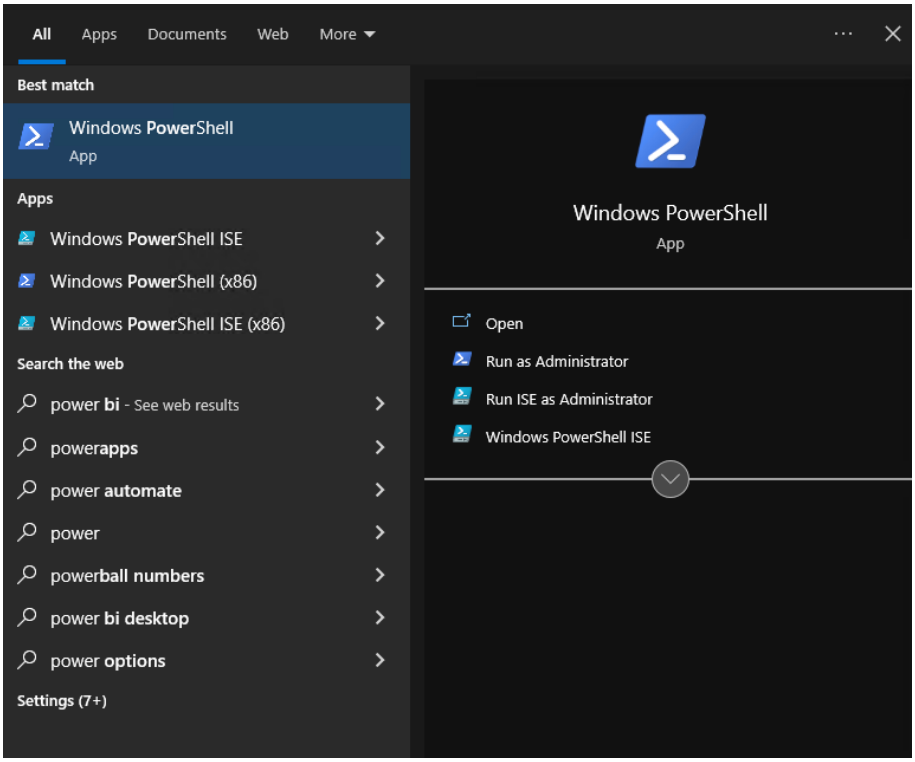
The parameters are the following:

- IP address of the WebDav server: 192.168.1.2
- IP address of the Osmond device: 192.168.6.244
- The user (registered Windows user with password): tesztg
- The password of the user: 123456
- The shared folder on Windows (upload path): C:\webdav_share
- The shared directory on Linux: /home/tesztg/webdav_share

16.1. INSTALLING AND SETTING THE WEBDAV SERVER ON WINDOWS 10

16.1.1. INSTALLING THE WEBDAV SERVER

1. Open a PowerShell terminal with administrator rights:
   - Open Start menu.
   - Enter "powershell".
   - Select the appearing **Windows PowerShell** application and click on the "**Run as Administrator**" option displayed on the right. (If the "**Run as Administrator**" text does not appear, then right click on the Windows PowerShell application and select "**Run as Administrator**".)



2. Create a library which will receive the uploads:

```
mkdir c:\webdav_share
```

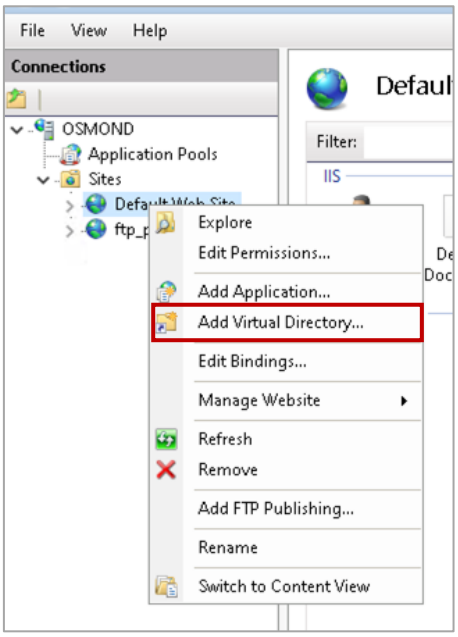
3. Copy the following command to the terminal, and press **[Enter]**:

```
$feats = @("IIS-WebServerRole","IIS-WebServer","IIS-CommonHttpFeatures","IIS-HttpErrors","IIS-Security","IIS-RequestFiltering","IIS-WebServerManagementTools","IIS-DigestAuthentication","IIS-StaticContent","IIS-DefaultDocument","IIS-DirectoryBrowsing","IIS-WebDAV","IIS-BasicAuthentication","IIS-ManagementConsole");foreach ($feat in $feats) {Enable-WindowsOptionalFeature -Online -FeatureName $feat};& "$env:windir\system32\inetsrv\InetMgr.exe";
```

   – This command installs the Internet Information Services (IIS) modules which are required for the installation and setup of WebDav.
   – Starts the IIS Manager.

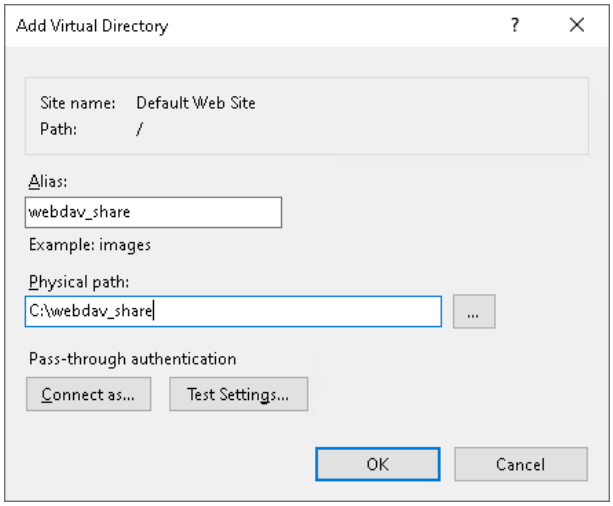
16.1.2. SETTING WEBDAV

1. After running the command, the ISS Manager (Internet Information Services (IIS) Manager) opens.
2. Under **Connections** (located on the left) click on the arrow next to the computer name to unfold additional items.
3. Then, click on the arrow next to the **Sites** to unfold its submenu.
4. In the appearing menu right click on the "**Default Web Site**" option.
5. In the appearing quick menu select the "**Add Virtual Directory...**" menu item.

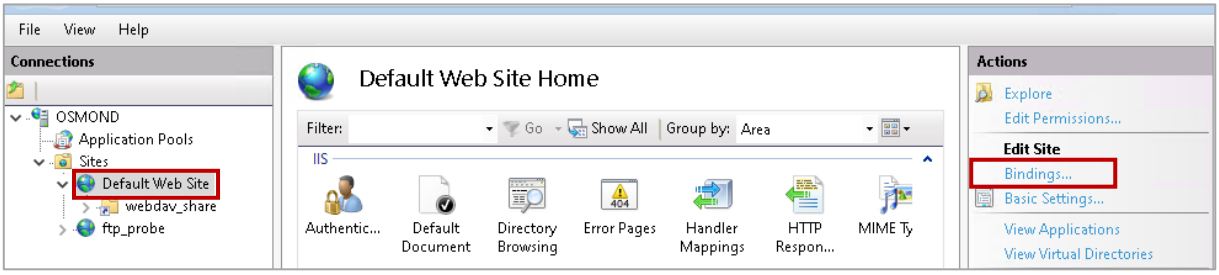


6. Type "webdav_share" to the **Alias** field.
7. Enter the name of the shared folder (or browse it by clicking on the **[...]** button) to the **Physical path** field:

   c:\webdav_share
8. Click on the **[OK]** button.

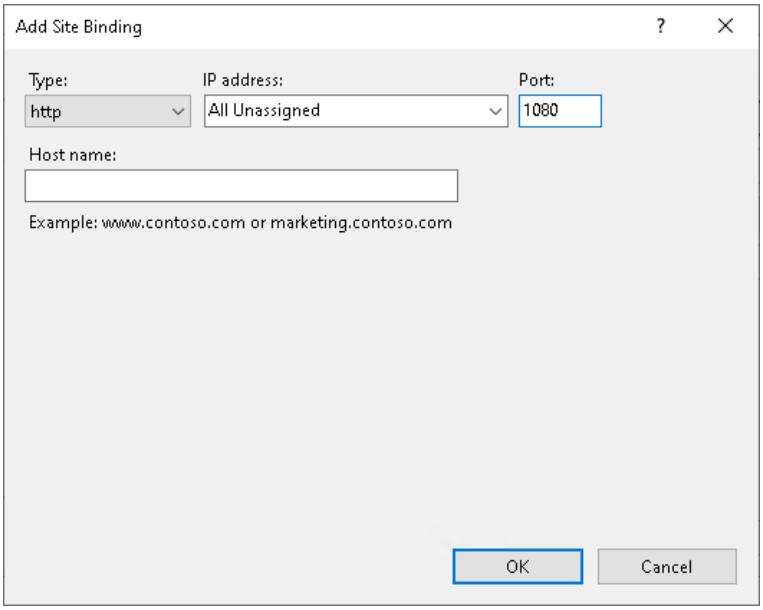


9. Under the **Connections** tree located on the left side of the IIS Manager window click on the **[Default Web Site]** option.
10. Under the **Actions** tree located on the right side of the IIS Manager window click on the **[Bindings...]** button.

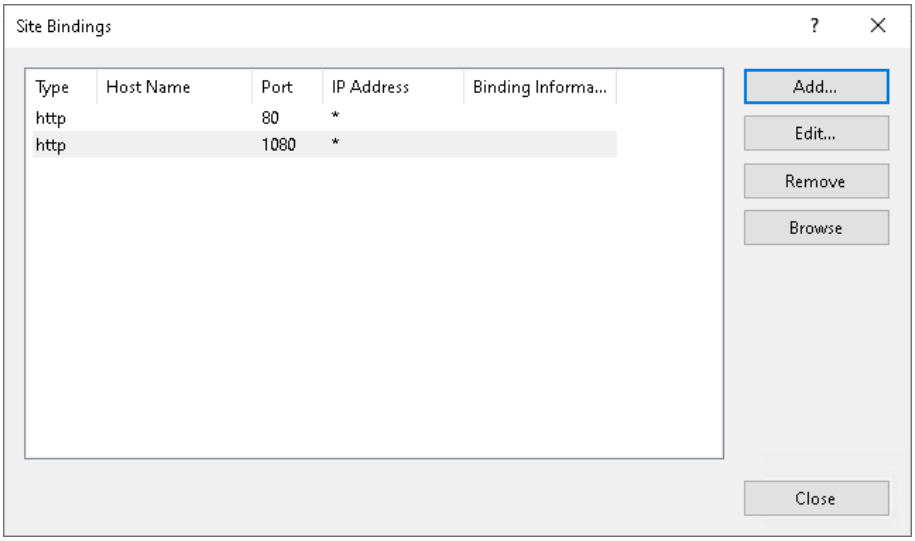


11. In the appearing window click on the **[Add...]** button.

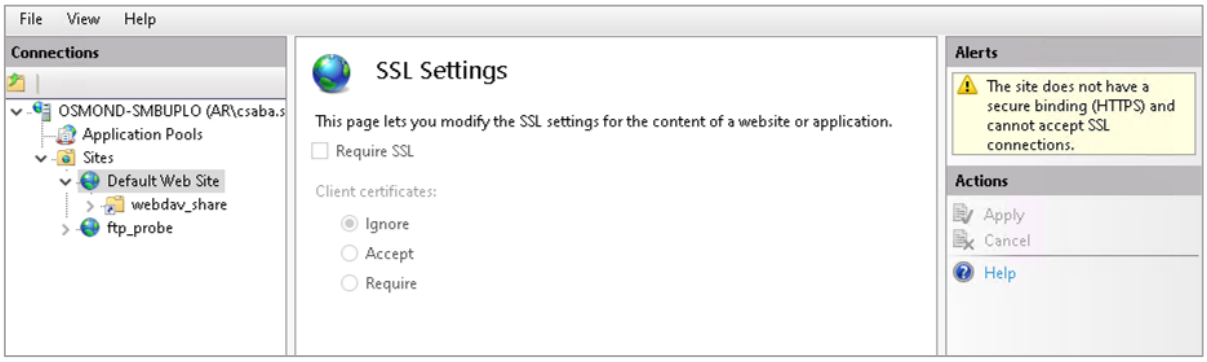
12. In the appearing **Add Site Binding** window select "http" under the **Type** parameter.
13. Under **IP address** keep the default option: "All Unassigned".
14. Enter the value "1080" to the **Port** field.
15. Click on the **[OK]** button.



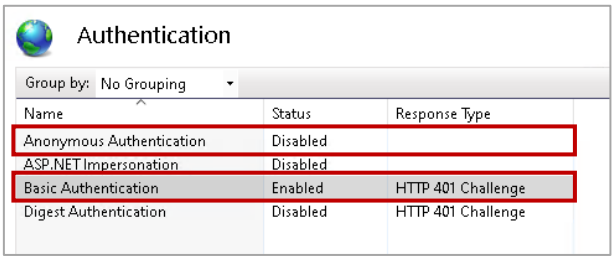
16. In the **Site Bindings** window click on the **[Close]** button.



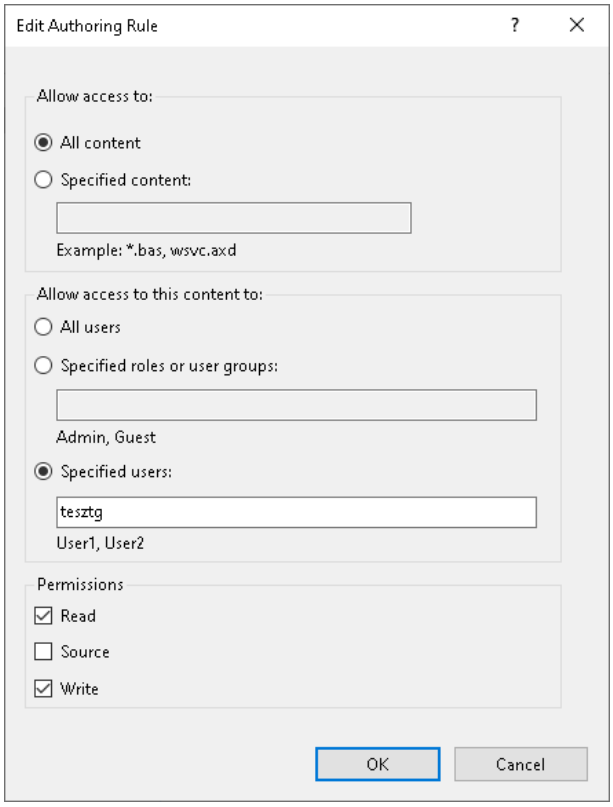
17. Under the **Connections** tree located on the left side of the IIS Manager window click on the **[Default Web Site]** option.
18. Double click on the **[SSL Settings]** icon located in the middle part of the window.
19. In the appearing window the "**Require SSL**" function must be disabled.
20. Under **Client certificates** the "**Ignore**" option must be selected.
21. If the default settings have been modified, click on **[Apply]** under the **Actions** tree.



22. Under the **Connections** tree located on the left side of the IIS Manager window click on the **[Default Web Site]** option.
23. Double click on the **[Authentication]** icon located in the middle part of the window.
24. Select the **Anonymous Authentication** bar and click on the **[Disable]** text located under the **Actions** tree on the right side.
25. Select the **Basic Authentication** bar and click on the **[Enable]** text located under the **Actions** tree on the right side.



26. Under the **Connections** tree located on the left side of the IIS Manager window click on the **[Default Web Site]** option.
27. Double click on the **[WebDAV Authoring Rules]** icon located in the middle part of the window.
28. Under the **Actions** tree located on the right side of the window click on the **[Enable WebDAV]** option.
29. Then, click on **[Add Authoring Rule]**.
30. In the "**Allow access to**" section select the "**All content**" option.
31. In the "**Allow access to this content to**" section:
    - Select the "**Specified users**" option and
    - Enter the "tesztg" username to the text field below.
32. In the "**Permissions**" section select the "**Read**" and the "**Write**" options by ticking their boxes.
33. Click on the **[OK]** button.



34. Under the **Connections** tree located on the left side of the IIS Manager window click on the **[Default Web Site]** option.
35. Double click on the **[Directory Browsing]** icon located in the middle part of the window.
36. Click on the **[Enable]** text located under the **Actions** tree on the right side.
37. Thereafter, the data located in the middle part of the window becomes active. Each value must be selected by ticking their boxes.
38. Then, click on the **[Apply]** button located under the **Actions** tree on the right side.

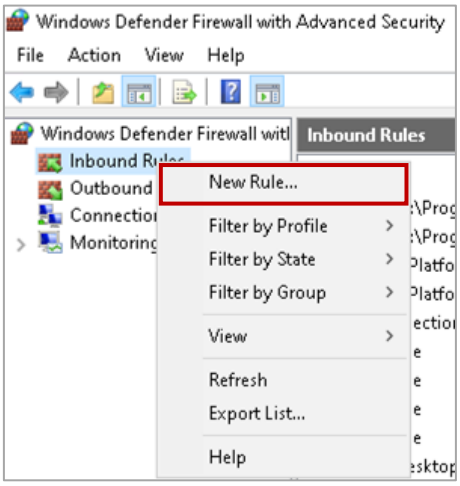
39. Under the **Connections** tree located on the left side of the IIS Manager window click on the **[Default Web Site]** option.
40. Then, under the **Manage Website** tree located on the right side of the IIS Manager window click on the **[Restart]** button.

> **Note**
>
> It is recommended to restart the PC as well.

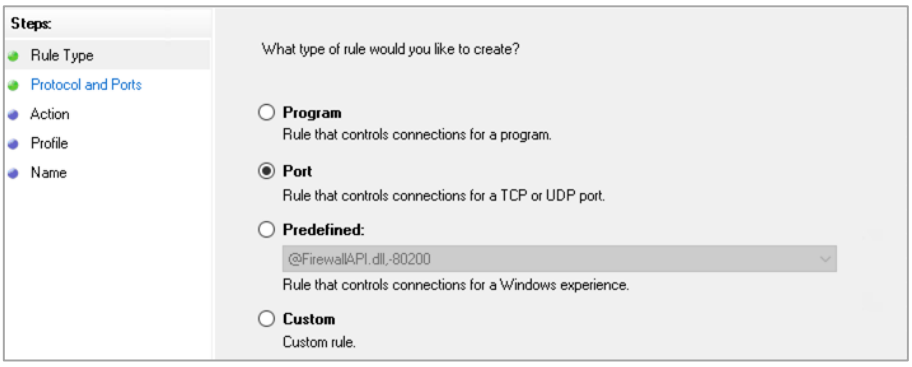
16.1.3. SETTING THE FIREWALL

It is recommended to check the Windows Firewall settings:

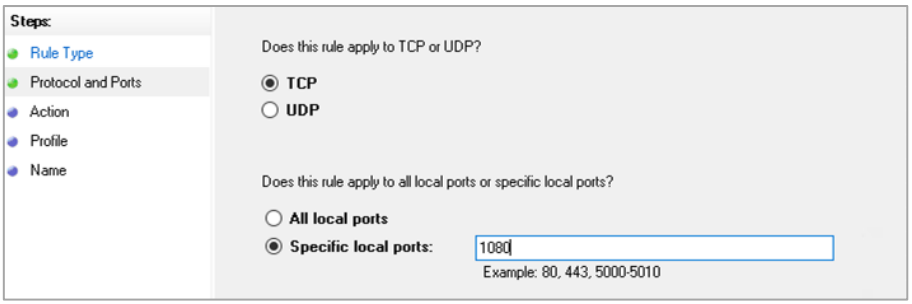
1. Navigate to **Control Panel / System and Security / Windows Defender Firewall / Advanced settings**.
2. Right click on **[Inbound rules]** located in the left section.
3. Select **New Rule...** from the appearing quick menu.



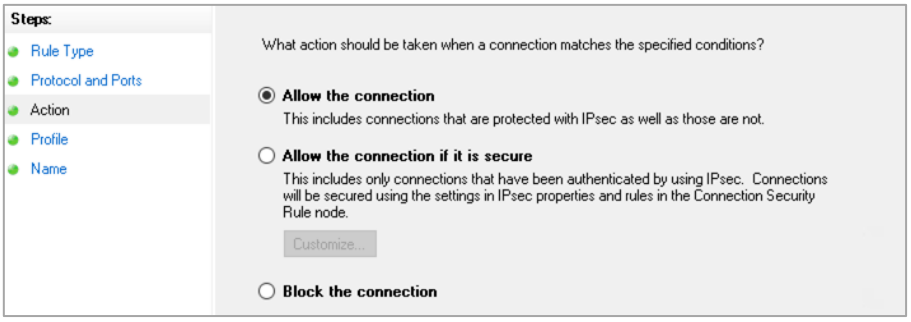
4. In the pop-up window select **Port**.
5. Then, click on the **[Next >]** button.



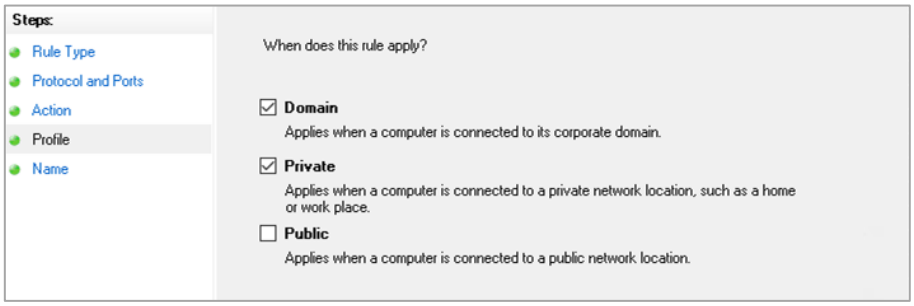
6. At "**Does this rule apply to TCP or UDP?**" select **TCP**.
7. At "**Does this rule apply to all local ports or specific local ports?**" select "**Specific local ports**" and enter the value **1080** to the text field.
8. Then, click on the **[Next >]** button.



9. On the following window select "**Allow the connection**" option and click on the **[Next >]** button.



10. On next window select "**Domain**" and "**Private**" options by ticking their checkboxes.
11. Then, click on the **[Next >]** button.



12. On the following window type "WebDav" to the "**Name:**" text field.
13. Then, click on the **[Finish]** button.

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

16.2. INSTALLING AND SETTING THE WEBDAV SERVER ON LINUX

16.2.1. INSTALLING THE WEBDAV SERVER

On Linux the WebDAV protocol is provided by the Apache2 server. Under Linux install and set up the Apache2 server from command line. The commands may depend on the distribution.
The following commands apply to Ubuntu 22.04.

16.2.2. INSTALLING THE APACHE WEBSERVER

1. Update Ubuntu:
   ```
   sudo apt update
   sudo apt upgrade -y
   ```

2. Install the Apache webserver:
   ```
   sudo apt-get install apache2 -y
   ```

3. Then, start the Apache webserver:
   ```
   sudo systemctl start apache2
   ```

4. Enable the Apache server to start automatically on every startup:
   ```
   sudo systemctl enable apache2
   ```

5. The status of the webserver can be checked with the following command:
   ```
   sudo systemctl status apache2
   ```

   If the returned message is "Active: active (running)", then the server is running. For example:
   Active: **active (running)** since Thu 2022-11-03 18:51:07 CET; 5min ago

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

16.2.3. SETTING THE APACHE WEBSERVER

1. Create the WebDav library:

```
sudo mkdir /home/tesztg/webdav
sudo chown -R www-data:www-data /home/tesztg/webdav
```

2. Then, create a library for the WebDav database:

```
sudo mkdir -p /usr/local/apache/var/
sudo chown www-data:www-data /usr/local/apache/var
```

3. Modify the Apache configuration file. Any text editor can be used for the modification except for nano.

```
sudo nano /etc/apache2/sites-available/webdav.conf
DavLockDB /usr/local/apache/var/DavLock

<VirtualHost *:1080>
        ServerAdmin webmaster@localhost
        DocumentRoot /home/tesztg/webdav

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        Alias /webdav_share /home/tesztg/webdav
        <Directory /home/tesztg/webdav>
                DAV On
                Options Indexes MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
                DirectoryIndex disabled
                AuthType Digest
                AuthName "webdav"
                AuthUserFile /usr/local/apache/var/users.password
                Require valid-user
        </Directory>
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

4. Enable WebDav:

```
sudo ln -s /etc/apache2/sites-available/webdav.conf
/etc/apache2/sites-enabled/webdav.conf
```

5. Enable the WebDav modules:
   ```
   sudo a2enmod dav
   sudo a2enmod dav_fs
   ```

6. Set the global server name.
   If it has a name (e.g., webdav.example.com), enter it. In other case enter the localhost. After the line `# Global configuration` type the following to the `/etc/apache2/apache2.conf` file:
   ```
   ServerName localhost
   ```

7. The Apache server must be listening through the port 1080 as well. In order to set this:
   Below the line **Listen 80** enter the following to the `/etc/apache2/ports.conf` file:
   ```
   Listen 1080
   ```

8. Create a file which will store the WebDav users and their passwords:
   ```
   sudo touch /usr/local/apache/var/users.password
   ```

9. Then, set the rights. Apache must be able to read and write this file.
   ```
   sudo chown www-data:www-data /usr/local/apache/var/users.password
   ```

10. Add the tesztg user to WebDav:
    ```
    sudo htdigest /usr/local/apache/var/users.password webdav tesztg
    ```
    - Set the password as well.

11. Enable the auth_digest module:
    ```
    sudo a2enmod auth_digest
    ```

12. Restart the Apache server (this will check the configuration files too.):
    ```
    sudo apachectl configtest && service apache2 restart
    ```

16.2.4. SETTING THE FIREWALL

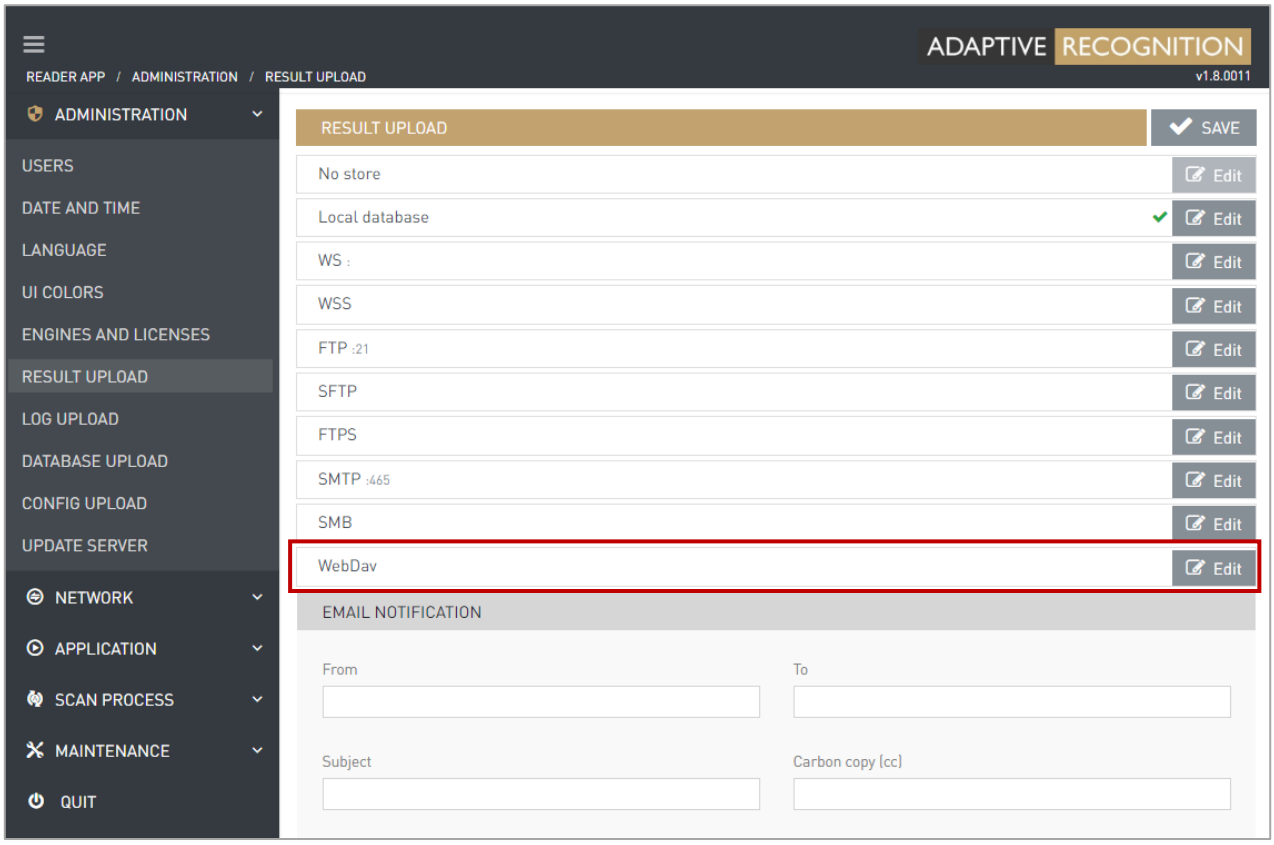
The ports used by WebDav must be set in the firewall, then restart it, if the firewall is active. On Ubuntu the `ufw` is the default firewall. Its state can be queried with the `sudo ufw status` command.
If it is active, then:

- `sudo ufw allow 1080/tcp`
- `sudo ufw disable`
- `sudo ufw enable`

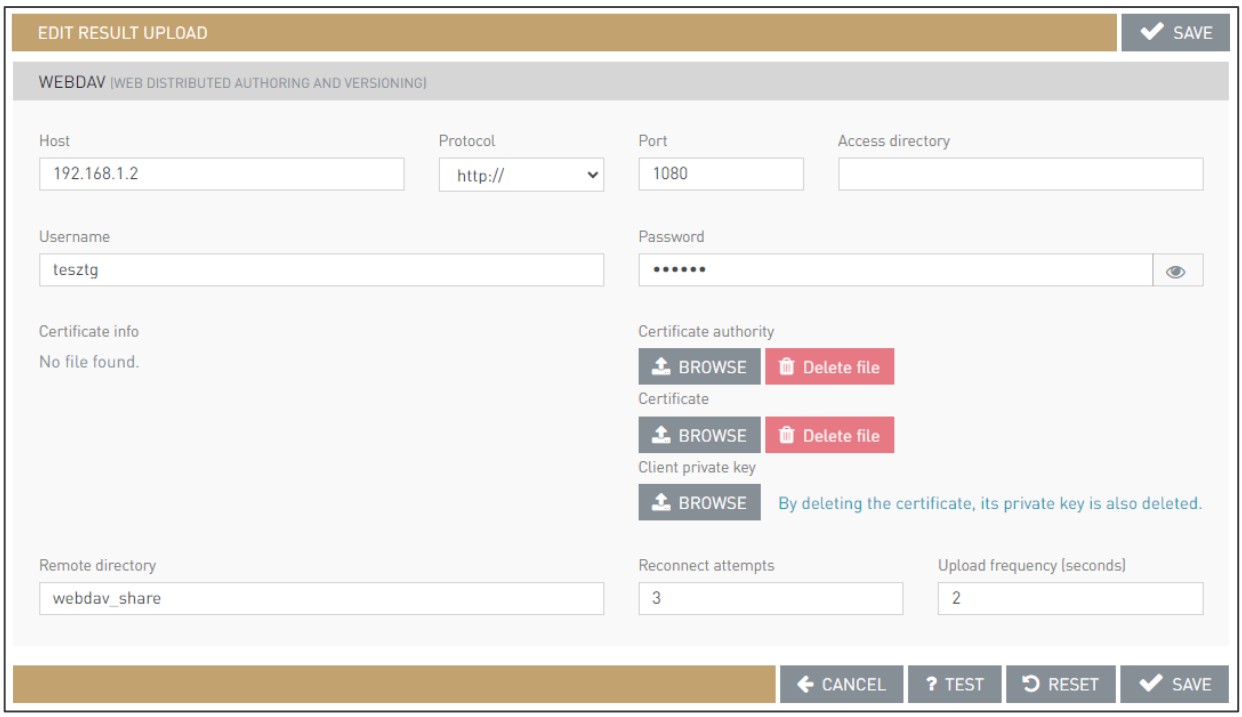
16.3. SETTING ON OSMOND

First, the parameters of the WebDav protocol must be set on the web interface of the Osmond device. By default, the web interface is accessible on 192.0.2.3:3000, but it can be set to another address as well. The IP address of the Osmond in the example is 192.168.6.244:3000.

1. After signing in to the web interface, click on the **Main menu** (the three horizontal stripes; at the top left corner of the webpage) in order to open the menu items.
2. Navigate to **ADMINISTRATION / RESULT UPLOAD**.
3. Click on the **[Edit]** button belonging to **WebDav** protocol.



4. On the appearing menu set the following:
   - **Host**: IP address of the WebDav server, in this case: 192.168.1.2
   - **Protocol**: http://
   - **Port**: Port of the WebDav server: 1080
   - **Access directory**: This field must be blank.
   - **Username**: Name of the user, in this case: tesztg
   - **Password**: Password of the user, in this case: 123456
   - **Remote directory**: Name of the folder accessible from the server's root directory, in this case: webdav_share
   - **Reconnect attempts**: The maximum number of the connections without error message, in this case: 3
   - **Upload frequency (seconds)**: The upload daemon checks if there is data to upload at specified intervals, in this case: 2

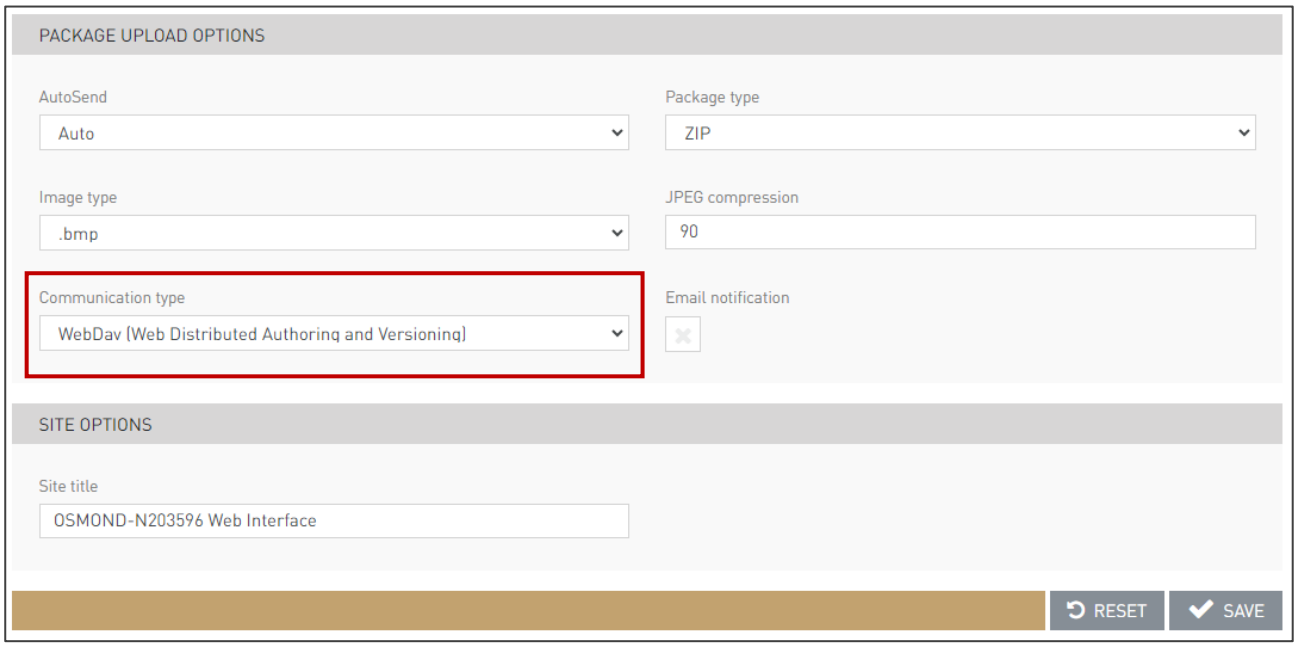


5. Check the correct settings are applied by clicking on the **[TEST]** button.
   Every test result must be passed (green).

6. If the test is passed, click on the **[SAVE]** button.

7. Then, navigate to **SCAN PROCESS / MAIN CONFIGURATION**. In this menu item, under **PACKAGE UPLOAD OPTIONS / Communication type** select **WebDav (Web Distributed Authoring and Versioning)** protocol.

8. Then, click on the **[SAVE]** button.



After performing these settings, the scanned documents are transferred to the upload server as a zip file.

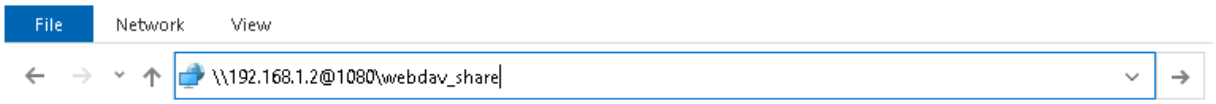
16.4. TESTING THE SETUP

16.4.1. WINDOWS

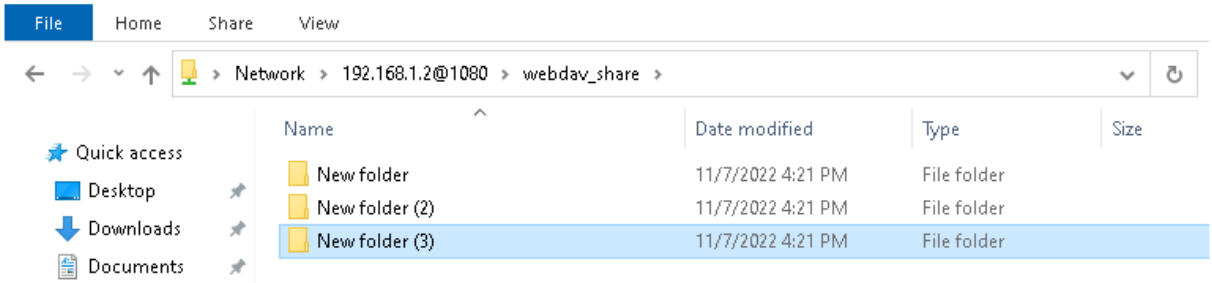
Check the WebDav server is running or is accessible by using the File Explorer.

1. Enter the address of the WebDav server to the address bar of the File Explorer:

   \\192.168.1.2@1080\webdav_share



2. Then, press **[Enter]**.
3. After successful connection, Windows requests the username and password.
4. Then, the content of the WebDav directory appears, and can be browsed as a file system.



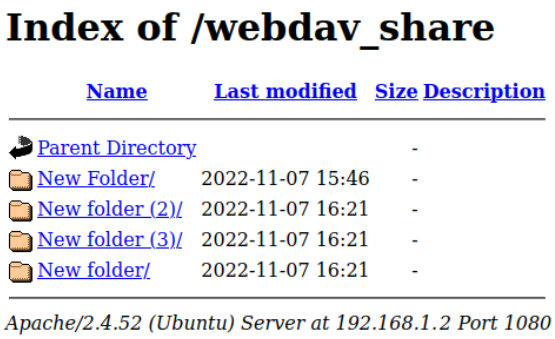
16.4.2. LINUX

On Linux the Firefox browser can be used to sign in.

1. Enter the address of the WebDav server to the address bar of Firefox:

   192.168.1.2:1080/webdav_share/

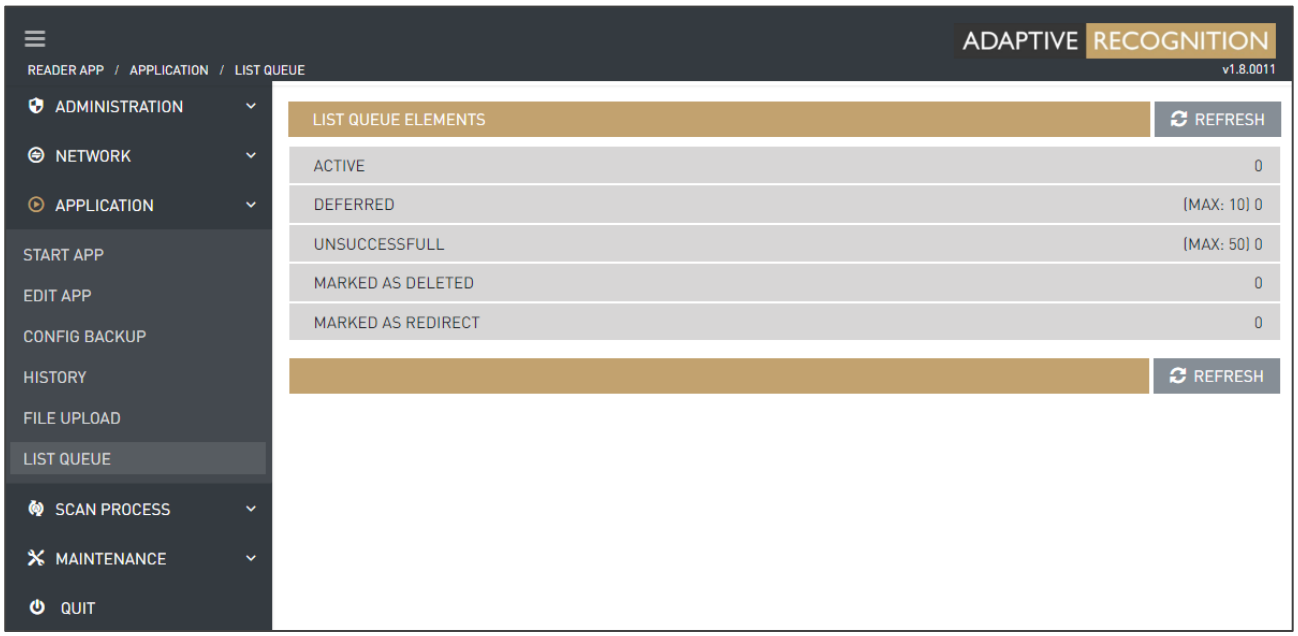
2. Then, press **[Enter]**.
3. After successful connection, enter the username and password.
4. Then, the page appears:



16.5. TROUBLESHOOTING

16.5.1. OSMOND

If upload is not working, Osmond will collect the unsuccessful documents to the **UNSUCCESSFUL queue** until its limit is not reached. When **UNSUCCESFUL** limit is reached, the oldest element in queue is overwritten by the result of the latest scan. Documents in unsuccessful status can be checked in the **APPLICATION / LIST QUEUE** menu. In case of correct operation this row is empty.



Note

If upload is not working, then the WebDav server firewall (Windows or Linux) or another network device may be blocking it.

16.5.2. LINUX

On Linux the WebDav protocol is provided by the Apache2. Its operation can be affected with the following commands:

- Check the configuration of Apache2:
  ```
  apachectl configtest
  ```
- Start the Apache2:
  ```
  sudo systemctl start apache2
  ```
- Restart the Apache2:
  ```
  sudo systemctl restart apache2
  ```
- Stop the Apache2:
  ```
  sudo systemctl stop apache2
  ```
- Enable the Apache2 to start automatically on startup (if it is not set, then it is recommended):
  ```
  sudo systemctl enable apache2
  ```
- Disable the Apache2 to not start automatically on startup:
  ```
  sudo systemctl disable apache2
  ```
- Query the status of the Apache2:
  ```
  sudo systemctl status apache2
  ```


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

17. SETTING THE WEBDAV SECURE PROTOCOL ON OSMOND

The current version (1.8) of the Osmond firmware is capable of uploading the scanned data to a server via multiple protocols.
In this section the settings of the WebDav secure protocol will be explained.

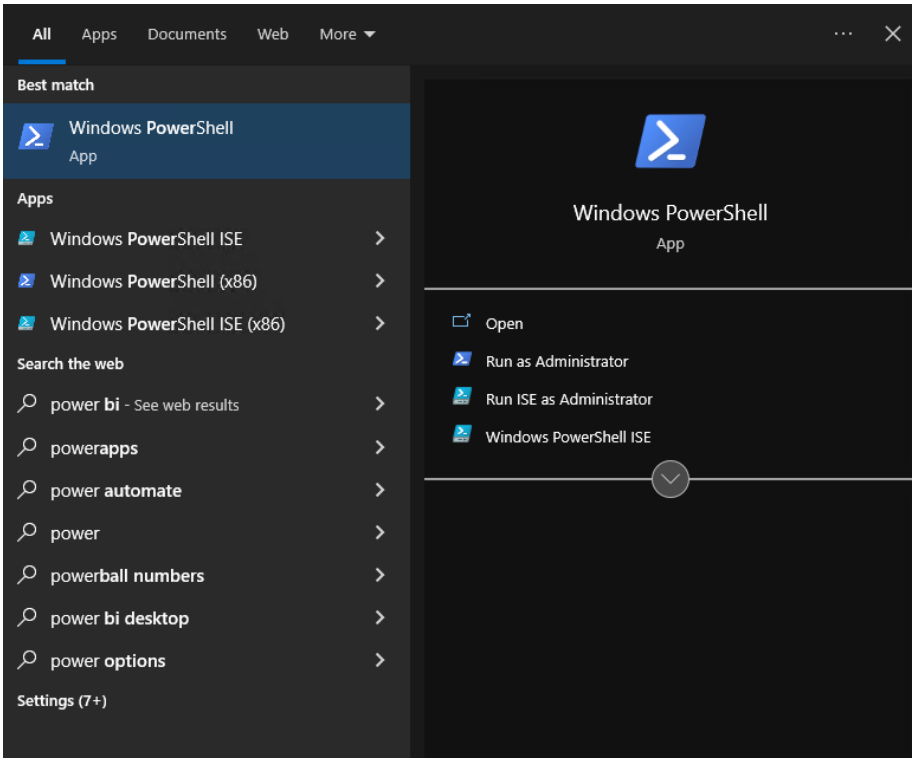
The parameters are the following:

- IP address of the WebDav server: 192.168.1.2
- Fully qualified domain name (FQDN) of the WebDav server: tesztg.example.hu
- IP address of the Osmond device: 192.168.6.244
- The user (registered Windows user with password): tesztg
- The password of the user: 123456
- The shared folder on Windows (upload path): C:\webdav_secure_share
- The shared directory on Linux: /var/www/webdav_secure_share

17.1. INSTALLING AND SETTING THE WEBDAV SERVER ON WINDOWS 10

17.1.1. INSTALLING THE WEBDAV SERVER

1. Open a PowerShell terminal with administrator rights:
   - Open Start menu.
   - Enter "powershell".
   - Select the appearing **Windows PowerShell** application and click on the "**Run as Administrator**" option displayed on the right. (If the "**Run as Administrator**" text does not appear, then right click on the Windows PowerShell application and select "**Run as Administrator**".)



2. Create a library which will receive the uploads:

```
mkdir c:\webdav_secure_share
```

3. Copy the following command to the terminal, and press **[Enter]**:

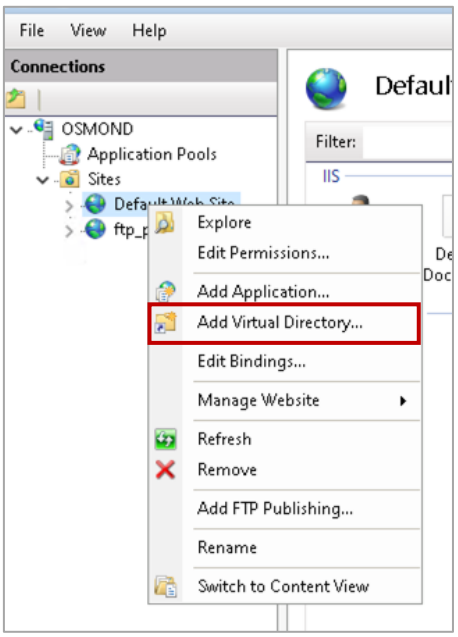
```
$feats = @("IIS-WebServerRole","IIS-WebServer","IIS-CommonHttpFeatures","IIS-HttpErrors","IIS-Security","IIS-RequestFiltering","IIS-WebServerManagementTools","IIS-DigestAuthentication","IIS-StaticContent","IIS-DefaultDocument","IIS-DirectoryBrowsing","IIS-WebDAV","IIS-BasicAuthentication","IIS-ManagementConsole");foreach ($feat in $feats) {Enable-WindowsOptionalFeature -Online -FeatureName $feat};& "$env:windir\system32\inetsrv\InetMgr.exe";
```

   – This command installs the Internet Information Services (IIS) modules which are required for the installation and setup of WebDav.

   – Starts the IIS Manager.

17.1.2. SETTING THE WEBDAV SERVER

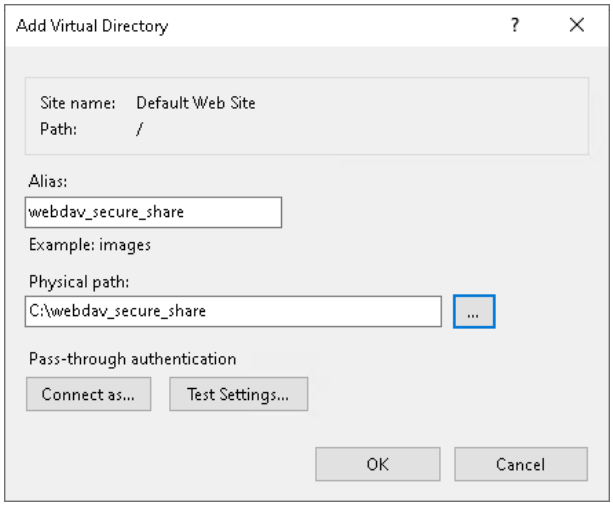
1. After running the command, the ISS Manager (Internet Information Services (IIS) Manager) opens.
2. Under **Connections** (located on the left) click on the arrow next to the computer name to unfold additional items.
3. Then, click on the arrow next to the **Sites** to unfold its submenu.
4. In the appearing menu right click on the "**Default Web Site**" option.
5. In the appearing quick menu select the "**Add Virtual Directory...**" menu item.



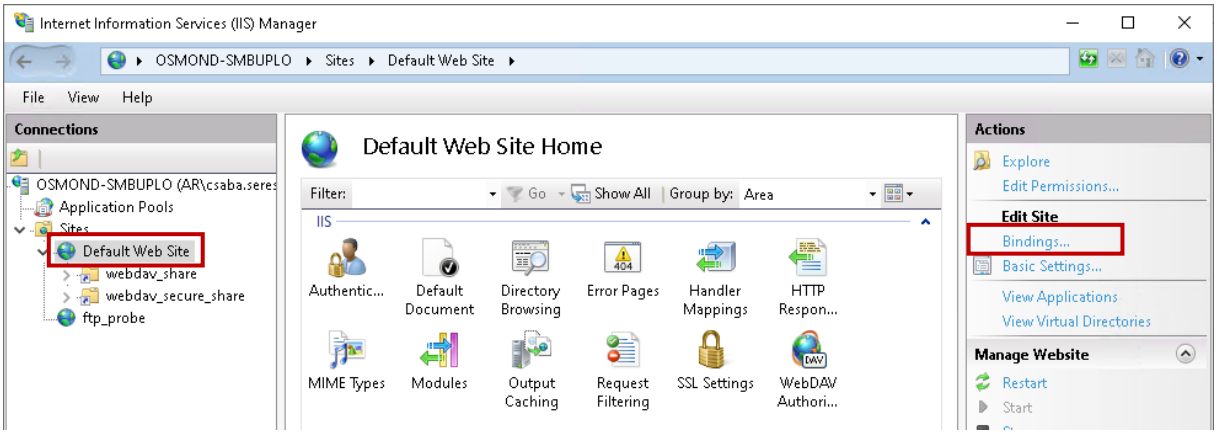
6. Type "webdav_secure_share" to the **Alias** field.
7. Enter the name of the shared folder (or browse it by clicking on the **[...]** button) to the **Physical path** field:

   c:\webdav_secure_share

8. Click on the **[OK]** button.

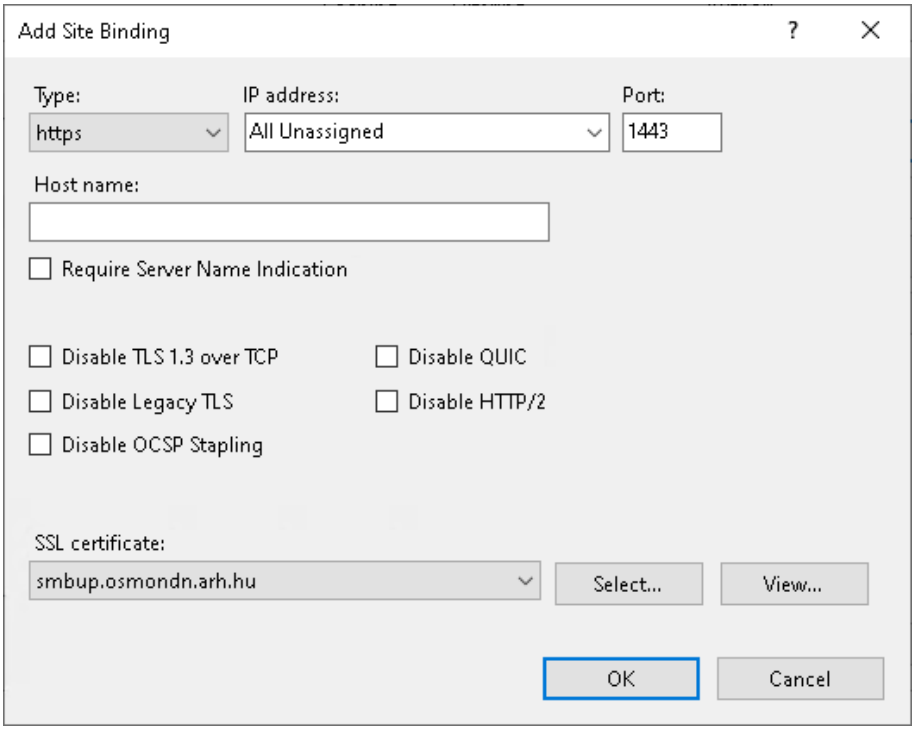


9. Under the **Connections** tree located on the left side of the IIS Manager window click on the **[Default Web Site]** option.
10. Under the **Actions** tree located on the right side of the IIS Manager window click on the **[Bindings...]** button.

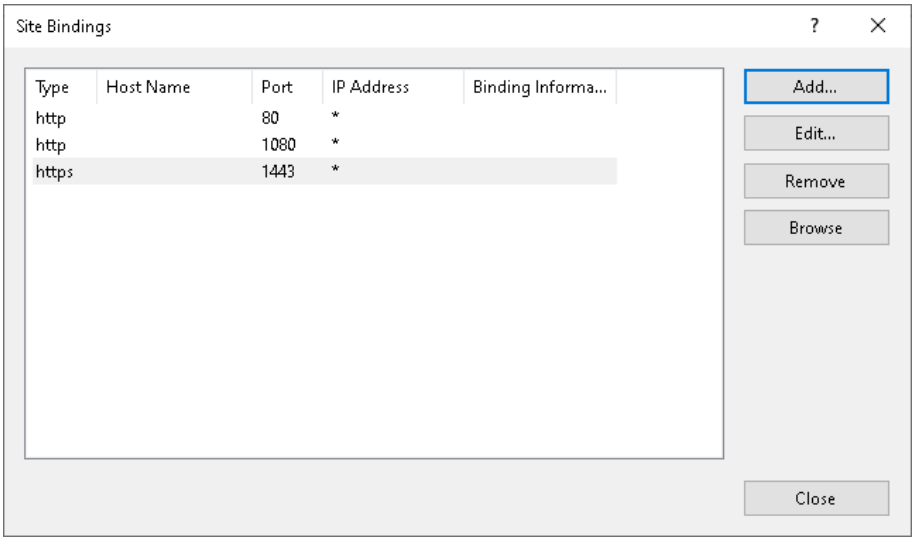


11. In the appearing window click on the **[Add...]** button.

12. In the appearing **Add Site Binding** window select "https" under the **Type** parameter.
13. Under **IP address** keep the default option: "All Unassigned".
14. Enter the value "1443" to the **Port** field.
15. Under **SSL certificate** select your own SSL certificate. (Self-signed certificates are not appropriate because Osmond will not accept them.)
16. Click on the **[OK]** button.

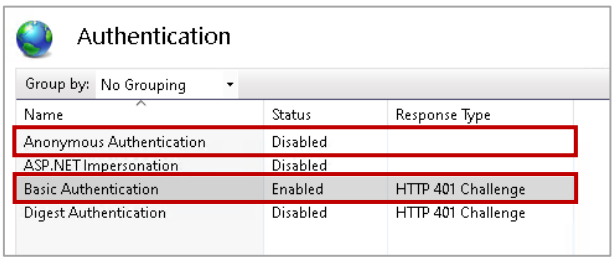


17. In the **Site Bindings** window click on the **[Close]** button.

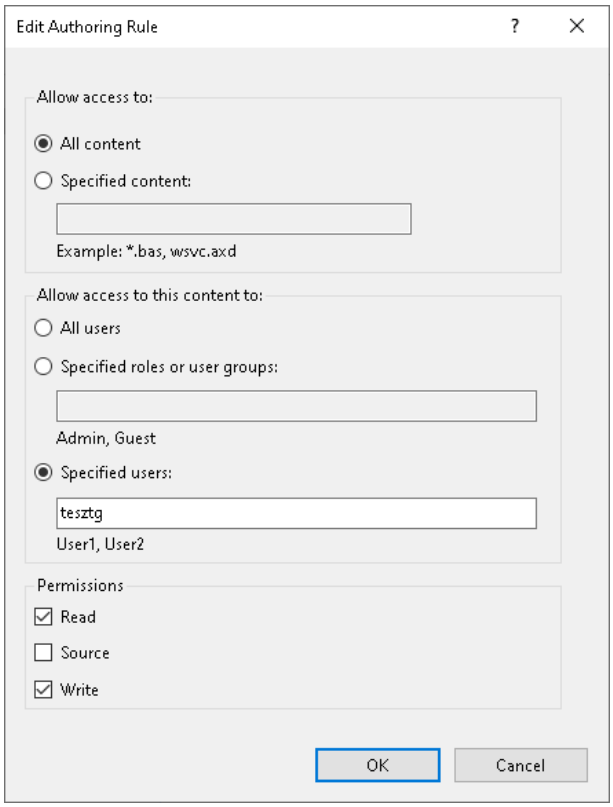


18. Under the **Connections** tree located on the left side of the IIS Manager window click on the **[Default Web Site]** option.
19. Double click on the **[SSL Settings]** icon located in the middle part of the window.
20. In the appearing window the "**Require SSL**" function must be enabled.
21. Under **Client certificates** select the "**Ignore**" option.
22. If the default settings have been modified, click on **[Apply]** under the **Actions** tree.

23. Under the **Connections** tree located on the left side of the IIS Manager window click on the **[Default Web Site]** option.
24. Double click on the **[Authentication]** icon located in the middle part of the window.
25. Select the **Anonymous Authentication** bar and click on the **[Disable]** text located under the **Actions** tree on the right side.
26. Select the **Basic Authentication** bar and click on the **[Enable]** text located under the **Actions** tree on the right side.



27. Under the **Connections** tree located on the left side of the IIS Manager window click on the **[Default Web Site]** option.
28. Double click on the **[WebDAV Authoring Rules]** icon located in the middle part of the window.
29. Under the **Actions** tree located on the right side of the window click on the **[Enable WebDAV]** option.
30. Then, click on **[Add Authoring Rule]**.
31. In the "**Allow access to**" section select the "**All content**" option.
32. In the "**Allow access to this content to**" section:
    - Select the "**Specified users**" option and
    - Enter the "tesztg" username to the text field below.
33. In the "**Permissions**" section select the "**Read**" and the "**Write**" options by ticking their boxes.
34. Click on the **[OK]** button.

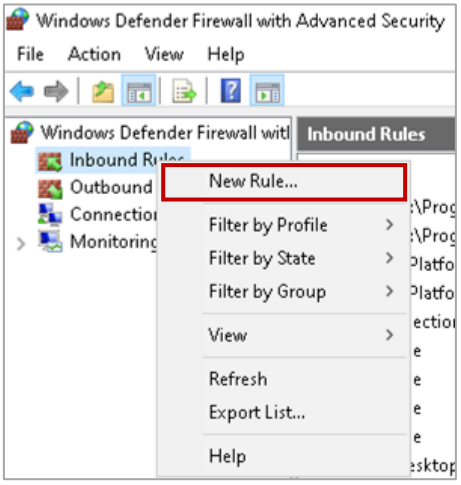


35. Under the **Connections** tree located on the left side of the IIS Manager window click on the **[Default Web Site]** option.
36. Then, under the **Manage Website** tree located on the right side of the IIS Manager window click on the **[Restart]** button.

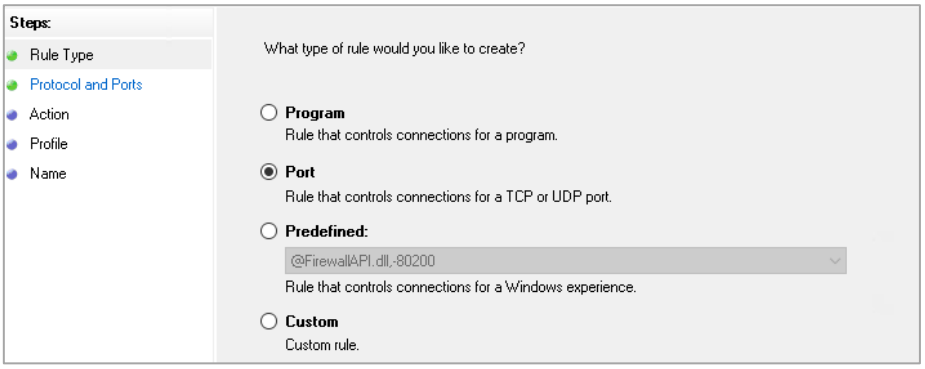
17.1.3. SETTING THE FIREWALL

It is recommended to check the Windows Firewall settings:

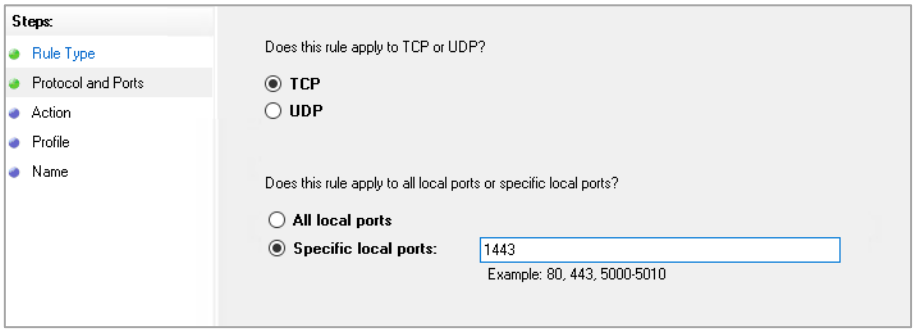
1. Navigate to **Control Panel / System and Security / Windows Defender Firewall / Advanced settings**.
2. Right click on **[Inbound rules]** located in the left section.
3. Select **New Rule...** from the appearing quick menu.



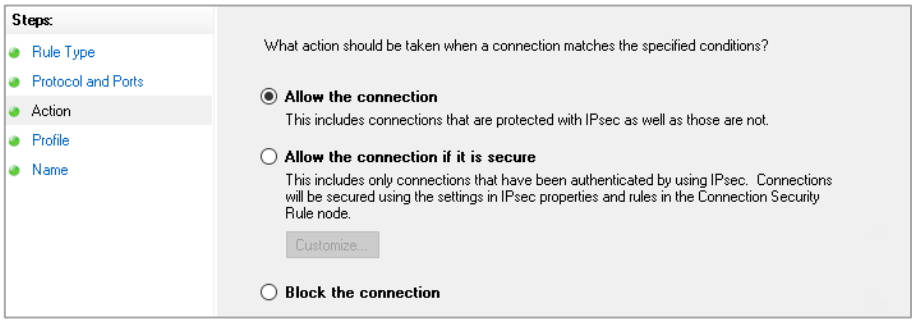
4. In the pop-up window select **Port**.
5. Then, click on the **[Next >]** button.



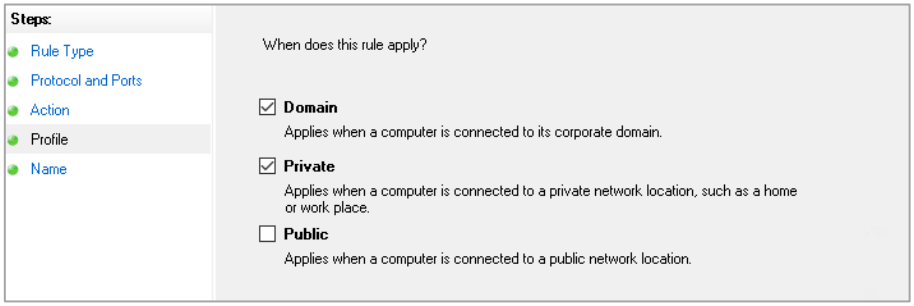
6. At "**Does this rule apply to TCP or UDP?**" select **TCP**.
7. At "**Does this rule apply to all local ports or specific local ports?**" select "**Specific local ports**" and enter the value **1443** to the text field.
8. Then, click on the **[Next >]** button.



9. On the following window select "**Allow the connection**" option and click on the **[Next >]** button.



10. On next window select "**Domain**" and "**Private**" options by ticking their checkboxes.
11. Then, click on the **[Next >]** button.



12. On the following window type "WebDavSecure" to the "**Name:**" text field.
13. Then, click on the **[Finish]** button.

17.2. INSTALLING AND SETTING THE WEBDAV SERVER ON LINUX

17.2.1. INSTALLING THE WEBDAV SERVER

On Linux the WebDAV protocol is provided by the Apache2 server. Under Linux install and set up the Apache2 server from command line. The commands may depend on the distribution.
The following commands apply to Ubuntu 22.04.

17.2.2. INSTALLING THE APACHE WEBSERVER

1. Update Ubuntu:
   ```
   sudo apt update
   sudo apt upgrade -y
   ```

2. Reboot the server if update has been performed.
   ```
   sudo reboot
   ```

3. Install the Apache webserver:
   ```
   sudo apt-get install apache2 -y
   ```

4. Then, start the Apache webserver:
   ```
   sudo systemctl start apache2
   ```

5. Enable the Apache server to start automatically on every startup:
   ```
   sudo systemctl enable apache2
   ```

6. The status of the webserver can be checked with the following command:
   ```
   sudo systemctl status apache2
   ```

   If the returned message is "Active: active (running)", then the server is running. For example:
   Active: **active (running)** since Thu 2022-11-03 18:51:07 CET; 5min ago

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

17.2.3. SETTING THE APACHE WEBSERVER

1. The hostname must be set to the hostname located in the fully qualified domain name (FQDN). In the example the FQDN is "tesztg.example.hu", where the hostname is "tesztg". To set this, the following command can be used:

```
sudo hostname tesztg
```

2. Then, set the fully qualified domain name (FQDN):

```
sudo hostnamectl set-hostname tesztg.example.hu
```

3. Check the performed setting is correct by entering the following command:

```
sudo hostnamectl
```

4. Create the WebDav library:

```
sudo mkdir /var/www/webdav_secure_share
sudo chown -R www-data:www-data /var/www/webdav_secure_share
```

5. Then, create a library for the WebDav database:

```
sudo mkdir -p /usr/local/apache/var/
sudo chown www-data:www-data /usr/local/apache/var
```

6. Create the WebDav configuration file. Any text editor can be used except for nano.

```
sudo nano /etc/apache2/sites-available/webdav_secure.conf
```

```
DavLockDB /usr/local/apache/var/DavLock

<IfModule mod_ssl.c>
<VirtualHost *:1443>
 ServerAdmin webmaster@localhost
 DocumentRoot /var/www/webdav_secure_share

 ErrorLog ${APACHE_LOG_DIR}/error.log
 CustomLog ${APACHE_LOG_DIR}/access.log combined

 Alias /webdav_secure_share /var/www/webdav_secure_share
 SSLEngine on
 SSLCertificateFile /etc/ssl/certs/cert1.crt
 SSLCertificateChainFile /etc/ssl/certs/intermediate.pem
 SSLCertificateKeyFile /etc/ssl/private/privkey1.pem
        <Directory /var/www/webdav_secure_share>
                DAV On
                Options Indexes MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
                DirectoryIndex disabled
                AuthType Basic
                AuthName "webdav"
                AuthUserFile /usr/local/apache/var/users.password
                Require valid-user
        </Directory>
</VirtualHost>
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

7. In the configuration file above, the line:

   `SSLCertificateChainFile /etc/ssl/certs/intermediate.pem`

   is only needed when there is a file containing intermediate certificate.

8. Enable WebDav:

```
sudo a2ensite webdav_secure
```

9. Enable the WebDav modules:

```
sudo a2enmod dav
sudo a2enmod dav_fs
sudo a2enmod ssl
sudo a2ensite default-ssl
sudo a2enmod auth_digest
```

10. Set the global server name.

    If it has a name (e.g., webdav.example.com), enter it. In other case enter the localhost. After the line `# Global configuration` type the following to the `/etc/apache2/apache2.conf` file:

    `ServerName` tesztg.osmondn.arh.hu

11. The Apache server must be listening through the port 1443 as well. In order to set this: complete the sections **IfModule ssl_module** and **IfModule mod_gnutls.c** of the `/etc/apache2/ports.conf` file with the following line:

    `Listen 1443`

    The complete `ports.conf` file:

```
Listen 80

<IfModule ssl_module>
        Listen 443
        Listen 1443
</IfModule>

<IfModule mod_gnutls.c>
        Listen 443
        Listen 1443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

12. Create a file which will store the WebDav users and their passwords:

```
sudo touch /usr/local/apache/var/users.password
```

13. Then, set the rights. Apache must be able to read and write this file.

```
sudo chown www-data:www-data /usr/local/apache/var/users.password
```

14. Add the tesztg user to WebDav:

```
sudo htpasswd -c /usr/local/apache/var/users.password tesztg
```

    - The `-c` parameter is only required for adding the first user. When adding other users:

```
sudo htpasswd /usr/local/apache/var/users.password tesztg
```

15. Enable the auth_digest module:

```
sudo a2enmod auth_digest
```

16. Restart the Apache server (this will check the configuration files too.):

```
sudo apachectl configtest && service apache2 restart
```

17.2.4. SETTING THE FIREWALL

The ports used by WebDav must be set in the firewall, then restart it, if the firewall is active. On Ubuntu the `ufw` is the default firewall. Its state can be queried with the `sudo ufw status` command.
If it is active, then:

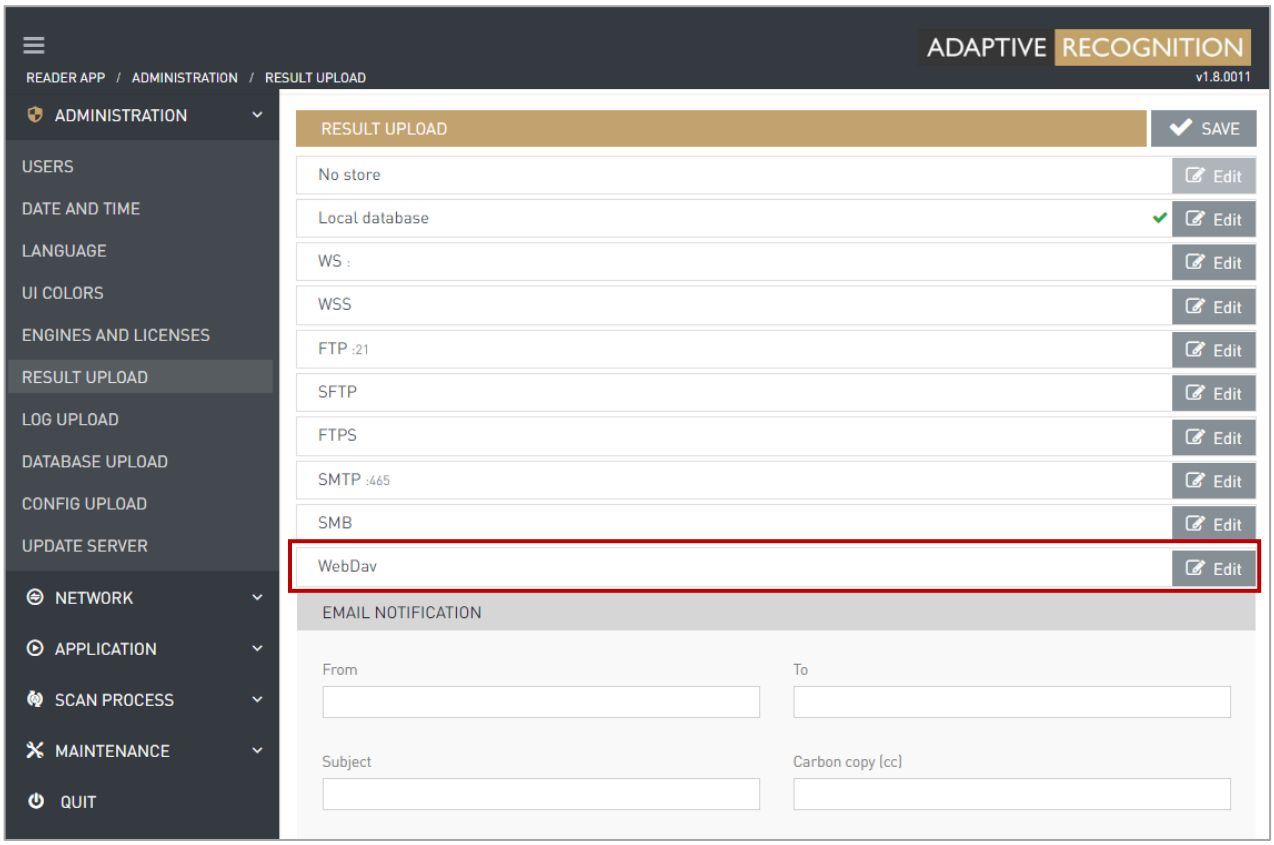
- `sudo ufw allow 1443/tcp`
- `sudo ufw disable`
- `sudo ufw enable`

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

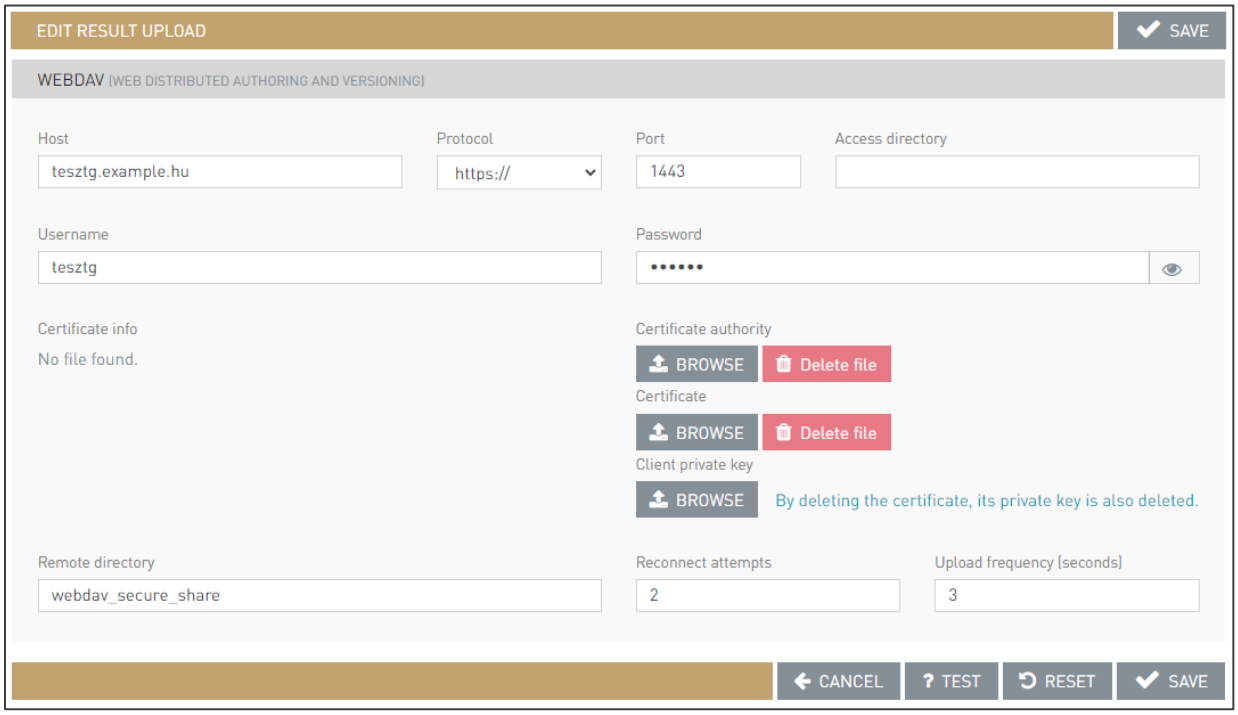
17.3. SETTING ON OSMOND

First, the parameters of the WebDav protocol must be set on the web interface of the Osmond device. By default, the web interface is accessible on 192.0.2.3:3000, but it can be set to another address as well. The IP address of the Osmond in the example is 192.168.6.244:3000.

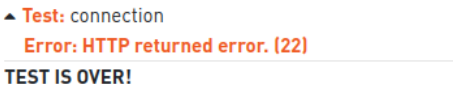
1. After signing in to the web interface, click on the **Main menu** (the three horizontal stripes; at the top left corner of the webpage) in order to open the menu items.
2. Navigate to **ADMINISTRATION / RESULT UPLOAD**.
3. Click on the **[Edit]** button belonging to **WebDav** protocol.



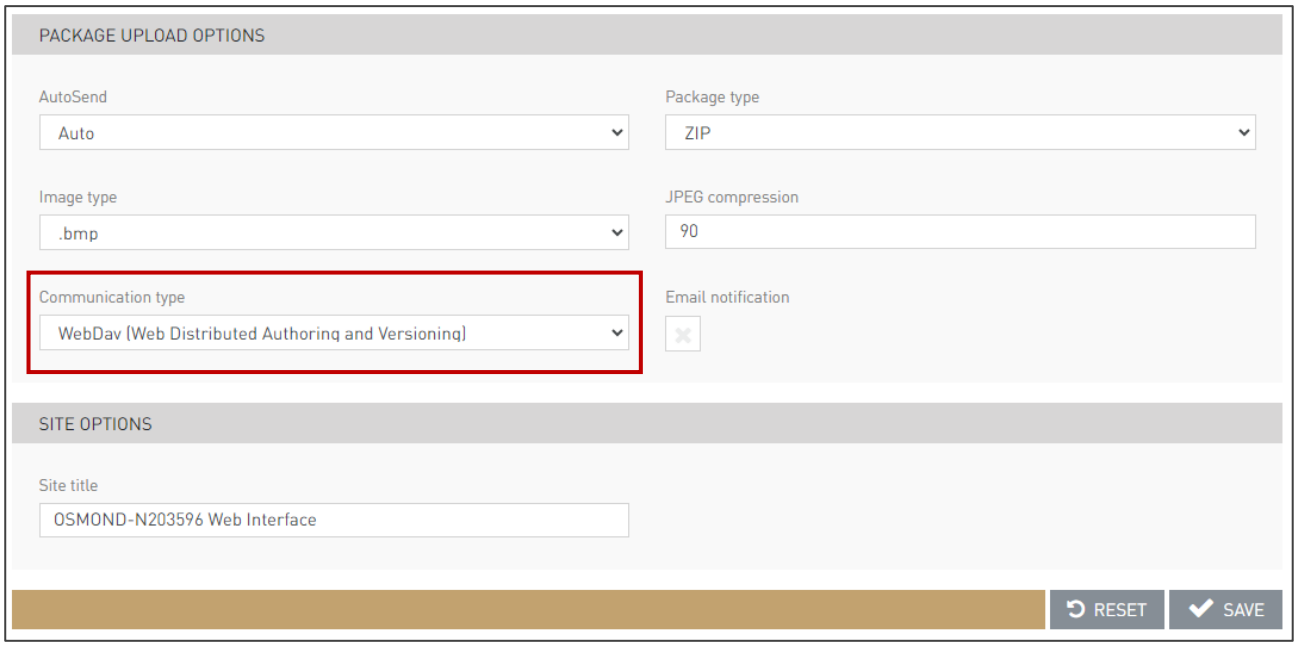
4. On the appearing menu set the following:
   - **Host**: IP address of the WebDav server or the fully qualified domain name (FQDN), depending on which one the certificate was issued for. In this case the certificate is issued for the FQDN, therefore: tesztg.example.hu
   - **Protocol**: https://
   - **Port**: Port of the WebDav server: 1433
   - **Access directory**: This field must be blank.
   - **Username**: Name of the user, in this case: tesztg
   - **Password**: Password of the user, in this case: 123456
   - **Remote directory**: Name of the folder accessible from the server's root directory, in this case: webdav_secure_share
   - **Reconnect attempts**: The maximum number of the connections without error message, in this case: 2
   - **Upload frequency (seconds)**: The upload daemon checks if there is data to upload at specified intervals, in this case: 3



5. Check the correct settings are applied by clicking on the **[TEST]** button.
   The last test step usually fails, even if the settings are correct. This error (22) message can be ignored.



6. If the test is passed, click on the **[SAVE]** button.
7. Then, navigate to **SCAN PROCESS / MAIN CONFIGURATION**. In this menu item, under **PACKAGE UPLOAD OPTIONS / Communication type** select **WebDav (Web Distributed Authoring and Versioning)** protocol.
8. Then, click on the **[SAVE]** button.



After performing these settings, the scanned documents are transferred to the upload server as a zip file.

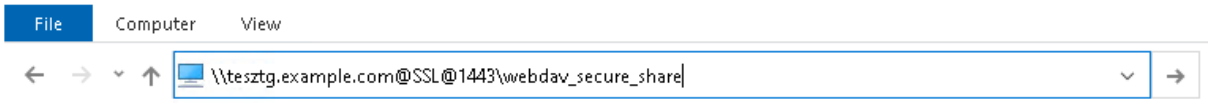
17.4. TESTING THE SETUP

17.4.1. WINDOWS

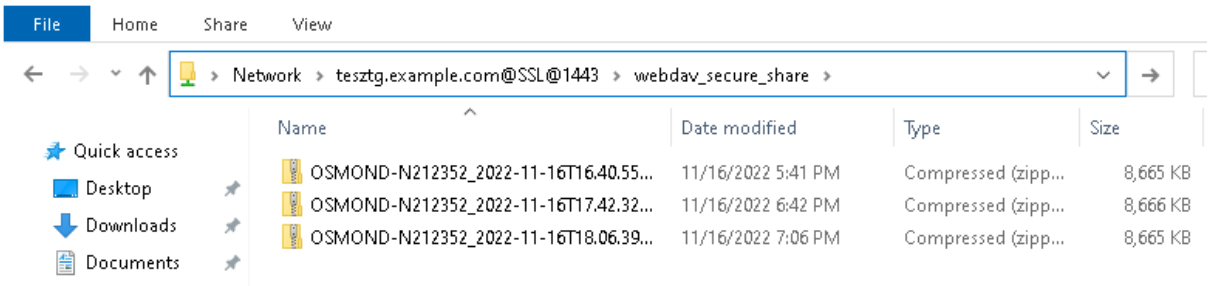
Check the WebDav server is running and is accessible by using the File Explorer.

1. Enter the address of the WebDav server (in this case: FQDN) to the address bar of the File Explorer:

   \\tesztg.example.com@SSL@1443\webdav_secure_share



2. Then, press **[Enter]**.
3. After successful connection, Windows requests the username and password.
4. Then, the content of the WebDav directory appears, and can be browsed as a file system.

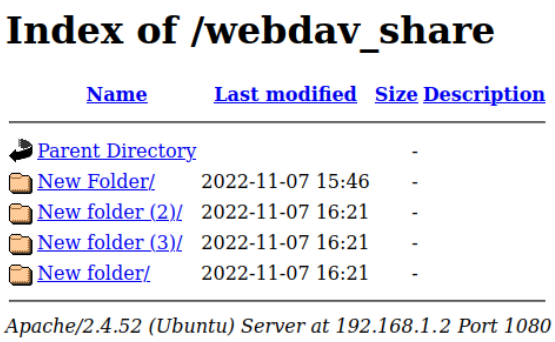


17.4.2. LINUX

On Linux the Dolphin file manager can be used to sign in.

1. Enter the address of the WebDav server to the address bar:

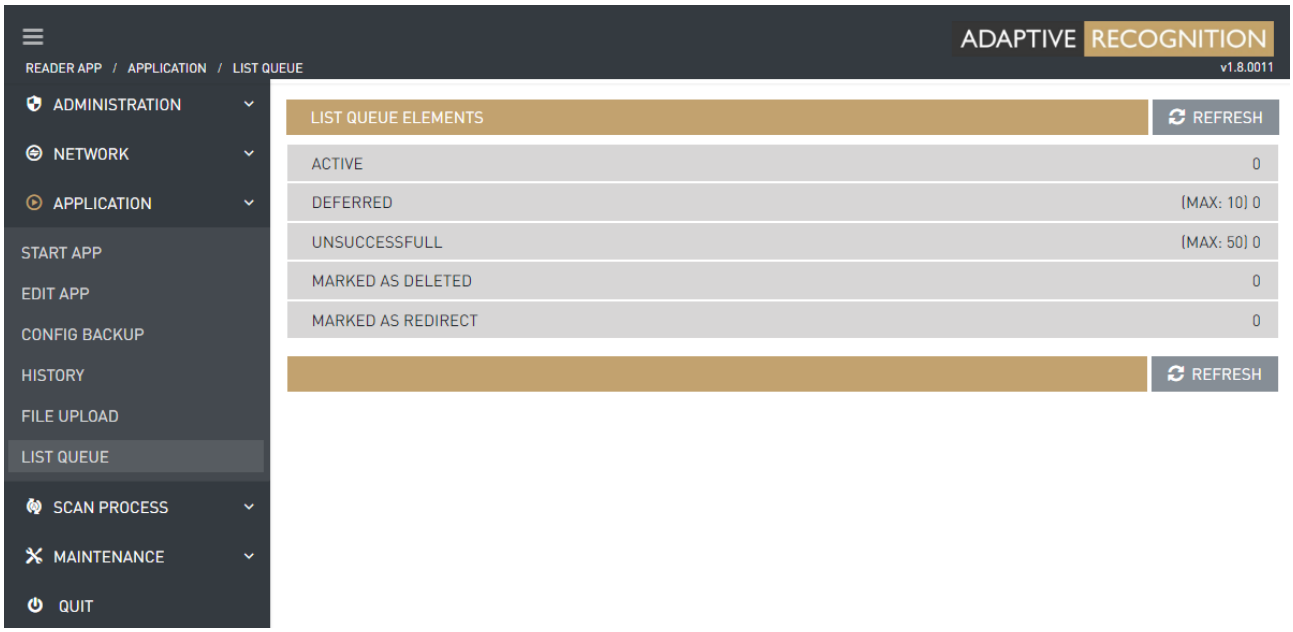
   webdavs://tesztg.example.com:1443/webdav_secure_share/
2. Then, press **[Enter]**.
3. After successful connection, enter the username and password.
4. Then, the page appears:



17.5. TROUBLESHOOTING

17.5.1. OSMOND

If upload is not working, Osmond will collect the unsuccessful documents to the **UNSUCCESSFUL queue** until its limit is not reached. When **UNSUCCESFUL** limit is reached, the oldest element in queue is overwritten by the result of the latest scan. Documents in unsuccessful status can be checked in the **APPLICATION / LIST QUEUE** menu. In case of correct operation this row is empty.



Note

If upload is not working, then the WebDav server firewall (Windows or Linux) or another network device may be blocking it.

17.5.2. CHECKING THE SERVER

The server can be checked by using the following command. This command tries to upload a file to the server:

```
curl -v -T 'main.txt' --user tesztg:123456
https://tesztg.example.com:1443/webdav_secure_share/
```

where:

`main.txt` is the name of the file to be uploaded

`tesztg` is the name of the user

`123456` is the password of the user

`tesztg.example.com` is the fully qualified domain name (FQDN) of the server

`1443` is the port through which the server is listening

17.5.3. CHECKING THE CERTIFICATE

The certificate can be checked by using the following command:

```
openssl s_client -connect tesztg.example.com:1443 -servername
tesztg.example.com
```

If the certificate is adequate, the returned message is the following:

```
Verify return code: 0 (ok)
```

17.5.4. MISSING INTERMEDIATE CERTIFICATE

If the intermediate certificate is missing, the `curl` command returns the following message:

```
curl: (60) SSL certificate problem: unable to get local issuer certificate
```

When checking the certificate, the openssl returns the following message if the certificate is missing:

```
Verify return code: 21 (unable to verify the first certificate)
```

In this case you must get the intermediate certificate. One way to get the certificate is described in the Installation of the SSL Certificate chapter.

17.5.5. LINUX

On Linux the WebDav protocol is provided by the Apache2. Its operation can be affected with the following commands:

- Check the configuration of Apache2:
  ```
  apachectl configtest
  ```
- Start the Apache2:
  ```
  sudo systemctl start apache2
  ```
- Restart the Apache2:
  ```
  sudo systemctl restart apache2
  ```
- Stop the Apache2:
  ```
  sudo systemctl stop apache2
  ```
- Enable the Apache2 to start automatically on startup (if it is not set, then it is recommended):
  ```
  sudo systemctl enable apache2
  ```
- Disable the Apache2 to not start automatically on startup:
  ```
  sudo systemctl disable apache2
  ```
- Query the status of the Apache2:
  ```
  sudo systemctl status apache2
  ```

18. SETTING THE CONFIGURATION AND SOFTWARE UPDATE ON OSMOND DEVICE THROUGH NETWORK

The Osmond firmware version 1.8 and above versions allow sending configuration updates (e.g., changing settings) and firmware updates from a remote update server to one or more Osmond N devices via network.

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

In this section the creation of the environment required for this, as well as the settings and the process of the different types of updates (config or software) will be described.

18.1. THE STRUCTURE OF THE UPDATE SERVER

The following are required for the update server:

1. A web server capable of serving via HTTP/HTTPS connection
   The section will show the usage and installation of a python-based web server. In practice, web servers based on any technology can be used, which are capable of serving via HTTP/HTTPS connection.

2. 'get' file
   See Description of the Configuration File (get file).

3. Update file and the associated signature file (.chk)
   The update can be of two types:
   - Software updates which contain the update of the software modules of the device (zip file). They are exclusively originated from the manufacturer.
   - Configuration updates, see Configuration File (config_new1.conf).
     They can be created by anyone.

4. Signing script and keys required for signing
   The device only accepts digitally signed updates. Unsigned updates are not downloaded to the device. The signature originates either from the manufacturer or the customer. When the configuration update is signed by the customer, the public key of the customer must be on the device. For more information on it, contact ADAPTIVE RECOGNITION support team.

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

18.2. INSTALLING AND SETTING THE UPDATE SERVER ON WINDOWS 10

18.2.1. INSTALLING PYTHON

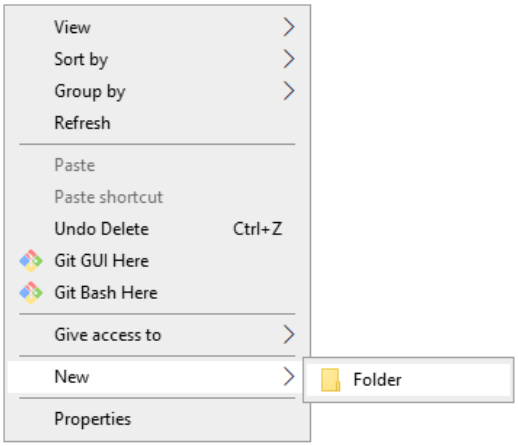
1. Download and install Python 3 or newer version (currently Python 3.11.3 can be accessed):
   - Navigate to https://www.python.org/downloads/.
   - Select "**Use admin privileges when installing py.exe**" and "**Add python.exe to PATH**" by ticking the checkboxes.
   - Then, click on **[Install Now]**.

   - After installation, it is recommended to restart the PC.

2. Open Command Prompt. Command Prompt can be accessed by entering "cmd" text to the search bar at Start menu and clicking on the appearing Command Prompt line.

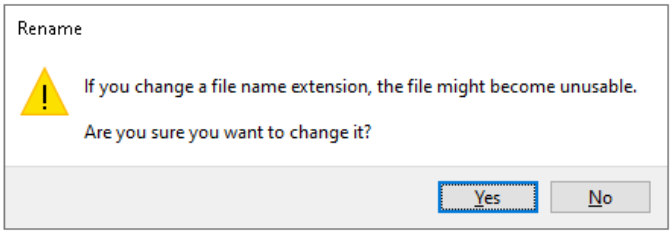
18.2.2. INSTALLING THE UPDATE SERVER

1. Create the library of the update server:
   - Navigate to **Start menu / Windows System / File Explorer**.
   - In the appearing window navigate to `C:\Users\user` library, where the `user` is the name of the user.
   - Right click on a neutral area, then select **New / Folder** menu item from the pop-up quick menu.

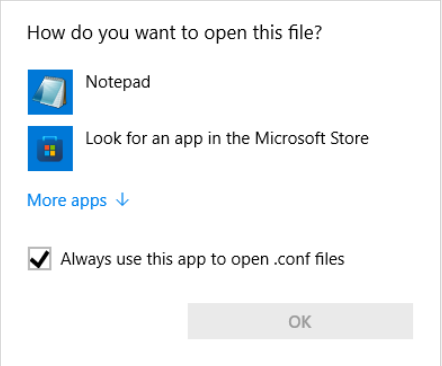


   - Rename the created library to: `update_server`

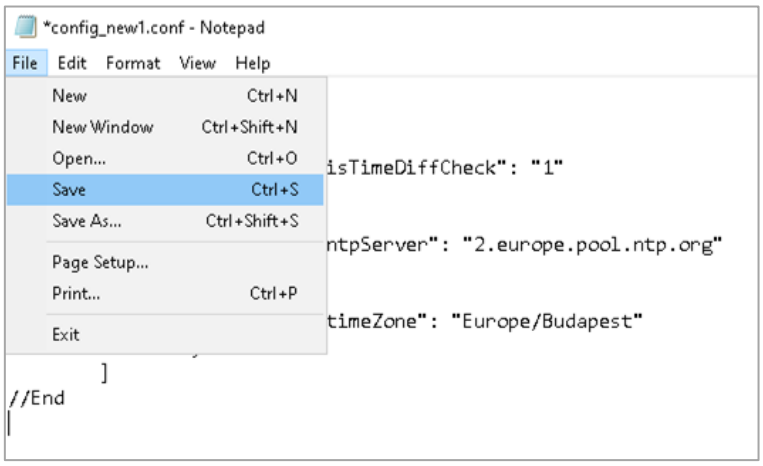
2. Open the `update_server` library.
3. Create or copy the configuration file to the `update_server` library. For example, copy the one located at Annex / Configuration File (config_new1.conf) chapter.
   - Right click, then select **New / Text Document** from the appearing quick menu.
   - Name the file to **config_new1.conf**
   - If an alert message pops up, click on the **[Yes]** button on the message box.



- Right click on the file name and select the **Edit** menu item. In the absence of this, click on the **Open with** menu item and browse the **Notepad** application.



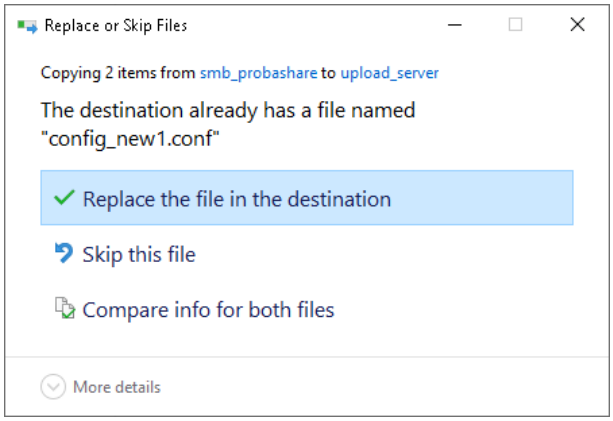
- To this location copy the content of the configuration file located in the Annex / Configuration File (config_new1.conf) chapter.
- Then, click on **File / Save** in the Notepad application.



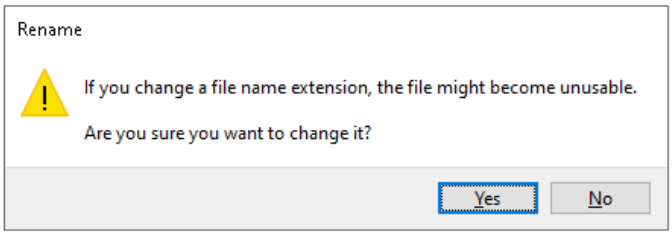
- At last, close the window by clicking on the "x" located in the upper right corner.

4. Sign the config_new1.conf file (see Signing the Configuration File chapter).

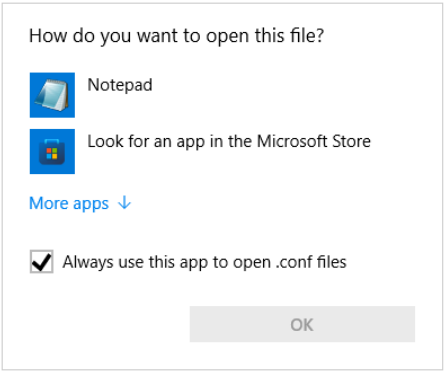
5. Copy the **config_new1.conf** and **config_new1.conf.chk** files to the `C:\Users\user\update_server` library.
   - The former **config_new1.conf** must be overwritten with the returned one.



6. Create or copy the 'get' file to the `update_server` library (see Annex / Description of the Configuration File (get file) chapter):
   - Right click in the File Explorer, then select **New / Text Document** from the appearing quick menu.
   - Name the file to: **get**
   - If an alert message pops up, click on the **[Yes]** button on the message box.



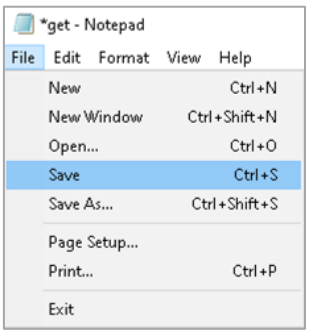
   - Right click on the file name and select the **Edit** menu item. In the absence of this, click on the **Open with** menu item and browse the **Notepad** application.



- To this location copy the following line and press the **[Enter]** key at the end of the line in order to start a new line:

  * | * | * | * | * | **`config_new1.conf`**

- Then, click on **File / Save** in the Notepad application.



- At last, close the window by clicking on the "x" located in the upper right corner.
- The content of the **`update_server`** library can be seen in the following image:

Name	Date modified	Type	Size
config_new1.conf	5/11/2023 5:09 PM	CONF File	1 KB
config_new1.conf.chk	5/11/2023 5:09 PM	Recovered File Fra...	1 KB
get	5/12/2023 5:16 PM	File	1 KB

7. Start the Python web server:

   - Open **Start menu / Windows System / Command Prompt**

   - Navigate to the update server in the Command Prompt:

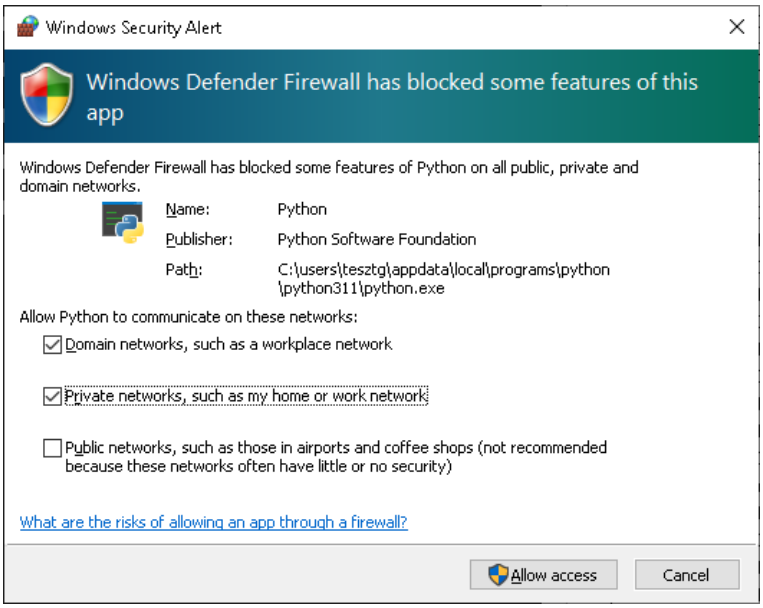
     ```
     cd update_server
     ```

   - Start the Python web server:

     ```
     python -m http.server 3280
     ```

     where: `3280` is the port through which the update server is listening

   - If a window pops up indicating that Firewall has blocked the Python server, click on the **[Allow access]** button on this window.



   - The availability of the server can be tested by entering its address to the address bar of the browser:

     ```
     http://192.168.1.3:3280
     ```

     where:

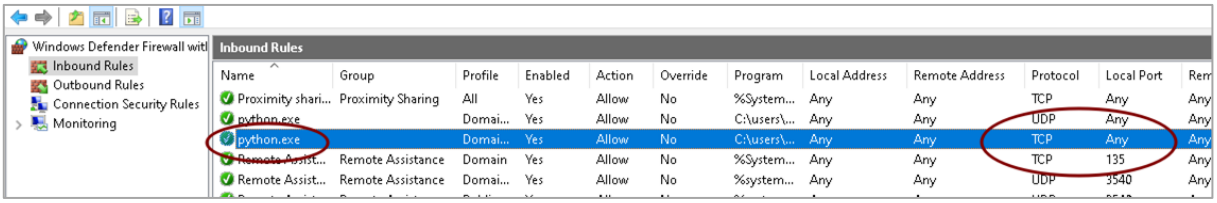
     `192.168.1.3` is the IP address of the update server on which the python server is started,

     `3280` is the port through which the update server is listening

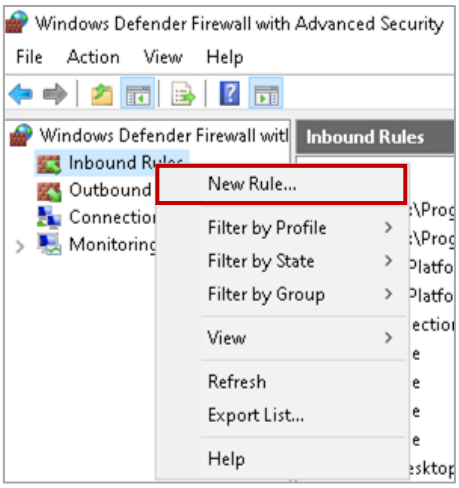
18.2.3. SETTING THE FIREWALL

If the server cannot be accessed from another PC, check the Windows Firewall settings.

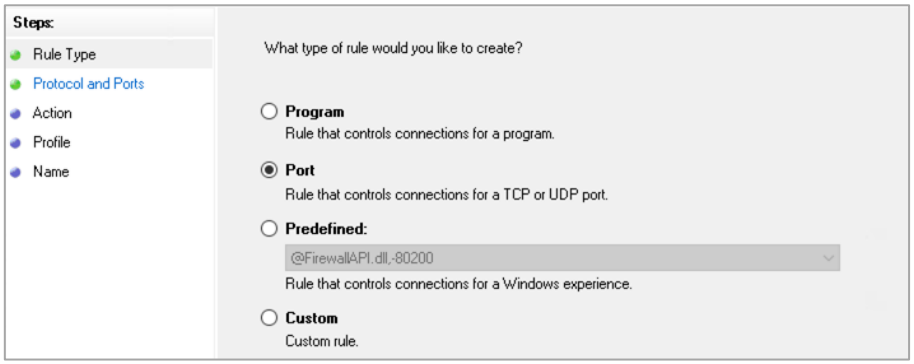
1. Navigate to **Control Panel / System and Security / Windows Defender Firewall / Advanced settings**.
2. Click on **[Inbound rules]** located in the left section.
3. If the **python.exe** is listed, which is valid for all local ports, or at least port **3280** with TCP protocol, and a green check mark is displayed next to its name, then the setting of Firewall is appropriate.



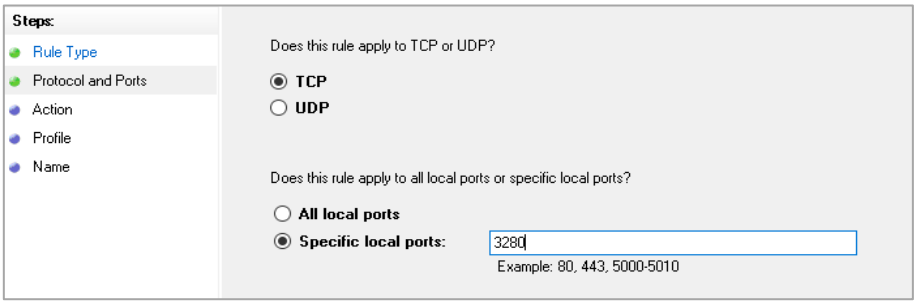
4. If the **python.exe** is not listed, right click on the **Inbound Rules**, then select **New Rule...** from the appearing quick menu.



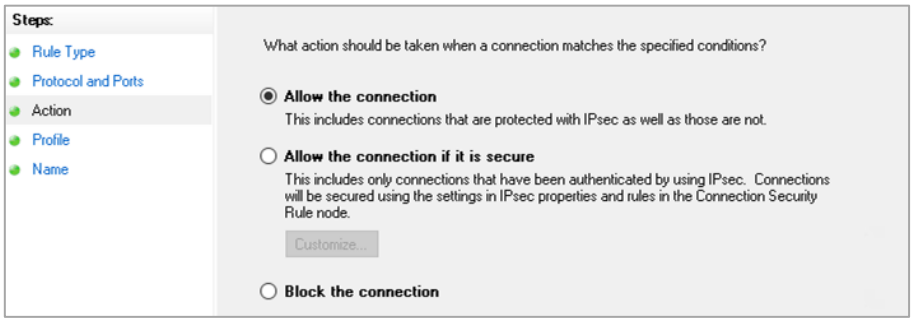
5. In the pop-up window select **Port**, then click on the **[Next >]** button.



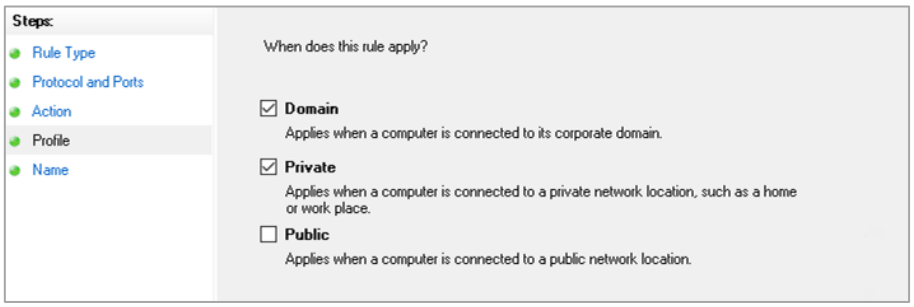
6. At "**Does this rule apply to TCP or UDP?**" select **TCP**.
7. At "**Does this rule apply to all local ports or specific local ports?**" select "**Specific local ports**" and enter the value **3280** to the text field. Then, click on the **[Next >]** button.



8. On the following window select "**Allow the connection**" option and click on the **[Next >]** button.

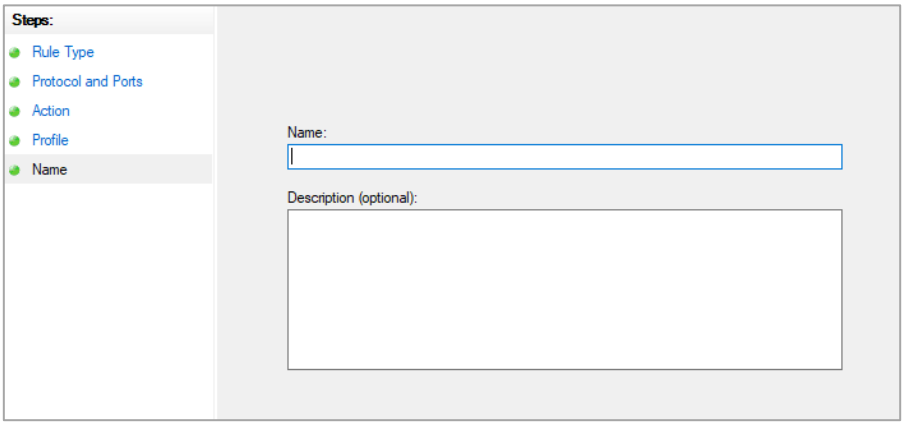


9. On next window select "**Domain**" and "**Private**" options by ticking their checkboxes. The "**Public**" option is not recommended, only if the PC is connected to a public network. Then, click on the **[Next >]** button.

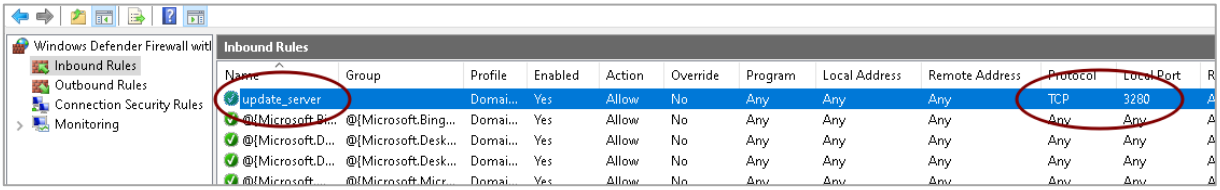


Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

10. On the following window type "**update_server**" to the "**Name:**" text field. Then, click on the **[Finish]** button.



11. The new rule ("update_server") appears in the list.



12. Restart the PC.

18.3. INSTALLING AND SETTING THE UPDATE SERVER ON LINUX

18.3.1. INSTALLING PYTHON

Most Linux distributions, including Ubuntu 22.04, install one of the Python versions during its installation. In order to perform the following steps, open a terminal.

1. Before querying the version, it is recommended to update the operating system:

   ```
   sudo apt update
   sudo apt upgrade -y
   ```

2. Restart the PC.

3. Query the Python version:

   ```
   python3 -V
   ```

   This queries the version of Python 3.

   - If **no error** is returned, the Python version is correct.
   - If **error** is returned, install Python 3:

     ```
     sudo apt-get install python3
     ```


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

18.3.2. INSTALLING THE UPDATE SERVER

Install the update server from command line:

1. Create the library of the update server:
   `mkdir /home/user/update_server`
   where the `user` is the name of the user

2. Enter the `update_server` library:
   `cd /home/user/update_server`
   where the `user` is the name of the user

3. Create or copy the configuration file to the `update_server` library. For example, copy the one located at Annex / Configuration File (config_new1.conf) chapter.
   - `nano config_new1.conf`
   - Copy the content of the configuration file located in the Annex / Configuration File (config_new1.conf) chapter.
   - Then, use the **Ctrl + X** keyboard shortcut
   - At "**Save modified buffer?**" press **Y** (Yes)
   - Then, press the **Enter** key

4. Sign the `config_new1.conf` file (see Signing the Configuration File chapter).

5. To this location copy the signed **config_new1.conf** and **config_new1.conf.chk** files:
   `cp /home/user/update_server_sign/config_new1.conf .`
   `cp /home/user/update_server_sign/config_new1.conf.chk .`

6. Create or copy the '**get**' file to the `update_server` library (see Annex / Description of the Configuration File (get file) chapter):
   - `nano get`
   - Copy the content of the '**get**' file located in the Annex / Description of the Configuration File (get file) chapter:
     `* | * | * | * | * | config_new1.json`
   - Then, use the **Ctrl + X** keyboard shortcut
   - At "**Save modified buffer?**" press **Y** (Yes)
   - Then, press the **Enter** key

7. The content of the **update_server** library can be seen in the following image:

```
user@ubuntu2204installtest:~/update_server$ ll
total 20
drwxrwxr-x  2 user user 4096 máj   15 16:15 ./
drwxr-x--- 17 user user 4096 máj   15 15:44 ../
-rw-rw-r--  1 user user  224 máj   15 16:14 config_new1.json
-rw-rw-r--  1 user user  547 máj   15 16:14 config_new1.json.chk
-rw-rw-r--  1 user user  547 máj   15 16:14 get
user@ubuntu2204installtest:~/update_server$
```

8. Start the Python web server:

   python3 -m http.server 3280

   where: **3280** is the port through which the update server is listening

9. The availability of the server can be tested by entering its address to the address bar of the browser:

   http://192.168.1.3:3280

   where:

   192.168.1.3 is the IP address of the update server on which the python server is started,

   3280 is the port through which the update server is listening

18.3.3. SETTING THE FIREWALL

The port used by the update server must be set in the firewall, then restart it, if the firewall is active. In general, the **ufw** runs on Ubuntu. Its state can be queried with the **sudo ufw status** command. If it is active, then:

- **sudo ufw allow 3280/tcp**
- **sudo ufw disable**
- **sudo ufw enable**

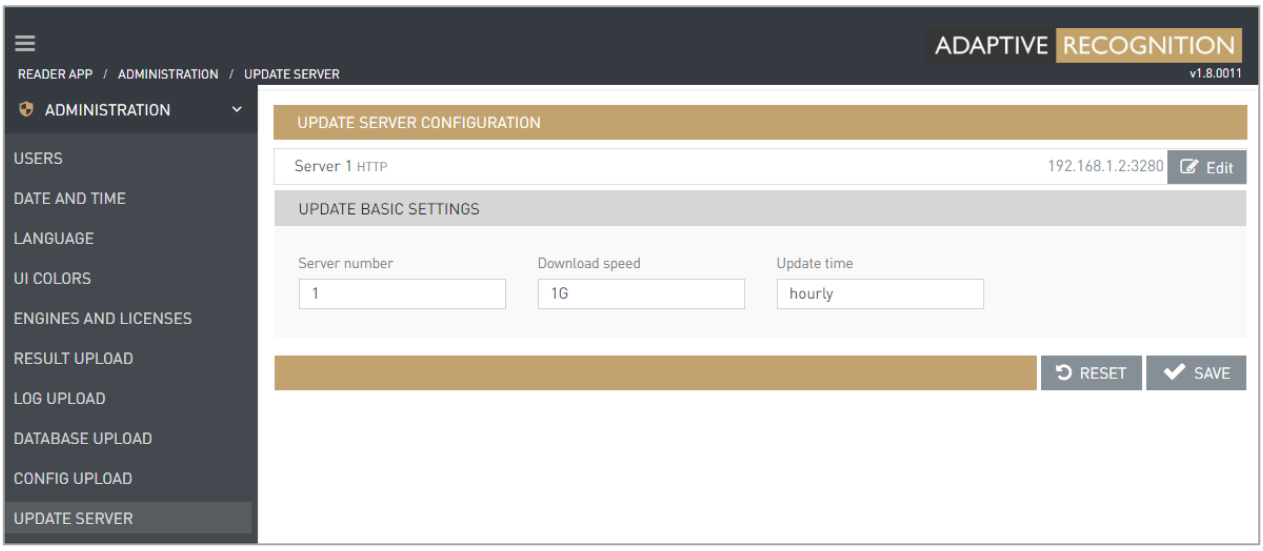
18.4. SETTING ON OSMOND

The parameters of the update server can be set on the web interface of the Osmond device. By default, the web interface is accessible on 192.0.2.3:3000, but it can be set to another address as well. The IP address of the Osmond in the example is 192.168.6.244:3000.

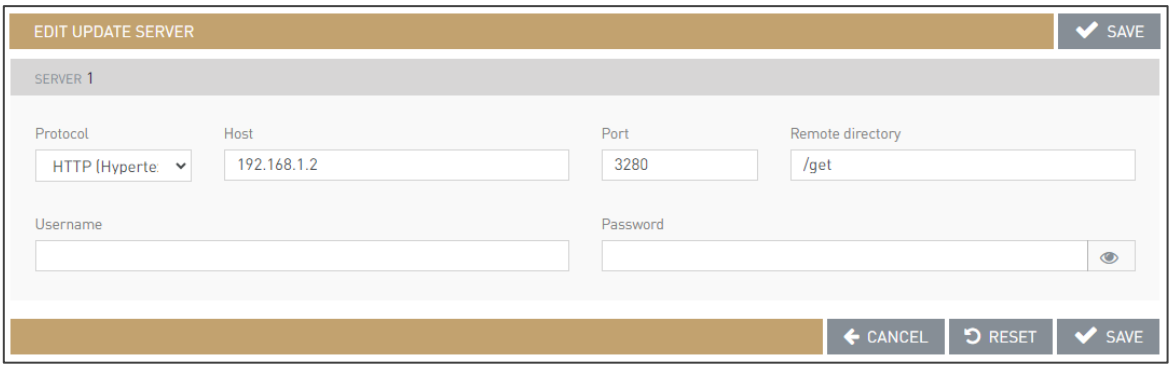
1. After signing in to the web interface, click on the **Main menu** (the three horizontal stripes; at the top left corner of the webpage) in order to open the menu items.

2. Navigate to **ADMINISTRATION / UPDATE SERVER**.

3. Click on the **[Edit]** button belonging to **Server 1**.

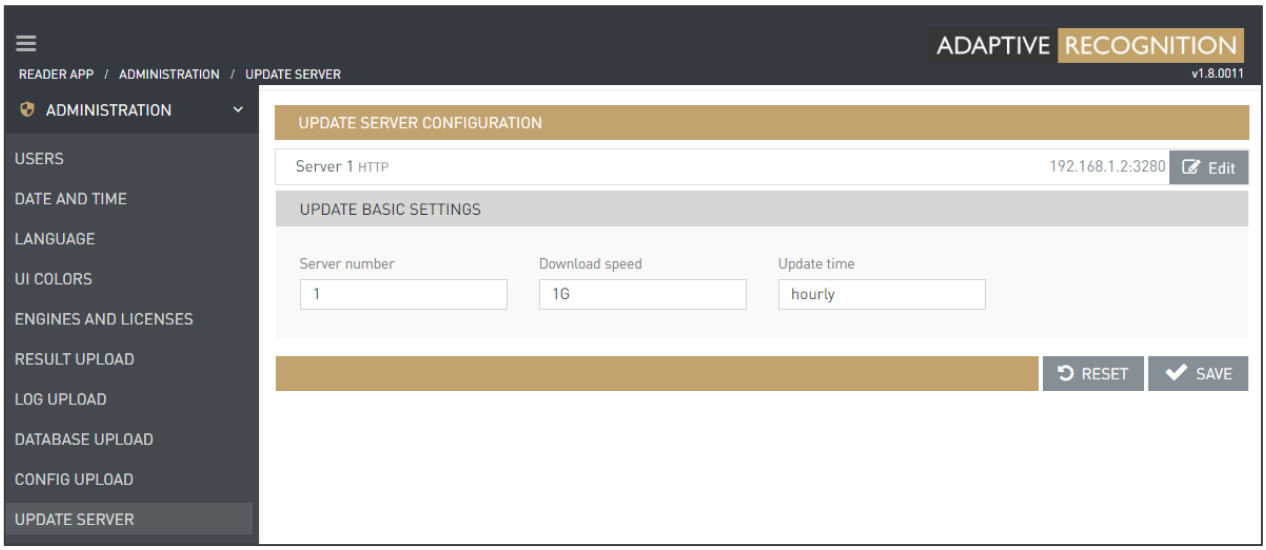


4. On the appearing menu set the following:
   - **Protocol**: HTTP (Hypertext Transfer Protocol)
   - **Host**: IP address of the update server, in this case: 192.168.1.2
   - **Port**: Port of the update server: 3280
   - **Remote directory**: Name of the folder accessible from the server's root directory: /get
   - **Username**: Name of the user. This field must be blank.
   - **Password**: Password of the user. This field must be blank.



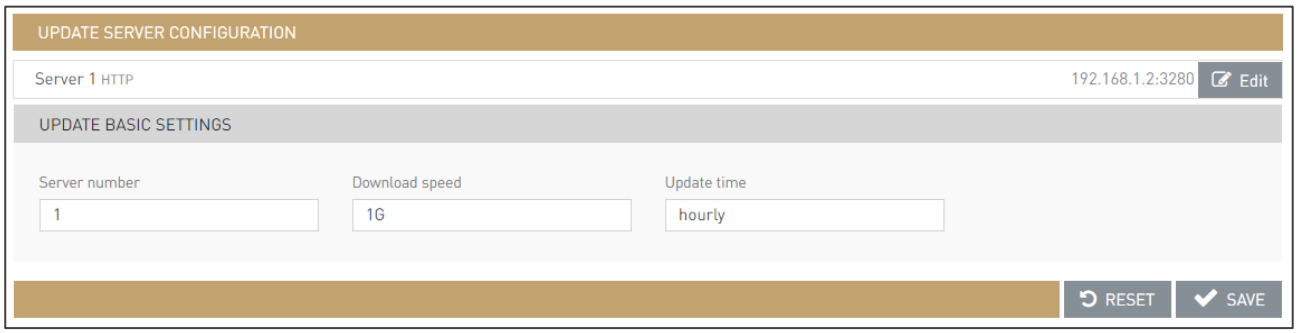
5. If all fields are filled in, click on the **[SAVE]** button.

   Wait until the **UPDATE SERVER CONFIGURATION** window appears:



6. On the **UPDATE SERVER CONFIGURATION** window specify the following:
   - **Server number**: The number of the update servers, in this case: 1
   - **Download speed**: The speed of the download, in this case: 1G
   - **Update time**: in this case: hourly

7. Then, click on the **[SAVE]** button.



Note

For more information, see ADMINISTRATION / UPDATE SERVER chapter.

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

18.5. NOTES FOR THE UPDATE SERVER

1. Osmond stores the name of the configuration file, therefore update with the same configuration file name is only possible once. If the settings must be reupdated, rename the '**conf**' file to e.g., config_new2.conf, config_new3.conf, etc.

2. If you rename the configuration file, do not forget to rewrite its name in the '**get**' file as well.

3. Multiple update servers can be set. In this case the Osmond device queries them in the specified order. If it finds a relevant update, Osmond applies it and does not continue the search.

4. With the described settings Osmond checks hourly and, on every startup, that whether there is a new configuration file on the server.
   The value of the **Update time** can be the following:
   - '**daily**'
   - '**hourly**'
   - '**weekly**'
   - '**cron**' e.g., "0 */2 * * *" to check for updates in every two hours

18.6. TESTING THE SETUP

In case of error the update server can be tested from command line with the following command:

```
curl -XGET 192.168.1.2:3280/get
```

where:

`192.168.1.2` is the IP address of the update server

`3280` is the port through which the update server is listening

This command returns the text located in the '**get**' file. If the text is not returned, use the `curl` command which can give a more detailed description of the error, especially when it is ran with detailed logging:

```
curl -XGET -vvv 192.168.1.2:3280/get
```


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

18.7. ANNEX

18.7.1. CONFIGURATION FILE (CONFIG_NEW1.CONF)

The configuration file contains those fields and their values that are to be set. Its format is similar to JSON, but it begins and ends with a note line (//). The first note is the name of the table, fields of which are included in the list, below the table name. The last note is the "End" element which indicates the end of the list.

For example:

```
//Properties
      [
            {
              " UpdateServer/1/host" : "192.168.1.2"
            },
            {
              " UpdateServer/1/protocol" : "HTTP"
            },
            {
              " run/configVersion" : "1.0.0.1"
            }
      ]
//End
```

The example above sets the IP address, the protocol and the version number of the given configuration of the Update Server 1.

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

18.7.2. SIGNING THE CONFIGURATION FILE

1. Perform the signing in a library, different than the update server (update_server). Therefore, create a library named as **`update_server_sign`** in the user account.

2. Copy the following files to the **`update_server_sign`** library:
   - ***.conf file** (e.g., **`config_new1.conf`**)
     This file contains the configuration. It can be created with text editor as described in Annex / Configuration File (config_new1.conf) chapter.
   - **genchkfile.py**
     This file performs the signing of the configuration file. Free to use software which should be requested from ADAPTIVE RECOGNITION Support Team.
   - **private.key**
     This file is the private key.
   - **public.key**
     This file is the public key.
   - **device.pub**
     This is the public key of the device.

3. Open a terminal and enter the **`update_server_sign`** library.

4. Sign the configuration file:
   `./genchkfile.py config_new1.conf`

   where:
   `config_new1.conf` is the text-based configuration file. Its name is optional, but the **.conf** extension should be kept.
   The created files:
   - **`config_new1.conf`**
     This is the signed configuration file. It does not match the text-based configuration file.
   - **`config_new1.conf~`**
     This is the original text-based configuration file.
   - **`config_new1.conf.chk`**
     This is the signature.

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

18.7.3. DESCRIPTION OF THE CONFIGURATION FILE (GET FILE)

The 'get' file describes which device gets which configuration file. This is a text file in which one line is divided into 5 sections. The sections are separated by pipe characters (|).
The structure of one line is the following:

<firmware version>|<device type, always prmcmini>|<device serial number>|<device architecture, always arm64>|<label, e.g., TEST>|<file name or file names separated by commas, if there are more>

For example:

```
1.7.0|*|208663|*|*|config_for_1.7.conf
```

The meaning of the example:
The device with the serial number 208663 must download the config_for_1.7.conf file, if the version number of its firmware is 1.7.0. In the sections the asterisk symbol (*) denotes an arbitrary sequence of character.
Thus, a line valid for all devices is the following:

```
*|*|*|*|*|config_new1.conf
```

After download, the updates are performed either immediately or on the next startup. This can be adjusted with the |F switch located at the end of the line in the 'get' file. If it is present, the update is performed immediately after download.

Important!

After each update execution, the device restarts automatically. The new settings or software version are only valid after restart.

18.7.4. CONFIGURATION FIELDS

```
//Properties
      [
            {
                  "UpdateServerMain/update_time" : "17 */2 * * * "
            },
            {
                  "UpdateServer/1/host" : "192.168.0.121"
            },
            {
                  "UpdateServer/1/remote_directory" : "get"
            },
            {
                  "UpdateServer/1/protocol" : "HTTPS"
            },
            {
                  "UpdateServer/1/password" : "test"
            },
            {
                  "ResultUpload/WSS/access_directory" : "test directory"
            },
            {
                  "ResultUpload/WSS/host" : "test wss host"
            },
            {
                  "ResultUpload/WSS/authority/RawData" : "-----BEGIN
CERTIFICATE-----
\nMIIEwDCCAqgCCQDKi/UZZC3p8DANBgkqhkiG9w0BAQsFADAiMSAwHgYDVQQDDBdQ\ {MORE
DATA} azbvCi3VvXK7Rb3uK5VeP0MrU\nK88gH3Q6NmxvLJn/ZbnOjb/OZm8=\n-----END
CERTIFICATE-----\n"
            },
            {
                  "ResultUpload/WSS/authority/UploadName" : "test_ca.crt"
            },
            {
                  "ResultUpload/WSS/certificate/RawData" : "-----BEGIN
CERTIFICATE-----
\nMIIE3TCCAsUCAQEwDQYJKoZIhvcNAQELBQAwIjEgMB4GA1UEAwwXUFdGIERpZW5z\ndGVuI
FNjYW5uZXIgQ0EwHhcNMjAwNzE0MTg1NzQ1WhcNMjEwNzE0MTg1NzQ1WjBH\ {MORE DATA}
\nc48bLiAi/hPkrEfvjyppaHmxKACcZ4HGew1Uq8LuCAfmeJKbMXPtkAv31ioq12GH\ndQ==\
n-----END CERTIFICATE-----\n"
            },
            {
                  "ResultUpload/WSS/certificate/UploadName" :
"testcertfilename.crt"
            },
            {
```

```
                "ResultUpload/WSS/private_key/RawData" : "-----BEGIN
PRIVATE KEY-----\nMIIJQwIBADANBgkqhkiG9w0BAQEFAASCCS0wggkpAgEAAoICAQC/
{MORE DATA} \nu5e8FrAWnzxcTTaswHU+ZO2015T4d7E=\n-----END PRIVATE KEY-----
\n"
          },
          {
                "ResultUpload/WSS/private_key/UploadName" :
"testkeyfilename.key"
          },
          {
                "ResultUpload/WSS/reconnect_attempts" : "6"
          },
          {
                "ResultUpload/WSS/upload_frequency" : "6"
          },
          {
                "UpdateServer/1/username" : "testupdateserver_username"
          },
          {
                "LogUpload/ipAddress" : "test_loguploadaddress"
          },
          {
                "LogUpload/port" : "6666"
          },
          {
                "LogUpload/protocol" : "tcp"
          },
          {
                "LogUpload/isRealtimeUpload" : "1"
          },
          {
                "queue/check_interval" : "88"
          },
          {
                "queue/minimal_available_space" : "88"
          },
          {
                "queue/package_limit" : "8"
          },
          {
                "queue/corrupted_package_limit" : "16"
          },
          {
                "queue/queue_warning_interval" : "24"
          },
          {
                "queue/should_send_queue_warning" : "1"
          },
```

```
            {
                  "queue/is_delete_deferred_uploads" : ""
            },
            {
                  "queue/is_delete_corrupted_uploads" : ""
            },
            {
                  "run/configVersion" : "1.9.1.9"
            },
            {
                  "ResultUpload/WSS/close_handshake_timeout": "32765"
            }
      ]
//End
```

19. PASSPORT READER PROPERTY LIST

The property list contains the short descriptions of the passport reader properties according to the following:

Property Path and Name

Every property has a path and a name. When referring to a property (e.g., in the Full Page Reader application) the path must be specified as well.

> Note
>
> If you write in the **gxsd.dat** file, pay attention to type between the <pr> and </pr> elements.

Value type/Values

The property types are specified to help to make managing them easier. Use values of the specified type when setting property values.

> Note
>
> For **boolean** values use 0 or 1.
> For **integer** values use decimal numbers only.

Accessibility

- **F (File)**: means the initialization from the gxsd.dat file.
  It can be found:
  - in the **ProgramData/gx** hidden directory on **Windows** systems,
  - in the **var/gx** directory on **Linux** systems.
- **R (Read)**: means that the **getProperty** method can be called in the program.
- **W (Write)**: means that the **setProperty** method can be called in the program.

Default Value

The values marked bold represent the values applied by default.

Description

In the following sections the short description of the properties will be provided.

Note

All properties located under the **docimageprops** and **log** tabs are described in the **GX Reference Manual**. Most of these advanced properties are not required to be adjusted in typical user applications.

Note

All properties located under **document/mqc** tab are described in the **MRZ Quality Assurance Reference Manual**. Most of these advanced properties are not required to be adjusted in typical user applications.

Note

The following properties can only be set when the device is already in use:

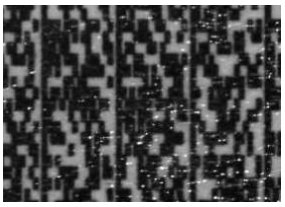
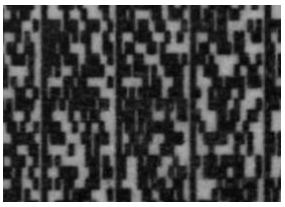
- properties starting with ctrl/
- preview_light
- testdoc_mode
- uvwarm_quality
- freerun_mode

When connecting the device again, these properties will be reset.

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

19.1. DETAILED PROPERTY DESCRIPTIONS

Property Path and Name	Value type/ Accessibility	Default Value	Description
act_page	Integer R		The ordinal number of the last scanned page.
api_date	String R		The date required for the PRSoftware license.
autosave/enddate	String F / R / W		Date after which the automatic saving is discontinued. E.g., 2020-12-02
autosave/filter	Integer F / R / W	**0** min: 0 max: 2	Enables the automatic encrypted saving. Such files can be decrypted if the appropriate private key is available. **NOTE**: The **autosave/path** property must be set too. **Possible values**: **0** – The automatic encrypted saving is turned off. **1** – The saving of every image after scanning. **2** – The saving of the images recommended by the engine.
autosave/keeptime	Integer F / R / W	min: 1	Number of days, after which the images are deleted automatically. **NOTE**: Check and Delete algorithm only runs with the saving next in line.
autosave/maxfilenum	Integer F / R / W	min: 1	The automatic saving saves up to this number of images. It always deletes the oldest ones, if it is needed. The files saved manually are not counted into this value. **NOTE**: Check and Delete algorithm only runs with the saving next in line.
autosave/path	Path F / R / W		The path of the automatic encrypted saving. Such files can be decrypted if the appropriate private key is available. **NOTE**: The **autosave/filter** property must be set too.

autosave/skip_text	Boolean F / R / W	False	In case of "autosave/filter" = 2, it enables or disables the system to generate txt files.
barcode/contrast	Float F / R / W	**1.5f** min: -3.f max: 10.f	**NOTE**: This property applies only to **1D** and **PDF417** barcodes. The **barcode/contrast** property controls the contrast compensation level. The default value is **1.5**. Changing this value affects the barcode reading accuracy. If it is set to **-2**, an automatic contrast adjustment is launched. If set to **-3**, an appropriate contrast setting is searched, but not preserved (used for the actual reading process only).
barcode/deglinter	Boolean F / R / W	False	There are some special cases when the **barcode/deglinter** property can be useful. It reduces the noise caused by the damages of the covering foil. It is specially developed to eliminate the light horizontal thin lines produced by the glinting of the broken foil. The deglinting process works only if the height of the noise line is significantly smaller than the size of the barcode signs.  
barcode/enable_vertical	Boolean F / R / W	False	Note, that this property applies only to 1D and PDF417 barcodes. Basically, barcodes can be read only in horizontal direction. This behavior can be changed with the **barcode/enable_vertical** property.
barcode/interchar_space	Boolean F / R / W	False	This property is needed for reading a particular barcode located in the inner side of the Mexican documents. (Code 39 with large gap between characters.)

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

barcode/recog_order	String F / R / W		The barcode reading process can be sped up by specifying this property. The order in which certain barcode types are read can be specified. The not needed types can be omitted. <recog_order value="51789a"/> **1** – for all 1D codes **5** – PDF417 **7** – DataMatrix **8** – QR code **9** – AZTEC **a** – UPU
calib_file	Path R		It returns the name and path of the used calibration file.
calib_path	Path F / R / W		Path of the calibration file. If not specified, the calibration file is searched at the following default locations: • A directory specified by the **calib_path** property. • `%SystemRoot%\system32\gx\pr` directory on Windows systems, • `/usr/share/gx/pr` directory on Linux systems. • `%CommonProgramFiles%\gx\pr` directory on Windows systems • `Programdata\gx\pr` on Windows operating systems • `/var/gx/pr` directory on Linux systems.
ctrl/always_gray	Boolean F / R / W	False	If **1**, it provides gray output images. Recommended for time-critical applications.
ctrl/autoread_calib	Boolean F / R / W	True	Internal property.
ctrl/capture_mode_mask	Integer R / W	**0**	Obsolete. Enables the low-resolution image capturing. Certain bits represent corresponding lights. Instead of this property, use the **capture_style** property.

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

ctrl/detdark	Boolean F / R / W	False	This property is specially developed for capturing dark documents (e.g., front cover of certain passports). By setting this property to **1**, the motion detector of the device will detect dark documents as well.
ctrl/ip or **ctrl/ip/#**	String R		In case of composite USB/network device, it returns the IP address of the device. In place of # ordinal number or connector type can be written. E.g., eth0.
ctrl/mdarea	String F / R / W		The area examined by the motion detection can be specified in thousandths using the following methods: **Example**: "400" → the middle 40% x 40% area "left,top-right,bottom" → the area specified by the left, top, right, bottom values (in thousandths).
ctrl/photo/adjust	Boolean F / R / W	False	This property is applicable for PRMc devices. The software correction of the accidental displacement of the photo image.
ctrl/raw_delay	Integer F / R / W	**1000/50** min: 10 max: 1600	**NOTE**: This value is applicable only for Combo Scan devices in order to control the speed of image capturing and transferring to the PC. The higher this value is, the slower the image transfer will be. Adjust this value according to the performance of your PC: Low values are preferred on fast PC-s, while high values are applicable on slow ones. Default value: 1000 or 50 depending on the device type.
ctrl/resolution	Integer F / R / W	**0** min: 0 max: 100000	The default resolution of the captured images can be set with this property (in pixel/meter). Setting the resolution to lower values results in smaller image size, which e.g., eases the insertion into a database. If it is set to **0**, the default resolution of the device will be applied.

ctrl/resolution_#		Integer F / W	**0** min: 0 max: 100000	**NOTE**: The number of the window is to be written in place of #, deviating from the regular, numbered from 1. This property is applicable for multi-window devices (e.g., devices equipped with photo camera). Single step setup of all resolutions belonging to a single window of a multi-window device.
ctrl/shield		Integer F / R / W	**0** min: -1 max: 4	The devices with cover colored white are indicated with this property, in order to recognize semi-transparent documents.
ctrl/white/ ctrl/infra/ ctrl/uv/ ctrl/coax/ ctrl/edge/	**resolution**	Integer F / R / W	**0** min: 0 max: 100000	Resolution of the captured image under the light specified in the Path. This value is provided in pixel/meter.
	capture_style	Integer F / R / W	**0**	The **capture_style** property can set different settings that modify certain elements of the captured image.
	rr	Boolean R		Defines, that the applied device supports the **Reflection Removal** on the given light.
debug/failures		Boolean F / R / W	False	Helps to discover the program freezes. If it is turned on, at every reading the (encrypted) image is saved temporarily, then deleted. It can increase significantly the processing time.
debug/floats		Boolean F / R / W	False	The **debug/floats** property enables/disables the tracking of invalid floating-point operations. When it is set to **1**, the system disables the floating-point exceptions for each API call and restores the state before exiting the function. This property also enables saving images in case of OCR error.
debug/memory		Boolean F / R / W	False	This property applies only to Windows operating systems. Enables memory test when entering or leaving the API code.

debug/path	Path F / R / W		The **debug/path** property specifies the directory for saving debug info if some internal image processing exception occurs. The occurrence of such errors is shown by the creation of one or more debug files containing images that caused the specific exception and/or error descriptions. Please send back these files to our support team in order to help us improving the recognition engine.
debug/recog	Boolean F / R / W	False	The **debug/recog** property enables/disables the tracking of image processing errors in some well-known situations. The system saves data when the failure is exactly known. E.g., checksum failed.
docimageformat	Integer F / R / W	**GX_JPEG** min: GX_BMP max: GX_WSQ	File format of the images which are saved in ZIP archives: **1**=BMP format (GX_BMP) **2**=JPEG format (ISO/IEC 10918-1) (GX_JPEG) **3**=JPEG-2000 Code stream syntax ISO/IEC 15444-1 (GX_JPEG2K_JPC) **4**=JPEG-2000 JP2 format syntax ISO/IEC 15444-1 (GX_JPEG2K_JP2) **5**=RAW format (uncompressed pixel data without header) (GX_RAW) **6**=PNG format – Portable Network Graphics (GX_PNG) **7**=WSQ format – Wavelet Scalar Quantization (GX_WSQ)
docimageprops/ #imageprops#	... F / R / W		Saving parameters for the images which are saved in ZIP archives. This path contains not a single, but multiple properties, which are described in the GX Reference Manual.
docrect/algorithm	Integer F / R / W	**0** min: 0 max: 2	**0** – First algorithm **1** – Second algorithm **2** – Both, if the first one is not successful

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

docrect/modify	Integer F / R / W	**MOD_DR_YES** min: MOD_DR_NO max: MOD_DR_ROTATION+MOD_DR_LS	This property enables the recalculation of "document views" by the result of the OCR functions. This option is necessary for e.g., recognition of upside-down documents. It is recommended to leave it turned on (1). **0** – Turned off **1** – Using new frame **2** – Only using the rotation **4** – Landscape in case of ID cards. It can be combined with **0**, **1**, **2** values.
document/database	Path F / R / W		Location of the automatic database. Such database contains sample images for authentication. Default: • Windows: `%ProgramFiles%\gx\docdb"` • Linux: `/var/gx/docdb`
document/fonttypes	String R		Returns a comma separated list of fonts usable for manual OCR.
document/icao_0o	Integer F / R / W	**0** min: 0 max: 3	During MRZ reading, the occasional 0-O character reading error (mix-up) is restored by pattern fitting algorithm. The property offers the option to skip the steps of the algorithm. **0** – Checksum based exchange **1** – Use of the direct OCR result **2** – Database based exchange **3** – Exchange, considering the environment
document/log/#logprops#	... F / R / W		Properties for logging. This path contains not a single, but multiple properties, which are described in the GX Reference Manual.

document/log/logprocess	String F / R / W		With the help of the logging option of the document processing module, performance logs can be created by setting the **log/logprocess** property to 'timing'. Example: `<default> <pr> <document> <log> <logprocess value="timing"/> <file value="prdoc.log"/> <filter value="6"/> <format value="$h:$m:$s ($l:$L) [$i] > $M\r\n"/> </log> </document> </pr> </default>`
document/mqc/#qcprops#	... F / R / W		This path contains not a single, but multiple properties, which are described in the MRZ Quality Assurance Reference Manual.
document/tip_century	Integer F / R / W	**0** min: 0 max. 1	In the case of the dates which do not contain the century, the algorithm tries to figure it out from the year and current date. **0** – Turned off **1** – Default algorithm
document/tip_names	Integer F / R / W	**0** min: 0 max: 3	Tip algorithms related to names. At present it works only with Australian documents. **0** – Turned off **1** – Division of the name parts **2** – Transformation of lowercase/uppercase **NOTE**: The values can be combined.
document/ weak_char_confidence	Integer F / R / W	**0** min: 0 max: 1000	If the confidence of a character is less than this value, then the character is replaced to **weak_char_value**. In most cases, this value can be applied for MRZ lines only.

document/ weak_char_value	Integer F / R / W	**'#'** min: 0x21 max: 0x7e	The value that replaces characters with confidence value below **weak_char_confidence**. Default value: # e.g., 65="A"
finger/cformat	Integer F / R / W	**0** min: 0 max: 1	Makes the saved fingerprint image more contrasted.
finger/check_hand	Boolean F / R / W	True	Enables hand swapping test. This test only gives signal when the four fingers of the scanned hand are present.
finger/check_upright	Float F / R / W	**-1.f** min: -1.f max: 4.f	Test upright position of the fingers. The value is the maximal allowed angle of fingers in radian. A negative value turns off the test.
finger/image_size	String F / R / W		Sets the size of the fingerprint images. • Fix size: xsize,ysize • All option: minx[-maxx][,miny[-maxy]][,prox/proy] • Minimal size: 80 pixels • Maximal size: 2048 pixels • Default size: 256 pixels • Default ratio: 2/3
finger/slap_quality	Boolean F / R / W	False	Use common quality for all fingers instead of individual qualities for each finger for collecting the best fingertips. Used when a slap image (that contains all fingers in one image) is required.

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

hide_fieldimage	String F / R / W		The codes of the fields that should be hidden, are to be written into the **hide_fieldimage** property separated by commas or semicolons. E.g., 2400 – VIZ face photo. The local value 1000 can be omitted. In such cases the system covers the VIZ as well as the MRZ fields. Naturally, only the fields read by the engine can be covered. E.g., the VIZ face photo will not be covered upon running GetMRZ. Neither the barcodes nor the RFID images should be covered. The text or binary data are left unmodified, similar to field images cut earlier. The coverage does not work on the Photo camera as well as it may work improperly on multi-camera devices (e.g., Big-eye). But upon setting the property, the algorithm runs on the already existing complete images and the document images are regenerated.
license_path	Path F / R / W		Path, where the system is searching for the licenses in order to upload automatically upon starting the device. Searches for them in the `rwdata_dir` regardless of the property.
log/#logprops#	... F / R / W		Properties for logging. This path contains not a single, but multiple properties, which are described in the GX Reference Manual.

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

log/logprocess	String
	F / R / W
			By logging the prapi module, the user can keep track of the device handling events like motion detection results, image capture events or device initialization events. In order to enable logging, set the **log/logprocess** property to one or more of the following values (separated by commas):
			• **apierror** - logging api errors independent of the user application
			• **timing** - logging process timings
			• **initialization** - logging the events of the device initialization
			• **motdetonchange** - logs motion detection only upon change
			Example:
			`<default>`
			`<pr>`
			`<log>`
			`<logprocess value="apierror,initialization"/>`
			`<file value="prapi.log"/>`
			`<filter value="6"/>`
			`<format value="$h:$m:$s ($l:$L [$i] > $M\r\n"/>`
			`</log>`
			`</pr>`
			`</default>`

module_dir	Path R		The path of the pr modules.
ocr_module	Path F / R / W		Name of the OCR module to use. It can be edited. If the module cannot be opened, then the program tries to use the default procr module.
omit_task_loading	Boolean F / R / W	False	If set to **1**, only images are loaded in case of LoadDocument, without results.
pcsc/autostart	Boolean F	False	Sets the autostart mode of the PC/SC upon the connection of the device. The pcsccontrol.exe file must be run in order to set autostart mode.

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

pcsc/max_air_speed	Integer F	**1700** min: 0 max: 1700	The maximum communication speed of the autostarted PC/SC control.
preview_light	Integer F / R / W	**Infra** min: 1 max: 0xff	The lighting conditions of the preview image can be set by the **preview_light** property. **Possible values:** **1** - Visible light **2** - Infrared light **3** - Ultraviolet light **4** - Visible coaxial light **5** - OVD image **6** - Photo image
rfid/air_speed	Integer F / R / W	**848** min: 106 max: 848	Speed of communication with the RFID chip.
rfid/extended_length	Boolean F / R / W	True	If **1**, fast RFID reading mode is enabled. This property may cause RFID reading errors in case of reading documents that do not comply with certain RFID standards, but they indicate incorrectly that they do. In these cases, the **extended_length** should be set to **0**. **NOTE**: This property is to be turned off in case of certain flawed cards.
rfid/log/#logprops#	... F / R / W		Properties for logging. This path contains not a single, but multiple properties, which are described in the GX Reference Manual.

rfid/log/logprocess	String F / R / W		The prrfid module log can be used for logging the communication and work flow between the card and the device. It is useful during the development or the testing process when communication tracing is necessary. It should not be used in production systems because it may contain personal data in this way violating security norms. The **log/logprocess** property for the prrfid module can be set to one or more of the following values (separated by commas): • **cardinfo** - logging information about the RFID card capabilities • **timing** - logging process timings • **initialization** - logging the events of the device initialization • **rfidstream** - logging binary data of the communication • **cryptodata** - logging cryptographic data • **formatting** - generates separator lines to the log Example: `<default> <pr> <rfid> <log> <logprocess value="cardinfo,timing,rfidstream"/> <file value="prrfid.log"/> <filter value="7"/> <format value="$h:$m:$s ($l:$L) [$i] > $M\r\n"/> </log> </rfid> </pr> </default>`

rfid/pref_ext_ds	Integer F / R / W	**0** min: -1 max: 2	This property controls the priority of document signer certificates Cert.DS during the checking process: If **0**, the checking process is executed with the file in the RFID chip first. If **1**, the checking process is executed with the external certificate first. If **-1**, the checking process is executed only with the file in the RFID chip. If **2**, the checking process is executed only with the external certificate only.
rfid/try_bac	Boolean F / R / W	False	If set to **1**, all errors are assumed as BAC error message upon trying to access the document. This property is specially developed to read RFID information from those non-standard documents that return other error message than "Command not allowed security status not satisfied" when the RFID chip is accessed.
rfid/use_serial_port	String F / R / W		Obsolete. Internal property.
rodata_dir	Path R		Path to read only data directory. • on Windows systems: `System32\gx\pr` • on Linux systems: `/usr/share/gx/pr`
rwdata_dir	Path R		Path to read/write data directory. • on Windows systems: `ProgramData\gx\pr` • on Linux systems: `/var/gx/pr`
save_cleanovd	Boolean F / R / W	False	Black OVD image is saved in the ZIP file.
save_cleanuv	Boolean F / R / W	False	Enhanced UV image is saved in the ZIP file.
save_fieldimage	String F / R / W		List separated by commas with codes of fields. Corresponding pictures of those fields are to be individually saved to the document file.

testdoc_mode	Integer F / R / W	**0**	Internal property.
twain/devno	Integer F	**0** min: 0 max: 8	Ordinal number of the device to use.
twain/docview	Boolean F	False	To scan cropped and rotated image.
twain/feeder_mode	Integer F	**0** min: 0 max: 1	**Possible values**: **0** – It is enough to just move the document to repeat the scanning. **1** – The document must be removed to repeat the scanning.
twain/light	String F		The name of the light to scan.
twain/window	Integer F	**1** min: 1 max: 2	The ordinal number of the window to scan from (numbered from 1).
update_licenses	Integer F / R / W	**1** min: 0 max: 3	Upon connecting to the device, the system is able to upload the licenses automatically. **0** – The automatic update is turned off. **1** – The automatic update always runs. **2** – Always runs, but upon successful update it voids the property in the .dat file. **3** – Only if "licupd.txt" file is present in the license_path or rwdata_dir path. Upon successful update, it deletes the file. The file can contain a request date in YYYYMMDD format, thus former licenses also can be uploaded.

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

uvwarm_quality	Integer F / R / W	**0** min: 0 max: 1000	This property is applicable only for PRM, CLR and PRMc devices equipped with UV tubes. Although, acceptable images can be captured with less warming time, the best image quality is achieved when the UV tubes are warmed up completely. The necessary warming quality can be controlled by the **uvwarm_quality** property in range of 0 to 1000. If the quality is set to 1000 and the tubes are cool, it takes 25 seconds to capture an UV image. If the UV tube warming task is set in the freerun mode and the **uvwarm_quality** property is set as well, the system waits for the UV tube to warm up before the first capture and the warmed state of the UV tube is continuously maintained between consequent captures.

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

19.1.1. PR 2.1 SDK PROPERTIES

The following properties can only be used in the **Pr 2.1 SDK**.

In the new SDK these properties are set automatically or via methods.

Important!

Do not set these properties from the **Pr 2.2 SDK**.

Property Path and Name	Value type/ Accessibility	Default Value	Description
api_version	String R		Returns the api version.
async_callback	Boolean F / R / W	False	The user implemented callback function has to be registered with the **SetEventFunction**. If the capture is started asynchronously by the **CaptureStart** function, then the callback function is called only while the **CaptureStatus** or the **CaptureWait** functions are called. This behavior can be changed with the **async_callback** property. Use this property with precaution because user programs might hang up in case of calling Windows functions from an internal capture thread that doesn't own a message queue.
document/ mrz_quality_check	Boolean F / R / W	False	If this property is set to **1**, then the quality of the MRZ line is checked and the results are saved into a variant. If **0**, then no checking is executed.
document/ ocr_version	String R		Returns the engine version. When starting the system or changing the engine, the new engine only loads at the first use. This property can be used to make the engine load earlier.
document/ test_fibres	Boolean F / R / W	True	Runs UV fiber search algorithm for unknown documents during **Recognize**.

event_types	Integer F / R / W	**0** min: 0 max: 15	There are two main event sources in the PR system: the **directly called processes** like the capture process, which can raise events to report their progress and the **parallel running freerun mode tasks**, which can raise events to report state changes like document detection or button testing. The raised event can be filtered with the **event_types** property. The event type values are defined in the PR_EVENT enumeration as well as the event values. Events in the PR system are arranged into groups. A bit signals a group. In the first group, there is only one event while the second group contains the rest of the events. There are three different types of events: **LED**, **capture** and **I/O**. Elements between **100** and **199** are **capture events**. Elements between **200** and **299** are **I/O events**.
fg_fail_mask	Integer R		List of finger positioning failures. The **FPS_FAILURE** enumeration contains its error flag bits.
freerun_mode	Integer F / R / W	**0** min: 0 max: 0x3f	Between two capturing processes the light and camera control modules are in a so called **freerun** mode. In this mode the system can run a set of the following tasks that the user can enable through the **freerun_mode** property: **UV tube warming** – for better UV image quality. **Motion test** – for autostarting the capturing process. **Lighting for preview capture** – for low resolution real-time preview capturing. **NOTE**: Certain combinations can be combined. E.g., 3 or 6. **Possible values:** **0** – Disable freerun activity. **1** – Direct controlled lights for real-time preview image capturing. **2** – UV tube warming control. **4** – Lights controlled by the HW/SW object motion detection algorithm.

rfid/selected_files	String F / R / W		Contains ID codes of the RFID files separated by space. It is used when the file identification parameter of the RFID file reading method is set to "Selected".
trigger_event	Integer W	**0**	Triggers an event. Not all the event can be triggered. Connection 1<<9 MotionDetection 1<<6 Power 1<<8
use_virtual_light	Integer F / R / W	**0** min: 0 max: 2	Enables the usage of the photo camera as "photo light" and OVD visualization on the scanned images.

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

20. DATA FIELDS

The Passport Reader system returns all OCR, RFID, barcode and basically all kinds of results as fields. For better understanding, this document classifies fields into four logical groups:

- General data fields: results of OCR, barcode-, and RFID reading processes
- Authentication fields: results of optical and RFID authentications
- Document type identification fields: data returned from the OCR engine database
- Image only fields that contain biometric data

20.1. FIELD VALUE

Most fields have textual values of three kinds: **raw**, **formatted** and **standardized**. It varies which value a field may contain. Even all three values can be available for the same field.

The following table will show you some typical examples. The detailed explanation can be found in the subchapters.

	Basic	Raw	Formatted	Standardized	Best
IssueCountry	SI<	SI<	SI	SVN	SVN
BirthDate	9201154	9201154	19920115	1992-01-15	1992-01-15
Authenticity 11	750		750	750	750
Name	KARPATI<<VIKTORIA<<<<<	KARPATI<<VIKTORIA<<<<<	KARPATI VIKTORIA		KARPATI VIKTORIA

20.1.1. RAW

Raw: as it is read, including checksum and filler characters. Raw value is empty when the data of a field is not read but produced logically e.g., VIZ authentication field and Document type identification fields.
In the above example for Raw value: the checksum of the birthdate is 4.

20.1.2. FORMATTED

Formatted: value without checksums and filler characters. Authentication fields and Document type identification field values are available in formatted form. The values of the authentication fields are in thousandths.

20.1.3. STANDARDIZED

Standardized: Using a standard, the field is converted to a format to ease further processing of data. Such format is document type independent thus can be compared to other documents and/or converted to other forms easily.

20.1.4. BASIC AND BEST

For getting data in any available text format, we introduced two format concepts called **Basic** and **Best**. When the **Basic** value is queried, the returned value is the least modified format: the first that is available in order of raw, formatted and standardized values. The **Best** value uses the opposite logic of selection. It returns the most processed format: the first that is available in order of standardized, formatted and raw values.

20.1.5. BINARY

If the value of a field cannot be converted into text (e.g., 2D barcode data or RFID face photo image file), it is returned as a **binary** value.

20.1.6. NO VALUE

Image only fields e.g., "VIZ Face" has no value.

20.2. OTHER

20.2.1. AMID

AMID refers to "Authentication Method Identifier" that is detailed in BSI TR-03135, section "spectrally selective check routines". The purpose of AMID is to describe all optical authentication fields.

21. ENCRYPTED SAVING

From pr-2.1.11 version the user specific file can be set for encrypted saving. In such case the encrypted file cannot be decoded with the ADAPTIVE RECOGNITION key.

> **Note**
>
> If you want to save encrypted files which can only be decoded in ADAPTIVE RECOGNITION's network, then, when saving the file in Full Page Reader or Authentication Checker application select .ecz extension and do not set anything else. This setting applies to autosave too.

21.1. KEY GENERATION

Key pair can be generated from command line by issuing the `ssh-keygen -b 4096 -f keyfilename -N ""` command. This command creates two files:

- The .pub extension file is the **public key**.
  This file can be copied and shared, even through the Internet.
- The file without extension is the **private key**.
  The encrypted files can be decrypted with the private key.

> **Note**
>
> The private key must be kept safe. Do not share it!

> **Note**
>
> The user key must be of RSA type with a key length of minimum 4096 bytes.

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

21.2. PROCESS OF THE ENCRYPTION

There are multiple options to give the public key in the SDK. The certificate containing the key can be loaded from the memory as is used at the ecard handling (Certificates.Load() method). Then, the returned key ID number must be handed over to "**rfid/encryption_key**" property.

> Note
>
> For more information on property use and setting property values, please check the Passport Reader Property List chapter.

> Note
>
> The Certificates.Load() method only works as programmed in source code. Otherwise, the filename must be entered.

If the key is stored in file, the path of the file can be set in the property as well. Thereby, the new key can be set through the gxsd.dat file in any program which can save encrypted files.
For ease of use, not only the certificate file but the ssh public key file can be given as well. (Single line ssh key file and ssh2 file are also suitable.) However, these files cannot be loaded with the Certificates.Load() method.

21.3. PROCESS OF THE DECRYPTION

For decryption, the prdecrypt command line program is given by ADAPTIVE RECOGNITION.

> Note
>
> The prdecrypt program is located in:
>
> - **C:\Program Files\Adaptive Recognition\utils\prdecrypt** or
> - **C:\Program Files (x86)\Adaptive Recognition\utils\prdecrypt** folder.

The file containing the private key must be handed over to the program. When starting the program without parameters, the following text is displayed:

```
usage: prdecrypt encryptedfile keyfile [outputfile]
```

Meaning:

`encryptedfile` – name of the encrypted file

`keyfile` – name of the private key file

`outputfile` – name of the extracted file (optional)

First, specify the name of the encrypted file as a parameter. Then, specify the name of the private key file as well. Optionally, the name of the extracted file can be specified too.

> Note
>
> The program does not manage password protected private key files.

The file format of the private key can be the following:

- PKCS #1 RSA PRIVATE KEY
- PKCS #8 PRIVATE KEY
- OPENSSH PRIVATE KEY
- putty ppk file

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

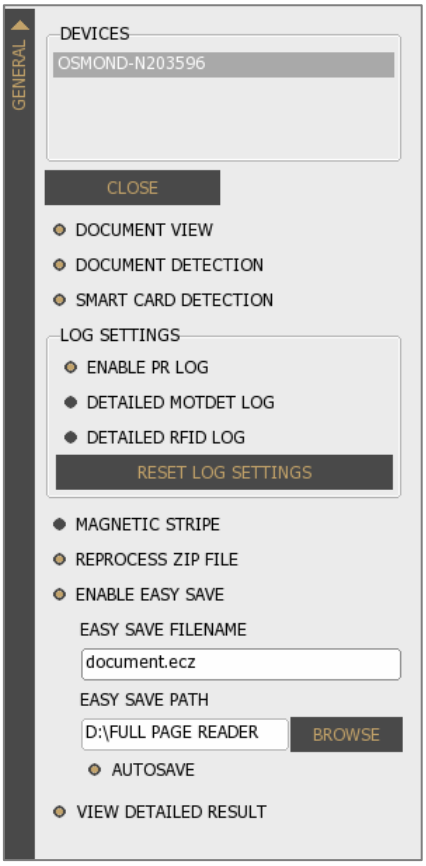
21.4. ENCRYPTED AUTOSAVE

This section provides a short description on how to save scanning results as encrypted files in the Full Page Reader and Authentication Checker applications.

21.4.1. ENCRYPTED AUTOSAVE IN FULL PAGE READER

In order to save the scanned data as encrypted file in Full Page Reader, turn on "**ENABLE EASY SAVE**" and "**AUTOSAVE**" options at "**GENERAL**" layer.

Then, enter a desired filename with **.ecz extension** and the path where the file will be saved.



Note

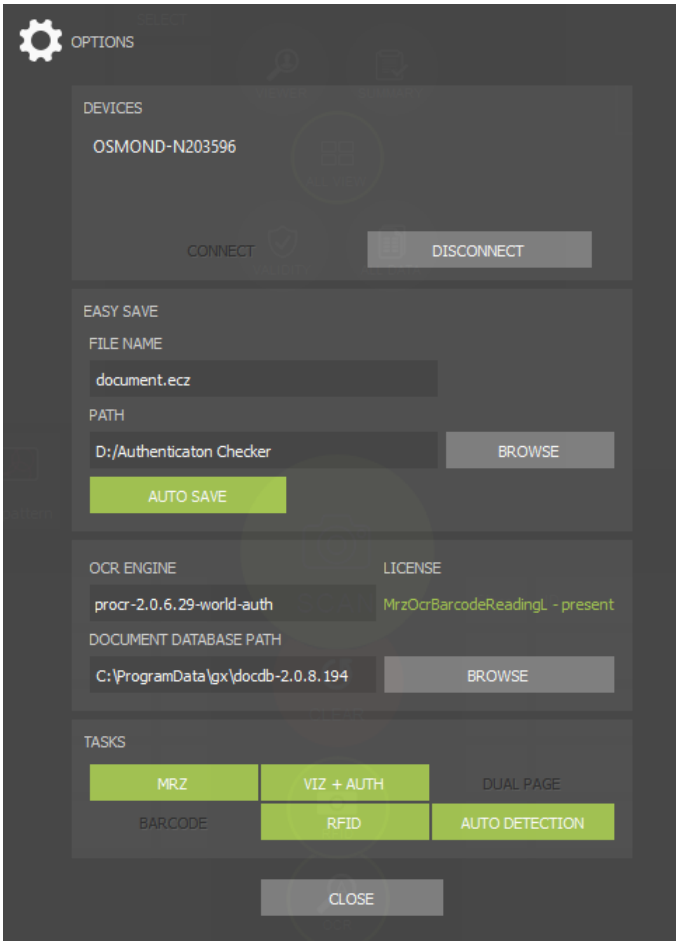
To make Full Page Reader write the same file during every reading, give a constant name of the file. **Do not use** any field name like "%DOCUMENT NUMBER%".

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

21.4.2. ENCRYPTED AUTOSAVE IN AUTHENTICATION CHECKER

In order to save the scanned data as encrypted file in Authentication Checker, turn on "**AUTO SAVE**" at "**OPTIONS**" menu.

Then, enter a desired filename with **.ecz extension** and the path where the file will be saved.



Note

To make Authentication Checker write the same file during every reading, give a constant name of the file. **Do not use** any field name like "<Counter>".

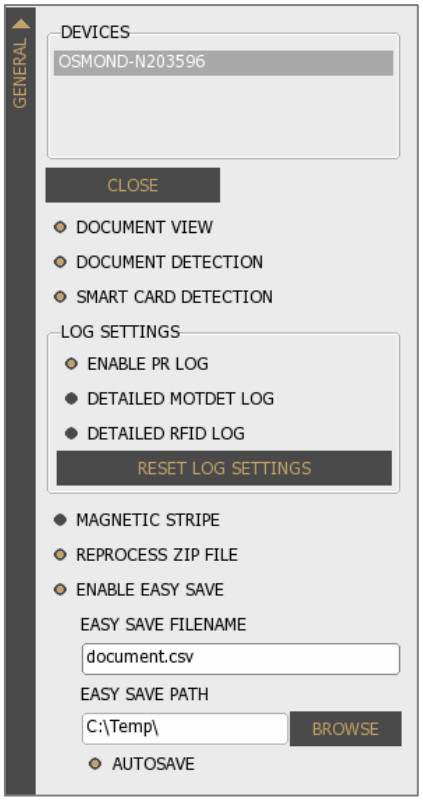
22. FULL PAGE READER – SAVING IN CSV FORMAT

This chapter provides a short guide how to save scanning results in CSV format in Full Page Reader application.

22.1. SETTINGS

In order to save the read data into a CSV file, you need to turn on "**ENABLE EASY SAVE**" and "**AUTOSAVE**" options in Full Page Reader's "**GENERAL**" layer.

Then, give a desired file name with **.csv extension** and the path where the file will be saved.



> **Note**
>
> To make Full Page Reader write the same file during every reading, give a constant name of the file. **Do not use** any field name like "%DOCUMENT NUMBER%".

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

22.2. CSV STRUCTURE

With the above settings, the Full Page Reader will generate the set CSV file. If the file already exists, it will append each scanning result to it.

In the headline of the CSV file, there are keywords which represents the field type of the particular column.

C13

	A	B	C	D	E	F	G
1	DOCUMENT NUMBER	TYPE	ISSUE COUNTRY	ISSUE PLACE	ISSUE DATE	EXPIRY DATE	ISSUE ORG
2	BH0002918	P	Hungary			1/1/2022	
3							
4							
5							
6							
7							
8							
9							

These headers are freely changeable or removable, so you can create a template which contains only the desired type of data in given order.

D13

	A	B	C	D	E	F
1	GIVEN NAME	SURNAME	NATIONALITY	EXPIRY DATE	BIRTH DATE	EXPIRY DATE
2						
3	ROZALIA	SPECIMEN	Hungary	1/1/2022	2/22/1978	1/1/20
4						
5						
6						
7						

23. FIRMWARE MANAGEMENT

In order to get the most out of your Osmond and have the latest fixes and modifications, it is recommended to have the latest firmware applied on your reader.

The main purpose of this section is to provide a short guide on the firmware update of Osmond devices (USB and network models).

The following options are available for performing a firmware update:

1. In case of **USB** devices:
   - The firmware of the Osmond USB device can be updated with MSI installer. For more information on this, see Firmware Installation with Updater MSI chapter.

2. In case of **Network** devices:
   - The firmware of the Osmond N device can be updated with MSI installer. For more information on this, see Firmware Installation with Updater MSI chapter.
   - In case of performing the firmware update on a larger quantity of scanners and an operating update server owned by the customer is at disposal, we can provide the required update file which can be sent to the given devices through the update server. For more information on it, contact ADAPTIVE RECOGNITION support team.
   - In case of a larger quantity of scanners without an operating update server, the device can download and install the required update file automatically, from the default AdaptiveRecognition update server ("update.adaptiverecognition.com") via web interface. Note, that the given device(s) must have access to this update server. For more information on it, contact ADAPTIVE RECOGNITION support team.

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

23.1. FIRMWARE INSTALLATION WITH UPDATER MSI

Note

This functionality is available for Osmond USB (R, L models) and network (N model) devices as well.

In this section the firmware installation and update of Osmond devices with MSI installer will be discussed.
The firmware is available on the ADAPTIVE RECOGNITION website where the latest firmware version can be checked and downloaded. After downloading the firmware, follow the installation steps described in this chapter.

In order to update your Osmond device as easy as possible, ADAPTIVE RECOGNITION provides you the latest firmware in MSI format. The MSI can be applied to USB devices (R and L models) and network devices (N model) as well.

Note

Only one Osmond can be updated at the same time on one PC. Before updating another reader on the very same PC, please uninstall the Osmond Updater MSI. After connecting another reader, install it again.

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

23.1.1. REQUIREMENTS

For the update process, you will need a USB A to C cable and a Windows PC which has at least 2.1.9.5 driver package preinstalled.

> **Note**
>
> If you do not have any of our USB driver package, please contact our technical support team for the download link.

If you have all the required components, please connect your Osmond device to the PC and turn it on.

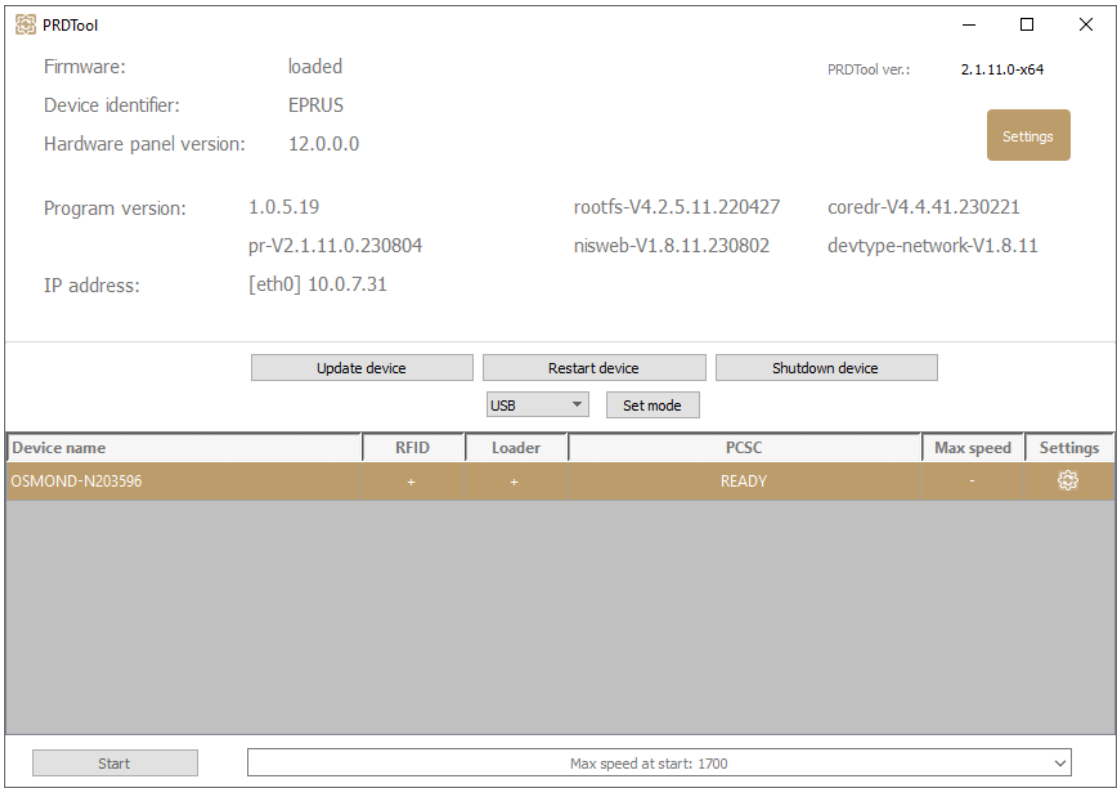
Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

23.1.2. THE UPDATE

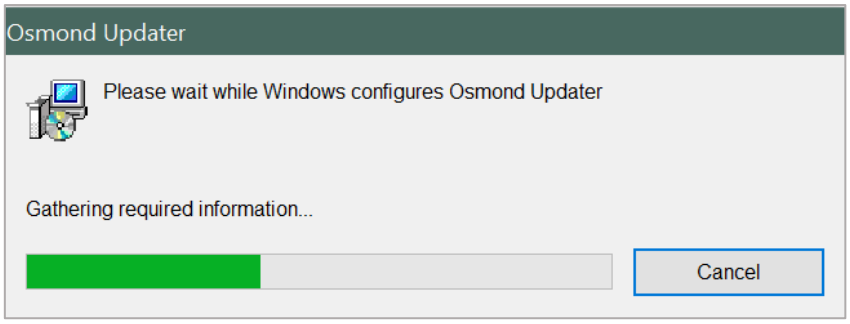
After the device boots up, please check with the "**C:\ProgramFiles\Adaptive Recognition\utils\PRDTool\PRDTool.exe**" utility tool whether the connection was established successfully.

> **Note**
>
> The **PRDTool** is installed alongside the Passport Reader software, and can be found in one of the following folders:
>
> - **C:\Program Files\Adaptive Recognition\utils\PRDTool** or
> - **C:\Program Files (x86)\Adaptive Recognition\utils\PRDTool**.

You should see the following information on your device upon successful connection (note that the version numbers might vary by reader):



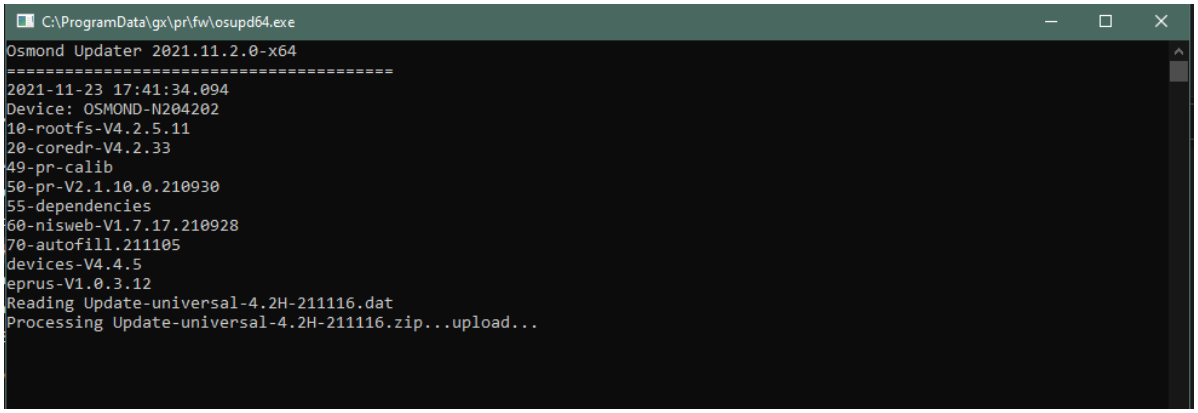
If the device has connected, please launch the "**OsmondUpdater yy.mm.n.msi**" in order to update the reader.

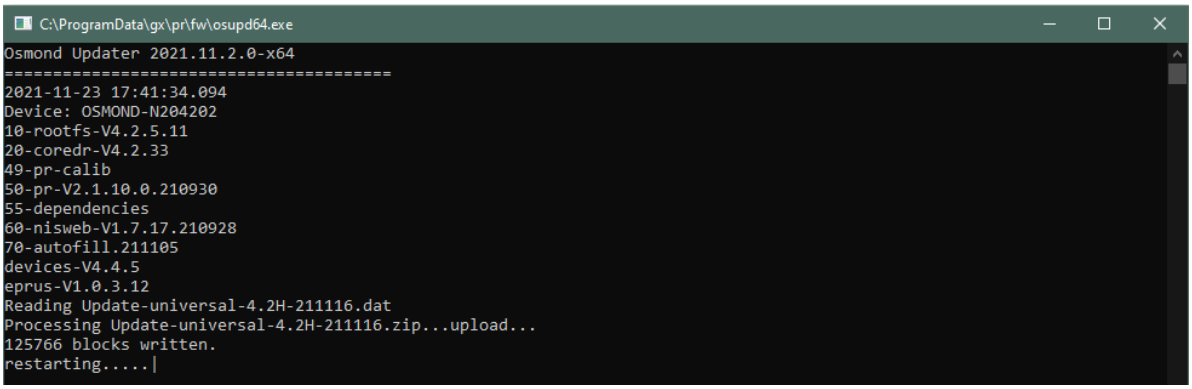


After the updater application is installed on the PC, the update process is started automatically.

> **Note**
>
> If your device already has the latest firmware version, the installer will stop without installing the firmware, and create a log file under **C:\ProgramData\gx\pr\fw** folder.

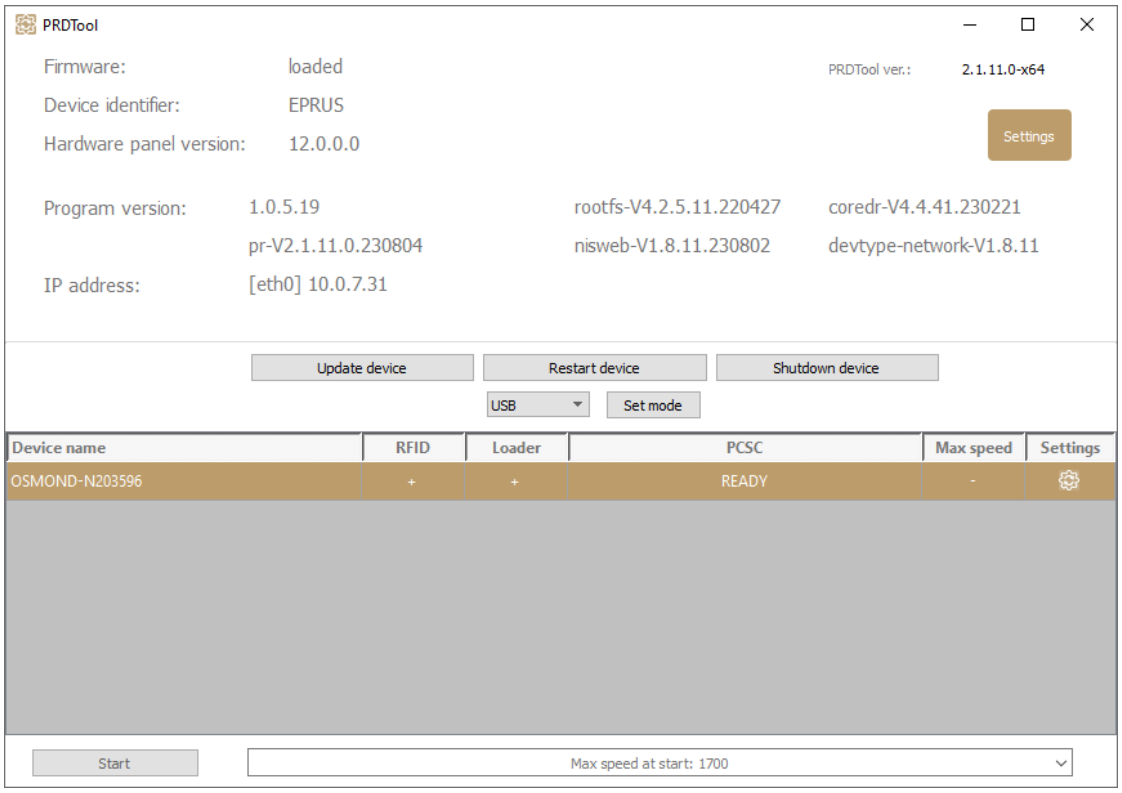
The reader will be updated automatically, and during the process you will see various information and the current state of the update in a console window:





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

During the update, **the device will be restarted two times**. After the process finishes, please check with the PRDTool whether you see an appropriate firmware version:



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

23.1.3. STATUS ICONS

While the update is in progress, you will see the following status icons on the OLED screen of the device.

DISPLAY ICON	STATUS NAME	STATUS DESCRIPTION
	File transfer	The firmware file is transferring
	In progress	Firmware update is in progress
	Update OK	Firmware update finished successfully
	Update error	Firmware update failed

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

24. NETAPI (NAI MODE)

The NetAPI is the network version of the Passport Reader SDK. Its interface implements WebSocket communication with JSON-RPC format packages. This WebSocket channel is either provided by an Osmond N network device (in NAI mode) or by the NetAPI service (prwebsrv) running on PC.

The NetAPI is designed to control remote Osmond N devices via Ethernet connection as well as Windows/Linux connected legacy USB document scanners from not natively supported operating systems.

Additional uses:

- It supports running UWP programs on Windows via localhost connection.
- It helps to optimize memory usage by balancing load between client and server.
- The Passport Reader software package includes a NetAPI client that allows accessing all supported document reader devices through the conventional SDK as well.
- The standalone version of the .NET interface can be operated without the installation of the PR system as well.

Note

This chapter provides information on how to set up NetAPI on Osmond N as well as describes the server and client setup.
The sample code (SDK) is available in the "sdk" folder of the PR Software Package or it can be downloaded from the ADAPTIVE RECOGNITION website.

24.1. SETUP ON THE OSMOND N DEVICE

1. Create a user with "NAI user" role in the web interface in the ADMINISTRATION / USERS menu. Only one user can be logged in at the same time.

2. Upload a HTTPS certificate in the NETWORK / WEB SERVER menu. NetAPI operates via HTTPS communication only.

> **Note**
>
> Upload HTTPS certificate to Osmond device and check your browser if secure connection is established with the web interface.

3. Set the operating mode of the device to "NAI" mode in the MAINTENANCE / OPERATING MODE menu.

4. The NetAPI is accessible via the same port number as the web interface.

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

24.2. SETUP SERVER ON PC

1. Create a NetAPI user with the PRDTool program. The user needs admin or user role. Maximum 5 users can be logged in at the same time in order to use several connected devices. The user sessions can be managed with admin role.

2. The operation parameters can be set with the PRDTool program:
   - Port number (default: 8000)
   - SSL certificate file and SSL private key file for encrypted communication
     If the encrypted communication is configured, the server cannot be accessed without encryption.
   - Enable external access
     If enabled, the server accepts requests from other devices. Otherwise, communication is restricted to localhost.
   - RFID certificate folder
     The path comprising files required for Passive and Terminal Authentications

3. The NetAPI service is realized by the prwebsrv program that can operate as a Windows service or Linux daemon. The server can be turned on/off with the PRDTool program as well.
   On Windows, the service state can be queried from command line with the `prwebsrv --svc-query` command. If the program is executed in foreground with the `prwebsrv --showlog` command, it displays the communication packages to assist developer.

4. The configuration files - prwebsrv.json and the webusr.json - can be copied freely between computers. Uninstalling the Passport Reader software package removes these files.

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

24.3. SETUP CLIENT

The NetAPI client is part of the Passport Reader software. In order to use it, set the following properties within the default/pr node in the gxsd.dat file manually, or by your client program:

- ipdev/url – Server IP address (or domain name) and port number.
- ipdev/user – Username.
- ipdev/password – Password. Not recommended, but possible to set it in the gxsd.dat file.
- ocr_module – OCR tasks can be performed on client side or on server side. Set this property to `procr-ip` to perform OCR on server side. If the server and the client are on the same PC (localhost connection), do not apply this setting in the gxsd.dat file.

Note

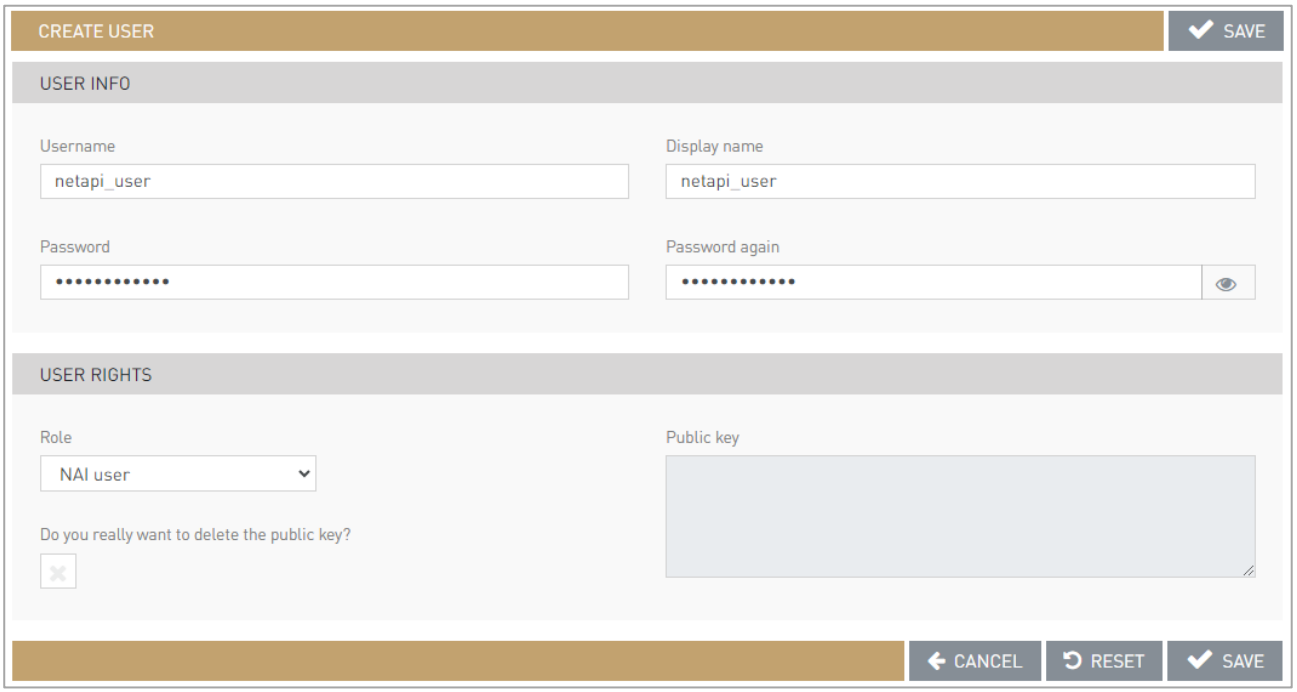
The gxsd.dat file is located in the "C:\Programdata\gx\" folder.
When editing gxsd.dat, use a text editor, e.g., Notepad++.

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

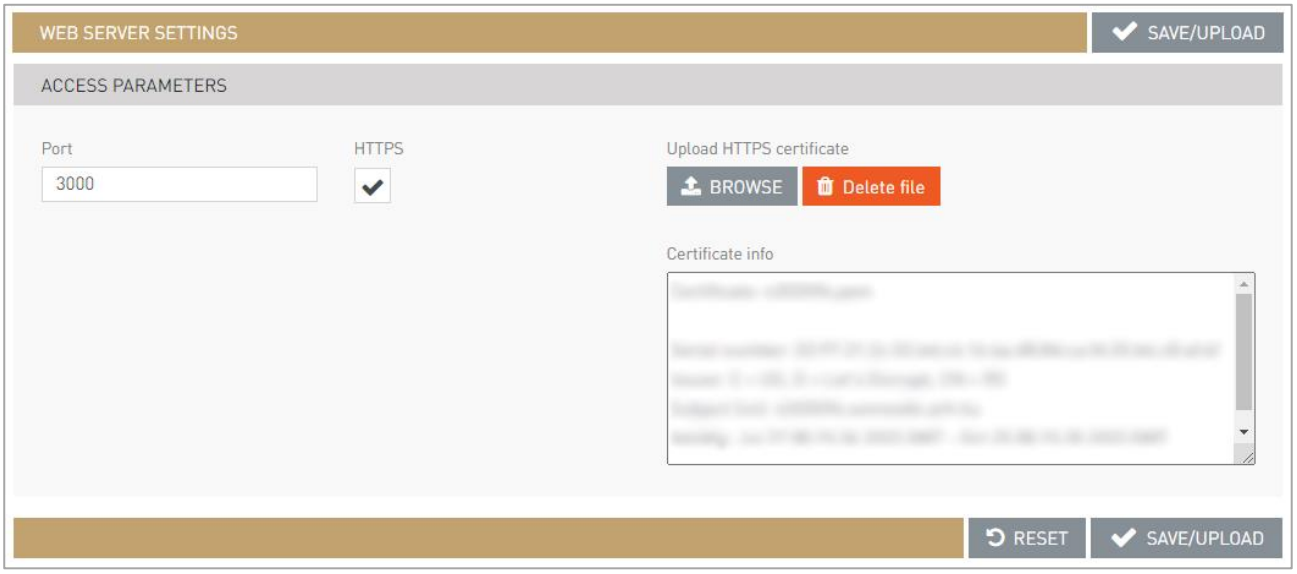
24.4. USING FULL PAGE READER WITH OSMOND N THROUGH NETAPI

Users have the possibility to use the Full Page Reader application through NetAPI. In this section the necessary steps to acquire this function will be described.

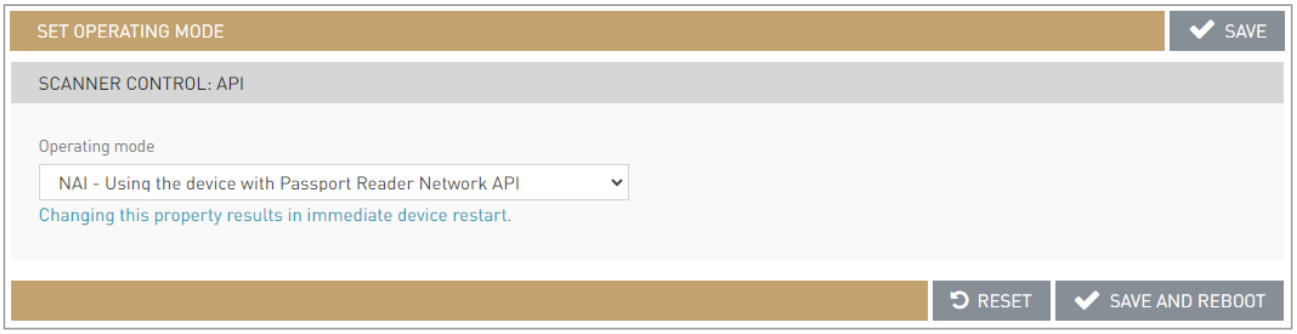
1. Sign in to the web interface of the Osmond N device.
2. Create a user with "NAI user" role in the web interface in the ADMINISTRATION / USERS menu. Only one user can be logged in at the same time.



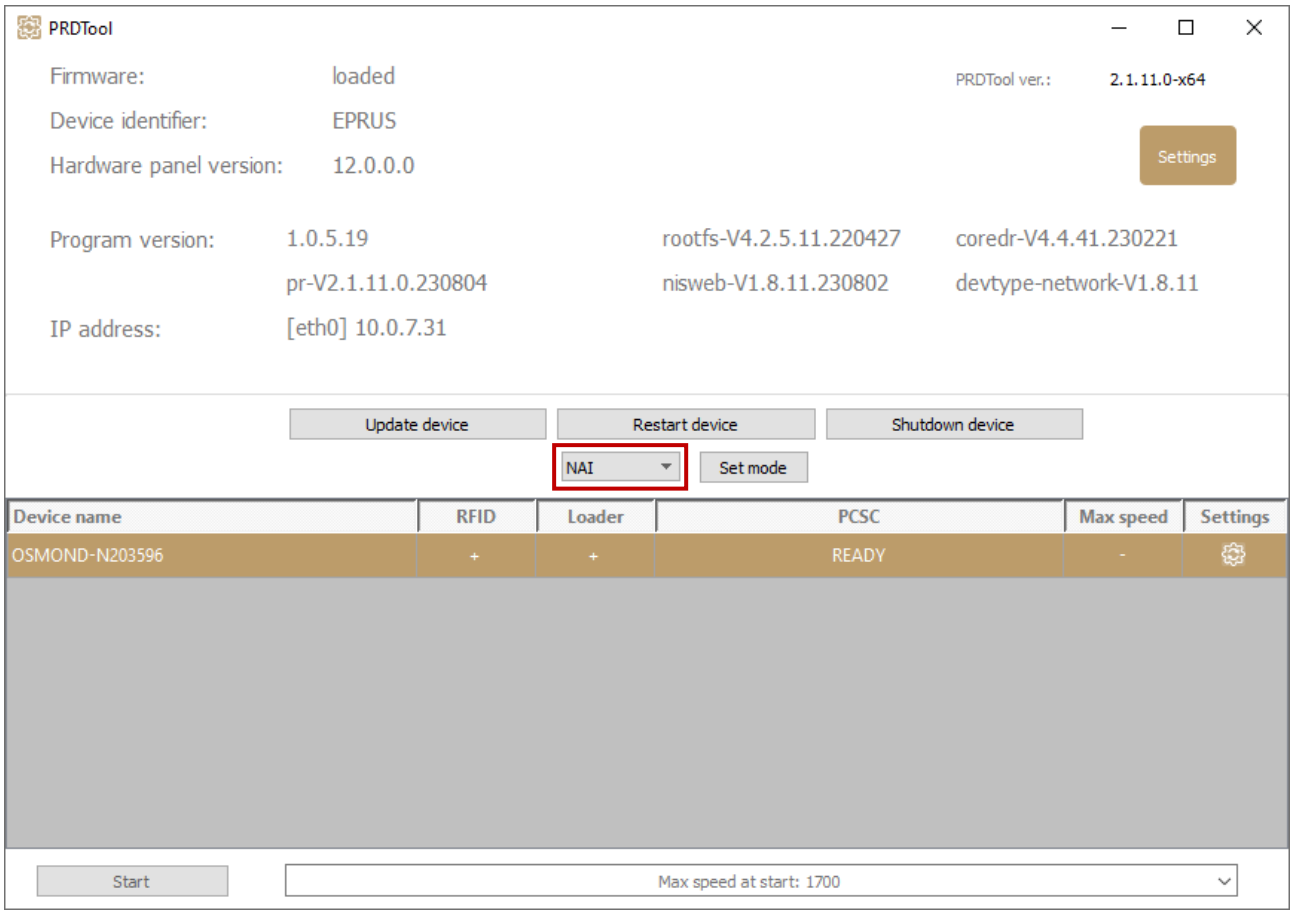
3. Upload a HTTPS certificate in the NETWORK / WEB SERVER menu. NetAPI operates via HTTPS communication only.



4. Set the operating mode of the device to "NAI" mode in the MAINTENANCE / OPERATING MODE menu.



5. Afterwards, open PRDTool.
6. In PRDTool check the mode of the device. It must be in **NAI** mode.



7. Navigate to **ProgramData/gx** hidden directory on Windows.
8. Open the **gxsd.dat** file.
9. Extend the gxsd.dat file with the appropriate user data in place of the blue highlighted text, according to the following example:

```
<pr>
.
.
.
   <ipdev>
         <url value="10.0.7.31:3000"/>
         <user value="netapi_user"/>
         <password value="netapi_password"/>
   </ipdev>
.
.
.
</pr>
```

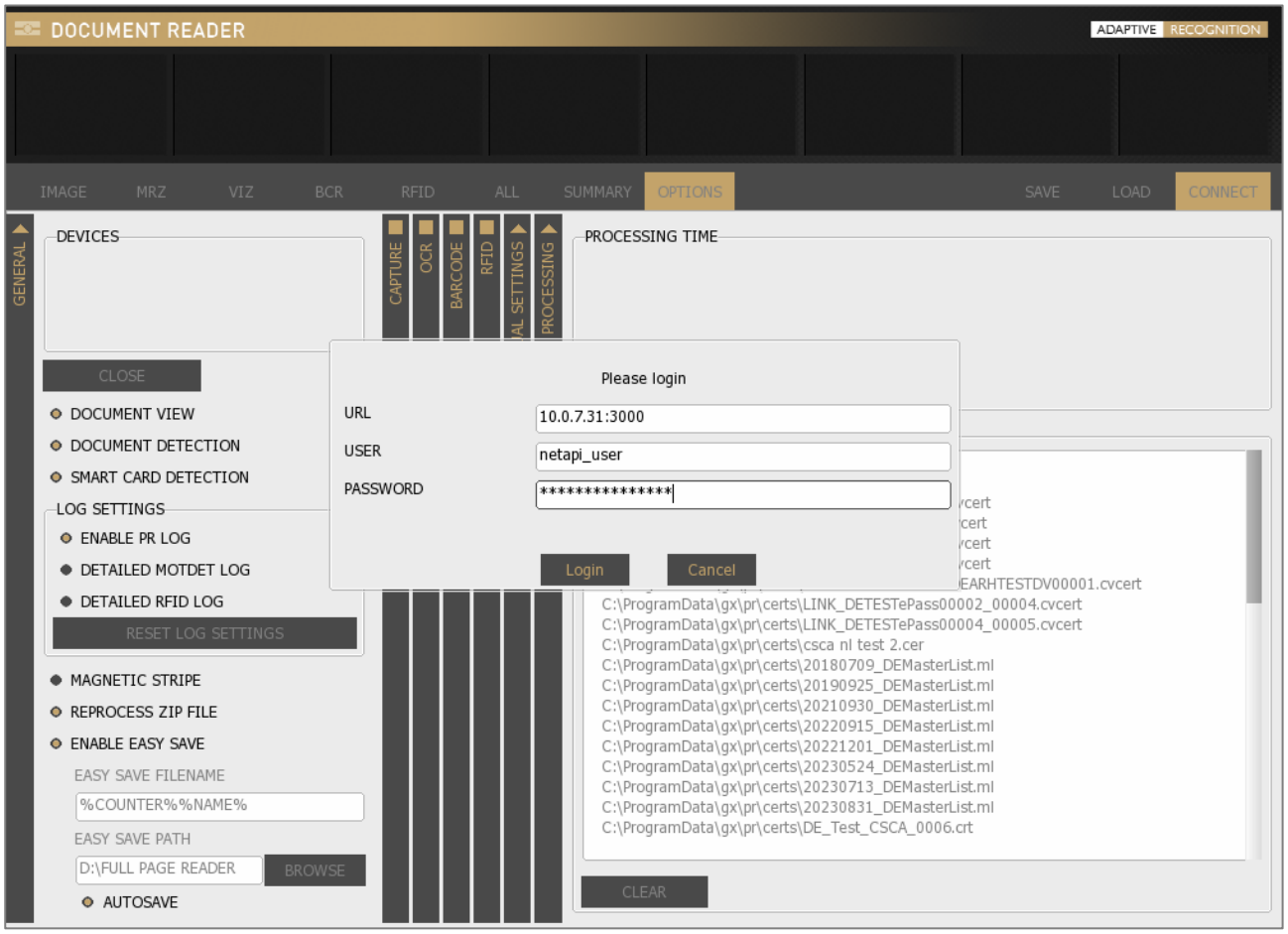
> **Note**
>
> The **URL value** consists of the **IP address** and the **port number**.
> In case of **Osmond N** devices, the IP address is displayed in the PRDTool at the IP address section. The port number is the same as the value found at the web interface.

> **Note**
>
> When editing the **gxsd.dat** file, pay attention to type between the <pr> and </pr> elements.

10. Save the modifications.

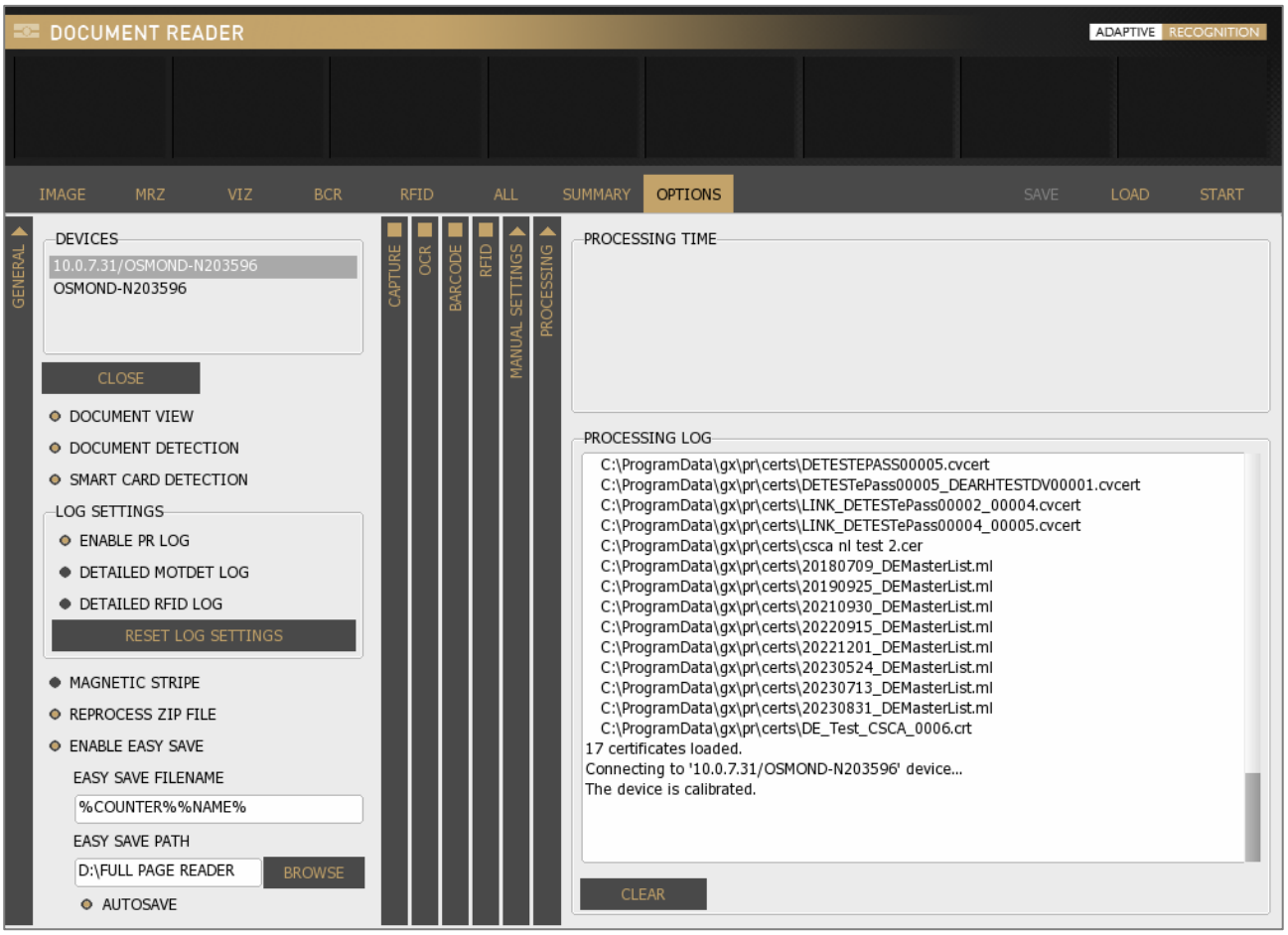
Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

11. Open Full Page Reader.
12. When the FPR application is opened, a login window pops up.
13. Enter the **PASSWORD** into this window.



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

14. After a few seconds, the device is calibrated and ready to be used in NetAPI mode.



25. NETWORK WEB APPLICATION API (NWA MODE)

The Network Web Application API is designed to provide a tool for managing main network interface functions remotely, without accessing device Web GUI from browser. The API includes functions for manipulating features like document scanning, package format, result upload protocol and queue. The API consists of HTTPS methods (POST, GET) described in a provided YAML file.
In order to ease integration into different systems, the Network Web Application API complies with OpenAPI specifications (https://www.openapis.org/) to enable generating code for numerous programming languages.

> **Note**
>
> The sample code (SDK) is available in the "sdk" folder of the PR Software Package or it can be downloaded from the ADAPTIVE RECOGNITION website.

25.1. REQUIREMENTS

25.1.1. HTTPS COMMUNICATION

HTTPS connection with Osmond device is required to use via Network Web Application API.

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

25.1.2. CREATE USER WITH NWA (NETWORK WEB APPLICATION API) ROLE

1. On your Osmond device web interface, navigate to **ADMINISTRATION / USERS** menu and click **[+NEW USER]**.
2. Specify user name and password (in the following sample: niswebapi_user and niswebapi_password).
3. Then, select the **NWA** role.
4. Click **[Save]**, then reboot device.
5. Once reboot is done, select the **NWA** mode in **MAINTENANCE / OPERATING MODE**.
6. Restart the device again.

25.1.3. GENERATING CERTIFICATES

> **Note**
>
> The following commands can be executed on Linux OS or Windows OS as well, if the openssl is downloaded.

Accessing the Osmond N device via Network Web Application API requires client-side certificate. This certificate must be trusted by the Osmond N device and is verified upon establishing secure connection.

Generating the necessary certificates:

- generating CA key:

  ```
  openssl genrsa -out CA-AR.key 4096
  ```

- generating CA certificate:

  ```
  openssl req -x509 -new -nodes -key CA-AR.key -sha256 -days 400 -out CA-AR.pem -subj "/CN=AR Root CA/C=HU/ST=Budapest/L=Budapest/O=AR"
  ```

At this point, send the **CA-AR.pem** to our support team. They create and send you an **update file**, that adds the sent .pem to the device trusted certificate list.

> **Note**
>
> For more information on the possible ways of update, please refer to the [Configuring HTTPS via Osmond device web interface] section.

- generating Network Web Application API client CSR:

  ```
  openssl req -new -nodes -out niswebapi_client.csr -newkey rsa:4096 -keyout niswebapi_client.key -subj "/CN=niswebapi_user/C=HU/ST=Budapest/L=Budapest/O=AR/OU=niswebapi"
  ```

> **Important!**
>
> The CN field must contain the username of the NWA user.
> The OU field must be "niswebapi" in all cases.

- signing CSR with CA certificate:

  ```
  openssl x509 -req -in niswebapi_client.csr -CA CA-AR.pem -CAkey CA-AR.key -CAcreateserial -out niswebapi_client.pem -days 300 -sha256
  ```

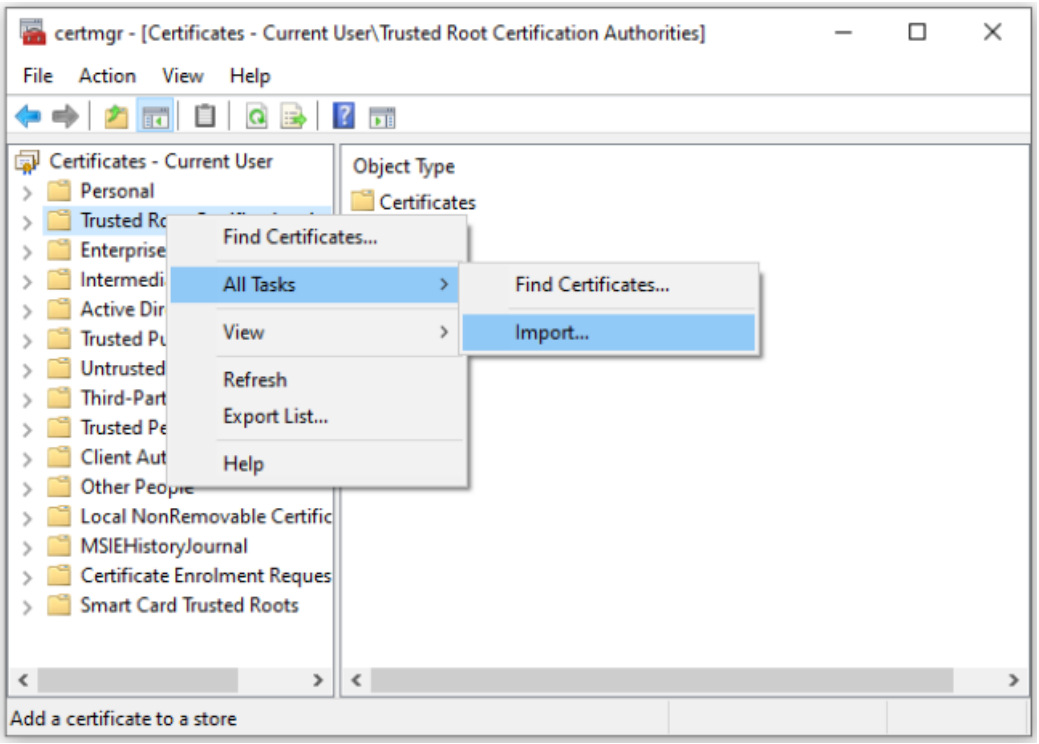
25.1.4. IMPORTING CERTIFICATES ON CLIENT

The OSMOND N HTTPS certificates (R3, osmondn*****.domain.company. hu e.g., osmondn211785.osmondn.arh.hu) must be added to the trusted certificate list of the client PC. For exporting the Osmond HTTPS certs, visit its login page and export the certificates via browser. The exact steps of export depend on the type and version of browser.

– The certificates can be imported using the following commands (Linux OS):

```
sudo cp R3.crt /usr/local/share/ca-certificates/R3.crt
sudo cp n211785.osmondn.arh.crt /usr/local/share/ca-certificates/
osmondn211785.osmondn.arh.crt
sudo update-ca-certificates
```

– On Windows, you can use the **certmgr** console for importing certificates by selecting the "**Trusted Root Certification Authorities**" folder.



25.1.5. INSTALLING PYTHON DEPENDENCIES

```
pip install six
pip install python-dateutil
pip install urllib3
pip install pydantic
```

25.1.6. CONFIGURING AND RUNNING THE PYTHON DEMO

Open the openapi_demo.py with an editor and change the following parameters to suit your environment:

```
api_server_host = " osmondn211785.osmondn.arh.hu"
api_server_port = 3000
```

> **Note**
>
> In order to address your device like devicename.subdomain.domain.hu, it must be configured in your DNS. E.g., OSMOND-N212888.osmondn.mycompany.com.

For running the python demo, the followings are necessary:

- niswebapi_client.pem (niswebapi client certificate)
- niswebapi_client.key (niswebapi client private key)
- openapi_demo.py (demo program)
- OPTIONAL: openapi_client directory (code generated by OpenAPI generator)

Running the Demo: `python3 openapi_demo.py`

25.2. SUPPORT FOR OTHER LANGUAGES

Using the openapi-generator-cli program, the Network Web Application API client code can be generated for other languages as well. The list of supported languages can be retrieved using the `openapi-generator-cli list` command.

Sample list: `- ada - android - apex - bash - c - 4 clojure - cpp-qt-client - cpp-restsdk - cpp-tiny (beta) - cpp-tizen - cpp-ue4 (beta) - crystal (beta) - csharp - dart - dart-dio - eiffel - elixir - elm - erlang-client - erlang-proper - go - groovy - haskell-http-client - java - java-helidon-client (beta) - java-micronaut-client (beta) - javascript - javascript-closure-angular - javascript-flowtyped - jaxrs-cxf-client - jetbrains-http-client (experimental) - jmeter - julia-client (beta) - k6 (beta) - kotlin - lua (beta) - n4js (beta) - nim (beta) - objc - ocaml - perl - php - php-dt (beta) - powershell (beta) - python - r - ruby - rust - scala-akka - scala-gatling - scala-sttp - scala-sttp4 (beta) - scalaz - swift-combine - swift5 - typescript (experimental) - typescript-angular - typescript-aurelia - typescript-axios - typescript-fetch - typescript-inversify - typescript-jquery - typescript-nestjs (experimental) - typescript-node - typescriptredux-query - typescript-rxjs - xojo-client - zapier (beta)`

Generating the client-side code is performed using the `openapi-generator-cli generate` command.

For more information on the generator visit https://openapi-generator.tech/docs/installation/.
For guidance on installation visit https://openapi-generator.tech/docs/usage/.

25.3. API FUNCTIONS

25.3.1. PR_CONTROL

It controls device-related functions like document scanning and uploading.

```
{
    "method": "autoScanNextStep | approveUpload"
    "params": "approve: true false"
}
```

25.3.2. GET_PR_CONFIG

Get main configuration parameters:

```
{
    "main-config/packageType" => ['zip', 'csv', 'pdf'],
    "main-config/scanMode" => ['Interactive','Automatic'],
    "main-config/communicationType" => ['no_store','local_database',
    'FTP', 'SFTP', 'FTPS', 'WebDav','SMB', 'SMTP', 'WS', 'WSS'],
    "main-config/autoSend" => ['approve', 'auto']
}
```

Note

For more information on the mentioned parameters and their values, click on the given link:

- Package Type (ZIP, CSV, PDF),
- Scan Mode (Autonomous, Interactive),
- Communication Type ("no store", "local database", WS, WSS, FTP, SFTP, FTPS, SMTP, SMB, WebDav),
- AutoSend (Auto, Approve).

25.3.3. SET_PR_CONFIG

Modify values returned by get_pr_config.

```
(Object:)
{
    result => ['1', 'FAIL']
}
```

25.3.4. PR_STATUS

Query scanning status and various settings of the web interface.

```
{
  "CURRENT_STATUS" => [(string)'0'..'3'] (enum RunningStatus {Sleep,
  Autonomic, Interactive, Load };),
  "CURRENT_PAGE" => [(string)'0'..MAX_PAGE_NUM],
  "MAX_PAGE_NUM" => [(string)'0'..'9'](idx setting),
  "READER_STATUS" => [(string)'0','1'],
  "READING_ENABLED" => [(string)'0','1'],
  "WAIT_FOR_CLICK_TO_READ" => [(string)'0','1'],
  "WAIT_FOR_CLICK_TO_UPLOAD" => [(string)'0','1'],
  "WAIT_FOR_MOVE_TO_READ" => [(string)'0','1'],
  "WAIT_FOR_MOVE_OUT" => [(string)'0','1'],
  "REMAINING_TIME_FOR_FLIP" => [(string)'0'..max_flip_time_config],
  "CONFIG_LOADED" => [(string)'0','1'],
  "DATE" => [(long int)] (Unix timestamp in seconds)
}
```

25.3.5. KEEP ALIVE

Usable to prolong the session.

```
{
    "keep_alive" => ['SUCCESS', 'FAILED']
}
```


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

25.3.6. QUEUE SUMMARY

Returns the number of items in queue.

```
[  {"active": [int]},
{"deferred": [int]},
{"corrupted":[int]},
{"predirect":[int]},
{"predelete":[int]} ]
```

25.3.7. QUEUE DELETED DEFERRED CORRUPTED

Delete all deferred and corrupted items from queue with a single command. The value "yes" deletes the content of the queue section.

```
{
    "is_delete_deferred_uploads":"yes|no",
    "is_delete_deferred_uploads": "yes|no"
},
```

25.3.8. QUEUE LIST

List items of the different queue sections.

```
{
    "queuename" => [string] (
        all
        active
        deferred
        corrupted
        predirect
        predelete )
}
```


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

26. PRDTOOL

PRDTool is a utility tool which is part of the Passport Reader software packages from version 2.1.9.1 and above. This program is for querying device information, as well as performing auto update configurations, NetAPI server settings and some low-level operations for PR devices connected via USB, especially for the Osmond device.

26.1. START PRDTOOL

- **Windows**

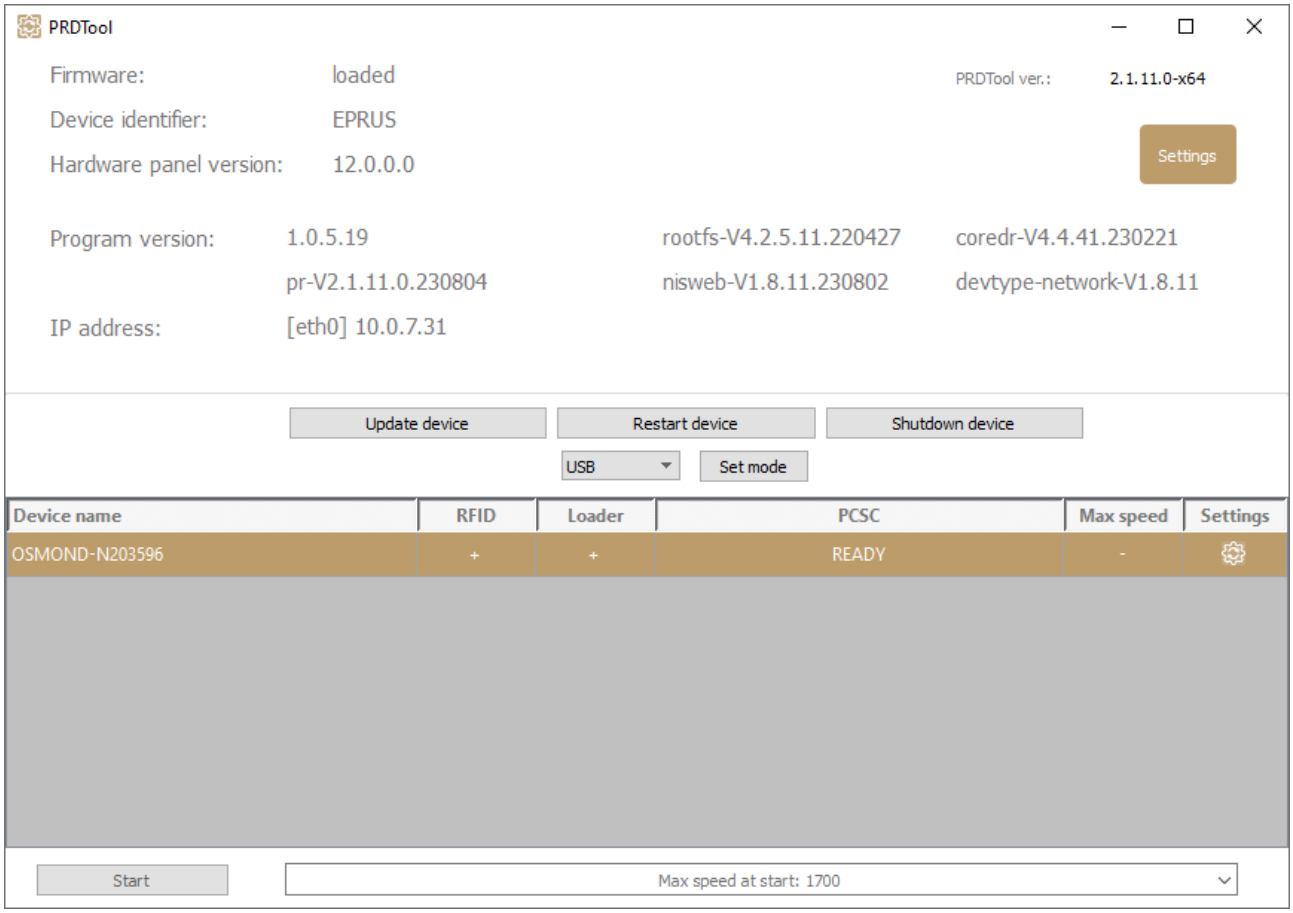
The PRDTool is usually located in **C:\Program Files\Adaptive Recognition\utils\PRDTool** or **C:\Program Files (x86)\Adaptive Recognition\utils\PRDTool**, depending on the architecture of the installed PR software.

- **Linux**

Depending on your distribution, you can open command terminal and insert: **PRDTool** or use dashboard search bar: **Linux Start menu > Applications > Adaptive Recognition Apps > PRDTool**.

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

Only one instance of the program is running. If the window is not opened on the desktop, then it can be found on the notification area. The program can only be closed through the pop-up menu of the notification icon. After launch, the devices connected via USB are displayed in a list located in the lower part of the window. To manage a given device, it must be selected from the list. Once it is selected, the firmware version information of the device appears. In case of a dual USB/Network interface device the IP address of the device also can be seen. This feature can be useful if the set address is forgotten or the address set by DHCP cannot be extracted in any other way.



26.2. OSMOND OPERATION MODES

Dual USB/Network interface Osmond devices have different operation modes:

- USB mode
- NAI (Network Application Interface - NetAPI) mode
- NWI (Network Web Interface) mode
- NWA (Network Web Application – Network Web Application API) mode

USB mode

In USB mode, the device operates as any other ADAPTIVE RECOGNITION passport reader. It can be used through our regular SDK, and with the Full Page Reader or Authentication Checker application as well.

NAI mode

In NAI mode the document reader device is used by the Passport Reader NetAPI.

NWI mode

In NWI mode, the reader is operated as a network device. It could be connected to any internal network with DHCP, and the reader could be controlled via Web GUI or in automatic reading and data transferring mode.

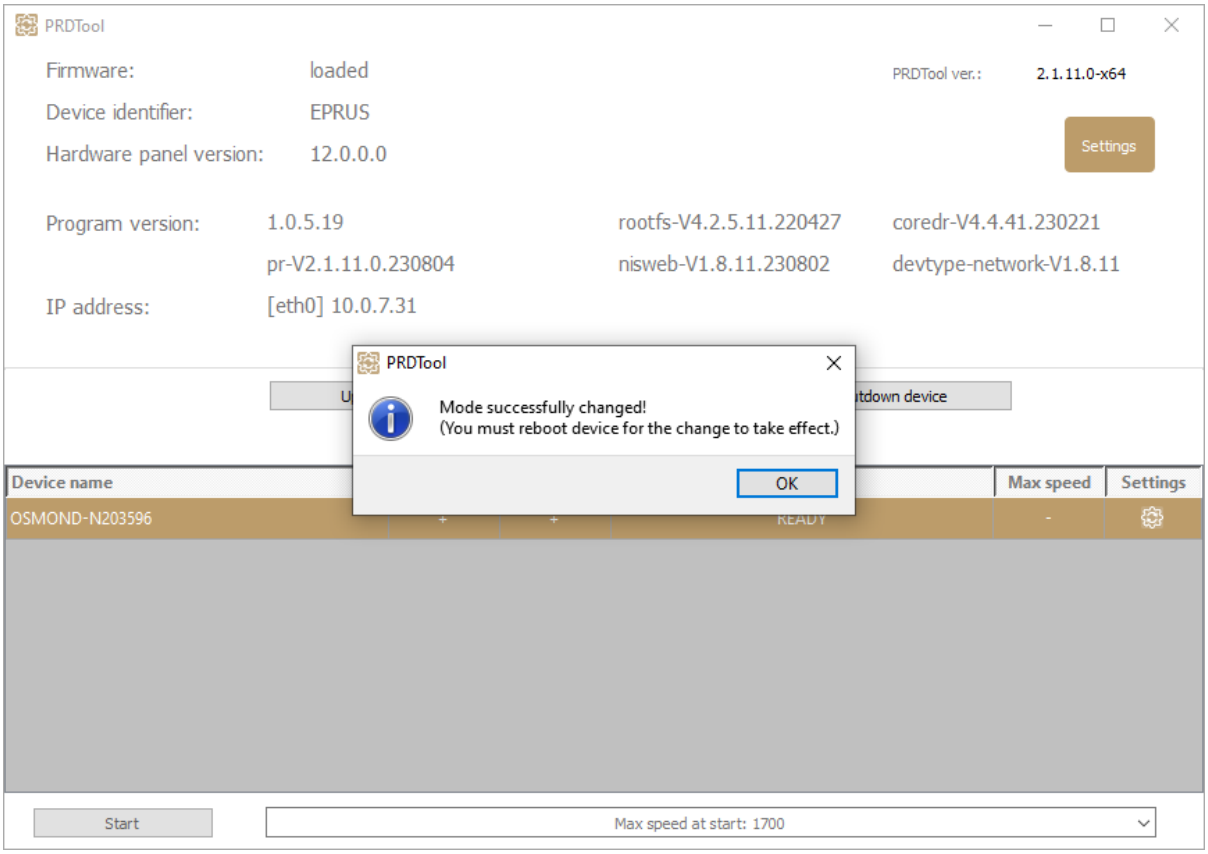
NWA mode

The Network Web Application API is designed to provide a tool for managing main network interface functions remotely, without accessing device Web GUI from browser.

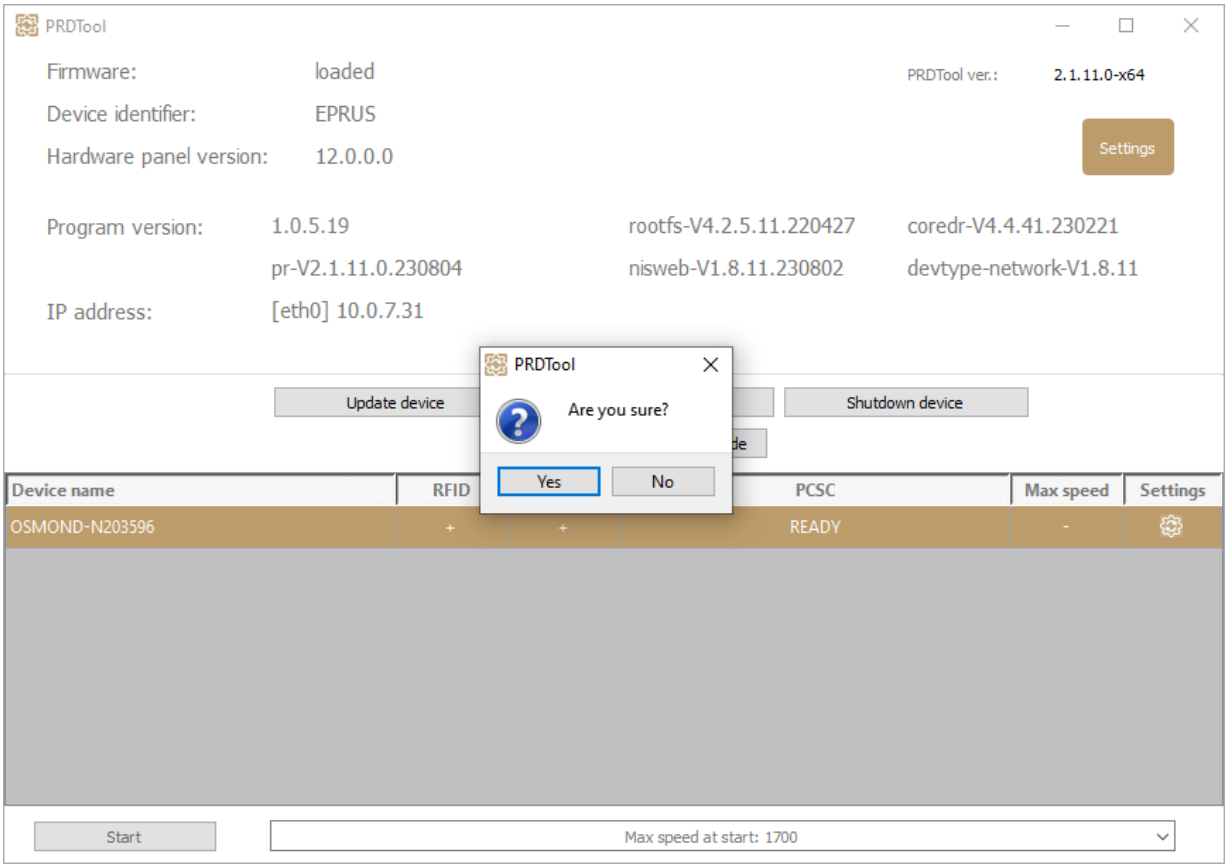
Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

26.2.1. SWITCHING BETWEEN OPERATION MODES

After the Osmond device has appeared and selected in the PRDTool, the current operation mode is displayed. In order to switch to another, please select the desired mode from the drop-down list by clicking on it, and then click on the **[Set mode]** button. A feedback message indicates the result of the change.

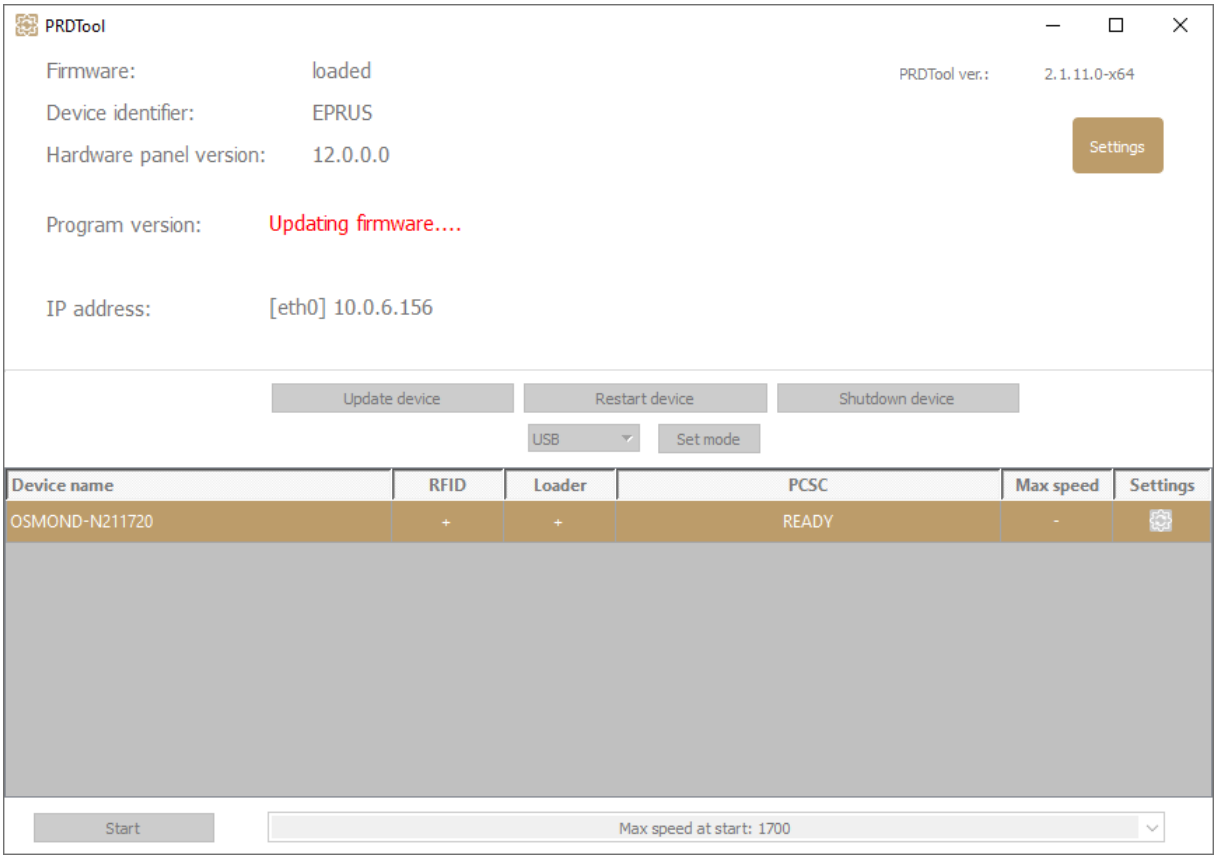


To apply these changes the device needs to be rebooted, so click on **[Restart device]** and then choose **[Yes]**. Now the device is rebooting in the selected operation mode. After the restart is finished, the reader is ready to be used.



26.3. FIRMWARE UPDATE

PRDTool utility application is capable of applying firmware updates to the Osmond devices. In order to do that, please connect the device to the PC via USB, select the corresponding device (in case of multiple devices) and click on the **[Update device]** button. Afterwards, browse the update file in the PRDTool. The update will be applied automatically, its status is marked in red at the **Program version** line. Once the update is finished, a feedback message is displayed. During the update process the device may reboot multiple times, signaled by „**Restarting device...**". When the update is completed, the new software version is displayed in the PRDTool.



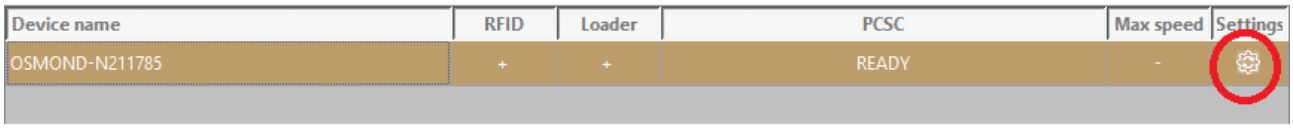
26.3.1. THE UPDATE FILE

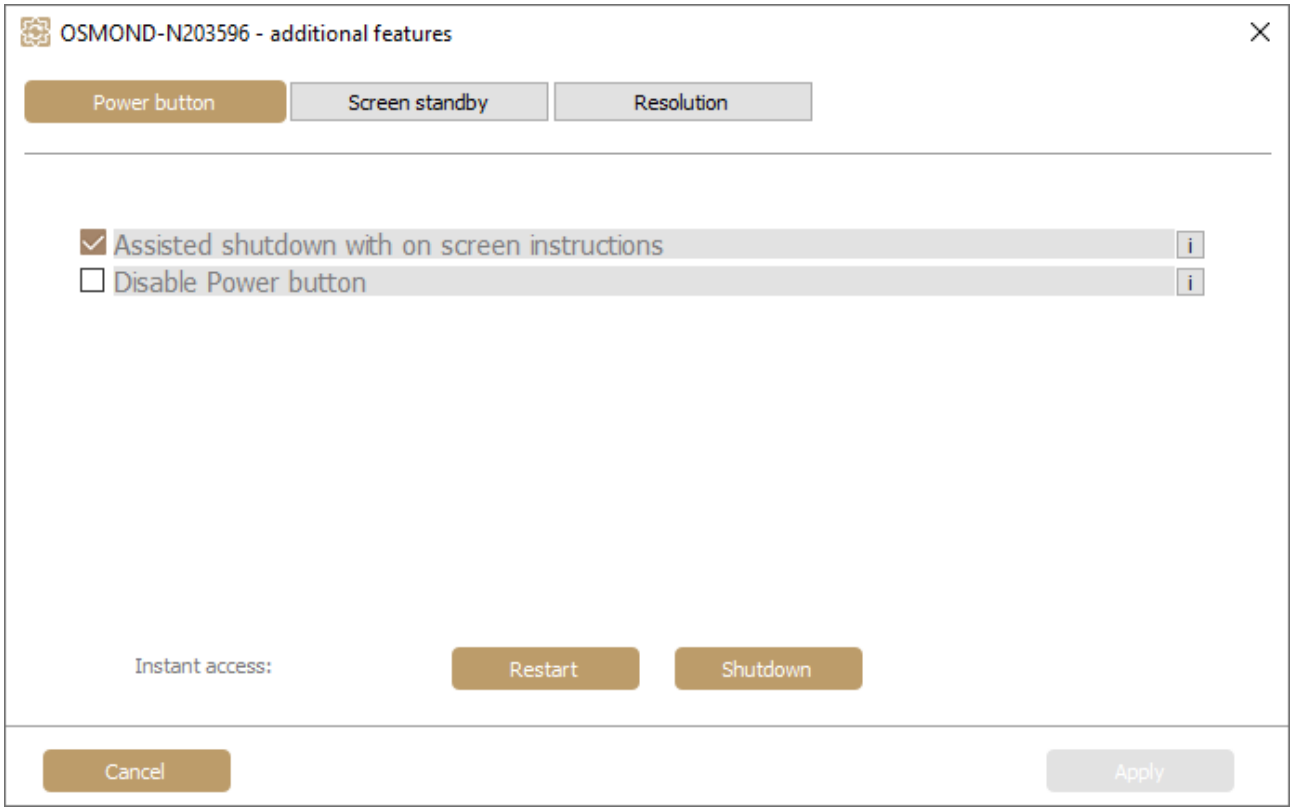
Osmond passport reader devices use ZIP archives as update files and to every ZIP file belongs a CHK file which is the hash signature of the update archive. The signature ensures that the update file is unmodified and undamaged. The two files should be in the same folder with the same name (e.g., update.zip, update.chk).

26.4. ADDITIONAL FEAUTURES

> **Note**
>
> This menu is only available in USB mode.

PRDTool utility is equipped with additional functionalities to customize power button usage and OLED display suspend parameters. Click on the cogwheel icon in the **Settings** column to open the additional features menu. Then, click **[i]** to show the details of each option.





> **Note**
>
> These functions of the PRDTool are only available from Passport Reader version 2.1.10.2.

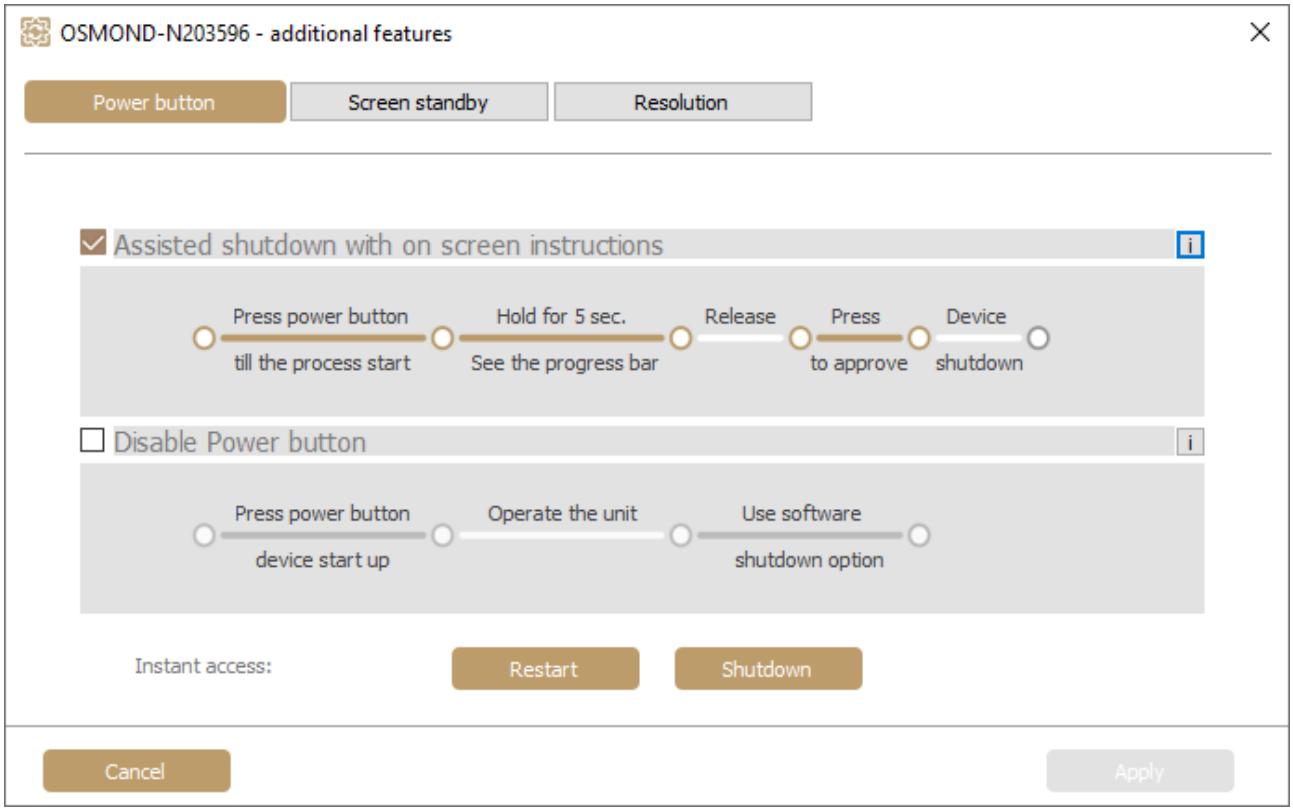
Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

26.4.1. POWER BUTTON FEATURES

For the device power button, two preconfigured functionalities are available. Users may select one of them.

1. Assisted Shutdown with On-screen Instructions (Default Setting)

Using the **Assisted shutdown** option, operators may switch the device off using its power button, following the method described in the diagram:



2. Disable Power Button

If the **Disable power button** option is selected, operators cannot switch the device off by its power button but via the **[Shutdown]** button (at **Instant access**) only.

> **Note**
>
> The **[Restart]** and the **[Shutdown]** buttons can be used in each power button mode.

> **Note**
>
> To make any change effective, click **[Apply]**.

26.4.2. SCREEN STANDBY

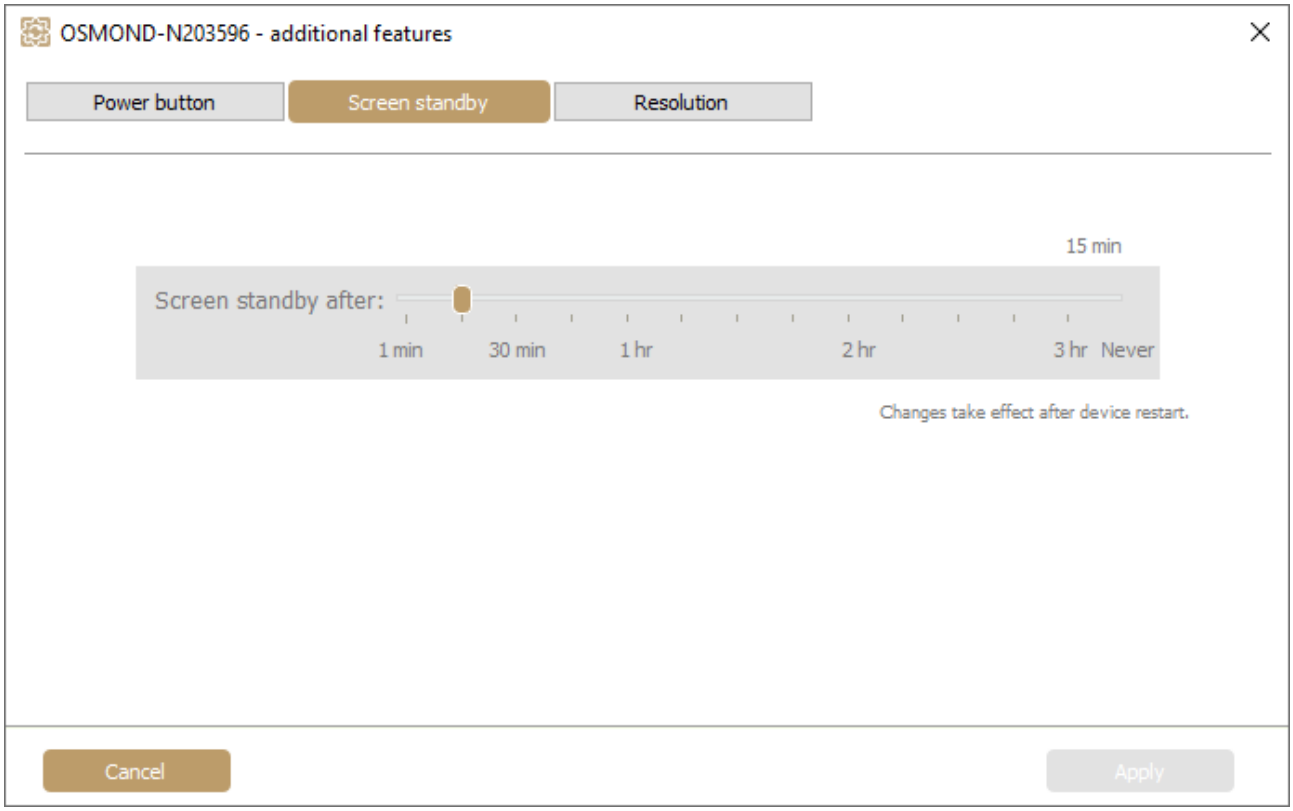
The brightness of the device built-in display can be reduced automatically, after a period of inactivity. Use the slide bar to specify that time period, then click **[Apply]** to save changes.

> **Note**
>
> Default setting: the OLED fades out after 1 hour of idle state.

> **Note**
>
> Changes are applied after device reboot only.

The OLED returns from sleep mode on the very first device status change: motion detected, pressed power button, scanning process started etc.

> **Note**
>
> Standby settings can also be specified in the gxsd.dat file. For more information on this topic, see OLED Standby Mode.

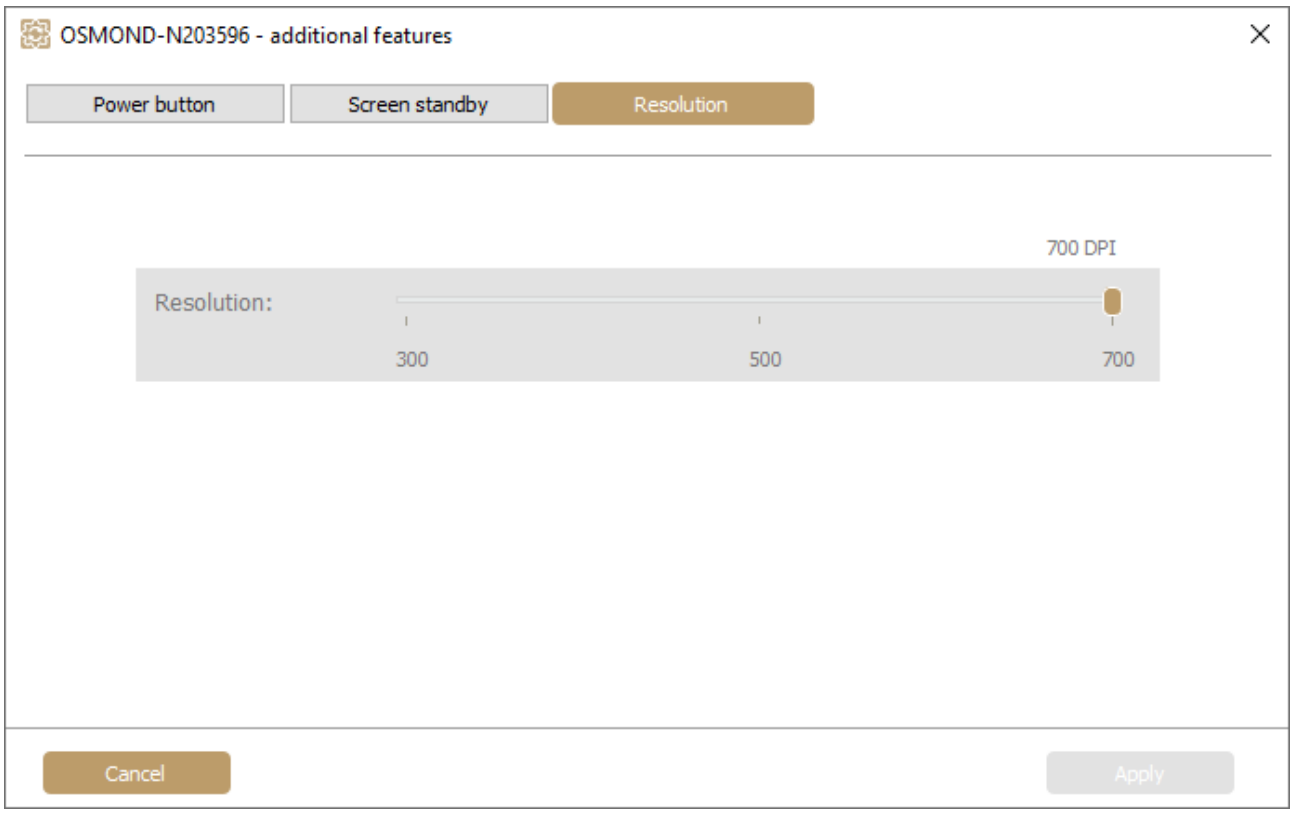


26.4.3. RESOLUTION

The resolution of the scanned document images can be selected, the following options are available:

- Low resolution: **300 DPI**
- Medium resolution: **500 DPI**
- High resolution: **700 DPI**

By default, this value is set to **700 DPI**. 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. Use the slide bar to specify the required value, then click on the **[Apply]** button to save the modification.



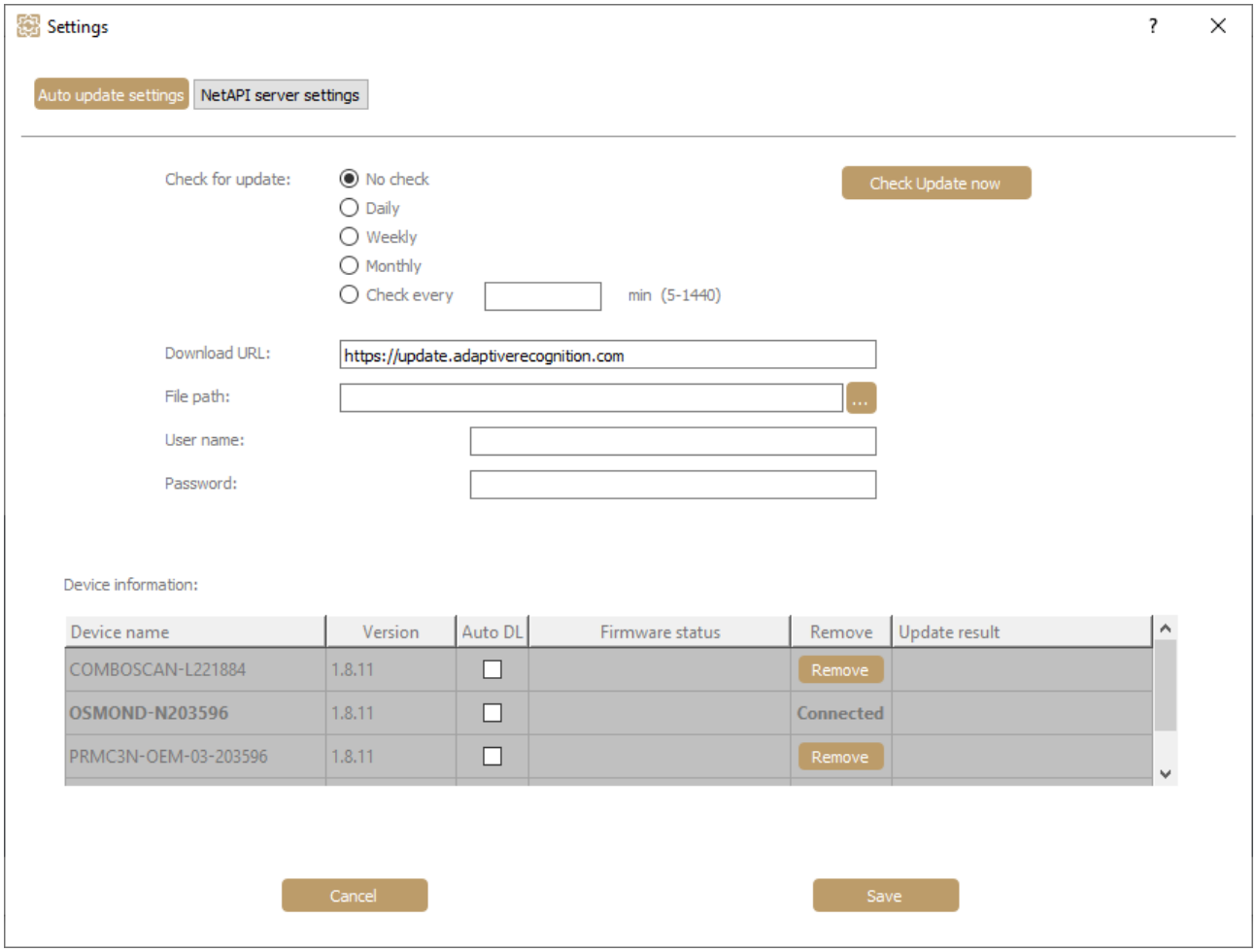
26.5. SETTINGS

26.5.1. AUTO UPDATE SETTINGS

Osmond N devices are capable of downloading and installing update files automatically. Such updates can be configured in this menu. Set frequency of checking for updates at **Check for update**, specify update server with port (**Download URL**), and provide username and password if remote server uses basic authentication. Supported protocols for remote servers are the following: **HTTP/HTTPS** with or without basic authentication.

History of earlier updates and downloads as well as option for automatic (or manual) firmware download (**Auto DL**) and removal (**Remove**) is available for each connected device at **Device information**.

> **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.



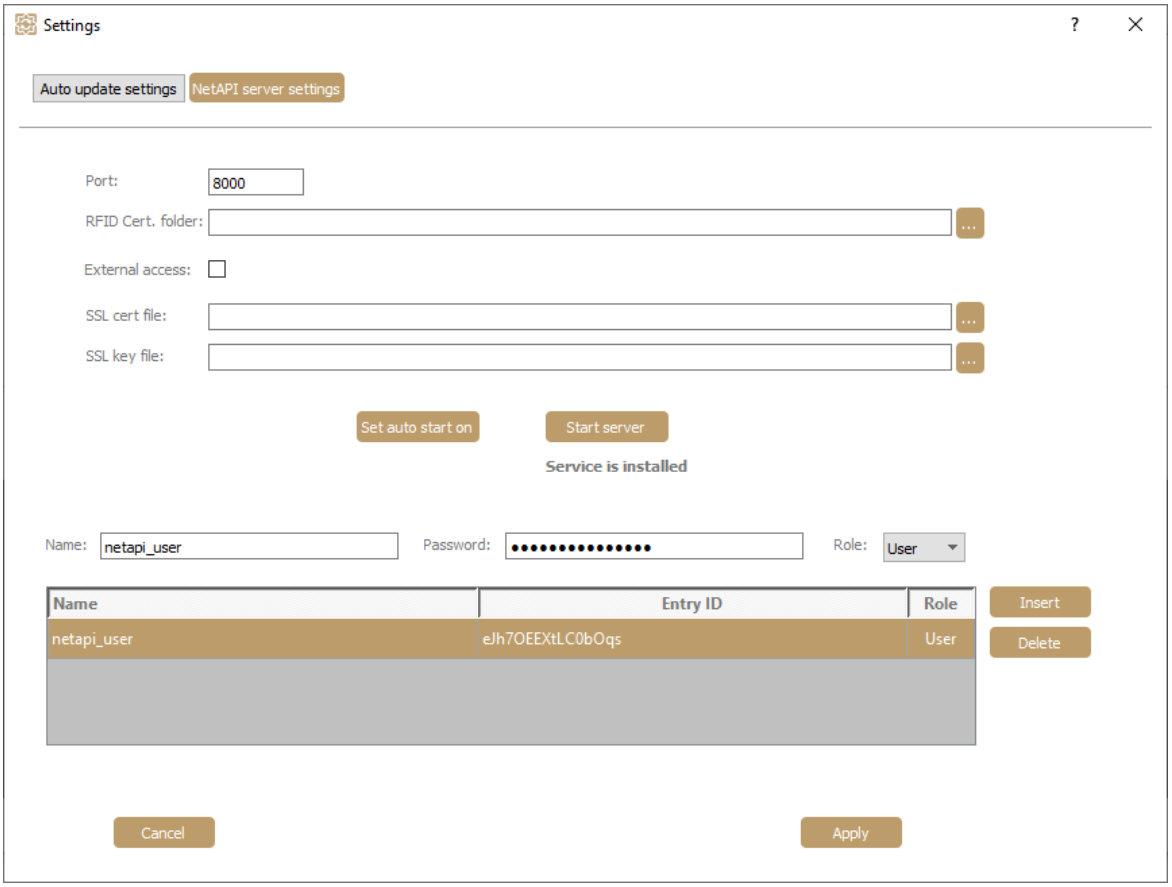
26.5.2. NETAPI SERVER SETTINGS

In the NetAPI server settings menu set the following values:

- **Port**: Port number of NetAPI
- **RFID Cert. folder**: Path of the certificates used for passive authentication
- **External access**: If it is enabled, NetAPI is not only available from localhost but from other network locations.
- **SSL cert file**: Certificate for NetAPI use
- **SSL key file**: Key belonging to the certificate
- **Set auto start on**: Starting prwebsrv automatically at Windows startup
- **Start/Stop server**: Starting or stopping the prwebsrv

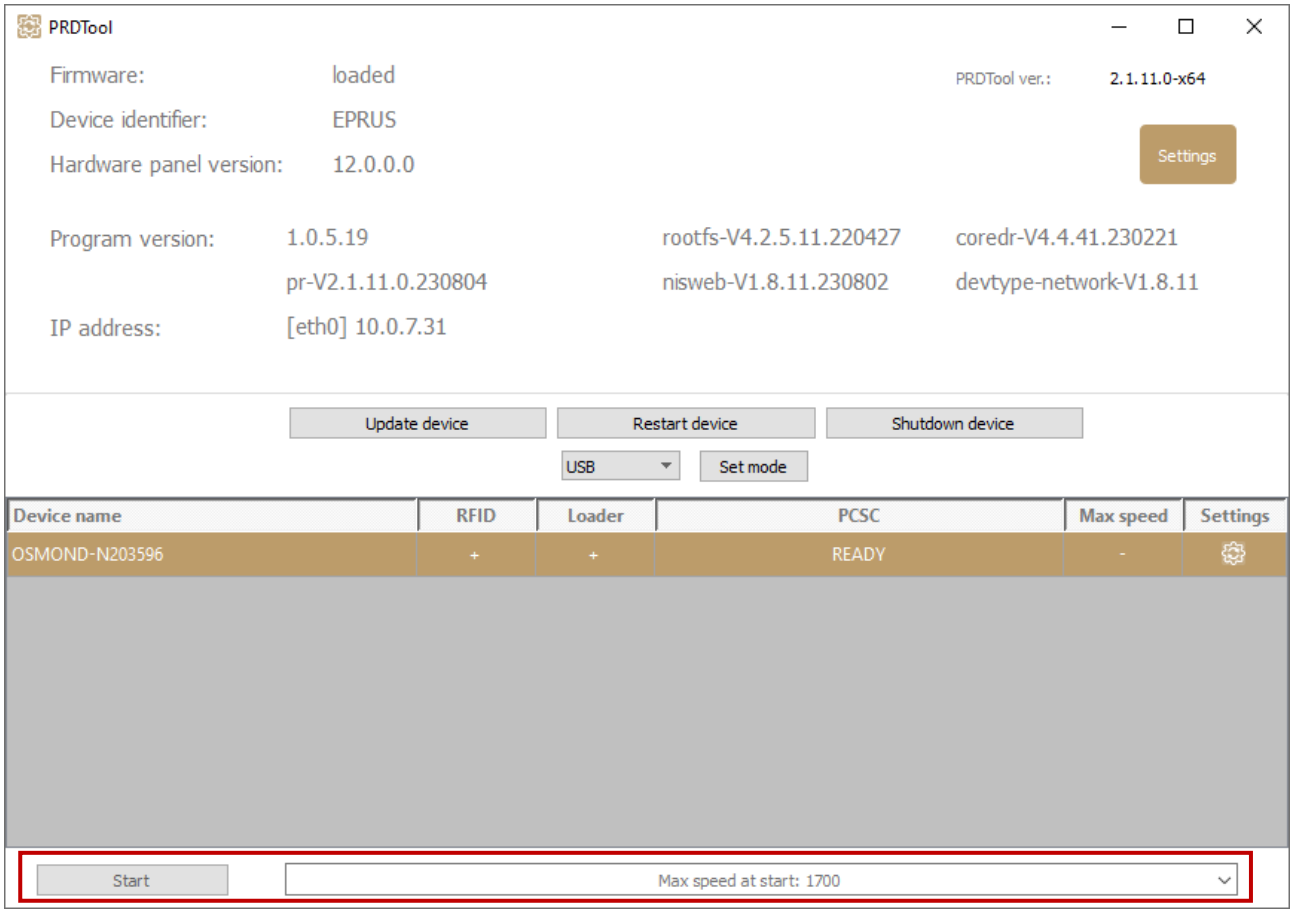
At least one user and the belonging password are required to enter in order to use the NetAPI. Specify the username to the **Name** field and the password to the **Password** field. After that, click on the **[Insert]** button in order to add the entered user.

> **Note**
>
> Run PRDTool as **Admin** to create new user.



26.6. PCSC CONTROL

The PCSC control is part of the PRDTool program. This is the command line version of the former PCSCCtrl.exe. The functions of the PCSC can be found at the bottom of the opened PRDTool window.

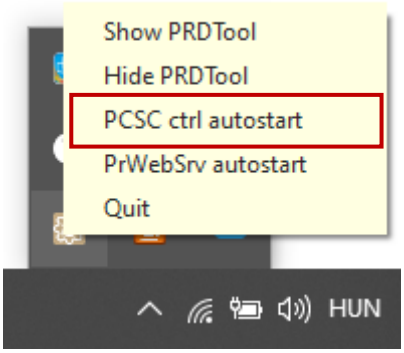


The default status is either **READY** or **STARTED** (if PCSC **Autostart** is enabled). The current status is displayed under the **PCSC** column. PCSC can be enabled or disabled by clicking on the device name, and then on **[Start]** or **[Stop]**. The "max RFID communication speed at start" can be selected under the **Max speed at start** drop-down menu.

Important!

Please make sure to close any application that uses the Passport Reader device before starting or stopping the PCSC interface.

PCSC can be started automatically via the quick menu of PRDTool: right click on the **PRDTool** icon and click on **PCSC ctrl autostart**.



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

26.7. COMMAND LINE MODE

The PRDTool can also be used in command line mode to query device information. By calling the „--help" switch, the correct use is displayed. The device list, the device version and the IP address information can be queried. The file format of the output can be specified for the easier automatic processability.

```
C:\Program Files\Adaptive Recognition\utils\PRDTool>PRDTool.exe --help

Usage: PRDTool [-start [-speed <speed>]/-stop/-status/-hide/-autostart [off] [-speed <speed>]] [-version] [-devicelist]
[-devicedetails [name]] [[-text] | -xml | -json]
```

```
C:\Program Files\Adaptive Recognition\utils\PRDTool>PRDTool.exe -devicedetails OSMOND-N211785 -xml

<?xml version='1.0' encoding='UTF-8' ?>
<PRDTOOL>
<panel_version>12.0.0.0</panel_version>
<program_version>1.0.3.12</program_version>
<ip_addresses>[eth0] 192.168.6.250</ip_addresses>
<system_versions>rootfs-V4.2.5.11</system_versions>
<system_versions>coredr-V4.2.33</system_versions>
<system_versions>pr-V2.1.10.0.210930</system_versions>
<system_versions>nisweb-V1.7.17.210928</system_versions>
</PRDTOOL>

C:\Program Files\Adaptive Recognition\utils\PRDTool>
```

27. OSMOND SYSTEM RECOVERY

With the system recovery the original manufacturer settings are restored, therefore all saved and stored data is erased.

To perform system recovery on the Osmond N device, do the following:

1. Turn the power touch button off and disconnect the connected cables (power supply, Ethernet and/or USB cables).

Disconnected device

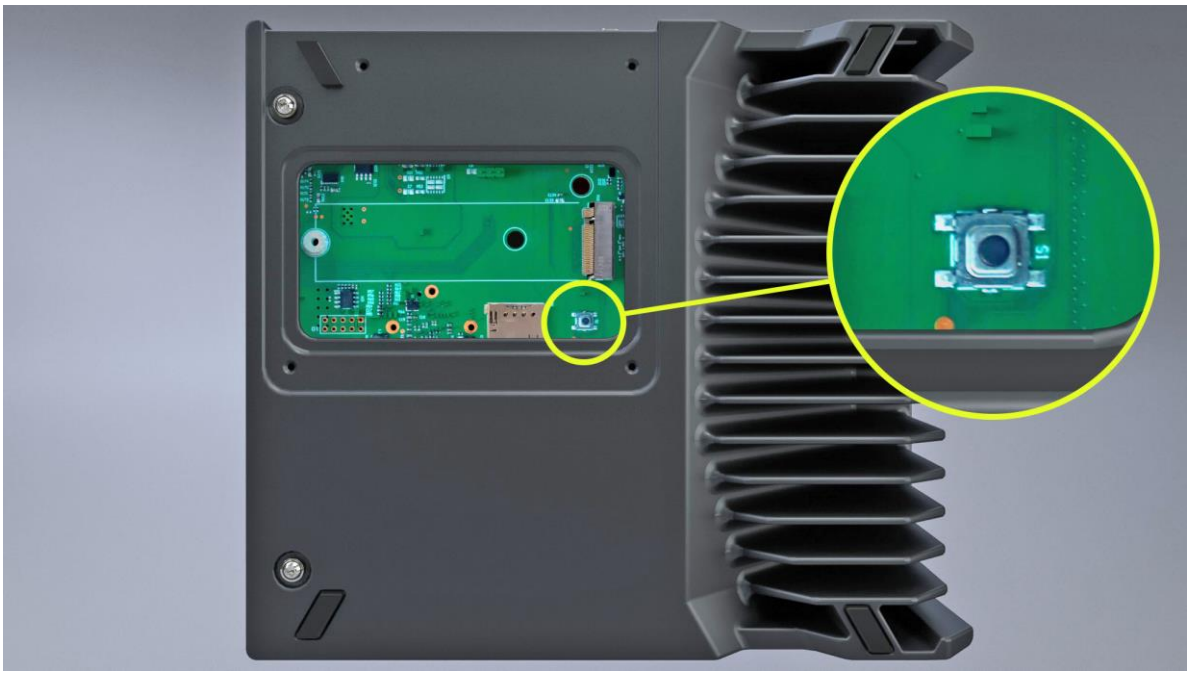
2. Place the device on its side looking out for the aluminum heat sink and unscrew the 4 smaller screws in order to remove the cover plate.

Note

Use an 8 TX screwdriver.

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

Search for the button located on the printed circuit board (see the following image).



3. Reconnect the disconnected cables (power supply, Ethernet and/or USB cables).
4. Press the button located on the printed circuit board (PCB) simultaneously with the power touch button, until the OLED screen displays the following:

5. The cogwheel icon appears for a couple minutes.
6. Then, the Adaptive Recognition static logo is being displayed for a longer period of time.
7. This is followed by the cogwheel icon again.
8. Again, the Adaptive Recognition static logo appears for another longer period of time.
9. Next, the screen begins to flash, until a check mark is displayed.
10. Afterwards, the factory settings are valid.
    In case of Osmond N, the device can only be reached via its default IP address. Before accessing the web interface of the device, wait about 1-2 minutes.

Important!

When performing factory reset, the device reverts to the factory firmware version which was supplied during its production.

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

28. FCC

28.1. FCC CAUTION – §15.21:

"Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment."

28.2. FCC STATEMENT – §15.105(B):

"This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help."

28.3. FCC STATEMENT – §15.19(A)3:

"This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation."

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

28.4. RSS-GEN STATEMENT

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

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes: (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement."

28.5. RESPONSIBLE PARTY INFORMATION – §2.909:

The identification, by name, address, and telephone number, or internet contact information, of the responsible party (must be located within the United States).

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

29. ACRONYMS AND TECHNICAL TERMS USED IN THE DOCUMENT

API

Application Programming Interface

Aztec

One of the readable two-dimensional (2D) barcode types.

BAC

Basic Access Control: An RFID security mechanism.

BCR

Barcode Recognition. Barcodes are line drawings designed to be recognized easily by computers.

Code 39

One of the readable one-dimensional (1D) barcode types.

Code 128

One of the readable one-dimensional (1D) barcode types.

CSCA

Country Signing Certification Authority

EAC

Extended Access Control: An RFID security mechanism.

EAN

One of the readable one-dimensional (1D) barcode types.

DataMatrix

One of the readable two-dimensional (2D) barcode types.

ICAO

International Civil Aviation Organization

Interleaved 2 of 5

One of the readable one-dimensional (1D) barcode types.

ISO

International Organization for Standardization

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

MRTD

Machine Readable Travel Document

MRZ

Machine Readable Zone: Lower part of the travel document. It contains text designed for reading optically with a travel document reader device.

OCR

Optical Character Recognition: Recognizing characters from a digitalized image.

OVD

Optically Variable Device: Security feature which shows different information, depending on the viewing and/or lighting conditions.

OVI

Optically Variable Ink: Printing ink that contains microscopic pigments acting as interference filters, resulting in large color shifts (strong variations in color) depending on the angle of observation or lighting.

PDF417

One of the readable two-dimensional (2D) barcode types.

QR Code

One of the readable two-dimensional (2D) barcode types.

RFID

Radio Frequency Identification: System based on built in chip that contains data and can communicate through air.

SDK

Software Development Kit

SOD

Document Security Object

VIZ

Visual Inspection Zone: Upper part of the travel document. It may contain face photo image and textual, human readable data.

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

X. CONTACT INFORMATION

Headquarters:
Adaptive Recognition, Hungary Inc.
Alkotás utca 41 HU
1123 Budapest Hungary
Web: adaptiverecognition.com

Service Address:
Adaptive Recognition, Hungary Inc.
Ipari Park HRSZ1113/1 HU
2074 Perbál Hungary
Web: adaptiverecognition.com/support/

Adaptive Recognition Hungary Technical Support System (ATSS) is designed to provide you the fastest and most proficient assistance, so you can quickly get back to business.

Information regarding your hardware, latest software updates and manuals are easily accessible for customers via our Documents Site (www.adaptiverecognition.com/doc) after a quick registration.

New User
If this is your first online support request, please contact your sales representative to register you in our Support System. More help here (www.adaptiverecognition.com/support)!

Returning User
All registered ATSS customers receive a personal access link via e-mail. If you previously received a confirmation message from ATSS, it contains the embedded link that allows you to securely enter the support site.