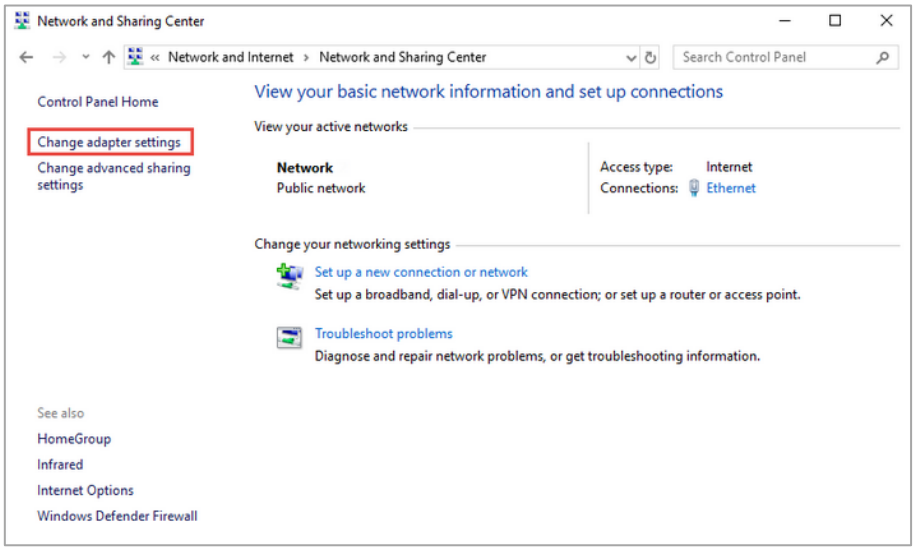
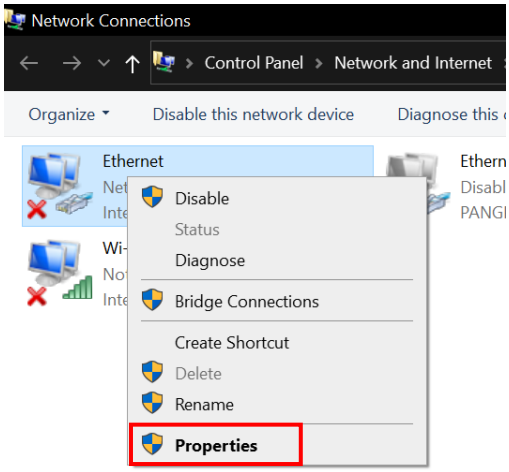
10. DIRECT ETHERNET CONNECTION

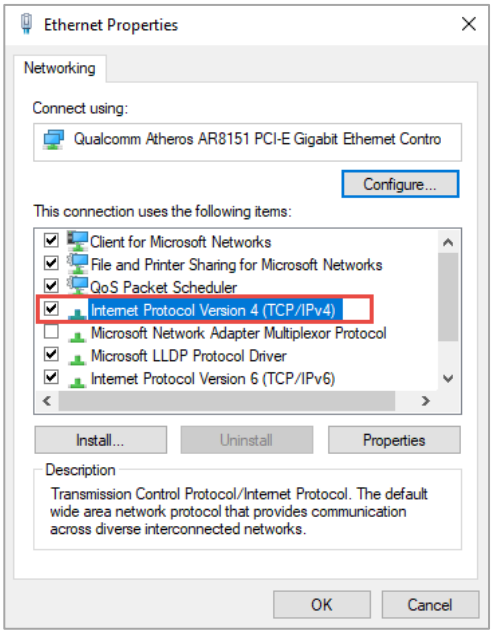
If you connect the device directly to the PC with an Ethernet cable, you can reach the device on its default IP 192.0.2.3, but you need to modify your Ethernet adapter settings manually.

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.

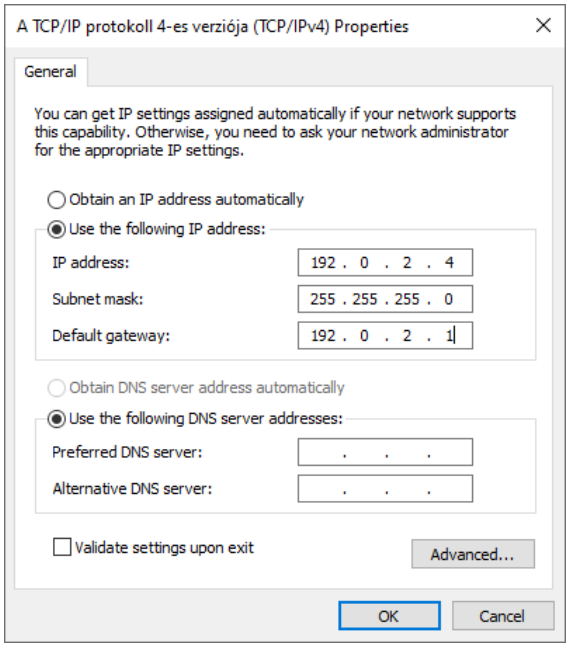


2. Right-click on **Ethernet**, then select **Properties**. In the appearing menu double-click "**Internet Protocol Version 4 (TCP/IPv4)**".





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.cert
```

- Windows:

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

Contents of the devicename.ssl.cert 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-----
```

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

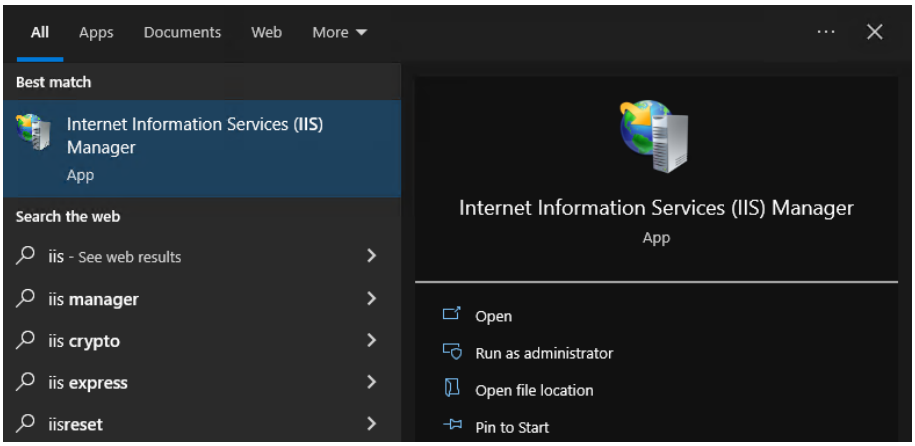
12. INSTALLATION OF THE SSL CERTIFICATE

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:

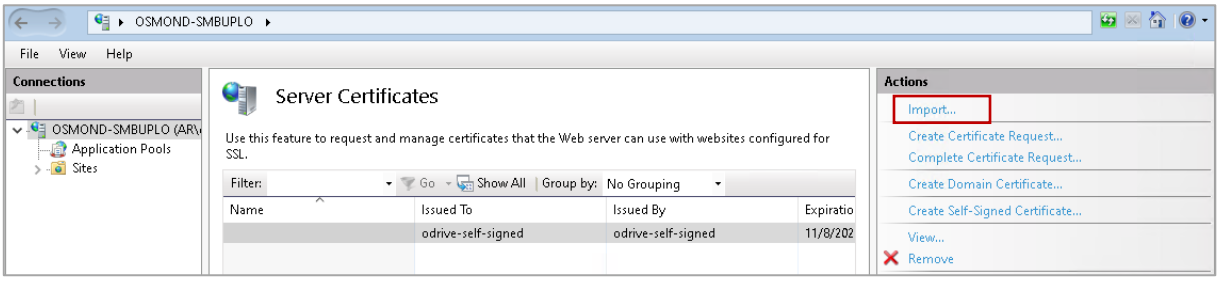
https://www.sslforfree.com/

12.1. INSTALLING THE SSL CERTIFICATE ON WINDOWS 10

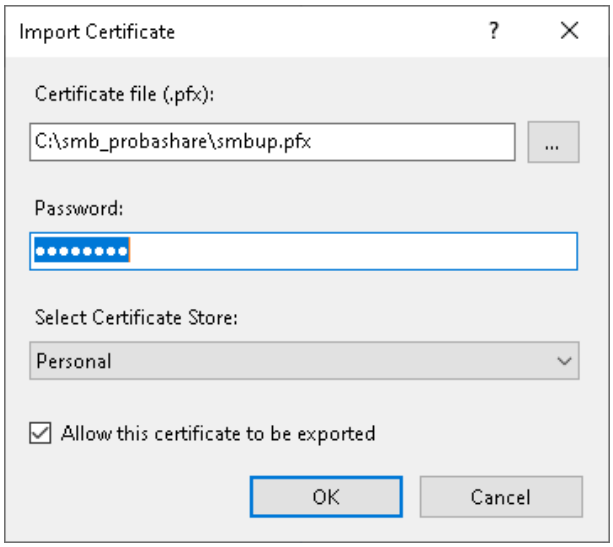
1. Start the **Internet Information Services (IIS)** program:
   - Open Start menu
   - Enter: iis



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
```

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/
   ```

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.

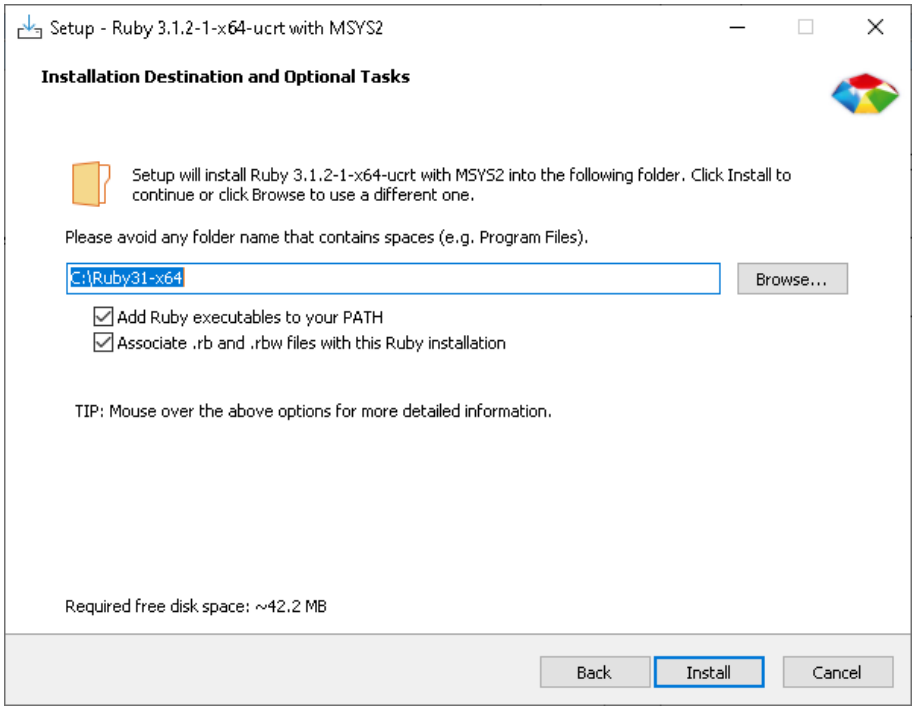
It is recommended to save the source code as a file named **ws_server_ruby.rb**, **ws_server_python.py** or **ws_server_java.java**, because this description will refer to the servers by these names.

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.

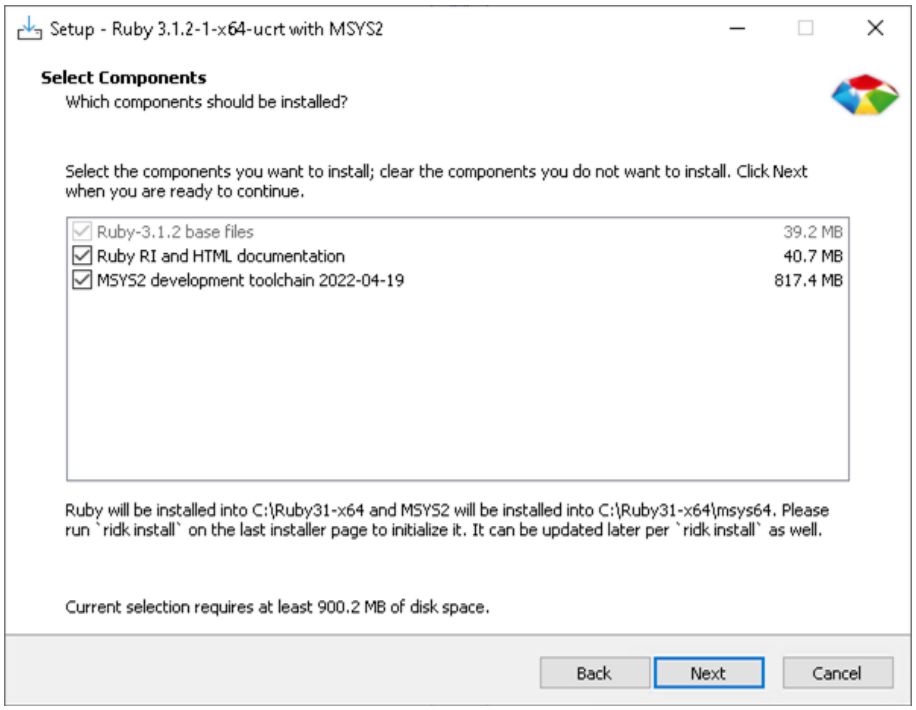
13.2. INSTALLING AND SETTING THE WS SERVER ON WINDOWS 10

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]**.



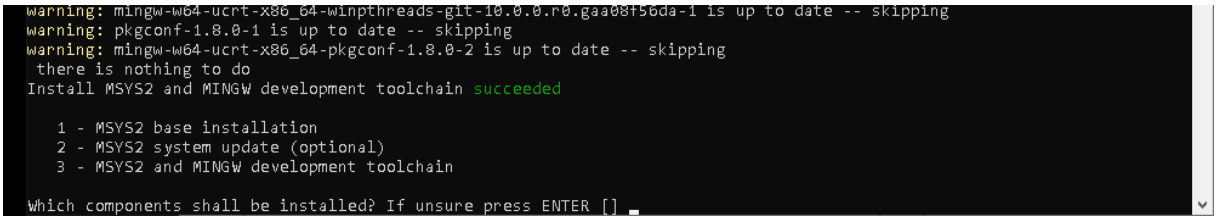
- Select "Ruby RI and HTML documentation" and "MSYS2 and MINGW development toolchain" by ticking the checkboxes.



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

- 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:

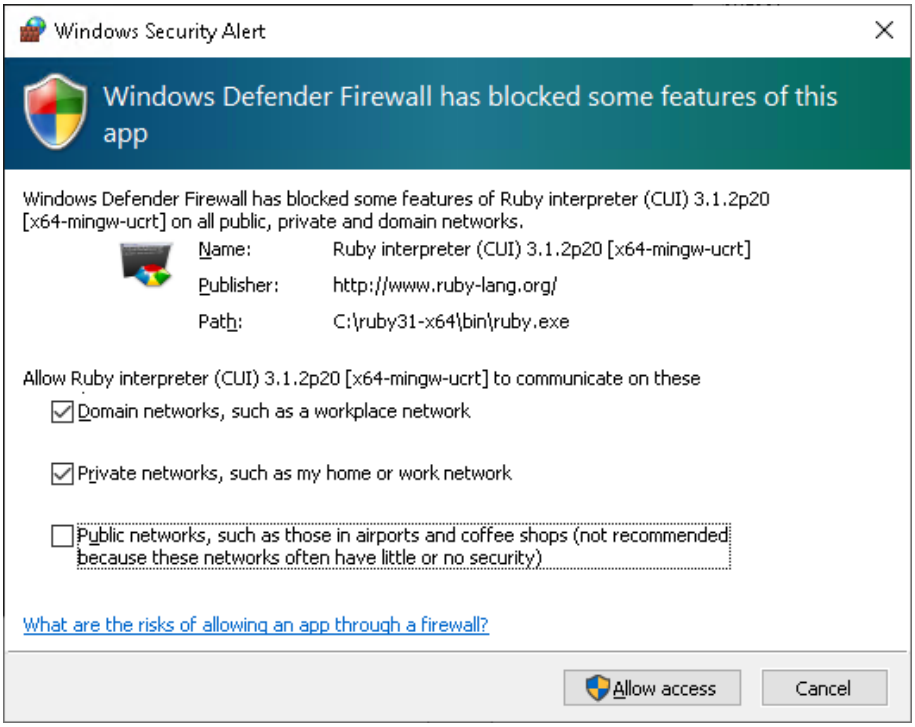
```
gem install websocket-eventmachine-server
```


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.

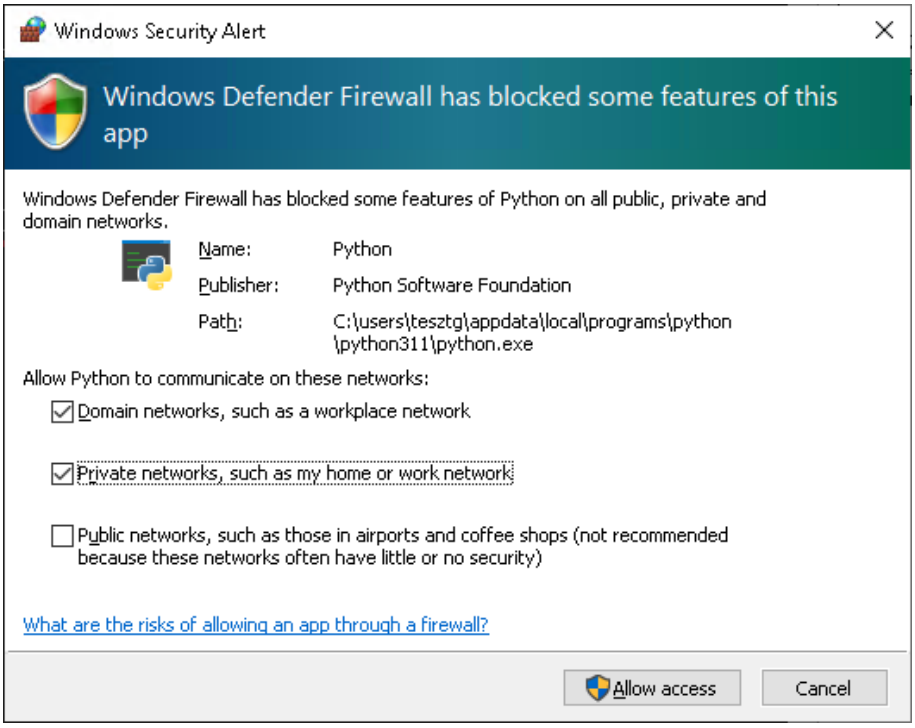
2. Open Command Prompt. Command Prompt can be accessed by entering "cmd" text to the search bar at Start menu and clicking on the appearing Command Prompt line.
3. Install the websockets python package in the Command Prompt:

```
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.

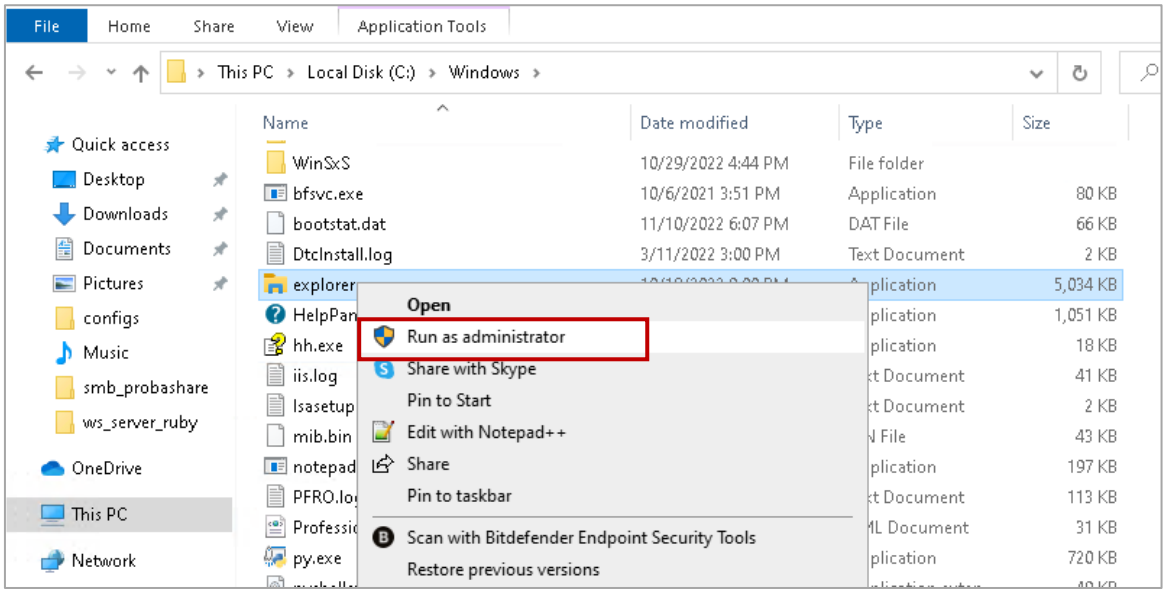


8. In order to stop the server, use the Ctrl + C keyboard shortcut or simply close the terminal.

13.2.5. INSTALLING JAVA

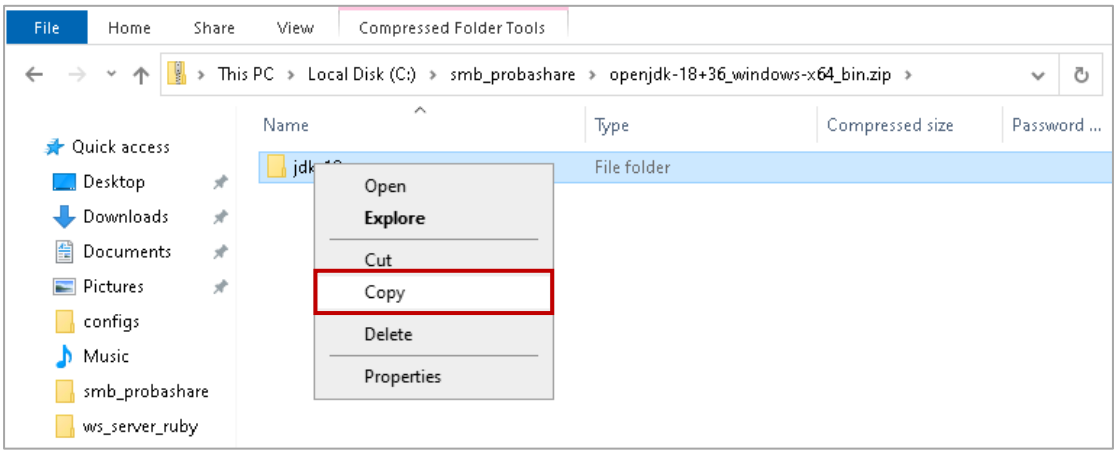
In the following section the installation of OpenJDK will be described. For running the WS server, any version of Java can be used. The testing on Windows has been performed with the version 18 of OpenJDK.

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.



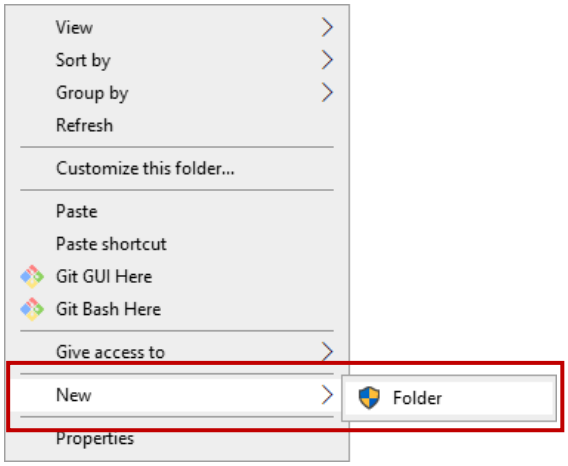
   - In the recently opened File Explorer browse the downloaded zip file. (The name of the current version is "openjdk-18+36_windows-x64_bin.zip".)
   - Double click on the zip file.

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



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

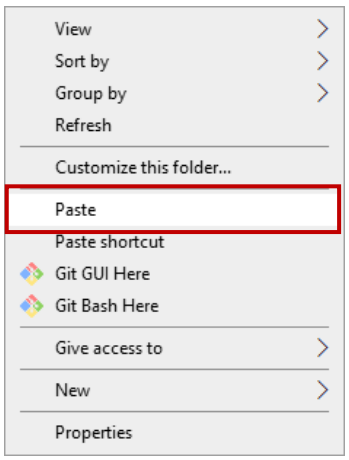
– Right click on a neutral area, then select **New / Folder** menu item from the pop-up quick menu.



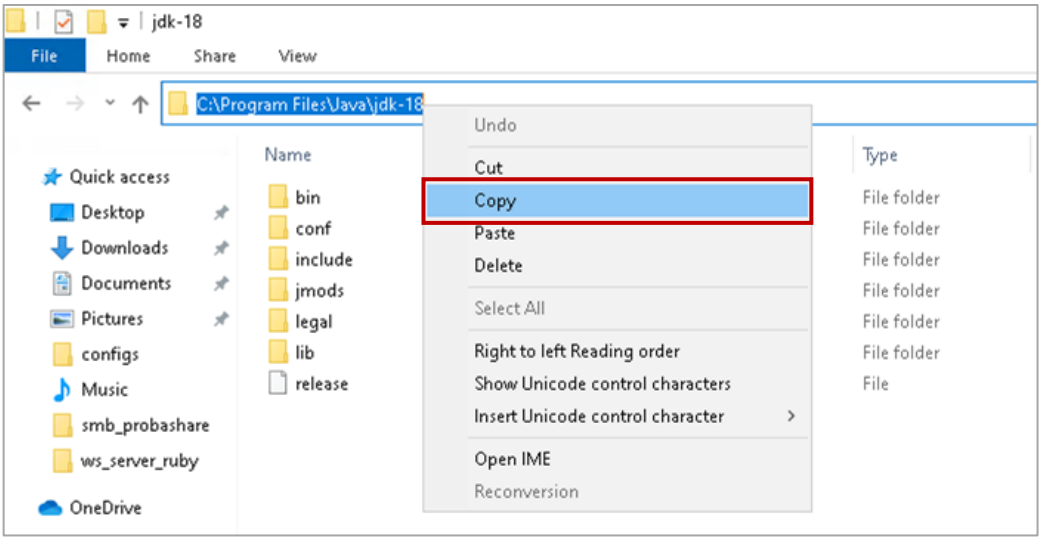
– After that, Windows creates a new directory. Rename it to "**Java**" and press **[Enter]**.

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

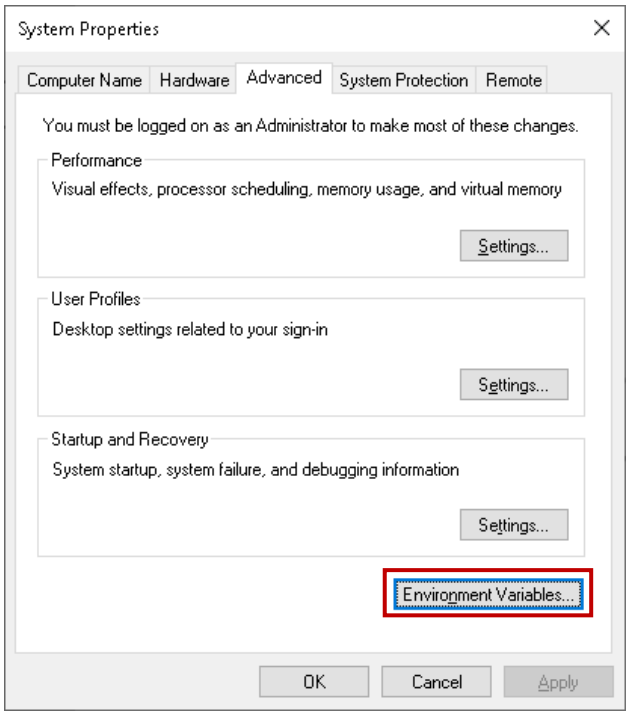
– Right click on a neutral area, then select **Paste**.



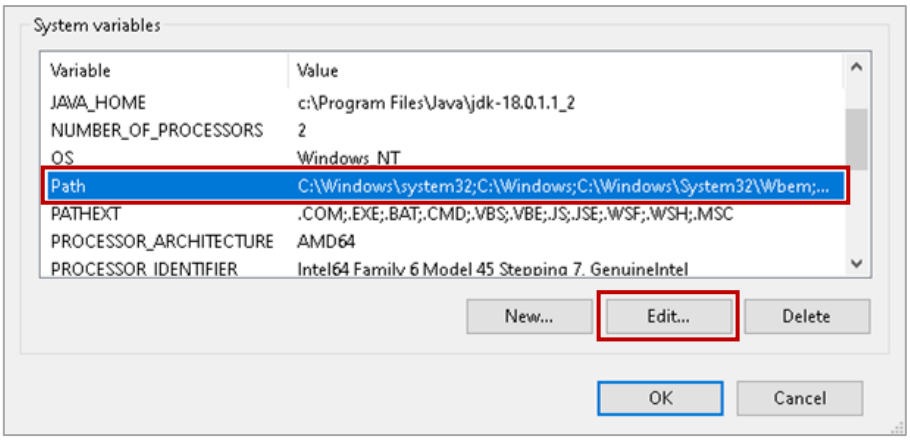
– After decompression, copy to clipboard the path of the Java directory:
  - Double click on the created directory (e.g., named jdk-18) to enter the holder.
  - Click on a neutral area of the address bar of the File Explorer (e.g., to the right of the path of the folder).
  - In the appearing quick menu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



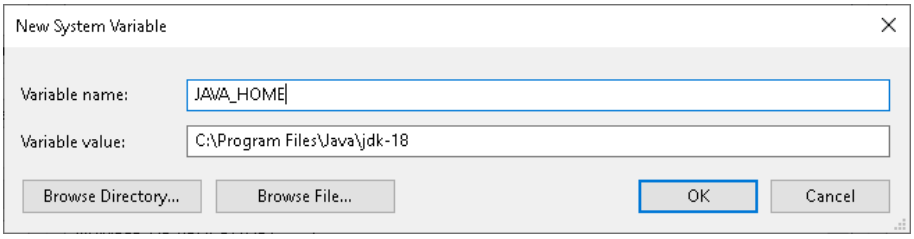
7. In the pop-up window under **System variables** select the **Path** variable. Then, click on the **[Edit…]** button.



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

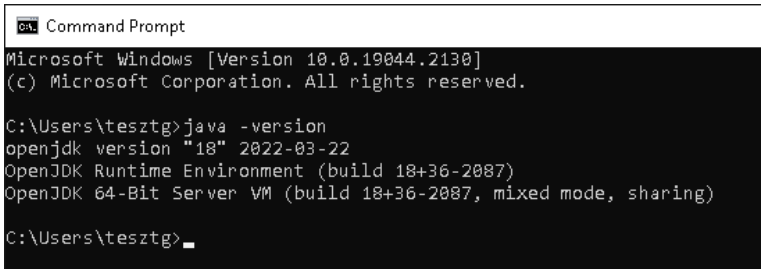


13. Then, click on **[OK]**.
14. After that, select the **[OK]** button again.
15. Close the window and restart Windows.

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
      ```

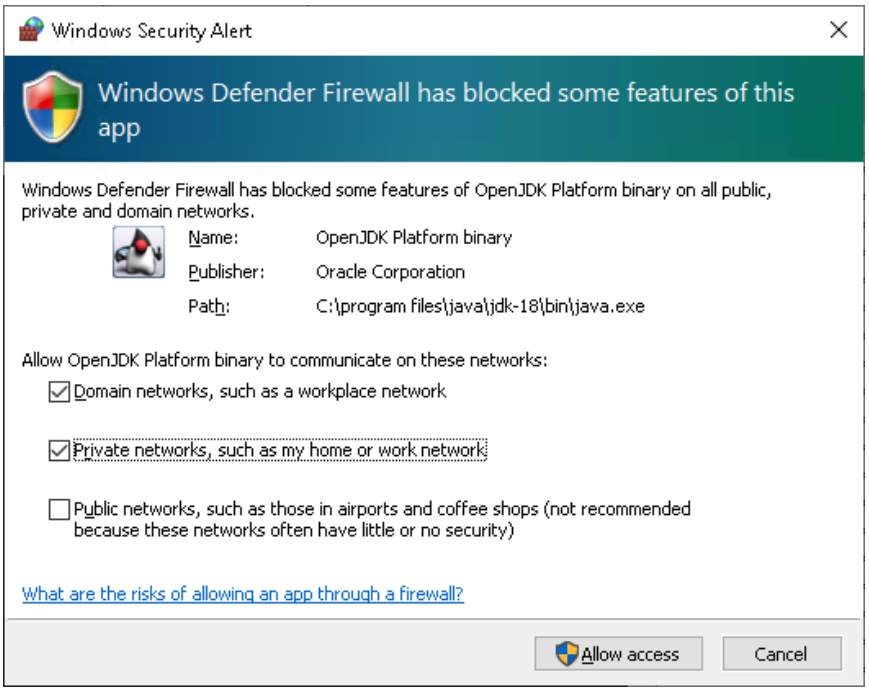
    - If the returned value is openjdk version "18", then Java is properly installed.



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.

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
   ```

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
   ```

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
   ```

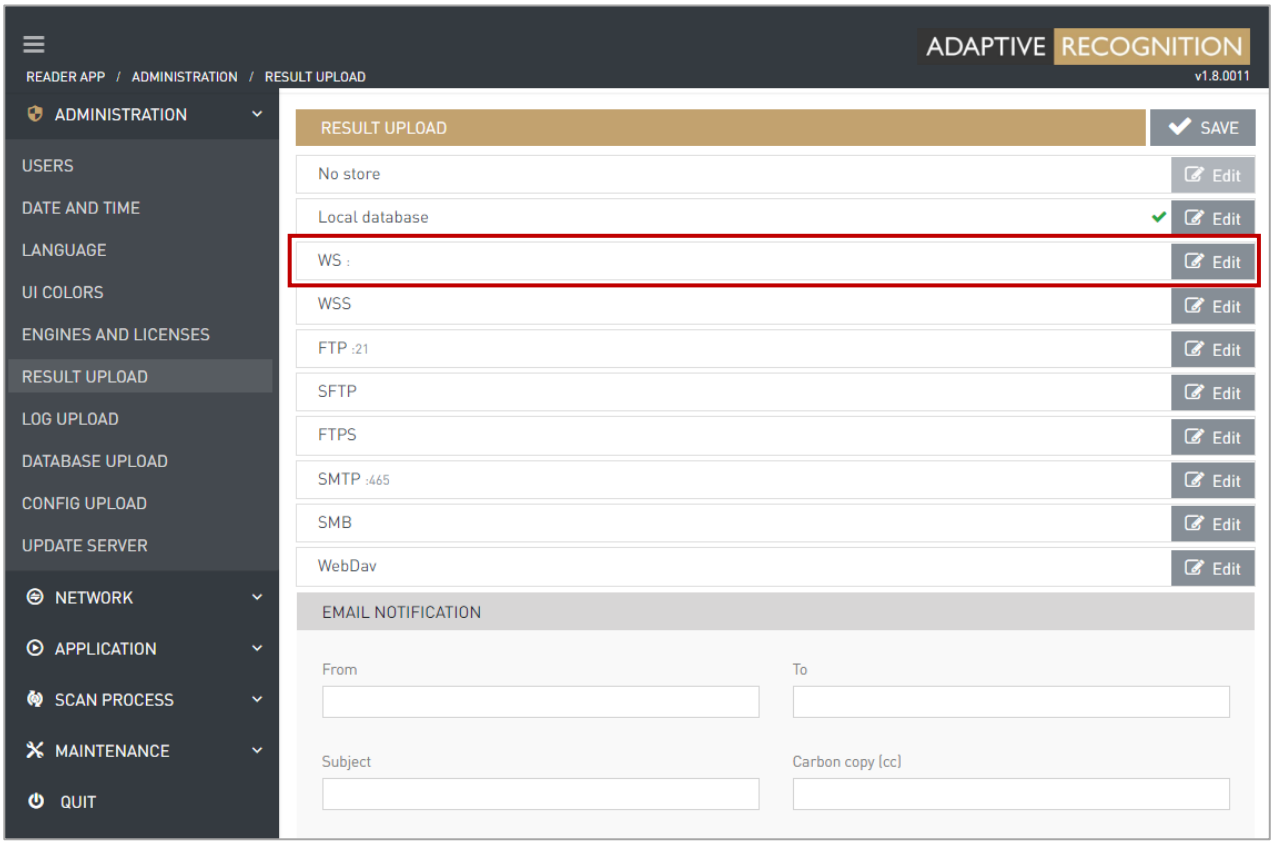
7. In order to stop the WS server, use the Ctrl + C keyboard shortcut or type "exit" in the running terminal.
    - The WS server may not shut down immediately. In this case the server throws an error message at the next startup:
      `java.net.BindException: Address already in use`
    - At this time 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

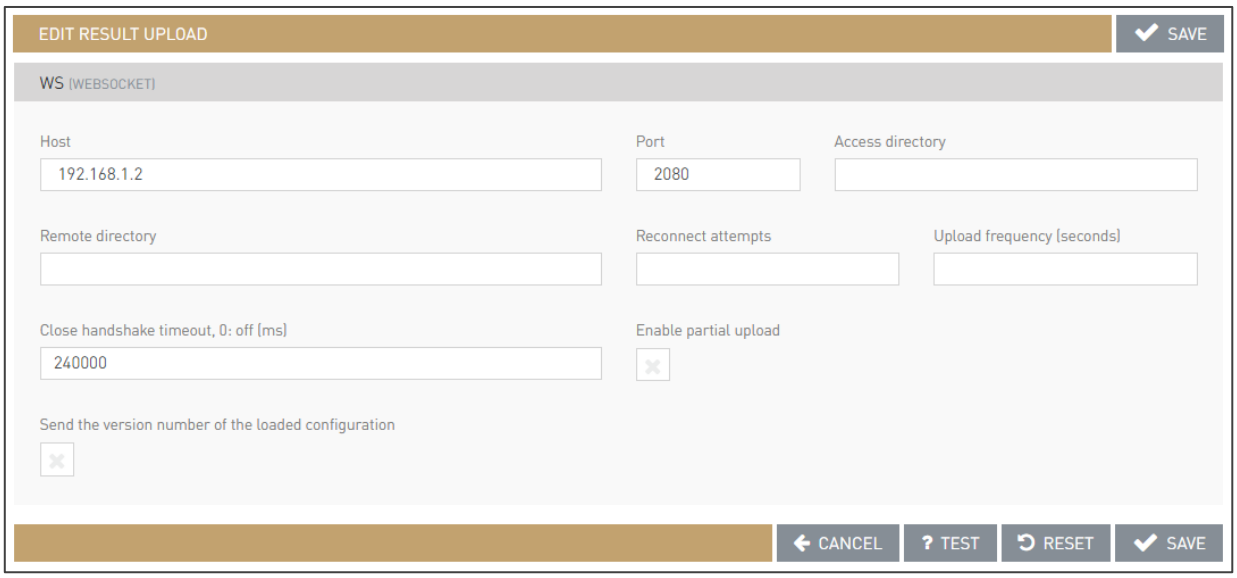
The parameters of the WS protocol can be set on the web interface of the Osmond device. By default, the web interface is accessible on 192.0.2.3:3000, but it can be set to another address as well. The IP address of the Osmond in the example is 192.168.6.244:3000.

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

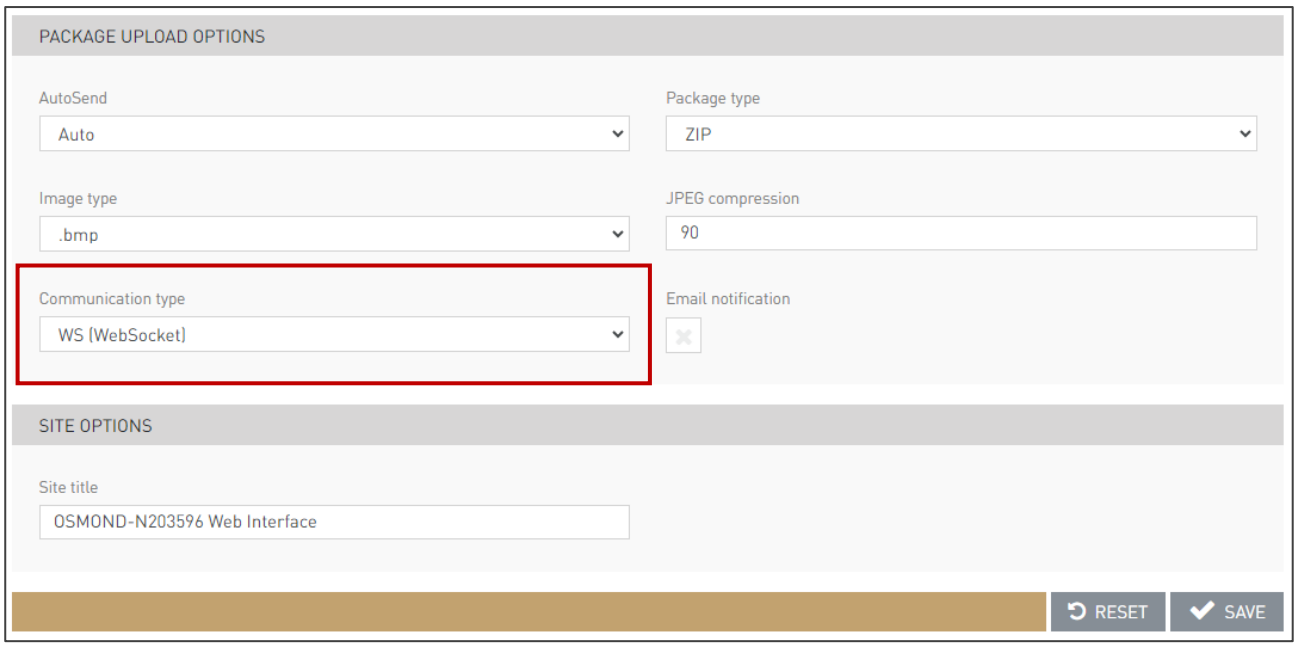
> **Note**
>
> Leave the other fields blank.



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.

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"
}
```


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

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"
}
```

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"
}
```


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

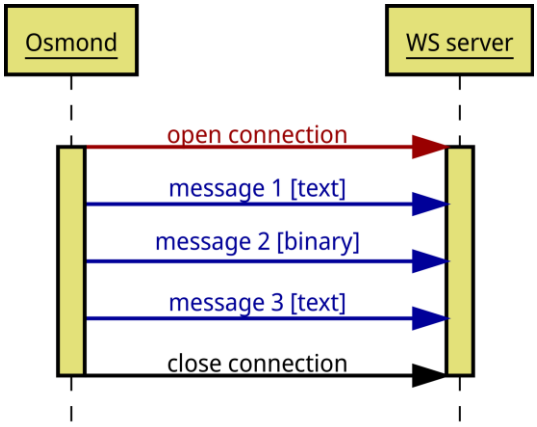
13.5.7. THE STRUCTURE OF THE WS COMMUNICATION DATA CONTENT

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

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.

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

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.

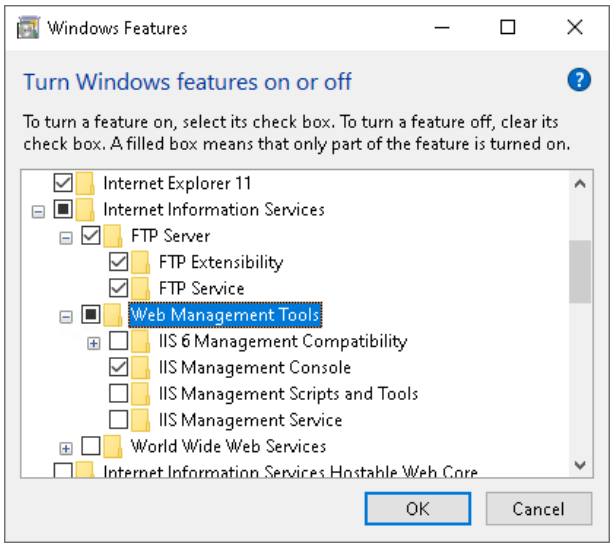
The parameters are the following:

- 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.

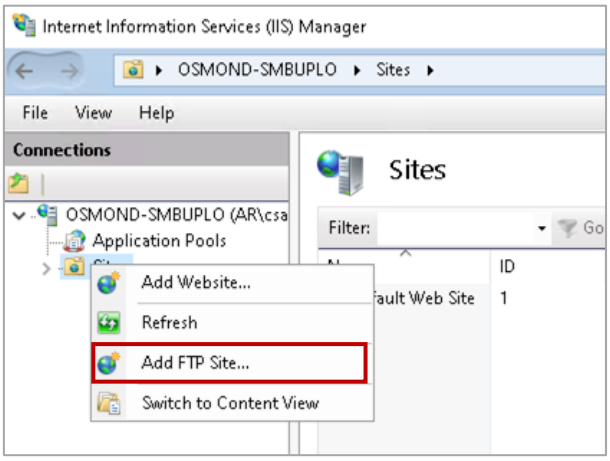
14.1.2. SETTING FTP

1. Create the library, for example:

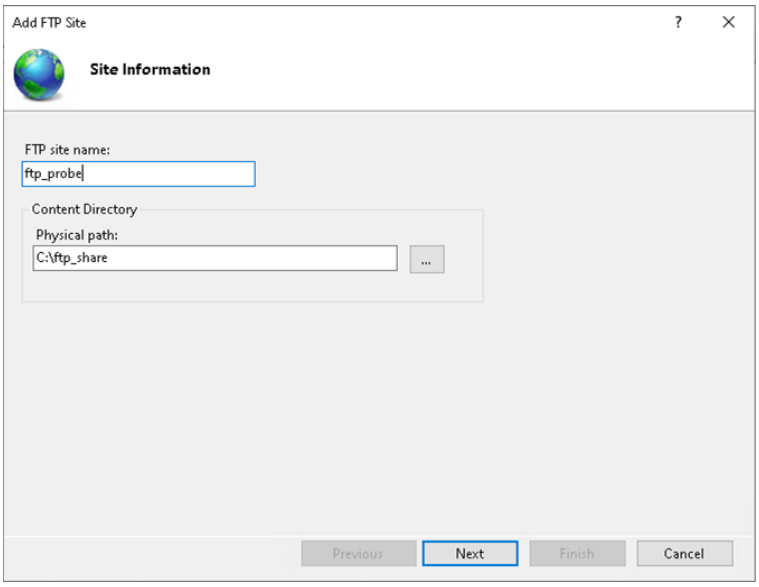
   C:\ftp_share

> **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.

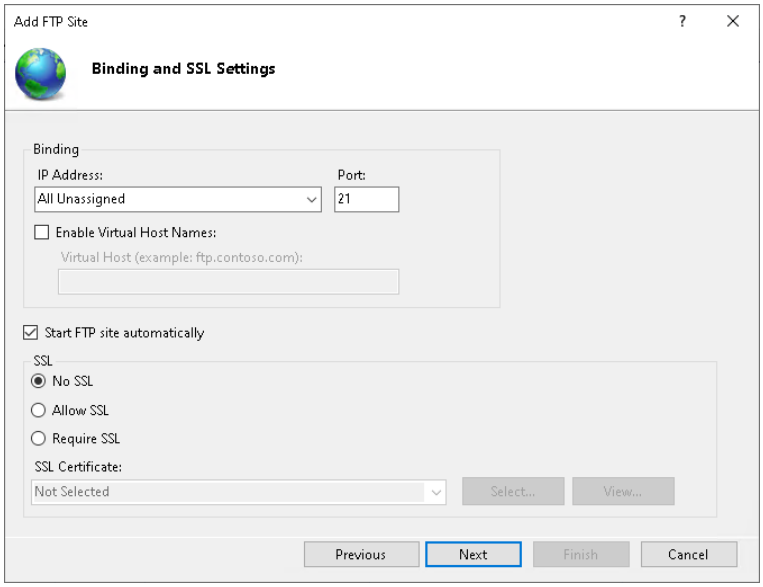
2. Navigate to **Start menu / Internet Information Services (IIS) Manager**.
3. On the left panel click on the arrow to unfold additional items.
4. Right click on "**Sites**".
5. Select the "**Add FTP Site...**" option.



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



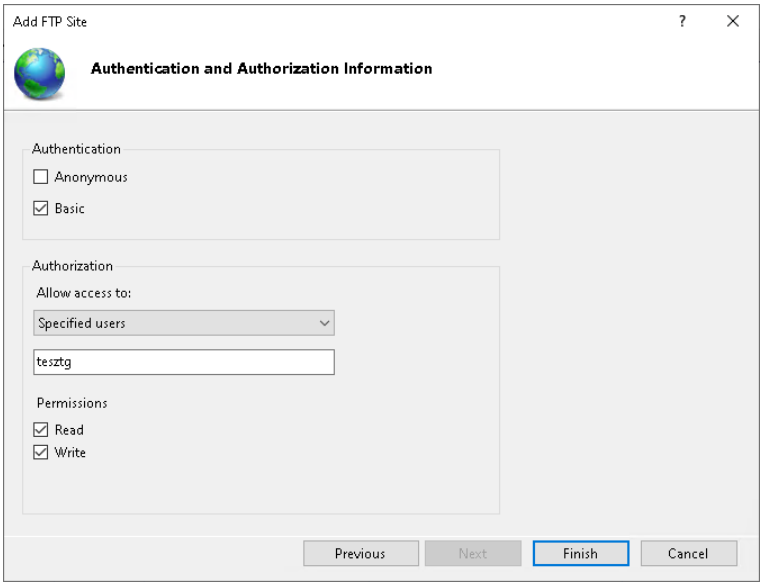
7. Then, click on the [Next] button.
8. In the next window select "No SSL". Leave the rest of the settings as default:
   - IP address: "All Unassigned"
   - Port: "21"
   - Enabled "Start FTP site automatically"



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**".

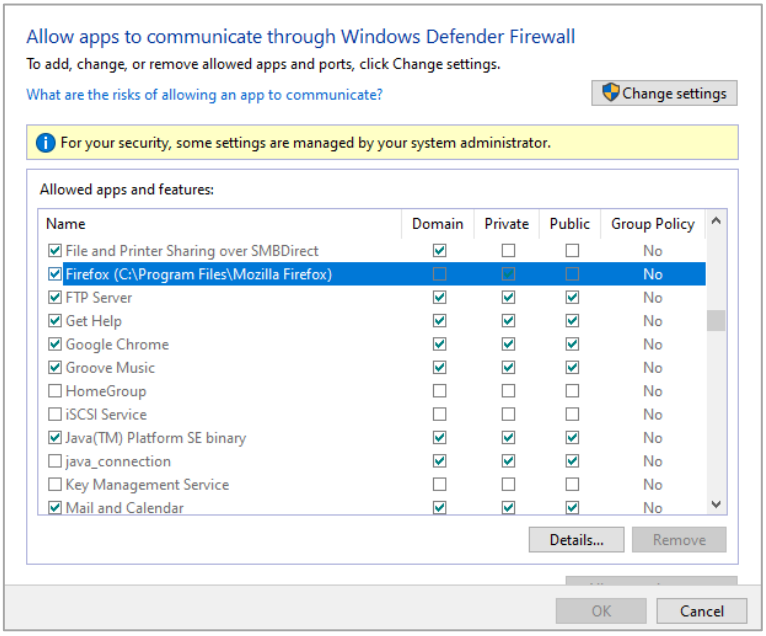


11. Then, click on **[Finish]**.

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.

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:

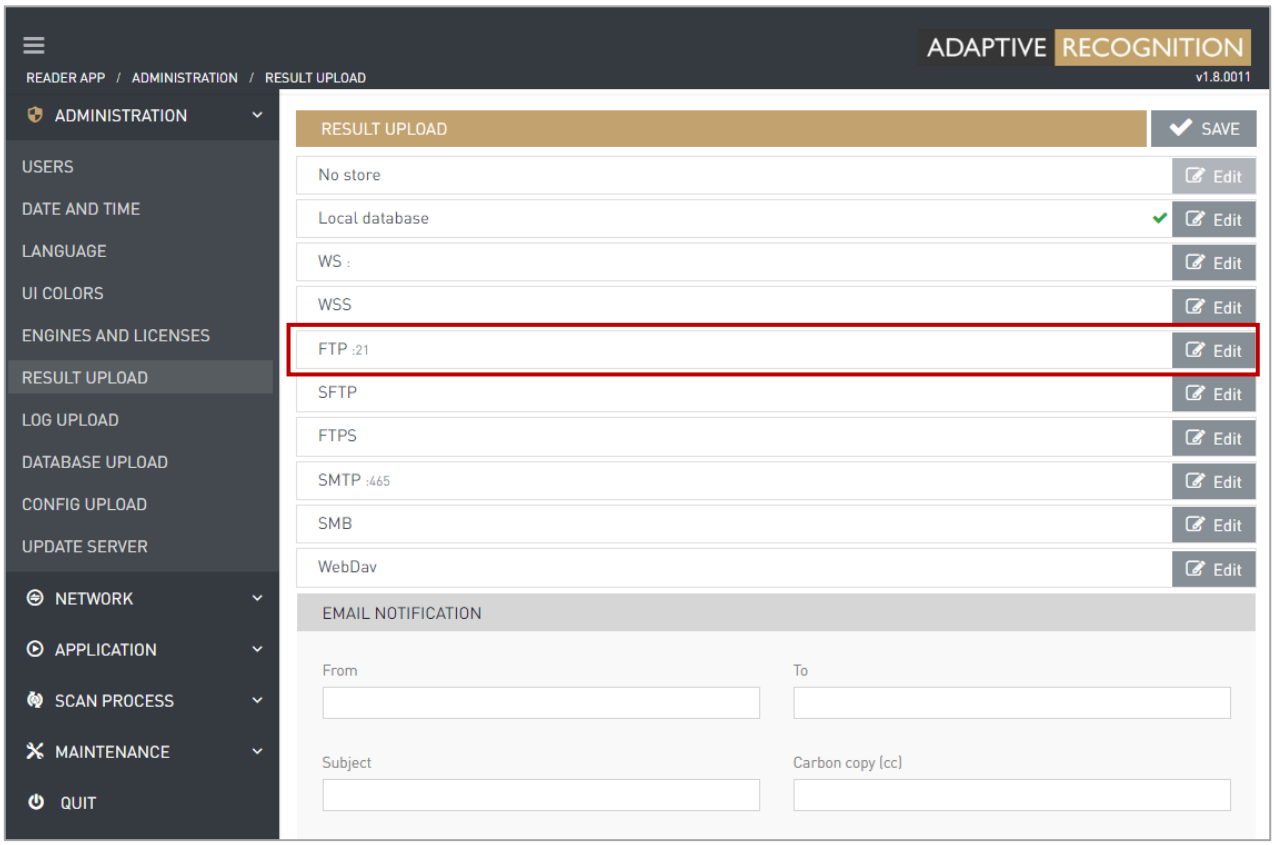
- `sudo ufw allow 20:21/tcp`
- `sudo ufw allow 30000:31000/tcp`
- `sudo ufw disable`
- `sudo ufw enable`

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

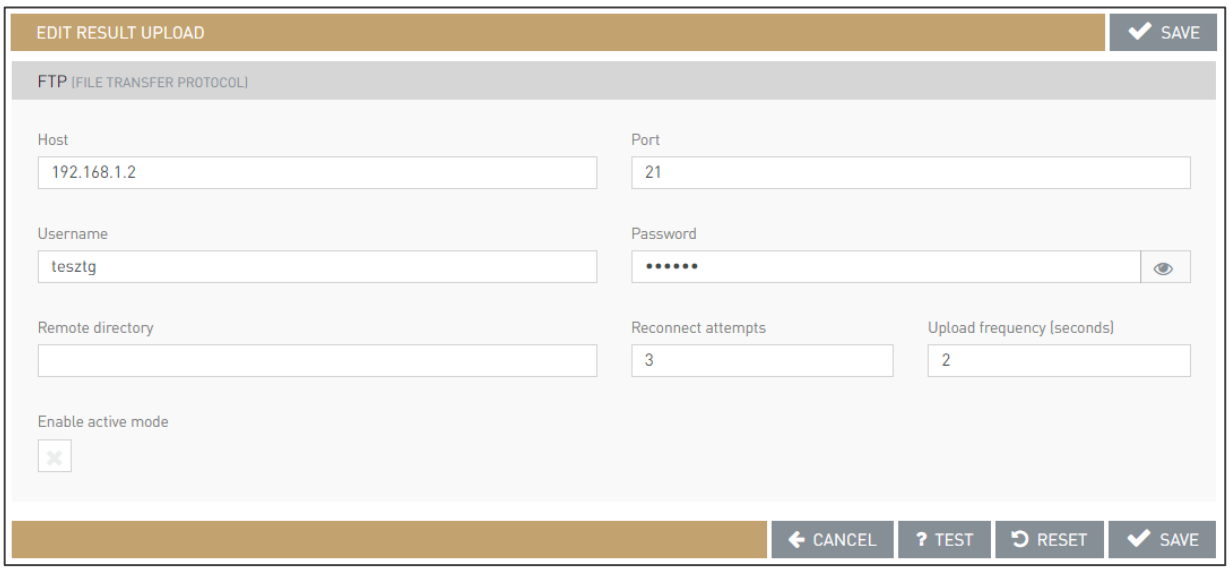
14.3. SETTING ON OSMOND

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.



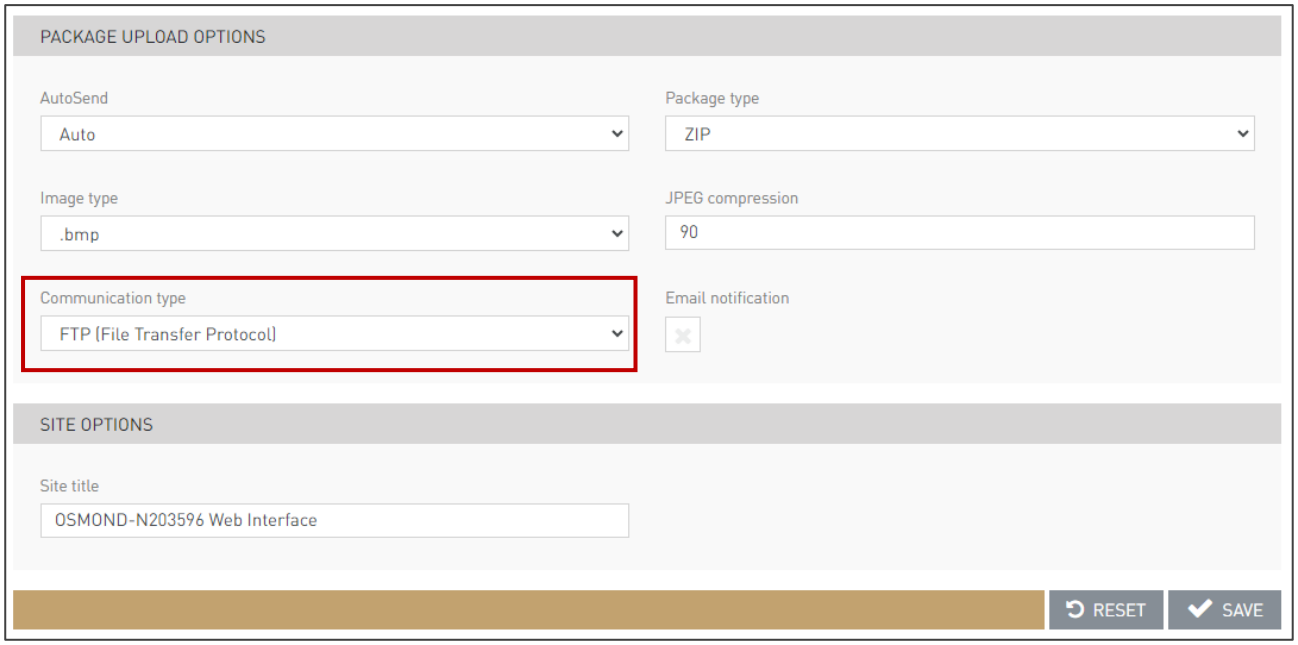
4. On the appearing menu set the following:
   - Host: IP address of the FTP server, in this case: 192.168.1.2
   - Port: Port of the FTP server: 21
   - Username: Name of the user, in this case: tesztg
   - Password: Password of the user, in this case: 123456
   - Remote directory: Name of the folder 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.

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.

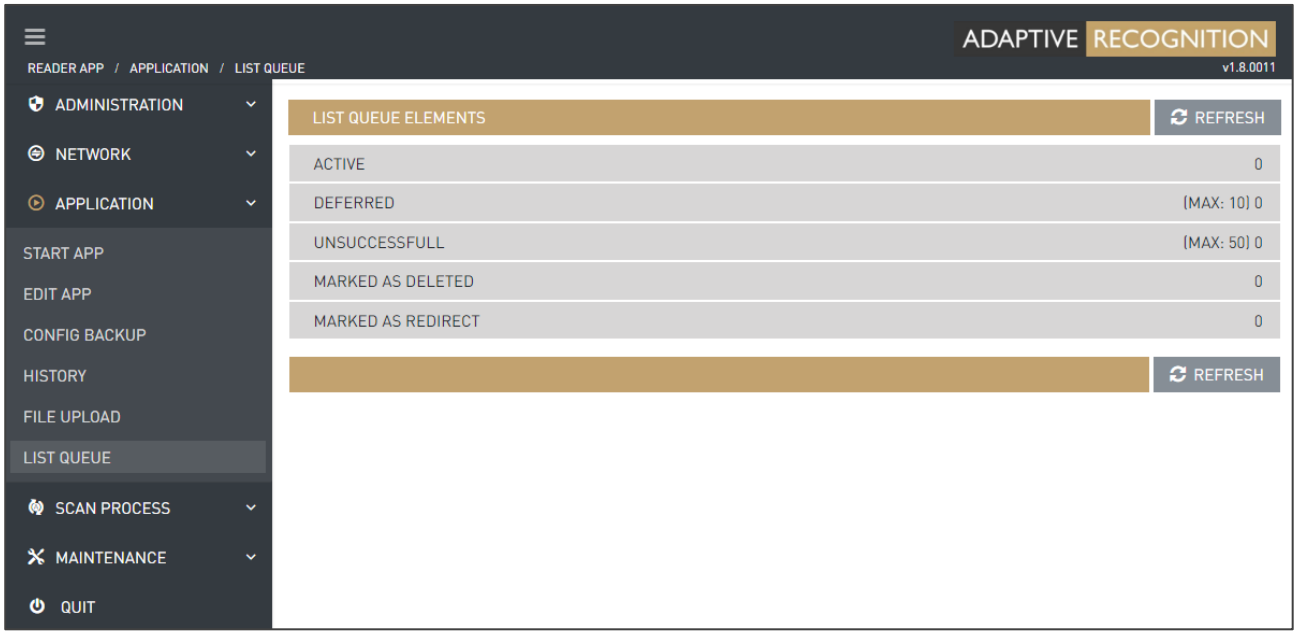
192.168.1.2 is the IP address of the FTP server.

> **Note**
>
> In case of error, the **curl** command will give a more detailed description than the web interface of Osmond.

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.

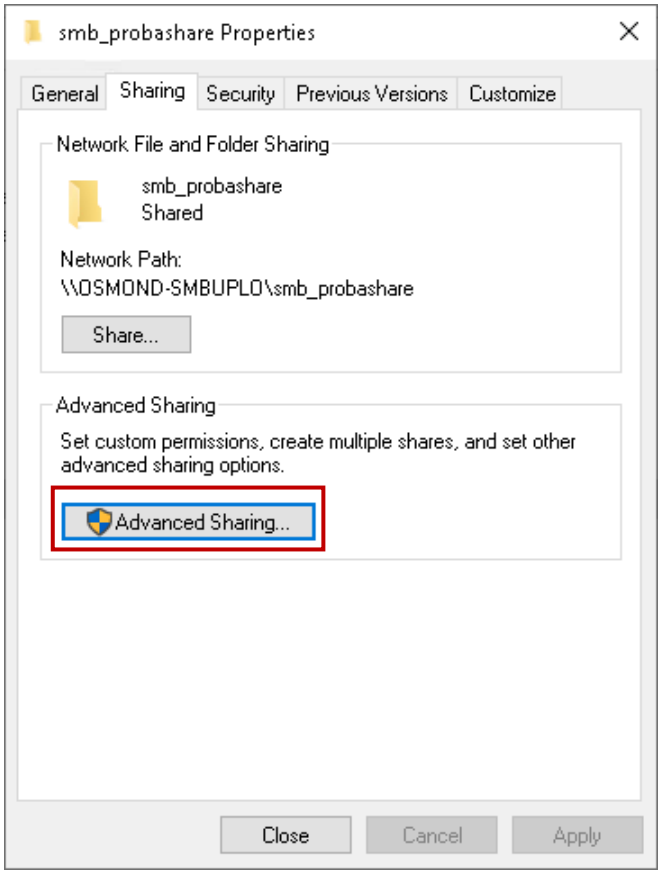
The parameters are the following:

- 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

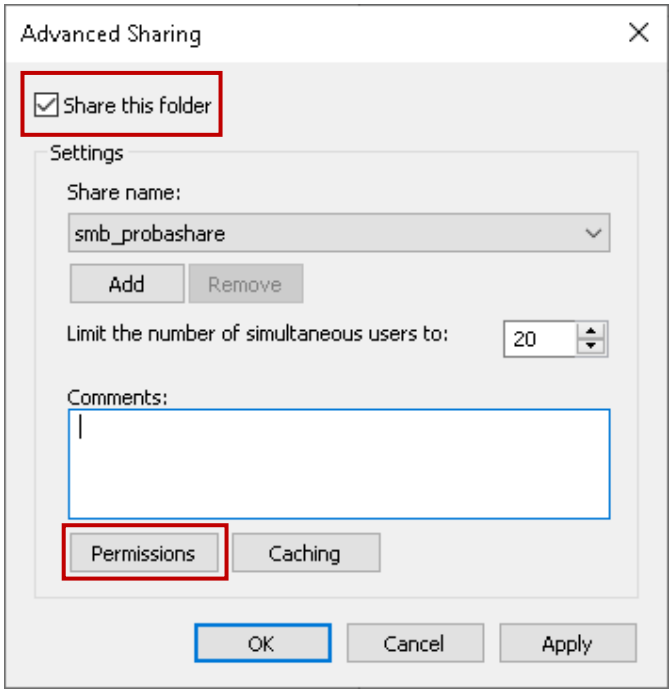
15.1. SETTING SMB ON WINDOWS 10

15.1.1. SHARING THE LIBRARY ON THE NETWORK

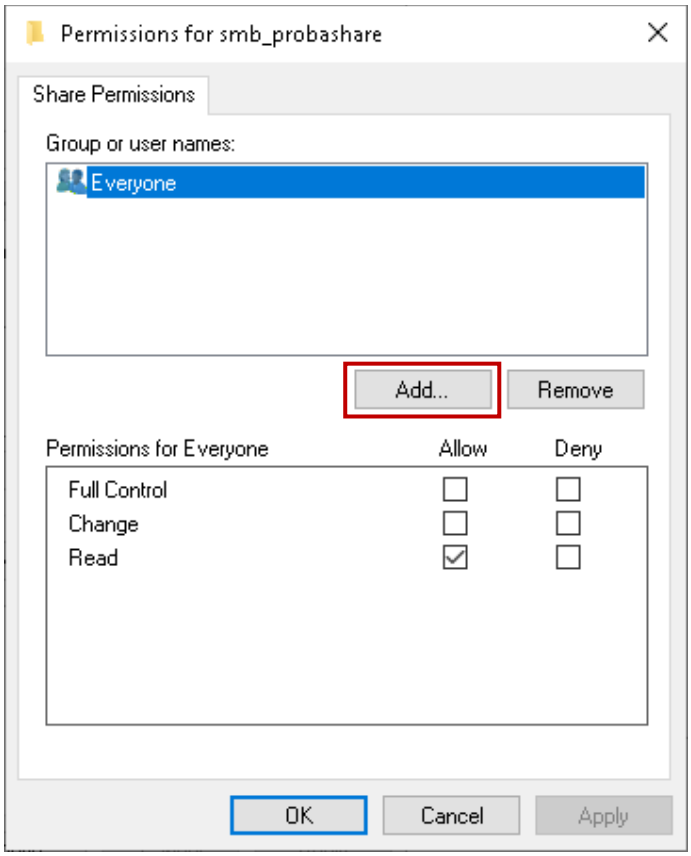
1. Create the library, for example:
   C:\smb_probashare
2. Right click on the library in the File Explorer, and from the appearing menu select "Properties".
3. In the pop-up window select the "Sharing" tab.
4. On the "Sharing" tab click on the [Advanced Sharing...] button.



5. Enable "Share this folder" by ticking the box
6. Click on the [Permissions] button.

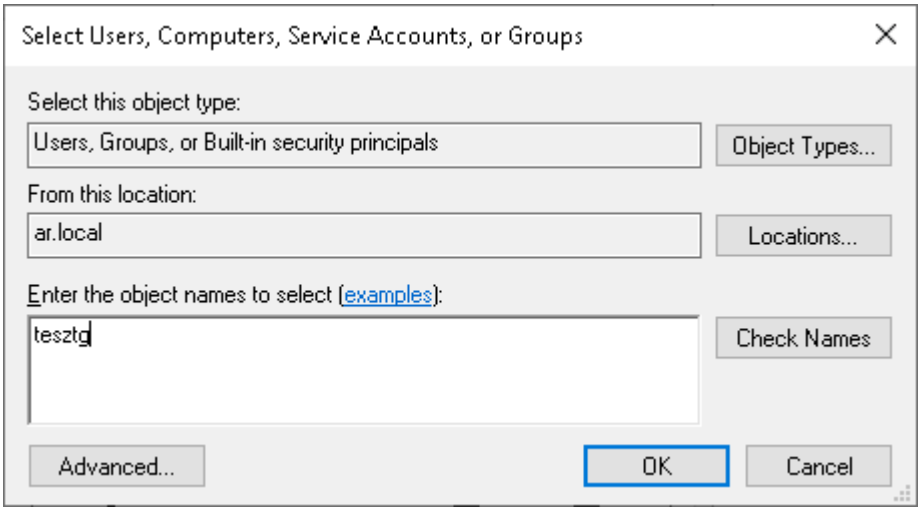


7. Then, click on the [Add...] button.

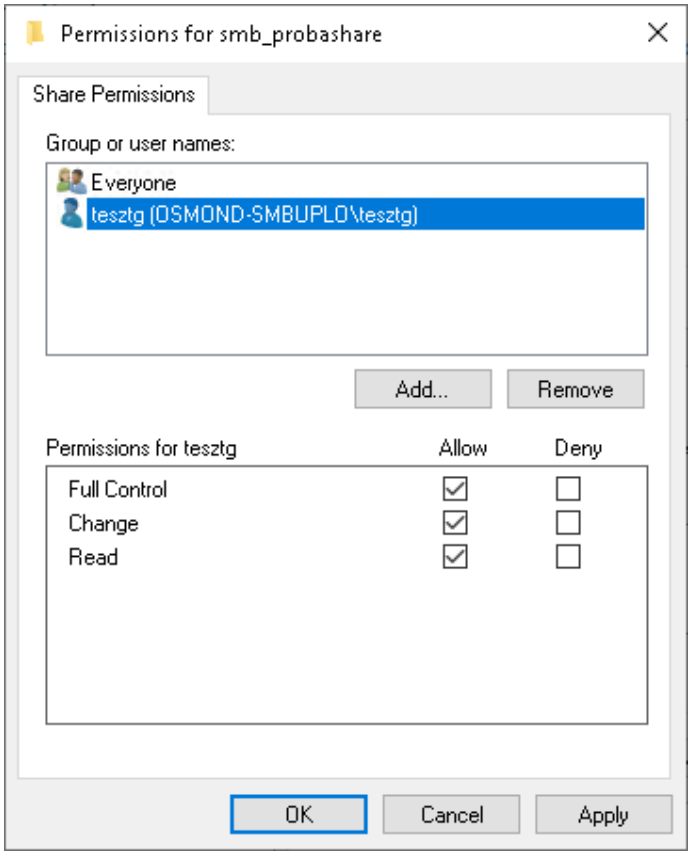


8. In the appearing window enter the name of the user on whose behalf the upload is performed. For example: tesztg

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.



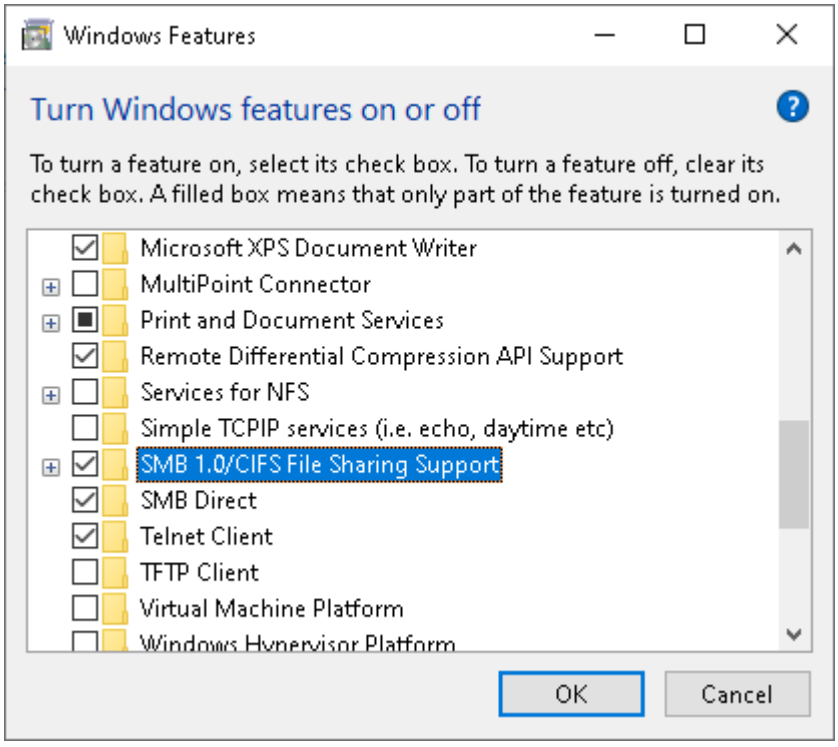
11. Afterwards click the [Apply], then the [OK] buttons.
12. Click on the [OK] button again.
13. Then, click on the [Close] button.

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.

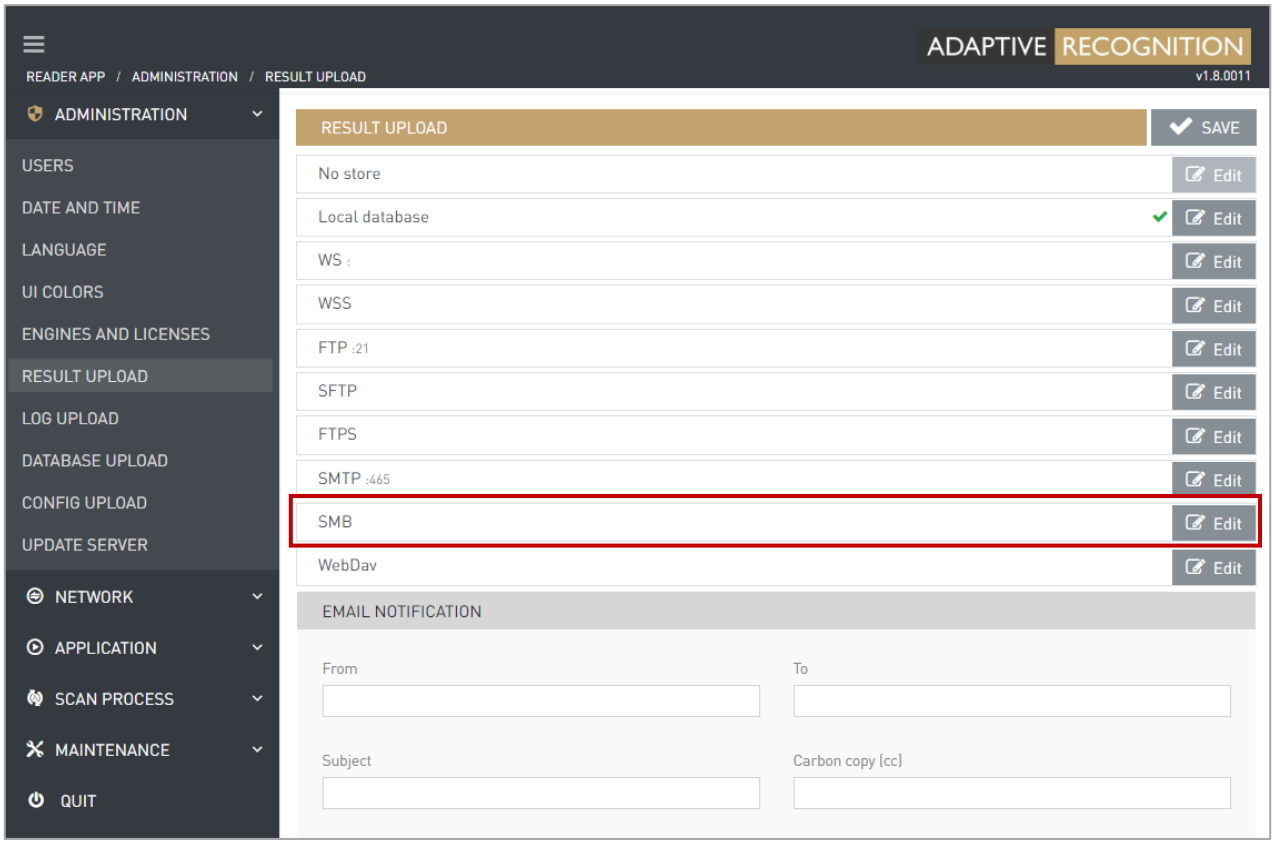


4. Restart the PC.

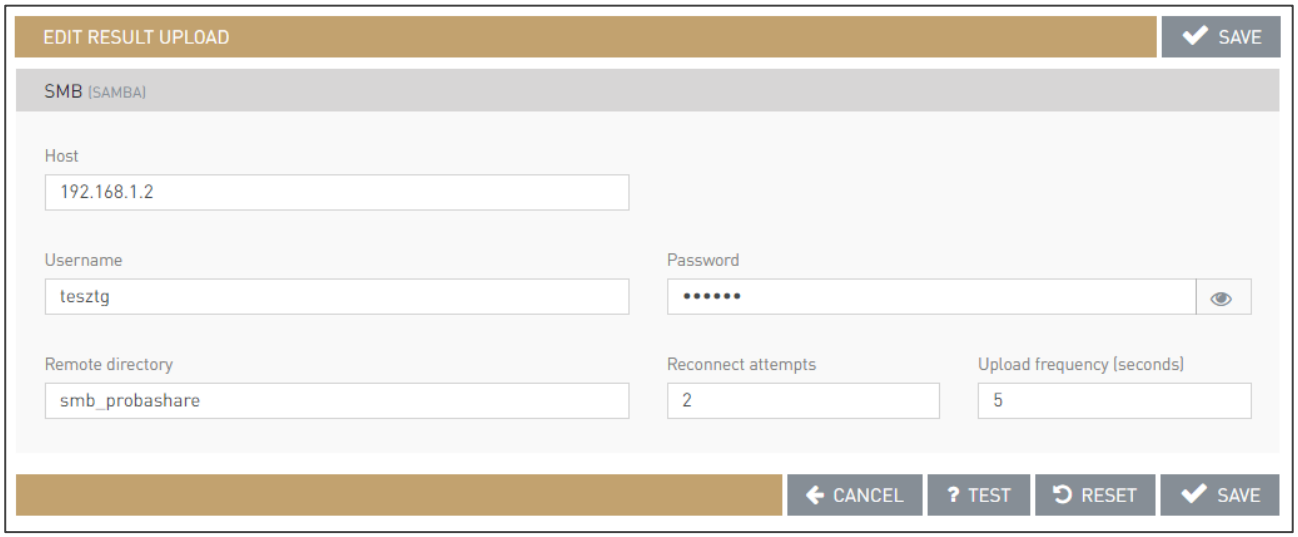
15.2. SETTING ON OSMOND

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.

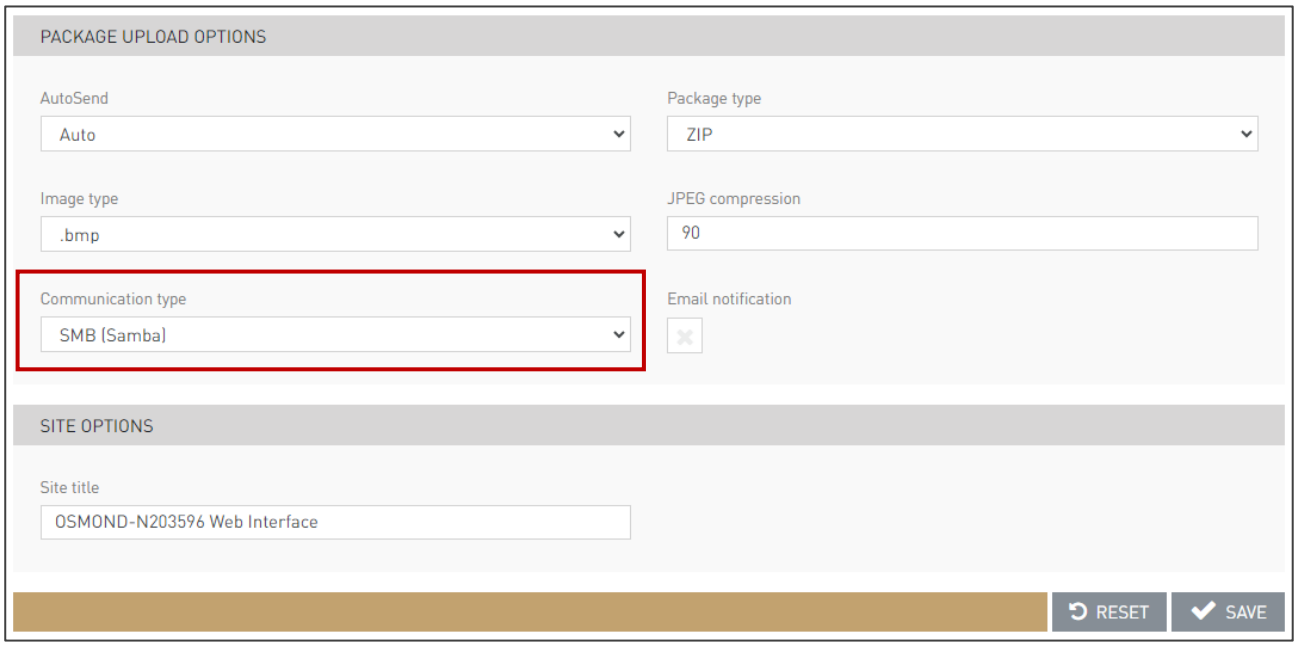


4. On the appearing menu set the following:
   - **Host**: IP address of the SMB server, in this case: 192.168.1.2
   - **Username**: Name of the user, in this case: tesztg
   - **Password**: Password of the user, in this case: 123456 (This password is required for the tesztg user to sign in to Windows 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.

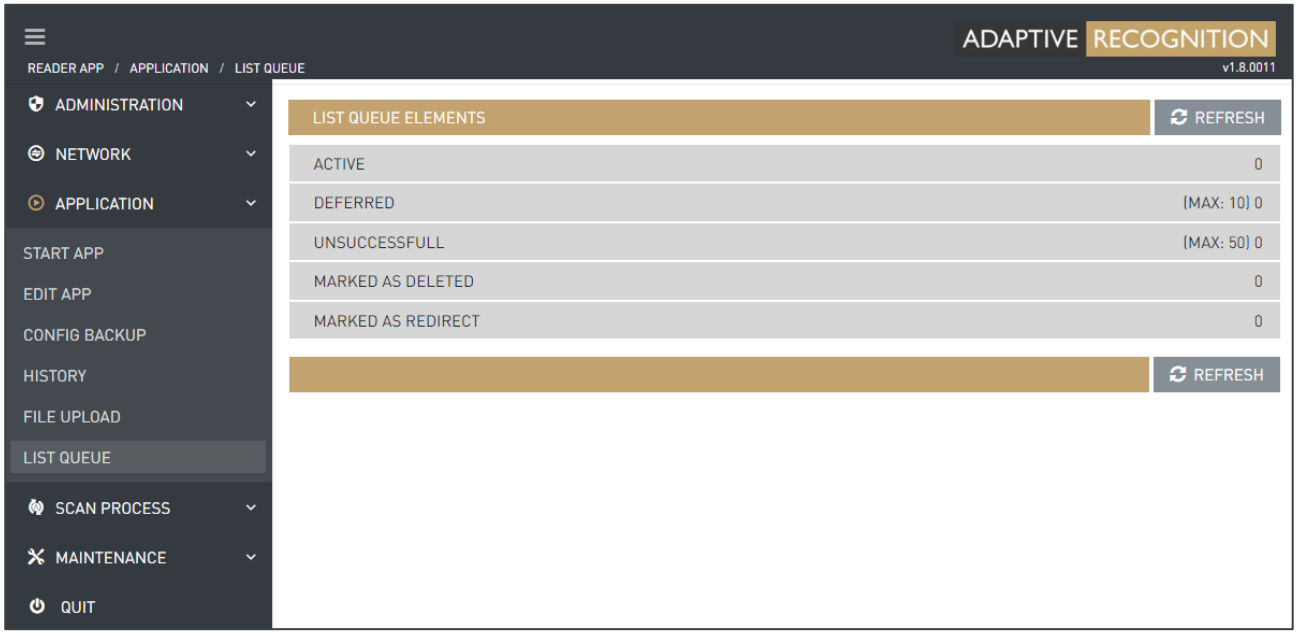
smb_probashare is the shared folder, actually a path, without marking the C: drive.

> **Note**
>
> In case of error, the **curl** command will give a more detailed description than the web interface of Osmond.

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

15.4. TROUBLESHOOTING

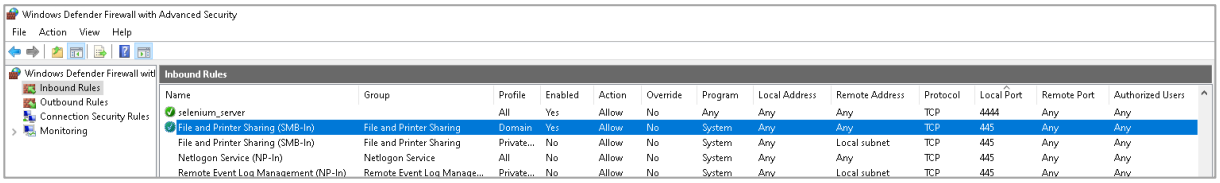
If upload is not working, Osmond will collect the unsuccessful documents to the **UNSUCCESSFUL queue** until its limit is not reached. When **UNSUCCESFUL** limit is reached, the oldest element in queue is overwritten by the result of the latest scan. Documents in unsuccessful status can be checked in the **APPLICATION / LIST QUEUE** menu. In case of correct operation this row is empty.



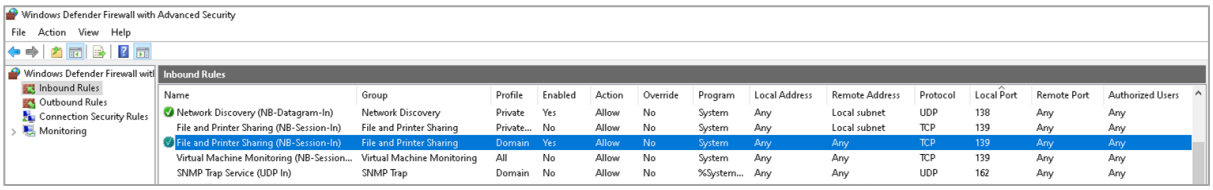
If upload is not working, then the Windows Firewall or another network device may be blocking it.

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.

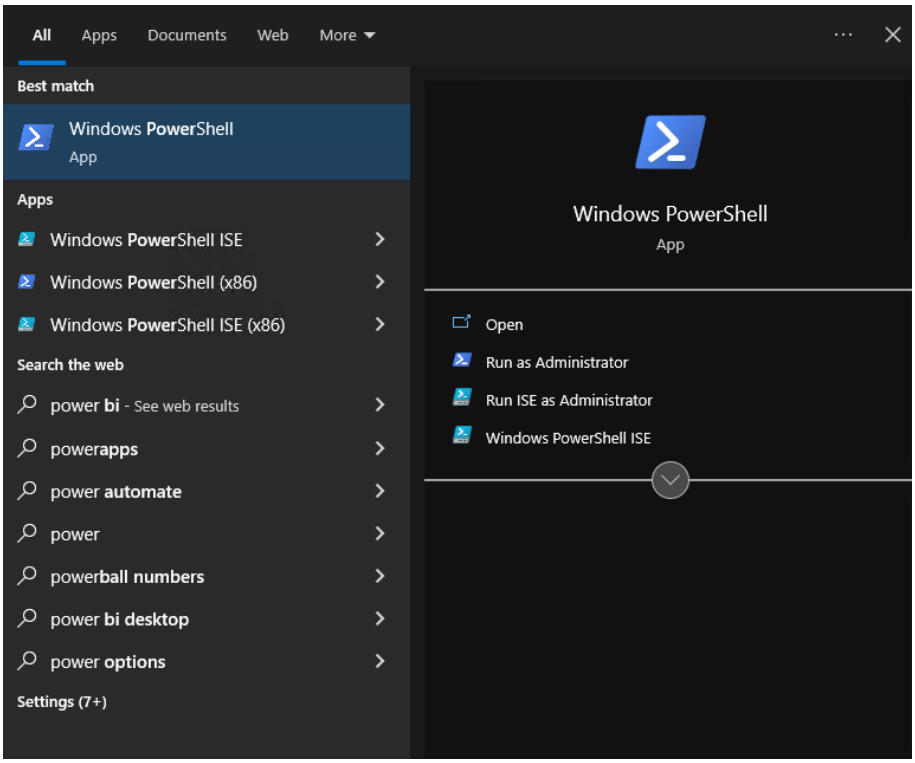
The parameters are the following:

- 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
```

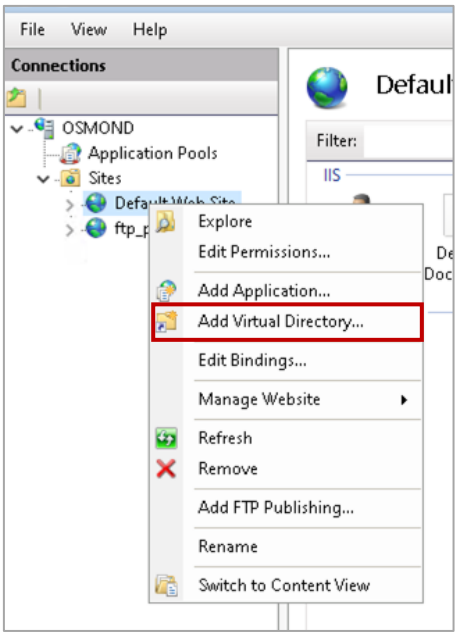
3. Copy the following command to the terminal, and press [Enter]:

```
$feats = @("IIS-WebServerRole","IIS-WebServer","IIS-CommonHttpFeatures","IIS-HttpErrors","IIS-Security","IIS-RequestFiltering","IIS-WebServerManagementTools","IIS-DigestAuthentication","IIS-StaticContent","IIS-DefaultDocument","IIS-DirectoryBrowsing","IIS-WebDAV","IIS-BasicAuthentication","IIS-ManagementConsole");foreach ($feat in $feats) {Enable-WindowsOptionalFeature -Online -FeatureName $feat};&"$env:windir\system32\inetsrv\InetMgr.exe";
```

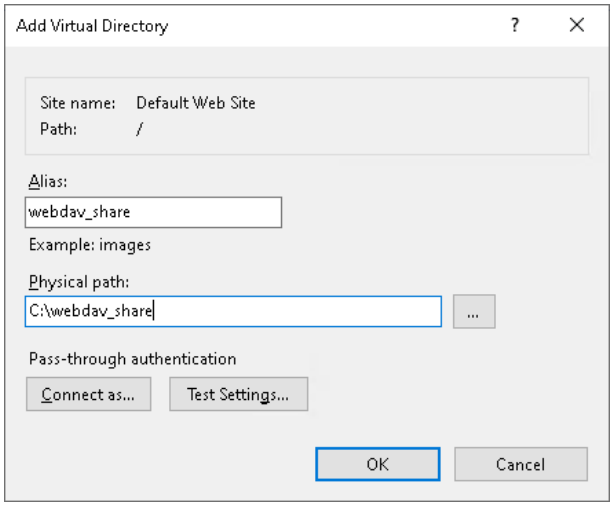
   - This command installs the Internet Information Services (IIS) modules which are required for the installation and setup of WebDav.
   - Starts the IIS Manager.

16.1.2. SETTING WEBDAV

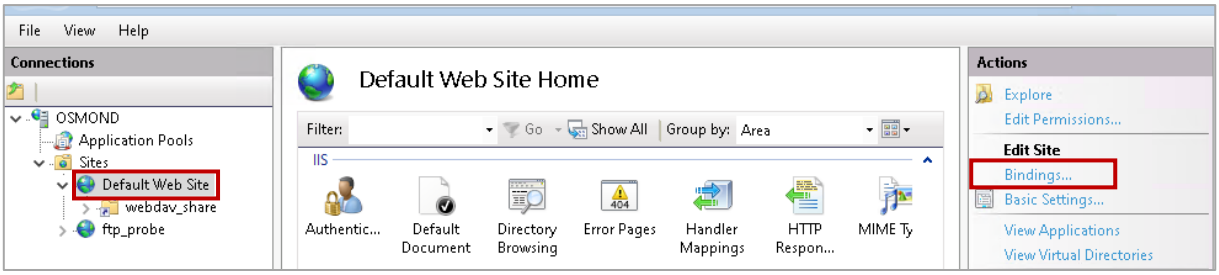
1. After running the command, the ISS Manager (Internet Information Services (IIS) Manager) opens.
2. Under Connections (located on the left) click on the arrow next to the computer name to unfold additional items.
3. Then, click on the arrow next to the Sites to unfold its submenu.
4. In the appearing 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.

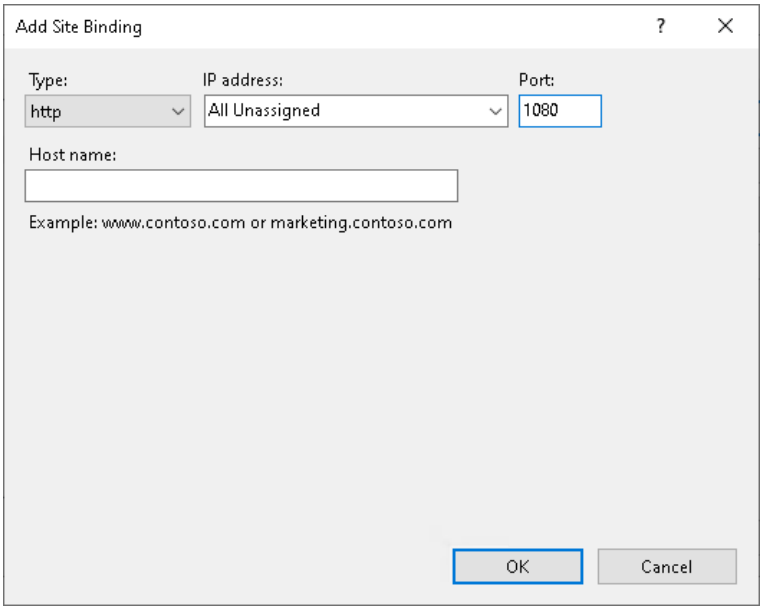


9. Under the **Connections** tree located on the left side of the IIS Manager window click on the **[Default Web Site]** option.
10. Under the **Actions** tree located on the right side of the IIS Manager window click on the **[Bindings...]** button.

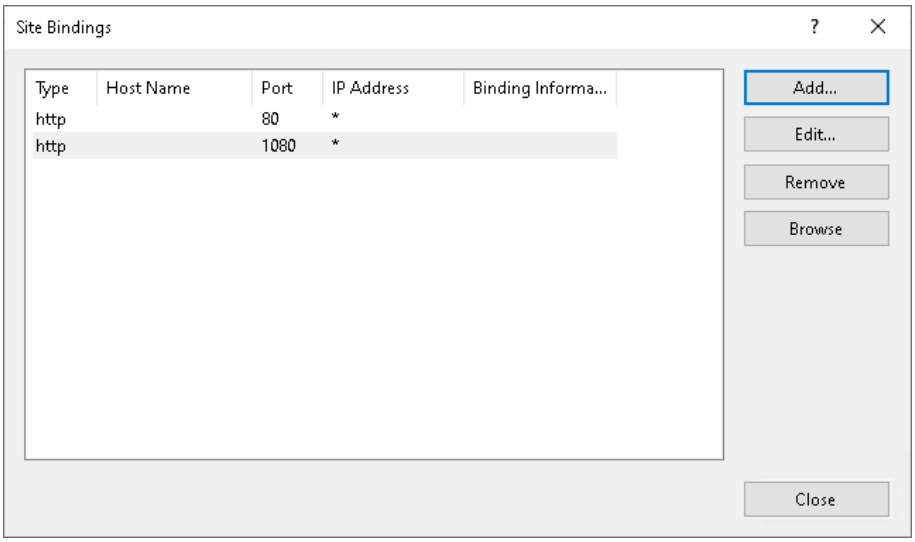


11. In the appearing window click on the **[Add...]** button.

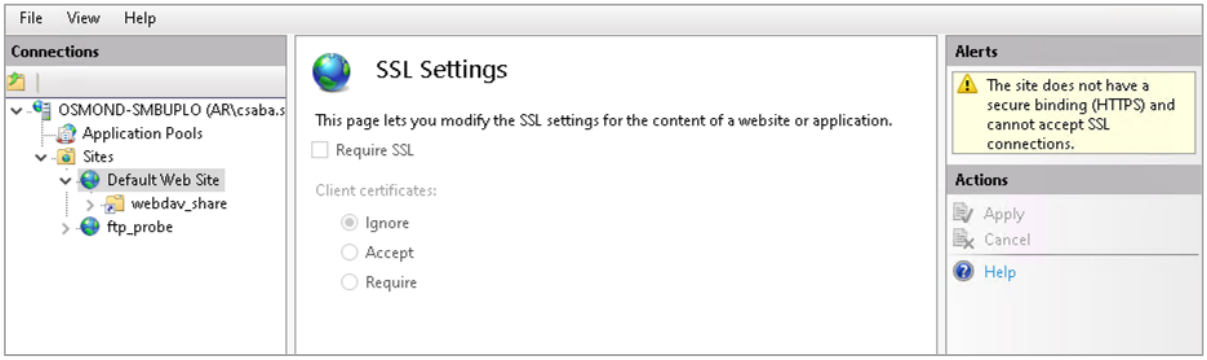
12. In the appearing **Add Site Binding** window select "http" under the **Type** parameter.
13. Under **IP address** keep the default option: "All Unassigned".
14. Enter the value "1080" to the **Port** field.
15. Click on the **[OK]** button.



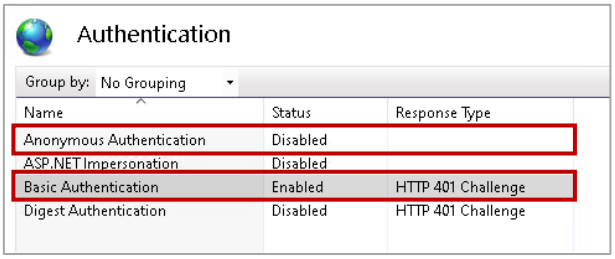
16. In the **Site Bindings** window click on the **[Close]** button.



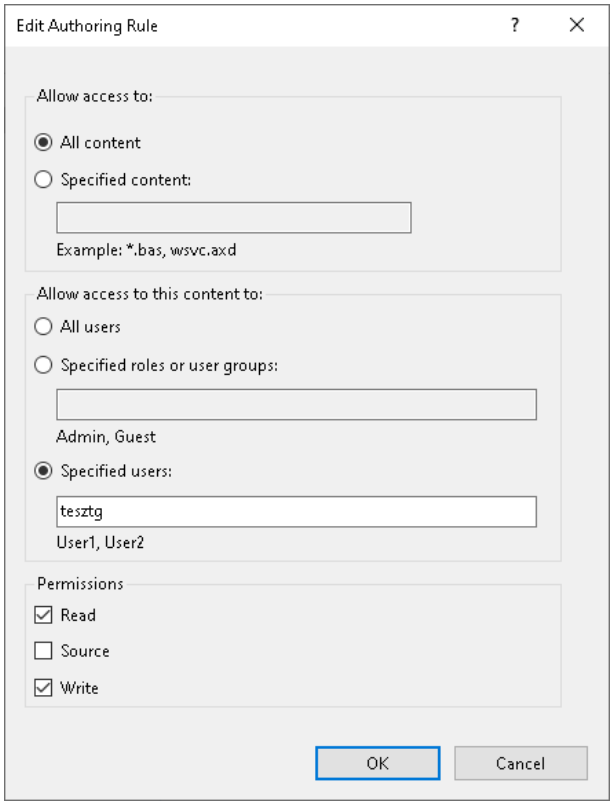
17. Under the **Connections** tree located on the left side of the IIS Manager window click on the **[Default Web Site]** option.
18. Double click on the **[SSL Settings]** icon located in the middle part of the window.
19. In the appearing window the "**Require SSL**" function must be disabled.
20. 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.

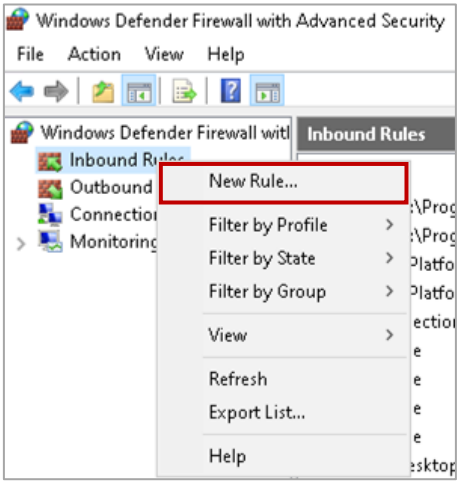
39. Under the **Connections** tree located on the left side of the IIS Manager window click on the **[Default Web Site]** option.
40. Then, under the **Manage Website** tree located on the right side of the IIS Manager window click on the **[Restart]** button.

> **Note**
>
> It is recommended to restart the PC as well.

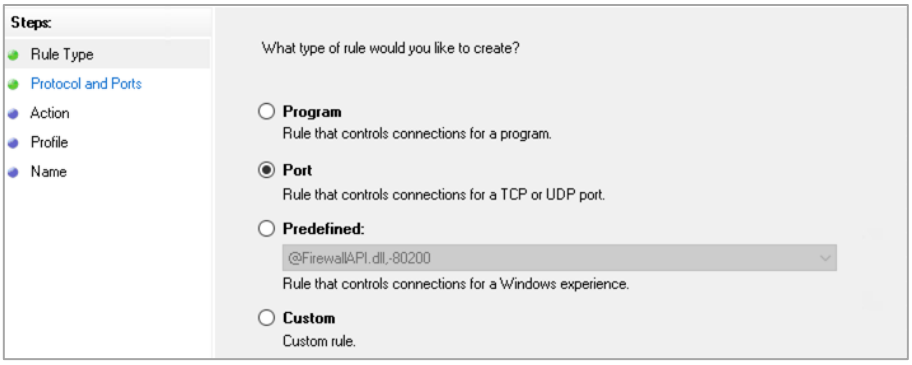
16.1.3. SETTING THE FIREWALL

It is recommended to check the Windows Firewall settings:

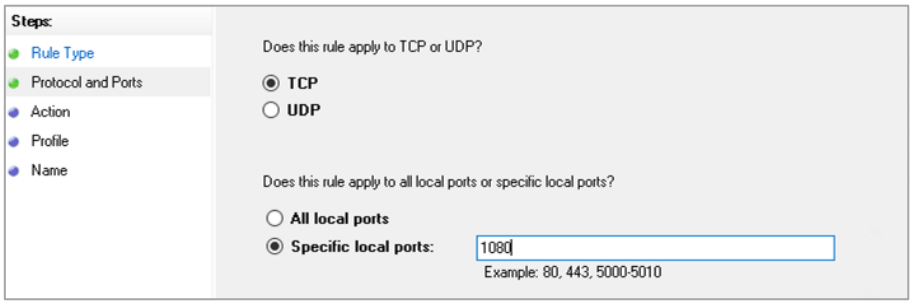
1. Navigate to **Control Panel / System and Security / Windows Defender Firewall / Advanced settings**.
2. Right click on **[Inbound rules]** located in the left section.
3. Select **New Rule...** from the appearing quick menu.



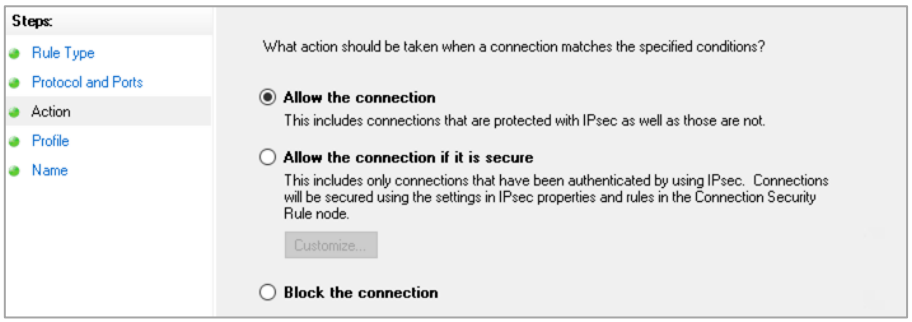
4. In the pop-up window select **Port**.
5. Then, click on the **[Next >]** button.



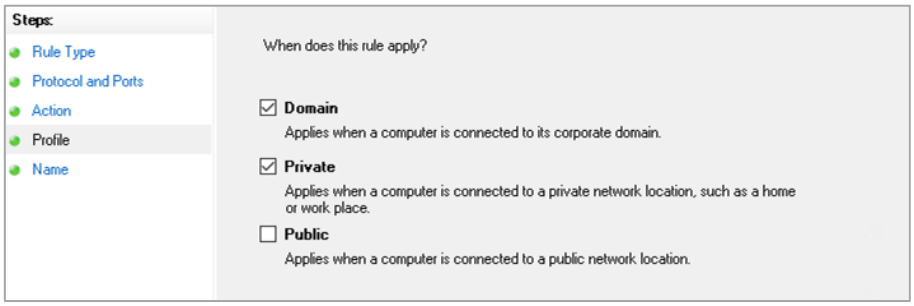
6. At "Does this rule apply to TCP or UDP?" select TCP.
7. At "Does this rule apply to all local ports or specific local ports?" select "Specific local ports" and enter the value 1080 to the text field.
8. Then, click on the [Next >] button.



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.

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

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

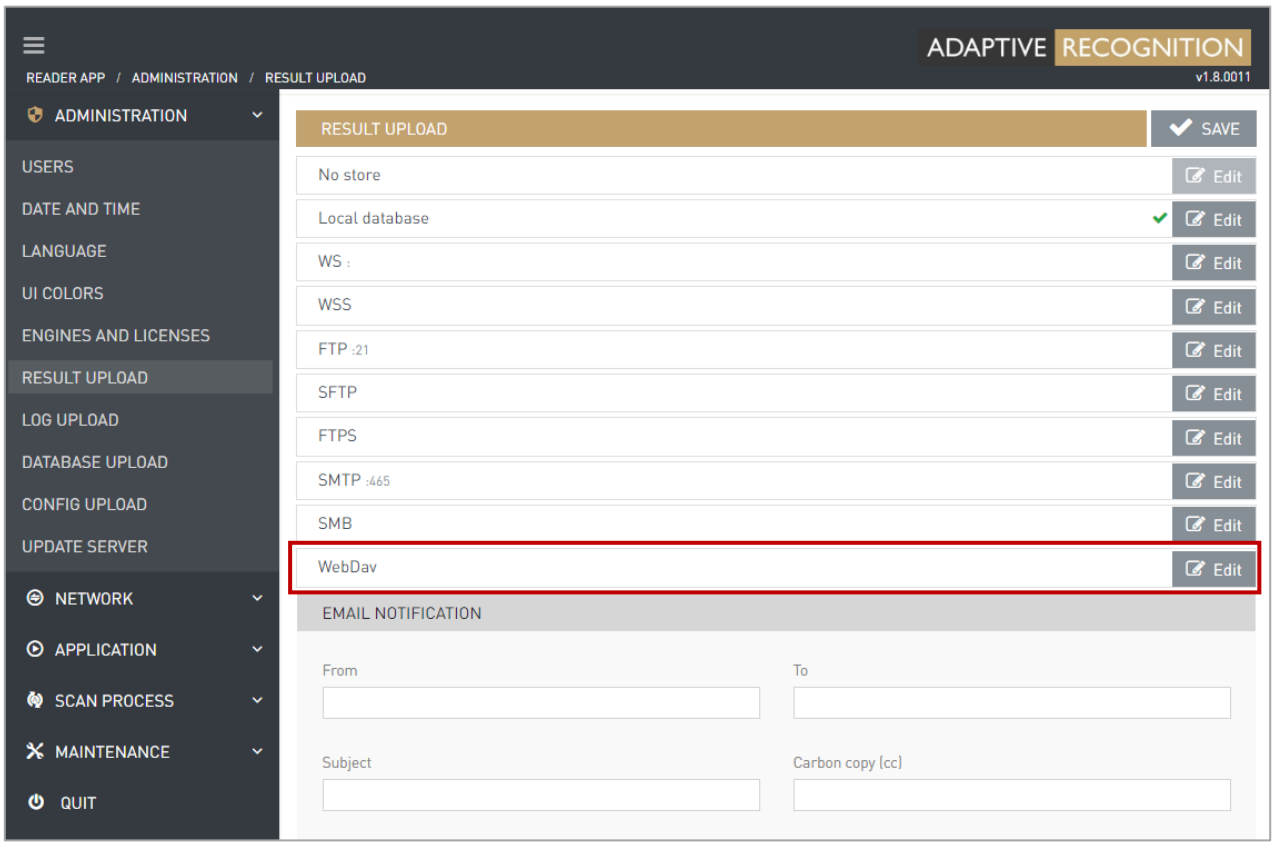
The ports used by WebDav must be set in the firewall, then restart it, if the firewall is active. On Ubuntu the `ufw` is the default firewall. Its state can be queried with the `sudo ufw status` command.
If it is active, then:

- `sudo ufw allow 1080/tcp`
- `sudo ufw disable`
- `sudo ufw enable`

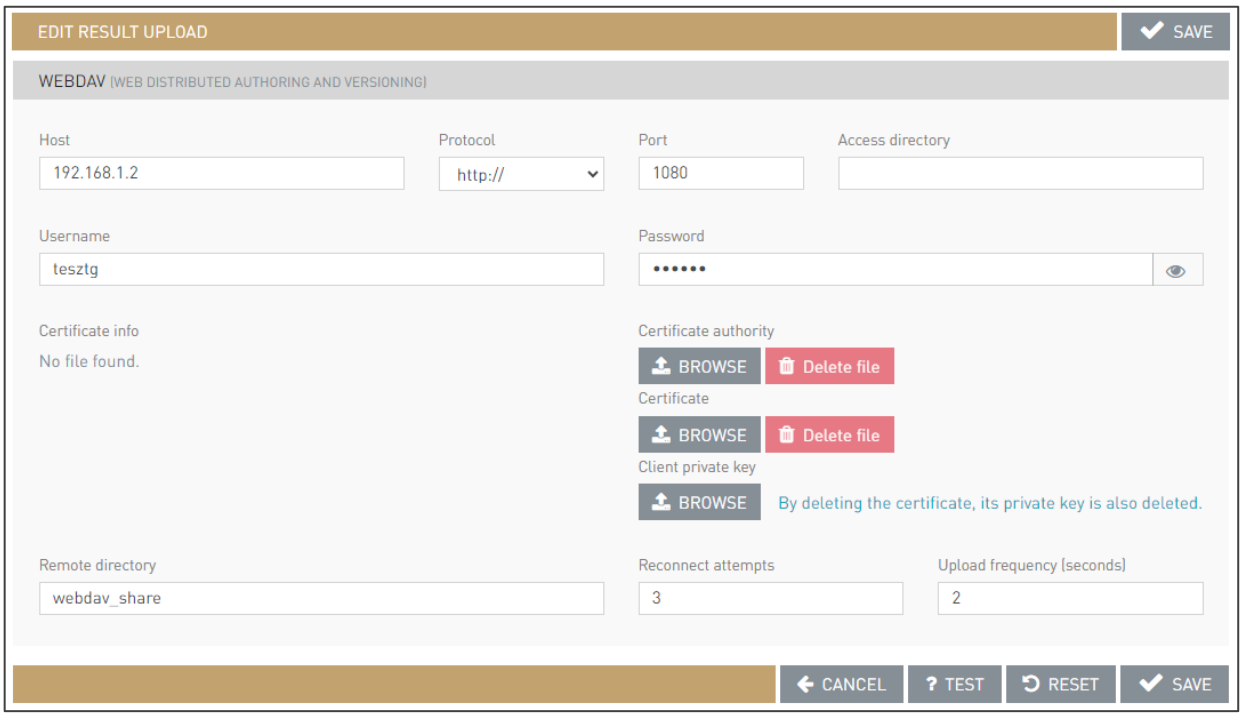
16.3. SETTING ON OSMOND

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



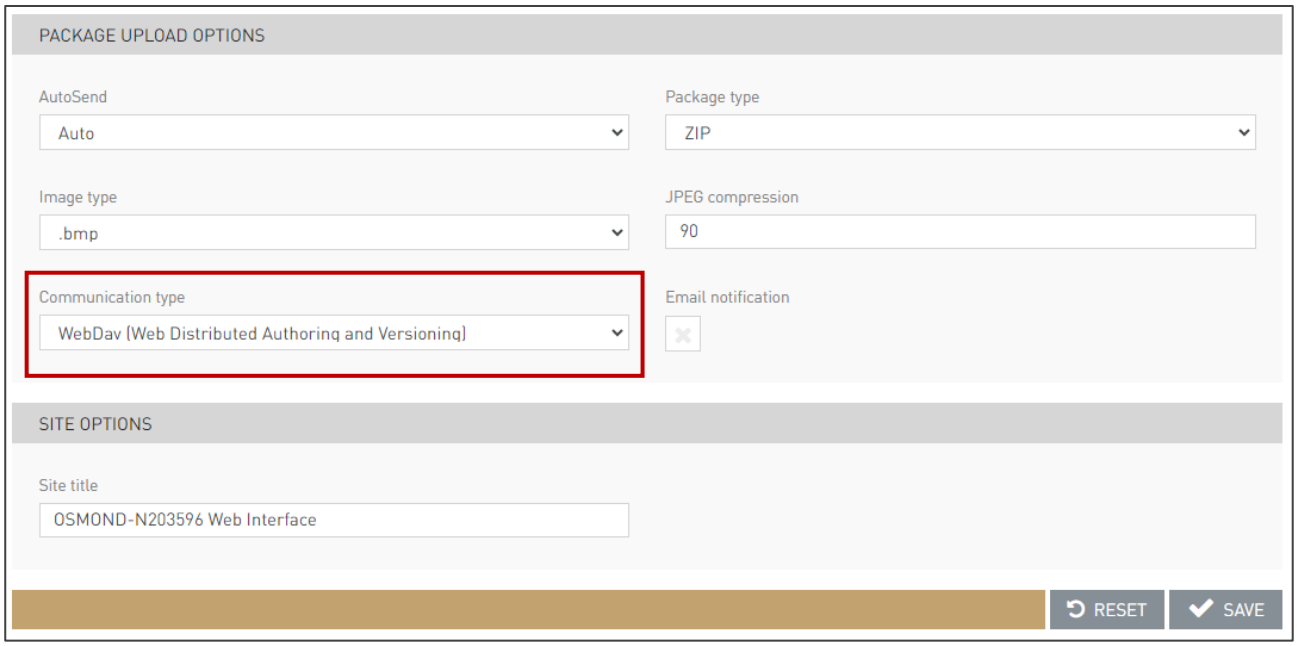
5. Check the correct settings are applied by clicking on the [TEST] button.
   Every test result must be passed (green).

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.

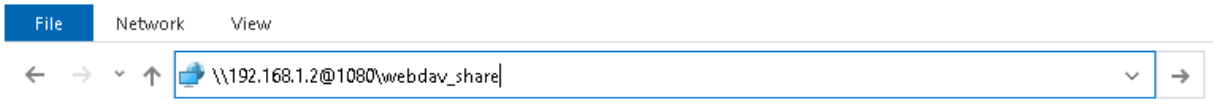


16.4. TESTING THE SETUP

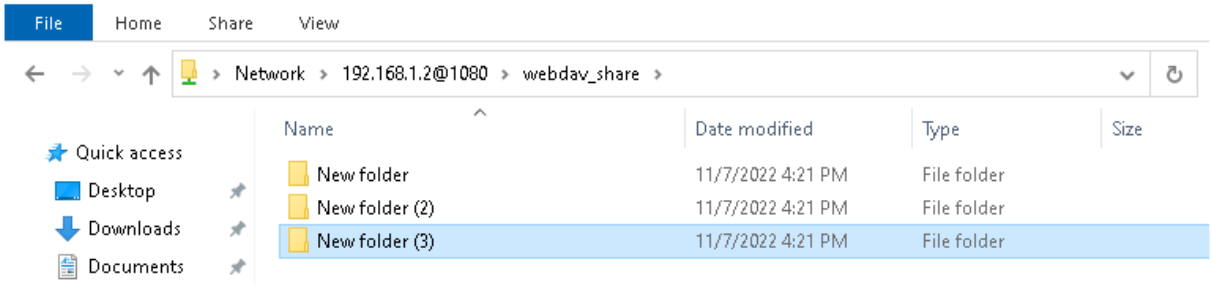
16.4.1. WINDOWS

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



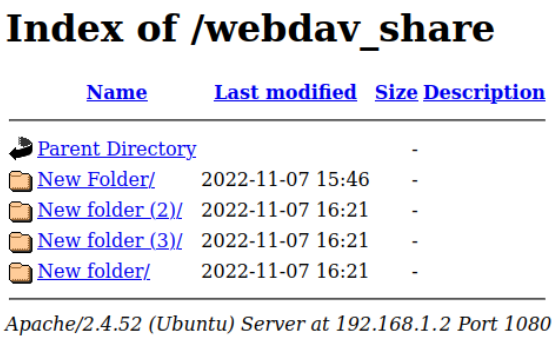
2. Then, press [Enter].
3. After successful connection, Windows requests the username and password.
4. Then, the content of the WebDav directory appears, and can be browsed as a file system.



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:



Index of /webdav_share

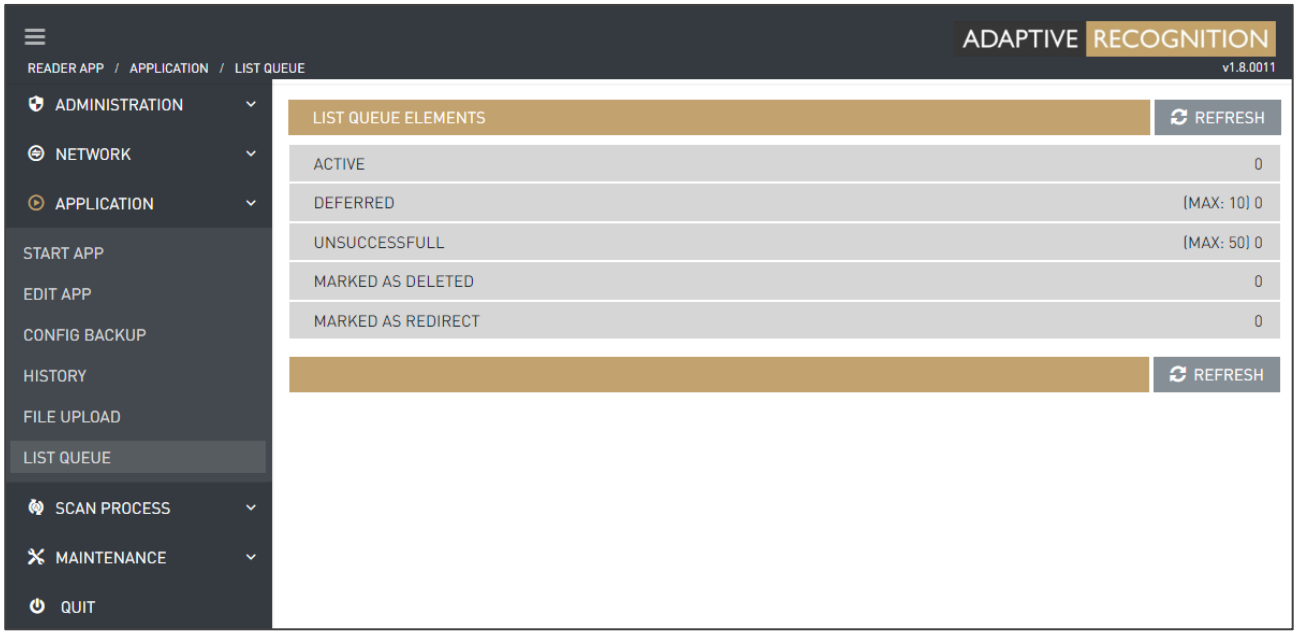
Name	Last modified	Size	Description
Parent Directory		-	
New Folder/	2022-11-07 15:46	-	
New folder (2)/	2022-11-07 16:21	-	
New folder (3)/	2022-11-07 16:21	-	
New folder/	2022-11-07 16:21	-	

Apache/2.4.52 (Ubuntu) Server at 192.168.1.2 Port 1080

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 OSMON

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.

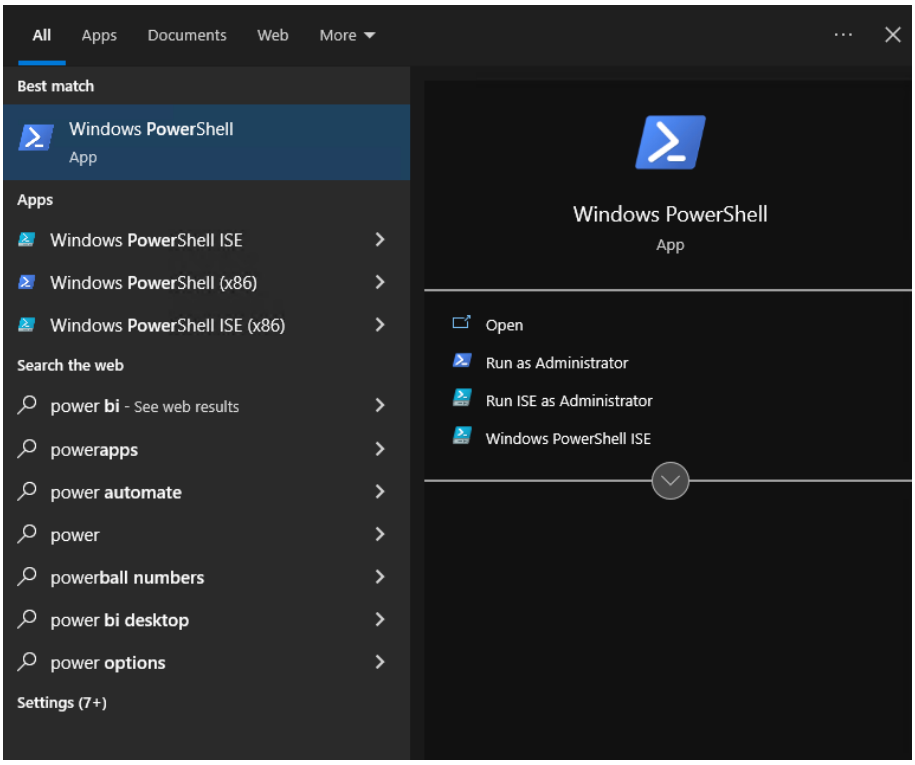
The parameters are the following:

- 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
```

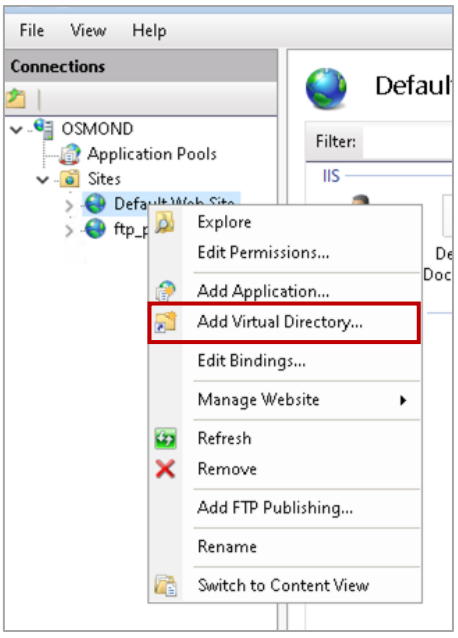
3. Copy the following command to the terminal, and press [Enter]:

```
$feats = @("IIS-WebServerRole","IIS-WebServer","IIS-CommonHttpFeatures","IIS-HttpErrors","IIS-Security","IIS-RequestFiltering","IIS-WebServerManagementTools","IIS-DigestAuthentication","IIS-StaticContent","IIS-DefaultDocument","IIS-DirectoryBrowsing","IIS-WebDAV","IIS-BasicAuthentication","IIS-ManagementConsole");foreach ($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.

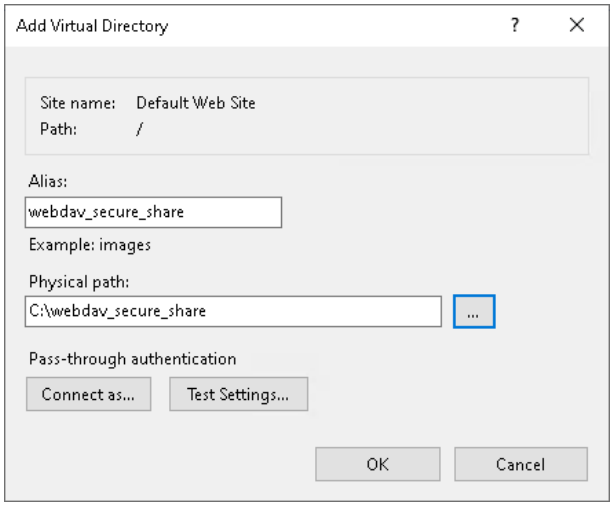
17.1.2. SETTING THE WEBDAV SERVER

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.

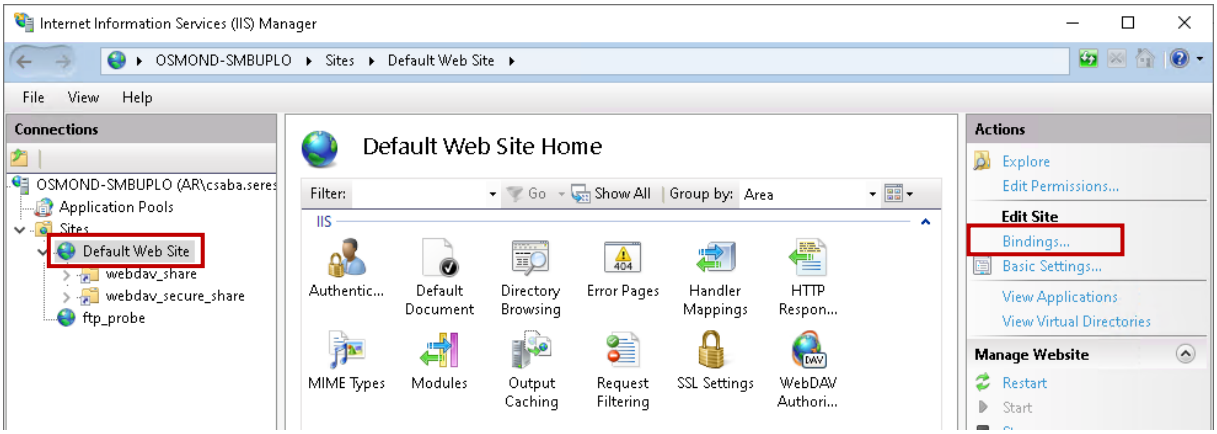


6. Type "webdav_secure_share" to the **Alias** field.
7. Enter the name of the shared folder (or browse it by clicking on the **[...]** button) to the **Physical path** field:
   c:\webdav_secure_share

8. Click on the **[OK]** button.

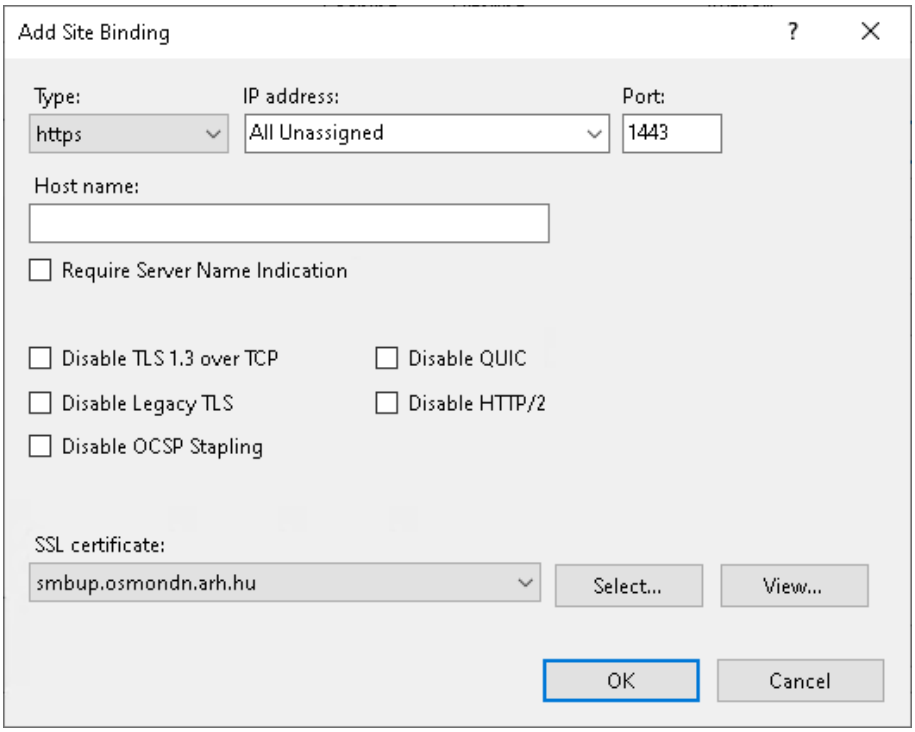


9. Under the **Connections** tree located on the left side of the IIS Manager window click on the **[Default Web Site]** option.
10. Under the **Actions** tree located on the right side of the IIS Manager window click on the **[Bindings...]** button.

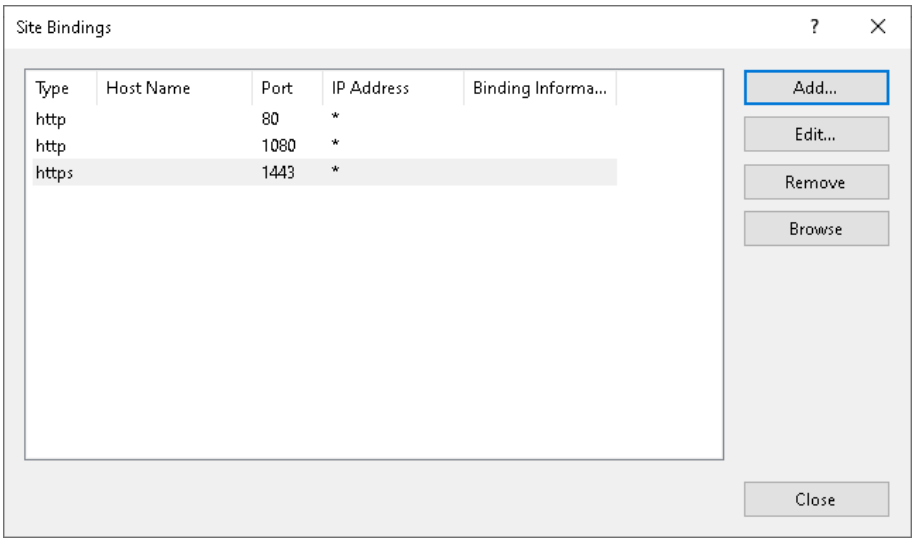


11. In the appearing window click on the **[Add...]** button.

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.

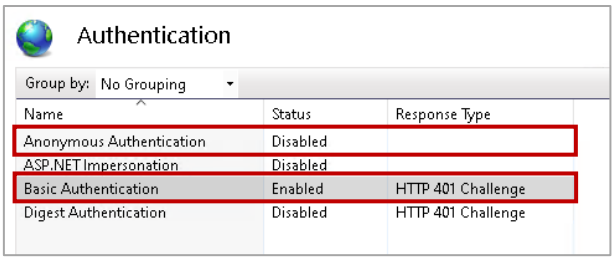


17. In the **Site Bindings** window click on the **[Close]** button.

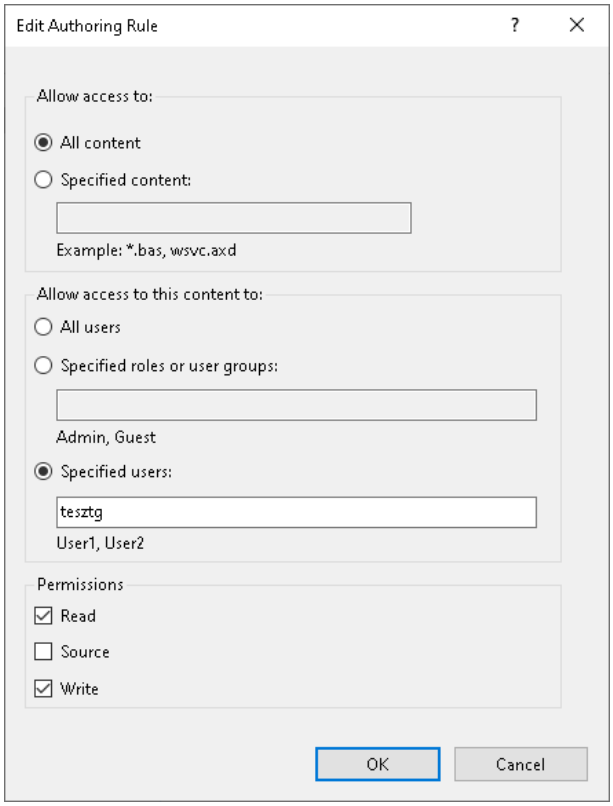


18. Under the **Connections** tree located on the left side of the IIS Manager window click on the **[Default Web Site]** option.
19. Double click on the **[SSL Settings]** icon located in the middle part of the window.
20. In the appearing window the "**Require SSL**" function must be enabled.
21. Under **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.

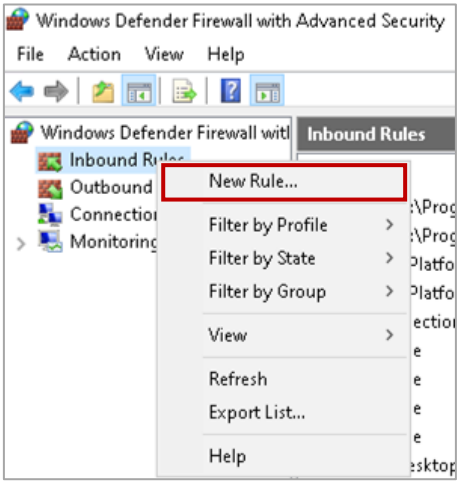


35. Under the **Connections** tree located on the left side of the IIS Manager window click on the **[Default Web Site]** option.
36. Then, under the **Manage Website** tree located on the right side of the IIS Manager window click on the **[Restart]** button.

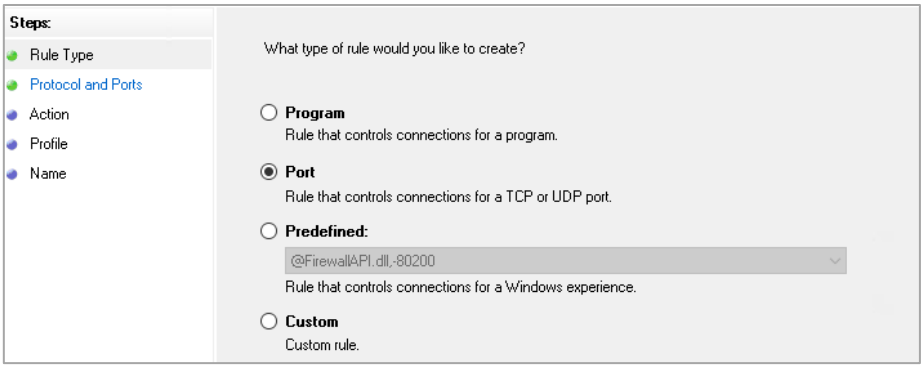
17.1.3. SETTING THE FIREWALL

It is recommended to check the Windows Firewall settings:

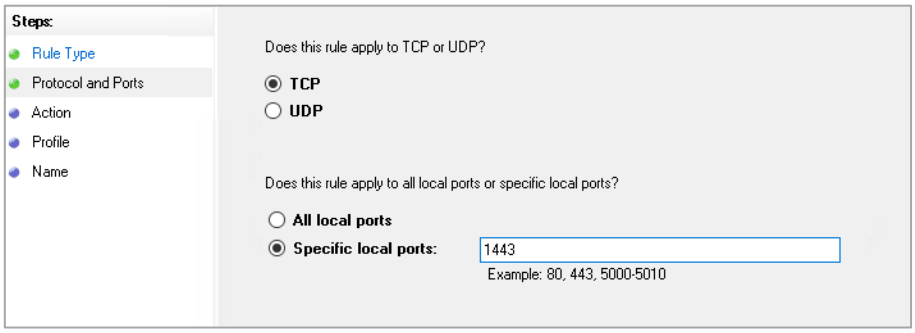
1. Navigate to **Control Panel / System and Security / Windows Defender Firewall / Advanced settings**.
2. Right click on **[Inbound rules]** located in the left section.
3. Select **New Rule...** from the appearing quick menu.



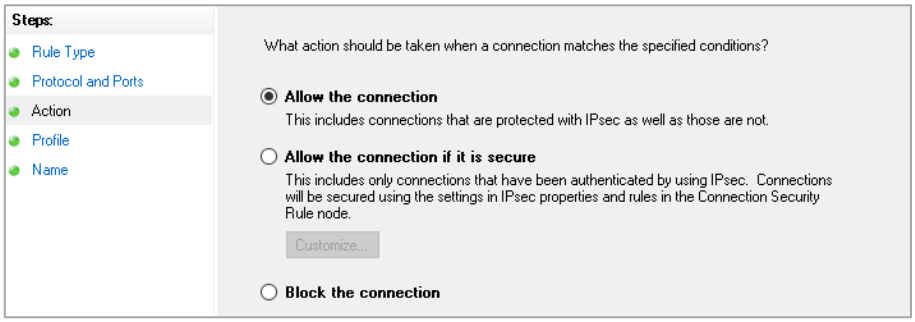
4. In the pop-up window select **Port**.
5. Then, click on the **[Next >]** button.



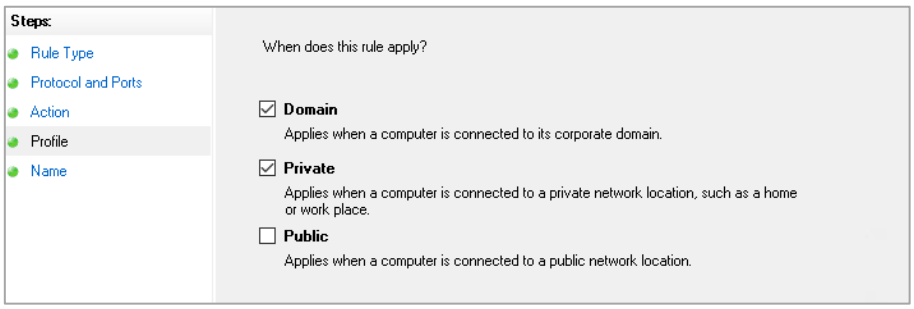
6. At "**Does this rule apply to TCP or UDP?**" select **TCP**.
7. At "**Does this rule apply to all local ports or specific local ports?**" select "**Specific local ports**" and enter the value **1443** to the text field.
8. Then, click on the **[Next >]** button.



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:

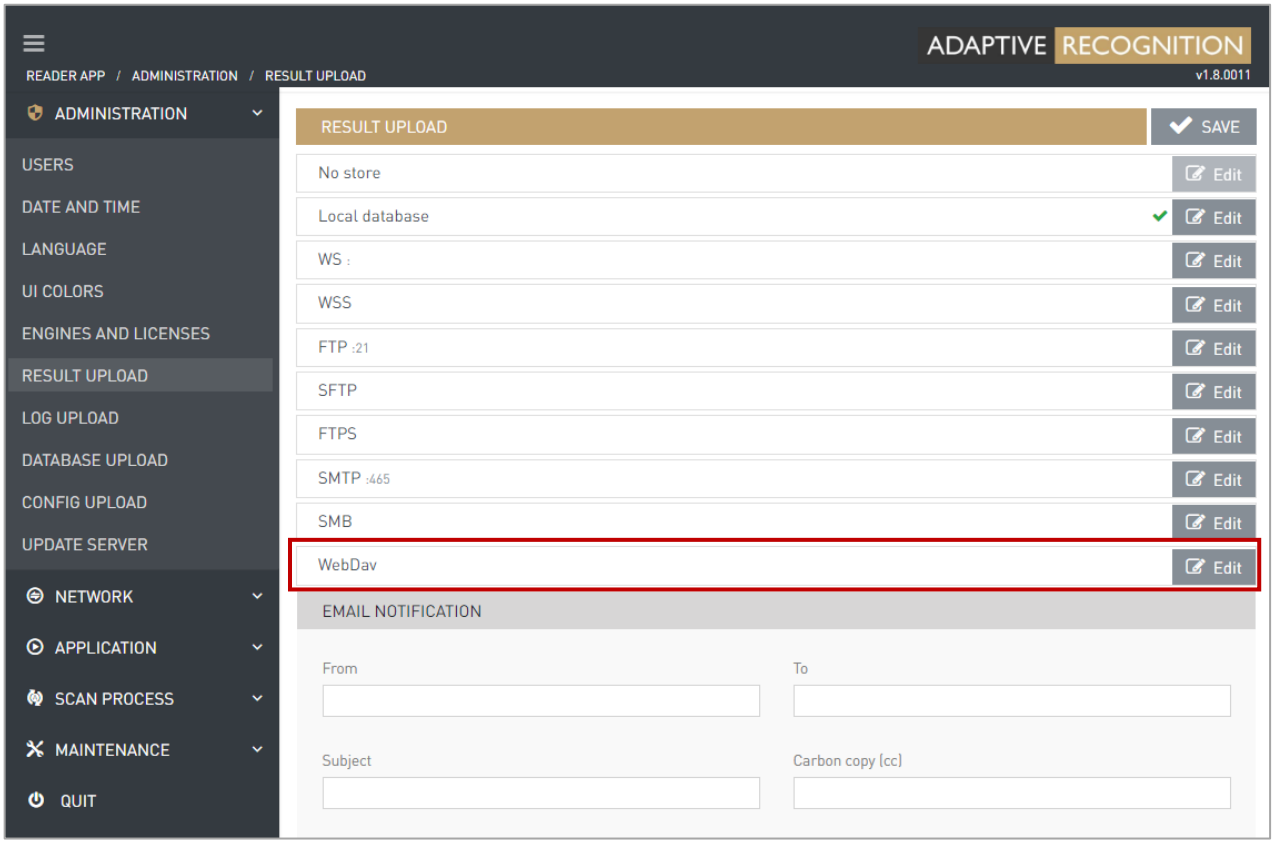
- `sudo ufw allow 1443/tcp`
- `sudo ufw disable`
- `sudo ufw enable`

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

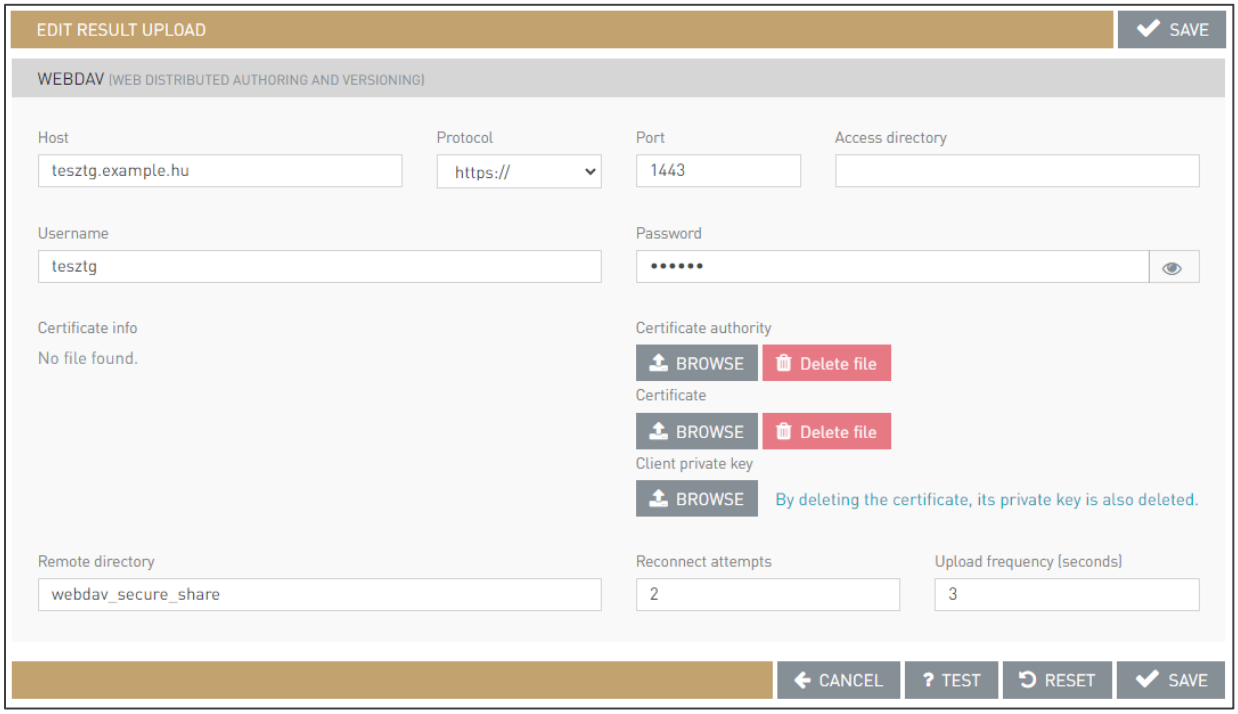
17.3. SETTING ON OSMOND

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.

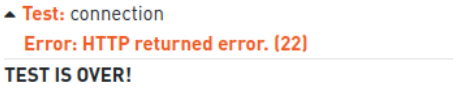
1. After signing in to the web interface, click on the **Main menu** (the three horizontal stripes; at the top left corner of the webpage) in order to open the menu items.
2. Navigate to **ADMINISTRATION / RESULT UPLOAD**.
3. Click on the **[Edit]** button belonging to **WebDav** protocol.



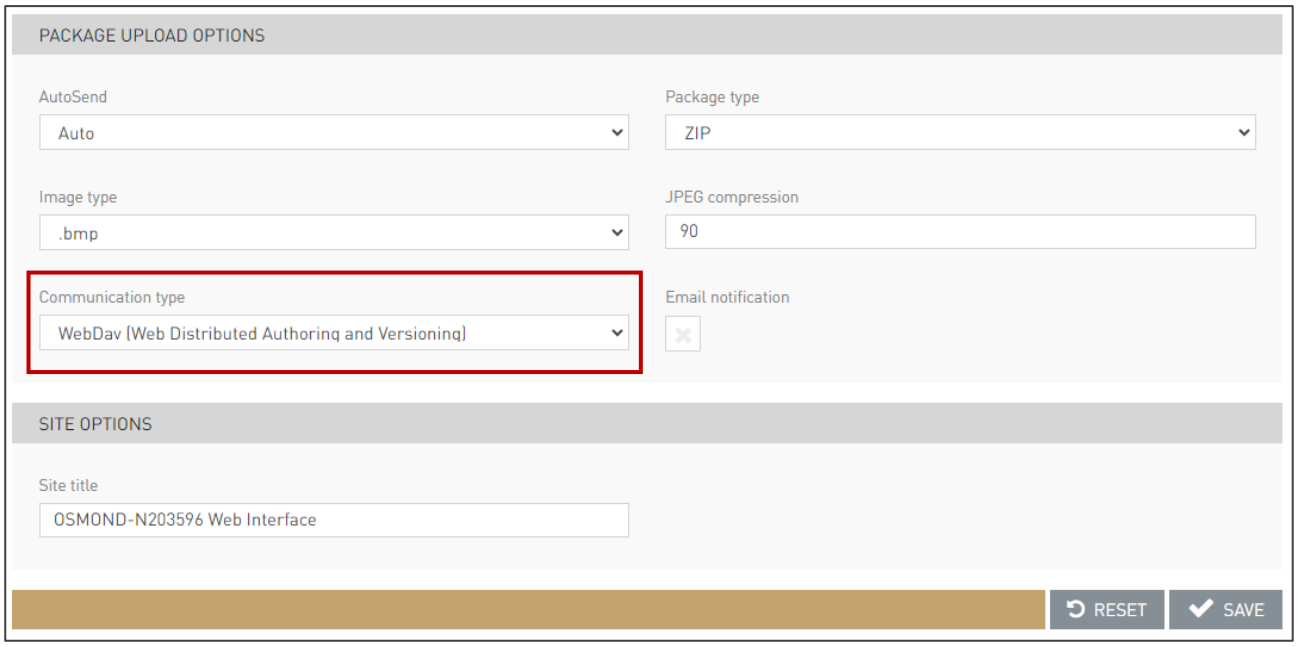
4. On the appearing menu set the following:
   - **Host**: IP address of the WebDav server or the fully qualified domain name (FQDN), depending on which one the certificate was issued for. In this case the certificate is issued for the FQDN, therefore: tesztg.example.hu
   - **Protocol**: https://
   - **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.



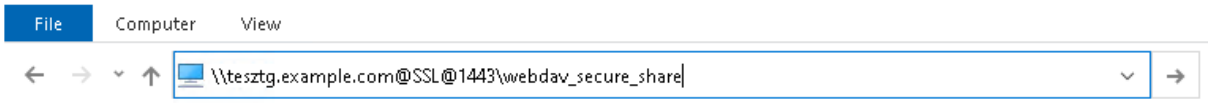
After performing these settings, the scanned documents are transferred to the upload server as a zip file.

17.4. TESTING THE SETUP

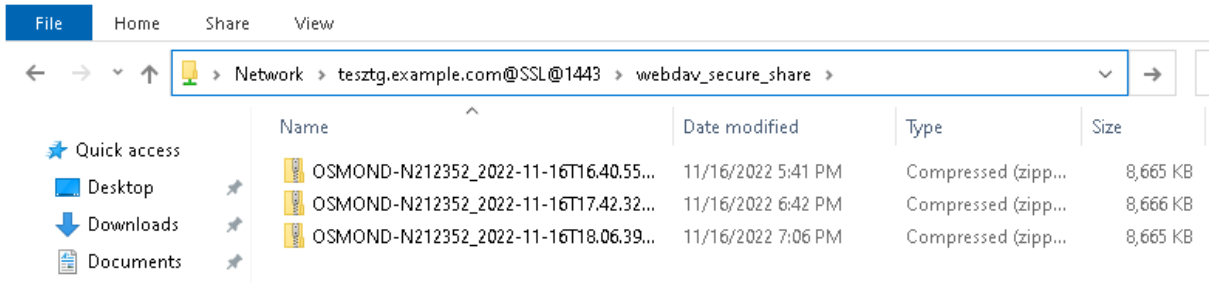
17.4.1. WINDOWS

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



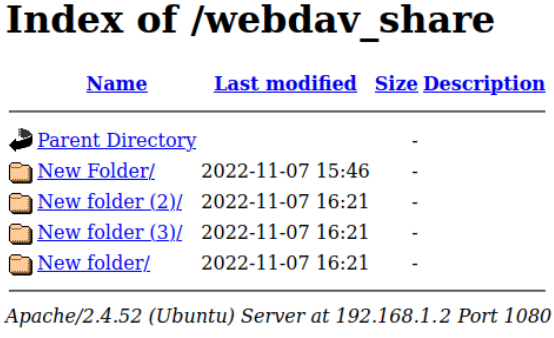
2. Then, press [Enter].
3. After successful connection, Windows requests the username and password.
4. Then, the content of the WebDav directory appears, and can be browsed as a file system.



17.4.2. LINUX

On Linux the Dolphin file manager can be used to sign in.

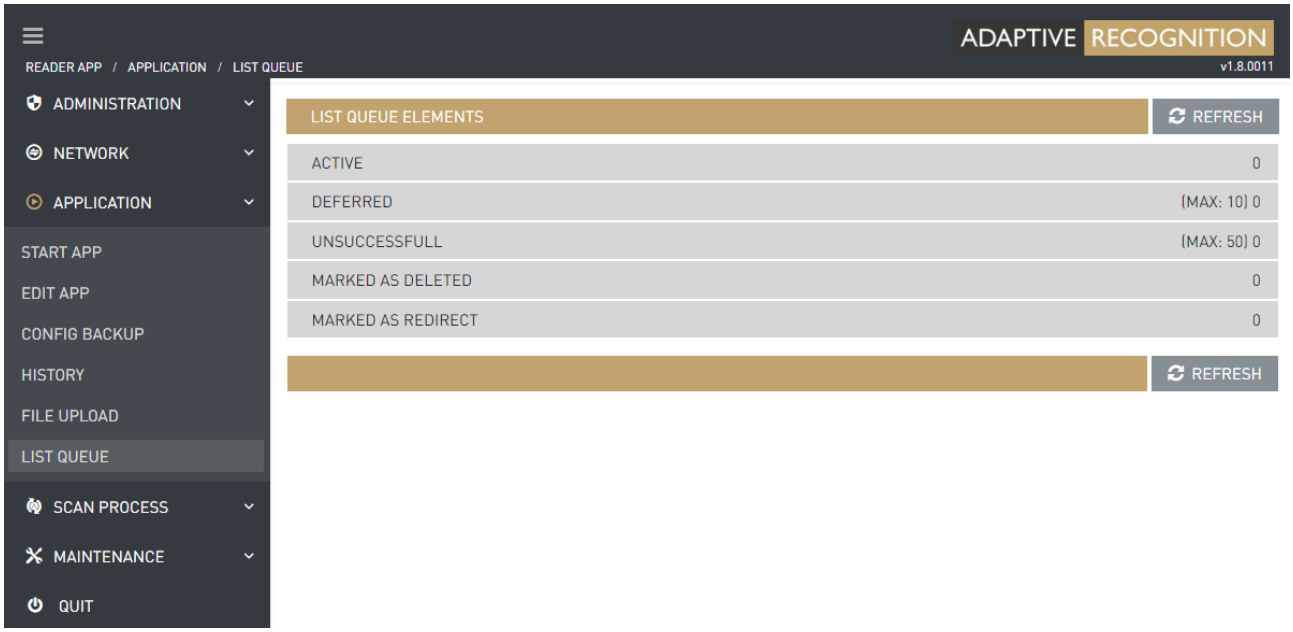
1. Enter the address of the WebDav server to the address bar:
   webdavs://tesztg.example.com:1443/webdav_secure_share/
2. Then, press [Enter].
3. After successful connection, enter the username and password.
4. Then, the page appears:



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.

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

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.

18.2. INSTALLING AND SETTING THE UPDATE SERVER ON WINDOWS 10

18.2.1. INSTALLING PYTHON

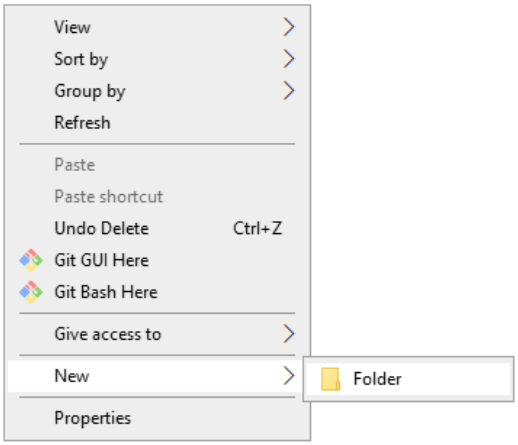
1. Download and install Python 3 or newer version (currently Python 3.11.3 can be accessed):
   - Navigate to https://www.python.org/downloads/.
   - Select "**Use admin privileges when installing py.exe**" and "**Add python.exe to PATH**" by ticking the checkboxes.
   - Then, click on **[Install Now]**.

   - 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.

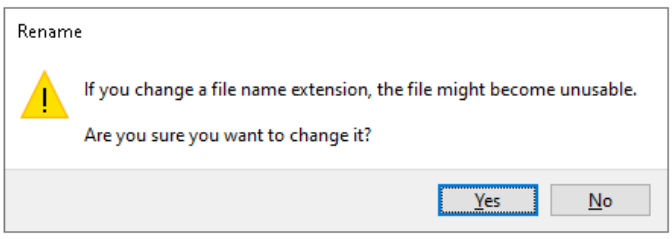
18.2.2. INSTALLING THE UPDATE SERVER

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.

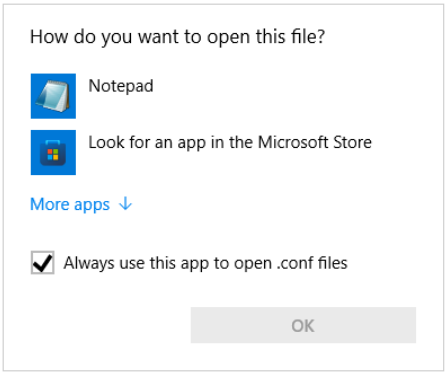


   - Rename the created library to: **`update_server`**

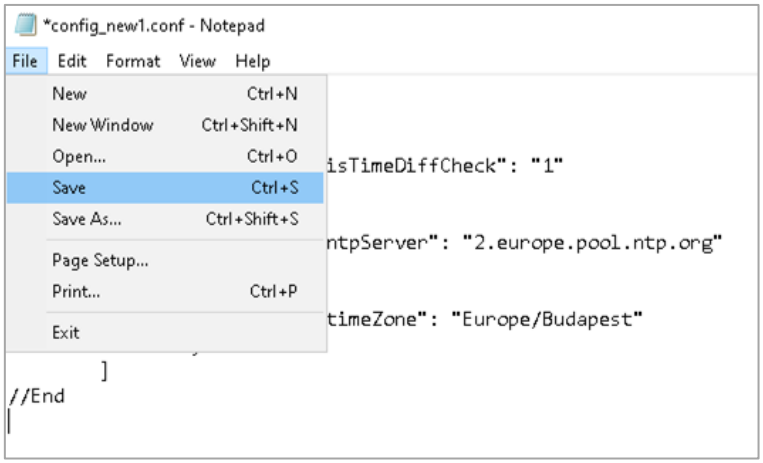
2. Open the **`update_server`** library.
3. Create or copy the configuration file to the **`update_server`** library. For example, copy the one located at Annex / Configuration File (config_new1.conf) chapter.
   - Right click, then select New / Text Document from the appearing quick menu.
   - Name 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.



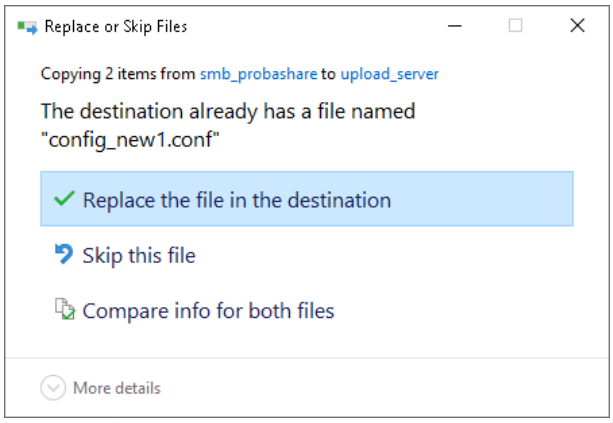
- To this location copy the content of the configuration file located in the Annex / Configuration File (config_new1.conf) chapter.
- Then, click on **File / Save** in the Notepad application.



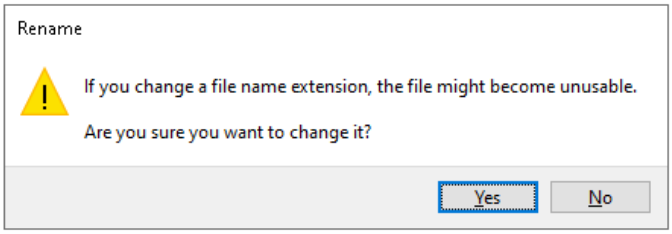
- At last, close the window by clicking on the "x" located in the upper right corner.

4. Sign the config_new1.conf file (see Signing the Configuration File chapter).

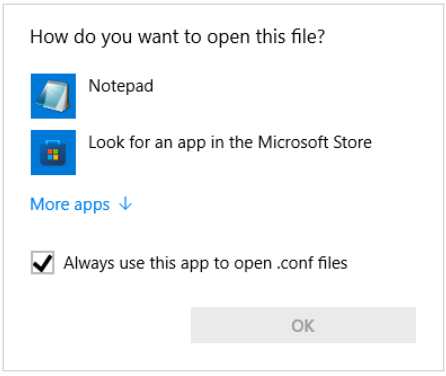
5. Copy the config_new1.conf and config_new1.conf.chk files to the **C:\Users\user\update_server** library.
   - The former config_new1.conf must be overwritten with the returned one.



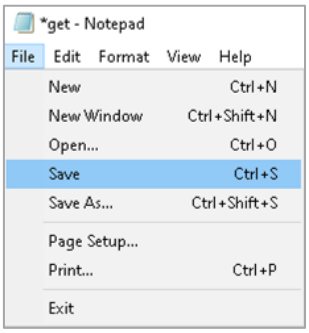
6. Create or copy the 'get' file to the **update_server** library (see Annex / Description of the Configuration File (get file) chapter):
   - Right click in the File Explorer, then select New / Text Document from the appearing quick menu.
   - Name the file to: get
   - If an alert message pops up, click on the [Yes] button on the message box.



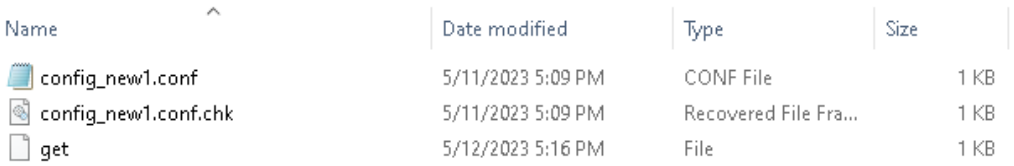
   - Right click on the file name and select the Edit menu item. In the absence of this, click on the Open with menu item and browse the Notepad application.



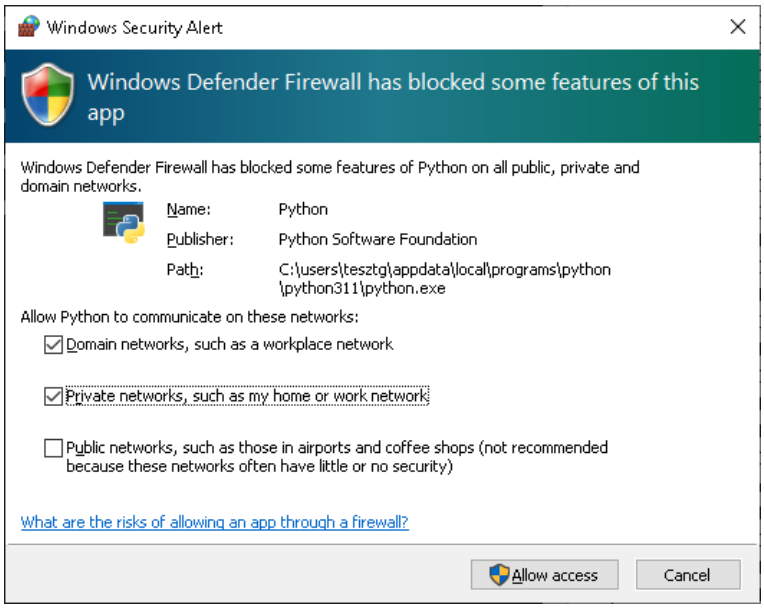
- To this location copy the following line and press the [Enter] key at the end of the line in order to start a new line:
  `*|*|*|*|*|config_new1.conf`
- Then, click on File / Save in the Notepad application.



- 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:



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.

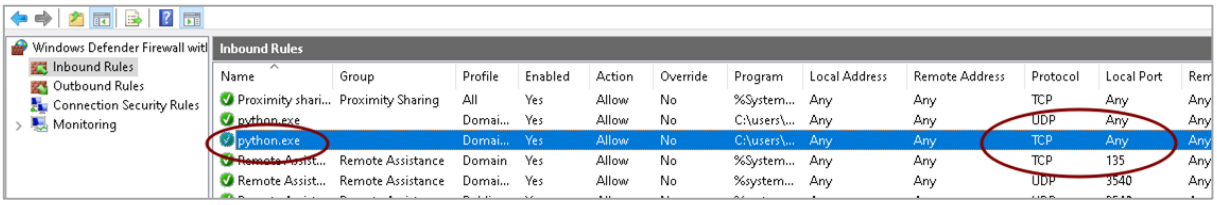


   - The availability of the server can be tested by entering its address to the address bar of the browser:
     ```
     http://192.168.1.3:3280
     ```
     where:
     `192.168.1.3` is the IP address of the update server on which the python server is started,
     `3280` is the port through which the update server is listening

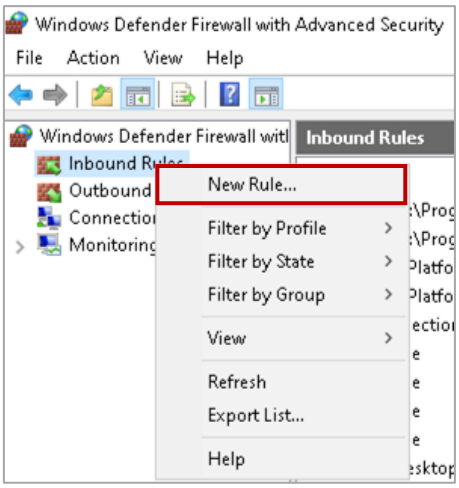
18.2.3. SETTING THE FIREWALL

If the server cannot be accessed from another PC, check the Windows Firewall settings.

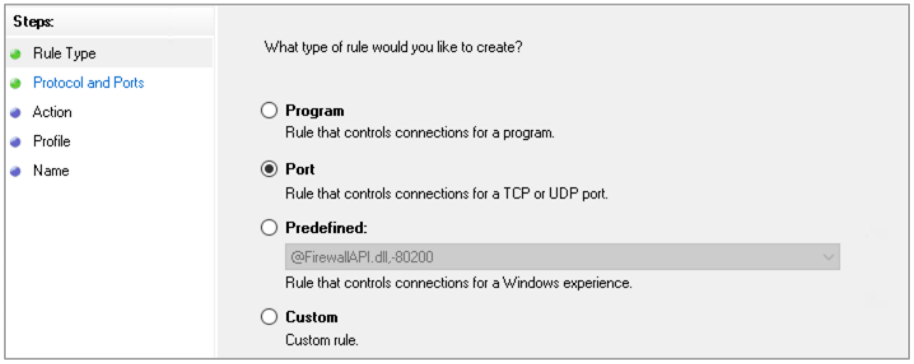
1. Navigate to **Control Panel / System and Security / Windows Defender Firewall / Advanced settings**.
2. Click on **[Inbound rules]** located in the left section.
3. If the **python.exe** is listed, which is valid for all local ports, or at least port **3280** with TCP protocol, and a green check mark is displayed next to its name, then the setting of Firewall is appropriate.



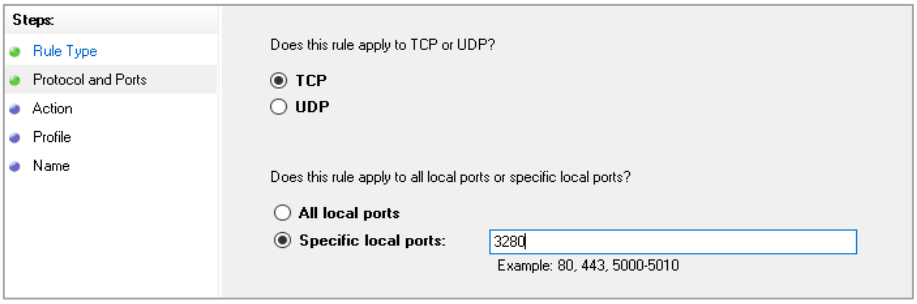
4. If the **python.exe** is not listed, right click on the **Inbound Rules**, then select **New Rule...** from the appearing quick menu.



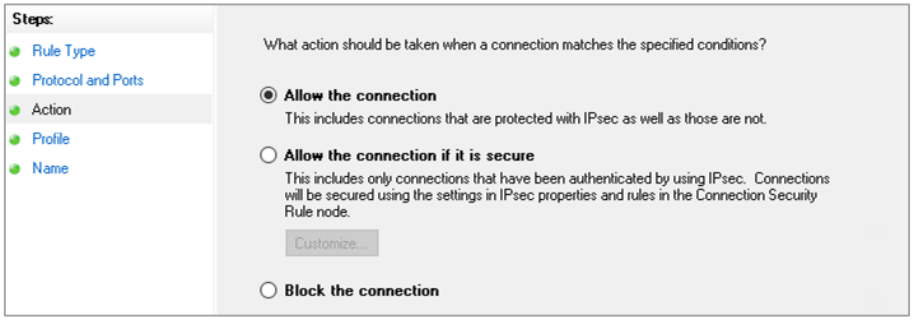
5. In the pop-up window select **Port**, then click on the **[Next >]** button.



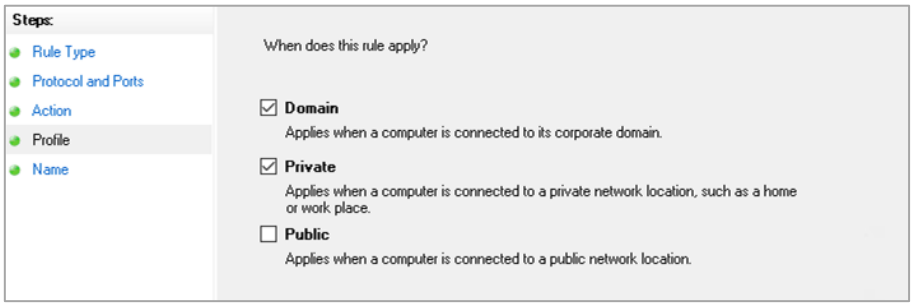
6. At "Does this rule apply to TCP or UDP?" select TCP.
7. At "Does this rule apply to all local ports or specific local ports?" select "Specific local ports" and enter the value 3280 to the text field. Then click on the [Next >] button.



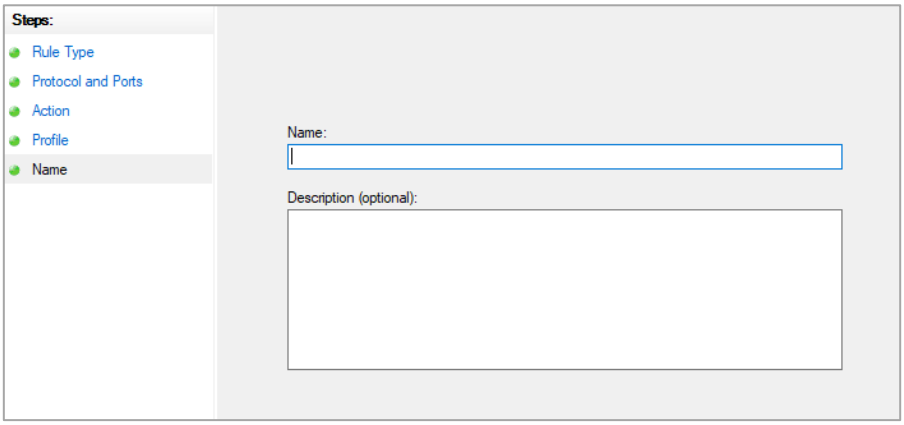
8. On the following window select "Allow the connection" option and click on the [Next >] button.



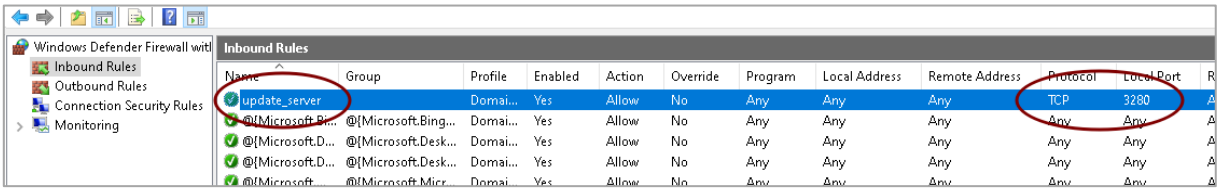
9. On next window select "Domain" and "Private" options by ticking their checkboxes.
   The "Public" option is not recommended, only if the PC is connected to a public network.
   Then click on the [Next >] button.



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

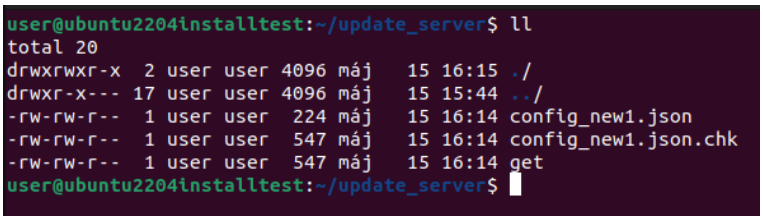
4. Sign the **config_new1.conf** file (see Signing the Configuration File chapter).

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

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

7. The content of the **update_server** library can be seen in the following image:



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

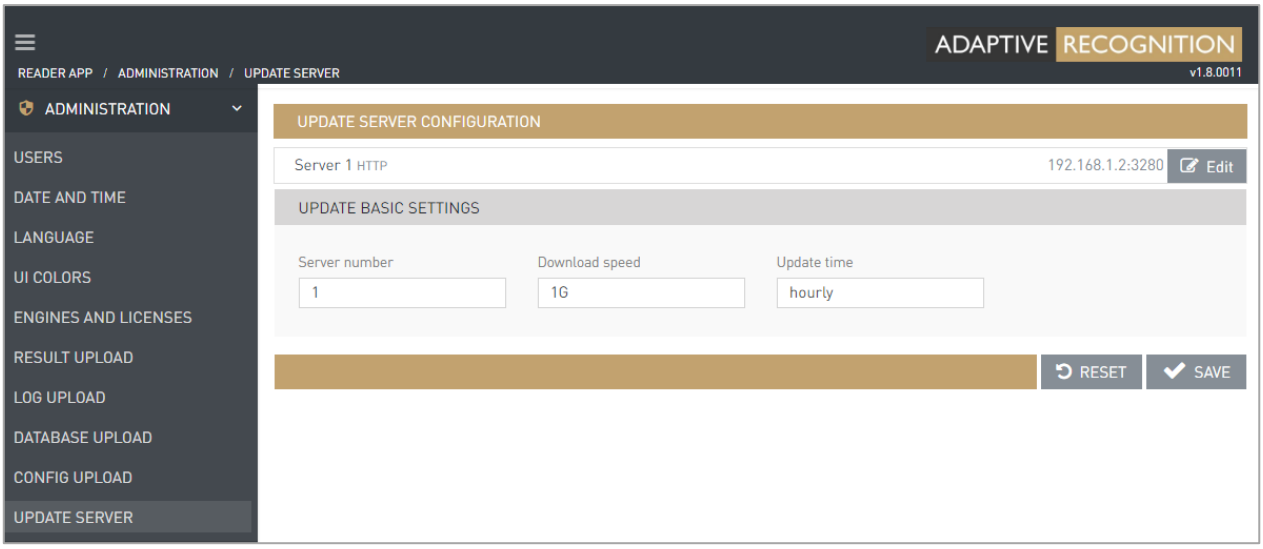
The port used by the update server must be set in the firewall, then restart it, if the firewall is active. In general, the **ufw** runs on Ubuntu. Its state can be queried with the **sudo ufw status** command. If it is active, then:

- **sudo ufw allow 3280/tcp**
- **sudo ufw disable**
- **sudo ufw enable**

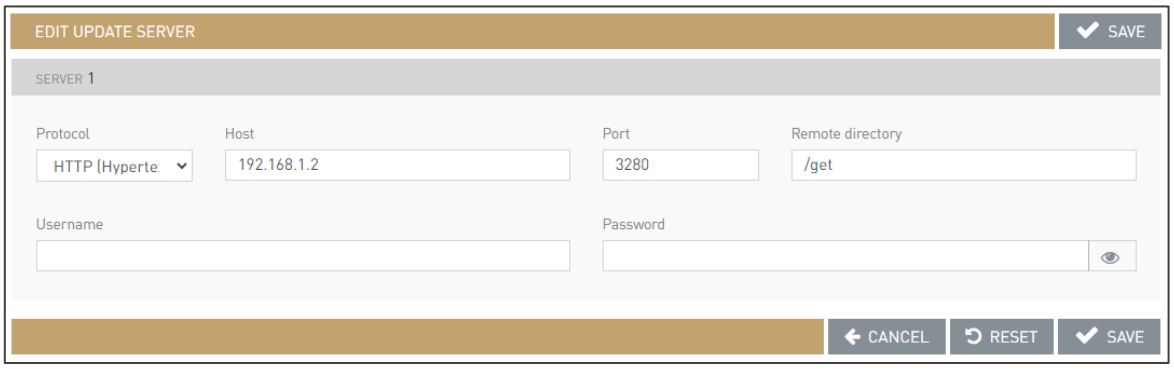
18.4. SETTING ON OSMOND

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.

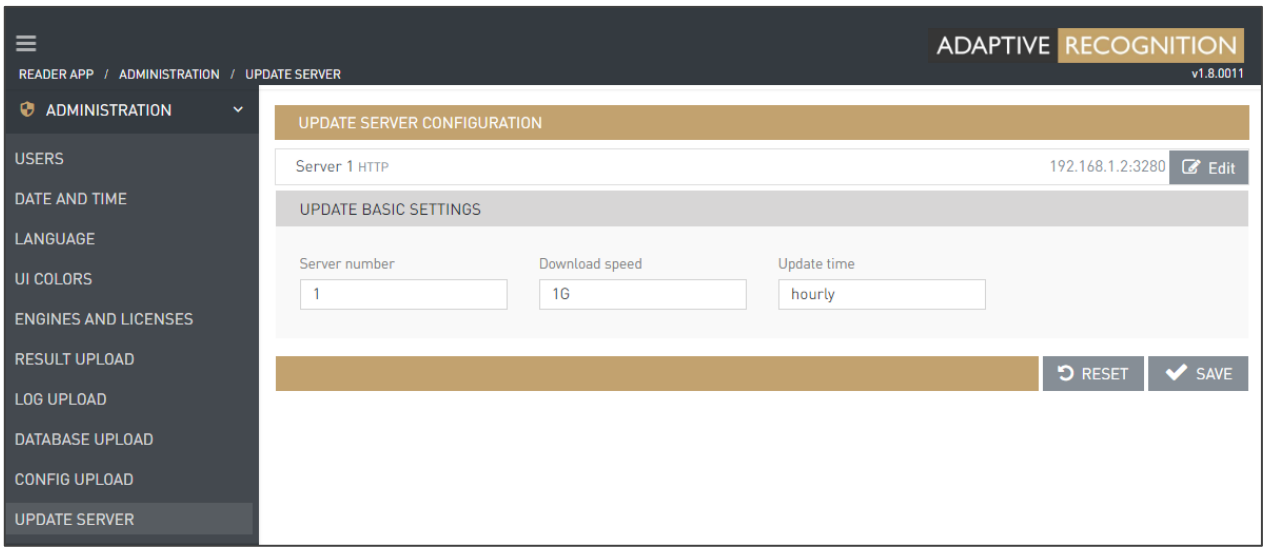
1. After signing in to the web interface, click on the Main menu (the three horizontal stripes; at the top left corner of the webpage) in order to open the menu items.
2. Navigate to ADMINISTRATION / UPDATE SERVER.
3. Click on the [Edit] button belonging to Server 1.



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.

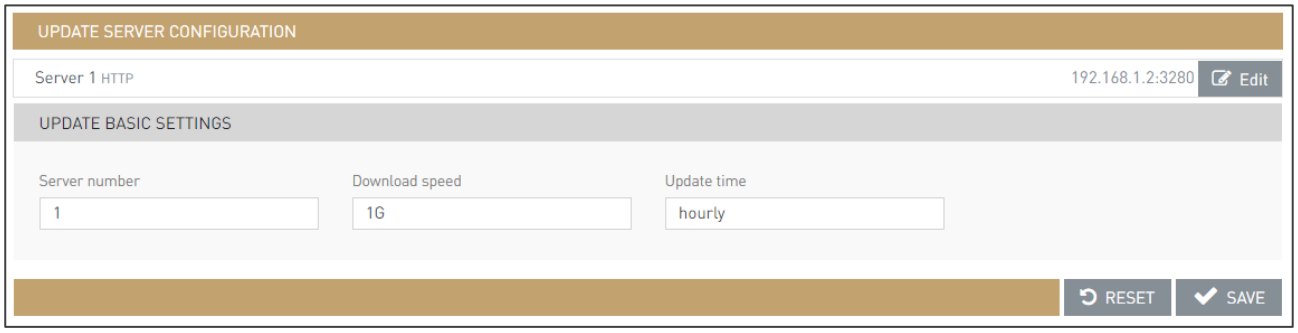


5. If all fields are filled in, click on the **[SAVE]** button.
   Wait until the **UPDATE SERVER CONFIGURATION** window appears:



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
```

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.

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 to 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.

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

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.

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

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:

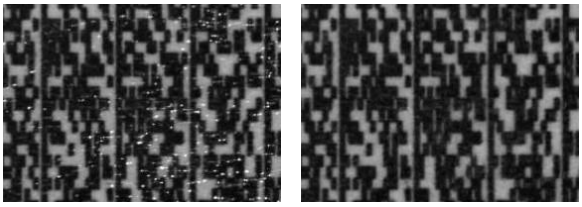
- properties starting with ctrl/
- preview_light
- testdoc_mode
- uvwarm_quality
- freerun_mode

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.)

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.

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

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.
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.
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.
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.

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.

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<<VIK TORIA<<<<<	KARPATI<<VIK TORIA<<<<<	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.

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.

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

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

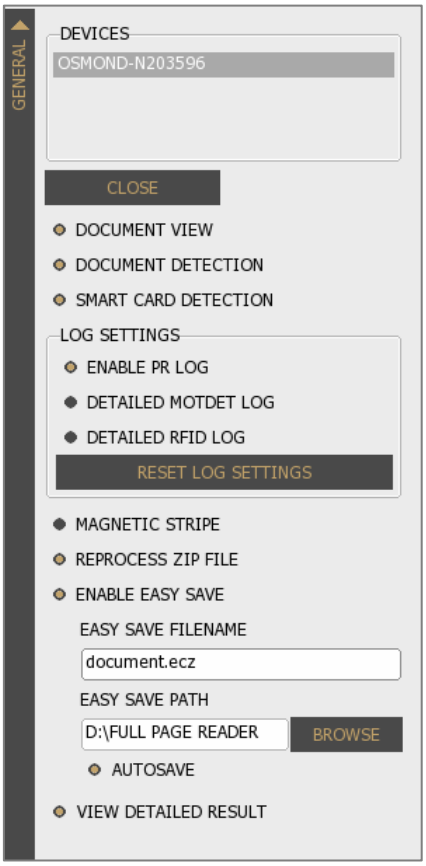
21.4. ENCRYPTED AUTOSAVE

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.



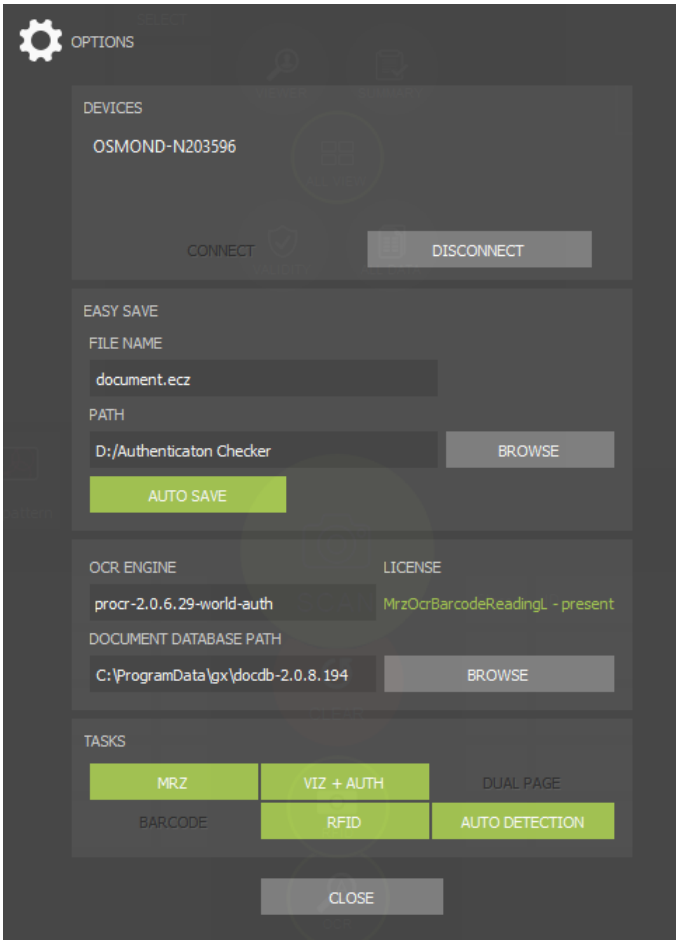
Note

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%".

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>".

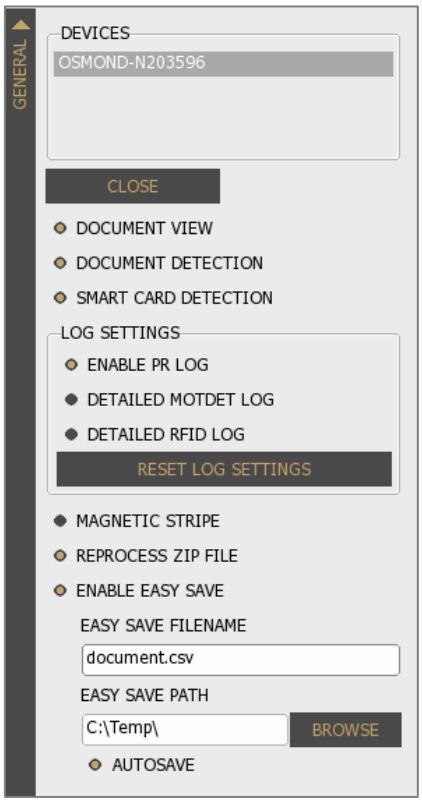
22. FULL PAGE READER – SAVING IN CSV FORMAT

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

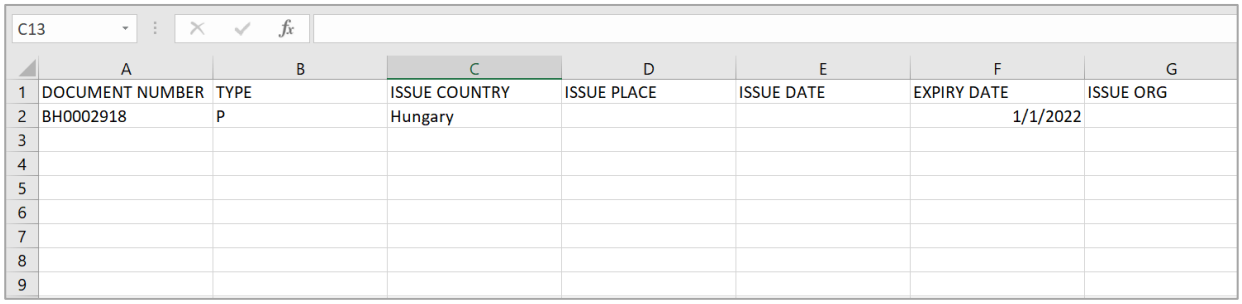
To make Full Page Reader write the same file during every reading, give a constant name of the file. Do not use any field name like "%DOCUMENT NUMBER%".

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

22.2. CSV STRUCTURE

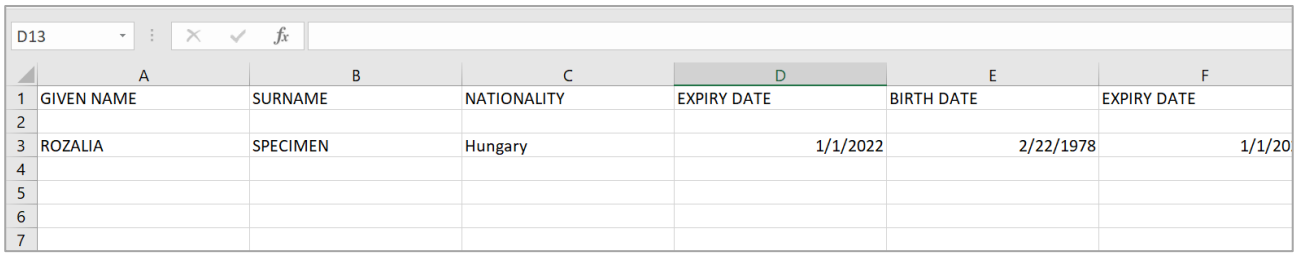
With the above settings, the Full Page Reader will generate the set CSV file. If the file already exists, it will append each scanning result to it.

In the headline of the CSV file, there are keywords which represents the field type of the particular column.



	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.



	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 INSTALLATION FOR OSMOND WITH UPDATER MSI

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 for firmware update MSI of Osmond devices.
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 R and L USB devices as well as N network devices.

> **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.

23.1. 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.

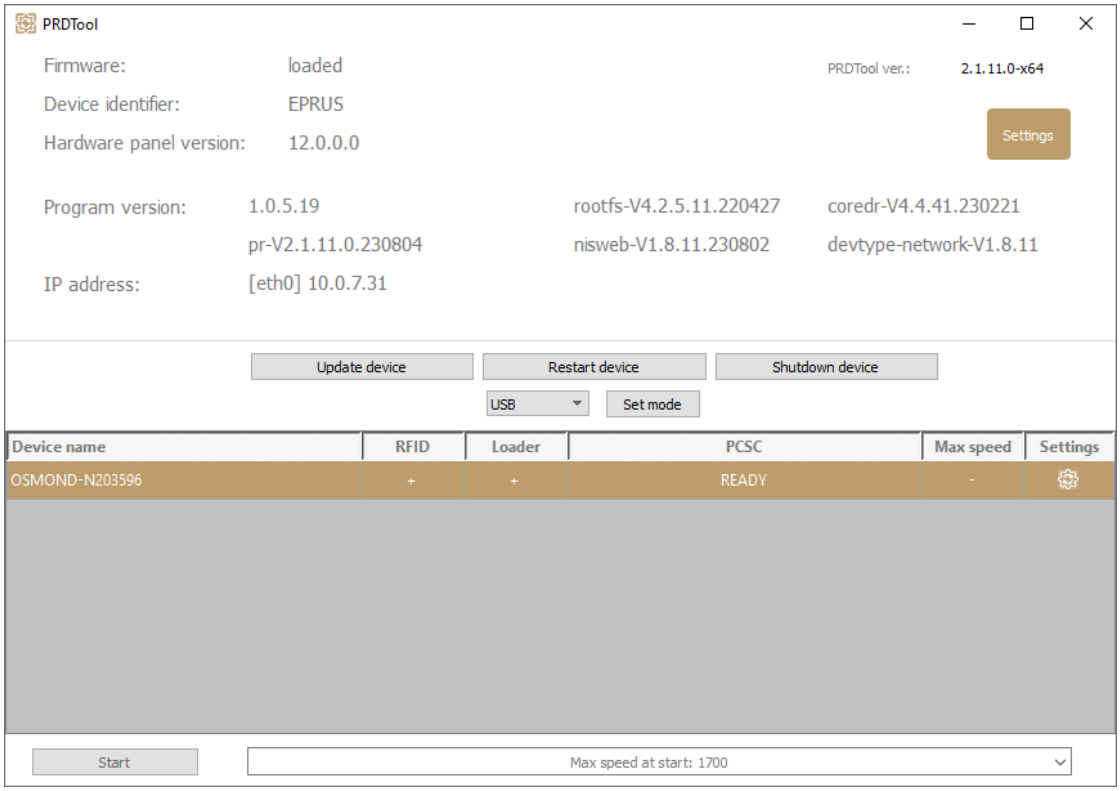
Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

23.2. THE UPDATE

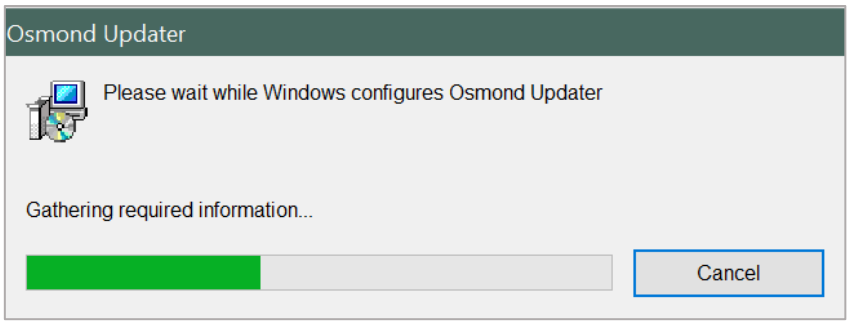
After the device boots up, please check with the "C:\ProgramFiles\Adaptive Recognition\utils\PRDTool\PRDTool.exe" utility tool whether the connection was established successfully.

> **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.

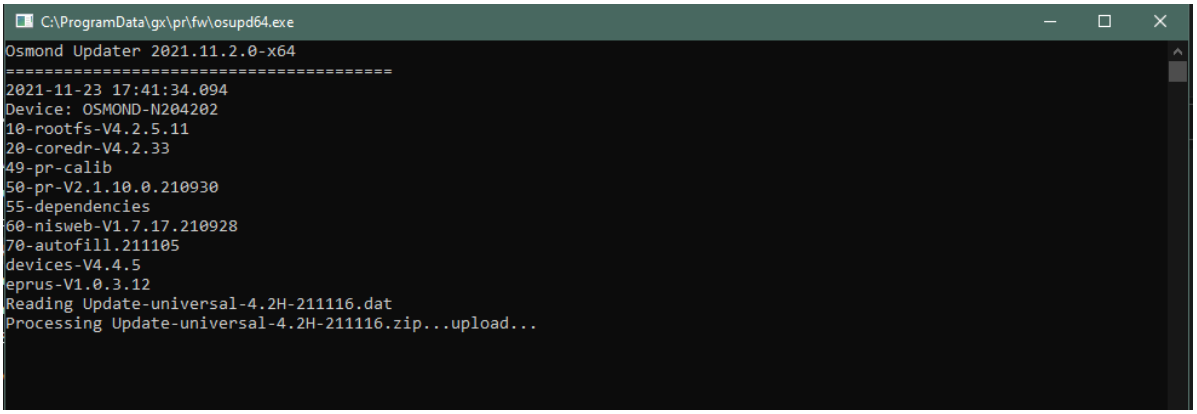


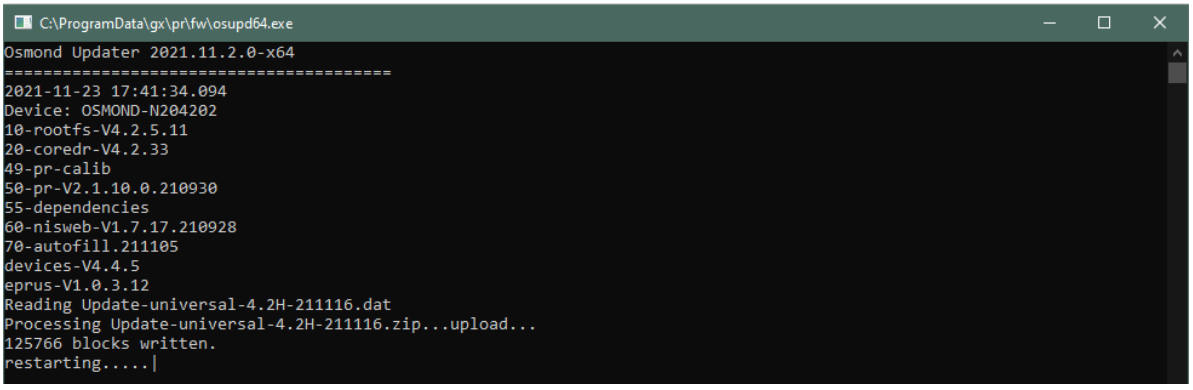
After the updater application is installed on the PC, the update process is started automatically.

Note

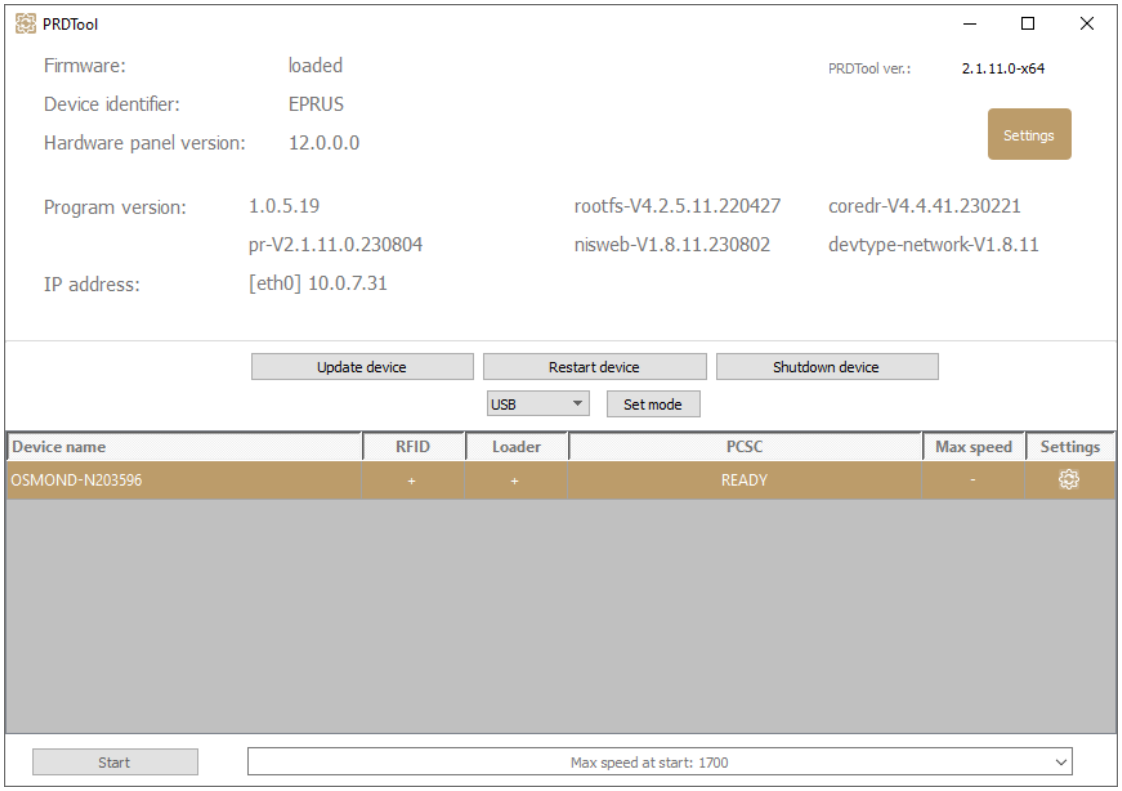
If your device already has the latest firmware version, the installer will stop without installing the firmware, and create a log file under C:\ProgramData\gx\pr\fw\ folder.

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:





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:



23.3. 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.

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

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.

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:

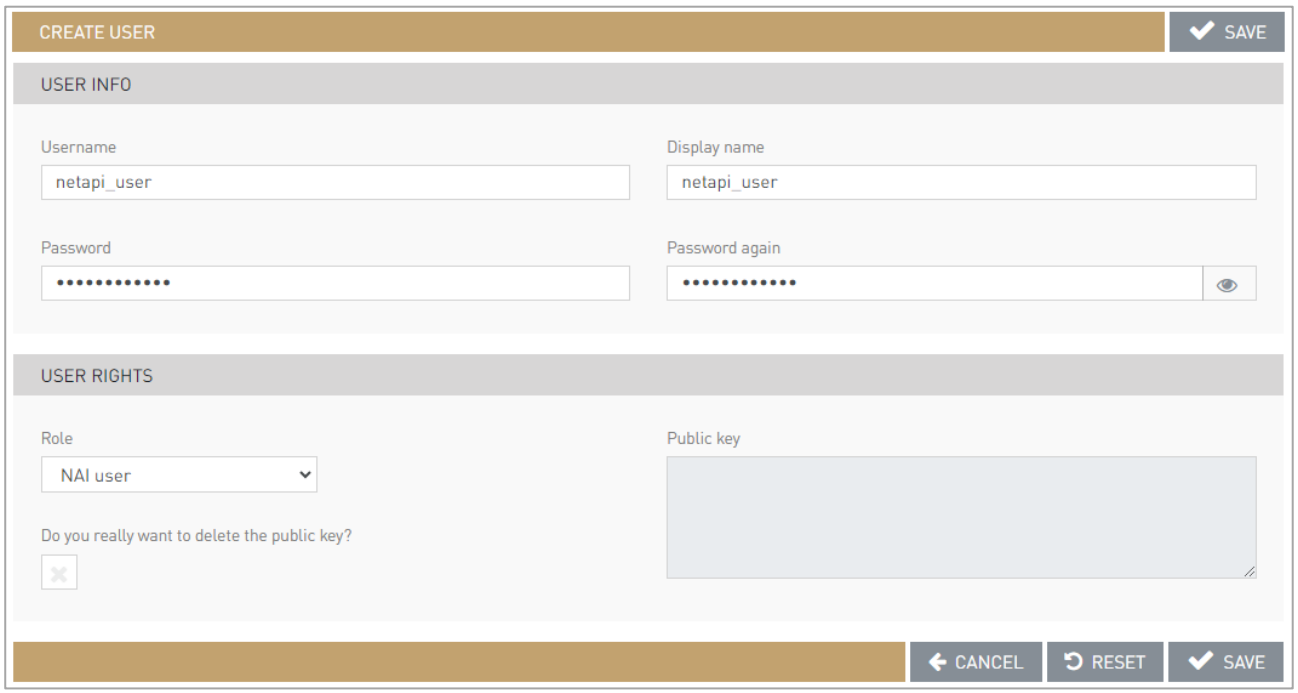
- ipdev/url – Server IP address (or domain name) and port number.
- ipdev/user – Username.
- ipdev/password – Password. Not recommended, but possible to set it in the gxsd.dat file.
- ocr_module – OCR tasks can be performed on client side or on server side. Set this property to `procr-ip` to perform 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++.

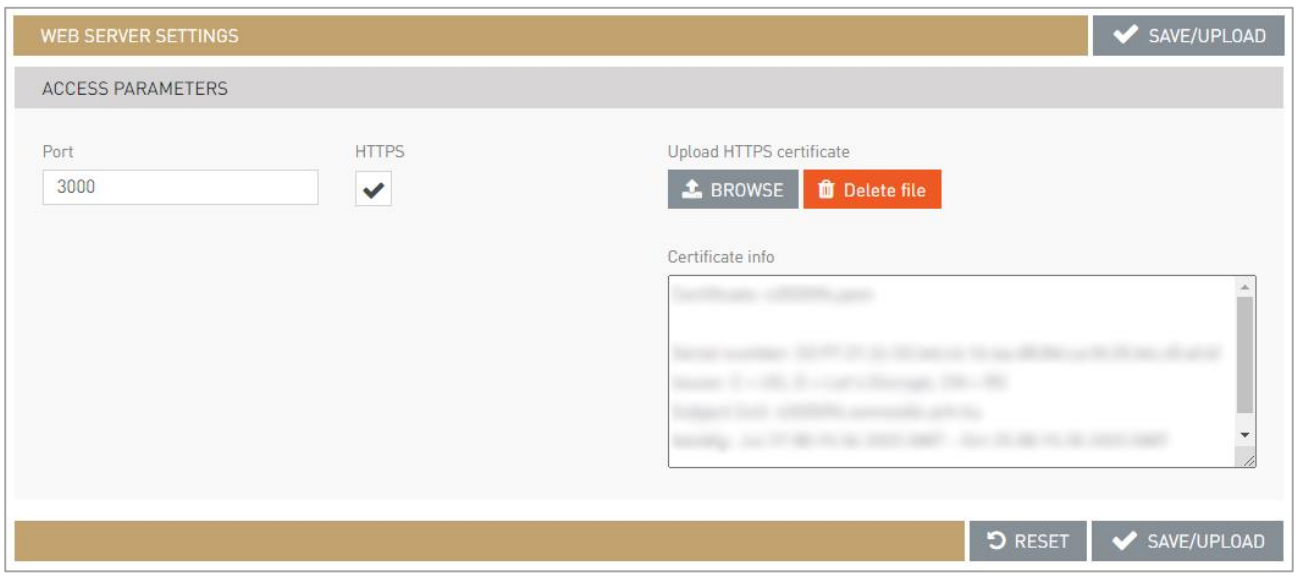
24.4. USING FULL PAGE READER WITH OSMOND N THROUGH NETAPI

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.

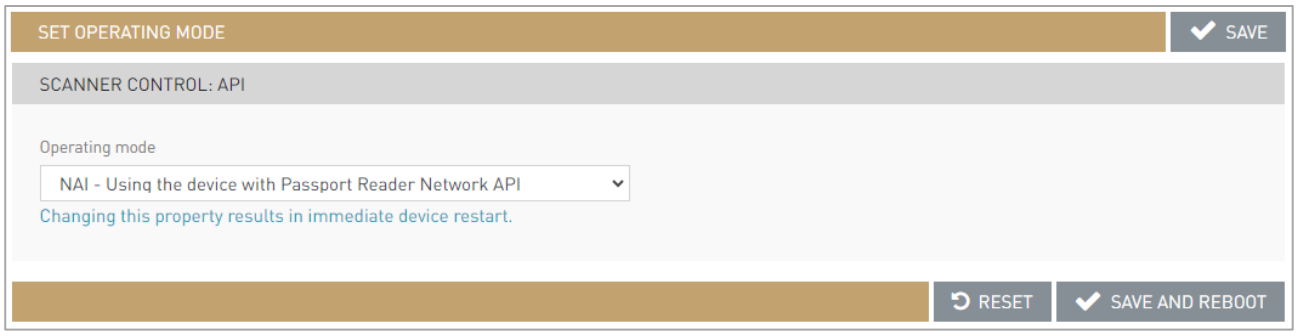
1. Sign in to the web interface of the Osmond N device.
2. Create a user with "NAI user" role in the web interface in the ADMINISTRATION / USERS menu. Only one user can be logged in at the same time.



3. Upload a HTTPS certificate in the NETWORK / WEB SERVER menu. NetAPI operates via HTTPS communication only.

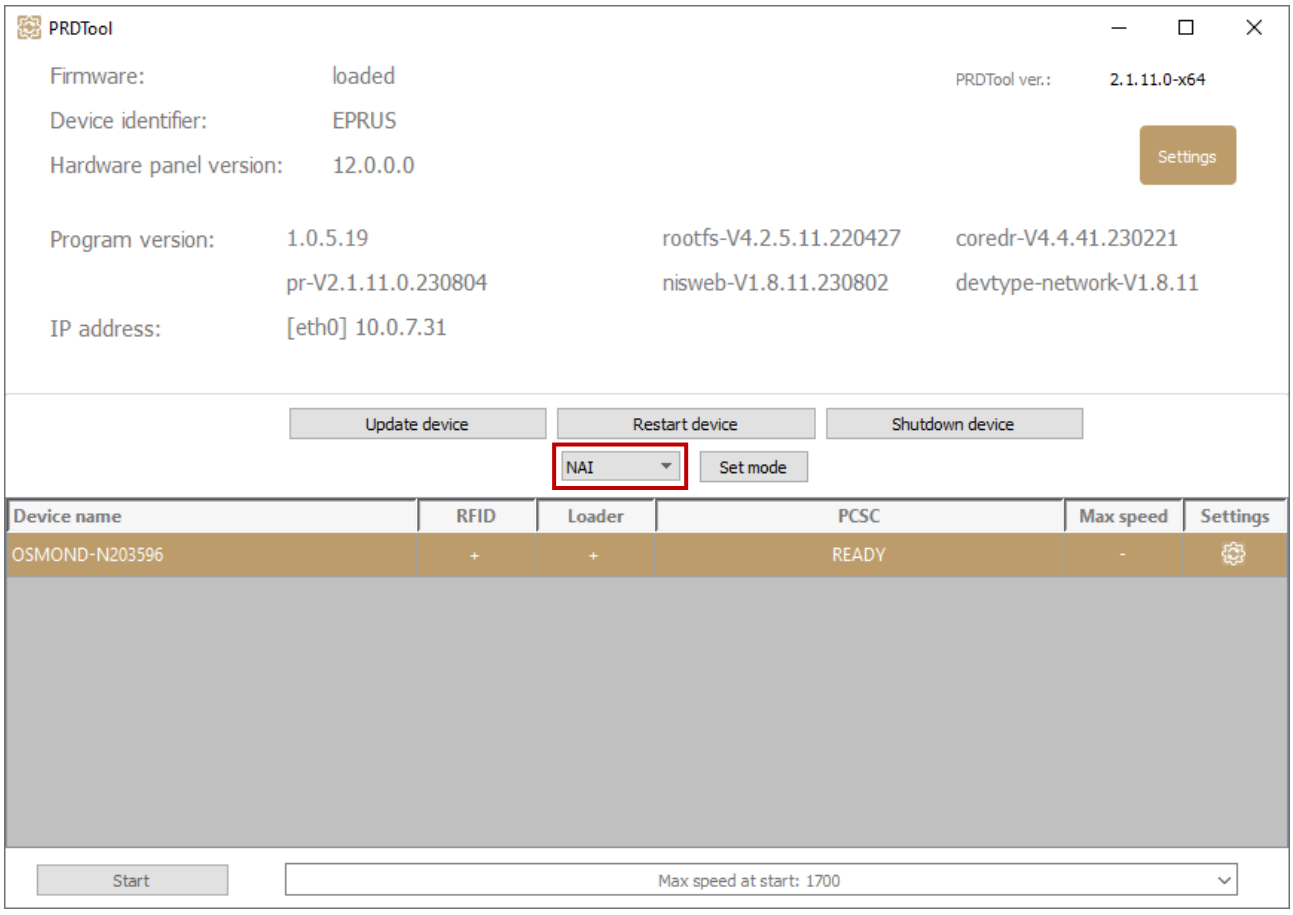


4. Set the operating mode of the device to "NAI" mode in the MAINTENANCE / OPERATING MODE menu.



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.

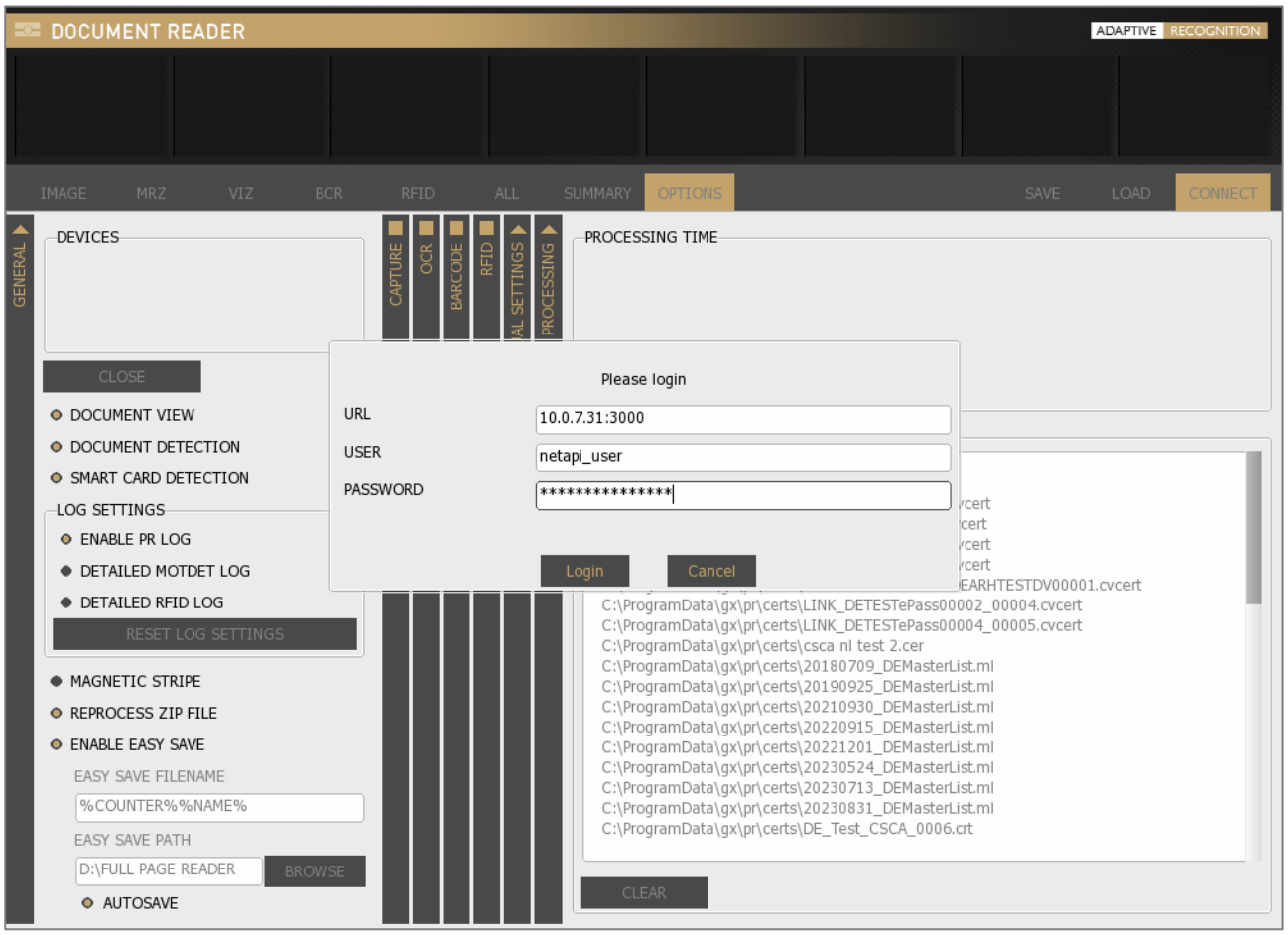
In case of Osmond N devices, the IP address is displayed in the PRDTool at the IP address section. The port number is the same as the value found at the web interface.

Note

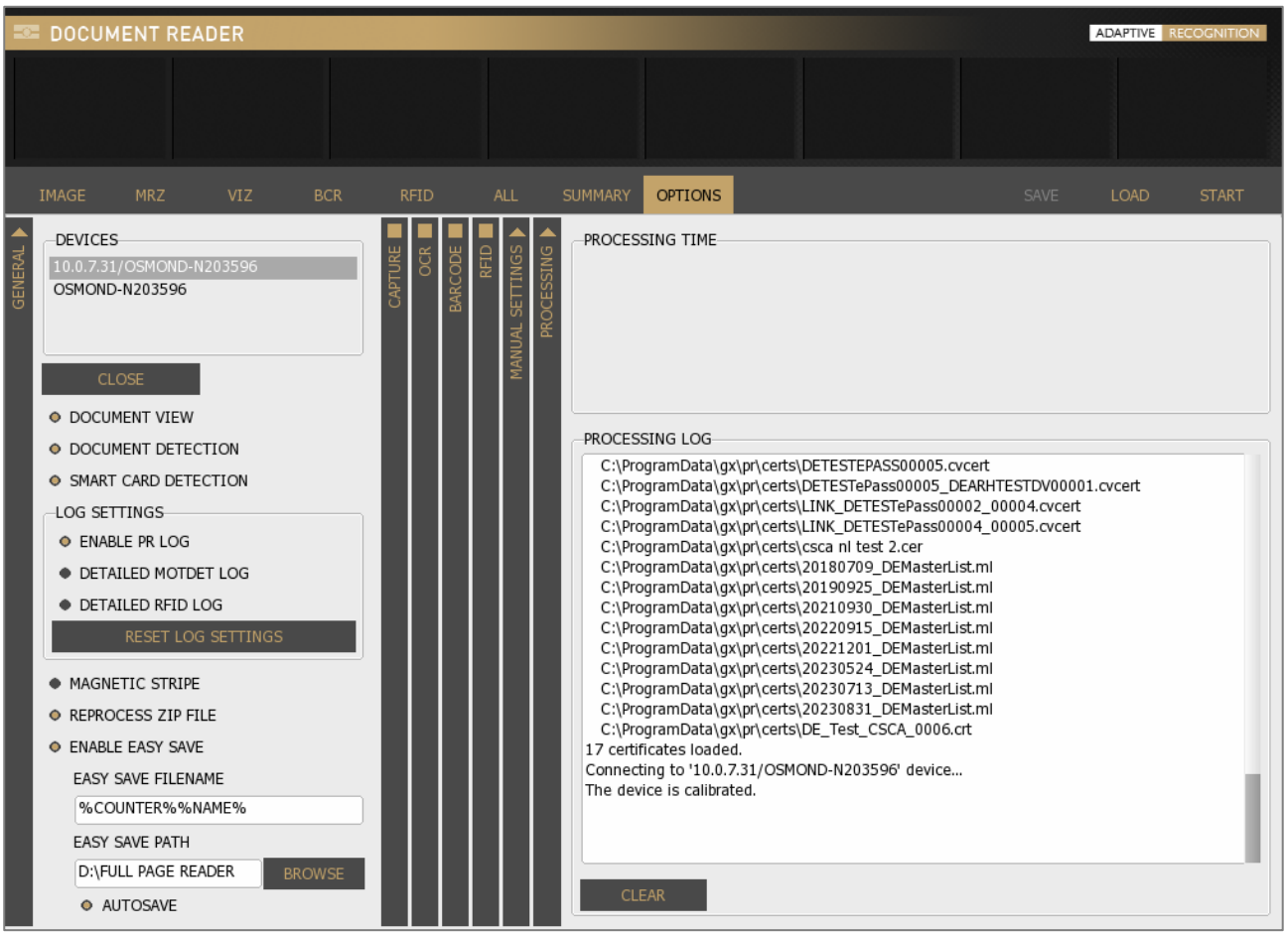
When editing the gxsd.dat file, pay attention to type between the <pr> and </pr> elements.

10. Save the modifications.

11. Open Full Page Reader.
12. When the FPR application is opened, a login window pops up.
13. Enter the **PASSWORD** into this window.



14. After a few seconds, the device is calibrated and ready to be used in NetAPI mode.



25. NETWORK API (NWA MODE)

The Network 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 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 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 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.

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

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 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 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
```


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

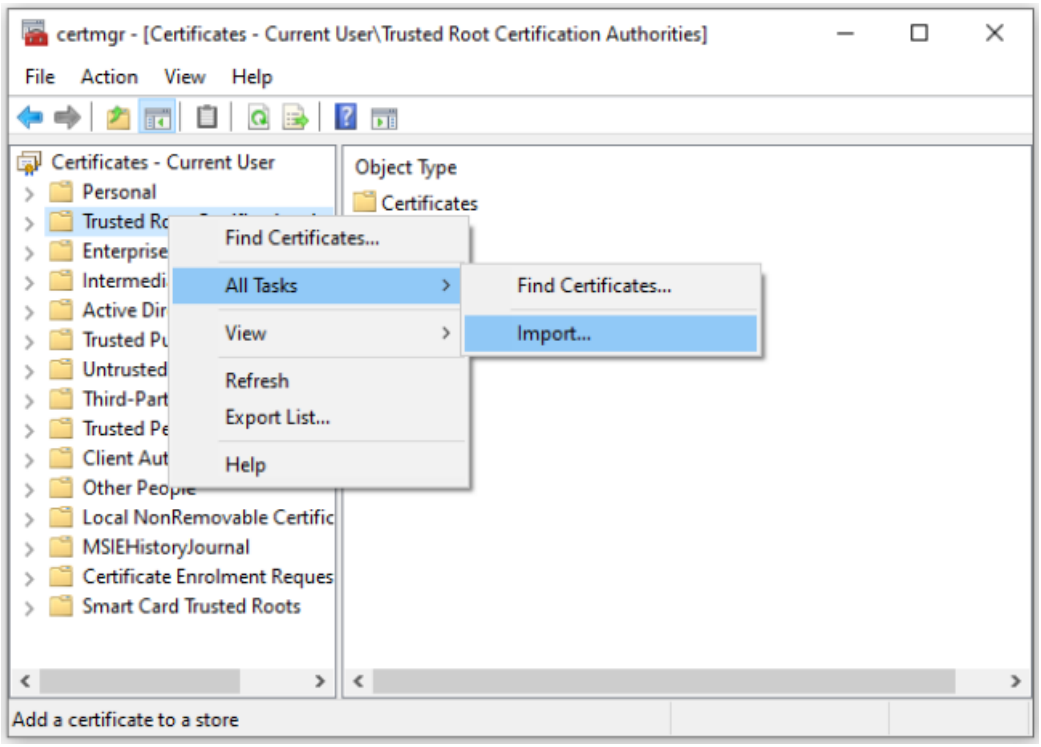
25.1.4. IMPORTING CERTIFICATES ON CLIENT

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`

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

25.2. SUPPORT FOR OTHER LANGUAGES

Using the openapi-generator-cli program, the Network 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']
}
```

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']
}
```

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

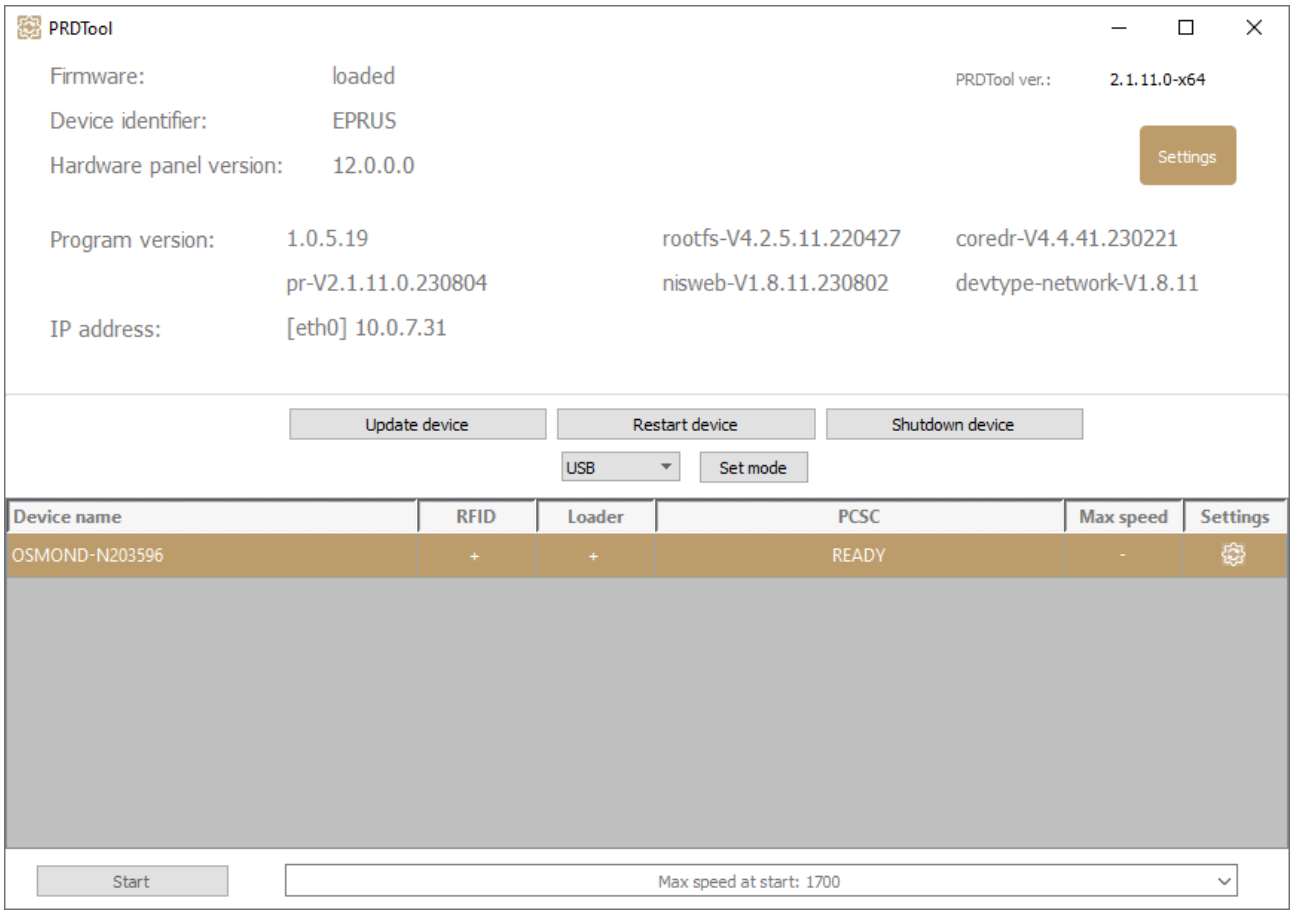
- Windows

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.

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 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.

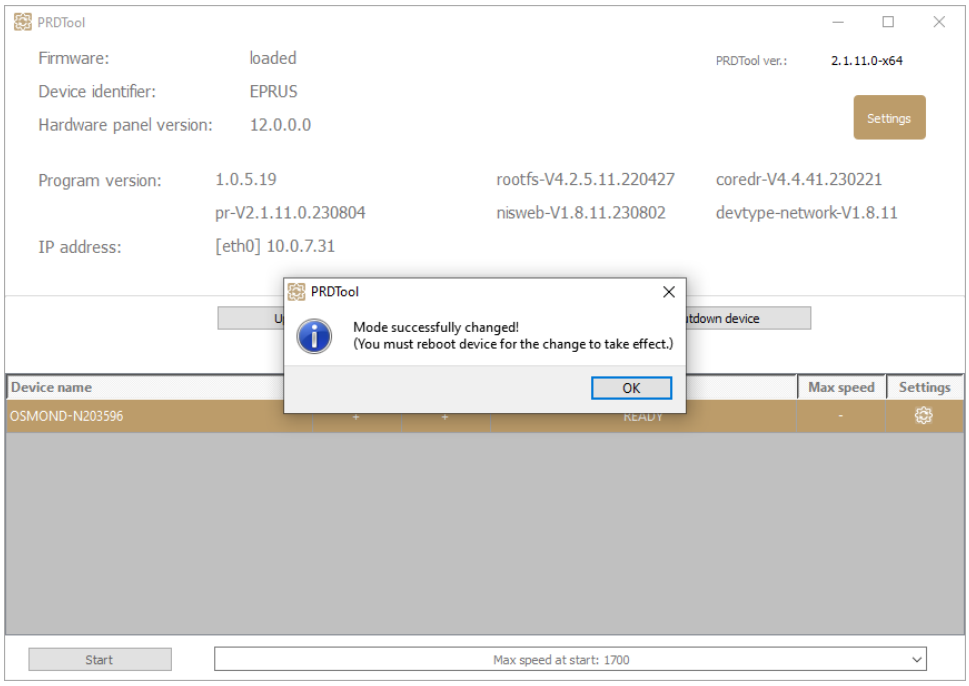
NWA mode

The Network API is designed to provide a tool for managing main network interface functions remotely, without accessing device Web GUI from browser.

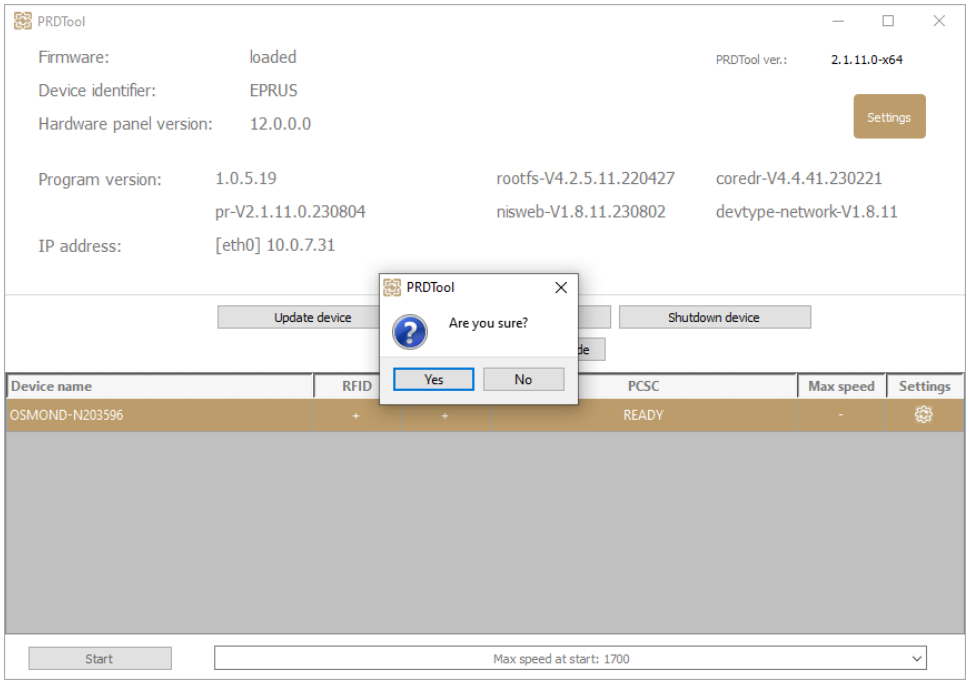
Adaptive Recognition **America**
Adaptive Recognition **Hungary**
Adaptive Recognition **Nordic**
Adaptive Recognition **Singapore**
REQUESTINFO@ADAPTIVERECOGNITION.COM
WWW.ADAPTIVERECOGNITION.COM

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.

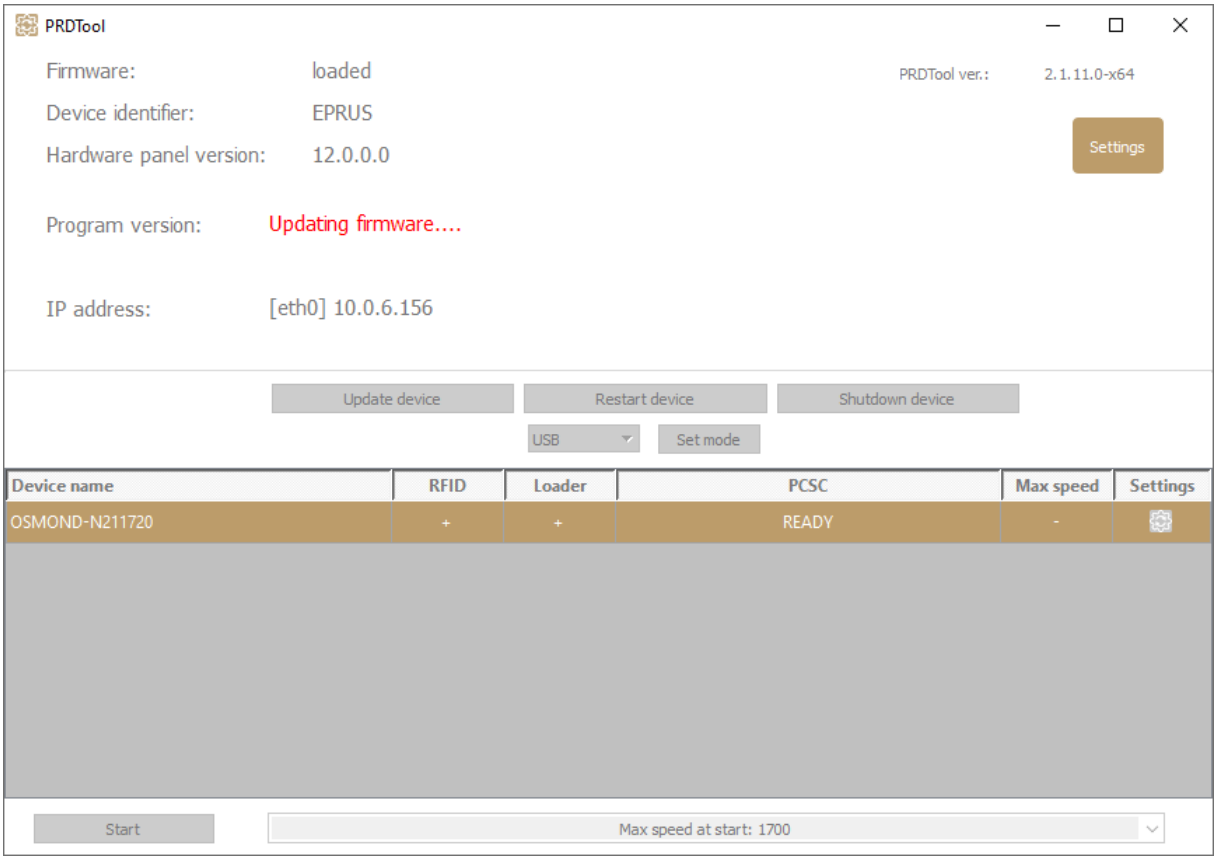


To apply these changes the device needs to be rebooted, so click on **[Restart device]** and then choose **[Yes]**. Now the device is rebooting in the selected operation mode. After the restart is finished the reader is ready to be used.



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.



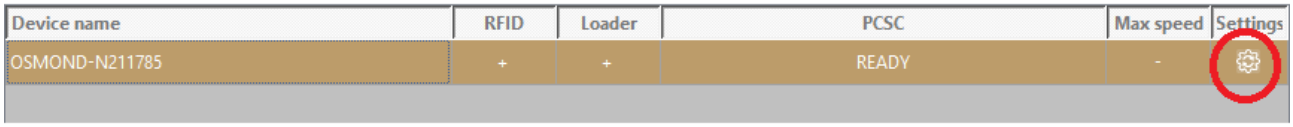
26.3.1. THE UPDATE FILE

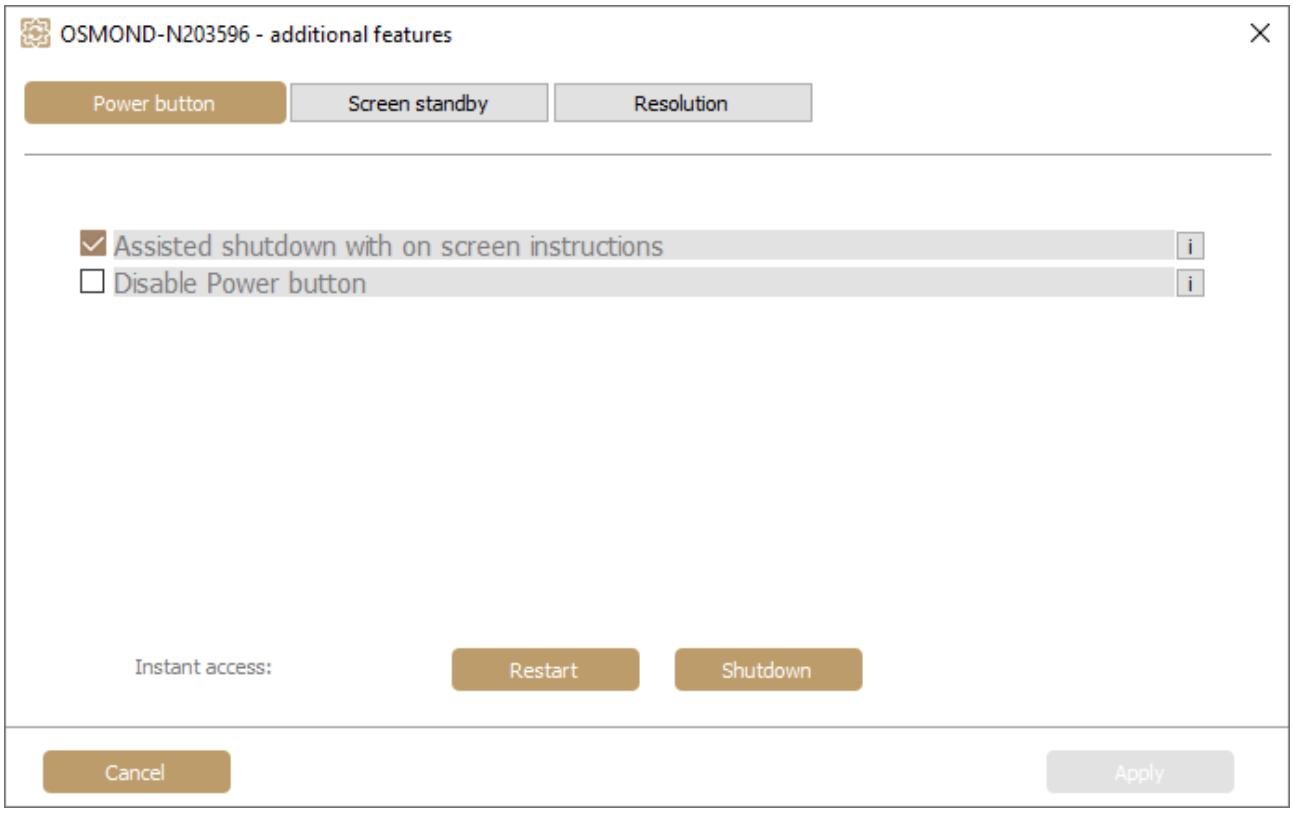
Osmond passport reader devices use ZIP archives as update files and to every ZIP file belongs a CHK file which is the hash signature of the update archive. The signature ensures that the update file is unmodified and undamaged. The two files should be in a same folder with the same name (e.g., update.zip, 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.





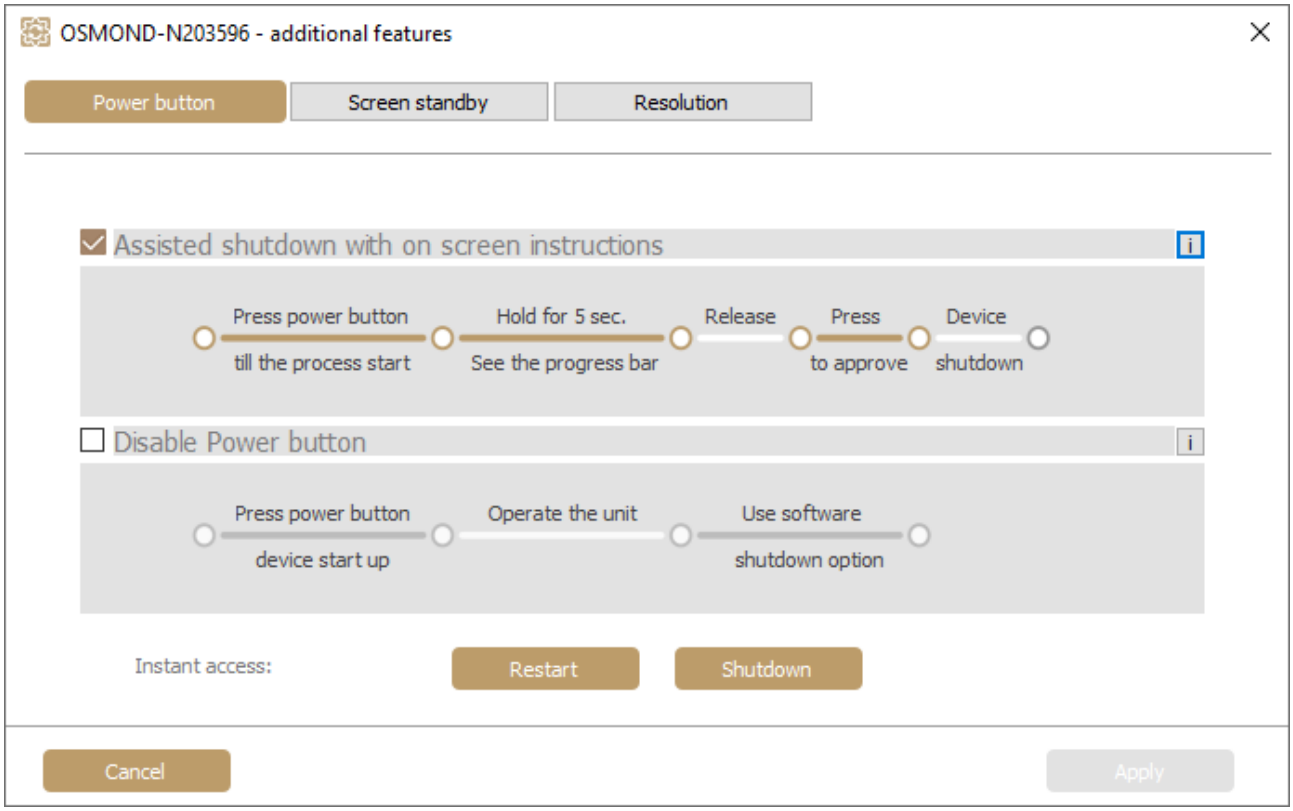
> **Note**
>
> These functions of the PRDTool are only available from Passport Reader version 2.1.10.2.

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

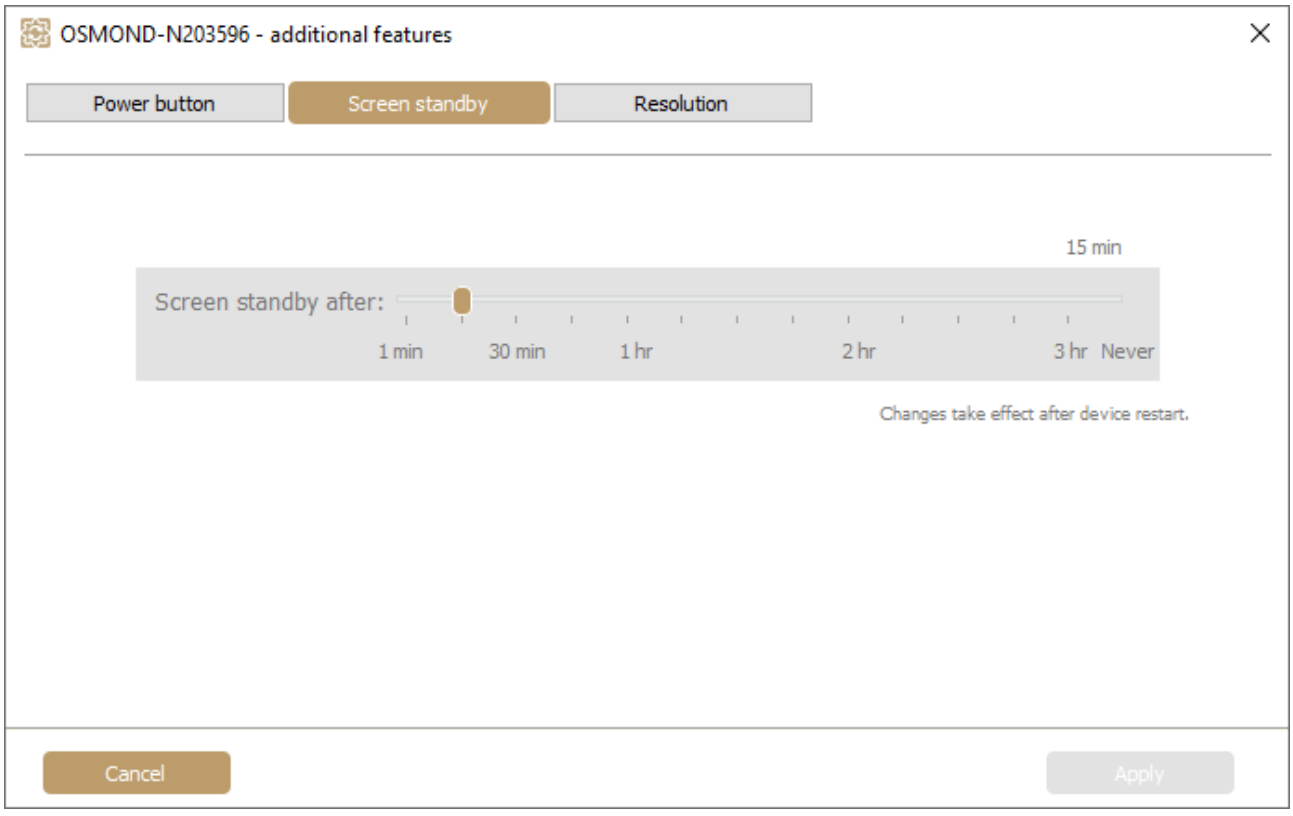
The brightness of the device built-in display can be reduced automatically, after a period of inactivity. Use the slide bar to specify that time period, then click [Apply] to save changes.

> **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.

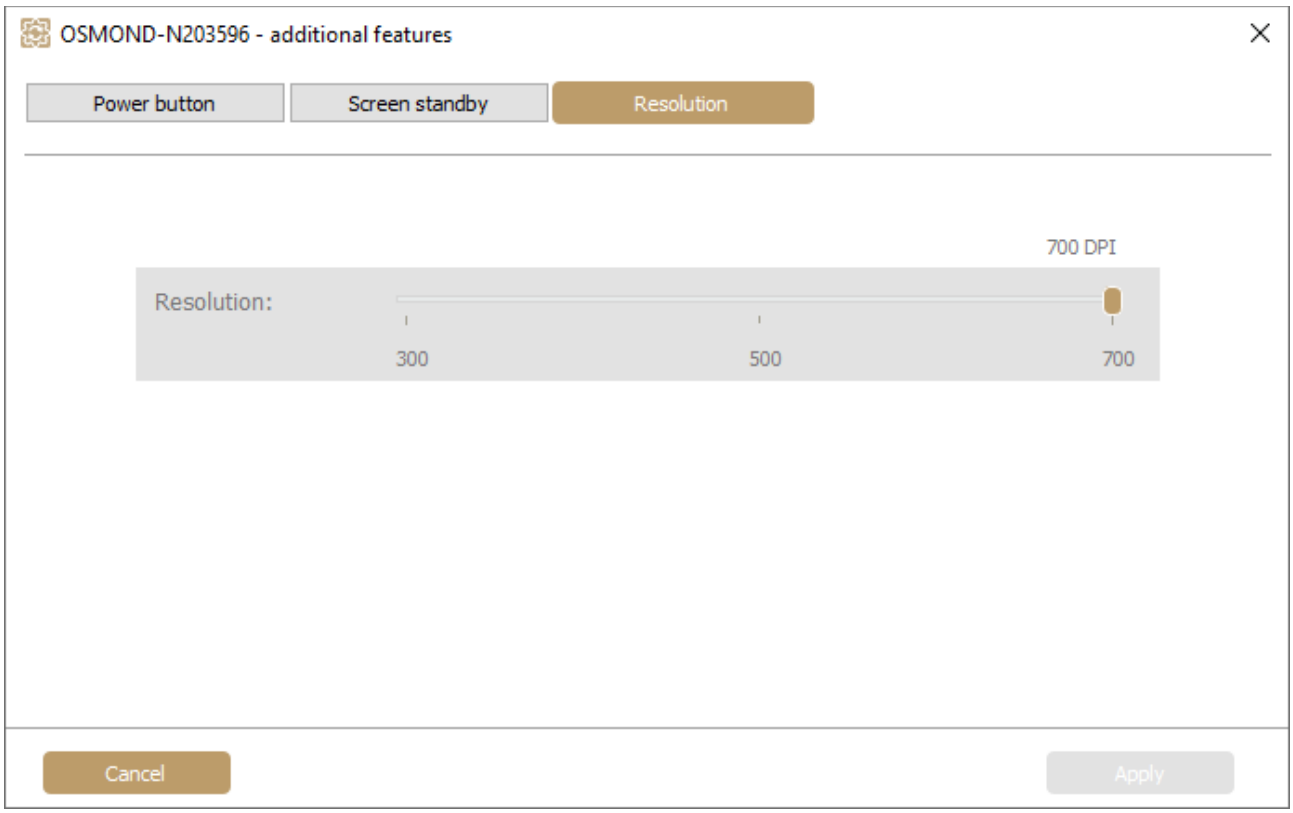


26.4.3. RESOLUTION

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

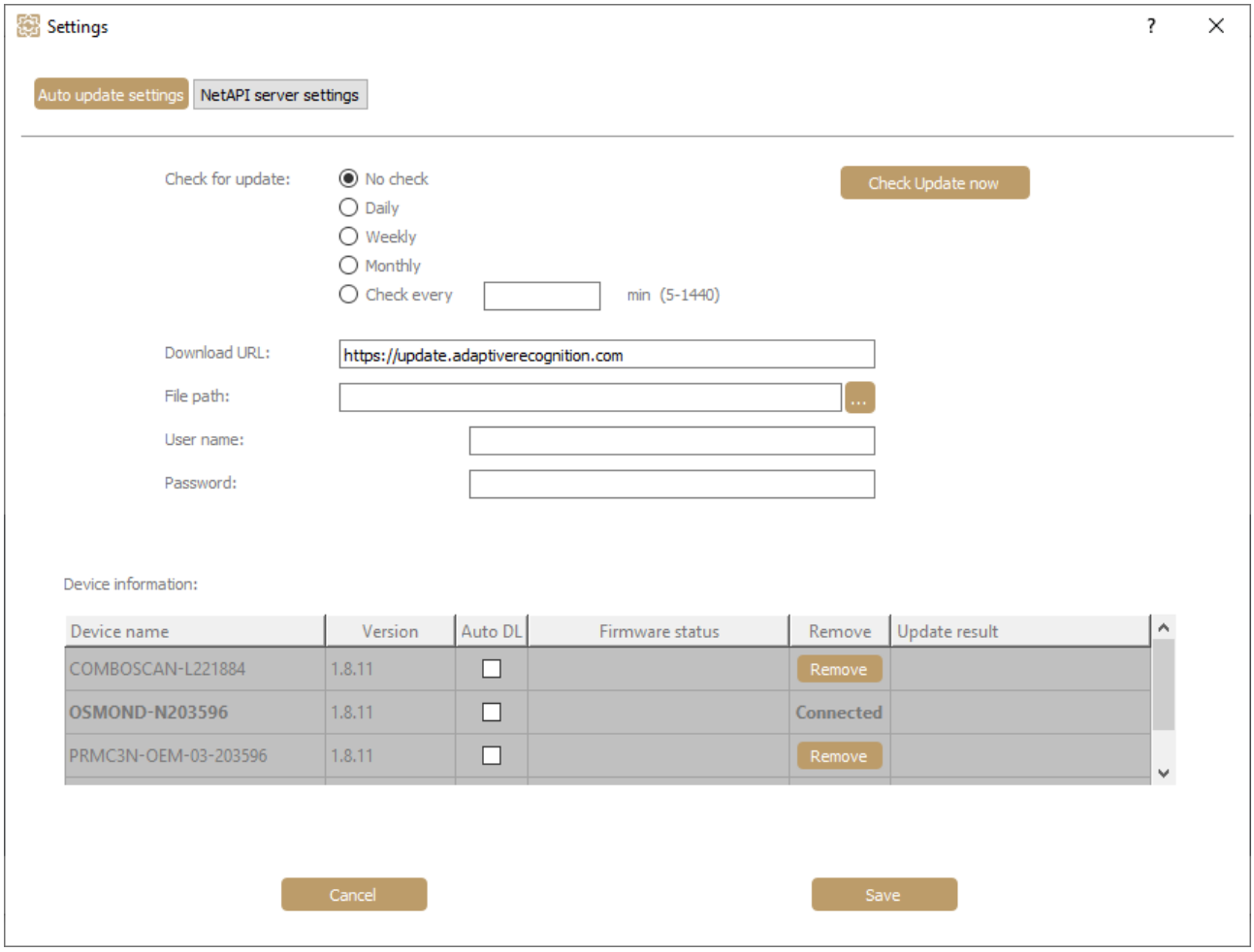
26.5.1. AUTO UPDATE SETTINGS

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.



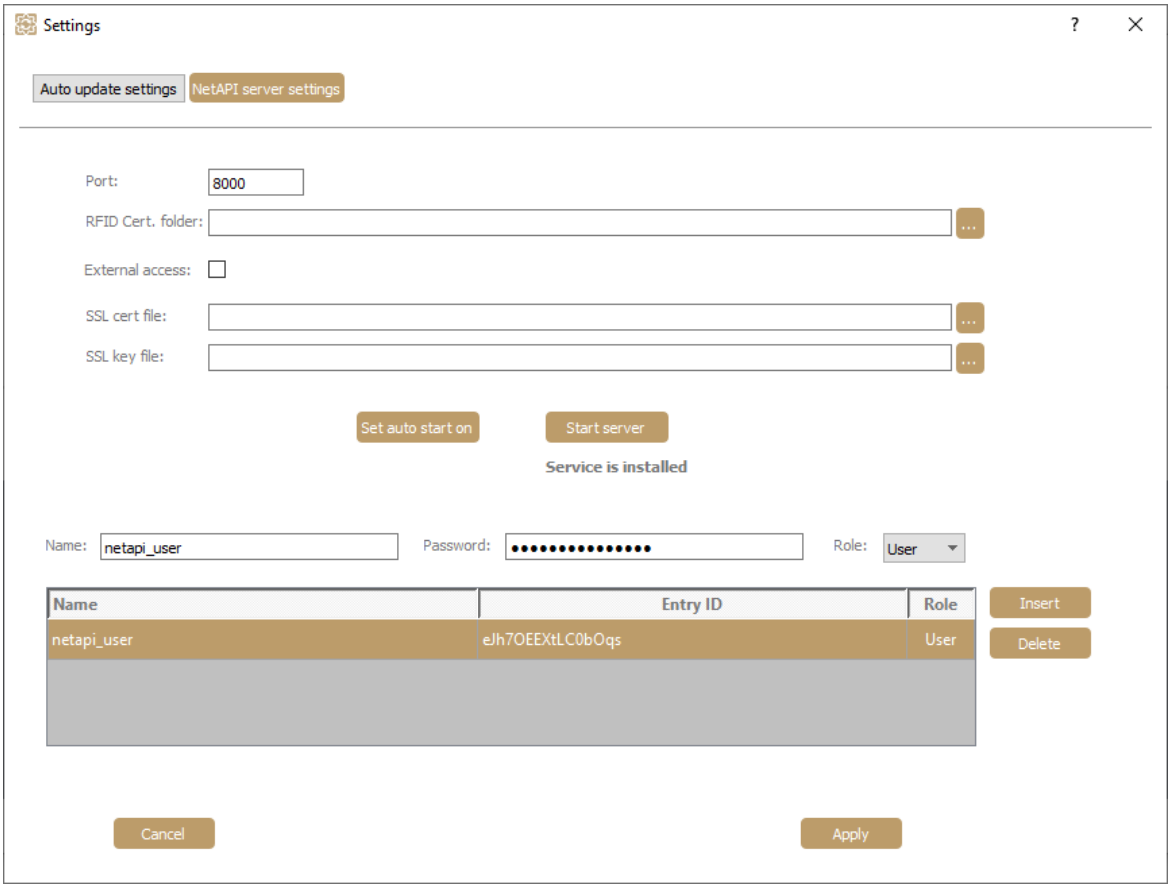
26.5.2. NETAPI SERVER SETTINGS

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

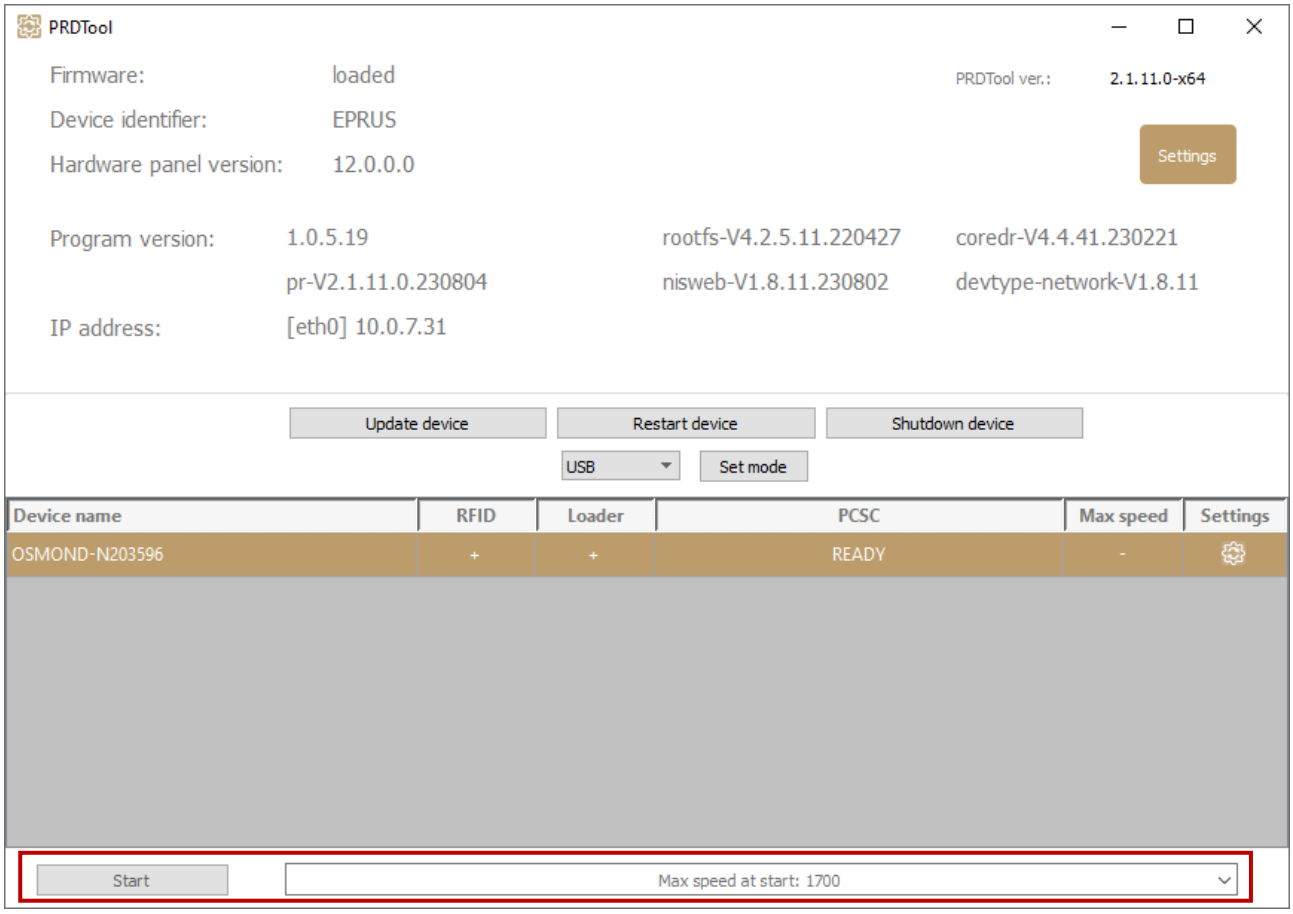
At least one user and the belonging password are required to enter in order to use the NetAPI. Specify the username to the **Name** field and the password to the **Password** field. After that, click on the **[Insert]** button in order to add the entered user.

> **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.

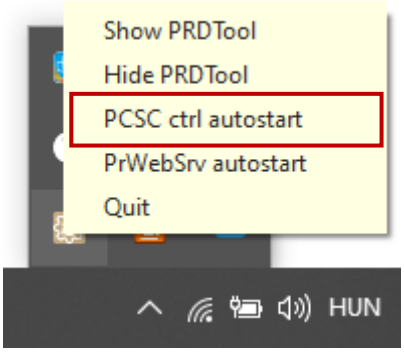


The default status is either READY or STARTED (if PCSC Autostart is enabled). The current status is displayed under the PCSC column. PCSC can be enabled or disabled by clicking on the device name, and then on [Start] or [Stop]. The "max RFID communication speed at start" can be selected under the Max 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>
```


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

27. OSMOND SYSTEM RECOVERY

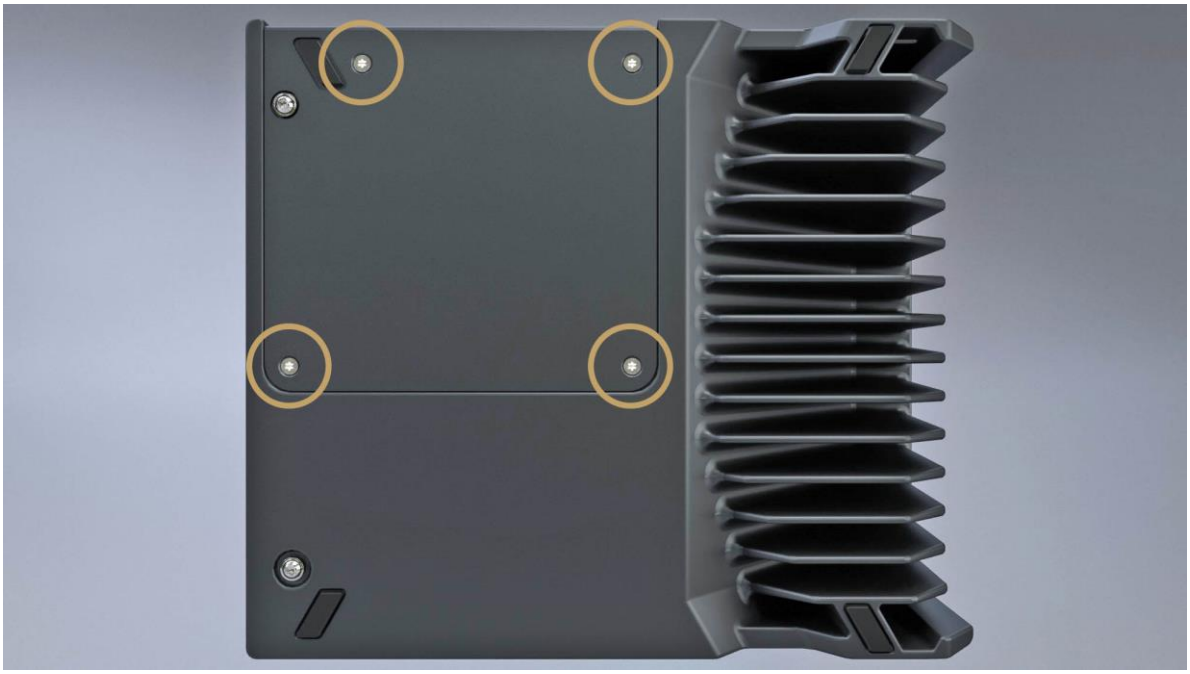
With the system recovery the original manufacturer settings are restored, therefore all saved and stored data is erased.

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

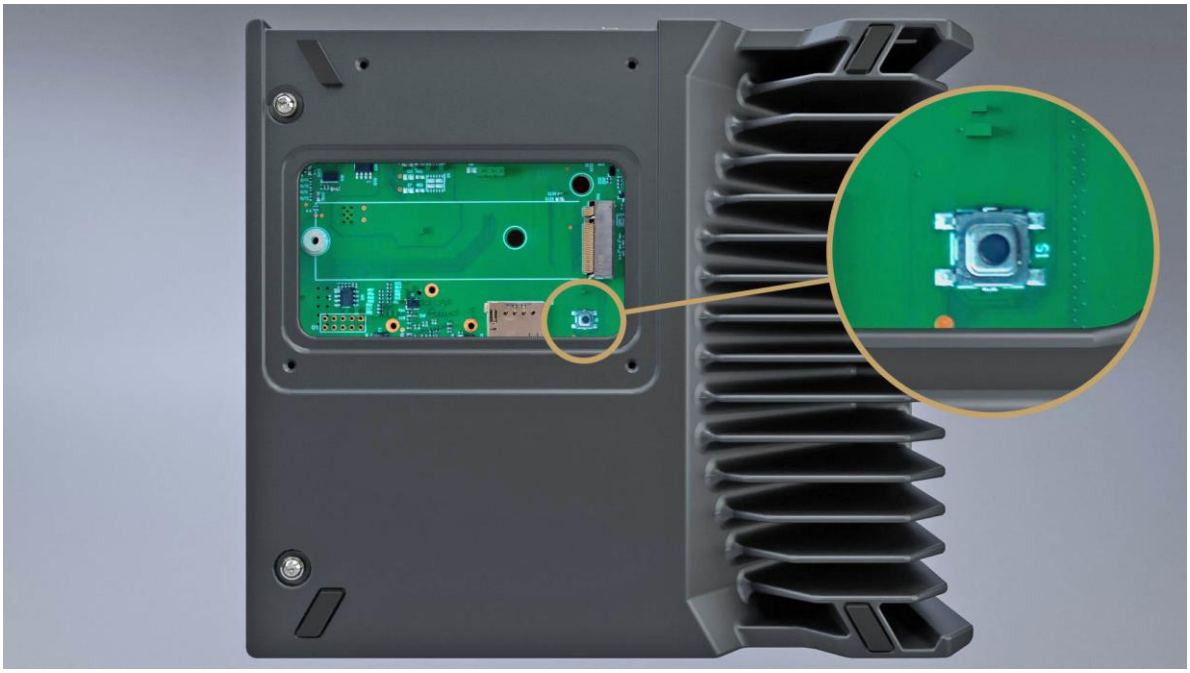
2. Place the device on its side looking out for the aluminum heat sink and unscrew the 4 smaller screws in order to remove the cover plate.



Note

Use an 8 TX screwdriver.

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.

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."

28.4. RSS-GEN STATEMENT (**CAN ISEDES-003(B) / NMB-003(B)**)

"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.

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

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

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

IX. 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.