sendys explorer

ADMINISTRATOR GUIDE

SENDYS EXPLORER

Output Manager

©Alidata

Version 4.2.0

Revision Date: 25-02-2021

ALIDATA SOFTWARE

INDEX

How to Read This Manual 7
Overview 8
Features Matrix 9
Supported languages 9
OCR Software 9
Installation 10
System Requirements 10
Hardware / Operating System 10
Software 10
Installing 11
Updating 17
Removing 18
Admin Config 19
Global Settings 19
Navigation Menu 21
After Installation / First Time Setup 22
Printer Management 23
Printer 23
Device Configuration 29
Output Manager Connector 86
Advantages 86
Installation 87
Overview 89
Dashboard 95
IT-Manager 95

Usage Rate 96
Devices 97
Environment 98
Devices 99
Printers/MFPs 99
Supplies 115
Unmanaged Devices 116
Queues 117
Configurations 122
RFID 142
Touch 148
Users & Groups 153
Users 153
Contacts 162
Groups 165
Map Users-Groups 173
Roles 174
Map Users-Roles 175
Permissions 176
Cards 178
Cost Center 180
Printing Policies 183
Quota management 183
Policies 185
Rules 190
Clean Spooler Job 191
Print Job Converts 192

Other Policies 194
Data Leak Prevention 196
Server Configurations 202
Application Settings 203
Directory Service 217
Server List 229
Connectors 230
Hard Link to a Specific Connector 230
Print 232
Me 234
Email 236
Home Folder 239
Fax Server 241
Upload Document 244
SharePoint 246
Google Drive 249
Dropbox 250
OneDrive 251
OneDrive 365 252
Yandex 254
Output Manager 255
Flex Connectors 256
Flex Connector Plus 268
Fleet Manager Connector 284
OCR Configurations 285
Tesseract 285
ABBYY Recognition Server (SENDYS Explorer PREMIUM) 286

Documents 292
Spooler Job 292
Spooler History 293
Scanned Files 294
DLP Documents 295
Reports 296
Data Analysis 298
Benefits 299
Costs 301
Volume 303
Environment 305
List 307
Other 309
Schedule Reports 311
Warnings & Logs 315
Printer Warnings 315
All Warnings 316
Alert Message Queue 317
Send Items 318
Application Logs 319
Email Message 320
File Configuration 321
Warning Supply/Status 322
Printer Warning Log 331
Log Report 332
License 333
Add 333

Update....335

Remove....336

Check for Updates....338

HOW TO READ THIS MANUAL

In this Administration Manual, we will cover all the administration features as you may encounter while using SENDYS Explorer web portal application. By using this if you have a specific problem you can go straight to the correspondent section.

OVERVIEW

SENDYS Explorer is a web based server application that transforms scanned images into editable formats (Microsoft Word, Microsoft Excel, TIFF, searchable PDF and PDF/A) using OCR (Optical Character Recognition) technology which is included in all versions.

With this application, users can scan documents and distribute the files to email, network folders, email-fax servers, cloud services and document management systems.

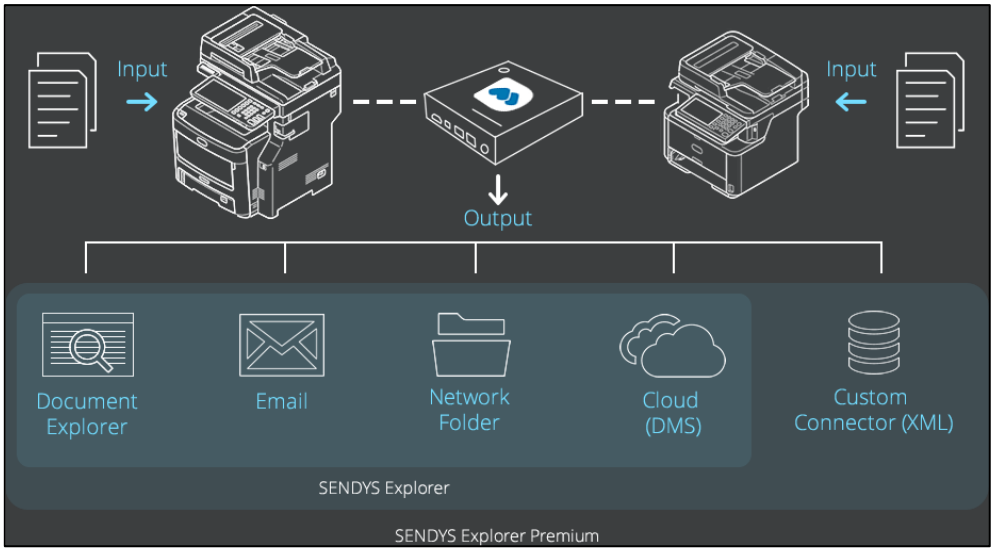


Fig. 1 - Overview

FEATURES MATRIX

Please go to the follow URL to review the application features:

https://www.sendysexplorer.com/support/feature-matrix/

SUPPORTED LANGUAGES

Please go to the follow URL to review the application supported languages:

https://www.sendysexplorer.com/support/specifications/

OCR SOFTWARE

SENDYS Explorer software comes with two OCR options:

The free version of SENDYS Explorer uses **Google Tesseract**, possibly the most accurate open source OCR engine available. Combined with the **Leptonica Image Processing Library** it can read a wide variety of image formats and convert them to text in over 60 languages.

To see the supported languages, refer to the online list at:

https://github.com/tesseract-ocr/tesseract/blob/master/doc/tesseract.1.asc#languages

SENDYS Explorer PREMIUM uses **ABBYY Recognition Server OCR** - An award-winning professional OCR software that offers a broad range of functionality for the various needs of small business, enterprise, academic and government environments. It helps to streamline document processing, turning scans, PDFs into searchable and editable formats, such as Microsoft Word and Microsoft Excel.

For a list of supported languages please refer to:

https://www.abbyyeu.com/rs/en:recognitionlanguages

SENDYS Explorer PREMIUM is designed for mid-to high-volume batch processing through different licensing tiers:

- Bronze server (up to 25,000 scanned pages per year)
- Silver server (up to 50,000 scanned pages per year)
- Gold server (up to 100,000 scanned pages per year)

INSTALLATION

SYSTEM REQUIREMENTS

HARDWARE / OPERATING SYSTEM

Please refer to:

https://www.sendysexplorer.com/support/specifications/

SOFTWARE

The following software is required and will be installed if not currently present on the system.

- Internet Information Service (IIS 7/IIS 8)
- FTP Server
- .Net Framework 4.0
- Windows Installer 4.5 (if you have not this requirement you will be need to restart the system after the installation).

INSTALLING

1. Run **SendysExplorer.exe** as administrator

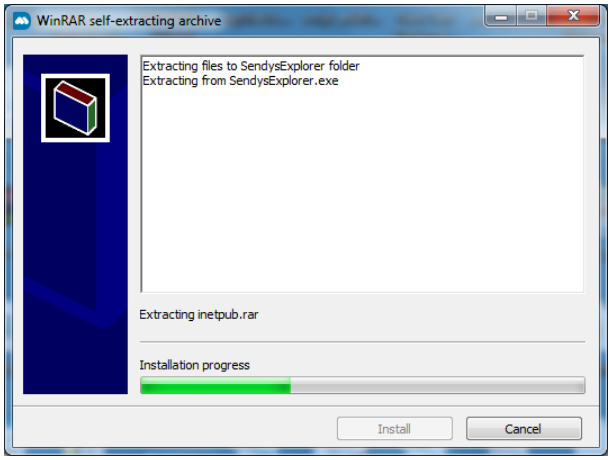


Fig. 2 - Installation start up

2. If the system does not have .NET framework 4.5 installed the installer will set it up before proceeding to the product installation.
3. If the system does not have the required features the installer will try to enable them.
4. Select setup language and press **OK**.

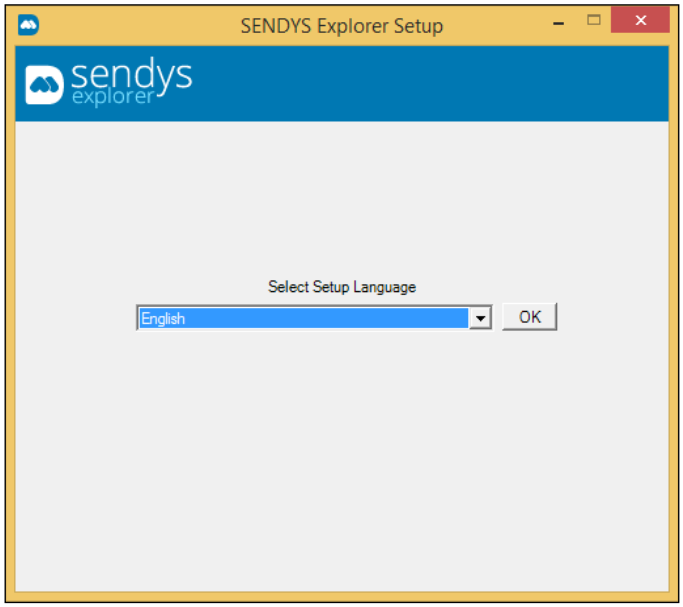


Fig. 3 - Language Selection

5. Click on **Install**.

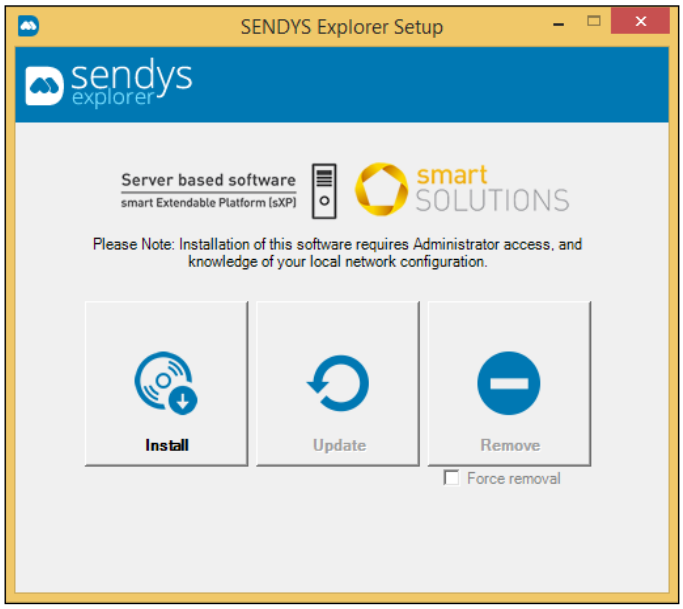


Fig. 4 - Setup Options

6. Click on **Next**.

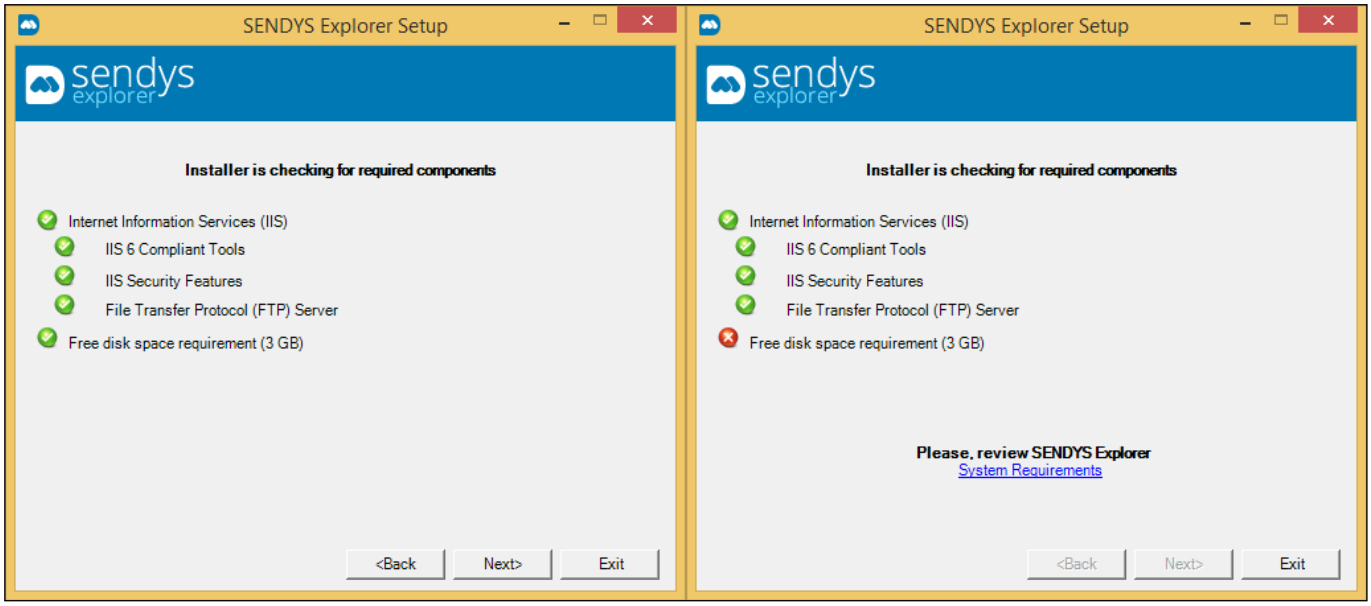


Fig. 5 - Installation requisites without/with error.

Note: If you have any missing components, the system will prompt to automatically install them but if there is any error, please review the troubleshooting guide.

7. Read and **Accept** licence terms and click on **Next**

Fig. 6 - Installation license

8. Insert username and password of a user with local **administrator privileges**.
   a. For a local account: account
   b. For a domain account: domain\account

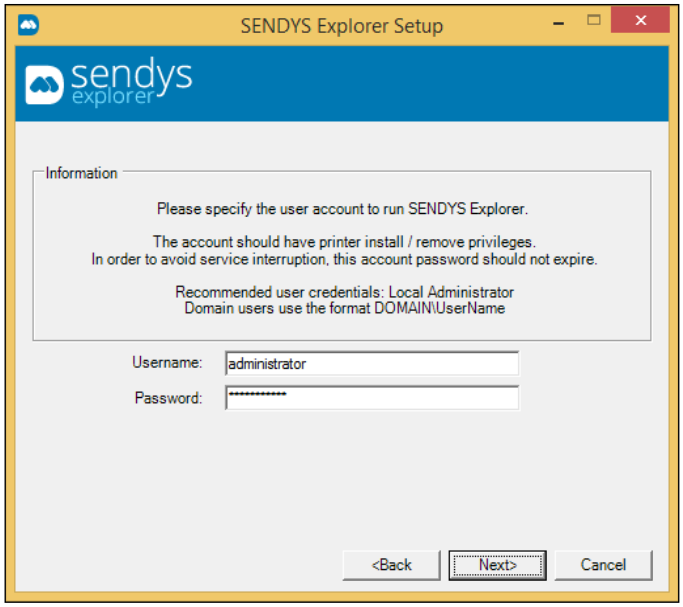


Fig. 7 - Installation Account setup

9. Select the Server IP address and Application port (the default port is 50091). If you are unsure about the port, press **Next** to accept the suggested port. If your choice of **IP address** is a host name, you must ensure that all connected devices (MFPs and printers) are correctly configured to use DNS.
10. Click on **Next**

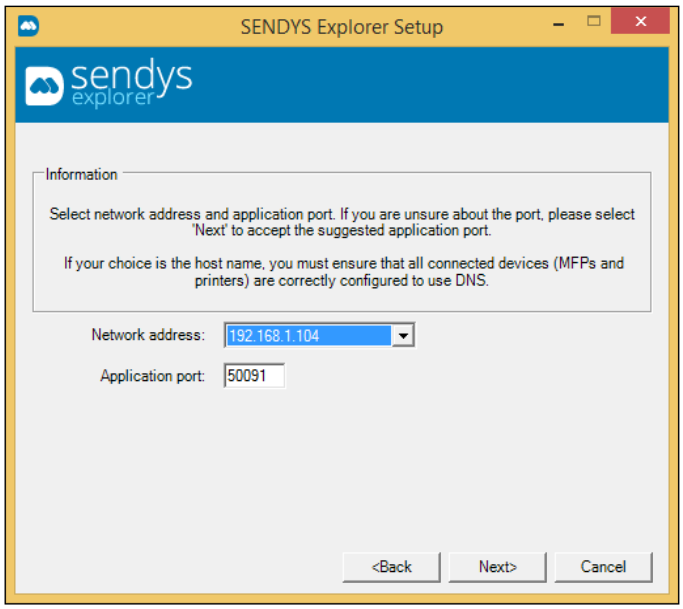


Fig. 8 - Installation IP setup

11. Wait for installation to complete

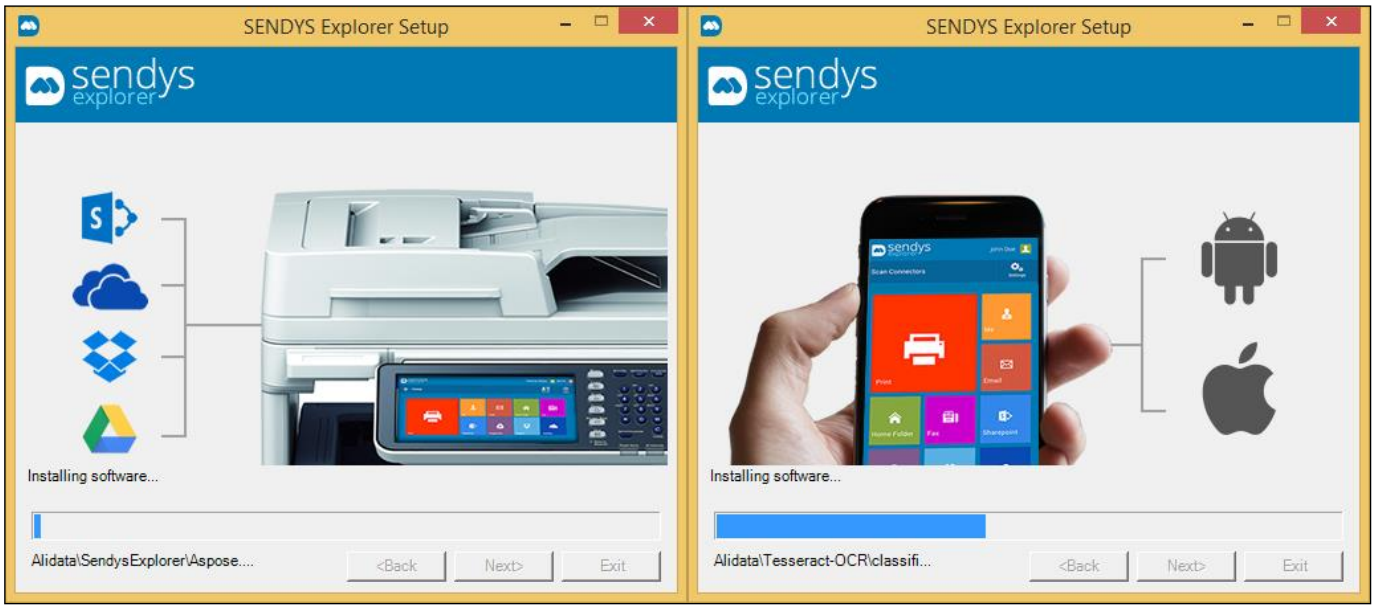


Fig. 9 - Installation progress

12. If you have **internet access** you can proceed with **online activation**. Otherwise go to step **[16]**.
13. **Insert the serial number** that you got from the registration website, and click **Next**
14. **Proceed to step [21]**.
    Note: The steps [16] to [21] are only required if you lack an **internet access** and can't use **online activation**.
15. **Insert the serial number** that you got from the registration website, and un-check the **online activation** box.
16. Click on **License file location**.
17. Send the file **SENDYSExplorer_lic** as attachment to activation@sendysexplorer.com.
18. You will receive the **Activation Key** in your email.
19. Insert the **Activation Key** into the installer.
20. Click **Next** to activate your product, if successful you will receive a message.

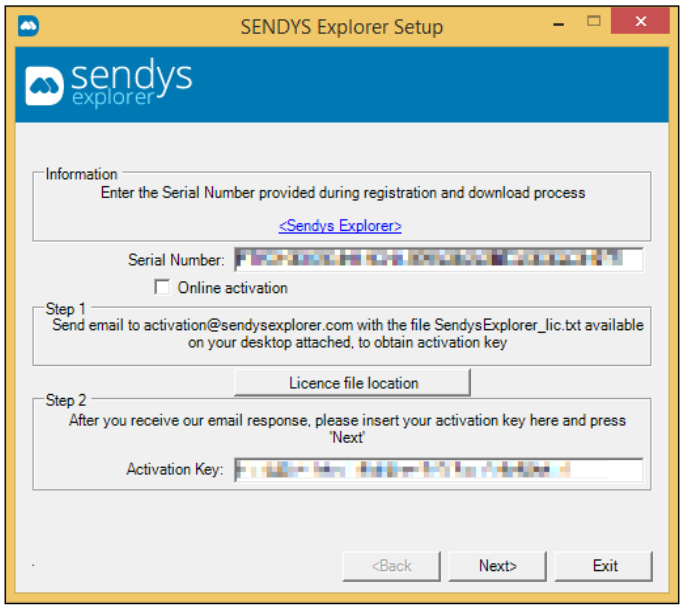


Fig. 10 - Installation Offline Activation

If the installation responds with "**Activation failed**", please contact support@sendysexplorer.com.

21. Click **Exit** to finish the installation and start the application.

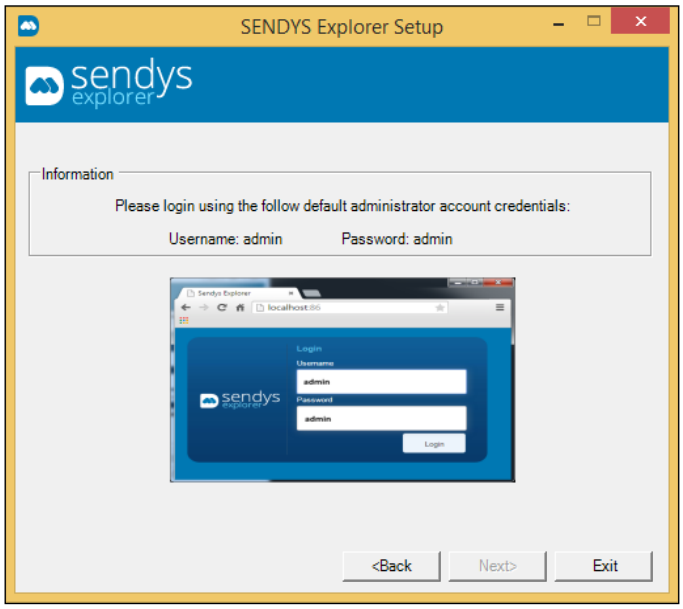


Fig. 11 - Installation Completed

22. The default administrator credentials are.
    a. Username: **admin**
    b. Password: **admin**
23. To complete the installation, go to **Admin Config**

UPDATING

The Update option is available if the SENDYS Explorer software is already installed on your server. The entire configuration in the database will not be deleted.

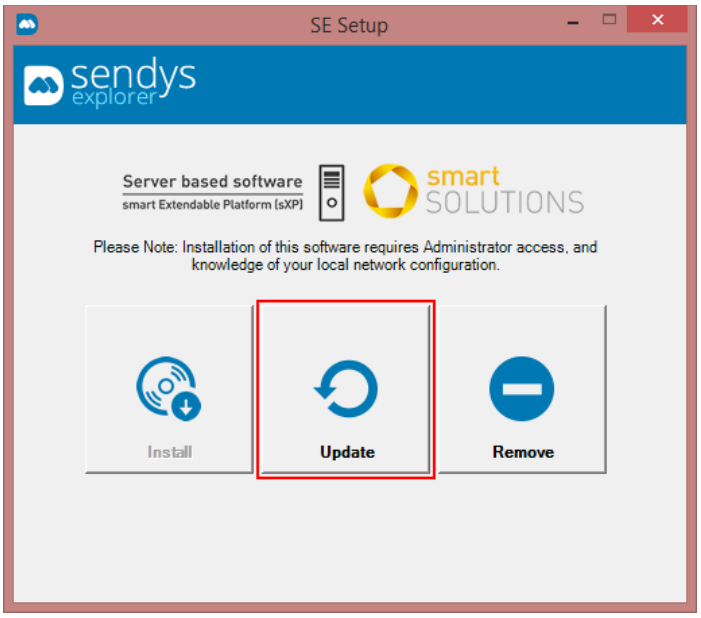


Fig. 12 - Updating

REMOVING

1. Click on **Remove**.

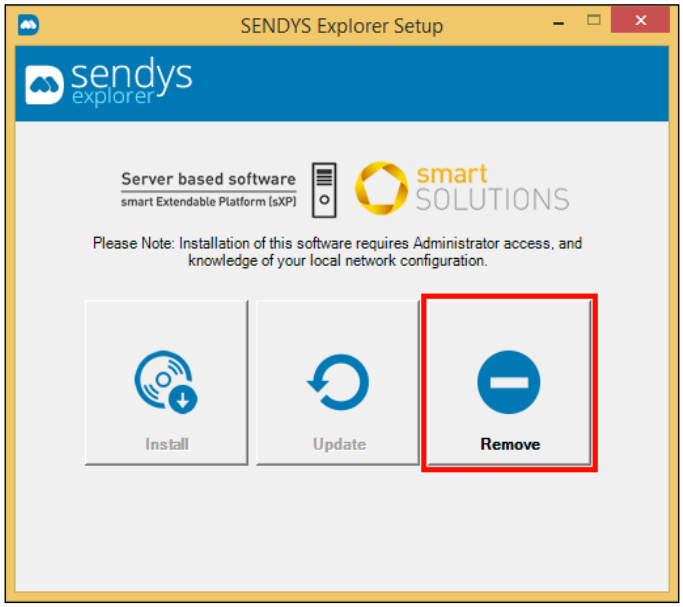


Fig. 13 - Uninstalling

2. Click on **Yes** to confirm uninstall
3. Click on **Yes** to remove the scanned files.

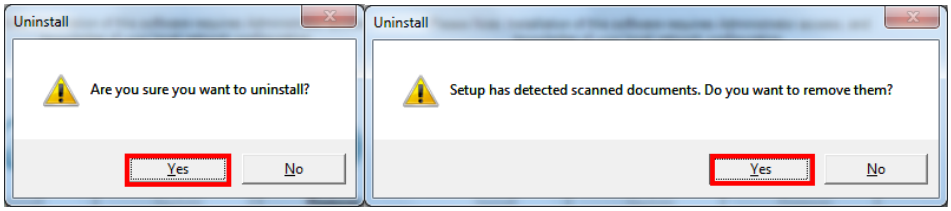


Fig. 14 - Removing files

4. Click on **Yes** to remove ABBYY Recognition Server installation if you have it installed.
5. Click **OK** to complete the removal.

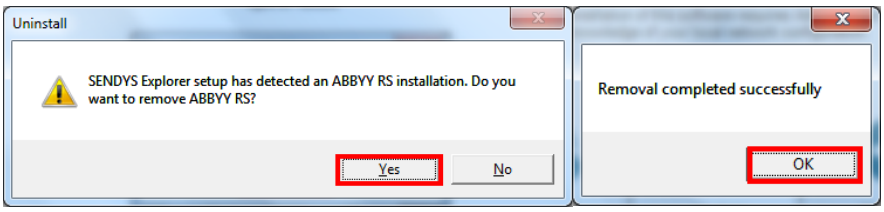


Fig. 15 - Uninstalling ABBYY

ADMIN CONFIG

GLOBAL SETTINGS

1. Go to the browser http://serverIP:50091/.
2. Login on the application as admin.
   Note: By default, you can sign in using **admin** both **username** and **password**.
3. Click on **Admin Config**.

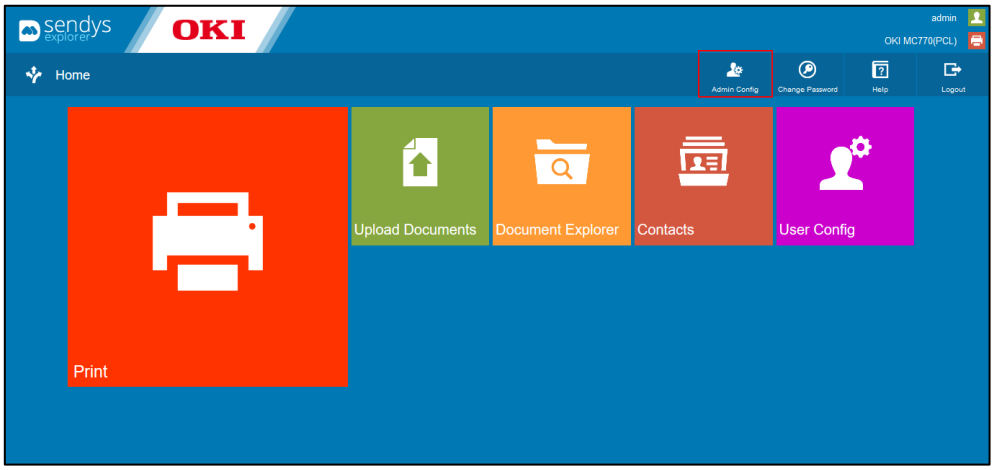


Fig. 16 - Web Portal

All configuration screens are work similarly, so we will start by explaining the basic icons and options of the admin configuration section.

Fig. 17 - Grid of possible Options

In the grids/table of contents we can find the above icons:

Selection element	Preview
Not possible to delete element	Link to device webpage
Delete element	Download
Edit element	

In most of the sections the edit and delete buttons are in the grid/table of contents on the left side, as in the following picture.

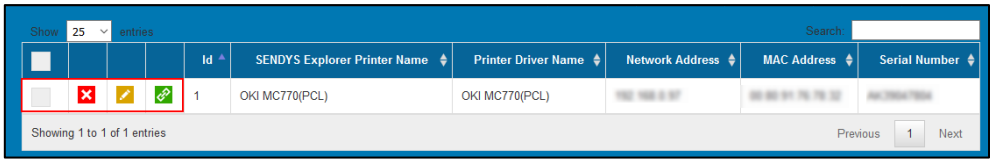


Fig. 18 - Grid buttons

The **Add** button and other section options are in the top right corner as in the below picture.

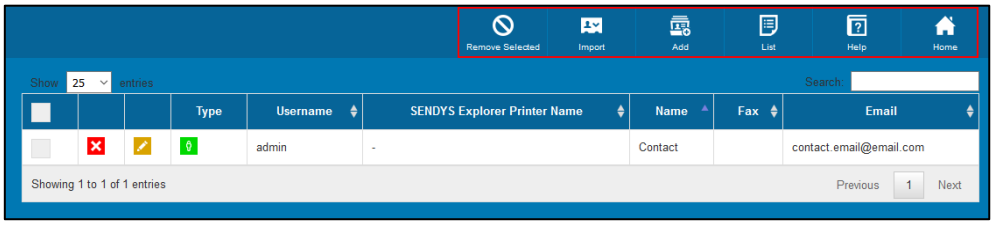


Fig. 19 - Section Options

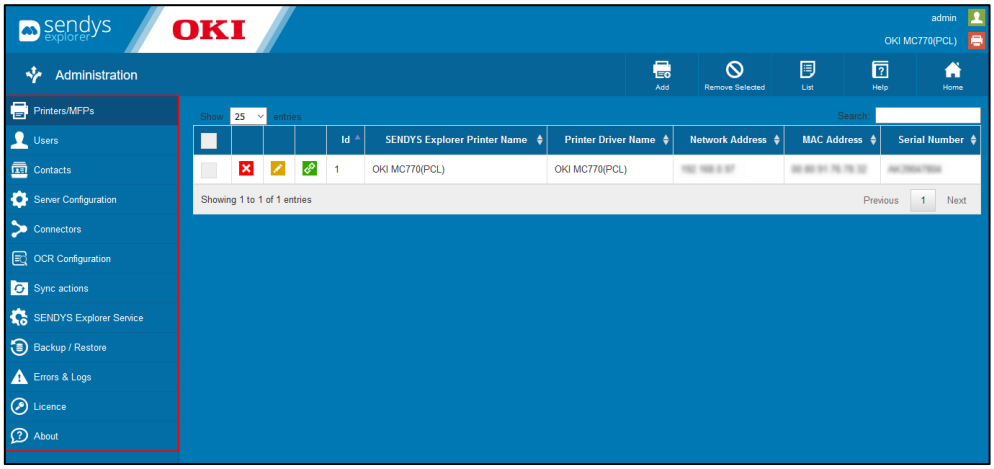


Fig. 20 - Admin navigation menu

NAVIGATION MENU

Name	Details
Printer	View, add, edit and delete devices
User	View, add, edit and delete users
Contacts	View, add, edit, import and delete contacts
Server Configuration	Configure all the settings of the application
Connectors	Configure all the profiles, parameters and views
OCR Configuration	Configure OCR options
Sync Actions	Synchronization, import and bulk actions
SENDYS Explorer Service	Start or re-start the service
Backup/Restore	Backup and Restore options
Errors & Logs	View Logs and send message to development team
License	License and activation
About	Verify the current version and some application information

Table 1 - Administration Details

AFTER INSTALLATION / FIRST TIME SETUP

There is a common series of steps that you should follow after the product installation. These topics are covered in the next part of the guide.

1. **Install the printer driver** on SENDYS Explorer server, this will be needed to print the scanned files.
2. **Add the Printer(s)** to SENDYS Explorer (if you are working with Directory Service, make the directory service configurations and synchronize the users before adding the devices).
3. **Setup the devices**.
4. **Users** and Error! Reference source not found.:
   a. If you are working with **Error! Reference source not found.** follow the steps [5 to 8].
   b. If you are working with SENDYS Explorer Authentication jump to step [9].
5. Go to **Error! Reference source not found.**.
6. **Setup Error! Reference source not found. map**.
7. **Setup Error! Reference source not found. settings**.
8. **Synchronize** with **Error! Reference source not found.** jump to step [10].
9. **Create the users** on SENDYS Explorer.
10. Now that you have defined the users' authentication type go to **Server Configuration>Application** and setup the correct authentication method.
11. **Setup** the **connectors**.
12. You can **start scanning and printing**.

PRINTER MANAGEMENT

PRINTER

For the application is only possible to add OKI devices. All other devices are unsupported by the application. You can only add unique devices[1] to the application.

- Go to Admin Config>Printer
- Use Add button to add a new printer
- Use Remove Selected to remove the selected devices
- Use List Button to list all printers and access the devices QR Codes
- Click Help to access the administration manual

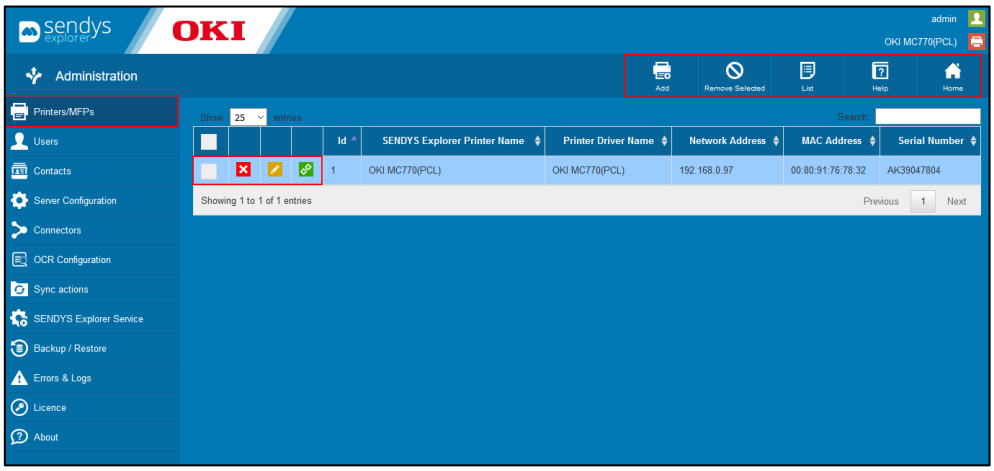


Fig. 21 - Printers/MFPs Section

[1] "Unique devices" meaning a unique device Serial Number, MAC address and IP address/Hostname.

ADD

When you add the devices if it is a smart device we will create a firewall exception for the device's scanned files reception on **SENDYS Explorer**.

Note: You should install the printer driver on the PC before adding the printer to SENDYS Explorer.

1. Click on **Admin Config > Printer**.
2. Click on **Add** to register a new device.

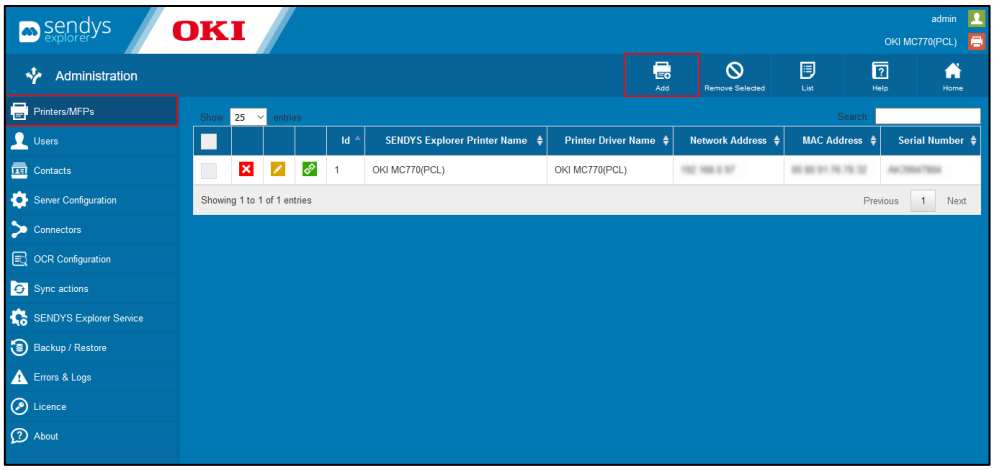


Fig. 22 - Adding a printer

3. Insert valid settings referring to the following information table:

Name	Details
Printer Driver Name	Select the printer on the server (image as example).
SENDYS Explorer Printer Name	Internal application name for the device.
IP Address or Hostname	IP address or Hostname of the device.
MAC Address	If you have some MAC restriction on the network you can configure the device MAC manually, otherwise the system will acquire this information automatically.
Email fax sender address	If you desire to send fax with the device email used in email fax server.
Default User	Insert one valid SENDYS Explorer User to be the default user on the device, when using other authentication then SENDYS Explorer
A3/Tabloid	Select if the device is A3/Tabloid, by default the option is disable.
Color	Whether this device is allowed to print in color
Online Activation	Uncheck for offline device activation.
Device activation key	Offline device activation only.

Table 2 - Printer Details

Note: **Printer Driver Name, SENDYS Explorer Printer Name** and **IP Address** or **Hostname** are required fields.

4. If you are using online activation this will create the device and activate it. Otherwise you will need to uncheck online activation. When you click on save this will create a file and will also give you a destination email, send the file as email attachment and you will receive the offline activation key.

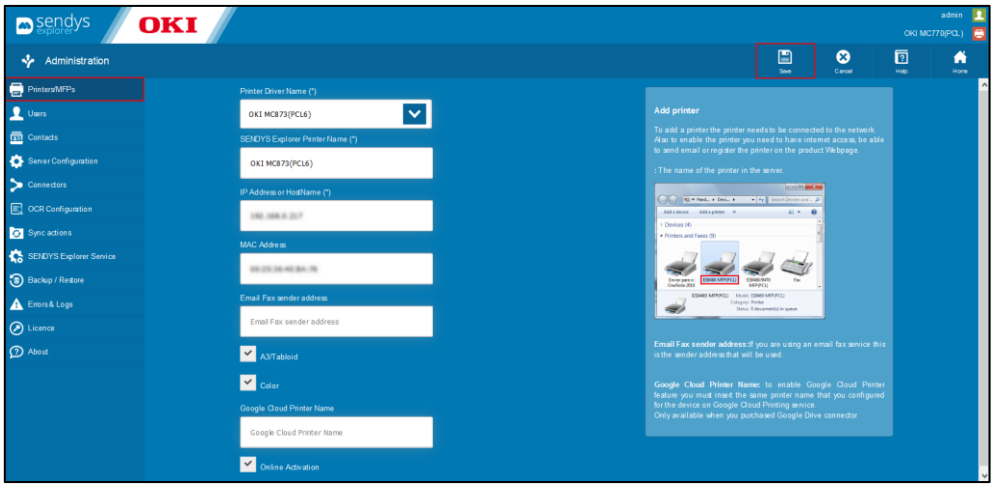


Fig. 23- Add Printer Form

5. A Pop-Up will appear. It will prompt you if you like to try to auto configure the device. Or if you prefer to proceed with manual device configuration.

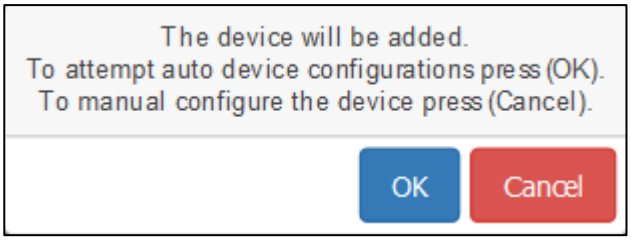


Fig. 24- Configure Printer Pop-up

ONLINE ACTIVATION

1. To use online activation, make sure that you have internet access.
2. Click **Save**.
3. After you activate the device you will need to set it up depending on the device type. Refer to [Device Configuration].

OFFLINE ACTIVATION

1. Uncheck **Online activation**.
2. Click **Save**, get the license file, and send email to activation@SENDYSexplorer.com
3. Send the email with the device information as an email attachment.
4. Wait for an email with the activation key.
5. Insert the activation key in **Device activation key**.
6. Click on **Save**
7. After you activate the device you will need to set it up depending on the device type. Refer to [Device Configuration].

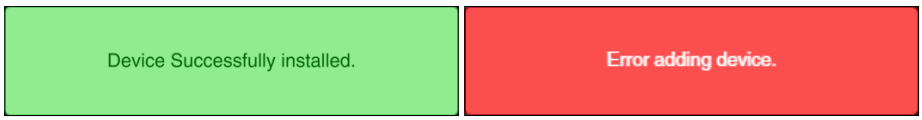


Fig. 25 - Success and Error messages

EDIT

1. Go to **Admin Config > Printer**
2. Click on the **pencil icon** to edit the device.

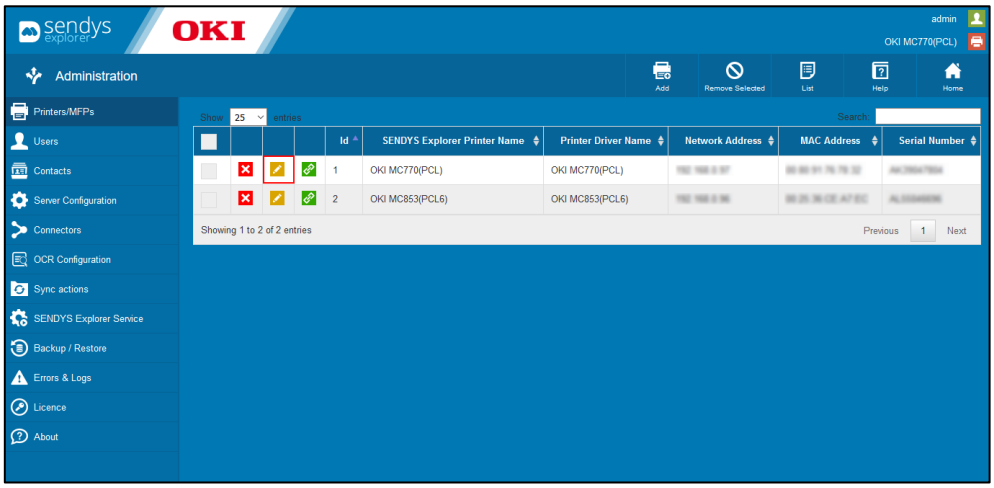


Fig. 26 - Edit Printer

3. Click **Save** to save the changes, **Setup Device** to send configurations to device or **Cancel** to discard them.

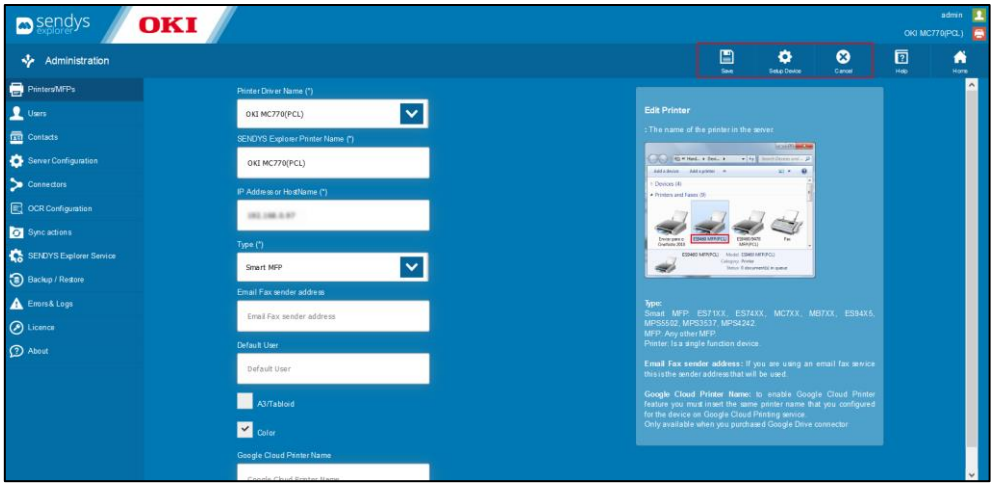


Fig. 27 - Printer Form

REMOVE

To remove the printer, you can either remove a single printer by using the cross icon, or several printers by selecting the printers and clicking on **Remove Selected**.

1. Click on **Admin Config > Printer**.
2. Click on the **cross icon** to remove one printer.

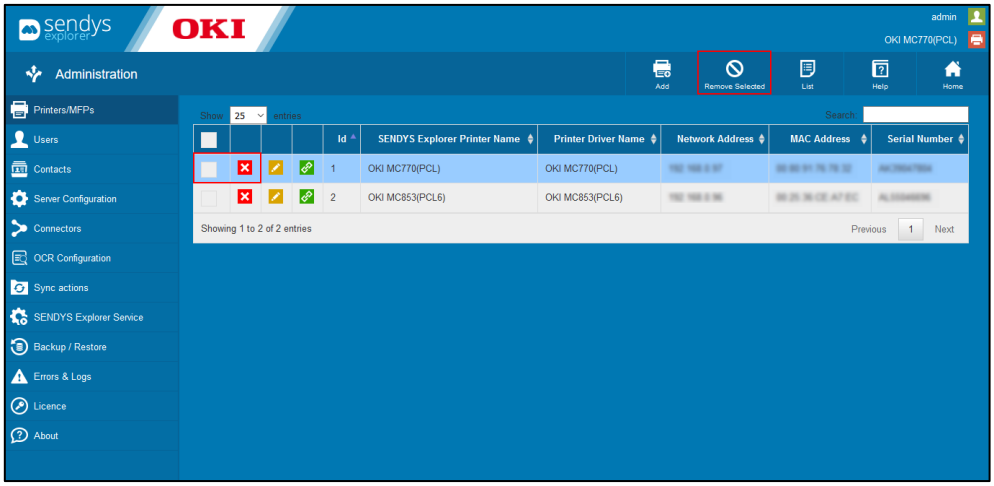


Fig. 28 - Remove Printer

3. Click OK to confirm the Printer removal.

Fig. 29 - Remove Printer confirmation

If you are removing more than one printer:

1. Select the printers that you need to remove.
2. Click on **Remove selected**.
3. Click "**OK**" to confirm the printer removal.

Fig. 30 - Remove Printer confirmation

DEVICE CONFIGURATION

AUTHENTICATION TYPES

There are several authentication methods: **Directory Service**, **MFP Local Authentication**, **SENDYS Explorer** and **SENDYS Explorer PIN**:

- **Directory Service** means that you authenticate on the application and device from a Directory Service and that all users will be imported from it to **SENDYS Explorer**. The device needs to be configured to use the same Directory Service authentication.
- **MFP Local Authentication** means that the users must be created on the device. **SENDYS Explorer** will create the user accounts based on the device in which the first user authentication occurs. The initial **SENDYS Explorer** password will be the same as the username.

Note: For the following two options device authentication must be disabled, otherwise you will have two authentication methods. For both options user accounts will be created through the application's **Admin Config**.

- **SENDYS Explorer** means that users will authenticate on the device using their username/password combo.
- **SENDYS Explorer PIN** means that users will authenticate on the device using their randomly generated PIN number.

Note: Configuration processes for smart and non-smart devices are quite different. Please be sure to refer to the appropriate following sections.

Type	Model
Smart MFP	ES94X5/ ES84X3/ MC8X3/ ES71XX/ ES74XX/ MB7XX/ MC7XX/ MPS5502/ ES5162/ ES5162LP/ MB562/ ES4192/ MB492/ MPS3537/ MPS4242/ MC573/ ES5473
Smart SFP	ES5442/ C542
MFP	any other MFP
Printer	single function device (such as printer)

Table 3 - Device types

SMART DEVICE CONFIGURATION (SXP VERSION 1.0 (MC7XX/ES74XX/ES9XXX SERIES))

BASIC CONFIGURATION

For each Smart device a **port** will need to be assigned for scanning. The base scanning port can be changed under **Server Configuration > Application** on the application's **Admin Config**, and defaults to port **8080**.

A port will then be set for each device added, equal to the sum of the **base port** plus the **device's id** (BasePort + DeviceId).

> **E.g.** if the base port is **8080**, the device with an id of **1** will be set to port **8081**.

When the devices are added to SENDYS Explorer the application will try to open these ports on the **firewall**. Depending on your Security Suite and networking setup the automatic opening of ports may fail.

If you are unable to scan, please confirm that you have these ports open.

SCAN SETUP

We have to configure the device to allow SENDYS Explorer to initiate the scanning process.

Configure Guest account access

1. Go to TopAccess **http://[DeviceIP]**.
2. Click on **Login**.
3. Insert admin username and password (**default**: admin/123456).

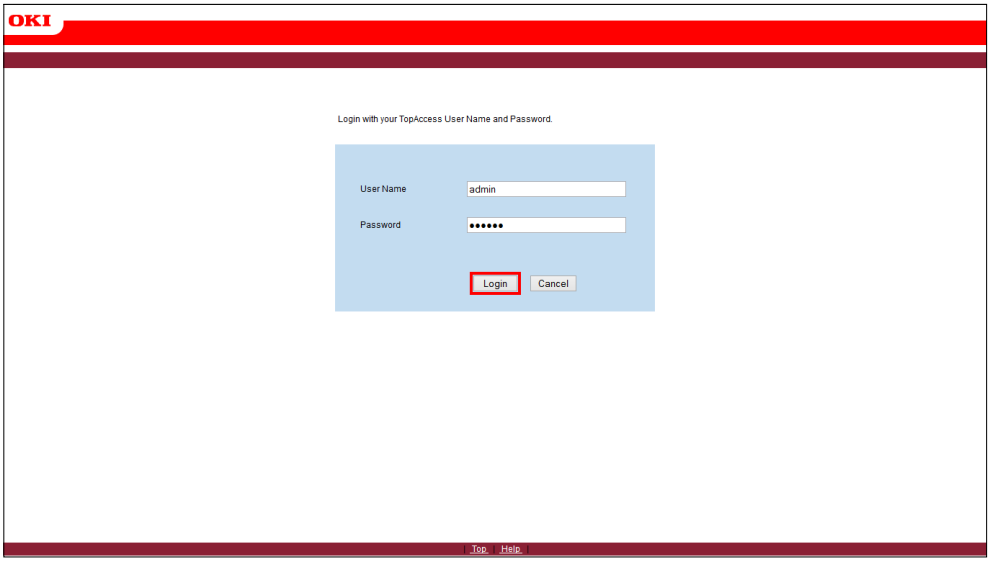


Fig. 31 - Smart Device Login

4. Click on **User Management> Role Management**.
5. Click on **Guest**.

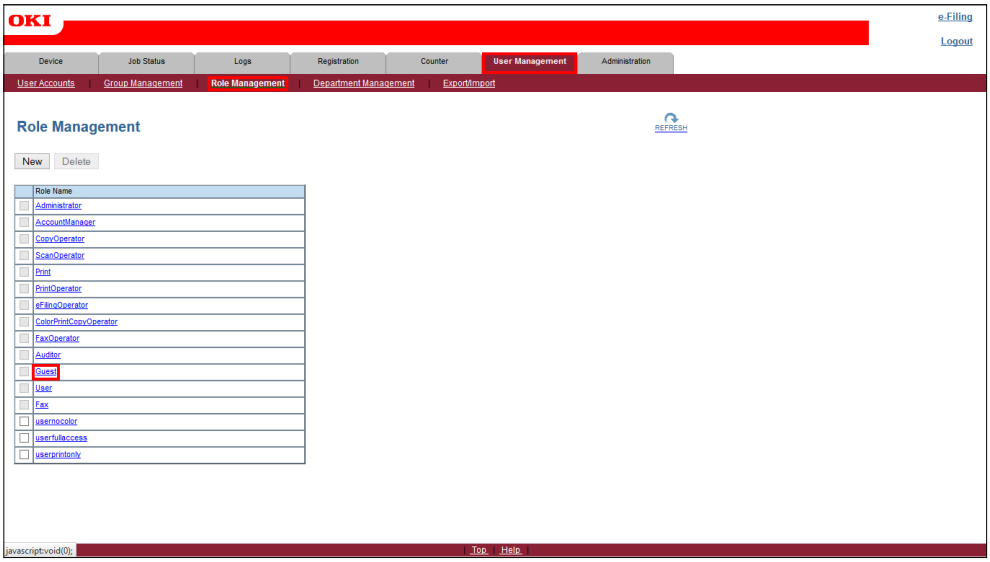


Fig. 32 - Smart Device Role Management

6. **Check**:
   a. Scan Function:
      i. Remote Scan/WS Scan(Pull).
   b. Remote:
      i. Send Email.
      ii. Store to Remote Server.
      iii. WS Scan(Push).
7. Click on **Save**.

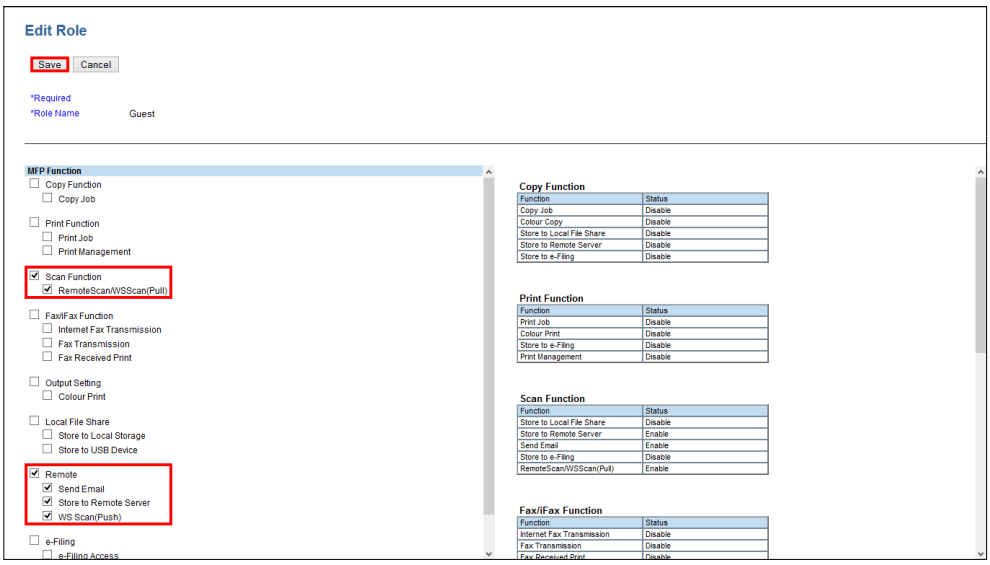


Fig. 33 - Smart Device Configuration

8. Check Web Service Settings
   a. Click on **Administration> Setup > Network**.
   b. Click on **Web Services Setting**.
   c. Click on **Web Services Setting** button.
   d. Enable **Web Services Scan**.
   e. Set **Authentication for PC Initiated Scan** as "***Accept any job***".
   f. Click on **OK**.

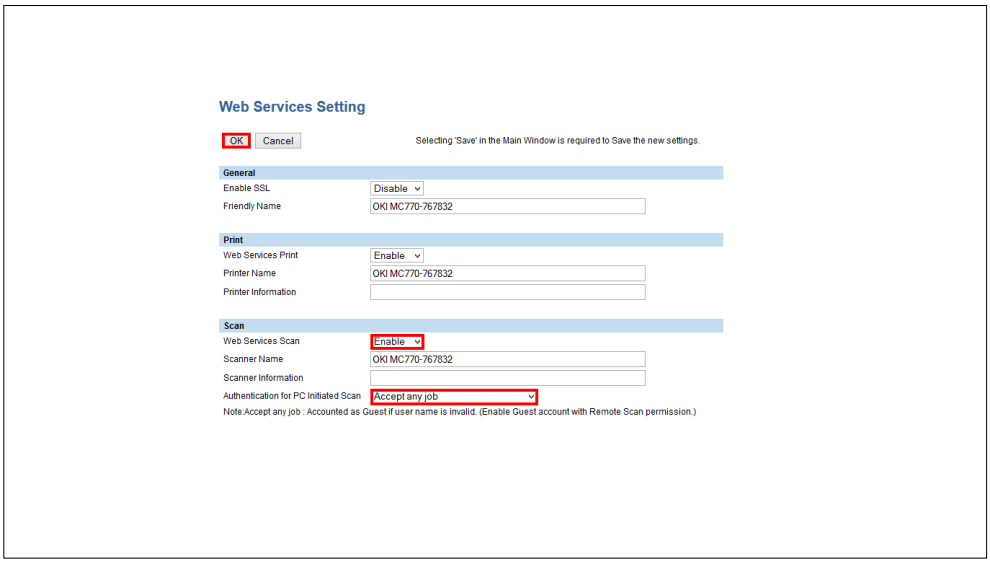


Fig. 34 - Web Services Settings

9. Click on **Save**.

SCREEN APPLICATION CONFIGURATION

In order to see the application on the device screen you need to configure the Embedded Web Browser application on the smart device.

The application address is http://[ServerIP]:50091/scan.aspx and you need to make the configurations on two places. **EWB application** and **server registration**.

1. Go to **TopAccess** http://[DeviceIP]/.
2. Click on **Login**.
3. Insert admin username and password (**default**: admin/123456).

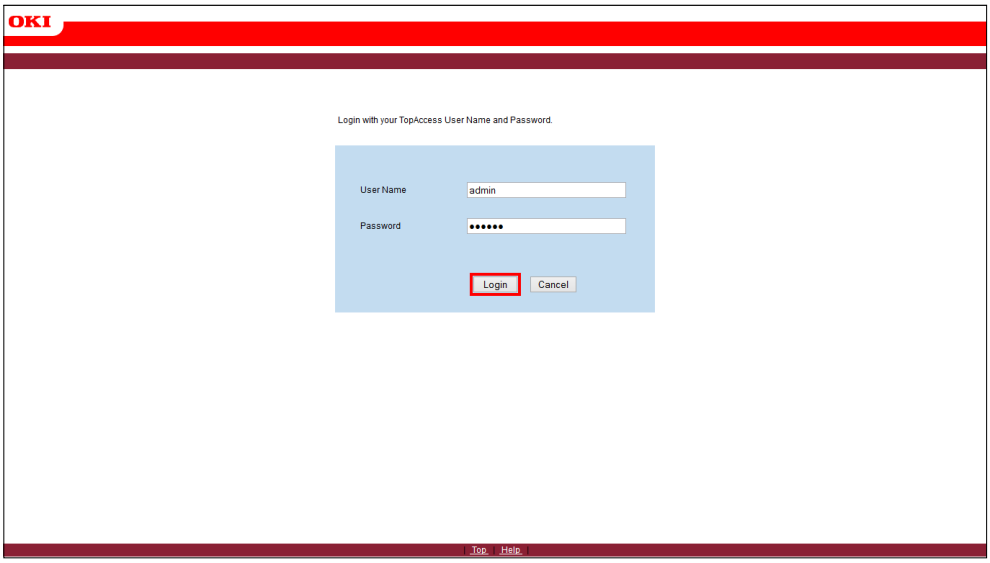


Fig. 35 - Smart Device Login

To configure SENDYS Explorer as default machine screen:

1. Click in **Administration >Setup> EWB**.
2. On Embedded Web Browser:
   a. Set **Home Page** to http://[ServerIP]:50091/scan.aspx.
3. Click **Save**.

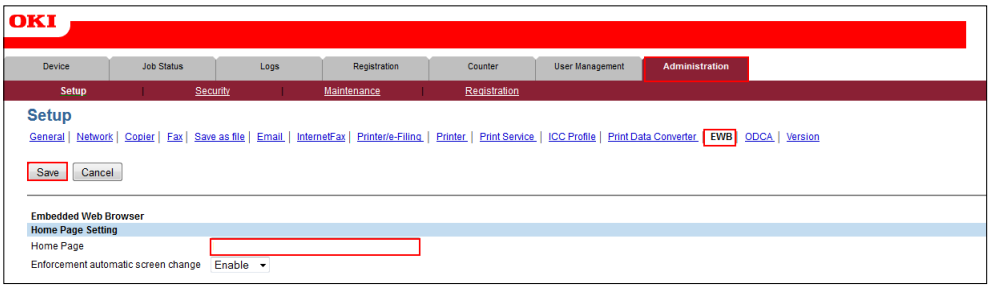


Fig. 36 - Smart Device Configuration

Note: Registering the application on the device is a **required** step in order for the application to function correctly.

4. Click in **Administration >Setup> EWB**.
5. On **Server Registration Settings**:
   a. Insert the address http://[ServerIP]:50091/scan.aspx.
6. Click **Add**.
7. Click **Save**.

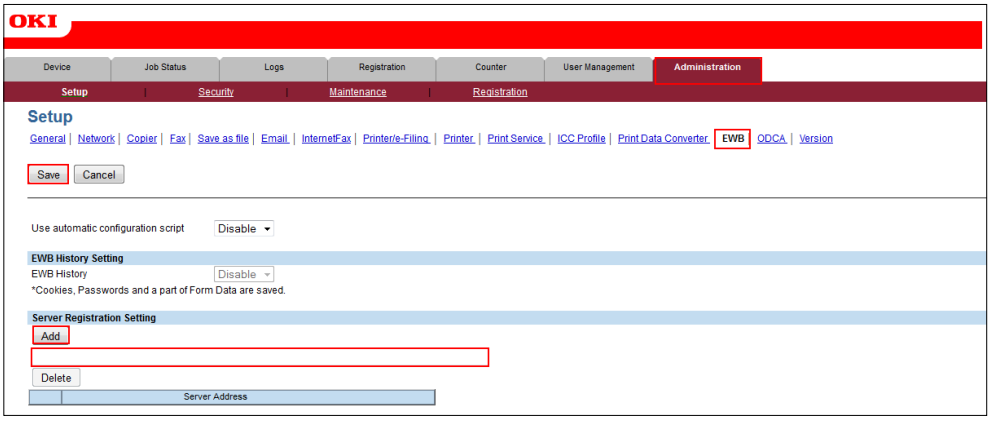


Fig. 37 - Smart Device Configuration

To configure SENDYS Explorer Shortcut On the device:

1. Click in **Administration >Setup> EWB**.
2. On **URL List for Menu Screen and Hard Button**:
   a. Click on **Add**.

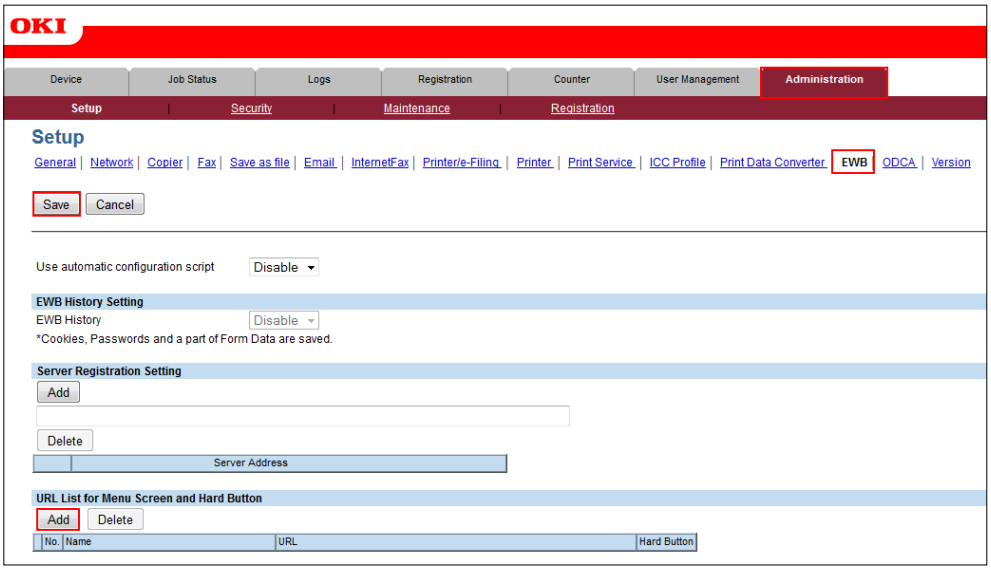


Fig. 38 - Smart Device EWB Configuration

   b. Set the **URL Name** to **SENDYS Explorer**.
   c. Set the **URL** to http://[ServerIP]:50091/scan.aspx.

3. If you wish to configure a **hard button**, select **Assignment for Hard Button**.

Note: We recommend configuring the **SCAN** button so that after logging-in users will be taken directly to the SENDYS Explorer screen by pressing the **SCAN** button.

4. Click **Save**.

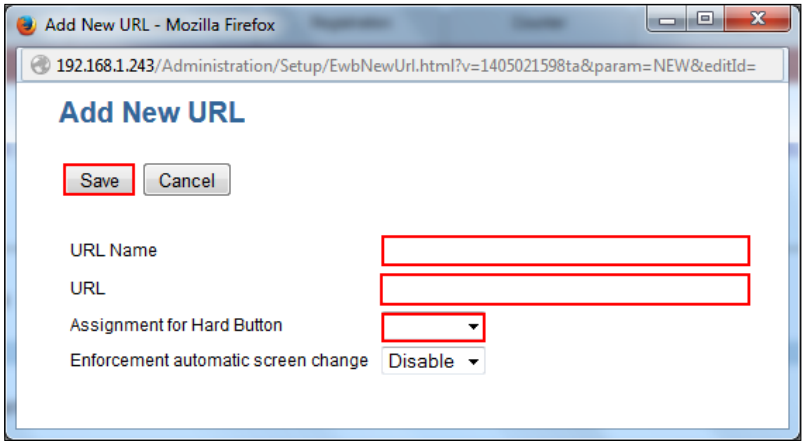


Fig. 39 - Smart Device URL Configuration

MFP LOCAL AUTHENTICATION

This section will describe how to configure the device to work with MFP local authentication.

1. Go to **TopAccess** http://[DeviceIP]/.
2. Click on **Login**.
3. Insert admin username and password (**default**: admin/123456).

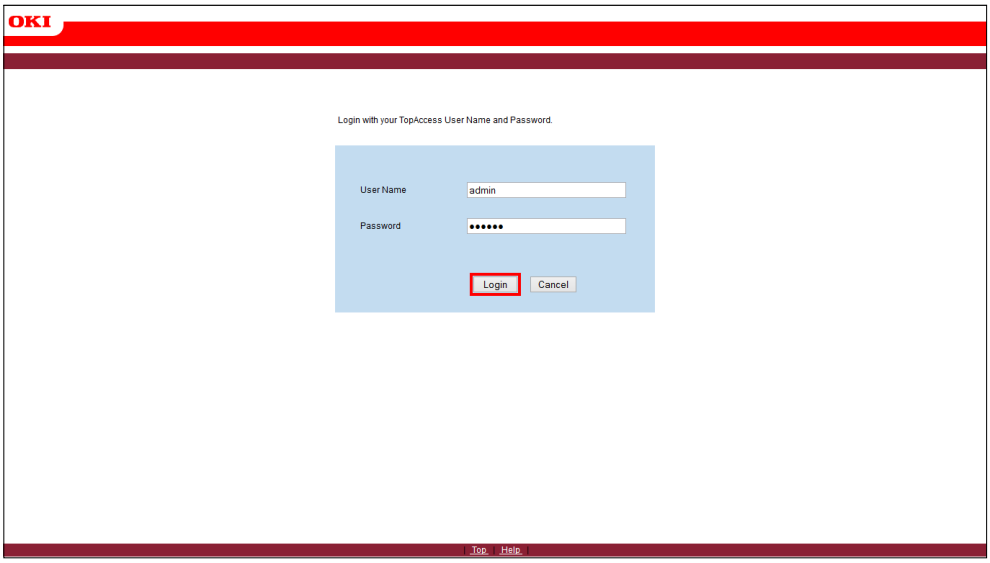


Fig. 40 - Smart Device Login

Configure Device Authentication

1. Click in **Administration> Security**.
2. Enable **User Authentication**.
3. Enable **Guest User**.
4. Set Authentication type to **MFP Local Authentication**.
5. To enable pin set **Pin Code Authentication** to enable.
6. Enable **Auto Change Login User**.
7. Enable **Create User Information Automatically**.
8. Enable **Guidance Screen**.
9. Click **Save**.

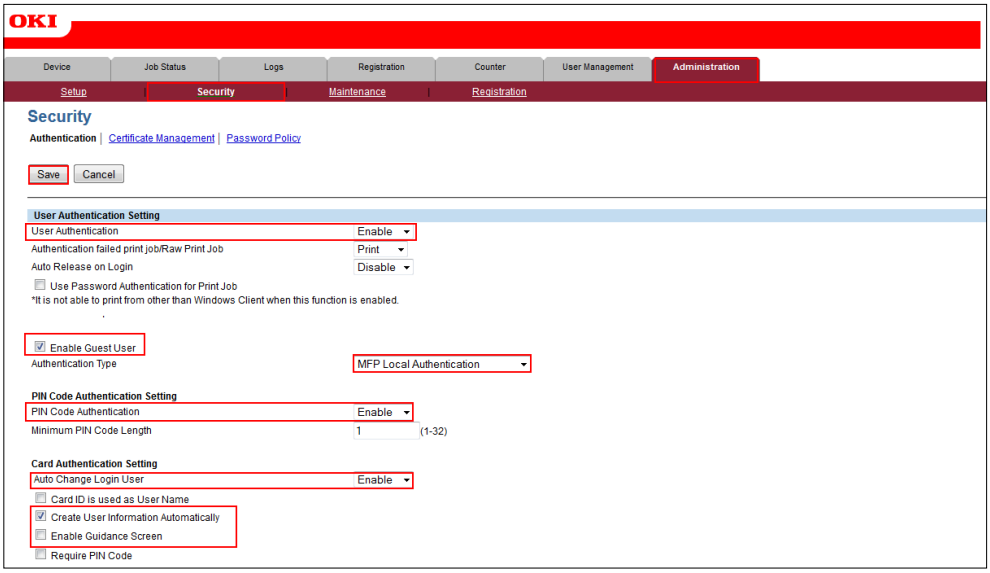


Fig. 41 - Smart Device Configuration

Note: You must create all users on the device. **SENDYS Explorer will automatically create the users within the application when each user first logs-into the device**. Their initial SENDYS Explorer **password** is the same as the **username** that is displayed on the device.

To create new users, go to **User Management > User Accounts > New**

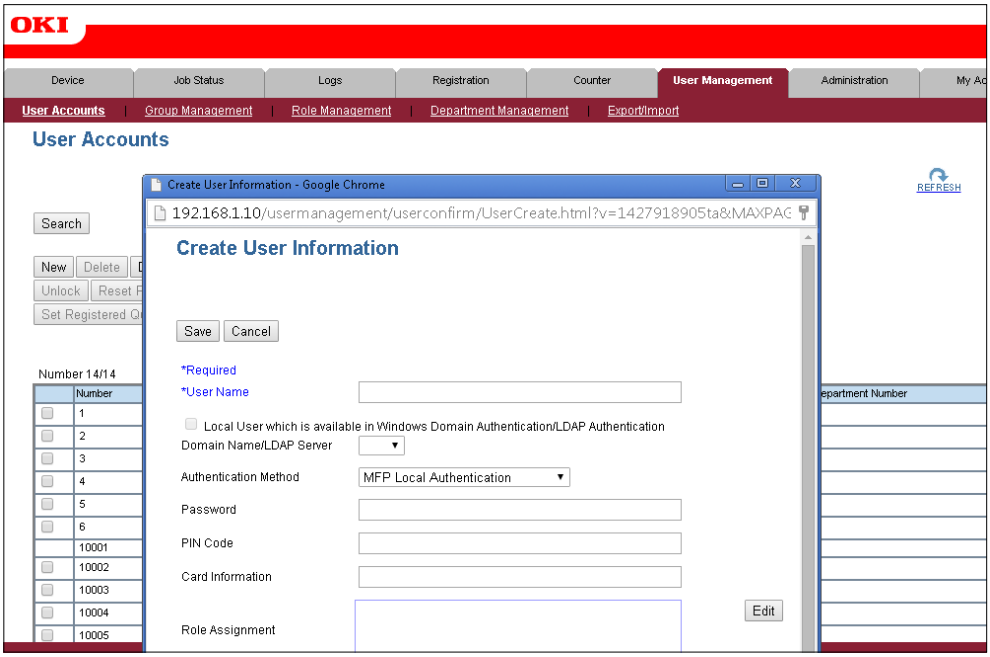


Fig. 42 - Smart Device User Creation

DIRECTORY SERVICE AUTHENTICATION - CONFIGURATION

This section will describe how to configure the device to work with your directory service for authentication.

1. Go to **TopAccess** http://[DeviceIP]/.
2. Insert admin username and password (**default**: admin/123456).
3. Click on **Login**.

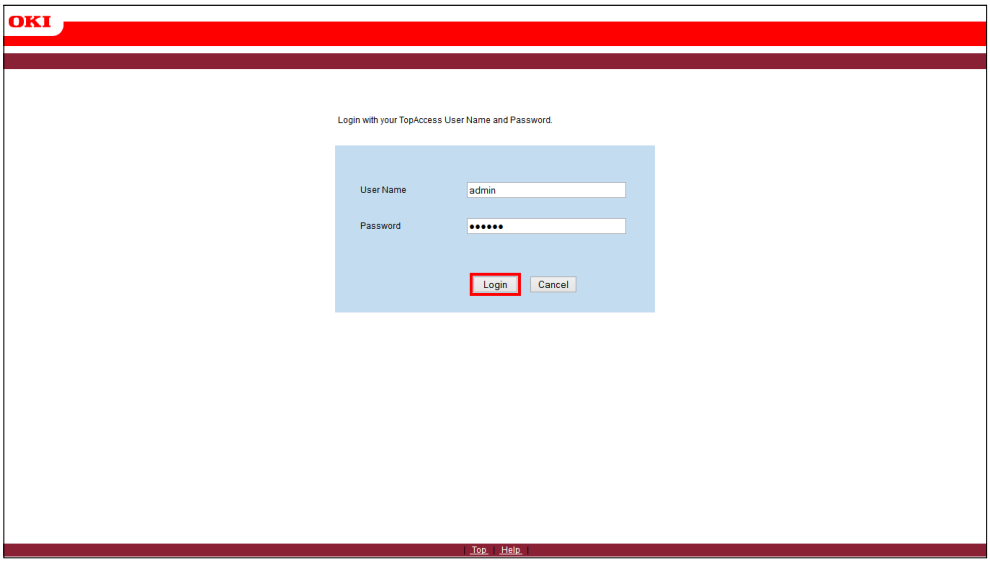


Fig. 43 - Smart Device Login

Configure Device DNS settings:

1. Click in **Administration>Setup> Network**.
2. Click on **DNS Session**.
3. Click on the **DNS Session** button.
4. Enable **DNS**.
5. Configure the primary **DNS Server Address**.
6. Click **OK**.
7. Click **Save**.

Configuring Device authentication:

1. Click on **Administration> Maintenance > Directory Service**.
2. Click on **New**.

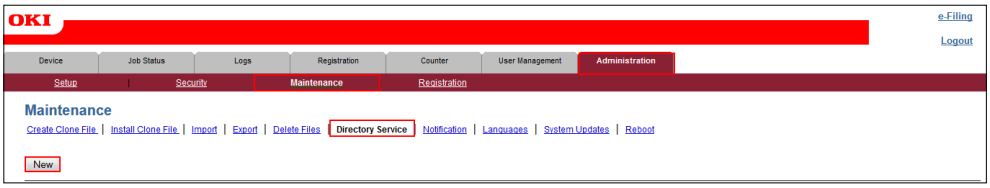


Fig. 44 - Directory Service Configuration

Fig. 45 - Directory Service Properties

Name	Details
Directory Service Name	Directory service name. Example: *company.com note this is only a name to identify the directory service on top access.*
Server IP Address	Directory Service IP address or Hostname.
Port Number	Default Directory Service port is 389. You should only change this if your LDAP server has been configured to use a different port.
Search Base	Directory Service or LDAP search base. E.g. CN=Users,DC=company,DC=com
Username	User from AD or LDAP that has access to read all the AD or LDAP groups that you need to synchronize.
Password	Password of that user.

Table 4 - Server Details

3. Make the Directory Service configurations and click on **OK**.

Test Directory Service Configurations

1. Go to **Registration>Address Book**.
2. Click on **Search**.
3. Select the **Directory Service** that you which to test.
4. Enter search criteria in one of the fields for a user that you know exists and has either fax or email contact.
5. Click **Search**.

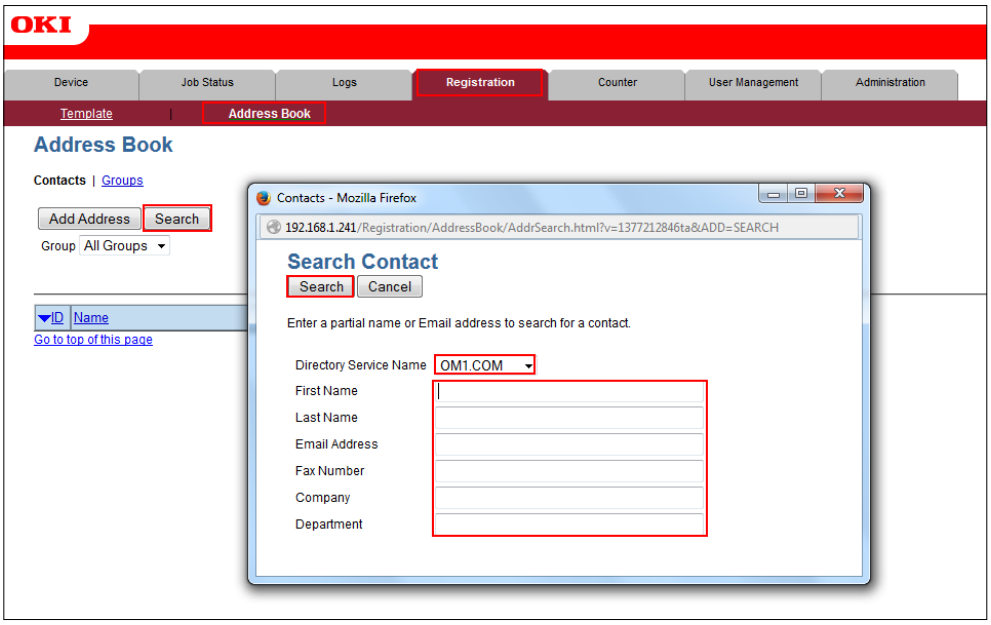


Fig. 46 - Contacts Search

Note: If the user is displayed then the connection between the device and the directory service is working properly.

Configuring Device Authentication:

1. Click in **Administration>Security**.
2. Enable **User Authentication**.
3. Enable **Guest User**.
4. Set **Authentication Type** to **LDAP Authentication**.
5. Click on **LDAP Server1**.
6. Select your **LDAP Server**.
7. Click **OK**.
8. Click **Save**.

Note: If you see the message "Please enter a valid value. (Mail Domain Name)", change the **From Address** to "**From Address' of Email Setting**" and click **Save** again.

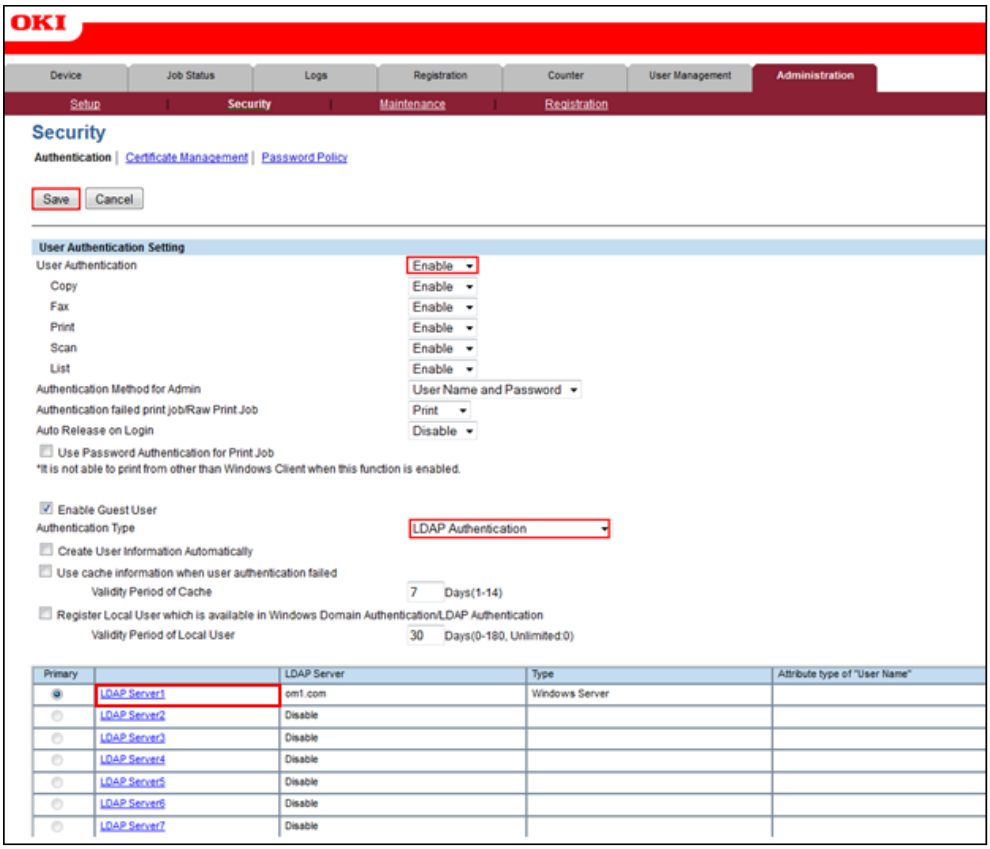


Fig. 47 - Smart Device User Authentication

If you wish to work with PIN in Directory Service then:

Note: SENDYS Explorer will not make any configurations of PINs in Directory Service, so if you are working with Directory Service PIN you need to configure the device PINs manually in your Directory Service.

1. Click in **Administration> Security**.
2. Go to **PIN Code Authentication Settings**.
3. Click **Enable**.
4. Set the **Minimum Pin Code Length**.
5. Click on **LDAP Server1**.
6. Select **LDAP Server (Other than Windows Server)**.

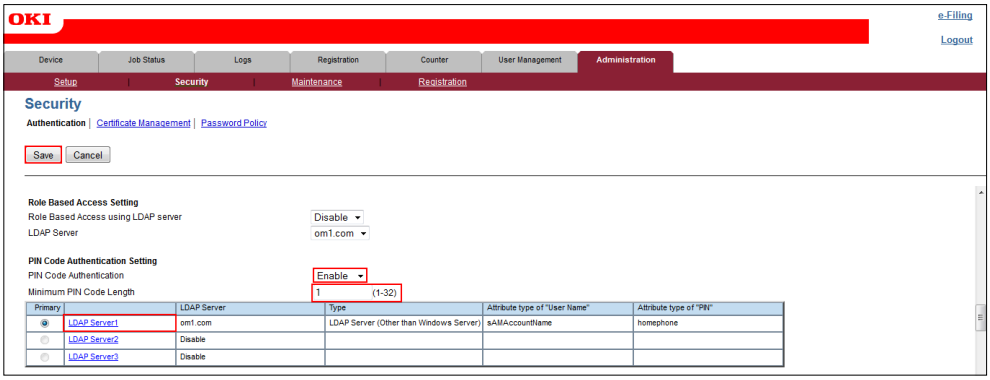


Fig. 48 - Smart Device PIN Configuration

7. Select the **LDAP Server** that you have set up.
8. Insert the field that you have mapped as **Username** in SENDYS Explorer (the default is **sAMAccountName** and it is **case sensitive**).
9. Insert the field that you have configured in **SENDYS Explorer** for **PIN** (the default is **homePhone**).
10. Click **OK**.

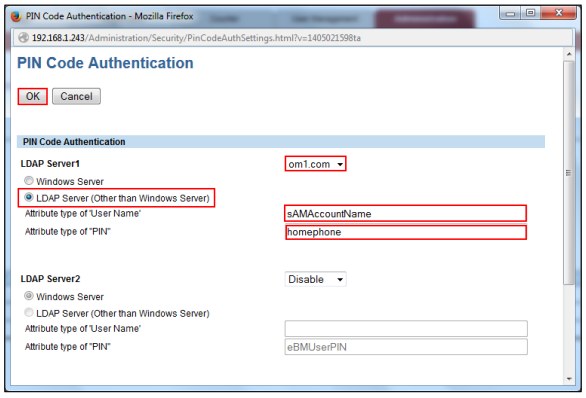


Fig. 49 - PIN Code Authentication

11. Click **Save**.

If you wish to work with Card Authentication in Directory Service, then:

Note: SENDYS Explorer will not setup any card ids in **Directory Service**, so if you are working with Directory Service Cards you need to configure the device cards manually in **Directory Service**.

1. Click in **Administration> Security**.
2. Go to **Card Authentication Settings**.
3. Enable **Auto Change Login User**.
4. Click on **LDAP Server1**.

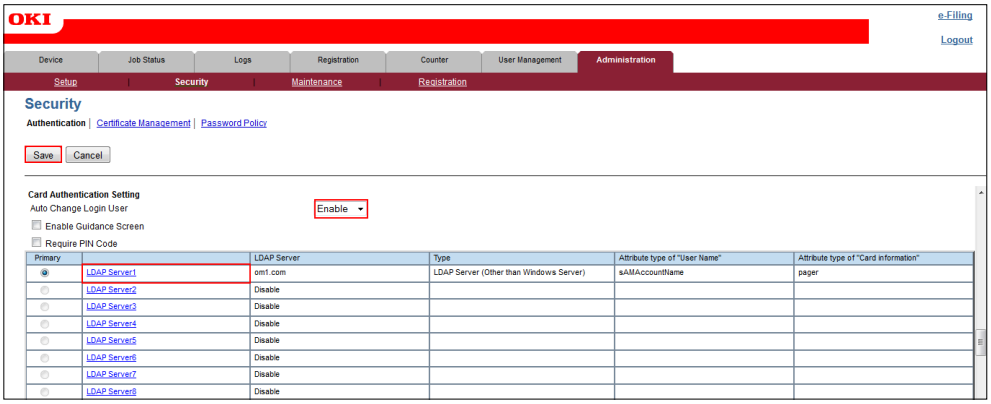


Fig. 50 - Smart Device Card Authentication

5. Select **LDAP Server (Other than Windows Server)**.
6. Select the LDAP server that you have configured.
7. Insert the field that you have mapped as Username in **SENDYS Explorer** (the default is **sAMAccountName** and it is **case sensitive**).
8. And insert the field from **Directory Service** where you had set up the **Card Id**.
9. Click **OK**.

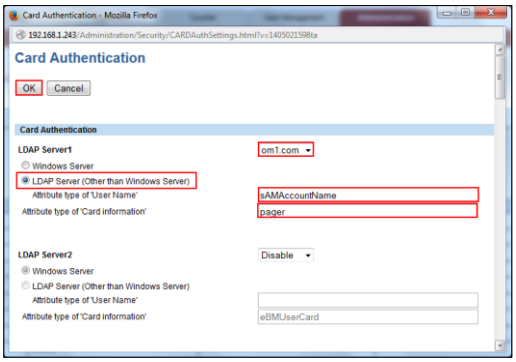


Fig. 51 - Card Authentication

10. Click **Save**.

SMART DEVICE CONFIGURATION (SXP VERSION 2.0 (MC8X3/ES84X3 MC573/ES5473 SERIES))

SCAN SETUP

We have to configure the device to allow SENDYS Explorer to initiate the scanning process.

1. Go to the device webpage **http://[DeviceIP]**
2. Click on [Administrator Login]
3. Insert admin username and password default credentials (**admin**/**aaaaaa**), in MC573/ ES5473 (**admin**/**999999**)
4. If the following screen is appeared, please click [**SKIP**]

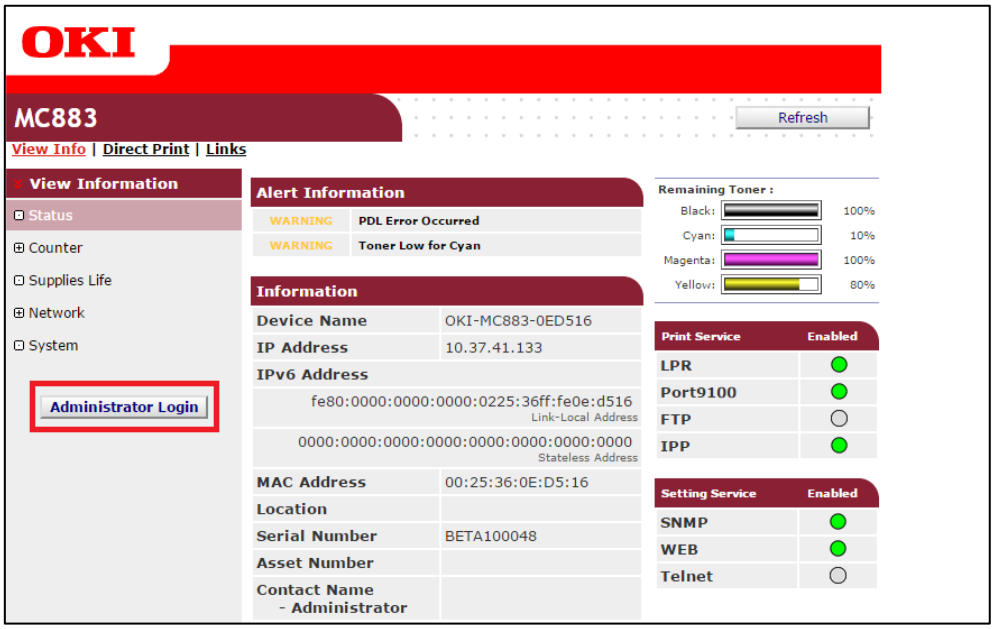


Fig. 52 - Smart Device Login

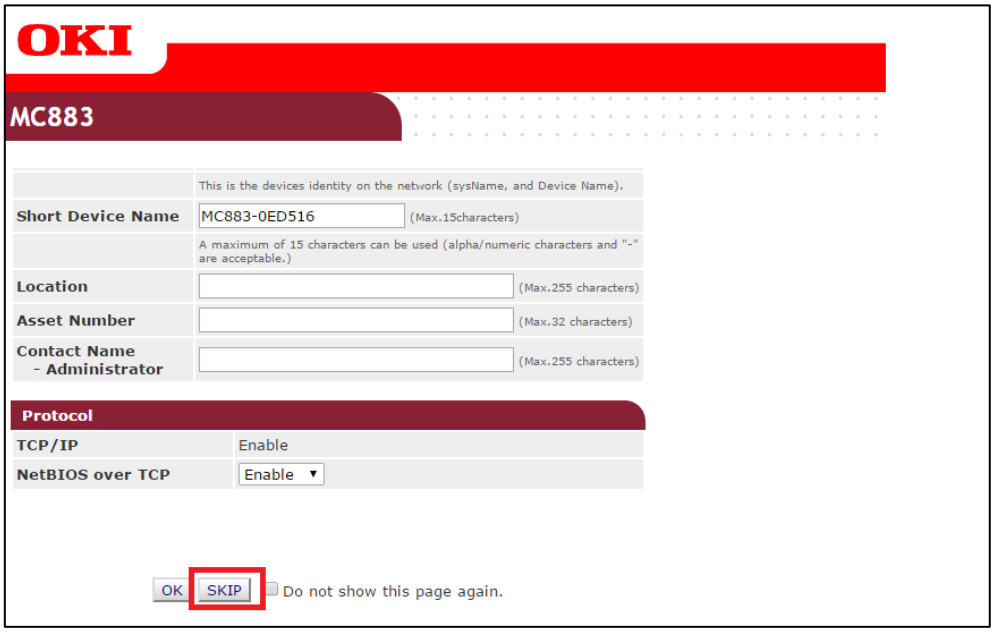


Fig. 53 - Smart Device Login

5. Click in **Admin Setup >Scanner Setup>WSD Scan Setup**
6. Enable **WSD Scan**
7. Click **Submit**

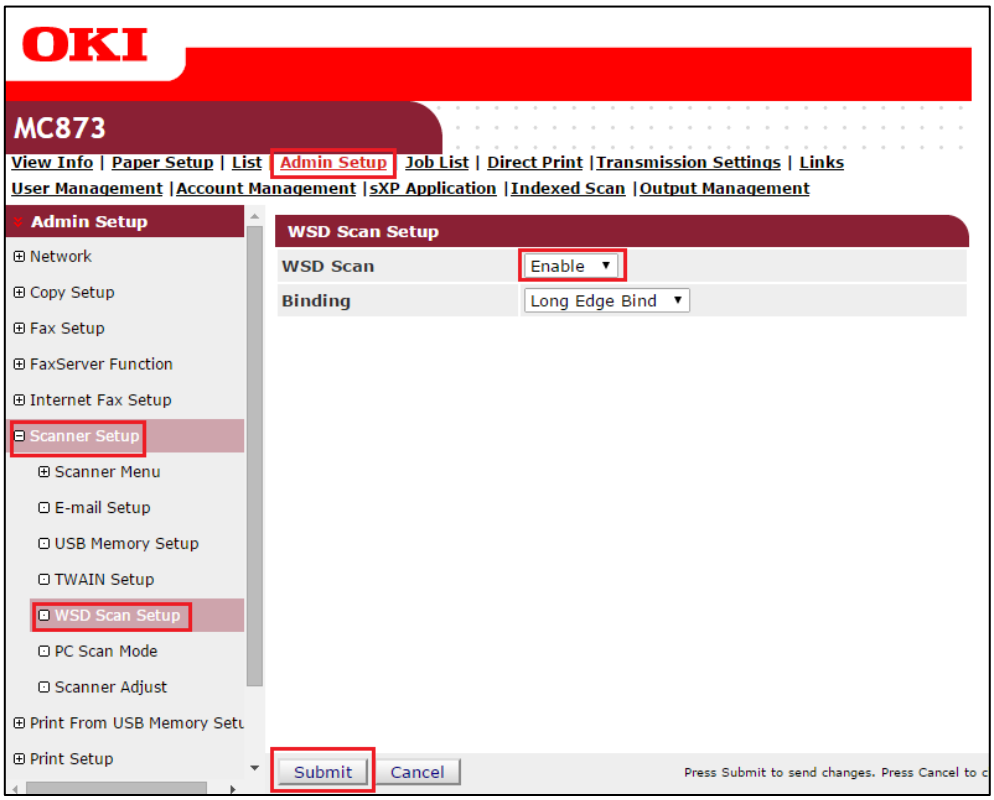


Fig. 54 - Scan Setup

SCREEN APPLICATION CONFIGURATION

In order to see the application on the device screen you need to configure the sXP application on the smart device.

The application address is **http://[ServerIP]:50091/scan.aspx**.

1. Go to the device webpage **http://[DeviceIP]**
2. Click on [Administrator Login]
3. Insert admin username and password default credentials (**admin**/**aaaaaa**), in MC573/ ES5473 (**admin**/**999999**)
4. If the following screen is appeared, please click [**SKIP**]

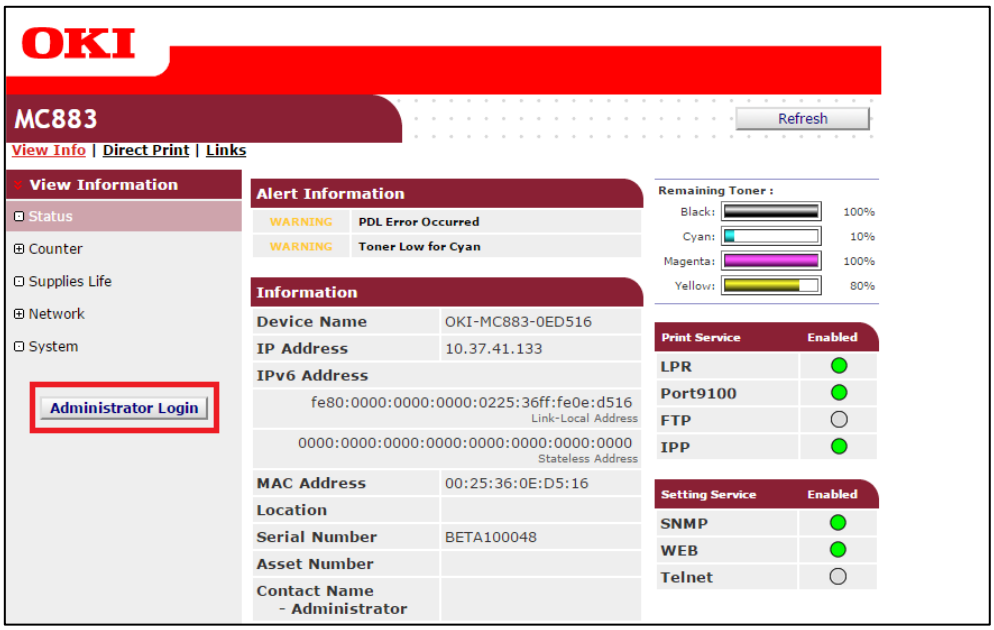


Fig. 55 - Smart Device Login

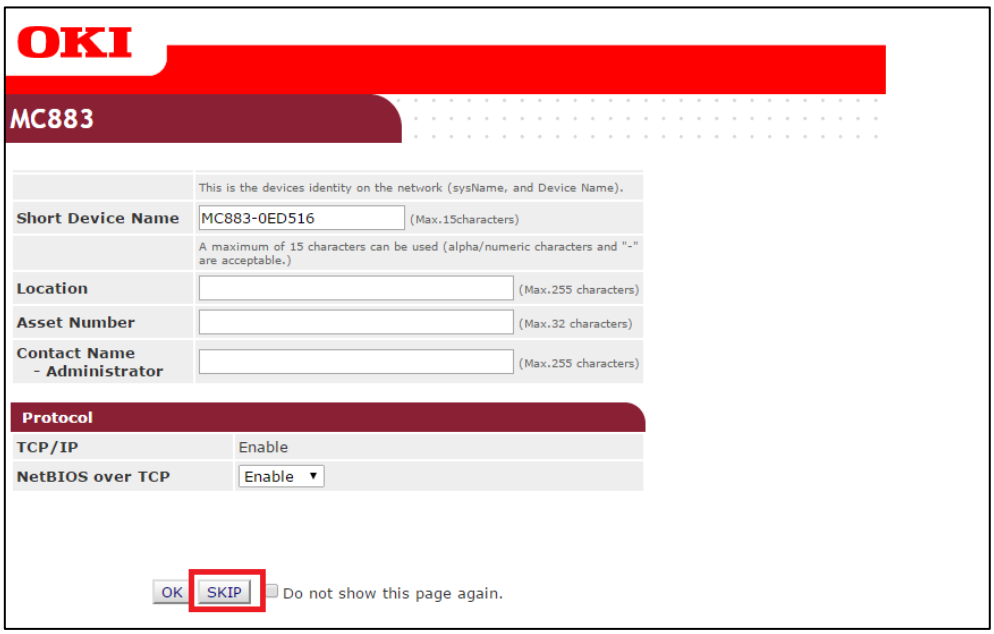


Fig. 56 - Smart Device Login

To configure SENDYS Explorer as default machine screen:

5. Click on **sXP Application**.
6. Click on [**+**].

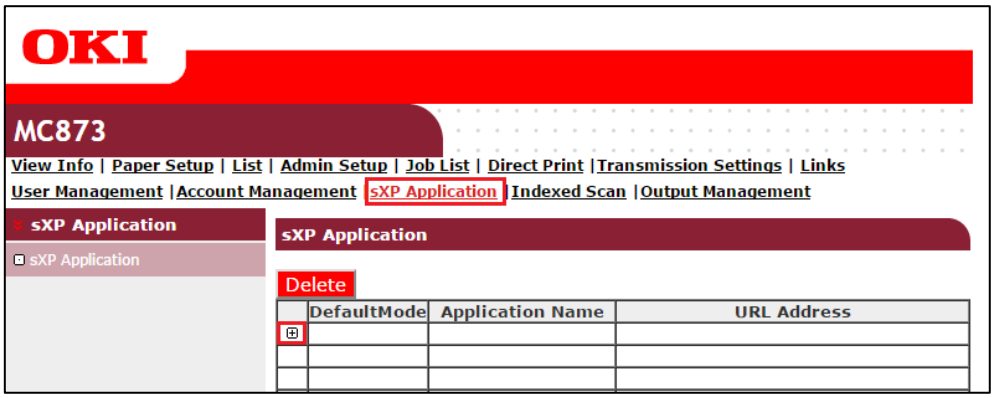


Fig. 57 - Screen Application Configuration

7. In the new window:
   a. Define the **Application Name**.
   b. Set **URL Address** to http://[ServerIP]:50091/scan.aspx.
8. Click **OK**.

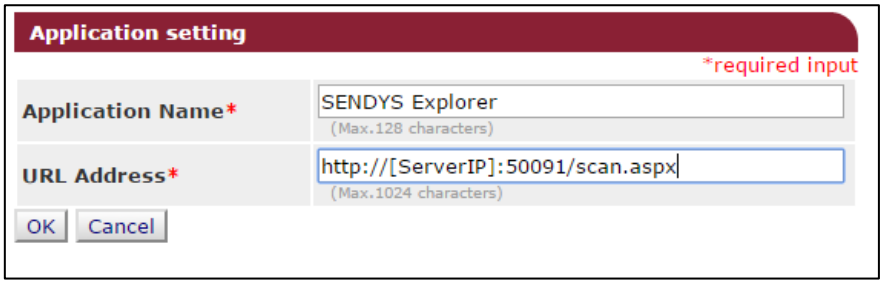


Fig. 58 - Screen Application Configuration

Note: This will add SENDYS Explorer to the device **JOB Macro**.

Then on the device you need to:

- Access as admin.
- Go to **Admin Setup > Configure Home Screen > Touch a blank space > ADD**
- Select **SENDYS Explorer** from the **JOB Macro**

9. Select **Default Mode**.
10. Click **Submit**.

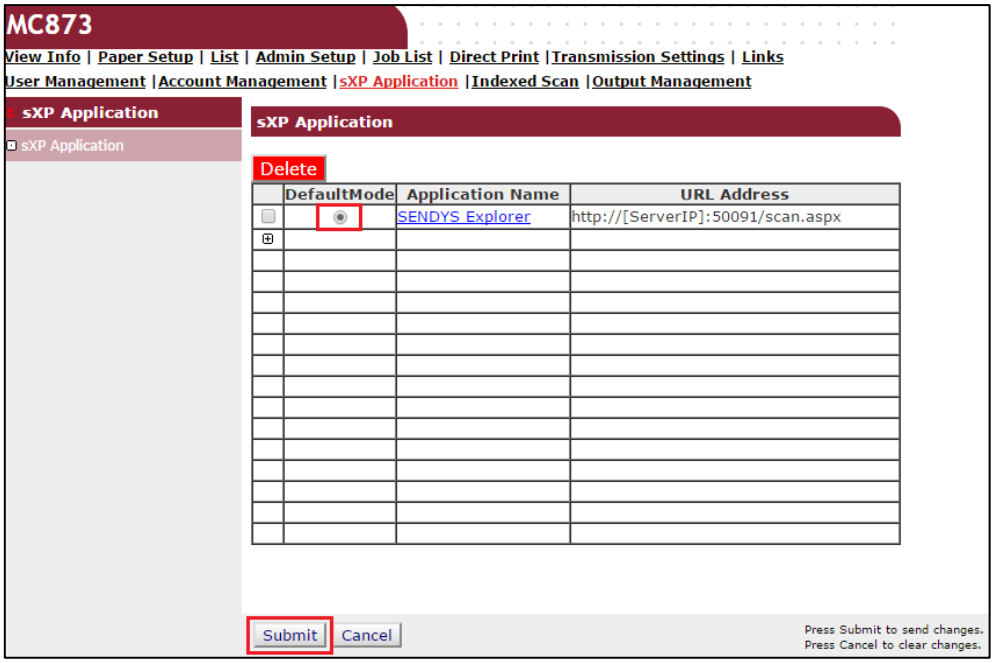


Fig. 59 - Screen Application Configuration

Note: This will only define the default screen application.

Then on the device you need to:

- Access as admin.
- Go to **Admin Setup > Manage Unit > Default Mode**
- Select **Web Browser**

FAX DELIVERY CONFIGURATION

In order to be able to work with **Fax Delivery**, you need to setting up the network ftp scan profile.

1. Go to the device webpage **http://[DeviceIP]**
2. Click on [Administrator Login]
3. Insert admin username and password default credentials (**admin**/**aaaaaa**), in MC573/ ES5473 (**admin**/**999999**)
4. If the following screen is appeared, please click [**SKIP**]

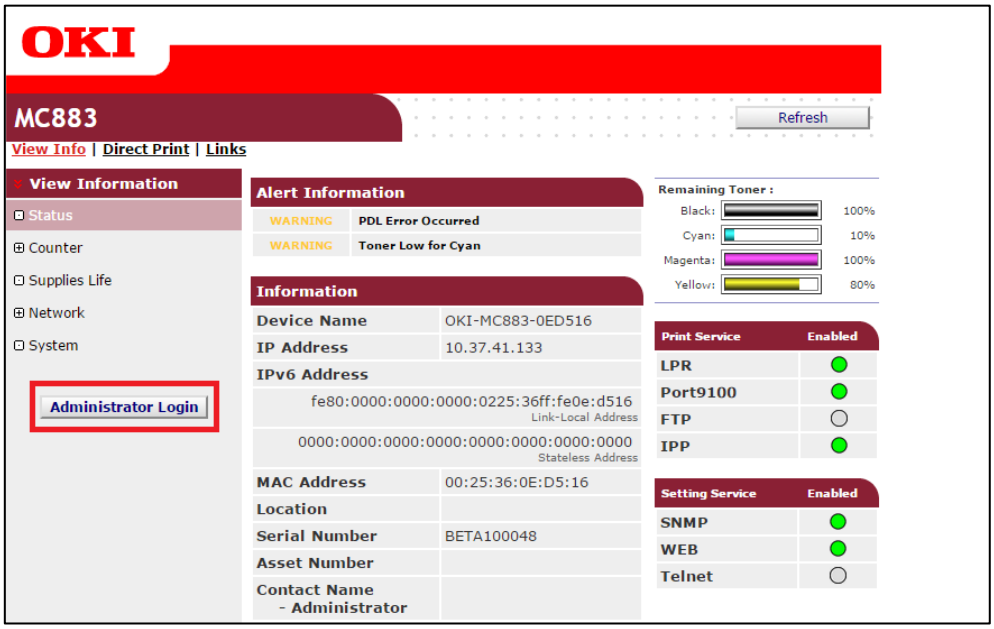


Fig. 60 - Fax Delivery Configuration

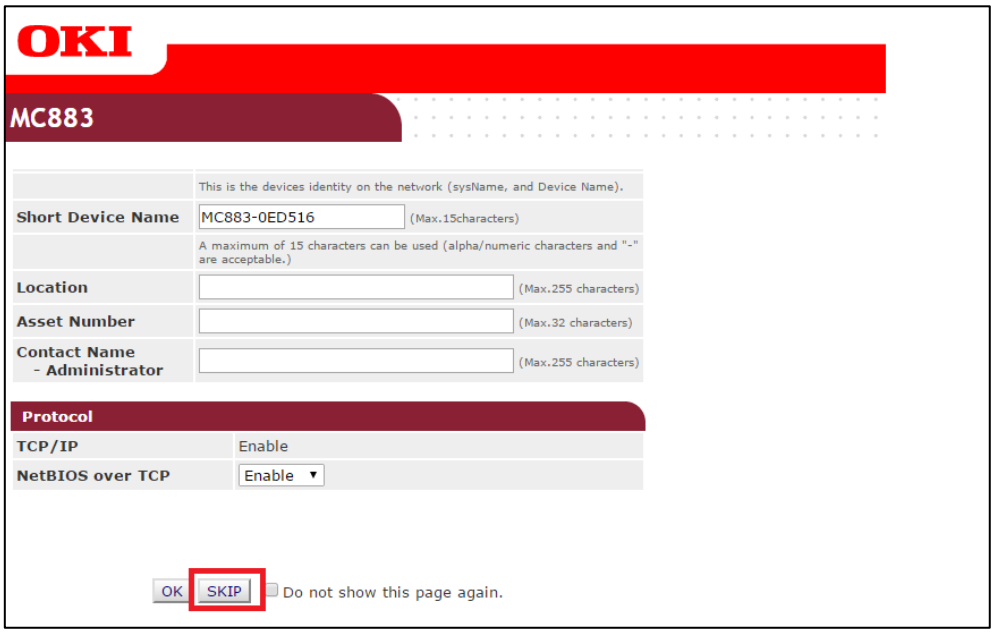


Fig. 61 - Fax Delivery Configuration

Setting up the network ftp scan profile.

1. Click on **List/Profile**.
2. Click on **New**.

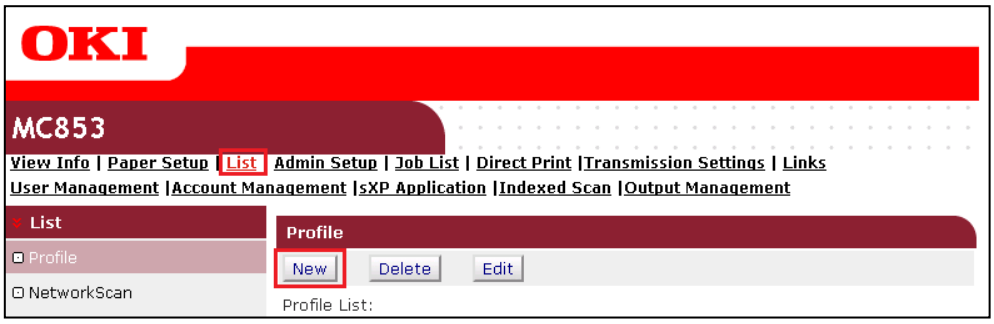


Fig. 62 - Fax Delivery Configuration

3. Refer to following table while filling the information:

Name	Details
Profile Name	Name of the profile.
Protocol	Protocol that will be used with this profile. Set to FTP.
Target URL	FTP path to *ScannedFiles/FaxReceptionFolder/[**Device Name**]* folder on the server.
Port Number	Port number for this profile. By default, 21 is the port assigned to FTP.
FTP Passive Mode	Set to OFF.
User Name	Same Administrator username that you used in the SENDYS Explorer installation.
Password	Same Administrator password that you used in the SENDYS Explorer installation.

Table 5 - Profile details.

4. Click on **Submit**

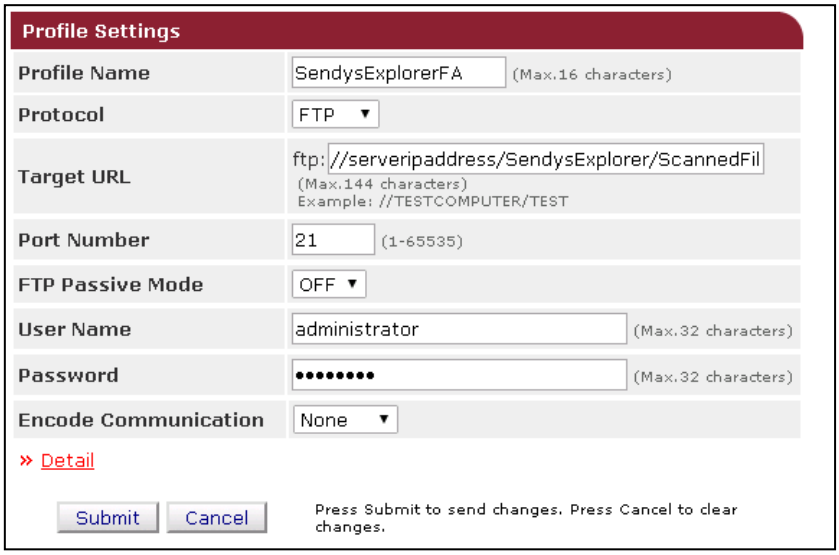


Fig. 63 - FAX Delivery Configuration

Enabling Automated Delivery Setup

1. Click on **Transmission Settings/Automated Delivery Setup**.
2. Click on **New**.

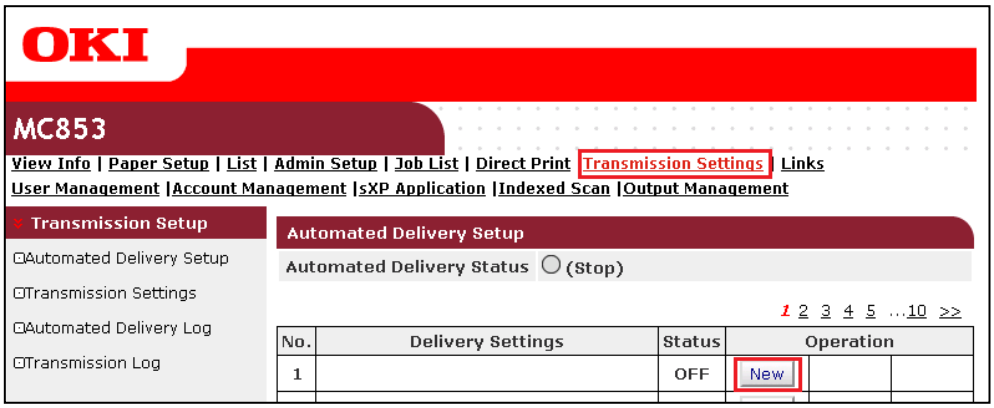


Fig. 64 - Fax Delivery Configuration

3. Refer to following table while filling the information:

Name	Details
Automated Delivery	Name of the automated delivery.
Automated Delivery	Set to ON.
Search Field	Select [**Received Fax**].
Delivered To	Click the **Edit of the Folder**, in the new view select the profile configured earlier.
Print	Set to OFF.

Table 6 - Automated Delivery details

4. Click on **Submit**

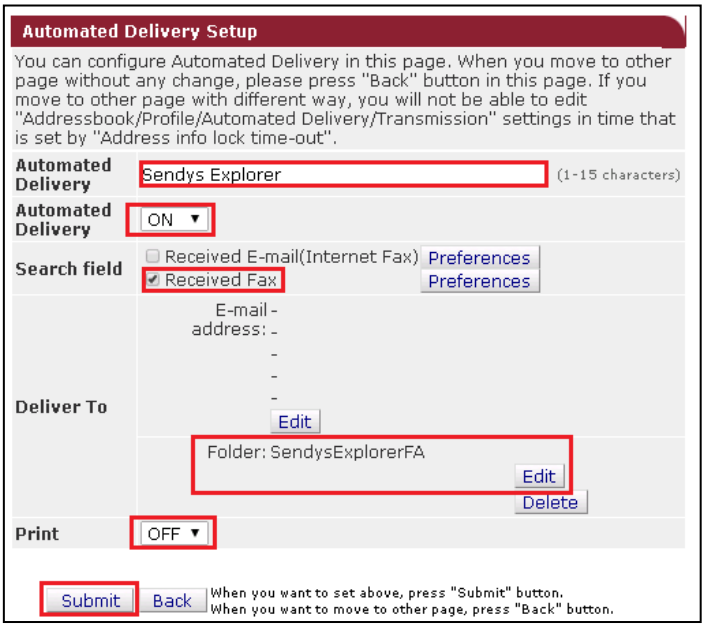


Fig. 65 **- Fax Delivery Configuration**

MFP LOCAL AUTHENTICATION

This section will describe how to configure the device to work with MFP local authentication.

1. Go to the device webpage **http://[DeviceIP]**
2. Click on [Administrator Login]
3. Insert admin username and password default credentials (**admin**/**aaaaaa**), in MC573/ ES5473 (**admin**/**999999**)
4. If the following screen is appeared, please click [**SKIP**]

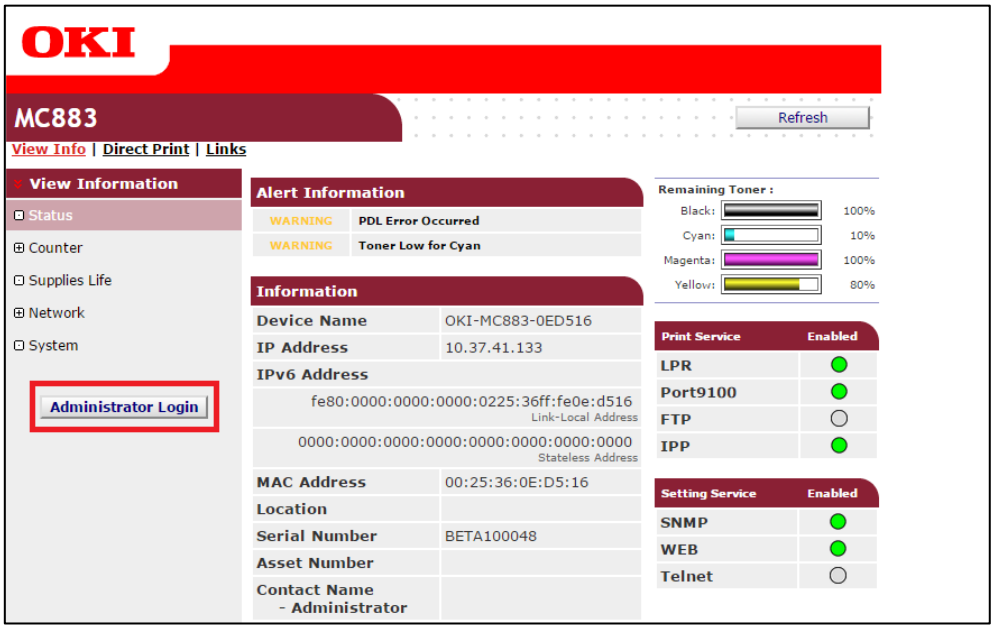


Fig. 66 - Smart Device Configuration

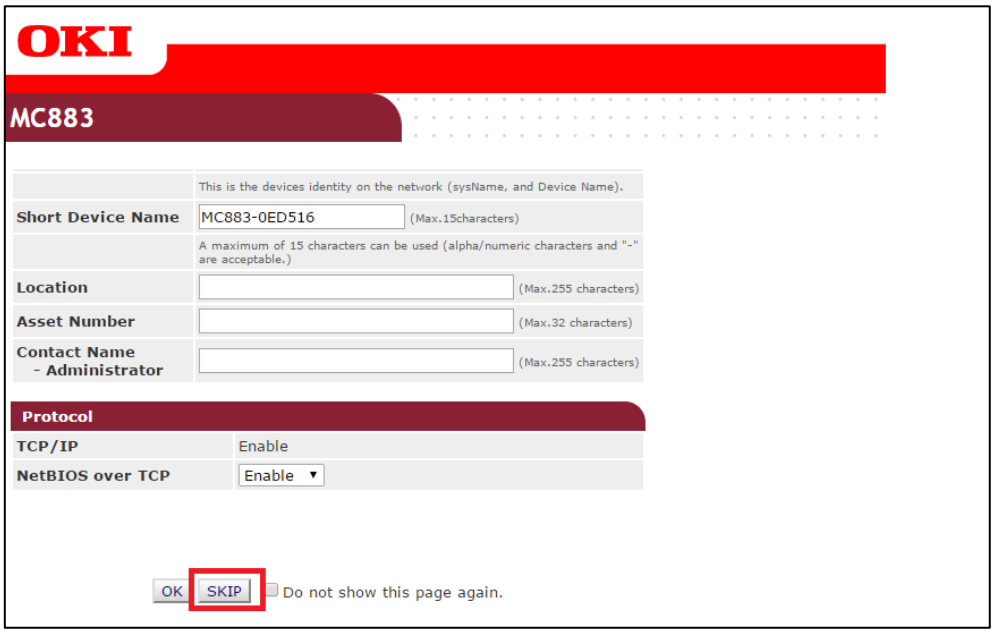


Fig. 67 - Smart Device Configuration

Configure Device Authentication

5. Click in **Admin Setup >Management>Access Control Setup**
6. Enable **Access Control**
7. Disable **Guest user use**
8. To enable **Authenticate Local Name**. (to enable **Authenticate Local PIN** and **Authenticate Local IC Card** if you need)
9. Click **Submit**

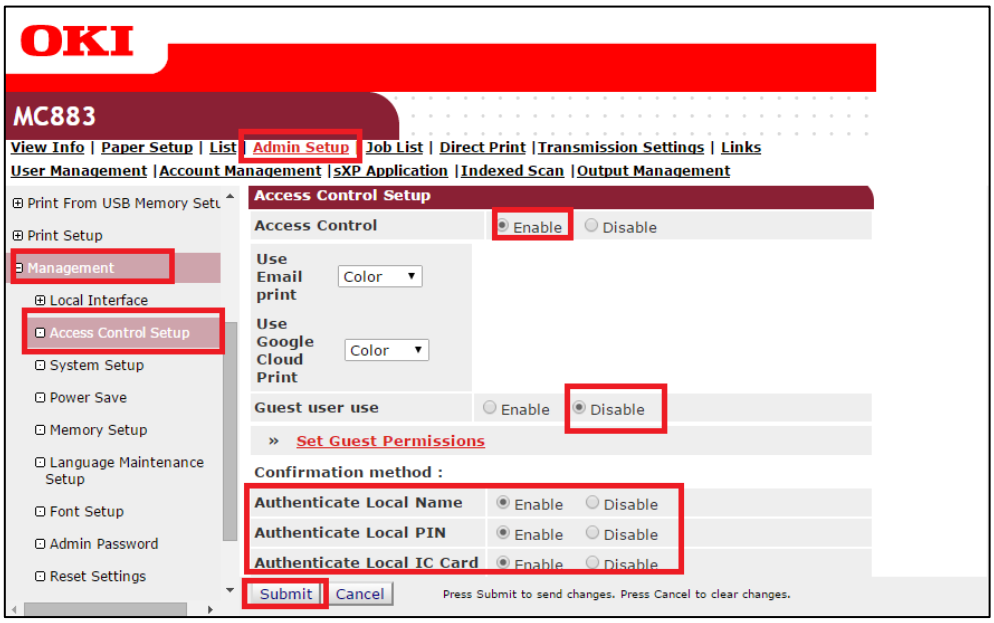


Fig. 68 - Smart Device Configuration

Note: You must create all users on the device. **SENDYS Explorer will then automatically create the users within the application when each user first logs-into the device**, their initial SENDYS Explorer web password is the same as the username that is displayed on the device.

Note: Users can select the authentication method by their selves. If you would like to restrict the authentication method, please disable **Confirmation Method (Authenticate Local Name, Authenticate Local PIN, Authenticate Local IC Card)** if you need.

Note: If you can allow users to associate their card ID with their account, enable **Register general user's IC card**.

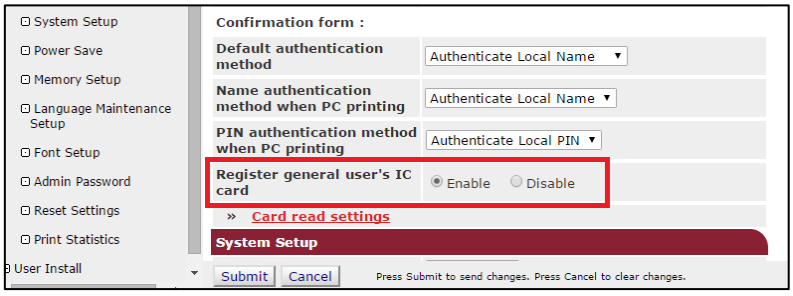


Fig. 69 - Smart Device Configuration

To create users go to **User Management > User List>Local User >[+]**

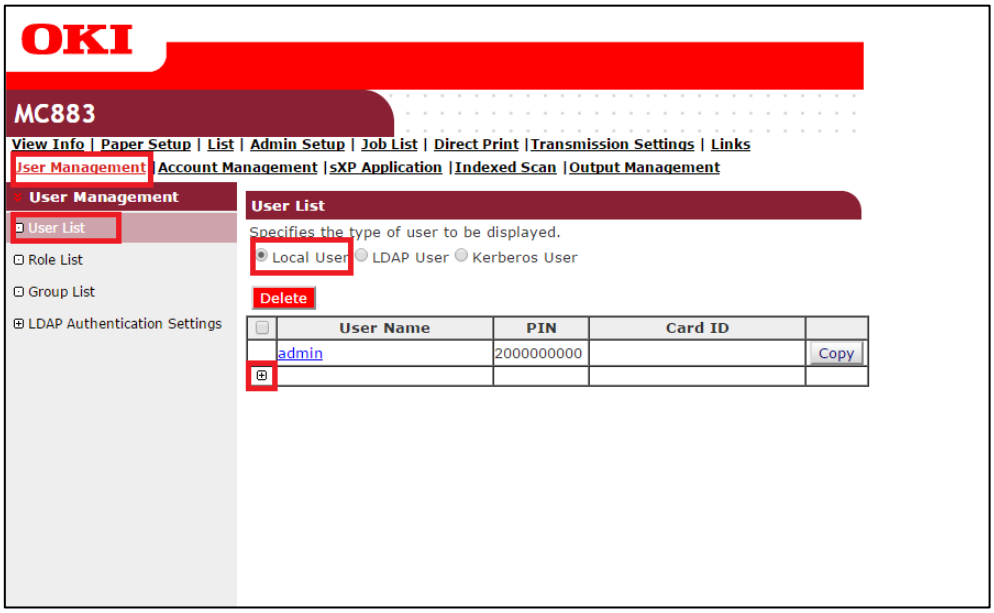


Fig. 70 - Smart Device Configuration

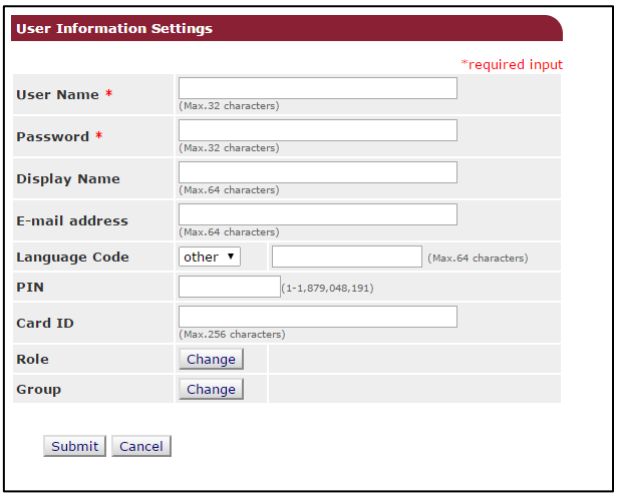


Fig. 71 - Smart Device Configuration

Note: You must enter **PIN** if you use **Authenticate Local PIN**.

Note: You must enter **Card ID** if you use Authenticate Local IC Card and disable **Register general user's IC card in Access Control Setup**. MC8x3/ES84x3 supports Elatec TWN4 card reader with keyboard interface for authentication by IC Card.

DIRECTORY SERVICE AUTHENTICATION

This section will describe how to configure the device to work with your directory service for authentication.

1. Go to the device webpage **http://[DeviceIP]**
2. Click on [Administrator Login]
3. Insert admin username and password default credentials (**admin**/**aaaaaa**), in MC573/ ES5473 (**admin**/**999999**)
4. If the following screen is appeared, please click [**SKIP**]

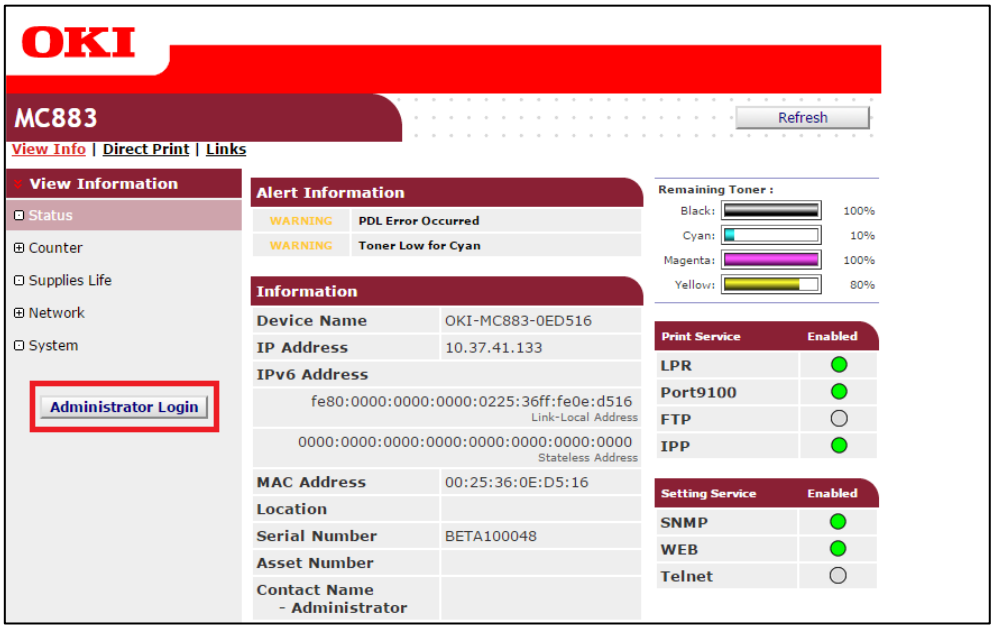


Fig. 72 - Smart Device Configuration

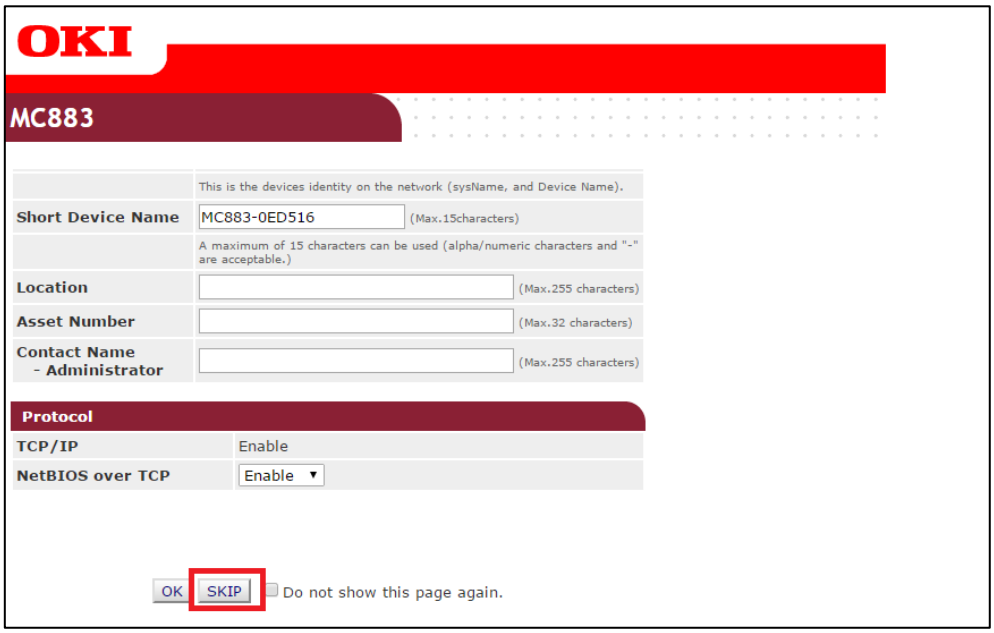


Fig. 73 - Smart Device Configuration

Configure Device DNS settings:

Note: If Device DHCP server information is retrieved from DHCP server correctly, you don't have to configure Device DNS setting manually.

1. Click in **Admin Setup > Network>TCP/IP**
2. Click on **(OPTIONAL) Change other TCP/IP settings**.
3. Configure the **primary DNS Server Address**
4. Click **OK**
5. Click **Submit**

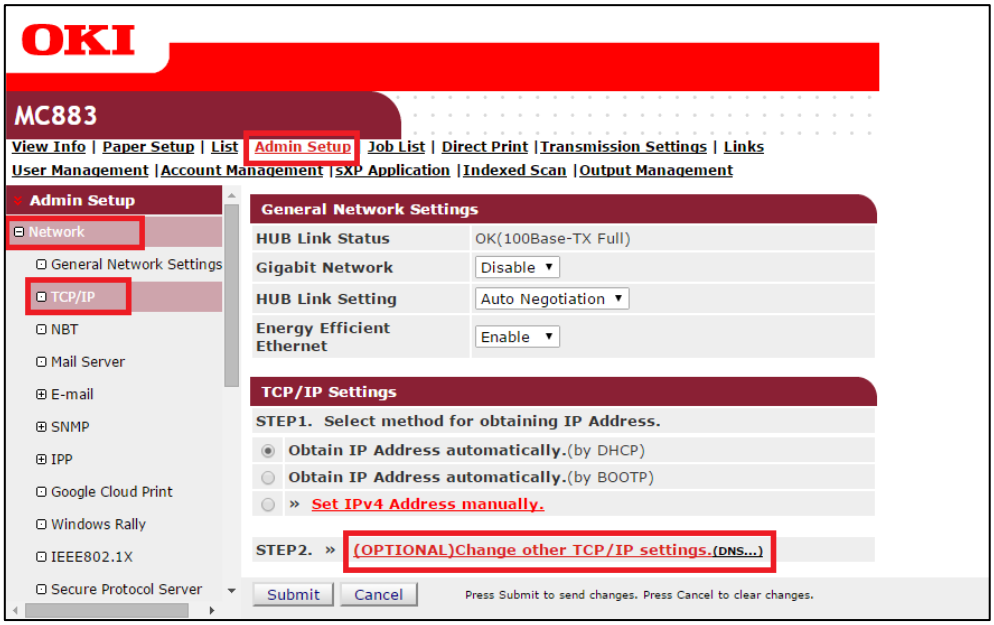


Fig. 74 - Smart Device Configuration

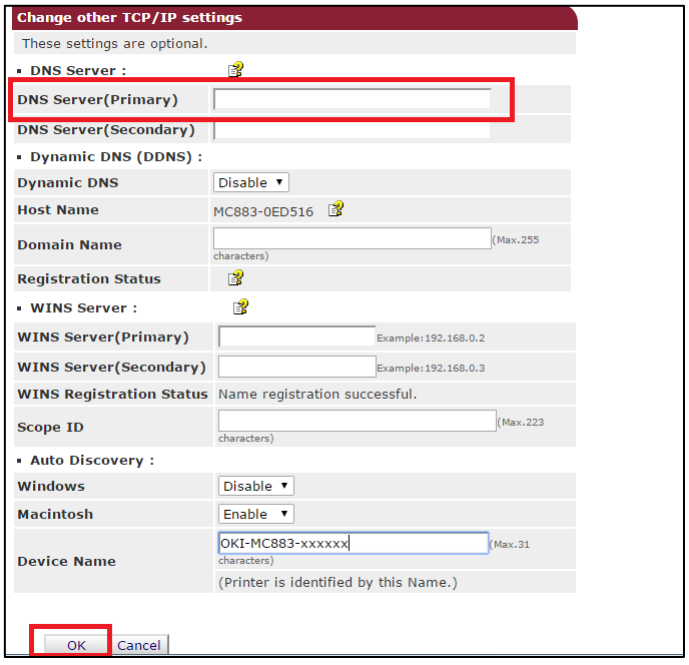


Fig. 75 - Smart Device Configuration

Configure Device SNTP settings:

Note: If Device SNTP server information is retrieved from DHCP server correctly, you don't have to configure Device DNS setting manually.

Note: If you set correct date and time manually, you don't have to configure Device SNTP server setting.

1. Click in **Admin Setup >User Install > Time Setup**
2. Set "**Auto**" in **Time Setup**
3. Configure the **SNTP Server (Primary) Address**
4. Click **Submit**

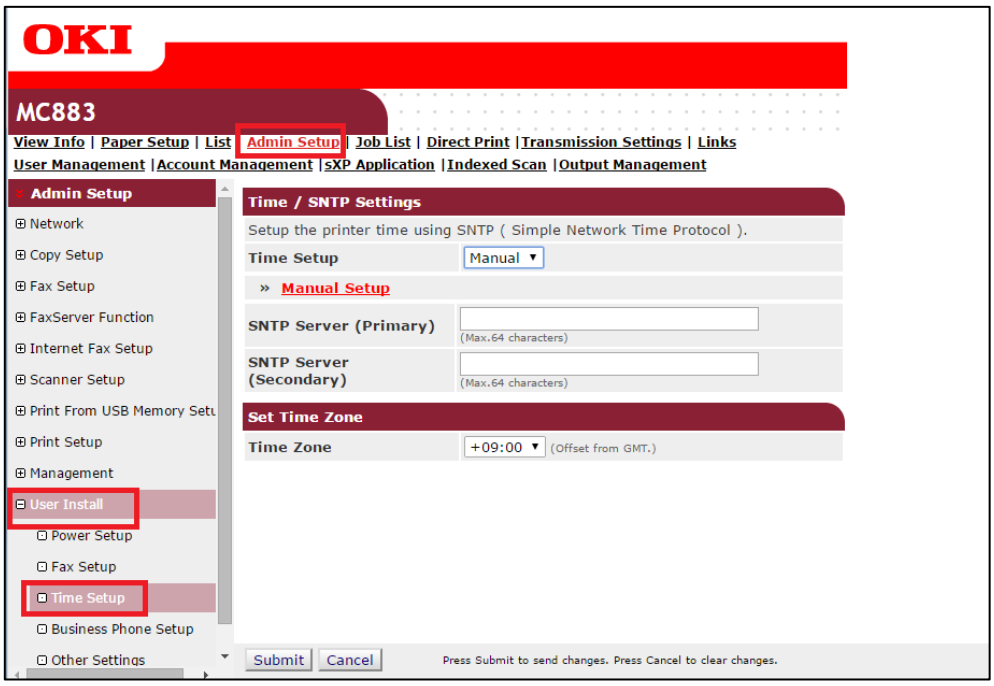


Fig. 76 - Smart Device Configuration

Configure Device authentication:

1. Click in **Admin Setup > Network >LDAP**

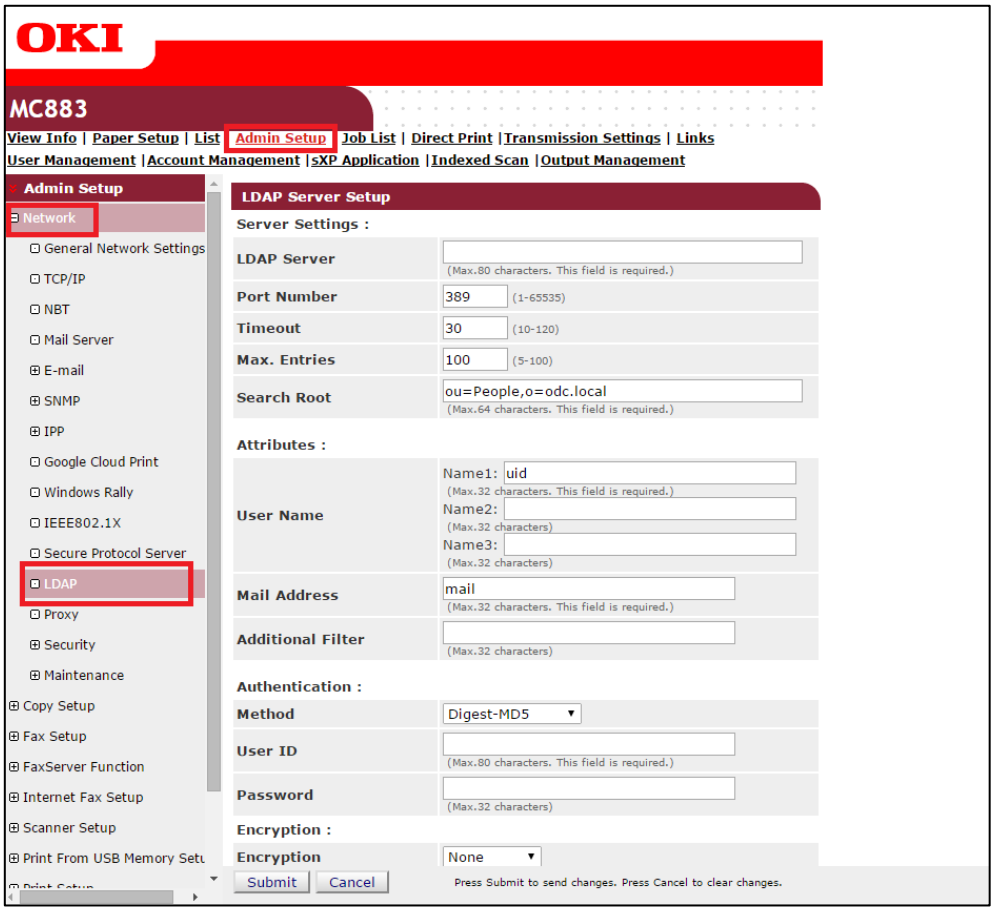


Fig. 77 - Smart Device Configuration

Name	Details
LDAP Server	Directory Service IP address or HostName. If you select Secure Protocol in Method, you have to set a host name or IP address which can be reversely resolve a host name from the DNS server.
Port Number	Default Directory Service port is 389. You should only change this if your LDAP server has been configured to use a different port.
Timeout	Timeout to get information from LDAP server after login the device. The setting is used when you set Authenticate LDAP PIN or Authenticate LDAP IC Card.
Max. Entries	Specify the maximum number of search results that are a response by e-mail address search. The setting is not used for LDAP authentication.
Search Root	LDAP search base. Ex : CN=Users,DC=company,DC=com The setting is not used for LDAP authentication.
User Name	Insert the field that you have mapped for the username. The setting is not used for LDAP authentication.
Mail Address	Insert the field that you have mapped for the email address. The setting is not used for LDAP authentication.
Additional Filter	This filter is to find email address from LDAP server. The setting is not used for LDAP authentication.
Method	Select [Digest-MD5] or [Secure Protocol] based on your LDAP server environment. Note: [Anonymous] and [Simple] doesn't work for the access control. Note: [Secure Protocol] requires DNS configuration and SNTP configuration in order to synchronize the device time with the Secure Protocol server's time.
Username	User from AD or LDAP that has access to read all the AD or LDAP groups that you need to synchronize. The setting is used when a user authenticates by Authenticate LDAP PIN or Authenticate LDAP IC Card
Password	Password of that user.
Encryption	Encryption type.

Table 7 - Server Details

2. Make the LDAP configurations and click on **Submit**

Configure Secure Protocol Server setting

Note: If you select **Secure Protocol Server** as **Method** in **LDAP Server Setup**, you must configure Secure Protocol Server.

1. Click in **Admin Setup > Network >Secure Protocol Server**
2. Configure Secure Protocol Server name in **Domain**.

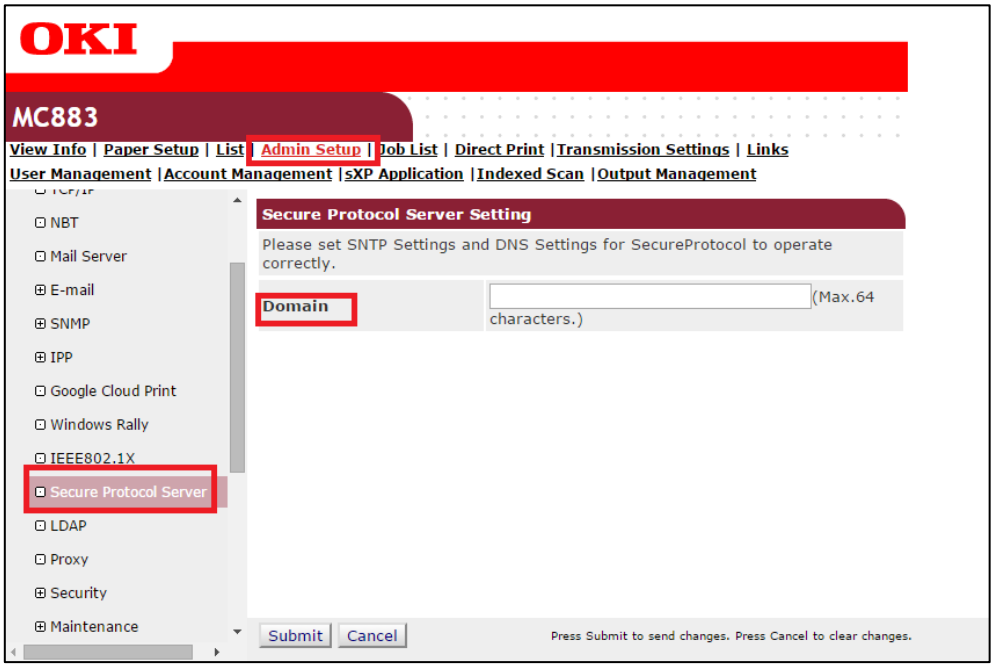


Fig. 78 - Smart Device Configuration

Note: The Secure Protocol Server name must be entered in capital letter.

Configure Device Authentication:

1. Click in **Admin Setup >Management>Access Control Setup**
2. Enable **Access Control**
3. Disable **Guest user use**
4. To enable **Authenticate LDAP Name**. (to enable **Authenticate LDAP PIN** and **Authenticate LDAP IC Card** if you need)
5. Click **Submit**

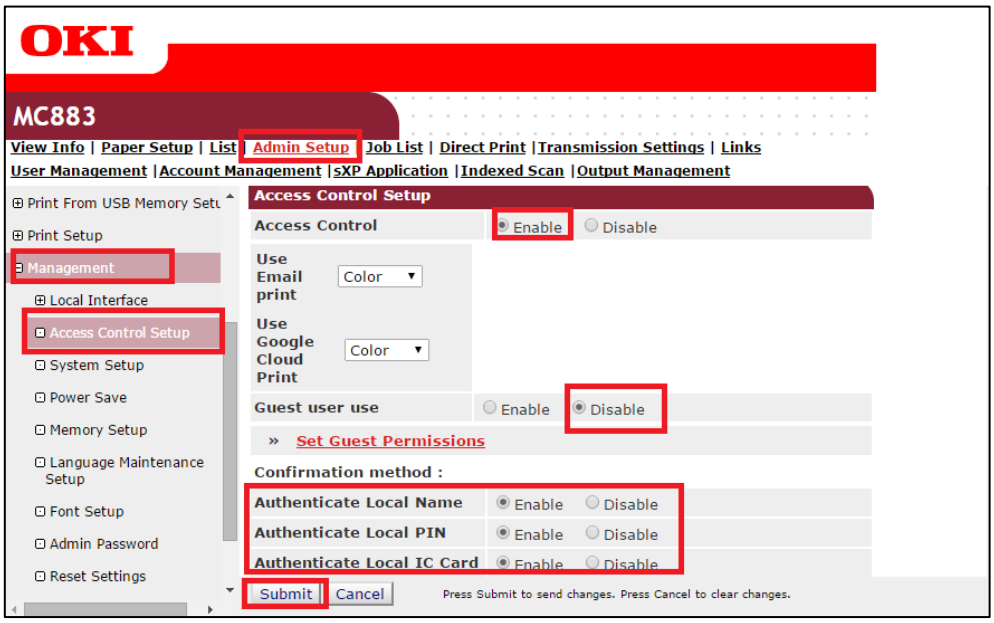


Fig. 79 - Smart Device Configuration

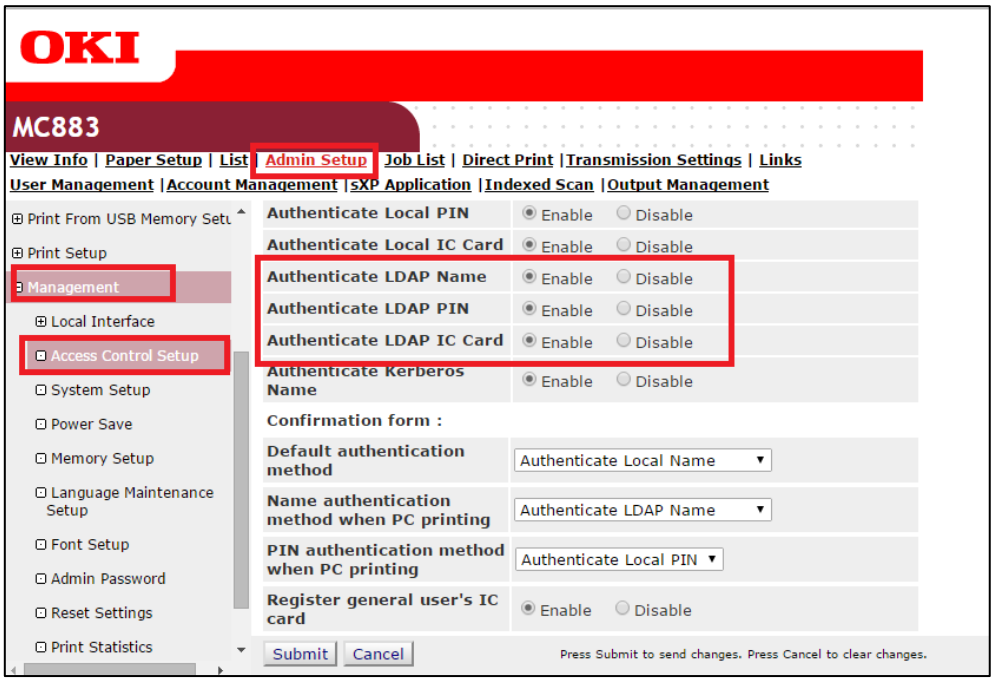


Fig. 80 - Smart Device Configuration

If you wish to work with **PIN** in **Directory Service**, please follow this procedure:

Note: SENDYS Explorer will not make any configurations of PINs in Directory Service, so if you are working with Directory Service PIN you need to configure the device PINs manual in your Directory Service.

1. Click in **User Management > User List > LDAP Authentication Settings > LDAP Authentication Settings**
2. Insert the field that you have map as PIN to **PIN**
3. Click **Submit**

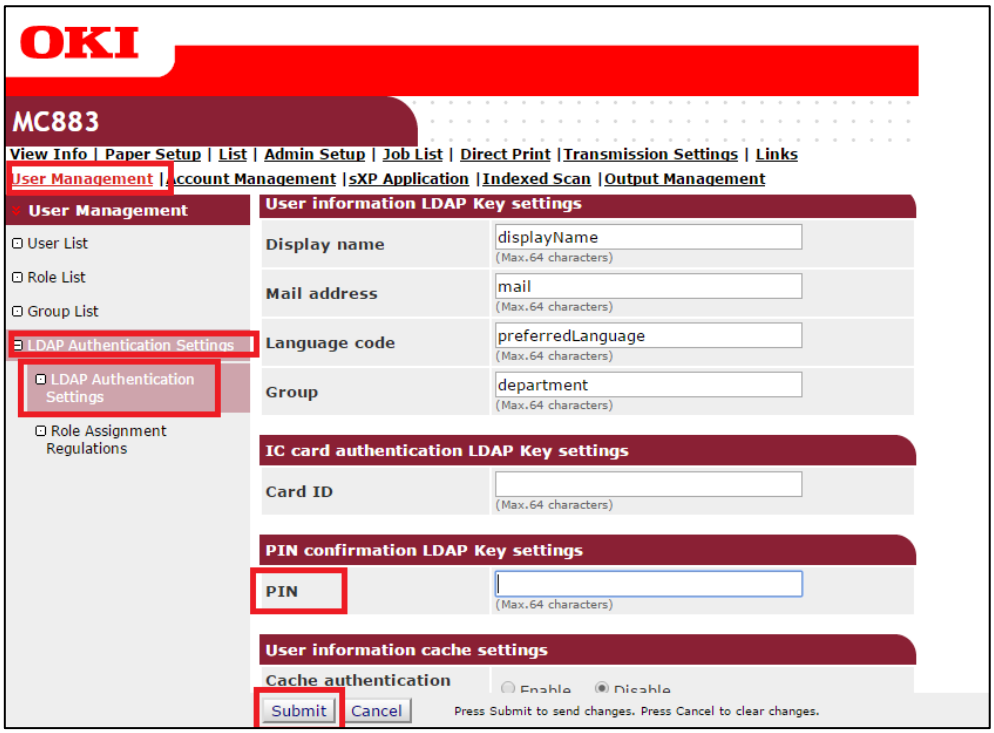


Fig. 81 - Smart Device Configuration

Note: The default field in SENDYS Explorer for PIN is "**homePhone**"

If you which to work with **Card** in **Directory Service**, please follow this procedure:

Note: SENDYS Explorer will not make any configurations of card id in Directory Service, so if you are working with Directory Service card you need to configure the device card's manual in Directory Service.

1. Click in **User Management > User List > LDAP Authentication Settings > LDAP Authentication Settings**
2. Insert the field that you have map as card id to **Card ID**
3. Click **Submit**

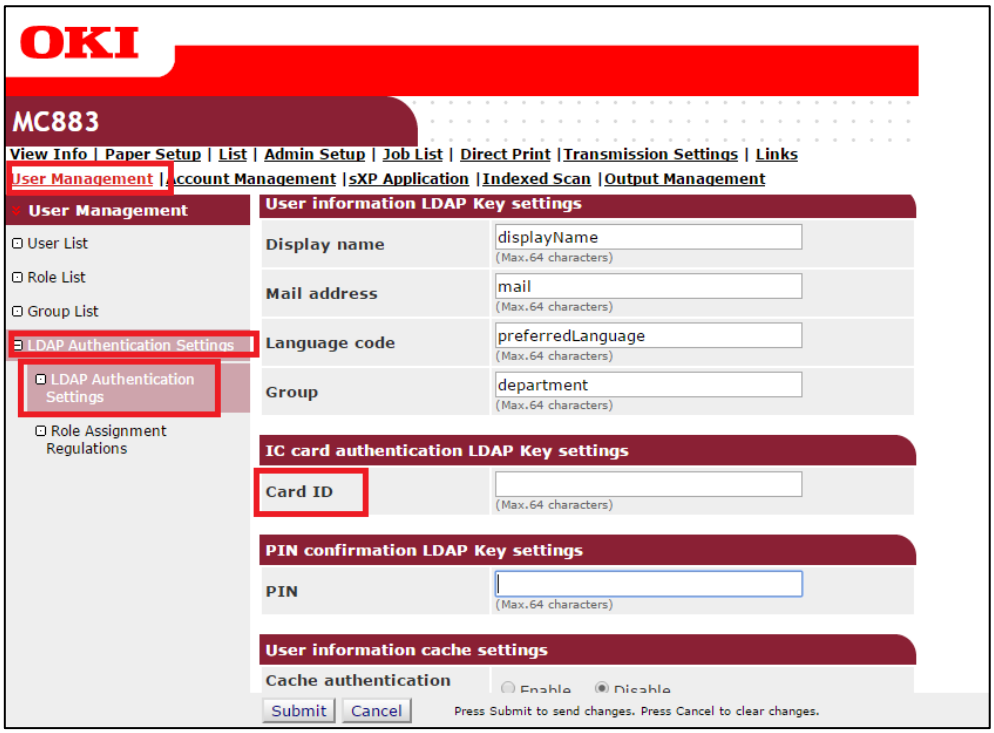


Fig. 82 - Smart Device Configuration

SMART DEVICE CONFIGURATION (SXP VERSION 2.0 (C542/ES5442 SERIES))

SCREEN APPLICATION CONFIGURATION

In order to see the application on the device screen you need to configure the sXP application on the smart device.

The application address is **http://[ServerIP]:50091/scan.aspx**.

1. Go to the device webpage **http://[DeviceIP]**
2. Click on [Administrator Login]
3. Insert admin username and password default credentials (**admin**/**999999**)
4. If the following screen is appeared, please click [**SKIP**]

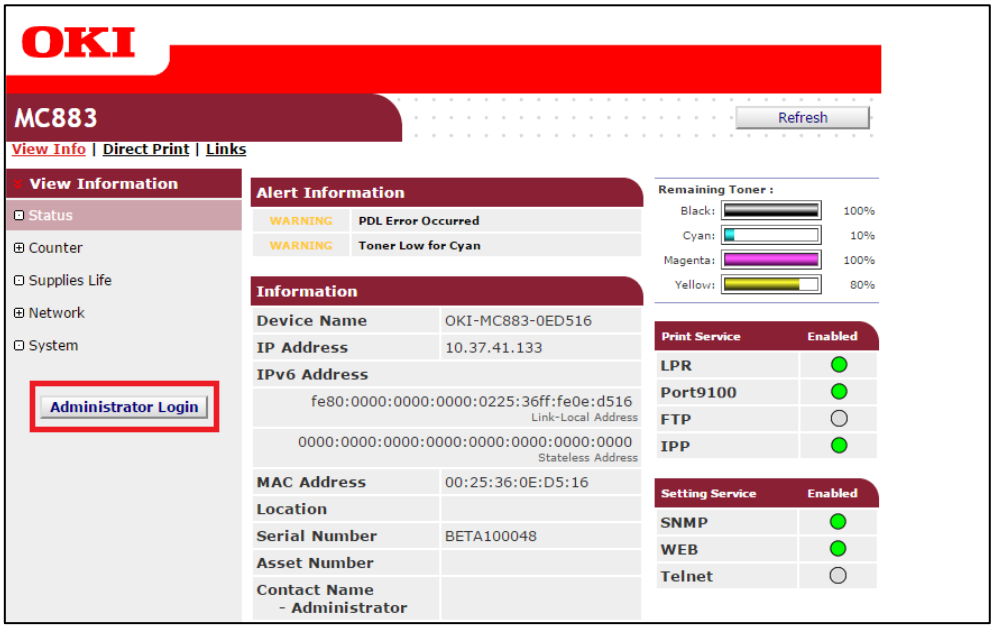


Fig. 83 - Smart Device Login

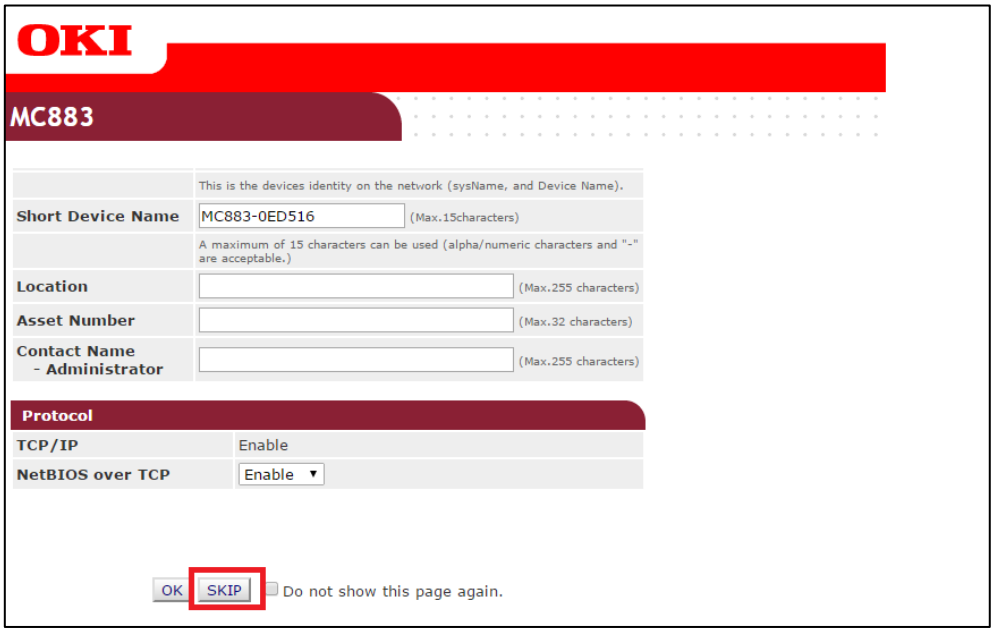


Fig. 84 - Smart Device Login

To configure SENDYS Explorer as default machine screen:

5. Click on **sXP Application**.
6. Click on **[+]**.

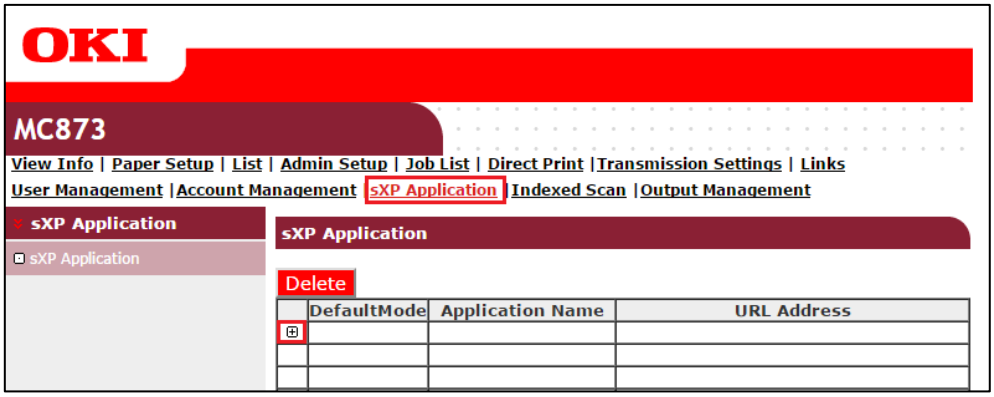


Fig. 85 - Screen Application Configuration

7. In the new window:
   a. Define the **Application Name**.
   b. Set **URL Address** to http://[ServerIP]:50091/scan.aspx.
8. Click **OK**.

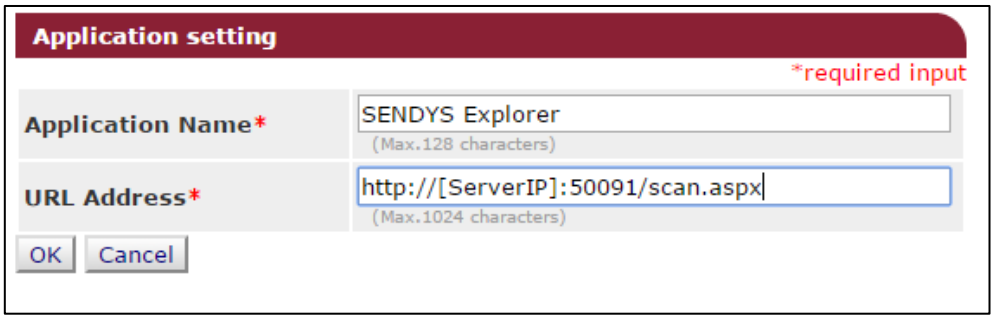


Fig. 86 - Screen Application Configuration

Note: This will add SENDYS Explorer to the device **JOB Macro**.

Then on the device you need to:

- Access as admin.
- Go to **Admin Setup > Configure Home Screen > Touch a blank space > ADD**
- Select **SENDYS Explorer** from the **JOB Macro**

9. Select **Default Mode**.
10. Click **Submit**.

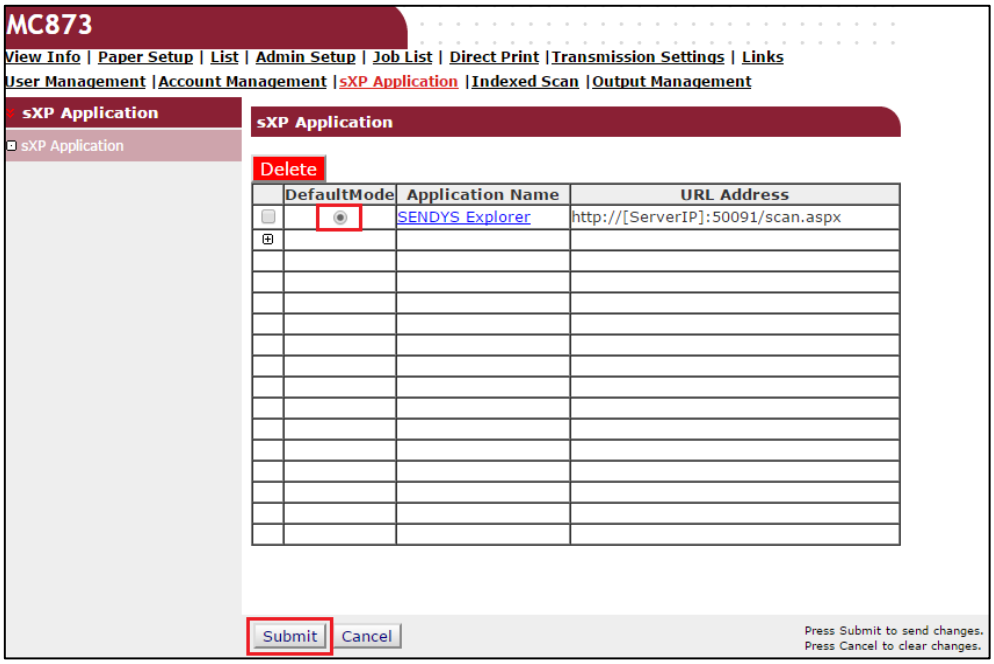


Fig. 87 - Screen Application Configuration

Note: This will only define the default screen application.

Then on the device you need to:

- Access as admin.
- Go to **Admin Setup > Manage Unit > Default Mode**
- Select **Web Browser**

SFP LOCAL AUTHENTICATION

This section will describe how to configure the device to work with MFP local authentication.

1. Go to the device webpage **http://[DeviceIP]**
2. Click on [Administrator Login]
3. Insert admin username and password default credentials (**admin**/**999999**)
4. If the following screen is appeared, please click [**SKIP**]

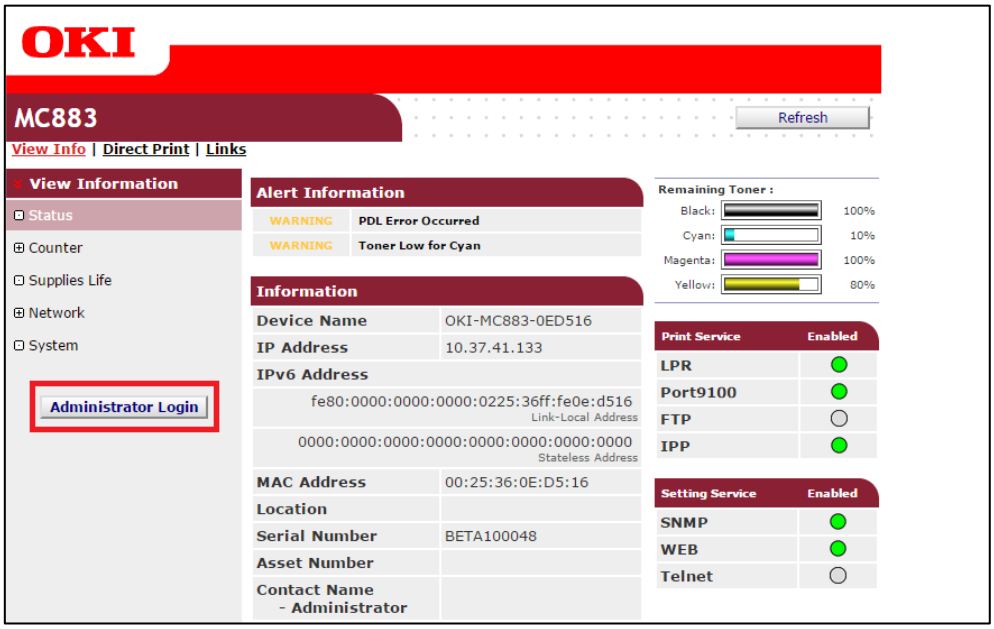


Fig. 88 - Smart Device Configuration

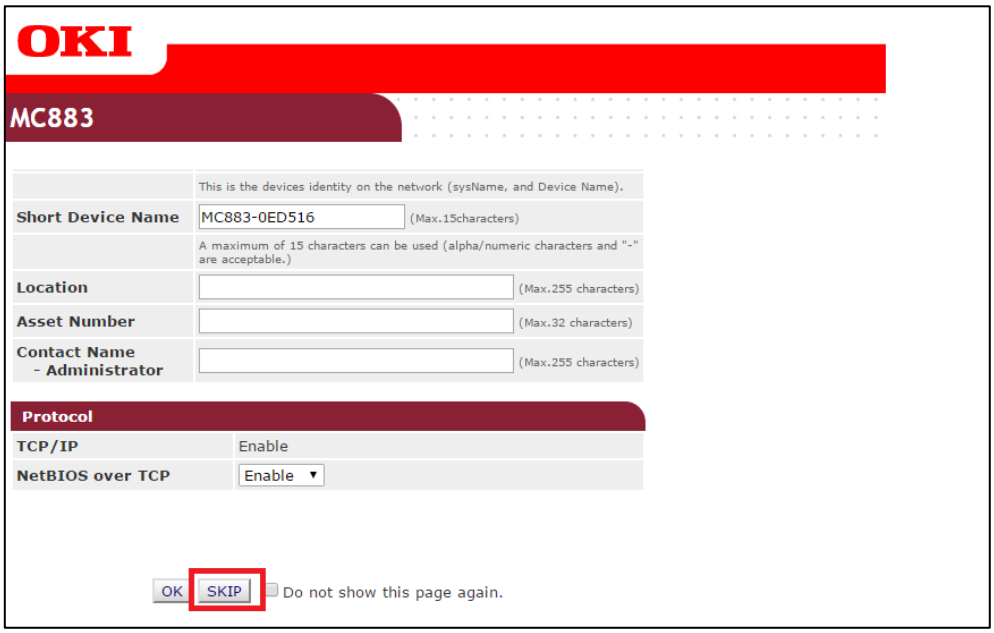


Fig. 89 - Smart Device Configuration

Configure Device Authentication:

5. Click in **Admin Setup >Management>Access Control Setup**
6. Enable **Access Control**
7. Disable **Guest user use**
8. To enable **Authenticate Local Name**. (to enable **Authenticate Local PIN** and **Authenticate Local IC Card** if you need)
9. Click **Submit**

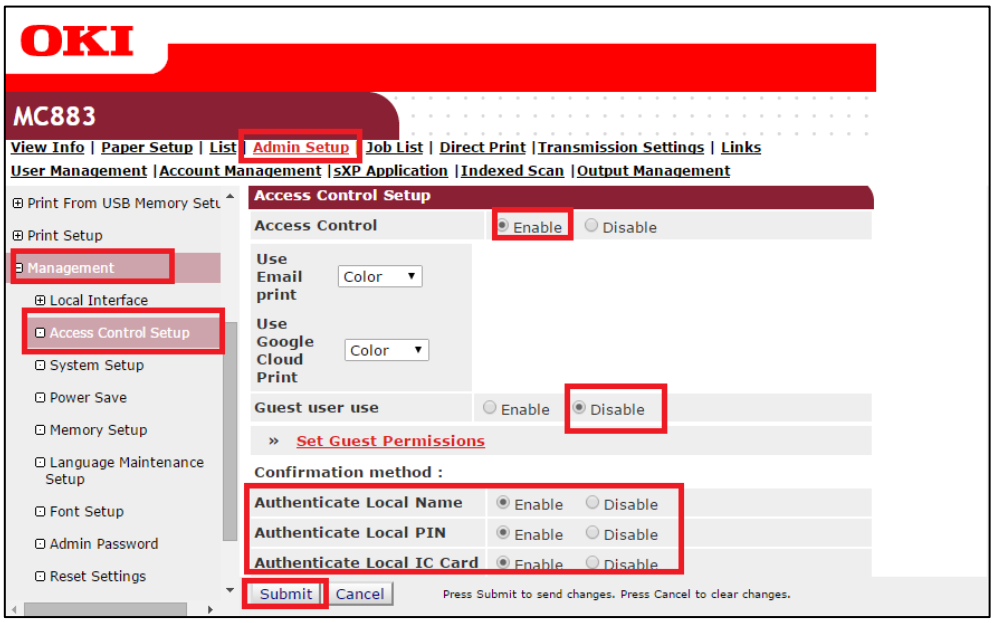


Fig. 90 - Smart Device Configuration

Note: You must create all users on the device. **SENDYS Explorer will then automatically create the users within the application when each user first logs-into the device**, their initial SENDYS Explorer web password is the same as the username that is displayed on the device.

Note: Users can select the authentication method by their selves. If you would like to restrict the authentication method, please disable **Confirmation Method (Authenticate Local Name, Authenticate Local PIN, Authenticate Local IC Card)** if you need.

Note: If you can allow users to associate their card ID with their account, enable **Register general user's IC card**.

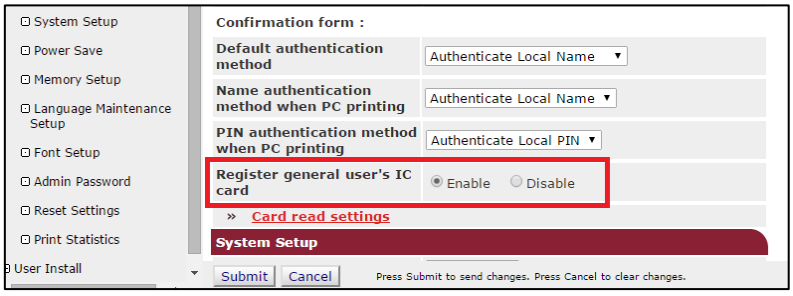


Fig. 91 - Smart Device Configuration

To create users go to **User Management > User List>Local User >[+]**

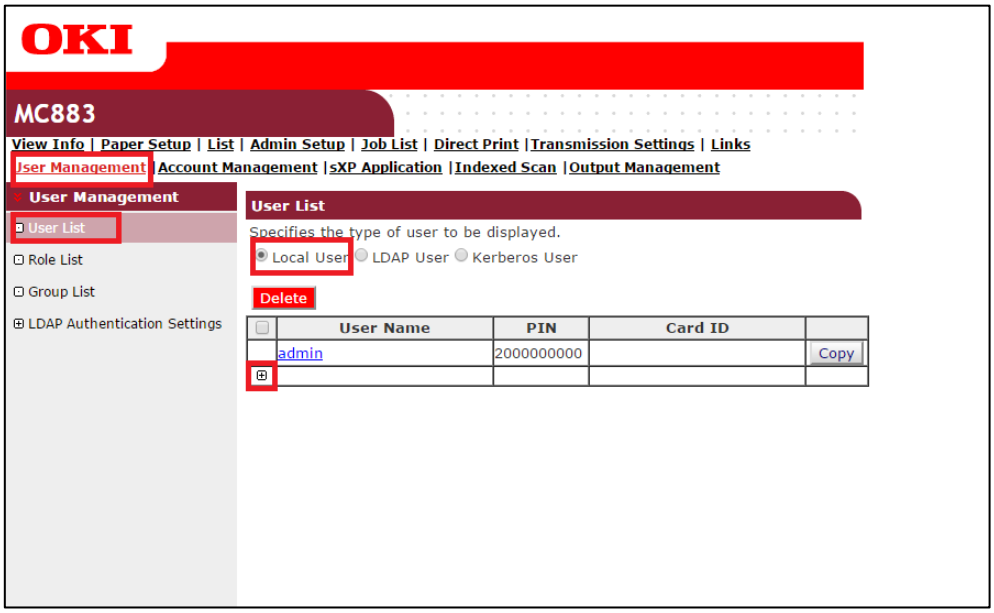


Fig. 92 - Smart Device Configuration

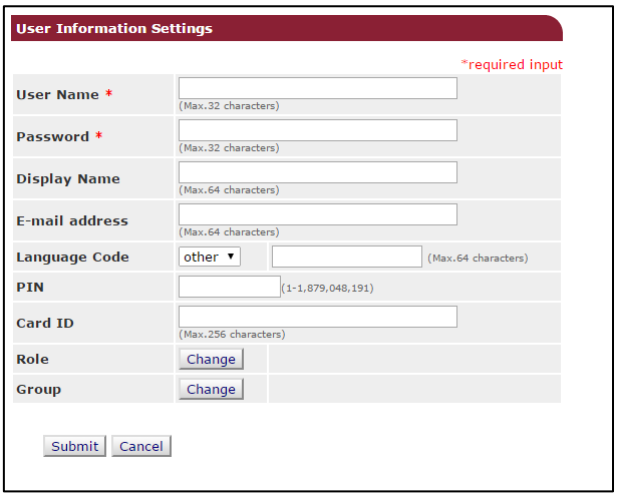


Fig. 93 - Smart Device Configuration

Note: You must enter **PIN** if you use **Authenticate Local PIN**.

Note: You must enter Card ID if you use Authenticate Local IC Card and disable **Register general user's IC card** in **Access Control Setup**. MC8x3/ES84x3 supports Elatec TWN4 card reader with keyboard interface for authentication by IC Card.

DIRECTORY SERVICE AUTHENTICATION

This section will describe how to configure the device to work with your directory service for authentication.

1. Go to the device webpage **http://[DeviceIP]**
2. Click on [Administrator Login]
3. Insert admin username and password default credentials (**admin**/**999999**)
4. If the following screen is appeared, please click [**SKIP**]

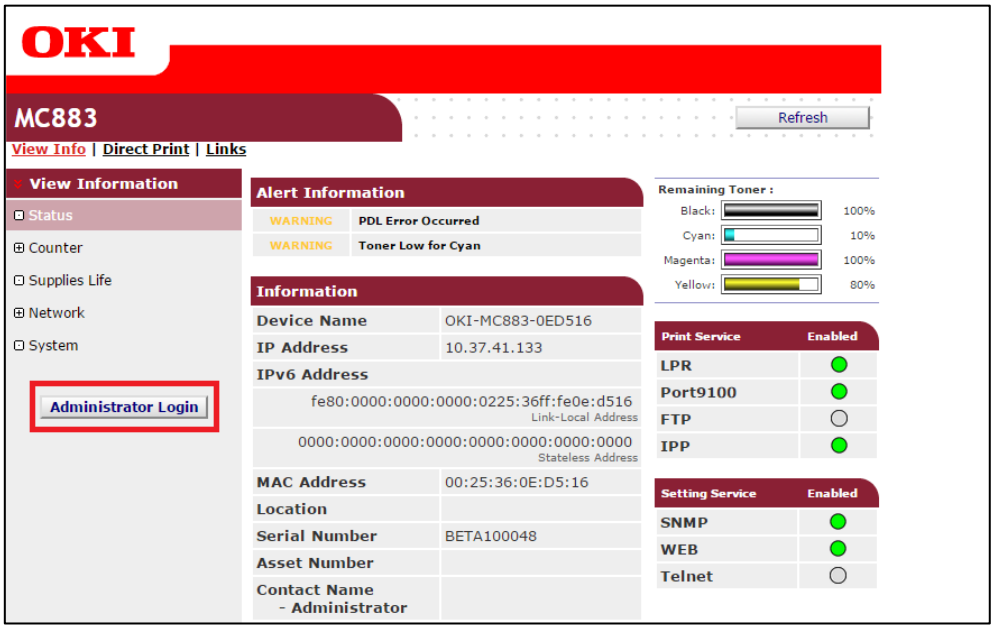


Fig. 94 - Smart Device Configuration

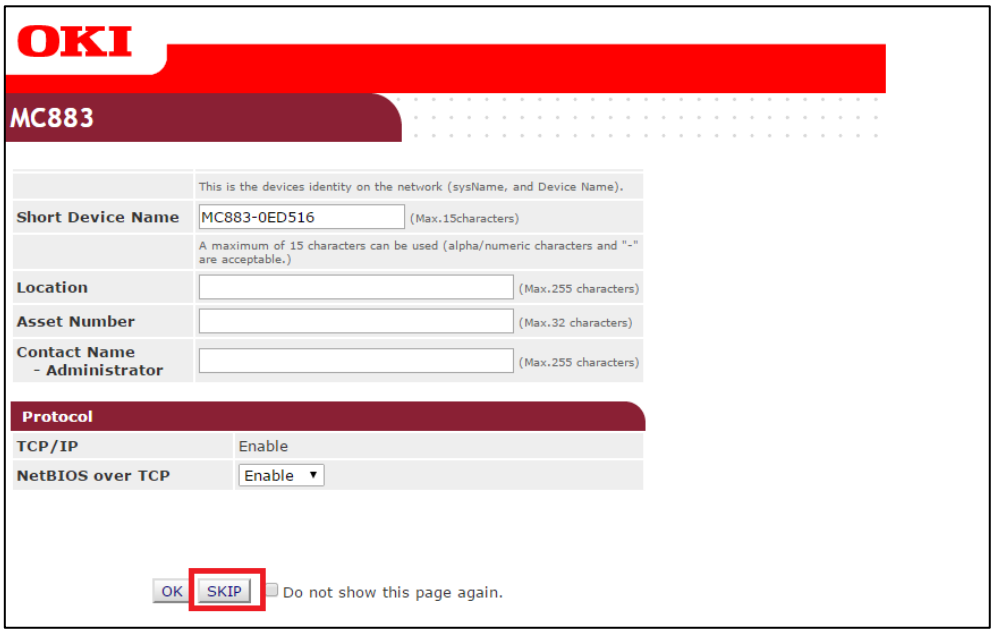


Fig. 95 - Smart Device Configuration

Configure Device DNS settings:

Note: If Device DHCP server information is retrieved from DHCP server correctly, you don't have to configure Device DNS setting manually.

1. Click in **Admin Setup > Network>TCP/IP**
2. Click on **(OPTIONAL) Change other TCP/IP settings**.
3. Configure the **primary DNS Server Address**
4. Click **OK**
5. Click **Submit**

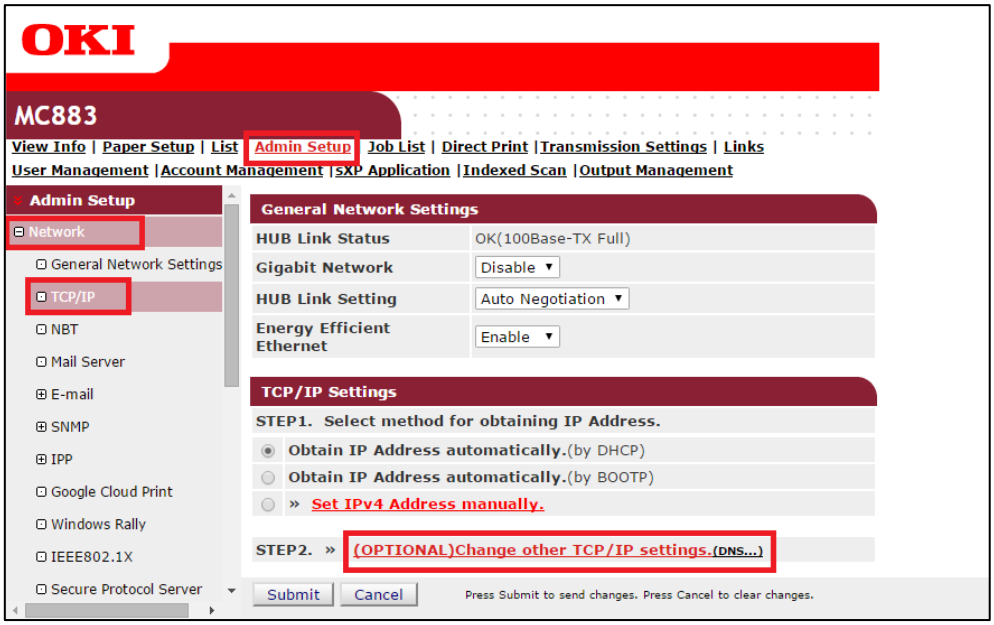


Fig. 96 - Smart Device Configuration

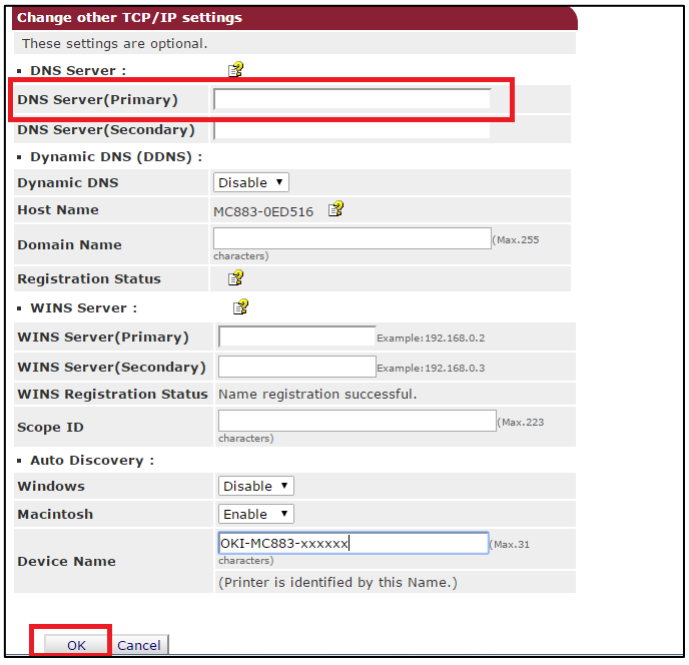


Fig. 97 - Smart Device Configuration

Configure Device SNTP settings:

Note: If Device SNTP server information is retrieved from DHCP server correctly, you don't have to configure Device DNS setting manually.

Note: If you set correct date and time manually, you don't have to configure Device SNTP server setting.

1. Click in **Admin Setup >User Install > Time Setup**
2. Set "**Auto**" in **Time Setup**
3. Configure the **SNTP Server (Primary) Address**
4. Click **Submit**

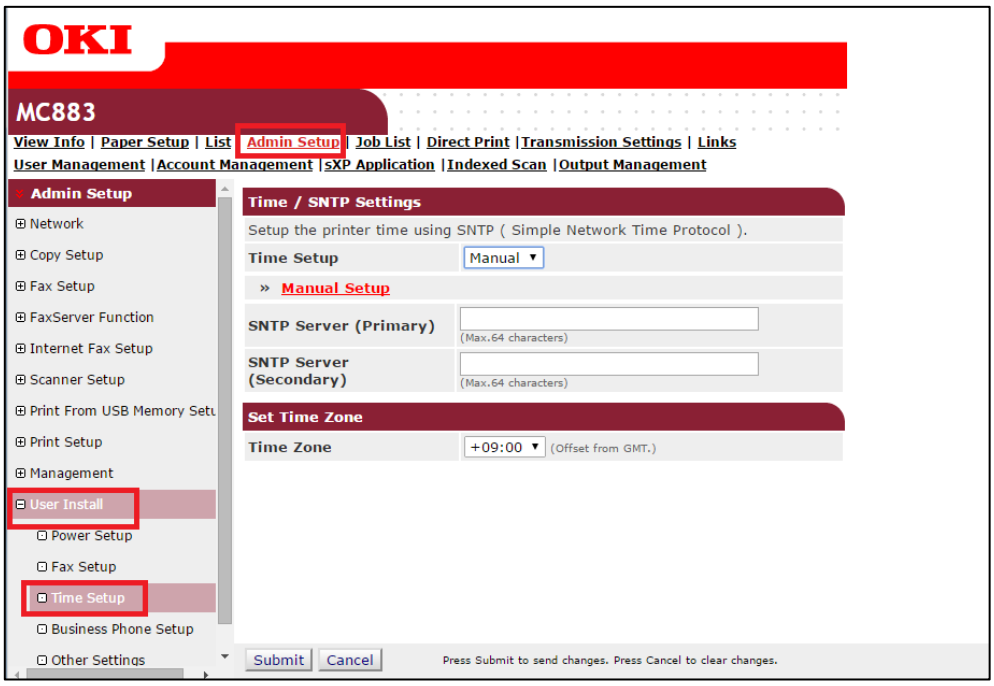


Fig. 98 - Smart Device Configuration

Configure Device authentication:

1. Click in **Admin Setup > Network >LDAP**

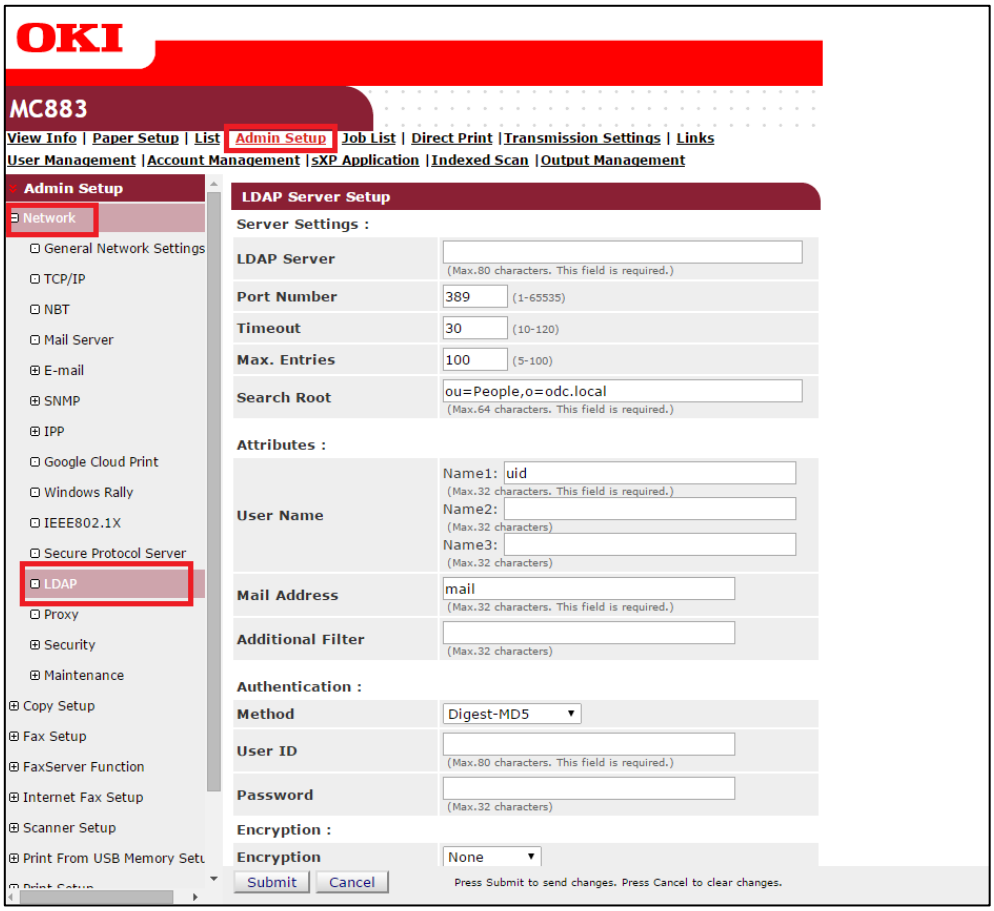


Fig. 99 - Smart Device Configuration

Name	Details
LDAP Server	Directory Service IP address or HostName. If you select Secure Protocol in Method, you have to set a host name or IP address which can be reversely resolve a host name from the DNS server.
Port Number	Default Directory Service port is 389. You should only change this if your LDAP server has been configured to use a different port.
Timeout	Timeout to get information from LDAP server after login the device. The setting is used when you set Authenticate LDAP PIN or Authenticate LDAP IC Card.
Max. Entries	Specify the maximum number of search results that are a response by e-mail address search. The setting is not used for LDAP authentication.
Search Root	LDAP search base. Ex : CN=Users,DC=company,DC=com The setting is not used for LDAP authentication.
User Name	Insert the field that you have mapped for the username. The setting is not used for LDAP authentication.
Mail Address	Insert the field that you have mapped for the email address. The setting is not used for LDAP authentication.
Additional Filter	This filter is to find email address from LDAP server. The setting is not used for LDAP authentication.
Method	Select [Digest-MD5] or [Secure Protocol] based on your LDAP server environment. Note: [Anonymous] and [Simple] doesn't work for the access control. Note: [Secure Protocol] requires DNS configuration and SNTP configuration in order to synchronize the device time with the Secure Protocol server's time.
Username	User from AD or LDAP that has access to read all the AD or LDAP groups that you need to synchronize. The setting is used when a user authenticates by Authenticate LDAP PIN or Authenticate LDAP IC Card
Password	Password of that user.
Encryption	Encryption type.

Table 8 - Server Details

2. Make the LDAP configurations and click on **Submit**

Configure Secure Protocol Server setting

Note: If you select **Secure Protocol Server** as **Method** in **LDAP Server Setup**, you must configure Secure Protocol Server.

1. Click in **Admin Setup > Network >Secure Protocol Server**
2. Configure Secure Protocol Server name in **Domain**.

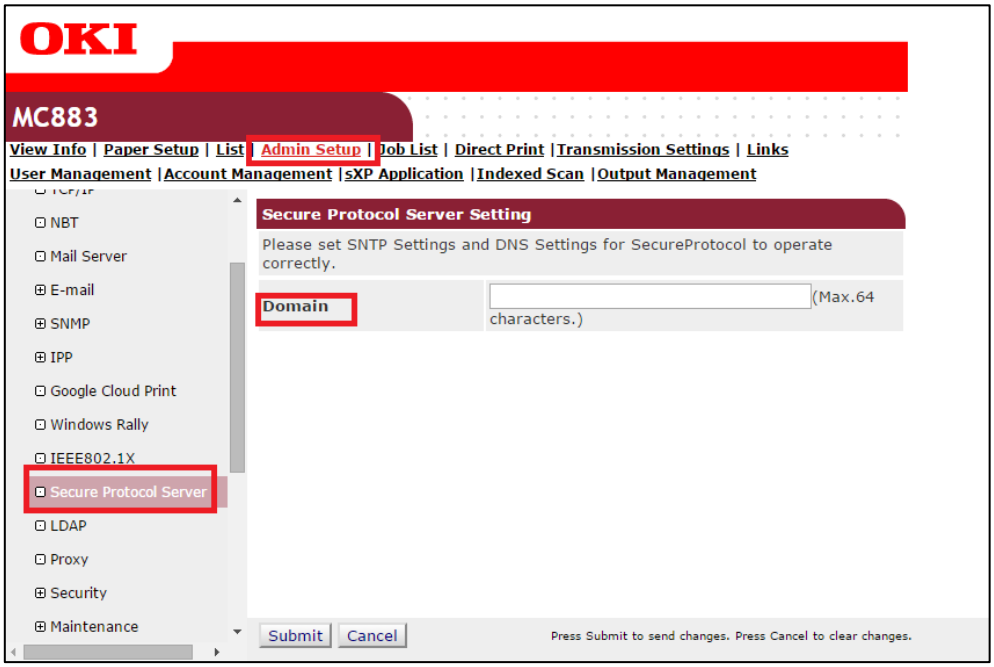


Fig. 100 - Smart Device Configuration

Note: The Secure Protocol Server name must be entered in capital letter.

Configure Device Authentication

1. Click in **Admin Setup >Management>Access Control Setup**
2. Enable **Access Control**
3. Disable **Guest user use**
4. To enable **Authenticate LDAP Name**. (to enable **Authenticate LDAP PIN** and **Authenticate LDAP IC Card** if you need)
5. Click **Submit**

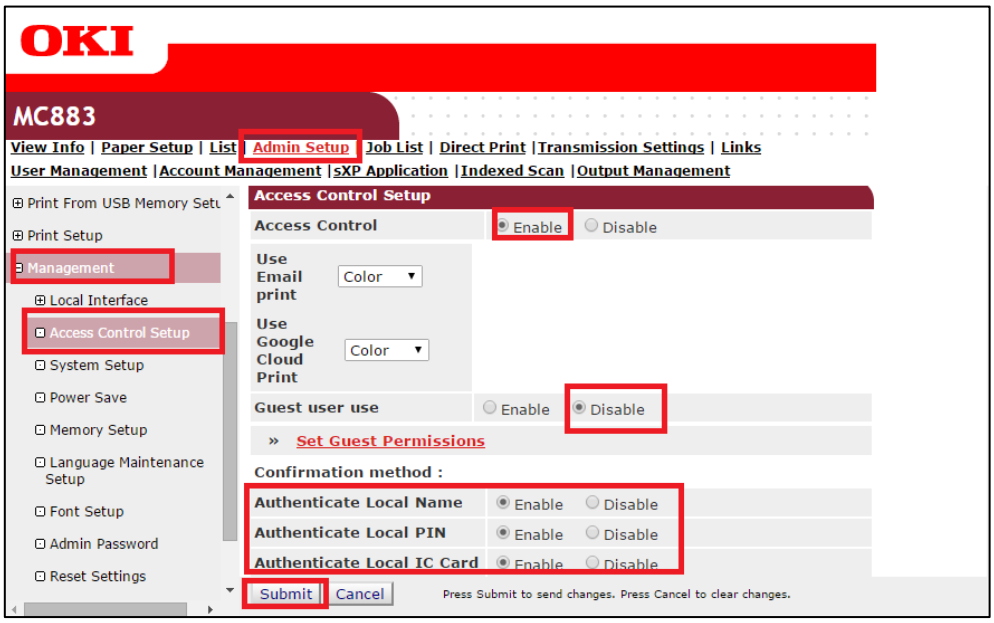


Fig. 101 - Smart Device Configuration

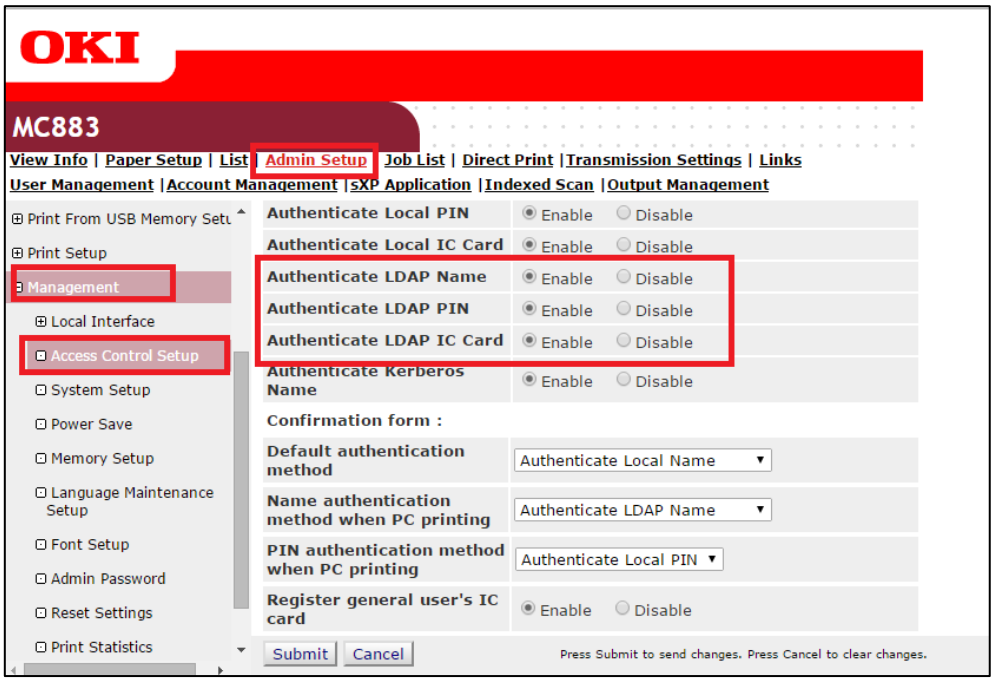


Fig. 102 - Smart Device Configuration

If you wish to work with **PIN** in **Directory Service**, please follow this procedure:

Note: SENDYS Explorer will not make any configurations of PINs in Directory Service, so if you are working with Directory Service PIN you need to configure the device PINs manual in your Directory Service.

1. Click in **User Management > User List > LDAP Authentication Settings > LDAP Authentication Settings**
2. Insert the field that you have map as PIN to **PIN**
3. Click **Submit**

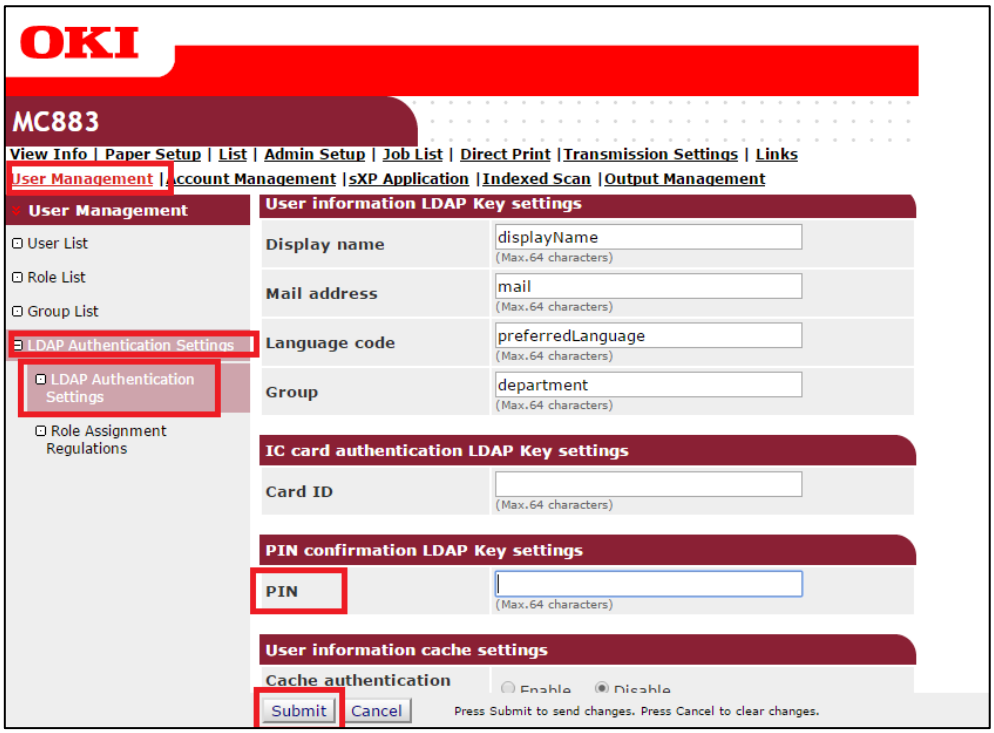


Fig. 103 - Smart Device Configuration

Note: The default field in SENDYS Explorer for PIN is "**homePhone**"

If you which to work with **Card** in **Directory Service**, please follow this procedure:

Note: SENDYS Explorer will not make any configurations of card id in Directory Service, so if you are working with Directory Service card you need to configure the device card's manual in Directory Service.

1. Click in **User Management > User List > LDAP Authentication Settings > LDAP Authentication Settings**
2. Insert the field that you have map as card id to **Card ID**
3. Click **Submit**

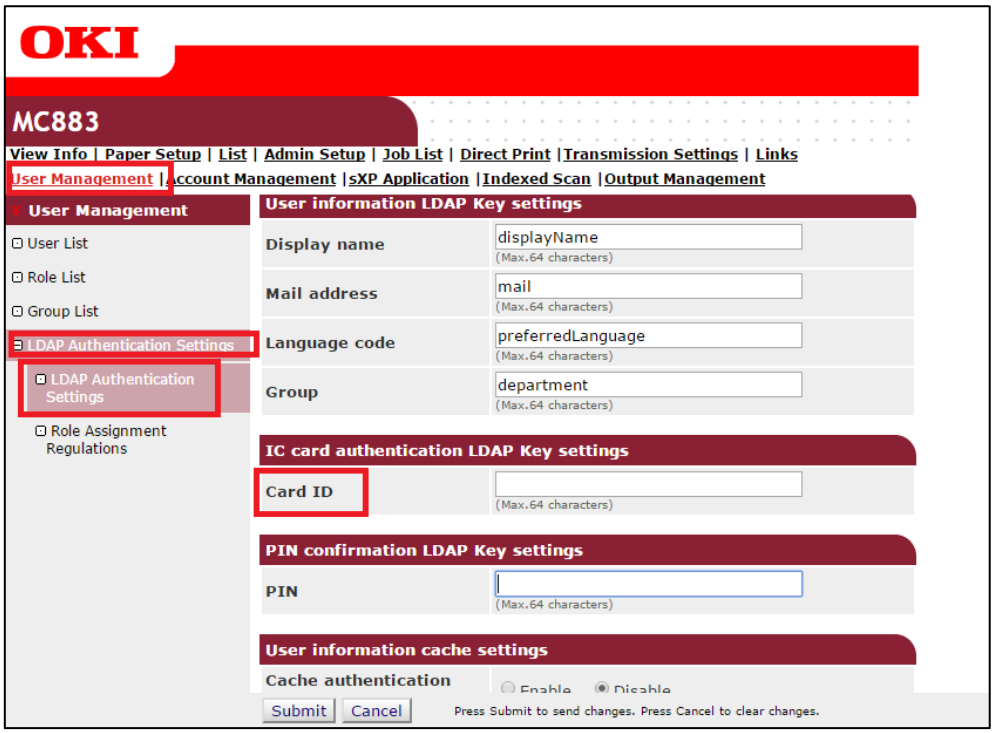


Fig. 104 - Smart Device Configuration

MFP DEVICE (NON-SMART) CONFIGURATION

Using MFP non-smart devices **requires** setting up the *network ftp scan profile*.

1. Go to the device's page **http://[DeviceIP]/**.
2. Insert admin credentials and click on Login (by default **admin**/**aaaaaa**).
3. Click on **Profile/List**.
4. Click on **New**.

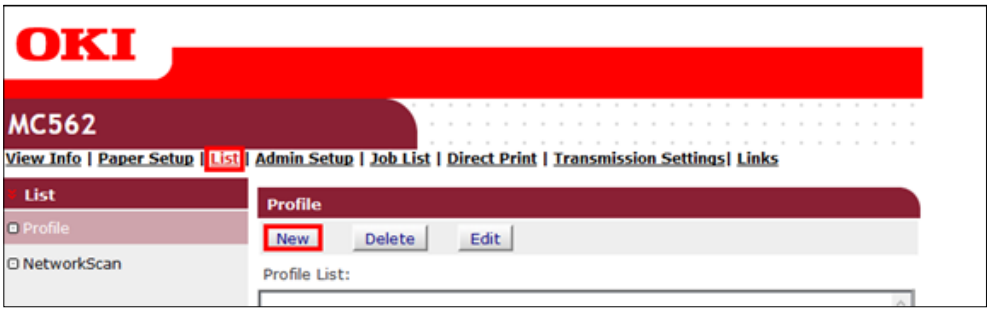


Fig. 105 - MFP Configuration

5. Refer to following table while filling the information:

Name	Details
Profile Name	Name of the profile.
Protocol	Protocol that will be used with this profile. Set to FTP.
Target URL	FTP path to *ScannedFiles* folder on the server.
Port Number	Port number for this profile. By default, 21 is the port assigned to FTP.
FTP Passive Mode	Set to OFF.
User Name	Same Administrator username that you used in the SENDYS Explorer installation.
Password	Same Administrator password that you used in the SENDYS Explorer installation.
File Name	File name for documents scanned while using this profile. It should be **mfp_[PrinterIP].#d** or **mfp_[PrinterName].#d**. **Note**: [**PrinterIP**] must be split by underscores and [**PrinterName**] must not contain periods.

Table 9 - Profile details.

Note: All other settings are document specific settings that should be defined by the user. You can also create as many profiles as needed with the same server settings and different document settings

6. Click on **Submit**

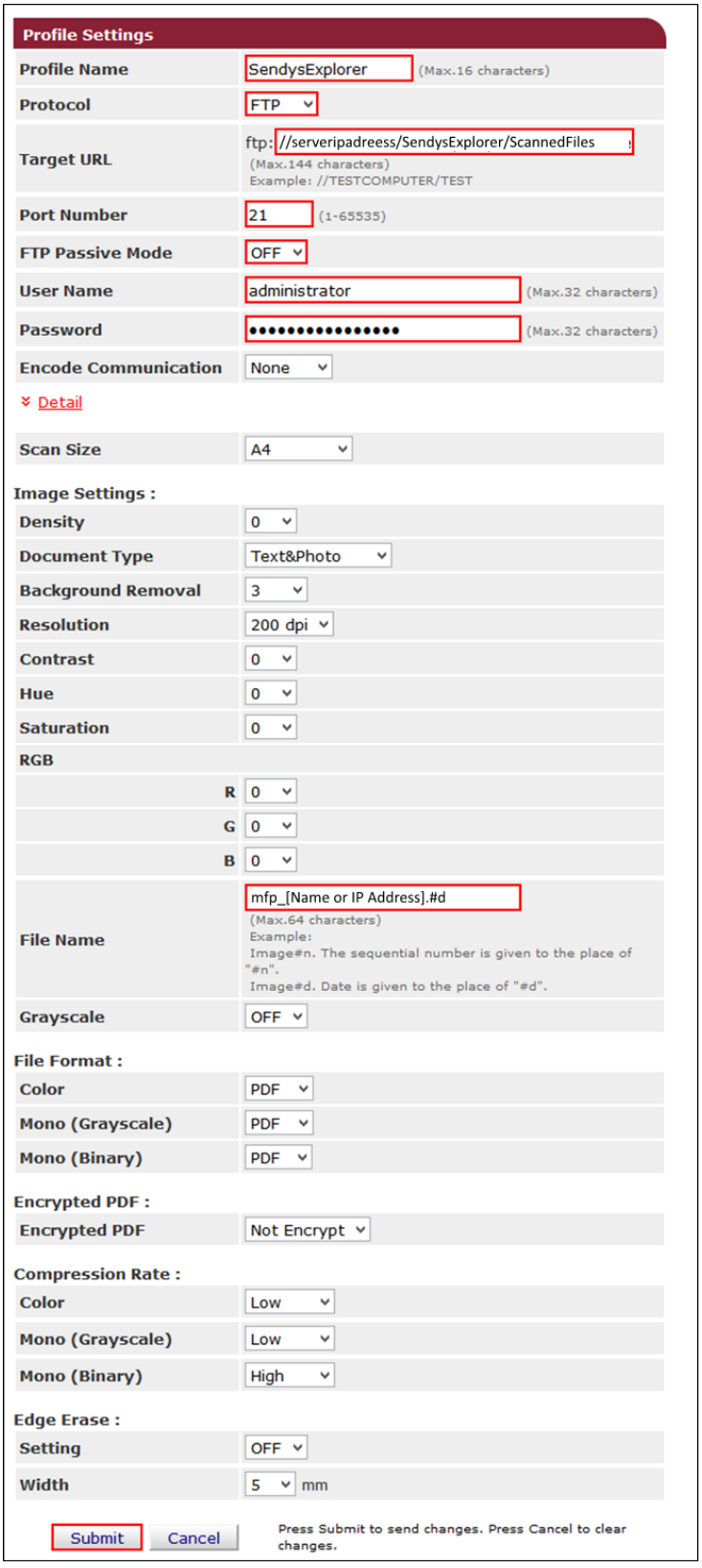


Fig. 106 - MFP Profile Configuration

OUTPUT MANAGER CONNECTOR

ADVANTAGES

SENDYS Explorer is a scalable solution that allow your organization to have full control over all document workflow in your organization.

The solution is composed by several components “Connectors” that provide your organization to have devices control, print management, document capture and workflows.

The integration and control over all devices, input and output of documents that allow you to automate your process, increase security and increase your company efficiency and productivity.

SENDYS Explorer with Output Manager connector provides a print management solution that delivers real savings for companies. It’s a scalable and customisable solution for companies of all sizes with varied demands and specific needs.

COST CONTROL

Visibility and control of print and copy usage, by user or department. Quota settings. Educated decisions on device consolidation.

PULL PRINTING & MOBILE

Print from any device and release at any enabled device. Smartphone, RFID card and PIN control

CENTRALISED ADMINISTRATION

Web interface for remote access configuration and system management. Import users from Active Directory.

PRINT POLICY MANAGEMENT

Customize polices and routing conditions. Track rules, usage of supplies and estimated CO2 consumption. Job restrictions by user, department, application or document type.

ENHANCED SECURITY

Print jobs only released after user authentication. Device access rights applied to users.

VENDOR AGNOSTIC

Open, scalable and vendor-neutral solution, compatible to any printer.

INSTALLATION

For the Output Manager Connector installation:

1. Enter on portal with **Administrator** credentials.
2. Click on **License** menu.

On this License menu view, if the license for Output Manager Connector is installed.

3. Start the installation pressing the button **Start Install OM** (placed on top menu).

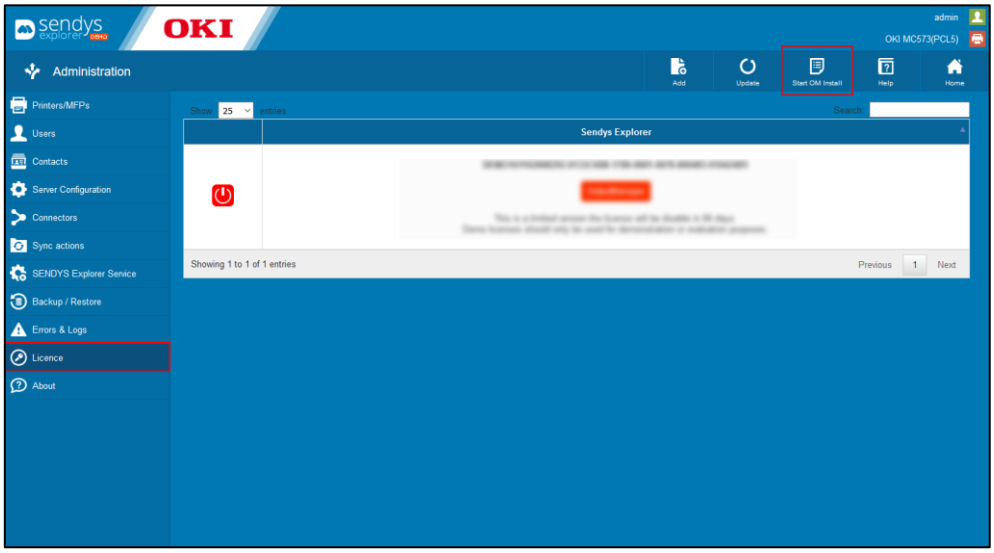


Fig. 107 -License view - Output Connector installation.

4. Select the type of installation and procced.

The options available are related with the creation of the database. The options are:

Name	Details
Quick	This installation will check if the SQL instance exists (if not then creates it) and then creates the database for the Output Manager automatically. This is a common type of installation when there isn´t any problem or requirements for the instance and database installation on the machine.
Advanced	On this installation, the instance and the database installation are configured if there are any specification for the installation on the machine.
Cancel	Cancel the installation of Output Manager and return to the License view.

Table 10 - Print job convert operation

5. Select the pretended options to procced the installation.

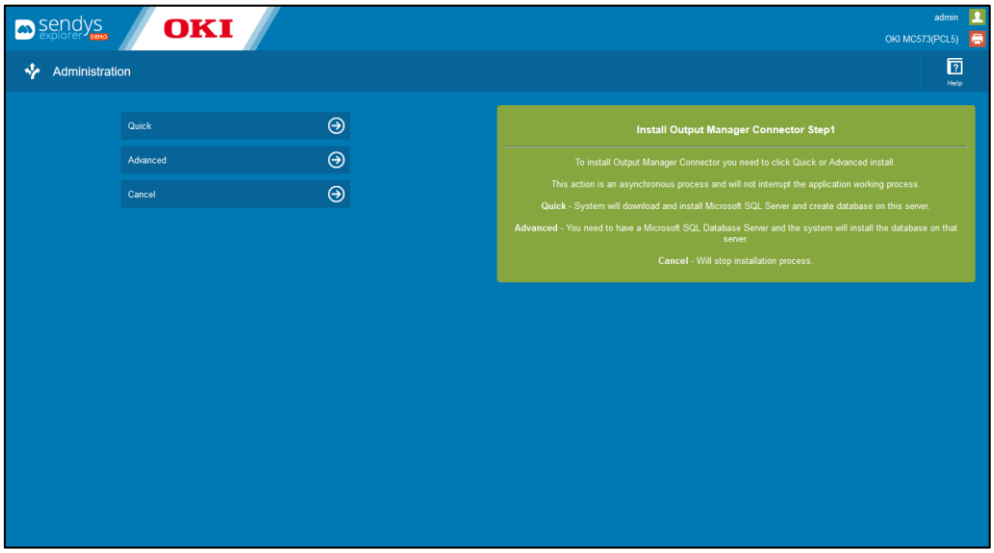


Fig. 108 - Output Connector type of installation.

At this moment, the installation started, creating the new content and database and only after the finalization of the installation, the new content of Output Manager Connector is accessible.

After this, the installation Output Manager Connector menu will appear on the top menu on the SENDYS Explorer portal.

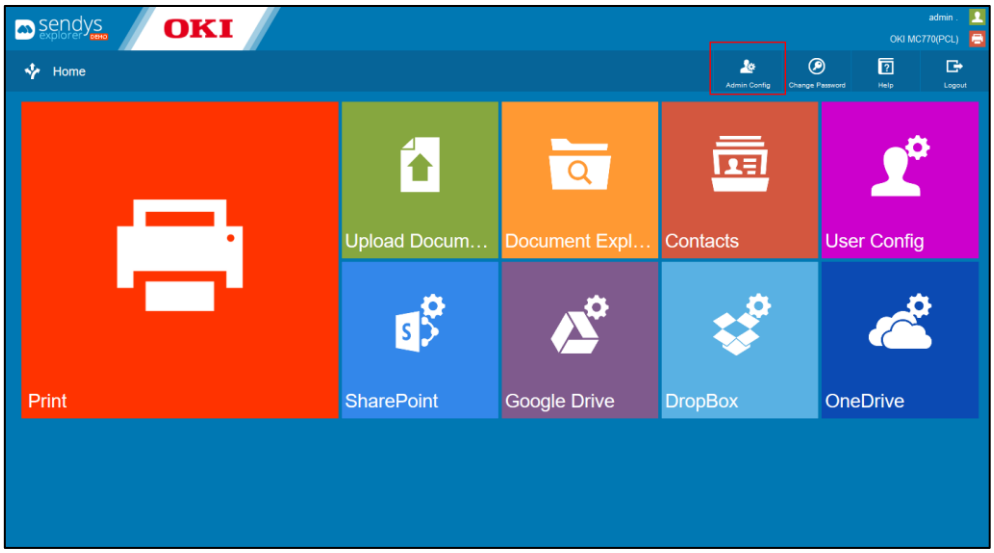


Fig. 109 -License view - Output Connector installation.

NOTE: The installation has several phases which in each phase some features on the portal are blocked.

OVERVIEW

1. Go to the browser http://serverIP:50091/.
2. Login on the application as admin.
   Note: By default, you can sign in using **admin** both **username** and **password**.
3. Click on **Admin Config**.

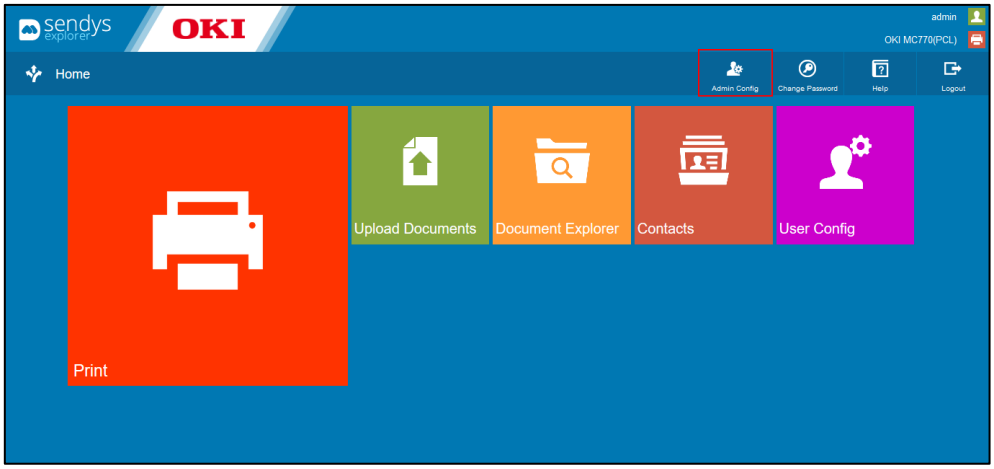


Fig. 110 - Web Portal

All configuration screens are work similarly, so we will start by explaining the basic icons and options of the admin configuration section.

Fig. 111 - Grid of possible Options

In the grids/table of contents we can find the above icons:

	Selection element		Deactivate
	Not possible to delete element		Link to device webpage
	Delete element		Download
	Edit element		Send email
	View Details		View Queue Details

These Icons represent the various status and type of messages shown on the grids/tables of contents.

Status OK		Status INFO	
Status WARNING		Status ERROR/FATAL	

In most of the sections the edit and delete buttons are in the grid/table of contents on the left side, as in the following picture.

The **Add** button and other section options are in the top right corner as in the below picture.

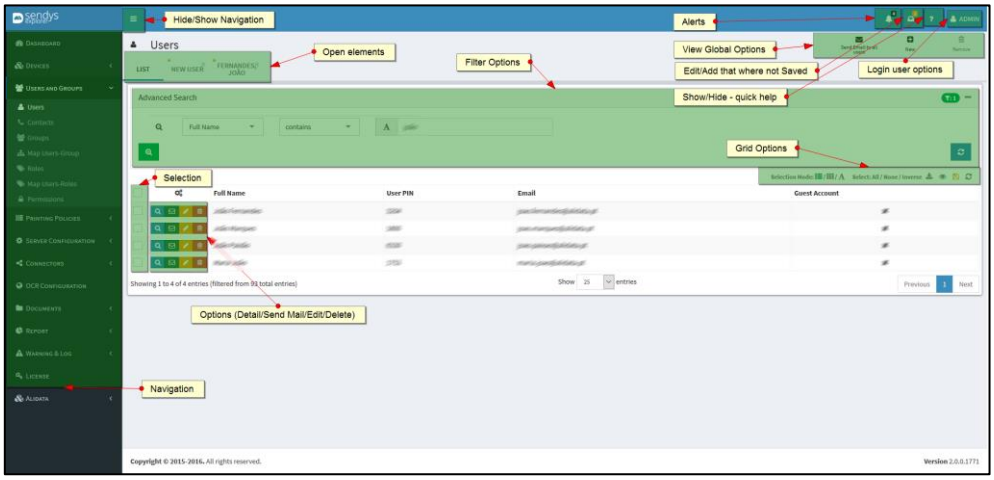


Fig. 112 - Platform Overview options

View Global Options: this buttons change between views and they are used to execute actions according with the view.

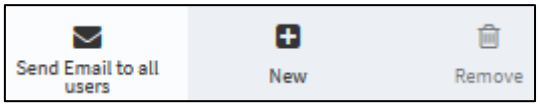


Fig. 113 - View Global Options

Grid Options: this options are associated with all grids and the actions that can be executed are:

- **Selection Mode**- Choose the mode to select the element on the grid. The modes are line selection, individual selection or only text selection.
- **Select** - use this tool to help on the pretended selection, for example clicking on "***All***" all the elements the grid will be selected.
- **Export** - grants the possibility to export the grid data, to an Excel file for example.
- **Eye symbol** - use this tool to choose the field to show on the grid.
- **Floppy disk symbol** - saves the grid configuration.
- **Refresh symbol** - refresh the grid data.

Fig. 114 - Grid Options

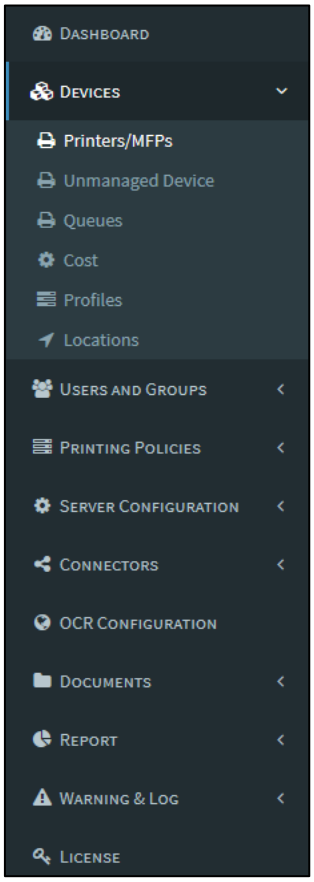


Fig. 115 - Navigation menu

In the top right corner of the application you have the following icons, those icons are always visible and show you a quick way to access some of the system options, also additional to this the application provide dynamic warnings from the devices and server, those alerts are display also on right corner above the icons.

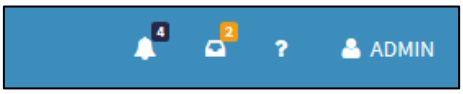
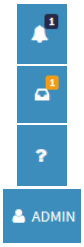


Fig. 116 - Alerts - Edit/Add not saved - Quick Help - Login User Options



Alerts & Warnings

Elements that where edited/added but are not yet save

Help

User Options

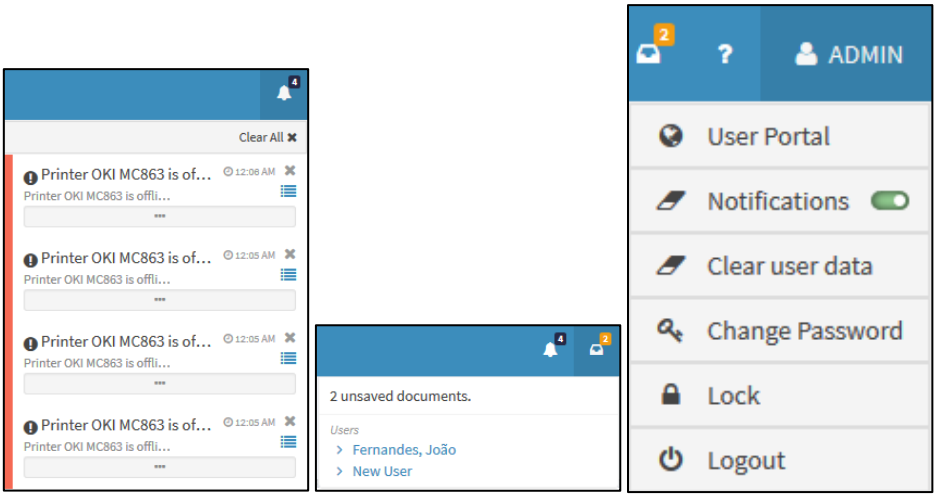


Fig. 117 - Alerts - Edit/Add not saved - Login User Options

Alerts & Warnings: This section will allow access to dynamic alerts and they can be consulted.

Element: this box represents the elements that where edited/added but are not yet saved. Clicking on them, it redirects to the element.

User Options: on this menu User Portal can be accessed, turn on/off Notifications, clearing User Data, changing Password, Lock and Logout of application.

Help: Information about the application, suggestions about what view options are available and changing color theme and language skins.

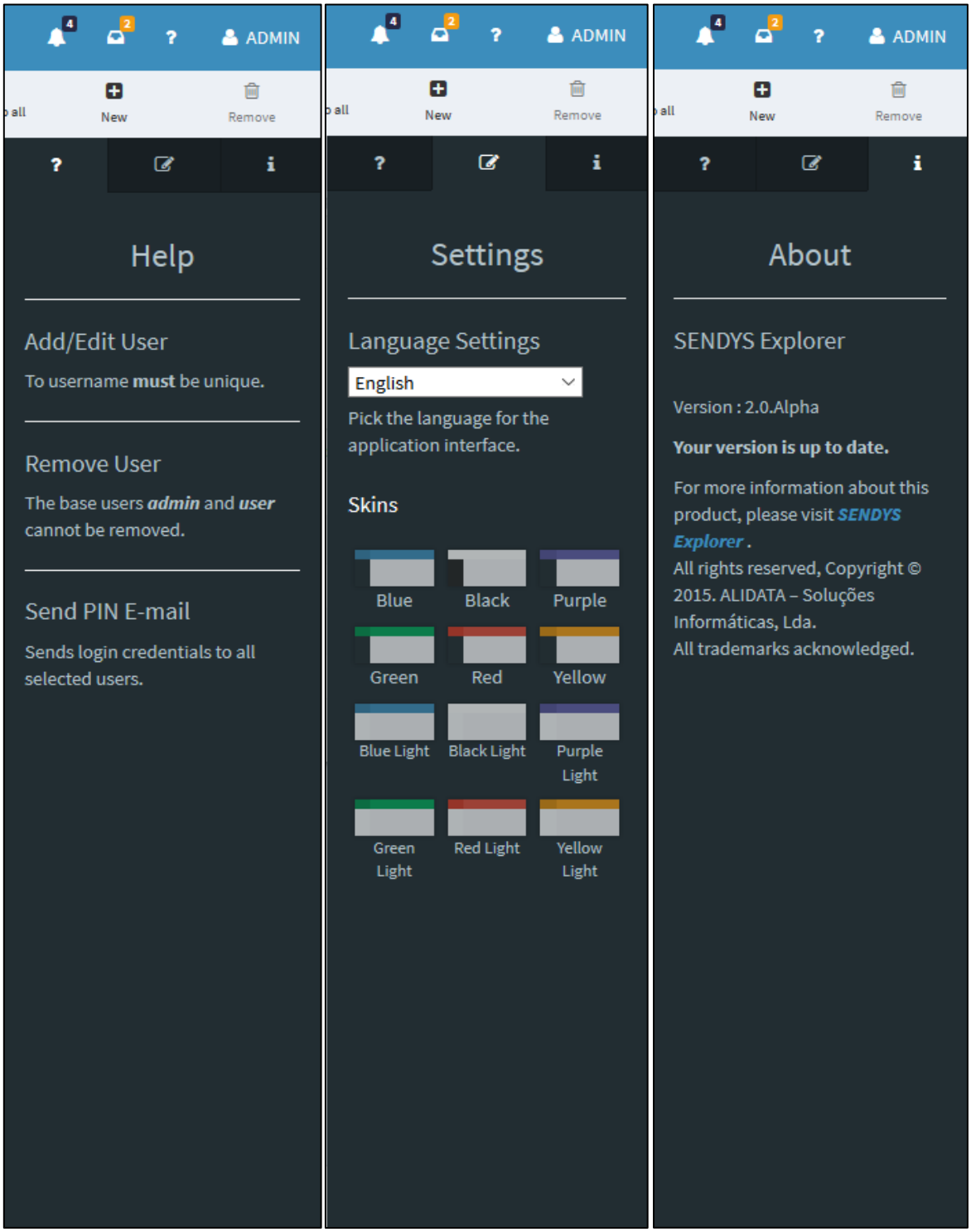


Fig. 118 - Help - Settings - About

DASHBOARD

This view shows important information about the SENDYS Explorer managing. Those graphics and tables can be refreshed individually or all at the same time.

IT-MANAGER

1. Click on **Dashboard** menu.
2. Click on **IT-Manager** tab.

- **SENDYS Explorer Status**: shows the Windows Services Status working with the application. The options **Start** and **Stop** are available. FTP Server button represent the hard-link to show on browser the FTP folder.
- **System Summary**: shows total counters presented on the server.
- **Last 30 Days Page Volume**: show the counters of printed pages on last 30 days.
- **Printer Status**: shows all printers and some information associated.
- **Network Scan Summary**: shows the summary of all network scan actions.

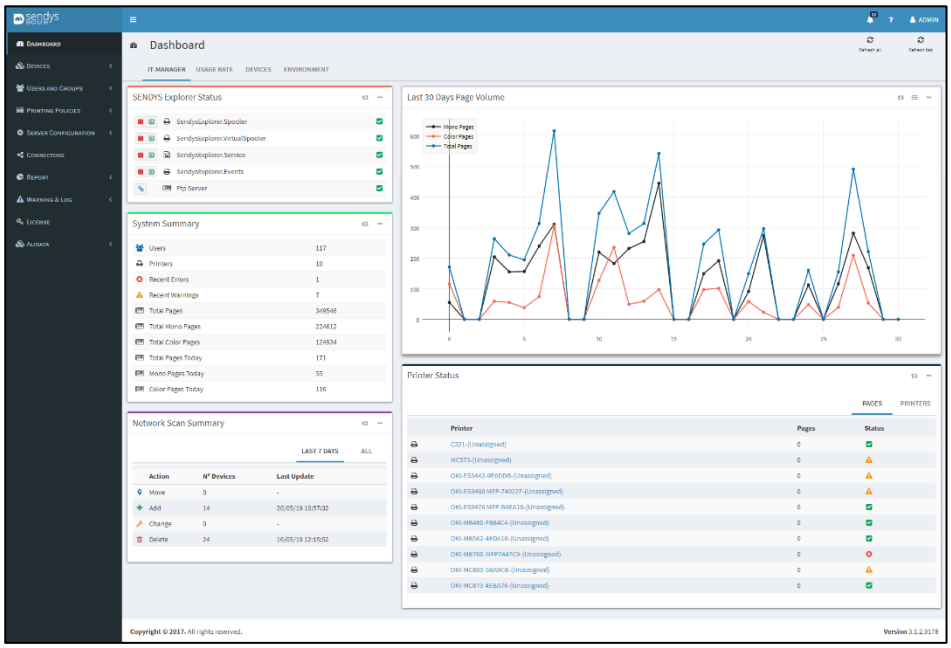


Fig. 119 - Dashboard - IT Manager

Printer Status Icons info:

	Status OK		Status INFO
	Status WARNING		Status ERROR/FATAL

USAGE RATE

1. Click on **Dashboard** menu.
2. Click on **Usage Rate** tab.

This view shows the rates of each type of print job done with the SENDYS Explorer application. Each graphic is dedicated to one subject. They are related with the type of jobs (copy or prints) and if it was color or mono.

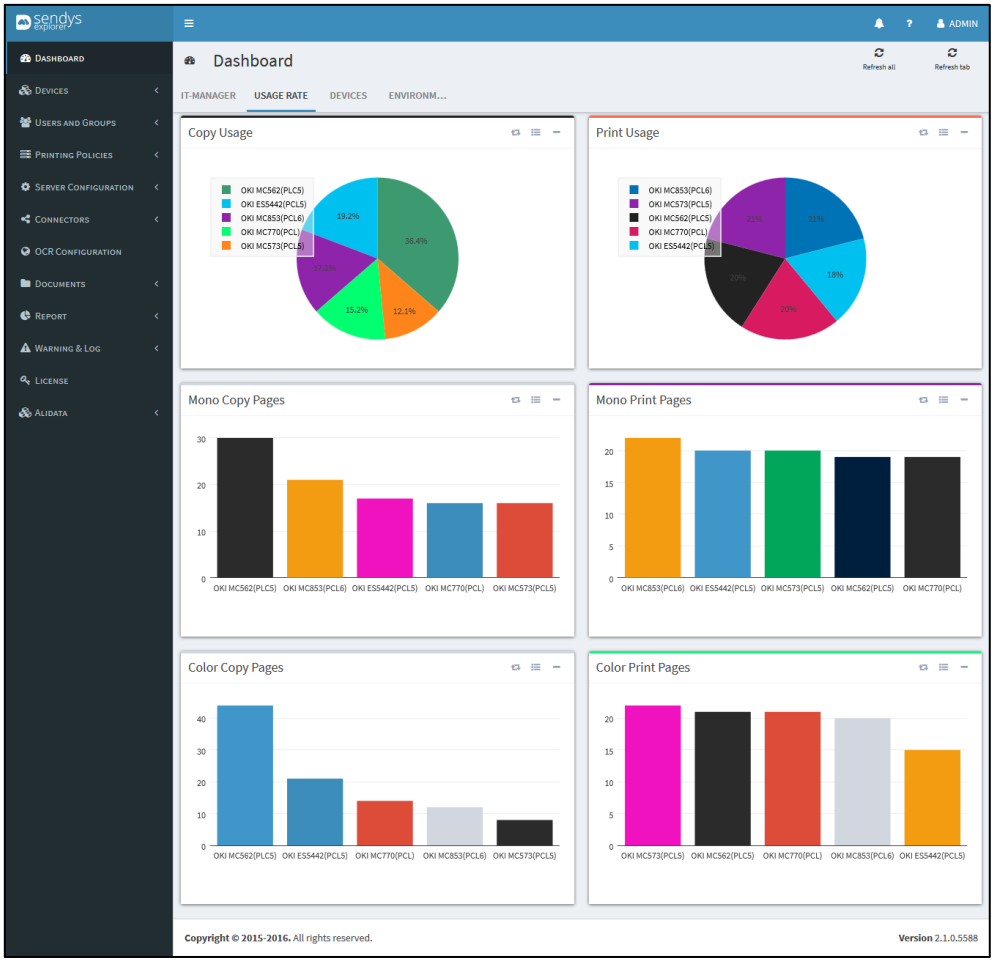


Fig. 120 - Dashboard - Usage Rate

DEVICES

1. Click on **Dashboard** menu.
2. Click on **Devices** tab.

This view shows all information related with all printers installed on application. Errors and availability rate are showed here.

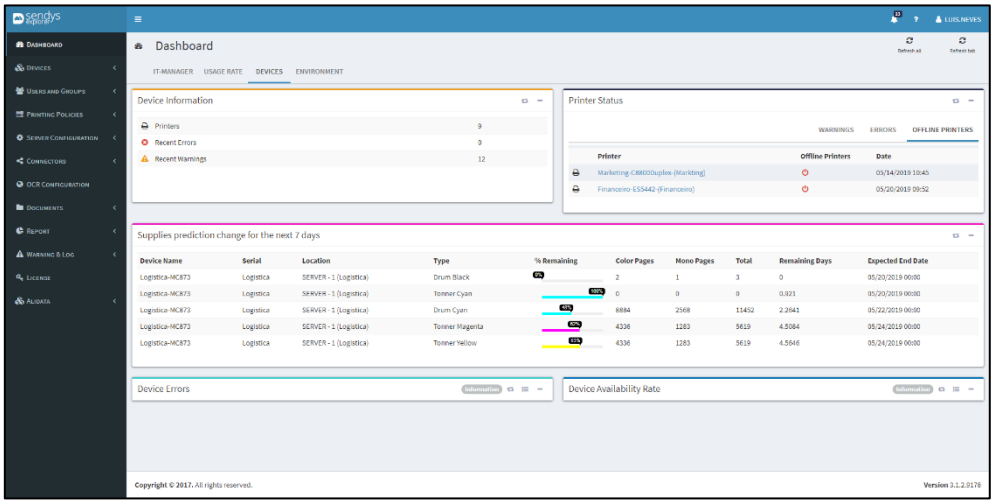


Fig. 121 - Dashboard - Devices

ENVIRONMENT

1. Click on **Dashboard** menu
2. Click on **Environment** tab.

This view shows information and graphics related with Savings, Consumed CO2, etc.

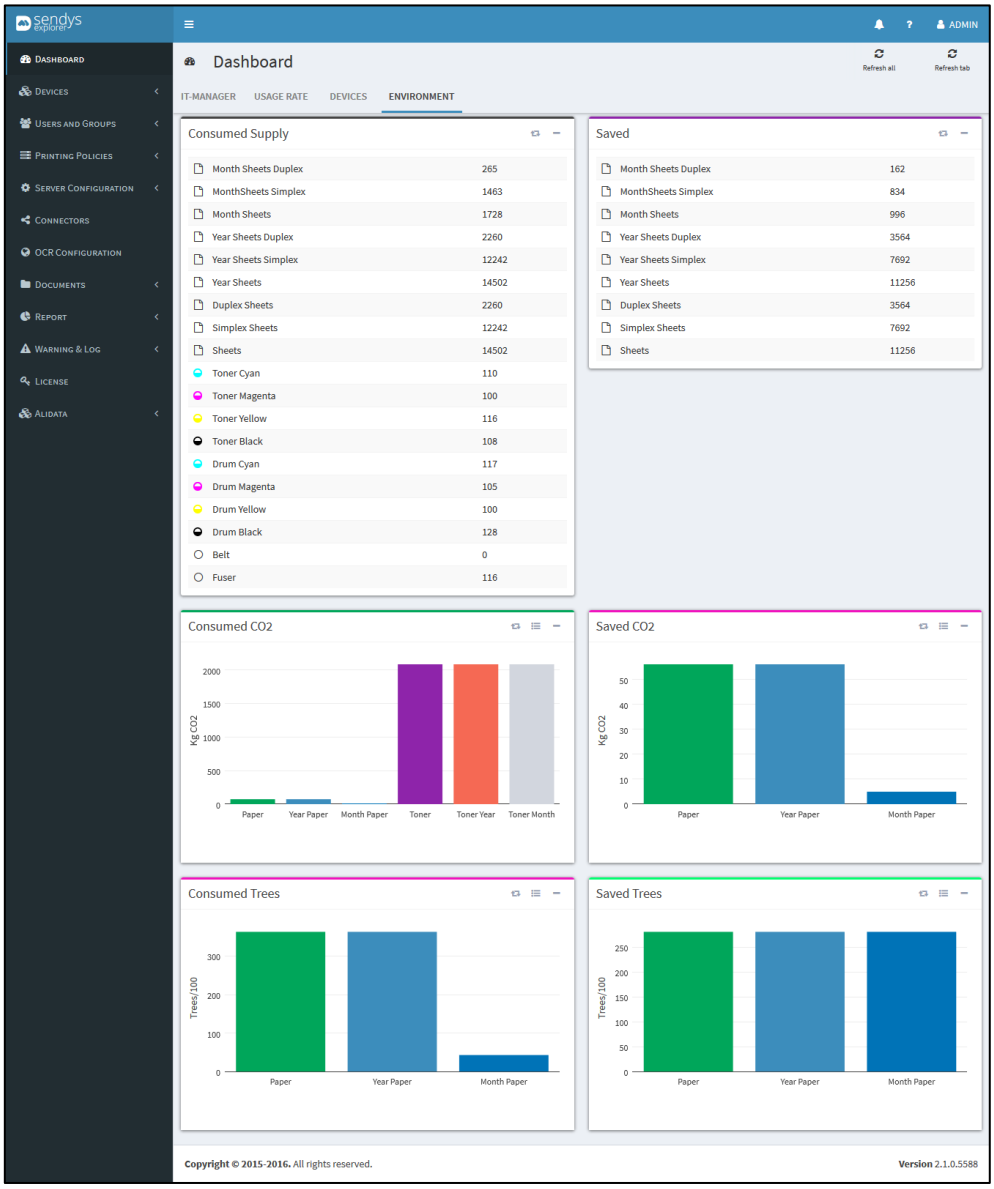


Fig. 122 - Dashboard - Environment

DEVICES

On the **Devices** Menu, all installed printers on the application and other devices can be managed.

PRINTERS/MFPS

1. Click on **Devices**.
2. Click on **Printers/MFPs**.

Printers/MFPs shows the list of printers added on SENDYS Explorer Output Manager. On these submenu, printers can be **added**, **edited** and **deleted** from Output Manager and the **Printer Page**, **Printer Details** and **Printer Queues** can be consulted.

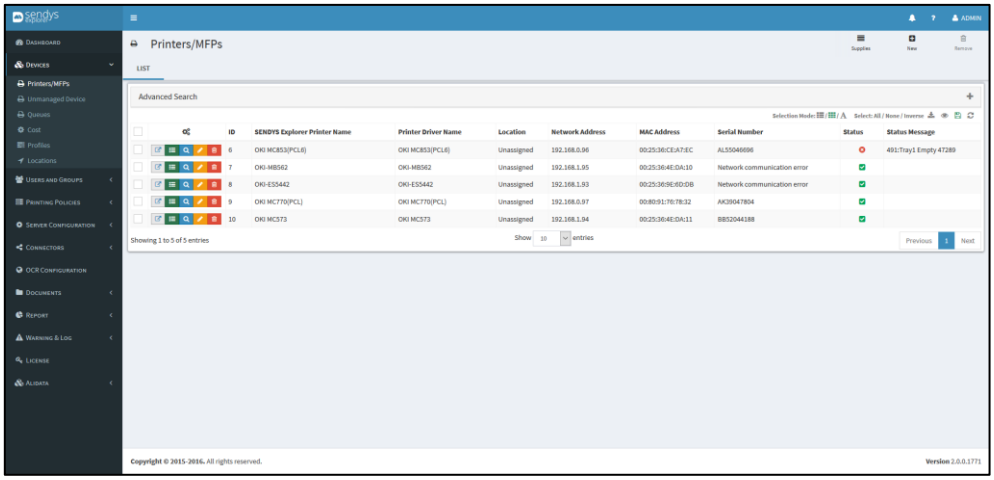


Fig. 123 - Devices - Printers/MFP's view

On this view you can consult information relative to the printers on the platform. The administrator can use this grid to monitor the printer conditions. There are fields on the grid **(Status or Status Message)** that can help detecting some issues/warnings about the printer, even the warnings created by the administrator indicating others aspects like low consumables. The next image shows an example of two situations one the printer is ok and the other indicates a warning situation (Tray2 Open).

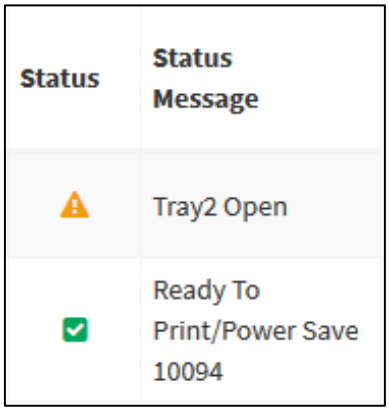


Fig. 124 - Devices - Status and Status Message fields on the grid

ADD PRINTER

ONLINE ACTIVATION

1. Click on **Devices**.
2. Click on **Printers/MFPs**.
3. Click on **New**.
4. Make the required configuration.

Name	Details
Printer	Select the printer from the server.
Output Manager	Choose printer management with Output Management, Job Accounting, Billing or only scan for SENDYS Explorer.
Create Direct Printer	Enable this option will create one Direct queue for this printer.
Setup Device	Determines if the configurations are loaded or not on the printer.
Online Activation	Enable or disable this option, depending if work with Online Activation or not.

Table 11 - Printer Add Details

5. Select "**Online activation**".

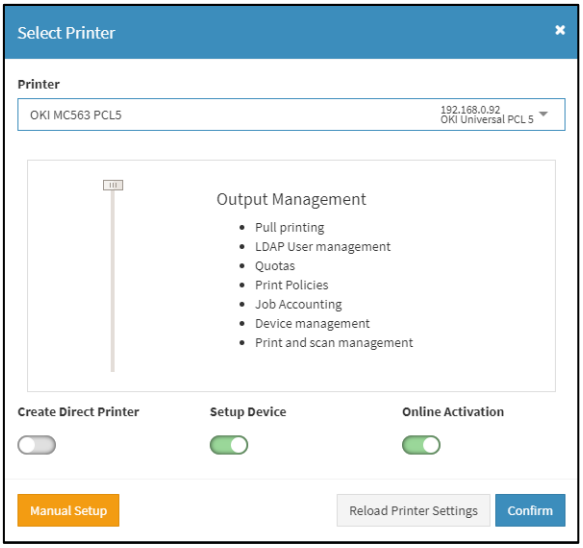


Fig. 125 - Printer Add - Online Activation

6. Click in "**Confirm**".
   Note: For online activation to work all you need is access to the internet.

OFFLINE ACTIVATION

1. Click on **Devices**.
2. Click on **Printers/MFPs**.
3. Click on **New**.
4. Make the required configuration.

Name	Details
Printer	Select the printer from the server.
Output Manager	Choose if this printer work with OM connector or only scan for SENDYS Explorer.
Create Direct Printer	Enable this option will create one Direct queue for this printer.
Setup Device	Determines if the configurations are loaded or not on the printer.
Online Activation	Enable or disable this option, depending if work with Online Activation or not.

Table 12 - Printer Add Details

5. Unselect "**Online activation**".

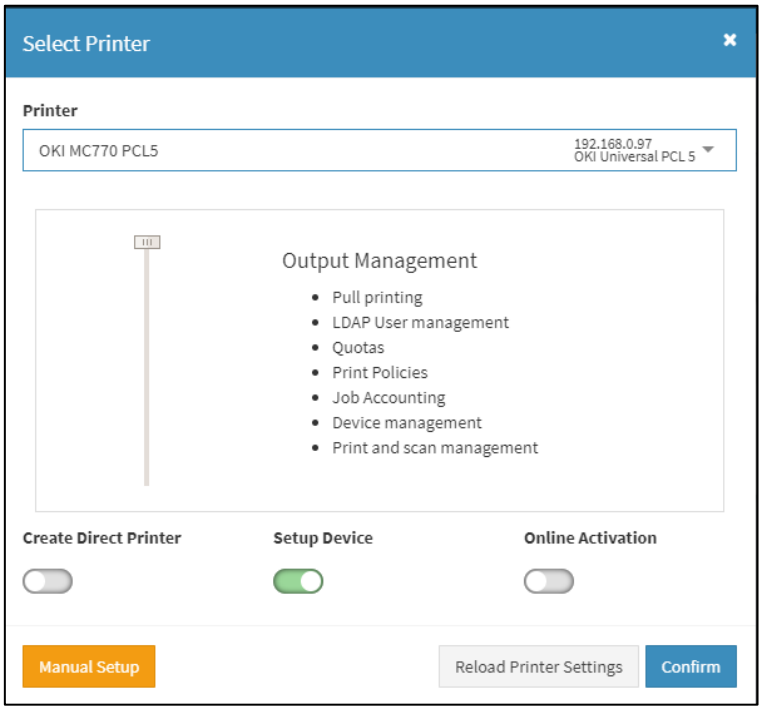


Fig. 126 - Printer Add - Offline Activation

6. Click in "**Confirm**".

7. This will create a file and will also give you a destination email
8. Click on **Offline Activation Request File** to download the created file.
9. Send the file ***xxxxxxxxx*_company_lic.txt** as email attachment to activation@sendysexplorer.com.
10. You will receive the offline activation as one attachment, download it to your server.
11. Click on **Browse** and select the downloaded **License File**.

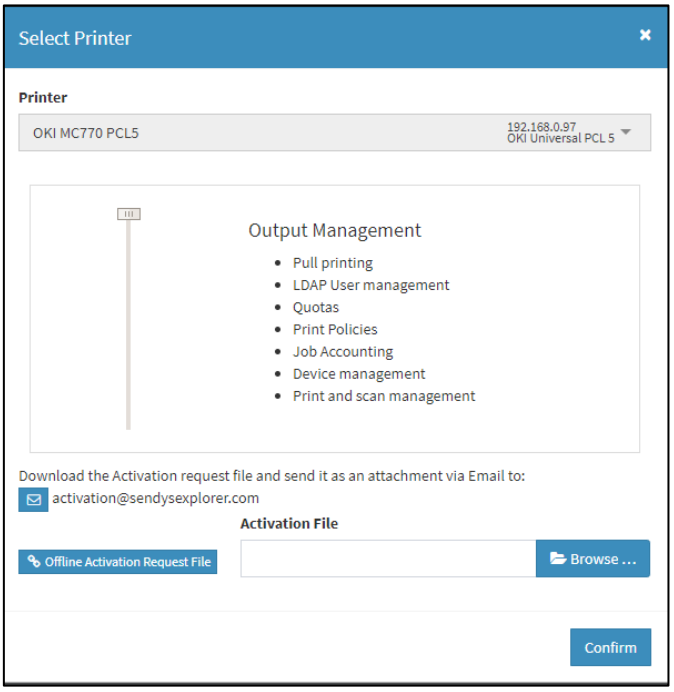


Fig. 127 - Printer Add - Offline Activation

12. Click in "**Confirm**".

PRINTER SETTINGS

In order to add the printer there are some required settings to be filled. By default, these settings are read automatically from the Device. But in case they are not read automatically, the settings will be prompt to you.

During printer ADD the **Reload Printer Settings** button will be active.

1. Click on **Reload Printer Settings** or **Confirm** for a new printer settings request.

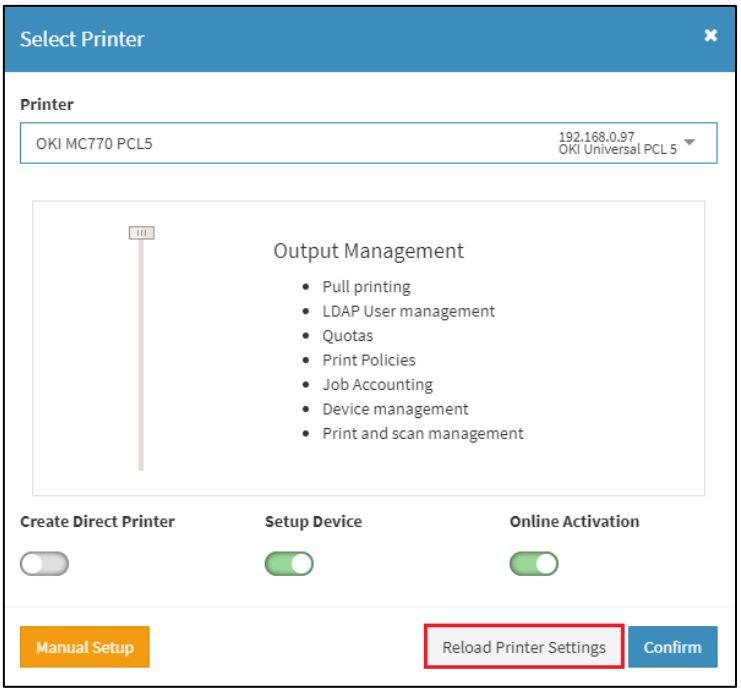


Fig. 128 - Devices - Printers/MFP's adding view

2. If the settings are correctly acquired from the printer it will be added to Output Manager.

1. In case the settings are not acquired from the printer, they need to be entered manually.
2. Make the required configuration.

Name	Details
Printer	Select the printer on the server.
MAC Address	Insert the MAC Address of the selected printer.
Device Manufacturer	Select the manufacturer on the list.
Profile	Select the printer profile from the list.
Serial Number	Insert the serial number of the printer.

Table 13 - Select Printer Details

3. Click **Confirm** to procced on add printer or **Cancel** to cancel the action.

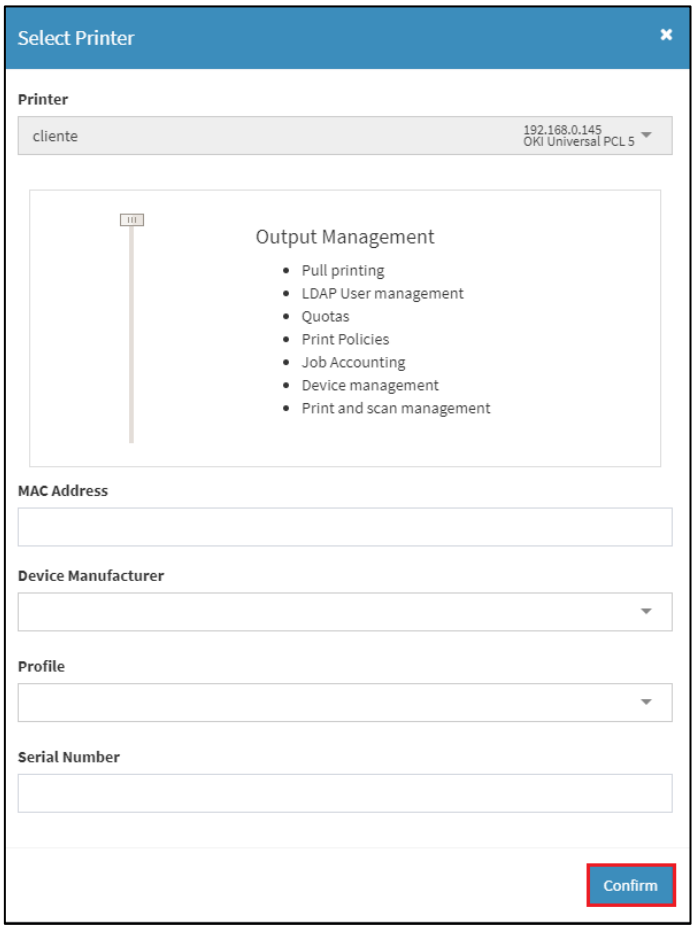


Fig. 129 - Devices - Load Profile Printers/MFP's

EDIT PRINTER

1. Click on **Devices > Printers/MFPs**.
2. Click on **pencil icon** to edit the pretended **Printer/MFP**.

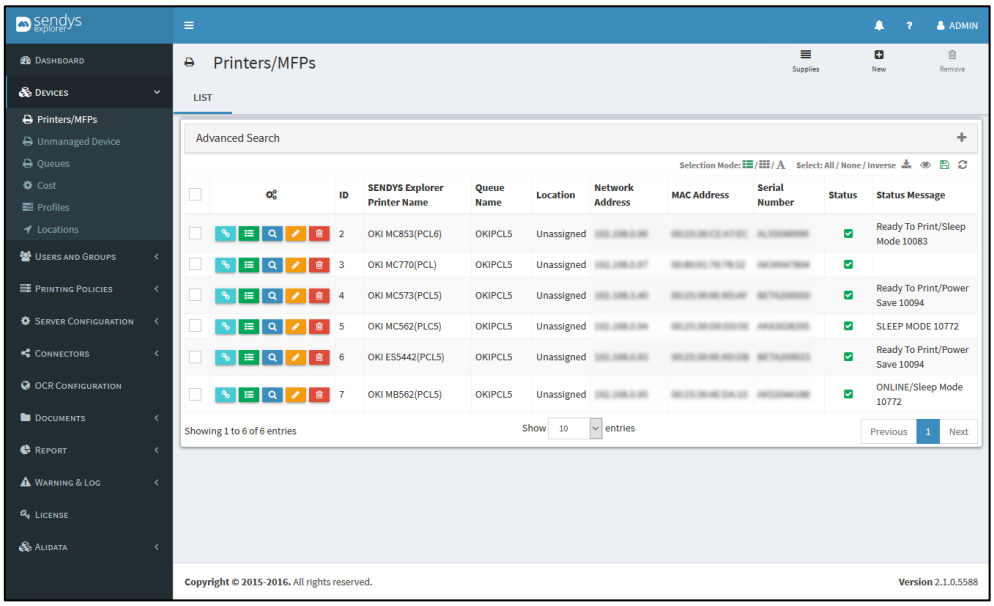


Fig. 130 - Edit Printer/MFP

3. Make the changes on Printer/MFP configuration.

Name	Details
Printer Driver Name	Printer driver name.
SENDYS Explorer Printer Name	Name of the printer displayed on Output Manager.
IP Address or Hostname	IP address or Hostname of the printer.
Queue Name	Name of the printer Queue generated
Profile	Profile selected for the printer.
Location	Insert the location for the printer.
Email	Email associated.
Default User	If is necessary to block a printer to work without an authentication. Choose a default user to block SENDYS Explorer. So the printer will have that user block on SENDYS Explorer without using authentication.
Color	Defines if the printer works with color (switch on) or not.
A3/Tabloid	Defines if printer works with A3/Tabloid option.
Google Cloud Printer Name	Defines a name for google cloud printer
Release All o LDAP login	When the login is successful, it will free the queued jobs in the spooler associated with that user.
Unlock Printer	This options is only able for the MFP printer type and it is used to unlock the printer directly from the control server by the administrator.
Lock Printer	This options is only able for the MFP printer type and it is used to lock the printer directly from the control server by the administrator.
Enable Remote View	Enable the option to make remote view on the printer. That button, on the printer, will send a hard-link to the control server, so the admin can use it so load the printer screen on the browser and see the information associated with that printer.

Table 14 - Edit Printer options

4. You can also click on **Setup Device** to re configure the Device and send those configurations to the selected printer.
5. Click **Save** to save the Printer/MFP changes.

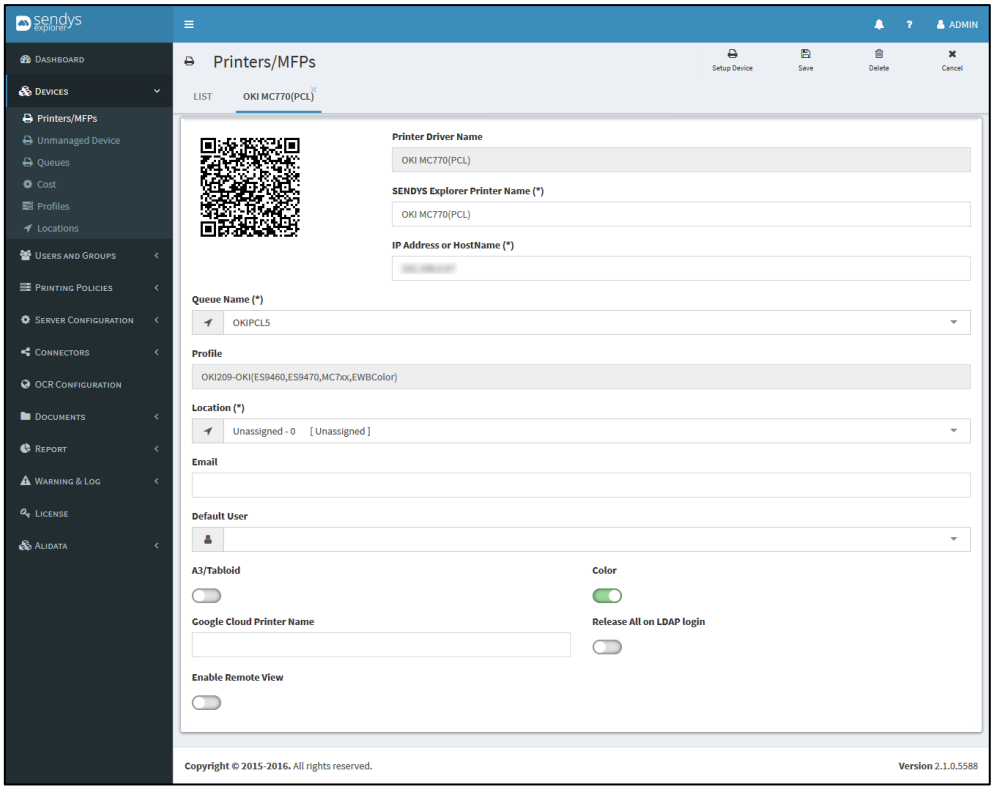


Fig. 131 - Edit Printer/MFP

PRINTER QUEUES

1. Click on **Devices > Printers/MFPs**.
2. Click on **view queue icon** to view the list of queues associated with this **Printer/MFP**.

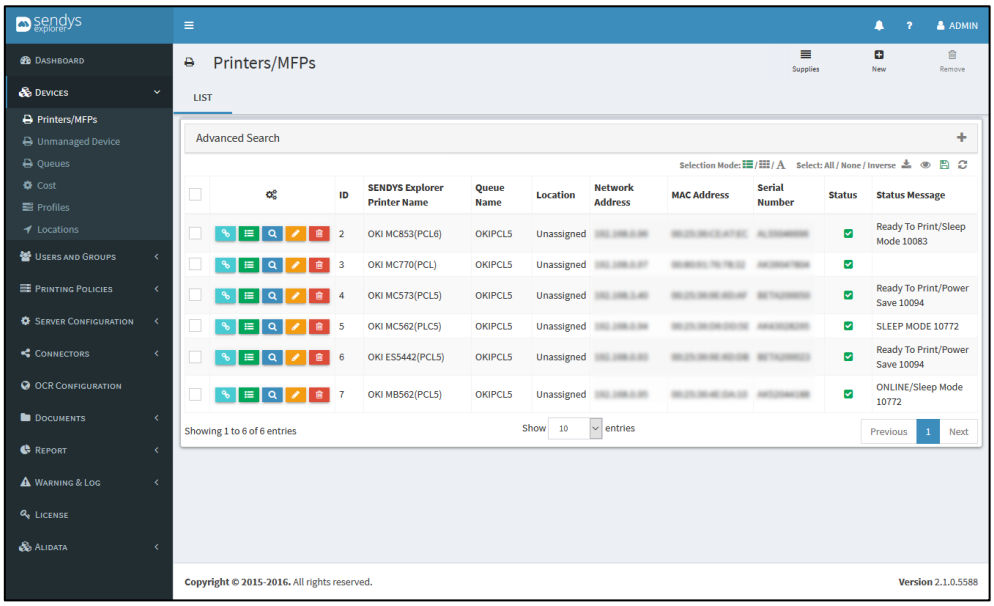


Fig. 132 - Printer/MFP Queue

Here jobs associated with the printer can be managed individually or with a selection by the buttons **Pause/Start**, **Cancel**, **Cancel All Jobs** buttons.

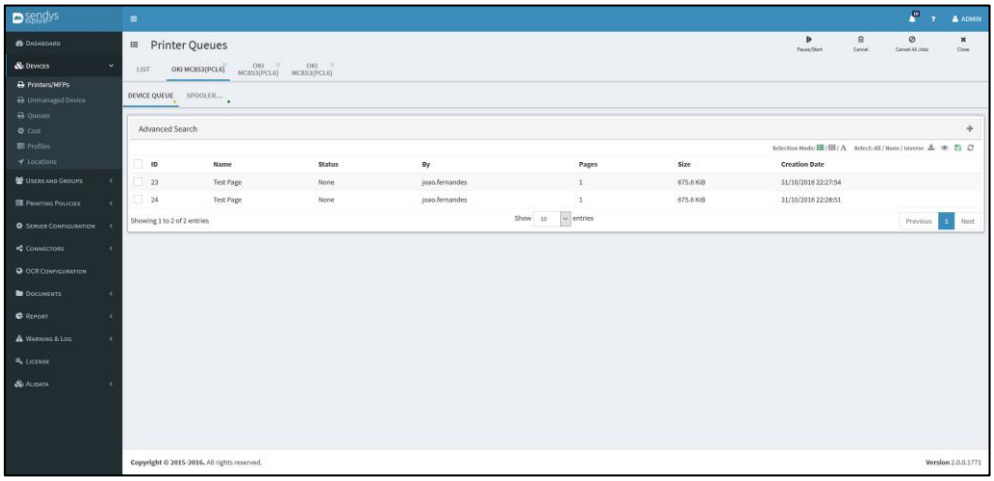


Fig. 133 - Devices - Printers/MFP's - Printer Queue

The Device Queue view represents the same option when consulting documents in queue on a printer using Windows Operating System.

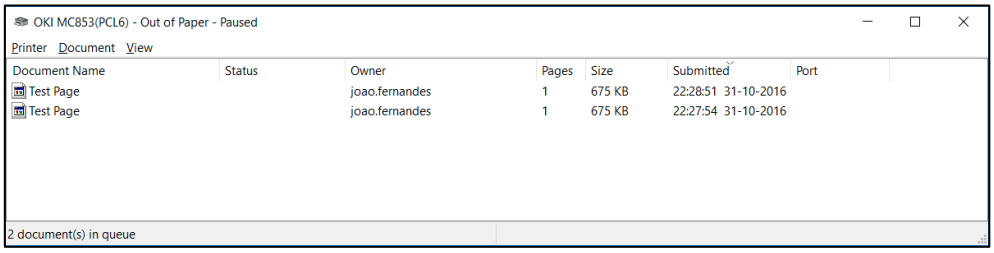


Fig. 134 - Devices - Windows Printer Queue

At the same time Spooler Queue view indicates the document on the spooler in queue at the moment and, like the last one, it represents the same view as the Windows Operating System that can be consulted.

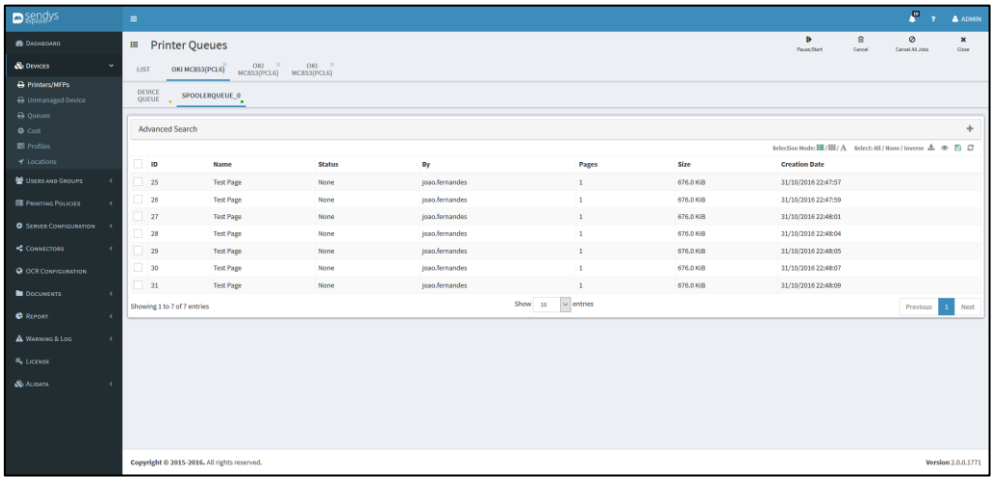


Fig. 135 - Devices - Printers/MFP's - Printer Queue

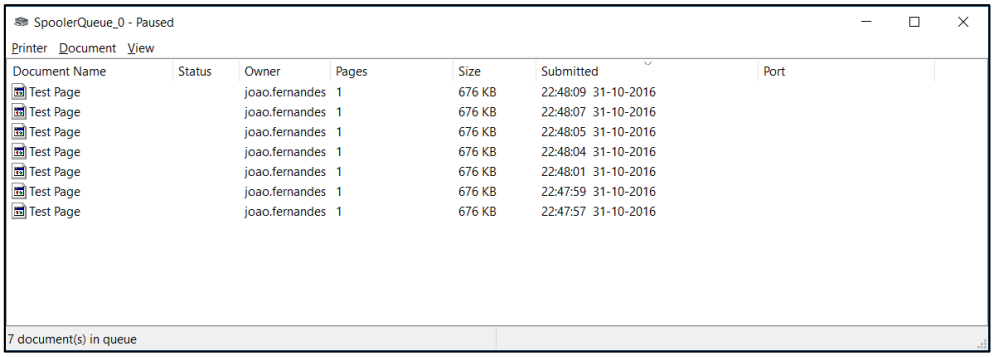


Fig. 136 - Devices - Windows Spooler Queue

PRINTER DETAILS

1. Click on **Devices > Printers/MFPs**.
2. Click on **printer details icon** to view the details of the selected **Printer/MFP**.

The **Printer Details** button shows more information related with the selected printer.

- **Information tab** shows the information of the selected printer.

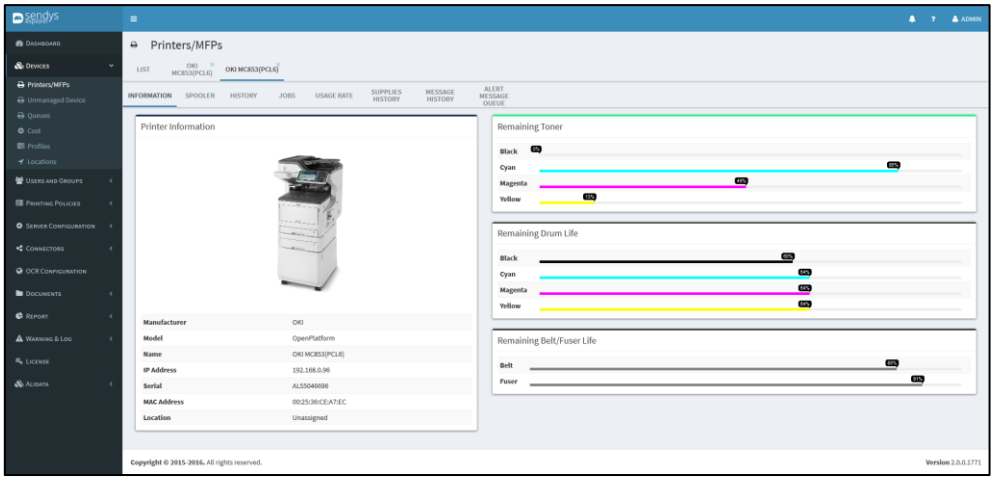


Fig. 137 - Devices - Printers/MFP's - Printer Details - Information tab

- **Spooler tab** shows the actual spooler jobs associated to the selected printer.

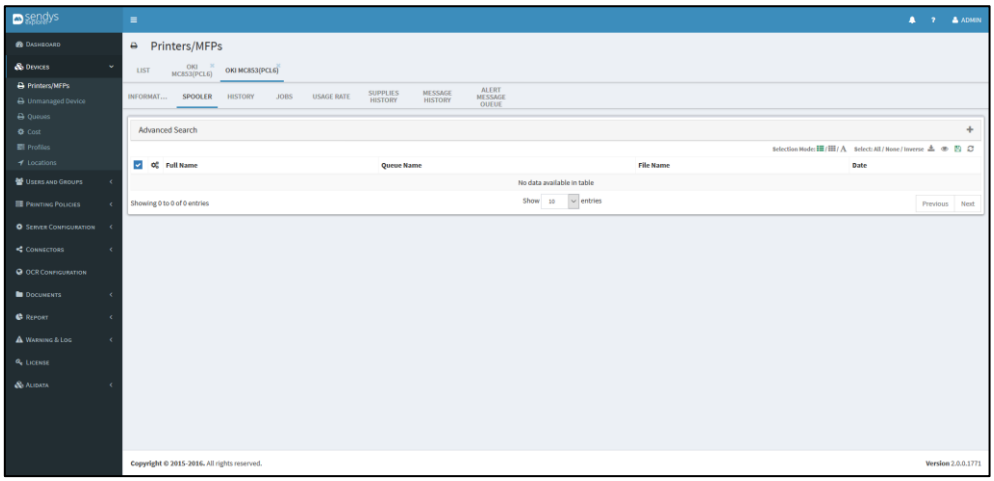


Fig. 138 - Device - Printers/MFP's - Printer Details - Spooler tab

- **History tab** shows the all the interaction between printer and user on the selected printer.

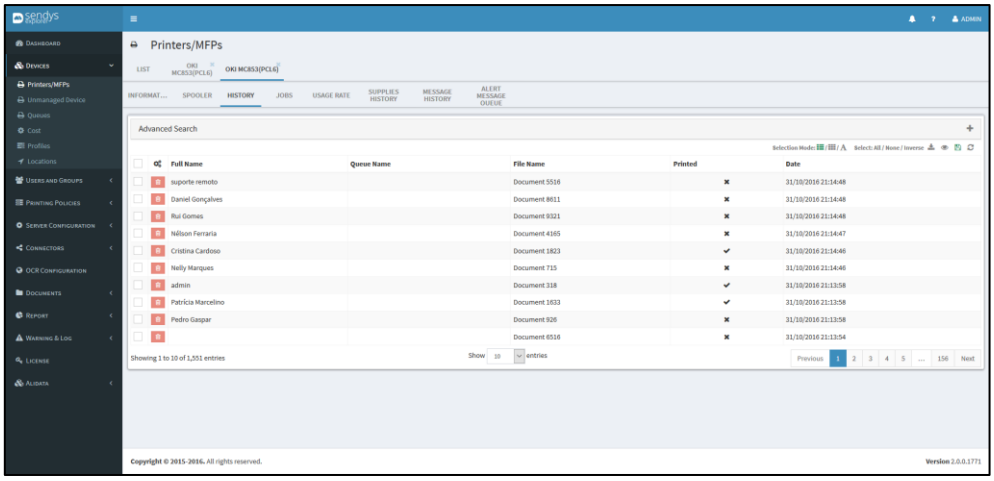


Fig. 139 - Device - Printers/MFP's - Printer Details - History tab

- **Jobs tab** shows all jobs submitted to the selected printer.

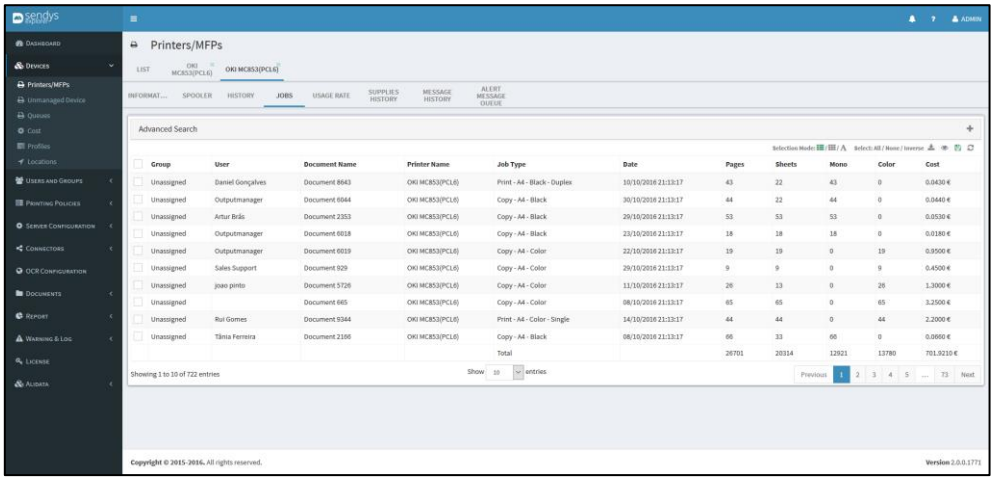


Fig. 140 - Device - Printers/MFP's - Printer Details - Jobs tab

- **Usage Rate tab** shows counters associated with the selected printer.

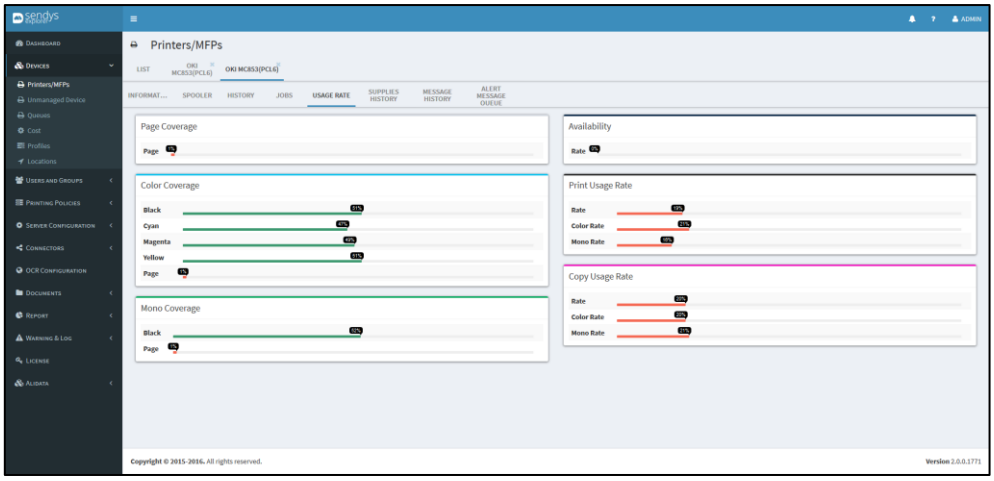


Fig. 141 - Device - Printers/MFP's - Printer Details - Usage rate tab

- **Supplies History tab** shows all consumables counter/statistics associated with the selected printer.

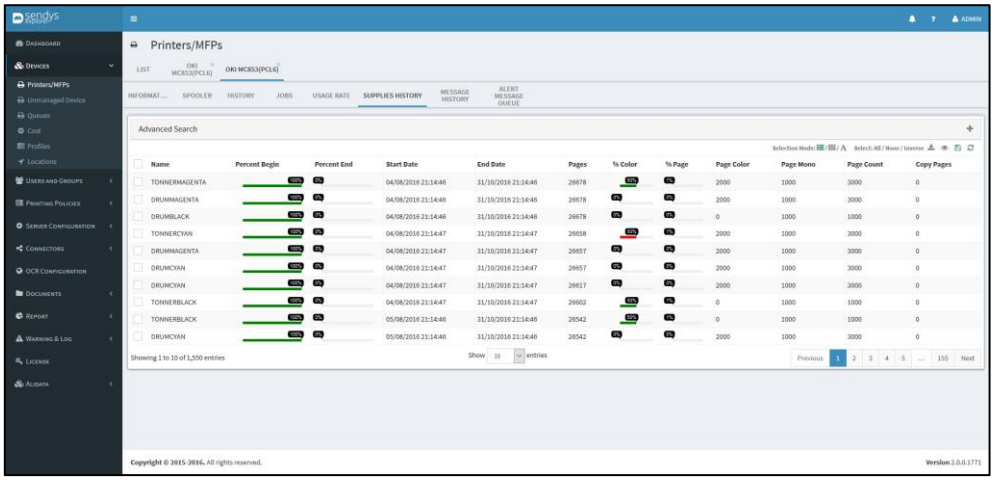


Fig. 142 - Device - Printers/MFP's - Printer Details - Supplies History tab

- **Counters tab** shows all counter reads on the selected printer

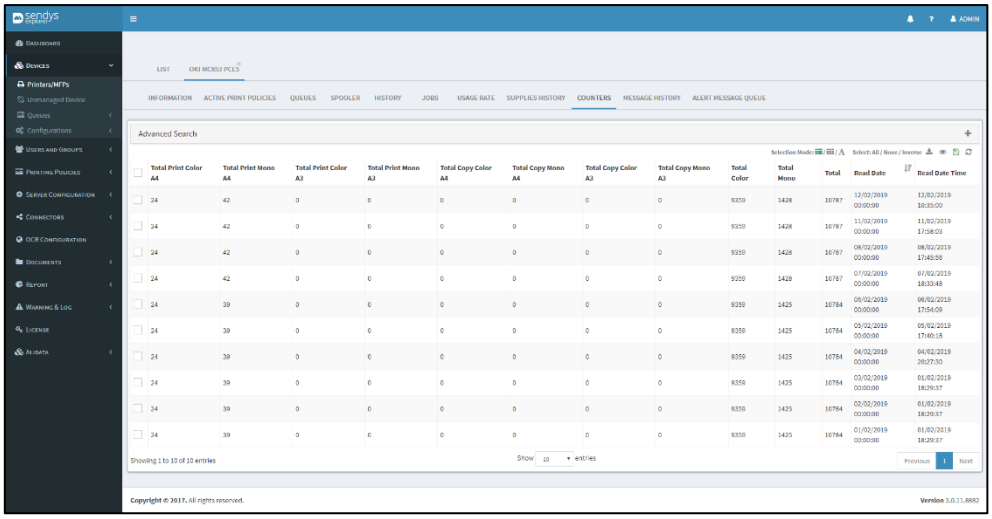


Fig. 143 - Device - Printers/MFP's - Printer Details –Counters tab

- **Message History tab** shows all messages related with the selected printer.

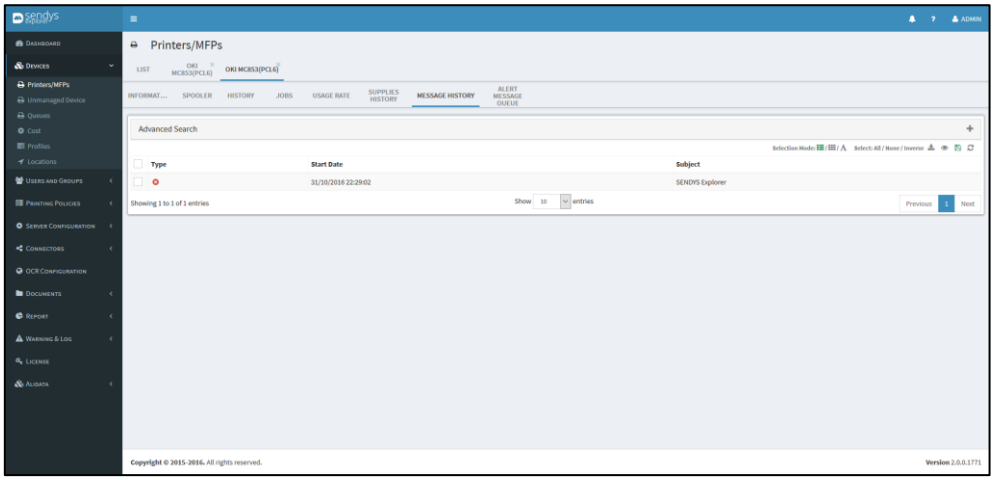


Fig. 144 - Device - Printers/MFP's - Printer Details –Message History tab

- **Alert Message Queue tab** shows all the alert messages associated with the selected printer.

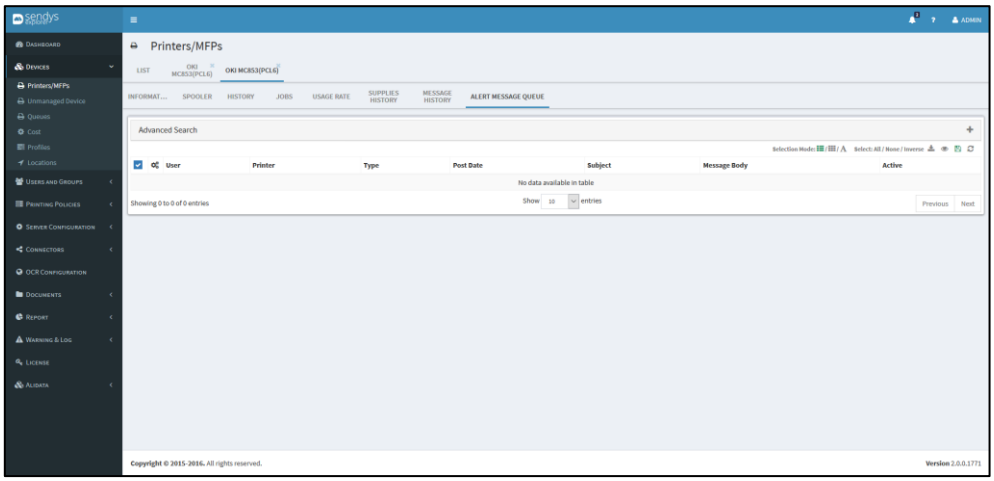


Fig. 145 - Device - Printers/MFP's - Printer Details - Alert Message Queue tab

SUPPLIES

1. Click on **Devices**.
2. Click on **Supplies**.

This will present one view with the list of all printers that indicates the details of **supplies** of each printer.

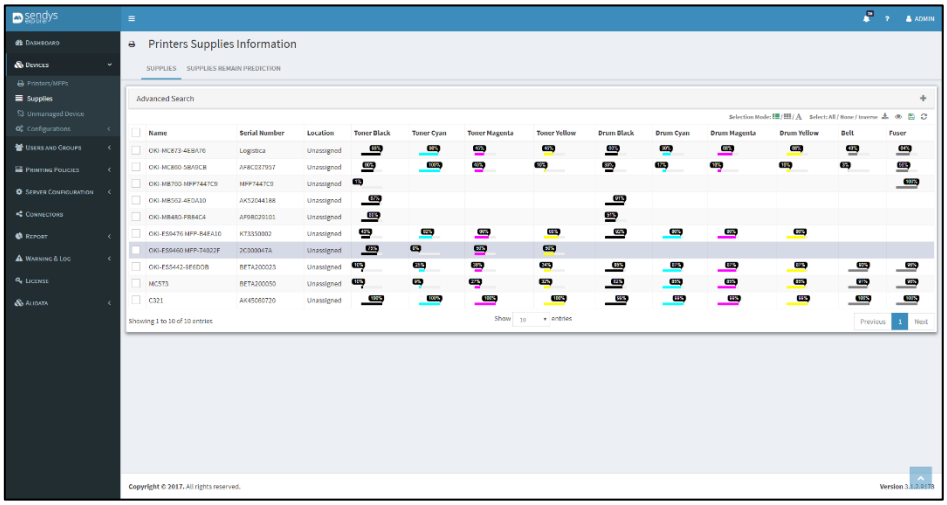


Fig. 146 - Devices - Supplies Supplies view

SUPPLIES REMAIN PREDICTION

1. Click on **Devices**.
2. Click on **Supplies** and then select the **Supplies Remain Prediction**.

This will present one grid with all printers that indicates the details of **supplies** with the remaining days prediction that the supplies have and predicted end date of each printer.

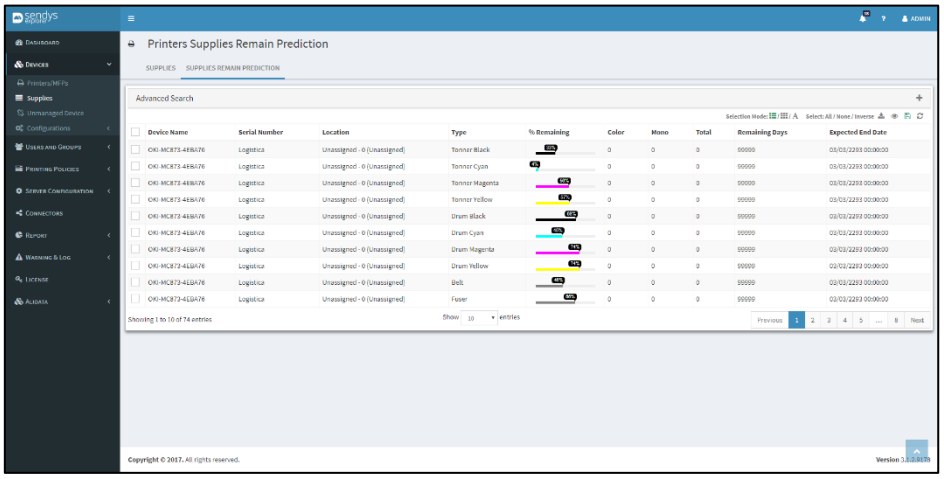


Fig. 147 - Devices - Supplies Supplies Remain Prediction Grid

UNMANAGED DEVICES

1. Click on **Devices**.
2. Click on **Unmanaged Devices**.

This view represents the list of installed printers on the server but not added on SENDYS Explorer Output Manager. This grants the possibility to have some information about those printers.

Printers from the server can be added to the list automatically by clicking on **Reload System Printers** button.

The **Add Printer** button allow you to add the selected printer on Output Manager and the **Remove** option to remove printers. The same options to add printer are showed on this option and works on the same way as the previous chapter.

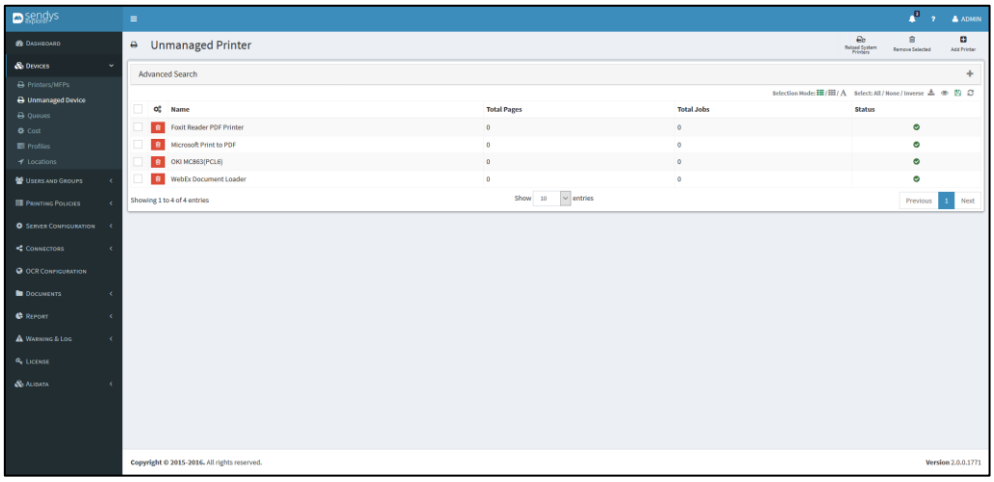


Fig. 148 - Devices - Unmanaged Device view

QUEUES

QUEUES

1. Click on **Devices**.
2. Click on **Queues**.

This view represents Windows Queues and it is used to configure and manage the Queues added by the Output Manager too. Queues can be added, edited or deleted as the necessity.

The options **Pause/Start**, **Cancel** and **Cancel All Jobs** are used for managing the spooler service.

This view represents Windows Spooler Queues and it is used to configure and manage the Spoolers added by the Output Manager too. Queues can be added, edited or deleted as the necessity.

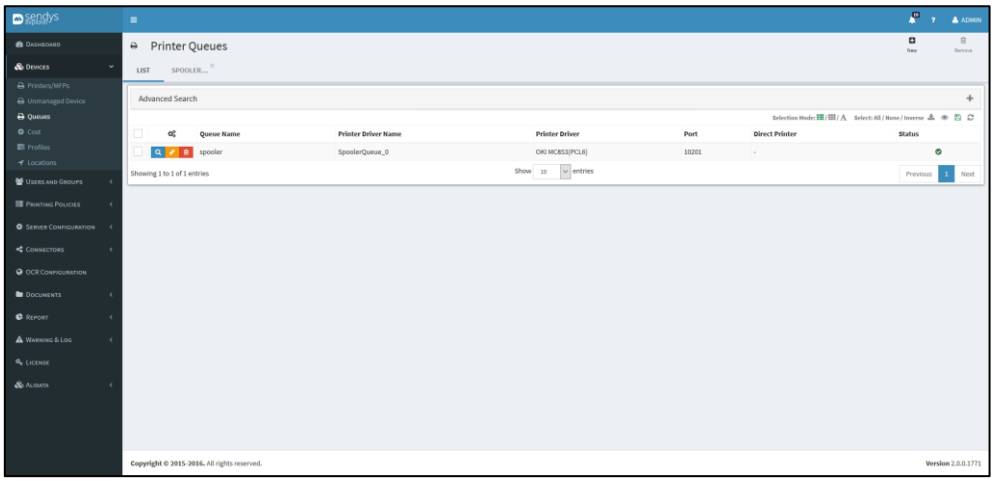


Fig. 149 - Printer Queue List

The administrator can consult the status of each queue and other information.

ADD/EDIT QUEUE

1. Click on **New** to add a new queue or **pencil icon** to edit an existent queue.

The new Queue will be added on Windows Operating System too and the configurations depends on the next table.

Name	Details
Printer Diver Name	Insert a printer driver name for the windows.
Queue Name	Insert a name for the queue name to work on the platform.
SENDYS Explorer Printer Name	Select a specific printer to turn this spooler queue as a direct spooler for the selected printer.
Printer Driver	Select the specific printer driver to use.
Enforce Mono Rule	Select a rule to force this spooler to work with it.
Print Job Convert to Duplex	Select a rule to force this spooler to work with it.

Table 15 - Printer Queue Add/Edit Queue configurations

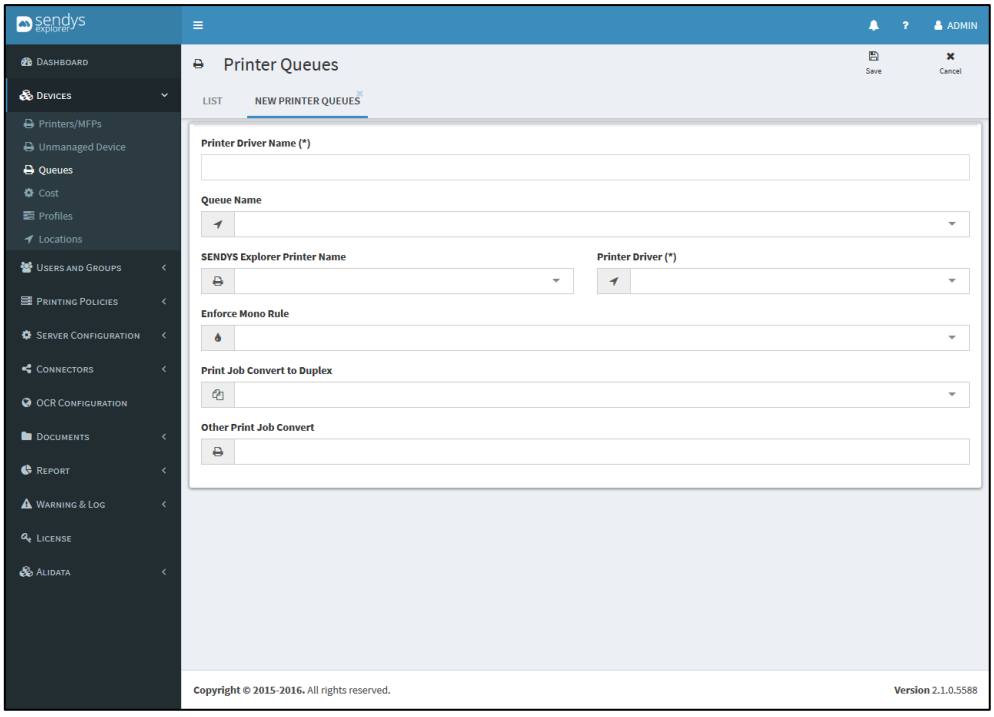


Fig. 150 - Devices - Queues - adding or editing queue view

VIEW QUEUE

Clicking on **Open Queue** button shows the list of documents and information associated to the queue selected. The options **Pause/Start**, **Cancel** and **Cancel All Jobs** are used for managing the spooler service.

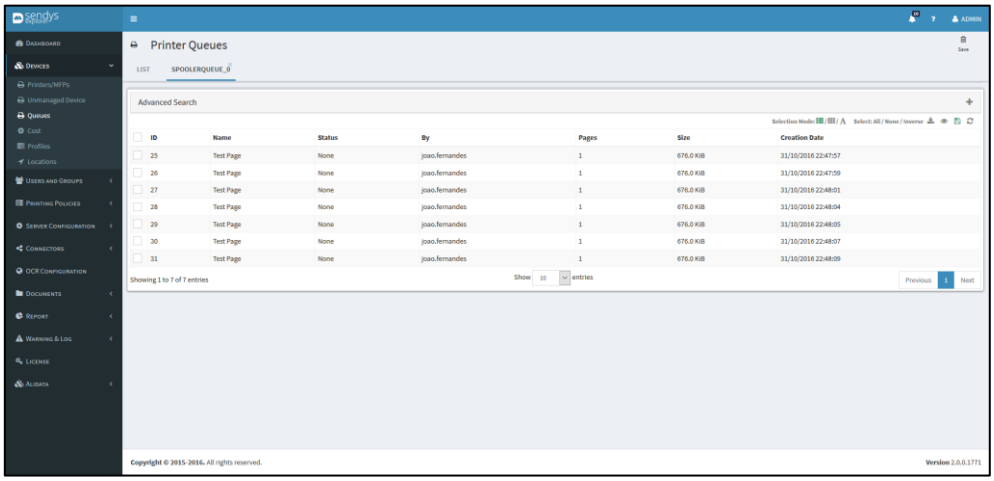


Fig. 151 - Devices - Queue - List of jobs on queue

The view before it is the same as the Spooler queue that is stored on Windows Operating System.

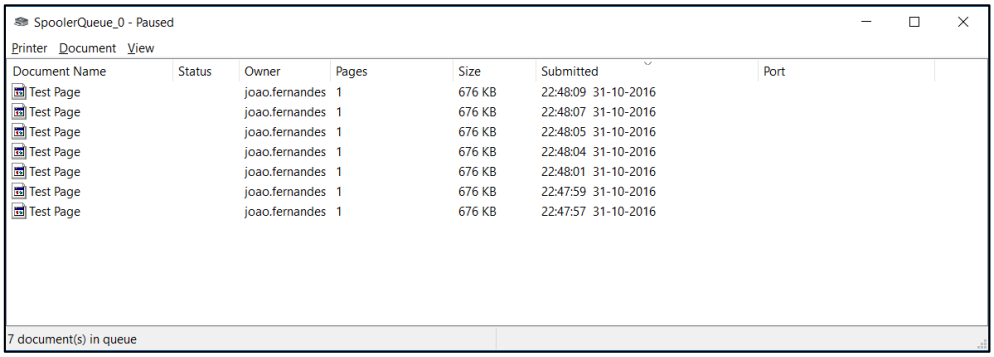


Fig. 152 - Windows Spooling document window

MAP PRINTERS-SPOOLER QUEUES

This is an easy way to make the mapping of spooler queues to devices, spooler queues and device compliance are defined by queue name, and on this section you have an easy view and way to define and specify device queue compliance.

1. Click on Devices>Map-Printers Spooler Queues
2. Select the devices on left side
3. Select the compliant queues name on the right
4. Click save

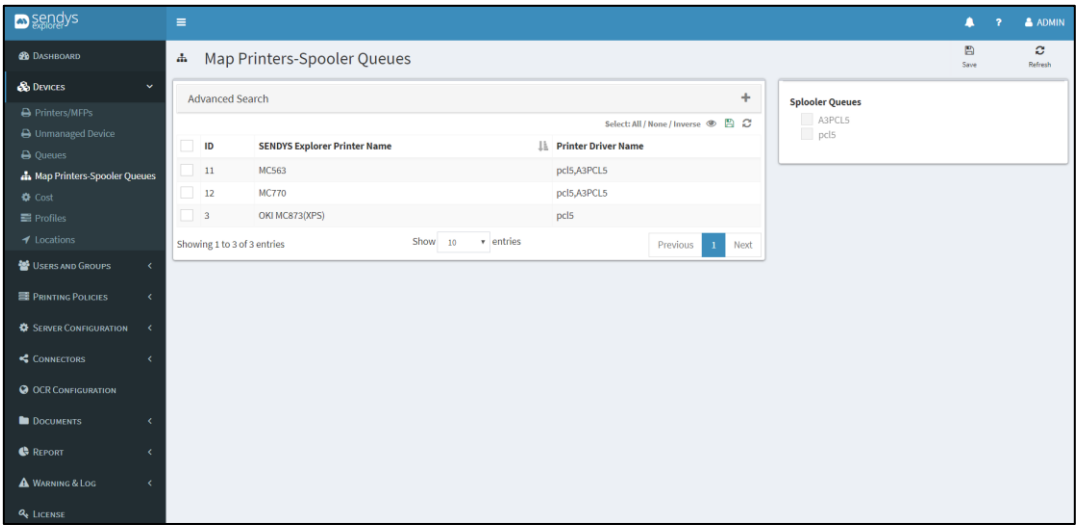


Fig. 153 - Printer Queue Mapping.

PRINTER QUEUE DRIVER MAP

When using multi-port on the queues we need to pick the information not only from windows but also from the driver header, to do that we need to extract the information from job header.

When a print job is submitted for the first time with a specific driver the system creates an entry on this section with the driver name and administrator needs to map expression to fields as explain on the above the edition tab. If this map is not done properly we can have mix user job's.

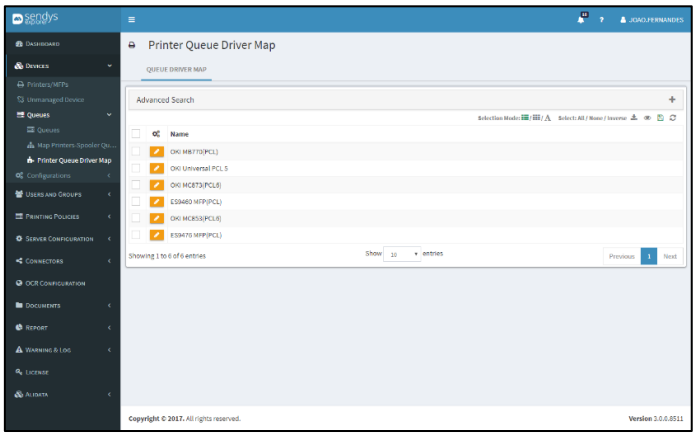


Fig. 154 - Printer Queue Driver Map.

EDIT

To edit the driver mapping properties:

1. Click on **Devices**
2. Click on **Queues**
3. Click on **Printer Queue Driver Map**
4. Click on the pencil with the specific driver name
5. Edit the expression as explain about the edition tab
6. Click on save

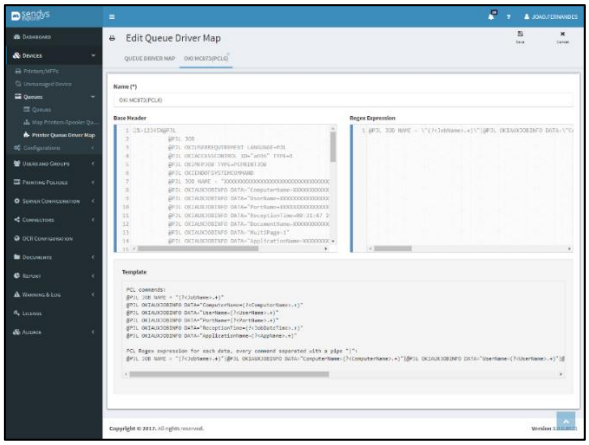


Fig. 155 - Printer Queue Driver Map edit.

CONFIGURATIONS

COST

1. Click on **Devices** menu.
2. Click on **Cost** menu

On this view, costs by printer can be managed.

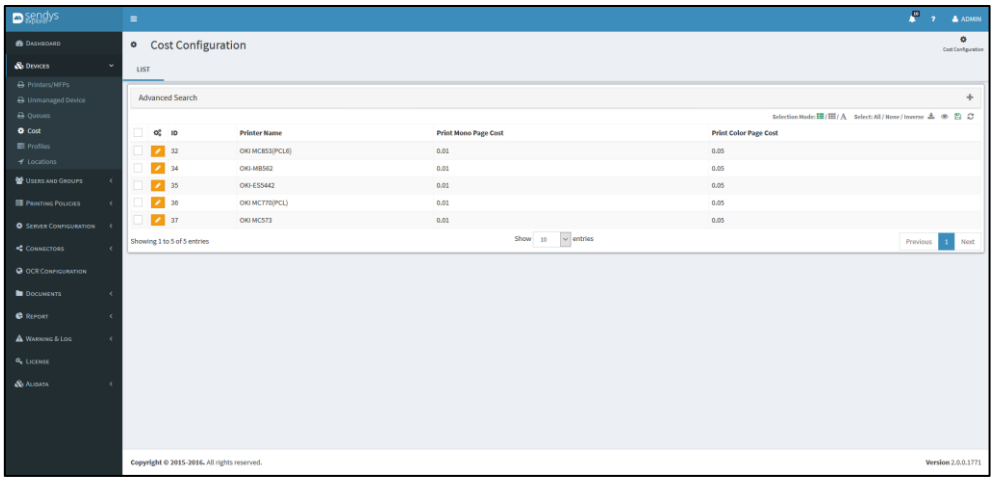


Fig. 156 - Devices Cost

On **Cost Configuration** button we can update the cost for one or more profiles and procced on **Update Cost** button to save or **Cancel** to cancel.

Edit button open a view to configure the cost of the printer selected and procced on **Save** button to save the alterations or **Cancel** to cancel.

On both views sheet and page cost can be defined and all the print, scan, fax and copy jobs (color and mono) cost can be defined.

PROFILES

1. Click on **Devices** menu.
2. Click on **Profiles** menu

View profiles shows the printer profiles existed on SENDYS Explorer Output Manager.

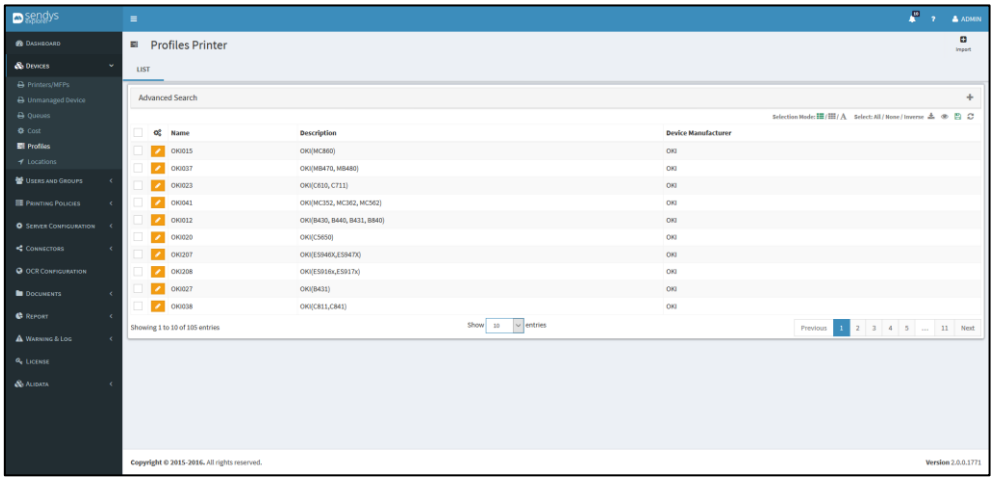


Fig. 157 - Devices - Profiles view

EDIT PROFILE

1. Click on **Edit** button to edit an existent profile

Edit button shows the next view where the configurations can be changed.

The next table shows the configurations that are always configured automatically and many fields are not possibly to change. These fields can be only change if they were cloned.

To clone a profile, select the printer profile and click on **Clone** button. On this option the configurations can be changed.

Note: It is not recommended to change these values if you don't know the specifications needed.

On the **Details** tab:

Name	Details
Name	Name of the profile selected.
Manufacturer	Name of the manufacturer.
Technology	Device type.
Model	Printer models.
Description	Description.
Picture Name	Url for the image of the printer profile.
Printer Driver Name	Printer driver name.
Printer Type Name	Printer type name.
Work Mode	Work mode.

Table 16 - Printer Details

Note: The others tabs on this sections are specific actions that are blocked and not recommended to change even on copying the profile unless the administrator knows the specifications.

Click **Save** to save the changes or **Cancel** to cancel the edit profile.

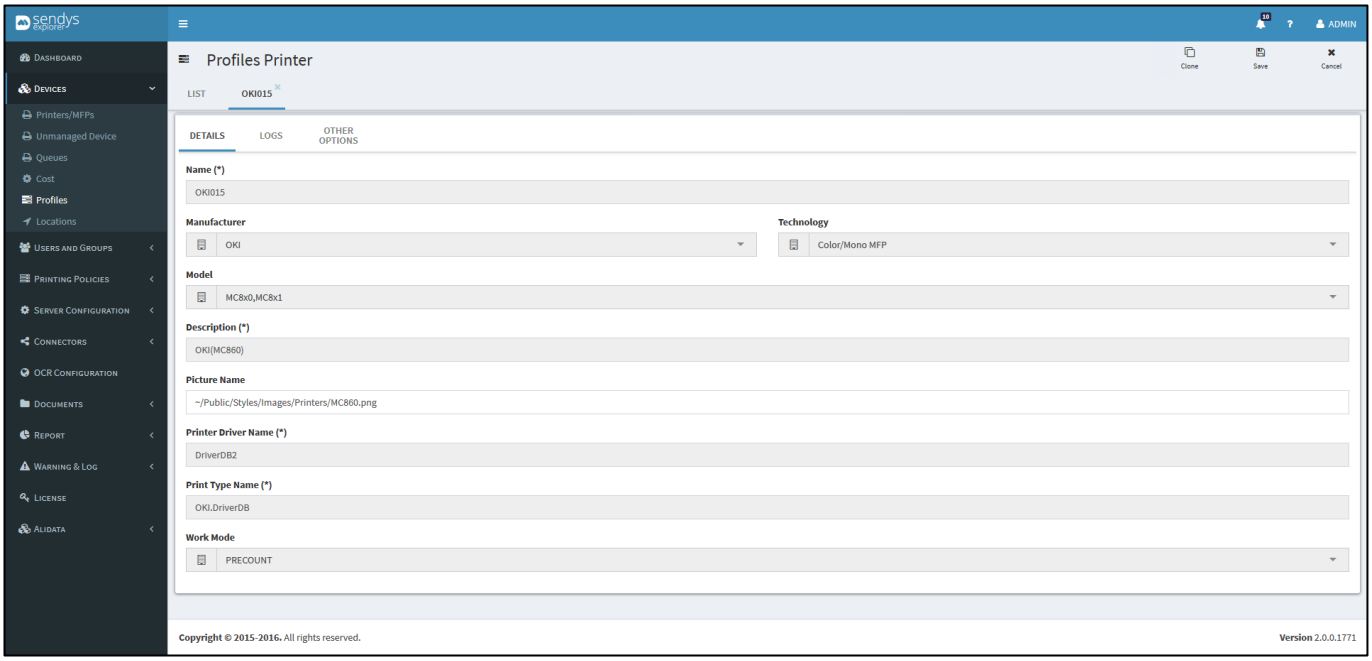


Fig. 158 - Devices - Profile - Editing

IMPORT PROFILE

1. Click on button **Import** to import an **XML file** to add a new printer profile.
2. **Browse** the file.
3. Click on **Upload** to confirm or **Remove** to clear the file.

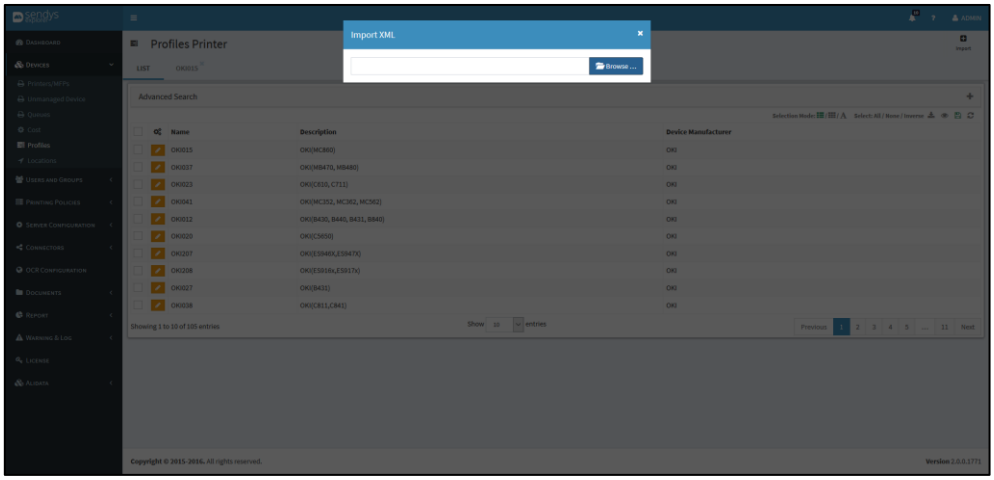


Fig. 159 - Devices - Profiles - Importing printer profile

PROFILE CONFIGURATION

Profile configurations is a section for advanced users only, in this section users can define PJL commands that will be used on Configuration rules and will be doing device configurations.

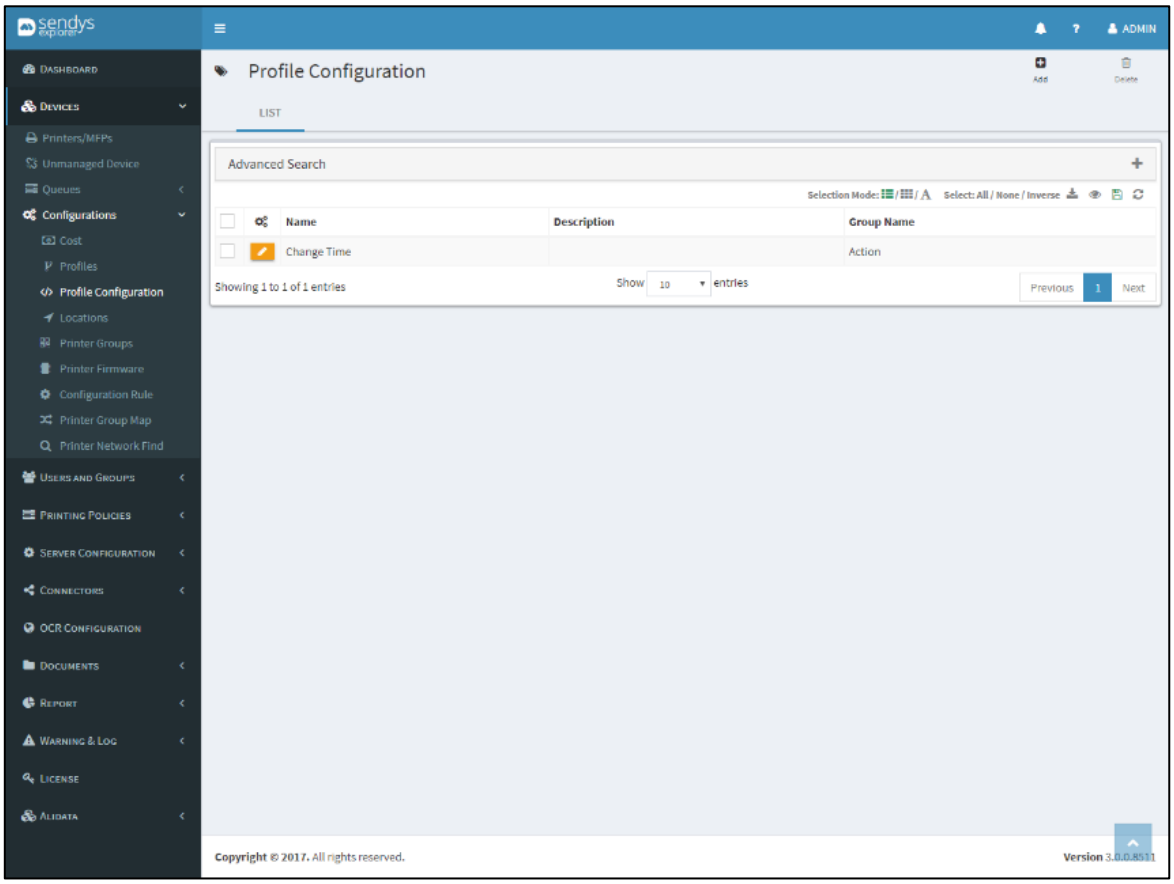


Fig. 160 - Devices - Locations view

ADD/EDIT

1. Click on **Devices**
2. Click on **Configurations**
3. Click on **Profile Configuration**
4. Click on **Add** to add a new profile configuration or **pencil icon** to edit an existent.

The new profile configuration will be added, and you can use it on Configuration rules section, assign the proper device types since all commands needs to be compliant with the device type.

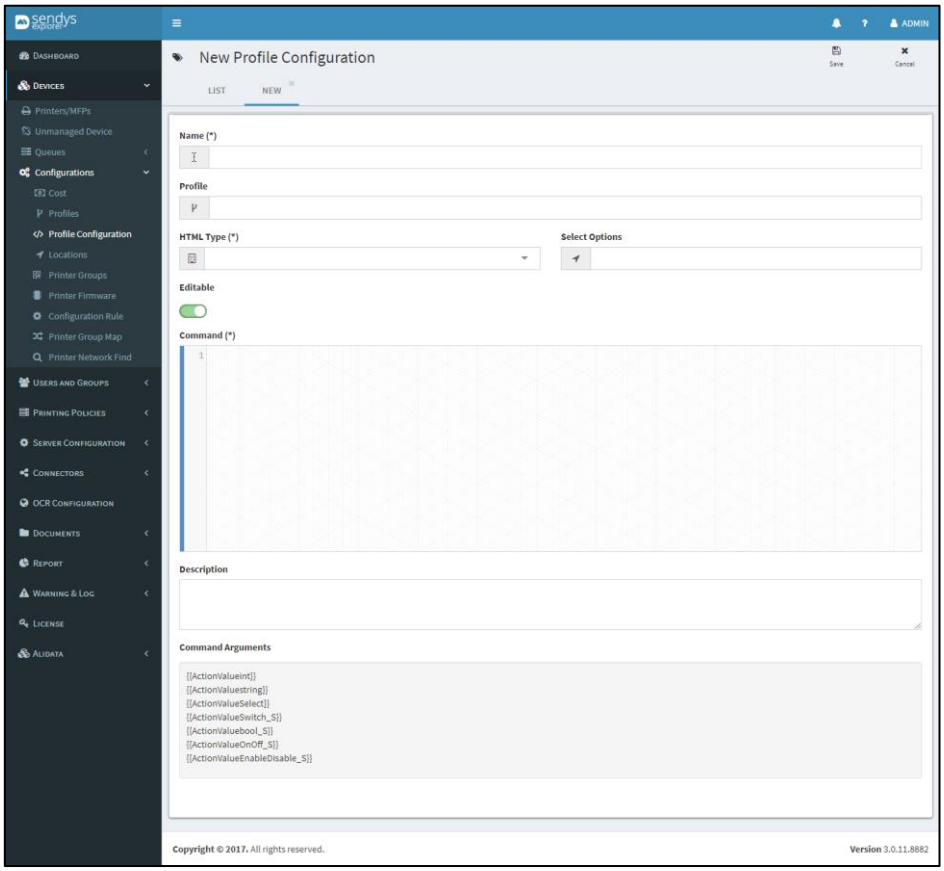


Fig. 161 - Devices - Locations view

LOCATIONS

1. Click on **Devices** menu.
2. Click on **Locations** tab.

This view is used to manage the printer locations.

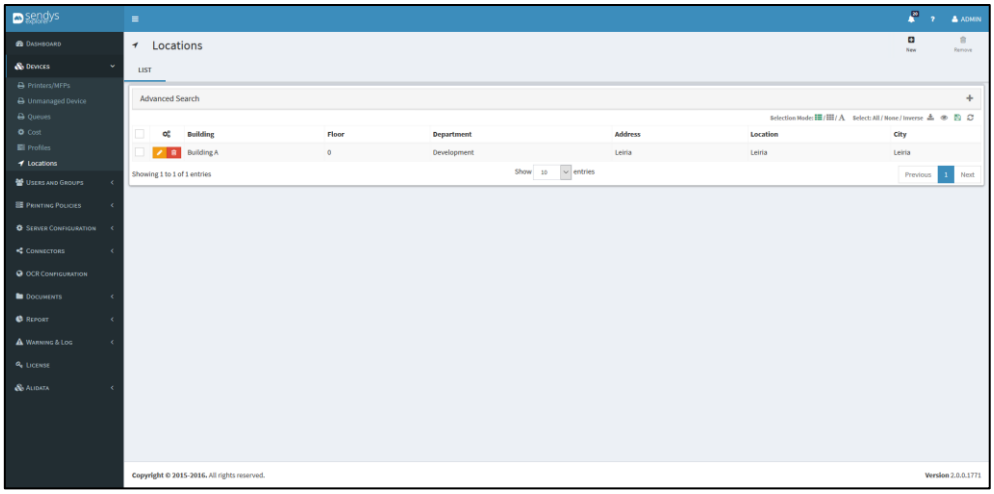


Fig. 162 - Devices - Locations view

ADD/EDIT LOCATION

1. Click on **New** menu.
2. Make the required configuration.

Name	Details
Building	Printer building name.
Floor	Printer building floor.
Department	Printer building department.
Location	Printer building location.
City	Printer building city.
Location	Printer building location.
Country	Printer building country.
Postal Code	Printer building postal code.
Address	Printer building address.

Table 17 - Locations Details

3. Click **Save** to save the changes or **Cancel** to cancel.

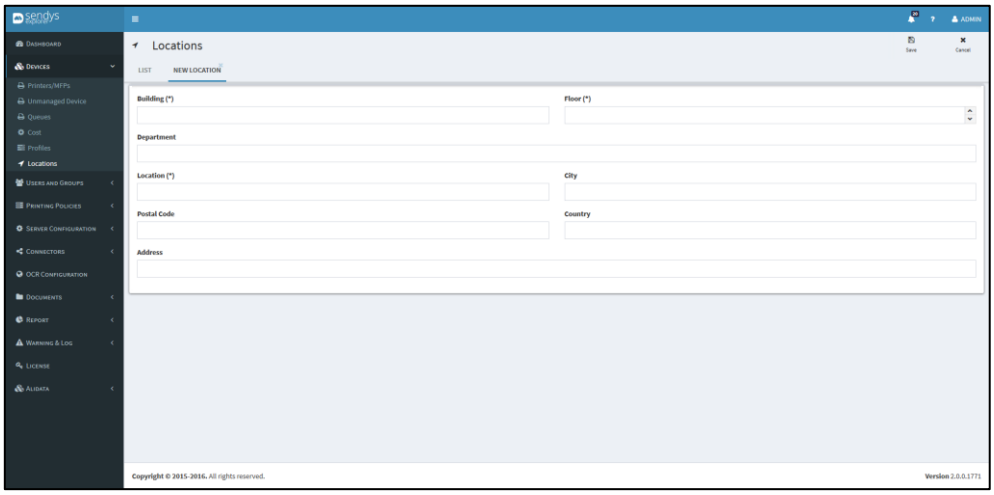


Fig. 163 - Devices - Locations - Adding location

PRINTER- LOCATION MAPPING

This is an easy way to make the mapping of devices to locations.

1. Click on **Configurations**>**Locations**>**Location Mapping**
2. Select the devices on left side
3. Select the location on the right
4. Click save

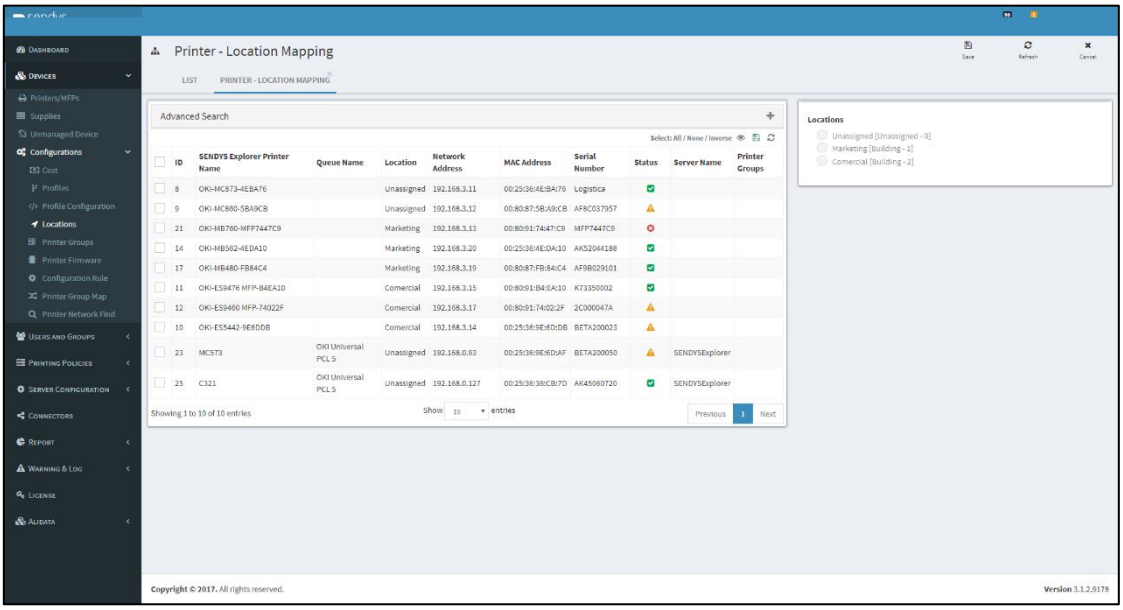


Fig. 164 - Printer Location Mapping.

PRINTER GROUPS

Create groups of devices to assign configuration rules, this will make easy the assign of configuration rules and also the printer network find.

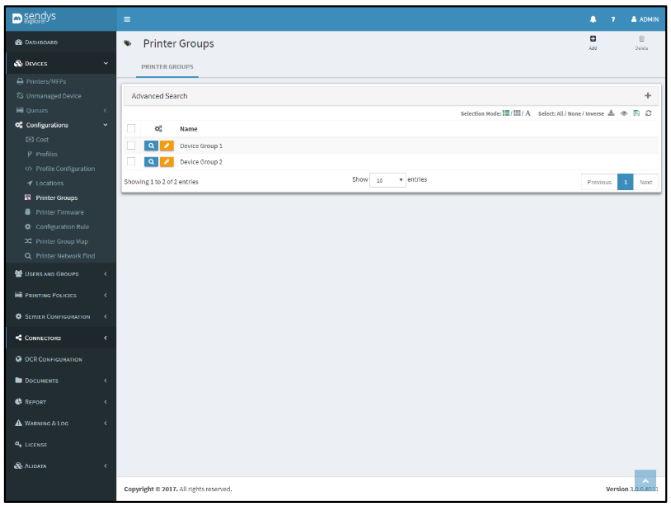


Fig. 165 – Printer Group View.

ADD/EDIT

1. Click on **Devices**
2. Click on **Configurations**
3. Click on **Printer Groups**
4. Click on **Add** to add a new Printer Group or **pencil icon** to edit an existent.
5. Edit or type a new group name

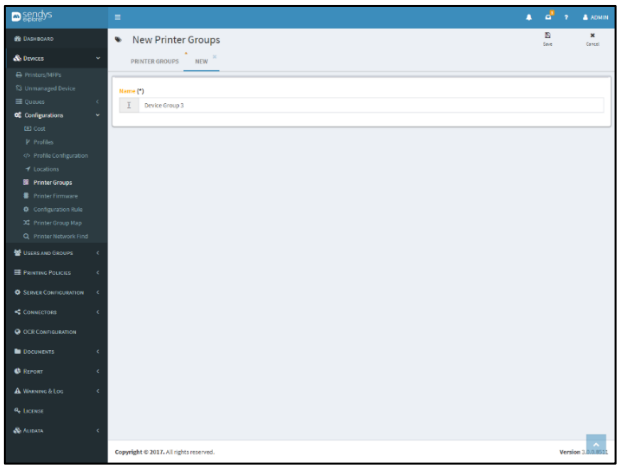


Fig. 166 - Printer Group Edit.

PRINTER FIRMWARE

Printer firmware section provides a way to make firmware update on OKI devices, on this section user needs to submit the firmware, assign a device type upload the firmware and then create a task for firmware update or force the update now.

To Upload/Insert a new firmware follow the above procedure:

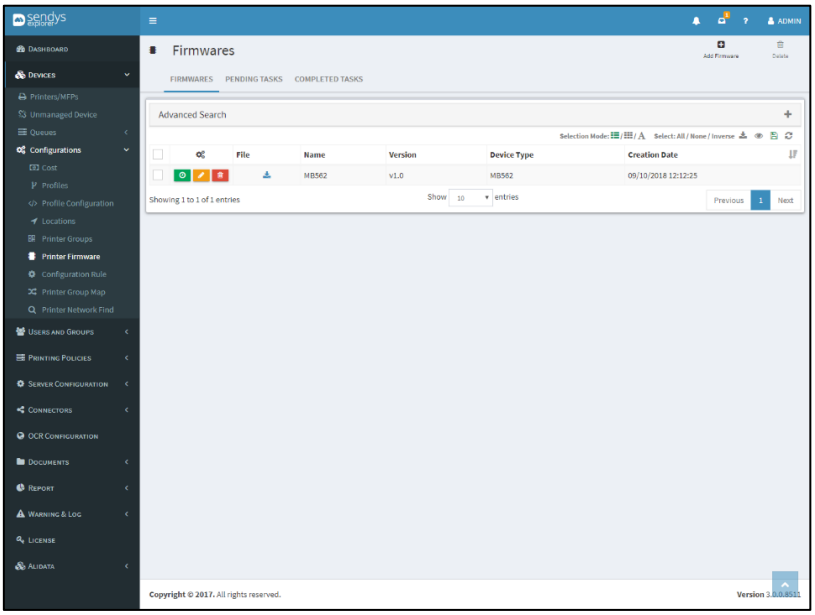
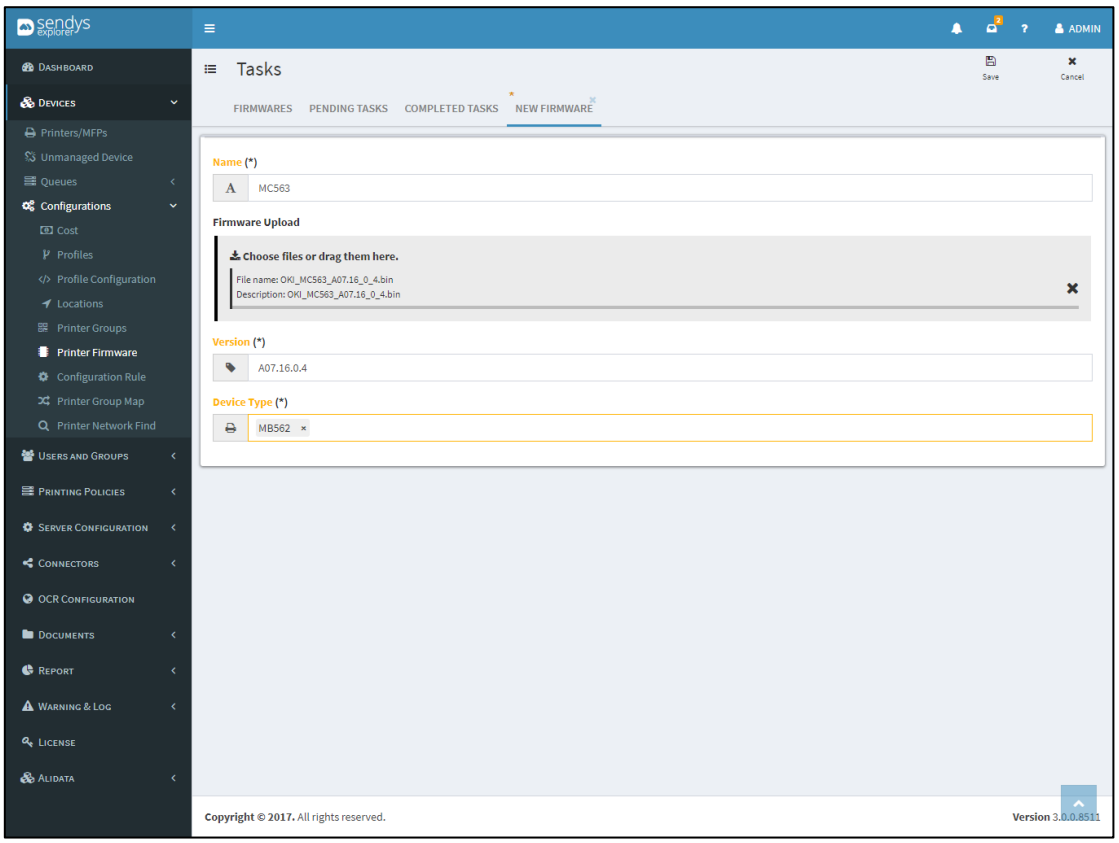


Fig. 167 – Printer Firmware View.

ADD/EDIT

1. Click on **Devices**
2. Click on **Configurations**
3. Click on **Printer Firmware**
4. Click on **New** to add or **Pencil** to edit.
5. Insert a **Name**
6. Insert a firmware file to upload
7. Insert the version
8. Select the device **Type**
9. Click Save
10. Click on the clock icon to create a firmware task



11. **Fig. 168 - Devices – Printer Firmware Upload**

12. Select the devices to make the firmware update or click on the button with the arrow to force the update to a specific device

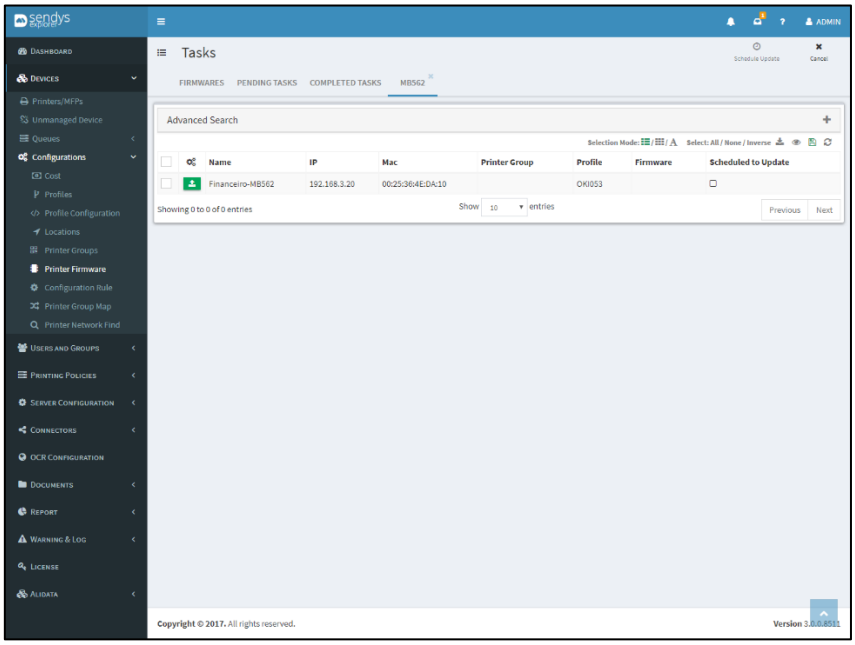


Fig. 169 – Printer Firmware Update.

13. Assign a name for this specific task
14. Specify a specific date for update
15. Specify a specific time
16. Click Save

The update firmware will be running after this date and will sequential update all devices specified.

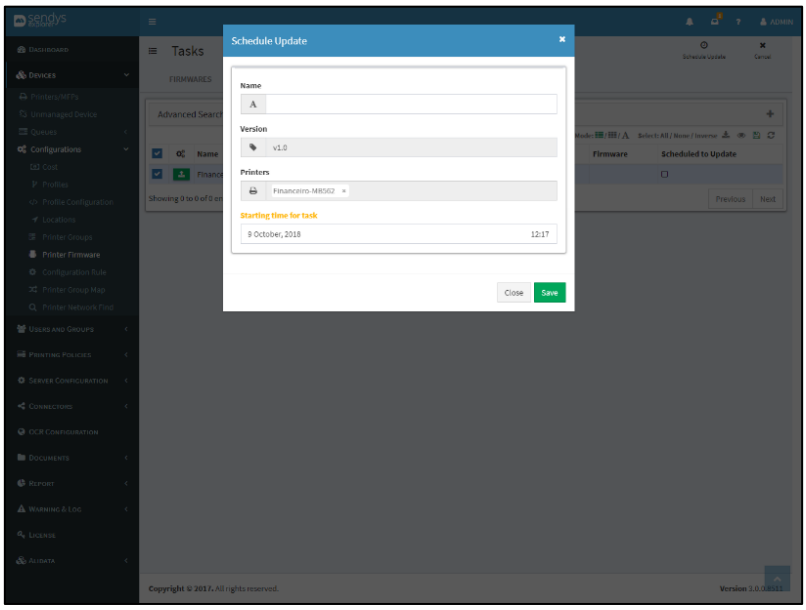


Fig. 170 - Printer Firmware update task.

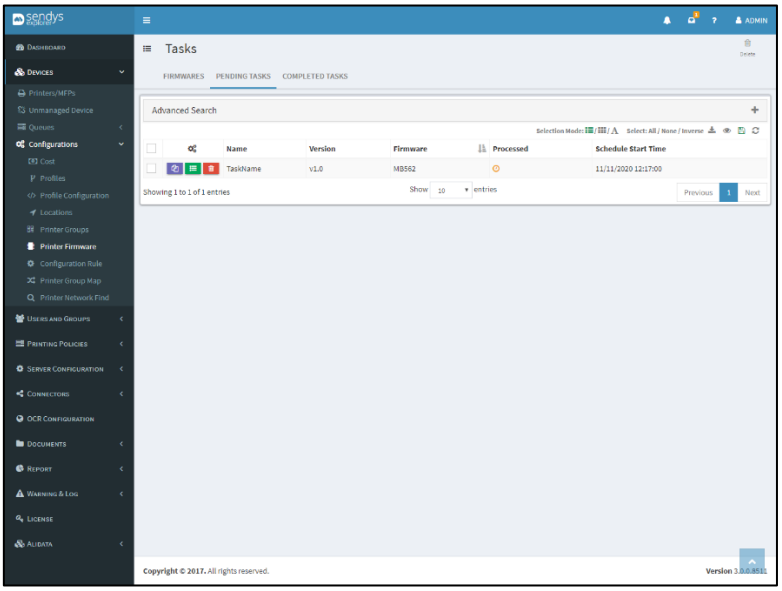


Fig. 171 - Printer Firmware Pending Task.

CONFIGURATION RULE

Configuration rules use profile configurations to reconfigure multiple devices at same time.

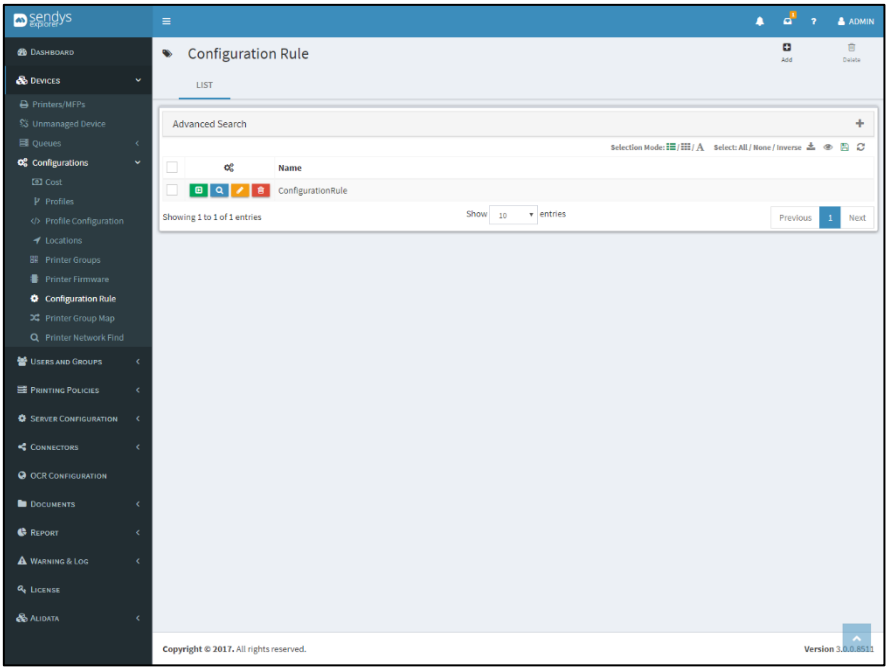


Fig. 172 – Configuration Rule.

ADD/EDIT

1. Click on **Devices**
2. Click on **Configurations**
3. Click on **Configuration Rule**
4. Click on **New** to add or **Pencil** to edit.
5. Insert a **Name**
6. Insert a Schedule Start Date
7. Add the specific configuration that you need to do on the devices
8. Assign the configuration to **Printers/Profiles/Printer Groups**
9. Specify the schedule for the configuration to be assign to the devices

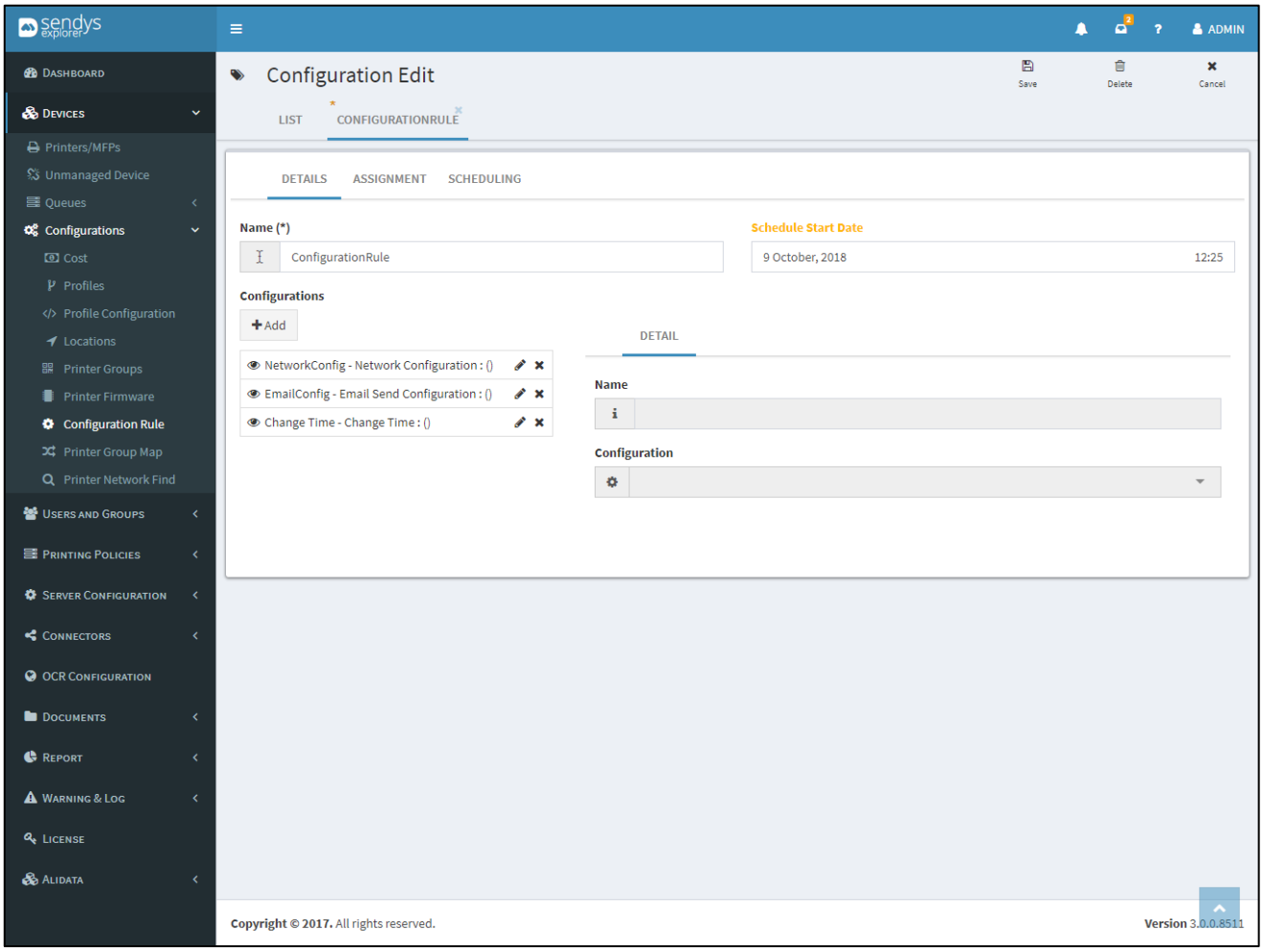


Fig. 173 - Devices - Locations view

Base configurations are available that allow to configure network setting or add new contacts to devices.

Name	Details
Network Configuration	Configure all network settings on OKI sXP2 devices.
Email Send Configuration	Configure SNMP settings on OKI sXP2 devices.
Email Receive Configuration	Configure POP settings on OKI sXP2 devices
LDAP Configuration	LDAP authentication and server configuration on OKI sXP2 devices.
Network Scan	Export network scan configurations from selected source or use a csv text format to create new configurations. All network scan configurations on the devices will be deleted before export or create.
Profile	Delete profiles on devices and exports source device profiles or creates new profiles using a csv text format
Create Device Local Users	Creates new local users on selected devices. Users can be selected individually, by group or by role, if a user with the same name already exists on the printer it will not be created.
Role Configuration	Creates a new role and its permissions on OKI sXP2.
Phone/Address Book	Add global contacts and creates new groups on devices. All contacts on the devices will be deleted before inserting new contacts.
Home Menu	Configures home menu display buttons.
Default Home Screen	Selects default home for selected devices.
Transmission Settings	Export source transmission settings into selected devices or creates new settings using a csv text format.
Auto Delivery	Export source auto delivery settings into selected devices or creates new settings using a csv text format.

Table 18 – Configuration Rule options - Configuration

PRINTER GROUP MAP

On this view we can manage the connection between groups and users. Groups creation and managing are done on the previous chapter.

If is necessary to change one or more users from a group to other. If it is necessary to change a user from a group, select the pretended user from the users list and then select the group and **Save** the alteration.

Using button **Refresh** to refresh the list of users and the list of groups.

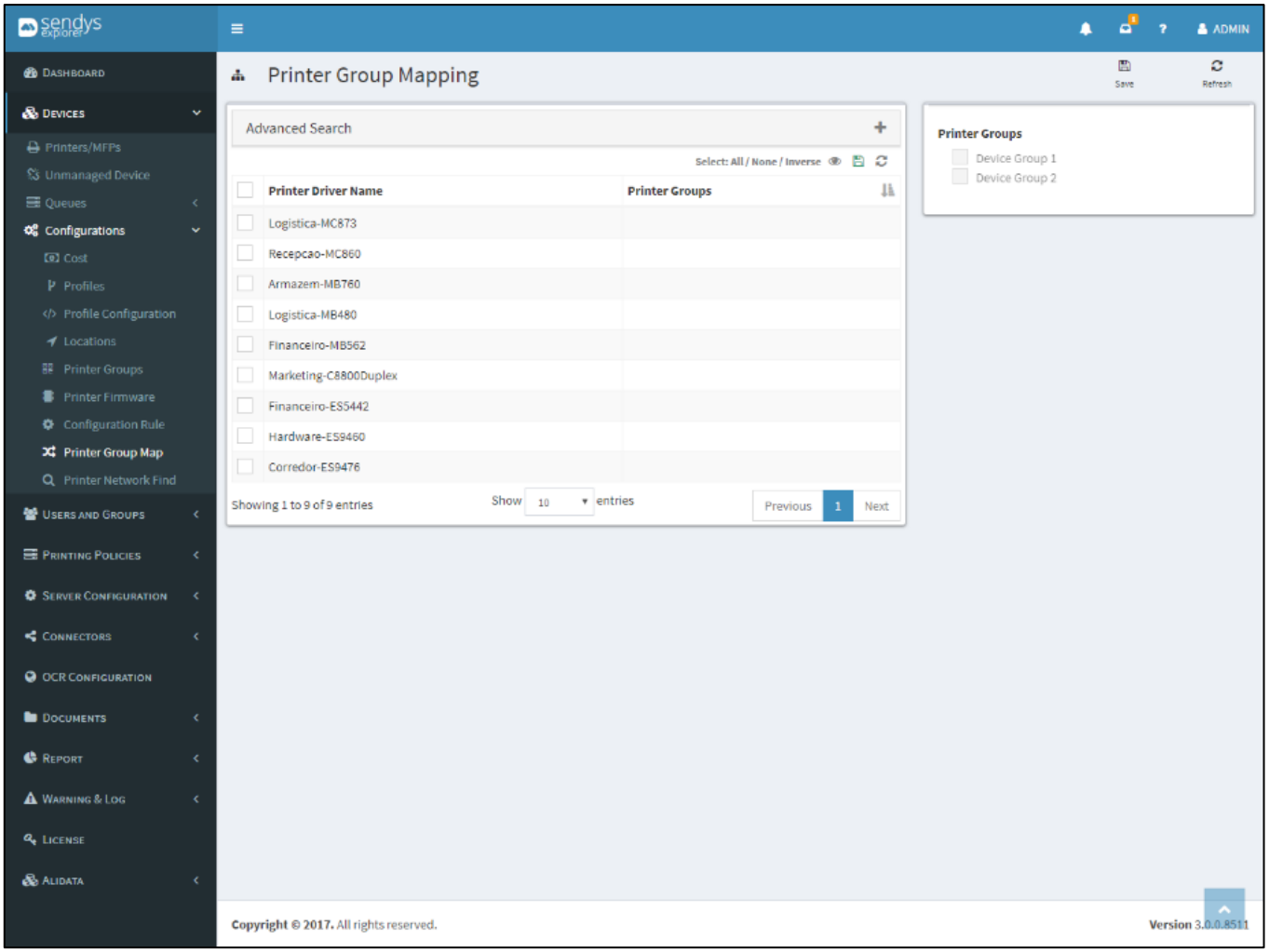


Fig. 174 - Devices - Locations view

PRINTER NETWORK FIND

On this view a network range can be configured to run a scan on the network, that will do one of the following actions:

1. **Move:** Change the Printer IP to the one found by the Scan based on Printer Serial
2. **Add:** Add a new Printer to SENDYS Explorer
3. **Change:** Change the Printer Serial on a existing Printer with the found IP
4. **Delete:** If a Printer was deleted it will be detected by the network scan

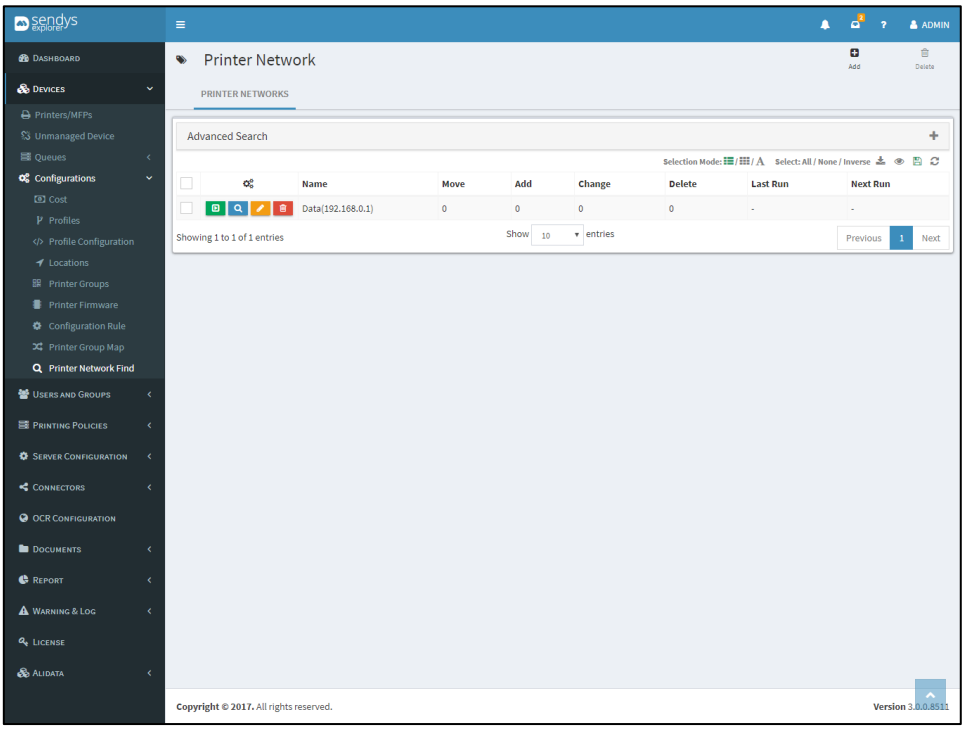


Fig. 175 – Printer Network Find.

The Network Find Logs page can be viewed by pressing the Log button, represented by the blue button with the magnifying glass.

Fig. 176 - Printer Network Find - Log Button.

The view Network Find Logs shows the history of all actions executed by the network, with the latest entry being on the top of each table.

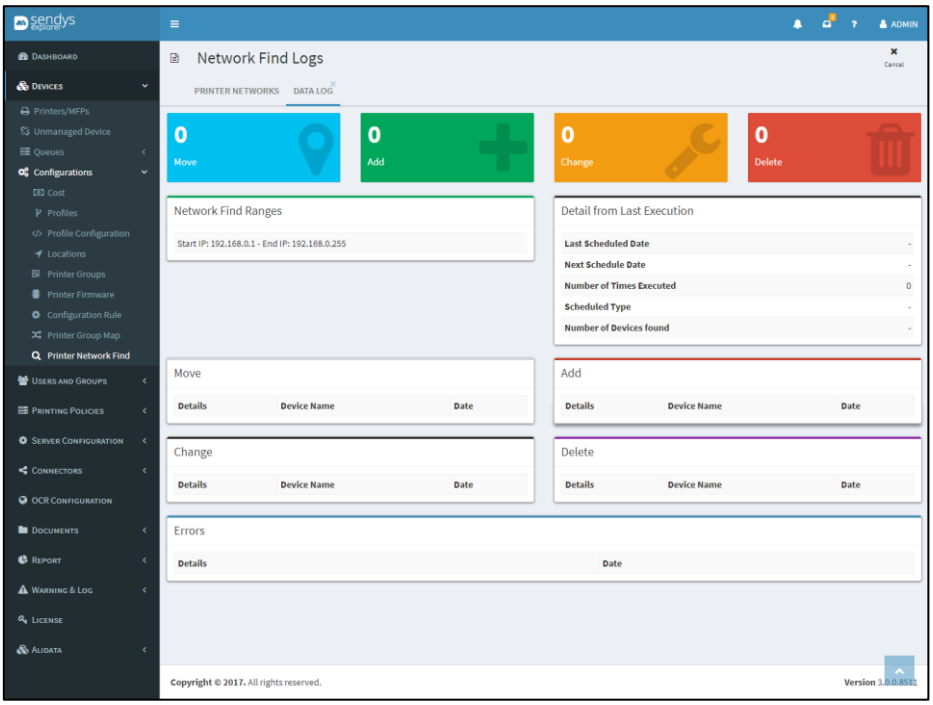


Fig. 177 - Printer Network Find Log view.

ADD/EDIT

1. Click on **Devices**
2. Click on **Configurations**
3. Click on **Printer Network Find**
4. Click on **New** to add or **Pencil** to edit.
5. Insert a **Name**
6. Add the specific ranges that you need
7. **Optional:** Specify which Printer Group the printer will be assigned
8. **Optional:** Chose a location for the printers
9. **Optional:** If you want to run a specific configuration on the printers you can chose them on the **Assign Printer Configuration Rules** field.
10. **Optional:** Configure the schedule for the network find to run
11. Click **Save**

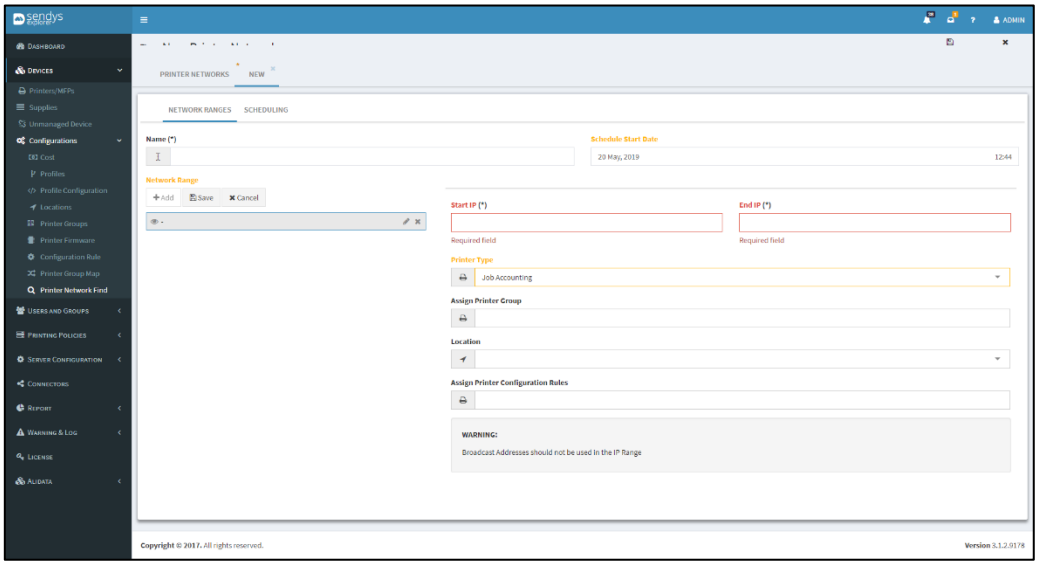


Fig. 178 - Printer Network Find.

A network scan can be run manually by using the option **Execute Scan** on the grid. After that the scan will run on the background and after terminating an alert popup will be shown.

Fig. 179 - Printer Network Find – Execute Scan Button.

RFID

1. Click on **Devices** menu.
2. Click on **RFID** menu

This is an option that offers a solution for printers that doesn't have a smart screen interface and using the fallow me option. For that, another device must be added and configured on the platform. To make this view accessible on the Devices menu you need to enable on the **Server Configuration** -> **Application Config** -> **Others** tab -> Enabling **Work with TPC convert** and/or **Working with RaspberryPi**.

You only need this section when you have external hardware like TCP Converter/Raspberry PI's.

On this view will be listed the Raspberry and TCP Converters devices added on the platform.

In this section you can consult and also configure those devices.

SBC

1. Click on **SBC** (Single Board Computers) menu.

Define the method add the device selecting the pretended tab, discovery (scanning the device) or USB configuration.

ADD DEVICE - DISCOVERY

1. Click on **Add Devices** button.
2. Click on **Discovery** tab.

To add a new device, using a scanning process, use the next configurations on the window that appears.

On tab **Discovery**:

Name	Details
Start IP	Insert the IP where it will start the scanning.
End IP	Insert the IP where it will end the scanning.
Advanced	Enable the next options for timeouts.
Start Scan	Execute the scanning devices between the start and end IP defined.
Timeout	Time in milliseconds that the scan will work.
Max Connections	Define the maximum connections.

Table 19 - Add devices options - Discovery

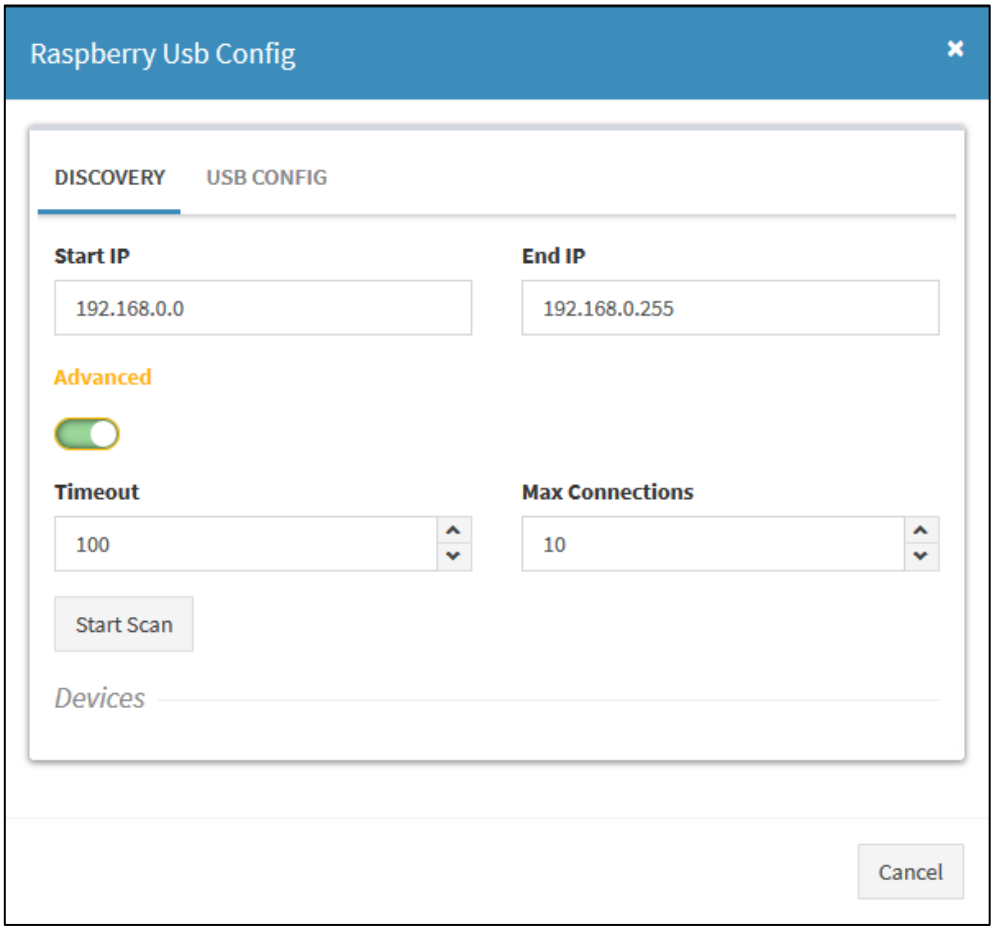


Fig. 180 - RFID - SBC– Add device - Discovery

After the scanning, and if the configurations are correct, a list of devices will be added to the window.

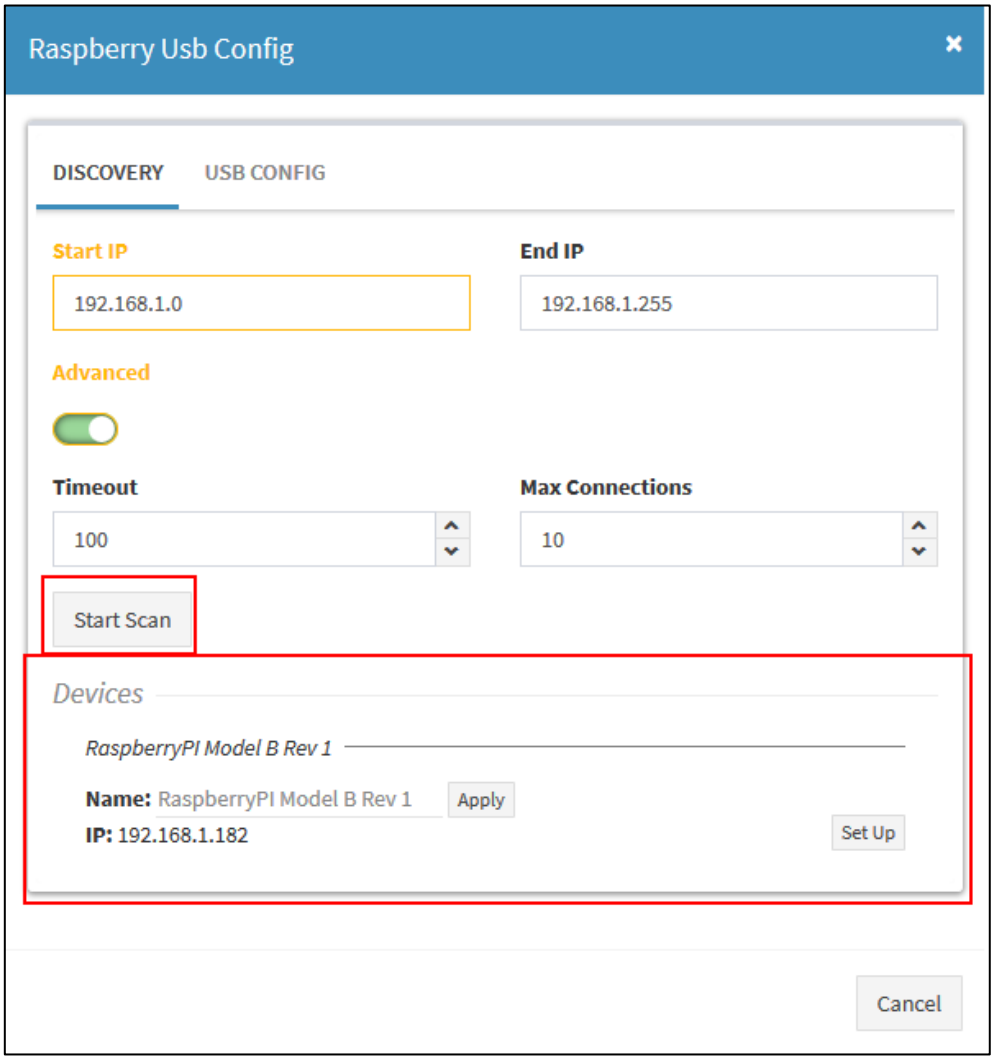


Fig. 181 - RFID - SBC– Device scanned

You can change the name directly on the list, clicking on the name (*RaspberryPI Modl B Rev 1*) and change it.

3. Click **Apply** to save the modifications on the name (if necessary to change).
4. Click on **Setup** to automatically setup the configurations.

After the **Setup** the device will added.

ADD DEVICE - USB CONFIG

1. Click on **Add Devices** button.
2. Click on **USB Config** tab.

On this configuration you need to Export a file from this menu containing the configurations and upload on the RaspberryPi using a USB drive.

On **USB Config** tab:

Note: some fields are filled up automatically but it is recommended a review.

Name	Details
Hostname	Name for the device.
Multiple Configurations	Enable the options to work with more Raspberry Pi (**Number of Devices**)
Server Address	Server IP.
Server Port	Server Port.
Number of Devices	Defines the number of devices to work.(Depends of the Multiple Configurations option)
Use DHCP	Defined if is used the option DCHP.
Bridging	Select the option for connection.
Export Config	Download a file with the configurations.

Table 20 - Add devices options - USB Config

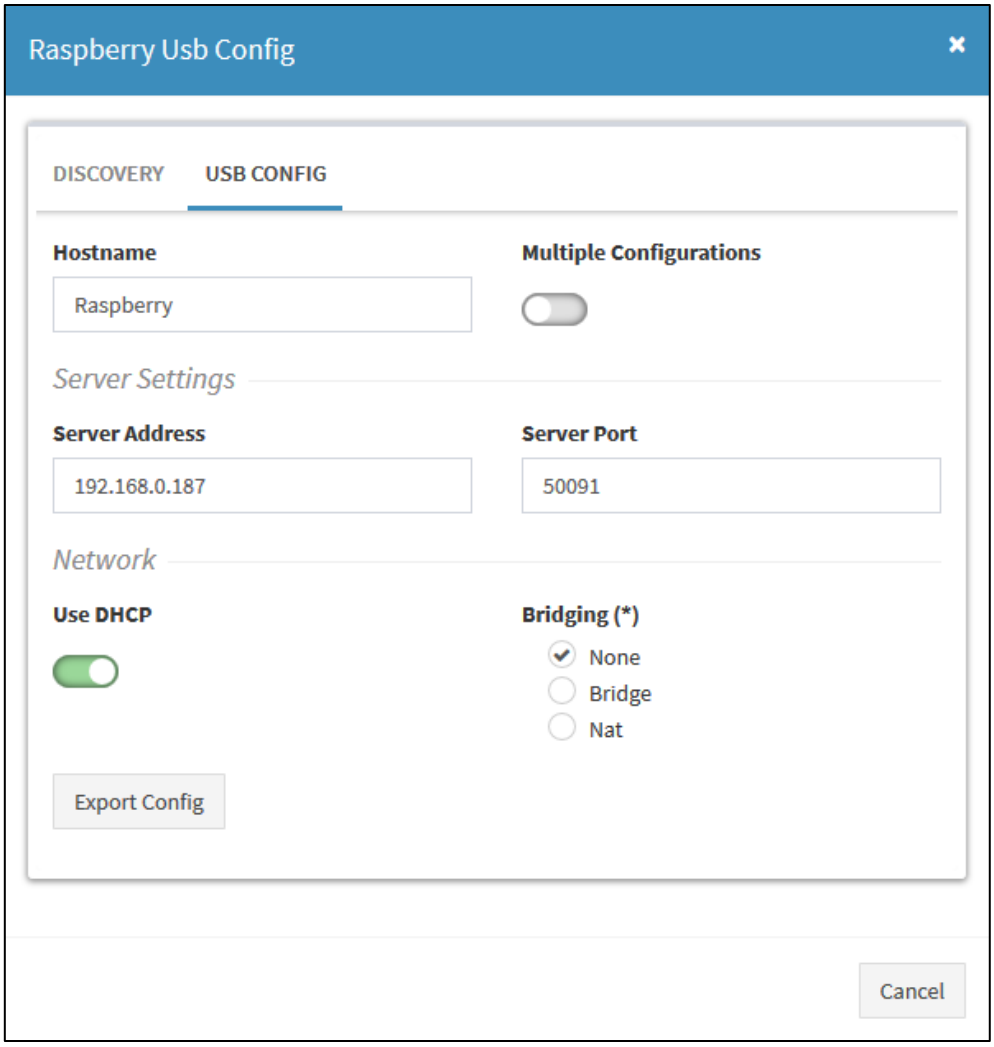


Fig. 182 - RFID - SBC– Add device - USB Config

Click on **Export Config** to download the configurations and use that file to upload on the RaspberryPi device by USB.

After the Upload the device list will be added automatically.

EDIT DEVICE

1. Click on **Edit** button on the pretended device to edit.

Name	Details
Name	Name for the device.
IP Address	Device IP Address.
MAC Address	Device MAC Address.
Brand	Device Brand.

Table 21 - Edit device options

Click **Save** to save the changes or **Cancel** to cancel.

If necessary to change some configuration on the RaspberryPi, click on **Setup RFID** to change.

Delete button will delete the device on platform.

CONFIGURATION

1. Click on **Configuration** button.

Printing Options:

Name	Details
Waiting for print	
Copy after print	
Lock to other user type	
Reading interval (ms)	
Initial interval (ms)	
Lock to user	
Printing type	Chose witch document order to print. Last document, First document or All Documents.

Table 22 - Add devices options - USB Config

TCP CONVERTER

1. Click on **TCP Converter** menu.

Note: It is necessary to open the port configured on the firewall.

After the TCP Configuration

PRINTING OPTIONS

TCP CONVERTER CONF.

TOUCH

For this option be accessible it is necessary to change the option **Work with Touch** on the Server Configuration on Others selector. (**Server Configuration** ->**Application Settings** -> **Others**).

With this option, on or more MFP printer will have a touch dedicated to them to simulate a smart screen EWB. The user can operate normally with the printer doing the actions normally has if the printer has a smart screen.

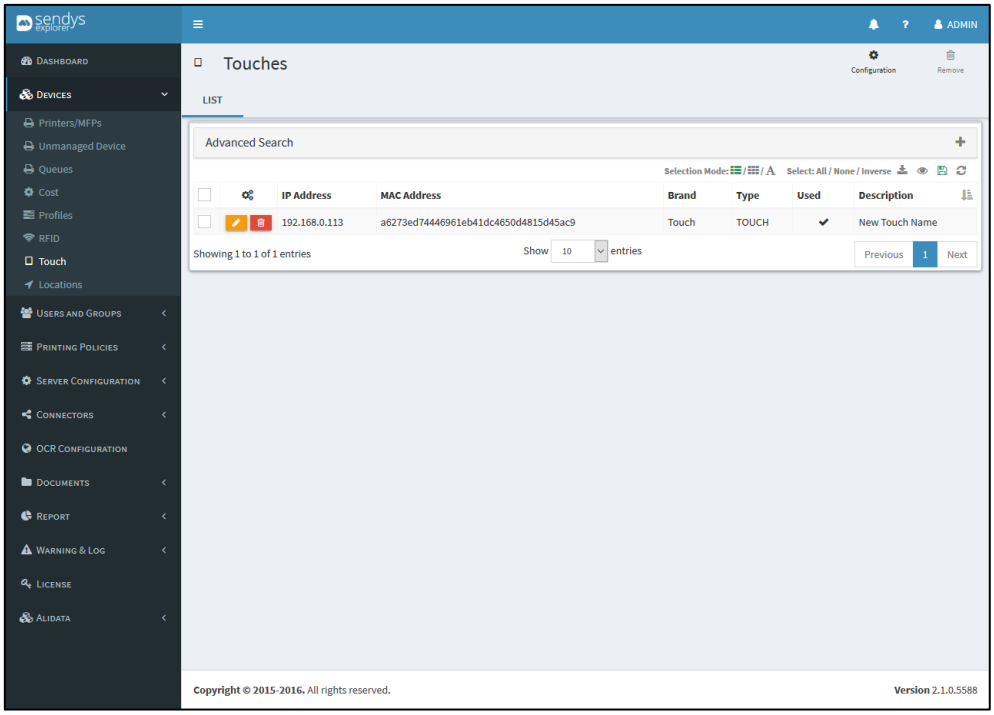


Fig. 183 – Touch view

ADD DEVICE

To configure with a printer, it is necessary to use a browser on the Touch dispositive.

1. Use a browser on the **Touch** device.
2. On the browser, access the URL: **[serverIP]:[serverPort]/Touch.aspx.**

Note: We recommend you to save that browser page as a shortcut on your touch device so it is more practical and quick to access the touch platform.

3. Authenticate with **Admin** credentials (**PIN** method).

Note: only admin credentials can be used to configure the touch device.

The configurations are:

Name	Details
Name	Name for the touch device.
GUID	Unique key for the server identification. This field is automatically filled.
Printers/MFPs	Select the pretended printer and/or MFP to associate with the touch device.

Table 23 – Add touch device options

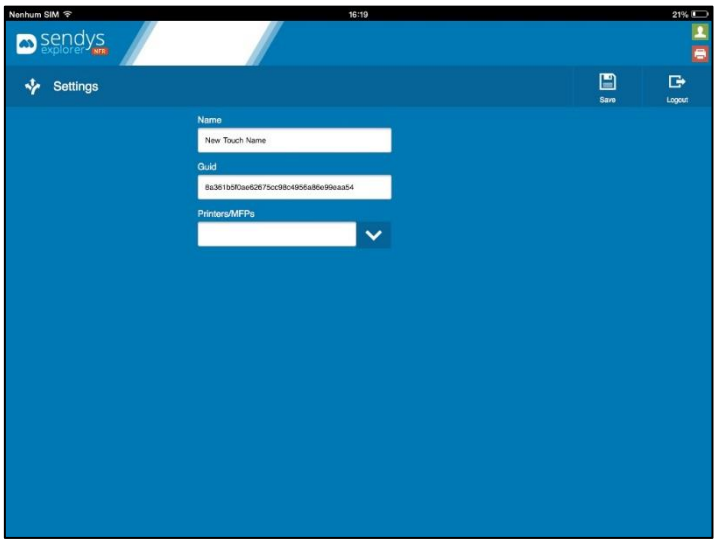


Fig. 184 – Touch configuration view

4. Use the drop box element to load a new view showing the **Printers/MFP's**.

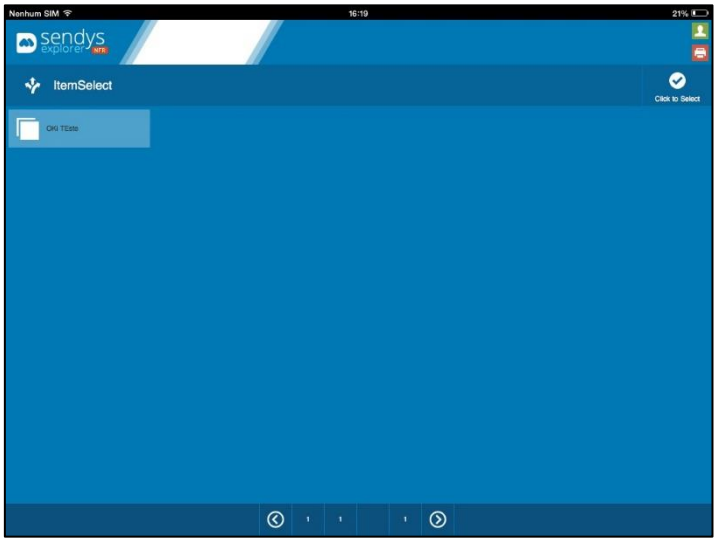


Fig. 185 – Touch configuration selecting printer

5. Select one or more printer from the list.
6. Click on button **Click to Select** to return to configuration view.

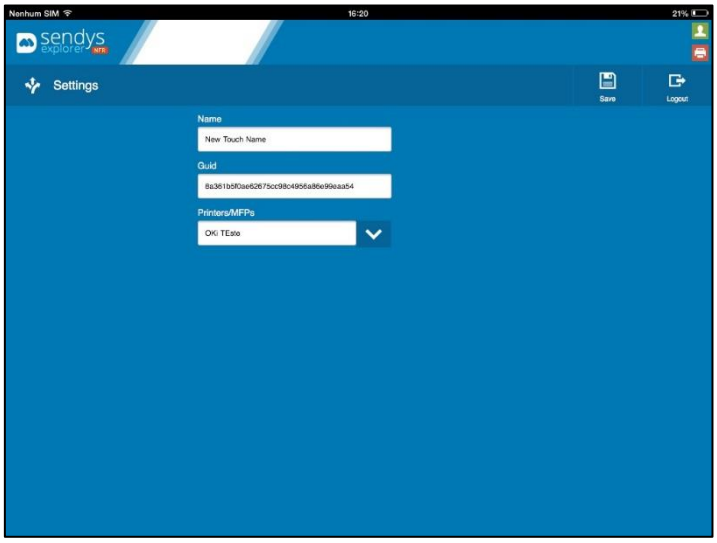


Fig. 186 – Touch configuration with printers selected

7. Click on **Save** button to save the configurations.

If the configurations are correct, the touch device now is ready to working for the printers selected.

After the authentication, if there is only one printer attached to the device, the printer will be chosen automatically, but in case that there are more printers, a list will be shown so the user can select the printer to use.

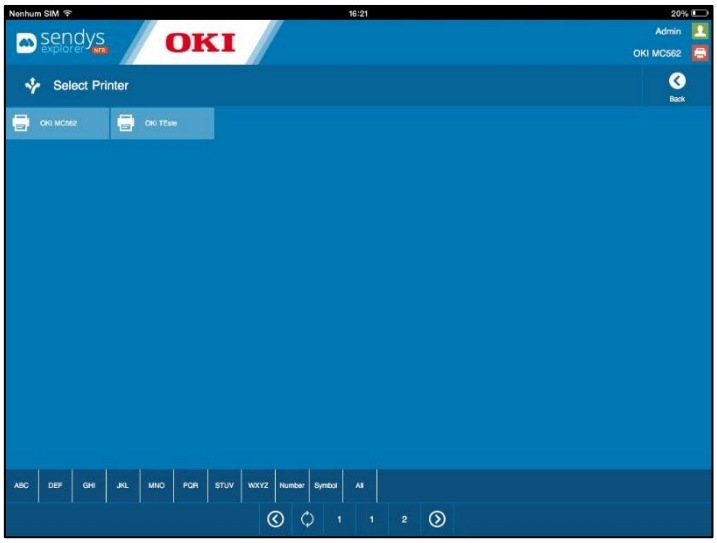


Fig. 187 – Touch configuration with printers selected

After selecting a printer, the Touch device is ready to be used.

EDIT TOUCH

Two tabs appear here for the editing of existing Touch devices.

DETAILS

1. Click on **Edit** button of the pretended device.
2. Click on **Detail** tab.

Details tab is where the information about the connected Touch selected appears and can be changed:

Name	Details
IP Address	Touch IP.
MAC Address	Touch GUID.
Brand	Touch Brand.
Touch Description	Touch name selected.

Table 24 - Edit - Configure

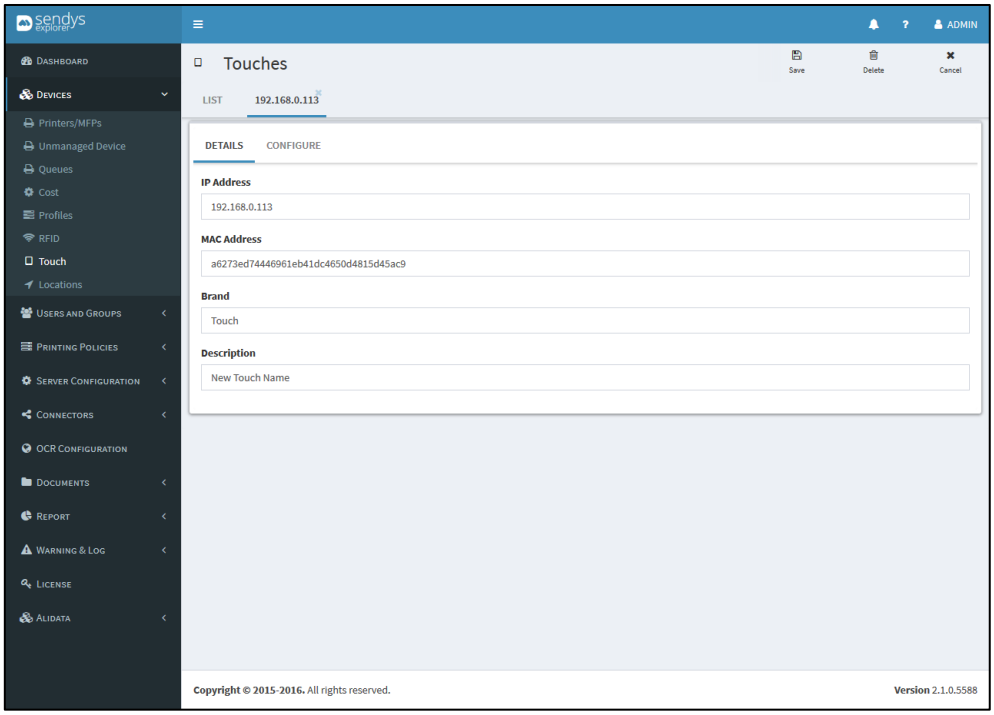


Fig. 188 – Touch edit configuration

CONFIGURE

1. Click on **Edit** button of the pretended device.
2. Click on **Configure** tab.

Configure tab where some other configurations can be applied on the selected touch edited.

Name	Details
IP Address	Touch IP.
MAC Address	Touch GUID.
Brand	Touch Brand.
Touch Description	Touch name selected.

Table 25 - Edit - Touch

Click **Save** to save the changes or **Cancel** to cancel.

USERS & GROUPS

This menu is used to manage user, contacts, groups and policies on the SENDYS Explorer Output Manager. So the access to the platform and privileges are defined here.

Note: on the installation of SENDYS Explorer, if the configuration/connection to the Active Directory was right and accessible, many information was imported from the AD and some fields are filled automatically. If some configuration it is need to be added the Administrator should access on Server Configuration. This will be later reviewed on other chapter.

USERS

1. Click on **Users and Groups** menu.
2. Click on **Users** tab.

The Users view shows the list of users that Output Manager is managing. For each user many actions can be made.

On this view the options are:

- **Add User** - button on the upper view used to add a new user.
- **Edit User** - button on the user list view that edit the user.
- **Delete User** or **Remove** - delete specific user (user list view) or remove a selection of users (button on the upper view).
- **Email user** - send an email to the specific user containing the information to access the platform.
- **Send Email to all users** - send an individually email to all user containing the information to access the platform.

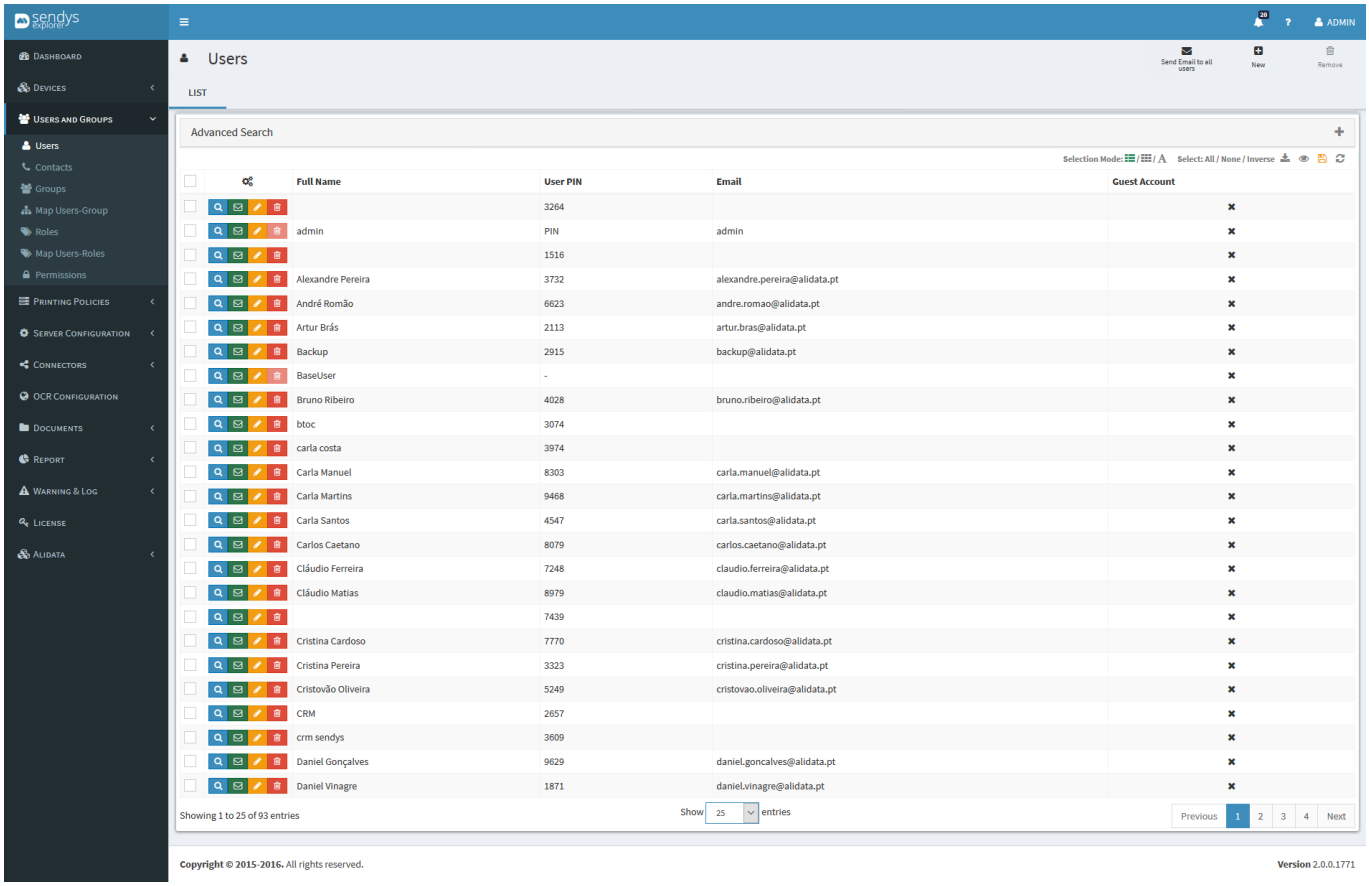


Fig. 189 - Users and Groups - Users overview

ADD - EDIT USER

1. Click on **New** button to add a new user or **Edit** user button on the list to edit an existing user.

Clicking on the **New** button a new view is shown to insert all the information for the new user. Depending on the operation type (Add or Edit) the upper buttons options will change.

As the Add user, Edit user works very similar, the only difference is the upper menu that has some different options because the user was already created and a few options on the user edit view.

Clicking on **Edit User** button the next view (tab with the edited username title) is shown and adding to the common options, some new options can be used. The view will show the **QR Code** associated with the user too.

On the upper buttons on the view:

Generate New Pin - Generate a new PIN for the edited user.

Update Other Users - Saves the configurations (Permissions, Print Policies and Quotas) associated to the edited user.

SEND INFO - if the platform email is configured correctly, clicking on this options, will send an email to the edited user showing the information how to access to the user portal and his credentials.

Save - saves the configurations.

Delete - deletes the edited user.

Cancel - cancels the edit action.

Inside the user edits view there are a few new options that doesn't exist on adding a new user. Those options are only presented on **Details** tab. The rest of the options and configurations are the same as adding user, described on the previous chapter.

The **Reset Password** button, on the user **Details** tab (upper to the user QR Code), will reset the user password. The reset will change the password equals to the Username. For example: the user "*John Doe*" forgets the password and he can´t enter on the user portal. The Admin can reset the password.

Username: John.Doe

Password: John.Doe

Now the user can enter on the user portal with this new credentials and change it anytime.

Enable switch - enable/disable the user access to the user portal. Turn the switch on and the user has access to the user portal, turn the switch off, blocks the access.

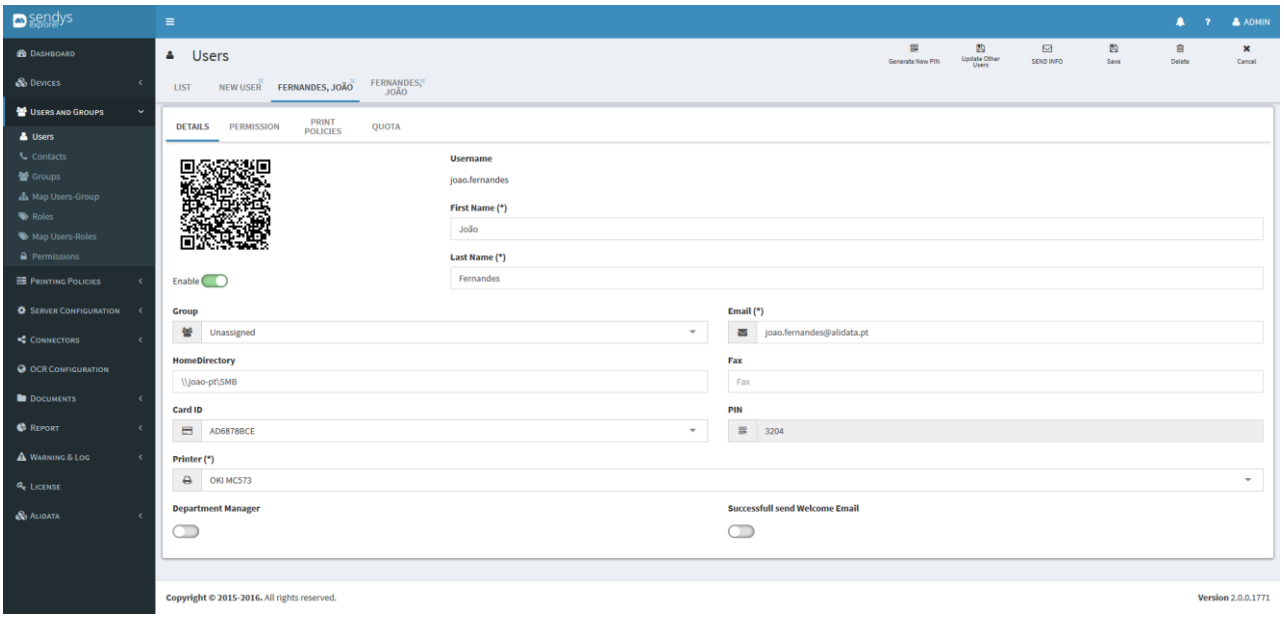


Fig. 190 - **Users and Groups - Users - Edit user –details tab**

USER DETAILS

1. Click **Edit** user button on an existing user on the list to edit.
2. Click on **Details** tab.

On **Details** tab, accessible on Adding or Editing user, the next table shows the configurations for the user:

Name	Details
Username	Defines the username that is shown on the platform.
First Name	Defines he first name for the user.
Last Name	Defines he last name for the user.
Group	Associates the user to an existent group.
Email	Defines the email for the user.
Card ID	Defines the Card ID code for the user.
Home Directory	Defines the user folder where the documents can be stored.
Fax	Defines the number of the fax to associate with user.
Printer	Defines the default printer for the user.

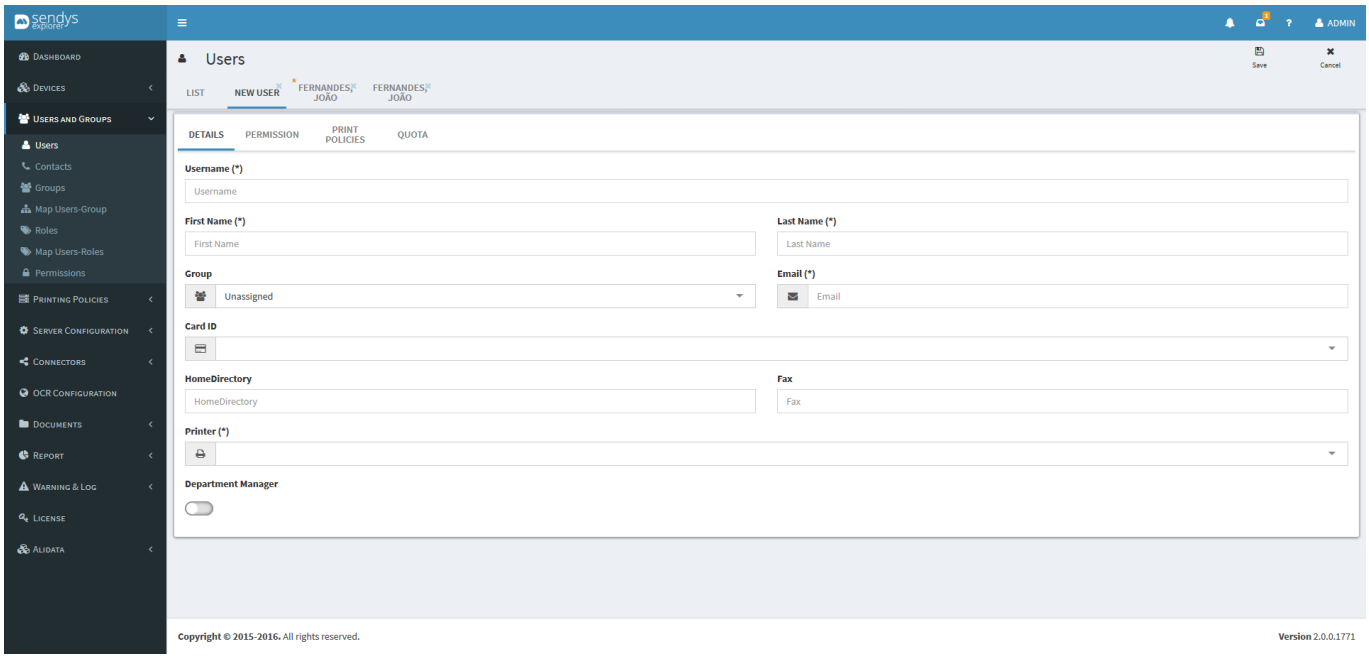


Fig. 191 - Users and Groups - Add User– Details tab

IMPORT USER

1. Click **Import** button on the header.

Clicking on **Import** opens a tab that allows to create new users, using a text format list. Each line should have the fields **username**, **email**, **first name**, **last name**, **group**, **role**, **card number**, **home folder** and **alias**, by that order, being the first four mandatory and with each field split by the **separator** option on the form.

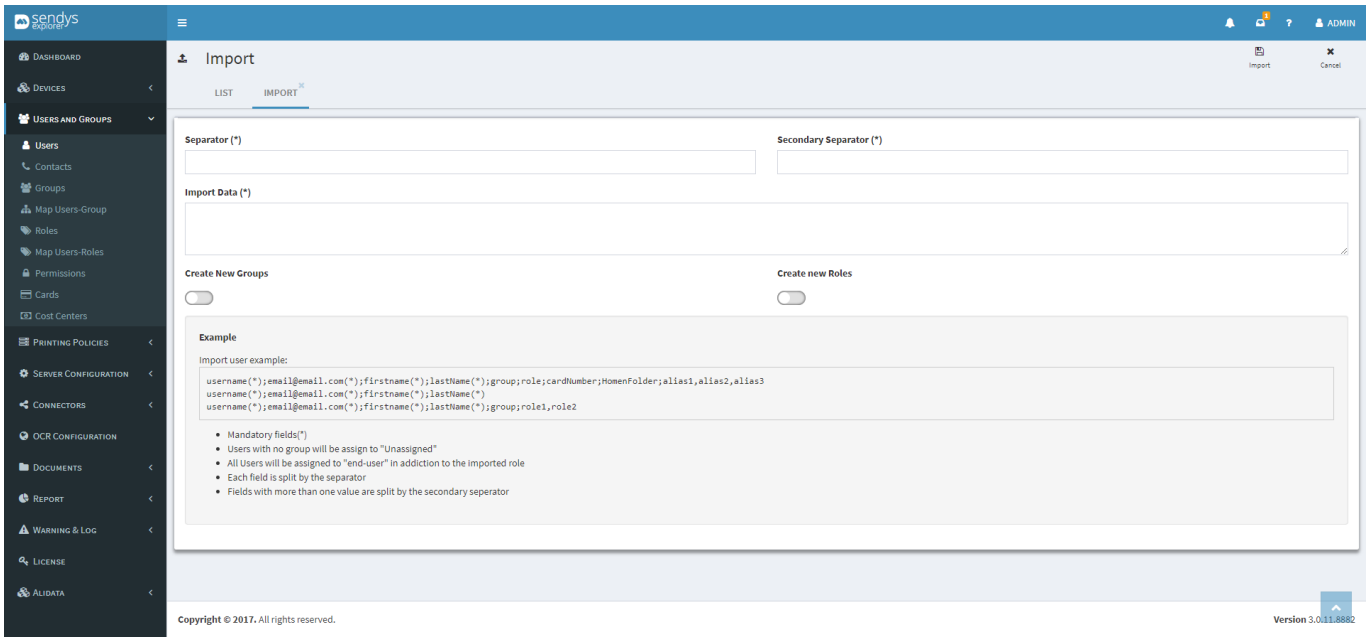


Fig. 192 - Users and Groups - Users - Import user –Import tab

Users are created assigned with their specified group and as “end-user” role in addiction to the imported roles, when a user has no group or role he will be assigned to the “Unassigned” group and “end-user” role. The fields role, card number and alias can have more than one input and are split by the **Secondary Separator.**

This is an example how to import contacts:

The **Separator** choose was “**;**” and “**,**” as the **Secondary Separator**:

```
username;user@email.com;firstname;lastname;group;role;12345;homefolder;alias1,alias2
username1;user1@email.com;firstname1;lastname1;;;12345
username2;user2@email.com;firstname2;lastname2;;role1,role2;12345,54321
username3;user3@email.com;firstname3;lastname3
```

With the option **Create New Groups** or **Create New Roles** enabled all new groups and roles will be created and mapped with its users, otherwise no new group or role will be created.

USER DETAILS

1. Click **User Details** button on an existing user on the list.

Clicking on **User Details** button of one user a view will appear to show us more information from the selected user. Navigate between tabs to consult all the next points.

- **Information** tab shows us the relevant information such as identification and other details.

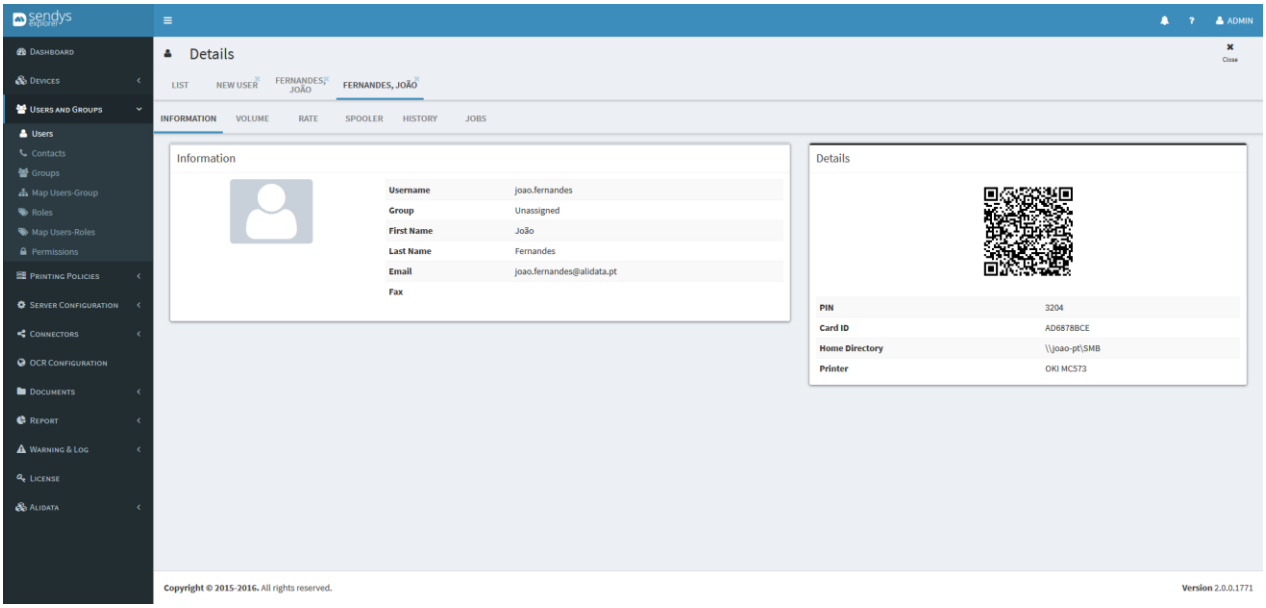


Fig. 193 - Users and Groups - Users Details - information tab

- **Volume** tab shows statistics associated to the selected user like the day or month counters and other aspects.

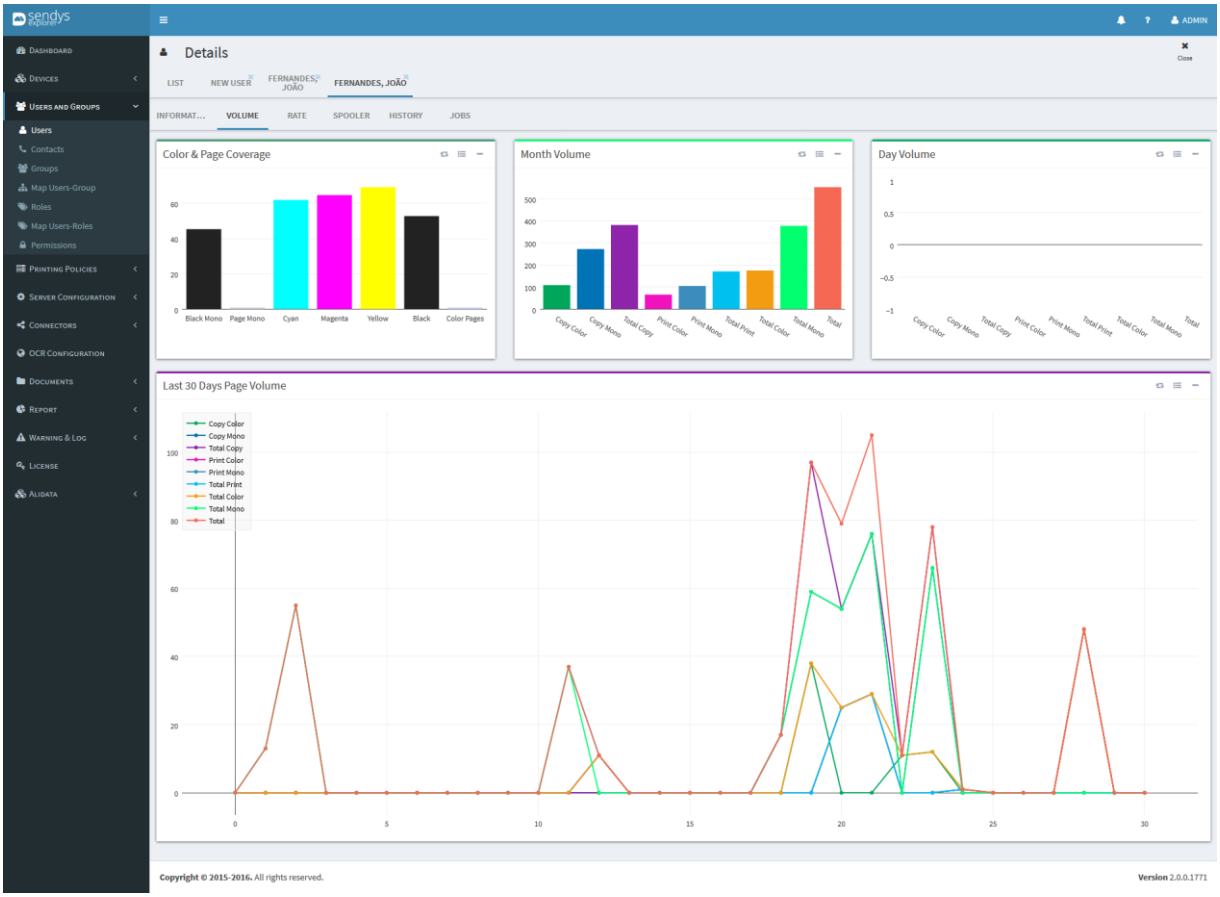


Fig. 194 - Users and Groups - User Details - Volume tab

- **Rate** view show another statistic associated to the selected user and their associated counter on many aspects.

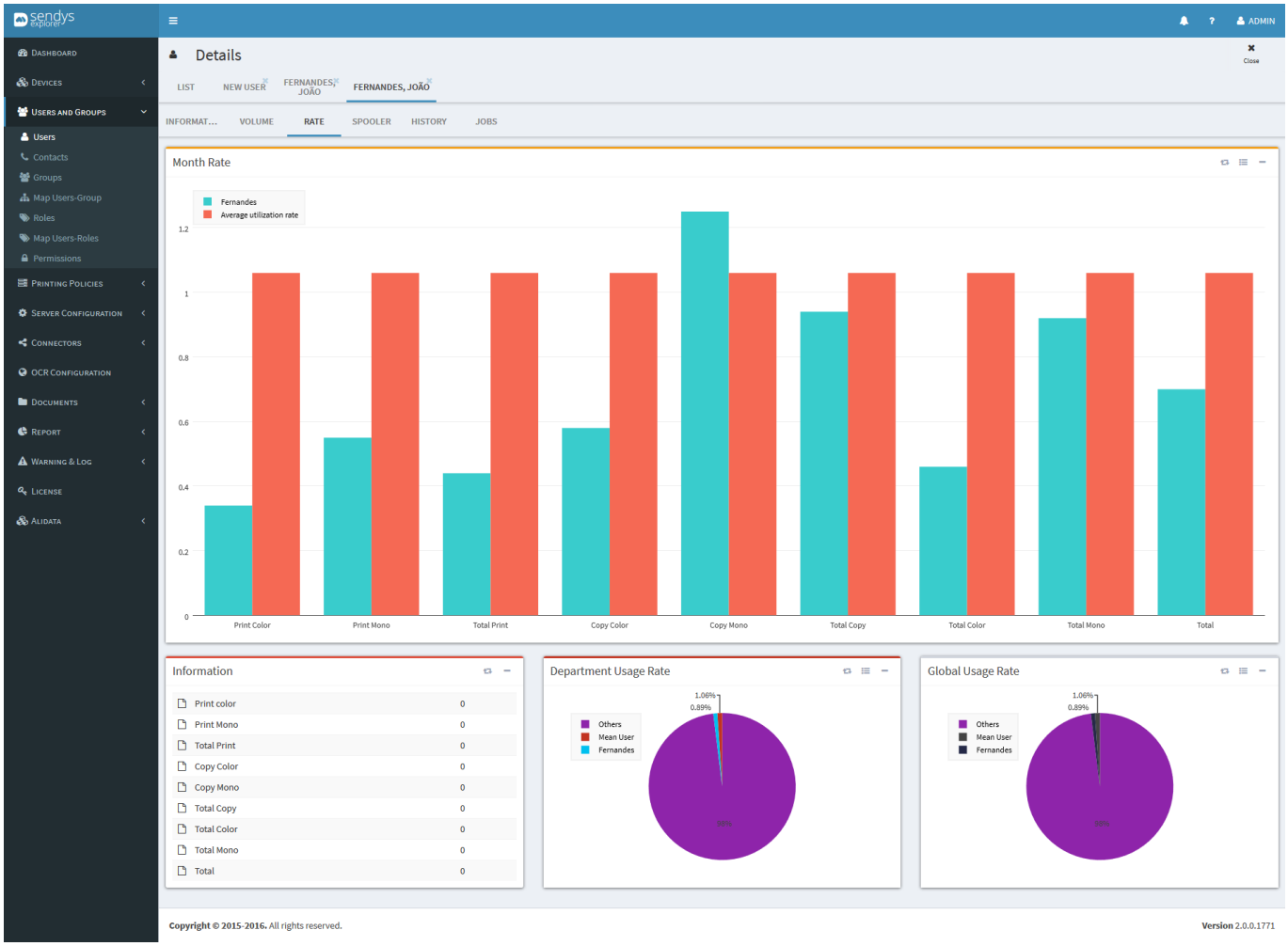


Fig. 195 - Users and Groups - User Details - Rate tab

- **Spooler** tab shows the documents in spooler associated to the selected user.

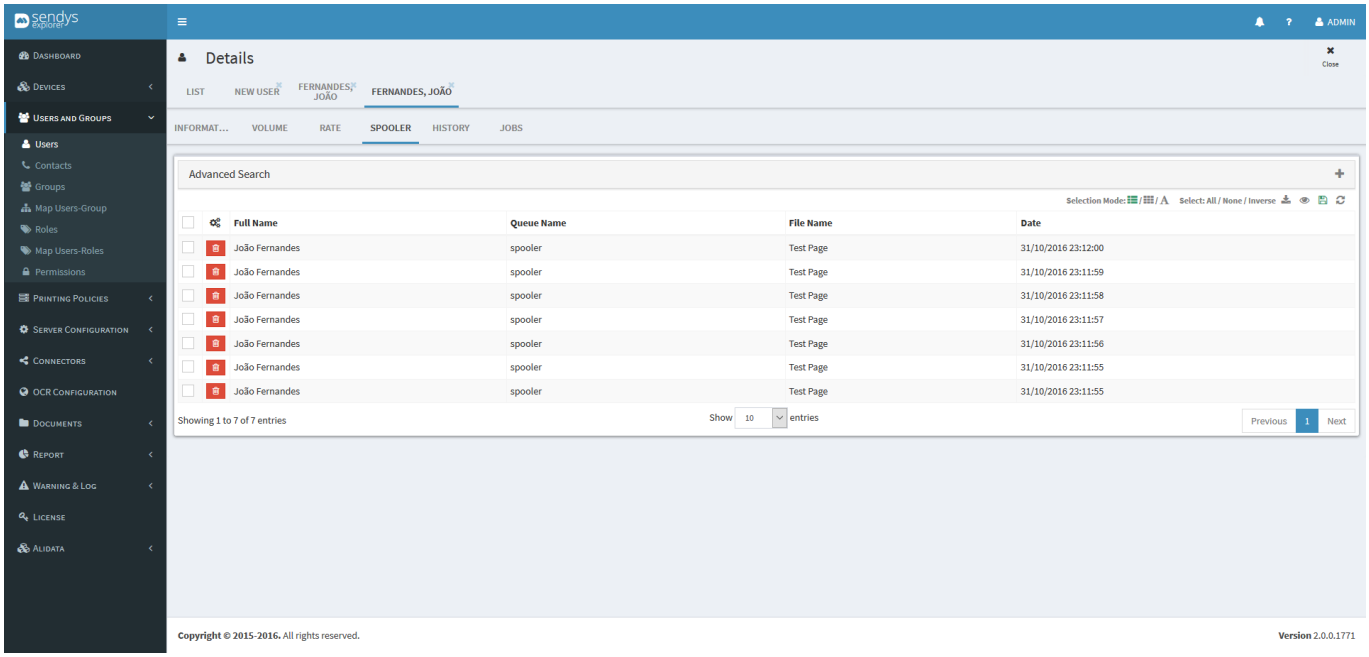


Fig. 196 - Users and Groups - User Details - Spooler tab

- **History** tab shows the document print history associated with the selected user.

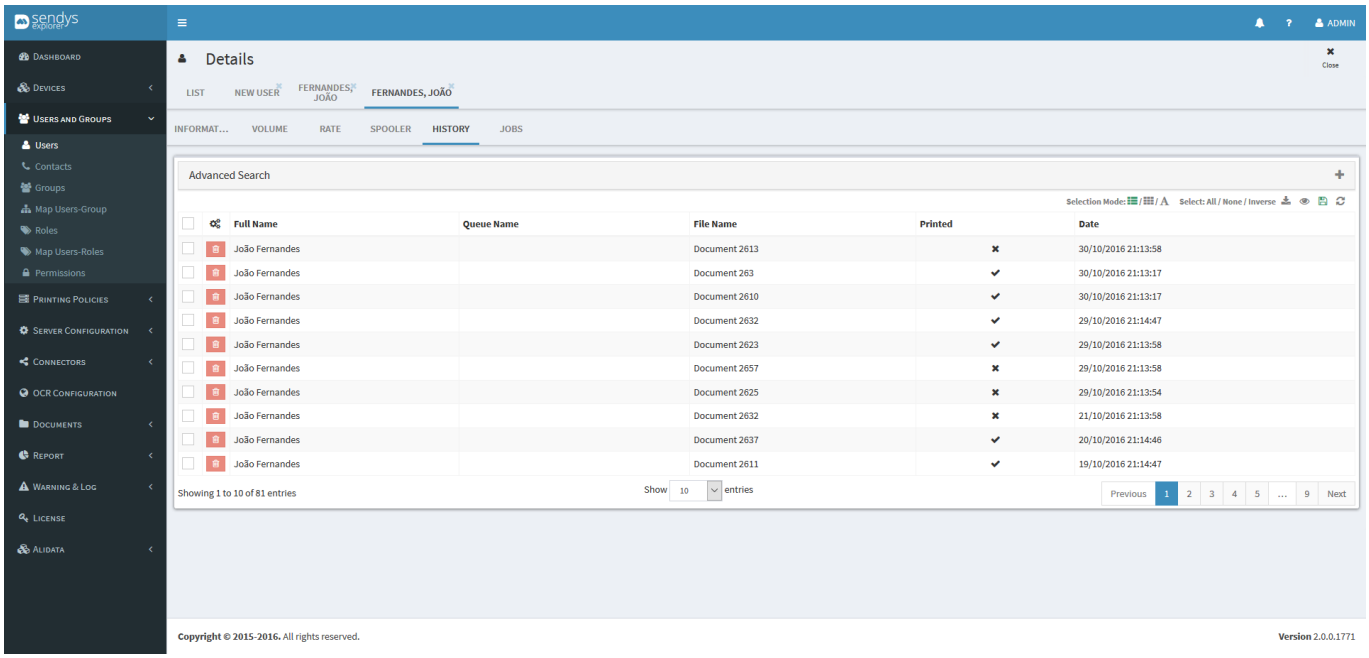


Fig. 197 - Users and Groups - User Details - History

- **Jobs** view show all jobs executed by the selected user.

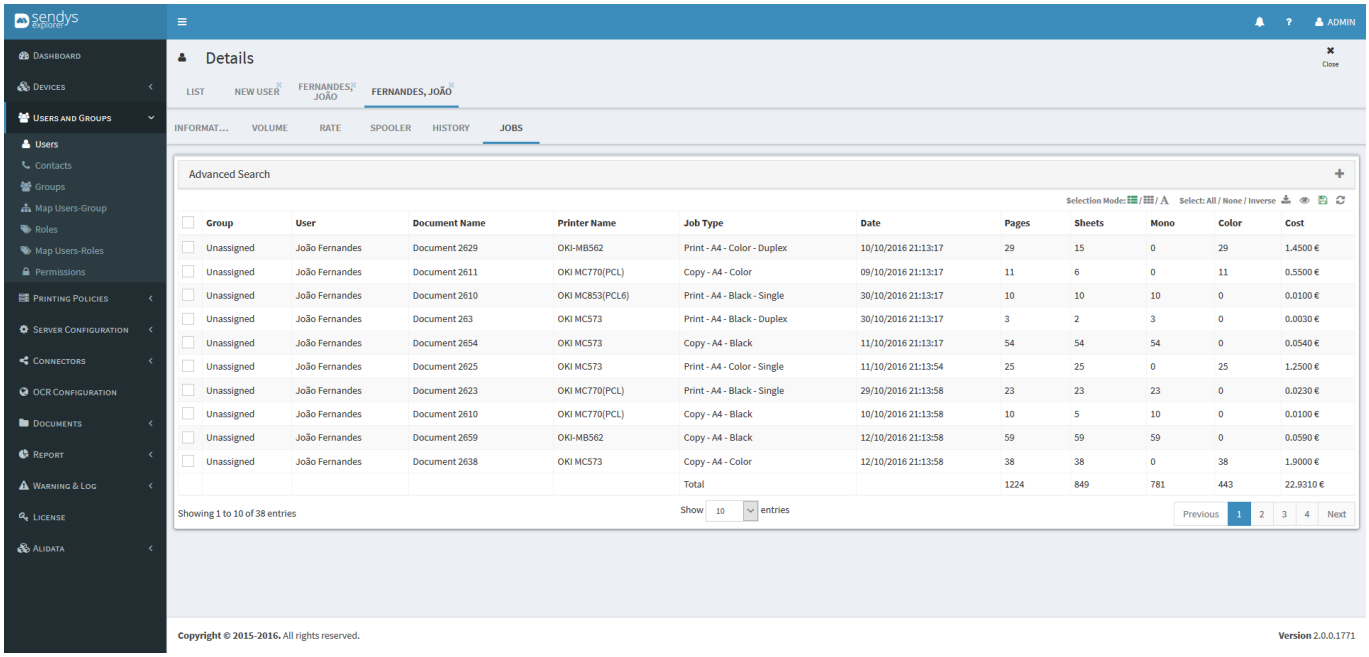


Fig. 198 - Users and Groups - User Details - Jobs view

CONTACTS

1. Click on **Users and Groups** menu
2. Click on **Contacts** menu.

On this view **Contacts** can be manged. They can be added individually or imported, edited or deleted one by one or with a selection.

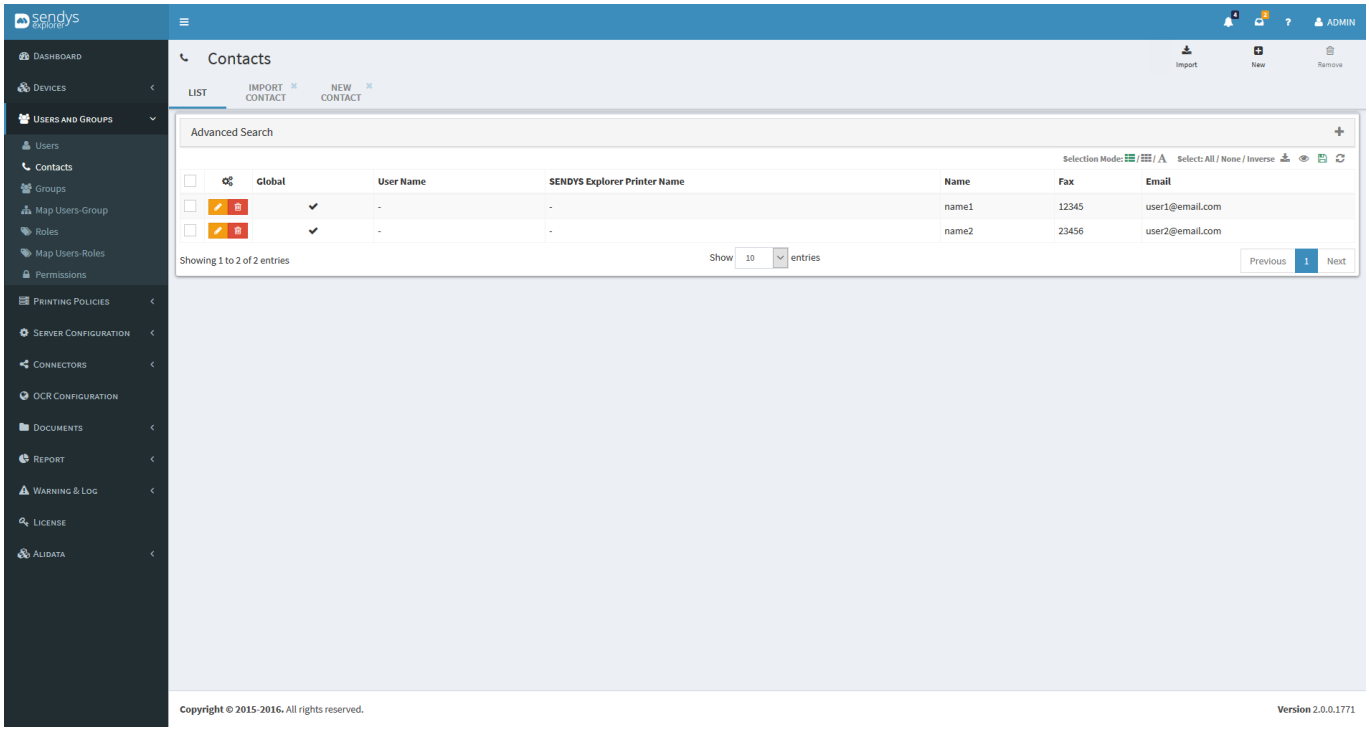


Fig. 199 - Users and Groups - Contacts

NEW CONTACT

1. Click on **New** button.

Clicking on **New** to add a new contact individually on the platform and fallow the next configurations:

Name	Details
Name	Name for the contact.
Email	Email associated with the contact.
Fax	Fax number of the contact.
Is Global	Enable/disable if the contact is global or not. Global means that every user can see that contact.
Restrict to Selected Printer	Switch button to enable/disable the option to restrict a contact to a single printer.
Printer	This option needs the **Restricted to Selected Printer** to be enable. Select the printer that only can have access to this contact.
User	Associate this contact to an existent user.
Address Group	Associate this contact to a Address group and creates a new group when one does not exists.

Table 26 - New contact details

Click **Save** to save the configurations on adding new contact or **Cancel** to cancel the insertion.

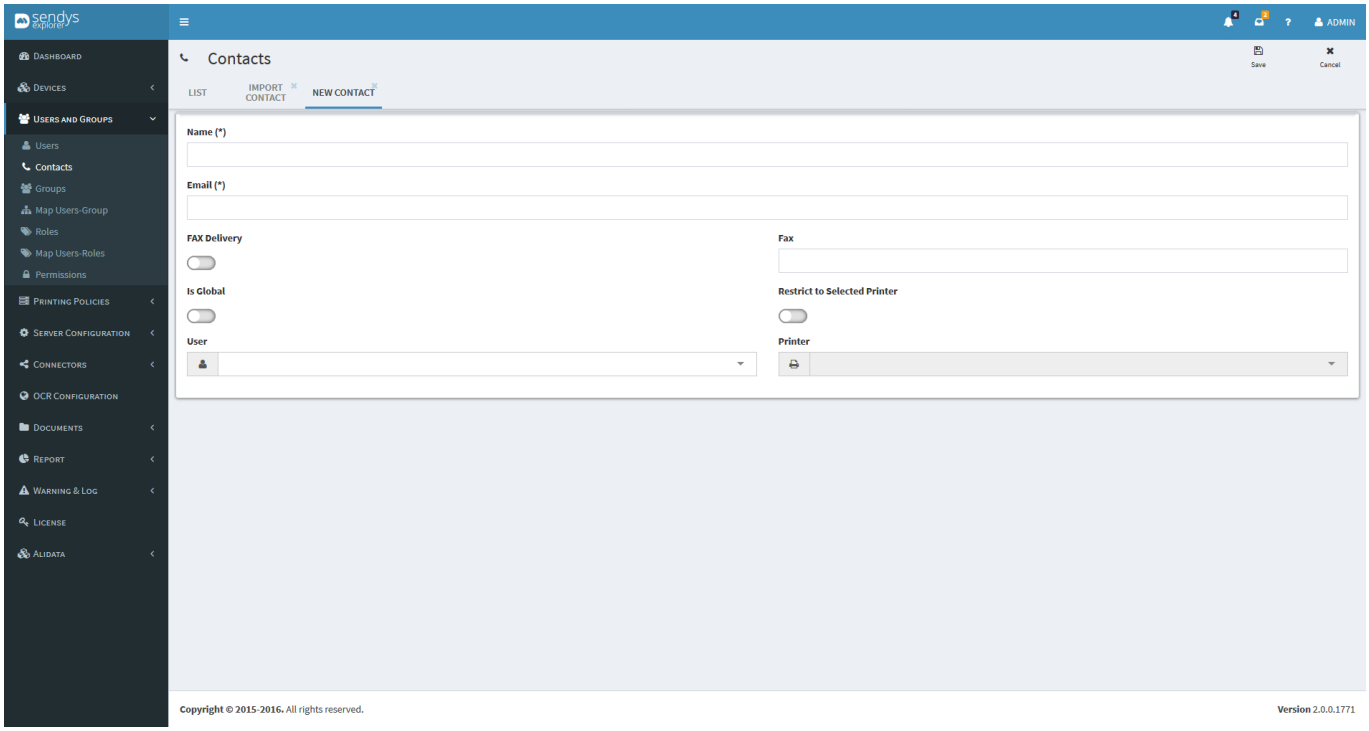


Fig. 200 - Users and Groups - Contacts - Add new contact

IMPORT CONTACTS

1. Click on **Import** button.

This option is useful when it is necessary to import more than one contact. Clicking on **Import** button a view appears (new tab) where we can import contacts with the next configurations:

Name	Details
Separator	Insert the type of separator as the next example shows.
Import Contacts Data	Insert the contacts here with the separator defined on previews field.
Is Global	Enable/disable if the contacts set is global or not. Global means that every user can see that contact.
Restrict to Selected Printer	Switch button to enable/disable the option to restrict a contact to a single printer.
Printer	This option needs the **Restricted to Selected Printer** to be enable. Select the printer that only can have access to this contact.
User	Associate this contact set to an existent user.
Name	Details
Separator	Insert the type of separator as the next example shows.
Import Contacts Data	Insert the contacts here with the separator defined on previews field.

Is Global	Enable/disable if the contacts set is global or not. Global means that every user can see that contact.
Restrict to Selected Printer	Switch button to enable/disable the option to restrict a contact to a single printer.
Printer	This option needs the **Restricted to Selected Printer** to be enable. Select the printer that only can have access to this contact.
User	Associate this contact set to an existent user.

Table 27 - Printer Details

This is an example how to import contacts:

The **Separator** choose was "**;**" and the **Import Contacts Data** field:

```
name1;user1@email.com;12345
name2;user2@email.com;23456
```

As we can see the order to insert is name then email and fax number.

Click **Save** to procced on import contacts or **Cancel** to cancel the action.

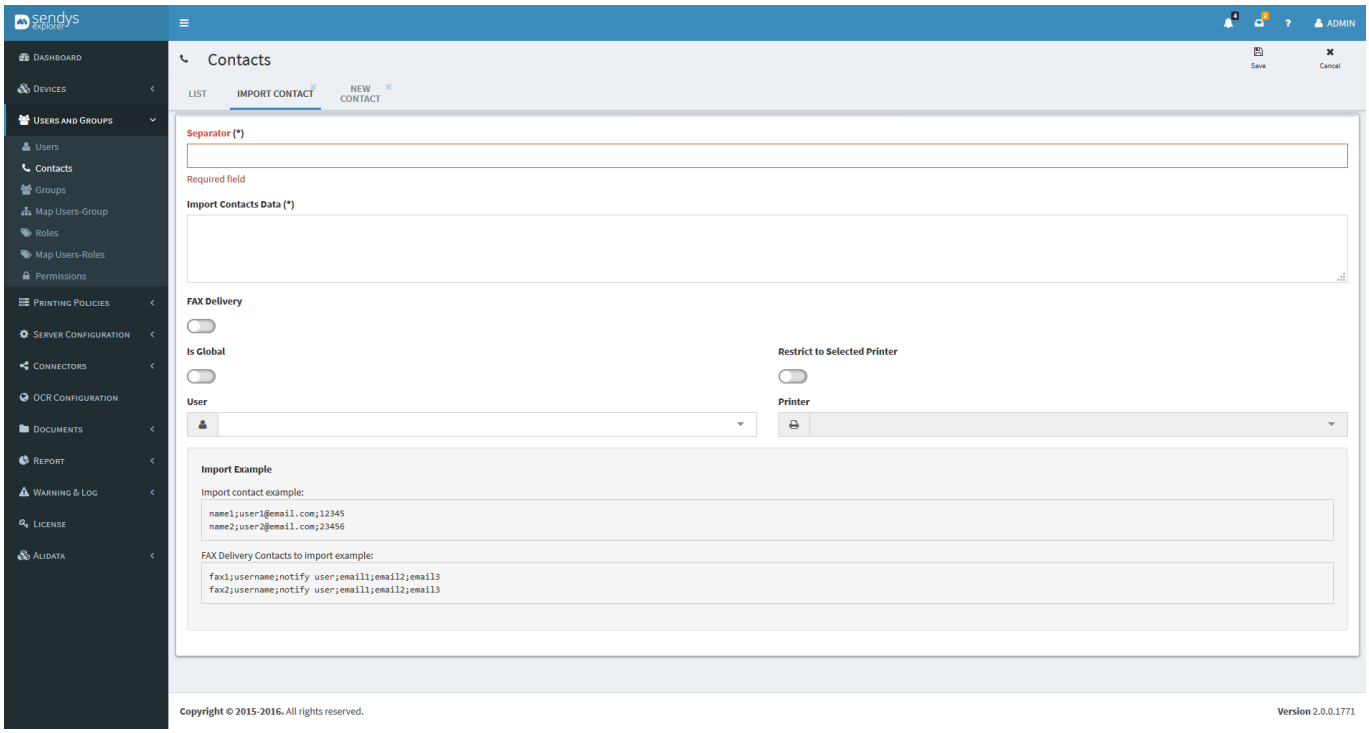


Fig. 201 - Users and Groups - Contacts - Import

GROUPS

1. Click on **Users and Groups** menu.
2. Click on **Groups** menu.

On **Groups** view it is possible to manage the user groups. Each Group can associate one or more users.

The next options are available:

New - inserting a new group individually.

Edit - edit an existent group.

Delete - delete individually a group.

Remove - delete one or more groups selected.

Import - importing one or more groups ate the same time.

Group Details - more information about the selected group can be consulted here.

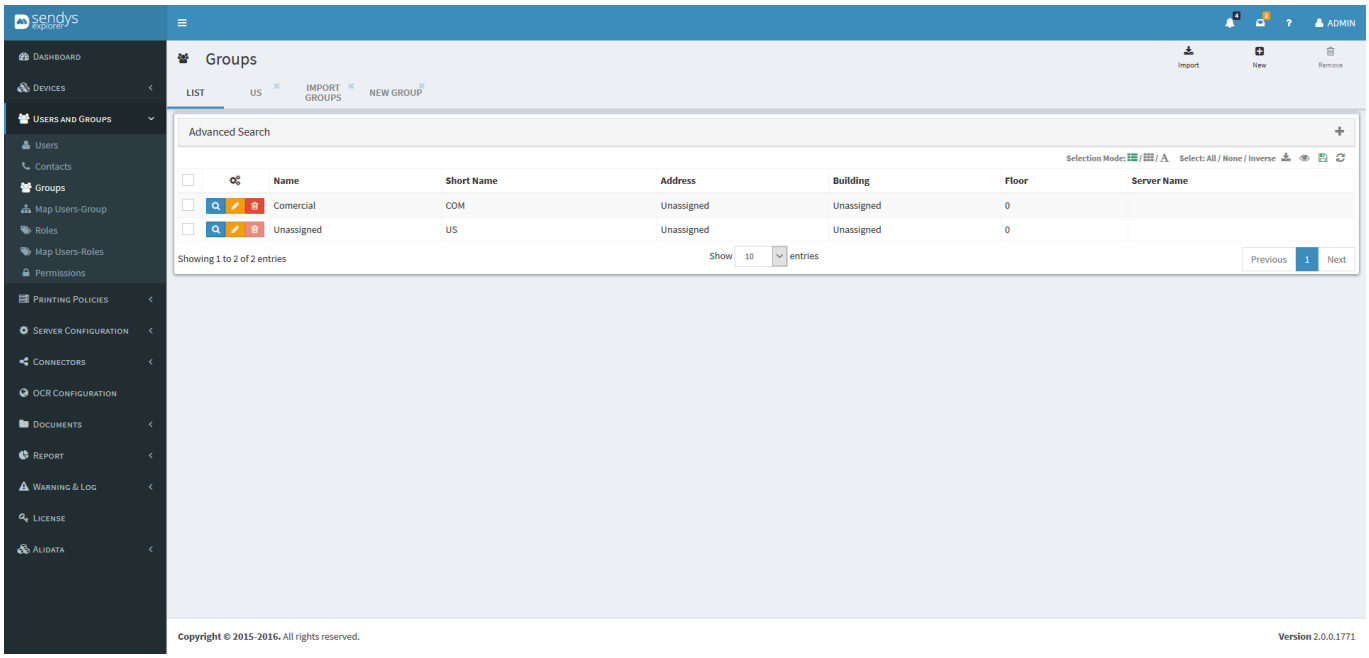


Fig. 202 - Users and Groups - Groups

NEW - EDIT GROUP

1. Click on **New** button to add a new group or **Edit** group button on the list to edit an existing group.

The **New** group option is used to insert a new group individually, using configurations on the next table. It is only need the next options:

Save - save the configurations for the new group.

Cancel - cancel the action.

On the **Edit** group option has the same configurations as the New group but the difference is on the upper menu where exist others options to work with:

Save for All Groups - Save the configurations for all groups.

Delete - delete the group edited.

Note: The configurations for group are similar to the configurations for user. But, the group configurations have priority, if they are configured, in relation with user configurations.

The configurations need on New/Edit Group on **Details** tab:

Name	Details
Name	Insert the name for the group.
Short Name	Insert the short name to identify the group.
Location	Insert the Location for the group (related with the printers Location).
Restrict Access by Location	Switch button to enable/disable the to be used on Print Policies adjusting to the group.
Description	Add a description for the group.

Table 28 - Group Details

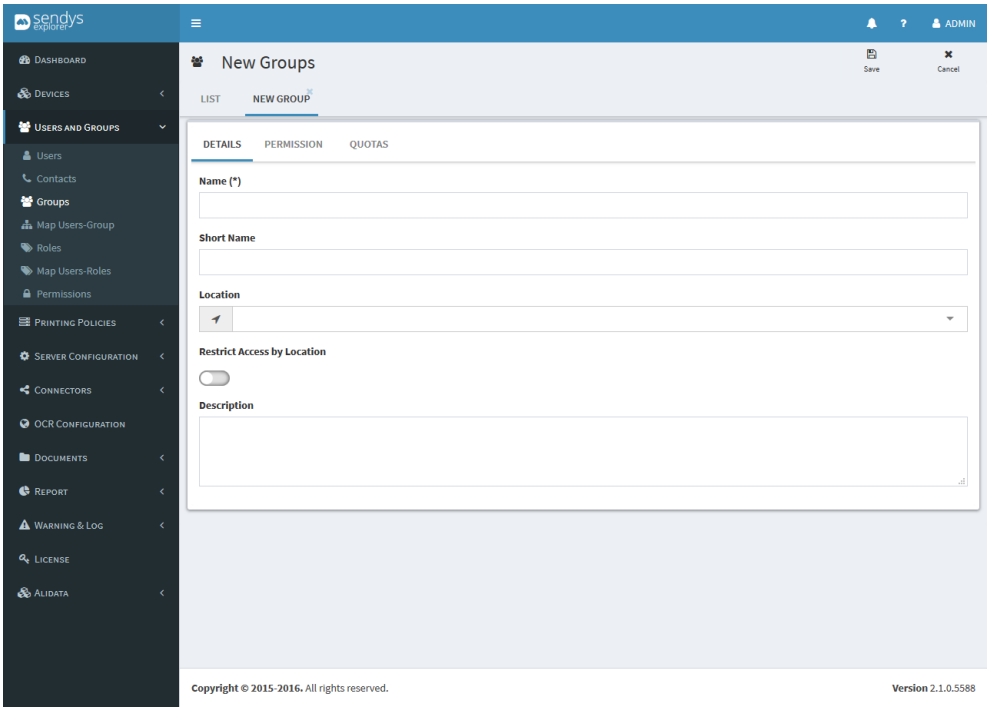


Fig. 203 –New group - details

Click **Save** to procced on adding a new group or **Cancel** to cancel the action.

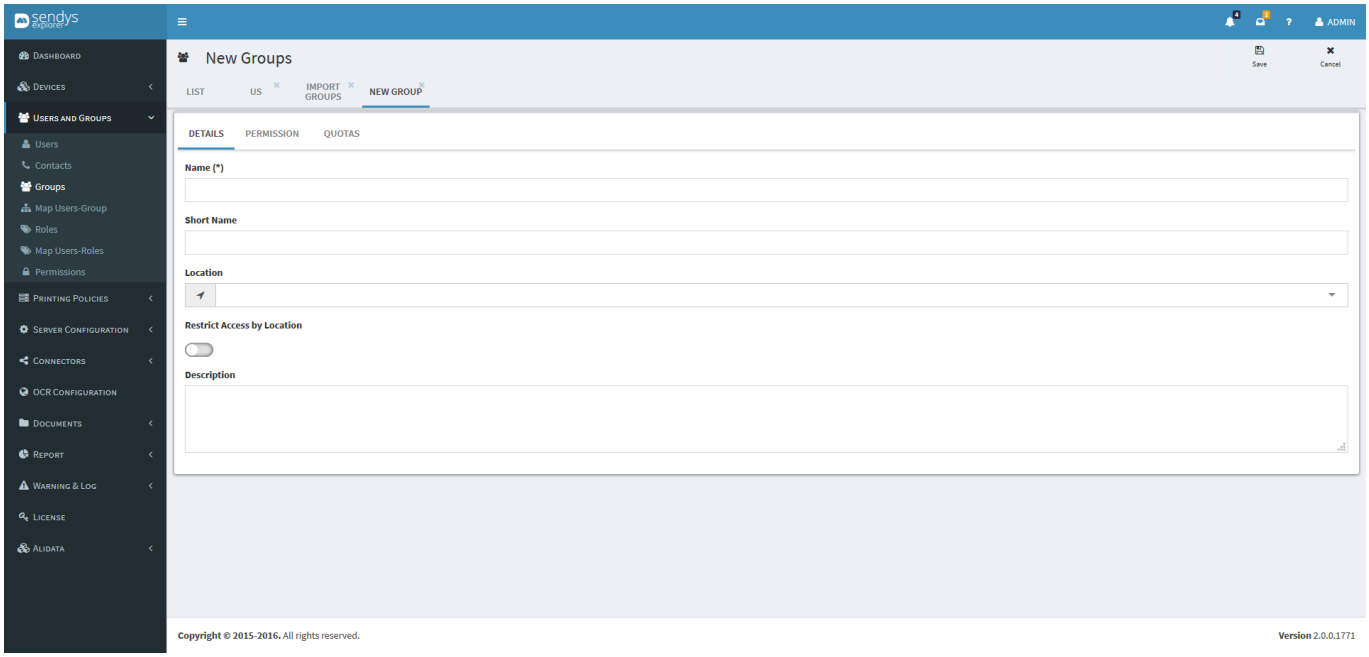


Fig. 204 - Users and Groups - New group view

IMPORT GROUP

1. Click on **Import** button to add a new group.

To import one or more Groups, follow the next configurations:

Name	Details
Separator	Insert the type of separator as the next example shows.
Group list	Insert the groups to import with the separation inserted on the previous field.

Table 29 - Import group details

This is an example how to import groups:

The **Separator** choose was "**;**" and the **Import Contacts Data** field:

```
GPA;Group A
GPB;Group B
```

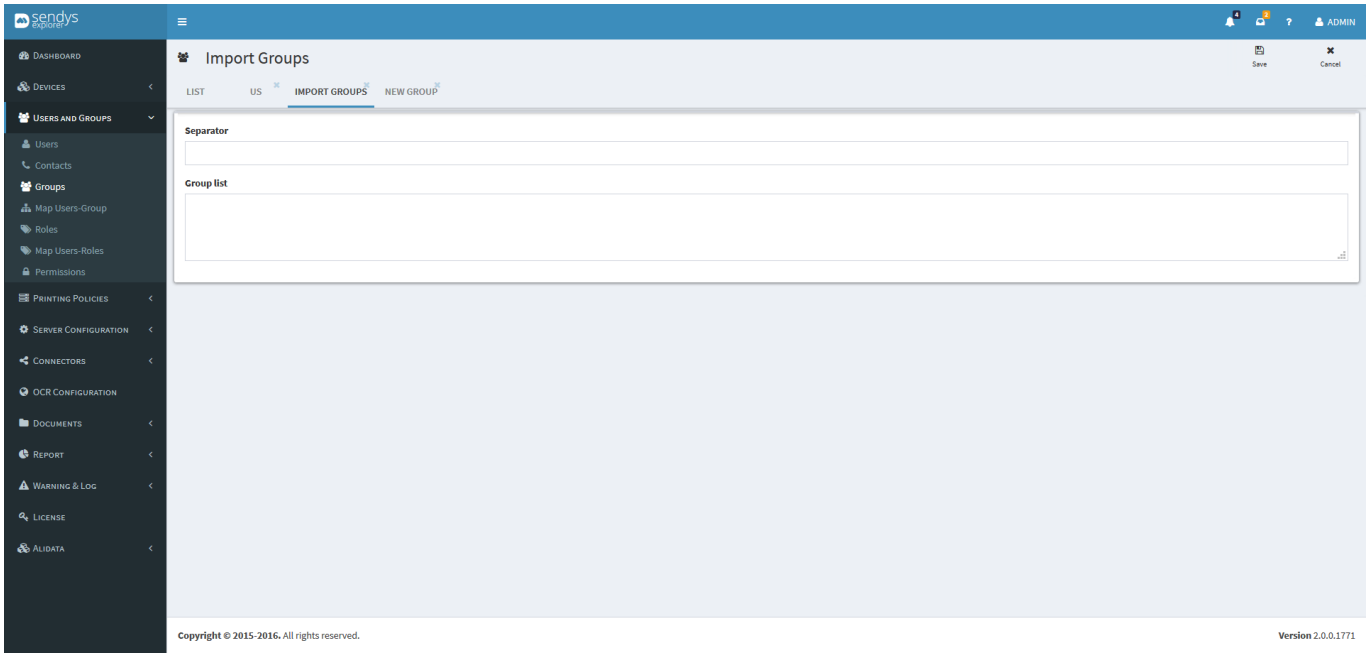


Fig. 205 - Users and Groups - Groups - Import group view

GROUP DETAILS

1. Click on **Group Details** button on the group list.

Clicking on **Group Details** we can consult the information aggregated to the selected group. Navigate between tabs to consult more information.

- On **Volume** tab contains information about the group and some statistics associated too.

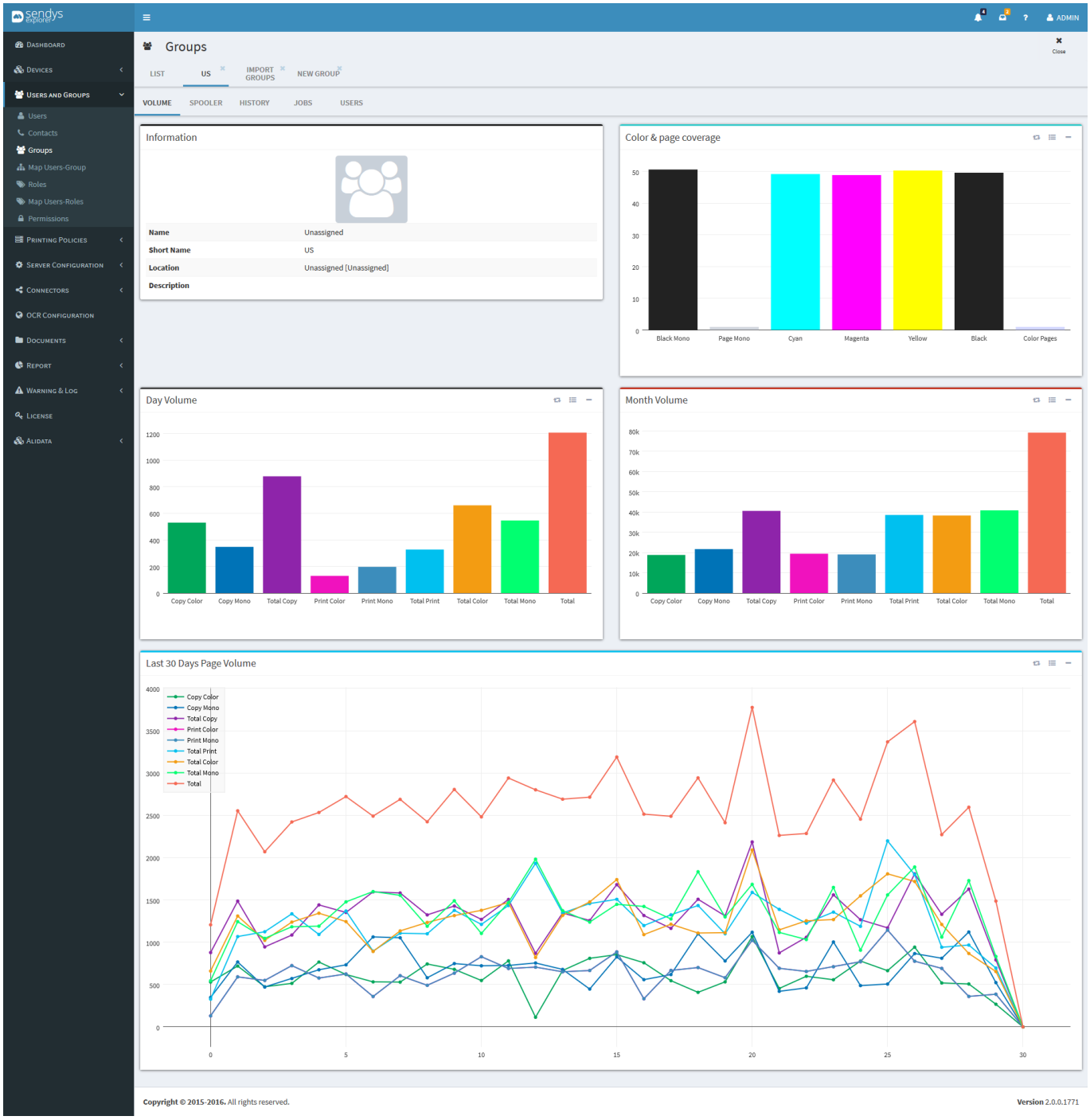


Fig. 206 - Group details - volume

- On **Spooler** tab a list of documents on Windows Spooler are shown.

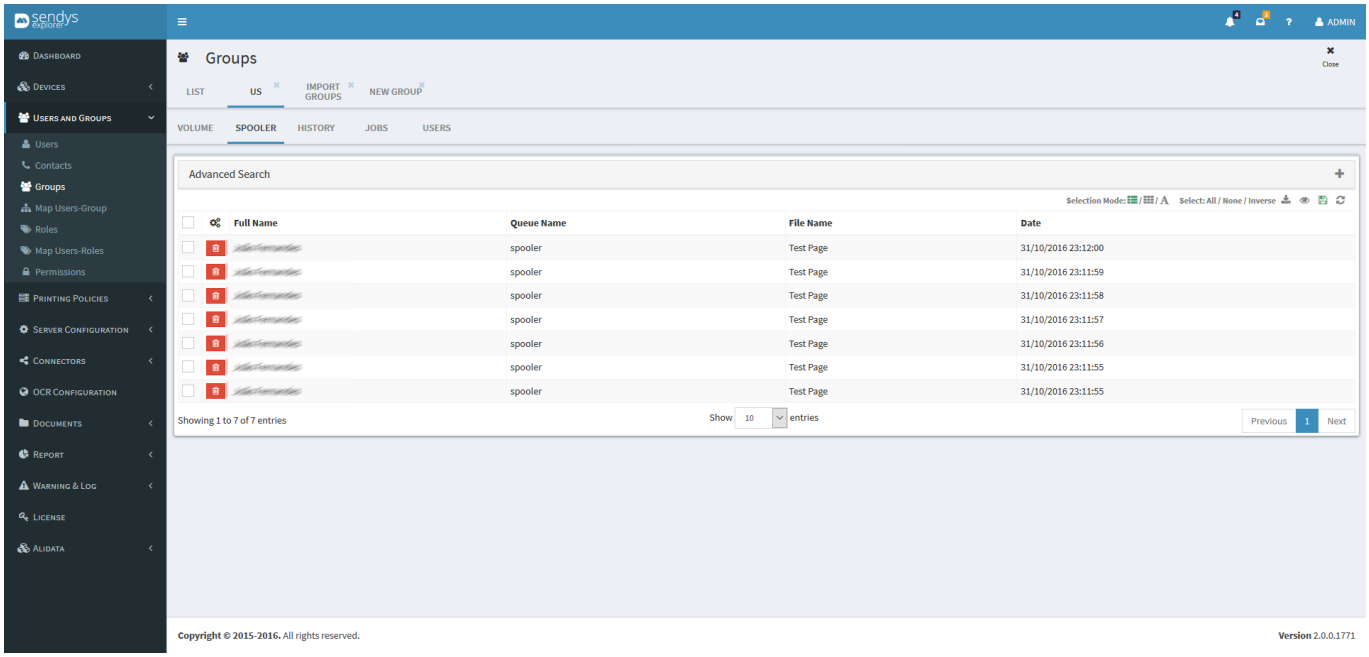


Fig. 207 - Group details - Spooler

- **History** tab shows the document print history associated by the selected user.

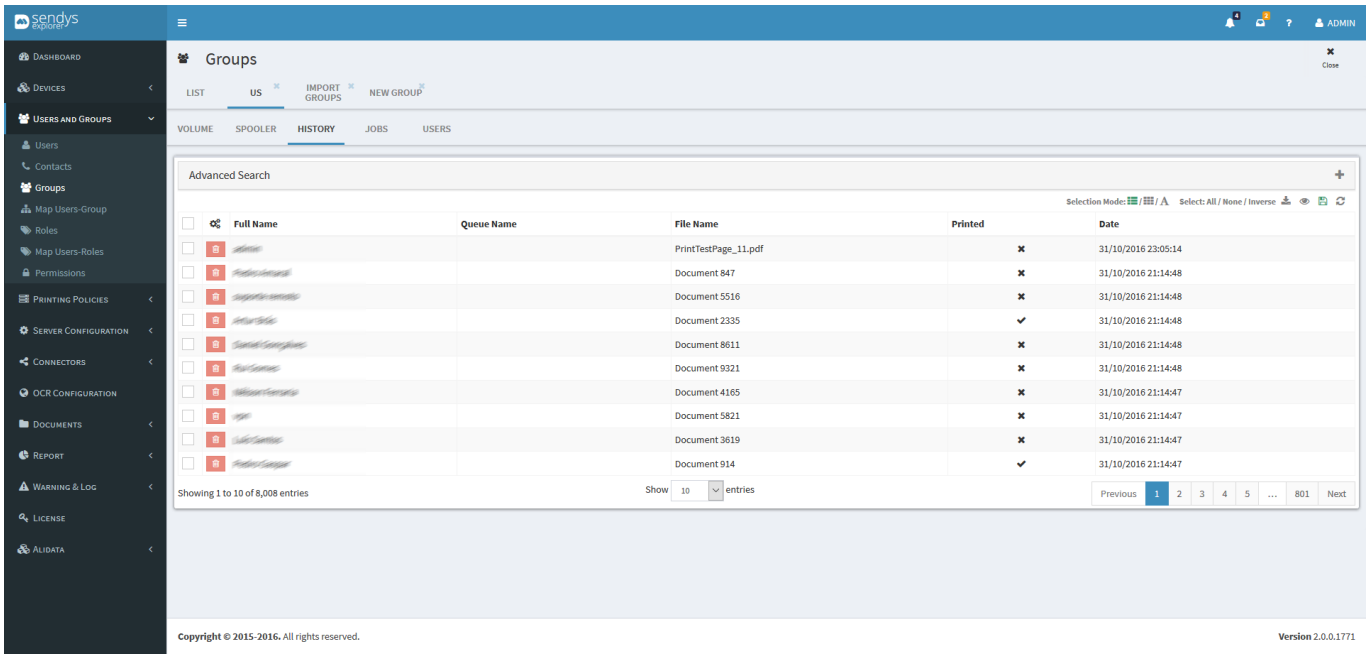


Fig. 208 - Group details - History

- **Jobs** tab show all documents on the selected group.

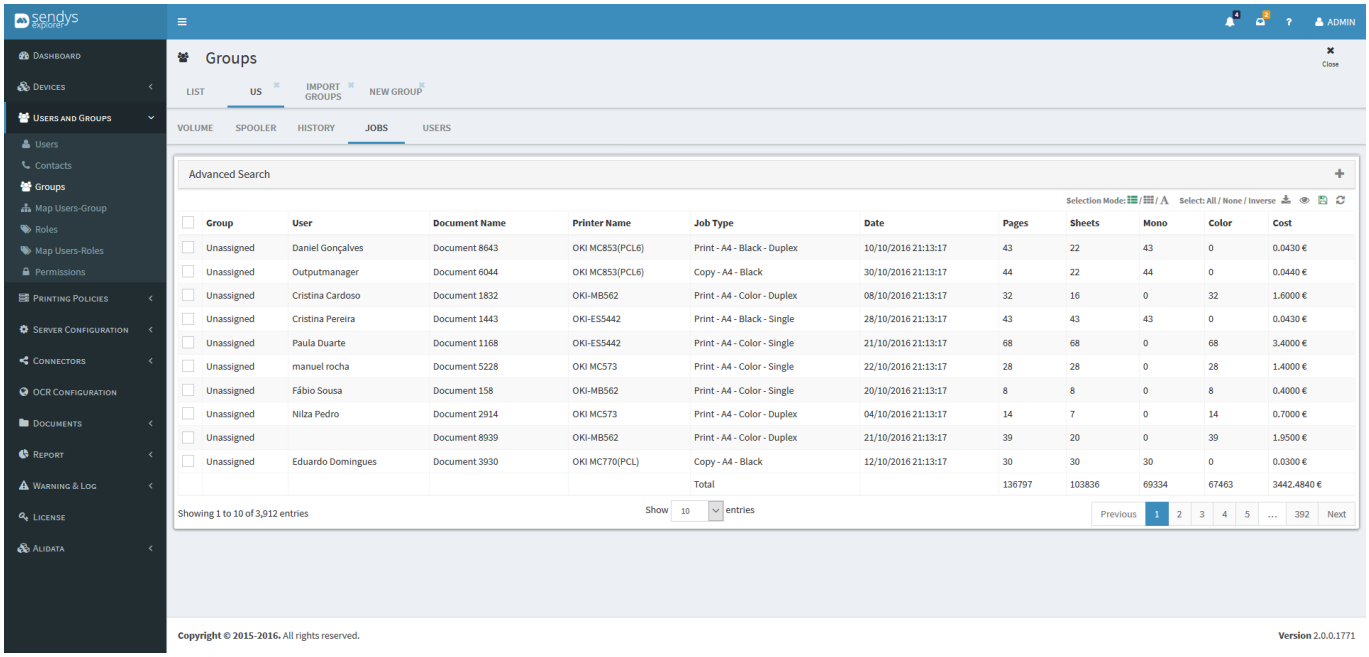


Fig. 209 - Group details - Jobs

- **Users** tab show all users associated with the group selected.

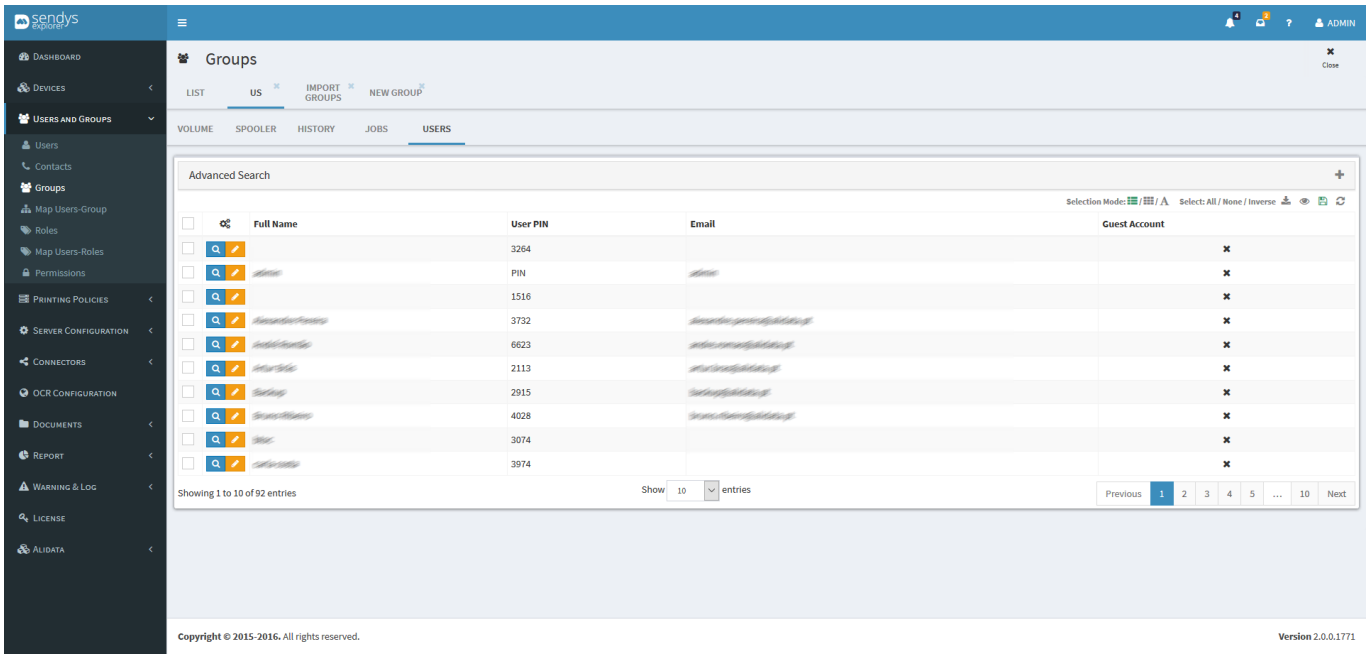


Fig. 210 - Group details - Users

MAP USERS-GROUPS

1. Click on **Users and Groups** menu.
2. Click on **Map Users-Groups** menu.

On this view we can manage the connection between groups and users. Groups creation and managing are done on the previous chapter.

If is necessary to change one or more users from a group to other. If it is necessary to change a user from a group, select the pretended user from the users list and then select the group and **Save** the alteration.

Using button **Refresh** to refresh the list of users and the list of groups.

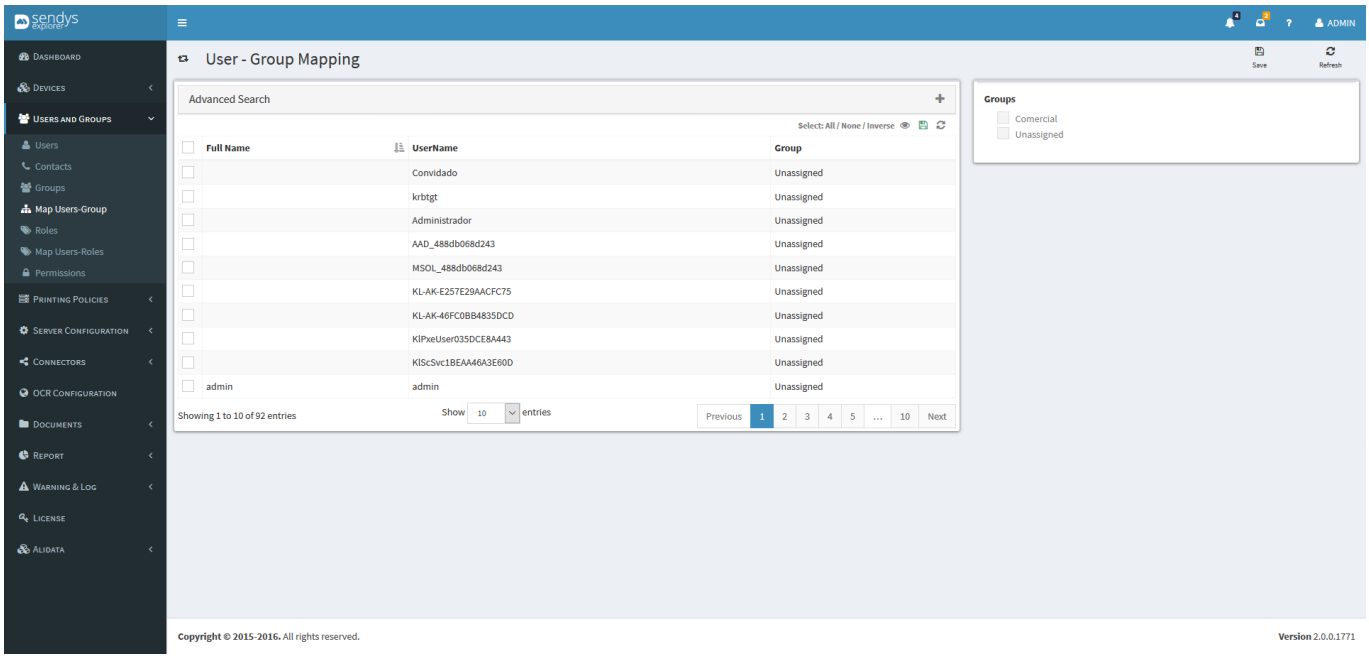


Fig. 211 - Users and Groups - Map Users-Group

ROLES

1. Click on **Users and Groups** menu.
2. Click on **Roles** menu.

The Roles view is used to manage the type of roles/access that are attributed to users on the platform. The function of this roles will be shown on the next chapters.Those defaults roles are:

- **Administrator** - role that grant administration access on platform.
- **End User** - role that grants basic user access on platform.

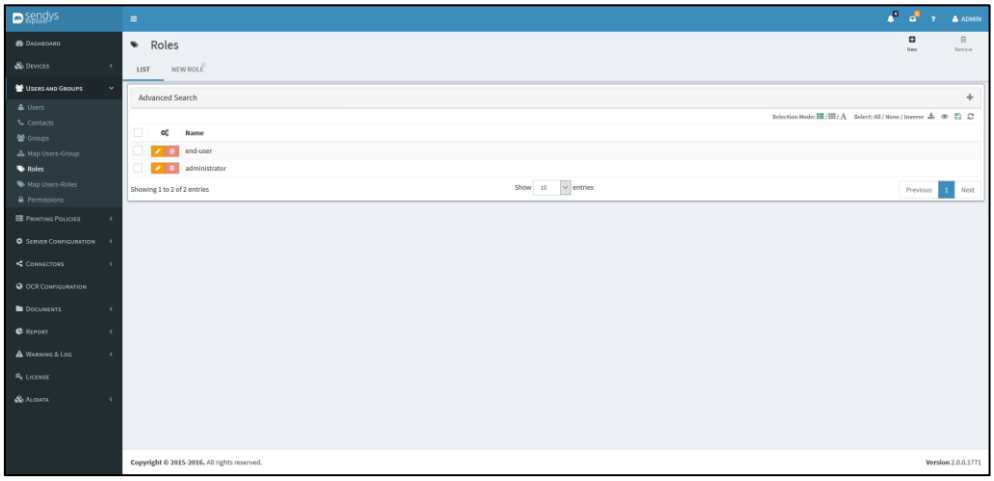


Fig. 212 - Users and Group - Roles

Adding a new Role, click on button **New** and the new view appear. Insert the Role Name field to name the role and then save the changes on button **Save** or **Cancel** to cancel the action.

The Roles can be edited to change their Role Name. Click **Save** button to save or **Cancel** to cancel the action.

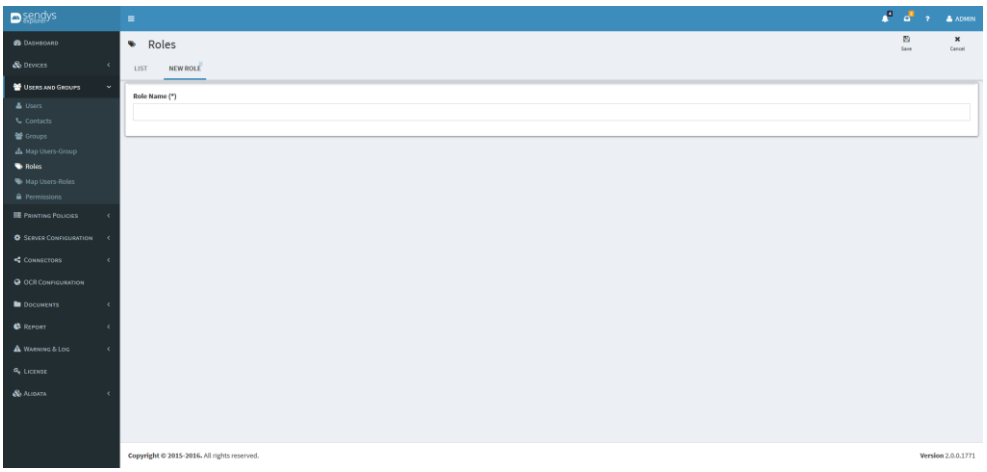


Fig. 213 - Users and Groups - New Role

MAP USERS-ROLES

1. Click on **Users and Groups** menu.
2. Click on **Map Users-Roles** menu.

The Map Users-Role is used to manage the user roles on the platform. Roles creation are shown on the previous chapter.

When it is necessary to change a user role, select the user (left table) and using the right table (roles list) to change the role.

Click button **Save** to save the action or **Cancel** to cancel the action.

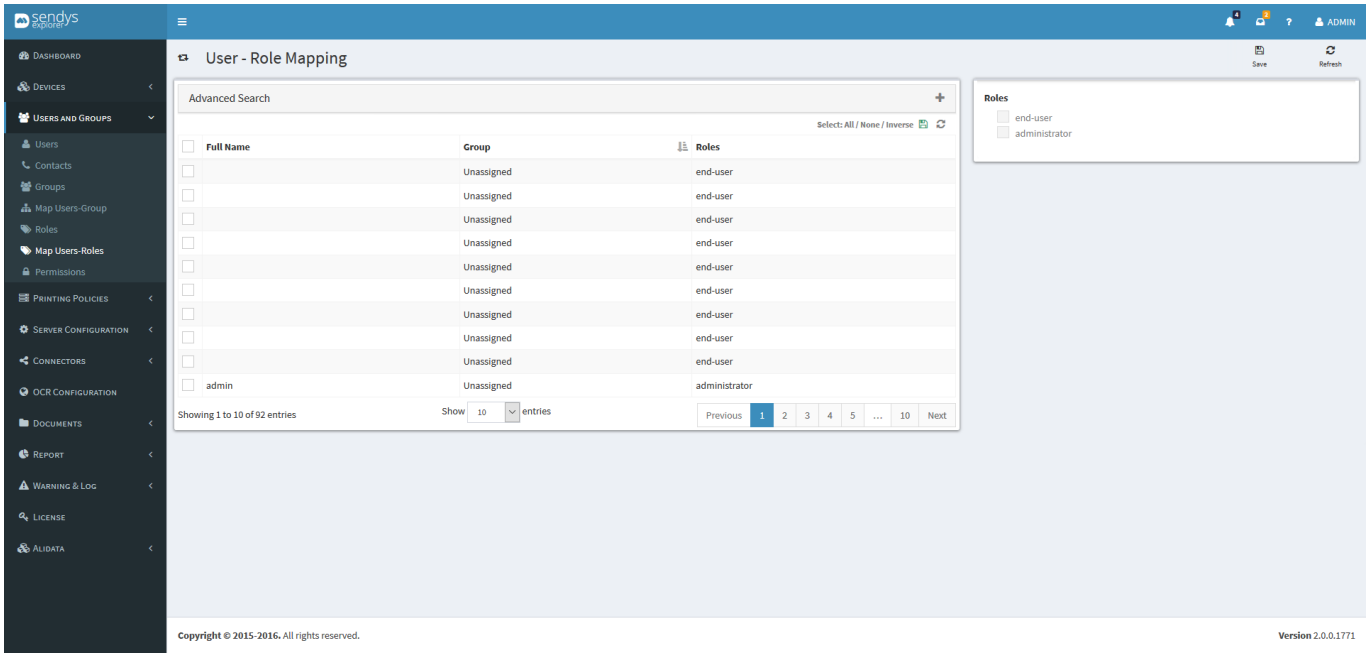


Fig. 214 - Users and Groups - Map Users-Roles

PERMISSIONS

1. Click on **Users and Groups** menu.
2. Click on **Permissions** menu.

The permissions view is used to grant access or not to the features on the platform. These permissions are defined by the existing user's roles.

On installation there are two defaults roles created (Administrator and End-user). If is necessary to create another role the administrator must go on Roles menu and procced on the role creation.

On this view exists the same button options for **Save** actions and **Cancel**. Another button option is shown (**Toggle Add**) that toggle on the view, options to search and define the permissions pretended for the role.

The options are:

Name	Details
Roles	Select the role to apply permissions.
Views	Textbox to search/filter for the views to apply the permissions.
Default Permission	Define the type of permissions for the view selected by clicking on box to check the type of permissions to apply on the role.

Table 30 - Printer Details

The **Default Permissions** type are:

Read - permissions to only access.

Delete - permissions to delete data.

Edit- permissions to edit data.

Add - permissions to add data.

Export - permissions to export data.

Access Group - permissions to give access to group role.

Access All - permissions to all type of roles.

Note: some of the Default Permissions type are applicable in to all views.

After this Toggle Add menu there is a list of **Details** about the permissions. In this list, all views in the platform are listed and they can be expanded, so we can consult the roles with the respective permissions for each view. For each role on every view, the **Default Permissions** are listed so they can be changed any time using the checkbox to able or disable.

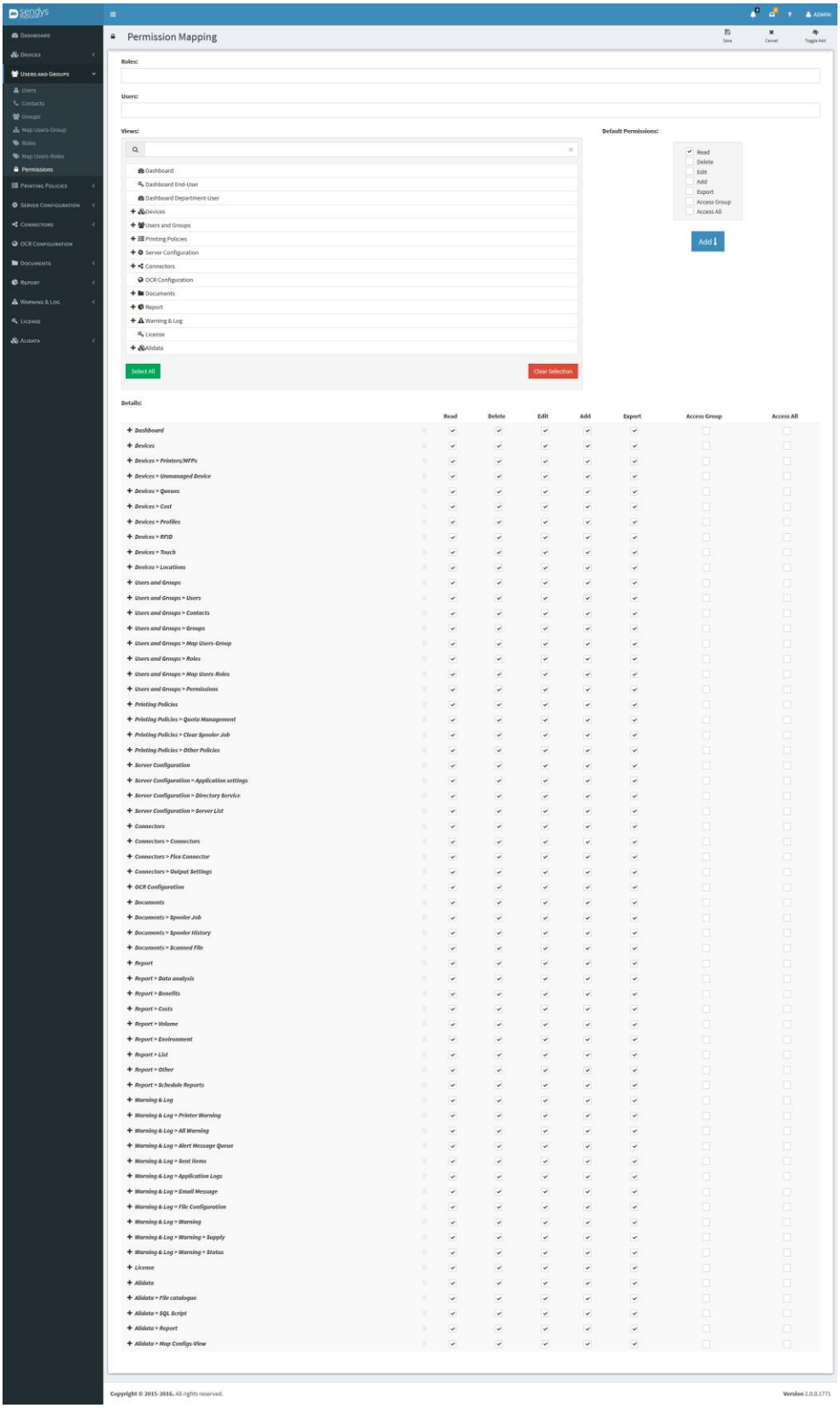


Fig. 215 - Permissions mapping

CARDS

OVERVIEW

Application gives you a several possibilities for card registration, sign in a after that assign the card or simple swipe the card and sign in after card swipe to make the registration of it.

You have the ability to add cards to the system and use this has guest cards “Temporary cards on Sendys” that you can use for internal users. For example, if some of the users Guest Cards and some of the company users forget is card he can associate the guest card for an amount of time keeping is original card on the system.

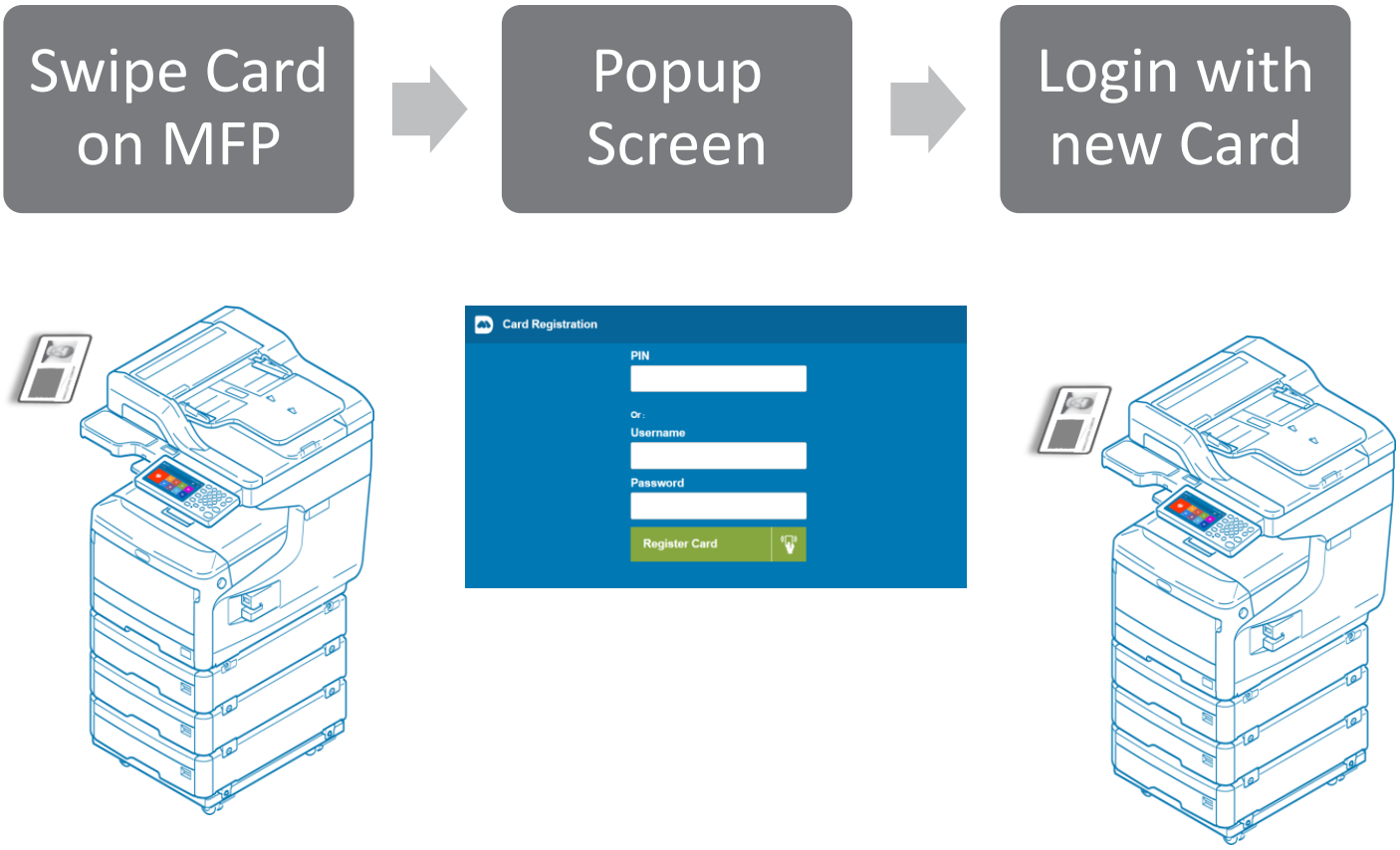


Fig. 216 – Card registration process.

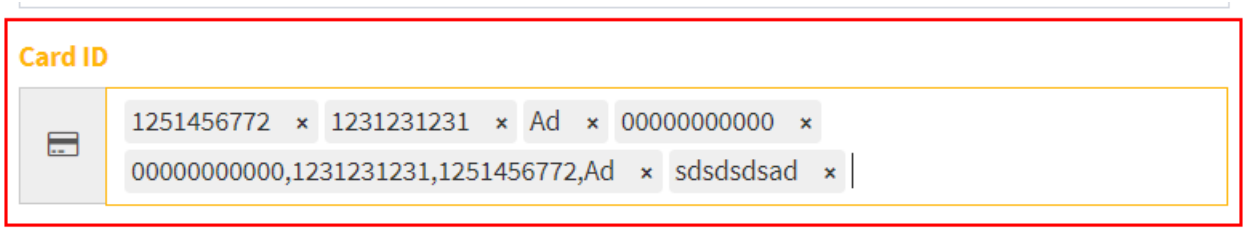


Fig. 217 – User multi-card association.

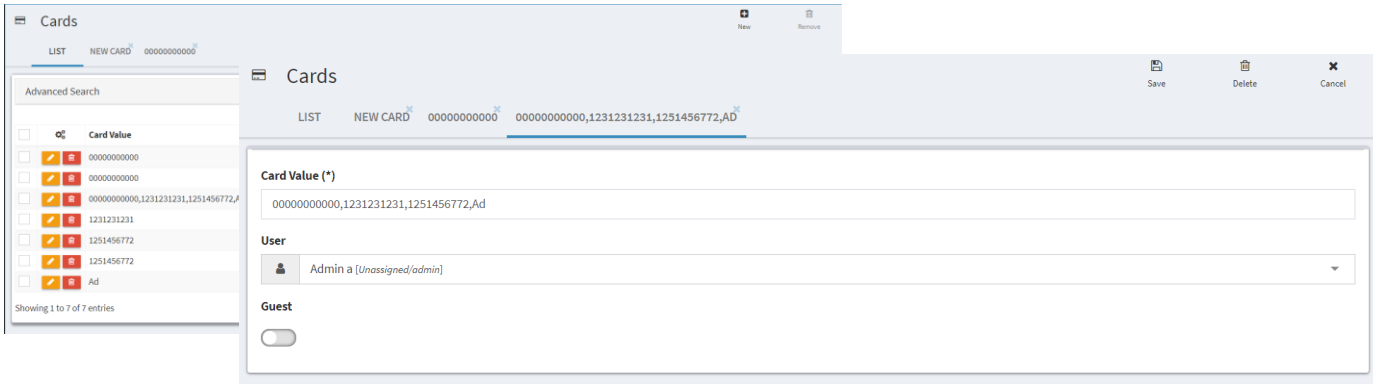


Fig. 218 – User Guest card creation.

COST CENTER

Cost-Center is a way to assign cost to specific projects and then retrieve this information in a report that is design to this end, when working with cost-center all jobs “Copy/Print” will be assigned to this specific cost center and the best way to do this is to force cost center selection has the first screen.

You have several cost center options, add, edit, remove and also cost center mapping where you map the cost center to the specific users that work in a specific project.

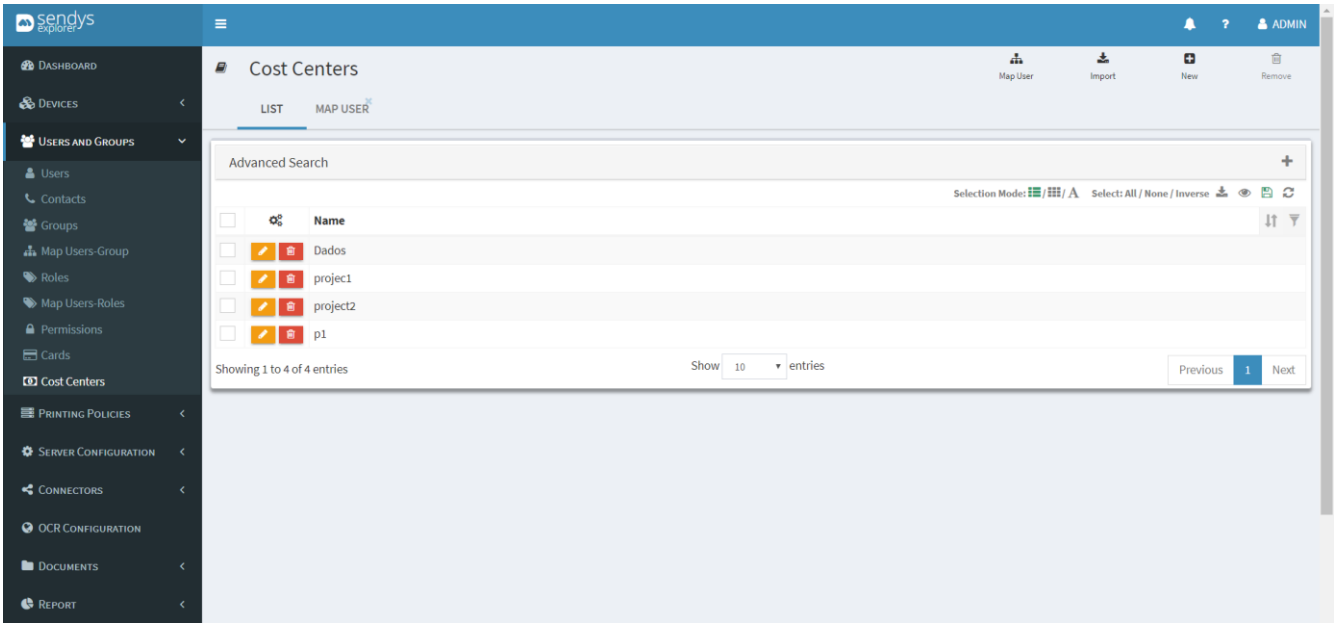


Fig. 219 – Cost center.

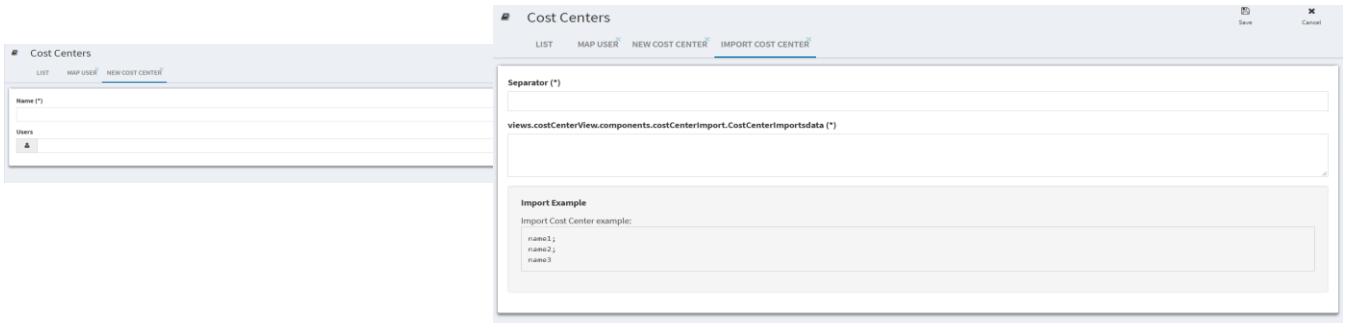


Fig. 220 – Import insert cost centers.

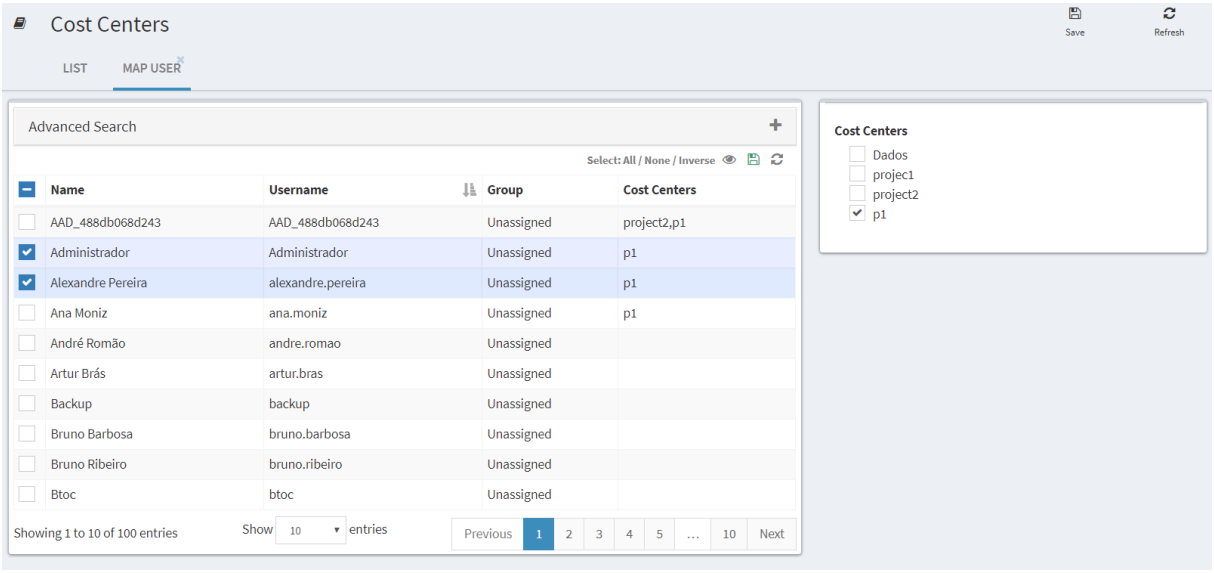


Fig. 221 – Cost-Center user mapping.

To force cost center selection on the device you need to follow the above steps :

1. Reconfigure the dvice url with the follow link
2. Link on the device : http://[ServerIP]:50091/scan.aspx?HardLink=costcenter
3. Go to Users and Groups> Users > select the user
4. Enable Cost Center

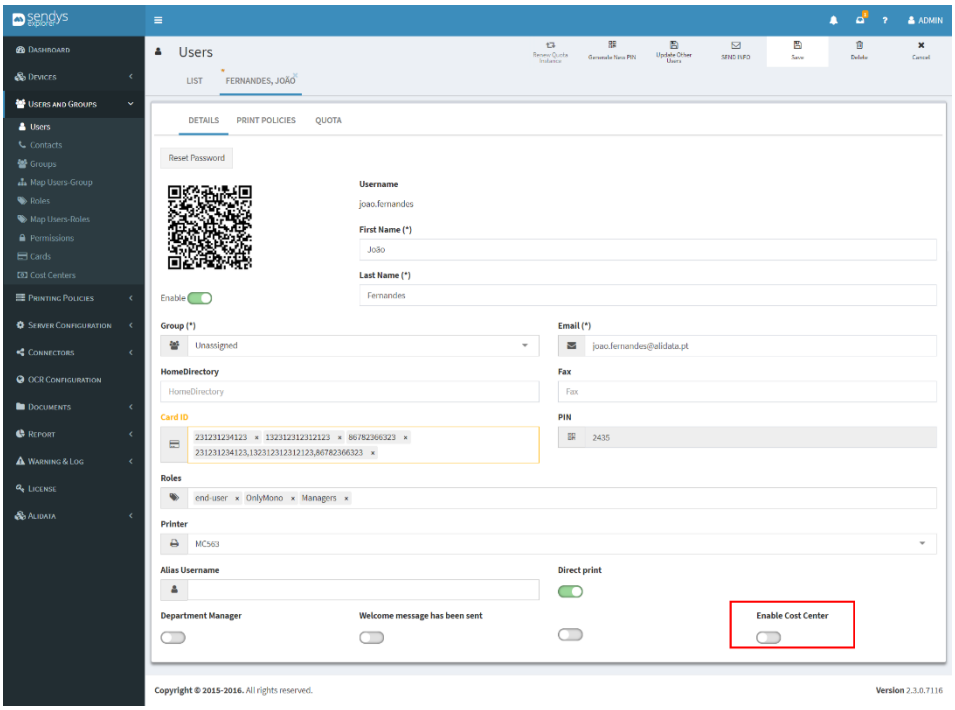


Fig. 222 – Enable User Cost-Center.

5. Click “Save”
6. Then on device when the user sign specify that the first screen is the EWB application with the previews defined URL

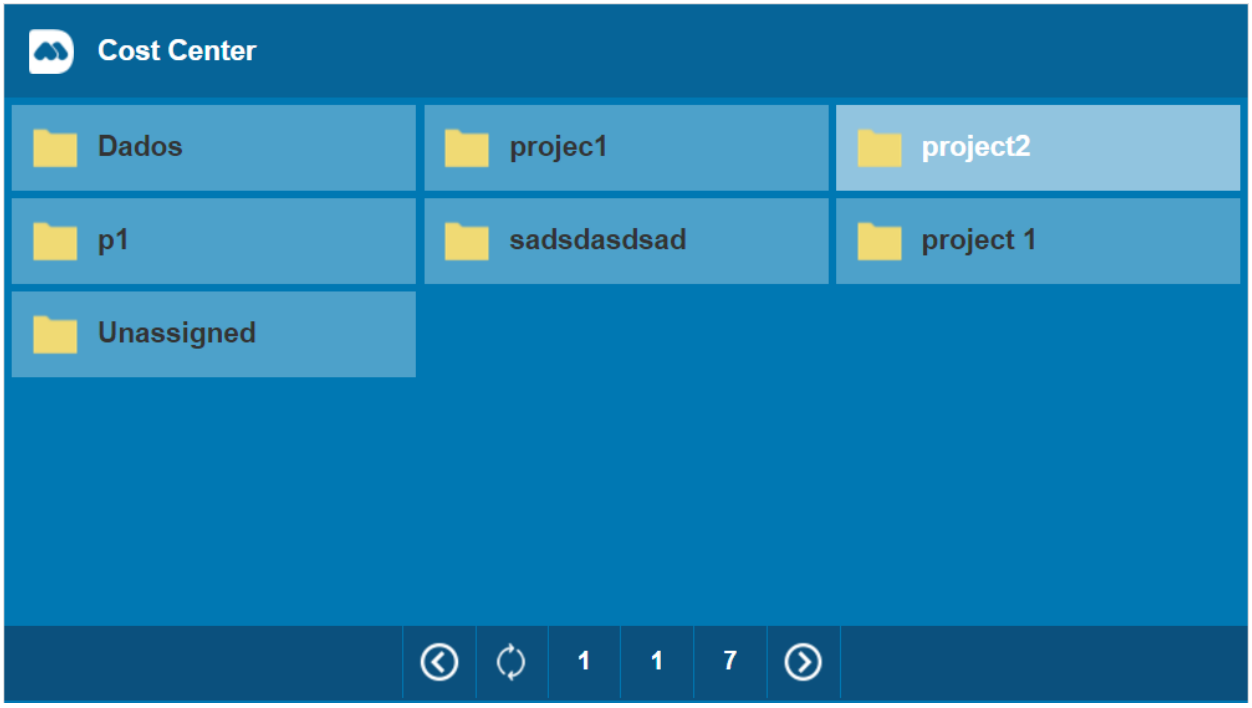


Fig. 223 – Cost-Center Device Selection.

7. All jobs done after cost center selection will be assigned to the specific selected CostCenter/Project

PRINTING POLICIES

On Printing Policies, we can manage policies defined on Output Manager that are related with printing for group/users.

These options represent configurations that are connected with others configurations on others menus. So if it is necessary, we need configure some options that affects this menu so they work on properly.

On **Printing Policies**, we can control the printing job flux and define the way they should work for a group/user, working with rules or even with scheduling.

QUOTA MANAGEMENT

Quotas are part of the application and independent of users, groups, devices and roles. But you can create different types of quota and after you create with the specification that you desire you can assign the quotas to users/Groups/Devices or roles.

You can define 3 different quota types:

- Volume, a simple volume independent if it is color or mono
- Color, where you can define different quantities for color and mono
- Value, where you define specific quota as a value and then will discount the print specified cost on the quota.

1. Go to Printing policies>Oher Policies>Other tab
2. Specify the working quota mode

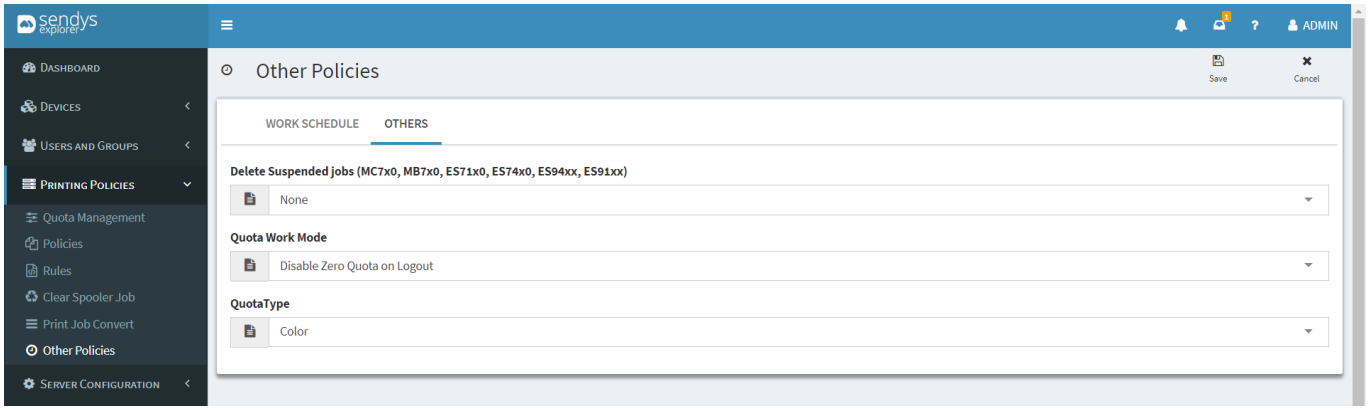


Fig. 224 – Define quota type.

3. Click "**Save**"

To define a quota follow the above steps :

1. Go to Printing policies>Quota Management

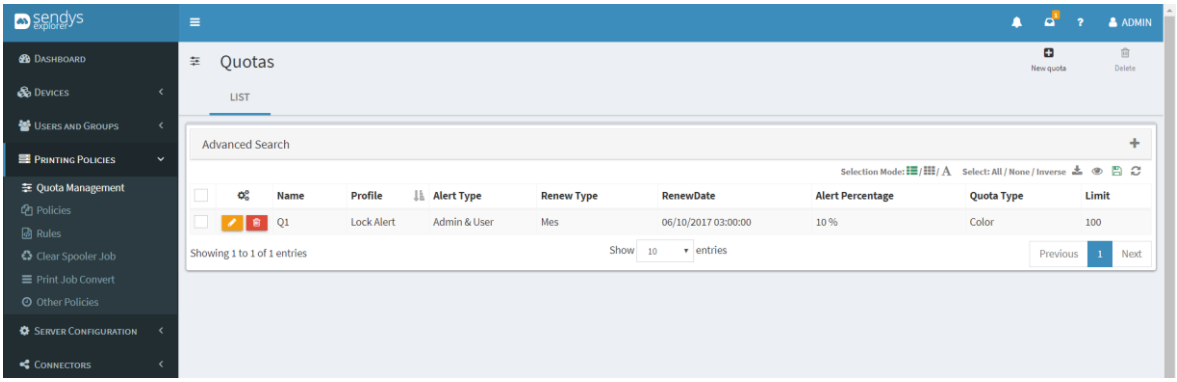


Fig. 225 – Quota Managment.

2. Click Add
3. Specify a name
4. Specify a profile
5. Specify Alert Type
6. Specify if quota has some renew type
7. Select the alert percentage
8. Specify the prioprity
9. Select a limit for Volume/MONO/Color/Value
10. Select discount type
11. Select assign type
12. Assign the it

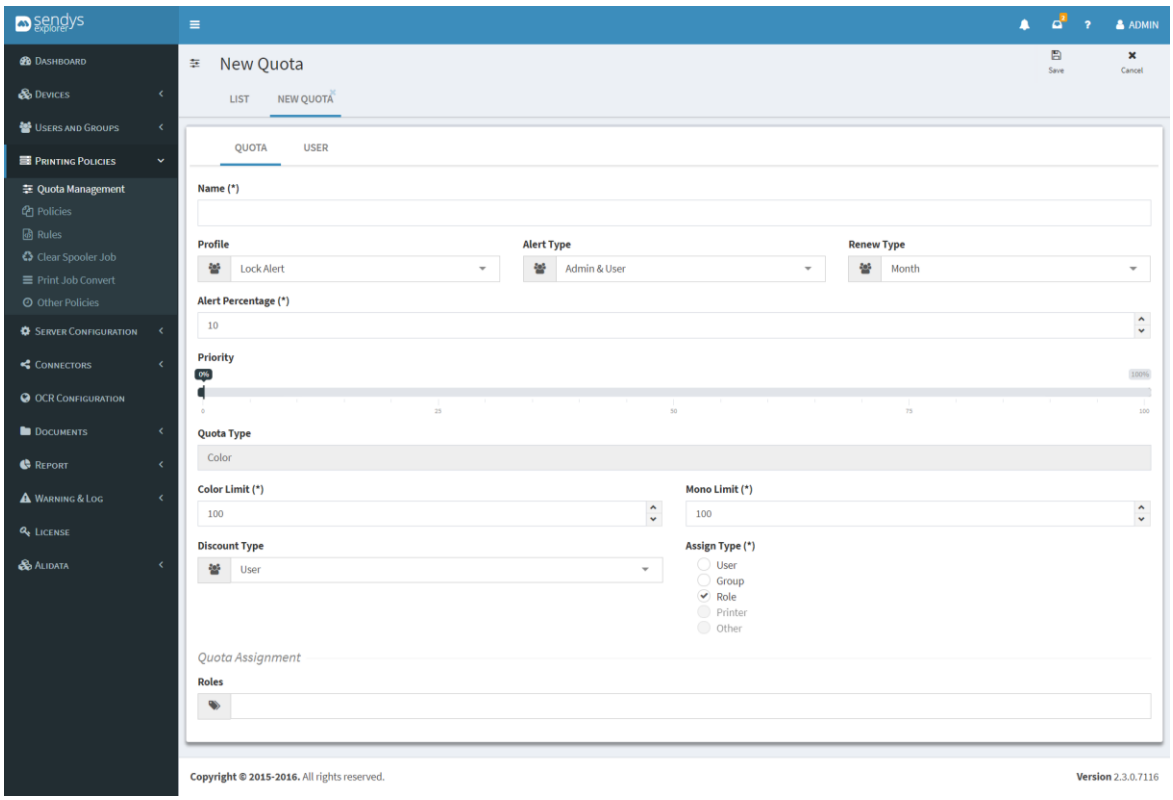


Fig. 226 – Add Quota.

13. Click **Save**

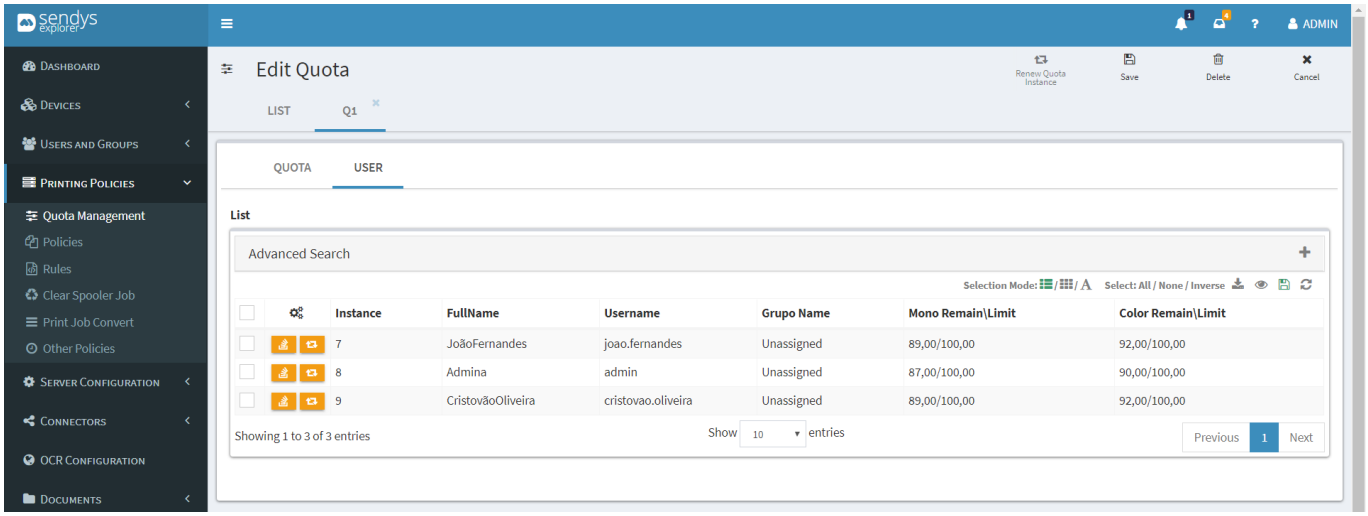


Fig. 227 – User quota instance.

POLICIES

PERMISSIONS

In policies, you have the ability to define application permissions and working modes “Policies”, you can increment permissions “OR” or you can have the conjugation of the permissions “AND”.

To create or define standard permissions just use the follow steps :

1. Select policy type permission
2. Select the operation AND/OR
3. Specify a name for the permission

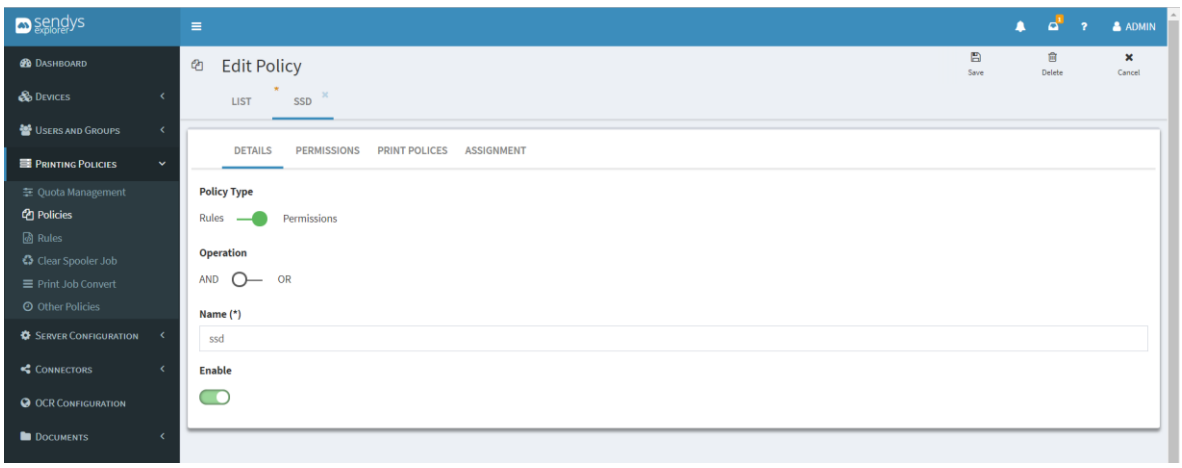


Fig. 228 – Policies permissions based.

4. Click on Permission tab
5. Specify the permissions that you need to have

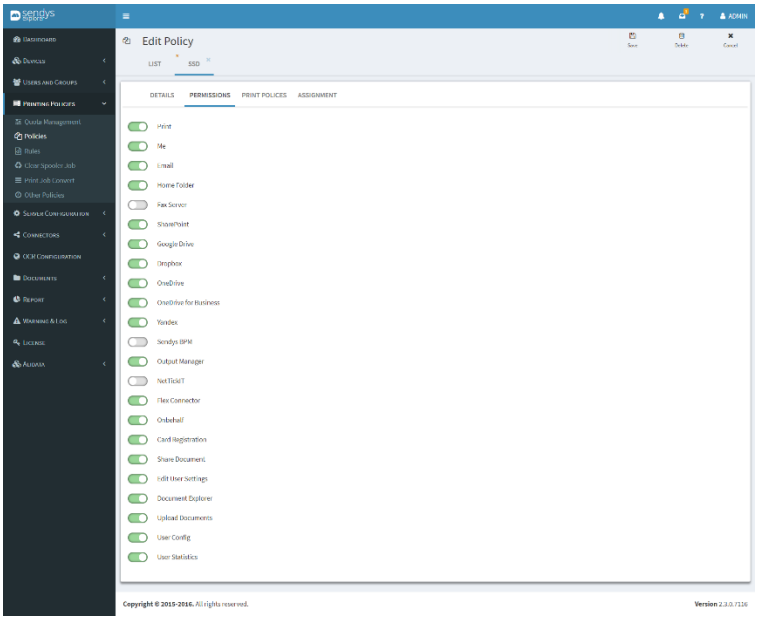


Fig. 229 – Policies permissions tab.

On **Permission** tab, accessible on Adding or Editing user, the access on platform for content can be managed. Administrator can define if the selected user has or not access to connectors or actions on the printers and platform portal. To change the options only need to turn on/off the switch on the pretended option.

Note: The connectors and actions available depends on some configurations, the license used on installation or/and the printer device type.

6. Click on Print Policies tab
7. Specify the Policies that you need to have

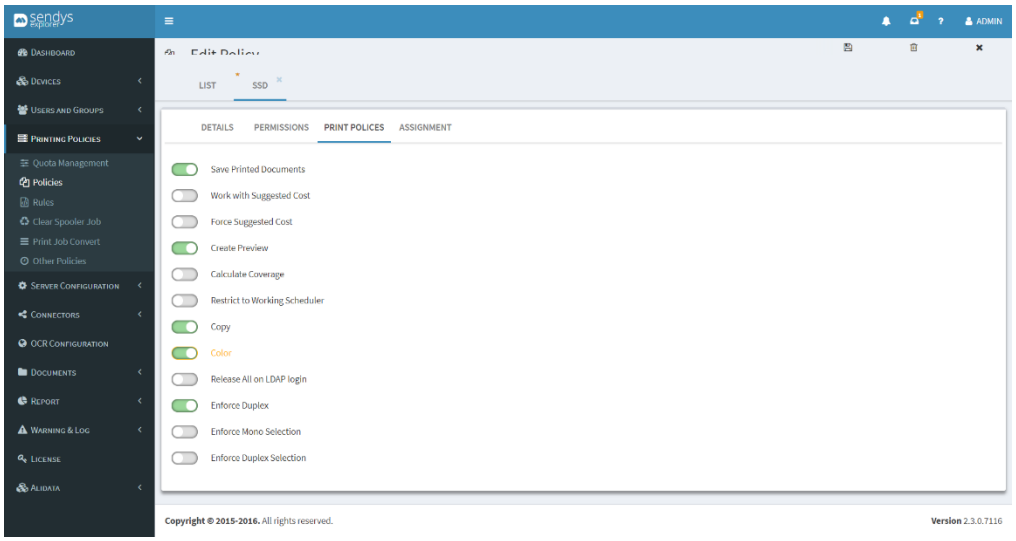


Fig. 230 – Policies Print Policies tab.

On **Print Policies,** accessible on Adding or Editing user, some policies can be defined for the selected user. To activate or deactivate use the switches.

Name	Details
Saved Print Documents	Enable/disable the option to save a document after print (History option).
Work with Suggested Cost	Enable/disable the option that the platform sends an email to the user suggesting a printer where print job is cheaper.
Force Suggested Cost	Enable/disable the option where forces a print job to be on print where the print job is more cheap, between compliant devices (devices are defined as compliant when they have the same Queue Name located on Printers/MFP's menu). Depending on **Minimum Redirect Volume (page)** located on Print Policies -> Other Policies and also the group **Restriction Configuration** for Location.
Create Preview	Enable/disable the option to create preview of the documents.
Calculate Coverage	Enable/disable the option that user jobs are used on calculations/statistics.
Restrict to Working Scheduler	Enable/disable the option to work with Scheduler. The Scheduler option can be configured on Printing Policies on Other Policies tab.

Table 31 - Printer Details

8. Click on Assignment tab
9. Assign the permissions to Users/Groups/Roles/Devices

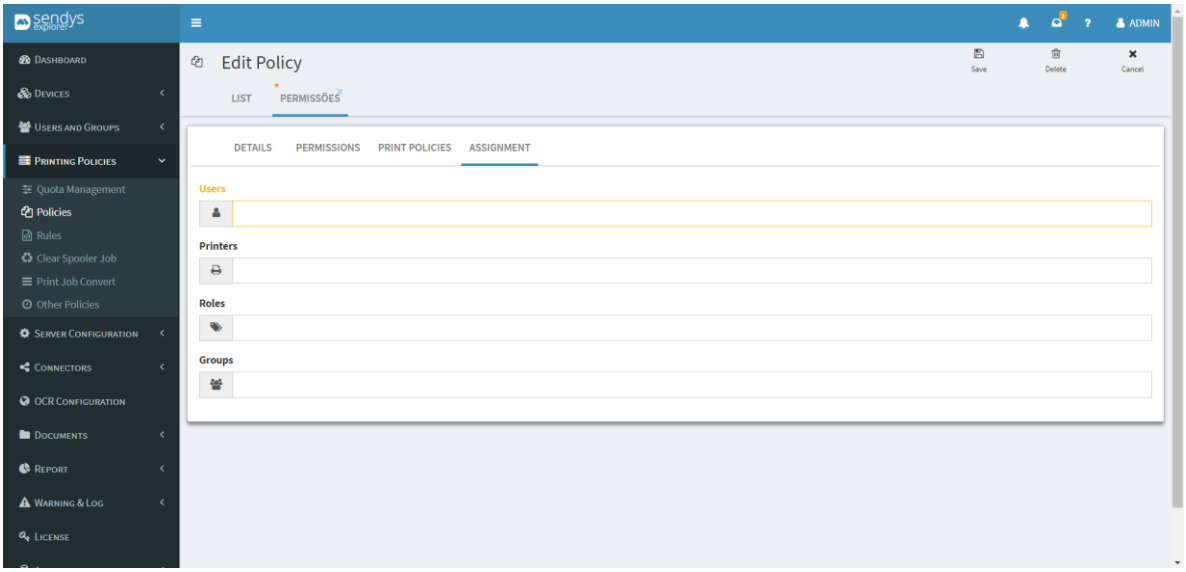


Fig. 231 – Assign policies permissions.

10. Click "**Save**"

RULES BASE POLICIES

On this view we have the possibility to assign one rules to several objects.

1. Click on **Printing Policies**.
2. Click on **Policies**.
3. Make the required configuration.

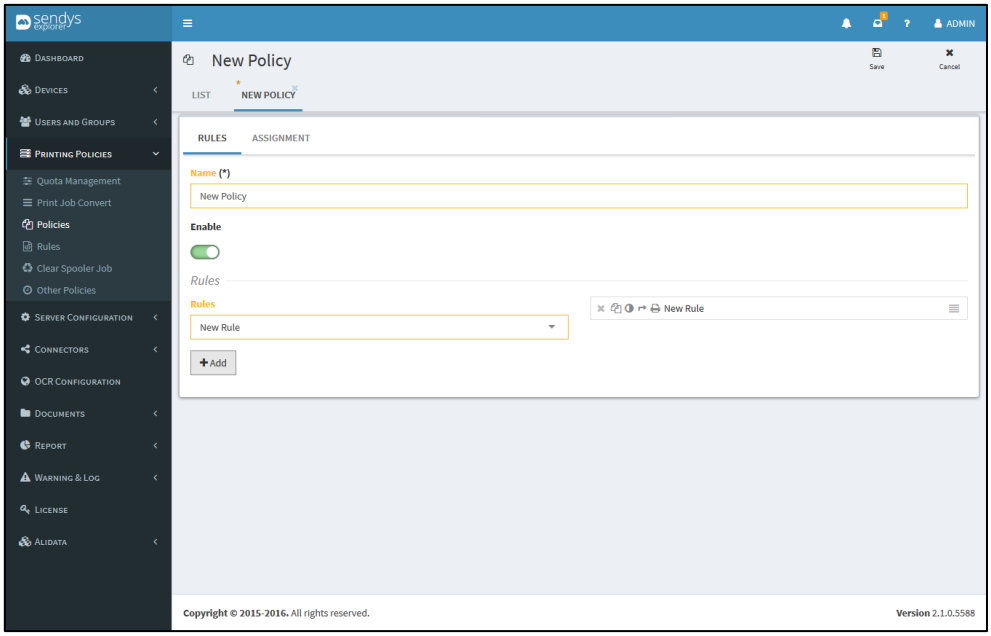


Fig. 232 - Policies overview

4. Assign the Policy to the desired elements.

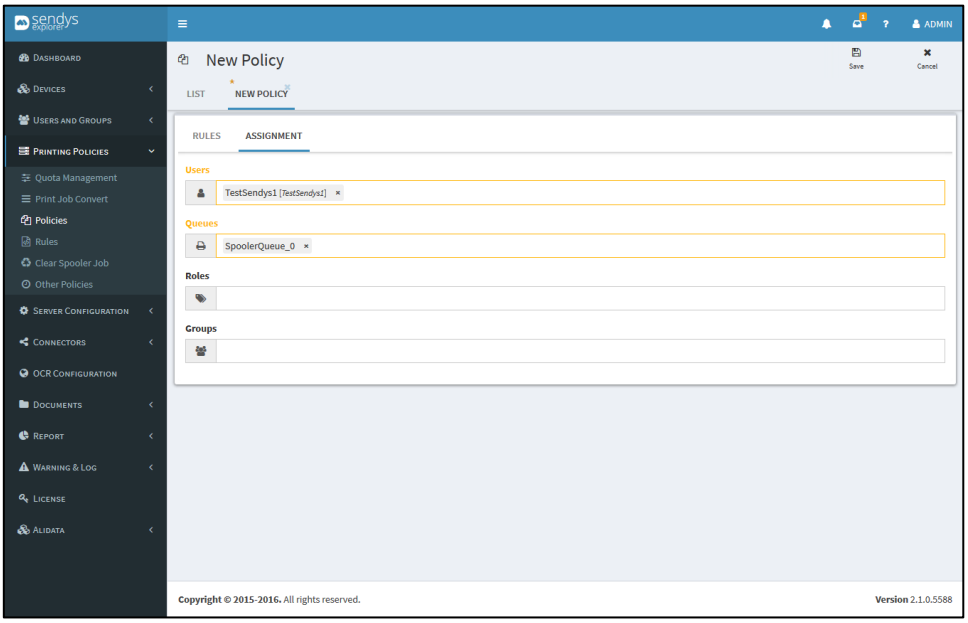


Fig. 233 - Policies overview

5. Click on "**Save**".

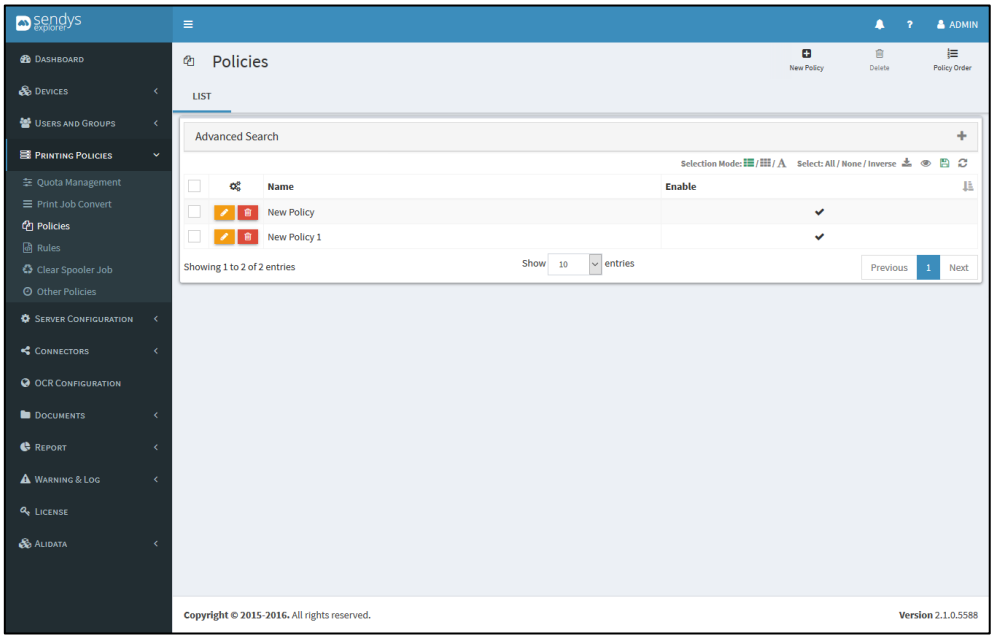


Fig. 234 - Policies overview

RULES

On this view we have the possibility to configure rules. Those rules will then be applied on the **Policies**.

1. Click on **Printing Policies**.
2. Click on **Rules**.
3. Make the required configuration.

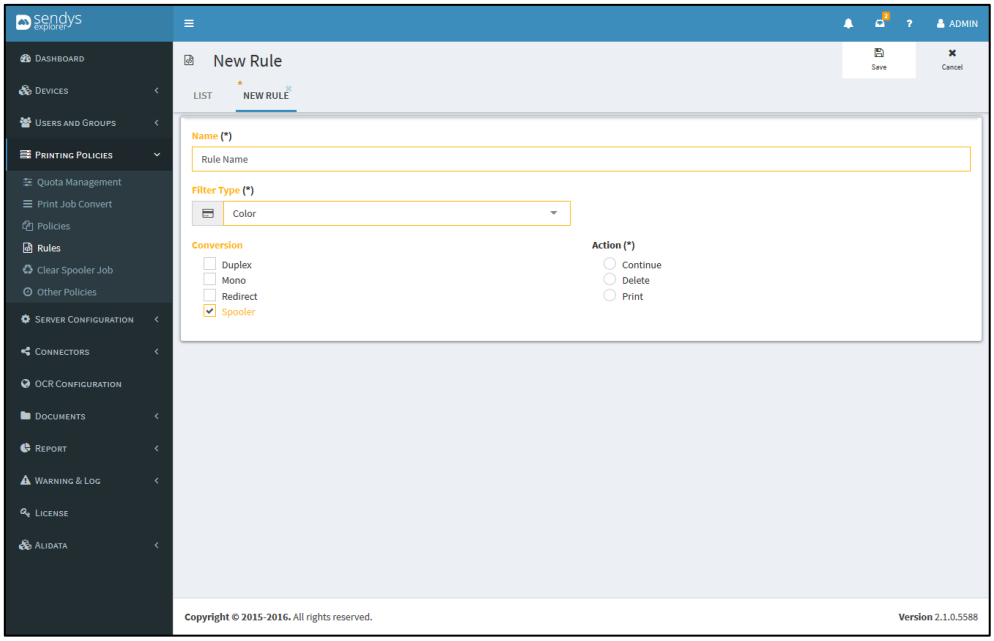


Fig. 235 - Rules overview

4. Click on "**Save**".

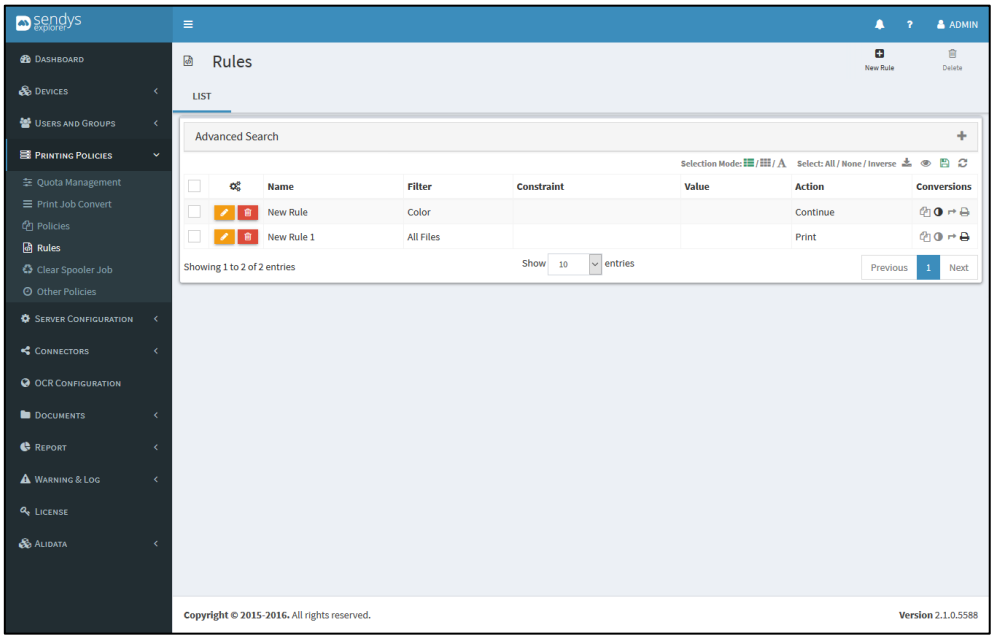


Fig. 236 - Rules overview

CLEAN SPOOLER JOB

This view is used to control the documents on queue on the Spooler. Is possible to control Spooler Jobs and way they work, using parameters like date and work on History documents, Scanned documents and Spooler documents.

On the upper menu we have the button options to **Save** and **Cancel**.

Another button option is the **Clean Spooler** and is used to clear all the documents in queue on Spooler Job. These documents will be marked as to be deleted and moved to the Spooler History. These documents are only marked to be deleted but they are not deleted form the applications folders.

For that, the administrator needs configure the schedule for each Spooler so the documents can be automatically deleted with routines services. With this options activated and configured we have the possibility to clean documents.

On this table are presented the configurations to control the three types of spoolers on the platform:

Name	Details
Enable	Enable/disable the option to work with clean spooler job.
Spooler Hold Period (H)	Defines the interval (Hours) of time that the schedule would not affect the Spooler documents.
History Hold Period (H)	Defines the interval (Hours) of time that the schedule would not affect the History Spooler documents.
Scanner Hold Period (H)	Defines the interval (Hours) of time that the schedule would not affect the Scanned documents.
Start date	Defines the date where this scheduler starts to woks.
Delete hour	Defines the hour that the scheduler service is activated.
Day Switches	Defines the days of the week that the scheduler service will work to clean the deleted files.

PRINT JOB CONVERTS

1. Click on **Printing Policies** menu.
2. Click on **Print Job Convert** menu

This view shows the list of the print convert actions that the server uses. If the Administrator needs a to force some conversion this is the place where they can be generated and edited. On the list, we already have one print job convert (**EnforceMono_OKI_Universal_pcl5**), that is configured during the installation. This convert can be used to force a job to be converted on Mono. This can be viewed as an example for future new conversions to be applied.

Click on **New** button to insert a new print job converts or **Edit** button to edit an existing one.

Name	Details
Name	Name of the Print Job Convert.
Print Option	Select the type of print option for conversion.

Table 32 - Print job converts details

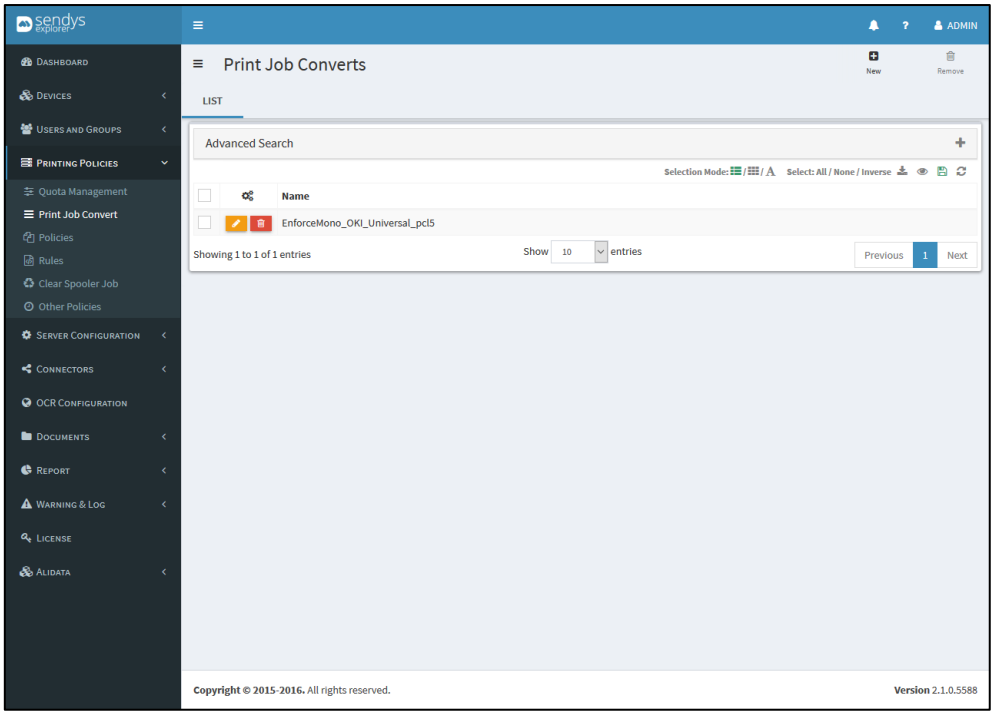


Fig. 237 - Print job convert overview

After this configuration we need to Add operations so the print conversions work properly. On **Operation** configurations:

Name	Details
Name	Name for the operation.
Search Pattern	Insert the Regex code to use as a search pattern.
Replacement	Insert the Replacement expression.

Operation Type	Insert the Operation type to work.

Table 33 - Print job convert operation

Use the button **Add** to add new the operations. There is the possibility to add more than one operation.

Click **Save** to save the configurations or **Cancel**. User button **Delete** to delete the Print Job Convert.

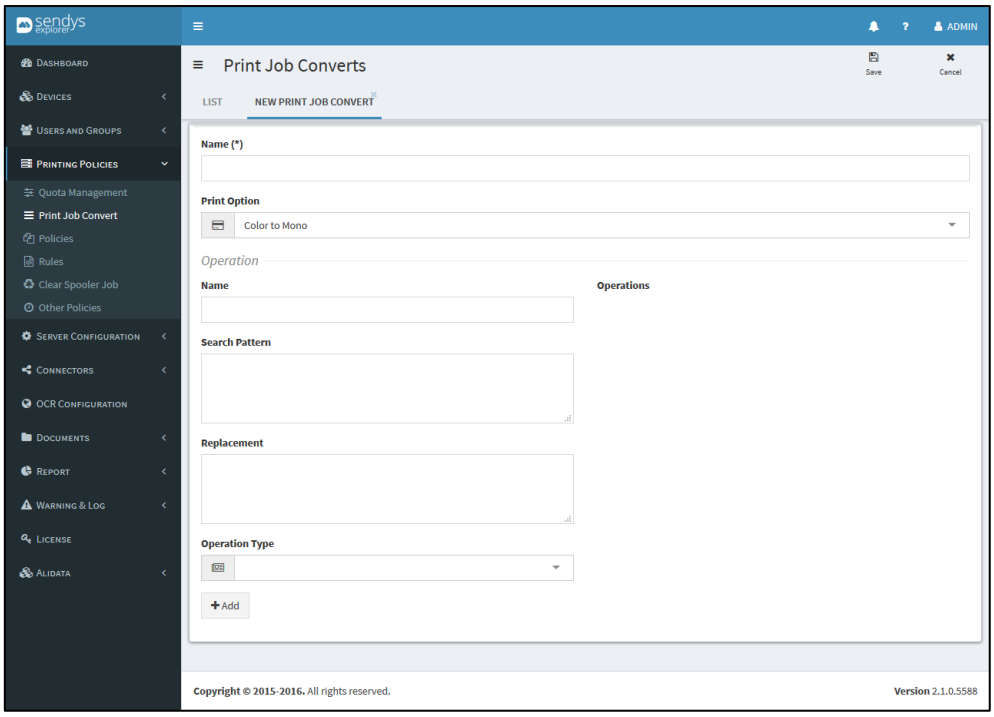


Fig. 238 - New print job convert

OTHER POLICIES

On this view we have the possibility to configure some other simply aspect.

1. Click on **Printing Policies**.
2. Click on **Other Policies**.

The **Save** buttons and **Cancel** works the same way as always for both views.

On **Work Schedule** tab we can define the work time or the period to work with printing jobs weekly.

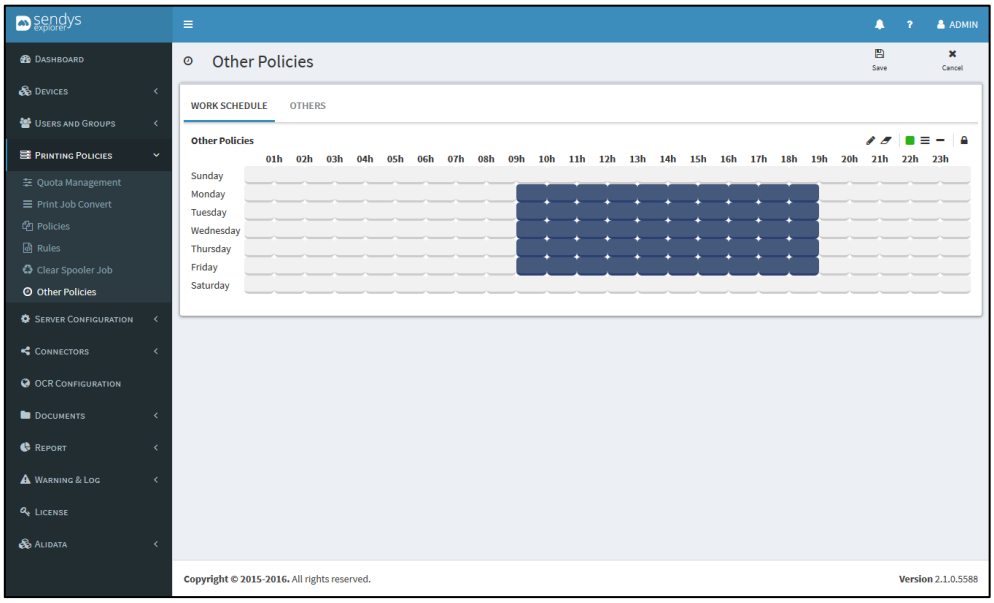


Fig. 239 - Other Policies

On **Others** tab we can configure the options that the platform will redirect a print job considering the job page number.

Defining the **Minimum Redirect Volume (page)** that will make a printing job to be redirected to a more economic printer.

Defining the **Delete Suspended jobs**, we define the action to take when the printing jobs are suspended. On this case selecting **Delete**, they will be deleted if they pass to the delete condition.

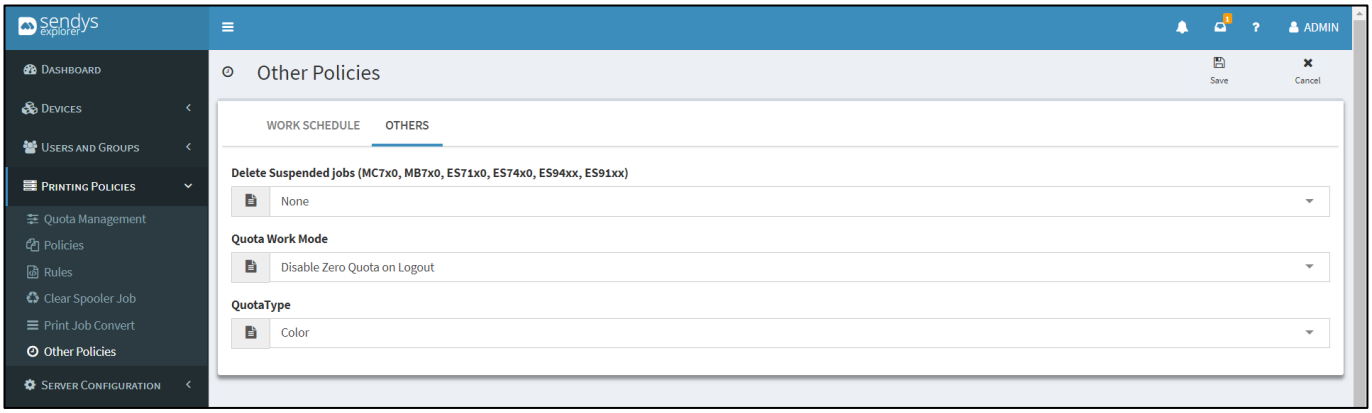


Fig. 240 - Other Policies Delete print Jobs

Quota type is defined in only one place

Color

Volume

Value

DATA LEAK PREVENTION

Data leak prevention was created to help customers to be more compliant with GDPR regulation. On this section of the application we can make configuration about company internal policies and with this definition help the company track the process and track the paper documents.

When did GDPR come into effect?

The GDPR was approved and adopted by the EU Parliament in April 2016. The regulation took effect after a two-year transition period and, unlike a Directive, did not require any legislation to be passed by government. GDPR came into force on 25th May 2018.

Who does the GDPR affect?

The GDPR not only applies to organizations located within the EU but also applies to organizations located outside of the EU if they offer goods or services to, or monitor the behaviour of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

What constitutes personal data?

The GDPR applies to 'personal data', meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organizations collect information about people.

What are the penalties for non-compliance?

Organizations can be fined up to 4% of annual global turnover for breaching GDPR or €20 Million.

What will happen to companies that have missed the deadline?

If the GDPR deadline has been missed, it is imperative the business in question acts urgently to become compliant. Demonstrating strong data rights management is important to both customers and employees; they should understand why the data is collected and how it is handled on a legal basis. Current business data processes need to be looked at as an immediate priority so that the company doesn't risk non-compliance penalties.

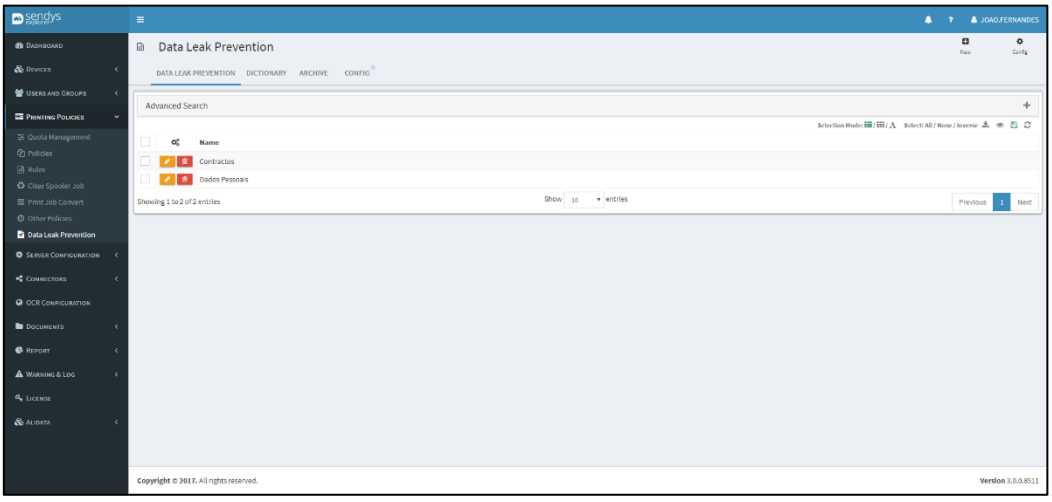


Fig. 241 – Data Leak Prevention.

ARCHIVE

Create names for archives on the system in order to help you follow up where the paper documents are store on the company.

1. Click on **Print Policies**
2. Click on **Data Leak Prevention**
3. Click on **Archive tab**

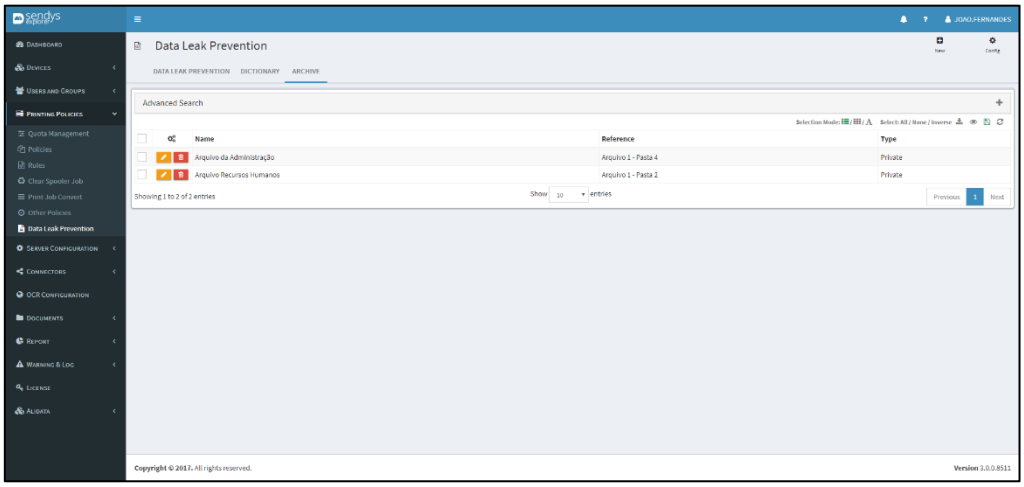


Fig. 242 - Data Leak Prevention Archive.

ADD/EDIT

10. Click on **Print Policies**
11. Click on **Data Leak Prevention**
12. Click on **Archive tab**
13. Click on **New** to add or **Pencil** to edit.
14. Insert a **Name**
15. Select a **Location**
16. Insert a **Reference**
17. Insert a **Type**
18. Insert a **Objective**

This information will help you track where the paper is after the document assign to the specific DLP policy.

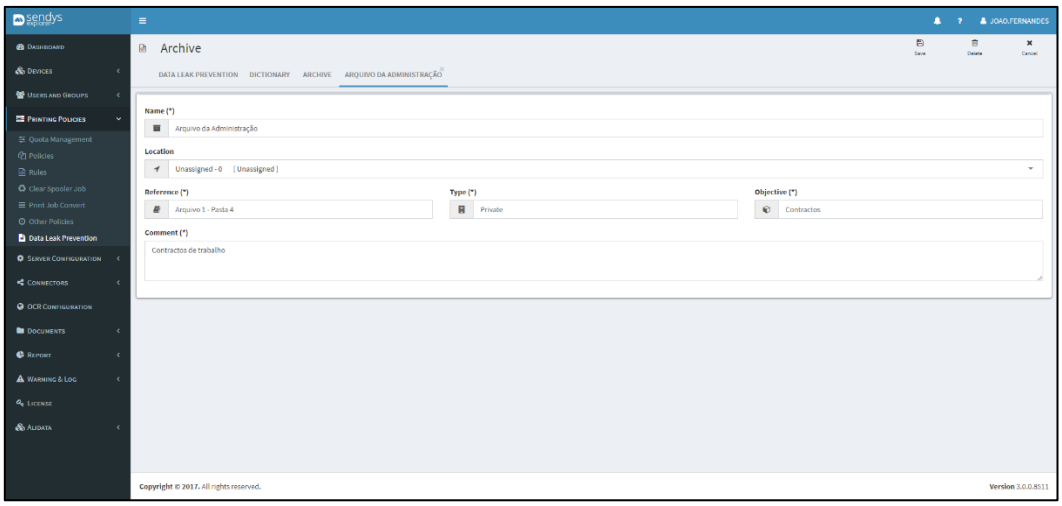


Fig. 243 - Data Leak Prevention Archive.

CONFIG

Configuration section is where you define the user policy agreement, where you define how you handle the data on the system and if the user needs to accept the document management policy or if you already have that on other internal company policy.

To define user agreement policy :

1. Click on **Print Policies**
2. Click on **Data Leak Prevention**
3. Click on **Config**
4. On **Application User Policy** Tab
5. Define **User is Unable to Login Before Policy Agree** (Enable/Disable)
6. Define **Enable User Policy Request** (Enable/Disable)
7. Define **Enable User Deletion Request** (Enable/Disable)

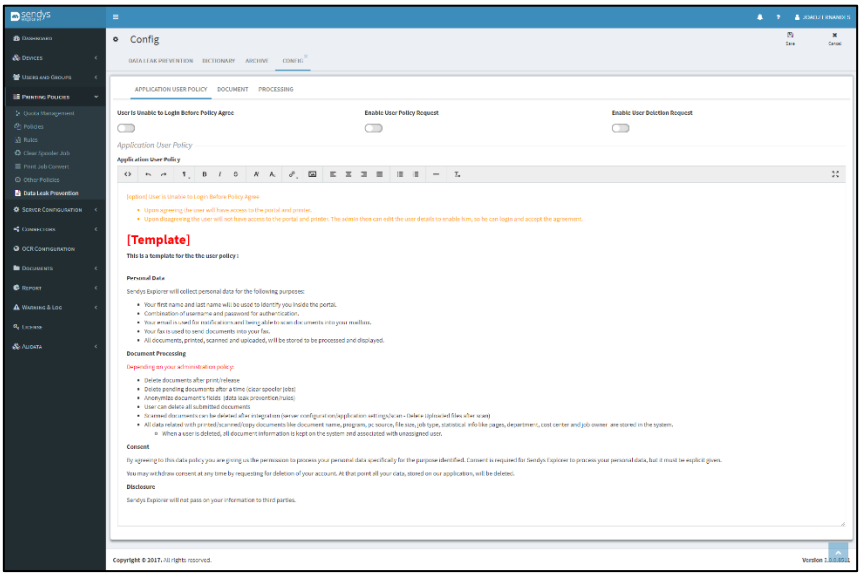


Fig. 244 - Data Leak Prevention User Policy.

8. On **Document** Tab
9. Define **Fields to be use on DLP Processing**
    a. Filename
    b. Cost Center
    c. PC Name
    d. IP Client
    e. File Type
    f. Scan Settings
    g. Process State
10. Define **Fields to be use on Anonymize Processing**
    a. Filename
    b. Cost Center
    c. PC Name
    d. IP Client
    e. File Type

f. Scan Settings
g. Process State

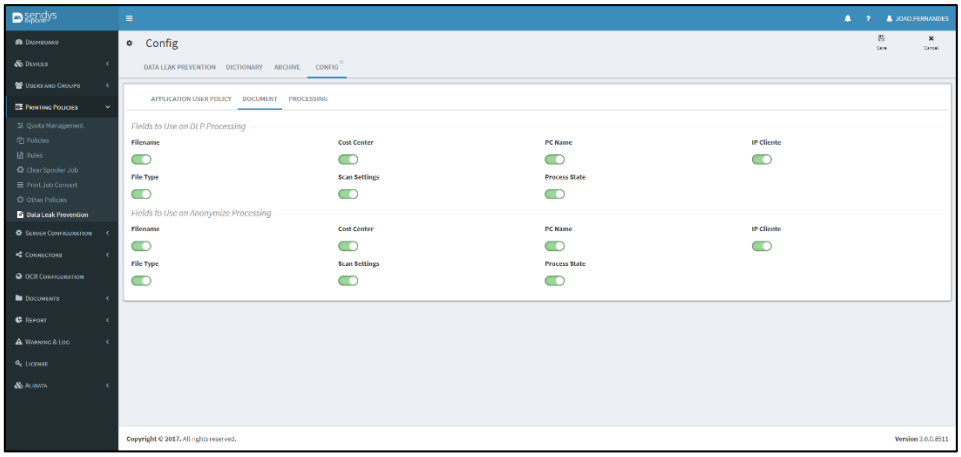


Fig. 245 - Data Leak Prevention Config Fields.

11. On **Processing** Tab
12. You can define print document cover for Copy/Print/Scan documents and process the specified fields to make the documents available on DLP Documents section.

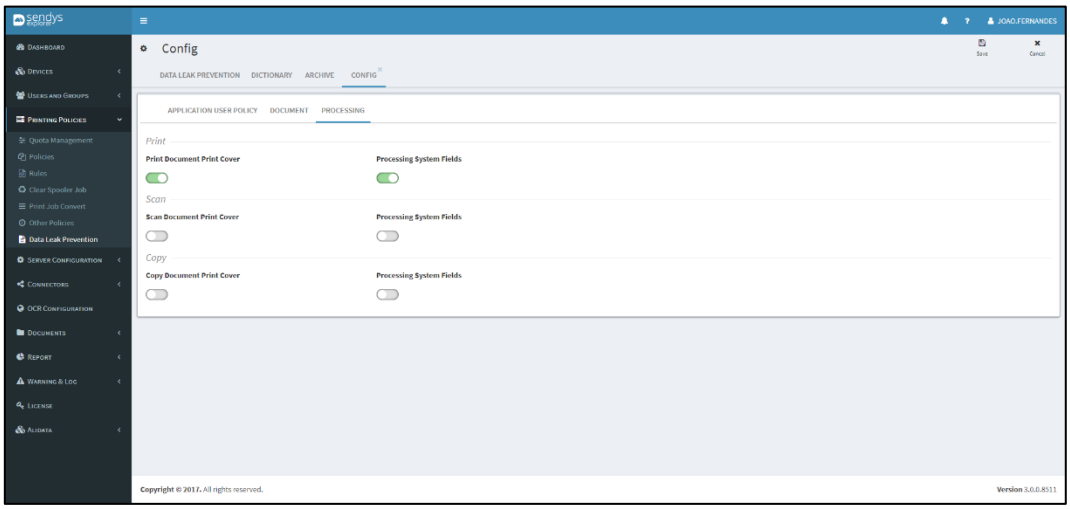


Fig. 246 - Data Leak Prevention Processing actions.

DICTIONARY

Dictionaries for Data Leak Prevention are set's of keywords that can be pick from processed fields and assign the documents to a specific Data Leak Prevention policy.

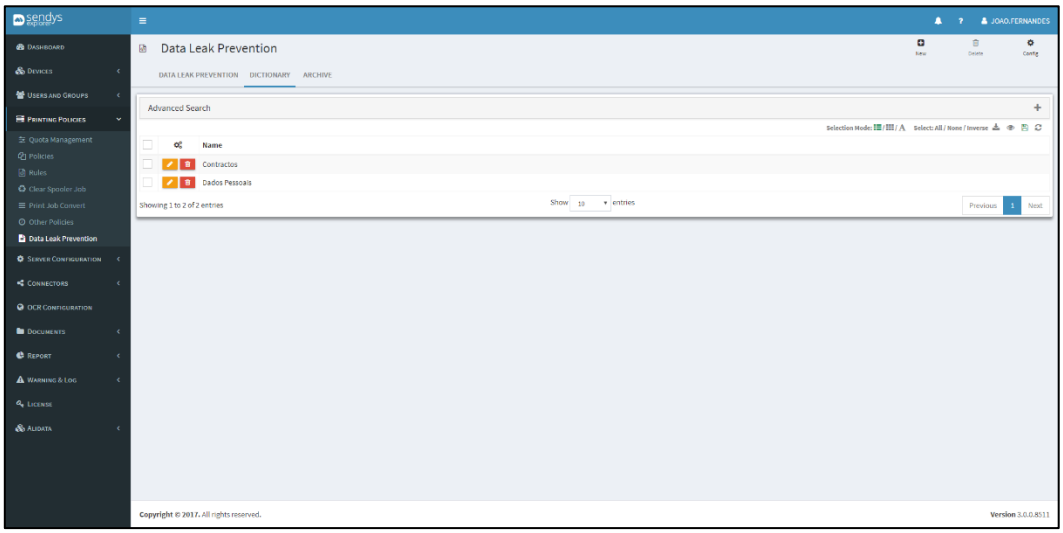


Fig. 247 - Data Leak Prevention Dictionary.

ADD/EDIT

1. Click on **Print Policies**
2. Click on **Data Leak Prevention**
3. Click on **Dictionary tab**
4. Click on **New** to add or **Pencil** to edit.
5. Insert a **Name**
6. Insert **Word's**/Keywords one per line

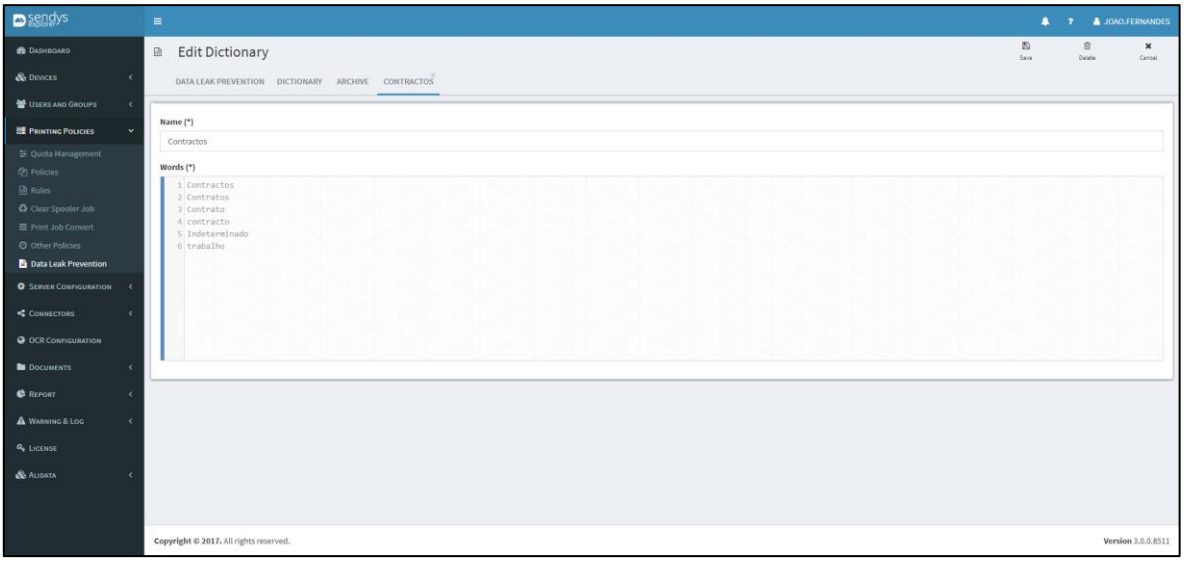


Fig. 248 - Data Leak Prevention Dictionary.

ADD/EDIT DLP POLICY

1. Click on **Print Policies**
2. Click on **Data Leak Prevention**
3. Click on **Click New to add or Pencil to Edit**
4. Insert a **Name**
5. Select a **Dictionary**
6. Select a **Archive**
7. Enable/Disable **Delete After Print**
8. Enable/Disable **Anonymize**
9. Specify the time that the document should be hold before notifying the user to destroy the physical document in paper **Time to Notify**
10. Specify **other time period** if none of the above is OK
11. Specify the type of notification and the person that should receive it
12. Specify the message to be send on notification

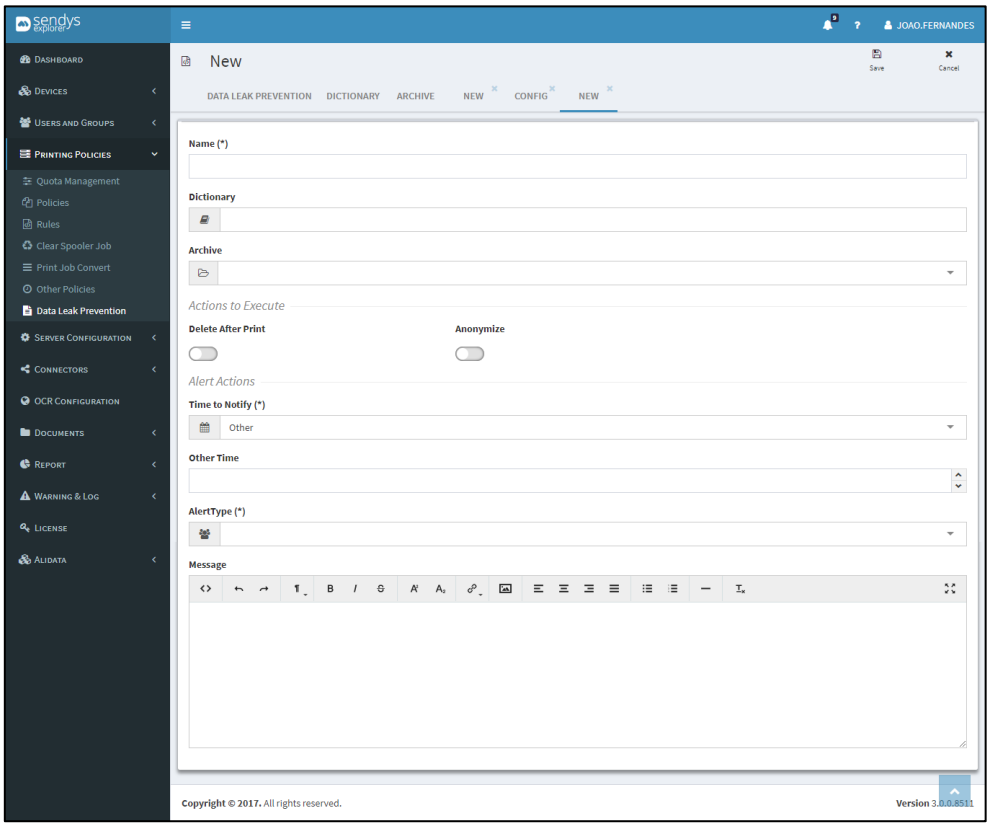


Fig. 249 - Data Leak Prevention Dictionary.

SERVER CONFIGURATIONS

This section is related with server configurations that are important to have a special attention so the platform works properly fine. Many of this configurations are done on installation but it is recommended to confirm if they are correct. The next points will describe each one of them.

APPLICATION SETTINGS

APPLICATION CONFIG

On this menu we can configure important content about the SENDYS Explorer Output Manager.

1. Click on **Server Configuration > Application Settings**.
2. Click on **List > Application Config**.

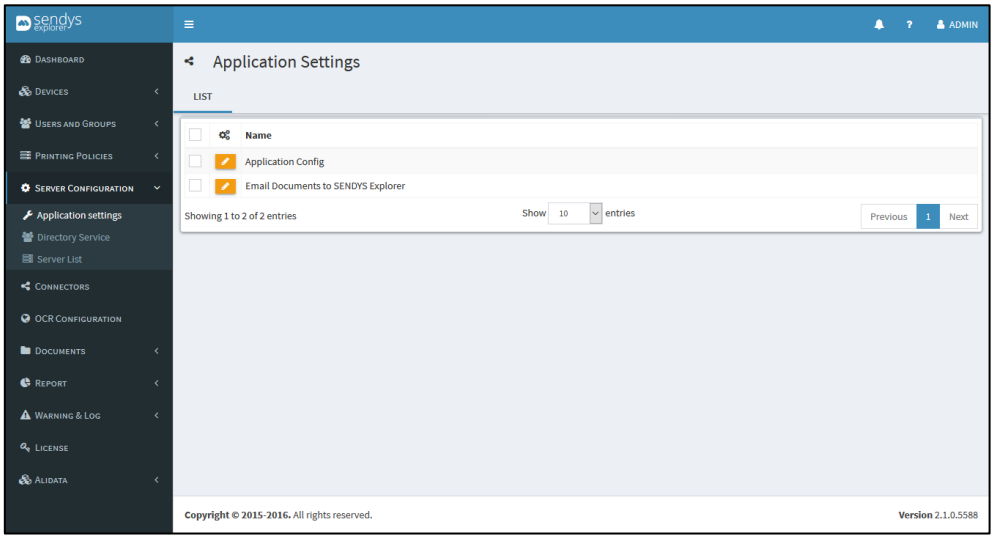


Fig. 250 - Application Settings

APPLICATION

1. Click on **Application Config**.
2. Click on **Application**

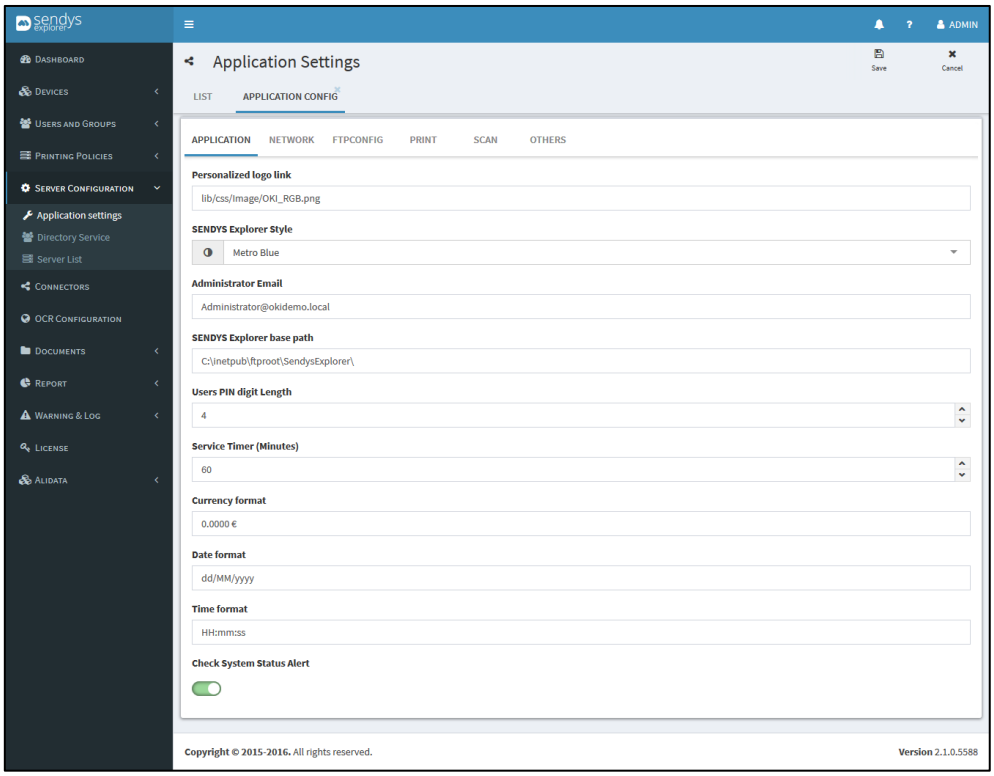


Fig. 251 - Application Settings

3. Make the required configuration.

Name	Details
Personalized logo link	You could set the path for a custom logo Image[2]
SENDYS Explorer Style	The application has several color schemes. You can select the most convenient based on your preferences.
Administrator Email	You could set the email of the system administrator.
SENDYS Explorer base path	This is the base application path.
Users PIN digit Length	Number of digits for user PIN, by default is 4
Service Timer (Minutes)	This is the time interval used on schedule tasks.
Currency format	You could define the most convenient format for the currency.
Date format	You could define the most convenient format for the date.
Time format	You could define the most convenient format for the time.
Check System Status Alert	Enable this option to receive alerts when exist some failure on SENDYS Explorer

Table 34 - Application Details

By default, the logo for the application will be:

Fig. 252 - Default Image Logo

4. Click **Save**.

[2]Please note that the logo image should not be bigger than 120 x 45 px

NETWORK

1. Click on **Application Config**.
2. Click on **Network**

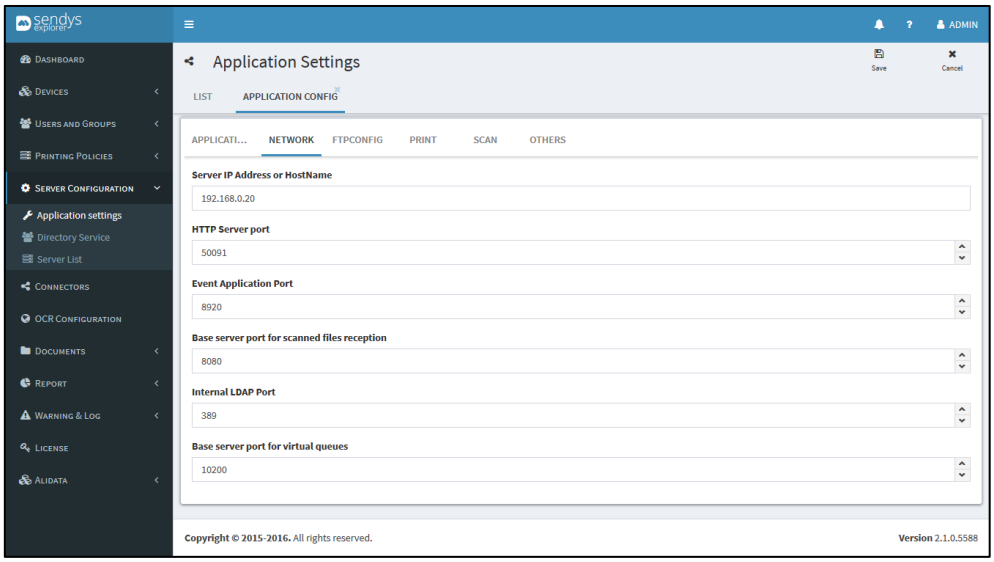


Fig. 253 - Network Settings

3. Make the required configuration.

Name	Details
Server IP Address or Hostname	This IP address (or Hostname) is used to all the application and is defined in the installation process.
HTTP Server port	This is the default web application access port, by default it is defined as 50091.
Event Application Port	This is the default events port, by default it is defined as 8920.
Base server port for scanned files reception	Each device that supports WSD Scan needs a port to transfer scanned files to SENDYS Explorer server. The **base server port for scan** defines the lower port to be used. Each device will use a simple algorithm to calculate its unique port (base port + device ID). e.g. 8080 defined as base port means (device 1 -> 8081, device 2 -> 8082, …).
Internal LDAP Port	This is the default port for internal LDAP, by default it is defined as 389.
Base server port for virtual queues	For each queue created on SENDYS Explorer, it will be created a new port on windows. The **base server port for queues** defines the lower port to be used. Each device will use a simple algorithm to calculate its unique port (base port + device ID). e.g. 10200 defined as base port means (device 1 -> 10201, device 2 -> 10202, …).

Table 35 - Network Details

4. Click **Save**.

SAP PRINT

1. Click on **Application Config**
2. Click on **SAP Print.**

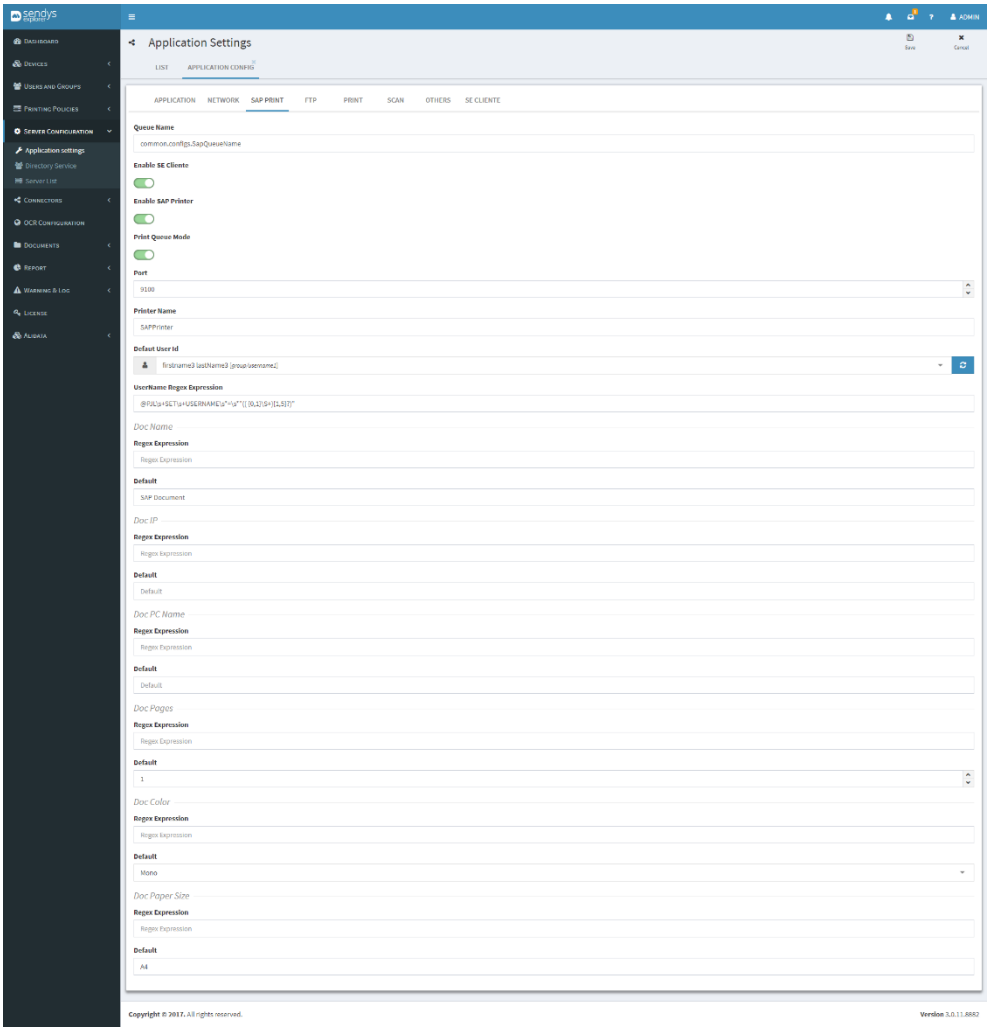


Fig. 254 – SAP Print Settings

3. Make the required configuration.
4. Click **Save**.

FTP

1. Click on **Application Config**.
2. Click on **FTP**

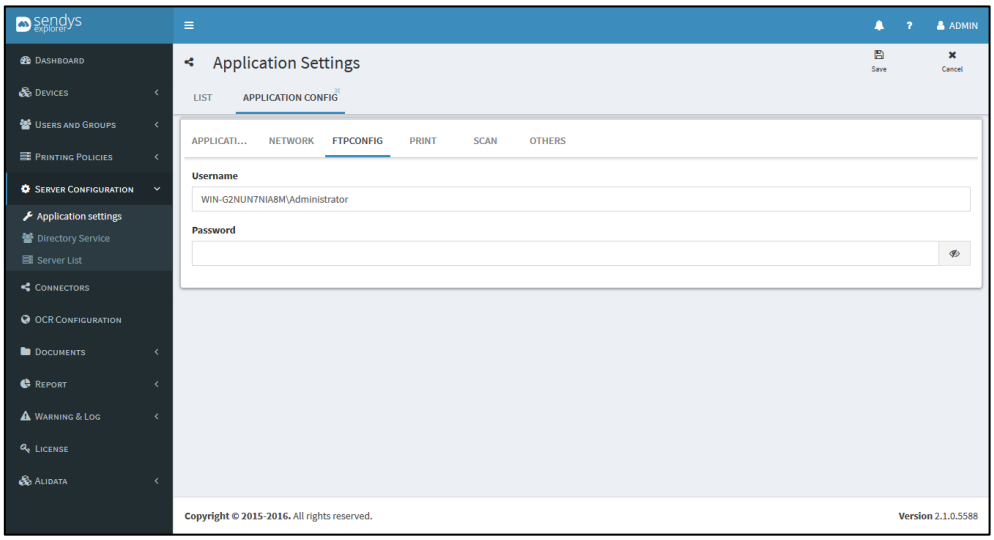


Fig. 255 - FTP Settings

3. Make the required configuration.

Name	Details
Username	User for FTP authentication.
Password	Password for the above user.

Table 36 - FTP Details

4. Click **Save**.

PRINT

1. Click on **Application Config**.
2. Click on **Print**

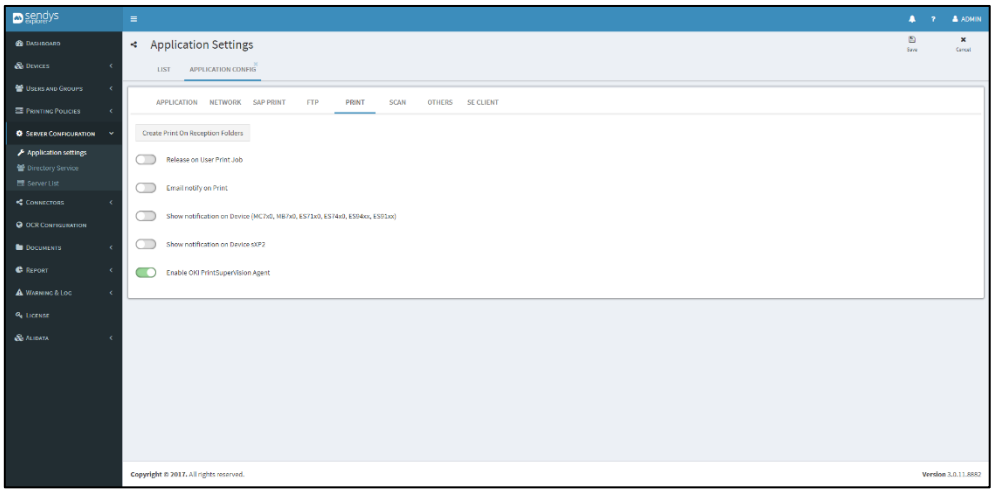


Fig. 256 - Print Settings

3. Make the required configuration.
4. Click **Save**.

OKI PRINTSUPERVISION AGENT

With the option “Enable OKI PrintSuperVision Agent” the client can use OKI PSV Agent to add billing printers to Output Manager. To Setup USB Agent use the Output Manager Server URL and click **Test URL & Save**

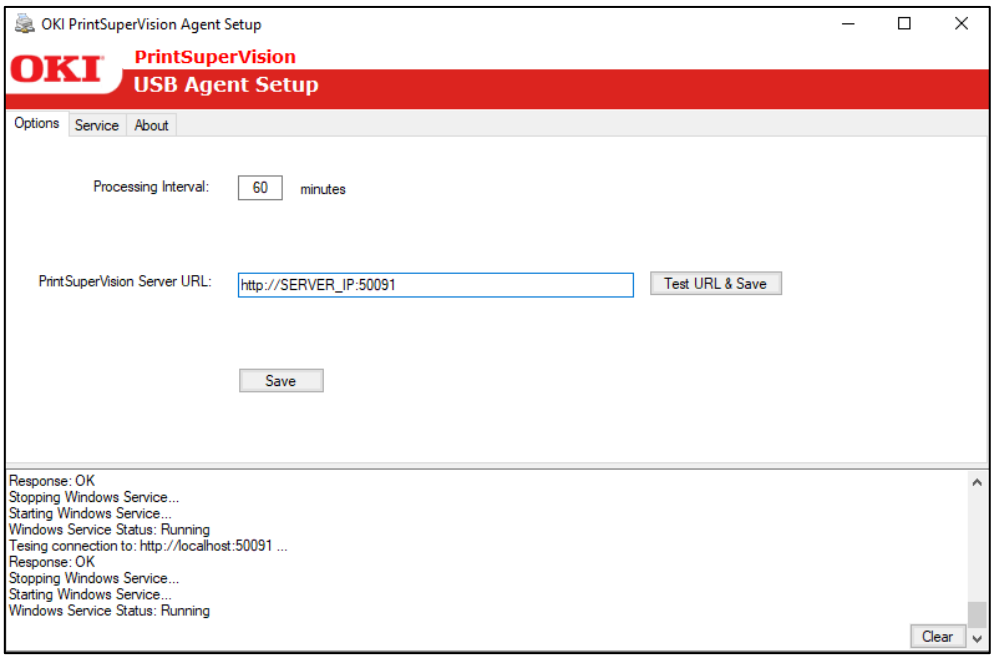


Fig. 257 – USB Agent Setup

SCAN

1. Click on **Application Config**.
2. Click on **Scan**

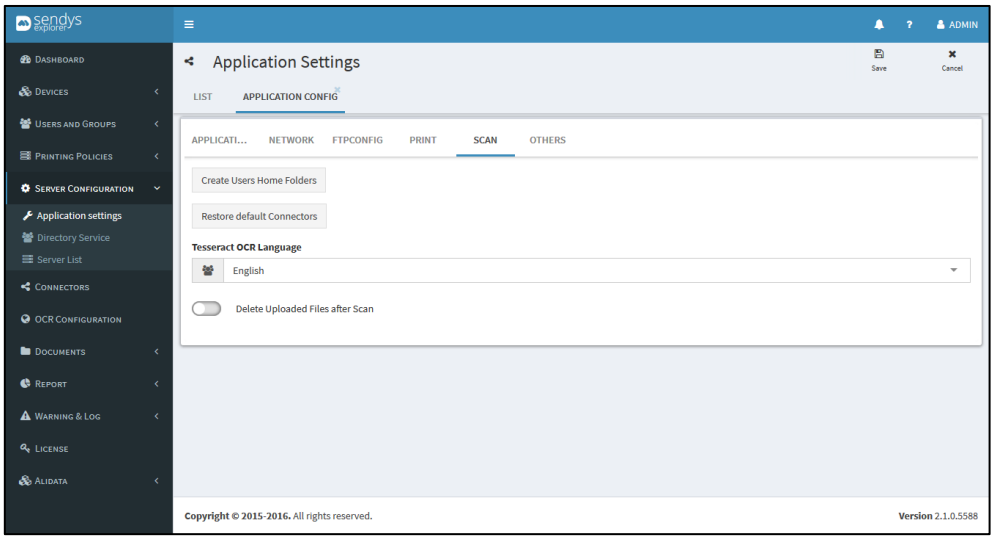


Fig. 258 - Scan Settings

3. Make the required configuration.

Name	Details
Create Users Home Folders	It will create the home folders in C:**\inetpub\ftproot\SENDYSExplorer\HomeDirectory**. You need to share the folder in order so both **users** and **SENDYS Explorer** have access to the scanned files. The user's **Home Folders** will be created based on the username, and the user account used to write the files in the folder is the user account that was set up during the installation process.
Restore default Connectors	To restore all connectors information to the default value.
Tesseract OCR Language	You have several supported OCR languages available. When you change the language SENDYS Explorer will try to download and install the new language. If you do not have internet access, please refer to the Offline installation process: [**Error! Reference source not found.>Error! Reference source not found.>Error! Reference source not found.>Error! Reference source not found.**]
Delete Uploaded Files after Scan	Enable this option in order to not integrate the scanned files on SENDYS Explorer

Table 37 - Scan Details

4. Click **Save**.

OTHERS

1. Click on **Application Config**.
2. Click on **Others**

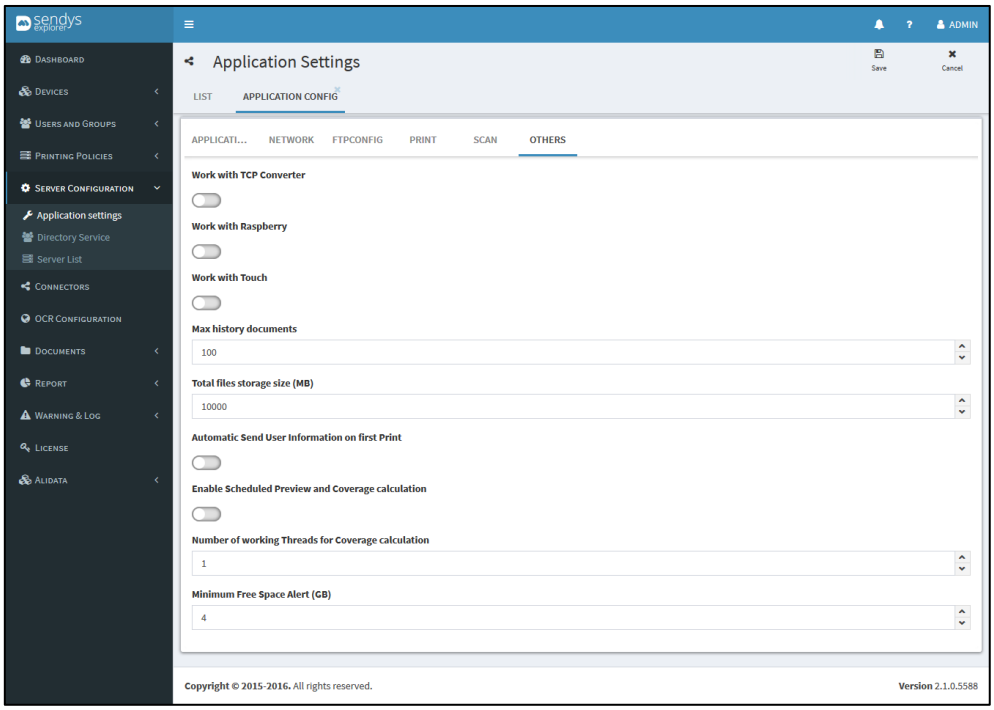


Fig. 259 - Others Settings

3. Make the required configuration.

Name	Details
Work with TCP Converter	Enables TCP converter configurations on the admin application.
Work with Raspberry	Enables Raspberry configurations on the admin application.
Work with Touch	Enables Touch configurations on the admin application.
Max history documents	Max number of jobs to display on device Print history option.
Total files storage size (MB)	Total size for scanned jobs this option was deprecated when using OM connector.
Automatic Send User Information on first Print	Enable auto send welcome email after first print job submission.
Scheduled Preview and Coverage calculation	Schedule the preview creation and coverage calculation to run outside defined working scheduler
Working Threads for Coverage calculation	Number maximum of concurrent requests for coverage calculation.
Minimum Free Space Alert (GB)	Minimum disk space to report low disk space.

Table 38 - Others Details

4. Click **Save**.

SE CLIENT

1. Click on **Application Config**.
2. Click on **SE Client**
3. Make the required configuration.

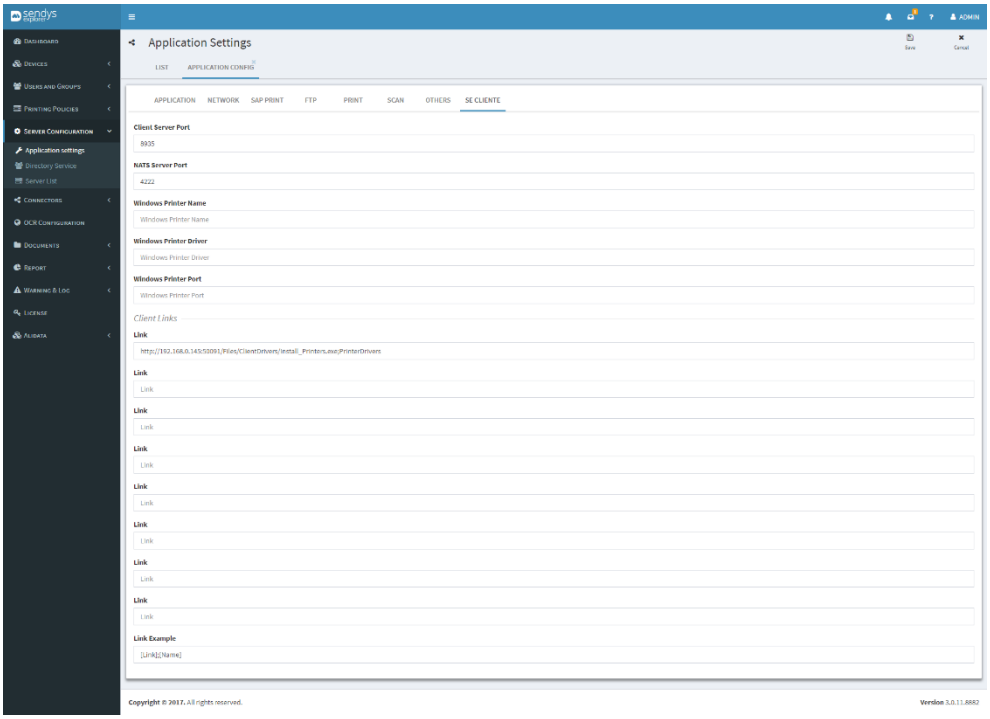


Fig. 260 SE Client setting

Name	Details
Client Server Port	Designates the port where the Client will be able to connect.
NATS Server Port	Value of the port where NATS is configured to listen.
Windows Printer Name	Windows printer name.
Windows Printer Driver	Windows printer driver.
Windows Printer Port	Windows printer port.
Client Links	Driver URL links to be shown on the client for download. The link needs to be configured with **Url** with "**;**" as separator and the **display name of Url** on the application.

Table 39 – SE Client Options

4. Click **Save.**

SE CLIENT APPLICATION

When opening SE Client Application, the user will be prompted to fill the **Server IP** and **Client Server Port** that was configured on **Output Manager admin panel** > **Server Configuration** >**Application Config** > **SE Client**

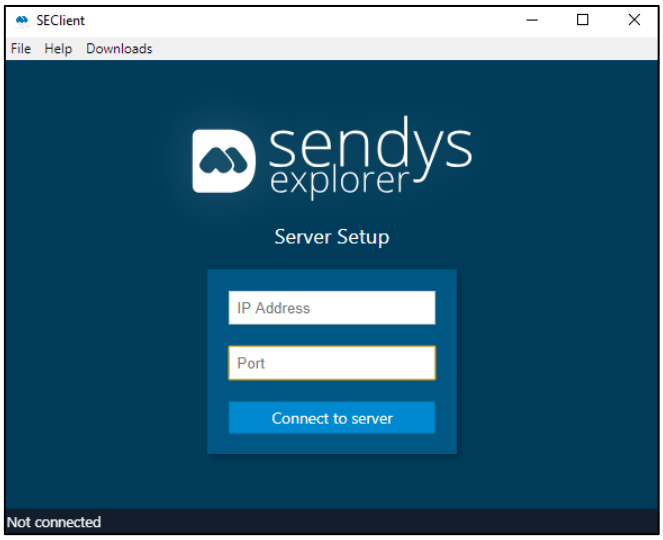


Fig. 261 - Email Documents to SENDYS Explorer

After connecting to the server, the user can log in into the application using one of the following options:

1. **ID/Pass:** Login using the username and password.
2. **Card:** Login using a card reader connected to the user machine and passing is card.
3. **Pin:** Login using the user Pin.

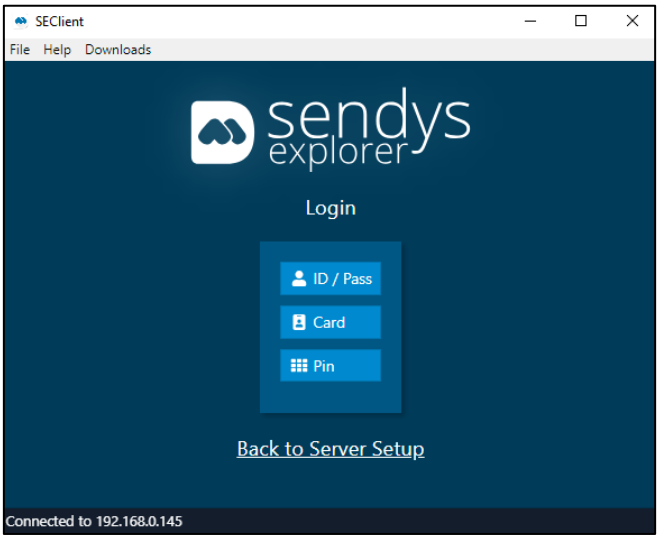


Fig. 262 - Email Documents to SENDYS Explorer

The tool allows a user to download any file, e.g., instruction manual file or printer drivers, on the **Downloads** tab. Any link can be configured to be downloaded on **Output Manager admin panel** > **Server Configuration** >**Application Config** > **SE Client**.

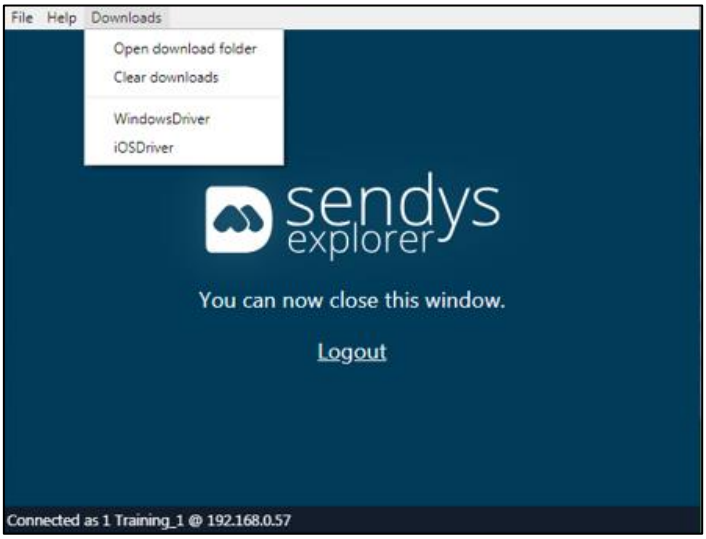


Fig. 263 - Email Documents to SENDYS Explorer

On SE Client icon the user can reopen the client window or change the type of notifications shown.

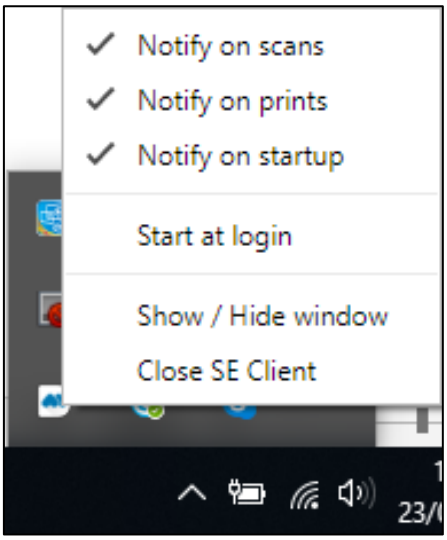


Fig. 264 - Email Documents to SENDYS Explorer

EMAIL DOCUMENTS TO SENDYS EXPLORER

This is a batch processing document queue, like **Upload Documents**. The users will be matched by the email address that he has on SENDYS Explorer and when a document reaches the system it will be used to identify the user.

You need to setup an email account so that when the users of SENDYS Explorer send emails to that address the system will process the documents and add them to SENDYS Explorer document.

1. Click on **Server Configuration > Application Settings**.
2. Click on **List > Email Document to SENDYS Explorer**.

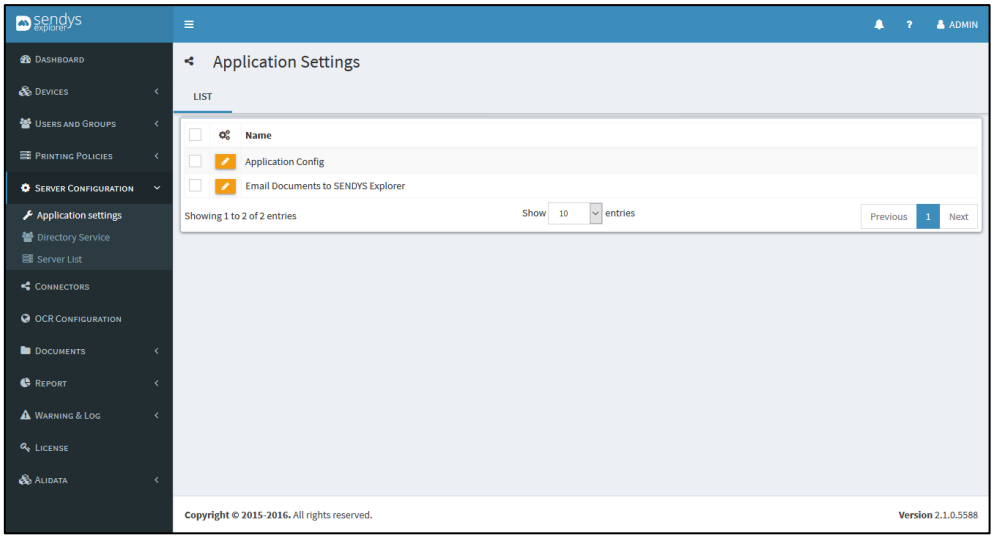


Fig. 265 - Email Documents to SENDYS Explorer

3. Make the required configuration.

Name	Details
Email Type	Choose between POP or IMAP
Email host	Server IP/Host
Email username	Email Username
Email password	Email Password
Email port	Host port
Email SSL	Check if you want to use SSL
File Type	Choose default file type conversion
Delete Email After Reception	Check if you want to delete emails after reception
Email Checking Interval(s)	Interval between new email verification (in seconds)

Table 40 - IMAP/POP Details

5. Click **Save** to save the changes.

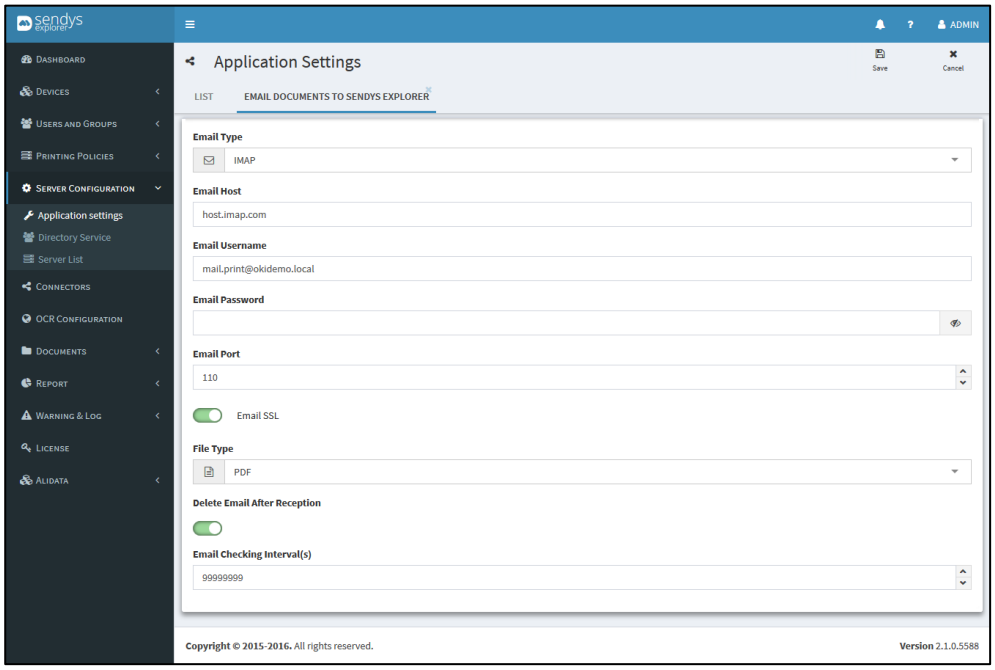


Fig. 266 - IMAP/POP Settings

DIRECTORY SERVICE

With Directory Service the application will work with single sign on. Configure **Directory Service** menu to assign each field and then you can synchronize with Directory Service.

Note: The installation of the SENDYS Explorer, will attempt to sync with the **Domain** that is configured on the server.

NEW AD CONFIG

1. Click on **Server Configuration > Directory Service**.
2. Click on **New AD Config**.

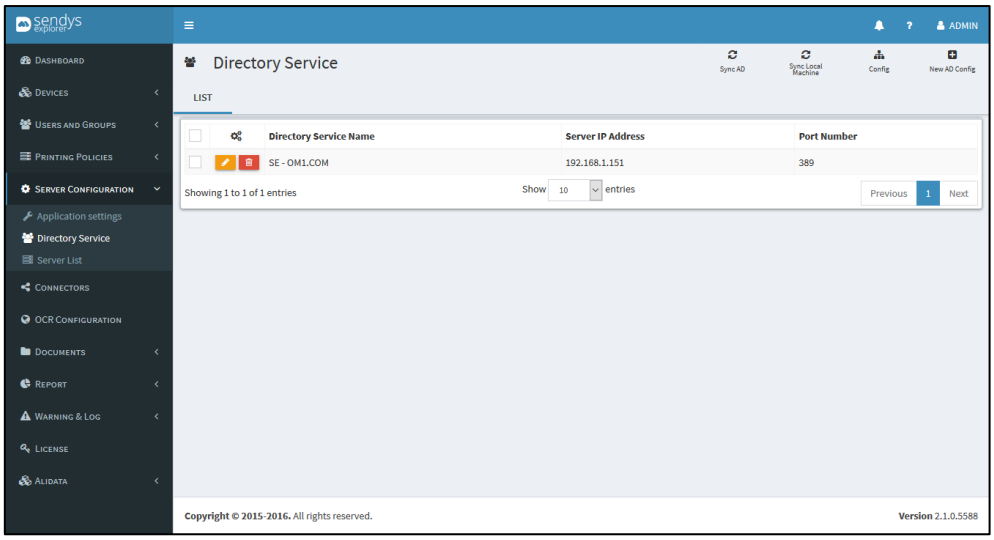


Fig. 267 - Directory Service

3. Make the required configuration.

Name	Details
Server IP Address or Hostname	Directory Service server IP or Hostname
Port Number	Access port to Directory Service or LDAP server. Default Directory Service port is 389
Directory Service Name	Domain extension. Example: *okidemo.net*
Search Base	Directory Service or LDAP search base
Username	User from Directory Service that has access to read all DS groups that you want to import
Password	Password for the above user
Enable SSL	Enable this option if the Directory Server or LDAP requires one SSL connection
Authentication Type	Select the correct Authentication Type to the Directory Server or LDAP
Filter	You can create filters to limit the Search Base. Example: *only sync users*
Encoding	Select the correct Encoding of your Directory Service or LDAP

Table 41 - Directory Service Details

4. Click **Save** to save the configuration.

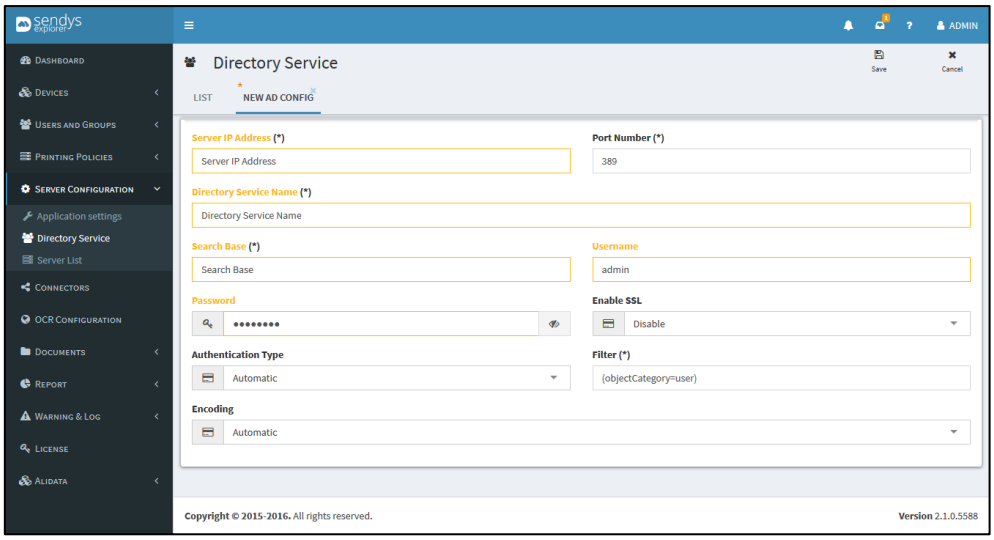


Fig. 268 - New AD Settings

EDIT AD

1. Click on **Server Configuration > Directory Service**.
2. Click on **List**.
3. Click on **pencil icon** to edit the **Directory Service**.

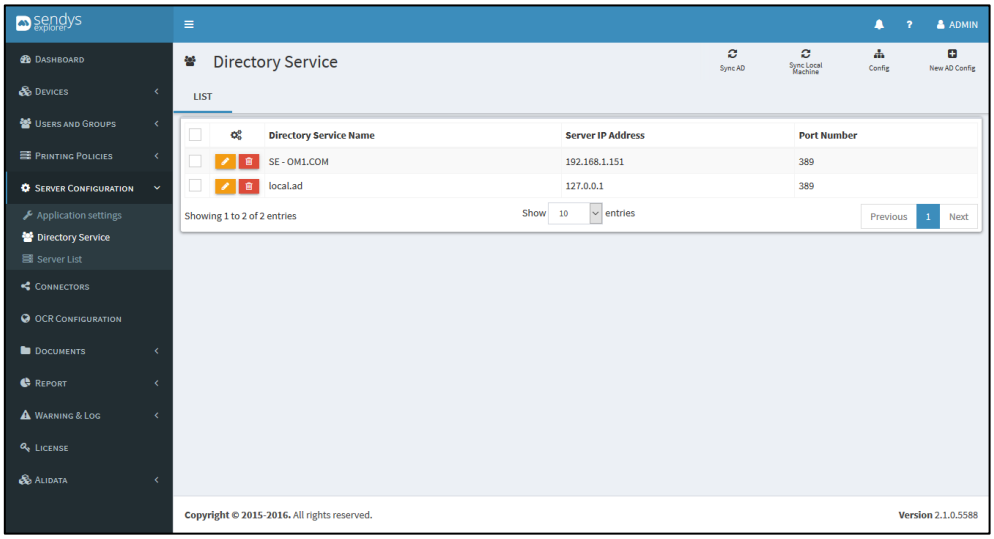


Fig. 269 - Directory Service

4. Make the changes on Directory Service configuration.

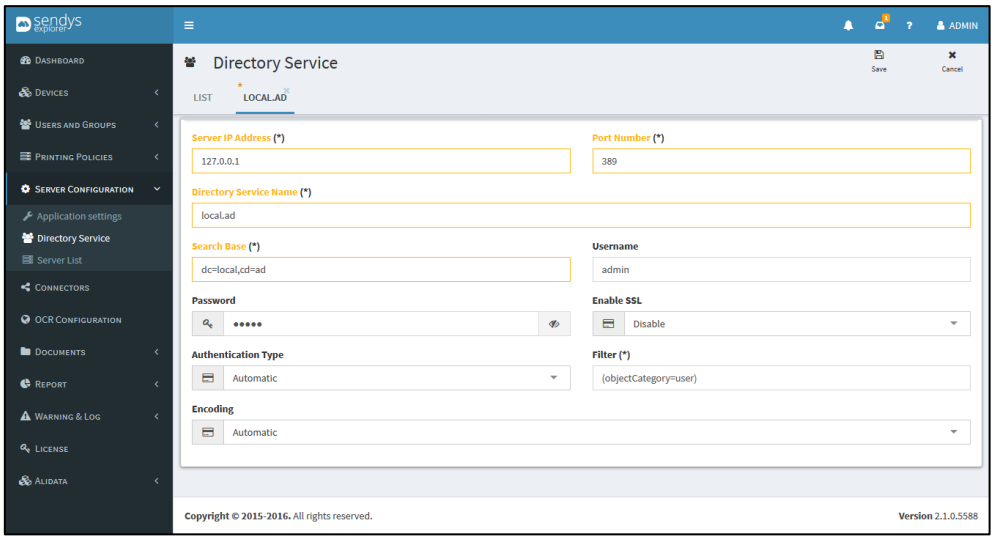


Fig. 270 - Edit AD Settings

5. Click **Save** to save the configuration.

REMOVE AD

1. Click on **Server Configuration > Directory Service**.
2. Click on **List**.
3. Click on **trash icon** to remove the **Directory Service**.

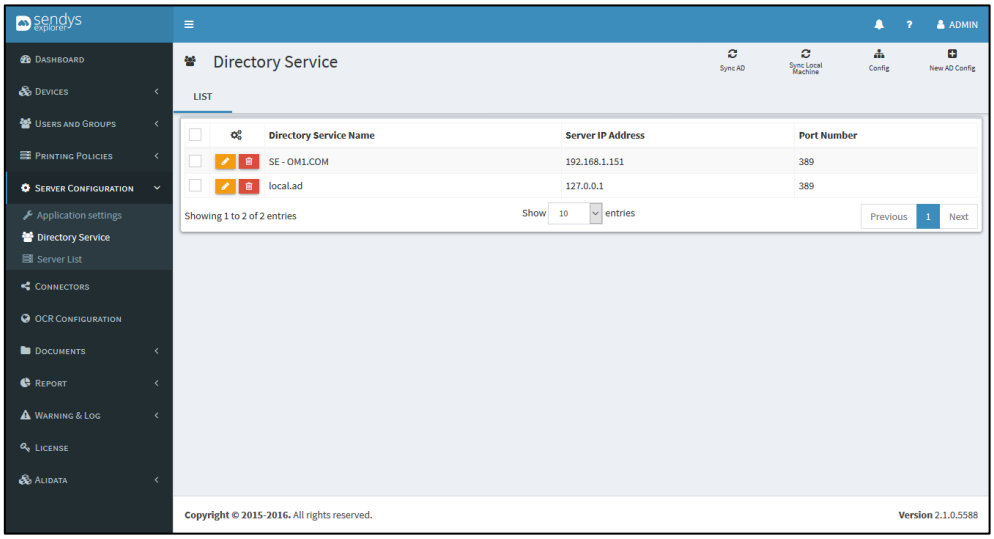


Fig. 271 - Directory Service

4. Click **Delete** to confirm removal.

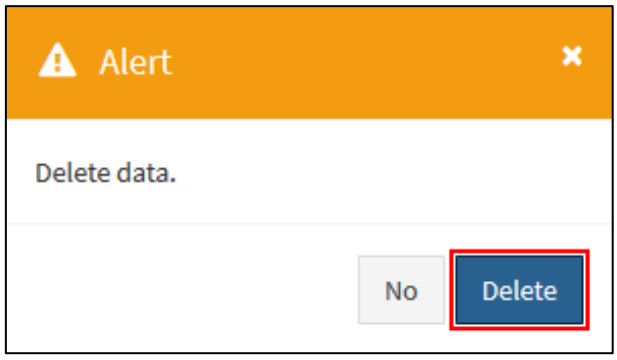


Fig. 272 - Confirm Remove AD

CONFIG

It's possible to configure the synchronized fields and several options related with sync action.

Note: You can use the "**Show/Hide Advanced Setting**" button to enable or disable the advanced mapping options, on tabs: User Mapping; Group Mapping and Location Mapping.

1. Click on **Directory Service > Config**.

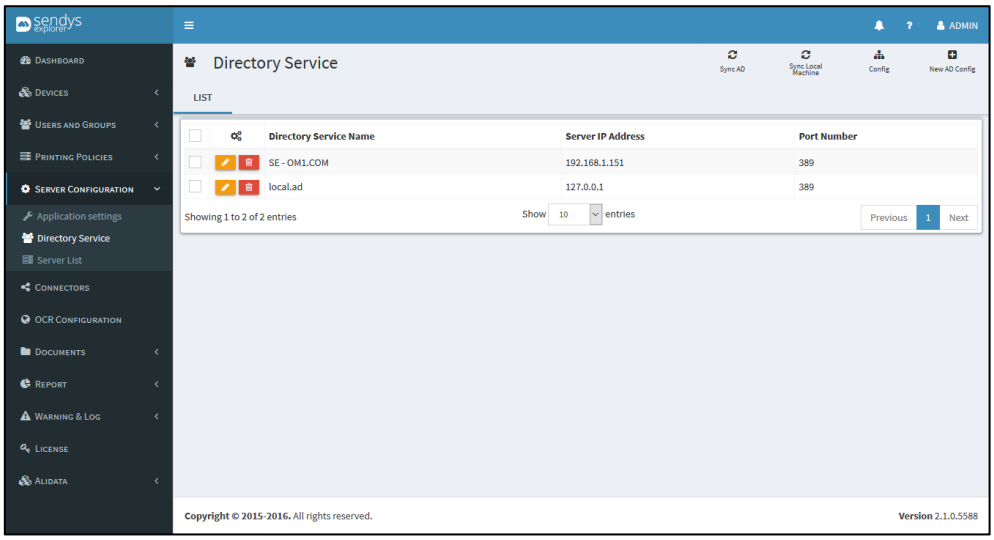


Fig. 273 - Directory Service Config

CONFIGURATIONS

1. Click on **Configurations**.

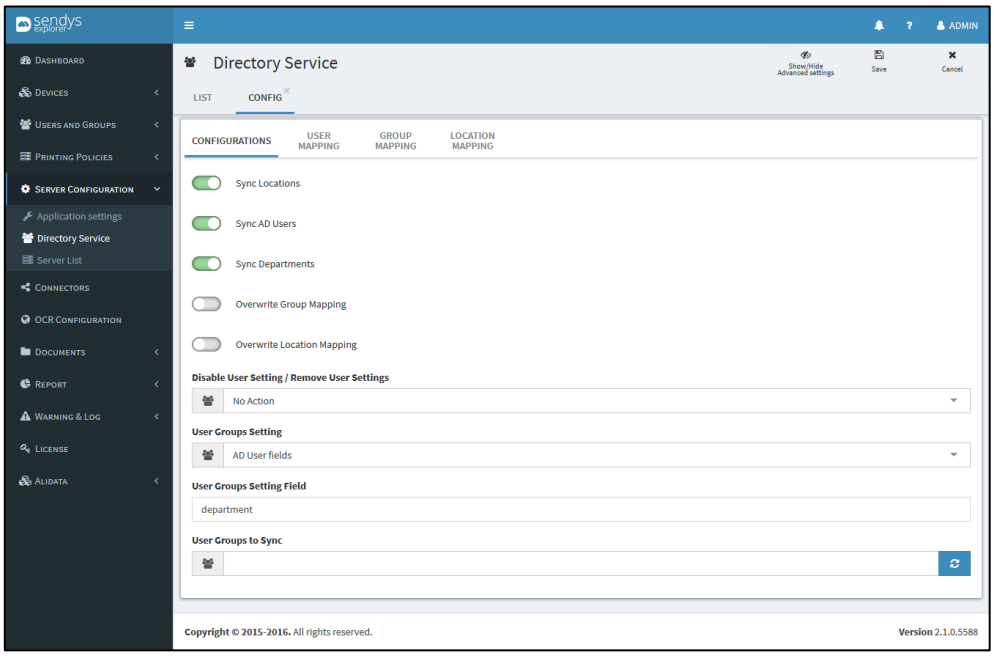


Fig. 274 - Directory Service Configurations

2. Make the required configuration.

Name	Details
Sync Locations	Enable this option and SENDYS Explorer will sync Locations from the Directory Service
Sync AD Users	Enable this option and SENDYS Explorer will sync Users from the Directory Service
Sync Departments	Enable this option and SENDYS Explorer will sync Departments from the Directory Service
Overwrite Group Mapping	Create Groups information based on specified Group options mapping.
Overwrite Location Mapping	Create Locations information based on specified Locations options mapping.
Disable User Setting / Remove User Settings	When a user is disable or not exists on directory service this will be the action taken on SENDYSExplorer.
User Groups Setting	Select how to Import Groups from Directory service to SENDYS Explorer.
User Groups Setting Field	Field to MAP User Group, this when groups are created from Directory Service User Field.
User Groups to Sync	When using Directory Service Groups Mapping select the desired groups to synchronize and map users.

Table 42 - Directory Service Configurations

3. Click **Save** to save the Directory Service Configurations.

USER MAPPING

1. Click on **User Mapping** .

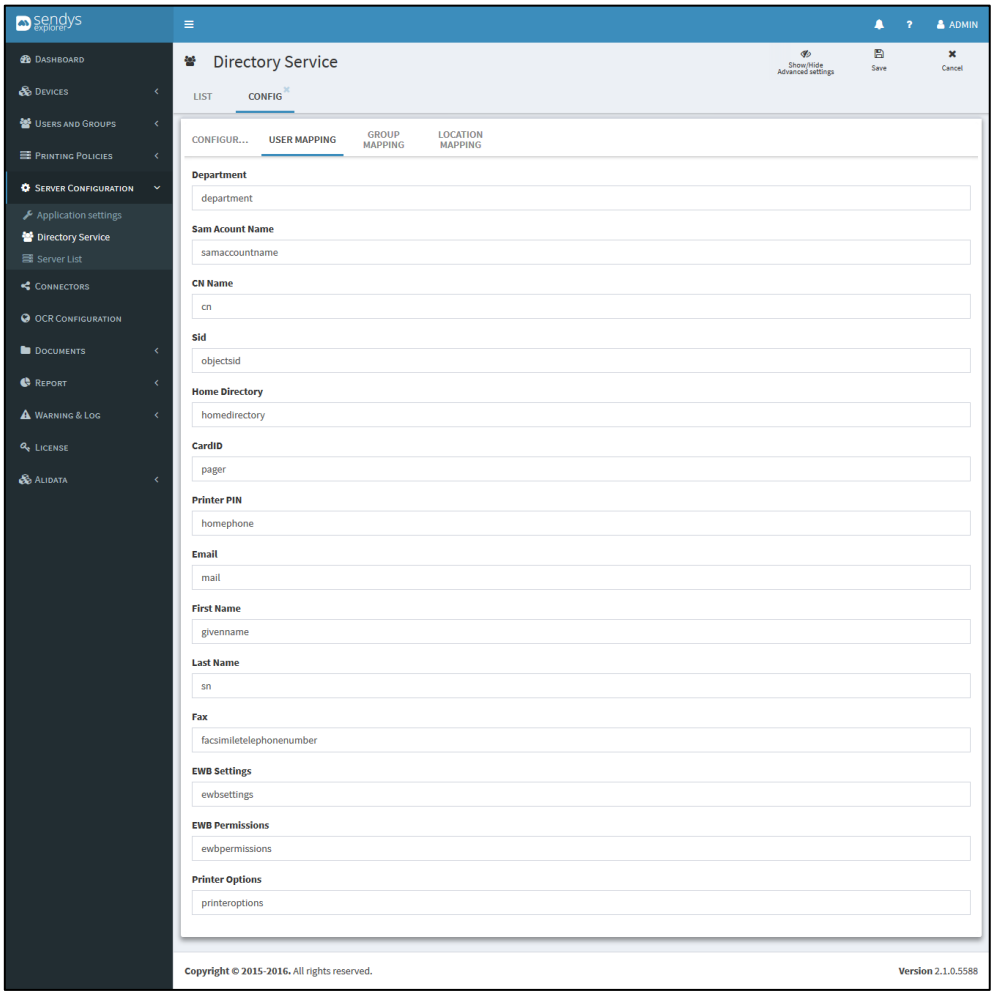


Fig. 275 - Directory Service User Mapping

2. Make the required configuration.

Field Name in Directory Service	Default
Department	department
SAM Account Name	samaccountname
CN Name	cn
Sid	objectsid
Home directory	homedirectory
CardID	pager
Printer PIN	homephone
Email	mail
First Name	givenname
Last Name	sn
Fax	facsimiletelephonenumber
EWB Settings	ewbsettings
EWB Permissions	ewbpermissions
Printer options	printeroptions

Table 43 - Directory Service User Mapping

3. Click **Save** to save the User Mapping Configuration.

GROUP MAPPING

1. Click on **Group Mapping**.

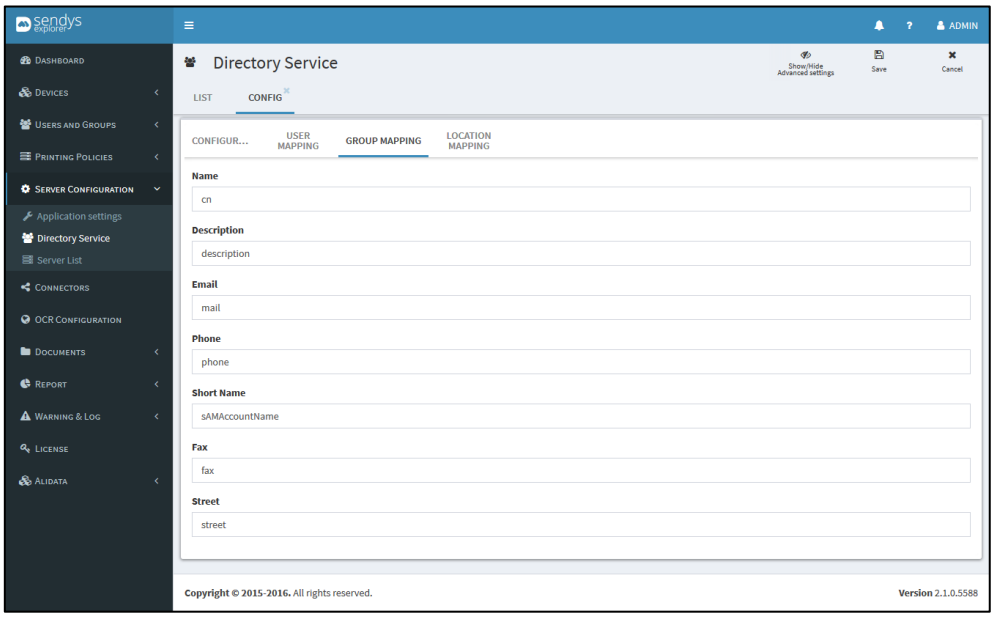


Fig. 276 - Directory Service Group Mapping

2. Make the required configuration.

Field Name in Directory Service	Default
Name	cn
Description	description
Email	mail
Phone	phone
Short Name	sAMAccountName
Fax	fax
Street	street

Table 44 - Directory Service Group Mapping

3. Click **Save** to save the Group Mapping Configuration.

LOCATION MAPPING

1. Click on **Location Mapping**.

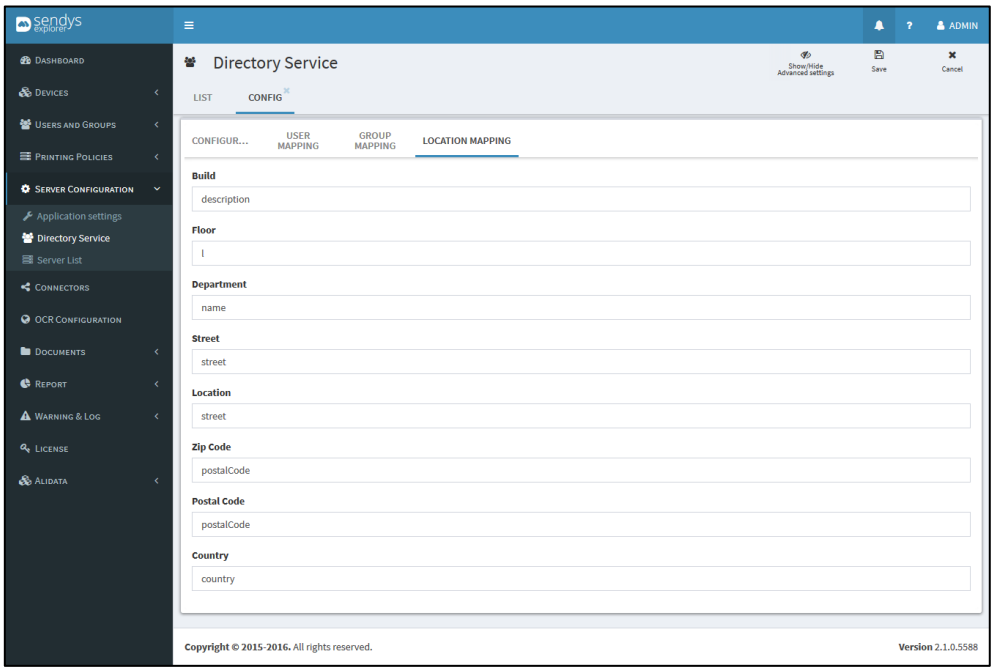


Fig. 277 - Directory Service Location Mapping

2. Make the required configuration.

Field Name in Directory Service	Default
Build	description
Floor	l
Department	name
Street	street
Location	location
Zip Code	zipCode
Postal Code	postalCode
Country	country

Table 45 - Directory Service Location Mapping

3. Click **Save** to save the Location Mapping Configuration.

Related with Synchronize we have two options:

SYNC AD

1. Click on **Directory Service > List**.
2. Select one or more **Directory Service** and click on **Sync AD**.
   Note: If you only have one Directory Service configured, there is no need to select it, the synchronization process will start for that DS

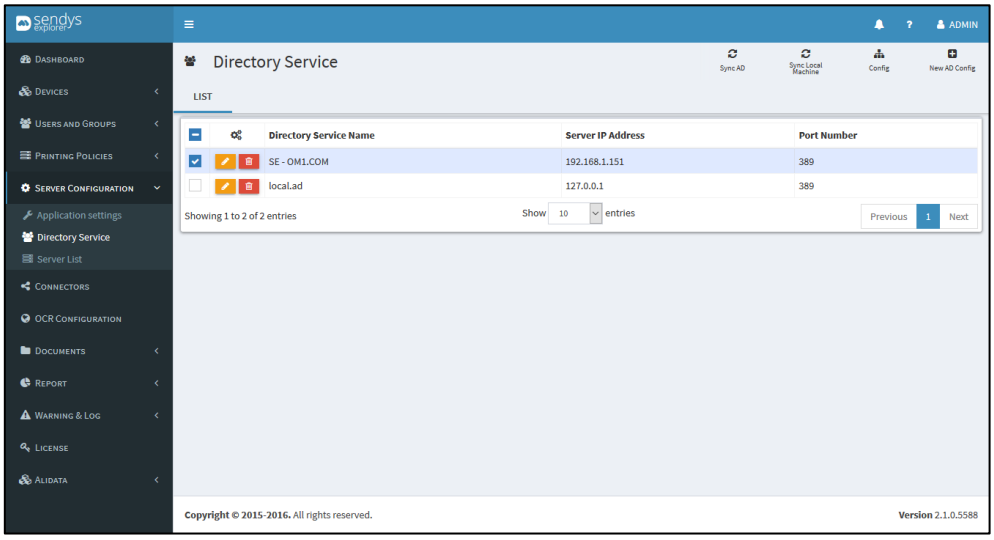


Fig. 278 - Sync AD

3. Click **YES** to confirm information synchronization.

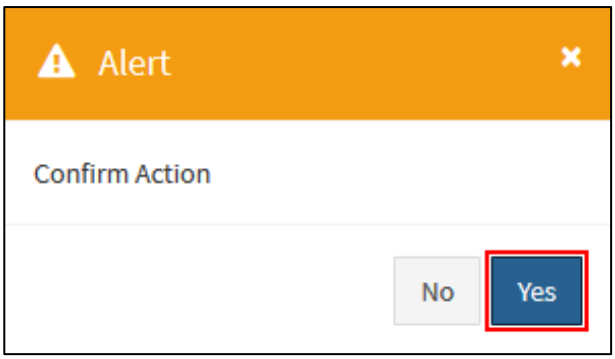


Fig. 279 - Sync AD

SYNC LOCAL MACHINE

1. Click on **Directory Service > List**.
2. Click on **Sync Local Machine**.

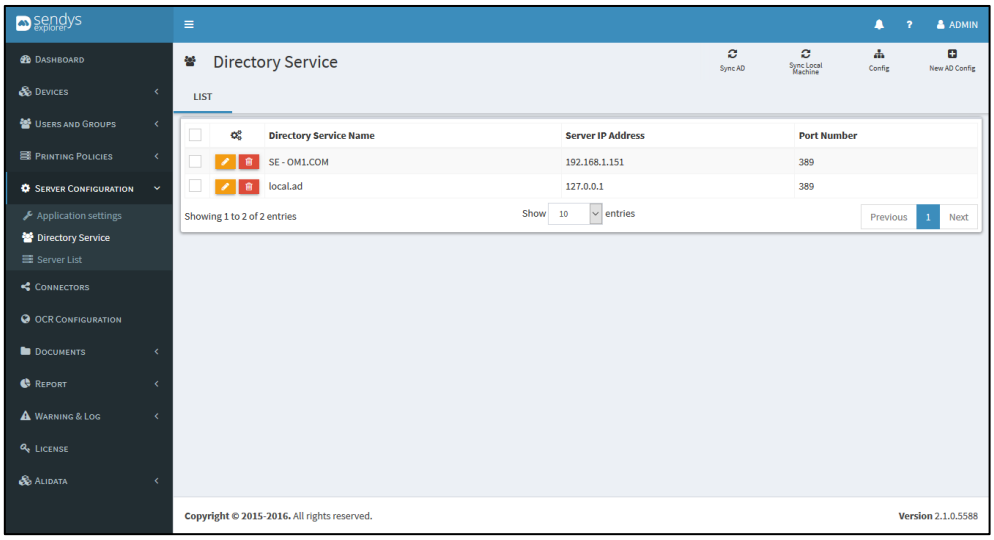


Fig. 280 - Sync Local Machine

3. Click **YES** to confirm information synchronization.

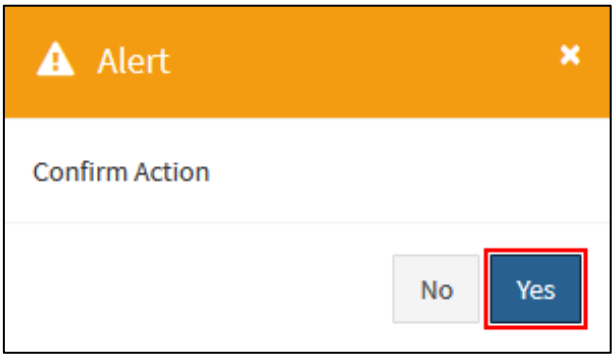


Fig. 281 - Sync Local Machine

SERVER LIST

This sections shows a list of all servers that the SENDYS Explorer Output Manager works with.

1. Click on **Server Configuration > Server List**.
2. Click on **pencil icon** to edit or consult some aspects.

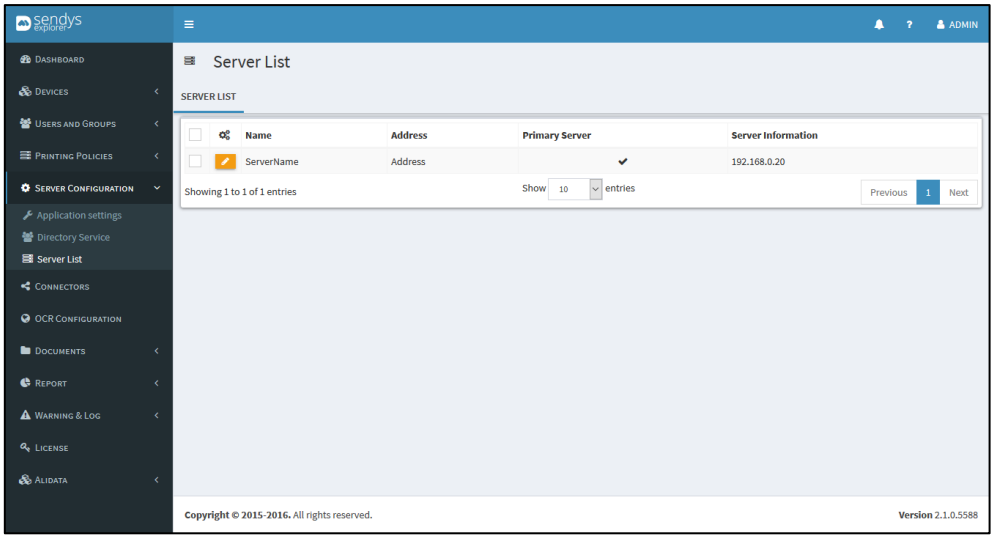


Fig. 282 - Server List

3. Make the required configuration.

Name	Details
Name	You can define one name for the server
Address	Address where the server is located
Server Information	This is the IP of the server
Internal Server Port	
Internal Server Port Add	

Table 46 - Server List

4. Click **Save** to save the configuration.

CONNECTORS

This section allows you to make the right configuration to each connector by click the **pencil icon**.

Home Folder and **Email** connector's only will be visible on device screen after correct configuration. So if the administrator does not configure properly the **Home Folder** configured on user options, Scan to Home Folder will not be present on device screen. Also if the **Email** connector is not well configured, **Scan to Email and Fax Server** will not be present on device screen.

The **Reorder** button shows a window to reorder the list of connectors. **Refresh** button to Refresh the list.

HARD LINK TO A SPECIFIC CONNECTOR

If you desire to configure on the device a direct link (**Hard-Link**) for one specific connector, you could click on the **link icon** and it will open a new window with the "direct link" for that connector, this is the link that you need to configure on the device.

Scan Connectors available in Output Manager:

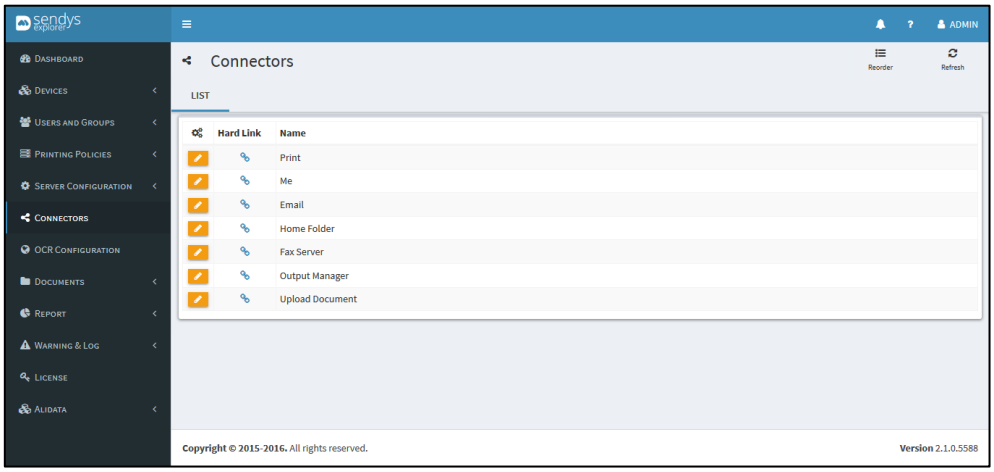


Fig. 283 - Scan Connectors

Scan Connectors including optional purchases:

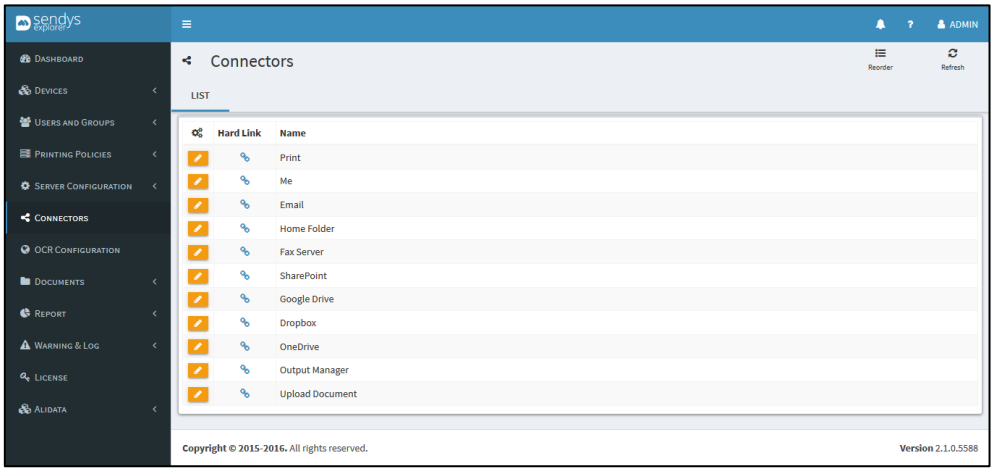


Fig. 284 - Scan Connectors (PREMIUM)

To restore all connectors information, to the default value please follow those steps:

1. Click on **Server Configuration > Application Settings**.
2. Click on **Application Config > Scan**.
3. Click on **Restore default Connectors**.

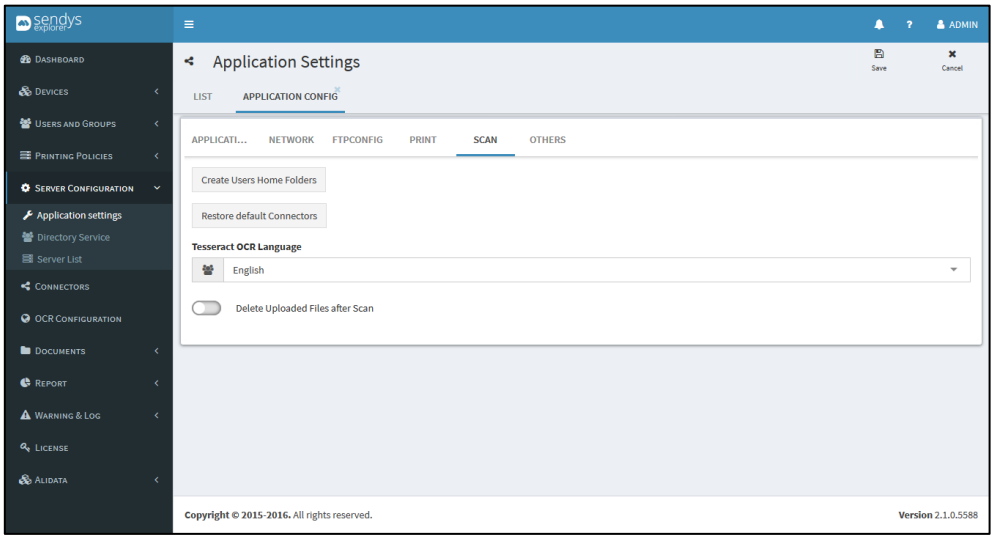


Fig. 285 - Scan Settings

4. Click **YES** to confirm restore.

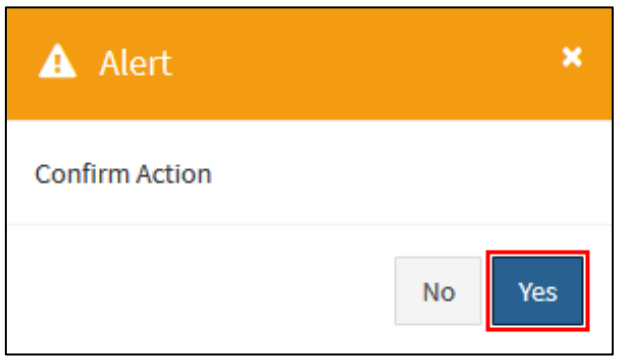


Fig. 286 - Restore Connectors

PRINT

1. Click on **Connectors**.
2. Click on the **pencil icon** to edit **Print**.

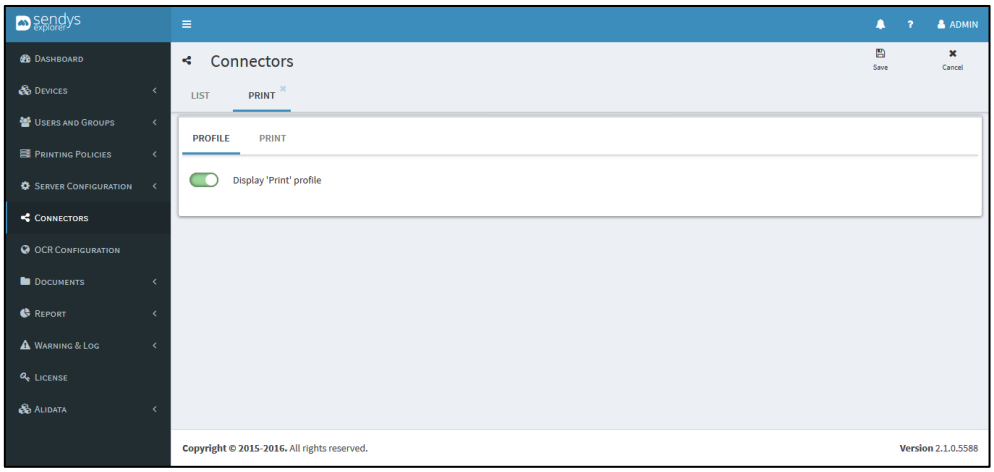


Fig. 287 - Print Connector

3. Change the **visibility (Display "Print" profile).** "Print" connector will be hidden if this option is not selected.
4. Click **Save** to apply the changes.

PRINT

1. Click on **Print**.

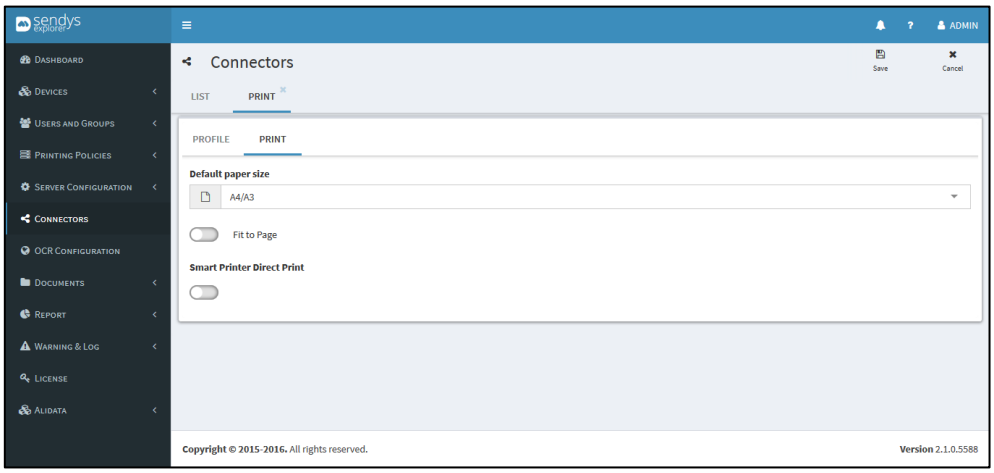


Fig. 288 - Print Connector

2. Make the required configuration.

Name	Details
Default paper size	This means that (A4 / A3) size convention / or (Letter and Tabloid) size convention will be selected.
Fit to Page	This function can resize the document pages to fit the selected paper size chose on the printing dialogue box.
Smart Printer Direct	If this option is enabled, MFP will show the native print dialogue on the panel (Print Settings).

Table 47 - Print Connector

If the option “Smart Printer Direct” is enable this will be present on printer panel:

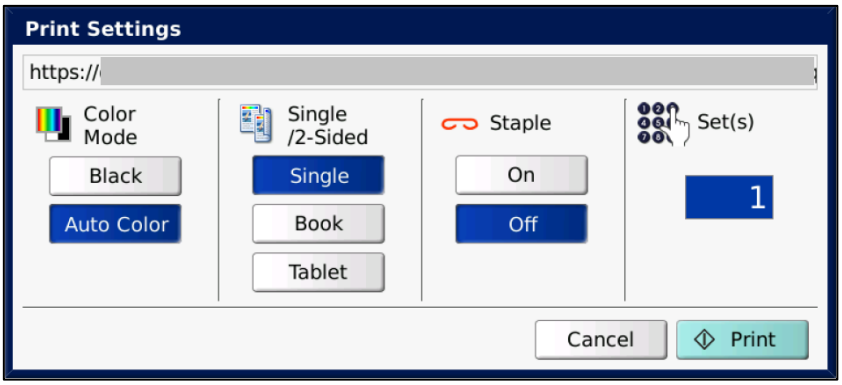


Fig. 289 - Smart Printer Direct

3. Click **Save** to save the configuration.

BOX

BOX is a container concept.

Administrator can add PDF files to **BOX** and they will be accessible immediately for all users to print.

The **BOX** container is allocated at SENDYS Explorer server:

“C:\inetpub\ftproot\SENDYSExplorer\ScannedFiles\Box”

Additionally, subfolders can be created inside above directory (**only one level deep**).

Please be sure that all documents within **BOX** are PDF documents.

ME

1. Click on **Connectors**.
2. Click on the **pencil icon** to edit **Me**.

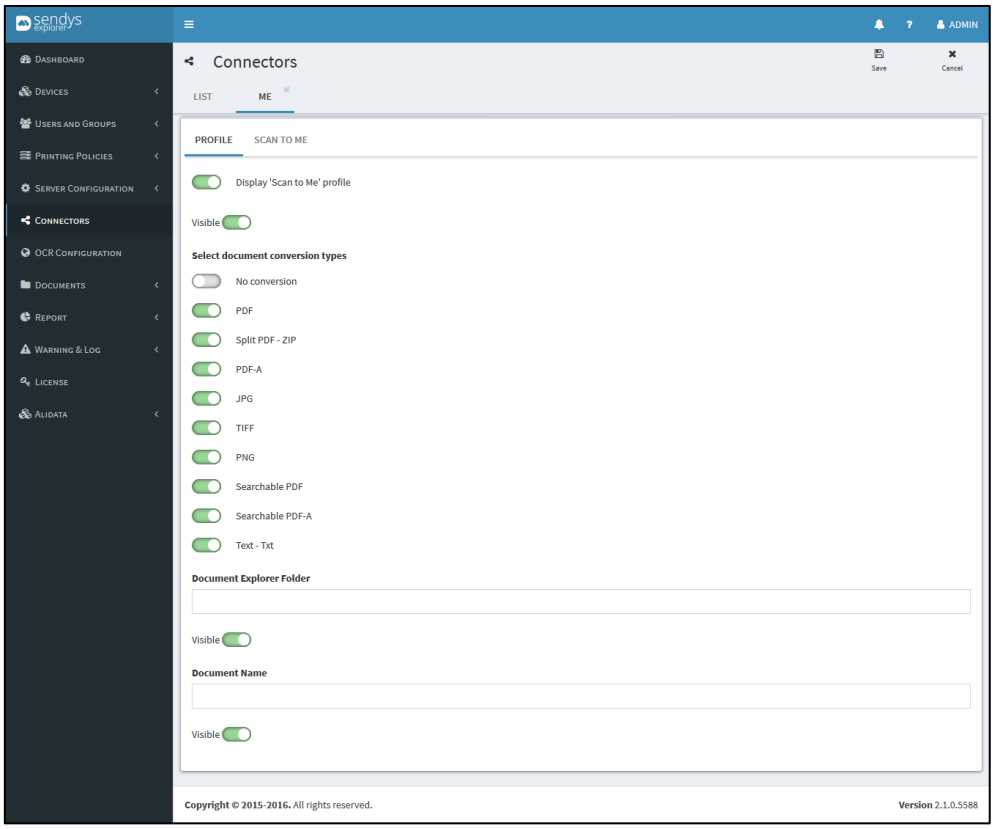


Fig. 290 - Scan to Me Connector

3. Change the **visibility** and choose which fields should be presented on Connector.
4. Click **Save** to apply the changes.

SCAN TO ME

1. Click on **Scan to Me**.

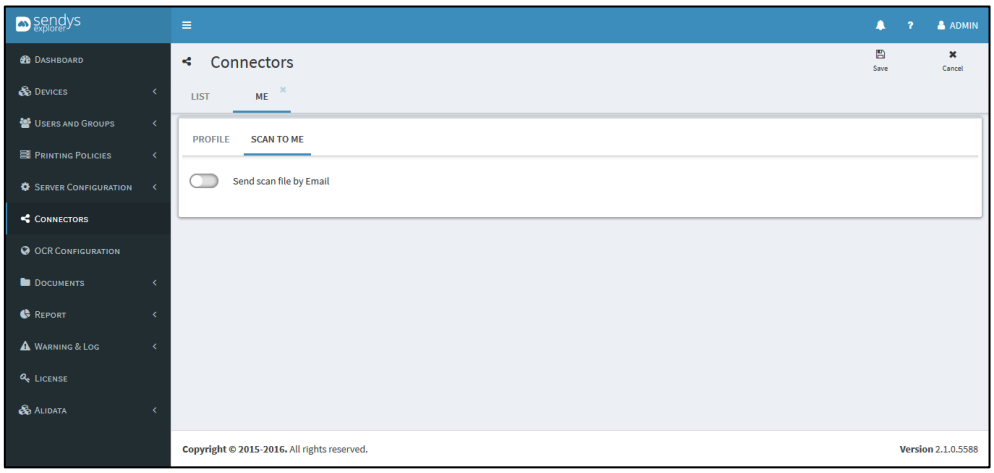


Fig. 291 - Scan to Me Connector

2. If you want to send a copy of the scanned files to the users' email, please check option **Send scan file by email**.
   Note: Please, configure **Email** connector before activate this feature, or the system will produce an error when using **Scan to Me**.
3. Click **Save** to save the configuration.

EMAIL

1. Click on **Connectors**.
2. Click on the **pencil icon** to edit **Email**.

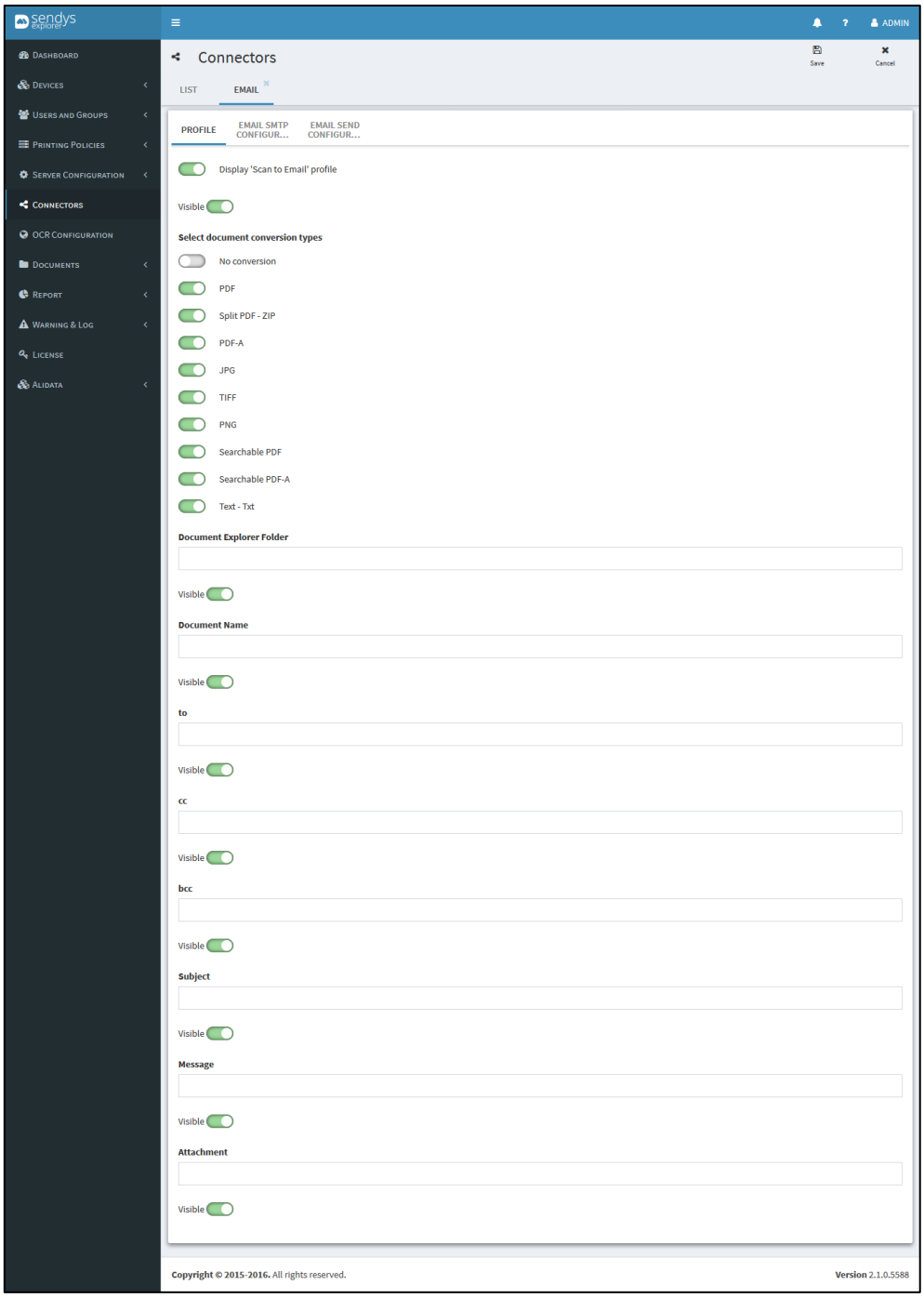


Fig. 292 - Scan to Email Connector

3. Change the **visibility** and choose which fields should be presented on Connector.
4. Click **Save** to apply the changes.

EMAIL SMTP CONFIGURATIONS

1. Click on **Email SMTP Configurations**.

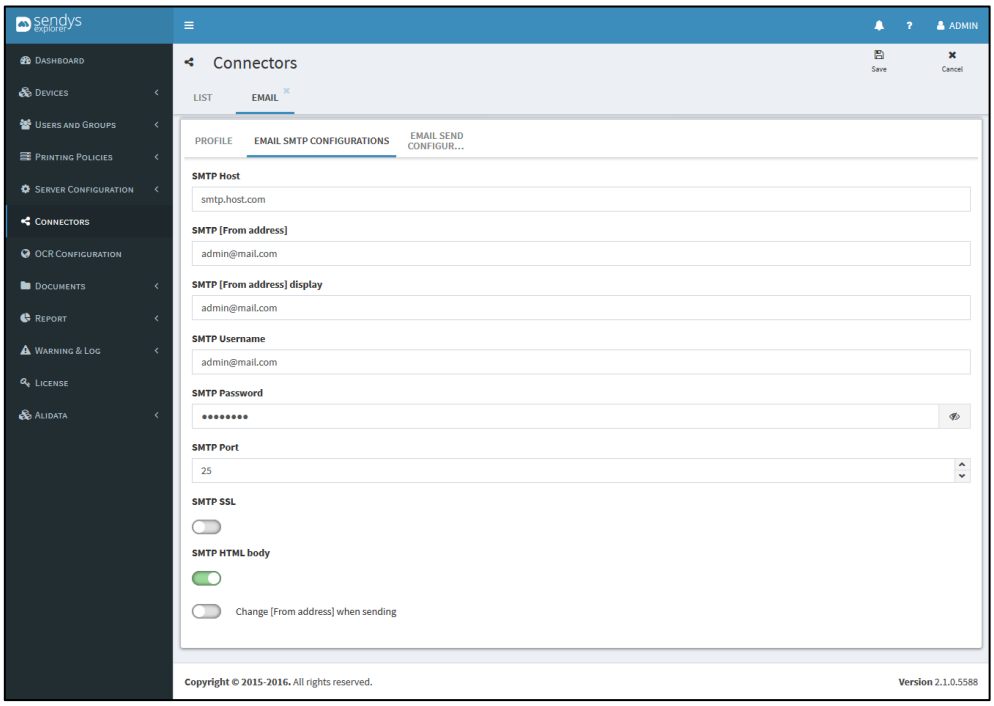


Fig. 293 - Email SMTP Configurations

2. Make the required configuration.

Name	Details
SMTP Host	Host name or IP address
SMTP [From address]	Default from email address
SMTP [From address] display	Default from display name email address
SMTP Username	Username for SMTP access
SMTP Password	Password for SMTP access
SMTP Port	Port for SMTP access
SMTP SSL	Enable/Disable SSL
SMTP HTML Body	Check this to send emails as html
Change [From address] when sending	If you want Users' email addresses to be used as senders' email, please use switch to turn on **Change [From address] when sending email**. Otherwise, the sender's email will be **SMTP [From address]**.

Table 48 - Email SMTP Configurations

3. Click **Save** to save the configuration.

EMAIL SEND CONFIGURATIONS

1. Click on **Email Send Configurations**.

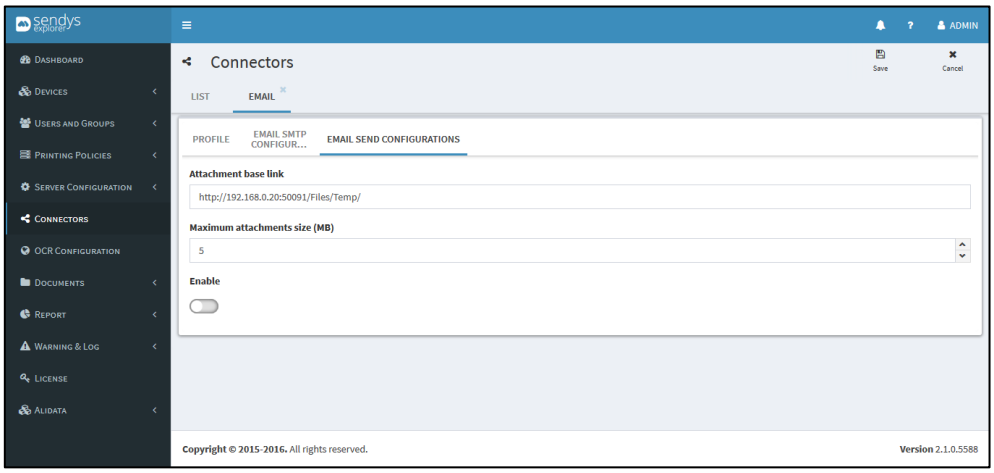


Fig. 294 - Email Send Configurations

2. Make the required configuration.

Name	Details
Attachment base link	Base URL of the system temporary folder
Maximum attachments size (MB)	Maximum file size in MB
Enable	Check for file size verification, uncheck to disable

Table 49 - Email Send Configurations

3. Click **Save** to save the configuration.

HOME FOLDER

1. Click on **Connectors**.
2. Click on the **pencil icon** to edit **Home Folder**.

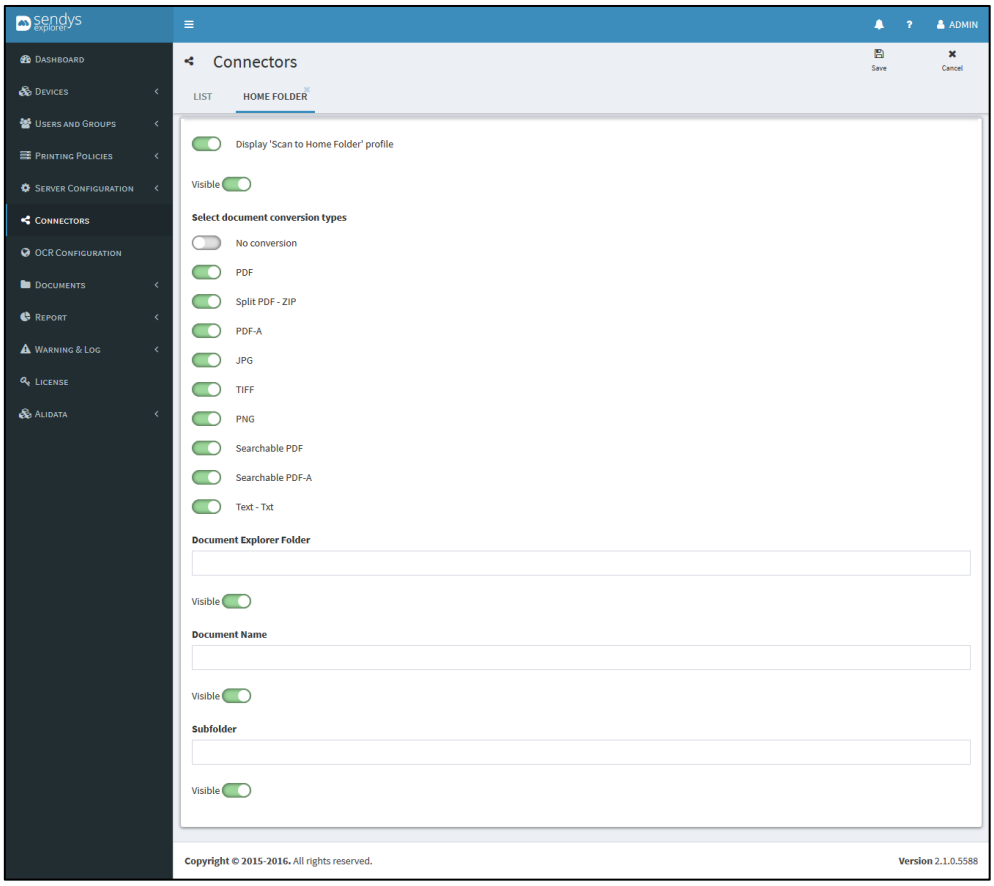


Fig. 295 - Scan to Home Folder Connector

3. Change the **visibility** and choose which fields should be presented on Connector.
4. Click **Save** to apply the changes.

Note: **Subfolder** means an additional path string that will be added to the **Home Folder**. If you have an additional folder inside **Home Folder**, and you insert that folder name as suffix, the document will be put inside that folder.

E.g. if you have an **Invoices** and **Scan** directories inside **Home Folder**, you can insert use **Invoices** or **Scan** as a suffix.

HOME FOLDER CONFIGURATIONS

The configuration of the **Home Folders** is set in the **User Settings**. If you are working with **Directory Service** and the users have **Home Folders** configured, the system will pick it up during the synchronization process.

SENDYS Explorer will create the home folders in **C:\inetpub\ftproot\SENDYSExplorer\HomeDirectory**. You need to share the folder in order so both **users** and **SENDYS Explorer** have access to the scanned files. The user's **Home Folders** will be created based on the username, and the user account used to write the files in the folder is the user account that was set up during the installation process.

1. Click on **Server Configuration > Application Settings**.
2. Click on **Application Config > Scan**.
3. Click on **Create Users Home Folders**.

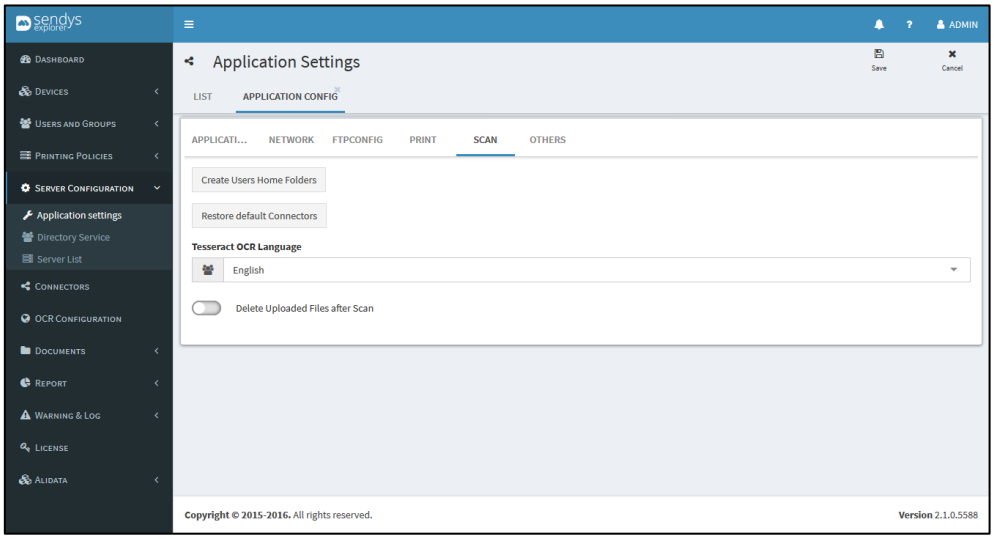


Fig. 296 - Scan Settings

4. Click **YES** to confirm Home Folder creation.

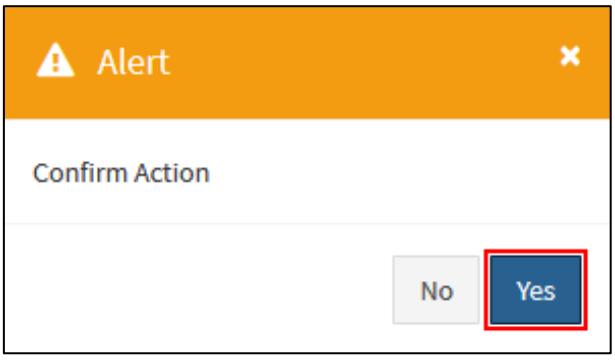


Fig. 297 - Create Users Home Folders

FAX SERVER

1. Click on **Connectors**.
2. Click on the **pencil icon** to edit **Fax Server**.

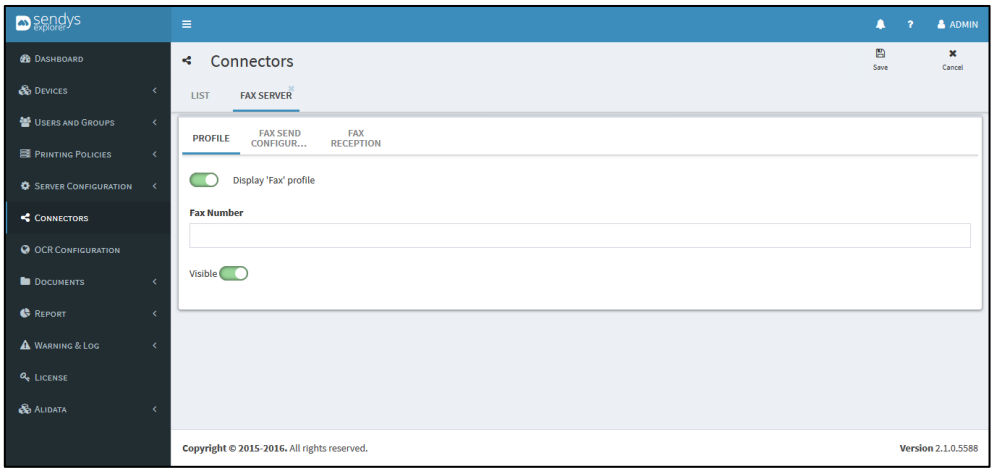


Fig. 298 - Scan to Fax Server Connector

3. Change the **visibility** and choose which fields should be presented on Connector.
4. Click **Save** to apply the changes.

FAX SEND CONFIGURATIONS

1. Click on **Fax Send Configurations**.

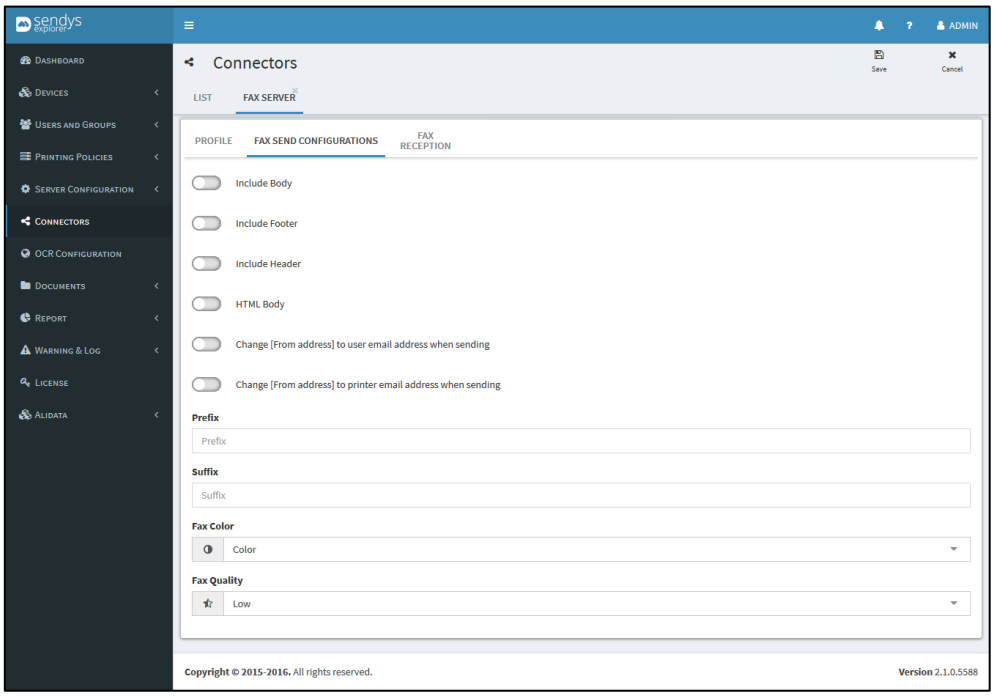


Fig. 299 - Fax Send Configurations

2. Make the required configuration.

Name	Details
Include Body	Insert default email body content
Include Footer	Insert email message footer
Include Header	Insert default email message header
HTML Body	Insert message body as html
User as source email	Change source email to be the user email
Prefix	Prefix to add to fax number
Suffix	Suffix content to add to fax number
Fax Color	Fax color options (mono, grayscale, color).
Fax Quality	Fax quality (low, medium, high).

Table 50 - Fax Send Configurations

3. Click **Save** to save the configuration.

FAX RECEPTION

1. Click on **Fax Reception**.

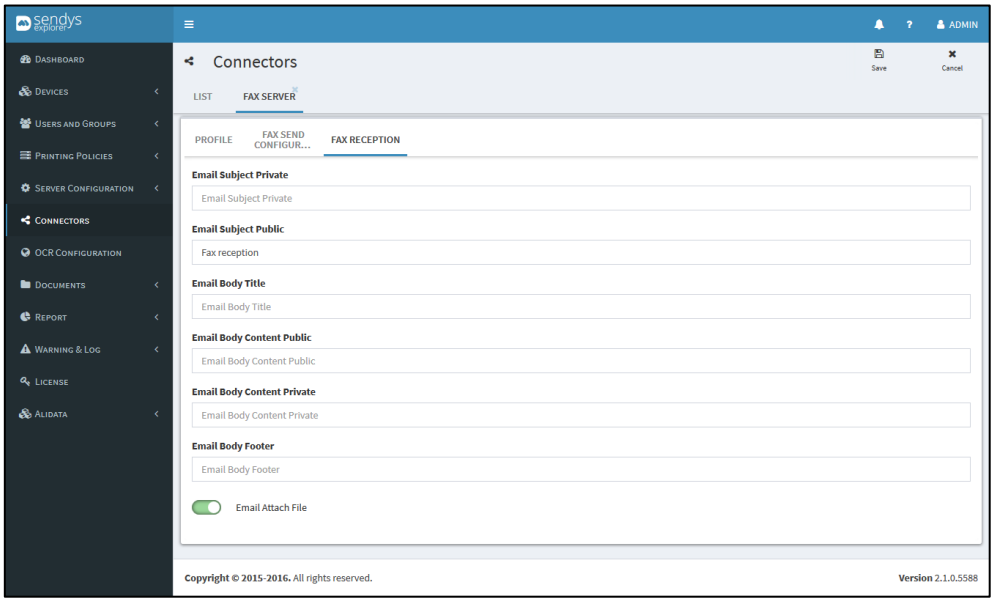


Fig. 300 - Fax Reception

2. Make the required configuration.

Name	Details
Email Subject Private	Insert the subject for Private send.
Email Subject Public	Insert the subject for Public send.
Email Body Title	Insert default email body title.
Email Body Content Public	Insert email body message for Public.
Email Body Content Private	Insert email body message for Private.
Email Body Footer	Insert default email body footer.
Email Attach File	Send the email with the file in attach.

Table 51 - Fax Reception

3. Click **Save** to save the configuration.

UPLOAD DOCUMENT

1. Click on **Connectors**.
2. Click on the **pencil icon** to edit **Upload Document**.

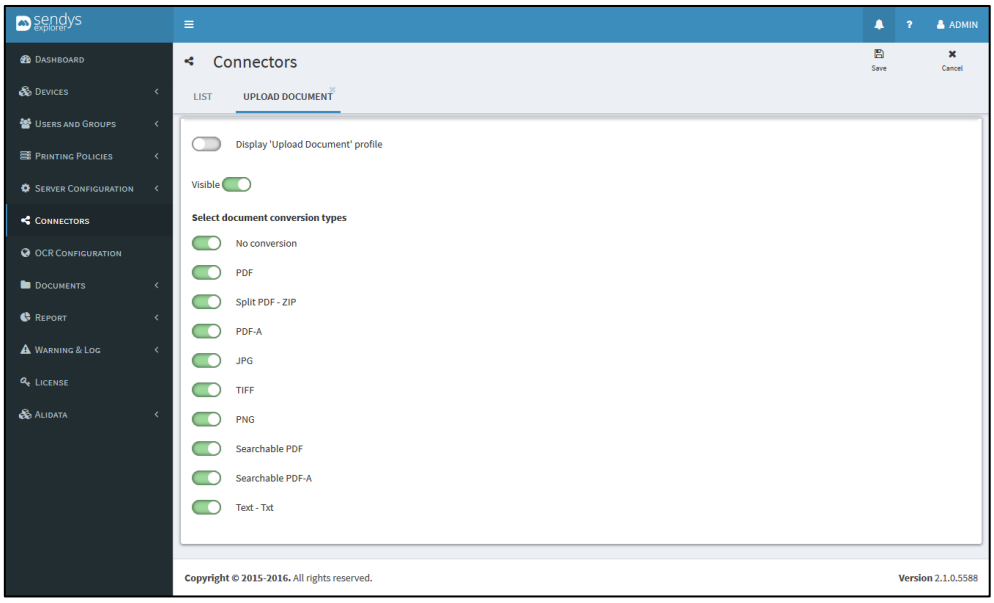


Fig. 301 - Upload Document

3. Change the **visibility** and choose which fields should be presented on Connector.
4. Click **Save** to apply the changes.

HOW TO USE

Uploading from the Web Portal supports multi-file upload. After the upload finishes files will be stored on the chosen system folder.

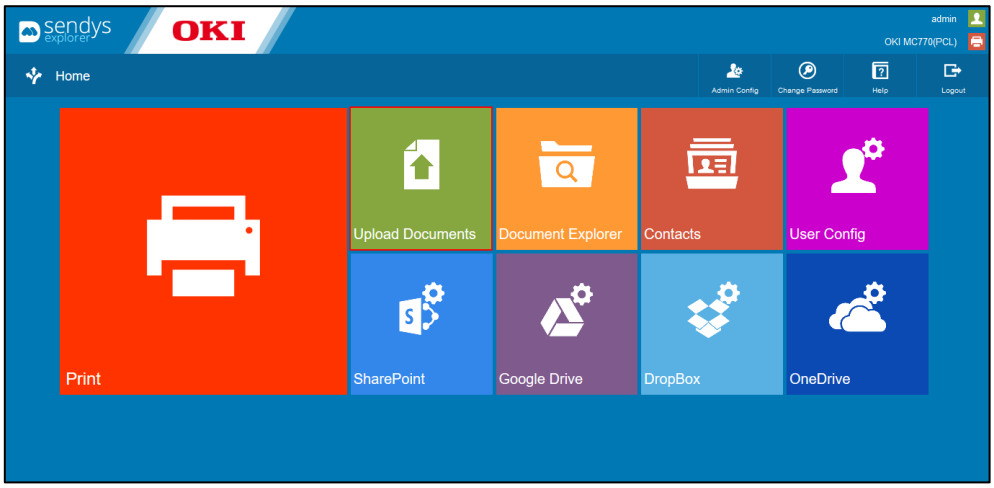


Fig. 302 - – Web Portal - Upload Document

1. Click on **Upload Document**.
2. Click to trigger file upload or drag and drop documents.
3. Choose **Output Format** from a group of file type conversion and OCR combination.
4. Choose the **Folder** in which to store your documents.
5. Click on **Upload**.

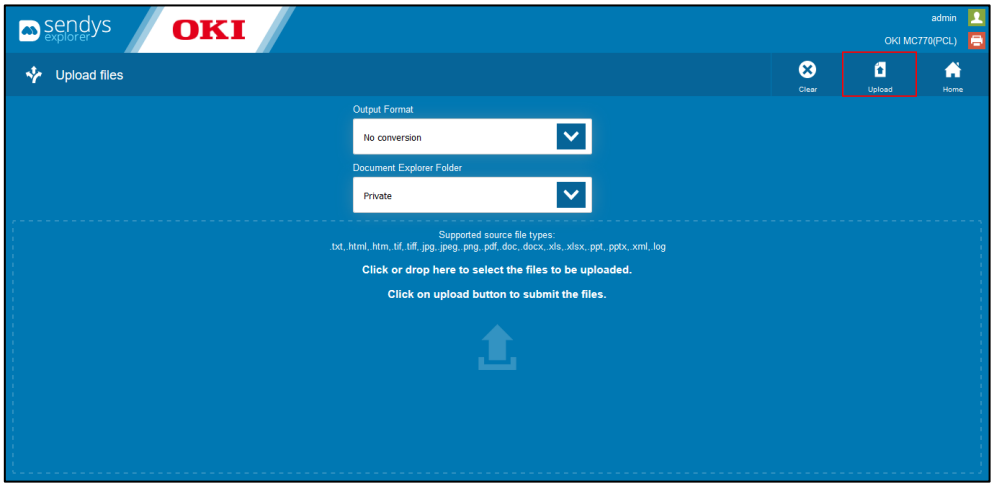


Fig. 303 - – Web Portal - Upload Document

SHAREPOINT

1. Click on **Connectors**.
2. Click on the **pencil icon** to edit **SharePoint**.

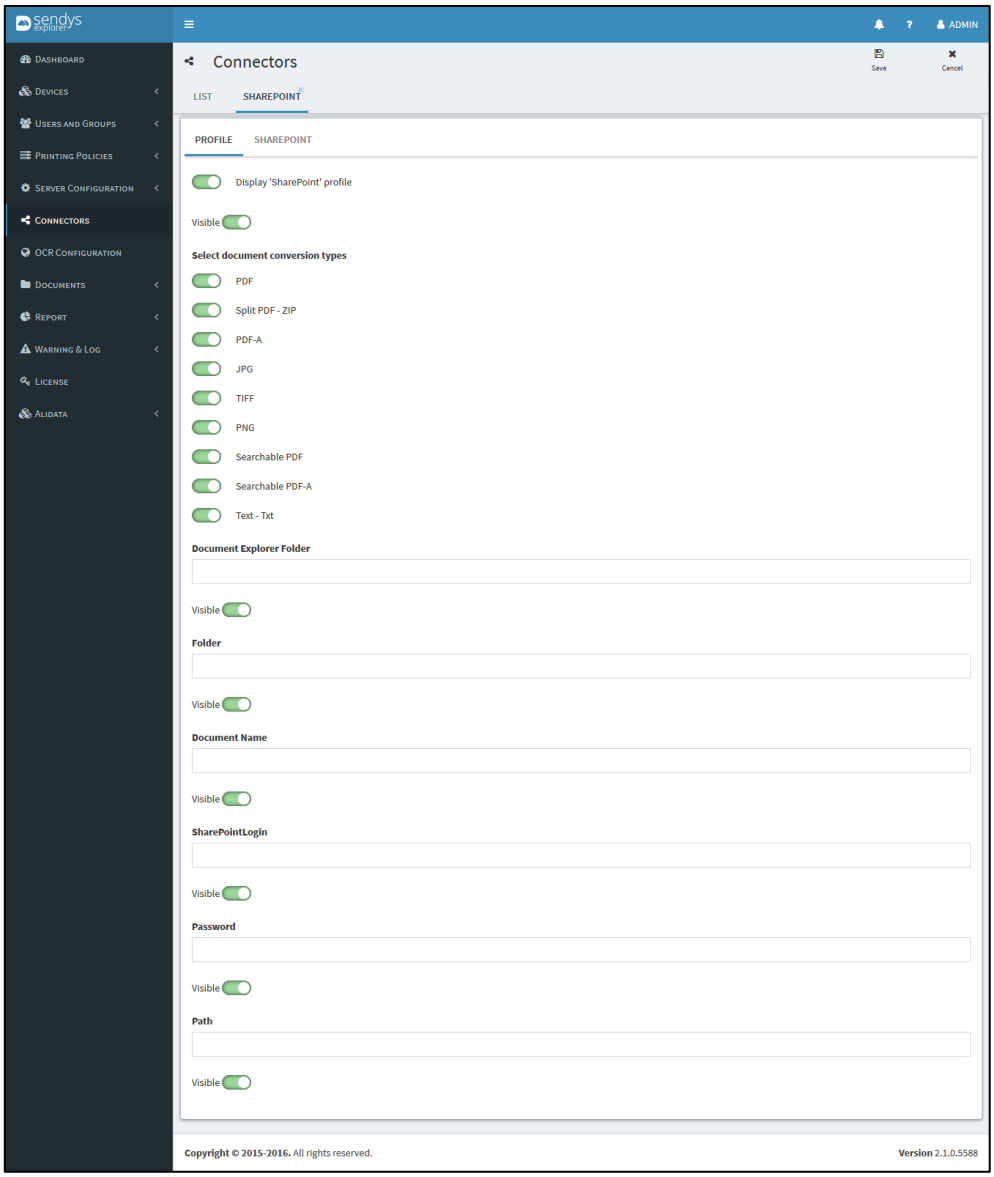


Fig. 304 - Scan to SharePoint Connector

3. Change the **visibility** and choose which fields should be presented on Connector.
4. Click **Save** to apply the changes.

SHAREPOINT

1. Click on **SharePoint**.

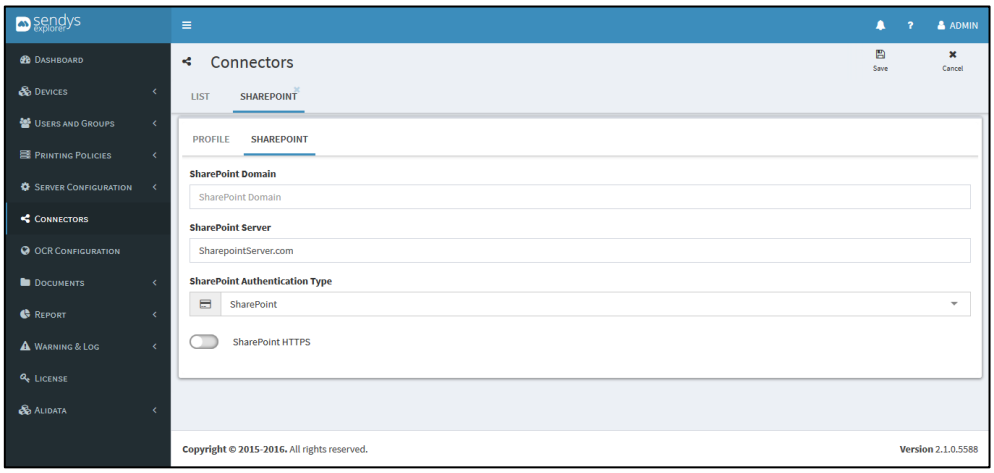


Fig. 305 - SharePoint Connector

2. Make the required configuration.

Name	Details
SharePoint domain	You only need to configure this if you are in the same domain as the SharePoint server, if you are accessing a SharePoint remotely you need to leave this field empty
SharePoint server Name	If you are in the same domain you can set this with the name of SharePoint machine, if you are not in the same domain you can set this with the full name to access SharePoint.
SharePoint type	Local/online 365
SharePoint Https	Select if SharePoint server uses https

Table 52 - SharePoint Connector

3. Click **Save** to save the configuration.

Note: SharePoint supported types have some limitation, on the types that are supported and also in each type definition.

Please review the follow types and types' definitions:

- **Text**: SENDYS Explorer does not restrict the max amount of characters.
- **Multi-line** Text: SENDYS Explorer does not restrict max amount of characters.
- **Choice Menu**: SENDYS Explorer does not support multi selection menu, multi-selection menu will be display as a single selector.
- **Number**: SENDYS Explorer supports INTEGER type only, no max/min values validation.
- **Currency**: No max/min values validation.
- **Date/Time**: SENDYS Explorer supports DATE type only.
  Note: **Date/Time** is displayed as "**DD/MM/YYYY**", but it is a cosmetic user interface **ONLY**. **No validation**.
- **Yes/No**: Supported.
- **Search**: Not supported.
- **Person or Group**: Not supported.
- **Hyperlink or Image**: Not supported.
- **Calculated Field**: Not supported.
- **Task Result**: Not supported.
- **External data**: Not supported.
- **Managed metadata**: Not supported.

For any non-supported types, if there is a default value set at SharePoint, SENDYS Explorer will be compliance with it.

GOOGLE DRIVE

1. Click on **Connectors**.
2. Click on the **pencil icon** to edit **Google Drive**.

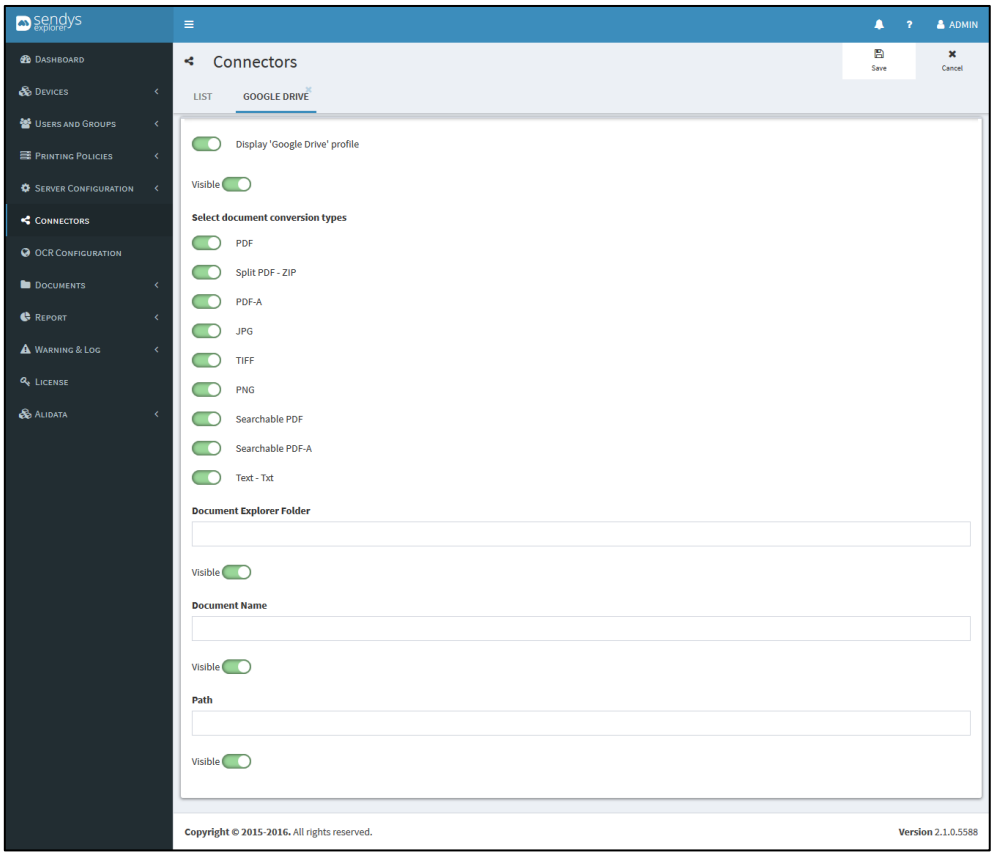


Fig. 306 - Scan to Google Drive

3. Change the **visibility** and choose which fields should be presented on Connector.
4. Click **Save** to apply the changes.

DROPBOX

1. Click on **Connectors**.
2. Click on the **pencil icon** to edit **Dropbox**.

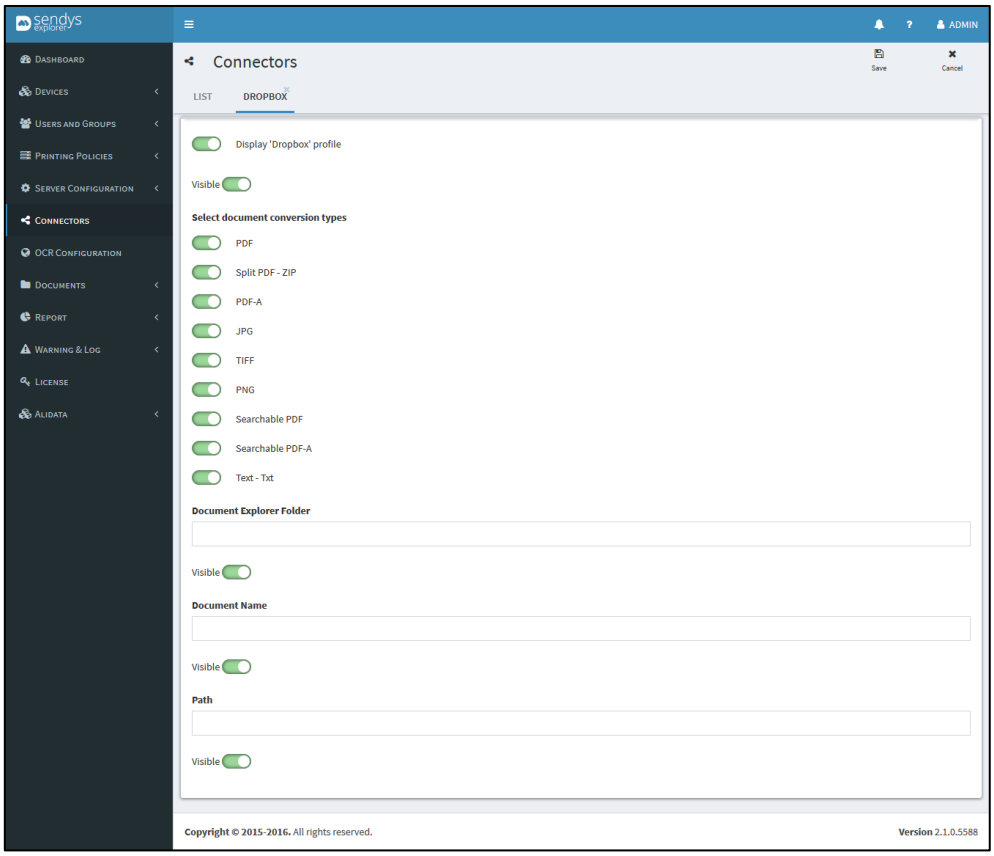


Fig. 307 - Scan to Dropbox

3. Change the **visibility** and choose which fields should be presented on Connector.
4. Click **Save** to apply the changes.

ONEDRIVE

1. Click on **Connectors**.
2. Click on the **pencil icon** to edit **OneDrive**.

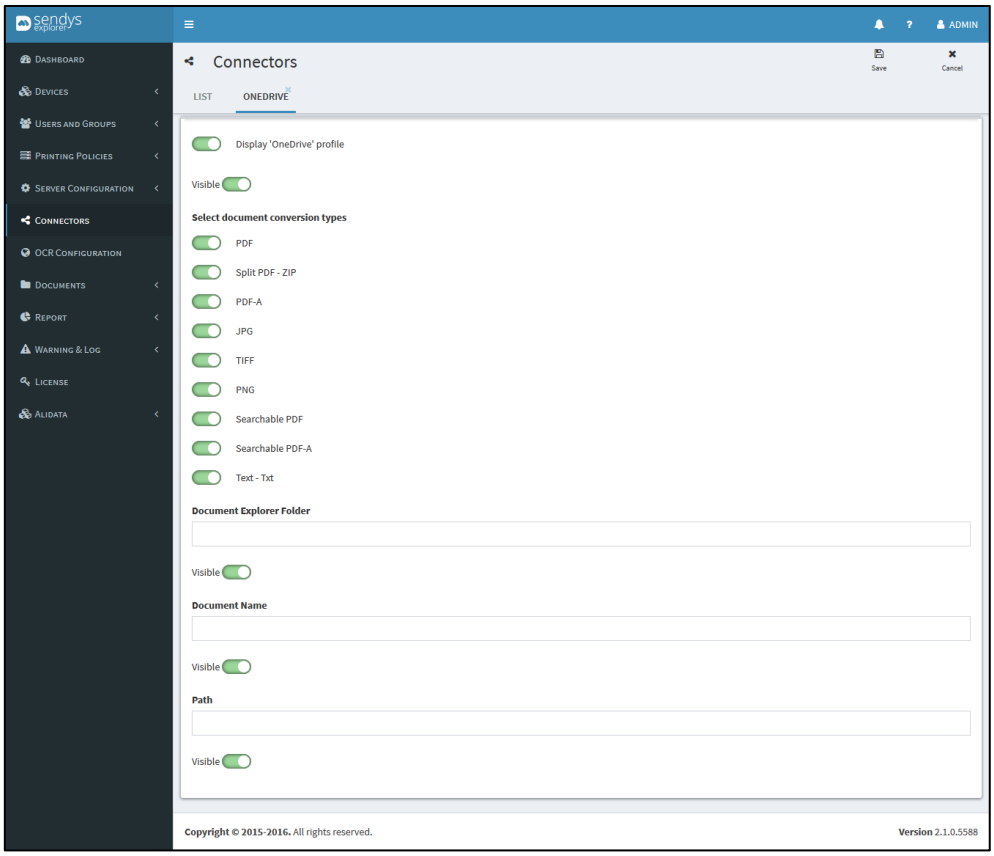


Fig. 308 - Scan to OneDrive

3. Change the **visibility** and choose which fields should be presented on Connector.
4. Click **Save** to apply the changes.

ONEDRIVE 365

1. Click on **Connectors**.
2. Click on the **pencil icon** to edit **OneDrive 365**.

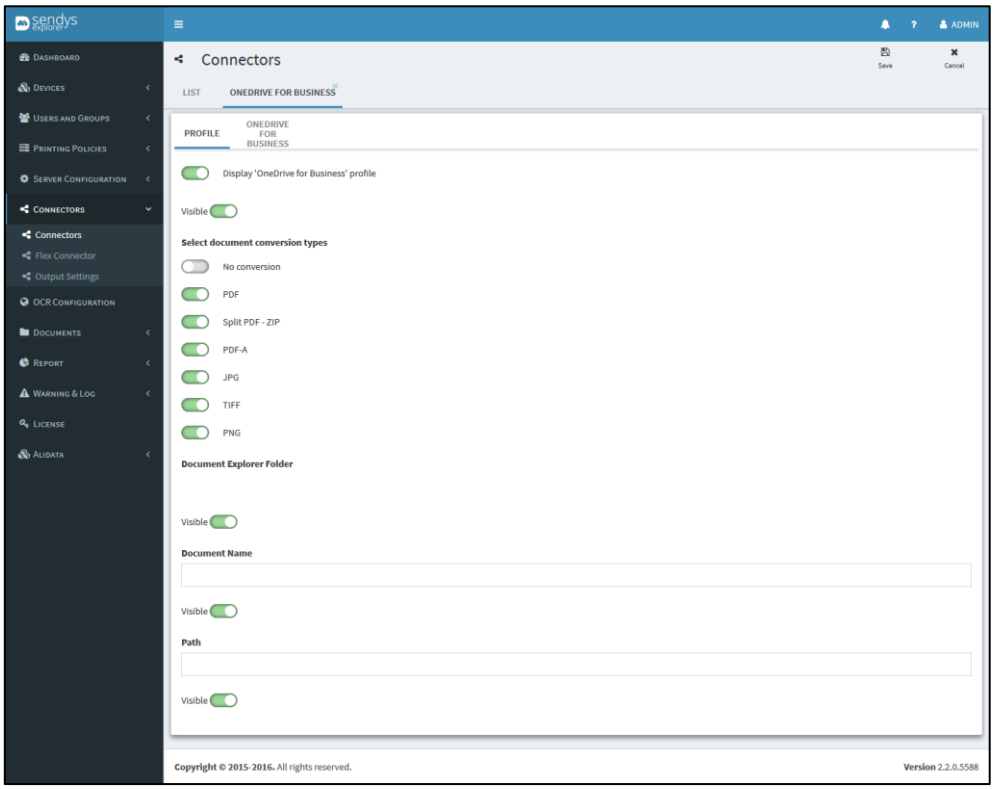


Fig. 309 - Scan to OneDrive 365

3. Change the **visibility** and choose which fields should be presented on Connector.
4. Click **Save** to apply the changes.

ONEDRIVE 365 CONFIGURATION

1. Click on **OneDrive 365**.

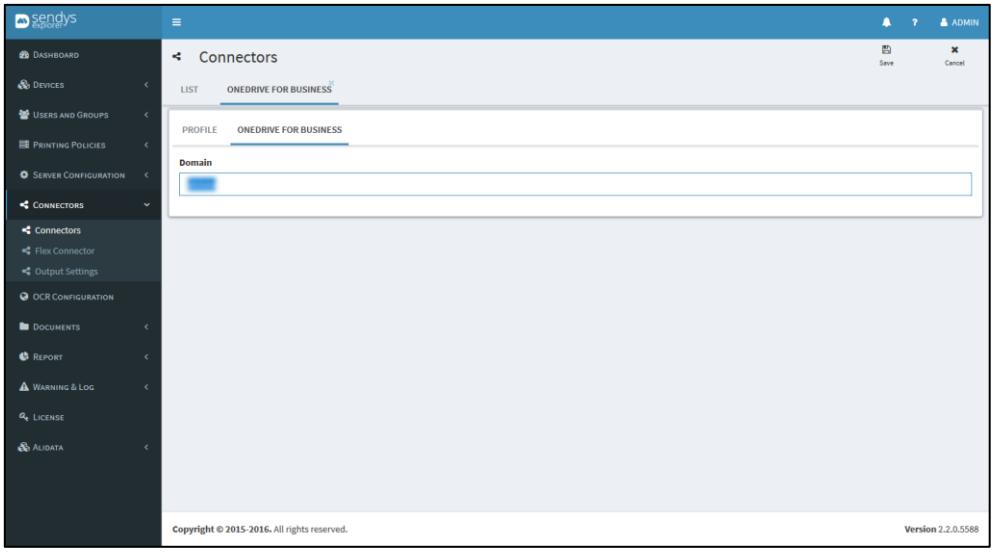


Fig. 310 - Scan to OneDrive 365

2. Make the required configuration.

Name	Details
Domain	You only need to configure this if you are in the same domain as the OneDrive server, if you are accessing a OneDrive remotely you need to leave this field empty.

3. Click **Save** to save the configuration.

YANDEX

1. Click on **Connectors**.
2. Click on the **pencil icon** to edit **Yandex**.

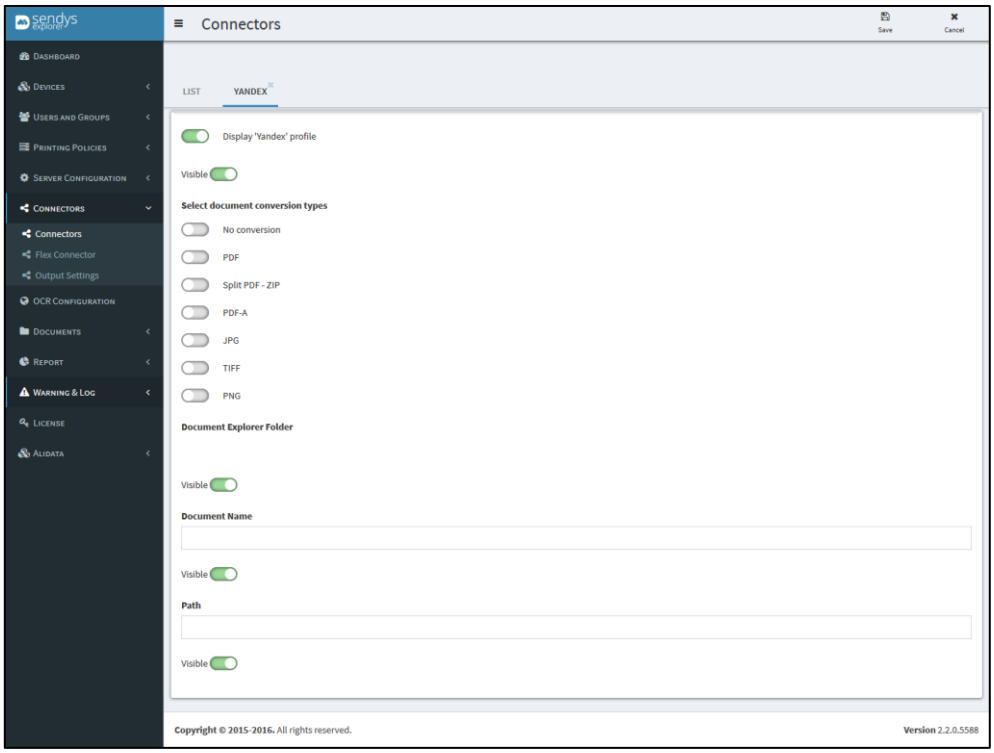


Fig. 311 - Scan to Yandex

3. Change the **visibility** and choose which fields should be presented on Connector.
4. Click **Save** to apply the changes.

OUTPUT MANAGER

1. Click on **Connectors**.
2. Click on the **pencil icon** to edit **Output Manager**.

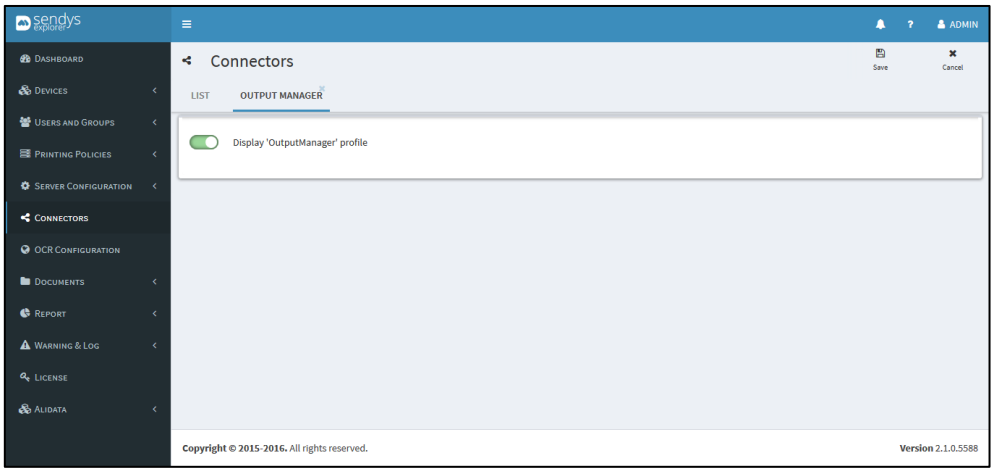


Fig. 312 - Output Manager Connector

3. Change the **visibility** and choose which fields should be presented on Connector.
4. Click **Save** to apply the changes.

FLEX CONNECTORS

Flex Connectors will allow you to create new and customized Connectors. There you can set and define different workflows for the scan documents.

The **Flex Connectors** could be very useful for integration with customer software, since it allows to set several output destinations, and also to generate Metadata for the output documents.

With **Flex Connectors** there are several workflow possibilities.

Note: to configure the **Flex Connectors** correctly you must have Output Settings configured first.

1. Click on **Connectors**.
2. Click on the **pencil icon** to edit/create **Flex Connectors**.

   Or optional:

1. Click on **Connectors**.
2. Click on **Flex Connectors**.

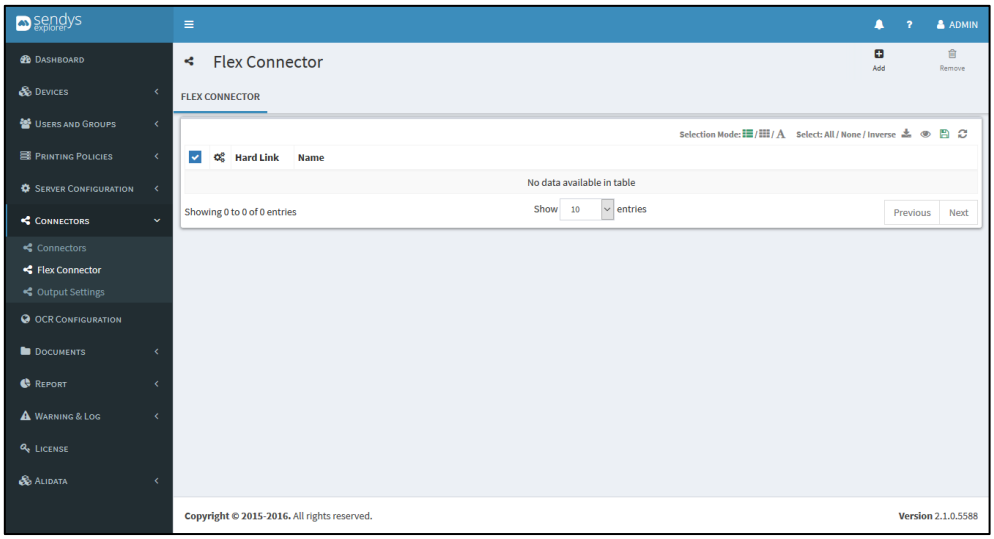


Fig. 313 - Flex Connectors

OUTPUT SETTINGS

CREATE OUTPUT SETTINGS

1. Click on **Connectors > Output Settings**.
2. Click on **Add**.

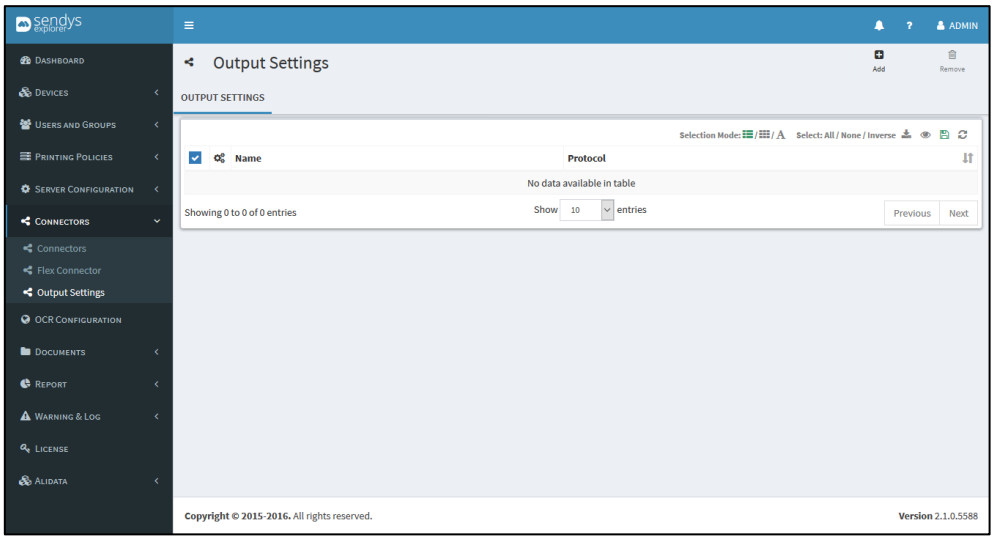


Fig. 314 - Add Output

3. Make the required configuration.

Name	Details
Name	Name to be presented on the Output
Protocol	Select the protocol used (**File** / **Samba** / **FTP**)
Path	Case you select File protocol insert the path for one exiting system folder E.g. C:/Temp Case you select **SMB** protocol insert the path for one exiting samba shared folder E. g. \\sambaserver\sharedfolder\ Case you select **FTP** protocol insert the path for one exiting FTP shared folder E. g. \sharedfolder\
Username	Username for **SMB** or **FTP** access
Password	Password for **SMB** or **FTP** access
Port	Port for **FTP** access
Server	IP for the **FTP** server

Table 53 - Add Output

Note: The configurations **username** / **password** / **server** / **port** will change depend of the selected protocol.

4. Click **Save** to save the configuration.

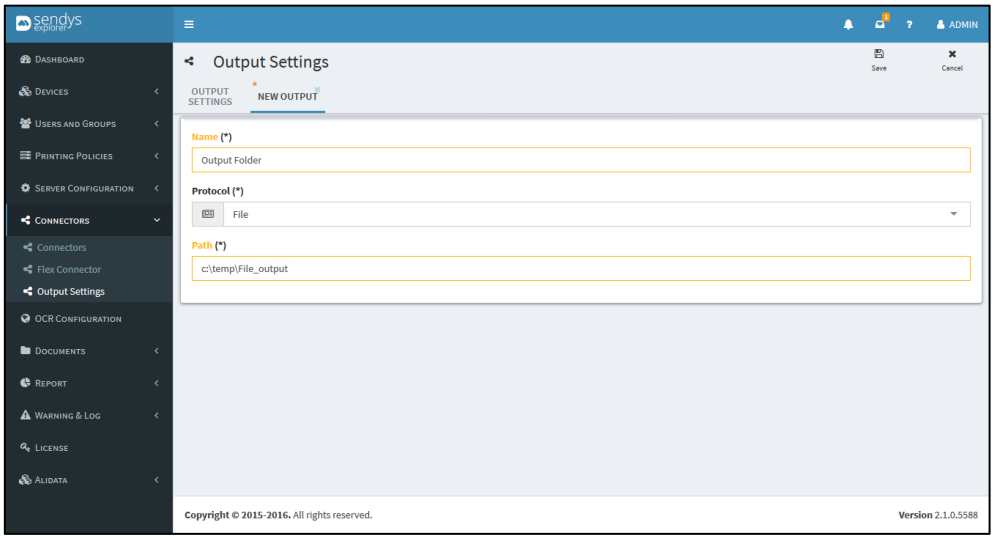


Fig. 315 - Add Output

EDIT OUTPUT SETTINGS

1. Click on **Connectors > Output Settings**.
2. Click on **pencil icon** to edit the **Output**.

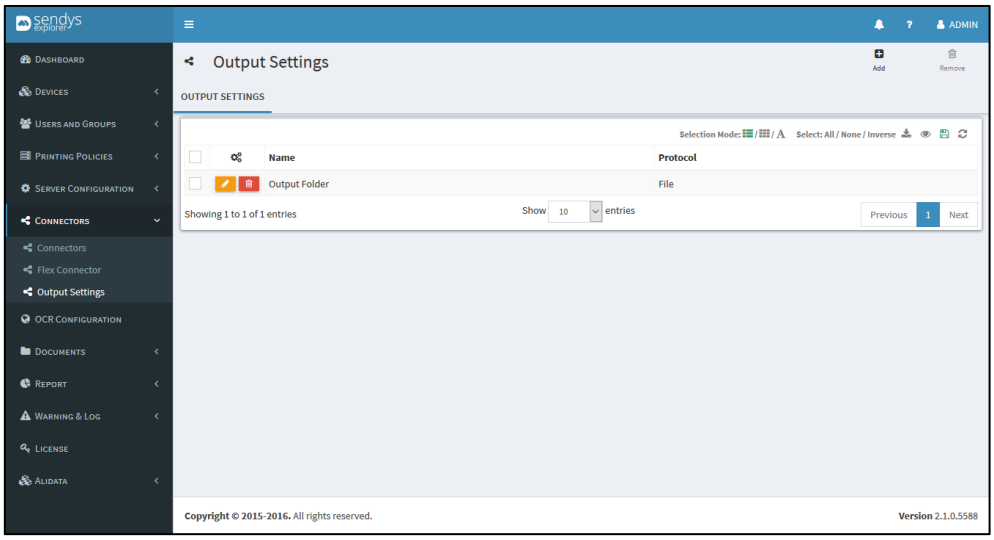


Fig. 316 - Edit Output

3. Make the changes on Output configuration.

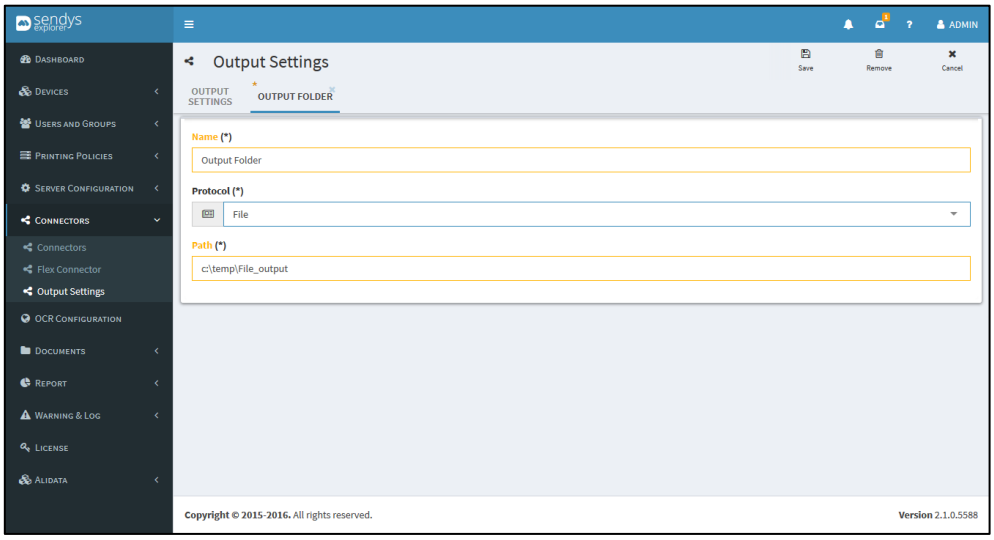


Fig. 317 - Edit Output

4. Click **Save** to save the Output changes.

REMOVE OUTPUT SETTINGS

1. Click on **Connectors > Output Settings**.
2. Click on **trash icon** to remove the **Output**.

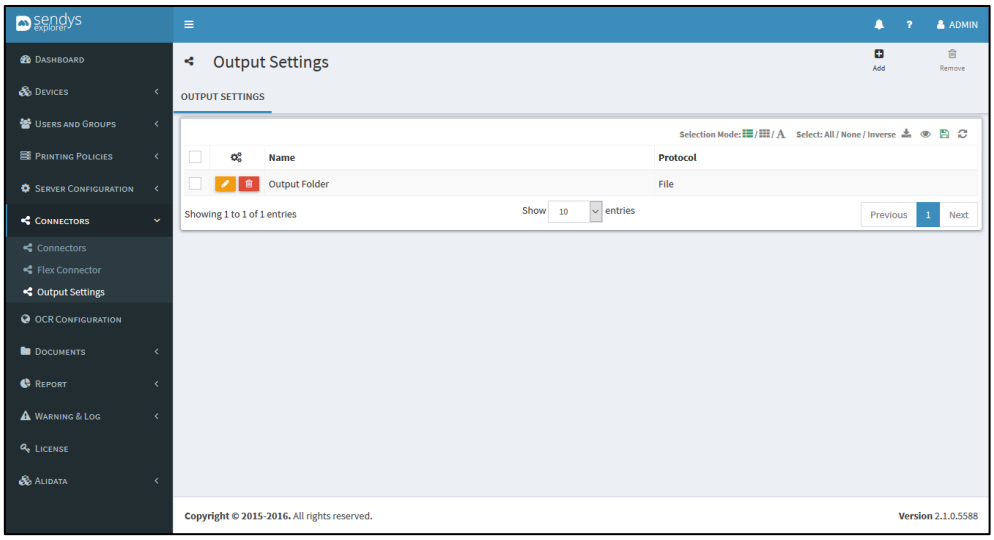


Fig. 318 - Remove Output

3. Click **Delete** to confirm removal.

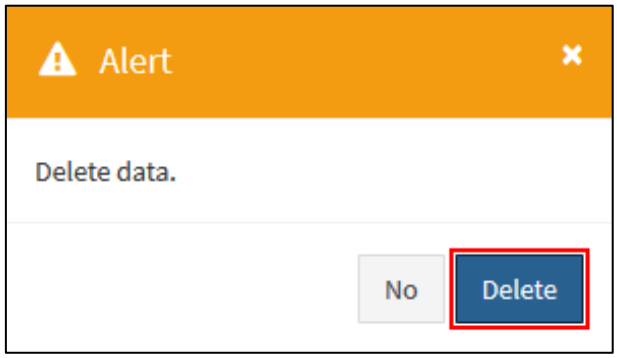


Fig. 319 - Confirm remove Output

ADD FLEX CONNECTOR

1. Click on **Connectors > Flex Connectors**.
2. Click on **Add**.

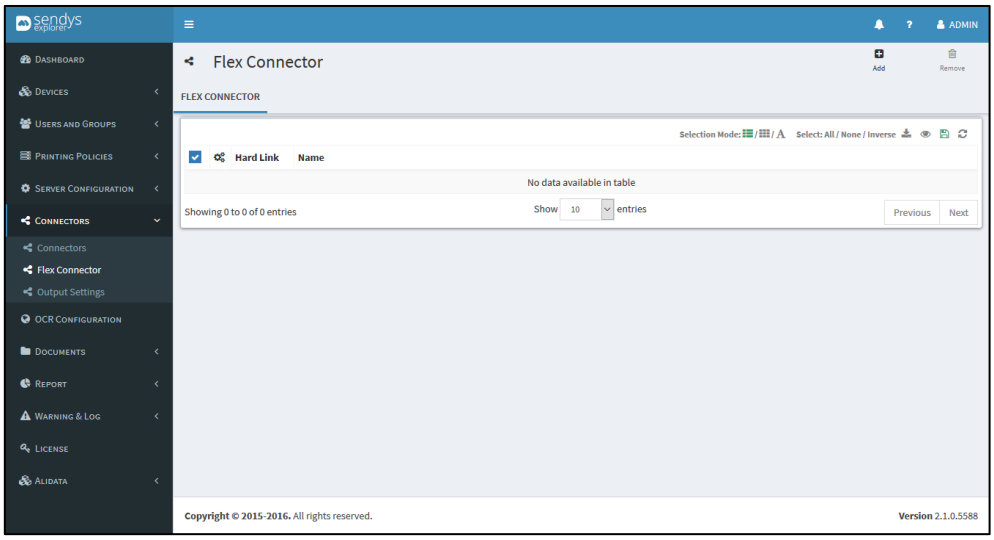


Fig. 320 - Flex Connectors

CONNECTOR SETTINGS

1. Click on **Connector Settings**.

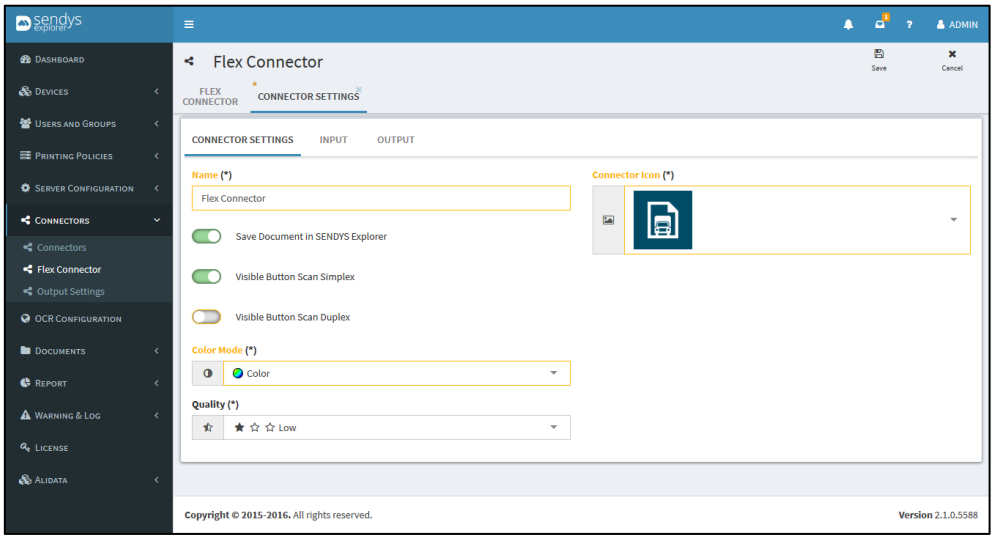


Fig. 321 - Flex Connectors

2. Make the required configuration

Name	Details
Name	Name for the Connector
Connector Icon	Select the icon for the Connector
Save Document in SENDYS Explorer	If checked, the scanned document will be saved on the Output and also integrated on SENDYS Explorer. IF not checked, the scanned document will only be saved on the Output
Visible Button Scan Simplex	Select to enable or not the Scan Button
Visible Button Scan Duplex	Select to enable or not the Scan Duplex Button
Color Mode	Select the Color option for Scan Document
Quality	Select the Quality option for Scan Document

Table 54 - Add Connector Details

3. Click **Input**.

INPUT

1. Click on **Input**.

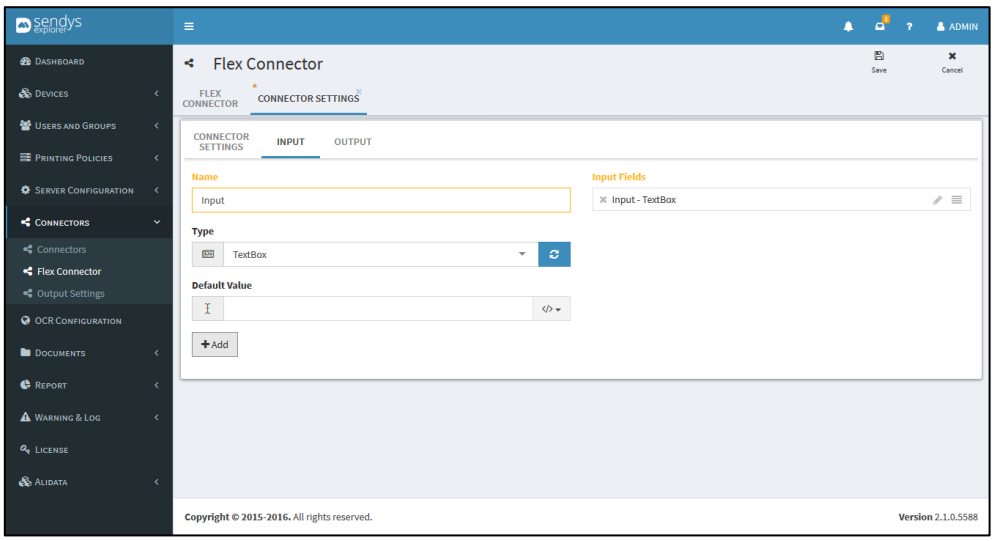


Fig. 322 - Flex Connectors

1. Make the required **Input** configuration.

Name	Details
Name	Name for the Input field. This name could be used on the output Filename.
Type	Select the type that you desire to use on the Input field
Default Value	If you desire you can enter the default value for the Input field

Table 55 - Add Input Details

2. Input **Type** configurations

Input Type	Details
Combo	This will create one combo box with the values enter on the "**Default Value**" field. This values need to be separated by coma. Example: "1,2,3,4"
CheckBox	This will create one checkbox. If you set the "**Default Value**" with 1, checkbox will be checked.
TextBox	This will create one textbox.
ODBC	This will create one combo box with the values returned from one query. For this to work it's need to configure one ODBC data source on the server. And then it's need to enter the Connection String for the ODBC and the desired Query for the results. This follow the ODBC creation rules.
Hidden	This will create one hidden field, it will not be editable or visible. Could be used to store values for the Output Filename. Or to integrate with other system.

Table 56 - Add Input Details

2. Click on **+ Add**. After you create all the Input's for the Connector, click on **Output**.

PROCESSING

Processing

OUTPUT

1. Click on **Output**.

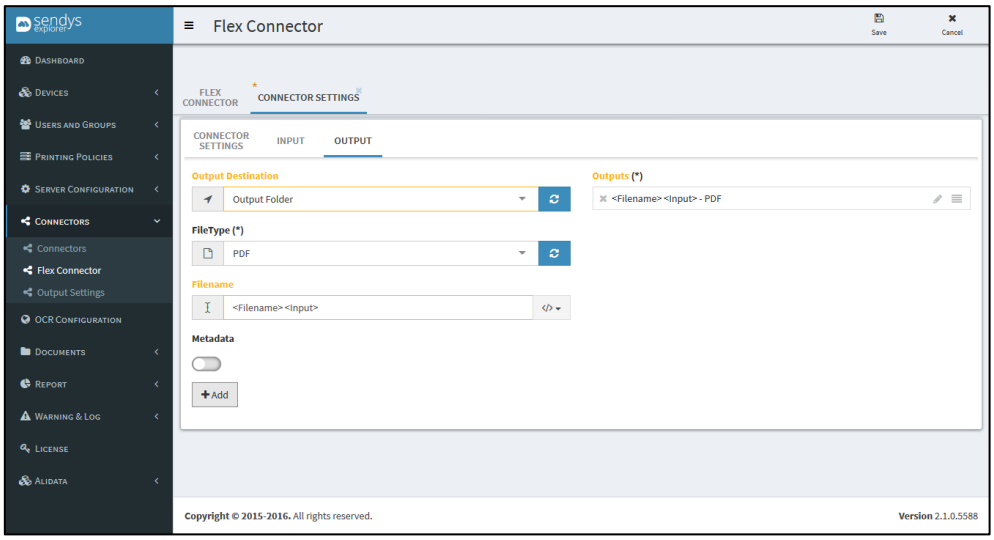


Fig. 323 - Flex Connectors

2. Make the required **Output** configuration.

Name	Details
Output Destination	Select one Output that was previous created
FileType	Select the format for the Scanned Document
Filename	Define the Name of the Scanned Document In the Filename you can use the Input's created previously, just need to enter the input name between "< >". Also you can enter the char "\" to use existing subfolders of the output location. Example for Filename: <Filename> **<input>** <Date> **\existing_folder**<Filename> **<input>** <Date>

Table 57 - Add Output Details

3. Click on **+ Add**. After you create all the Output's for the Connector, click on **Save**.
4. Flex Connector was created and it will forward to **Flex Connectors**. The new connector will be visible on your Smart MFP.

EDIT FLEX CONNECTOR

1. Click on **Connectors > Flex Connectors**.
2. Click on **pencil icon** to edit the **Flex Connector**.

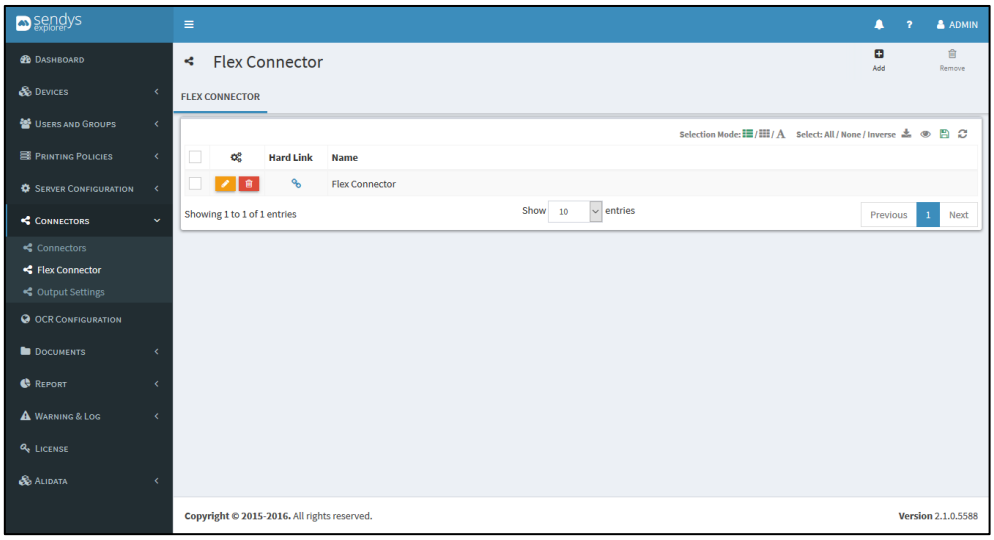


Fig. 324 - Flex Connectors

3. Make the changes on **Connector Settings / Input /Output** configurations.

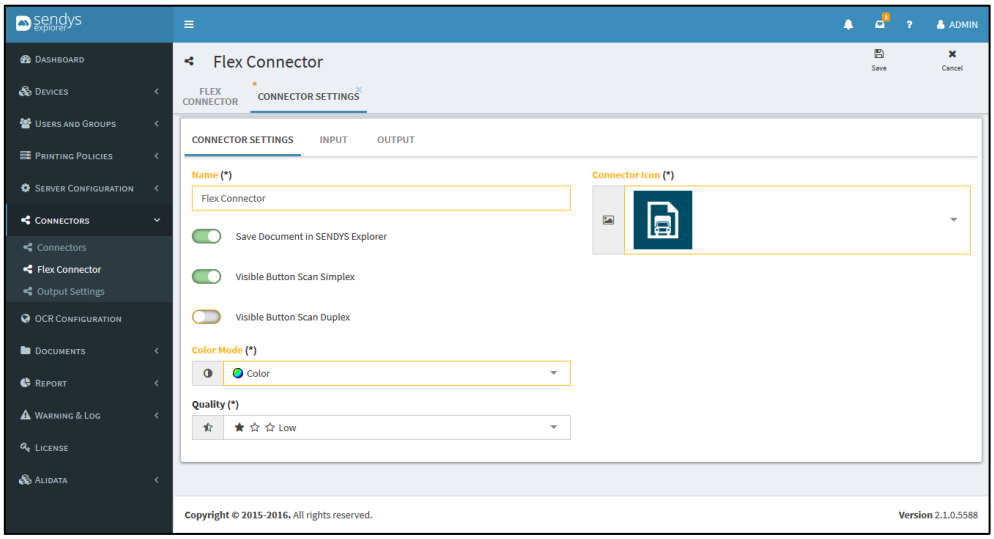


Fig. 325 - Edit Flex Connector

4. Click **Save** to save the configuration.

REMOVE FLEX CONNECTOR

1. Click on **Connectors > Flex Connectors**.
2. Click on **trash icon** to remove the **Flex Connector**.

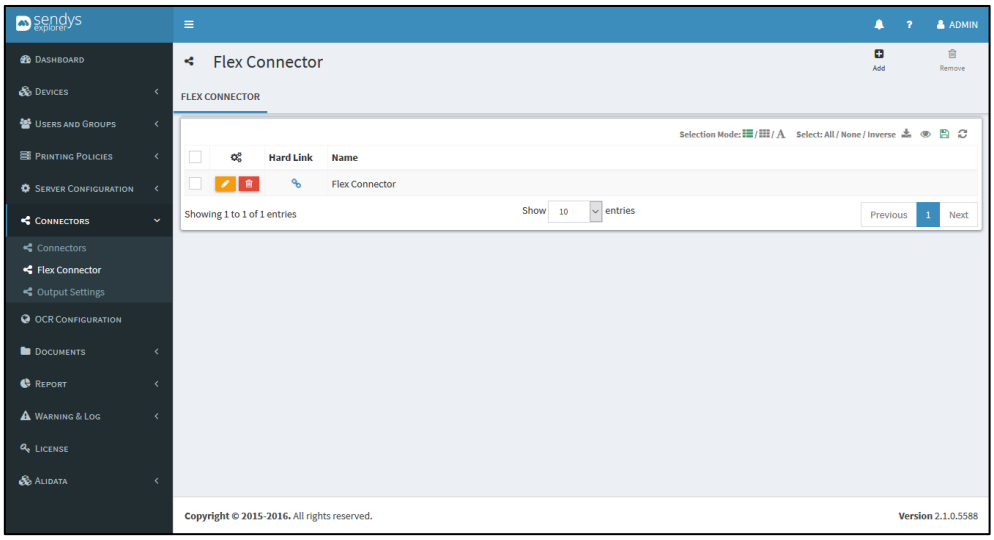


Fig. 326 - Flex Connectors

3. Click **Delete** to confirm removal.

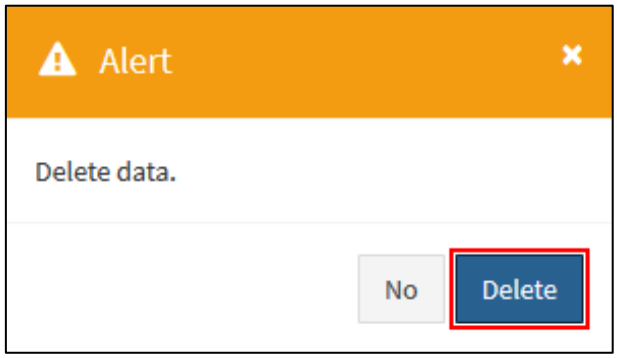


Fig. 327 - Confirm Remove Flex Connector

FLEX CONNECTOR PLUS

OVERVIEW

Flex Connectors will allow you to create new and customized Connectors. There you can set and define different workflows for the scan documents.

The **Flex Connectors** could be very useful for integration with customer software, since it allows to set several output destinations, and also to generate Metadata for the output documents.

With **Flex Connectors Plus** you have all functionalities from Flex Connector and additional to this you have a new range of possibilities:

- PDF Page Split
- OCR Template creation
- Zonal OCR
- Document Deskew
- Document noise removal
- White page removal
- Auto Page Rotation
- Regular expressions over input/OCR Zone Fields
- String Format over input/OCR Zone Fields
- String remove empty spaces and new lines over input/OCR Zone Fields

With all of this new setting it will be a lot easy to define standard workflows and make integration of documents into Document management systems or company ERP's.

Additional to all of this when you push flex connector plus you also push SQL Server database integration and advanced admin platform.

1. Click on **Connectors**.
2. Click on the **pencil icon** to edit/create **Flex Connectors**.
   Or optional:
3. Click on **Connectors**.
4. Click on **Flex Connectors**.

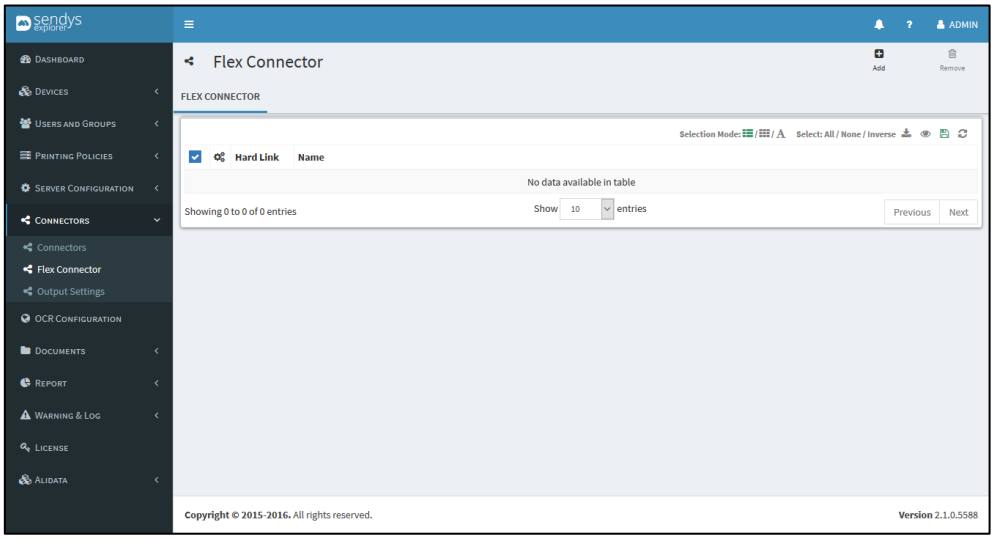


Fig. 328 - Flex Connectors

OCR TEMPLATES

OCR templates are documents that you can use to specify zones that can be capture from a document, this zones will be defined has output metadata variables that you can use to integrate the scanned documents.

To create a OCR Template document you need to follow the next steps:

5. Go to management application has administrator
6. Go to OCR Configurations
7. Change the name of any of the OCR ABBYY templates, make sure that you save this information.
8. Go to any of the connectors, could be “Scan to me” for example
9. Enable OCR Template on this connector
10. Go to the device
11. Click on “Scan to me”

12. Select has Output Format “OCR Template”

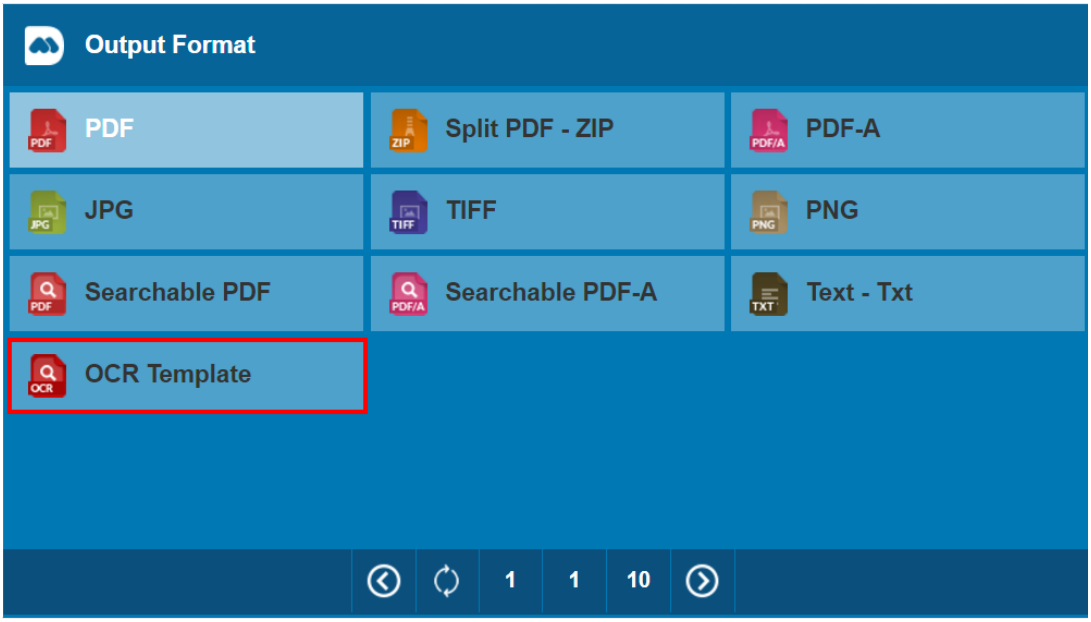


Fig. 329 – Create document template sample.

13. Give a name to the document
14. Scan the document
15. Go to Administration console
16. Click on Connectors> OCR Templates>Scanned Docs
17. Select the scanned document

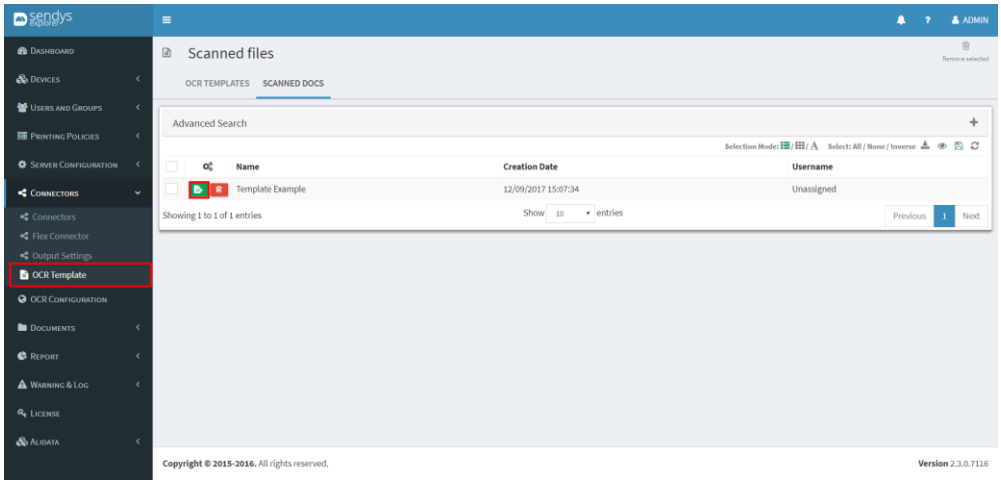


Fig. 330 – Select Document to Template.

18. Create the document Zonal OCR Template
19. Specify a name
20. Select a language
21. Add a page(s) template
22. Select the different areas and define the variables naming

23. Save the page(s) template
24. Save the full template

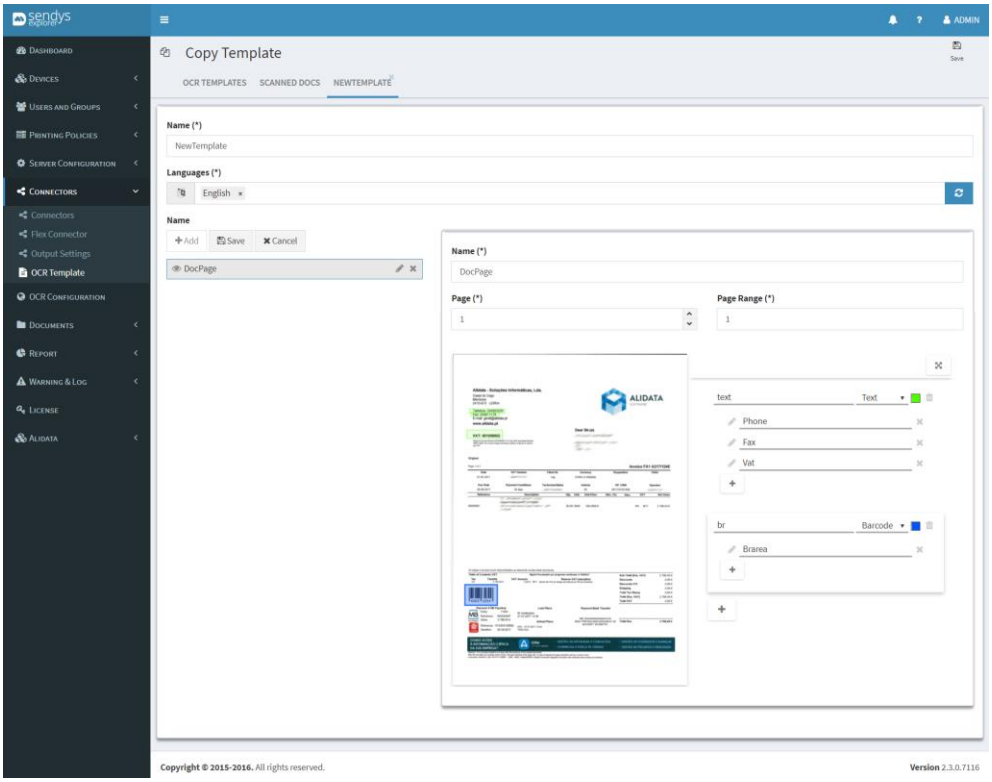


Fig. 331 – Zonal OCR Template.

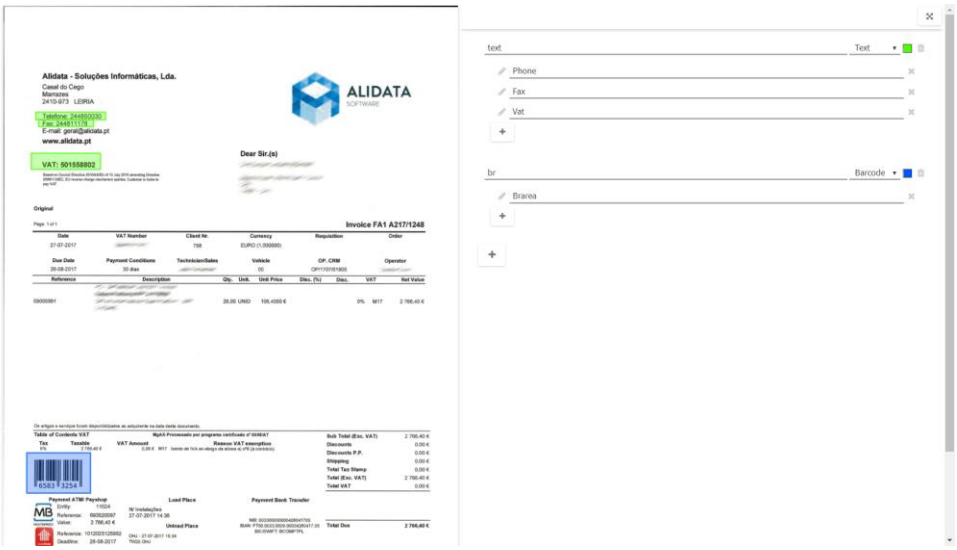


Fig. 332 – Template area definition.

25. After defining the full template for the document
26. Go to the Flex-Connector that you have defined

27. Select the connector for edition
28. Go to the tab “Processing”
29. Select the “OCR Template”

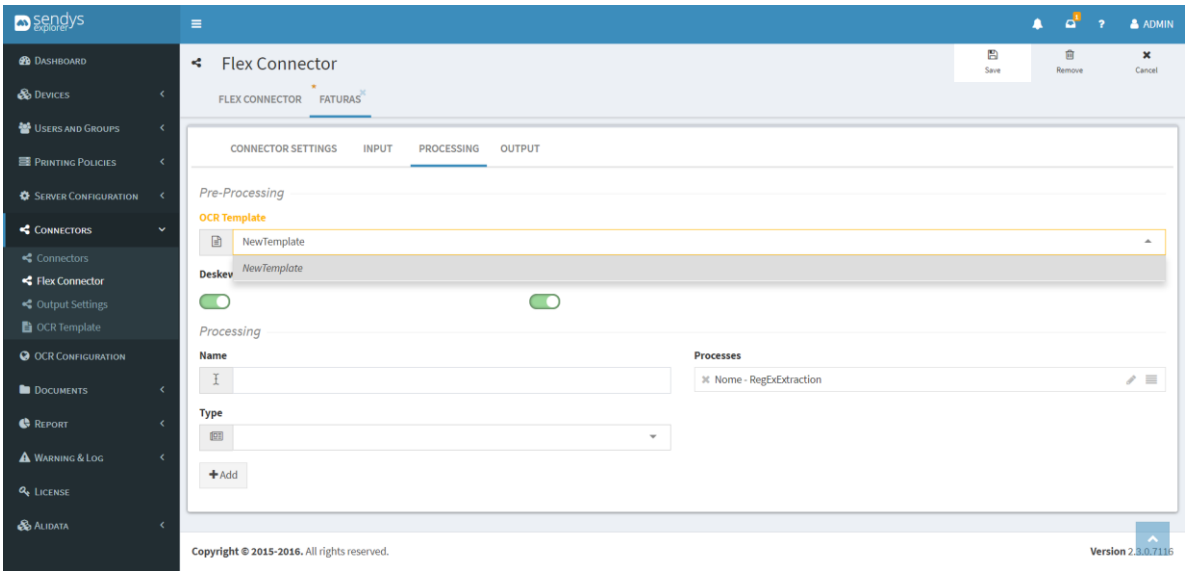


Fig. 333 - Flex Connectors plus processing.

OUTPUT SETTINGS

CREATE OUTPUT SETTINGS

5. Click on **Connectors > Output Settings**.
6. Click on **Add**.

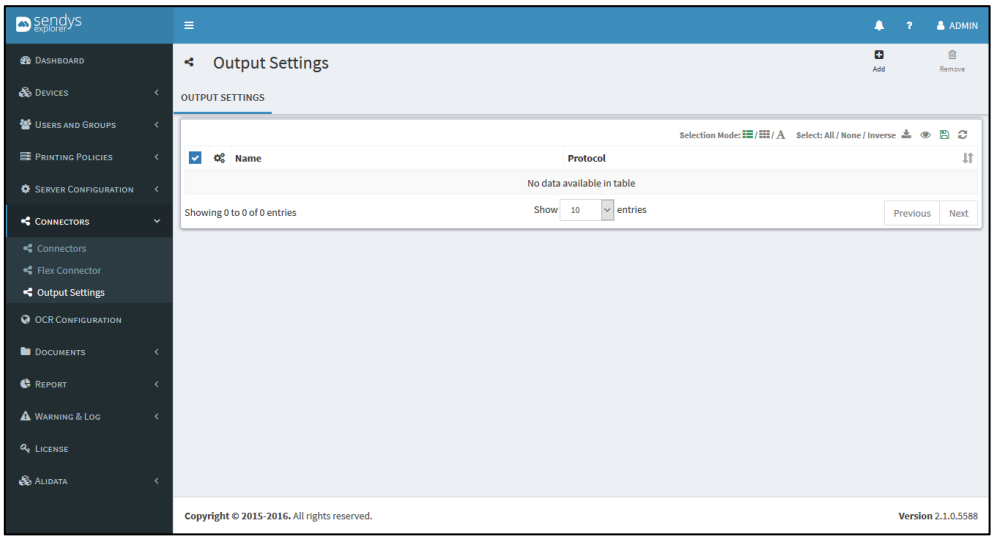


Fig. 334 - Add Output

7. Make the required configuration.

Name	Details
Name	Name to be presented on the Output
Protocol	Select the protocol used (**File** / **Samba** / **FTP**)
Path	Case you select File protocol insert the path for one exiting system folder E.g. C:/Temp Case you select **SMB** protocol insert the path for one exiting samba shared folder E. g. \\sambaserver\sharedfolder\ Case you select **FTP** protocol insert the path for one exiting FTP shared folder E. g. \sharedfolder\
Username	Username for **SMB** or **FTP** access
Password	Password for **SMB** or **FTP** access
Port	Port for **FTP** access
Server	IP for the **FTP** server

Table 58 - Add Output

Note: The configurations **username** / **password** / **server** / **port** will change depend of the selected protocol.

8. Click **Save** to save the configuration.

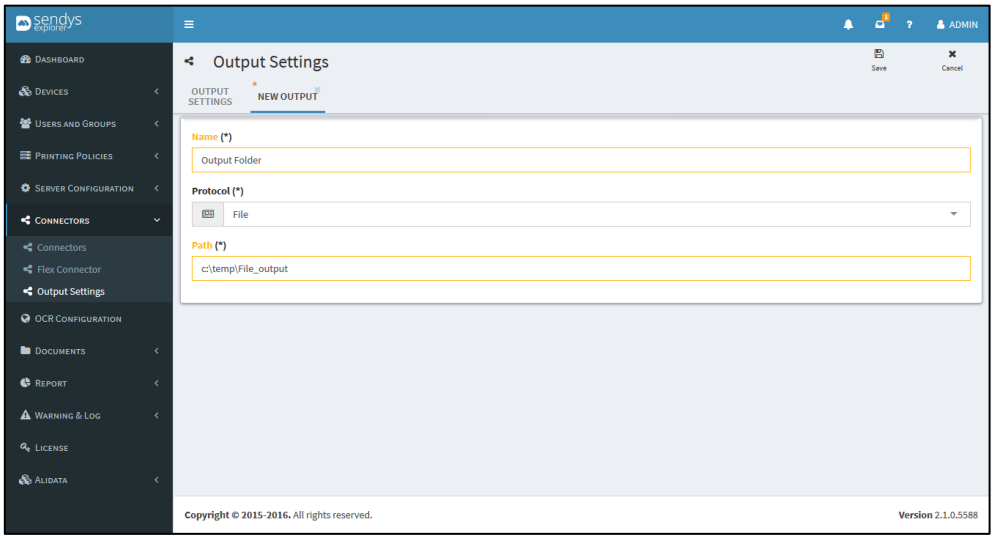


Fig. 335 - Add Output

EDIT OUTPUT SETTINGS

5. Click on **Connectors > Output Settings**.
6. Click on **pencil icon** to edit the **Output**.

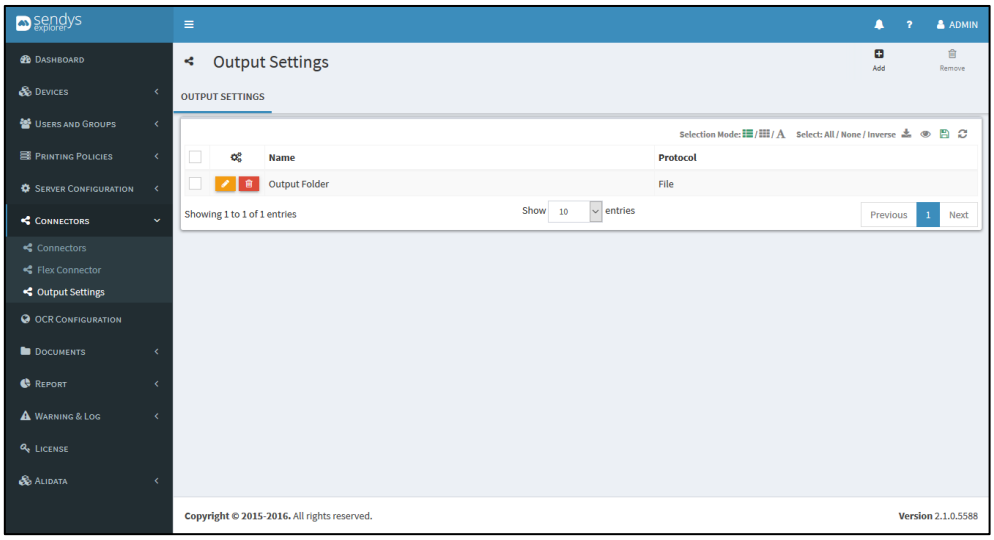


Fig. 336 - Edit Output

7. Make the changes on Output configuration.

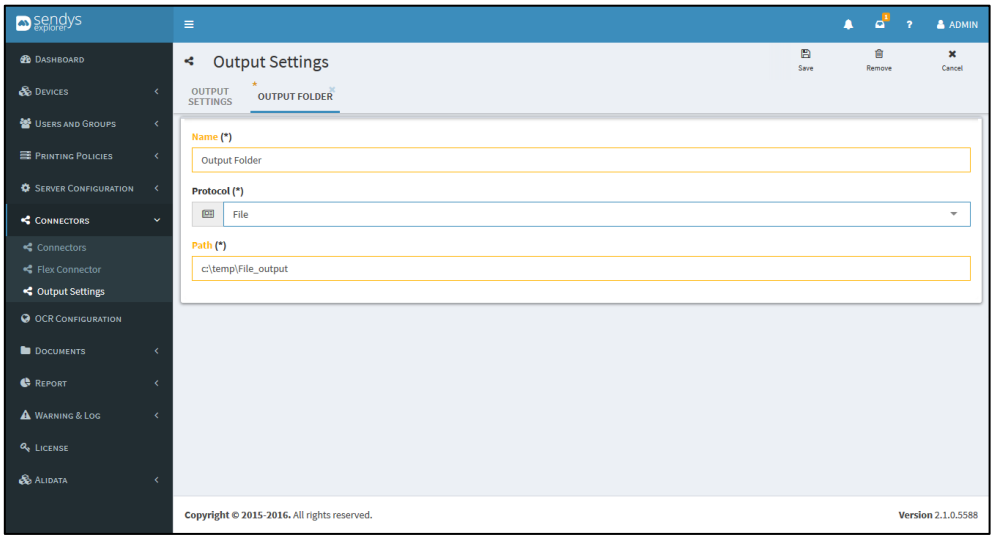


Fig. 337 - Edit Output

8. Click **Save** to save the Output changes.

REMOVE OUTPUT SETTINGS

4. Click on **Connectors > Output Settings**.
5. Click on **trash icon** to remove the **Output**.

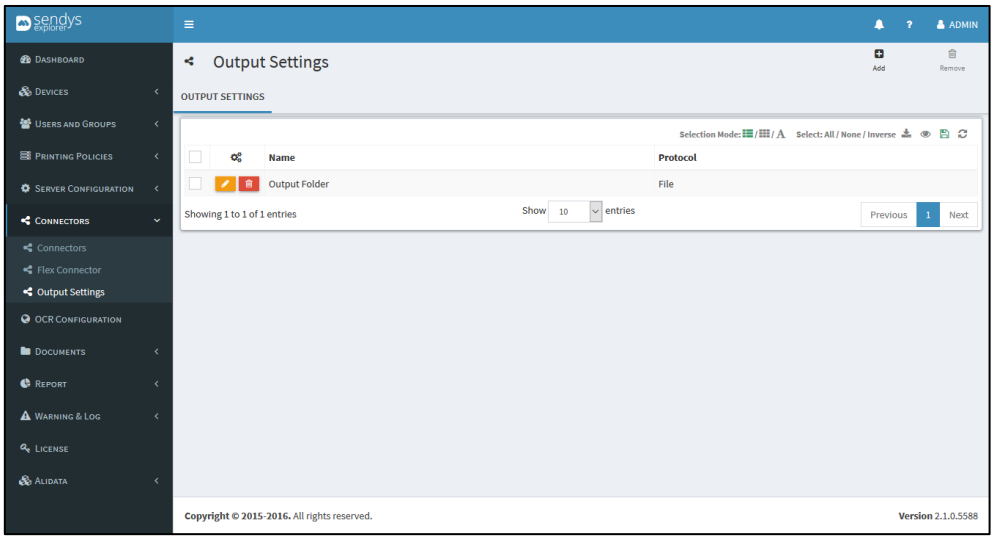


Fig. 338 - Remove Output

6. Click **Delete** to confirm removal.

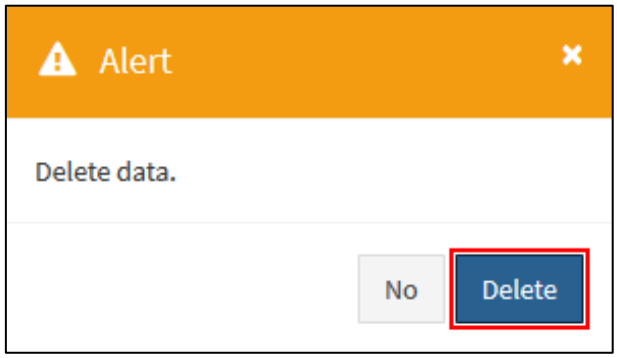


Fig. 339 - Confirm remove Output

ADD FLEX CONNECTOR

4. Click on **Connectors > Flex Connectors**.
5. Click on **Add**.

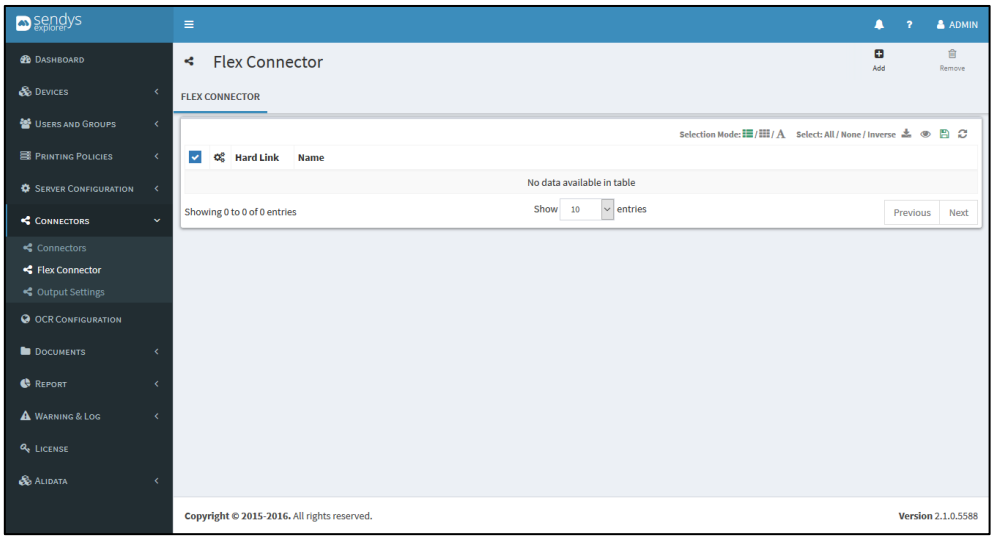


Fig. 340 - Flex Connectors

CONNECTOR SETTINGS

3. Click on **Connector Settings**.

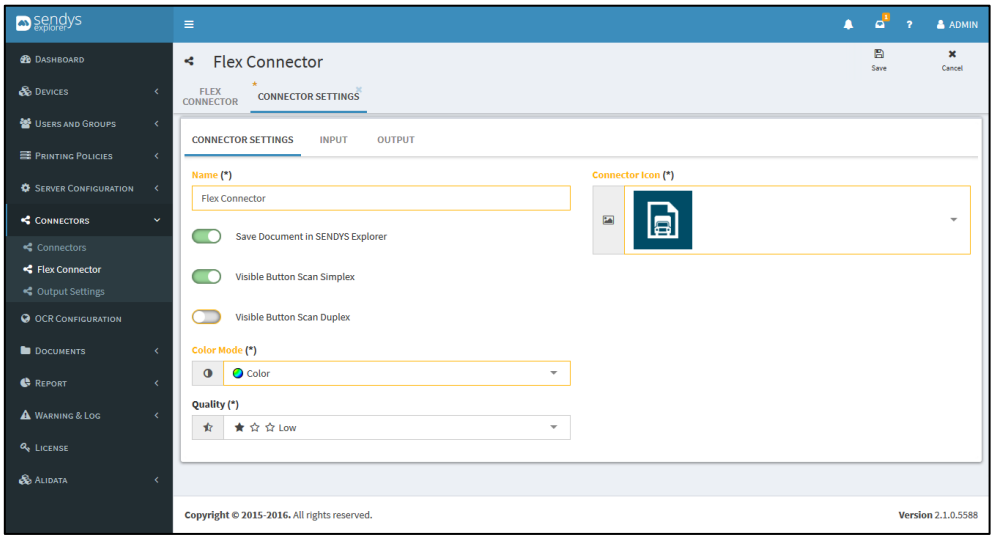


Fig. 341 - Flex Connectors

4. Make the required configuration

Name	Details
Name	Name for the Connector
Connector Icon	Select the icon for the Connector
Save Document in SENDYS Explorer	If checked, the scanned document will be saved on the Output and also integrated on SENDYS Explorer. IF not checked, the scanned document will only be saved on the Output
Visible Button Scan Simplex	Select to enable or not the Scan Button
Visible Button Scan Duplex	Select to enable or not the Scan Duplex Button
Color Mode	Select the Color option for Scan Document
Quality	Select the Quality option for Scan Document

Table 59 - Add Connector Details

6. Click **Input**.

INPUT

3. Click on **Input**.

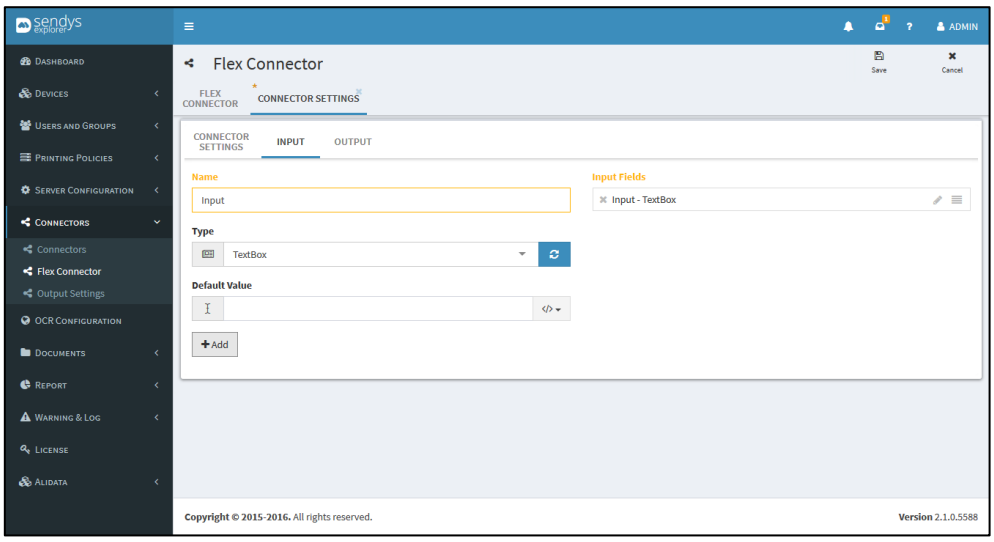


Fig. 342 - Flex Connectors

3. Make the required **Input** configuration.

Name	Details
Name	Name for the Input field. This name could be used on the output Filename.
Type	Select the type that you desire to use on the Input field
Default Value	If you desire you can enter the default value for the Input field

Table 60 - Add Input Details

4. Input **Type** configurations

Input Type	Details
Combo	This will create one combo box with the values enter on the "**Default Value**" field. This values need to be separated by coma. Example: "1,2,3,4"
CheckBox	This will create one checkbox. If you set the "**Default Value**" with 1, checkbox will be checked.
TextBox	This will create one textbox.
ODBC	This will create one combo box with the values returned from one query. For this to work it's need to configure one ODBC data source on the server. And then it's need to enter the Connection String for the ODBC and the desired Query for the results. This follow the ODBC creation rules.
Hidden	This will create one hidden field, it will not be editable or visible. Could be used to store values for the Output Filename. Or to integrate with other system.

Table 61 - Add Input Details

4. Click on **+ Add**. After you create all the Input's for the Connector, click on **Output**.

PROCESSING

1. Select the connector for edition
2. Go to the tab “Processing”
3. Select the “OCR Template”

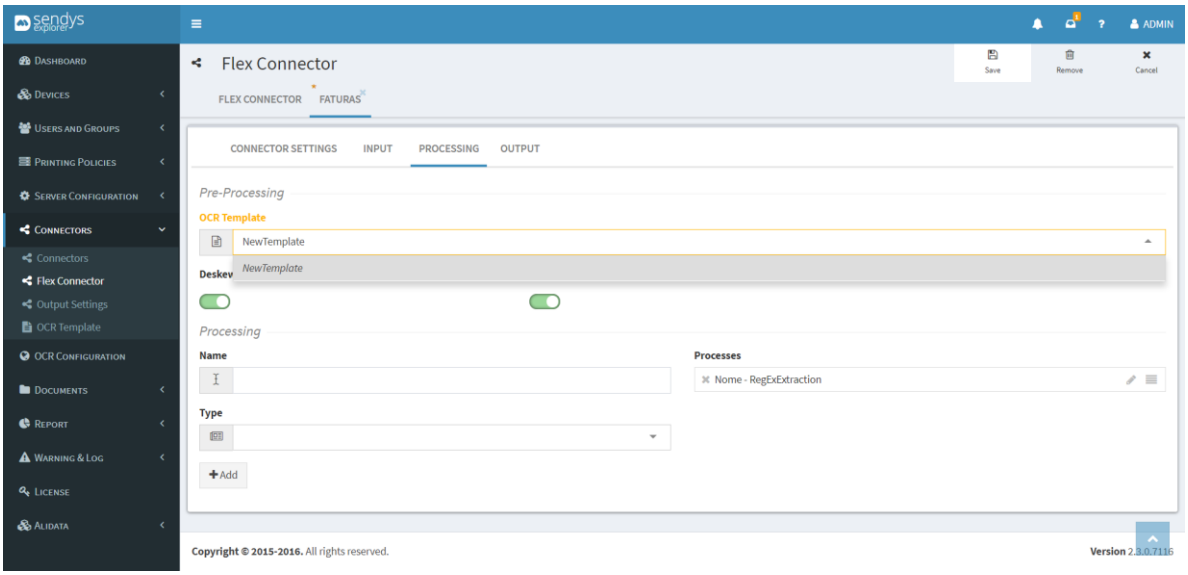


Fig. 343 - Flex Connectors plus processing.

4. Click “**Save**”

OUTPUT

5. Click on **Output**.

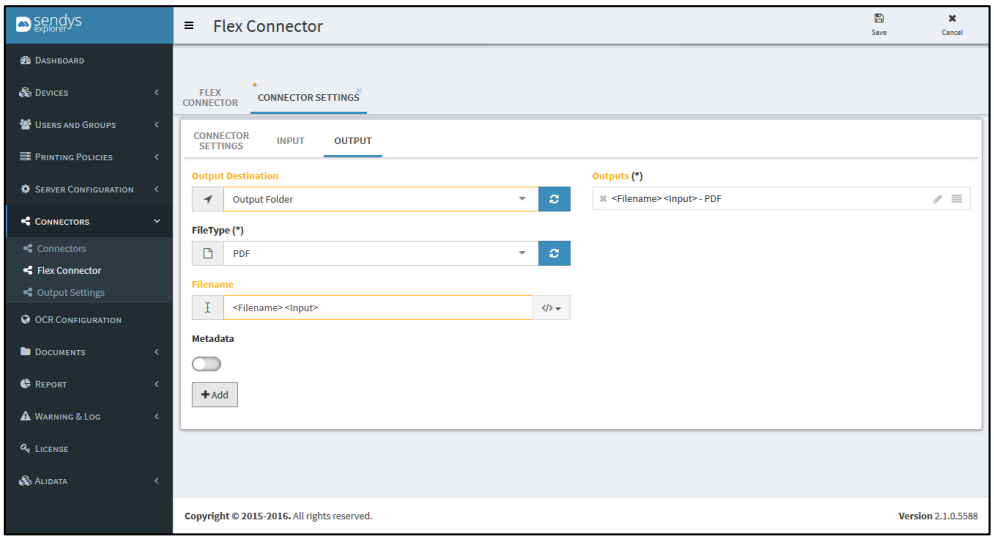


Fig. 344 - Flex Connectors

6. Make the required **Output** configuration.

Name	Details
Output Destination	Select one Output that was previous created
FileType	Select the format for the Scanned Document
Filename	Define the Name of the Scanned Document In the Filename you can use the Input's created previously, just need to enter the input name between "< >". Also you can enter the char "\" to use existing subfolders of the output location. Example for Filename: <Filename> **<input>** <Date> **\existing_folder**<Filename> **<input>** <Date>

Table 62 - Add Output Details

7. Click on **+ Add**. After you create all the Output's for the Connector, click on **Save**.
8. Flex Connector was created and it will forward to **Flex Connectors**. The new connector will be visible on your Smart MFP.

EDIT FLEX CONNECTOR

5. Click on **Connectors > Flex Connectors**.
6. Click on **pencil icon** to edit the **Flex Connector**.

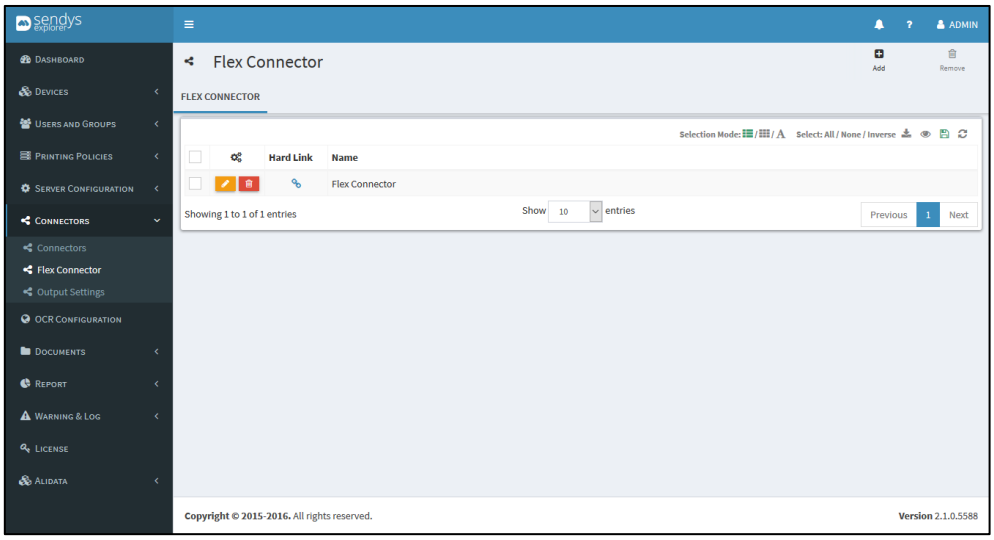


Fig. 345 - Flex Connectors

7. Make the changes on **Connector Settings / Input /Output** configurations.

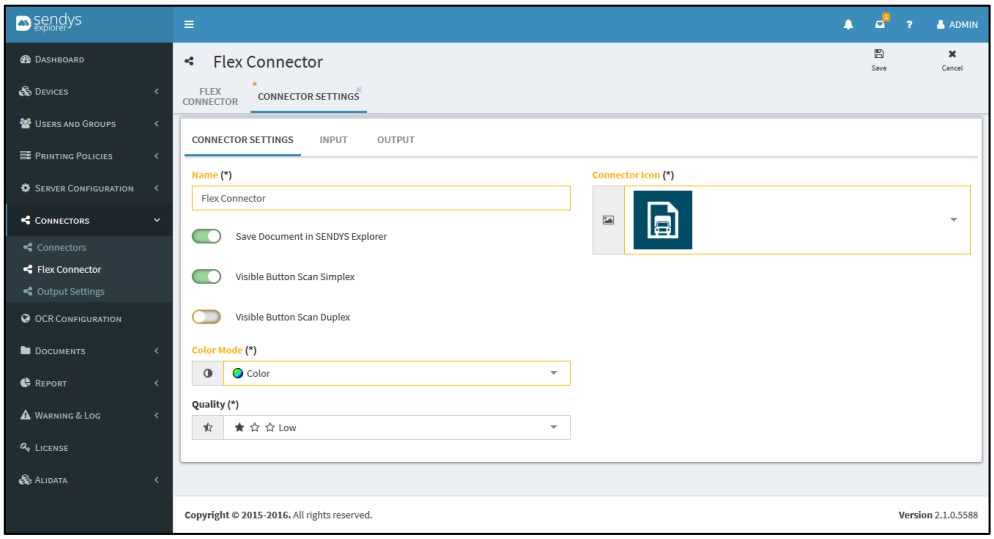


Fig. 346 - Edit Flex Connector

8. Click **Save** to save the configuration.

REMOVE FLEX CONNECTOR

4. Click on **Connectors > Flex Connectors**.
5. Click on **trash icon** to remove the **Flex Connector**.

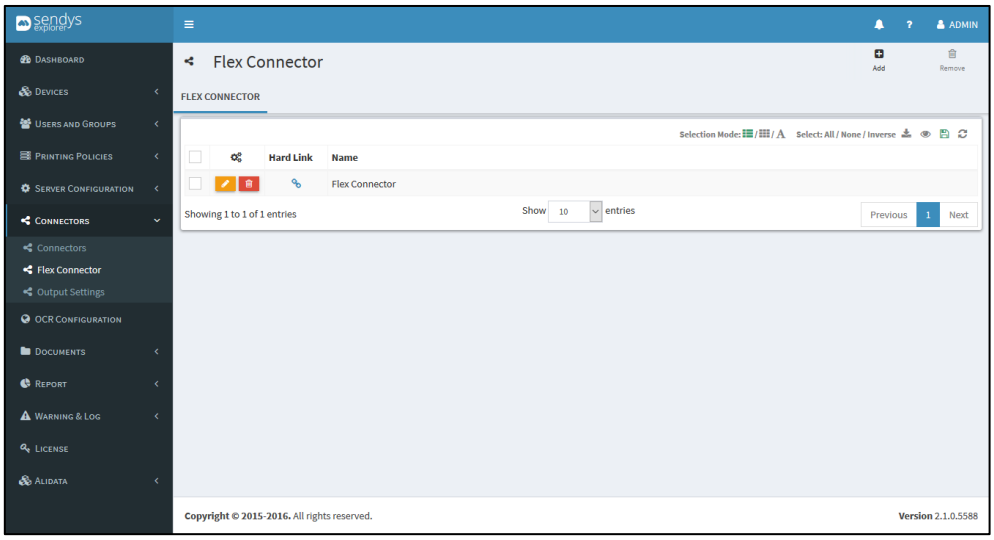


Fig. 347 - Flex Connectors

6. Click **Delete** to confirm removal.

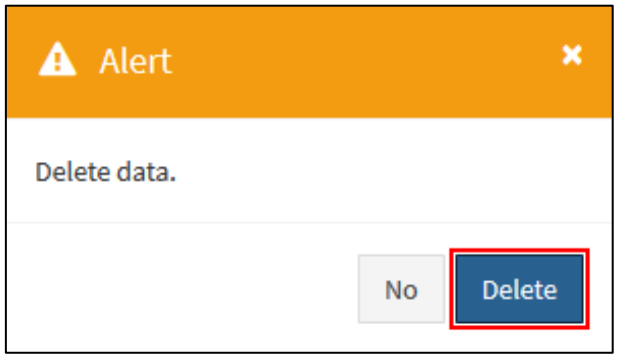


Fig. 348 - Confirm Remove Flex Connector

FLEET MANAGER CONNECTOR

This connector provides a way for you to control and manage devices and offers usage statistics and device

alerts on a personalised dashboard for easier maintenance and increased cost-effectiveness.

OVERVIEW

MONITOR and MANAGE YOUR DEVICES IN REAL TIME

SENDYS Explorer's Fleet Manager tool allows you to remotely view the real-time status of all your printers and MFPs. The hardware fleet overview offers usage statistics, as well as device alerts on a personalised dashboard in the event of jams or power issues.

Device alerts in real-time and error logs enable easier maintenance, improving efficiency, as well as increased cost-effectiveness through faster, more efficient consumables management, ensuring you're never without toner when you need it.

MAIN ADVANTAGES

- Device accounting - A reporting tool that quickly displays print volumes for one or several devices at a time. Create graphs and print results right from the application, or export data in a variety of formats.
- Job accounting - Provides management Information detailing printer use on a departmental or individual basis, so you can enjoy the time and money saved by automating and streamlining business processes.
- Device Management – Offers an overview of your hardware fleet including a device/alerts dashboard with real-time error logs (paper alert, power-off). Automatic email notifications, remote device configuration and supplies dashboard allows you to quickly see what your print fleet is doing.
- Device discovery - Scan your network so you can quickly install and configure your new added devices.
- Firmware updates - Manage the firmware on your devices remotely, allowing you to upgrade at a time that suits you, for example, overnight or over the weekend.
- Alerts & Consumables management - Receive alerts, and proactively manage your consumables to minimise downtime and improve productivity.

OCR CONFIGURATIONS

TESSERACT

Google Tesseract is possibly the most accurate open source OCR engine available. Combined with the **Leptonica Image Processing Library** it can read a wide variety of image formats and convert them to text in over 60 languages. It was one of the top 3 engines in the 1995 UNLV Accuracy test. Between 1995 and 2006 it had little work done on it, but since then it has been improved extensively by Google.

INSTALLING LANGUAGES

To install a new language in the OCR engine there are two options:

ONLINE

1. Go to http://serverIP:50091/controlserver/default.aspx.
2. Click on **Server Configuration > Application Settings**.
3. Click on **List > Application Config**.
4. Click on **Scan**.
5. Select the **Tesseract OCR Language**.
   Note: When you change the language SENDYS Explorer will try to download and install the new language

OFFLINE

For offline mode go to https://github.com/tesseract-ocr/tessdata

1. Download the language pack.
2. Extract the language pack.
3. Copy the files to **Program Files** or **Program Files (X86) \Alidata\Tesseract-OCR\tessdata**.
4. Go to http://serverIP:50091/controlserver/default.aspx.
5. Click on **Server Configuration > Application Settings**.
6. Click on **List > Application Config**.
7. Click on **Scan**.
8. Select the **Tesseract OCR Language**.

ABBYY RECOGNITION SERVER (SENDYS EXPLORER PREMIUM)

SENDYS Explorer will silently install ABBYY when a valid SENDYS Explorer PREMIUM license is activated, but you will still need to manually insert the ABBYY license and import/create the ABBYY workflows.

A sample workflow file that you can import to ABBYY is provided in the installation files. These workflows are already preconfigured in SENDYS Explorer.

ABBYY INSTALL

When you insert a SENDYS Explorer PREMIUM license, the system will try to install ABBYY recognition server. If this action fails it will try to guide the user through the installation process.

ABBYY CONFIGURATION

ABBYY LICENSE ACTIVATION

To insert an ABBYY license and activate the product go through the following steps:

1. In your Start Menu find and click on ABBYY's **Remote Administration Console**.
2. Click on **License**.
3. Click on **Add Key Icon**.
4. Select the **Activation method**
5. Click **Next**.

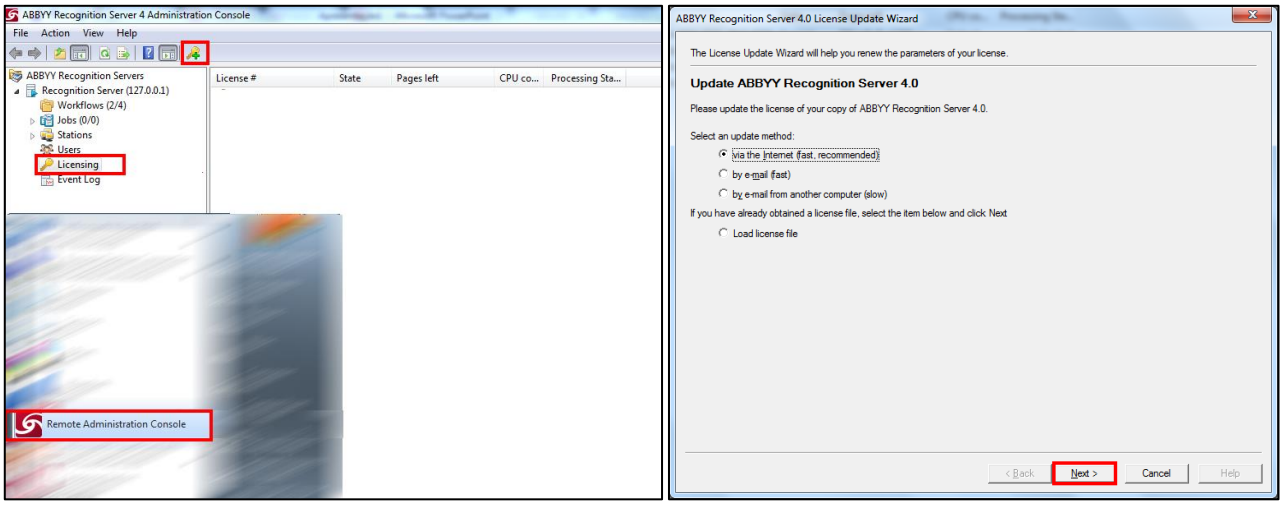


Fig. 349 – ABBYY

ABBYY IMPORTING WORKFLOWS

1. Open ABBYY's **Remote Administration Console**.
2. Click on **Workflow**.
3. Right-click on the Workflow's window.
4. Click on **Load Workflows Settings**…

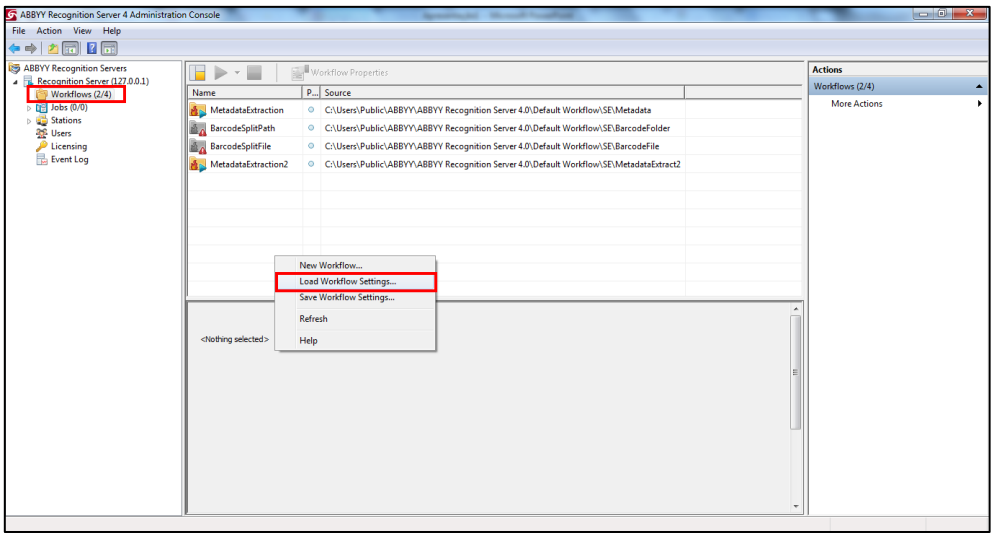


Fig. 350 - ABBYY

5. Select the file with the connectors to import.
   Note: A sample file is provided in **C:\inetpub\ftproot\SENDYSExplorer\Abbyy\SESampleWorkflows.xml**.
6. Click **Import**.

SENDYS EXPLORER PREMIUM AND ADDITIONAL ABBYY WORKFLOW IMPORT

You can Remove/Edit existing ABBYY workflows or Import new ones.

OCR configuration (new ABBYY Workflows):

1. On ABBYY Remote Console:
   a. Create a new ABBYY workflow
      - Workflow name (any)
      - Input folder (any)
      - File format (any)
      - Output folder (**C:\inetpub\ftproot\SENDYSExplorer\ScannedFiles**)
   b. Export new ABBYY workflow (file)
2. On SENDYS Explorer:
   a. **OCR Configuration >Import (file)** and provide the name to be displayed to SENDYS Explorer users.

IMPORT WORKFLOW

1. Click on **OCR Configuration**.
2. Click on **Import**.
3. Select the **ABBYY configuration file**.

Note: This action will create all workflows that contain **SENDYS Explorer Scanned Files Folder** as **Output Folder** on **SENDYS Explorer**.

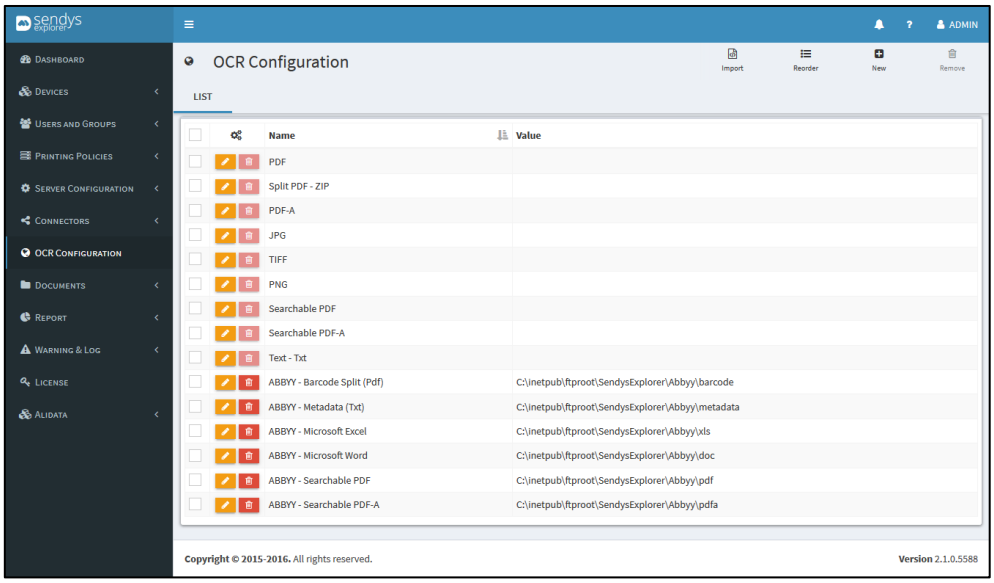


Fig. 351 - Import ABBYY Workflow

ADD WORKFLOW

1. Click on **OCR Configuration**.
2. Click on **New**.

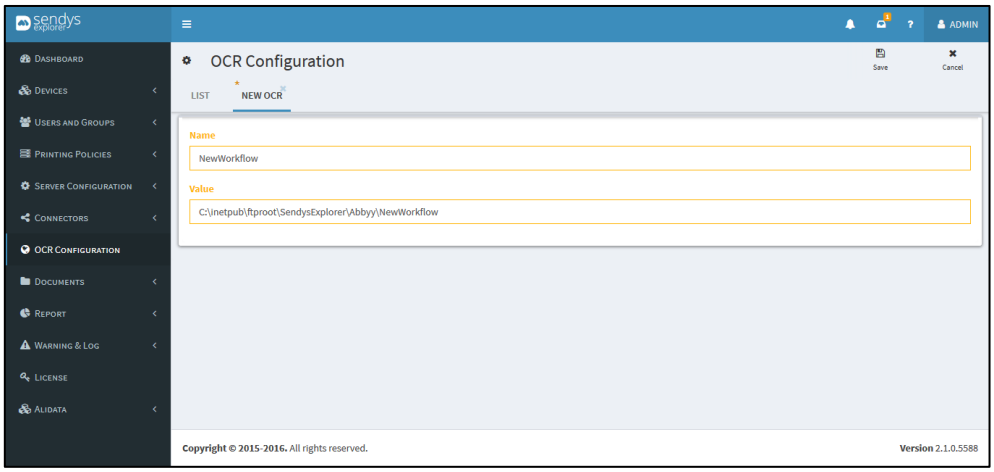


Fig. 352 - Add Workflow

3. Make the required configuration

Name	Details
Name	Name for the ABBYY workflow
Value	Input folder for ABBYY

Table 63 - Workflow Details

4. Click on **Save** to add the workflow.

EDIT WORKFLOW

1. Click on **OCR Configuration**.
2. Click on **pencil icon** to edit the **Workflow**.

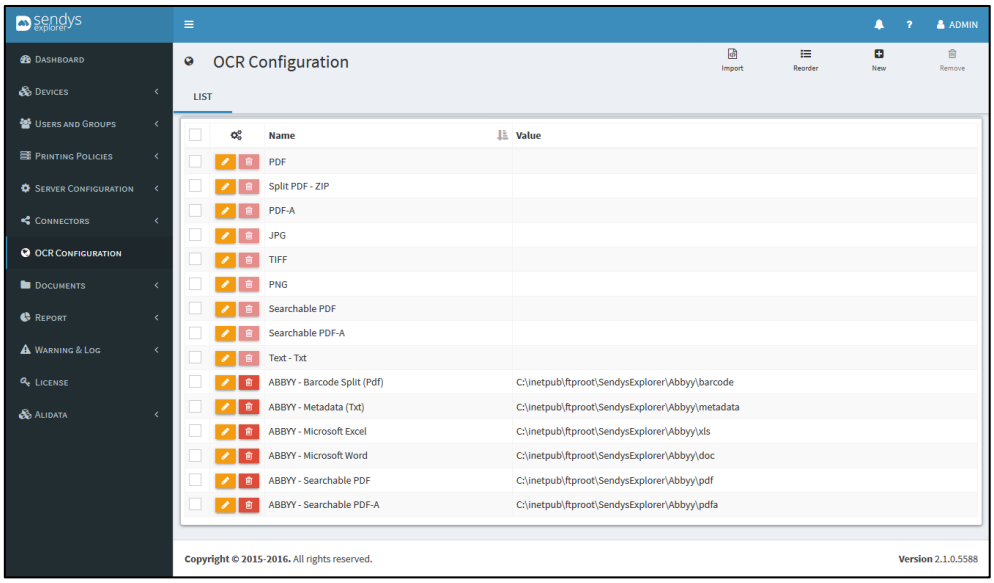


Fig. 353 - Edit Workflow

3. Make the changes on **Workflow**.

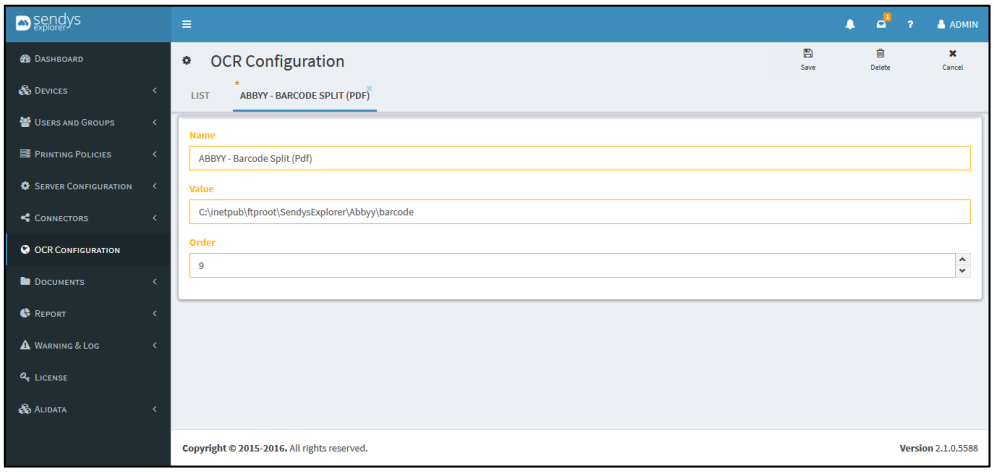


Fig. 354 - Edit Workflow

4. Click **Save** to save the configuration.

REMOVE WORKFLOW

1. Click on **OCR Configuration**.
2. Click on **trash icon** to remove the **Workflow**.

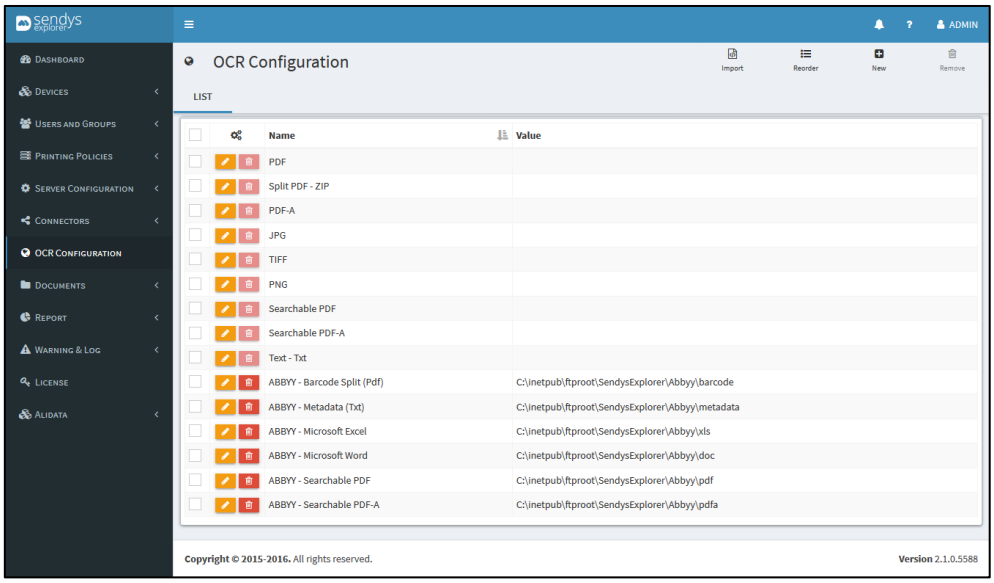


Fig. 355 - Remove Workflow

3. Click **Delete** to confirm removal.

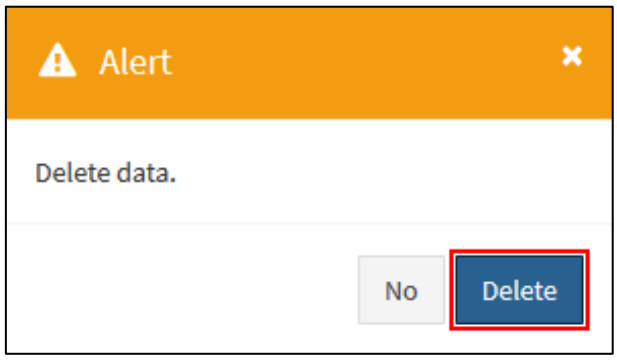


Fig. 356 - Remove Workflow

DOCUMENTS

This section is used to made a quick search on the printing and scanning jobs that were processed by SENDYS Explorer.

SPOOLER JOB

Spooler documents are the documents printed to pull prim queue, and that will be stay on hold until they are released by user. When the user enters on the printer he can consult the Spooler documents

This view shows the actual printing jobs on the Spooler of the system.

1. Click on **Documents**.
2. Click on **Spooler Job**.

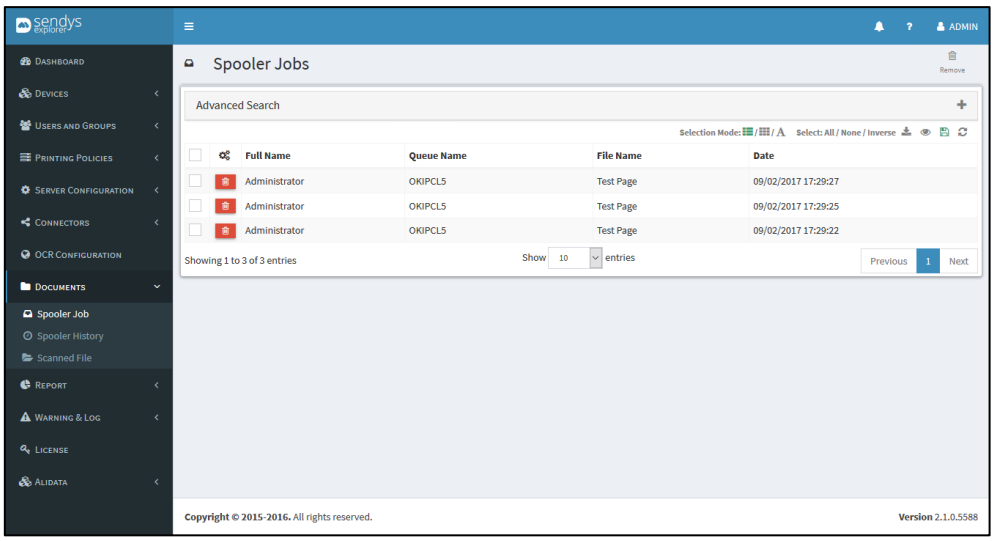


Fig. 357 - Spooler Job

3. Click on **trash icon** to remove the spooler job pretended.
   Select one or more Jobs to delete them by click the **Remove**.
4. Click **Delete** to confirm removal.

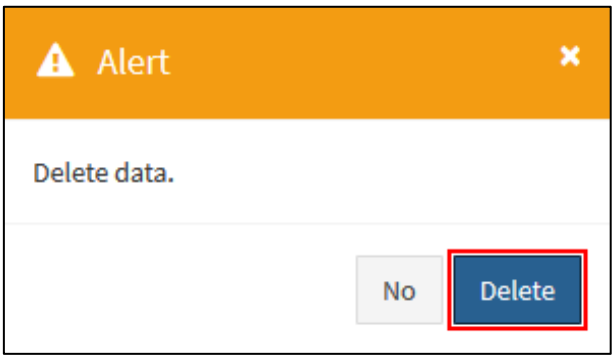


Fig. 358 - Confirm Remove Spooler Job

SPOOLER HISTORY

History documents are the documents printer. They still be accessible by the user, until the Clean Spooler Job deletes them.

This view shows the history documents of the system.

1. Click on **Documents**.
2. Click on **Spooler History**.

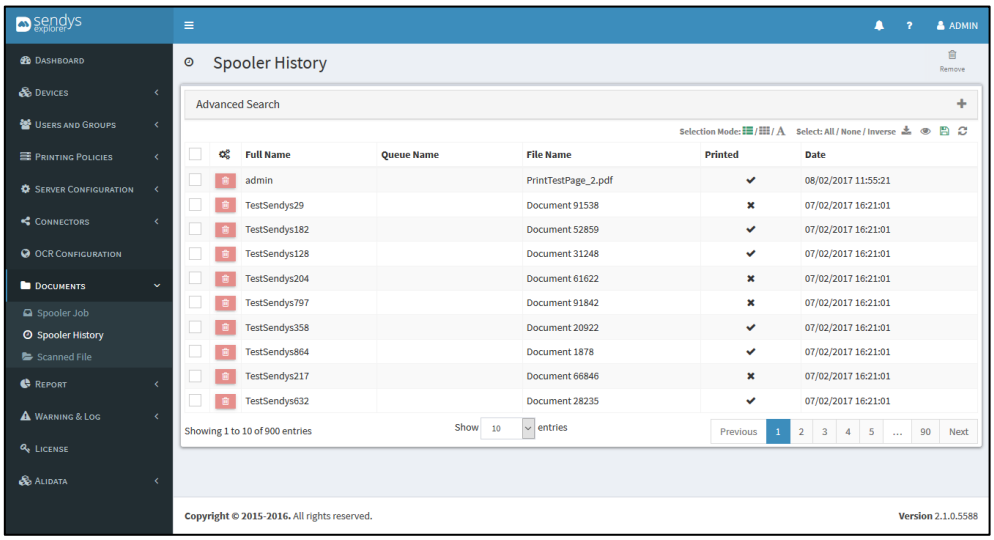


Fig. 359 - Spooler History

3. Click on **trash icon** to remove the spooler history pretended.
   Select one or more Jobs to delete them by click the **Remove**.
4. Click **Delete** to confirm removal.

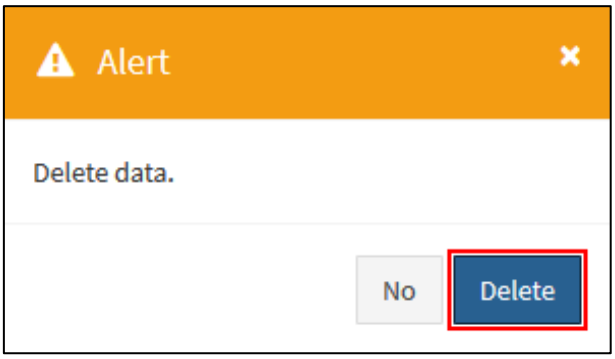


Fig. 360 - Confirm Remove Spooler History

SCANNED FILES

This view shows the list of scanned jobs processed on the system.

1. Click on **Documents**.
2. Click on **Scanned Files**.

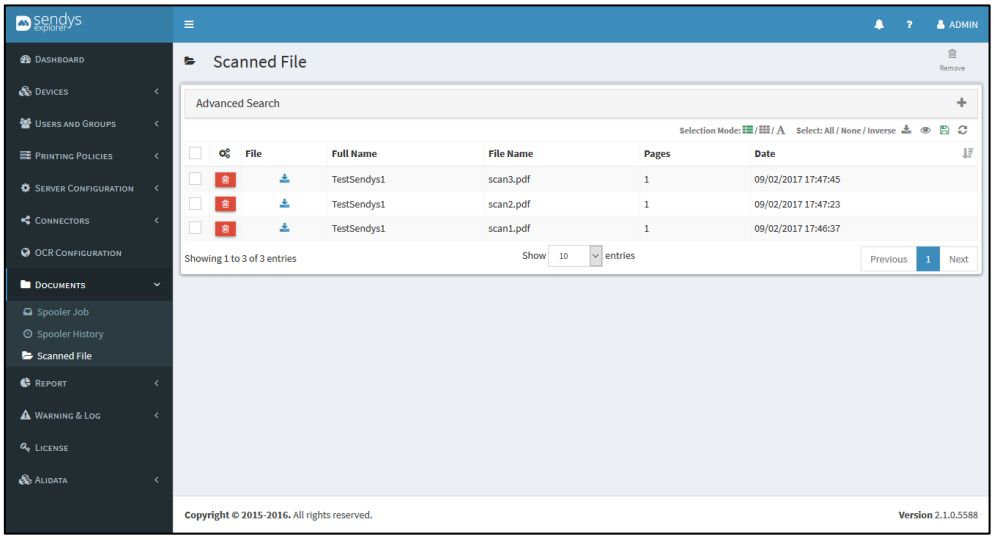


Fig. 361 - Scanned Files

3. Click on **download icon** to download the scanned file.
4. Click on **trash icon** to remove the spooler history pretended.
   Select one or more Jobs to delete them by click the **Remove**.
5. Click **Delete** to confirm removal.

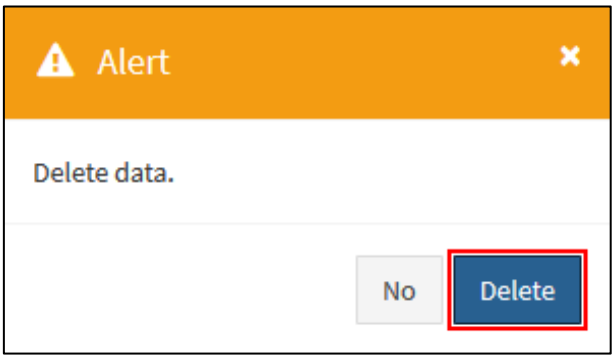


Fig. 362 - Confirm Remove Scanned Files

DLP DOCUMENTS

Data leak prevention was created to help customers to be more compliant with GDPR regulation. On this section of the application we can make configuration about company internal policies and with this definition help the company track the process and track the paper documents.

When did GDPR come into effect?

The GDPR was approved and adopted by the EU Parliament in April 2016. The regulation took effect after a two-year transition period and, unlike a Directive, did not require any legislation to be passed by government. GDPR came into force on 25th May 2018.

Who does the GDPR affect?

The GDPR not only applies to organizations located within the EU but also applies to organizations located outside of the EU if they offer goods or services to, or monitor the behaviour of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

What constitutes personal data?

The GDPR applies to 'personal data', meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organizations collect information about people.

What are the penalties for non-compliance?

Organizations can be fined up to 4% of annual global turnover for breaching GDPR or €20 Million.

What will happen to companies that have missed the deadline?

If the GDPR deadline has been missed, it is imperative the business in question acts urgently to become compliant. Demonstrating strong data rights management is important to both customers and employees; they should understand why the data is collected and how it is handled on a legal basis. Current business data processes need to be looked at as an immediate priority so that the company doesn't risk non-compliance penalties.

This section is responsible for document inspection and for the user to handle the documents when notify, with this the company as evidence of the document handling from the person that should be responsible for that specific action.

That person can be the user that has copy/print the document or the company Data protection officer, responsible for company GDPR compliance.

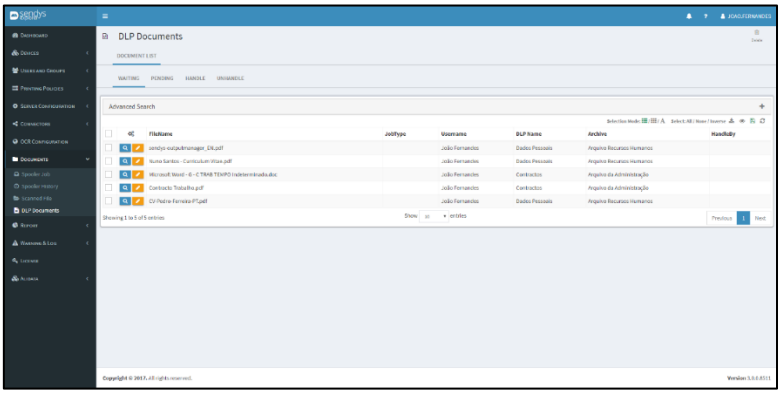


Fig. 363 - DLP Document View.

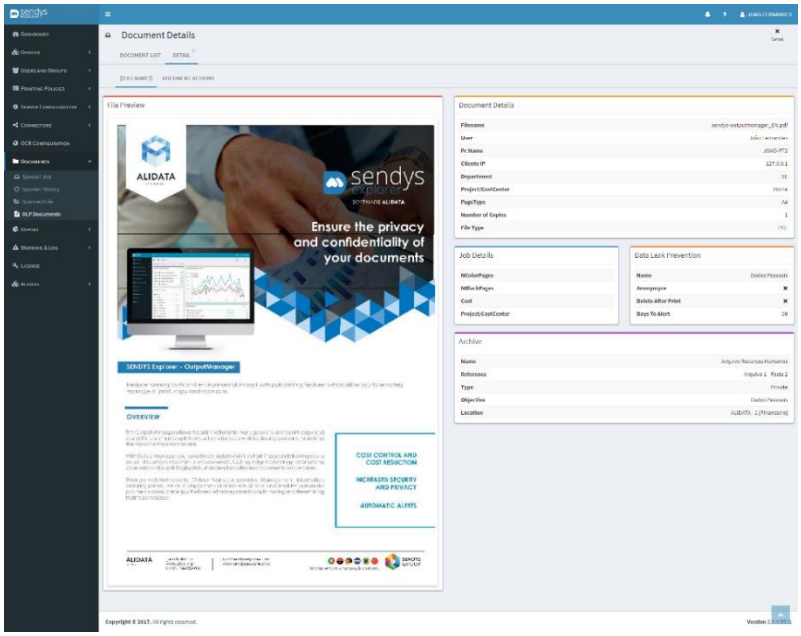


Fig. 364 - DLP Document View.

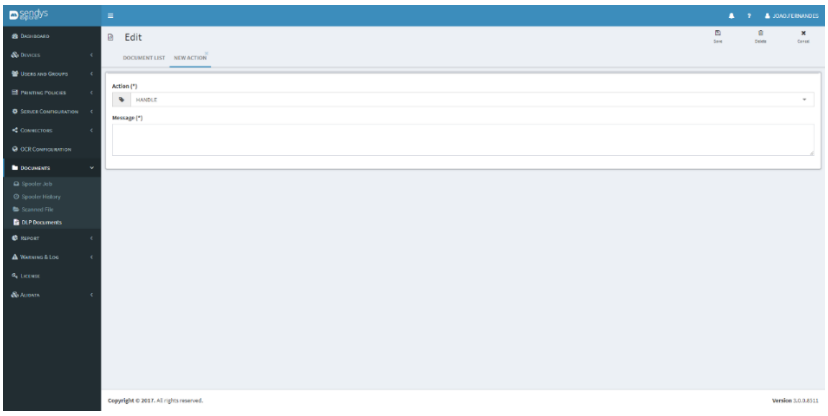


Fig. 365 – DLP Document View.

REPORTS

This section is used for data analysis and to generate various types of reports. The reports can be accessed by clicking individually on the wanted report.

Almost all the Reports works on a similar way. Most of them have a **Begin** and **End** dates to insert so the reports are restricted between a date. Others reports have another input field (**Search**) that is required to insert to proceed the build of the report. After the required fields are filled we can click on **Reload**.

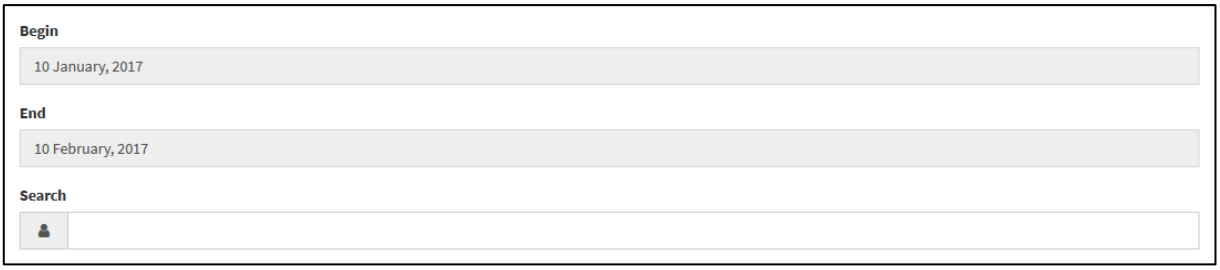


Fig. 366 - Report Parameters

While the reports are showed there are options on the report view:

Fig. 367 - Report Options

DATA ANALYSIS

This Report list all the jobs processed by SENDYS Explorer.

1. Click on **Reports**.
2. Click on **Data Analysis**.

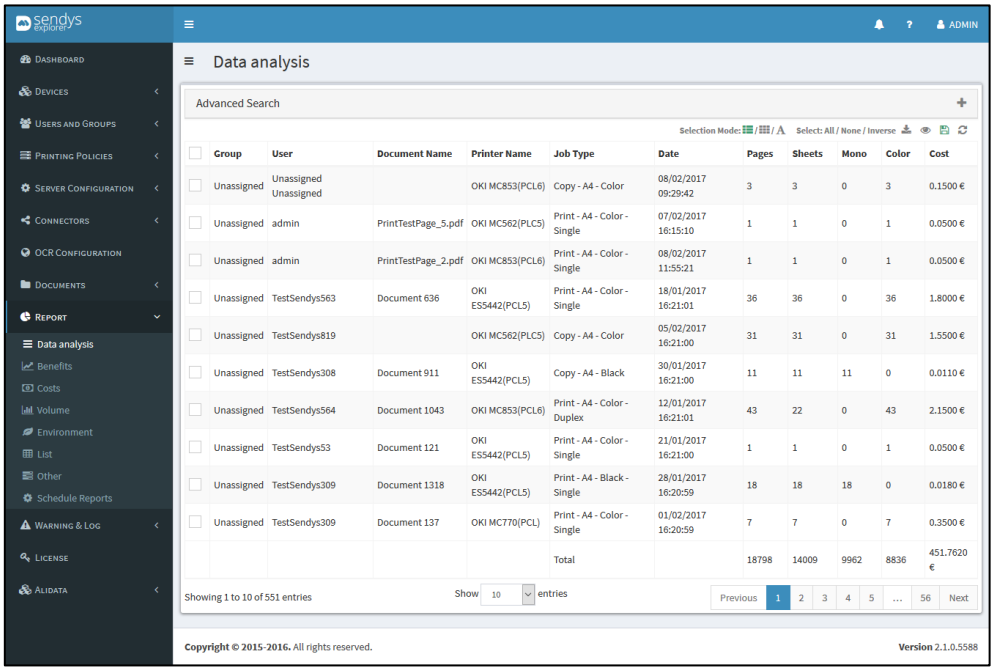


Fig. 368 - Data Analysis

ANONYMIZE/DELETE

All Data can be anonymized or deleted using the top right button. There are 3 option:

1. **Anonymize Selected:** Anonymizes user data from the documents selected.
2. **Anonymize All:** Anonymizes all user data from all documents.
3. **Delete All Data:** Prompts the user to confirm the delete action by inserting a random generated pin and Deletes all documents data.

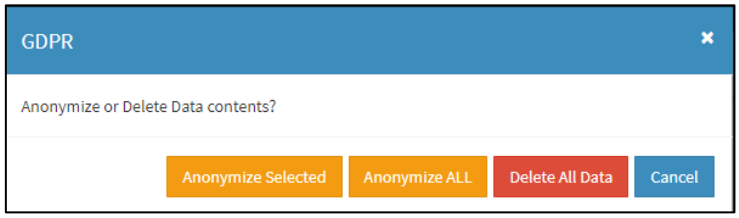


Fig. 369 - Data Analysis – Anonymize/Delete

BENEFITS

This Report list all the jobs that were not printed. Jobs that were sent to Spooler or Pull Print Queue and then were deleted.

There are 3 possible **Benefits Reports:**

- **Department Benefits**: report that shows the jobs count and costs grouped by Department of the non-printed jobs.
- **Device Benefits**: report that shows the jobs count and costs grouped by Printer of the non-printed jobs.
- **User Benefits**: report that shows the jobs count and costs for each User of the non-printed jobs.

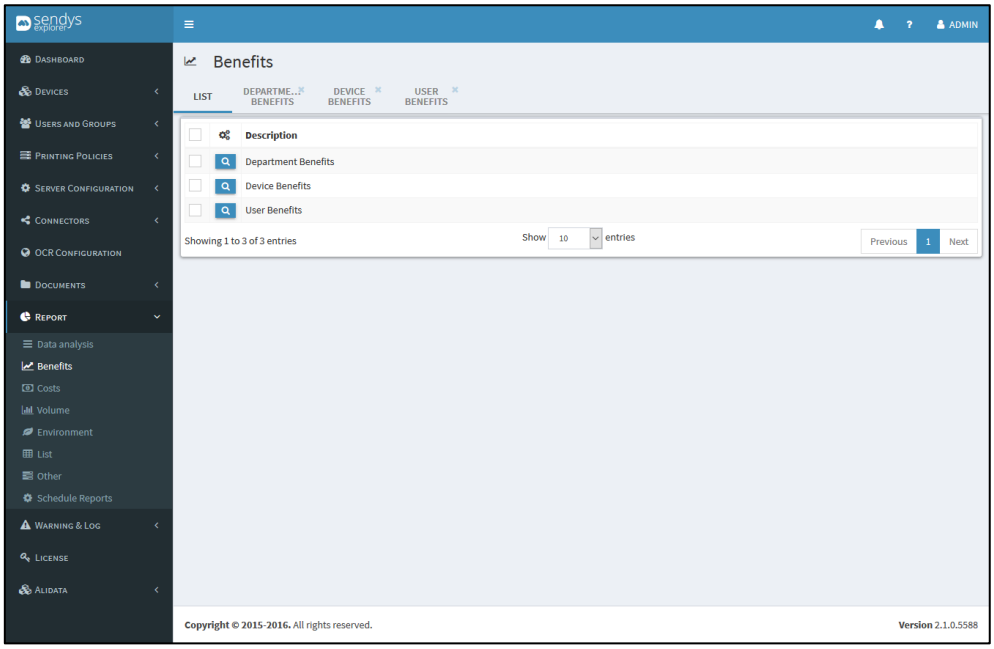


Fig. 370 - Benefits Report

GENERATING REPORT

1. Click on **Reports**.
2. Click on **Benefits**.
3. Click on **view details icon** to open the report pretended.
4. Click on **Begin** to define the start date for the report.
5. Click on **End** to define the end date for the report.
6. Click on **Search** if you would like to enter some search criteria.
   Note: The search criteria will change between **Department / Device / User** depending on the report.

7. Click on **Reload** button to generate the report.
   Note: After report creation is possible to export it by clicking on **Export**.

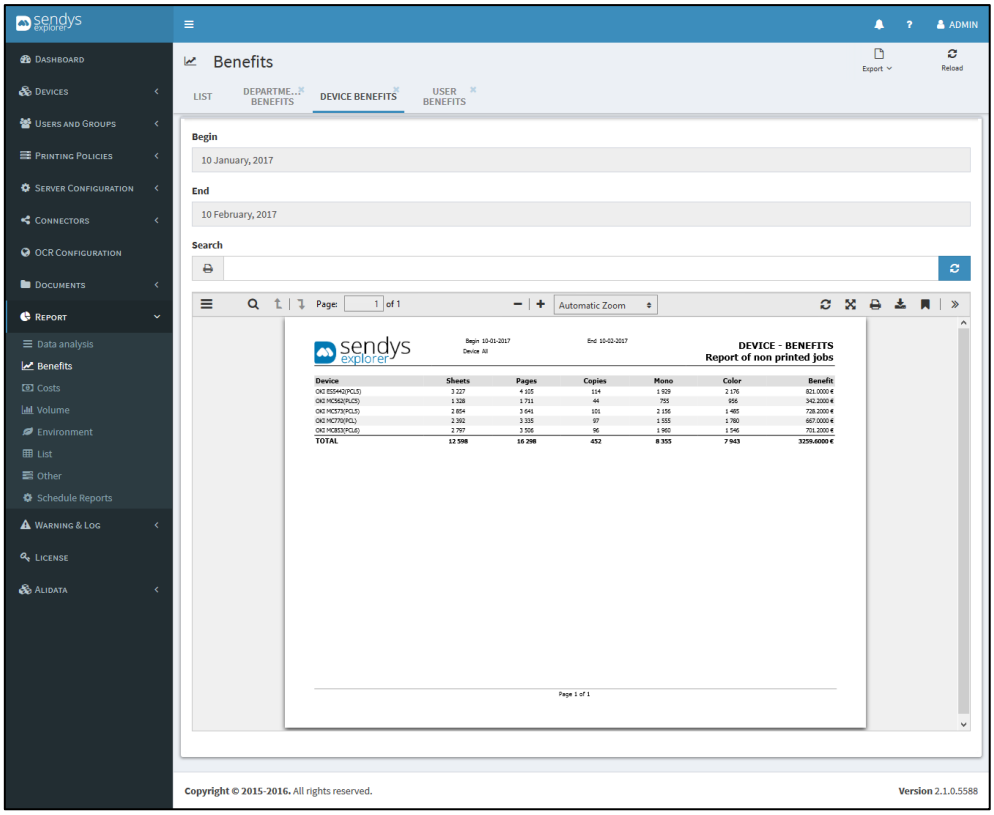


Fig. 371 - Device Benefits Report

COSTS

This Report list all the jobs that were printed and their costs.

There are 5 possible **Costs Reports:**

- **Department Cost**: report that shows the job costs grouped by Department.
- **Device Cost**: report that shows the job costs grouped by Printer.
- **User Cost**: report that shows the job costs for each User.
- **User Job Cost**: report that shows all the printed job costs.
- **Department Detail Cost**: report that shows job cost by user grouped by Department.

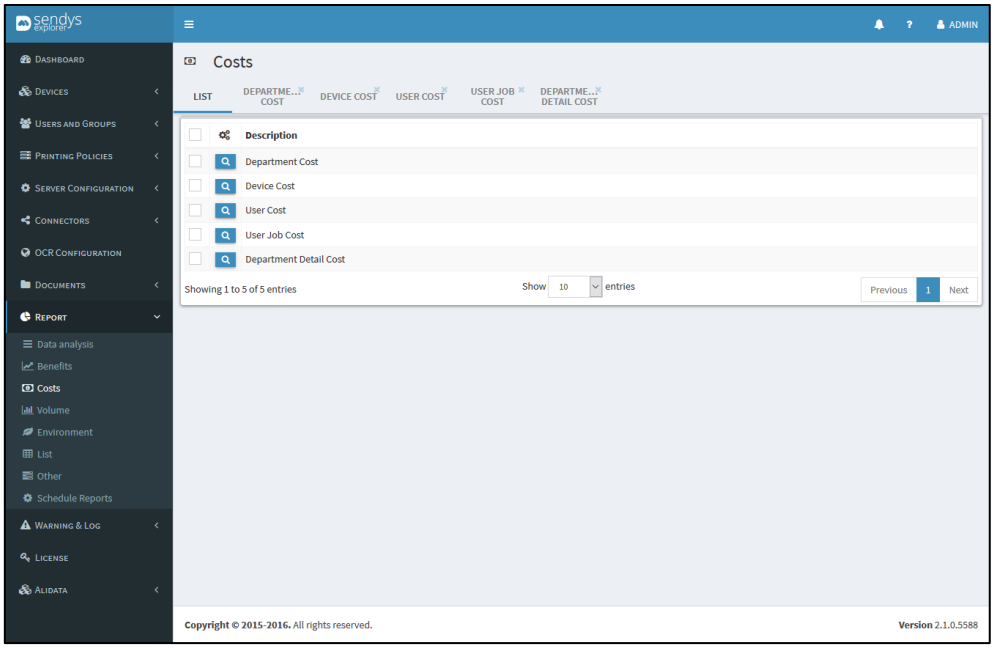


Fig. 372 - Benefits Report

GENERATING REPORT

1. Click on **Reports**.
2. Click on **Costs**.
3. Click on **view details icon** to open the report pretended.
4. Click on **Begin** to define the start date for the report.
5. Click on **End** to define the end date for the report.
6. Click on **Search** if you would like to enter some search criteria.
   Note: The search criteria will change between **Department / Device / User** depending on the report.

7. Click on **Reload** button to generate the report.
   Note: After report creation is possible to export it by clicking on **Export**.

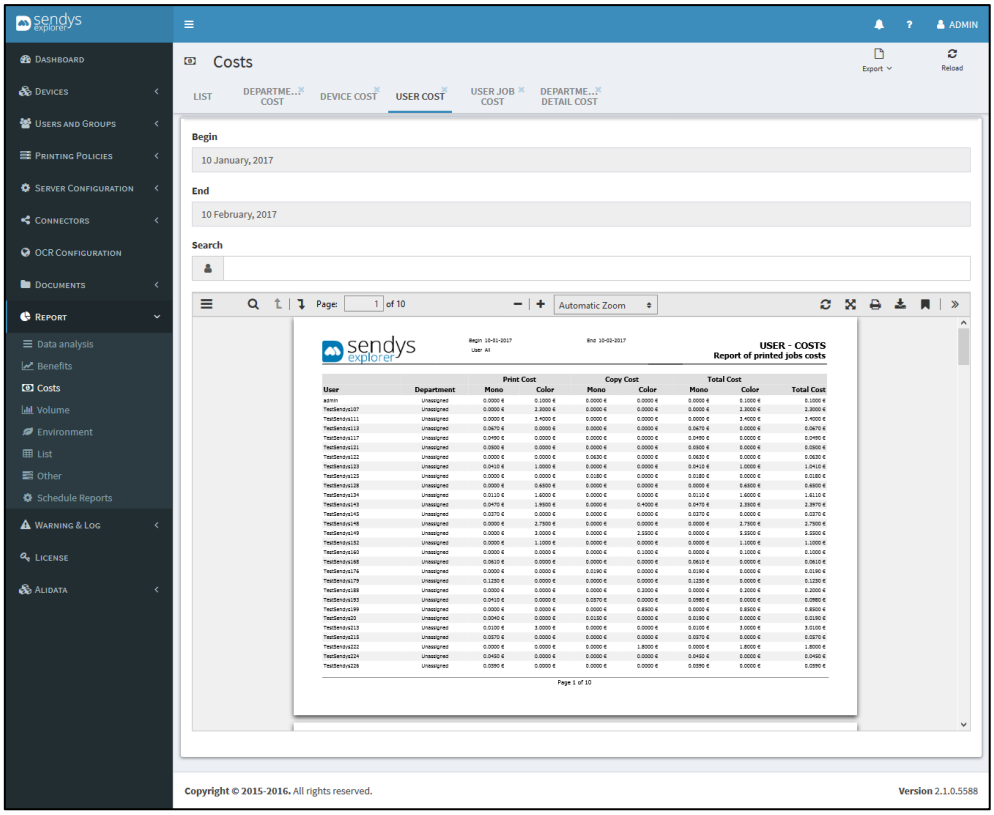


Fig. 373 - User Cost Report

VOLUME

This Report list the counters of all the jobs that were printed.

There are 3 possible **Volume Reports:**

- **Department Volume**: report that shows the job counters grouped by Department.
- **Device Volume**: report that shows the job counters grouped by Printer.
- **User Volume**: report that shows the job counters for each User.

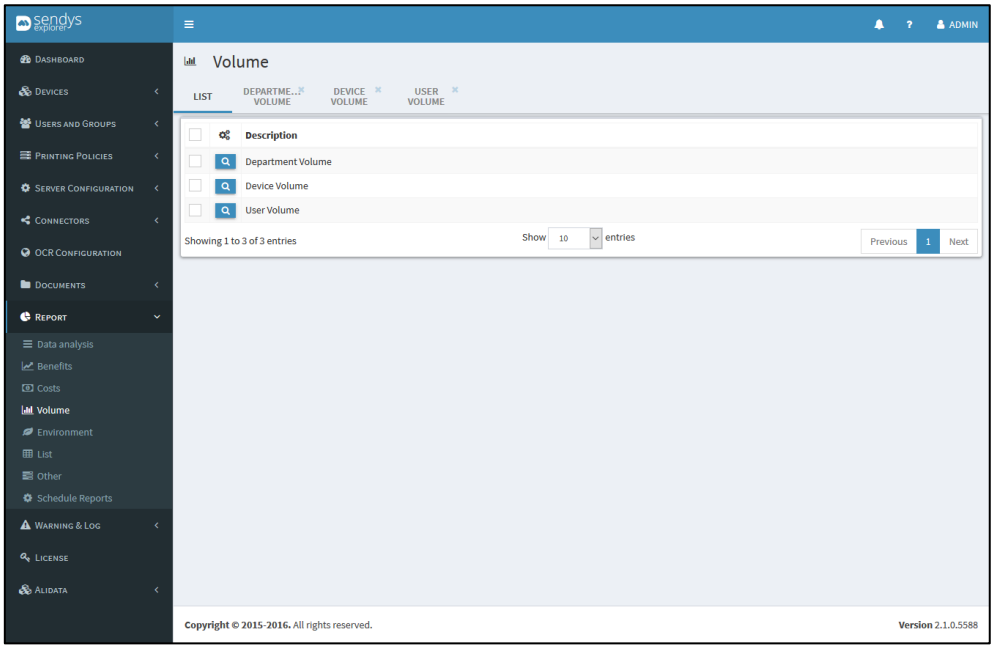


Fig. 374 - Volume Report

GENERATING REPORT

1. Click on **Reports**.
2. Click on **Volume**.
3. Click on **view details icon** to open the report pretended.
4. Click on **Begin** to define the start date for the report.
5. Click on **End** to define the end date for the report.
6. Click on **Search** if you would like to enter some search criteria.
   Note: The search criteria will change between **Department / Device / User** depending on the report.

7. Click on **Reload** button to generate the report.
   Note: After report creation is possible to export it by clicking on **Export**.

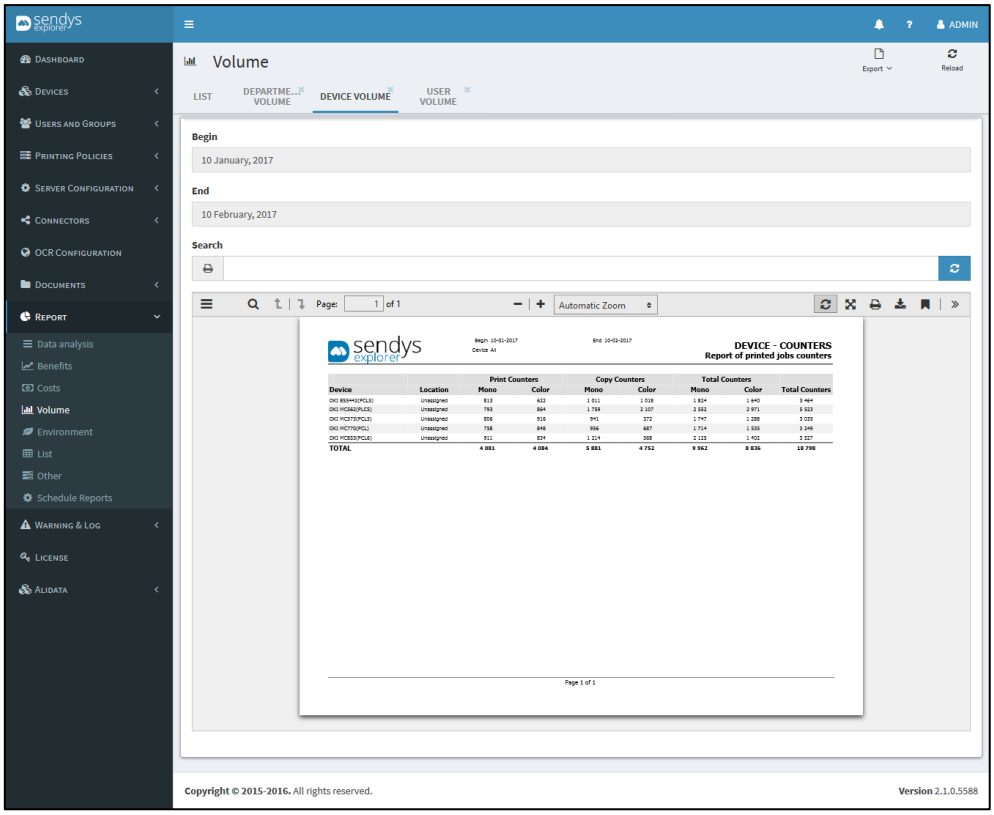


Fig. 375 - Device Volume Report

ENVIRONMENT

This Report show various types of graphics related with Environment.

There are 3 possible **Environment Reports:**

- **Consumed Sheets**: graphics showing type of consumed sheets on different perspectives.
- **Supplies**: graphics showing the printer the various consumables.
- **Savings**: graphics showing sheet savings on different perspectives.

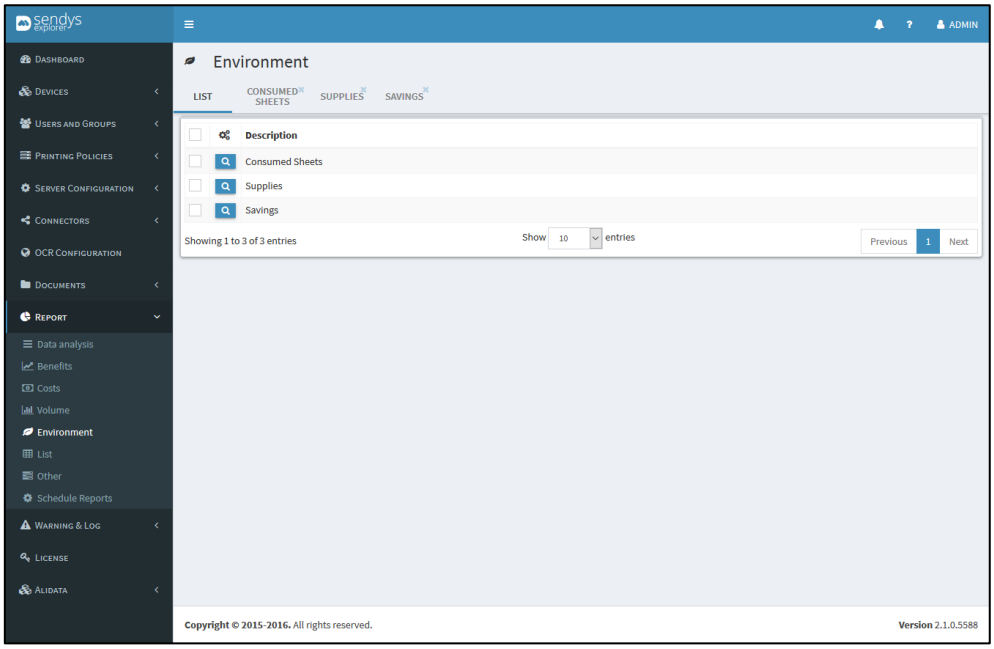


Fig. 376 - Environment Report

GENERATING REPORT

1. Click on **Reports**.
2. Click on **Environment**.
3. Click on **view details icon** to open the report pretended.
   Note: This reports will be generated automatically when they are opened and they do not need parameters.

4. Click on **Reload** button to refresh the report.
   Note: After report creation is possible to export it by clicking on **Export**.

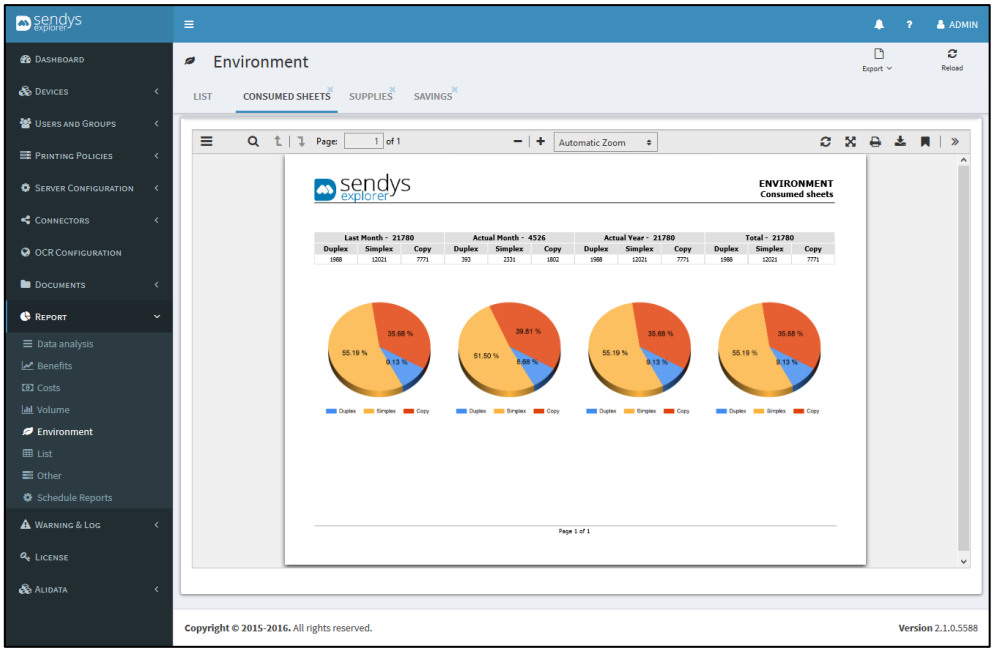


Fig. 377 - Environmental Consumed Sheets Report

LIST

This Report list the printers and the counters of all printers.

There are 2 possible **List Reports:**

- **Device List**: report that shows a list the devices installed on the platform.
- **Device Billing**: report that shows a list about the billing associated to each printer used on the platform.

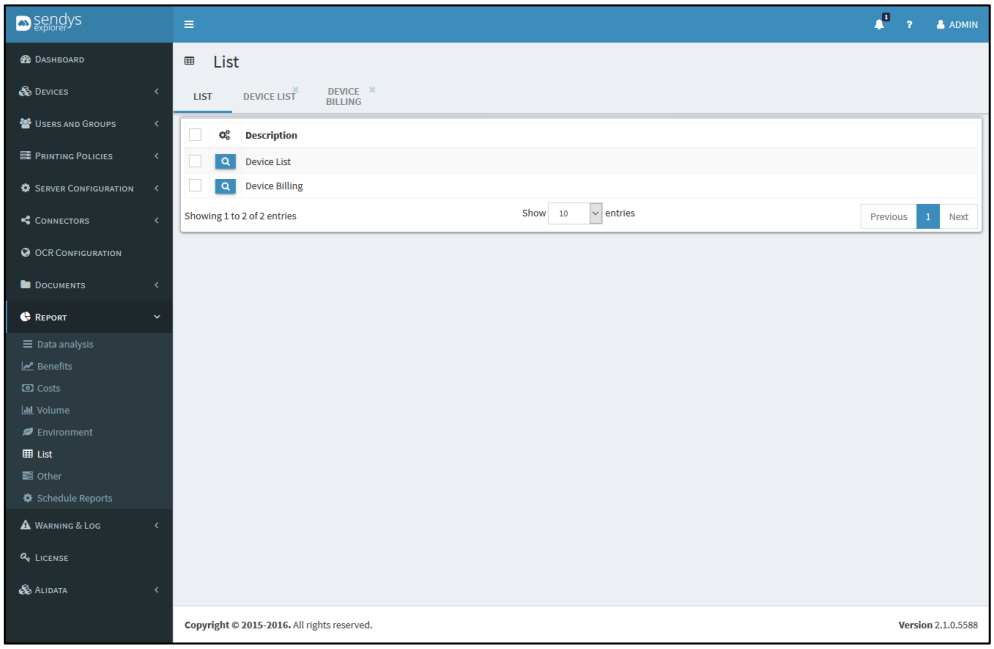


Fig. 378 - List Report

GENERATING REPORT

1. Click on **Reports**.
2. Click on **List**.
3. Click on **view details icon** to open the report pretended.
4. Click on **Search** if you would like to enter some search criteria.

5. Click on **Reload** button to refresh the report.
   Note: After report creation is possible to export it by clicking on **Export**.

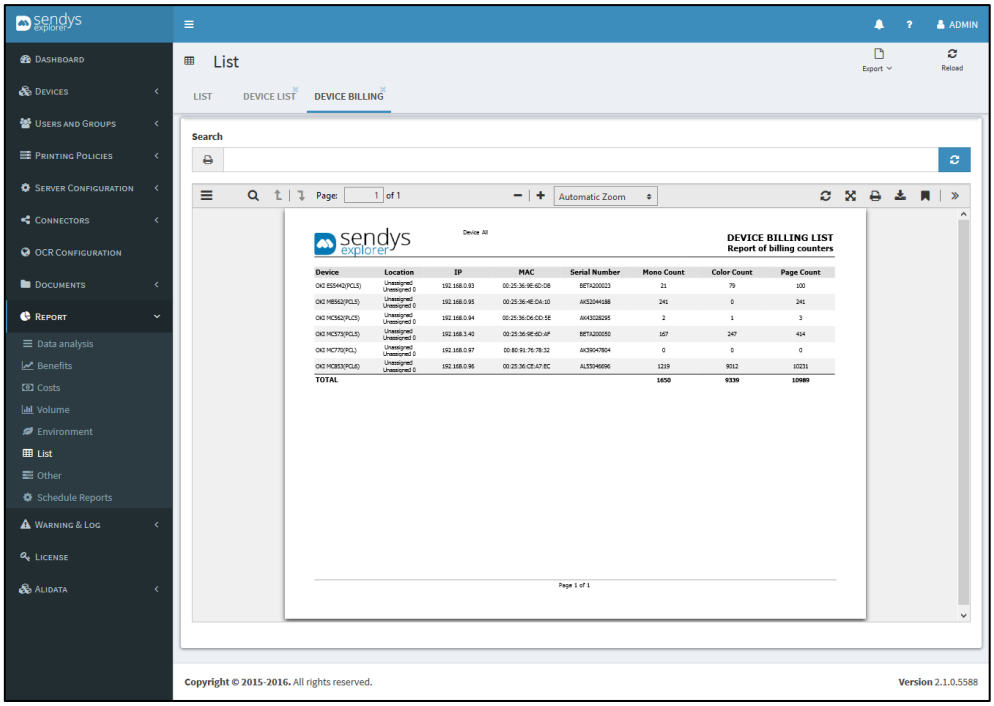


Fig. 379 - List Device Billing Report

OTHER

This are other useful reports.

There are 3 possible **Other Reports:**

- **Printer QR Code**: report that shows a list the QR Code associated to each printer used on the platform.
- **Device Status**: report that shows a list the Status of each printer used on the platform.
- **Last 30 Days**: report that shows a list of the last 30 days counters on the platform.

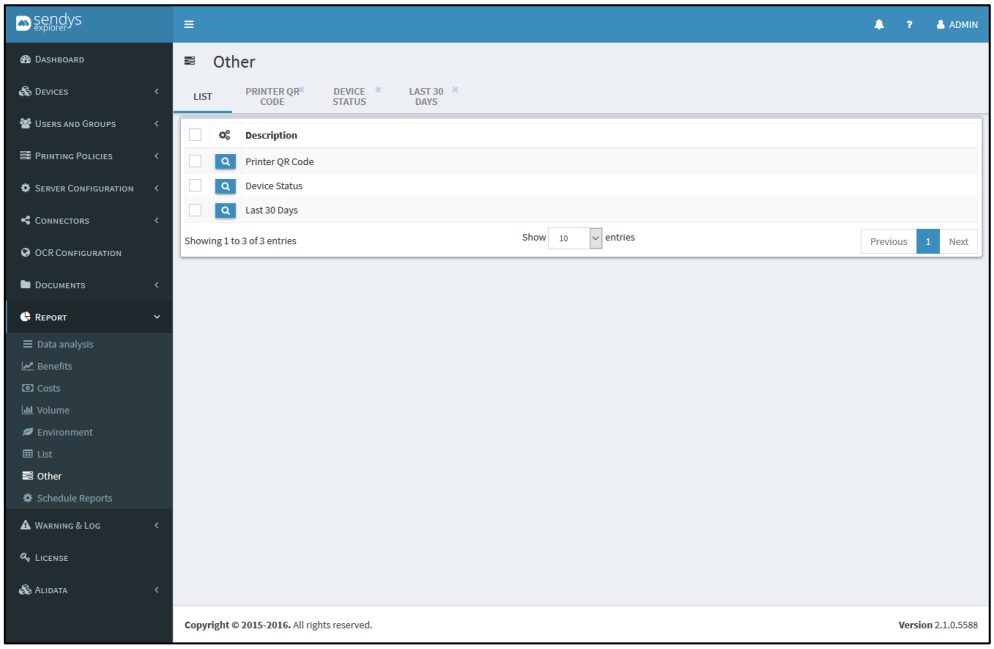
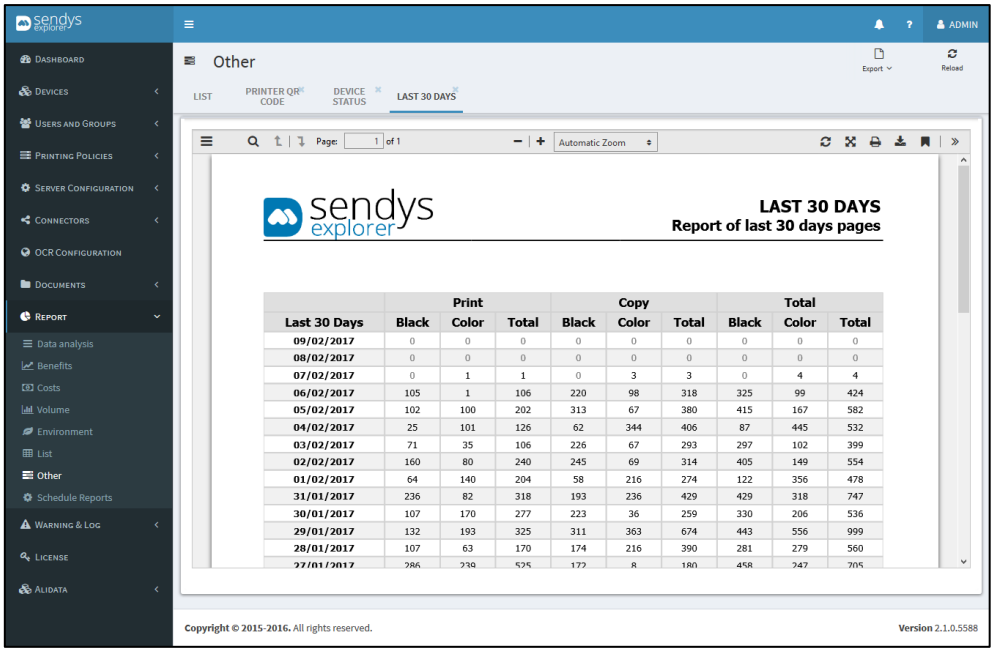


Fig. 380 - Other Report

GENERATING REPORT

1. Click on **Reports**.
2. Click on **Other**.
3. Click on **view details icon** to open the report pretended.
   Note: This reports will be generated automatically when they are opened and they do not need parameters.

4. Click on **Reload** button to refresh the report.
   Note: After report creation is possible to export it by clicking on **Export**.



Last 30 Days	Print			Copy			Total		
	Black	Color	Total	Black	Color	Total	Black	Color	Total
09/02/2017	0	0	0	0	0	0	0	0	0
08/02/2017	0	0	0	0	0	0	0	0	0
07/02/2017	0	1	1	0	3	3	0	4	4
06/02/2017	105	1	106	220	98	318	325	99	424
05/02/2017	102	100	202	313	67	380	415	167	582
04/02/2017	25	101	126	62	344	406	87	445	532
03/02/2017	71	35	106	226	67	293	297	102	399
02/02/2017	160	80	240	245	69	314	405	149	554
01/02/2017	64	140	204	58	216	274	122	356	478
31/01/2017	236	82	318	193	236	429	429	318	747
30/01/2017	107	170	277	223	36	259	330	206	536
29/01/2017	132	193	325	311	363	674	443	556	999
28/01/2017	107	63	170	174	216	390	281	279	560
27/01/2017	286	239	525	172	8	180	458	247	705

Fig. 381 - Other Last 30 Days Report

SCHEDULE REPORTS

In this section, we can schedule reports to be sent by email (one or more) and you can configure certain parameters, such as date of sending, message and others.

1. Click on **Reports > Schedule Reports**.
2. Click on **New**.

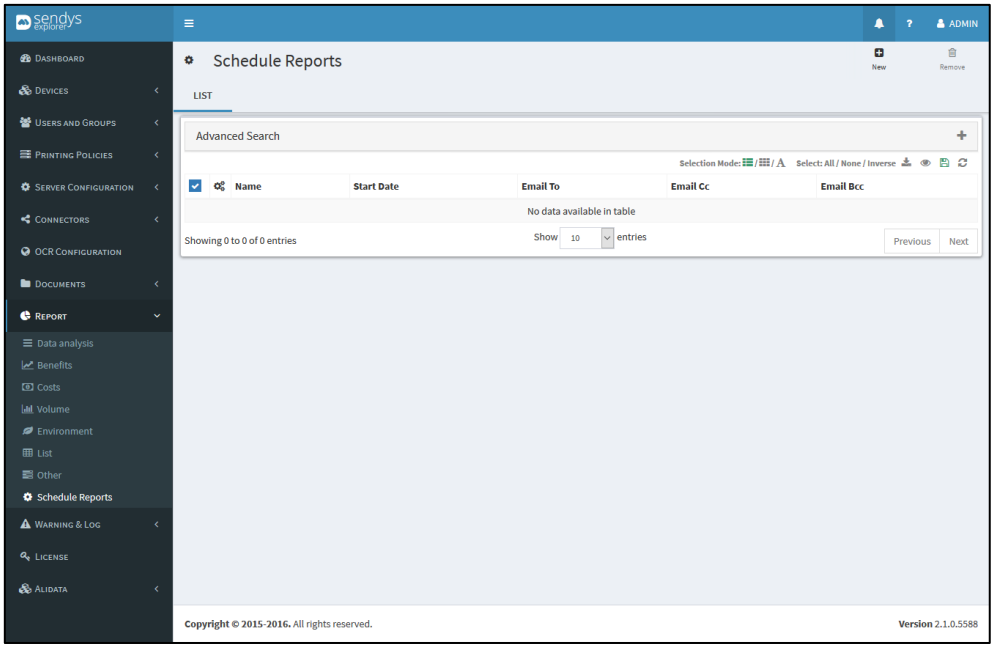


Fig. 382 - Schedule Reports

DETAILS

1. Click on **Details**.

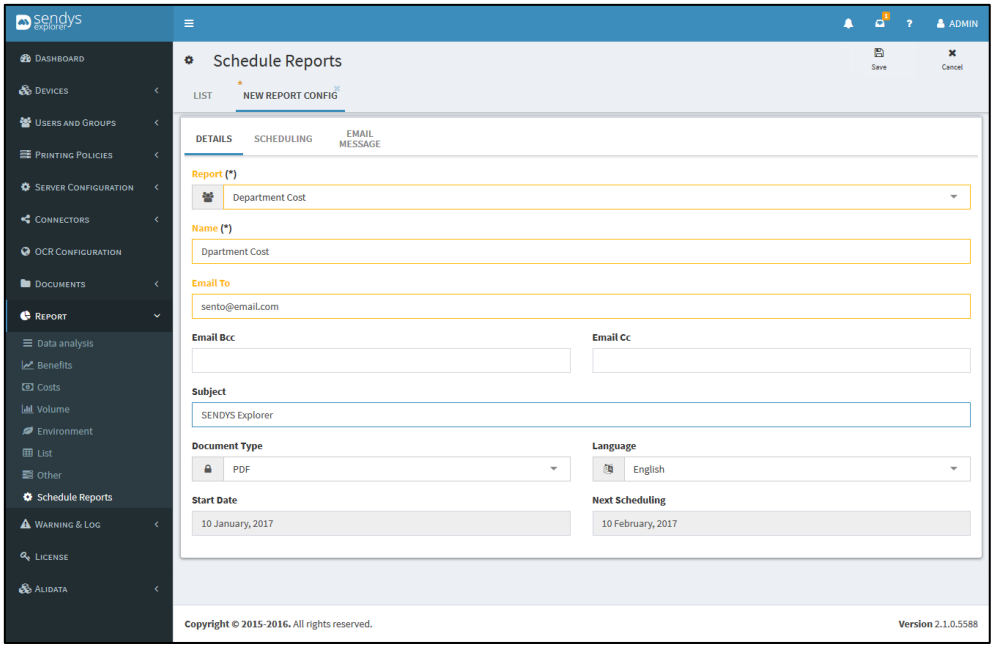


Fig. 383 - Schedule Reports Details

2. Make the required configuration.

Name	Details
Report	Choose the report to schedule.
Name	Name of the schedule report.
Email To	Email to send.
Email Bcc	Email Bcc.
Email CC	Email CC.
Subject	Insert the email subject.
Language	Select the language.
Start Date	Start date.
Next Scheduling	Next scheduling date.

Table 64 - Schedule Reports Details

3. Click **Scheduling**.

SCHEDULING

1. Click on **Scheduling**.

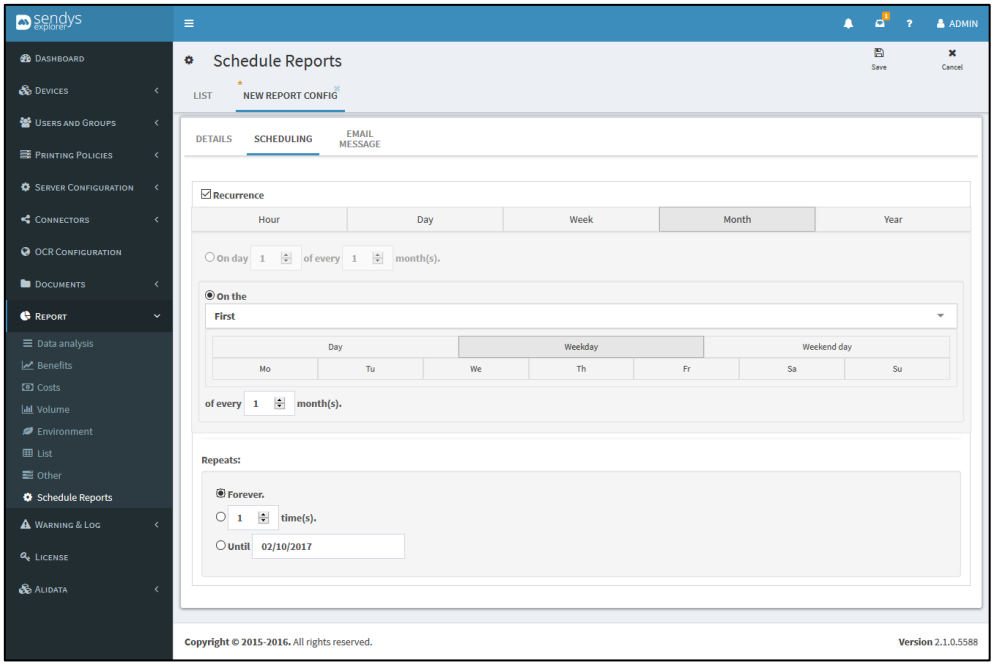


Fig. 384 - Schedule Reports Scheduling

2. Make the required configuration.
3. Enable/disable the date/time option.
4. For each option select time and date to schedule and you can configure the repeats.
5. Click **Email Message**.

EMAIL MESSAGE

1. Click on **Email Message**.

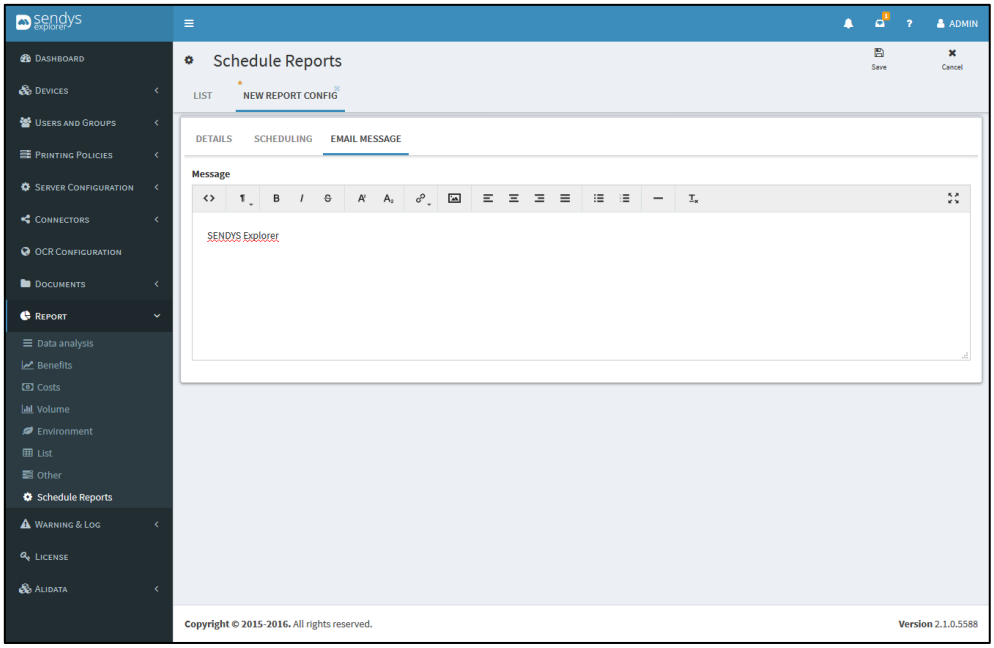


Fig. 385 - Schedule Reports Email Message

4. Click **Save** to save the configuration.

WARNINGS & LOGS

In this section, we can consult the errors, warnings and log associated with the printers and platform.

PRINTER WARNINGS

1. Click on **Warning & Log**.
2. Click **Printer Warnings** menu.

On this view a list of warnings is shown.

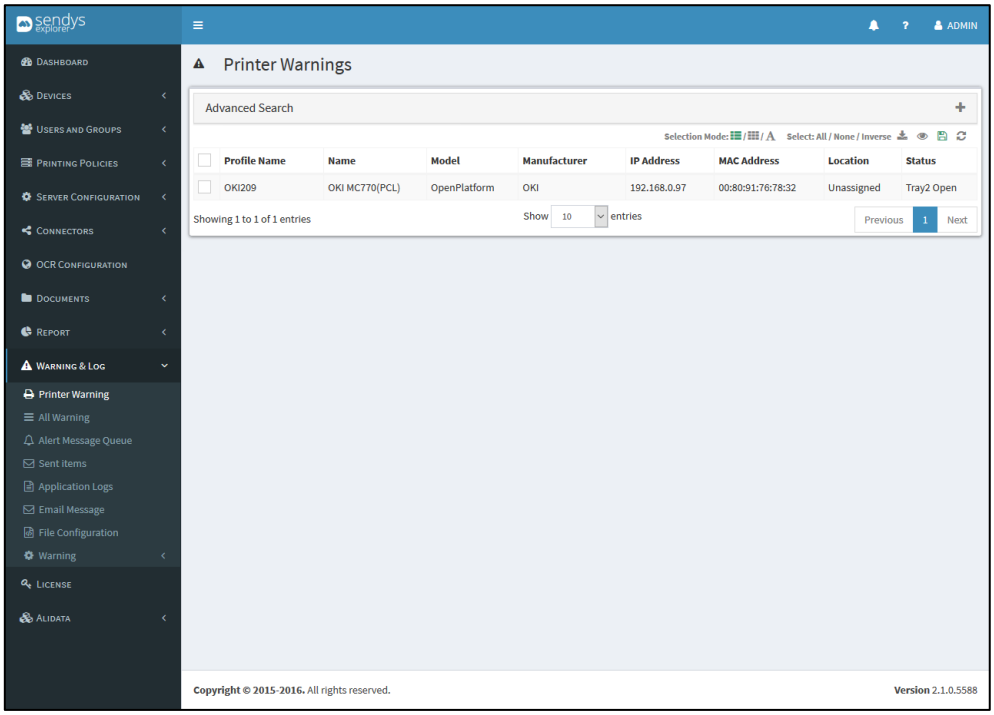


Fig. 386 - Printer Warnings

ALL WARNINGS

1. Click on **Warning & Log**.
2. Click **All Warning**.

This view shows the warnings of the system containing specific information.

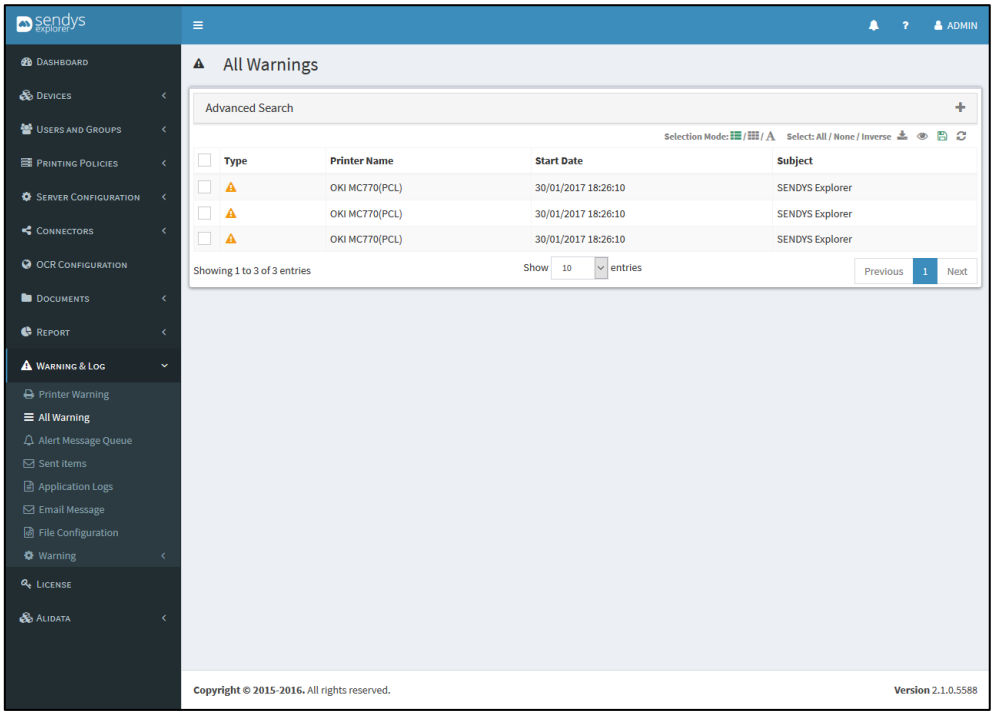


Fig. 387 - All Warnings

All warnings have a type represented by a icon:

	Status OK		Status INFO
	Status WARNING		Status ERROR/FATAL

ALERT MESSAGE QUEUE

1. Click on **Warning & Log**.
2. Click **Alert Message Queue**.

This view shows the alerts/warnings messages queue from the platform. It is important the Administrator use this view to check the system warnings and treat them. On the list, there are some parameters to check the stability of the system, for example, the **Active** is the parameter that indicates if the warning/alert was already checked or not. When checked the alert changes to not **Active (cross).**

The possible actions to operate with this view are:

Remove - remove the selected messages.

Delete - delete individually the queue.

Check As Read - select an alert that still **Active** and click on Check as Read button. It will appear a window requiring the **Result** field the **Comment** field. Clicking on confirm to save the changes and now the alert is not Active.

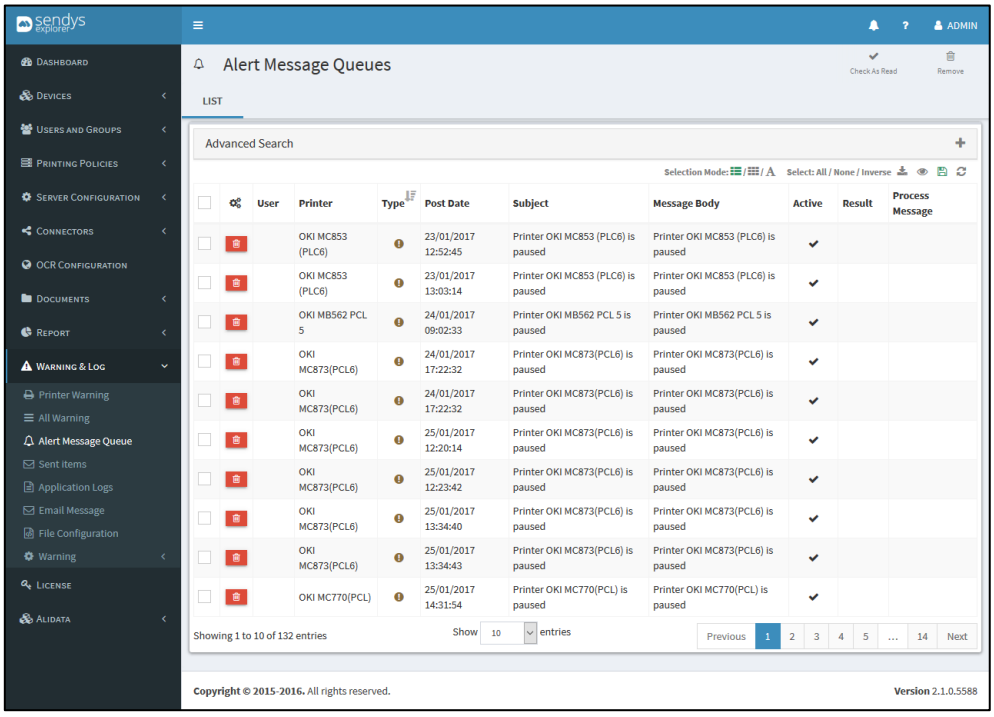


Fig. 388 - Alert messages queues

SEND ITEMS

1. Click on **Warning & Log**.
2. Click **Sent items**.

This view shows the list of Sent Email configured on the platform.

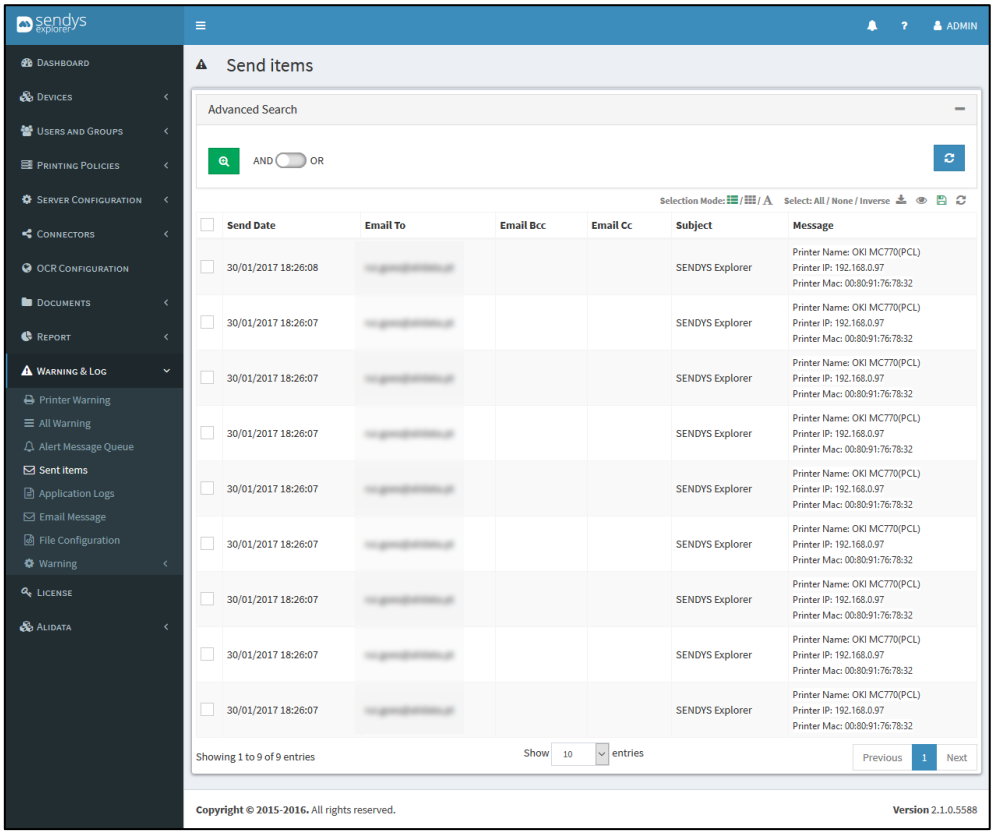


Fig. 389 - Sent items

APPLICATION LOGS

1. Click on **Warning & Log**.
2. Click **Applications Logs**.
3. **Select Application** to show on the **Log Content**.

On this view it is possible to consult the application logs related with the **Document Spooler**, **Virtual Spooler**, **Service**, **Events**, **Monitor** and **Control Server**.

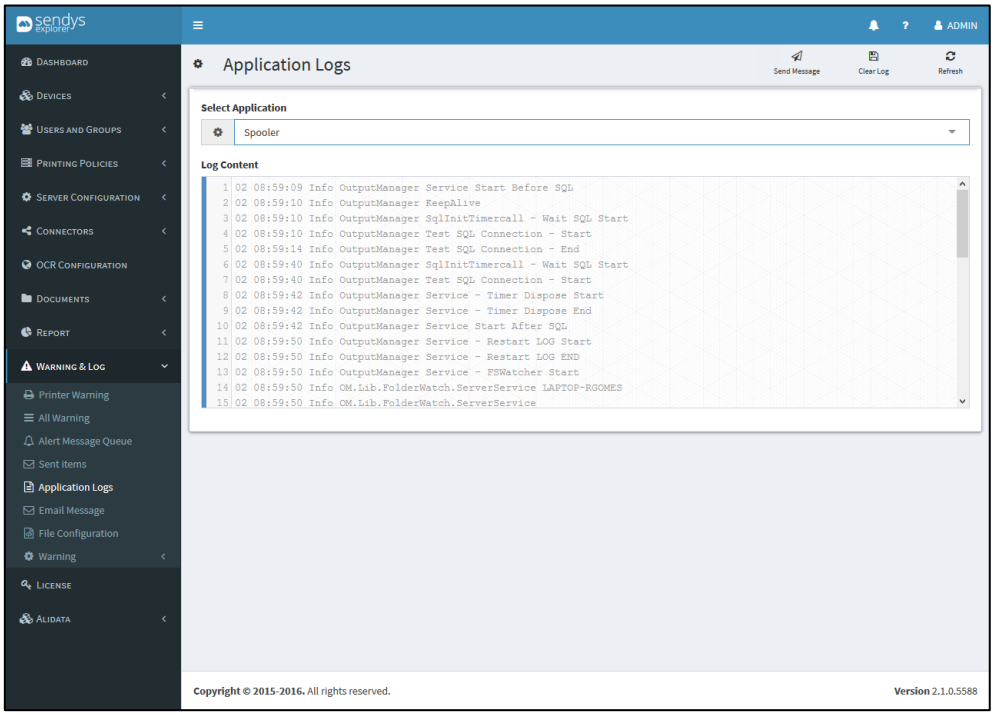


Fig. 390 - Application Logs

EMAIL MESSAGE

This view shows the Standard Platform Email configurations that are used to send automatic emails.

1. Click on **Warning & Log** menu.
2. Click on **Email Message**.
3. Select the **Email Message**.
4. Select the **Subject** for the Email.
5. Configure the **Body** elements.

Click **Save** to apply or **Cancel** to cancel the actions.

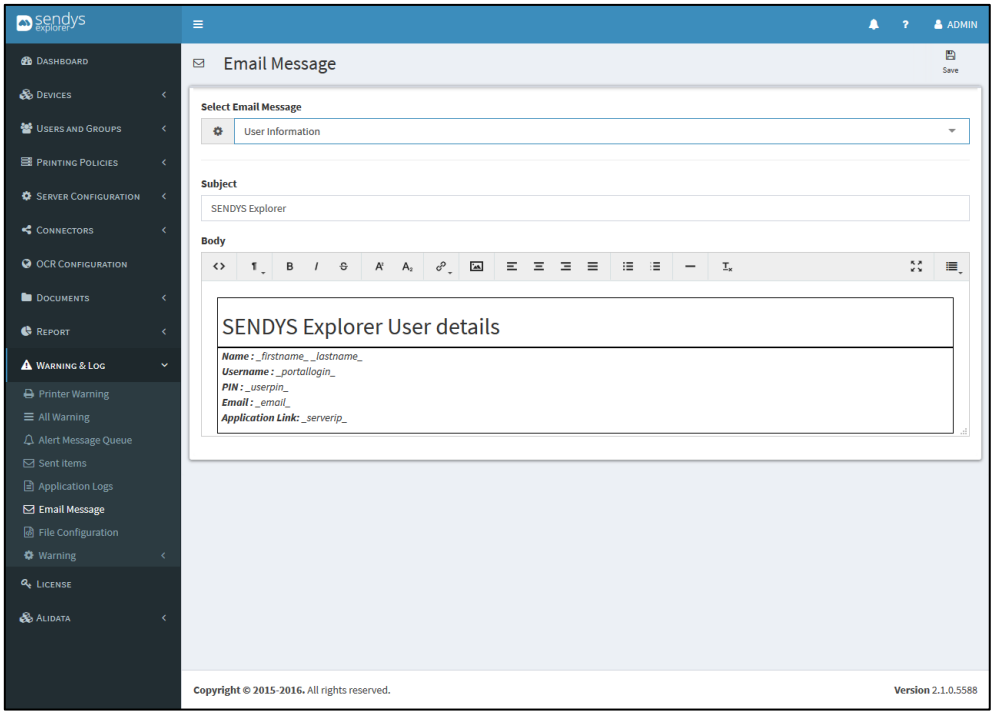


Fig. 391 - Emails message

FILE CONFIGURATION

1. Click on **Warning & Log** menu.
2. Click on **File Configuration**.
3. **Select Application** option to load the xml on the **Log Content**.

This view shows the file configurations for each Select Application.

Click **Save** to apply or **Cancel** to cancel the actions.

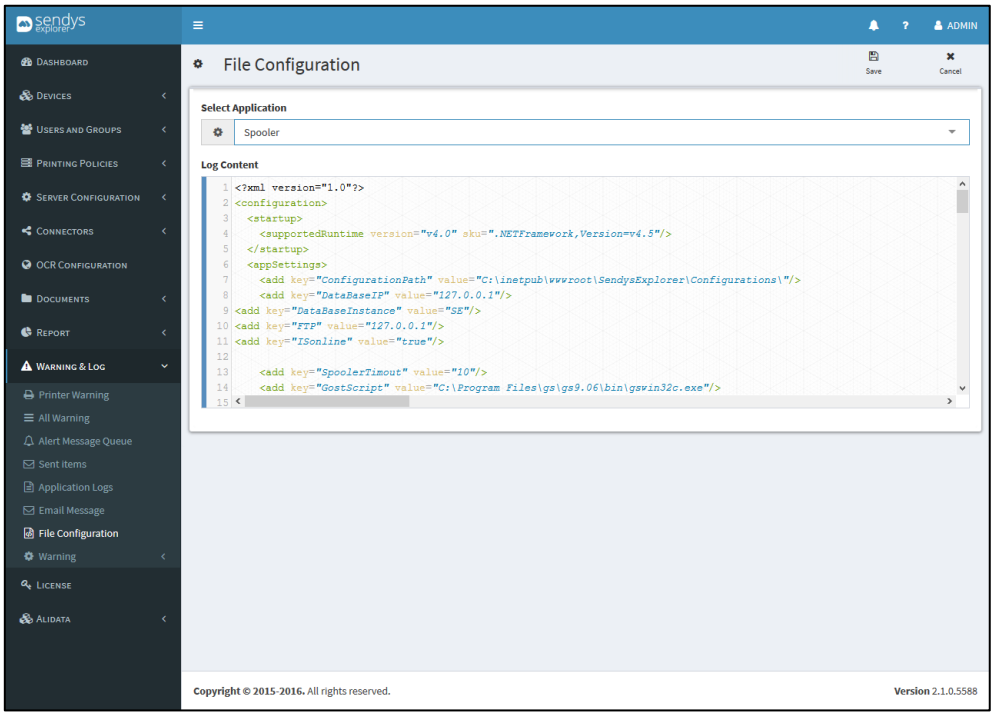


Fig. 392 - File configuration

WARNING SUPPLY/STATUS

Here in this section are shown warning related with the consumables and status of the printers.

So the next submenus are showed.

SUPPLY

1. Click on **Warning & Log** menu.
2. Click on **Warning**.
3. Click on **Supply** submenu.

Use this view to control the supply warnings created for the platform to help controlling the printer supplies.

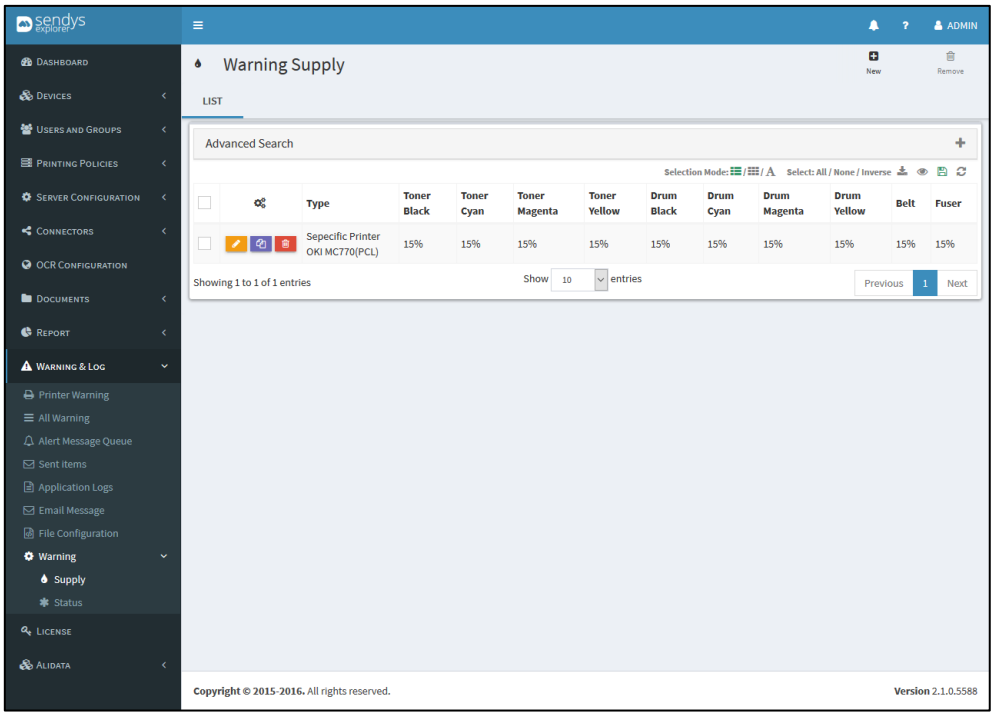


Fig. 393 - Warning Supply

SUPPLIER

1. Click on **New** button.
2. Configure the next options.

Name	Details
Profile	Select the printer profile (one or more).
Printer	Select the printer (one or more).
Warning Level	Select the warning.

Select the tonners and/or the drum color percentage level to trigger the warning.

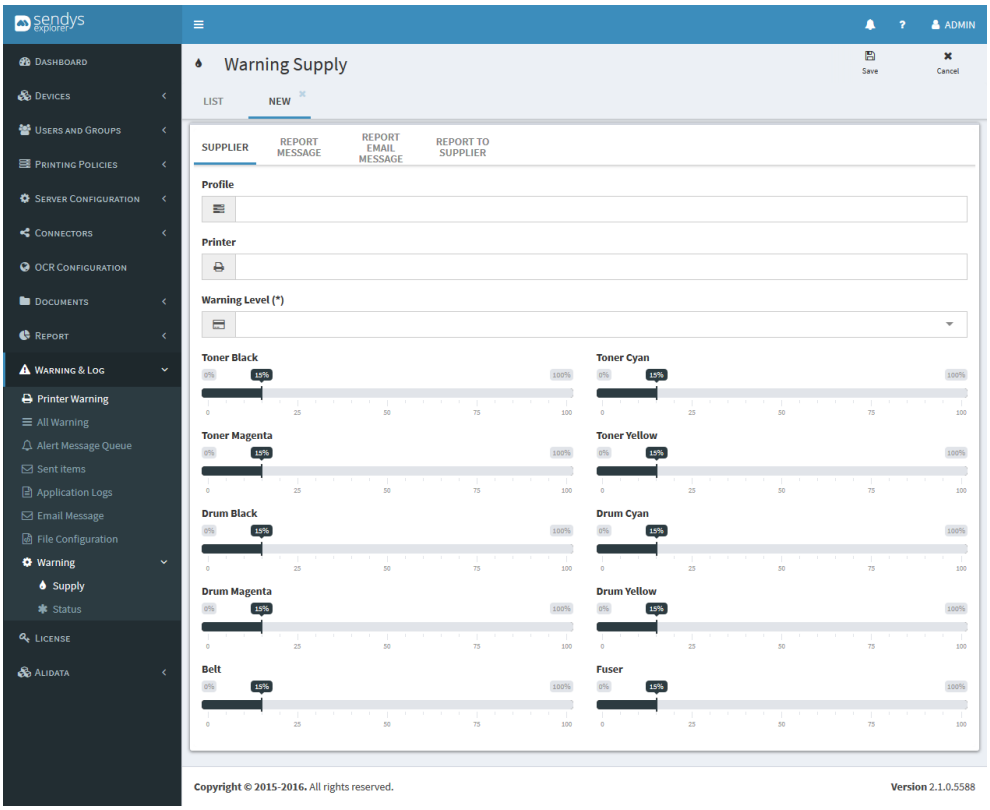
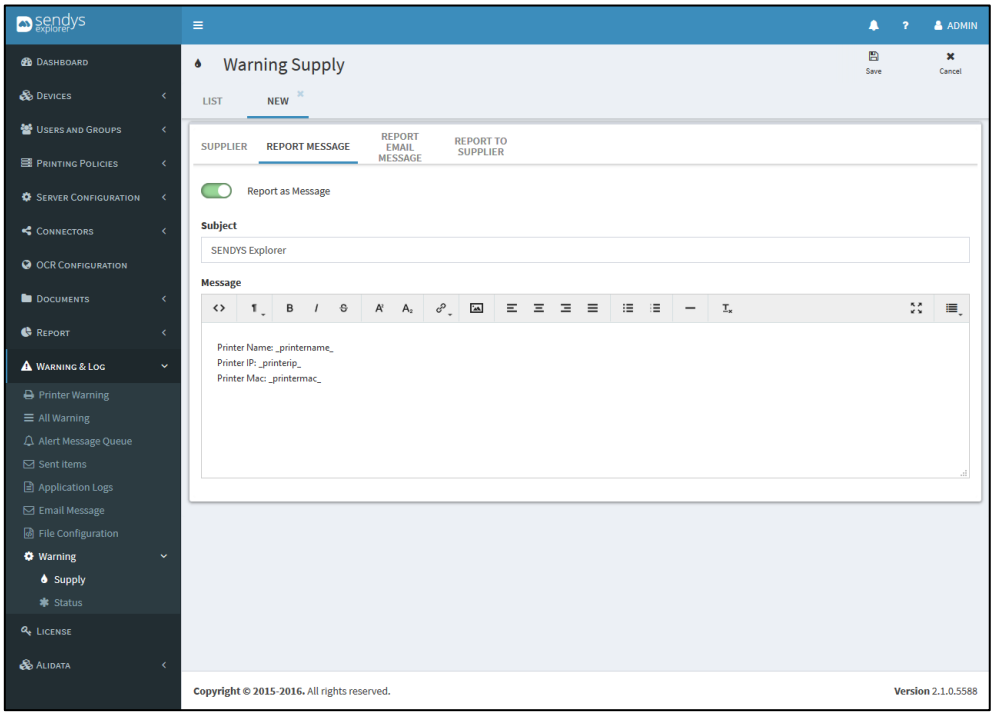


Fig. 394 - Warning supply configuration

REPORT MESSAGE

Configure this to generate a warning message to show on all warning submenu.

Name	Details
Report as Message	Define is the status warning will message show on the All Warning menu.
Subject	Define the subject for the message.
Message	Define the message content.



fFig. 395 - Warning supply configuration - report message

REPORT EMAIL MESSAGE

Configure this to generate an email message(warning) to send an email automatically.

Name	Details
Report as Email	Select the option to use this as an email message.
To	Send to field.
Bcc	Send Bcc field.
CC	Send Cc field.
Subject	Define the subject for the email.
Message	Define the message content for the email.

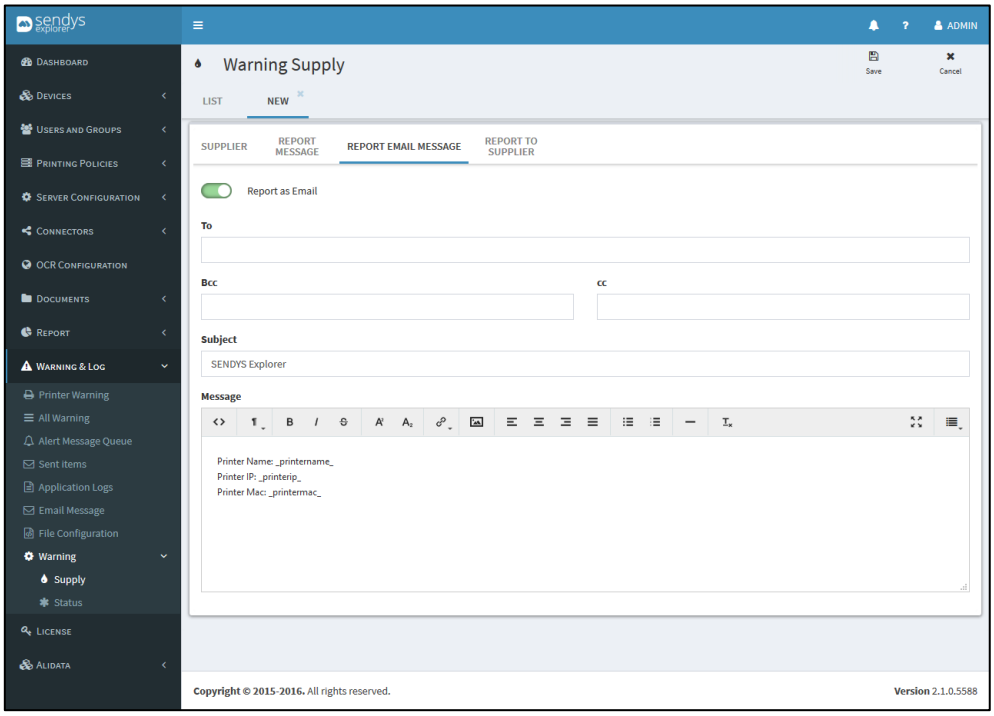


Fig. 396 - Warning supply configuration - report email message

REPORT TO SUPPLIER

Configure this to generate an email message(warning) to send an email to the supplier automatically.

Name	Details
Auto Require Supply	Select the option to use this as an email message to supply.
To	Send to field.
Bcc	Send Bcc field.
CC	Send Cc field.
Subject	Define the subject for the email.
Message	Define the message content for the email.

Click **Save** to apply or **Cancel** to cancel the actions.

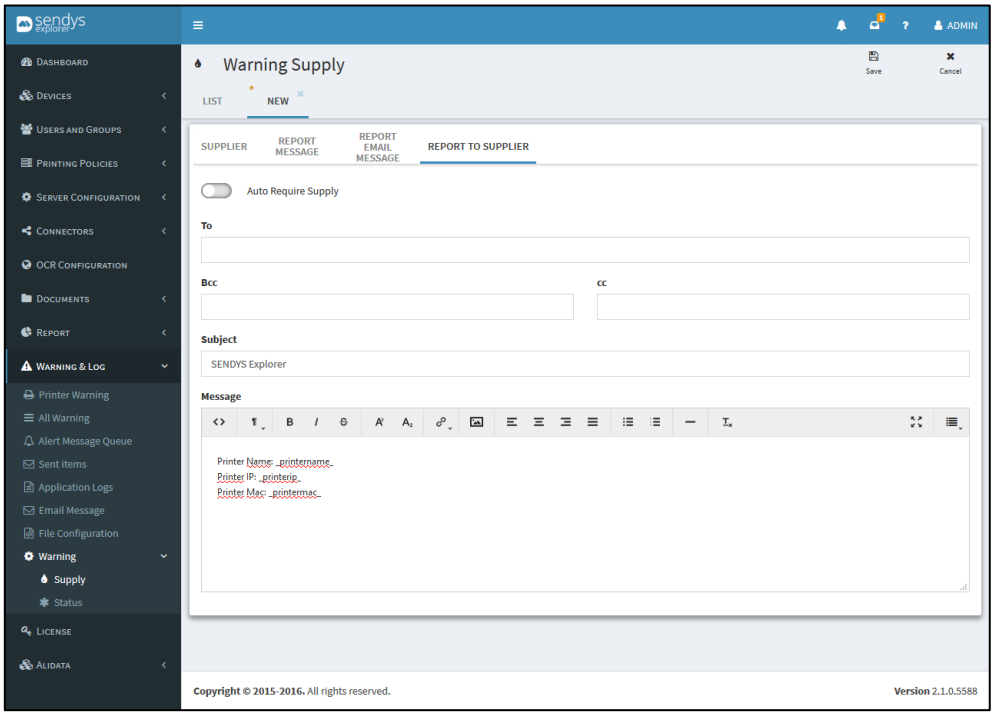


Fig. 397 - Warning supply configuration - report to supplier

STATUS

1. Click on **Warning & Log** menu.
2. Click on **Warning** menu.
3. Click on **Status** submenu.

Use this view to control the status warnings created for the platform to help controlling the printer status.

SUPPLIER

1. Click on **Status** submenu.
2. Configure the next options.

Name	Details
Profile	Select the printer profile (one or more).
Printer	Select the printer (one or more).
Warning Level	Select the warning.
Status	Insert the type of status.

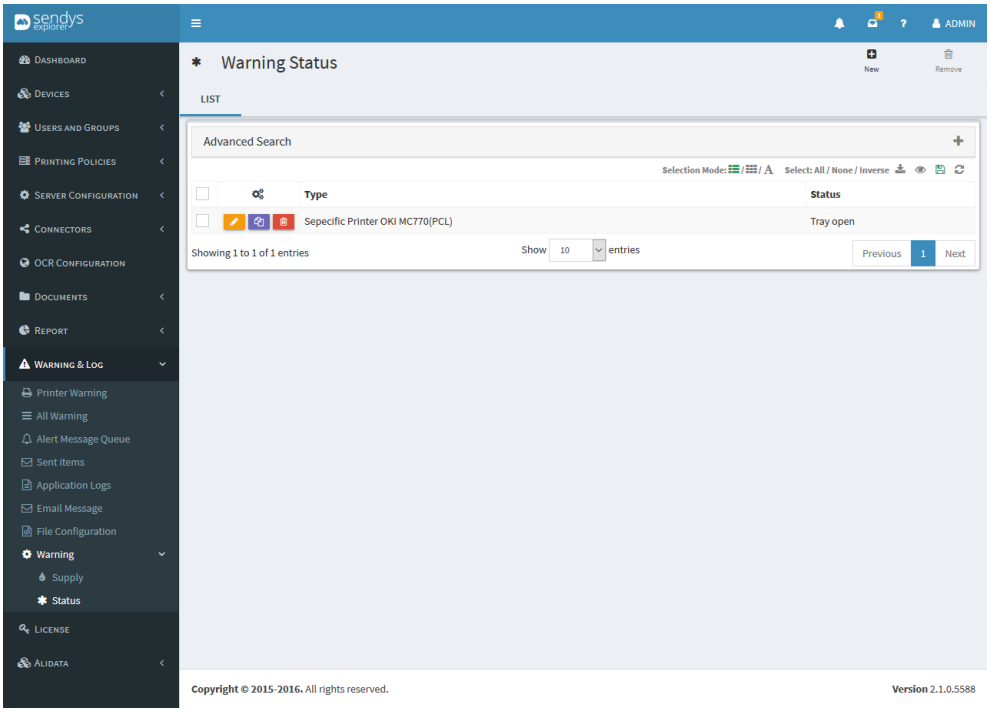


Fig. 398 - Warning status–supplier

REPORT MESSAGE

1. Click on **Report Message** submenu.

2. Configure this to generate a warning message to show on all warning submenu.

Name	Details
Report as Message	Define is the status warning will message show on the All Warning menu.
Subject	Define the subject for the message.
Message	Define the message content.

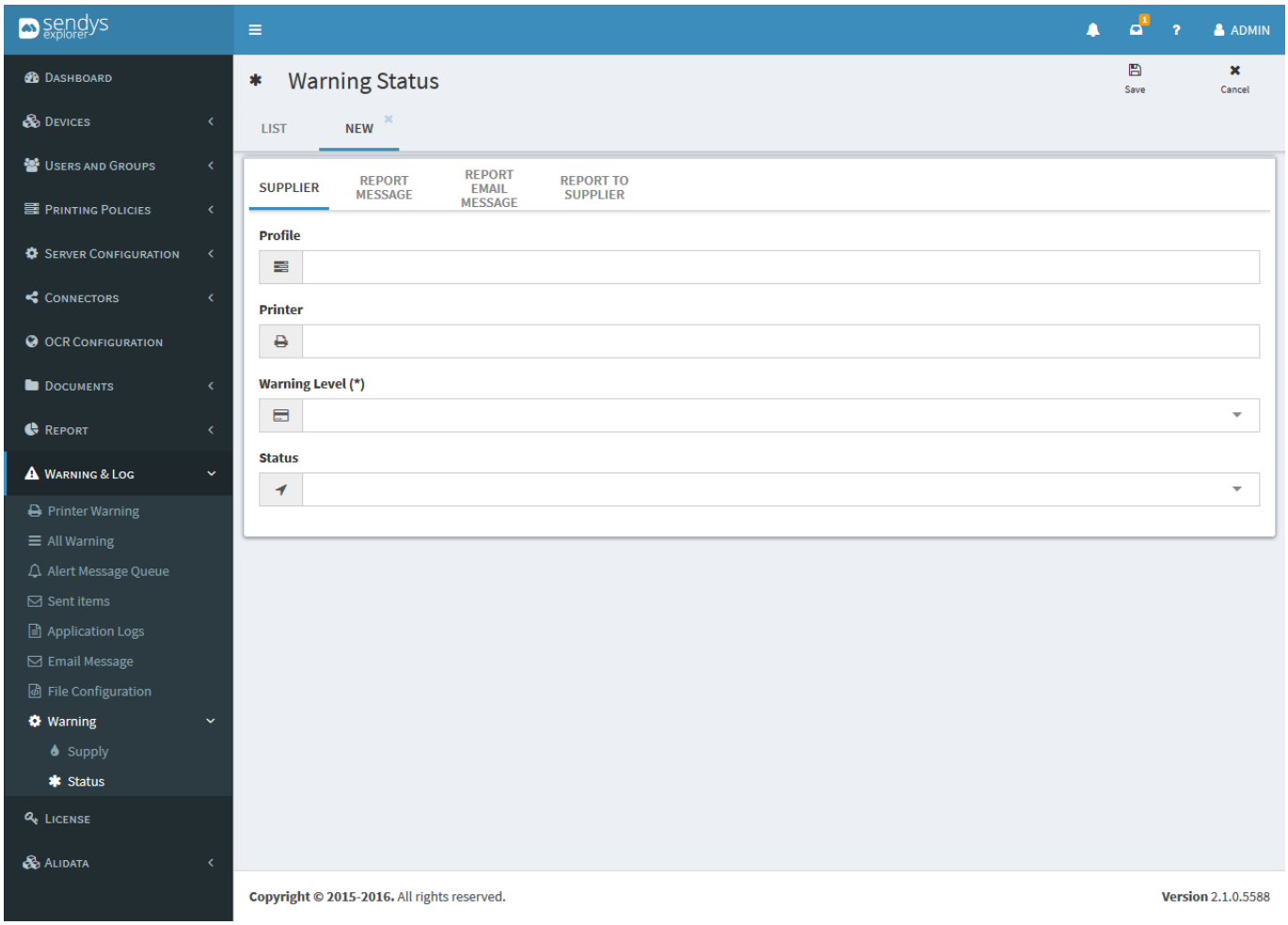


Fig. 399 - Warning status–report message

REPORT EMAIL MESSAGE

1. Click on **Report Email Message** submenu.
2. Configure this to generate an email message(warning) to send an email automatically.

Name	Details
Report as Email	Select the option to use this as an email message.
To	Send to field.
Bcc	Send Bcc field.
CC	Send Cc field.
Subject	Define the subject for the email.
Message	Define the message content for the email.

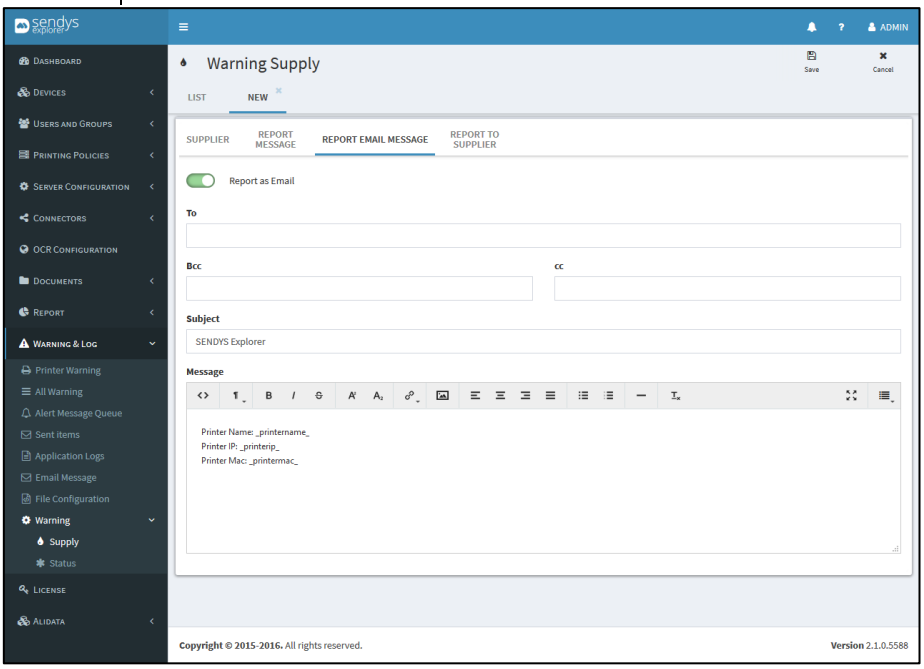


Fig. 400 - Warning supply configuration - report email message

REPORT TO SUPPLIER

1. Click on **Report Message** submenu.
2. Configure this to generate an email message(warning) to send an email to the supplier automatically.

Name	Details
Auto Require Supply	Select the option to use this as an email message to supply.
To	Send to field.
Bcc	Send Bcc field.
CC	Send Cc field.
Subject	Define the subject for the email.
Message	Define the message content for the email.

Click **Save** to apply or **Cancel** to cancel the actions.

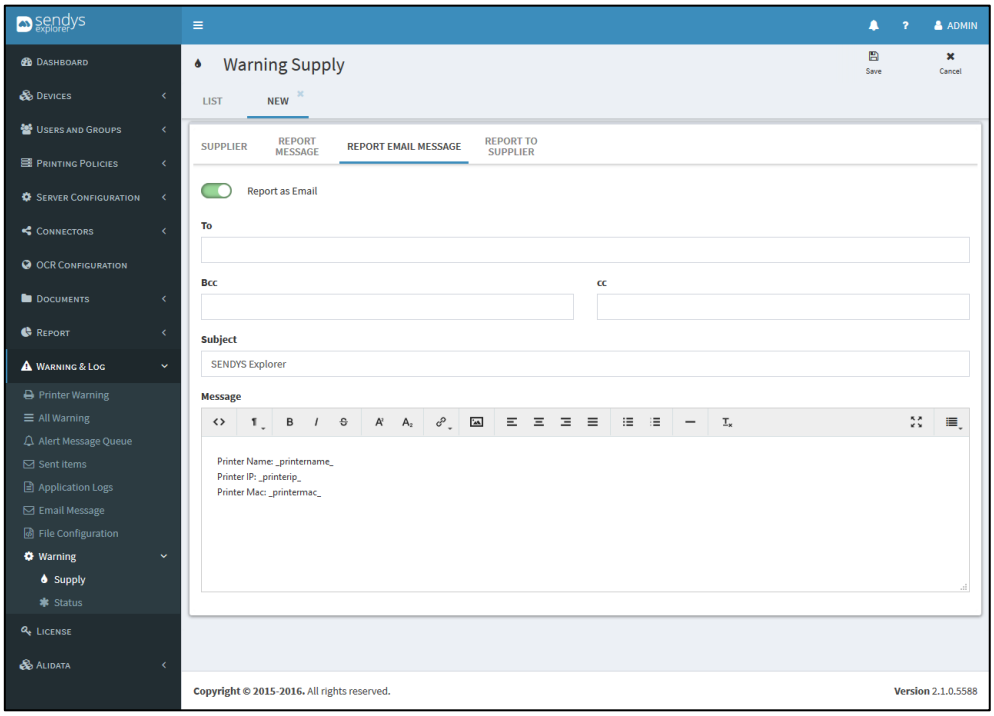


Fig. 401 - Warning supply configuration - report email message

PRINTER WARNING LOG

All status warnings configurations detected are logged with date that the status warning was found and when was resolved. The logs can be reviewed on the menu, **Warning & Log** > **Printer Warning Log.**

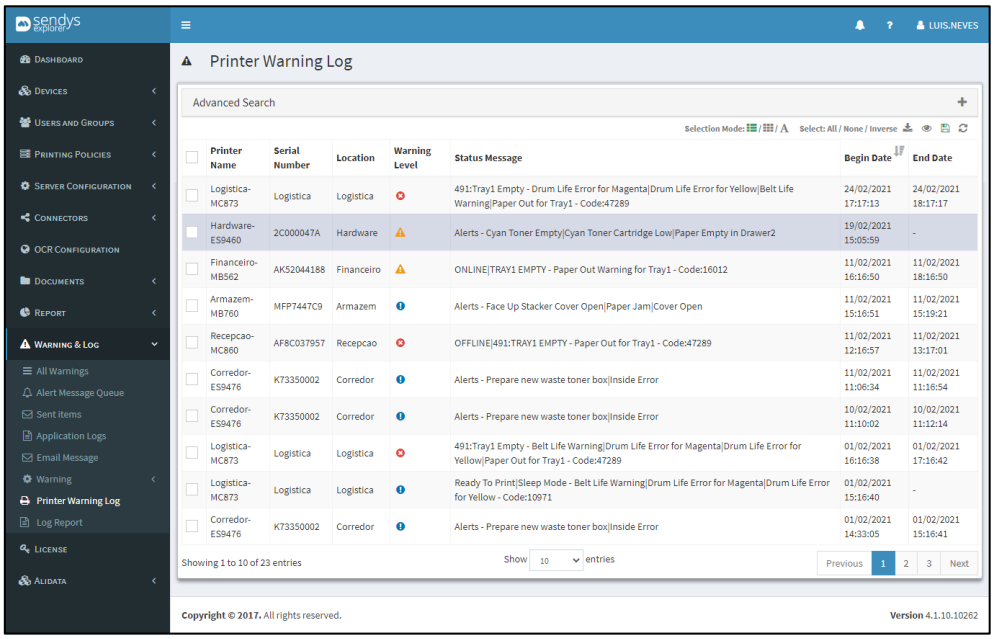


Fig. 402 – Printer Warning Log – Output Manager Printer Warning Logs

All logs have the following information:

Name	Details
Printer Name	Device Sendys Explorer name that recorded the warning.
Serial Number	Device Serial Number.
Location	Configured device location.
Warning Level	Warning level of caught warning.
Status Message	The device warning message.
Begin Date	Date when the warning was logged.
End Date	Date when the warning was resolved on the device.

Table 65 - Printer Warning Log

LOG REPORT

All actions on the Output Manager are logged and can be reviewed on the menu, **Warning & Log** > **Log Report**.

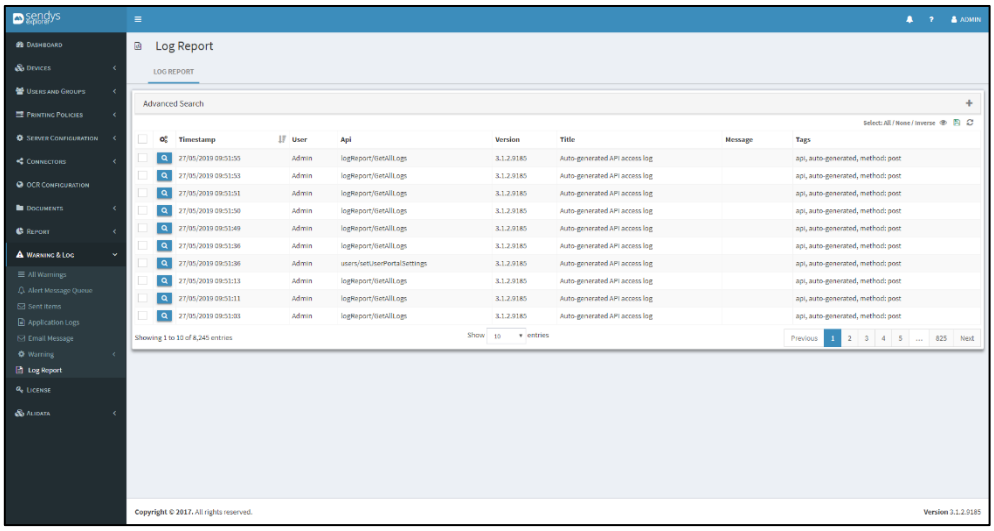


Fig. 403 – Log Report – Output Manager log report

All logs have the following information:

Name	Details
Timestamp	The date and time when the action was called.
User	The user that called the action.
Api	The Action called.
Version	Output Manager version when the action was called.
Title	Title of the log.
Message	Message of the log.
Tags	Method type of the action and log tags

Table 66 – Log Report

LICENSE

ADD

ONLINE ACTIVATION

1. Click on **License**.
2. Click on **Add**.
3. Insert the **Serial Number**.
4. Select "**Online activation**".

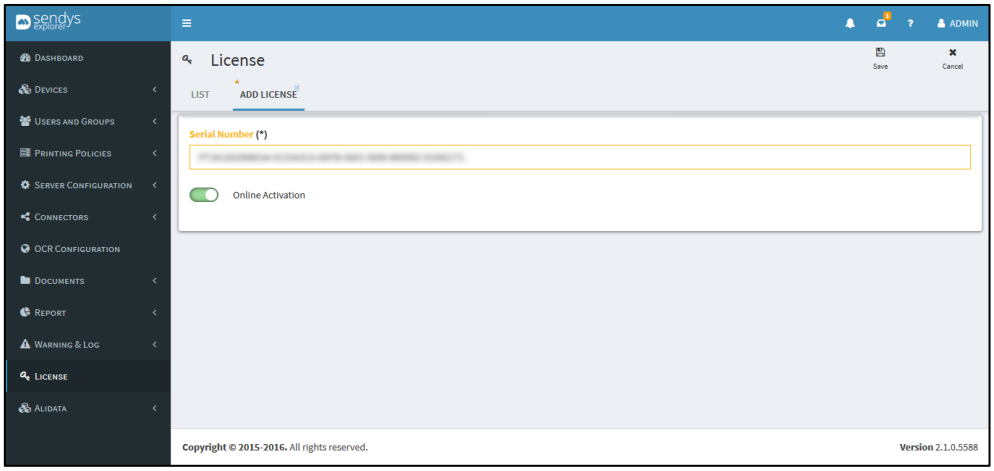


Fig. 404 - Online Activation

5. Click in "**Save**".
6. Confirm the license activation, if there is any error, please contact to support@sendysexplorer.com.
   Note: For online activation to work all you need is access to the internet.

OFFLINE ACTIVATION

1. Click on **License**.
2. Click on **Add**.
3. Insert the **Serial Number**.
4. Unselect "**Online activation**".

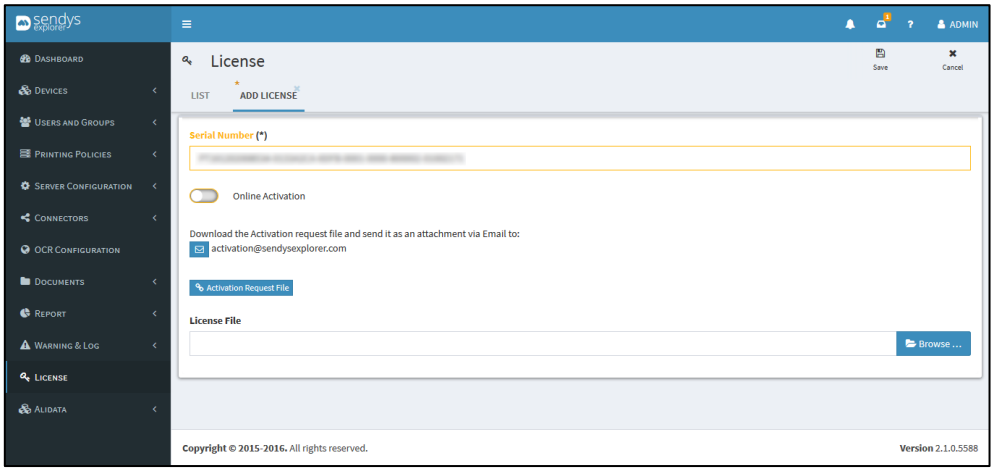


Fig. 405 - Offline Activation

1. This will create a file and will also give you a destination email
2. Click on **Activation Request File** to download the created file.
3. Send the file ***xxxxxxxxx*_company_lic.txt** as email attachment to activation@sendysexplorer.com.
4. You will receive the offline activation as one attachment, download it to your server.
5. Click on **Browse** and select the downloaded **License File**.

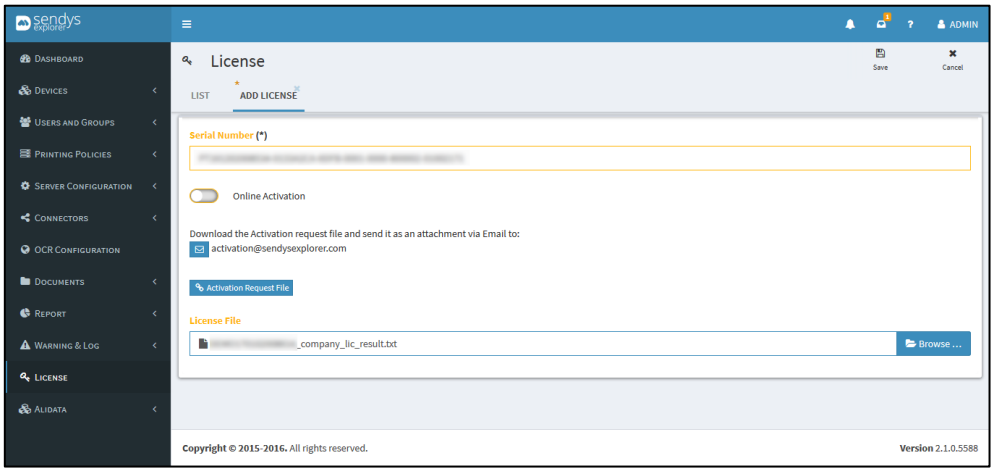


Fig. 406 - Offline Activation

6. Click on **Save**. This will activate the product.
7. If there are any errors, please contact support@sendysexplorer.com.

UPDATE

1. Click on **License > List**.
2. Click on **pencil icon** to Update the **License**.
3. Update the **Serial Number**.

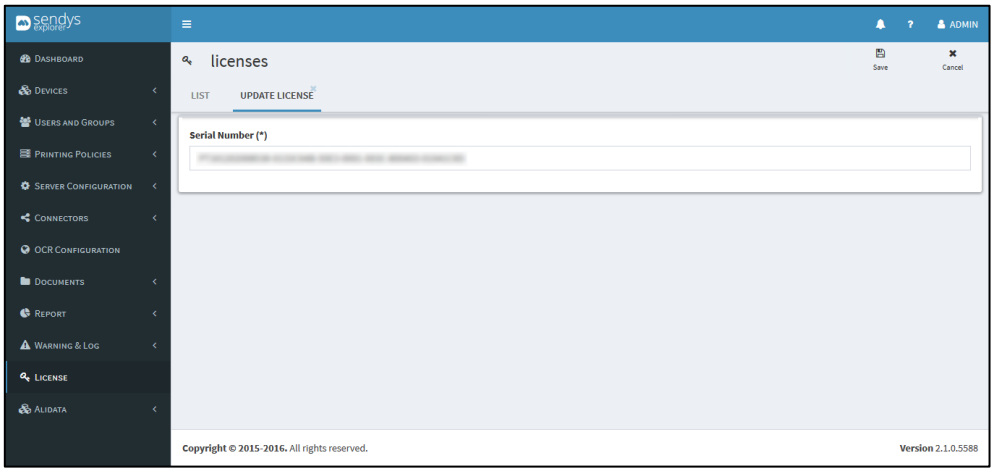


Fig. 407 - Update License

4. Click in "**Save**".
5. Confirm the license update, if there is any error, please contact to support@sendysexplorer.com.
   Note: For the update to work you need is access to the internet.

REMOVE

ONLINE DEACTIVATION

1. Click on **License > List**.
2. Click on **deactivate icon** to Remove the **License**.
3. Select "**Online deactivation**".

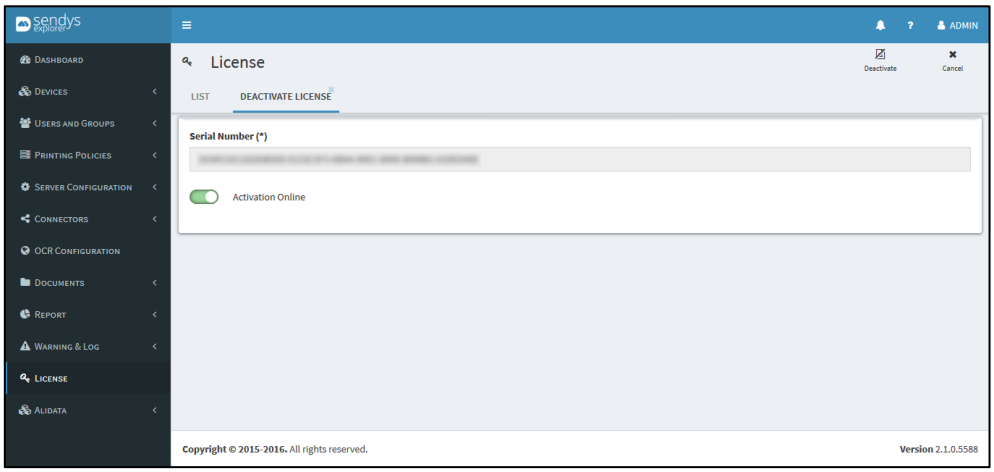


Fig. 408 - Online Deactivation

4. Click in "**Deactivate**".
   Note: For online deactivation to work all you need is access to the internet.

OFFLINE DEACTIVATION

1. Click on **License > List**.
2. Click on **deactivate icon** to Remove the **License**.
3. Unselect "**Online deactivation**".

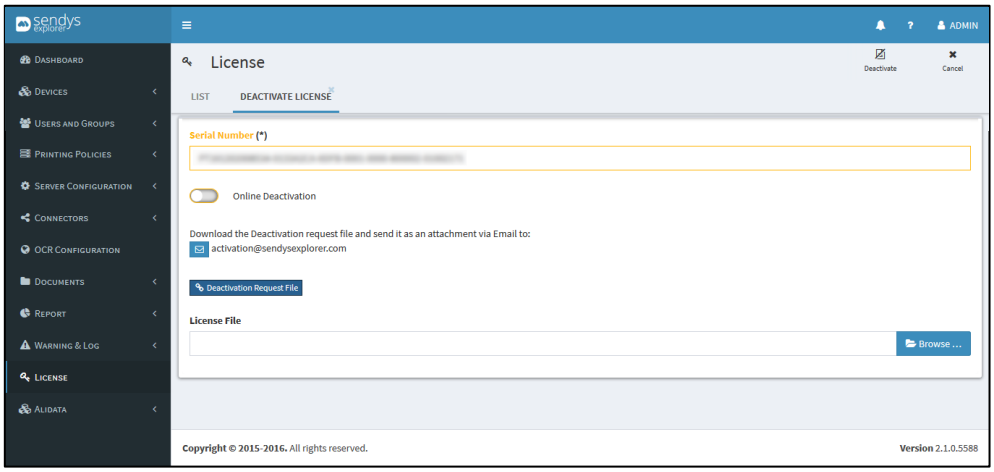


Fig. 409 - Offline Deactivation

4. This will create a file and will also give you a destination email.
5. Click on **Deactivation Request File** to download the created file.
6. Send the file ***xxxxxxxxx*_company_lic.txt** as email attachment to activation@sendysexplorer.com.
7. You will receive the offline activation as one attachment, download it to your server.
8. Click on **Browse** and select the downloaded **License File**.
9. Click on **Save**. This will activate the product.
10. If there are any errors, please contact support@sendysexplorer.com.

CHECK FOR UPDATES

To update the **manuals** and to update the **translation** of SENDYS Explorer, you just need to:

1. Click on **Licence**.
2. Select **Check for Update**.

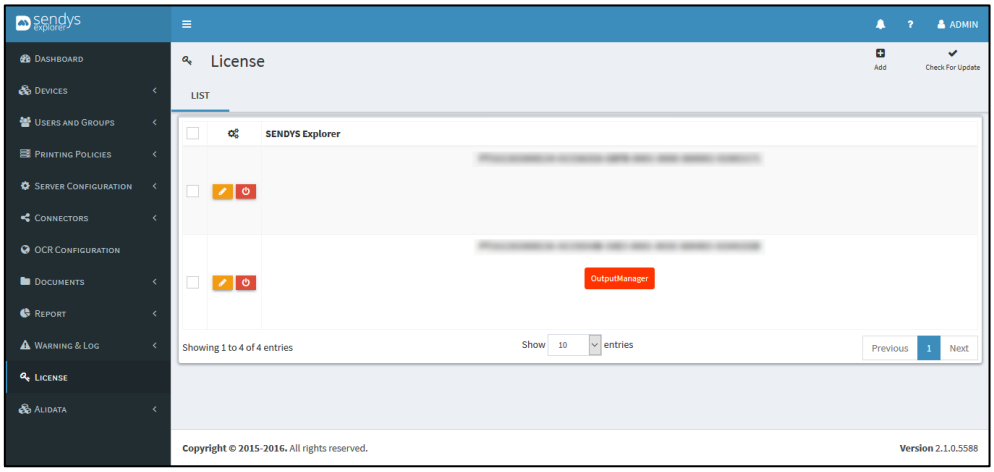
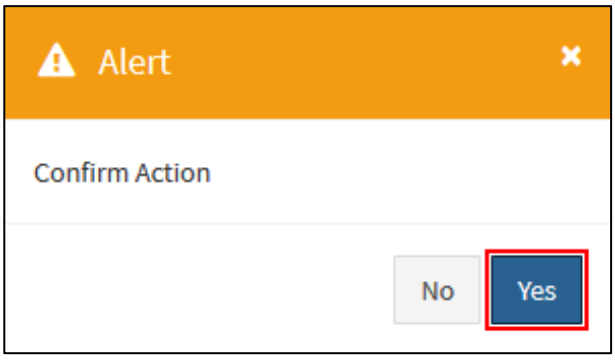


Fig. 410 - Update manuals and translation

3. Click **YES** to confirm update.



4. **Fig. 411 - Update manuals and translation**

ALIDATA

FILE CONFIGURATION

3. Click on **Warning & Log** menu.
4. Click on **File Configuration**.
5. **Select Application** option to load the xml on the **Log Content**.

This view shows the file configurations for each Select Application.

Click **Save** to apply or **Cancel** to cancel the actions.

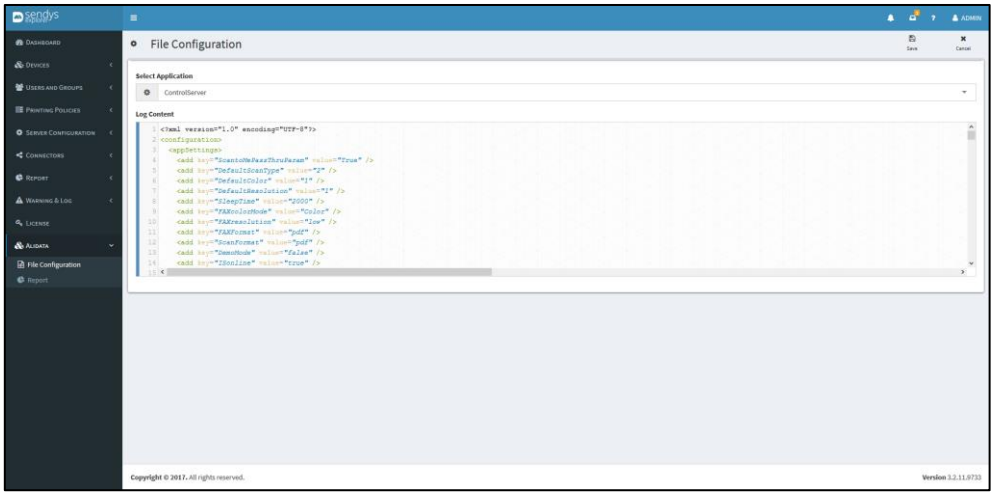


Fig. 412 - File configuration

REPORT

1. Click on **Alidata** menu
2. Click on **Report** menu.

On this view **Reports** can be managed. They can be cloned, edited, hide, show or deleted one by one or with a selection.

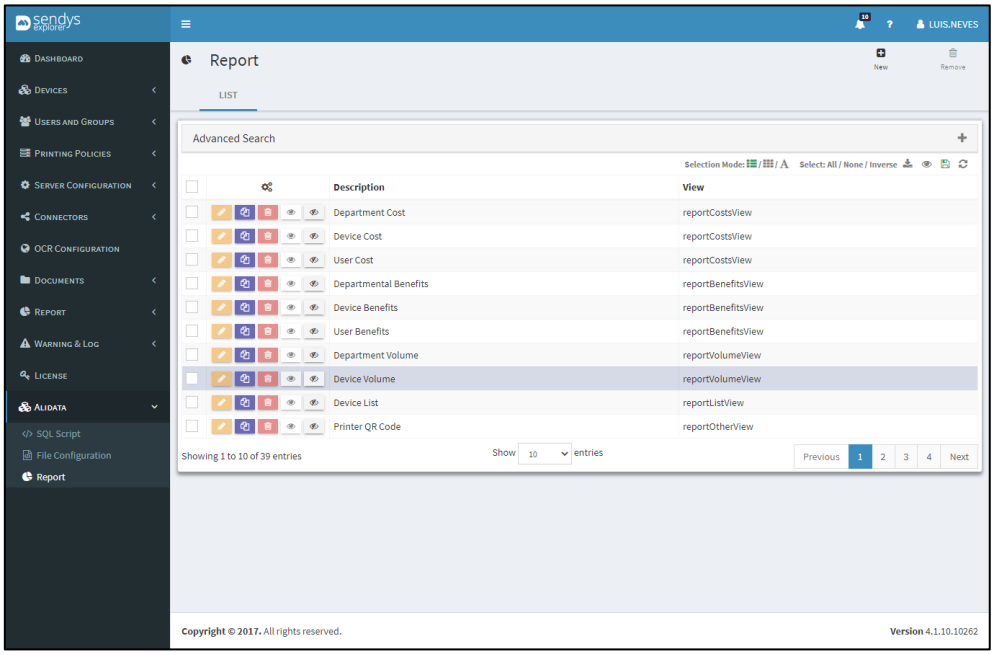


Fig. 413 - Alidata - Report

NEW REPORT

1. Click on **New** button.

Clicking on **New** to add a new contact individually on the platform and fallow the next configurations:

Name	Details
View	Select the view where the new report should be saved.
I18n Key	Insert the name for the new Report.
Report Data	Paste the report XML that contains the layout. You can clone this information from the base reports and edit it from there.
Report Parameters	Choose the parameters that should be used on the report.

Table 67 - New Report Details

Click **Save** to save the configurations on adding new contact or **Cancel** to cancel the insertion.

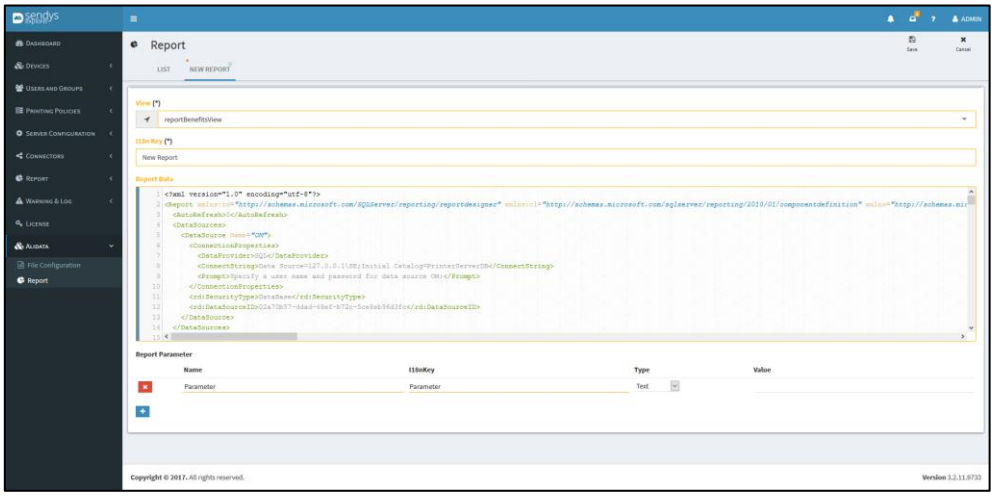


Fig. 414 - New Report Details