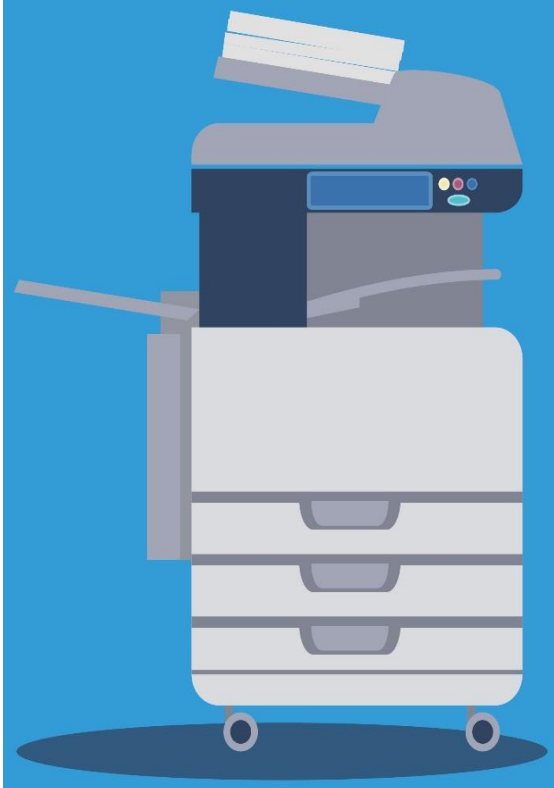
EIDAS SCAN USER MANUAL

Software executed into HP equipment

English



eIDAS Scan is a product by **GiDoc Integral**, a company specialized in digitization, digital object optimization and document management.

GiDoc Integral is committed to **R&D.**

We study the needs of each client, and we value a customized solution in systems of capture and digitization of any type of data for subsequent treatment in document management systems.

More than **15 years** of experience in the digitization and document management sector guarantee our solutions.

www.gidocintegral.com
Tel. 91 196 86 67
info@gidocintegral.com

DIGIFACT: Application integrated within HP equipment for the certified digitization of supplier invoices.

AUTHENTIC COPY: Application integrated into HP scanners, generating an authentic electronic copy for the AAPP of documents received on paper with the same legal validity as the original document.

OUTSOURCING SERVICE: Outsource your documentary processes. We take care of digitizing and managing the documentation of your company. We are specialists in digital processes with the most advanced and specialized software on the market.

1. INTRODUCTION TO EIDAS SCAN

eIDAS SCAN is an application integrated into HP MFPs for the management of document flows prepared for compliance with **eIDAS (electronic IDentification, Authentication and trust Services) regulations.**

Generates documentation flows. Worflows can be created by associating them with a button.

Separates documents by barcode, assigns metadata, or enters specific parameters.

Introduction of metadata, electronic signature and timestamp.

Sending documents based on their typology to different systems via FTP, SFTP, SMB or HTTPS.

Option to make the signature later, in other programs via HTTPS.

eIDAS Scan is a European Union regulation on electronic identification standards and trust services for electronic transactions within the European Single Market.

1.1. Download and Settings

The installation of **eIDAS SCAN** from **GIDOC INTEGRAL** in the HP equipment, is done following the **HP Command Center** software.

Only authorized distributors can manage the configuration centrally and remotely and, are those who can facilitate access through an IT administrator user to **HP Command Center**.

1.2. MFP Requirements

The MFP will need to have the firmware updated to the latest version.

1.3. Work Scheme

There are two user roles with different permissions: administrator and user.

User Role

Click the workflow button to start.

Flow settings are displayed and some data can be modified or allocated before starting the scanning process.

Administrator Role

Certificate management.

Create or edit flows.

Assign the button name and, the users or roles that will have it available.

Click accept.

2. APPLICATION START

The **HP MFPs** home screen displays the icons of the installed programs; in this case we see **eIDAS Scan**. The screen may defer depending on the multifunctional model.

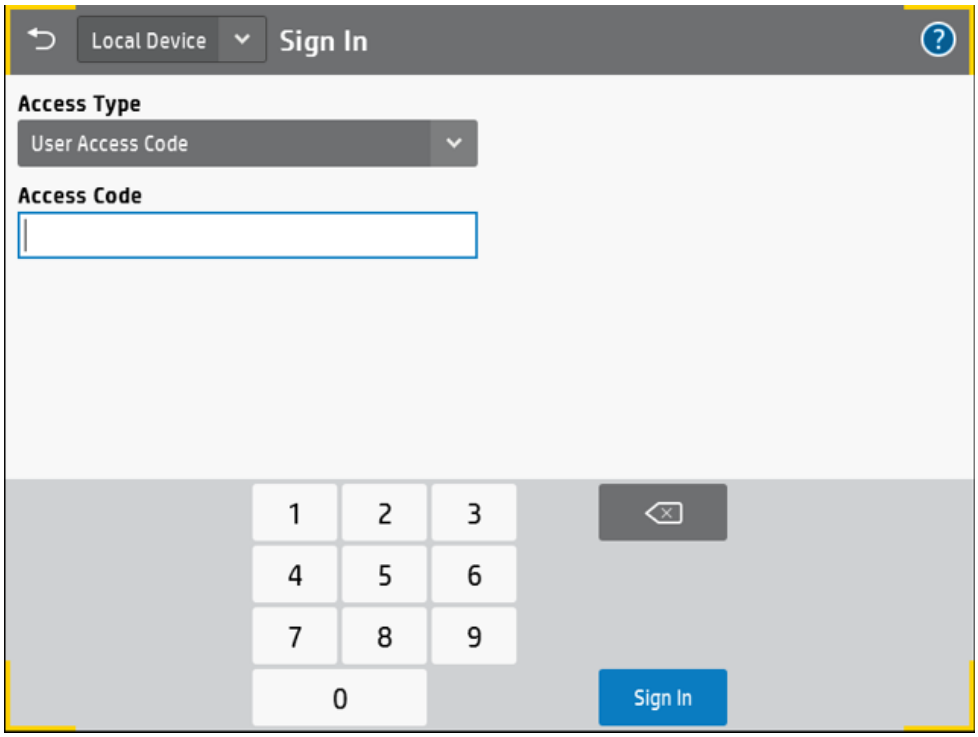
eIDAS Scan allows to configure different actions depending on the user of the equipment. In order to be able to access with a user other than *Guest*, we will have to identify ourselves.

In every equipment there is the option to identify the work user.

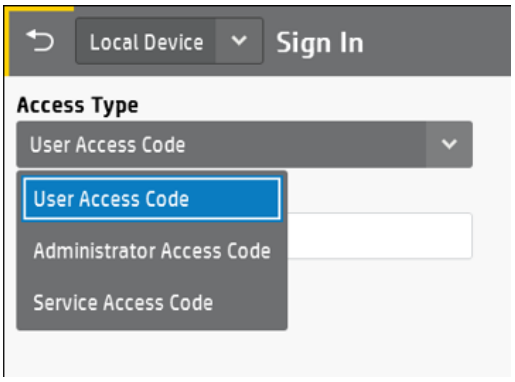
If you want to access options assigned to a specific user (not the guest user or Guest), you must identify yourselves in the usual way:

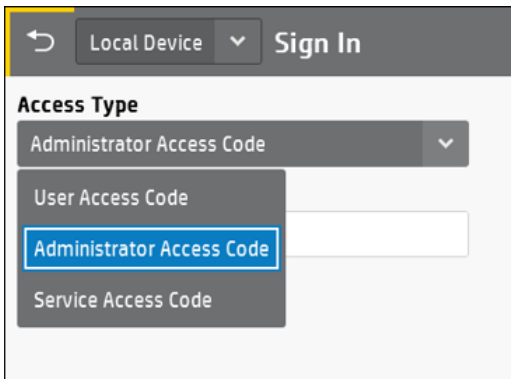
Reset	Logs out the active user by switching to guest mode.
Sign In	**User identification**. Processes can be configured so that they can only be run by specific users. This option will allow us to change user.

To change users, you can access the **Registration** option**.** A form will be displayed asking for the access code, each user has only one role associated with it:

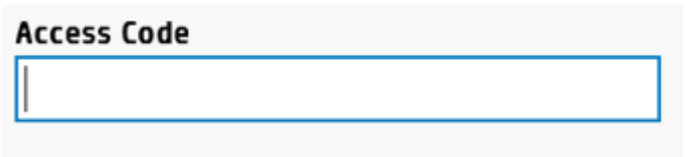


Access mode must be selected: only users with administrator role will access **elDAS Scan** with the administrator role:





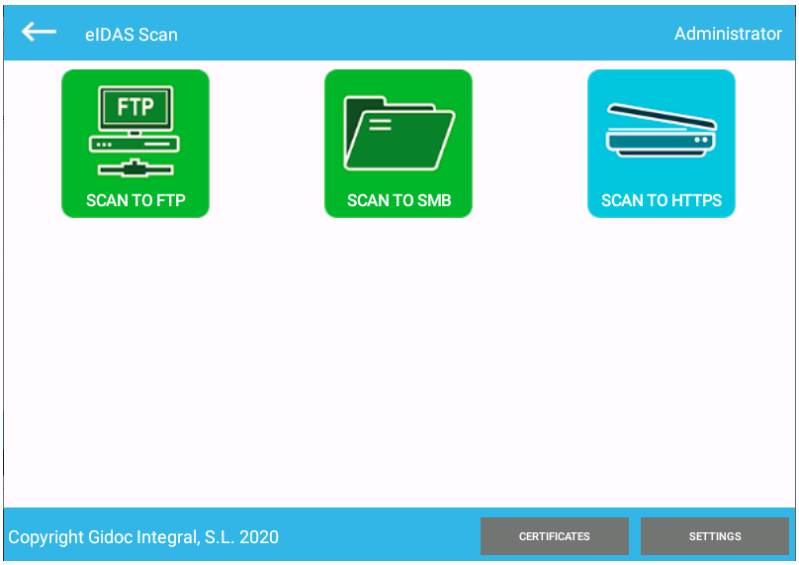
Once you have selected the appropriate option enter the **access code:**



Once the user is identified (or logged in as Guest), we can access **eIDAS Scan** by clicking on the button on the screen:

Once logging in, the options defined for that user are available along with those defined for all users.

The main screen contains buttons that allow you to execute the defined flows. An example of a configuration with three buttons is shown below:

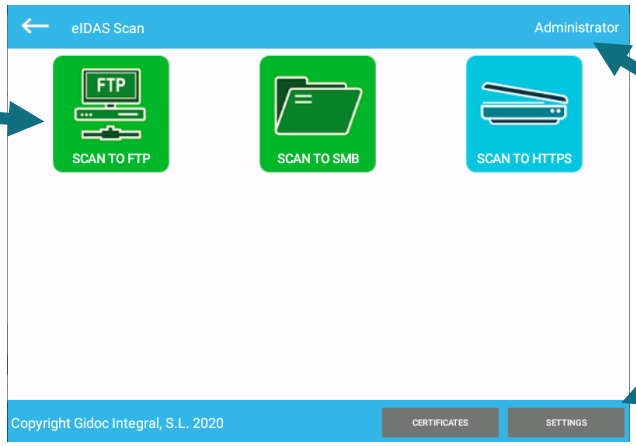


3. ACCESS

The available options of the administrator user are the same as for the rest of the users.

Once you have entered the access code, you will see the following screen:

At the central section you there are the buttons that allows to execute defined flows.



Administrator

User name you 've logged in with.

SETTINGS

Settings button (only available for administrator users).

SETTING button is available for all the users.

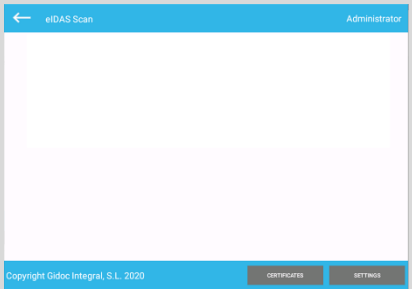
If a user with administrator role accesses this option, the App configuration form will be straight opened.

If the user is not the administrator, it will show up a form asking to fill in name and password.

The first time you logg in after installing the App, user and password are empty.

To take into account...

If when you access you can't find any button at the central it could be due to the fact that no flow has been defined or because the logged-in user doesn't have permissions to execute any flow.



Important

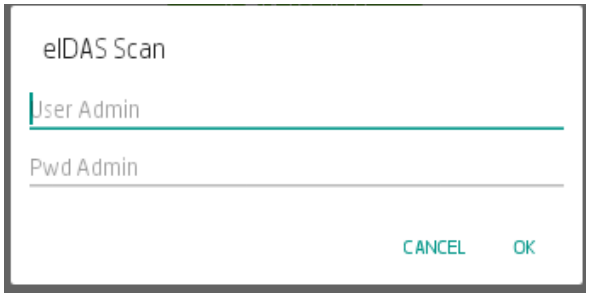
To exit the app, click the **button above**

You will find it in all system screens at the left top corner

4. SETTINGS

When you access to the program with HP MFP'S administrator user, you can access to Settings form straight through the button at the right bellow corner.

If the user is not the administrator, it will show up a form asking to fill in name and password.



4.1. Settings Screen

Once you access the Settings button, this screen will be displayed:

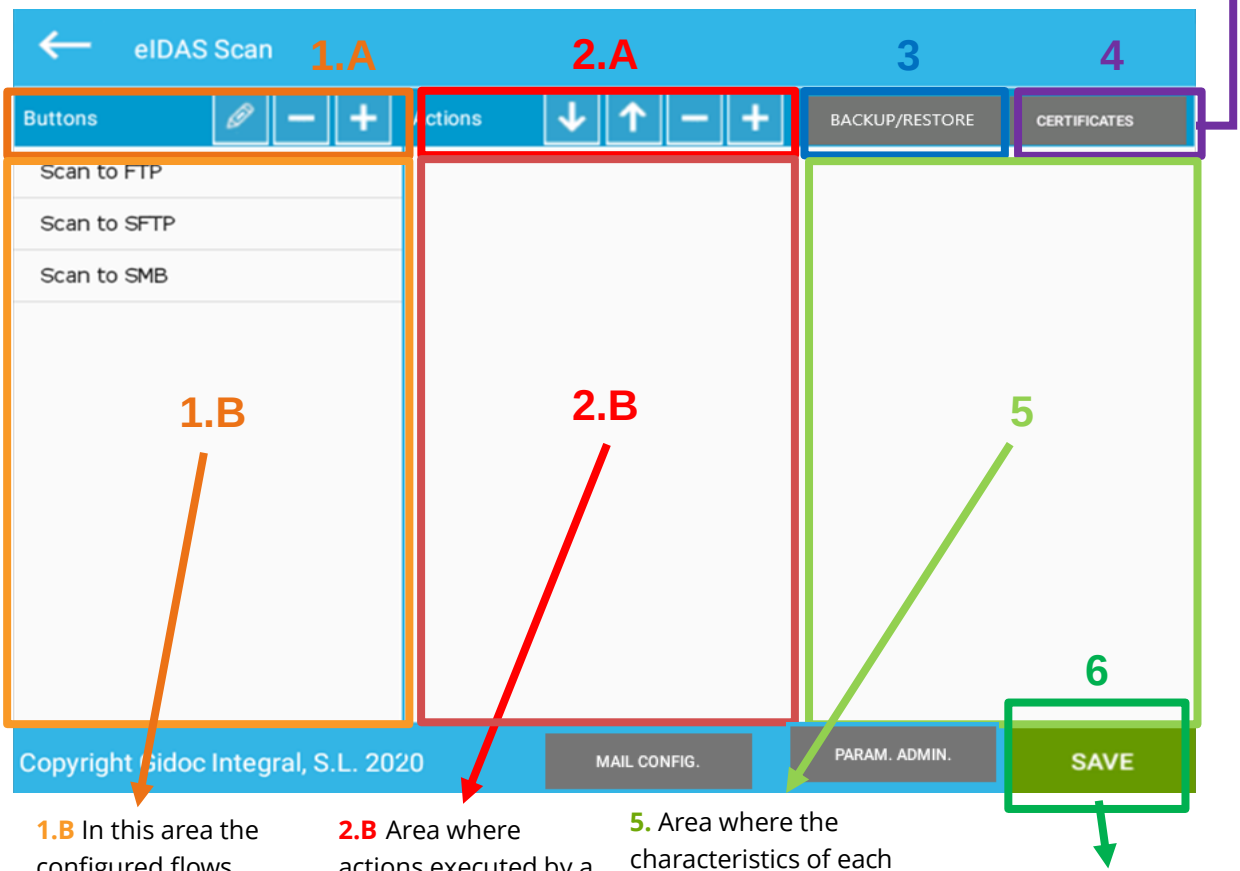
1.A Here you (creation, modification and deletion). More information in the **'Flow Settings'** subsection.

2.A. Management of the actions that implement the flows. More information '**Settings actions**'.

3. Button to make a copy (backup) or restore the default settings (restore).

More information in **'Back-ups Management´.**

4. Button to access **certificate** management**.** More information in the section **'Certificate management**'.



1.B In this area the configured flows listing is displayed, and the flows might be selected or edited.

2.B Area where actions executed by a workflow are displayed. When an action is selected, its configuration is displayed in **zone 5**.

5. Area where the characteristics of each action selected in zone 2.B are displayed More information in the **'Action Settings'** subsection.

6. Button to save the chosen settings. More information in the **'Button Settings'** subsection.

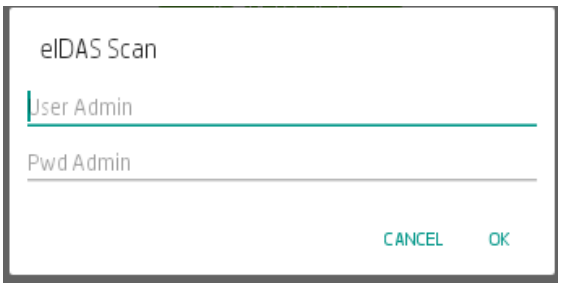
With the button 'MAIL CONFIG' you can access to the email shipment settings.

With 'PARAM. ADMIN.' button you could define user and password to a user who is not administrator can access to setting.

4.2. Access to settings for a no administrator user

When a user who is not the administrator wants to access settings, must identify as a user with administration permissions.

At the time accessing to **'PARAM. ADMIN.'** a form to fill in credentials will be displayed.



Once they have been informed you could access to Settings with the user and password configured.

When accessing this option for the first time after it has been installed, you do not have to enter any value in the user's name and password fields, just click on the OK button.

eiDAS Scan allows you to set a user name and password to access the system configuration without being an administrator user. eiDAS Scan does not have a user management so that you can only define a name and password to access the administration options without being an administrator of the multifunctional.

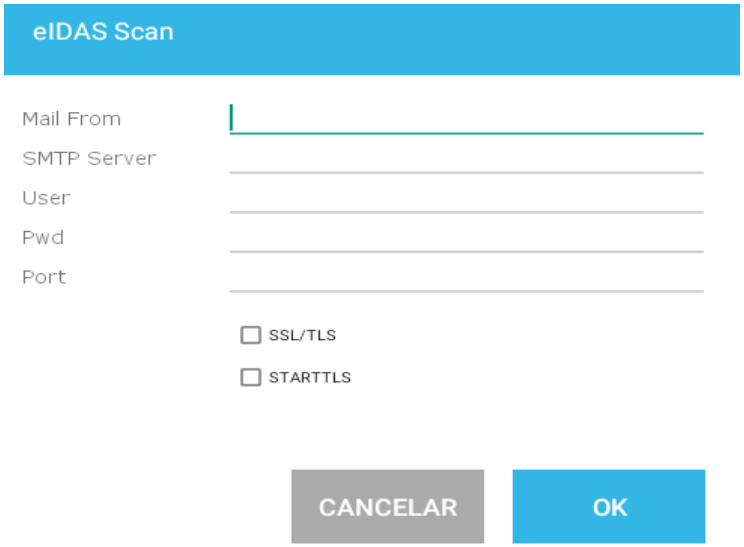
When accessing this option, it is not necessary to inform the current user and password, you only have to inform the new user and password.

4.3. E-mail configuration

When you click 'MAIL CONFIG', a form to inform about email account details used by the System, will be displayed.

The mailing protocol is SMTP (Simple Mail Transfer Protocol).

The setup screen is:

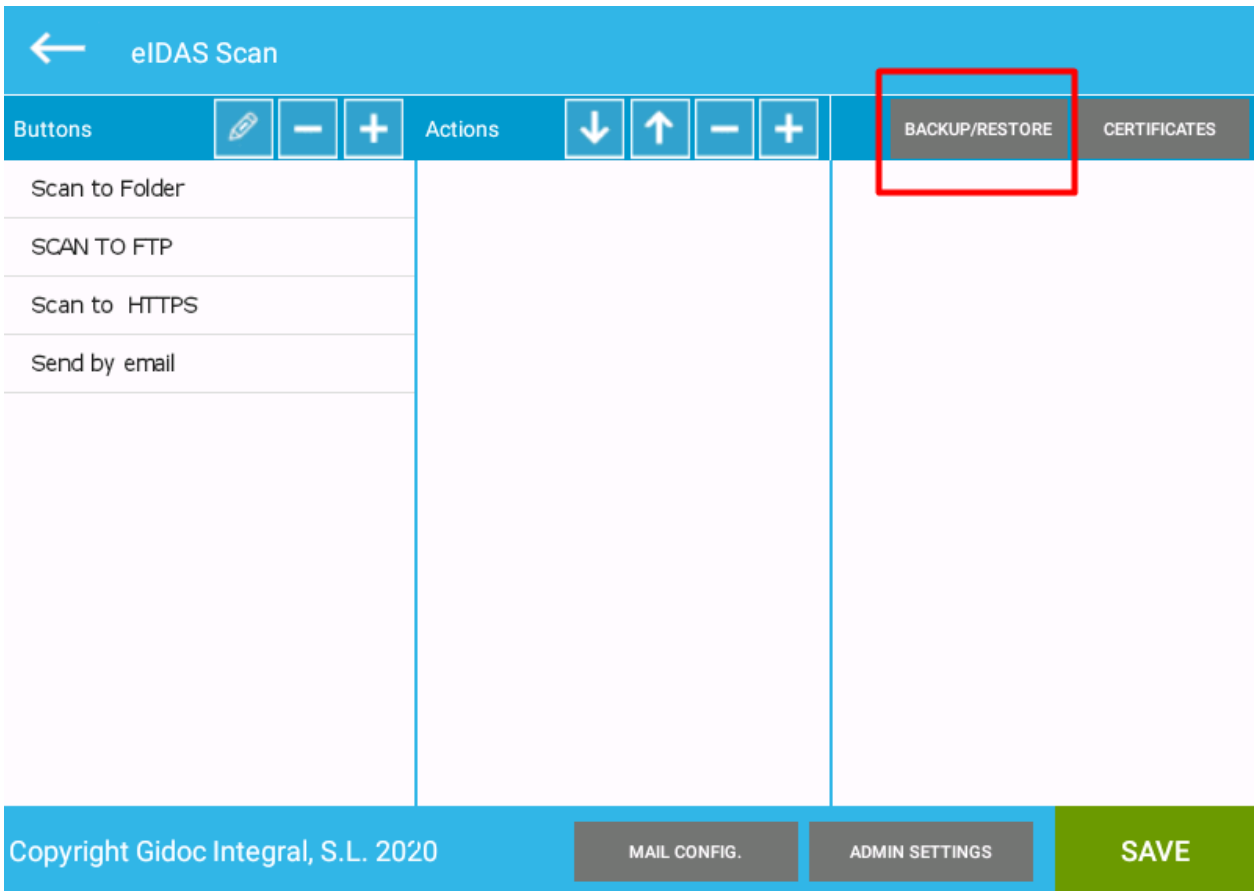


Next details must be filled in:

- Mail form: e-mail address from which messages will be sent.
- STMP Server: IP address or mail server name.
- User: Name of the user of the email account to be used for sending mails.
- Pwd: User's password.
- Port: Port. Normally port 25.
- Select one the following protocols:
    - SSL/TLS
    - SARTTLS

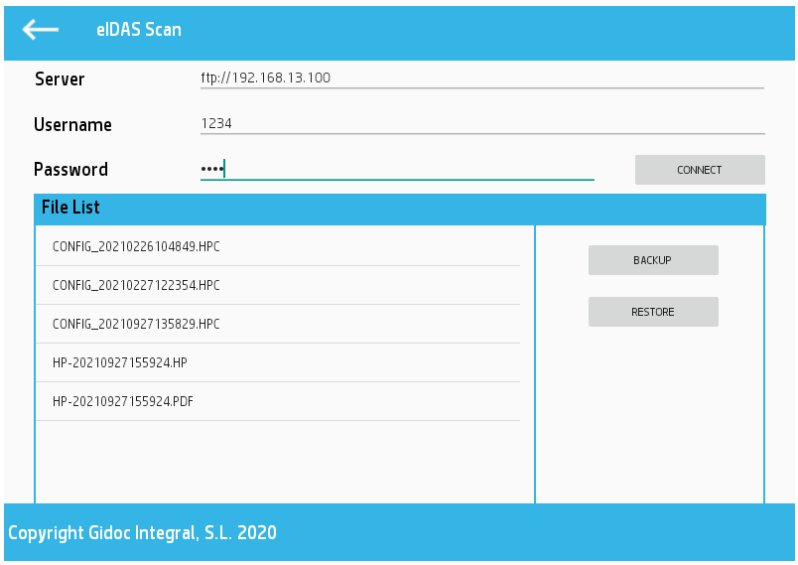
4.4. Back-up management

'Backup/Restore' button allows backing up the entire configuration (*backup*) and to restoring the entire configuration from a previous export (*restore*).



This option will allow us to configure the solution in a computer, save it in a file and import this configuration in other computers later.

Settings form in the picture below:



First step to import or export is to inform the remote location where we want to save or retrieve the settings.

Available protocols to access a location:

- **FTP:** File Transfer Protocol.
- **SFTP:** Secure File Transfer Protocol.
- **SMB:** samba 2.x or 3.0 (Shared folders protocol).

  HTTPS: web service installed on a server (if you are interested, please contact us to download the service definition).

Next details must be filled in:
The protocol to be used must be written in lower case followed by two slashes and the server address:

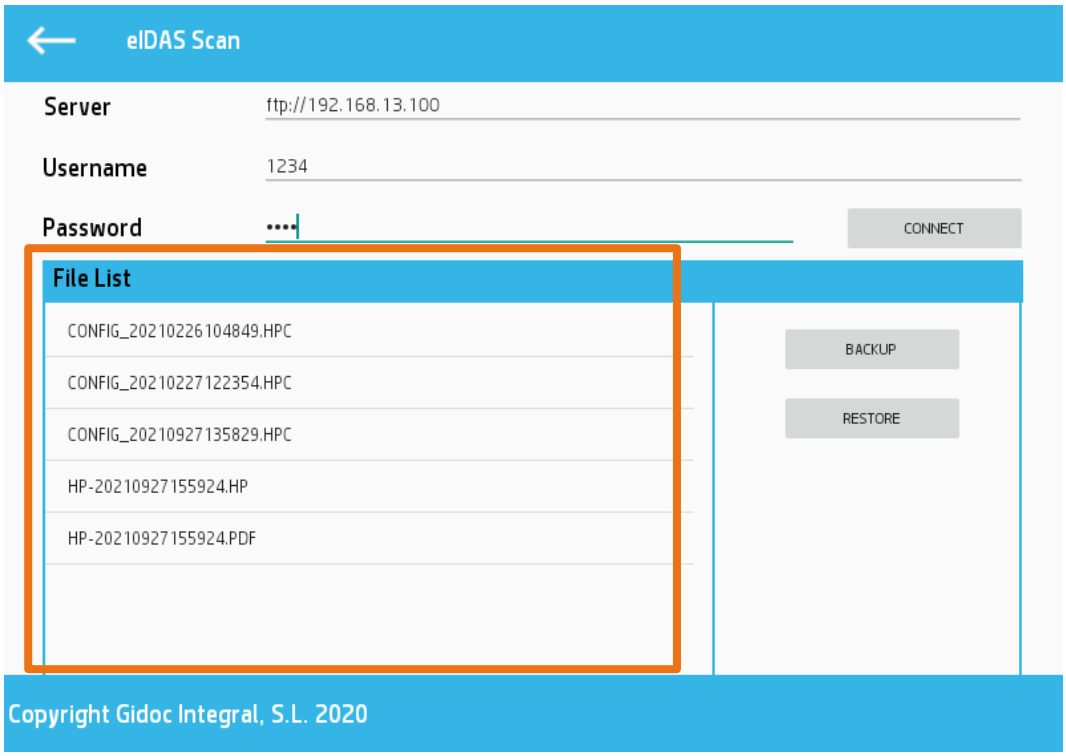
- ftp://server
- Sftp://server
- Smb://server/SharedFolder
- https://server

Where it says "server", server IP address must be informed (its format is 192.168.69.128) or the server's name.

- User: the user accessing the resource must be entered.
- Password: the user accessing the resource must be entered.

Once the three fields have been filled in, the CONNECT button can be accessed and **a list of the files** in the indicated location will be displayed in **zone B.**

Below is an example where the three checkboxes have been filled in, the connect button has been pressed and several configuration files are displayed:



Once the connection has been configured and you have checked that it's working properly, you can click 'backup' to create a backup copy.

Once the backup copy has been done it will pop up the next message:

A single file will be created containing all the App configuration information except for the digital certificate files. The name of the generated file shall be in the format:

CONFIG_DATE.HPC

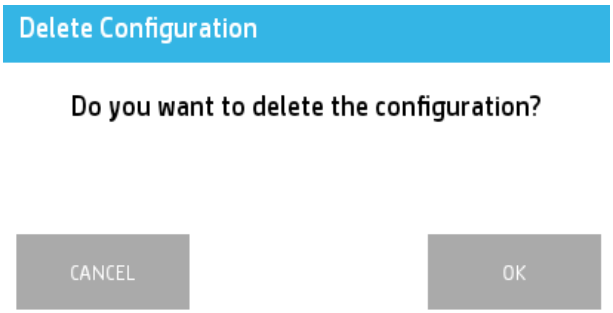
The date consists of the year, month, day, hour, minute and second without spaces.

Important

It is not possible to export a certificate saved in the multifunctional.

If you want to import a configuration, you must first configure the connection, list the remote configurations, select a configuration and finally access the 'Restore' button.

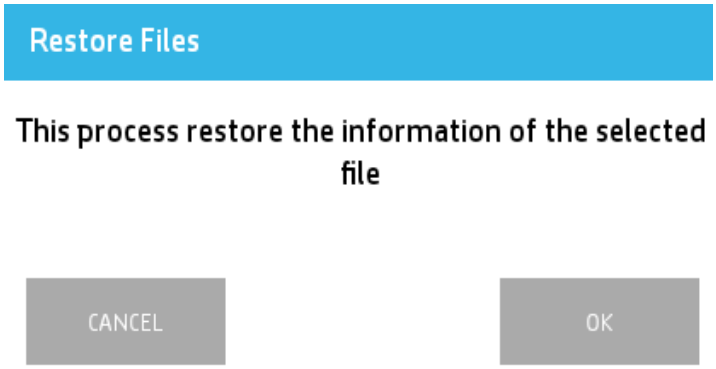
When this option is executed, the next form is displayed:



In case the '***CANCEL***' option is selected, the import process **adds** all the data from the import file to the current setup. If the restore process is performed using a backup of the current configuration, all buttons will be duplicated.

In case the '***OK***' option is selected, all defined flows and certificates are deleted and are **overwritten** with the data from the import file.

If you accept, the following confirmation message will appear because it will modify your current configuration.



If the cancel option is selected, the process is canceled.

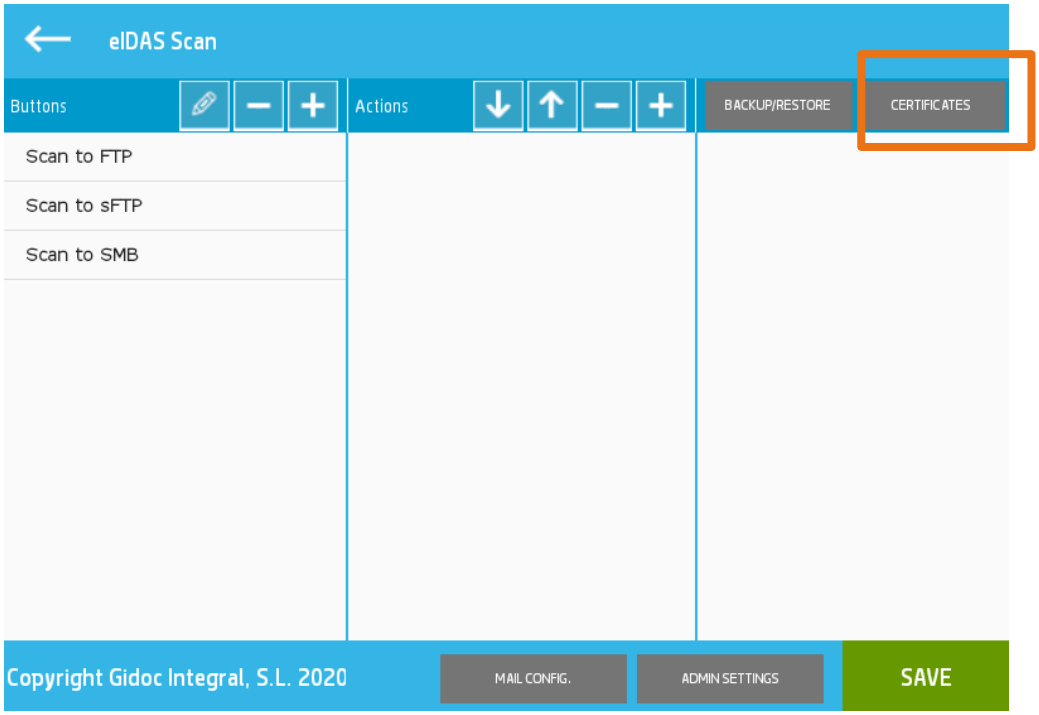
Finally, the message that will be shown when the process has been successfully completed will be the following:

When the import process of a configuration containing a digital certificate is executed, prior to executing the import process, the digital certificates must be saved in the import folder with the same name that they had in the process of incorporating the certificate.

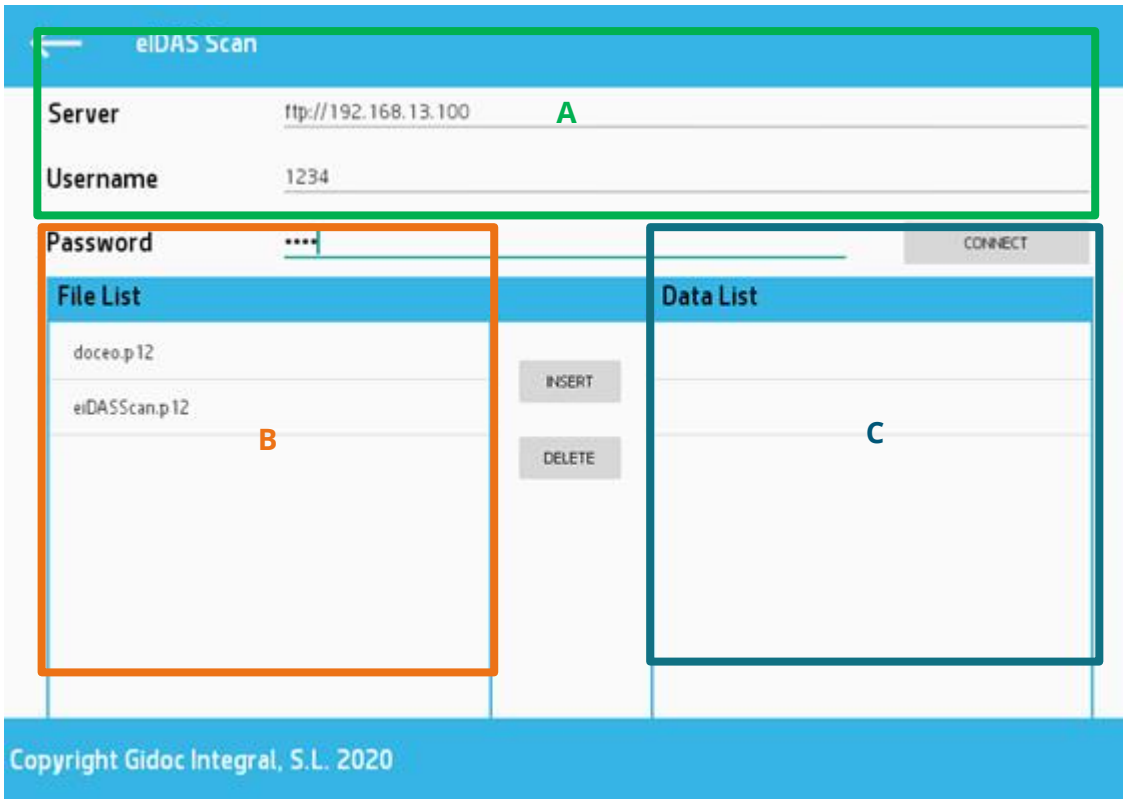
4.5. Certificate management

If you want to activate a digital signature action, you must first import the digital certificate you want to use.

To import or delete certificates on the MFP's, must access to 'CERTIFICATE' button in the main display:

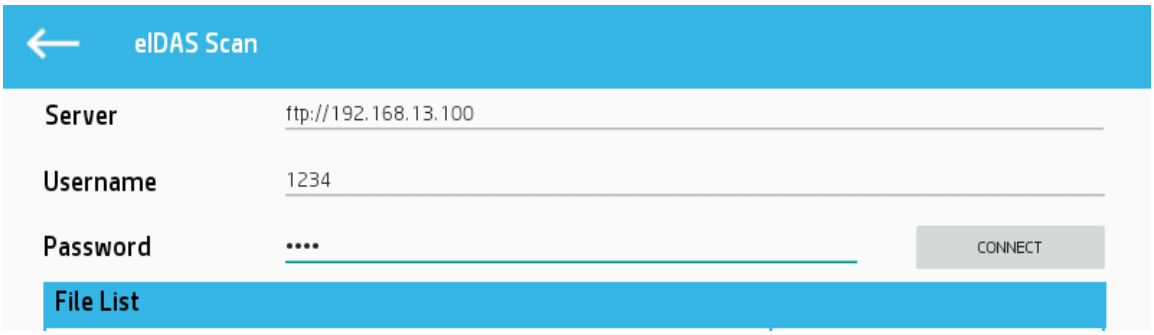


'CERTIFICATES' links to the next setting display:



The certificates used in the flows are saved in the App. To incorporate a certificate within the application, the access data to the server where the digital certificate to be incorporated is located must be provided.

At the top of the display, A area, there are three fields that allows to introduce credentials to access an external System:



These are the protocols available to access an extern location where the digital certificates are (the access options are the same as those for the backup):

- **FTP:** File Transfer Protocol.
- **SFTP:** Secure File Transfer Protocol.

- **SMB:** samba 2.x 3.0 (Shared folder protocol).
- **HTTPS:** web service installed in a server (if you are interested, please contact us to download the definition of the service).

In order to incorporate a certificate, the protocol to be used, the location of the external service, the user and the password to access the protocol must be provided. This information is reported with the three fields of zone A:

- Server:

The protocol to be used must be written in lower case followed by two slashes and the address of the server.

- ftp://server
- sftp://server
- smb://server/SharedFolder
- https://server

Where it says "server", server IP address must be informed (its format is 192.168.69.128) or the server's name.

- User: the access user to the resource must to be entered.
- Password: the access password to the resource must to be entered.

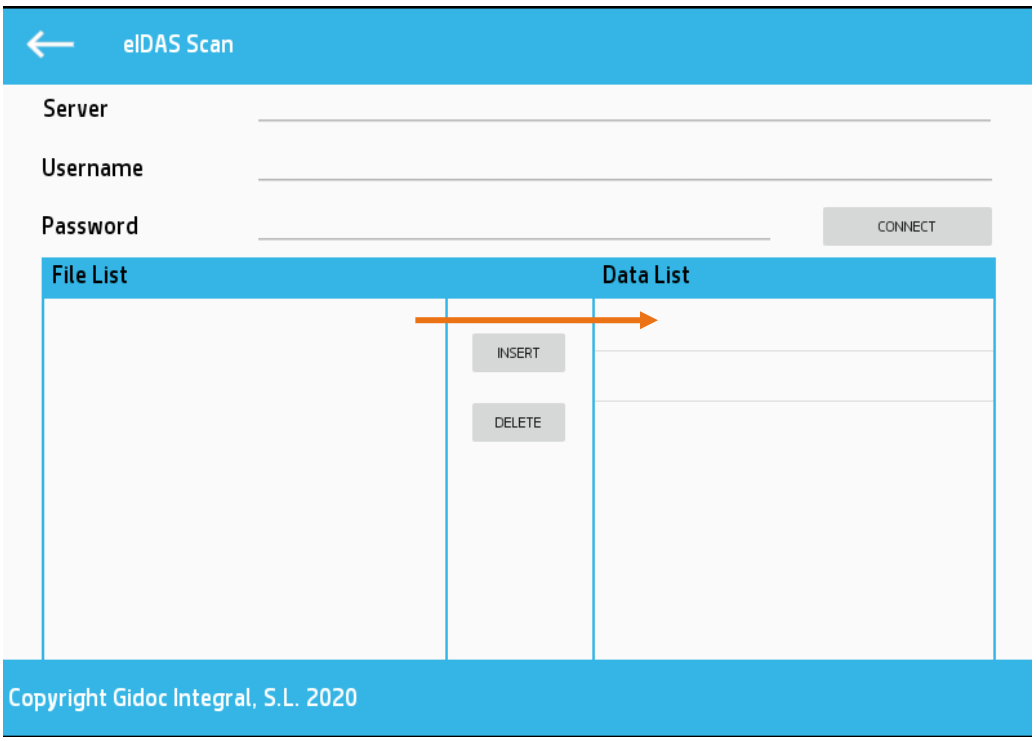
Once these three fields have been informed, you could click "**CONNECT**" and the **fields list** in the indicated location, will be displayed **in zone B** (as all the files will be displayed, may be some of them is not a digital certificate).

The digital certificates must be in the inbox which has been configured in the user account of each protocol (can't navigate in subfolders).

Take into account...

the list, all the fields of the server are displayed, you must select the ones with **.pfx** or .**p12** extension.

At **zone C** (tagged as **Data list**), the certificates imported in the App are displayed.



To add a certificate, simply select it from the list of files on the left and click on the **INSERT** button.

To **delete a certificate** loaded in the application, select it in the data list and click on the **REMOVE** button.
It is not possible to export a certificate incorporated in the system.

Once a certificate has been deleted or added it will be needed to click SAVE button to save the configuration.

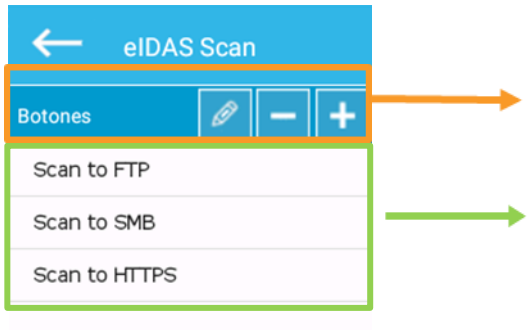
When a certificate configuration is saved, no validation process in the digital certificate is run (it is not checked if it is really a digital certificate, if it is a qualified certificate, if it has signing permissions, if it is expired, if it is revoked, etc).

There is no limitation on the number of certificates to be incorporated into the system.

Once a certificate is incorporated into the system, it can be removed from the server where it was at the time of import; the certificate is copied into the MFP.

4.6. Flows configuration

At the at the left top there are all the options available to manage the flows and the flows list created:



Available **options** to flows management.

List of created flows. When accessed for first time to setting this zone has no content.

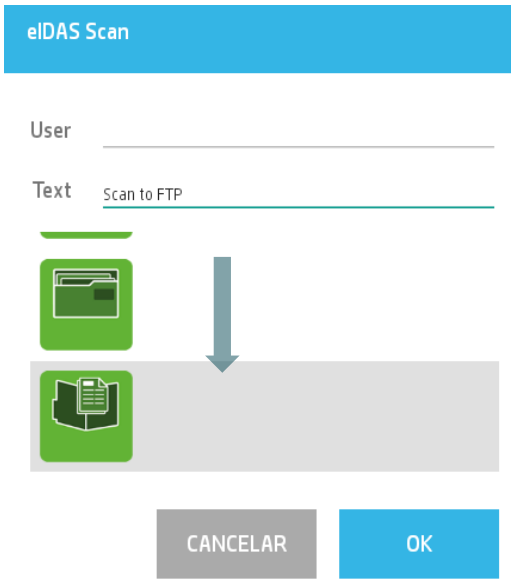
The buttons available are:

Add a new flow

Delete a Flow (It Will delete the configuration selected from the flows list)

Modify a flow

When create flow option is selected the next form will be displayed:



User: User name which could access to the button. In case of omission, it will be public for all users.

Text: write the flow name (it will be displayed under the icon).

Buttons: can be scrolled dawn to see all the buttons available and choose the one that best fits the work process to be performed with the flow.

Once the user who will have access to the flow has been defined, the name of the flow and a button has been selected, we can press **OK** to save the flow or **CANCEL** to discard the defined flow.

Note that...

Thirty icons are available representing document destinations, devices, ...

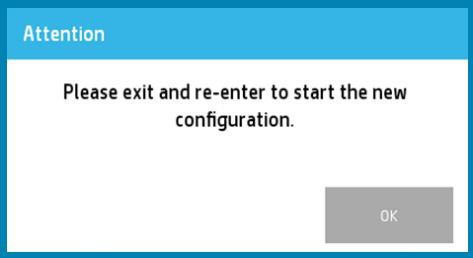
All the icons are in thirty colors (total of 90 icons available).

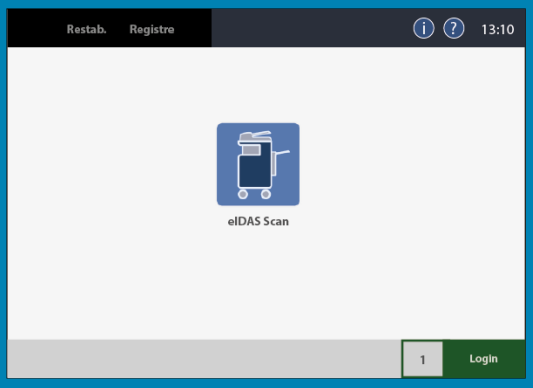
For better comprehension, we recommend reading the examples of use.

Important

The creation or deletion of a flow is not automatically synchronized within the start screen.

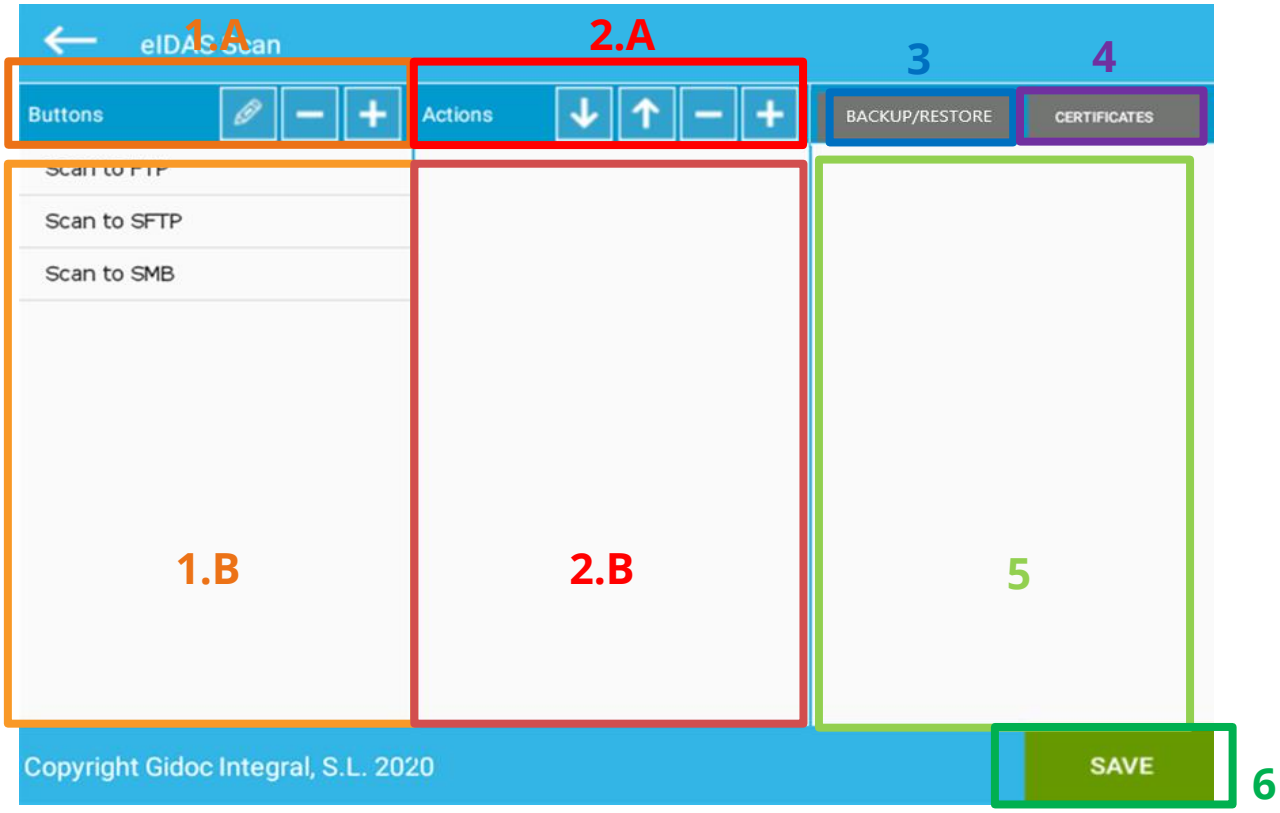
If you want to immediately display a button and its configuration, you have to log out and log back in.





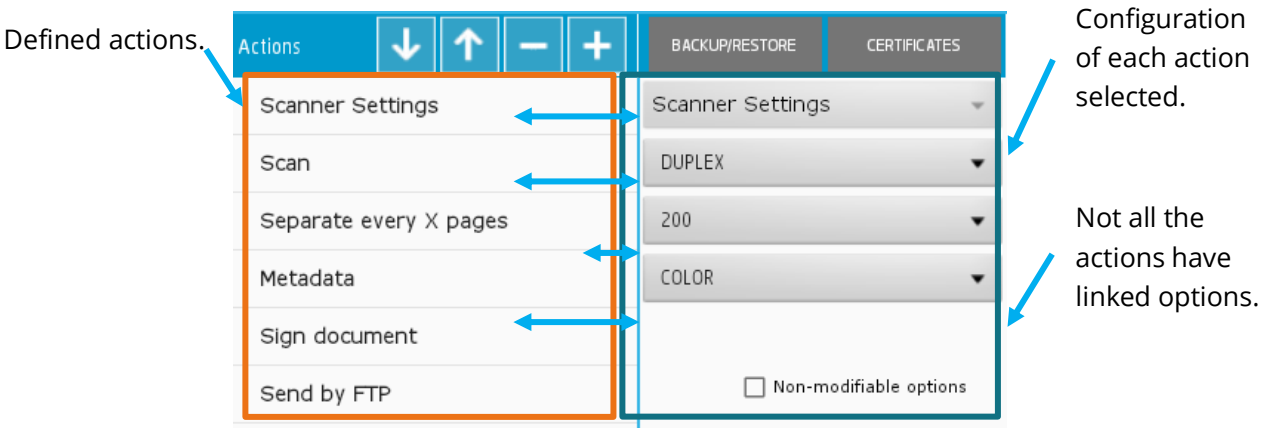
4.7. Actions configuration

This section describes how the actions contained in each defined workflow are assigned and configured.



Once a botton has been created, it must be selected in **Zone 1.B.** and actions can be added using option in Zone 2.A.

Once an action has been added and/or configured, **zones 2.B** and **5** will vary its content:



The available options to manage actions:

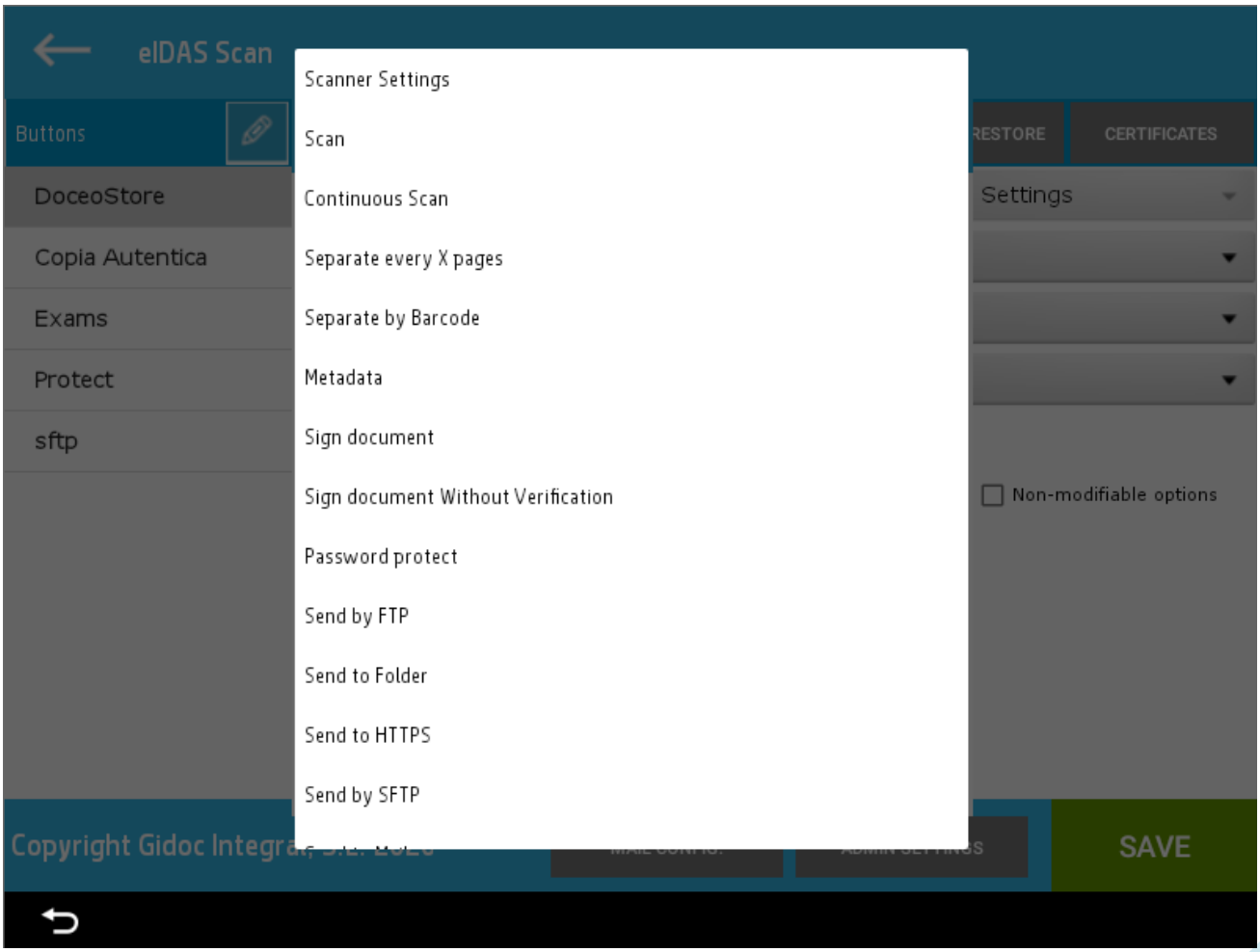

Insertion of a new action. A drop-down list of all actions is displayed.


Delete a configured action.


The actions will be carried out in the configured order.


The up and down arrows allow you to move the selected action up or down in the list of created actions.

The actions list is dispayed like this:



It is possible to scroll through the list with the help of the bar on the right side of the list in order to choose the required action.

Below are several tables with the actions available to be added to a flow, grouped according to their nature:

	Digitization actions	
	Action	Function / Characteristics
A	Scanner parameters.	Definition of the scanning mode.
B	Continuous Scanning.	Option to scan documents where the pages will be captured by the sheet feeder and the flat surface.
C	Scanning.	Scanning action.

	Shapping actions	
	Action	Function / Characteristics
D	Separate every several pages.	Creation of documents with a fixed number of pages.
E	Password protection.	It is used to create password-protected PDFs so that the document is saved encrypted.
F	Separate by barcode.	Creation of documents based on the reading of a barcode and optionally assignment of the file name.

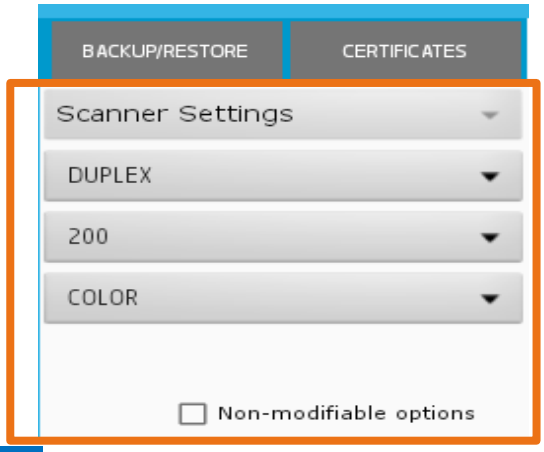
	Indexation actions	
	Action	Function / Characteristics
G	Metadata	User can manually enter metadata.

	Digital signature actions	
	Action	Function / Characteristics
H	To sign a document	Digital signature and optionally time signature of the generated PDF document.
I	Signing document without verification	To use non-recognized certificates.

Shipment actions		
	Actions	Function / Characteristics
J	Send by FTP.	Sending the document generated in a FTP server.
K	Send to a folder (SMB).	Sending the document generated with the samba protocol (shared folder).
L	Send to a HTTPS.	Sending the document generated in an external server by https protocol.
M	Send by SFTP.	Sending the document generated in a SFTP server.
N	Send by mail	Sending the document generated by mail

A. Scanner parameters

In this option can be defined digitalization mode to apply. Selecting this action these are the available options:



Duplex / Simple	If you want to scan only one side of the document (**Simple option**) or both sides (**Duplex option**).
200 / 300/ 400 / 600	Dots per inch (dpi). Administrative documentation can be read correctly with a resolution of 200. The higher the resolution, the more weight the document will have. A single page document at 600 dpi in color can take up several Mb.
Color | Gray | B/W	You can choose whether the document is to be scanned in **color**, greyscale (**Gray option**) or black and white (**B/W option**).
☐ Non-modifiable options	You can configure that the scanning parameters won't be modifiable by users.

Important

Always start a flow by adding an action such as 'Scan Settings', 'Scan' or 'Continuous Scan'.

In case the first action specified is not of this type, the error message will appear:

"Must specify a level 0.1 action"

B. Continuous scan

When the 'continuous scan' option is added to a workflow, the scanner will scan all existing pages in the sheet feeder or an existing sheet on the flat surface and then ask the user if they want to scan more pages. In case the user indicates that he/she wants to continue scanning, the process will be repeated (scan + ask the user if he/she wants to continue) until he/she indicates that he/she has finished scanning.

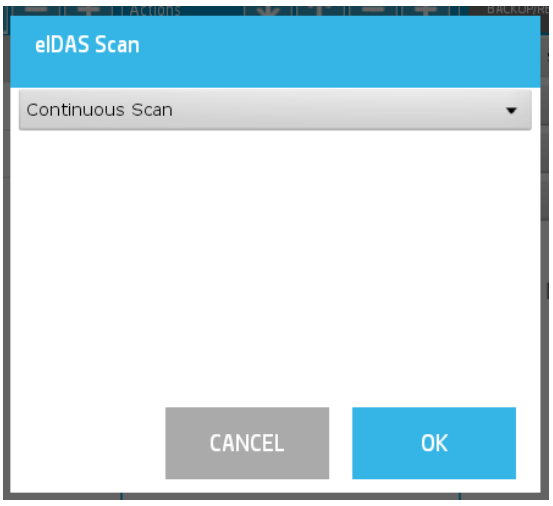
This option solves different problems:

1. Documents where pages must be scanned with the sheet feeder and flat surface, e.g. when a document has many A4 sheets and one A3 sheet.
2. Documents with many pages that cannot all be put into the sheet feeder and the sheets have to be deposited in the feeder more than once.
3. A document that has a sheet in bad condition and has to be scanned with the flat surface and the rest can be captured with the sheet feeder.

In some firmware versions of the devices, when first scanning a sheet with a flat surface, the system asks if you want to insert more pages (the working process is similar to the one described here), but in some firmware versions the option is not available.

Please note that when there are no sheets in the sheet feeder of the device, the MFP directly scans on the flat surface. If the document consists of a first page to be scanned with the flat surface, it is necessary that there are no sheets in the sheet feeder.

When this option is added, the following content is displayed in the action configuration area:



There is no additional option and nothing to configure.

C. Scan

Scan action.

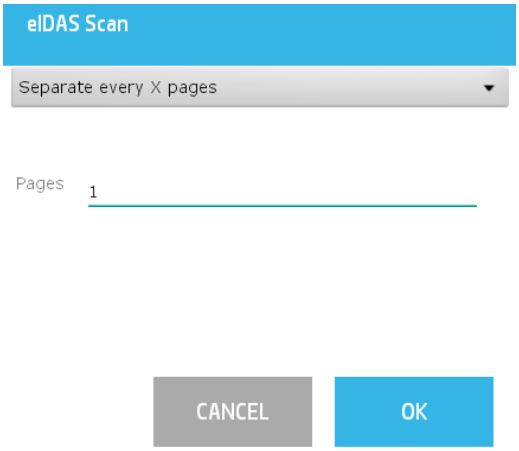
The scanning process will be based on the settings made in a 'scan settings' action and will ask if you want to insert more pages if there is a 'Continuous scan' action.

D. Separate every several pages

When digitizing documentation of a common typology (e.g. work orders or PPE applications), the documentation can be standardized and the number of pages of the form can be determined.

In these cases, you can use this action to scan several documents at once and have the system generate a PDF for each document automatically.

In this action you only have to indicate the **number of images** that each document will contain.



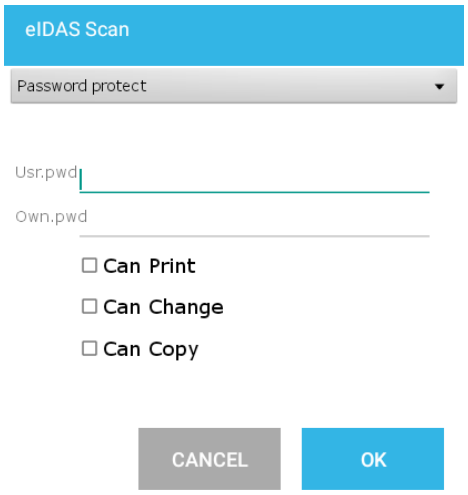
Example

Case: You want to digitize a form that only has one sheet with information on both sides, in this case it will be a duplex digitization.
In this case the value 2 must be assigned, as each sheet will have two digitized images (front and back sides).
Case: You want to digitize a form that only has one sheet with information on one face. In this case it will be simplex digitization and the value will be 1.

E. Password protection

This action is used to create password-protected PDFs so that the document is saved encrypted.

This action has two configuration options:



1) **Usr pwd:**

   Used to set a document **opening password** (also known as a **user password**). It requires a user to enter a password to open the PDF file to prevent unauthorised users from opening or displaying a PDF document.

2) **Own. Pwd**

   Used to set the owner password or permissions password (also known as **master password**). When the PDF document is created, you can *restrict functions such* as *printing, editing, copying PDF content,* etc.

   Once you have defined the master password for a PDF and want to change one of the permissions, this password will be required.

It is possible to set the following password configurations:

1. **Only the user password** (the second owner password field is not reported).

   In this case, whatever PDF viewer that allows to display password-protected documents will require typing the user password to open the PDF document.

2. **Owner password only** (the first user password field is not reported).

   In that case, the user will not be required to enter the password when opening the PDF document, but programs such as **Adobe Acrobat** (Adobe Reader does not have such an option),

require the owner's password when accessing the option to **change restricted functions** (print, edit, copy content, etc.).

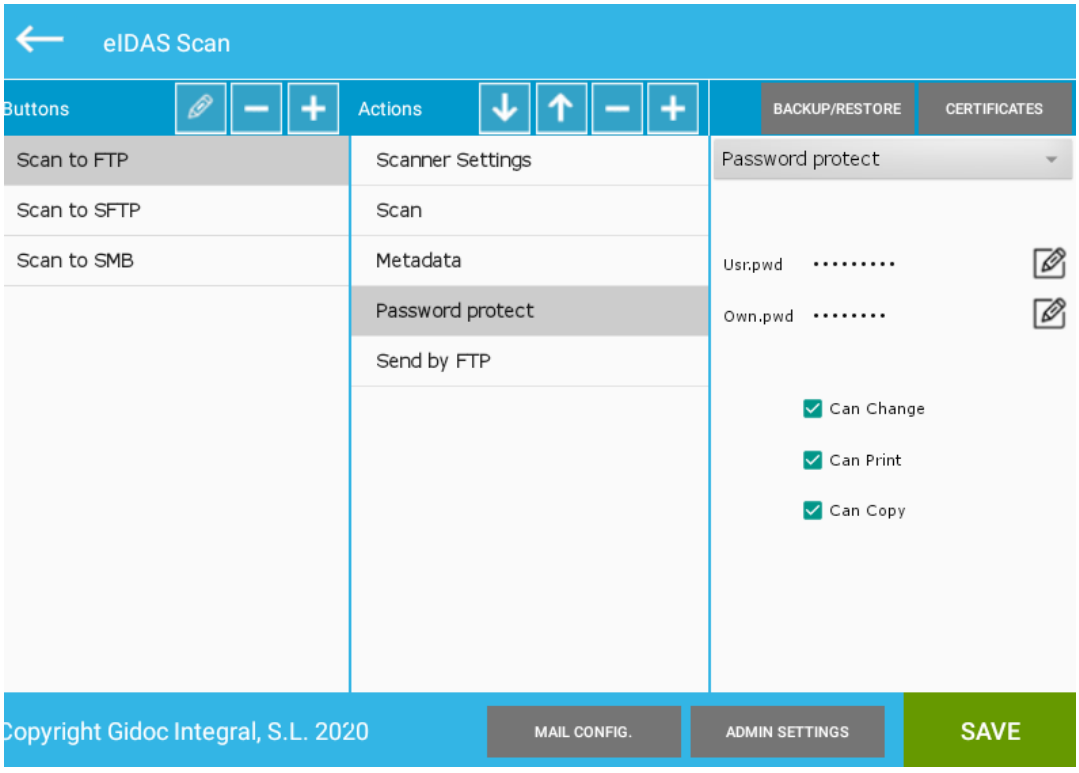
3. **Different passwords for user and owner.**

   When the user password and owner password are set and both are different, the PDF document **can be opened with either of them.** However, only when the owner password is informed, you will be able to change the restricted functions.

4. **The same password for user and owner.**

   You will have to inform the password to open a document and you will have permissions to change restricted functions.

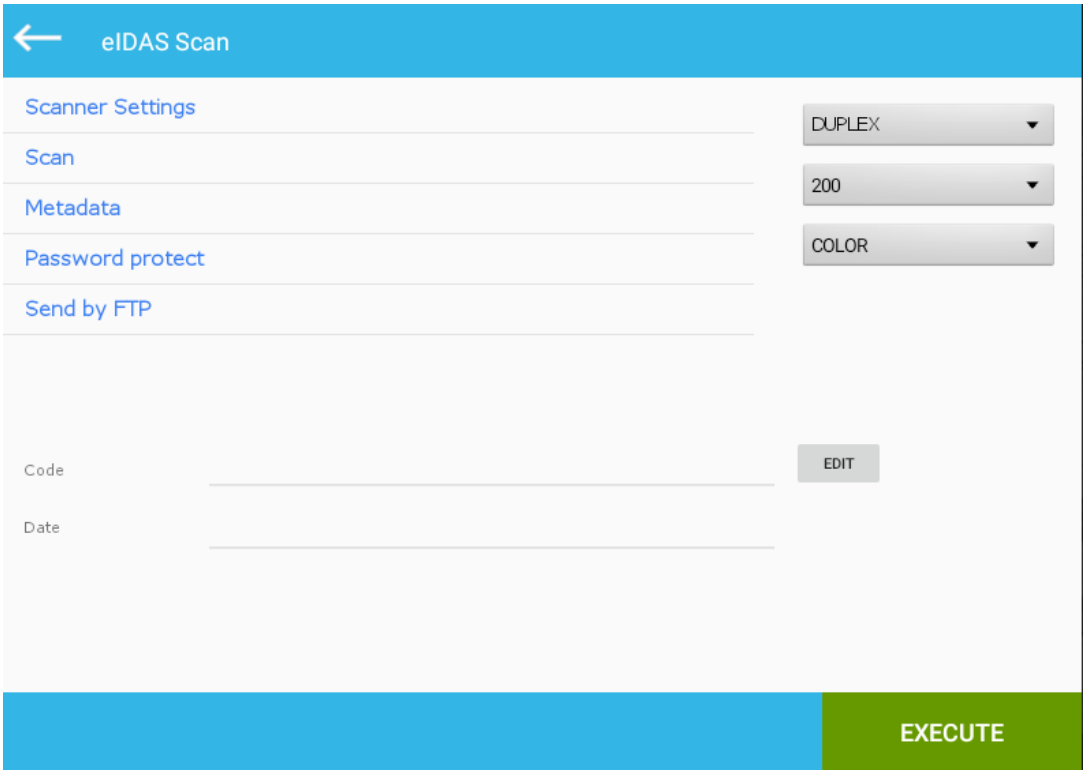
Once the 'Password protection' option has been added, either password can be changed directly with the side pencil button:



Once the 'Password protection' action has been added, it will be displayed in the list of actions that are executed with the button and no additional parameters need to be set.

Additional owner permissions can be enabled for the PDF document:

- Can edit: allow the user to extract pages from the document
- Can print: allow printing of the document
- Can copy: allow to copy contents of the document,



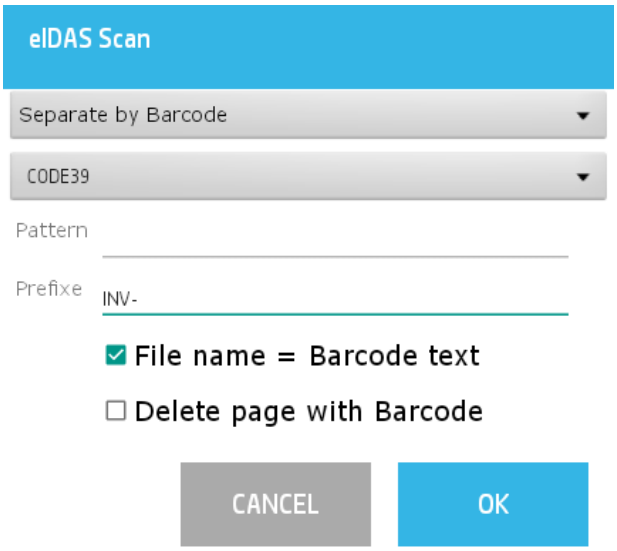
Important

This option is incompatible with the actions of signing a document and signing a document without verification.

F. Separate by barcode

The action of separating by barcode allows several documents to be scanned and different documents to be generated based on the reading of the defined rules.

When creating such an action, the action must be configured:



In the drop-down menu you have to choose which type of barcode you want to read.

Types of barcodes

In the drop-down menu you have to choose which **type of barcode** you are going to read.

These are the options in the drop-down:

- ALL
- EAN13
- Code39
- QR
- DATAMATRIX

In case ALL is selected, any barcode format from the list will be read.

When the barcode scan engine is run, codes from any position are read (there is no need to indicate at which coordinates the barcode should be).

Pattern

The **Pattern** box is used to indicate which barcode pattern the read value can have.

A regular expression must be written. Examples are shown below (the purpose of this document is not to train in the creation of regular expressions):

Regular expression	Examples value
FAC\d*	FAC1 FAC2 FAC333 FAC4441
FAC\d*-21	FAC44-21 FAC123-21 FAC44441-21
[A-Z0-9]{2,3}-20\d*	PED-2044 OT-201234 T8-201

File name = Text barcode.

In case a barcode is read that meets the defined expression, it can be configured that the name of the generated document contains the read barcode (activatable option called 'File name = Barcode text').

With this option enabled, the file name will always be:

[Barcode read]-Sequential

The number after the barcode read is a session sequential: if two documents with the same barcode are read, the first one will end with -1.pdf and the second one with -2.pdf.

In the following example we can see how two documents with the same barcode (value FAC-106475631) and a third document with the value FAC-106657501 have been read.

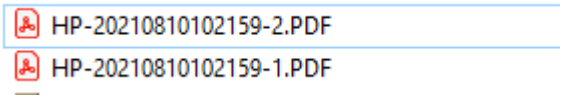
If the same barcode is read in another scanning session, and in the destination location where the documents are sent there is such a document, the previous file will be overwritten (the last scanned document will always be there).

If the option **"File name = Barcode text"** is **not activated**, the default file name will be

HP-[Date of scan]-sequential.pdf.

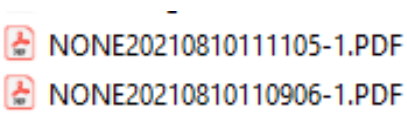
The Date of scan being formed by: year, month, day, hour, hour, minute and second of the barcode reading or transfer without any space or separator.

The sequential is used to allow the generation of more than one document in the same second. If the hyphen wasn't added, the generated document would be overwritten. It also allows us to keep the generated documents in order:



When the option "File name = barcode text" is active and no barcode is read on the first scanned page, the document that is generated starts with the text 'NONE' and has the following form:

NONE-[Date of scan]-sequential.pdf



Prefix

You can also configure the name to contain **a prefix**, e.g. if a document is an invoice and you have read a barcode with the value 2030, you can make the generated document read FAC-2030.

Note that ...

Only characters valid for Windows files may be included in the "Prefix" field.

The characters "/ : * " ? < > | may not use

To make this configuration, you only have to assign in the **Prefix** field the value **FAC-** (or the one you want).

Important

The value indicated as a prefix refers to the value with which the name of a file begins.

For a document to start with a special text (a prefix), this can only be done via the barcode reader module.

There are two options:

1. The barcode read starts with the desired prefix.
2. Configure in the barcode reading action the prefix field (this is the case that can be seen in this section).

Note that ...

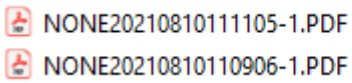
When separating by barcode, you can specify to save the files with a prefix and then make different shipments according to the stored prefixes.

(See sections I to M of the sending actions)

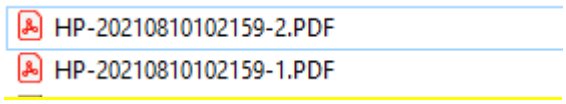
Remove page with Barcode.

Sometimes separator sheets with barcodes are inserted between different documents. In this case it may be of interest to delete the separator sheet. To delete this page of the separator sheet, the option **'Delete page with barcode'** must be ticked.

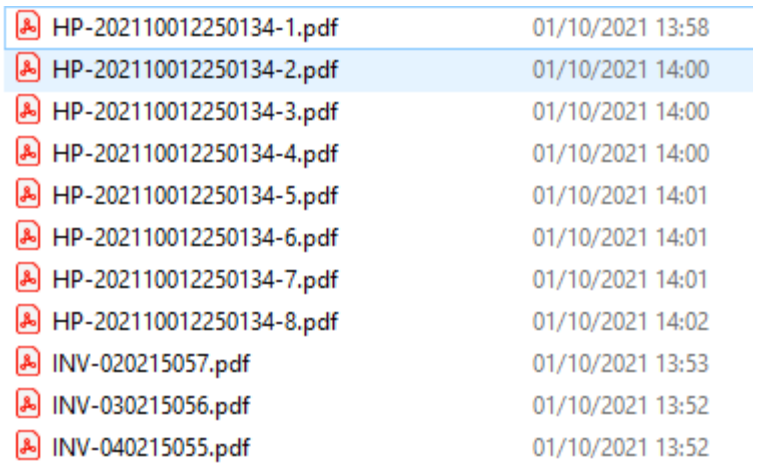
The methodology applied for the assignment of a barcode name is until a code or end of scan is found (if no code is found, the document will be assigned as NONE followed by the date of the scan).



If the option "Assign name = Text Barcode" is assigned, and the document does not have a barcode, a file with the standard HP-YearMonthDay format will be generated.



If both options "Separation by barcode" and "Separation by fixed number" are included, the documents will be sent twice, once by one methodology and once by the other.



If the option “File Name = Barcode Text” is set and no barcode is found, the files will be named NONE followed by the scan date.

In some cases, separator sheets with barcodes are inserted between documents to indicate the end of one document and the beginning of the next. In this case it may be of interest to delete the separator page. To delete this page, check the option **'Delete page with Barcode'**.

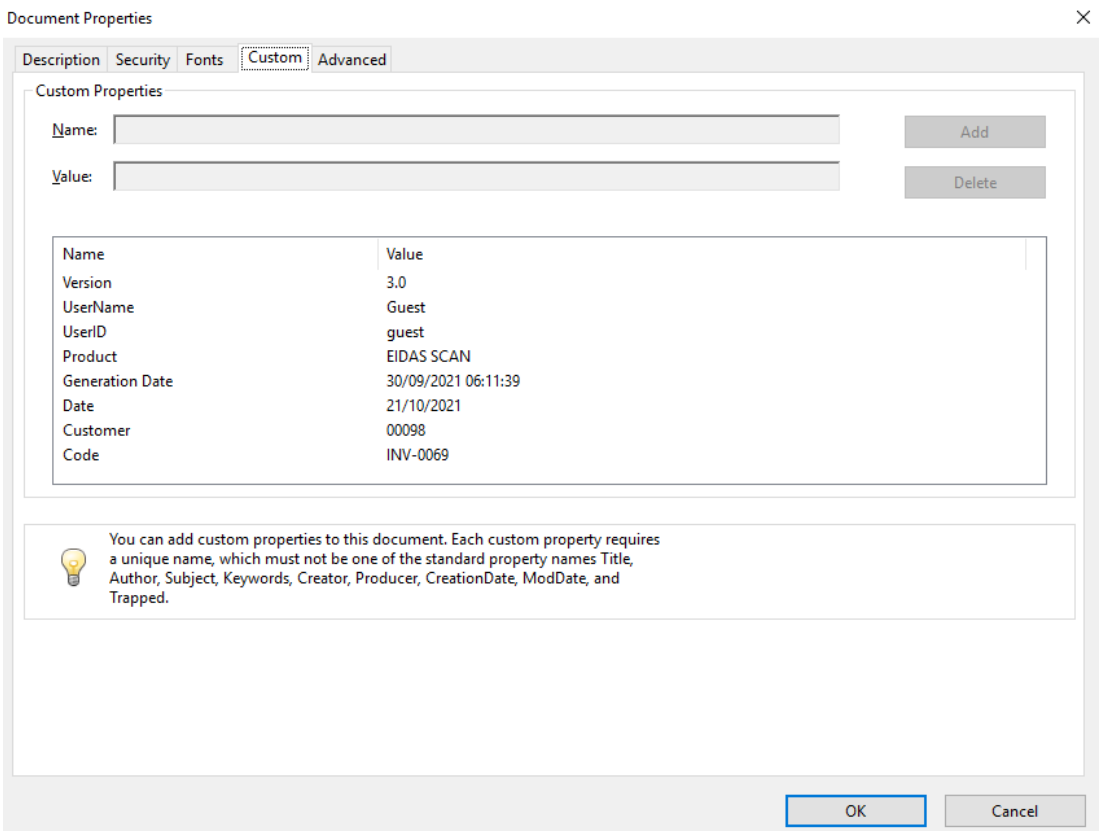
G. Metadata

There are system that when embedding PDF documents, can read metadata assigned and can index them automatically. The use of this option greatly speeds up the process of incorporating the information.

eiDAS Scan includes the following information as metadata within the documents:

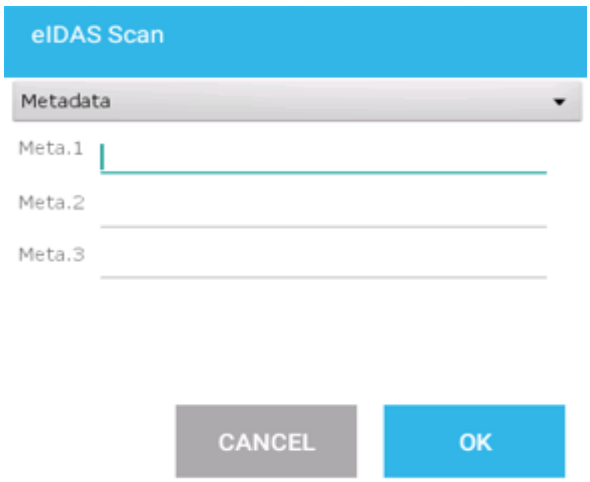
1. Version of the solution.
2. Name of the user who scanned.
3. Identifier of the user who has scanned.
4. Product name (EIDAS SCAN).
5. Date of document generation.

If you want to see the metadata embedded in the PDF document, simply open the document with a viewer that allows you to see the embedded metadata, for example, with Adobe Reader, right click on the document and select "Document Properties", and a screen will appear. If we go to the fourth tab we will see the defined metadata:

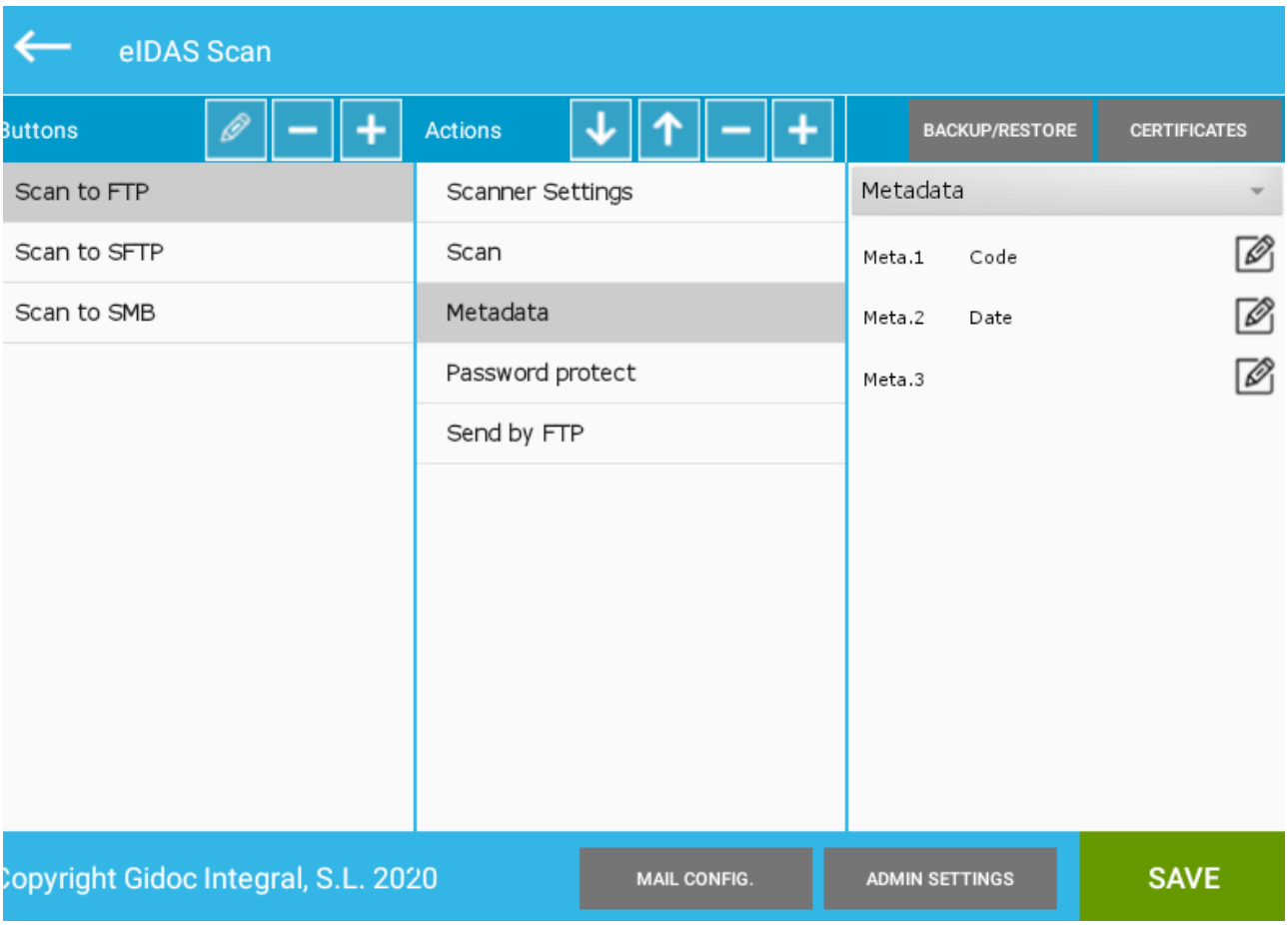


When an action of type 'Metadata' is added, it instructs the application that when the scanning process is started, the user will be requested to enter information.

The action configuration is:



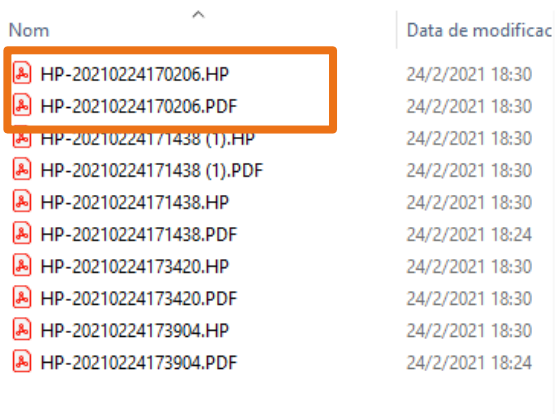
In the **'Meta 1', 'Meta 2' and, 'Meta 3'** boxes you have to put the label that should be shown to the user. n the following example we can see how the three metadata to ask with the tags have been configured. The configuration is as follows:



In case no text is put in a tag within the configuration, it means that the user does not have to be asked for that metadata afterwards.

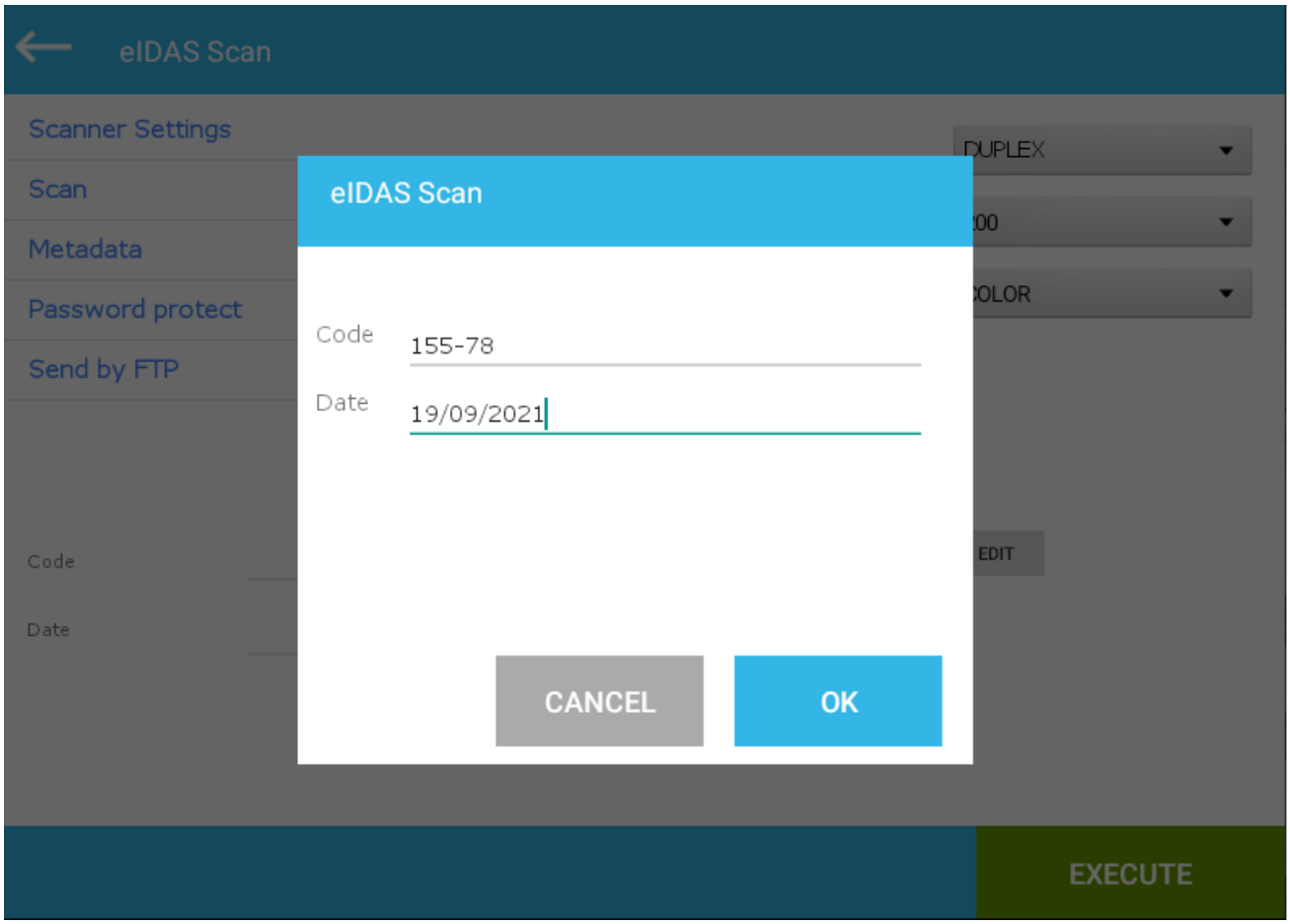
When this option is activated, a file with the same name as the PDF, but with a **.HP extension**, is also generated in the target location containing the metadata written by the user.

The **.HP file** contains the information in **JSON** format to facilitate the integration of the documents with external systems.

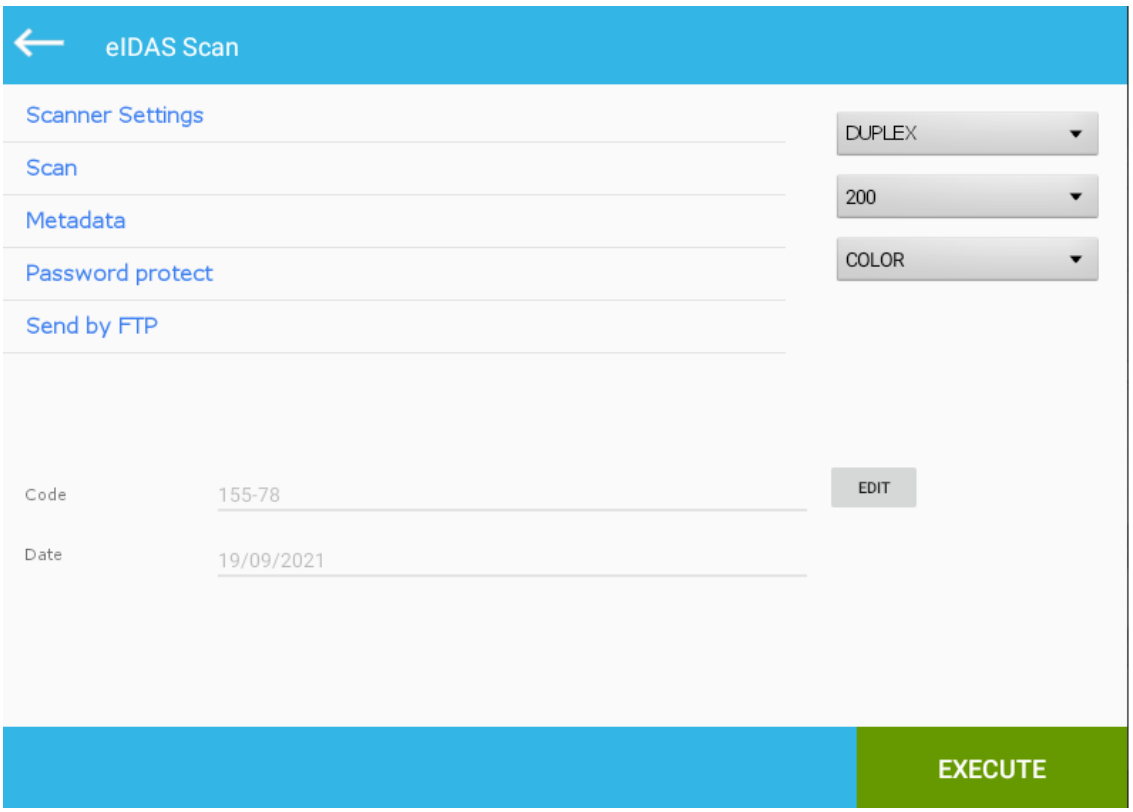


The metadata reported by the user are embedded in the document.

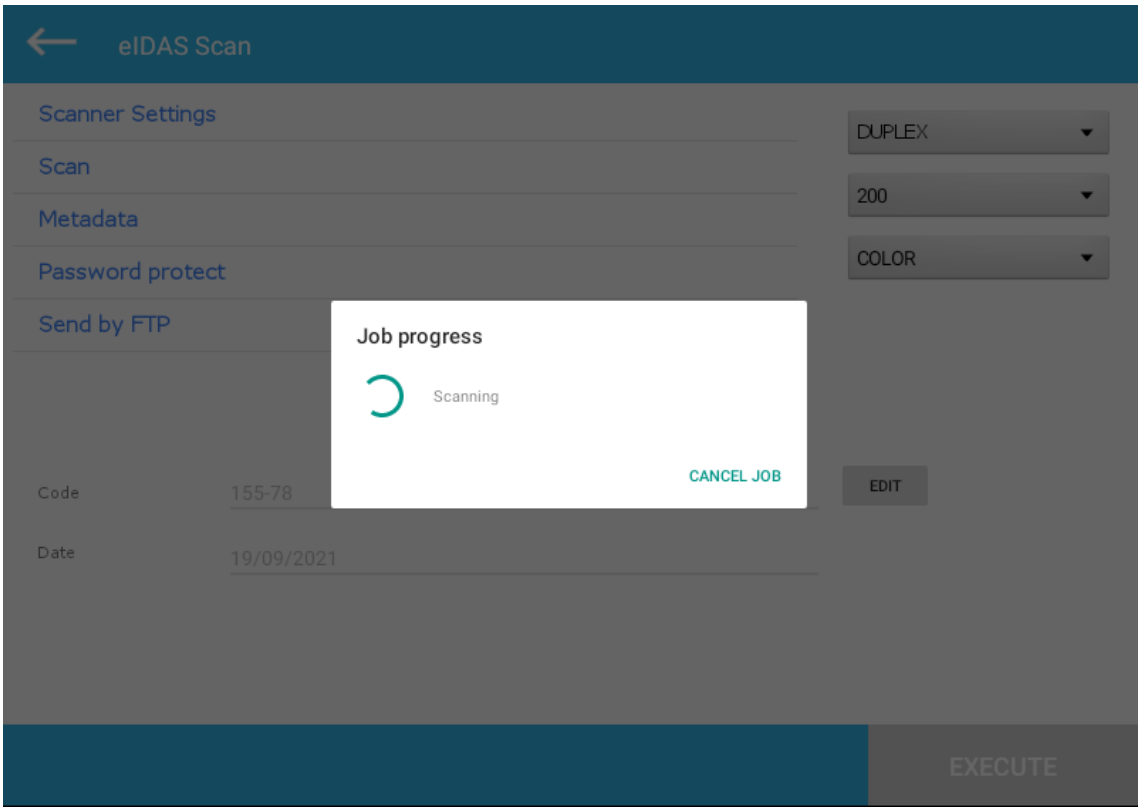
Below, a flow is shown where two metadata (order code and order date) have to be entered and accessed for information:



Once the metadata is accepted, the form displays the metadata in the lower area:



Finally, executing the digitization process the progress form will be shown:



After scanning and transferring a one-page document at 200 dpi, **the .HP file** is generated with the following content:

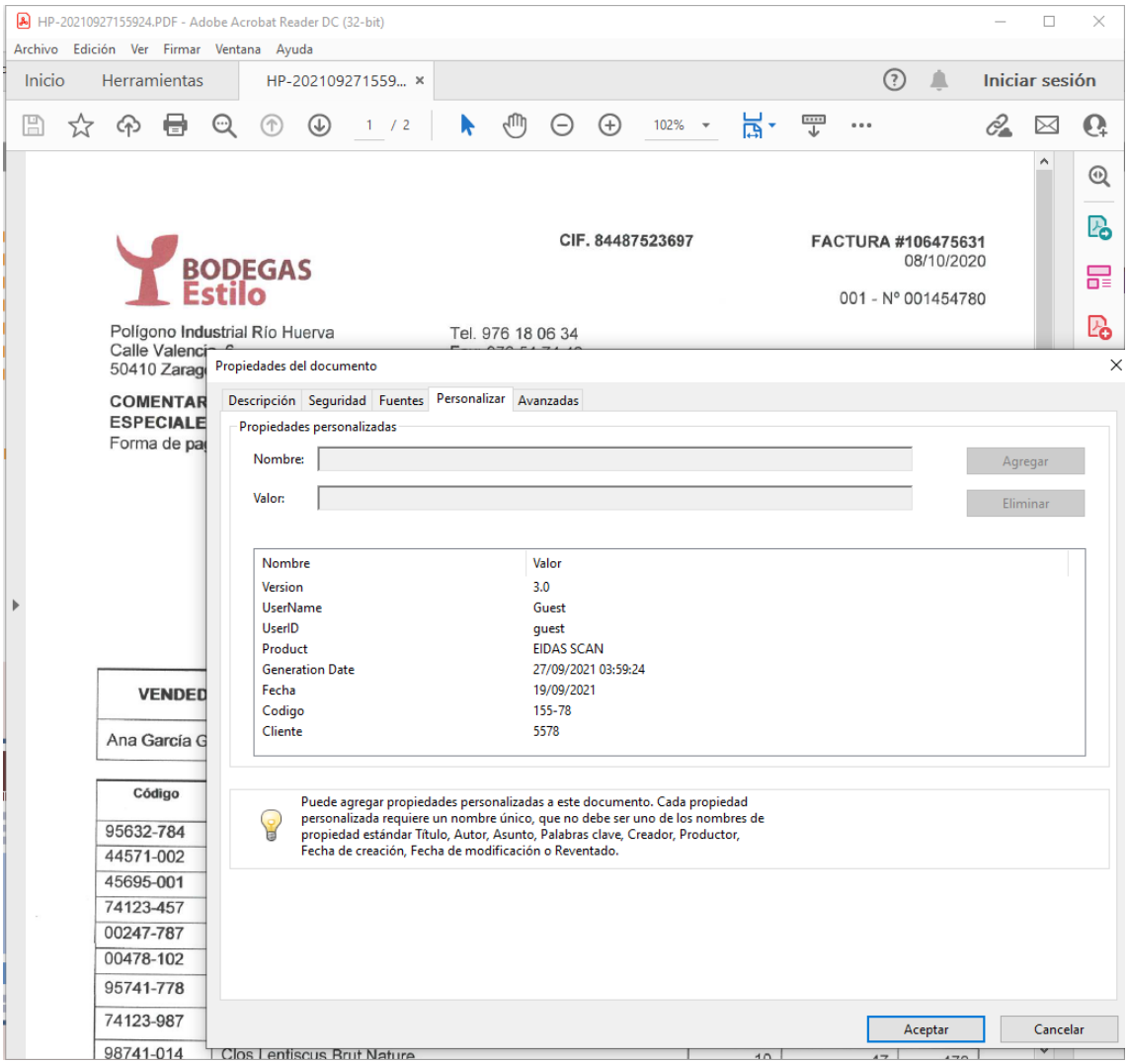
{"UsuarioID":"guest","Usuario":"Guest","Meta1":"155-78","Meta2":"19/09/2021","Meta3":"5578","Resol":"DPI_200","Pages":"0"}

{"UserID":"guest","Userio":"Guest","Meta1":"155-78","Meta2":"19/09/2021","Meta3":"5578","Resol":"DPI_200","Pages":"0"}

The ***Resol*** metadata reports the resolution used in the scanning process.

The ***Pages*** metadata indicates the number of pages that make up a document (value set in the system when the fixed number of pages separation action is specified).

The tab with the metadata previously reported would look like this:



When the metadata option is added, the scan date, scan user code and scan user name are also added to the PDF.

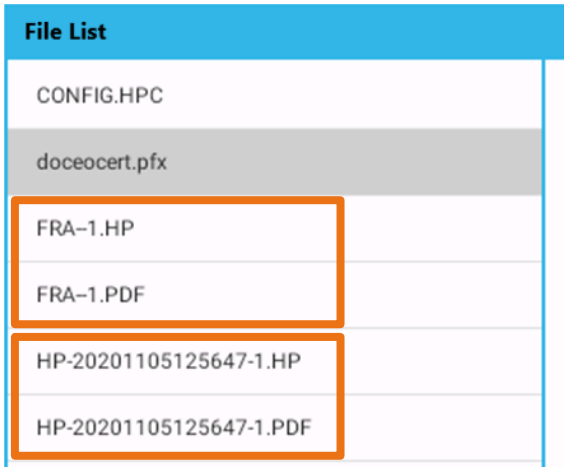
Below is a flow where two pieces of metadata (order code and order date) have to be entered.

Once the document has been digitized and transferred, **the .HP** file has been generated with the following content:

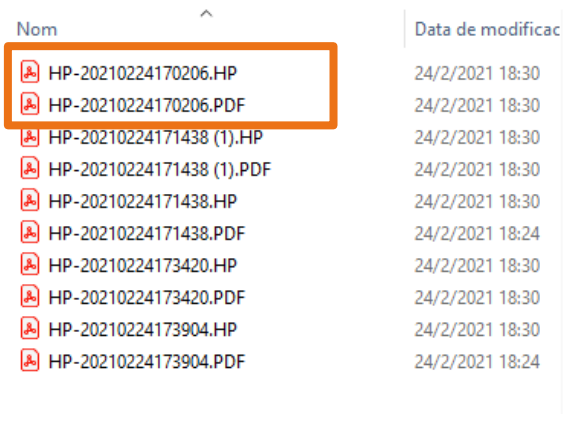
Meta1":"fac00000145","Meta2":"fac00000145","Meta3":"","Resol" :"DPI_200","Pages":"1"

Here's how the PDF document looks with the embedded metadata:

On the eIDAS Scan screen

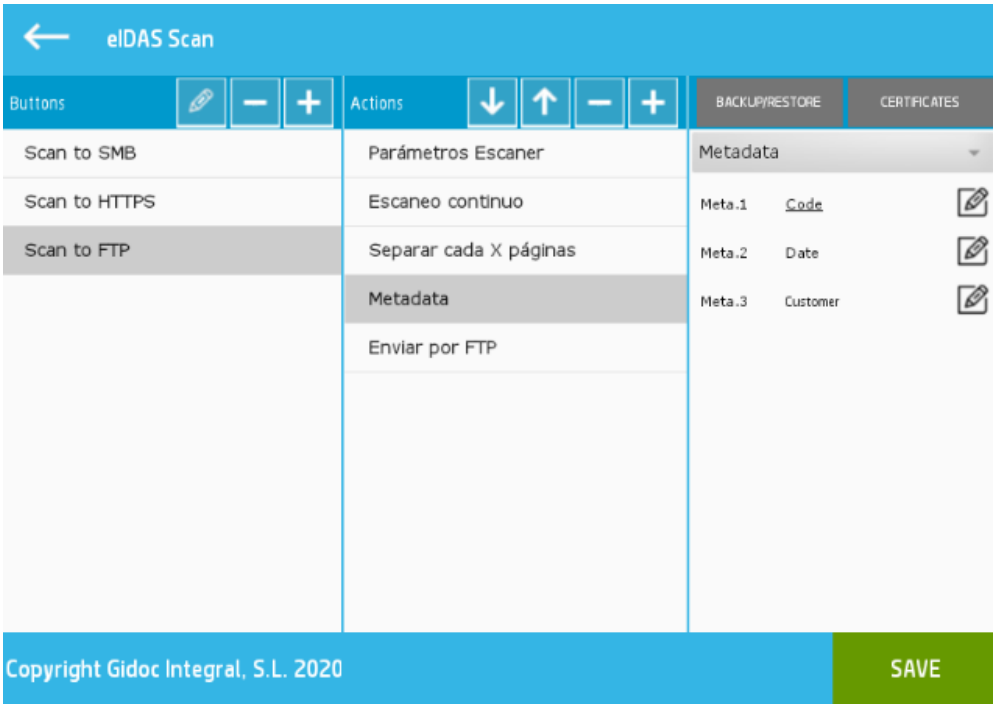


On storage (e.g. local folder)



The .HP termination is the metadata and the .PDF termination is the file.

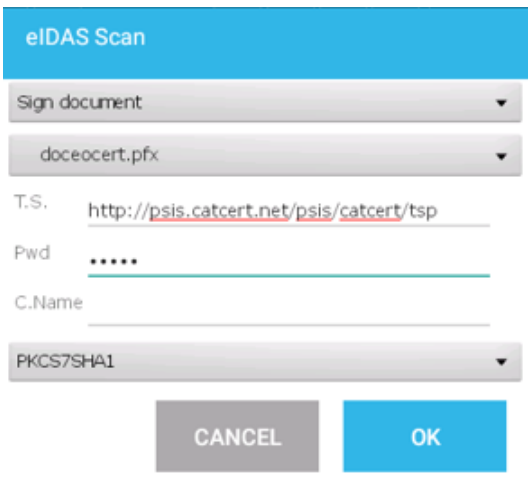
Where you can see that "Client code" appears underneath as an embedded metadata.
After the metadata configuration the main screen is displayed as follows:



H. Document Signature

The 'Sign document' action is used to generate PDF documents with a digital signature and optionally a time signature.

When adding the Document Signature action, the system displays the following settings:



In the **first drop-down** menu are the certificates defined in the certificate management form. You must choose the certificate to be used.

In the **PWD field** you must indicate the password of the digital certificate.

When a PDF document is digitally signed, the time at which the signing process was performed is included. In certain cases, the time at which a document is signed may be important.

The date that is included in the document can be the date of the multifunctional equipment that is carrying out the signing process or it can be the date indicated by an external service called a specialised date service (TSA or Time Stamping Authority).

If we incorporate the date of the MFP, it could be that the date of the MFP is manipulated in such a way that an invented date is embedded.

When it is important that the date on the document is really what it says it is, recognised TSAs are used and we say that a time stamp is incorporated.

In case you want to include a time stamp in the document, you have to inform in the **T.S. box** the address of the TSA server.

In the **T.S. box**, you must enter the address of the TSA server if you want to include a timestamp in the generated document.

- When choosing the **catCert** timestamp address (**http://psis.catcert.net/psis/catcert/tsp**), **PKCS7SHA1** must be selected in the last drop-down menu.
- When choosing the **TS@** timestamp address (**https://des-tsafirma.redsara.es/tsamap/CreateTimeStampWS**), **X509.RSA.SHA1** must be selected in the last drop-down menu.

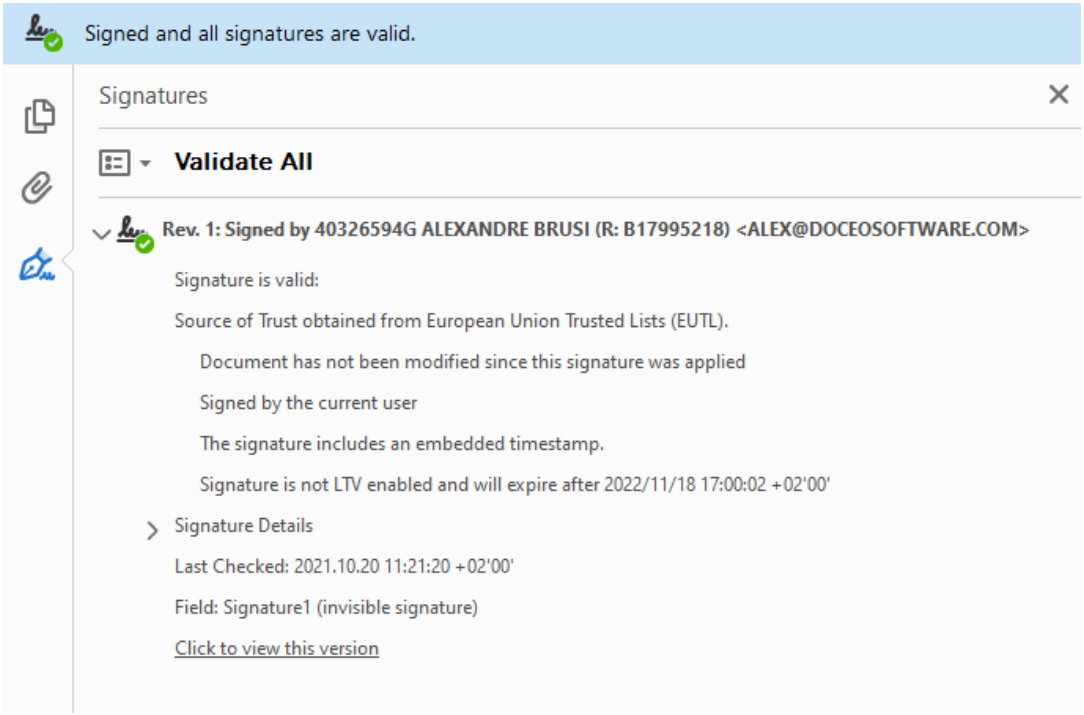
In this second case, it is necessary to enter in the **C.Name field** the name of the application authorized by the **Ministry of Finance and Public Administrations of Spain**.
Any standard time-stamping server can be used. Other servers are listed below:

- http://psis.catcert.net/psis/catcert/tsp
- http://timestamp.digicert.com/
- http://timestamp.entrust.net/TSS/RFC3161sha2TS
- http://aatl-timestamp.globalsign.com/tsa/aohfewat2389535fnasgnlg5m23
- http://tsa.quovadisglobal.com/TSS/HttpTspServer

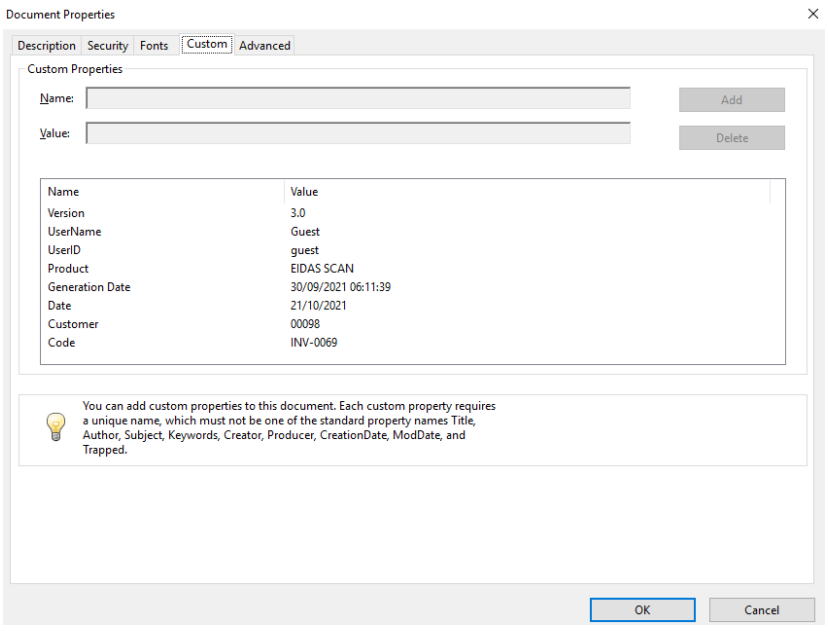
For most sealing servers, you will only have to inform the address of the service and select the PKCS7SHA1 option from the drop-down menu.

In this second case, the name of the application authorized by the **Spanish Ministry of Finance and Public Administrations** must be entered in the **field C.Name**.

Below is an example of what a signature would look like in the Adobe Reader viewer (you have to scroll down the side bar on the left):



In order to see the certificate used in the time stamping, we have to go to the option "Signature properties -> Advanced properties -> Time stamping authority":



The validity of a digitally signed document depends on the legislation of each country.

Important

The send to destination options J through M below perform a direct send to **smb, ftp, sftp or https**. To do this, you only need to specify the path.

For example: "smb: // server / shared_folder" and also specify the password.

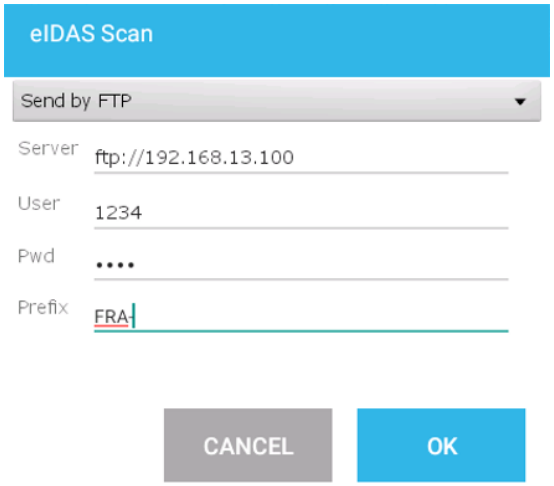
I. Signing document without verification

It is used to use **non-recognized certificates** (their revocation and authenticity cannot be validated).

It is very easy to generate an unqualified digital certificate to sign documents internally to an organisation. However, being unqualified, it cannot be validated if it is revoked.

J. Send by FTP

The action **'Send by FTP'** sends the generated documents via an FTP protocol. When adding the action, the configuration options displayed are:



The input data are:

- **SERVER:** You need to value of type ftp://XXX where the XXX is the FTP server IP.
- **USER:** FTP Service User Name.
- **Pwd:** FTP service user password.
- **Prefix:** the indicated value shall be added as a prefix to the name of the generated document.

Once the fields have been filled in, you can test the connection with the ***'CONNECT'*** button.

Note that...

- If the "PREFIXED" field is empty, it shall send all documents to be processed.
- If the field "PREFIX" has a value, only documents whose document name starts with this prefix shall be sent.

In the case that has been determined in the process written in the section "Separate by barcode", the one that has been entered there will be replaced by the one entered in this section. In other words, it will be overwritten, with the first one disappearing and not being repeated.

When no prefix is assigned and **the barcode reading is disabled**, the documents generated will have the following nomenclature:

HP-20210223135528-001.HP
HP-20210223135528-001.pdf

HP-YEAR + MONTH + DAY + HOUR + MINUTE + SECOND + Scan Sequential .Extension

The only way to validate the correction of the input data is by digitizing a document and checking if it is sent correctly to the FTP server; there is no test button.

In case a barcode has been read and a prefix has been defined in the transfer process, the document name shall contain the prefix and the barcode read.

Example:

Barcode 18/2020 has been read and, the prefix factor has been defined.

The name of the document shall be FAC-18/2020.

If a document is transferred by FTP and a file with the same name already exists at the destination, the current file will be deleted and the new document generated will be saved.

Correct use of prefixes

It is important to pay special attention to the prefix value, in case only one transfer action is added and a document does not start with the indicated prefix, the document will not be sent and will be lost.

An example of this case could be:

Use case: we have barcode scanning function activated and we want to scan documents whose scanning prefix is FAC.

Configuration done:

- Barcode reading and the option **File name = Text barcode is activated**.
- A single sending action is configured (FTP, SFTP, SMB or HTTPS) and the FAC value is specified in the prefix.

Problematic case: if the barcode of the first scanned page is not read, the name will be prefixed with NONE, it will not be sent to any external system and the document will be lost.

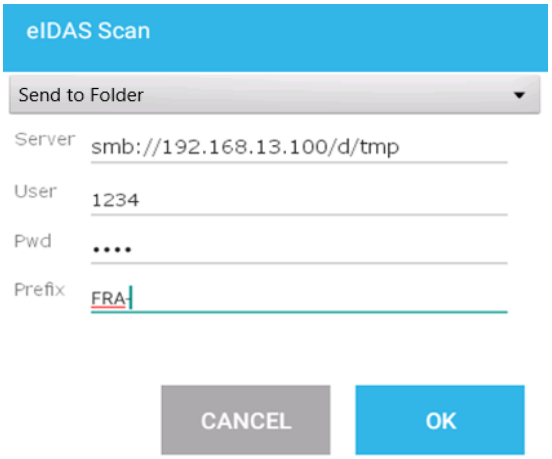
Permissions

It is important to use the connect button; the sending process is carried out within the multifunctional equipment and we have to validate that we have access to the detailed server; access to an external resource may be different depending on where we execute the action.

For example, it may happen that the network where the equipment is connected does not have a server visible.

K. Send to Folder

'Send to Folder' action sends the generated documents to a folder shared with samba protocol. When adding the action, the configuration options displayed are:



The data to be entered are:

- **SERVER:** You must input a type of value smb://IPAdress/Shared Folder/Subfolders
  In server it is necessary to inform the name of the server or the IP.
- **USER:** name of the user who can access the shared resource.
- **Pwd:** User password specified in User.
- **Prefix:** the value indicated in this box shall be used to filter which documents shall be sent in this transfer action.

Once the fields have been filled in, it is possible to test the connection with the **'CONNECT'** button.

Note that...

- If the "PREFIXED" field is empty, it shall send all documents to be processed.
- If the field "PREFIX" has a value, only documents whose document name starts with this prefix shall be sent.

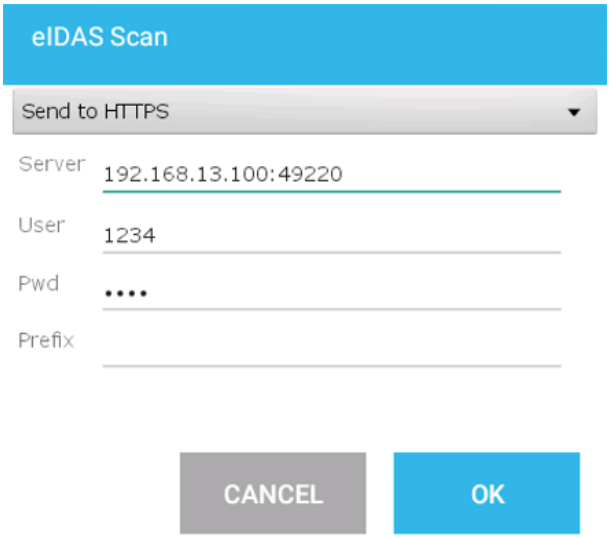
The file naming logic is the same as for FTP.

The explanations for the action 'Send by FTP' also apply to this action.

Read them carefully

L. Send to HTTPS

Action 'Send to HTTPS' sends the generated documents to a secure web service. When adding the action, the configuration options displayed are:



The data to be entered are:

- **SERVER:** You must input a type of value IPAddress:Port
- **USER:** User name who can access the service
- **Pwd:** User password specified in USER
- **Prefix:** the value indicated in this box will be used to filter which documents will be sent in this transfer action.

Once the fields have been informed, the connection can be tested with the **'CONNECT'** button.

Note that...

- If the "PREFIXED" field is empty, it shall send all documents to be processed.

- If the field "PREFIX" has a value, only documents whose document name starts with this prefix shall be sent.

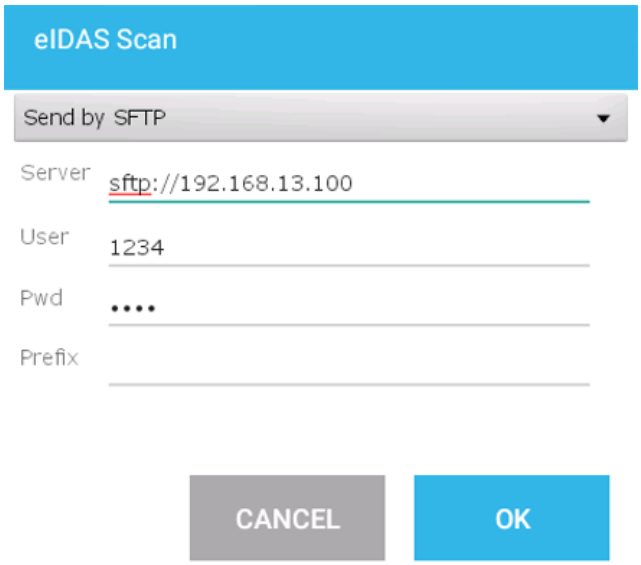
The naming logic is the same as in FTP.

The explanations for the action 'Send by FTP' also apply to this action.

Read them carefully.

M. Send by SFTP

'Send by SFTP' sends the generated documents on a SFTP server. When adding the action the configuration options displayed are the same as for 'Send by FTP:



After informing the fields, you can test the connection with the **'CONNECT'** button.

The explanations for the action 'Send by FTP' also apply to this action.

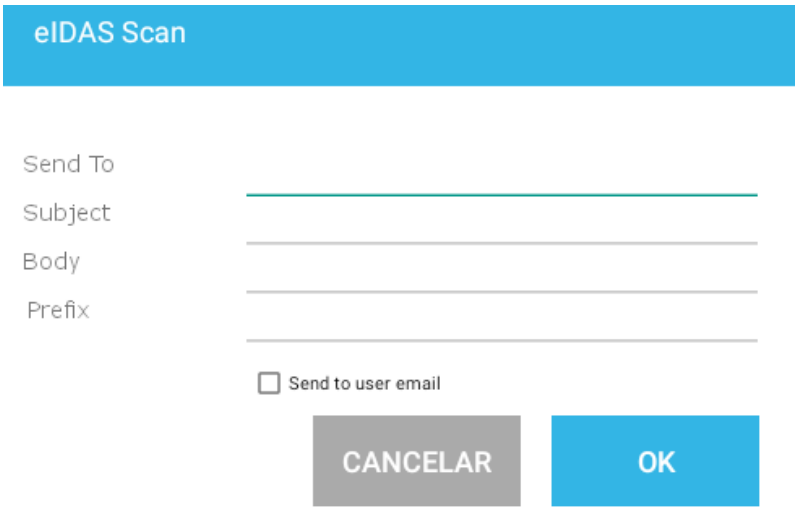
Read them carefully.

Note that...

- If the "PREFIXED" field is empty, it shall send all documents to be processed.
- If the field "PREFIX" has a value, only documents whose document name starts with this prefix shall be sent.

N. Send to mail

Sending the generated document to an e-mail address. The following parameters have to be configured:



- **Send to**: e-mail address to which you want to send the file.
- **Subject:** title of the email.
- **Body:** body of the email to be sent (it will always have the PDF document attached).
- **Prefix:** You can define a prefix in case the mail is linked to a document manager and can opt for automatic classification.
- **Send to user mail:** If you activate this option, a copy of the message with all the content will be sent to the user who is digitizing.

5. SUMMARY TABLE OF TRANSFER PROTOCOLS

Summary of the modalities that can be allocated the final files to server	
Scan to FTP (File Transfer Protocol)	Send to FTP Server
Scan to SFTP (SSH File Transfer Protocol)	Send to an SFTP server
Scan to SMB (Server Message Block)	Send to Shared Folder
Scan to HTTPS (Hypertext Transfer Protocol Secure)	Sending the file to a secured web service.

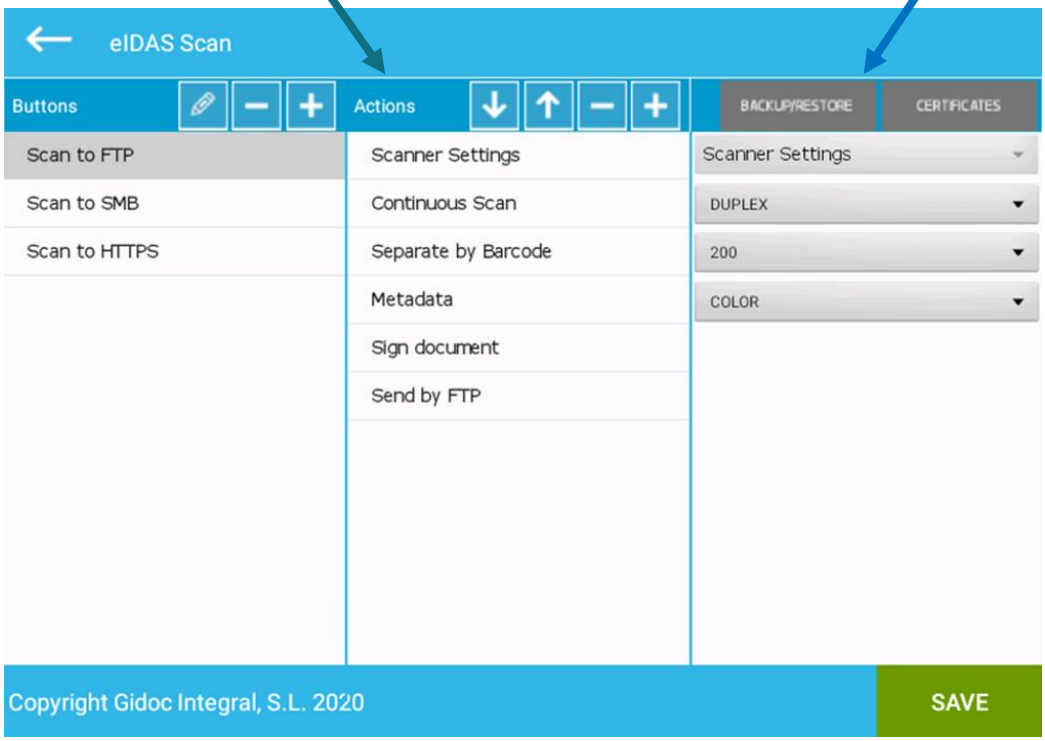
6. SUMARY TABLE OF ACTIONS

Below is a table with a summary of all available actions and the options available to them:

	Action	Action options	Function / Characteristics
A	Scan parameters	Duplex or Simple | Size (200 to 600) | Color or Grey or Mono	Options for the basic scanning mode of documents.
B	Continuous scanning	No options	Scanning option where every time the documents run out, the system stops to wait for more documents.
C	Scan	No options	Scanning option.
D	Separate every few pages	Partitioning of digitized documents on the basis of a fixed number of pages.	Every few numbers of pages the document will be separated.
E	Password protection	No options	This action is used to create password protected PDFs so that the document is saved encrypted.
F	Separate by barcode	Barcode type | Pattern | Prefix | Filename = Barcode text | Delete separator page	Reading of different barcode formats. The file can be separated and named by barcode.
G	Metadada	No options	Manual metadata entry.
H	Sign document	Options for entering various parameters.	Digital signature with a certificate configured in the system.
I	Sign document without verification	Same options as 'Sign document'.	In case of non-recognized certificates.
J	Send to FTP	TS | Pwd | C.Name	Sending to a FTP server.
K	Send to a folder (SMB)	Server | user | pwd | prefix	Sending to a shared folder.
L	Send to HTTPS	Server | user | pwd | prefix	Sending to a secure web service.
M	Send to SFTP	Server | user | pwd | prefix	Sending to a SFTP server.
N	Send via mail	Mail | Subject | Body | Prefix	Sending the generated document to an email.

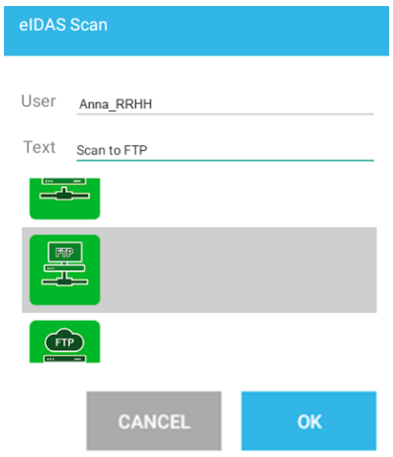
7. EXAMPLE OF CREATING A FLOW

In the next display you can see three configurations created: (Scan to FTP, Scan to SMB and Scan to HTTPS, it shows the **actions of the Scan to FTP flow** and the characteristics of the first **action** (Scanner settings).



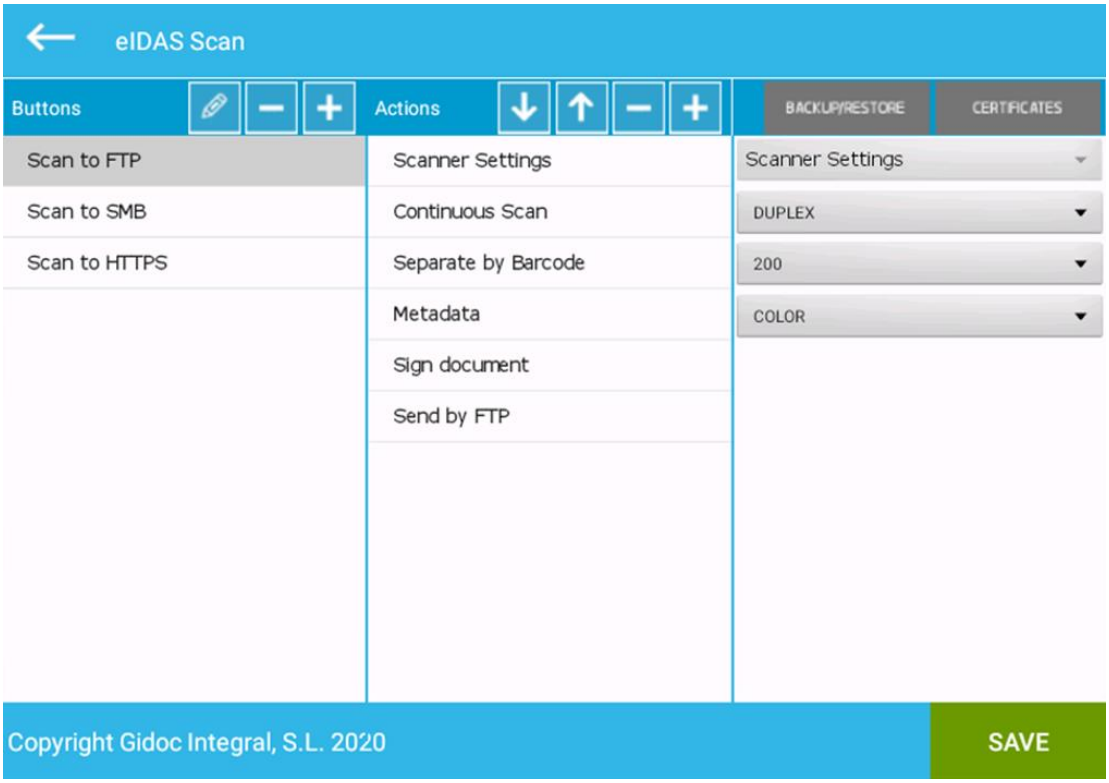
The process of creating a flow is very simple:

1. We create a new button, and assign the user to whom it is addressed (it can be left blank), the descriptive text and the icon that will be seen on the button:



Press **OK** to access the configuration of the particular actions.

2. Access the actions screen and **add and configure** actions as required (example of possible configuration):



Click on SAVE the button to save the created configuration.

Note that ...

- If a user has not been assigned a flow, when accessing the application, there will be no icon.
- There are options that by default will appear sorted in a practical sense in case their placement is not appropriate.

The following actions can only be added once:

Action
Scanner Settings

Continuous scanning
Scan
Separate every X pages
Metadata
Sign document

The following actions can be inserted more than once:

Action
Separated by barcode
Send by FTP
Send to Folder (SMP)
Send to HTTPS
Send by SFTP

8. HTTPS DESCRIPTION

In case you are interested in setting up the https server, please contact the **GIDOC INTEGRAL** team and we will provide you with the installable https server.

There is the option to develop an https service which can communicate with the **eiDAS Scan**. You will need to implement the following calls:

A. LOGIN

Usage: In order to consume the rest of the calls, we must first identify ourselves with this call. The call returns a Tocken which must then be sent in the rest of the calls.

POST URL:	https://localhost:49220/api/Login/authenticate
Body Content-Type:	application/json
BODY:	{
	"Username":"doceo",
	"Password":"doceo",
	}
RETURN:	Token

{
"Id_Token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1bmlxdWVfbmFtZSI6ImRvY2VvIiwicm9sZSI6IlVzZXIiLCJuYmYiOjE1ODU5MDg2MTgsImV4cCI6MTU4NKxMDQxOCwiaWF0IjoxNTg1OTA4NjE4LCJpc3MiOiJodHRwOi8vbG9jYWxob3N0OjQ5MjIwIiwiYXVkIjoiaHR0cDovL2xvY2FsaG9zdDo0OTIyMCJ9.368O7IPuY2pzJCscnq3v8nhnVMGu51Qh6WelqKtbGLY"
}

Send File

Usage: This call allows you to send a **base65** encapsulated document to the server.

- You only need to report the **Filename and Date fields**.
- The call must return the ID assigned to the document.

POST URL: https://localhost:49220/api/docuements/send

Body Content-Type: application/json

Authorization: "Bearer" + Token

BODY:

```
Public Class Msg_Upload_Image

Public Filename As String
Public FilenameSign As String
Public data As String (encoded Base64 File)
Public dataSign As String

End Class
```

RETURN: ID

```
{
"Id": "7"
}
```

B. Reception of a file

Usage: This call allows you to retrieve a **base64**-encapsulated document on the server.

- Only the **Filename and date fields** need to be reported.
- The call must return the identifier that has been assigned to the document so that eidas Scan knows that the process has been executed correctly.

POST

URL: https://localhost:49220/api/docuements/send

Body Content-Type: application/json

Authorization: "Bearer " + Token

BODY:

```
Public Class Msg_Upload_Image

   Public Filename As String
   Public FilenameSign As String
   Public data As String (encoded Base64 File)
   Public dataSign As String

End Class
```

RETURN: ID

```
{
"Id": "7"
}
```

C. Get Document List in a Folder

Usage: This call allows you to get files in a folder. Specifically, it is used to select the digital certificates contained in a folder.

GET URL: https://localhost:49220/api/documents/signature

Body Content-Type: Application/json

BODY: Authorization, Bearer + Token

RETURN: Listo of FileNames

D. Obtain a Certified File

Usage: This call allows you to send a digital certificate to the multifunctional team.

GET URL: https://localhost:49220/api/documents/signature? FileName=

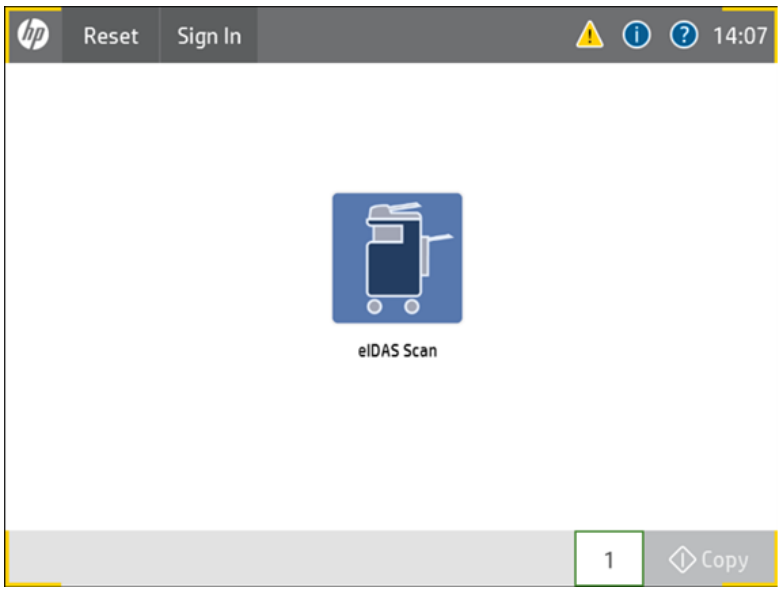
Body Content-Type: Application/json

BODY: Authorization, Bearer + Token

RETURN: JSON date Base64

9. USER ROLE

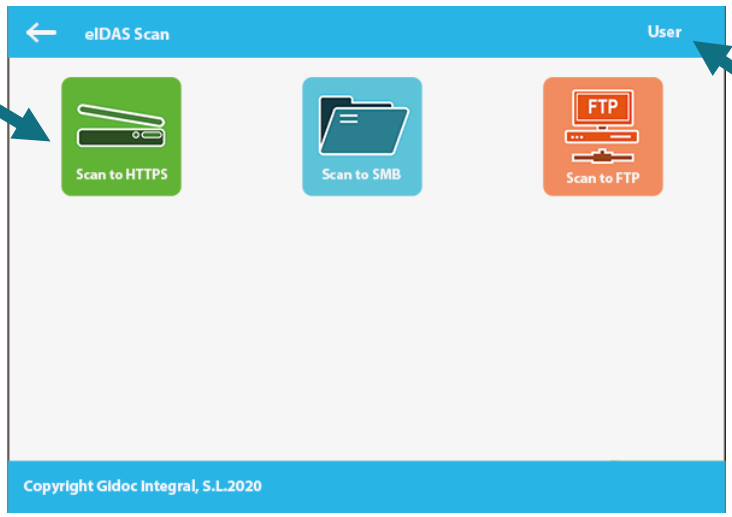
To start the app with a specific user, you'll need to use the common registration options **on HP equipment**. Once we have identified ourselves, we can start the application:

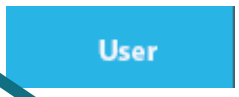


When accessing the application, you can see the flows that the user has access to (the assign button is displayed and below the name assigns).

See sections **2.3. Button Settings** and **2.4. Action Settings**.

Defined flows that the user can start.

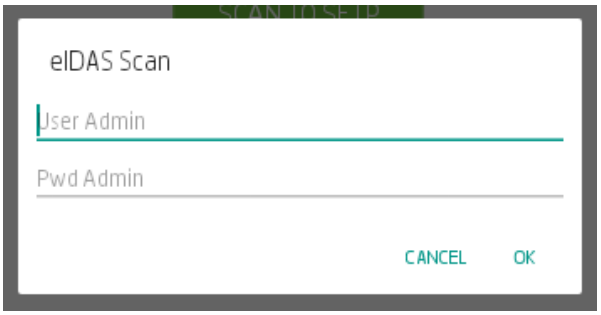




User Name

If we access the CONFIGURATION button, without being in the administrator role, a screen will appear asking for a username and password.
The first time after installing the App, the user's name and password is blank.

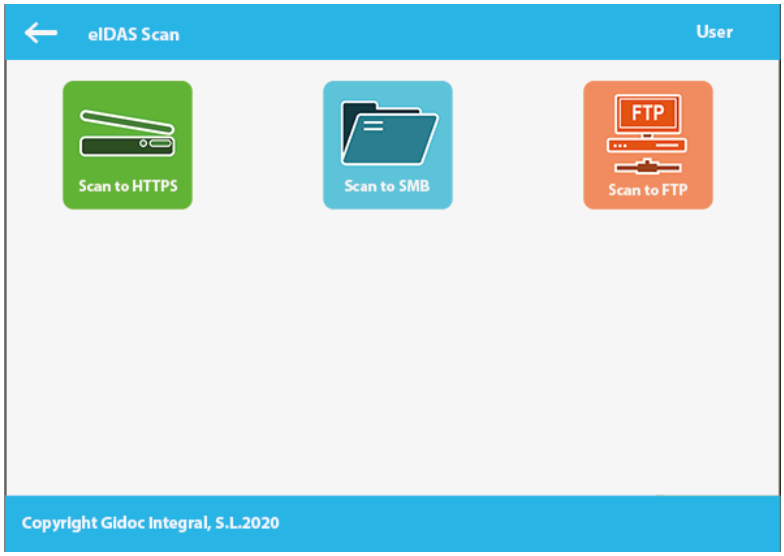
The first time after installing the App, the user name and password are blank.



More information is in section **1. Application Start**.

9.1. Buttons and Scanning

Remember that the scanning buttons and modes as well as their actions and properties must be previously configured from a user with administrator role. Therefore, the screen we see in this manual is an example.



9.2. Use Examples

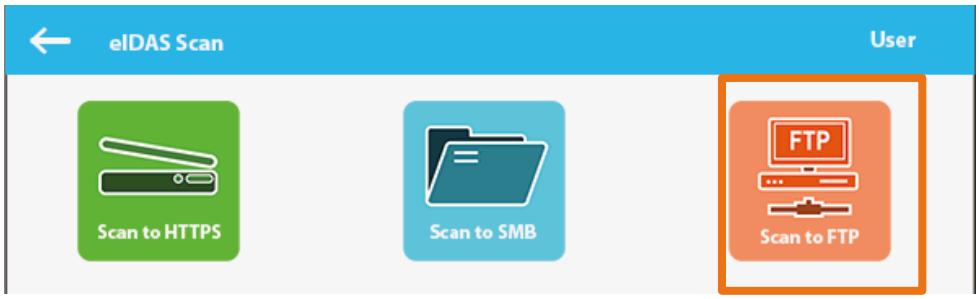
We will see three scanning models with a possible configuration made by the administrator. Remember that the scanning modes are four but FTP and SFTP have the same configuration parameters.

EXAMPLE 1: SCAN TO FTP

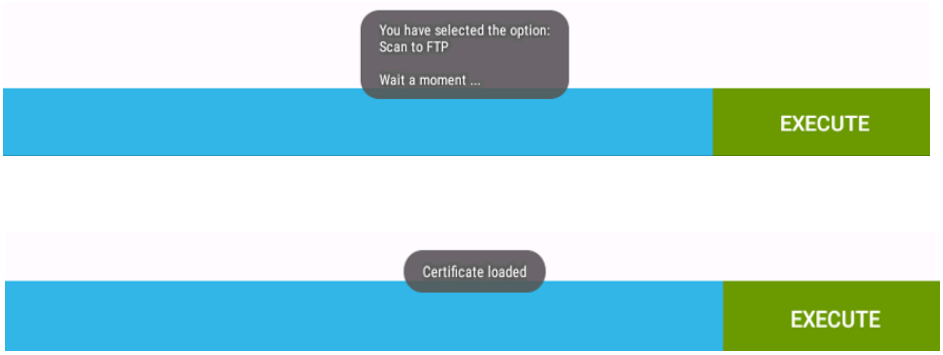
In this case, the configuration is as follows:		
Scanner Settings	Duplex 200 Color	(*) This data can be modified when you run a flow with any user role.
Continuous Scanning	Each time the paper is finished, the application will not stop, it will be waiting for more documents until the end option is chosen.	
Separated by Barcode	When reading a barcode in a valid format, a new PDF document will be generated.	
Metadata	Two text codes are requested	
Document Signature	Digital signature of the text document	
Send by FTP	Finally, it will send the document or documents generated in PDF, signed and with metadata via FTP according to the configured address.	

The scanning option in SFTP is exactly the same, except for the protocol used.

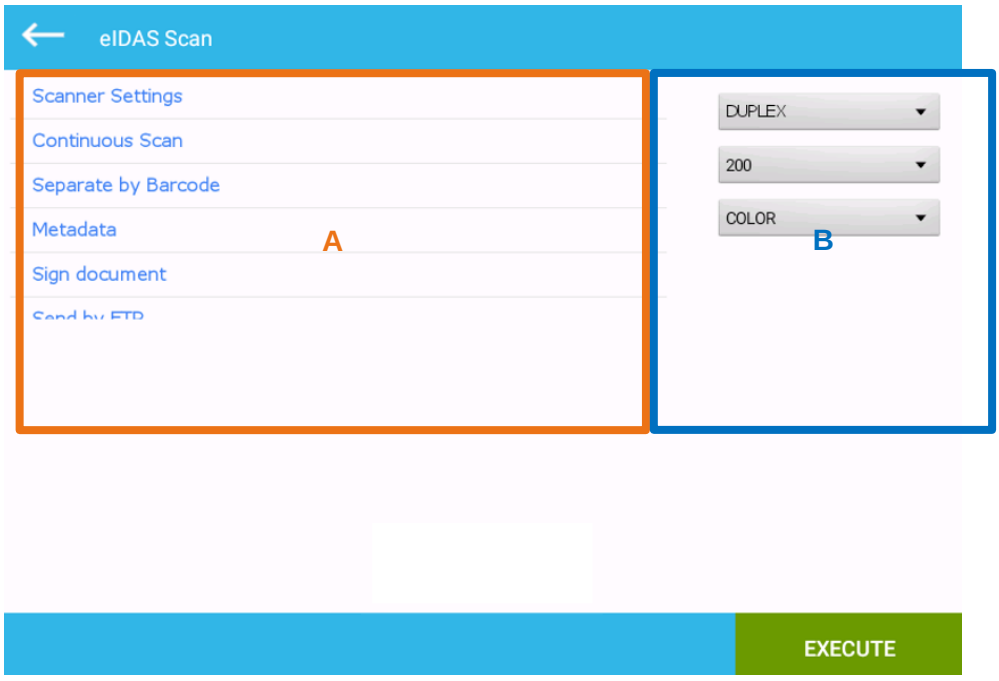
1. Choose a configuration. In this case, for example, we will choose **SCAN TO FTP**.



The following messages appear:



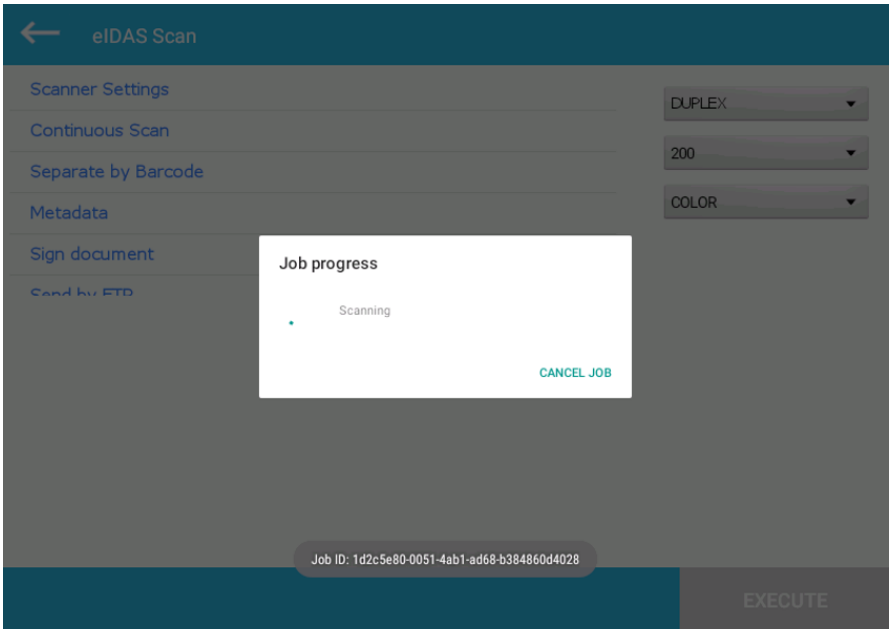
2. Automatically loads **the associated settings with that button**. Including **the certificate**. As you can see, only related **Scanner Settings** options are modifiable.



3. Metadata input:

4. Click on EXECUTE

5. From here, the application automatically runs what we have configured.

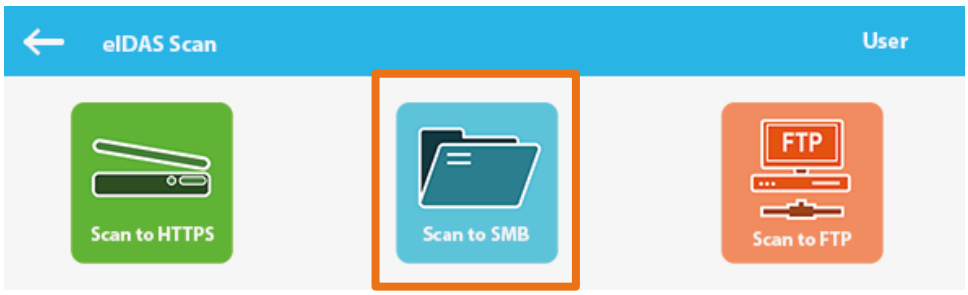


6. Finally, it will continue to scan (waiting for documents) until we inform you that the process has finished.

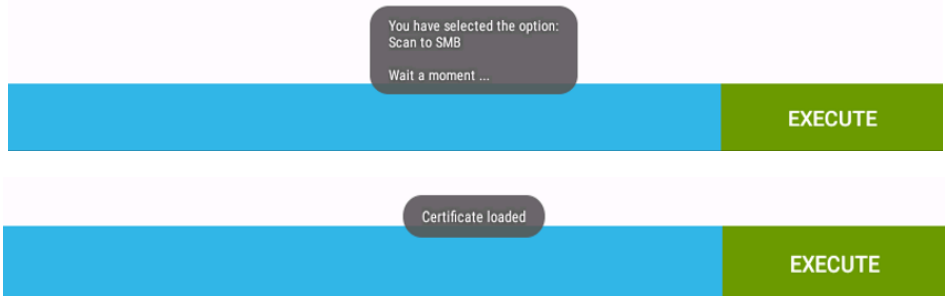
EXAMPLE 2: SCAN TO SMB

In this case the configuration is as follows:		
Scanner Settings	Simple 400 Grayscale	(*) This data can be modified when you run a flow with any user role.
Continuous Scanning	Scan indefinitely until the user indicates that the scanning process is complete ()	
Send by SMB	Finally, it will send the document or documents generated in PDF to the folder we have configured.	

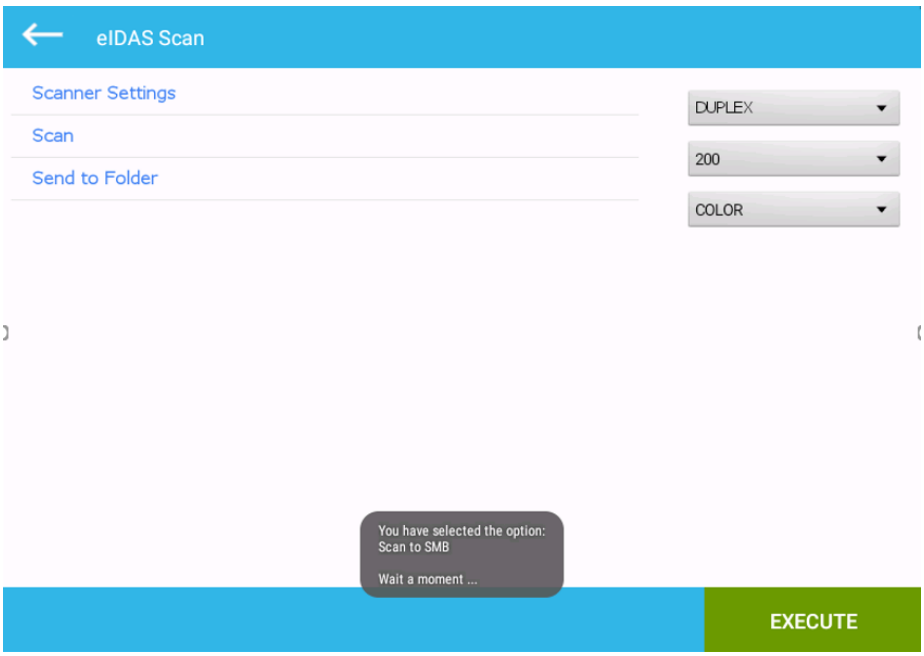
1. Start the flow process by choosing it:



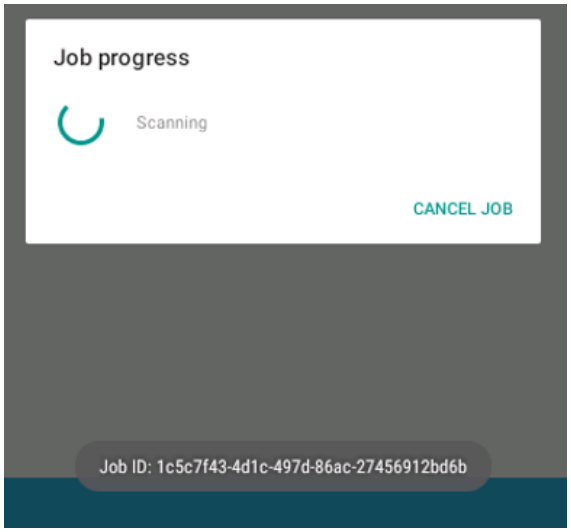
The following messages appear:



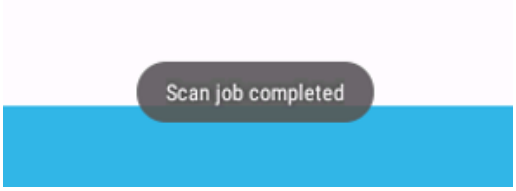
2. The associated settings with that button are automatically loaded.

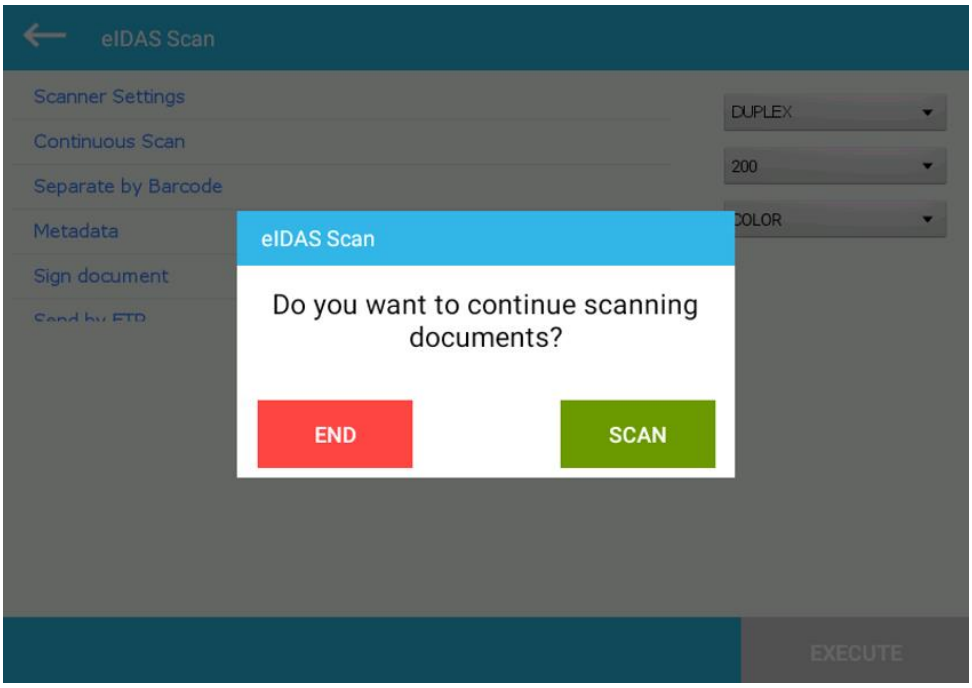


3. We execute it. Automatically performs the whole process. We will see that it is done correctly through the following messages.



4. Finally, once the process is completed, it asks if we want to scan more documents using the same configuration or cancel.



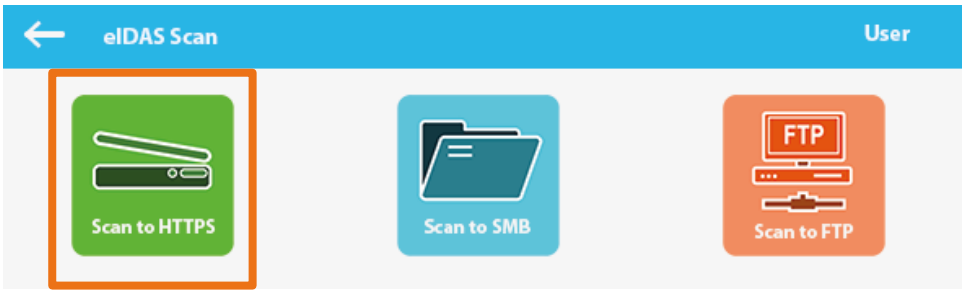


END to exit, **SCAN** to continue.

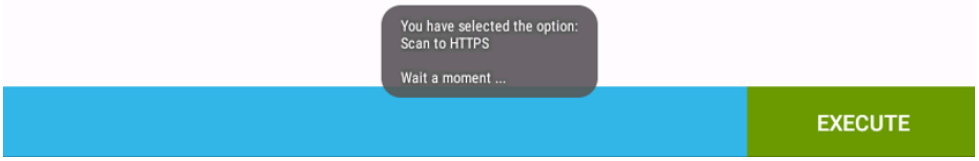
EXAMPLE 3: SCAN TO HTTPS

In this case, the configuration is as follows:		
Scanner Settings	Simple 200 Mono	This data can be modified from any user role.
Separate Every 5 Pages	It will generate a PDF every 5 pages with simple scanning (one side).	
Metadata	The minimum. In this case, there is no digital signature because we need to send the document to another application in order for the signature to be done there.	
Scanning	Scan until the documents placed in the tray are finished.	
Send to HTTPS	Finally, it will send the document or documents generated in PDF to another application to continue with the management and further signature performance.	

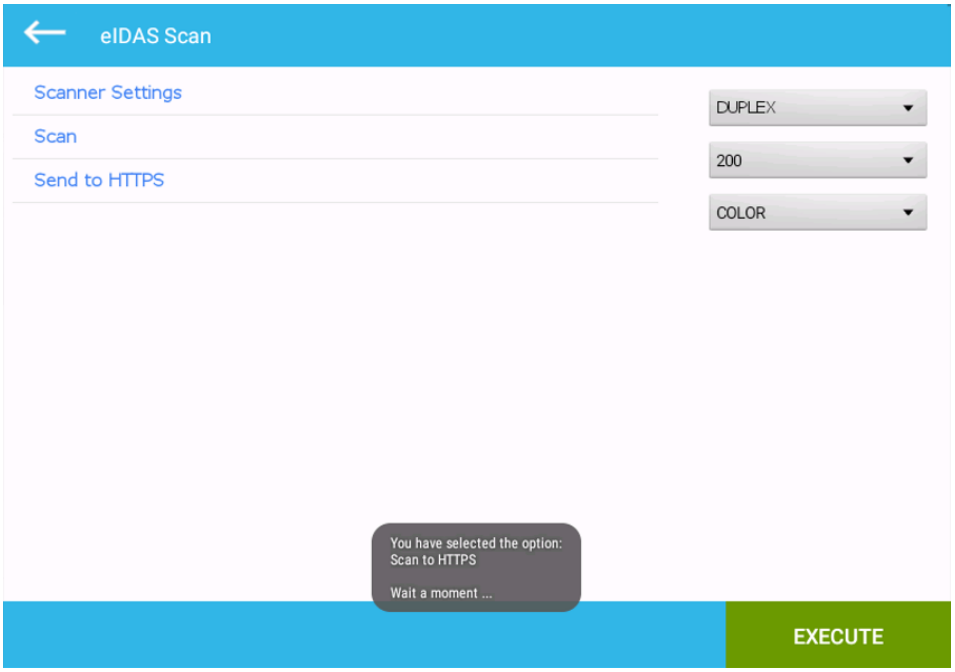
1. Choose a configuration. In this case, we will choose **SCAN TO HTTPS.**



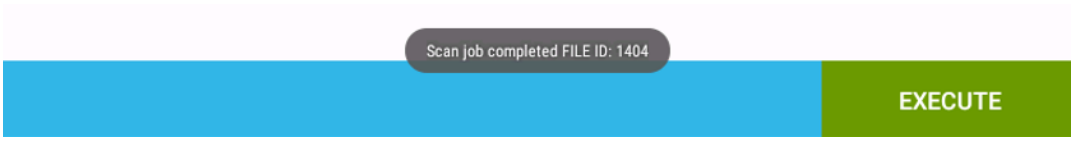
The following message appears:



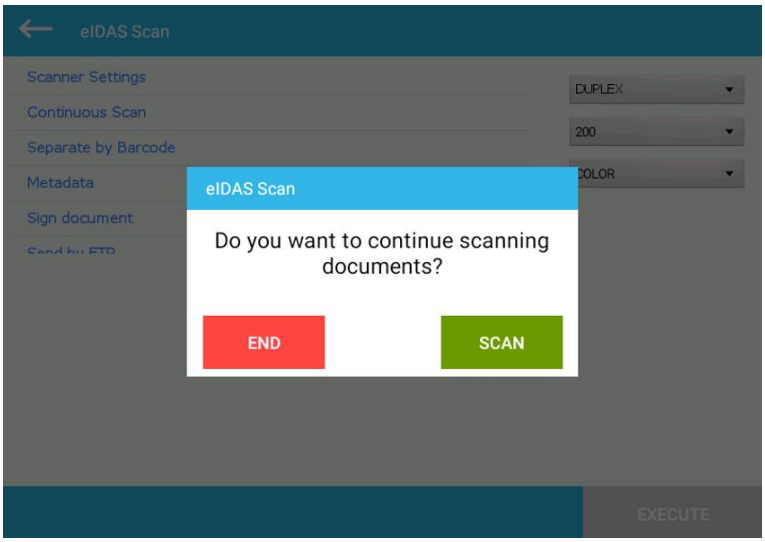
2. The settings associated with that button are automatically loaded.



3. We execute it. It automatically performs the whole process. We will see that it is done correctly through the following message.



4. Finally, once the process is complete, it asks if we want to continue scanning documents using the same configuration or cancel.


eIDAS Scan
Scanner Settings
Continuous Scan
Separate by Barcode
Metadata
Sign document
DUPLEX
200
COLOR
eIDAS Scan
Do you want to continue scanning documents?
END
SCAN
EXECUTE