USER MANUAL
Safe LTA

INFOCERT

TINEXTA GROUP

TABLE OF CONTENTS

INFOCERT
TINEXTA GROUP

1 INTRODUCTION

Safe LTA is the InfoCert cloud-based service designed for the long-term preservation of any digital document.

Safe LTA adheres to European standards for long-term preservation and, where necessary, adopts specific regulations of individual European countries.

This document describes the usage methods of its web navigation interface.

Safe LTA is organized into **two distinct environments:**

- *Provisioning*: https://safelta-provisioningfrontend.infocert.digital/it

- *Preservation and search*: https://safelta.infocert.digital/it/

Paragraphs 4-9 describe how to independently configure the environment from the Provisioning area. If you have chosen to delegate this activity to InfoCert, you can directly refer to paragraph 10 for details on the functionalities available in the Preservation and Search area.

2 DEFINITIONS

Safe LTA includes the following definitions:

- **Company Group**: identifies a logical container that allows organizing documents internally. Each Company Group is exclusively used by a single Customer and contains one or more Companies. Company Groups are uniquely identified by their name, so there cannot be two Company Groups with the same name in Safe LTA.
- **Company**: an area for storing documents of a specific company. In the case of a corporate group, you can create as many Companies as there are individual companies within it. The Company contains one or more Document Classes. Companies can only exist within a Company Group and are uniquely identified by their name within the Company Group. This means that within the same Company Group, there cannot be two or more Companies with the same name.
- **Country**: identifies the regulatory standards adopted by the system for preservation and can be configured at the Company level. Currently, the following standards are available:
  - o *Italy*: for Italy, based on the AgID guidelines.
  - o *Other*: for all European countries that do not have specific regulations.

  These standards adopt two different formats to generate the file that certifies the correctness of the process, respectively:
  - o **PIndex_signed.xml** for "Italy"
  - o **METS_FULL_signed.xml** for "Other"
- **Document Class**: identifies a category of documents with its metadata and contains the documents. An example of a Document Class is "invoice" Document Classes can only exist within a Company and are uniquely identified by their name within the Company. Therefore, within the same Company, there cannot be two or more Document Classes with the same name.
- **Document**: represents an individual preserved document, along with its metadata. Documents can only exist within a Document Class.
- **Template**: represents a Document Class template aimed at facilitating the creation of multiple similar Document Classes.

Access users are defined within the Company Group and the following **roles** are provided:

- **Manager**: the user authorized to perform configuration operations within the Company Group. This user allows independent configuration by the Customer (including user configuration). Alternatively, it is possible to request InfoCert to fully configure the preservation environment, including the Companies within the Company Group (in both cases, the Company Group is defined by InfoCert).

- **Enduser**: the user authorized to perform preservation, search, and document download operations.

- **Auditor**: the user authorized only for search and document download operations.

Safe LTA allows the following **functionalities**:

- Self-configuration: configuring Companies, Document Classes, templates, viewers, and users within one's own Company Group (optional usage).

- Document preservation.

- Searching for preserved documents using search indexes (metadata).

- Download of preserved documents, both as individual files and as a complete AIP package.

- Display of statistics on Safe LTA usage.

INFOCERT
TINEXTA GROUP

3 ACCESS AND LOGIN

Safe LTA is organized into **two distinct environments:**

- *Provisioning*: https://safelta-provisioningfrontend.infocert.digital/it

- *Preservation and search*: https://safelta.infocert.digital/it/

To access each of the two areas, you need to have your own credentials, username, and password, and click on the "**Login**" button on the login page (Figure 1).
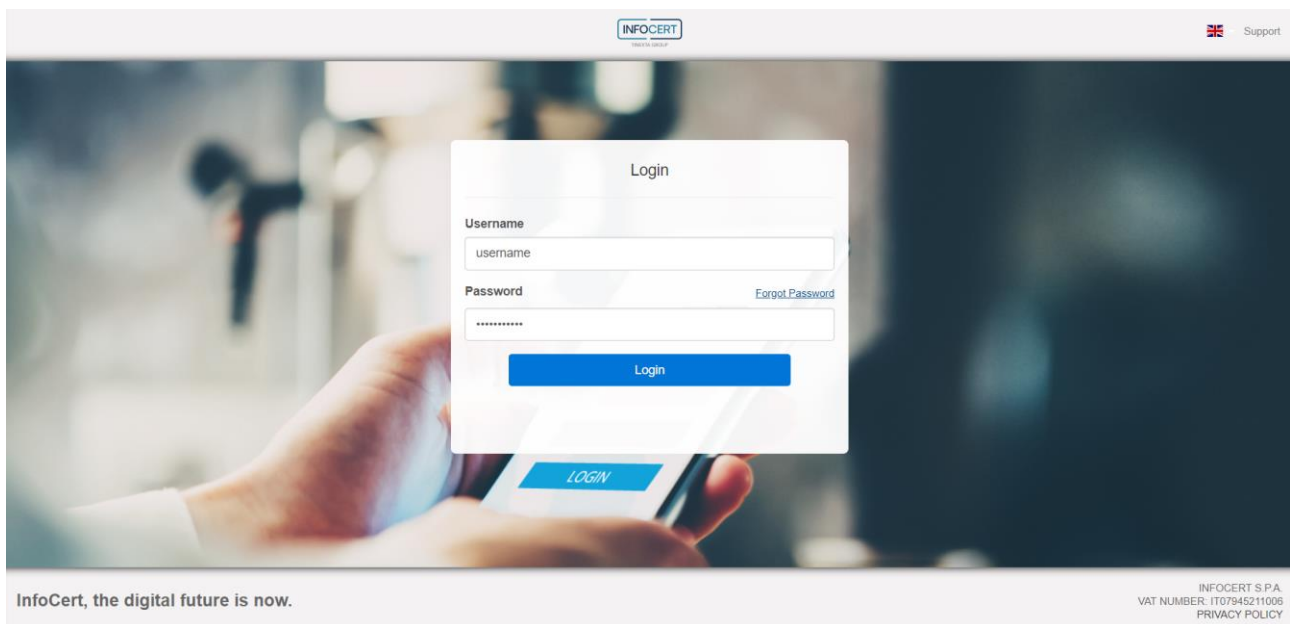

FIGURE 1

4 CREATING A COMPANY

Safe LTA allows a Group Manager user to configure a Company. Within the Company, authorized personnel belonging to a specific company are grouped together, along with the definition of the Document Classes intended for that Company.

After logging in, the Manager is directed to their reserved area, which is associated with their respective Company Group (Figure 2).
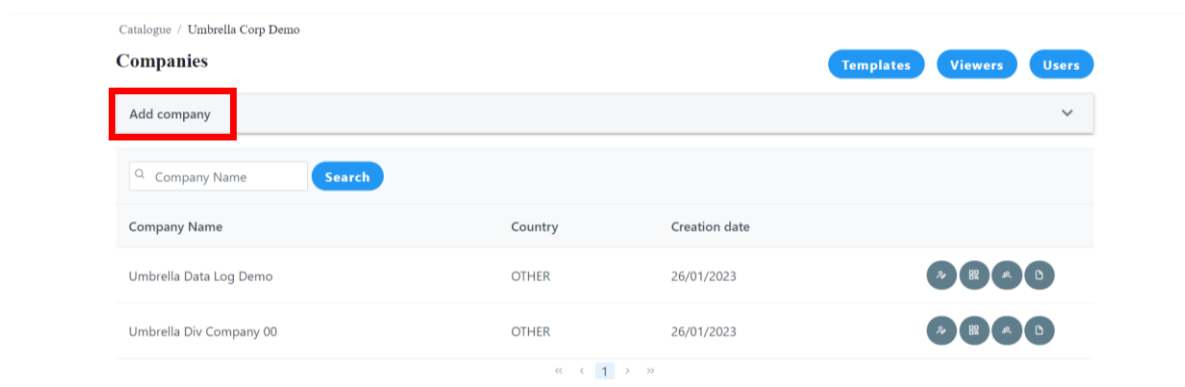

FIGURE 2

To register a new Company, click on "**Add Company**" to expand the data entry area (Figure 2). Then, simply enter the name of the Company, for example, "Acme Logistics," select the corresponding Country (Italy or Other) and click the "**Create Company**" button.

At any time, it will be possible to modify the name of the Company and its Country using the respective button (Figure 3).
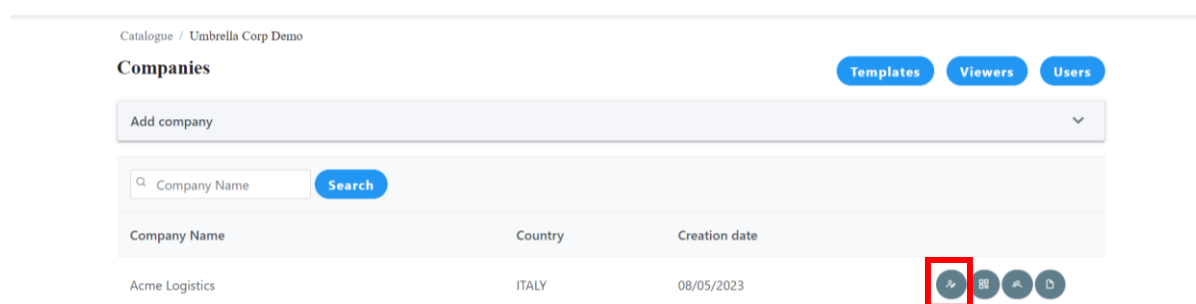

FIGURE 3

5 CREATING A USER

Safe LTA allows a Manager user to configure a new user. A Group Manager can register the following new users at the Company Group level: Manager, Enduser, Auditor.

A Manager registered at the company level can register the following users only for their respective company: Manager, Enduser, Auditor.

5.1 CREATING A USER AT COMPANY GROUP LEVEL

Safe LTA allows, as a Group Manager, the registration of other users with visibility across the group, such as Acme Group. To perform this operation, click on "**Users**" in the top right corner (Figure 4) and navigate to the user management screen.
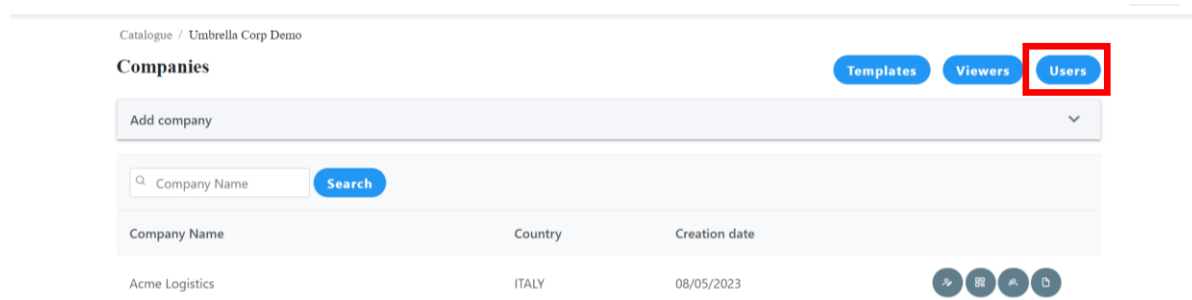

FIGURE 4

To register a new user, click on "**Add User**" and expand the data entry area (Figure 5). In this area, you can define the user's username and password and specify the user type (Manager, Enduser, Auditor). You can also provide the full name of the new user. Once you have entered the data, click on the "**Create User**" button.
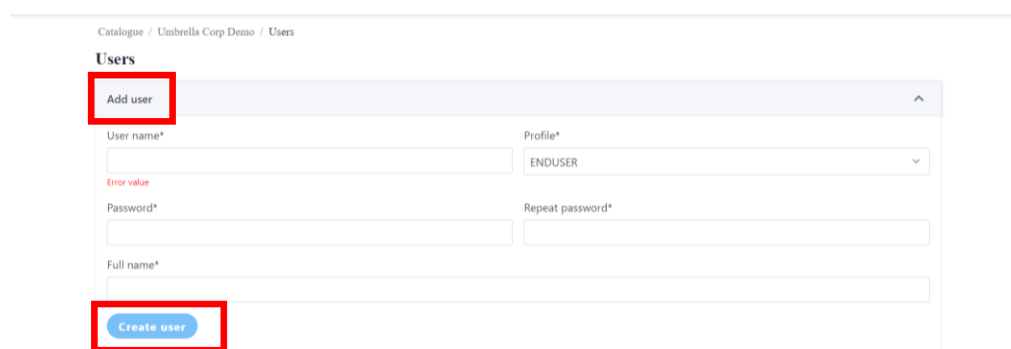

FIGURE 5

5.2 CREATING A USER AT COMPANY LEVEL

Similarly to the previous paragraph, it is possible to register a specific user for a given Company and provide access only to the relevant business objects of that company (e.g., "Acme Logistics" as shown in Figure 6). This can be done by clicking on the "**Users**" function for a specific Company.
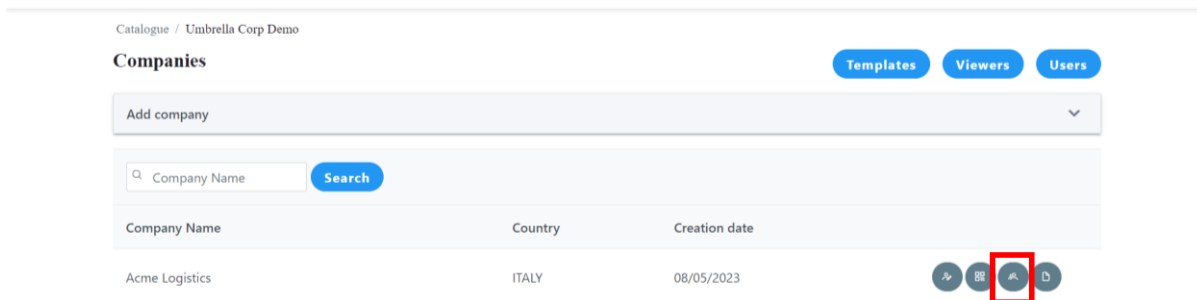

FIGURE 6

At that point, the creation of the user follows the same principles described earlier.

6 CREATING A TEMPLATE

Safe LTA allows the definition of templates to facilitate the subsequent creation of Document Classes. To create a template, click on the dedicated option in the top right corner (Figure 7).
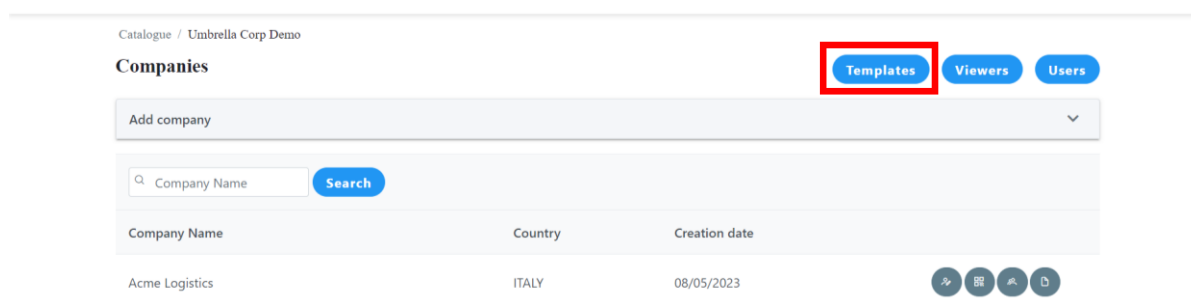

FIGURE 7

At this point, by expanding the data entry area, you can proceed with defining the necessary parameters such as Name, Retention Period, Schema, as well as the metadata and MIME type associated with the template. To create the template, click on "**Create Template**".

After creating the template, it will be saved as a draft and can be modified at any time through the dedicated menu. To use the template, it needs to be published using the appropriate option (Figure 8). It is always possible to disable the template from the same section.
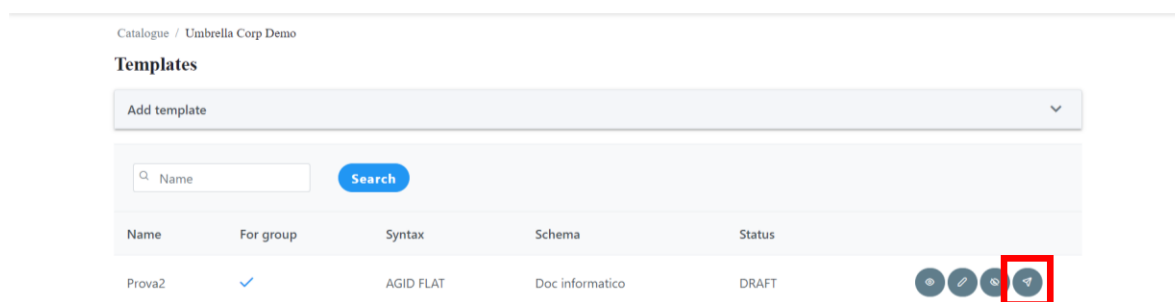

FIGURE 8

7 CREATING A DOCUMENT CLASS

Safe LTA allows a Manager user to define one or more Document Classes for a specific Company. A Manager user can also determine whether one or more Document Classes should be used by all users registered within that specific Company, or if they should be limited to only certain users.

To define a Document Class for a Company, click on "**Document Classes**" (Figure 9), then expand the data entry area by clicking on "**New Document Class**".
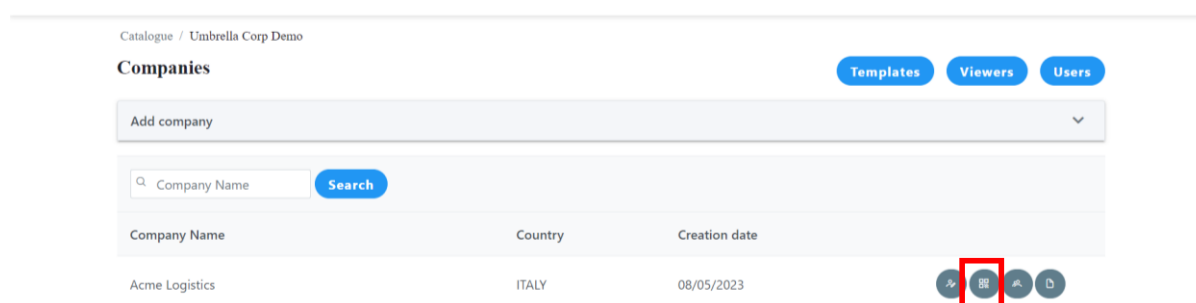
FIGURE 9

Specifically, you can define the following information for a Document Class:

- Reference Template, if previously created.

- Name.

- Mode: If the Company has the Country set to Italy, choosing "AGID" is mandatory.

- Schema.

- Retention period.

- Attributes (mandatory or optional), only if the Company does not have the Country set to Italy.

- MIME Type (mandatory or optional), which defines the file format associated with the documents that the Document Class will handle (e.g., PDF or images).

Once you have defined this information, click on the "**Create**" button (Figure 10).

Document Classes

Templates Manage viewers Manage users

New document class ∧

Template
Select template ▾

Document class name*
Prova1

Retention period
10

Allowed charset: [a-zA-Z0-9-_].

Attibutes

☑ Mandatory

Attribute name
test

Attribute type
string ▾

Regular expression

Add attribute

MIME types

☐ mandatory

Add another MIME type

Create

FIGURE 10

INFOCERT
TINEXTA GROUP

8 ASSOCIATING A DOCUMENT CLASS TO A SPECIFIC USER

As a Manager, you can associate a specific user with the newly created Document Class. To perform this operation, click on the "**Users**" button in the section of the specific Document Class (Figure 11).
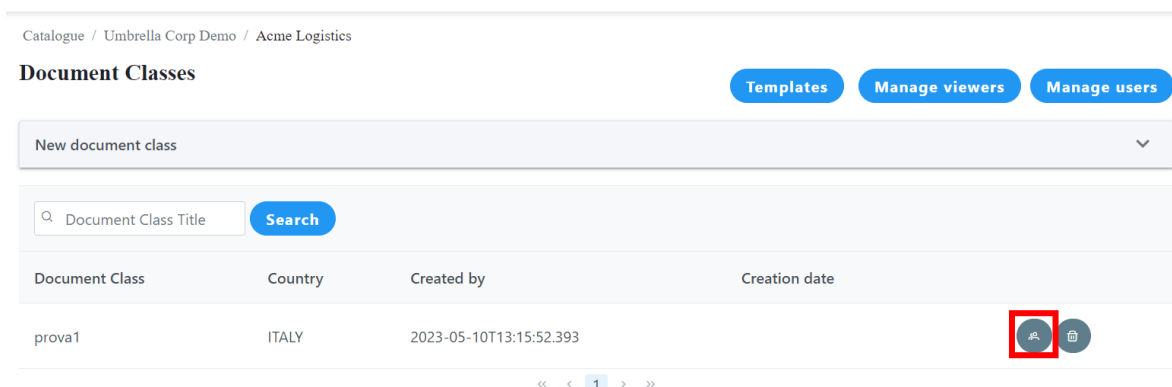

FIGURE 11

Similar to registering a new user, you will navigate to the user registration view, where the user will be enabled to use only the selected specific Document Class.

9 CREATING A VIEWER

Safe LTA also allows the storage of viewer software, which can be accessed during the display phase to ensure the readability of the preserved documents.

To add a new viewer, click on "**Viewers**" as shown in Figure 12.
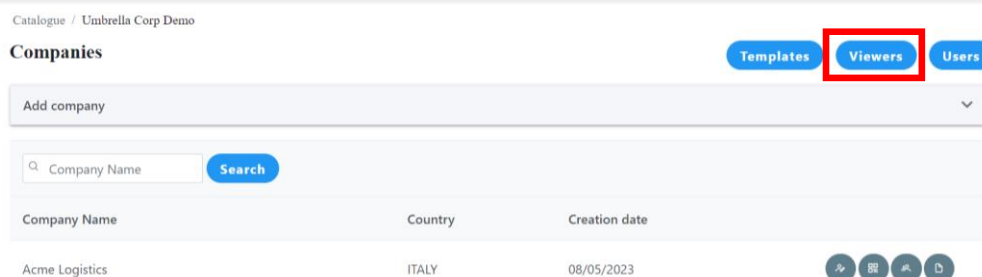
FIGURE 12

At that point, expand the selection area to define the viewer's information such as name and the MIME types (formats) it can handle. To complete the process, select the appropriate option to upload the software file from your device, then click on "**Create Viewer**" (Figure 13).
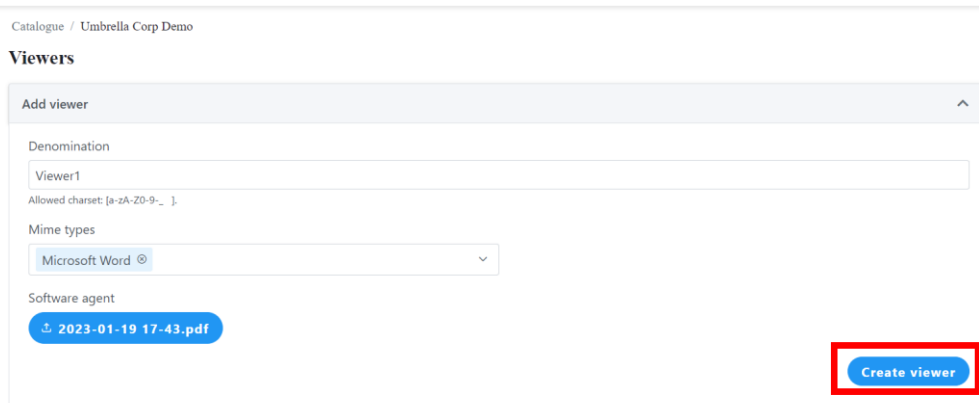
FIGURE 13

10 UPLOADING A DOCUMENT

Safe LTA allows an Enduser user to store a document by associating it with a specific Document Class. An Enduser user can only access the Document Classes associated with them or those that are generally available at the Company level without any restrictions.

To store a document, click on "**Ingestion**" in the left column of the dashboard, as shown in Figure 14.
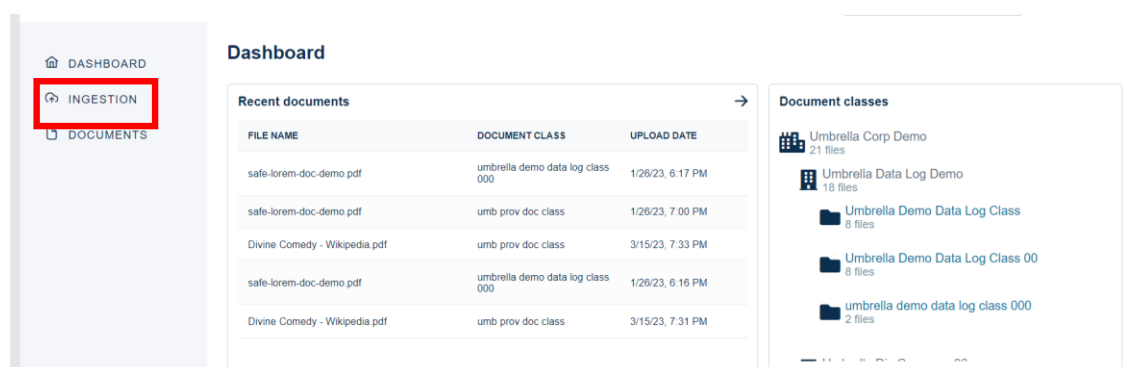

FIGURE 14

After selecting the file to be stored, the user will need to follow the instructions to enter the data related to the specific Document Class of their interest to complete the document upload.

The user will initially enter the first set of document data, referring to the Producer (e.g., the company associated with the Company) and the Submitter, who is usually the actor performing the storage. As shown in Figure 15, the user will also need to indicate: a name to associate with the document, the corresponding Document Class, and the file format to be preserved (MIME Type).
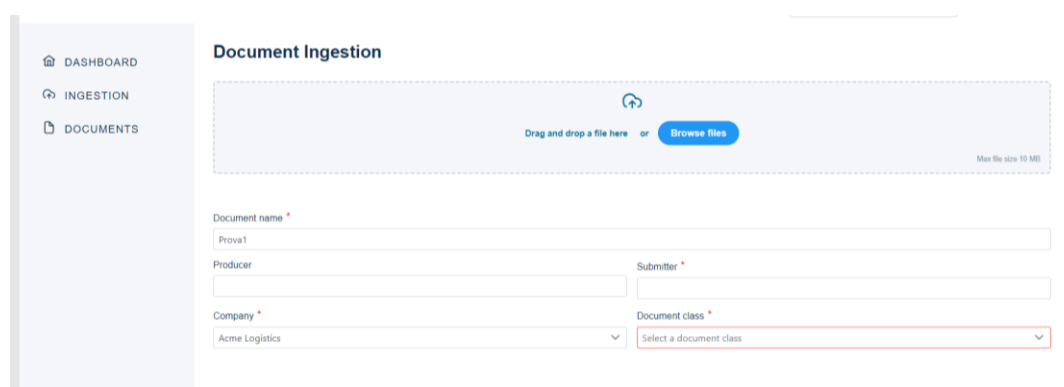

FIGURE 15

Next, you will proceed to the metadata section, which represents the attributes defined by the Manager and identifies the Document Class.

It will be mandatory to populate the required metadata set for the specific Document Class. Additionally, if the Company does not have the country set as Italy, you can also enter custom metadata. If the Company is set as Italy, a predefined metadata input area will be presented, adhering to the AgID guidelines for metadata in Italy.

Once you have finished entering the necessary metadata, you can submit the document for storage by clicking on the "Submit" button at the bottom of the page. The successful upload will be indicated on the screen.

11 SEARCHING FOR A DOCUMENT

Safe LTA allows users, regardless of their role, to search for stored documents based on the attributes defined in the Document Classes. Each user can only search for documents that they have visibility to.

To perform a search, you need to click on the "**Documents**" menu, as indicated in Figure 16.
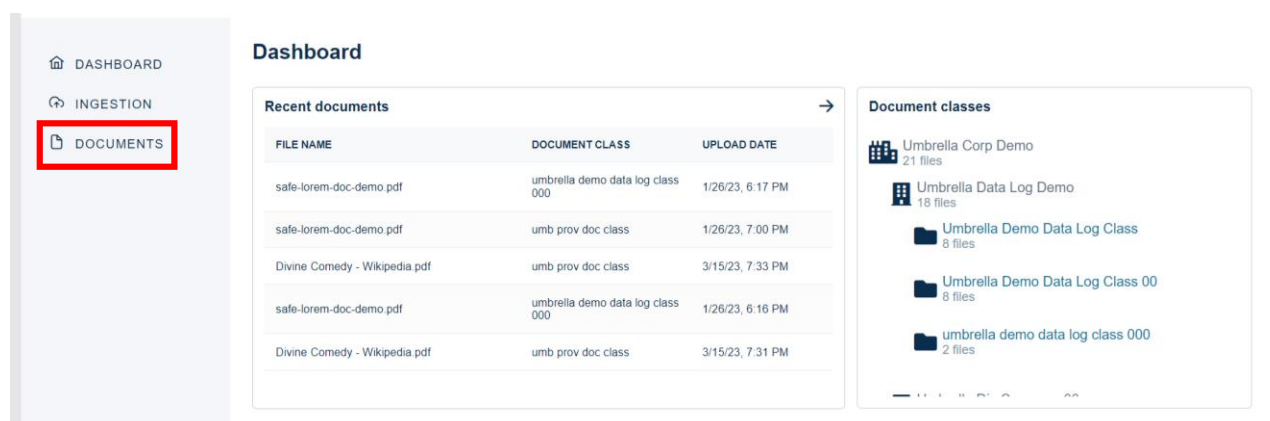

FIGURE 16

Through the search dashboard, you can search for a document by name or filter the search based on the attributes provided by the Document Classes, after specifying the Company and Document Class of the document, as shown in Figure 17.
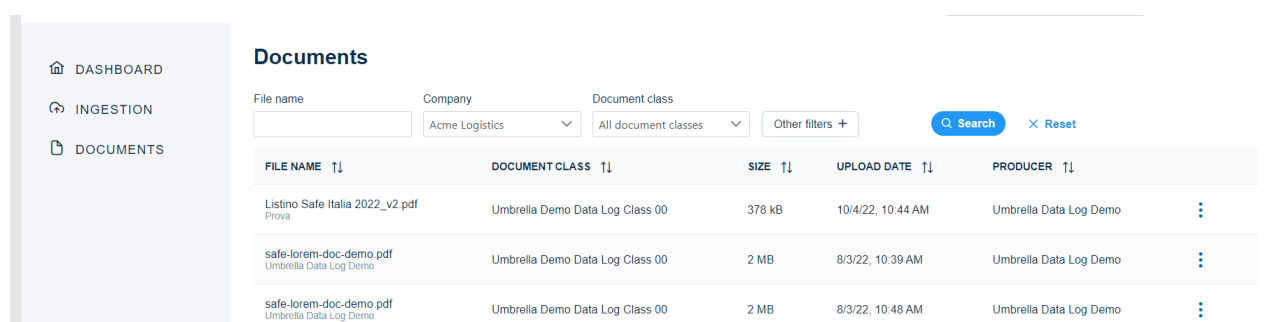

FIGURE 17

12 DOCUMENT DETAILS AND DOWNLOAD

An authorized user can view the details of a document and request its download, either for the individual document being preserved or for the entire preservation package.

Figure 18 shows the contextual menu that allows for download requests and access to the detailed view of the preservation package, as well as the display of uploaded viewers capable of reading that document.
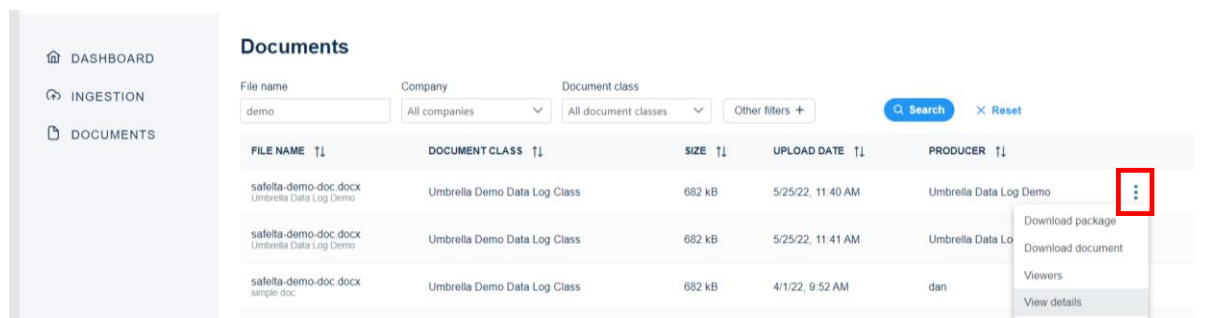

FIGURE 18

The information displayed in the detail screen includes:

- Company Group, Company, Producer, user who performed the preservation, document class;

- File name, format, upload date, and retention period expiration date;

- Metadata: attributes entered and their associated values provided by the operator during preservation (to view all of them, click on "Show more");

- Integrity data in terms of hash or fingerprint;

- Information related to the audit trail.

13 DISTRIBUTION PACKAGE (DIP) CONTENT

The package distribution (PDD) file that is returned to the user after requesting a download consists of the following structure:

deposit_slip	Folder containing the signed deposit report
doc_sign_validation_report	Folder containing audit information of signature objects, if any, in the preserved document

metadata/descriptive	Folder containing:
	• AGID metadata, sent to preservation by the client along with the document, as required by AGID technical documents
	• additional metadata required by InfoCert, which define:
	    • the title assigned to the package
	    • the producing subject
	    • the submitter

metadata/preservation	Folder containing data related to the actions taken during the preservation process, in compliance with the PREMIS standard.
PIndex.xml	Package descriptor, in compliance with the UNISINCRO standard.
PIndex_signed.xml	Package descriptor, compliant with the UNISINCRO standard, including the eSEAL signature and Timestamp Markings applied by InfoCert.
representations/rep1/data	Folder containing the document effectively submitted for preservation by the client.

representations/rep1/metadata/preservation	Folder containing additional files, in compliance with the PREMIS standard, that describe:
	    • The file submitted for preservation
	    • Information on integrity checks (checksums)

schemas	Folder containing the XSD schemas used by the standard, AGID, and InfoCert.

14 VALIDATION REPORT

The user can request a validation report by clicking on the "Validation Report" button (Figure 19).
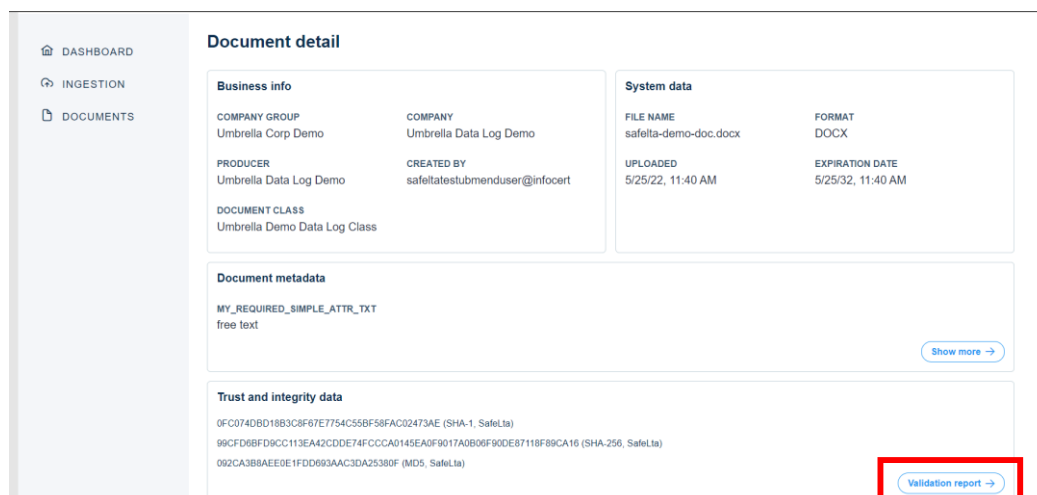

FIGURE 19

The outcome of the report will be divided into three sections (Figure 20, Figure 21, Figure 22).

In the first view, the integrity of the document is verified (by comparing the hashes generated during the preservation phase with those calculated during the **Validation Report** request).
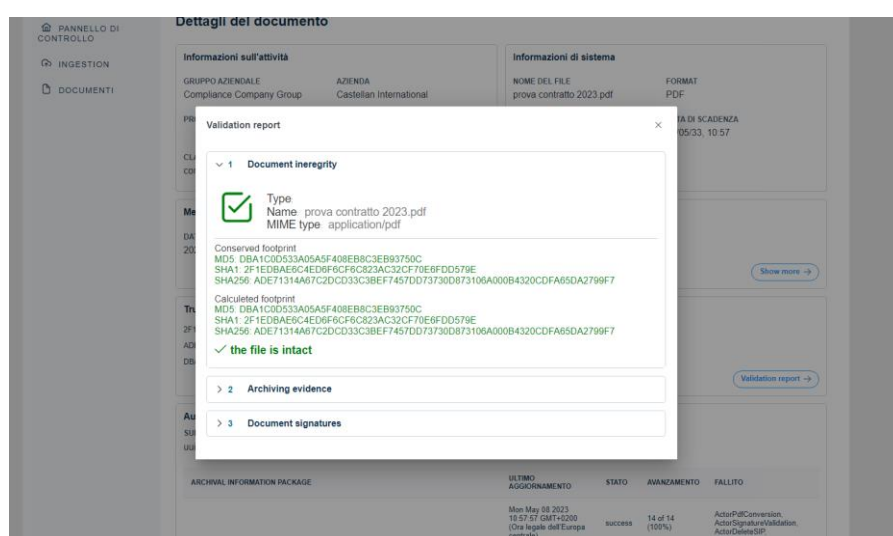

FIGURE 20

In the second view, information related to the signature and timestamp applied to the package description file (e.g., METS_FULL_signed.xml) is displayed, along with additional information about the used electronic certificate.
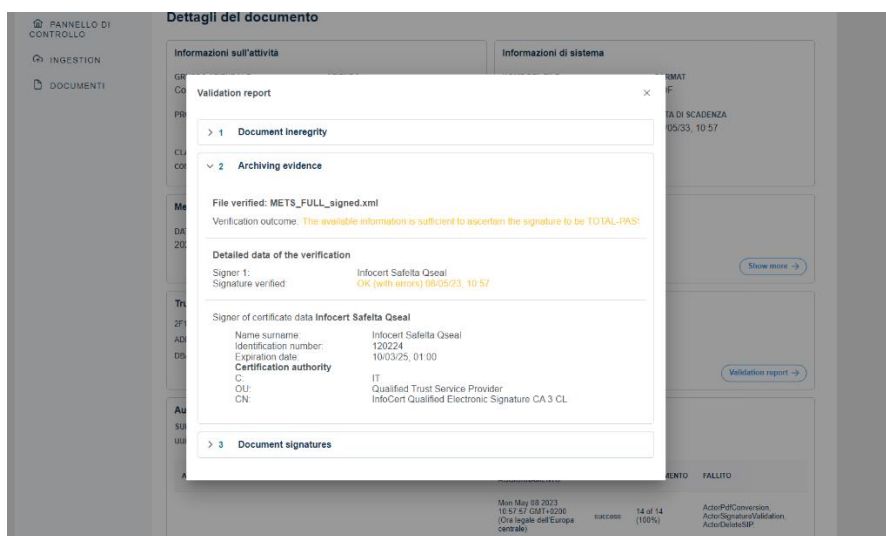

FIGURE 21

In the third view, information regarding any signatures present in the document is displayed.
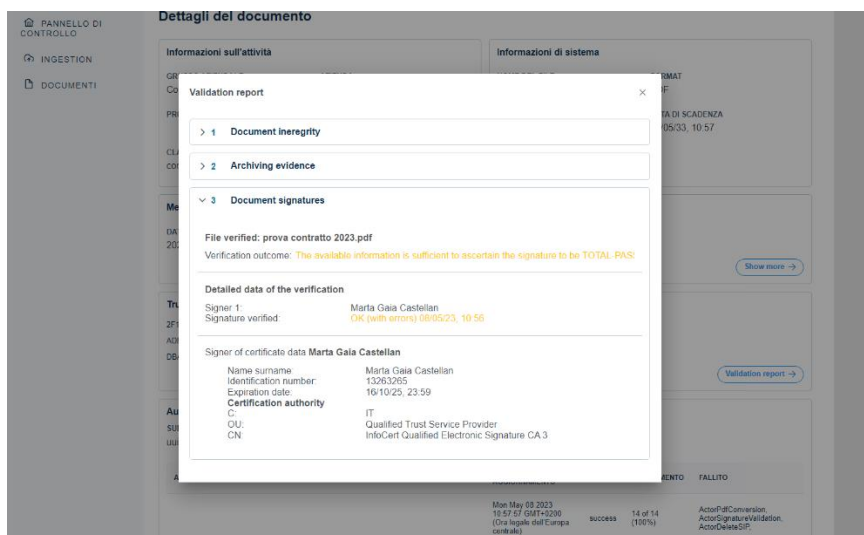

FIGURE 22

15 USAGE STATISTICS

An user can access the "Control Panel" section, from which they can view the usage statistics of the platform.

This provides information about the usage of the platform over time in terms of uploaded (archived) and downloaded documents. It also indicates the storage space occupied by documents and metadata.

As shown in Figure 23, the user can also filter the "Usage in Time" data based on the desired period (e.g., current month, last year, etc.), as well as view the data in terms of document quantity or size.
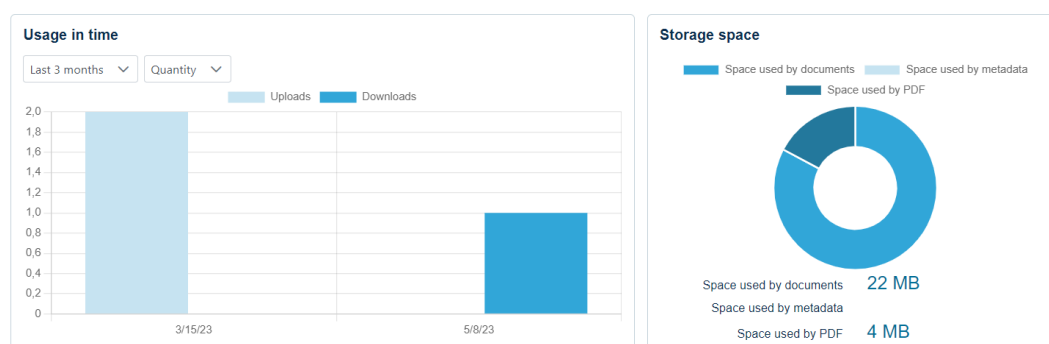

FIGURE 23