Evidence 2.3.0
User manual
Rev. A

Index

Chapter I

1 Welcome to the Digifort 2.3.0 manual

This user manual and technical references provide all information necessary to effectively implement and use all of the basic and advanced features found in Evidence 2.3.0. This manual is constantly updated and does not describe the features of the Beta or Dev versions of the system.

1.1 Screenshots

The screenshots contained in this manual may not be identical to the interface you will see using the software. Some differences may appear, without affecting the use of this manual. This is due to the fact that frequent updates and inclusion of new features are carried out with the aim of continually improving the system.

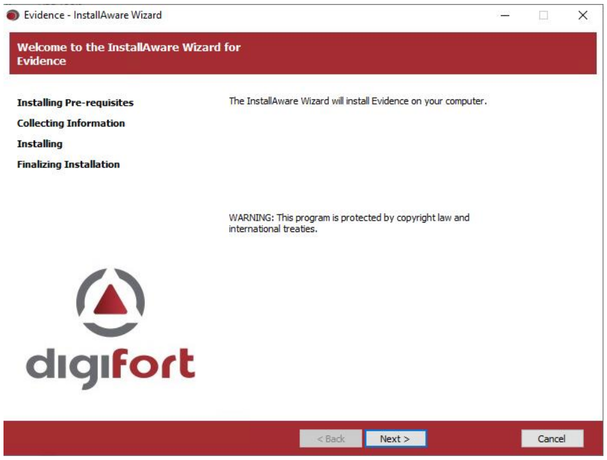
1.2 Who is this manual for

This manual is intended for system administrators and operators.

Chapter II

2 Installing the system

After running the installation program file, follow the steps below to install the system.



Evidence - InstallAware Wizard

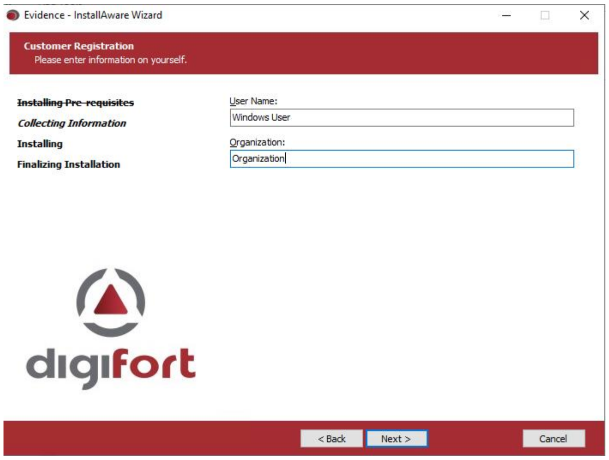
Welcome to the InstallAware Wizard for Evidence

Installing Pre-requisites
Collecting Information
Installing
Finalizing Installation

The InstallAware Wizard will install Evidence on your computer.

WARNING: This program is protected by copyright law and international treaties.

Click **Next.**



Evidence - InstallAware Wizard

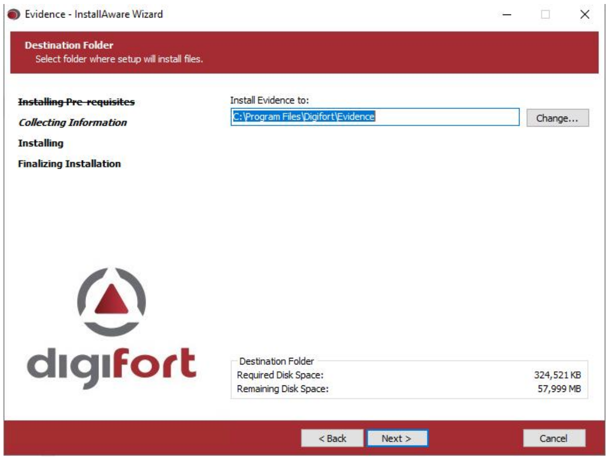
Customer Registration
Please enter information on yourself.

~~**Installing Pre-requisites**~~
Collecting Information
Installing
Finalizing Installation

User Name: Windows User

Organization: Organization

Enter your registration information and click **Next.**



Evidence - InstallAware Wizard

Destination Folder
Select folder where setup will install files.

~~**Installing Pre-requisites**~~
Collecting Information
Installing
Finalizing Installation

Install Evidence to: C:\Program Files\Digifort\Evidence

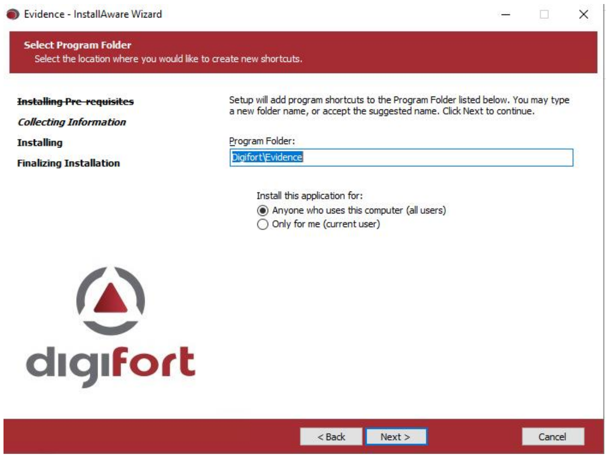
Destination Folder

Required Disk Space:	324,521 KB
Remaining Disk Space:	57,999 MB

Select the location where the files will be installed and click **Next**.

Important

! In addition to the files necessary for the system to function, a database instance will be initialized in this folder. The database is responsible for storing all system data.



Evidence - InstallAware Wizard

Select Program Folder

Select the location where you would like to create new shortcuts.

~~Installing Pre-requisites~~

Collecting Information

Installing

Finalizing Installation

Setup will add program shortcuts to the Program Folder listed below. You may type a new folder name, or accept the suggested name. Click Next to continue.

Program Folder:

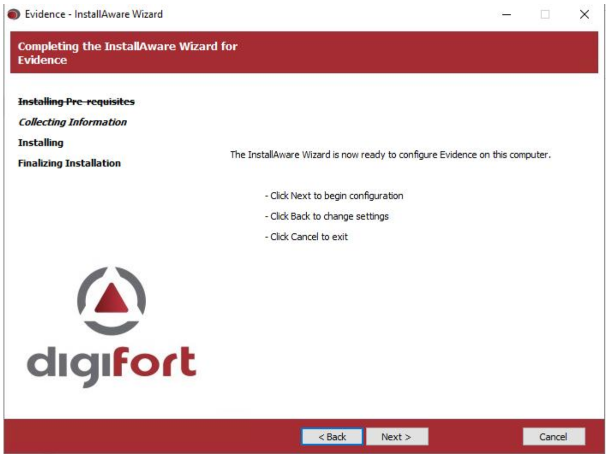
Digifort\Evidence

Install this application for:

● Anyone who uses this computer (all users)

○ Only for me (current user)

Select the Windows start menu folder where the shortcuts will be created and click **Next**.



Evidence - InstallAware Wizard

Completing the InstallAware Wizard for Evidence

~~Installing Pre-requisites~~

Collecting Information

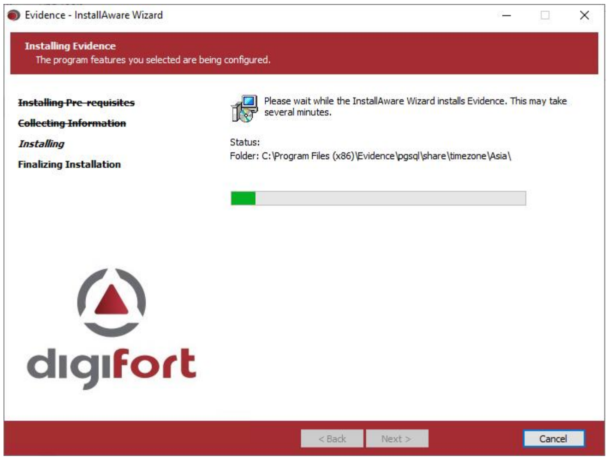
Installing

Finalizing Installation

The InstallAware Wizard is now ready to configure Evidence on this computer.

- Click Next to begin configuration
- Click Back to change settings
- Click Cancel to exit

Click Next again to confirm the settings and begin the installation.



Evidence - InstallAware Wizard

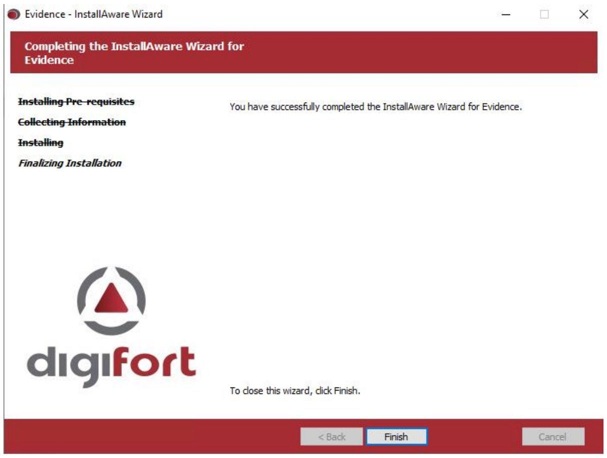
Installing Evidence
The program features you selected are being configured.

~~Installing Pre-requisites~~
~~Collecting Information~~
Installing
Finalizing Installation

Please wait while the InstallAware Wizard installs Evidence. This may take several minutes.

Status:
Folder: C:\Program Files (x86)\Evidence\pgsql\share\timezone\Asia\

Wait for the installation process.



Evidence - InstallAware Wizard

Completing the InstallAware Wizard for Evidence

~~Installing Pre-requisites~~
~~Collecting Information~~
~~Installing~~
Finalizing Installation

You have successfully completed the InstallAware Wizard for Evidence.

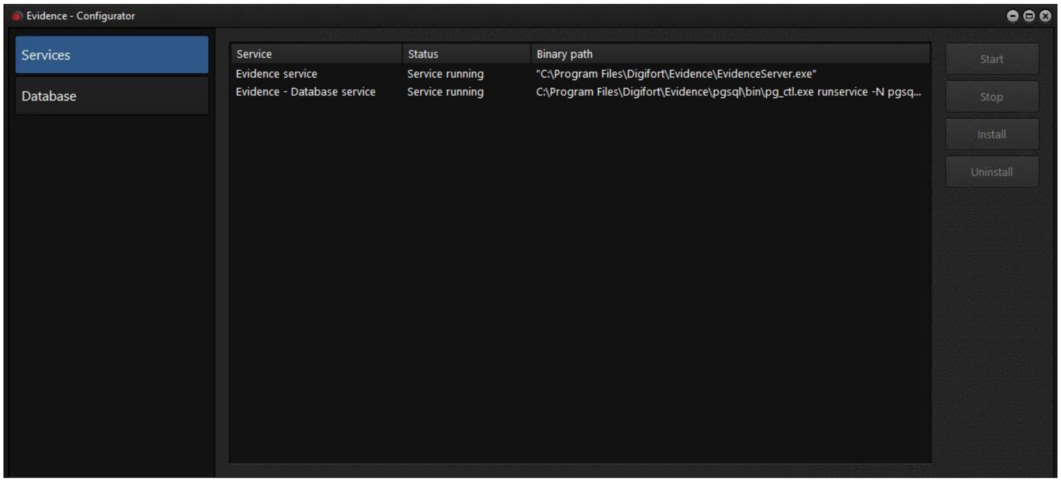
To close this wizard, click Finish.

Click **Finish** to complete the installation.

Chapter III

3 Post installation

After installing Evidence, the configuration software will run automatically, as shown in the image below:



Service	Status	Binary path
Evidence service	Service running	"C:\Program Files\Digifort\Evidence\EvidenceServer.exe"
Evidence - Database service	Service running	C:\Program Files\Digifort\Evidence\pgsql\bin\pg_ctl.exe runservice -N pgsq...

This application can be run later to perform some configuration tasks. Simply locate it on the Windows desktop or start menu.

3.1 Managing services

Evidence is a software developed on the web client-server platform, taking advantage of all the features and benefits that this platform provides.

In this type of platform, all information is stored on a central server responsible for its management. The server is the component responsible for, among other functions, maintaining created incidents, configurations and allowing users to navigate the system through an Internet browser.

The Evidence Server is an application that runs as a Windows service, therefore, it runs automatically when Windows starts, without the need for user intervention.

The Service Manager is the software responsible for controlling its execution, showing information about its operating state and providing service installation and startup controls.

This solution is made up of two services responsible for different functions:

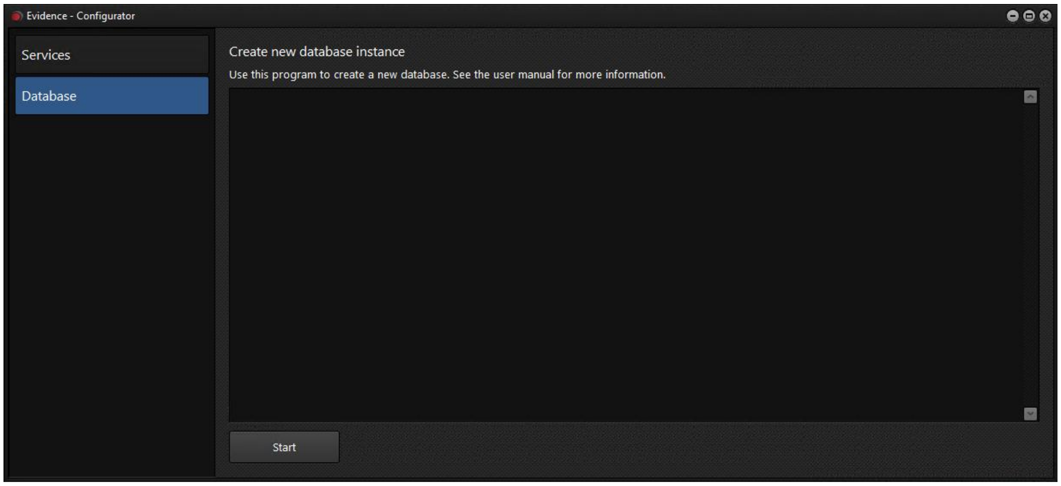
- **Evidence:** This is the service responsible for, among other functions, maintaining created incidents, configurations and allowing users to navigate the system through an Internet browser.
- **Evidence - Database:** This service provides access to a PostgreSQL database, responsible for storing configurations and incidents.

To perform the actions of starting, stopping, installing or uninstalling services, simply select the desired service and click on the corresponding button.

Important
! Before starting the services for the first time, it is necessary to create the database. See the topic Creating database.

3.2 Creating the database

After installing Evidence, before the first run, it is necessary to create the system database. To accomplish this task, locate the **Database** menu in the side menu.



Create new database instance

Use this program to create a new database. See the user manual for more information.

When you click the **Start** button, the program will try to create a new database in the location C:\PostgreSQLData\Evidence.
If the operation is successful, the services can be started. See the topic Managing services.

3.3 Starting a database from scratch

If necessary, you can delete the current database and start a new one from scratch.

Follow the steps below:

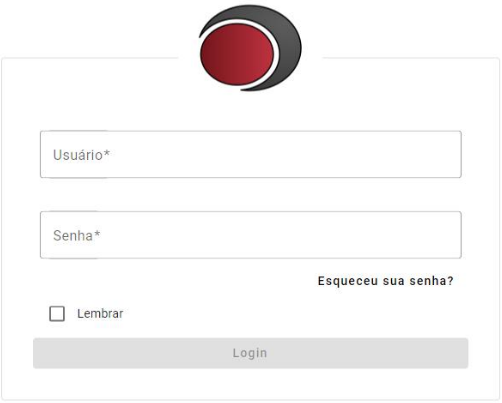
1. Stop all services using the service manager. Managing services.
2. Delete the C:\PostgreSQLData\Evidence folder manually.
3. Delete the incidents folder. You can see the current folder in Configuring the repository.
4. Create a new database. Creating database.
5. Start the services again using the service manager. Managing services.

! **Important**
By performing the above procedure, all data will be lost and cannot be recovered.

Chapter IV

4 Accessing the system for the first time

The system must be accessed via the Internet browser using the link:
https://127.0.0.1:4433



Enter the username and password to access the system.

Important
The default user has the following credential:
User: admin
Password: admin

Important
For security reasons, we recommend changing the admin user password upon first access.

4.1 First configuration steps

Use the following steps to have your system ready to use:

1. Add the licenses to the software. See the topic Licensing.
2. Prepare system settings. See the topic System settings.
3. Add the Digifort servers. See the topic Digifort servers. You can skip this step if you don't need to import users or add cameras to incidents.
4. Add or import users. See the topic Users.
5. Add user groups to define their permissions. See the topic User groups.
6. Add incident priorities. See the topic Priorities.
7. Add incident forms. See the topic Forms. You can skip this step if you don't need to add custom fields to the incident form.
8. Add incident types. See the topic Incident types.

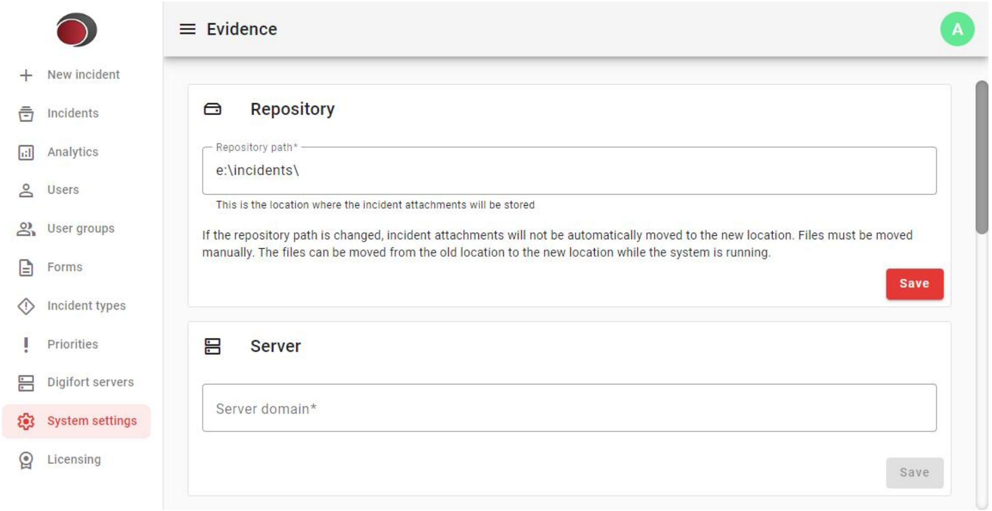
Chapter V

5 System serttings

The system settings module is a crucial tool that allows administrators to adjust and customize various functionalities. This module offers a set of options that help adapt the system to the organization's specific needs, ensuring that it operates efficiently and aligned with internal processes.

5.1 Accessing system settings

In the side menu, click on the **System Settings** option to access the module.



Repository

Repository path*: e:\incidents\

This is the location where the incident attachments will be stored

If the repository path is changed, incident attachments will not be automatically moved to the new location. Files must be moved manually. The files can be moved from the old location to the new location while the system is running.

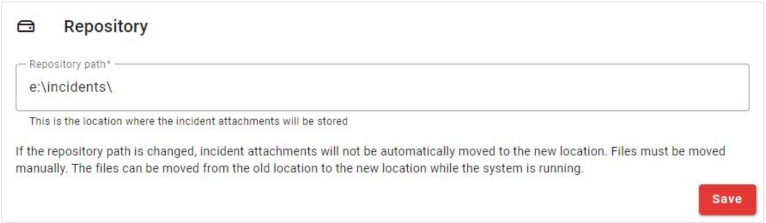
Server

Server domain*

5.2 Configuring the repository

Defining the repository is a crucial step in system configuration, as this is where files attached to incidents will be stored. Depending on how the system is used, it is very likely that the demand for disk space will be high, so you can choose to specify a dedicated disk or storage unit or a mapped network drive.

Important
By default, the system is configured to save data in a subfolder of the location where it is installed.



Repository

Repository path*: e:\incidents\

This is the location where the incident attachments will be stored

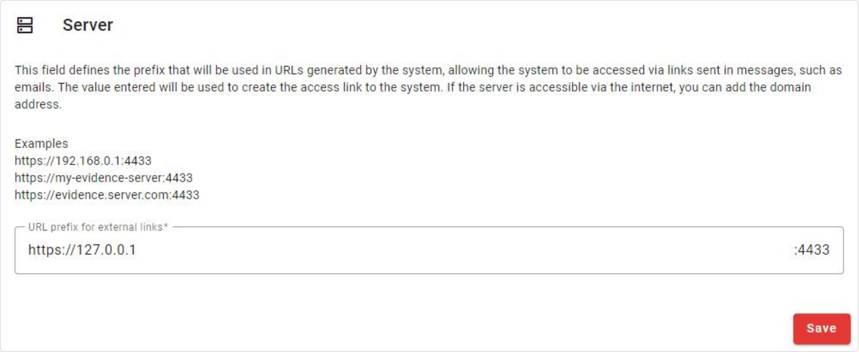
If the repository path is changed, incident attachments will not be automatically moved to the new location. Files must be moved manually. The files can be moved from the old location to the new location while the system is running.

5.3 Server settings

Sometimes the system needs to generate links that can be used to access some area of the system. For example, when a user wants to recover their password through the login form. In this case, the system will send an email to the user with the link to reset the password. This link is generated based on this information, which tells how the system can be accessed externally.
You can set this address based on the following examples:

- https://192.168.0.1:4433. Points to the server's IP address.

- https://evidence-server:4433. Points to the server name.
- https://www.company-name:4433. Points to the FQDN of the server where the system is hosted.



Server

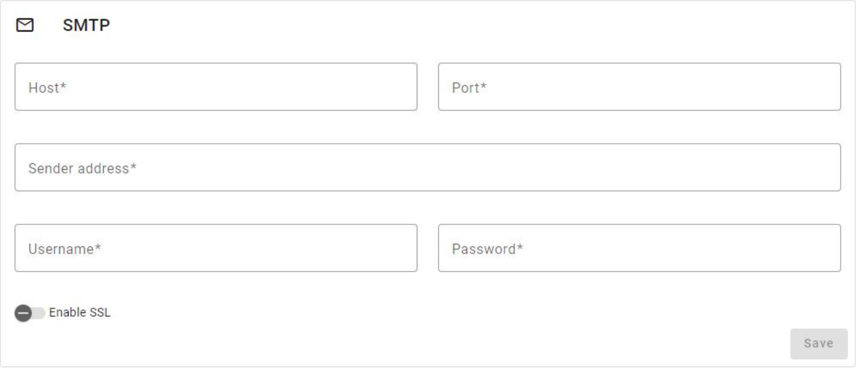
This field defines the prefix that will be used in URLs generated by the system, allowing the system to be accessed via links sent in messages, such as emails. The value entered will be used to create the access link to the system. If the server is accessible via the internet, you can add the domain address.

Examples
https://192.168.0.1:4433
https://my-evidence-server:4433
https://evidence.server.com:4433

URL prefix for external links*: https://127.0.0.1 :4433

5.4 Configuring the SMTP server

SMTP configuration, used by the system to send emails.



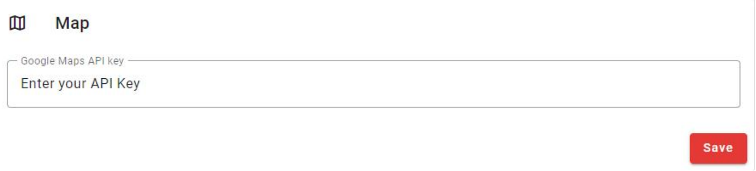
- **Address:** SMTP server address.
- **Port:** SMTP server port.
- **Sender:** Email address that will be used to send emails.
- **User:** SMTP server username.
- **Password:** User password.
- **Enable:** SSL: Enables communication using SSL.

5.5 Map settings

Use the field below to set the Google Maps API key.
Google Maps is used in some areas of the system, such as the custom location field.

The following services must be activated on your key:

- Maps JavaScript API
- Geocoding API
- Maps Static API
- Places API



Map

Google Maps API key

Enter your API Key

Chapter VI

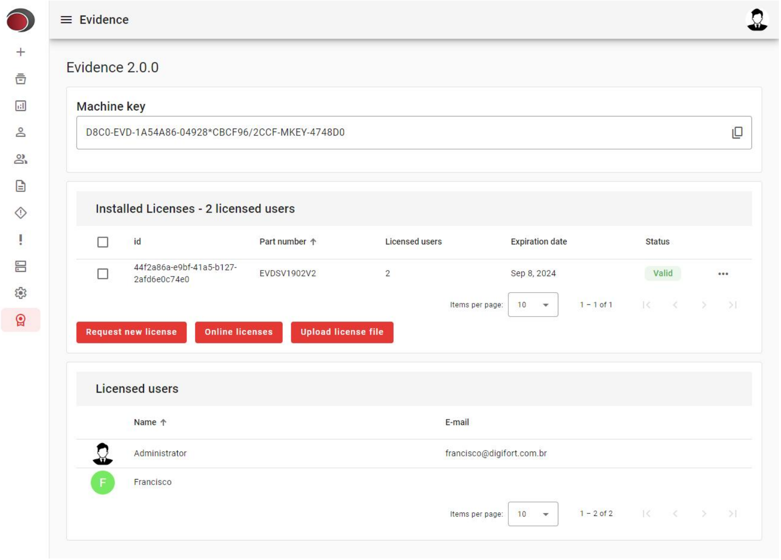
6 Licensing

Evidence must be licensed for incident insertion and search functionality to be enabled.
All configuration features do not require a license.

Licenses enables a certain number of users to use the system. Multiple licenses can be added to free up more users.

6.1 Accessing the licensing module

In the side menu, click on the **Licensing** option to access the module.



Evidence 2.0.0

Machine key

D8C0-EVD-1A54A86-04928*CBCF96/2CCF-MKEY-4748D0

Installed Licenses - 2 licensed users

□	id	Part number ↑	Licensed users	Expiration date	Status	
□	44f2a86a-e9bf-41a5-b127-2afd6e0c74e0	EVDSV1902V2	2	Sep 8, 2024	Valid	•••

Items per page: 10 1 – 1 of 1

Licensed users

	Name ↑	E-mail
	Administrator	francisco@digifort.com.br
F	Francisco	

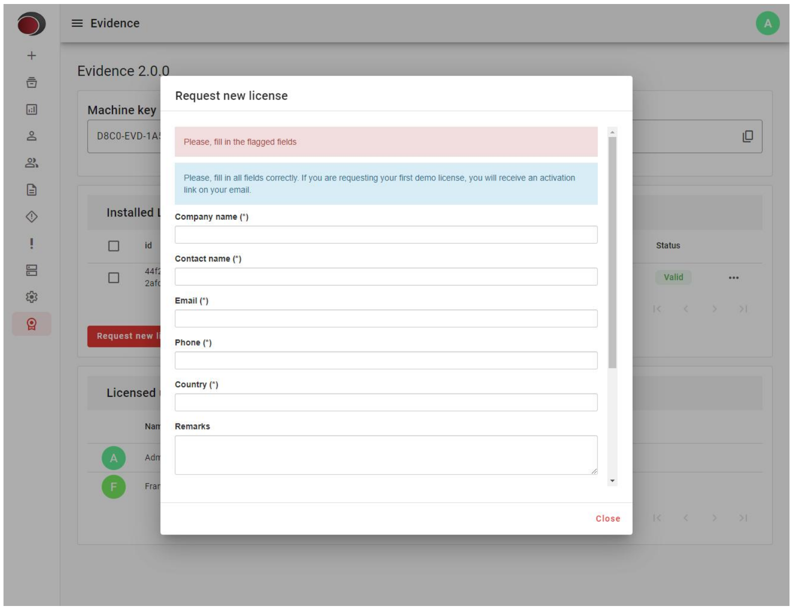
Items per page: 10 1 – 2 of 2

Machine key

Licenses are generated exclusively for your server based on this unique ID called **Machine Key**.

6.2 Requesting new licenses

To request new licenses that you have purchased or trial licenses for the software, click the **Request new license** button.



Request new license

Please, fill in the flagged fields

Please, fill in all fields correctly. If you are requesting your first demo license, you will receive an activation link on your email.

Company name (*)

Contact name (*)

Email (*)

Phone (*)

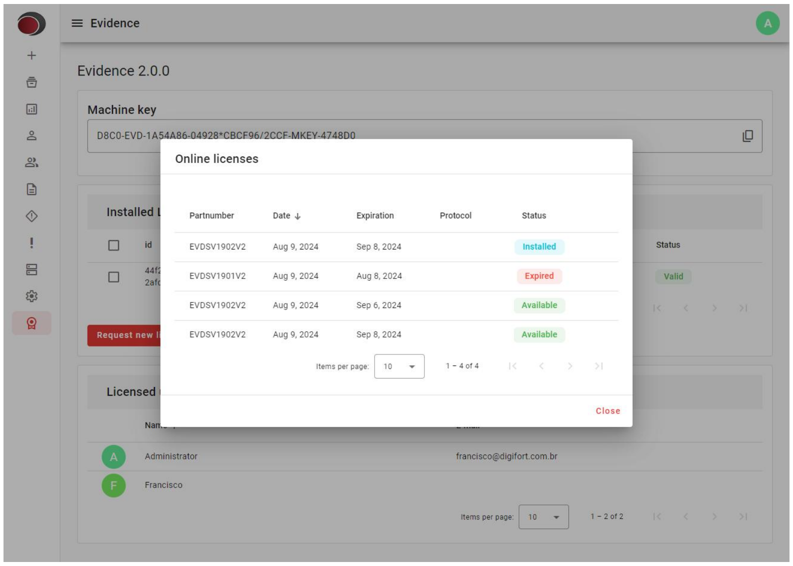
Country (*)

Remarks

Close

6.3 Adding new licenses online

Click the button **Online Licenses** to view all your licenses available for installation.



Machine key

D8C0-EVD-1A54A86-04928*CBCF96/2CCF-MKEY-4748D0

Online licenses

Partnumber	Date ↓	Expiration	Protocol	Status
EVDSV1902V2	Aug 9, 2024	Sep 8, 2024		Installed
EVDSV1901V2	Aug 9, 2024	Aug 8, 2024		Expired
EVDSV1902V2	Aug 9, 2024	Sep 6, 2024		Available
EVDSV1902V2	Aug 9, 2024	Sep 8, 2024		Available

Items per page: 10   1 – 4 of 4

Close

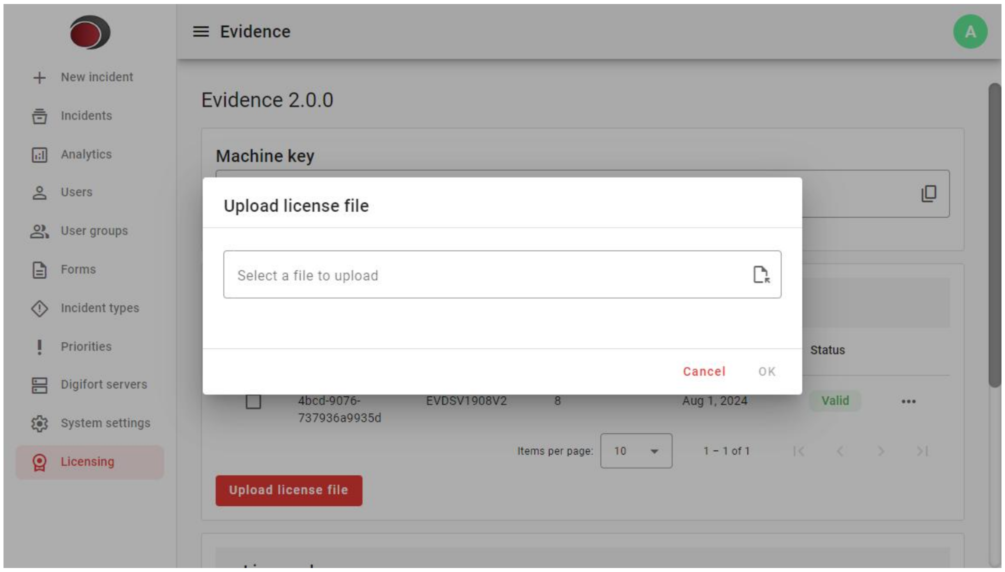
Name	E-mail
Administrator	francisco@digifort.com.br
Francisco	

Items per page: 10   1 – 2 of 2

To install a license, click the button + next to a license marked as available.

6.4 Adding license files

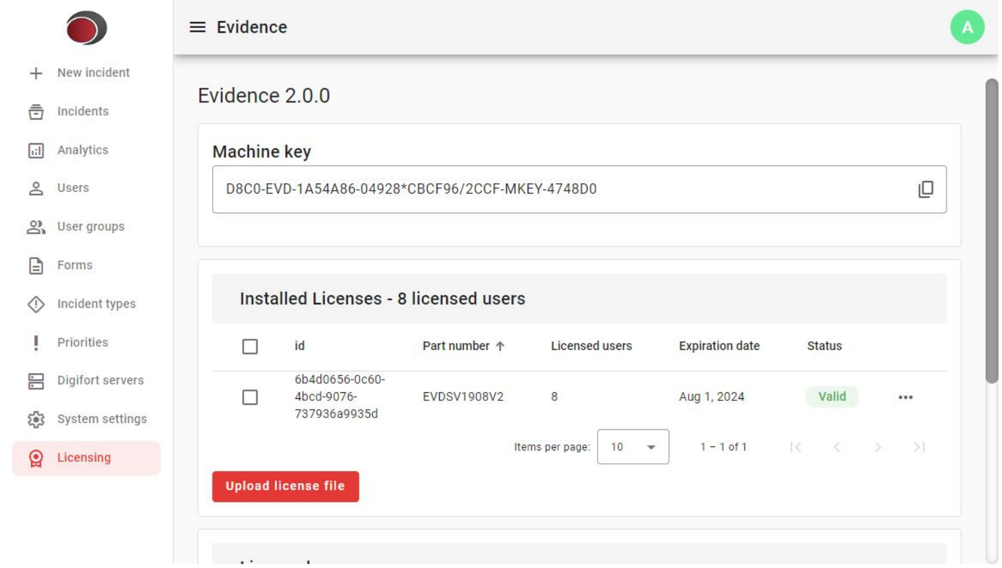
To add licenses, click the **Upload license file** button. Select the license file and confirm.



4bcd-9076-737936a9935d EVDSV1908V2 8 Aug 1, 2024 Valid

Repeat this operation for each license file to be added.

If the license is valid, your data will be displayed in the table on this page.



Evidence 2.0.0

Machine key

D8C0-EVD-1A54A86-04928*CBCF96/2CCF-MKEY-4748D0

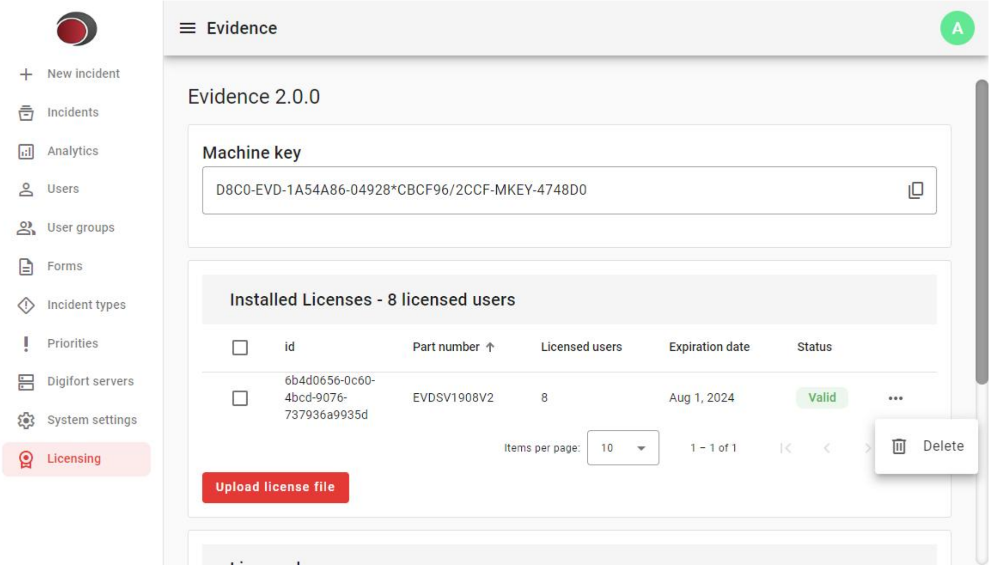
Installed Licenses - 8 licensed users

☐	id	Part number ↑	Licensed users	Expiration date	Status	
☐	6b4d0656-0c60-4bcd-9076-737936a9935d	EVDSV1908V2	8	Aug 1, 2024	Valid	•••

- **Id:** License identification
- **Part number:** License code
- **Licensed users:** Number of users enabled by this license.
- **Expiration date:** Expiration date of the license, if it is a trial license.
- **Status:** State of the license which can be **Valid**, **Invalid** or **Expired**.

6.5 Removing licenses

If necessary, licenses can be removed by clicking the 3-dot button next to each item, and then **Delete**.



Evidence 2.0.0

Machine key

D8C0-EVD-1A54A86-04928*CBCF96/2CCF-MKEY-4748D0

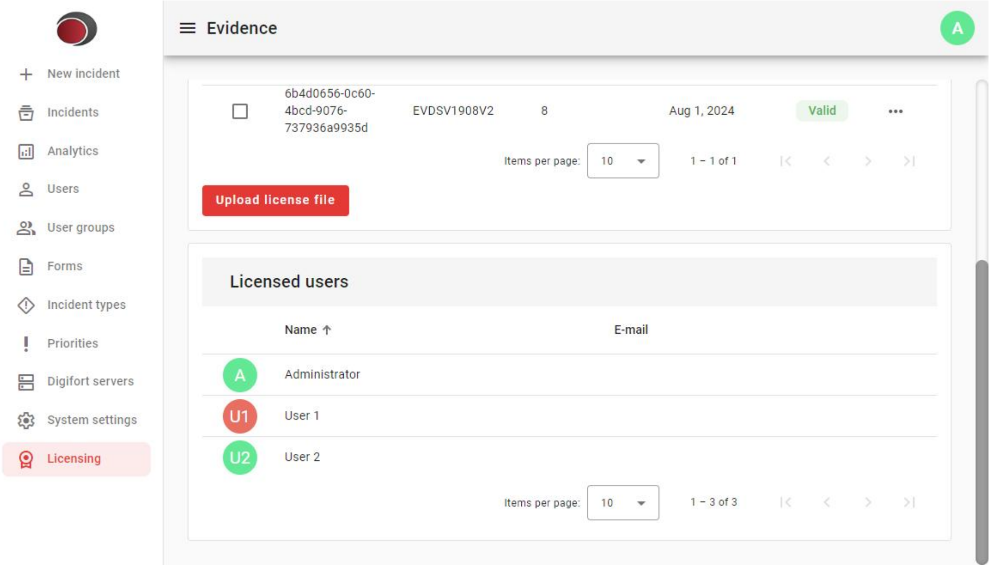
Installed Licenses - 8 licensed users

□	id	Part number ↑	Licensed users	Expiration date	Status
□	6b4d0656-0c60-4bcd-9076-737936a9935d	EVDSV1908V2	8	Aug 1, 2024	Valid

Items per page: 10 1 – 1 of 1

6.6 Viewing licensed users

Licensed users can be viewed at the bottom of the page.
If you do not have enough licenses for all users, you can suspend some users. Licenses are only applied to active users. See the topic Suspending users.



□	6b4d0656-0c60-4bcd-9076-737936a9935d	EVDSV1908V2	8	Aug 1, 2024	Valid

Items per page: 10 1 – 1 of 1

Licensed users

	Name ↑	E-mail
A	Administrator	
U1	User 1	
U2	User 2	

Items per page: 10 1 – 3 of 3

Chapter VII

7 Digifort servers

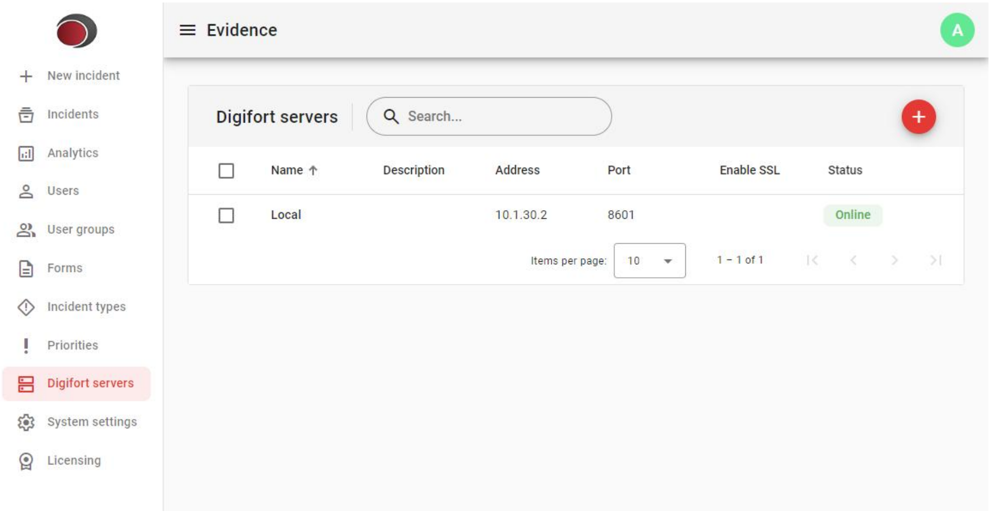
Evidence can be integrated with Digifort to add some functionality to both systems:

- Allows you to import users registered in Digifort. Imported users will be logged in directly to the server from which they were imported.
- Allows you to import videos from cameras and attach them to incidents.

Multiple servers can be imported to work at the same time.

7.1 Accessing the Digifort servers module

In the side menu, click on the option **Digifort Servers**.

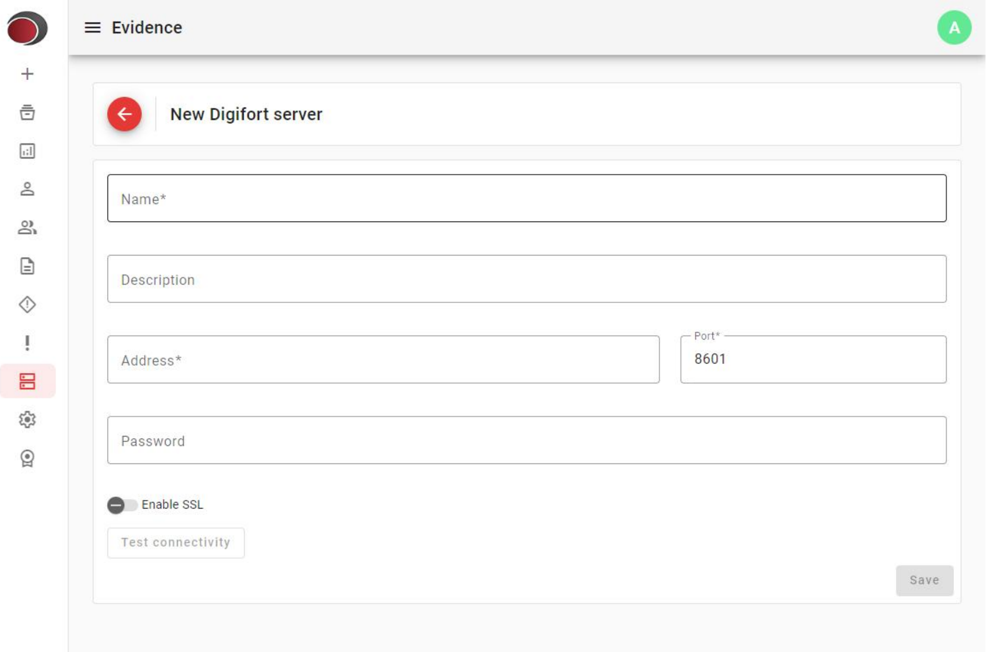


☐	Name ↑	Description	Address	Port	Enable SSL	Status
☐	Local		10.1.30.2	8601		Online

Items per page: 10 ▾ 1 – 1 of 1

7.2 Adding Digifort servers

To add servers, click the button ⊕.



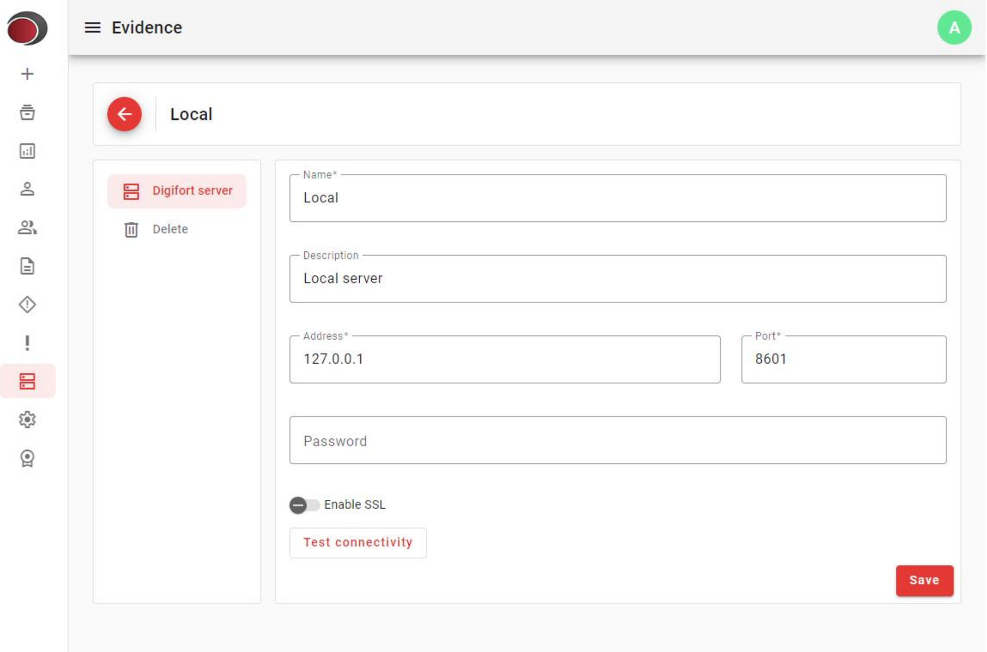
- **Name:** Server name.
- **Description:** An optional description.
- **Address:** IP address, computer name, or FQDN of the server.
- **Port:** TCP port
- **Password:** Password of the Digifort **admin** user.
- **Enable SSL:** Enables communication using SSL.

After filling in all the necessary data, you can click the **Test connectivity** button to validate the access settings.

At the end of the configuration, click the **Save** button. You will be automatically redirected to the server modification page. See the topic Modifying Digifort servers.

7.3 Modifying Digifort servers

To modify servers, click on the name of the server you want to modify.



Name* Local

Description Local server

Address* 127.0.0.1

Port* 8601

Password

Enable SSL

On the left side there is a menu where more settings can be made.

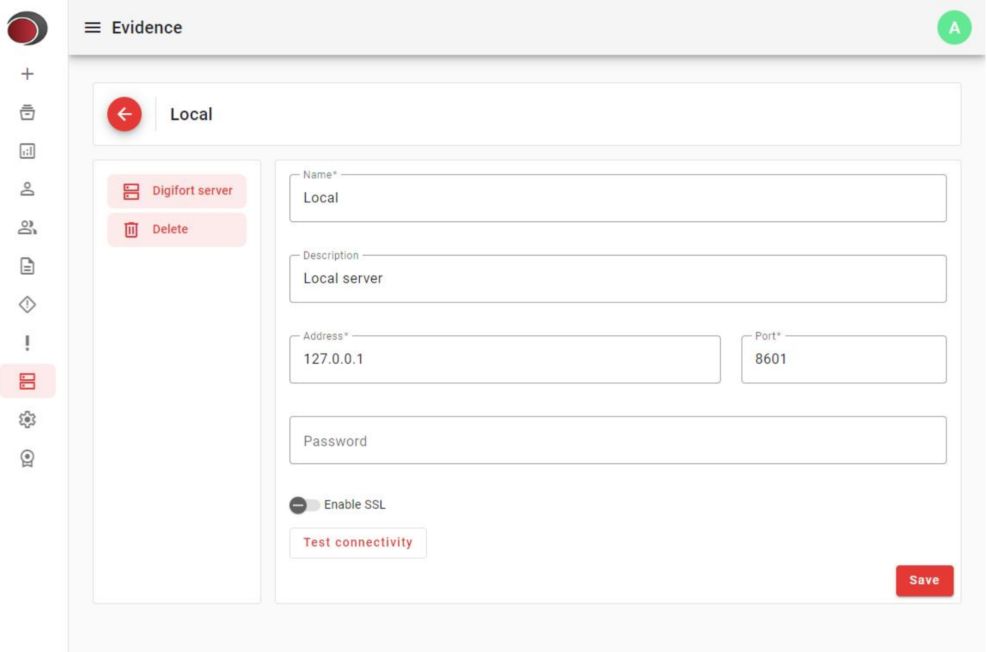
- **Digifort server:** Allows you to modify the server's main data.
- **Delete:**Removes the server from the system. See the topic Deleting Digifort servers.

7.4 Deleting Digifort servers

When deleting a server the following features will be removed:

- Users imported from this server will only be able to authenticate if there is another server added with the same registered users. See the topic User authentication process.
- Cameras from this server can no longer be imported and attached to incidents.

To delete servers, click the **Delete** button, as shown in the image below:



Name*: Local

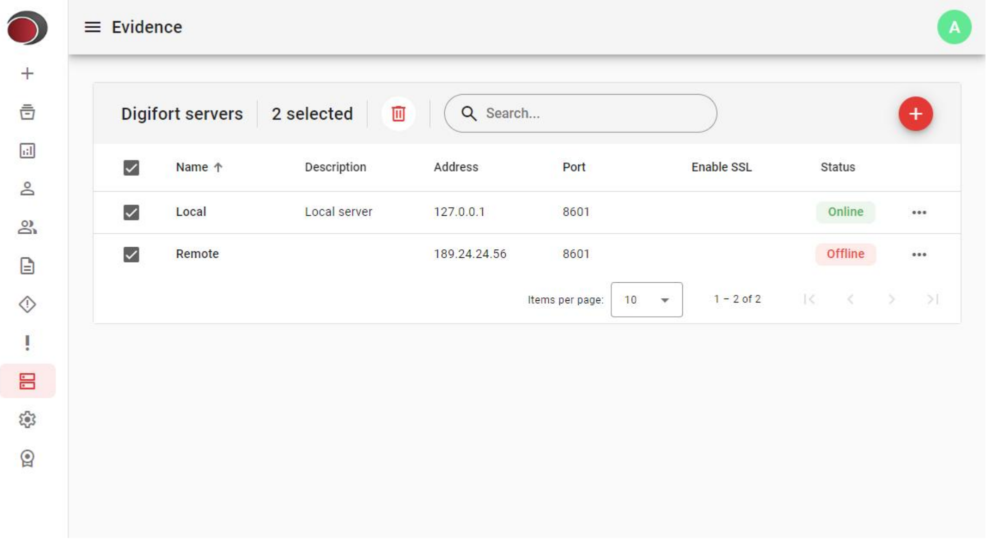
Description: Local server

Address*: 127.0.0.1

Port*: 8601

Password

Another way to exclude servers is through server registration. Next to each item there is a three-dot button with the option to remove it.
You can also use check boxes to remove more than one item at the same time. Select the items to be removed and then click 🗑 .



☑	Name ↑	Description	Address	Port	Enable SSL	Status	
☑	Local	Local server	127.0.0.1	8601		Online	•••
☑	Remote		189.24.24.56	8601		Offline	•••

Items per page: 10 1 – 2 of 2

Chapter VIII

8 Users

The user module allows the management of system users. This module is essential to ensure that only authorized people can access and interact with the software. Users can be registered manually or imported from Digifort, facilitating data integration and administration.

8.1 User types

Evidence can work standalone or integrated with Digifort.

The system provides 2 types of users:
- Native user
- Imported user

The way you will use the software will determine the type of user you will use. You can combine native and imported users to work at the same time.

8.1.1 Native user

Native users can use all software functions, except importing videos from Digifort to be included in incidents. See the topic Managing cameras.

8.1.2 Imported user

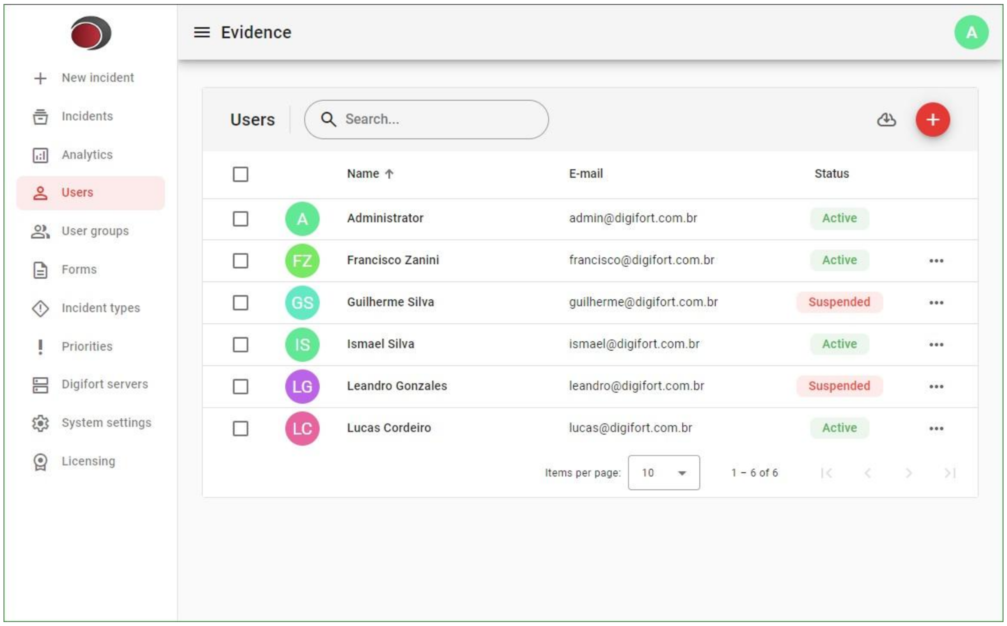
Imported users can use all system functions, including the functionality to import videos from Digifort cameras to incidents. See the topic Managing cameras.

8.1.3 Differences between native and imported users

Feature	Native user	Imported user
Authentication	Authentication is done in the local database	Authentication is done on the remote server
Active Directory authentication	No	Yes, through the integration of Digifort with Active Directory
Import videos from Digifort cameras	No	Yes
Changing user passwords	The password can be changed directly in Evidence	The password must be changed directly in Digifort

8.2 Accessing the users module

In the side menu, click on the **Users** option to access the module.

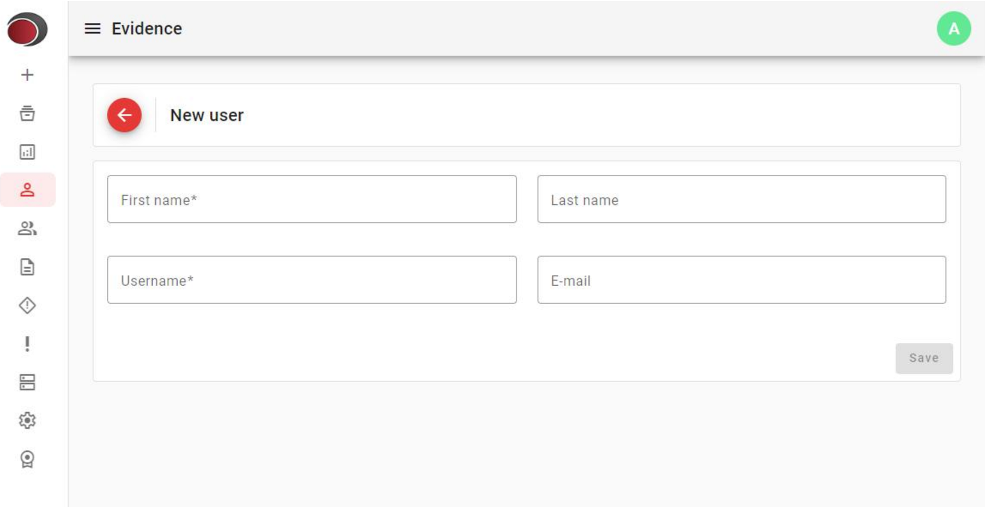


□		Name ↑	E-mail	Status	
□	A	Administrator	admin@digifort.com.br	Active	
□	FZ	Francisco Zanini	francisco@digifort.com.br	Active	•••
□	GS	Guilherme Silva	guilherme@digifort.com.br	Suspended	•••
□	IS	Ismael Silva	ismael@digifort.com.br	Active	•••
□	LG	Leandro Gonzales	leandro@digifort.com.br	Suspended	•••
□	LC	Lucas Cordeiro	lucas@digifort.com.br	Active	•••

Items per page: 10 1 – 6 of 6

8.3 Adding users

To add users, click the button .



- **Name:** The user's first name.
- **Last name:** The user's last name. This is optional information.
- **Username:** This is the username that will be used to log in to the system.
- **E-mail:** The user's e-mail is optional information. If this value is entered, it can be used by the system to send messages by email.

After filling in the data, click the **Save** button. You will be automatically redirected to the user change page, where further settings can be made. See the topic Modifying users.

Important

Newly created users do not have any access rights to the system. To configure access rights, see the topics Managing groups e User groups.

Important
Newly created users do not have a defined password and cannot access the system. If the email has been informed, the user will automatically receive a link to set their password. See the topic Resetting the user's password on the login screen. If the email has not been provided, you can set the user's password yourself, see the topic Modifying the user password.

8.3.1 Setting the user's first password

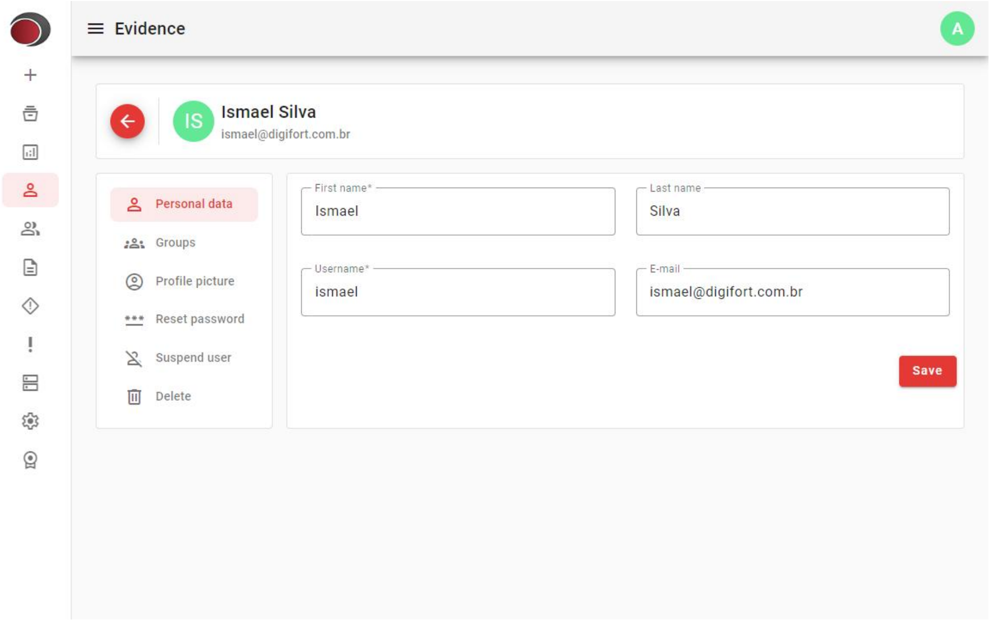
When adding a user, if the email address is provided, the system will automatically send an email to the user to set their password. For automatic email sending to work, the SMTP settings must be previously configured. See the topic Configuring the SMTP server.

If the email is not provided, a password must be created in one of the following ways:

- Clicking on the **"Forgot your password?"** on the login page. See the topic Resetting the user's password on the login screen.
- Setting a password through user registration. See the topic Modifying the user password.

8.4 Modifying users

To modify users, click on the name of the user you want to modify.



First name* Ismael
Last name Silva
Username* ismael
E-mail ismael@digifort.com.br

On the left side there is a menu where further user settings can be made.

- **Personal data:** Allows you to modify the user's main data.
- **Groups:** Allows you to add and remove users from groups. See the topic Adding users to groups.
- **Profile picture**: Allows you to add and remove the user's profile picture. See the topic Setting profile picture.
- **Reset password:** Allows the administrator to set a password for the user. See the topic Modifying the user password.
- **Suspend user:** Allows you to suspend the user. Suspending a user blocks complete access to the system. See the topic Suspending users.

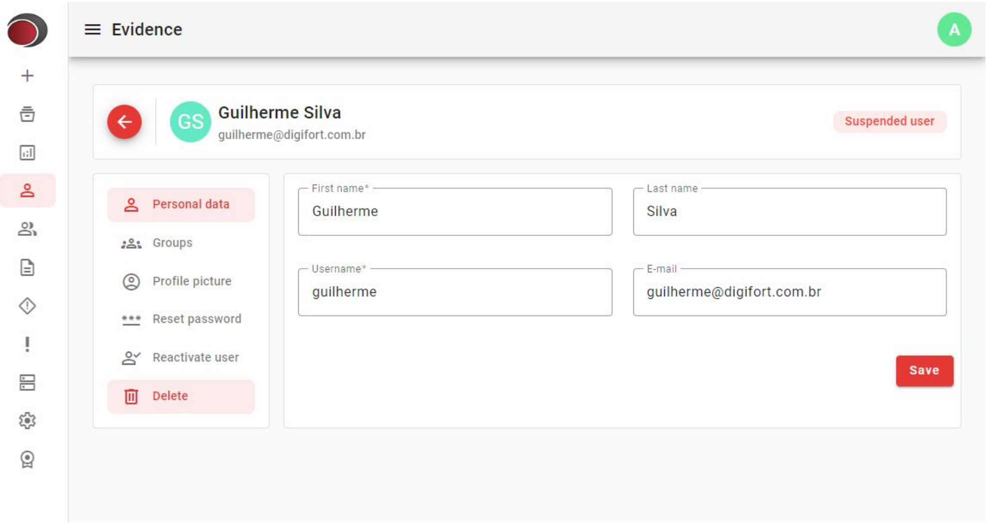
- **Delete:** Removes the user from the system. See the topic Deleting users.

8.5 Deleting users

When deleting a user, they will no longer be listed in the user registry and their access will be permanently blocked, but their data will not be removed. This way all incidents created by this user will still have their name linked.

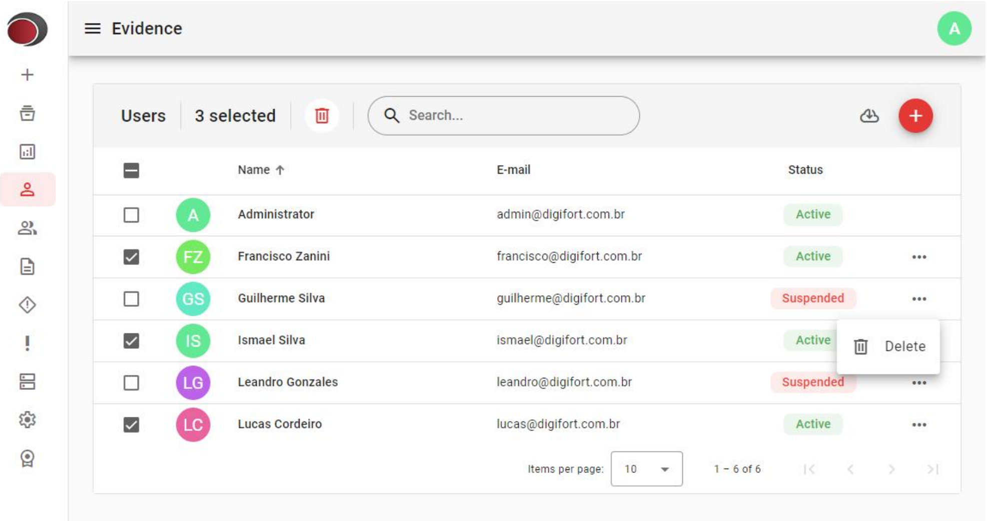
Although the user's data is preserved when removing it, a user with the same data may be created in the future.

To delete users click the **Delete** button.



First name*: Guilherme
Last name: Silva
Username*: guilherme
E-mail: guilherme@digifort.com.br

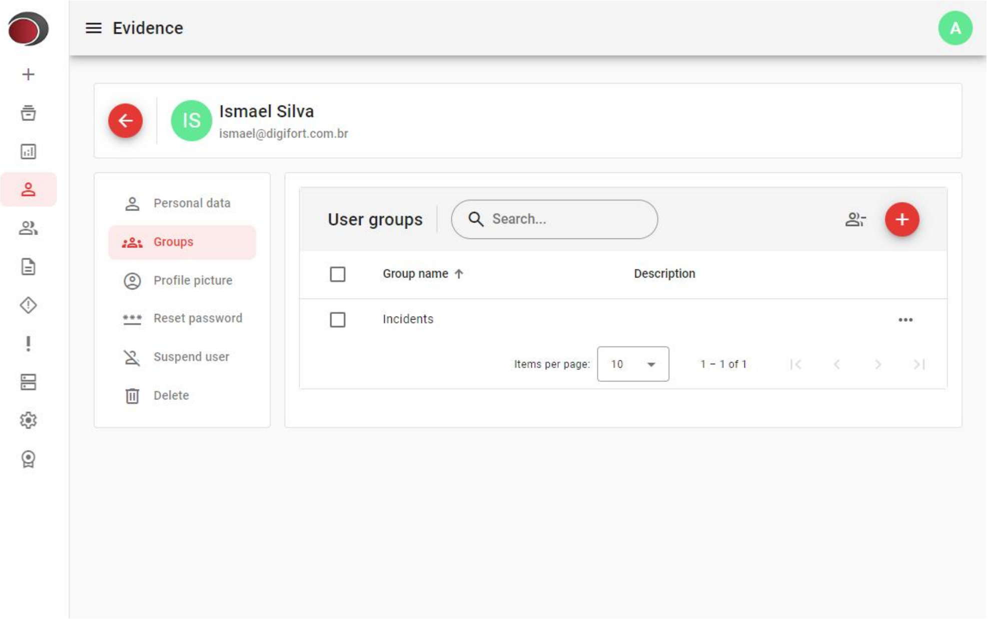
Another way to exclude users is through user registration. Next to each item there is a three-dot button with the option to remove it.
You can also use check boxes to remove more than one item at the same time. Select the items to be removed and then click 🗑 .



		Name ↑	E-mail	Status	
☐	A	Administrator	admin@digifort.com.br	Active	
☑	FZ	Francisco Zanini	francisco@digifort.com.br	Active	•••
☐	GS	Guilherme Silva	guilherme@digifort.com.br	Suspended	•••
☑	IS	Ismael Silva	ismael@digifort.com.br	Active	
☐	LG	Leandro Gonzales	leandro@digifort.com.br	Suspended	•••
☑	LC	Lucas Cordeiro	lucas@digifort.com.br	Active	•••

8.6 Managing groups

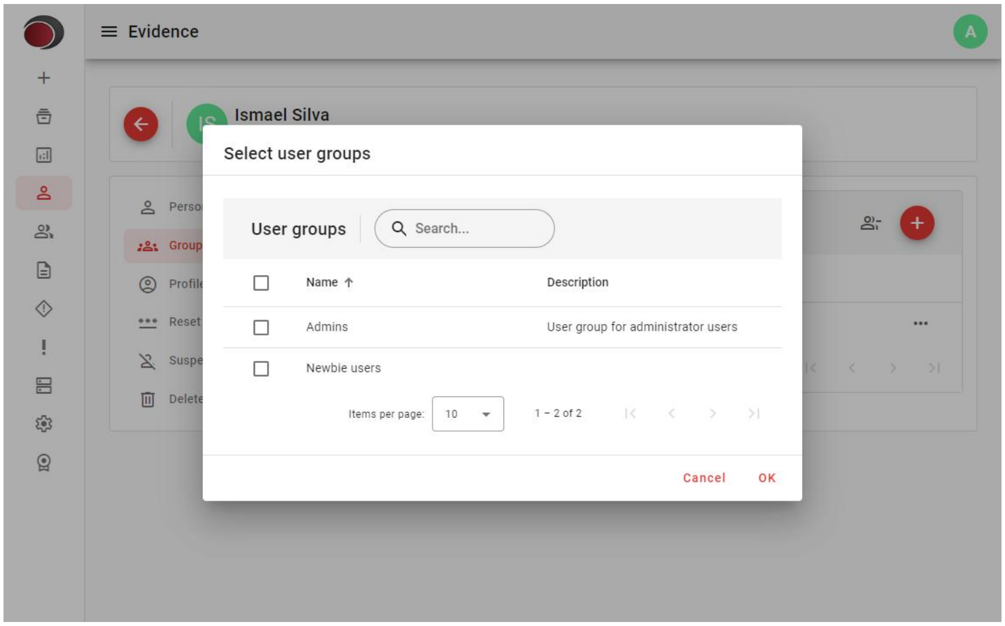
To add or remove user groups, click the **Groups** button.
A list of groups will be displayed containing all the groups this user belongs to.



□	Group name ↑	Description
□	Incidents	

8.6.1 Adicionando grupos à usuários

To add groups to the user, click the button ⊕.



□	Name ↑	Description
□	Admins	User group for administrator users
□	Newbie users	

Select the desired groups and click **OK**.

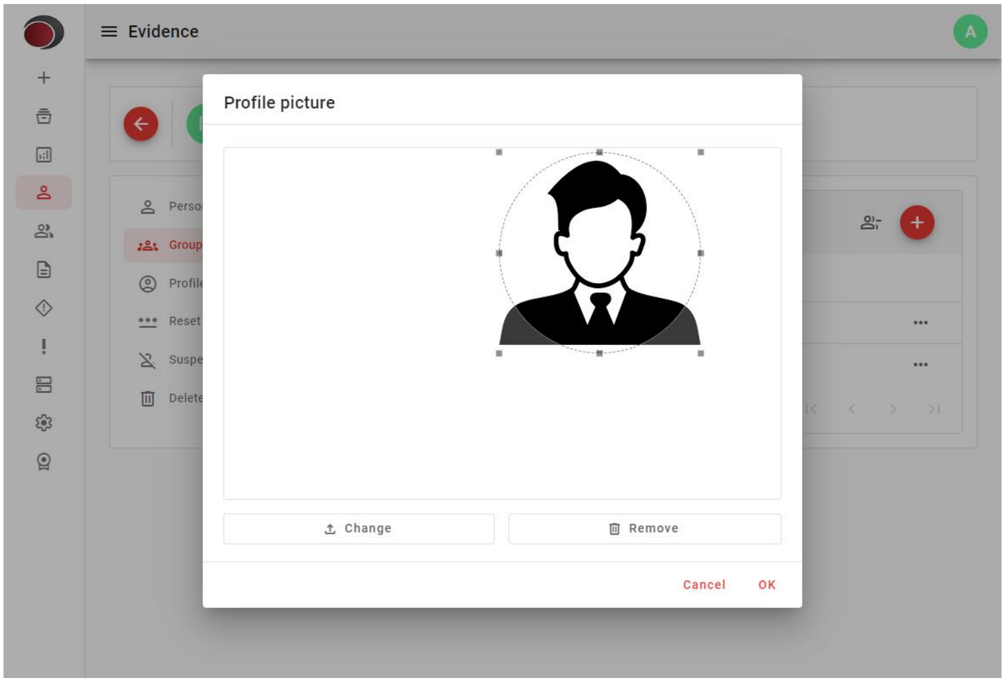
8.6.2 Removing groups from users

To remove a user's group, click the three-dot icon next to each group name and then select **Remove user from group**, or select one or more groups using the check boxes and then click the .

8.7 Setting the profile picture

The profile picture allows the user to be identified in an easier and more personalized way on all screens where the user is referenced.

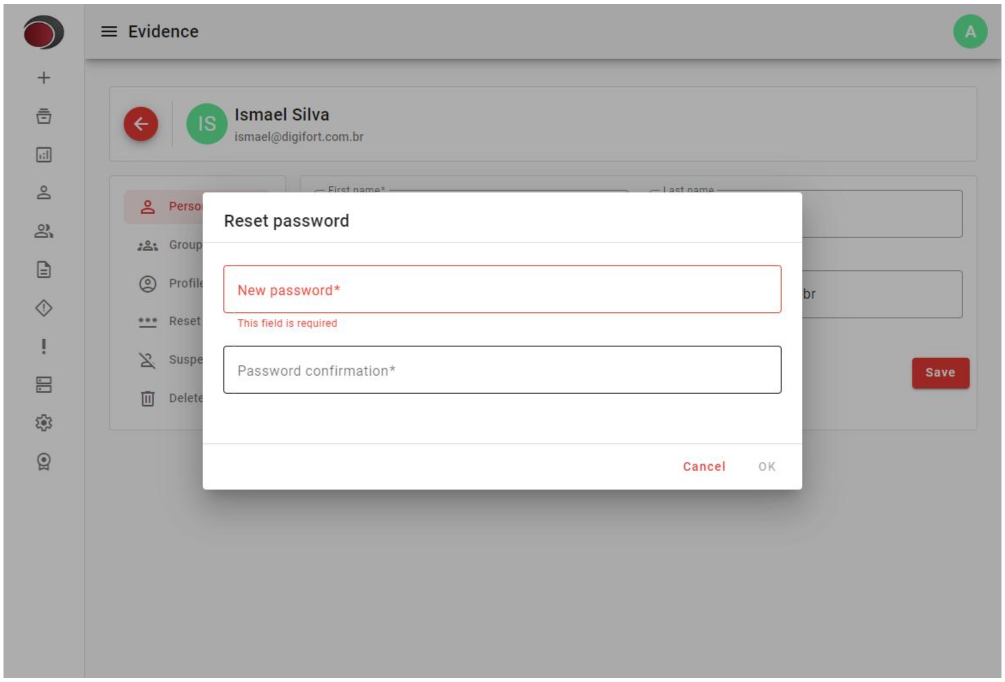
To set your profile picture, click the **Profile picture** button.



Use the positioning and resizing tools to crop the image as needed and then click **OK**.

8.8 Modifying the user's password

To change the user's password, click the **Reset password** button.



This field is required

Important

! Imported users cannot have their password changed. It must be changed directly in the system into which it was imported.

Tip

✓ The user can reset their password using the **Forgot your password? button** on the login page. See the topic Resetting the user's password on the login screen.

8.9 Suspending users

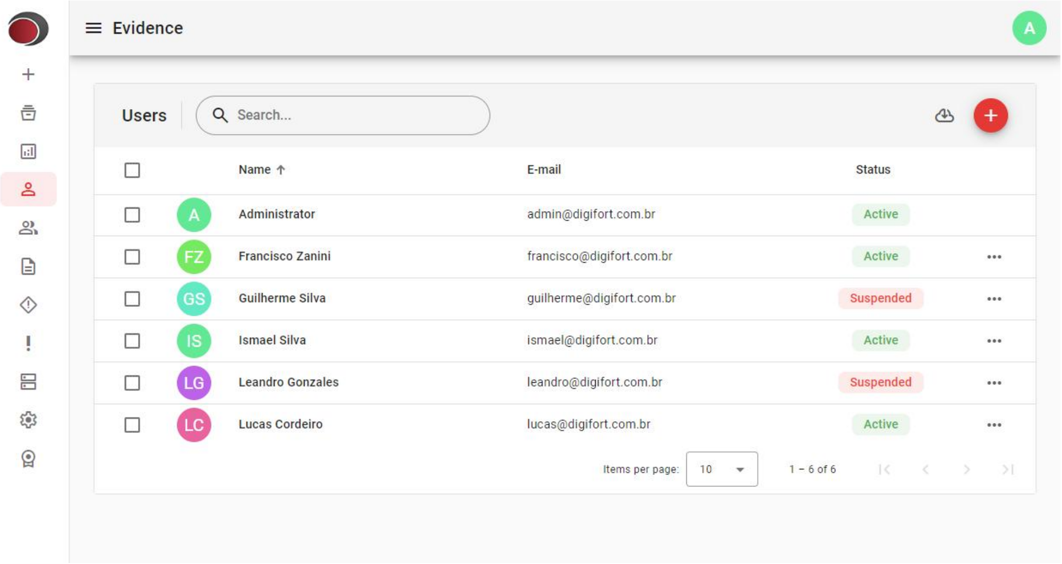
To suspend a user, click the **Suspend user** button.
A suspended user will have their access blocked until they are reactivated again.

8.10 Importing users

Importing users is a big advantage if you are using Evidence integrated with Digifort, such as:

- Centralized user database.
- Import videos from Digifort cameras.

To import users click the button .

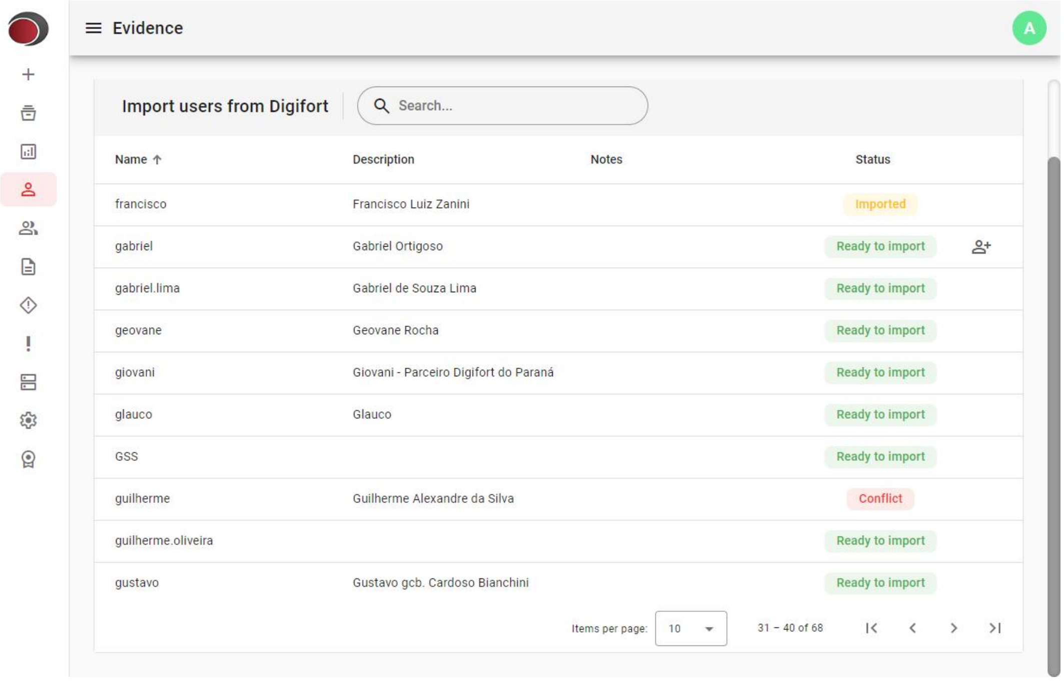


☐		Name ↑	E-mail	Status	
☐	A	Administrator	admin@digifort.com.br	Active	
☐	FZ	Francisco Zanini	francisco@digifort.com.br	Active	•••
☐	GS	Guilherme Silva	guilherme@digifort.com.br	Suspended	•••
☐	IS	Ismael Silva	ismael@digifort.com.br	Active	•••
☐	LG	Leandro Gonzales	leandro@digifort.com.br	Suspended	•••
☐	LC	Lucas Cordeiro	lucas@digifort.com.br	Active	•••

Select the server that contains the users you want to import.

! **Important**
The server must be previously registered, see the topic Digifort servers.

After selecting the server, the system will query the available users.



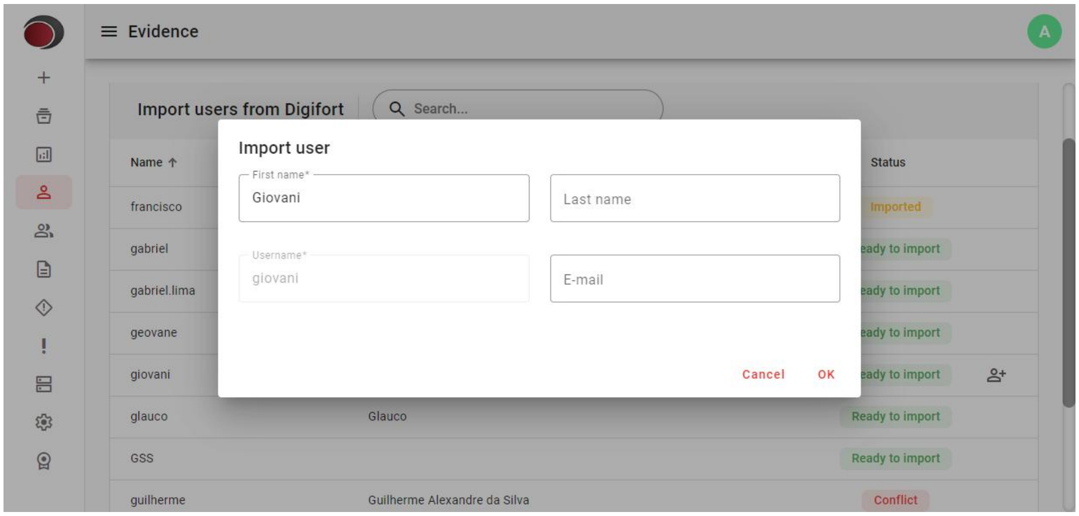
Name ↑	Description	Notes	Status
francisco	Francisco Luiz Zanini		Imported
gabriel	Gabriel Ortigoso		Ready to import
gabriel.lima	Gabriel de Souza Lima		Ready to import
geovane	Geovane Rocha		Ready to import
giovani	Giovani - Parceiro Digifort do Paraná		Ready to import
glauco	Glauco		Ready to import
GSS			Ready to import
guilherme	Guilherme Alexandre da Silva		Conflict
guilherme.oliveira			Ready to import
gustavo	Gustavo gcb. Cardoso Bianchini		Ready to import

Each listed user has the following statuses:

- **Ready to import:** User can be imported
- **Imported:** The user has already been imported
- **Conflict:** There is already a native user registered with the same username. You cannot import this user without first removing the native user. To understand more about types of users, see the topic

User types.

After locating the user you want to import, click the button 👤+.



First name*: Giovani
Last name
Username*: giovani
E-mail

Name ↑		Status
francisco		Imported
gabriel		eady to import
gabriel.lima		eady to import
geovane		eady to import
giovani		eady to import
glauco	Glauco	Ready to import
GSS		Ready to import
guilherme	Guilherme Alexandre da Silva	Conflict

Fill in the mandatory user data and click **OK**.

Important
❗ Newly imported users do not have any access rights to the system. To configure access rights, see the topics Managing groups e User groups.

8.11 User authentication process

The user authentication process is different for each type of user. See below the authentication method for each type of user.

8.11.1 Authentication of native users

Native users authenticate directly to the local database with the provided credential.

8.11.2 Authentication of imported users

Imported users are authenticated directly on their source system, that is, they are authenticated on the server from which they were imported. At login time, Evidence server attempts to authenticate to the Digifort server, which in turn will validate the credentials in its local database or, if integrated, in Active Directory.

In scenarios where more than one Digifort server is used in the same environment, it is common practice for the same users to be registered on all servers. In this case, all these servers can be registered in Evidence. During the login process for an imported user, Evidence will first attempt to log in to the server where the user was imported. If the server is unavailable, Evidence will attempt to log in to all other servers sequentially. If no server accepts the credentials, access will not be permitted.

8.12 Resetting the user's password

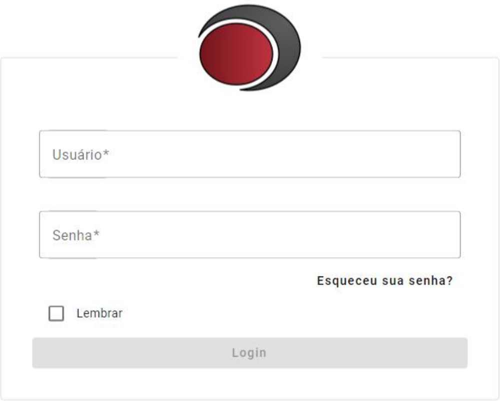
The user password can be reset in the following ways:
- Through the login page
- Through user register

- Through user account management

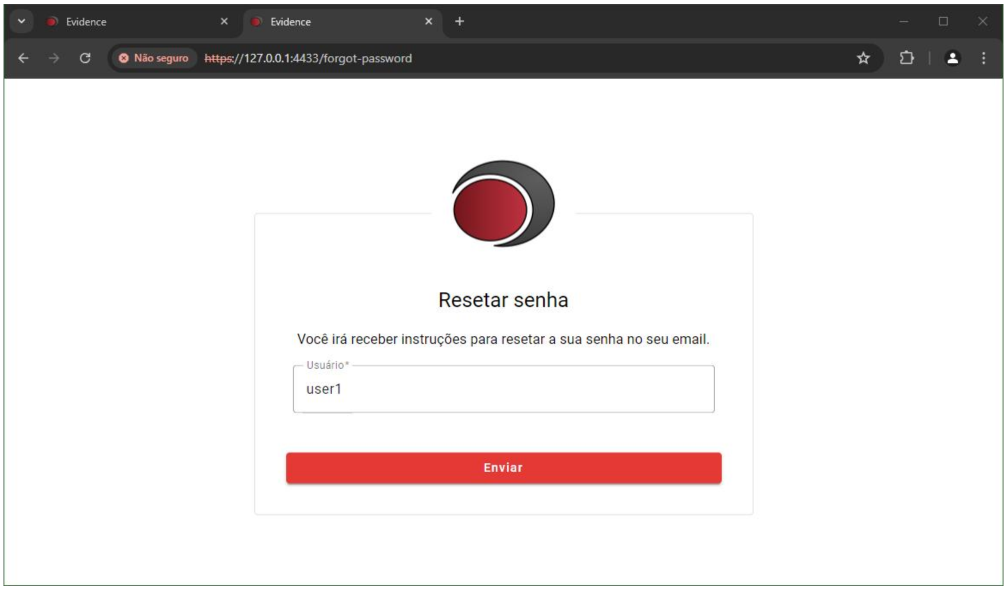
8.12.1 Resetting the user's password on the login page

When trying to reset the password using the login form, the user will receive an email with instructions to reset the password.
This email has a link that will take the user to the password reset page.

To reset the user's password via the login page, click the **Forgot password?** button.



You will be redirected to the password reset page, where you must enter your username.

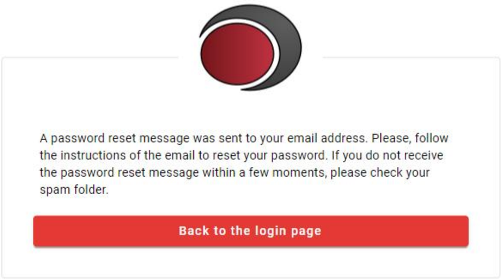


Resetar senha

Você irá receber instruções para resetar a sua senha no seu email.

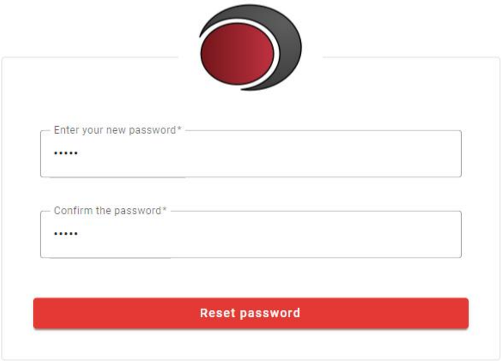
Usuário*: user1

After entering the user name, click the **Submit** button.



A password reset message was sent to your email address. Please, follow the instructions of the email to reset your password. If you do not receive the password reset message within a few moments, please check your spam folder.

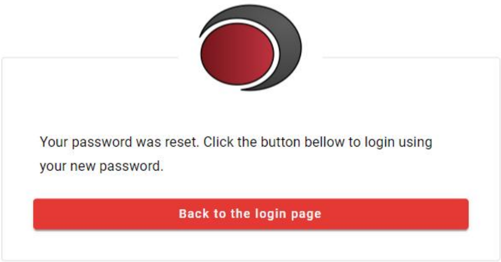
The user should receive an email with a password reset link. When you click on the link, the password reset page will be displayed:



Enter your new password*: •••••

Confirm the password*: •••••

Enter the new password and confirm.



Your password was reset. Click the button bellow to login using your new password.

Important

❗ For this feature to work, the SMTP server must be properly configured. See the topic Configuring the SMTP server.

8.12.2 Resetting the user's password from the users register

To reset the user password using user registration, see the topic Modifying the user's password.

8.12.3 Resetting user password in account management

To reset the user's password through account management, see the topic Managing the user's account.

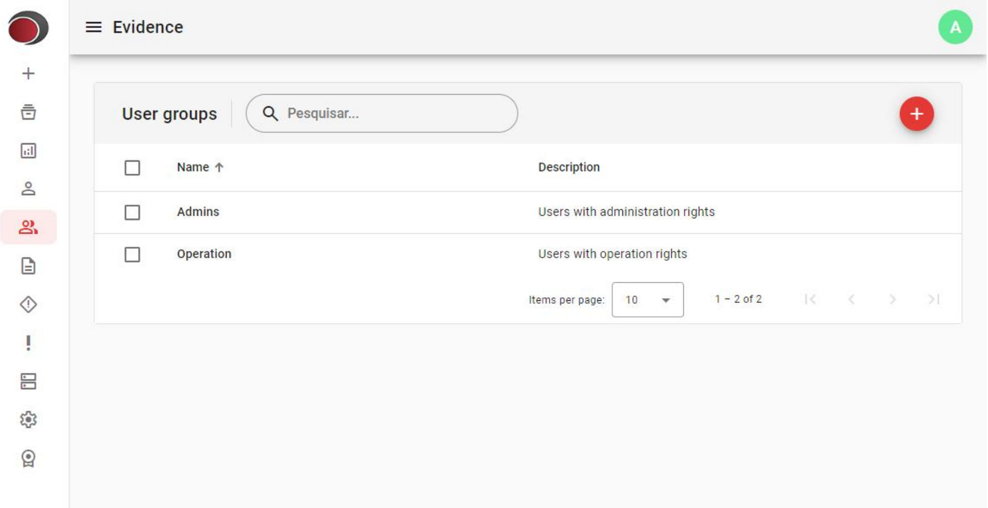
Chapter IX

9 User groups

The user groups module allows the grouping of users with pre-determined roles in the system. You can, for example, create groups for system administrators, operators, among others.
Creating user groups is a mandatory step in user configuration, as users without groups do not have any access permissions.

9.1 Accessing the user groups module

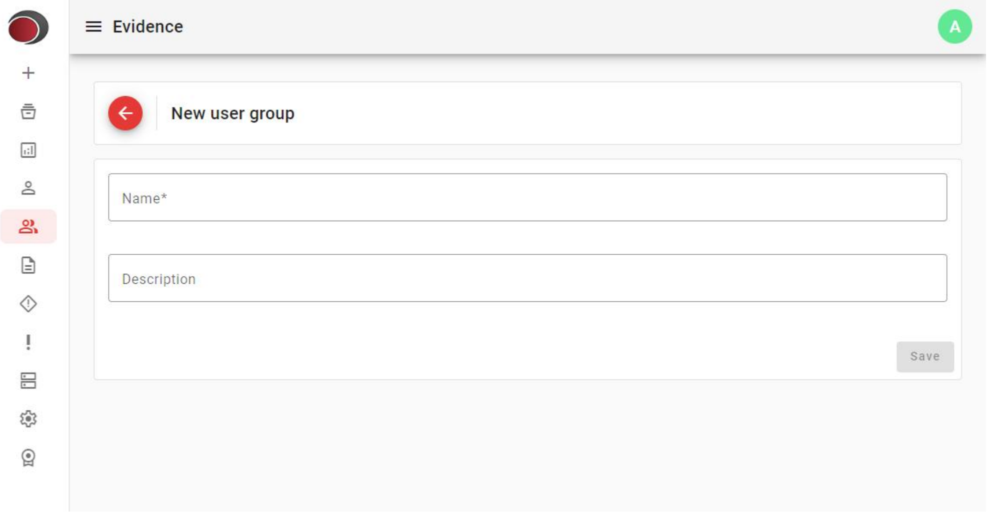
In the side menu, click on the **User groups** option to access the module.



Name ↑	Description
Admins	Users with administration rights
Operation	Users with operation rights

9.2 Adding user groups

To add user groups, click the button ⊕.

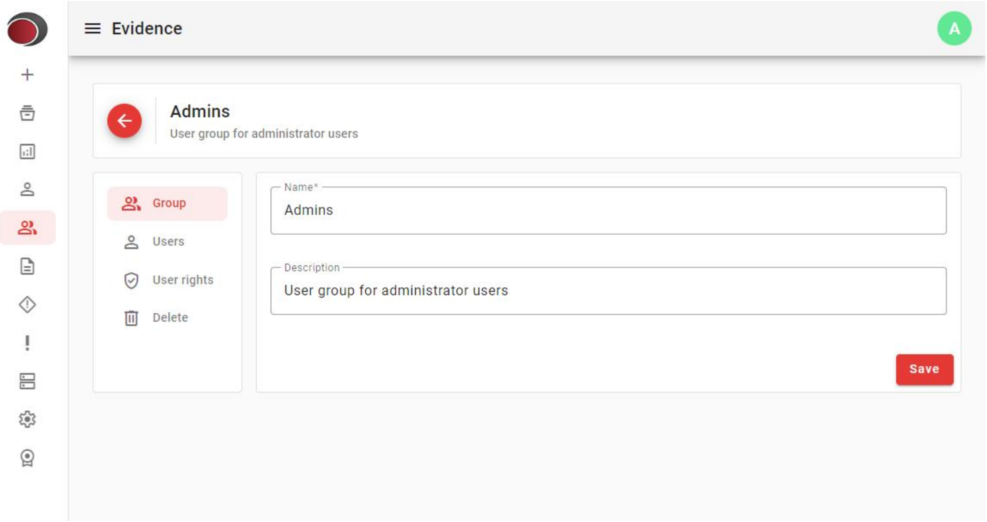


- **Name:** The name of the group
- **Description:** Optional description of the group

After filling in all the necessary data, click the **Save** button. You will be automatically redirected to the user change page, where further settings can be made. See the topic Modifying user groups.

9.3 Modifying user groups

To modify user groups, click the name of the group you want to modify.



Admins
User group for administrator users

Name* Admins

Description User group for administrator users

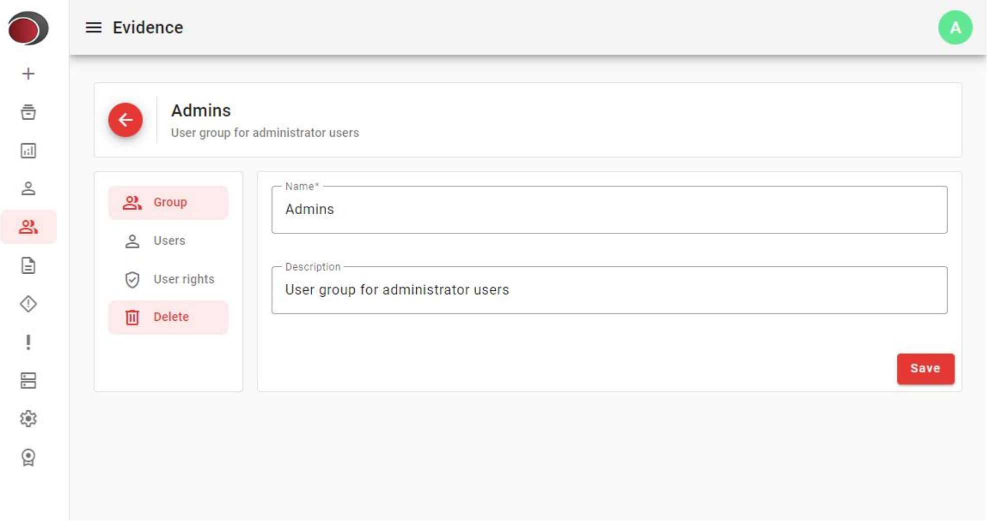
On the left side there is a menu where more group settings can be made.

- **Group:** Allows you to modify the group's main data.
- **Users:** Allows you to add and remove users from groups. See the topic Adding users to groups.
- **User rights:** Allows you to configure the access rights of users belonging to the group. See the topic Configuring access rights.
- **Delete:** Removes the group from the system. See the topic Deleting user groups.

9.4 Deleting user groups

When deleting an user group, users belonging to the group will not be removed from the system, only their access rights will be removed.

To delete groups click the **Delete** button.

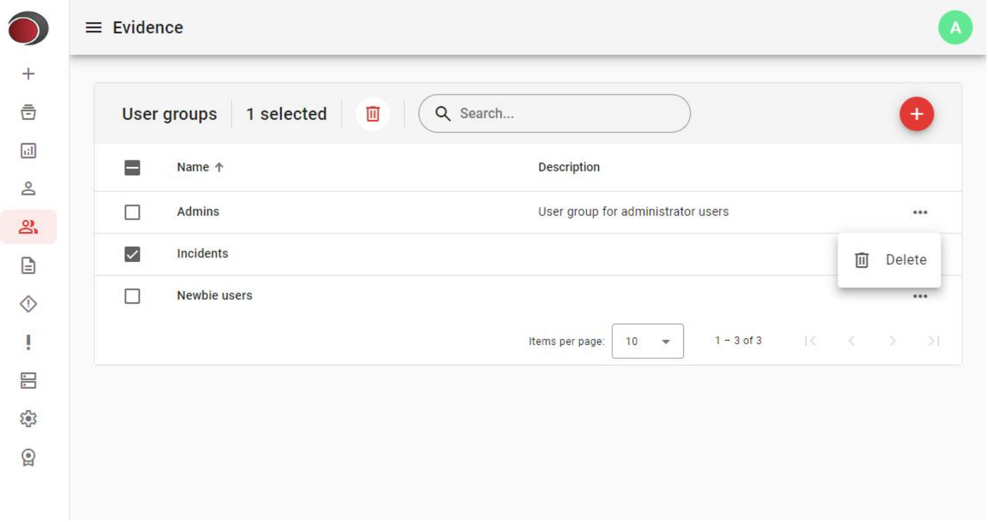


Admins
User group for administrator users

Name* Admins

Description User group for administrator users

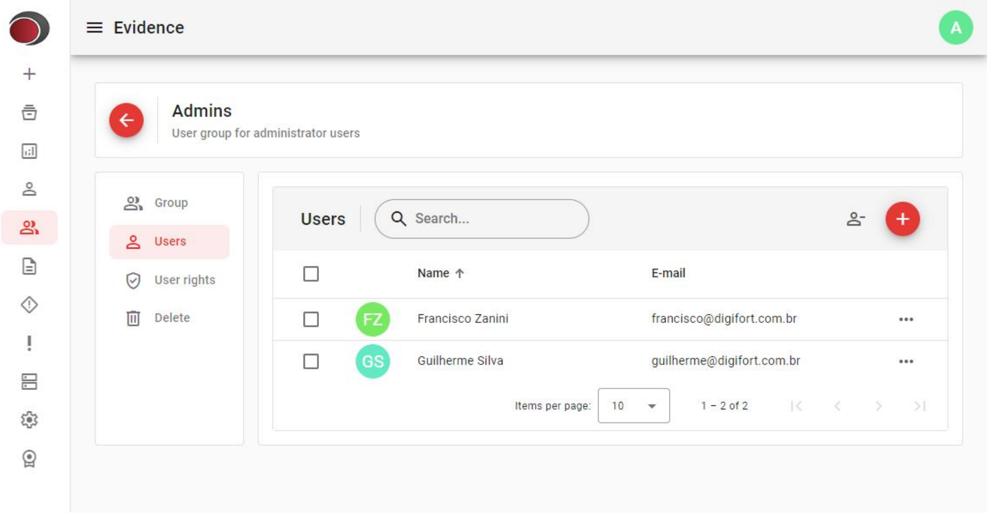
Another way to remove user groups is through group registration. Next to each item there is a three-dot button with the option to remove it.
You can also use check boxes to remove more than one item at the same time. Select the items to be removed and then click 🗑.



□	Name ↑	Description
□	Admins	User group for administrator users
☑	Incidents	
□	Newbie users	

9.5 Managing users

To add or remove users from the group, click the **Users** button.
A list of users will be displayed containing all users belonging to this group as shown in the image below:

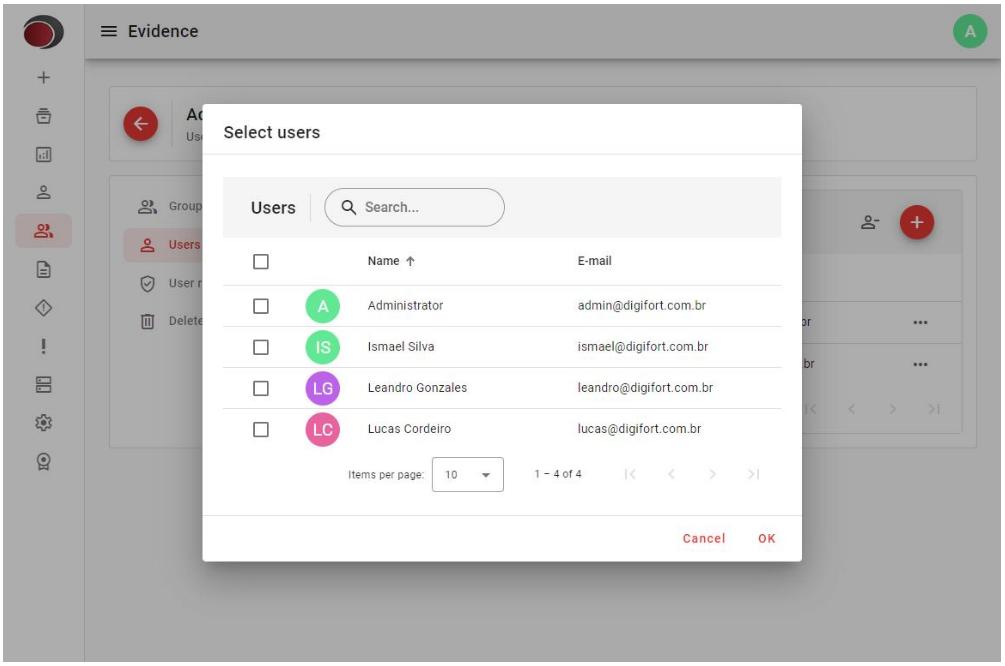


□		Name ↑	E-mail	
□	FZ	Francisco Zanini	francisco@digifort.com.br	•••
□	GS	Guilherme Silva	guilherme@digifort.com.br	•••

,

9.5.1 Adding users to groups

To add users to the group, click the button ⊕.



□		Name ↑	E-mail
□	A	Administrator	admin@digifort.com.br
□	IS	Ismael Silva	ismael@digifort.com.br
□	LG	Leandro Gonzales	leandro@digifort.com.br
□	LC	Lucas Cordeiro	lucas@digifort.com.br

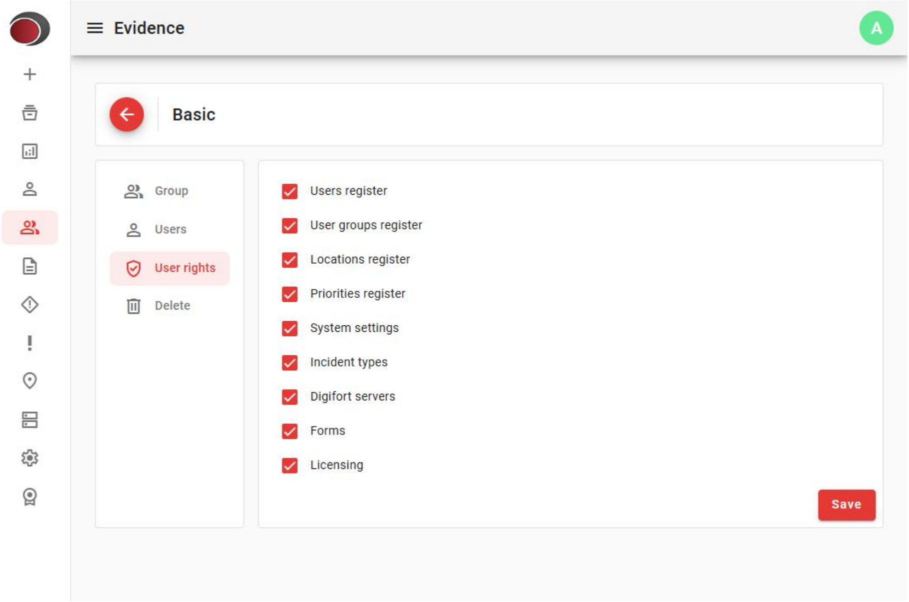
Select the desired users and click **OK**.

9.5.2 Removing users from groups

To remove a user from groups, click the three-dot icon next to each user's name and then select **Remove user from group**, or select one or more users using the check boxes and then click the button. 👥−.

9.6 Configuring access rights

To configure access rights, click the **User Rights** button.



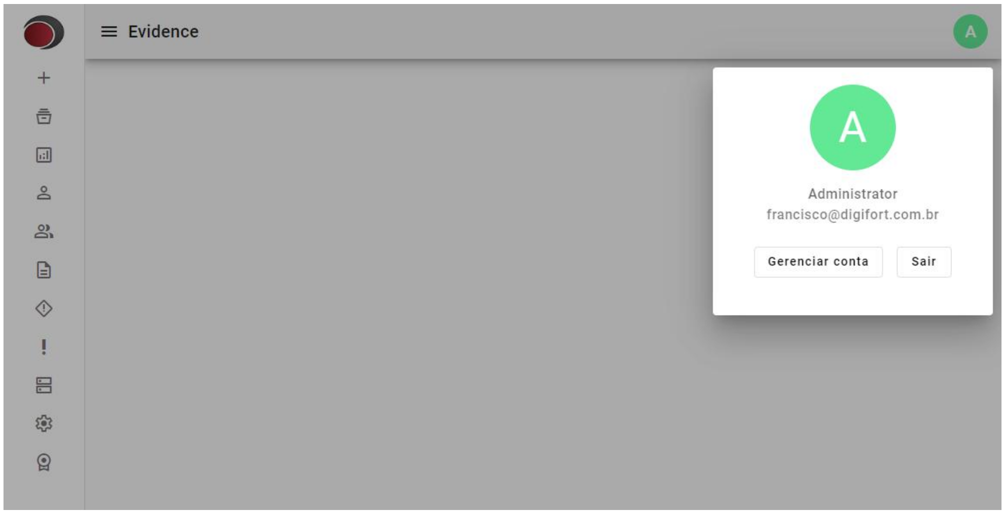
☑ Users register
☑ User groups register
☑ Locations register
☑ Priorities register
☑ System settings
☑ Incident types
☑ Digifort servers
☑ Forms
☑ Licensing

- **Users register:** Allows you to access registration, import, add, change and delete users.
- **User groups register:** Allows you to access the registration, add, change and delete user groups.
- **Locations register:** Allows you to access the registration, add, change and delete locations.
- **Priorities register:** Allows you to access the registration, add, change and delete priorities.
- **System Settings:** Allows you to modify system settings.
- **Incident types:** Allows you to access the registration, add, change and delete incident types.
- **Digifort servers:** Allows you to access registration, add, change and delete servers.
- **Forms:** Allows you to access registration, add, change and delete forms.
- **Licensing:** Allows you to access, add and remove licenses.

Chapter X

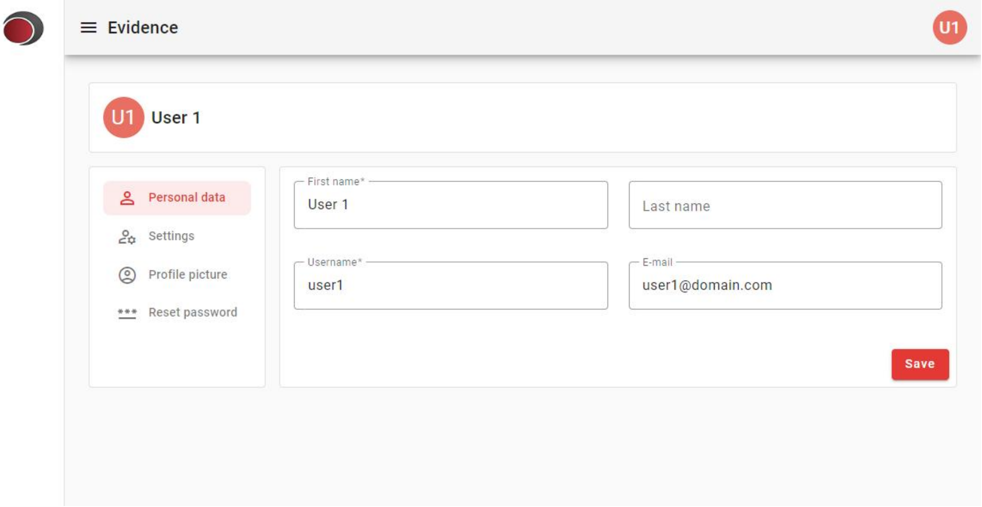
10 Managing the account of the logged user

The system provides a page where the logged in user can change some of their settings.
To access this page, click on the user's avatar button located at the top right of the page, and then on the **Manage account** button.



10.1 Modifying the user's data

To change the logged in user's personal data, click the **Personal data** button.



First name*: User 1

Last name

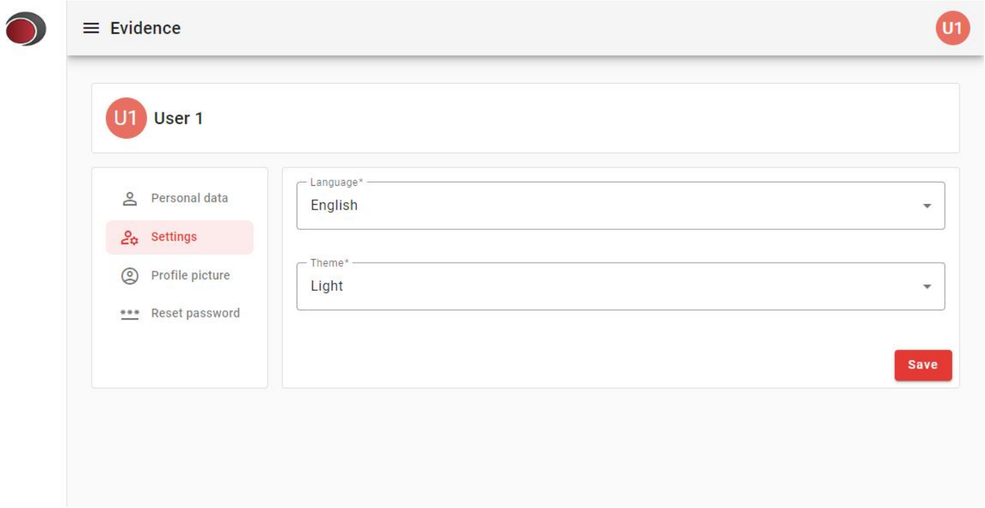
Username*: user1

E-mail: user1@domain.com

- **First name:** User's name.
- **Last name:** User's last name.
- **Username:** User for authentication.
- **E-mail:** User's email.

10.2 Modifying the user's settings

To change the logged in user's settings, click the **Settings** button.



U1 User 1

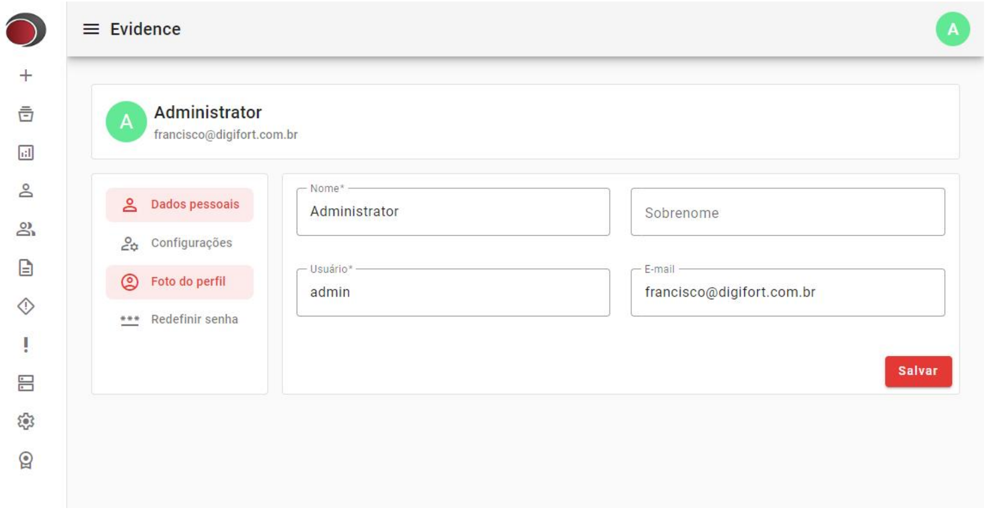
Language*: English

Theme*: Light

- **Language:** User display language. Each user can use a different language of their choice.
- **Theme:** Display theme.

10.3 Modifying the profile picture

To change the profile picture of the logged user, click the **Profile picture** button.



A Administrator
francisco@digifort.com.br

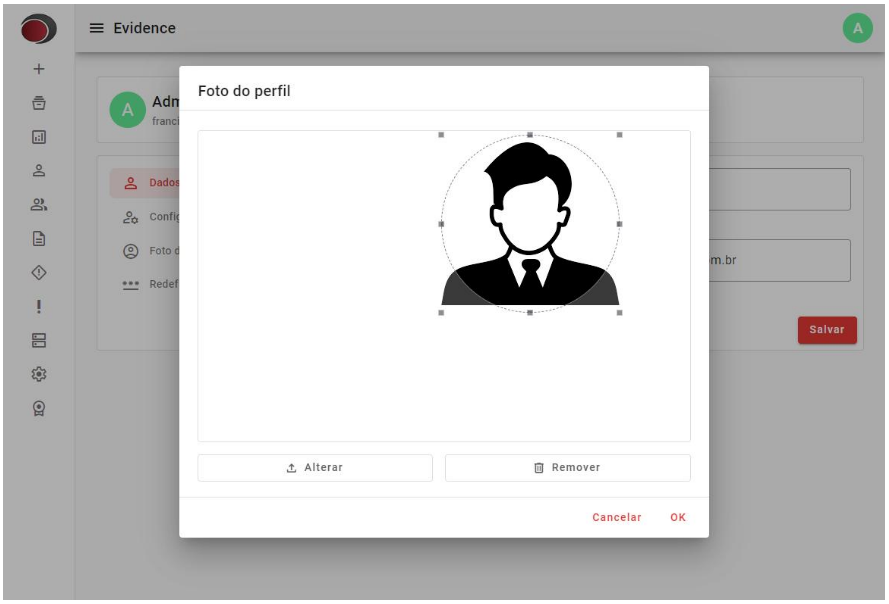
Nome*: Administrator

Sobrenome

Usuário*: admin

E-mail: francisco@digifort.com.br

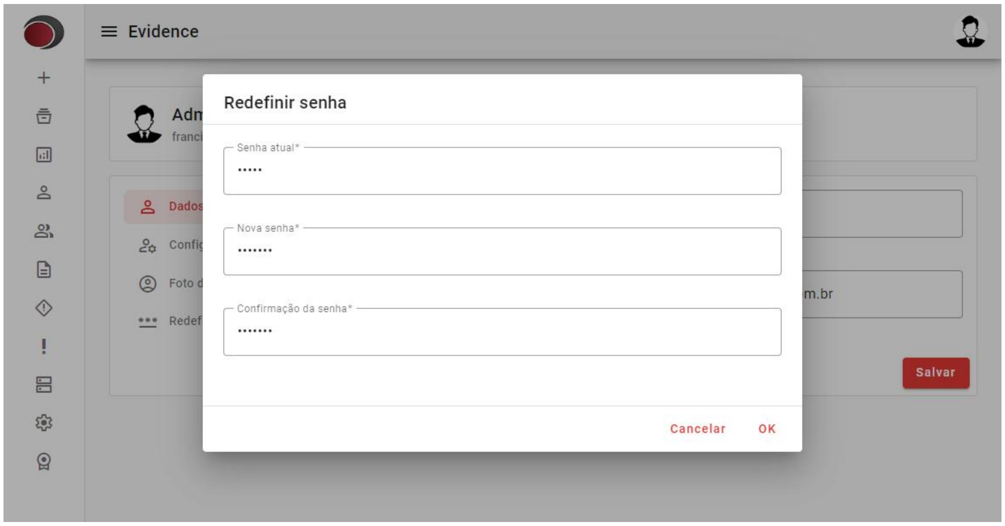
Select an image from your computer by clicking the **Change** button. You can use the framing controls to crop the image as needed.



To remove the profile picture, click the **Remove** button. This way the initials of the user's name will be used to represent the user.

10.4 Resetting the password

To reset the logged in user's password, click the **Reset password** button.



Redefinir senha

Senha atual* •••••

Nova senha* •••••••

Confirmação da senha* •••••••

- **Current password:** Enter the user's current password. If you don't know your current password, use the **Forgot your password?** button on the login page. See the topic Resetting the user's password on the login page.
- **New password:** Enter the new password.
- **Password confirmation:** Enter the new password again to confirm.

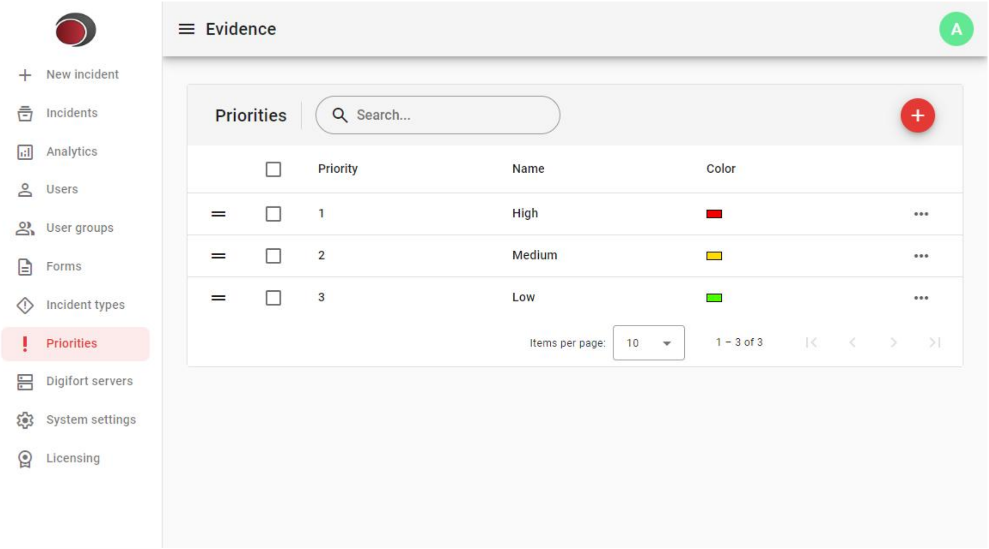
Chapter XI

11 Priorities

This module allows the user to manage priorities that can be assigned to incidents. Despite being optional, assigning priorities is essential to organize and handle incidents according to their urgency and importance, ensuring that critical events are handled in an efficient and timely manner.

11.1 Accessing the priorities module

In the side menu, click on the **Priorities** option to access the module.



Evidence

- New incident
- Incidents
- Analytics
- Users
- User groups
- Forms
- Incident types
- Priorities
- Digifort servers
- System settings
- Licensing

Priorities

Search...

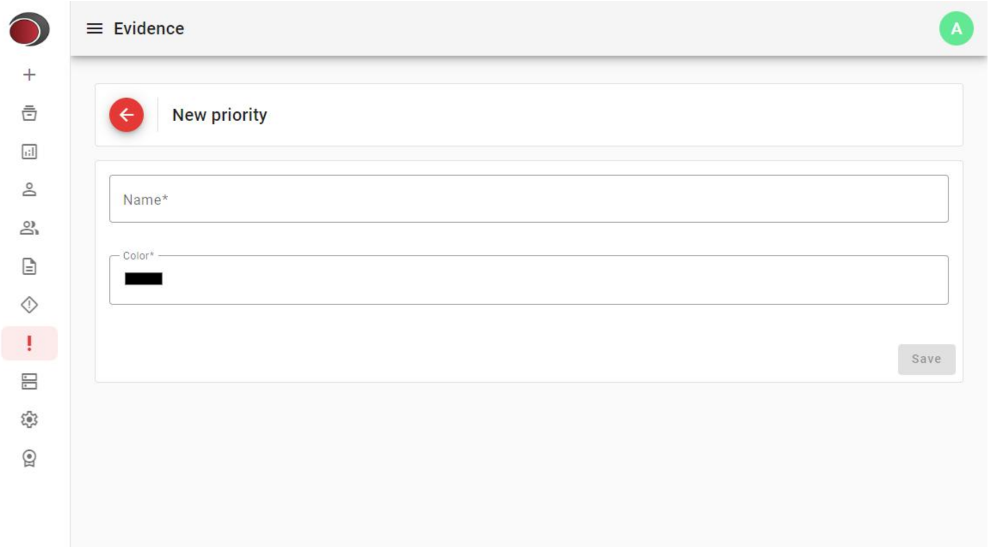
	□	Priority	Name	Color
═	□	1	High	🟥
═	□	2	Medium	🟨
═	□	3	Low	🟩

Items per page: 10

1 – 3 of 3

11.2 Adding priorities

To add priorities, click the button ⊕.



Evidence

New priority

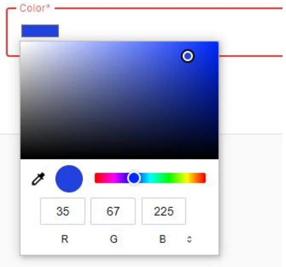
Name*

Color*

Save

- **Name:** Name of the priority.
- **Color:** The priority's color. Color helps visually identify the priority of incidents.

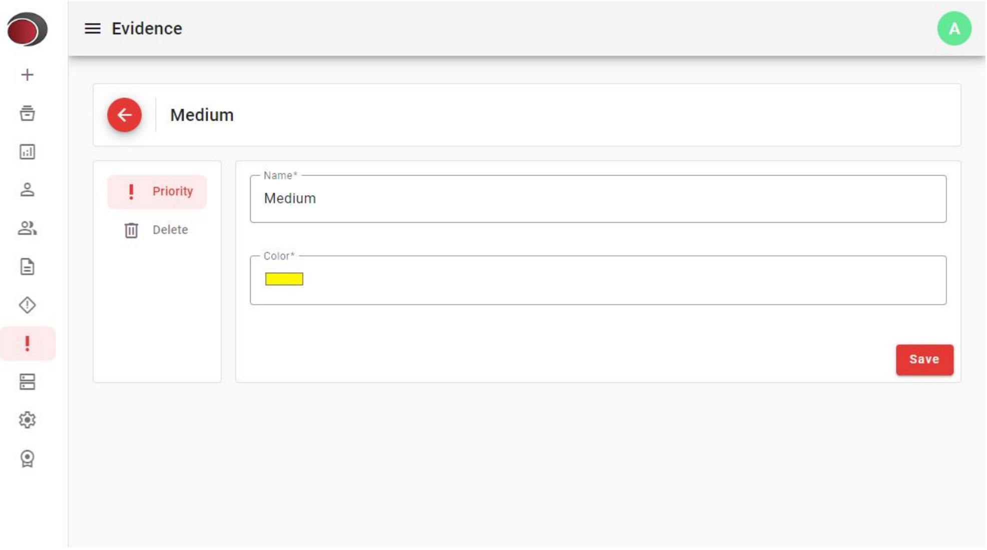
To select a color, click the black rectangle. A color selection window will appear as shown in the image below.



After filling in all the necessary data, click the Save button. You will automatically be redirected to the priority change page. See the topic Modifying priorities.

11.3 Modifying priorities

To modify priorities, click on the name of the priority you want to modify.



Name*
Medium

Color*

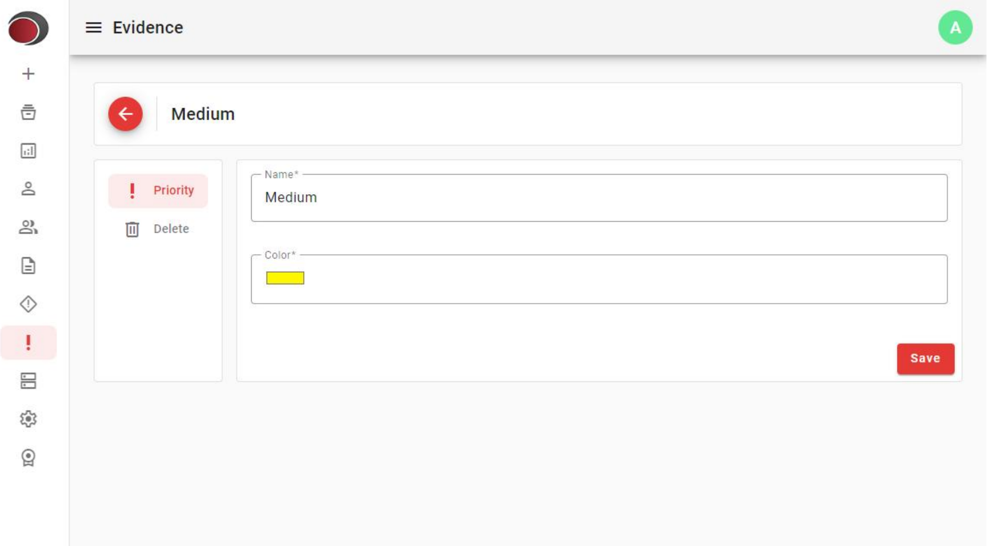
On the left side there is a menu where more settings can be made.

- **Priority:** Allows you to modify the main priority data.
- **Delete:** Removes priority from the system. See the topic Deleting priorities.

11.4 Deleting priorities

When you delete a priority, it will be disconnected from all incidents that were added with that priority. This way these incidents will not be prioritized.

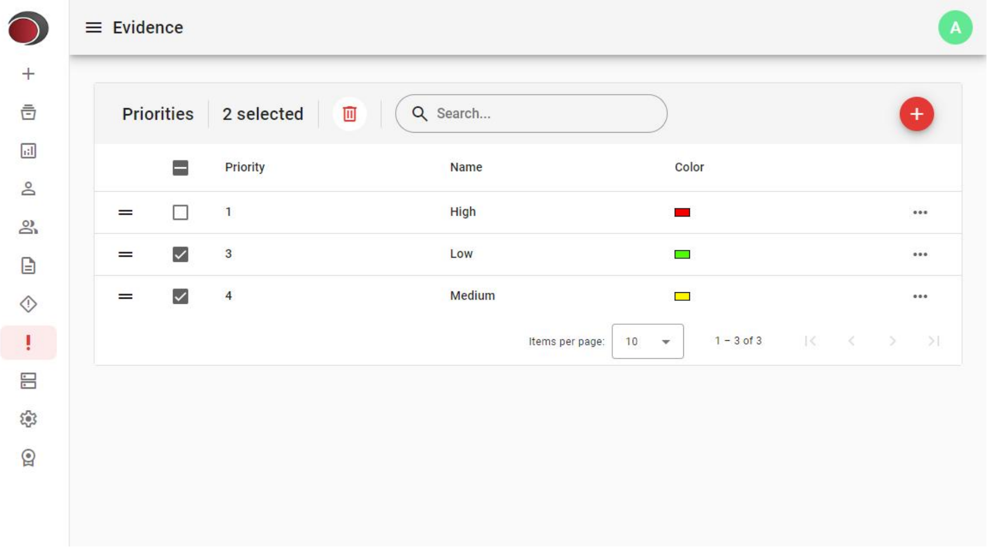
To delete priorities click the **Delete** button.



Name*
Medium

Color*
🟨

Another way to exclude priorities is through the priority register. Next to each item there is a three-dot button with the option to remove it.
You can also use check boxes to remove more than one item at the same time. Select the items to be removed and then click 🗑.

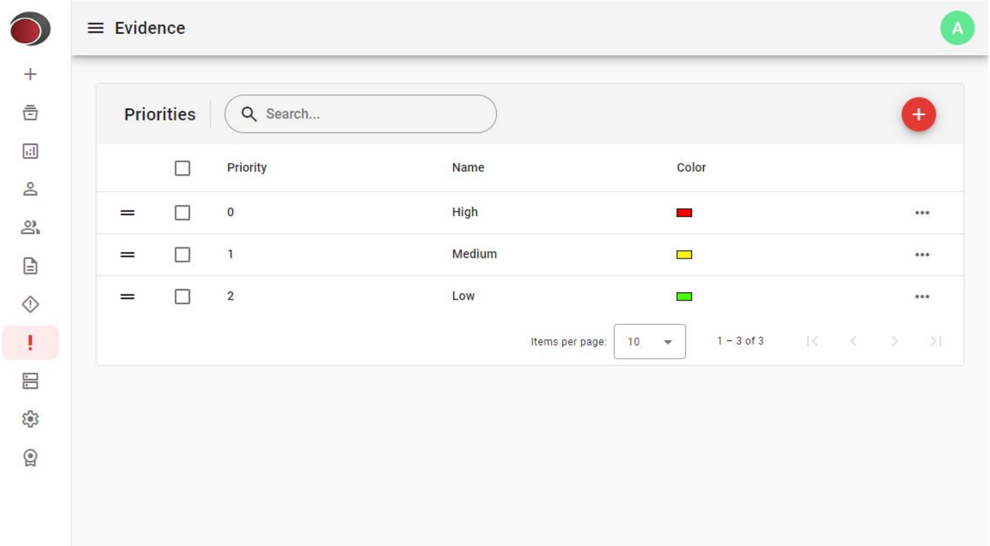


	☐	Priority	Name	Color	
═	☐	1	High	🟥	•••
═	☑	3	Low	🟩	•••
═	☑	4	Medium	🟨	•••

11.5 Ordering priorities

Priorities can be ordered so that they appear for user selection in a logical manner defined by the administrator.

To order priorities click on the button ═ and drag the item up or down, positioning it in the desired order.



	□	Priority	Name	Color
═	□	0	High	🟥
═	□	1	Medium	🟨
═	□	2	Low	🟩

Items per page: 10

1 – 3 of 3

Chapter XII

12 Locations

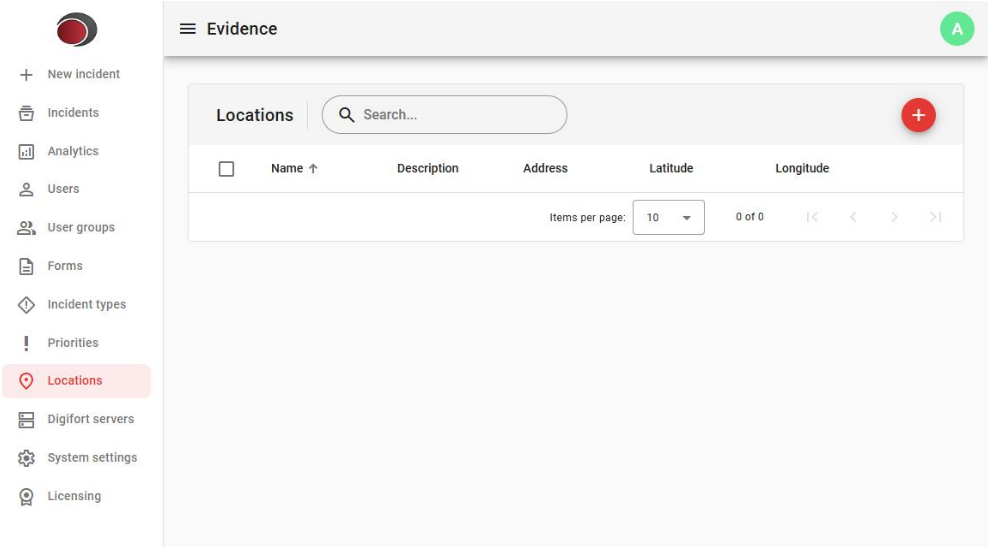
This feature was developed to facilitate and standardize the inclusion of geographic information when creating incidents. By pre-registering the most frequent locations, the system allows the user to select these locations directly on the incident form, avoiding the manual repetition of addresses for each new occurrence.

The user can select an address directly on a map, which will be displayed when viewing the incident, making it easier to understand the location involved. However, if the incident cannot be associated with a specific address, such as internal sectors of a company, this feature can still be used normally. In these cases, it is sufficient to enter only the name of the location and, optionally, a description.

A registered location has a fixed address, which will always be the same. Therefore, when filling out an incident, the user simply needs to select the desired location from the list for the data to be automatically applied. This process ensures consistency and saves time. However, in situations where addresses vary frequently or there are a large number of possible locations, making manual registration unfeasible, it is recommended to use custom fields of the Location type in the incident form. This approach offers greater flexibility for the user to enter the location directly when registering the incident.

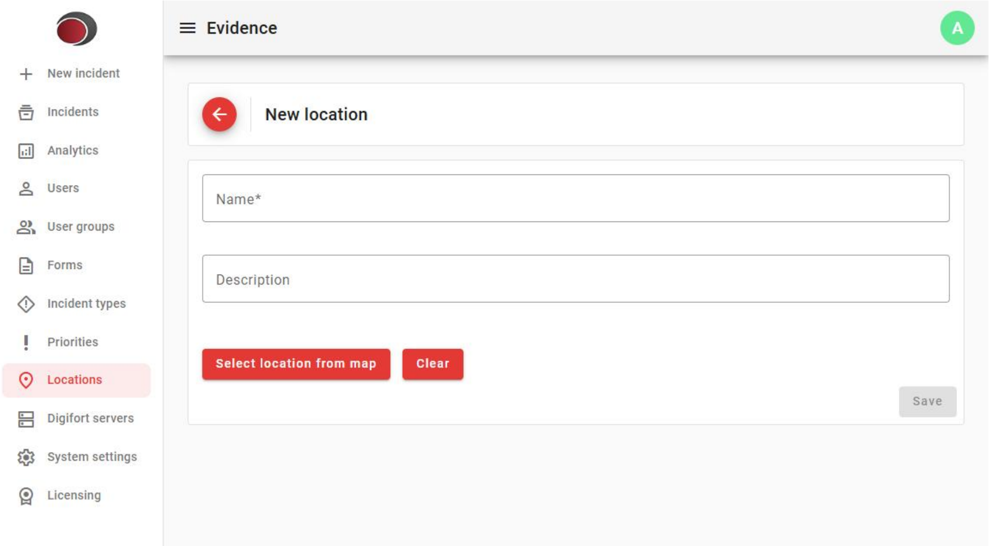
12.1 Accessing the locations module

In the side menu, click on the **Locations** option to access the module.



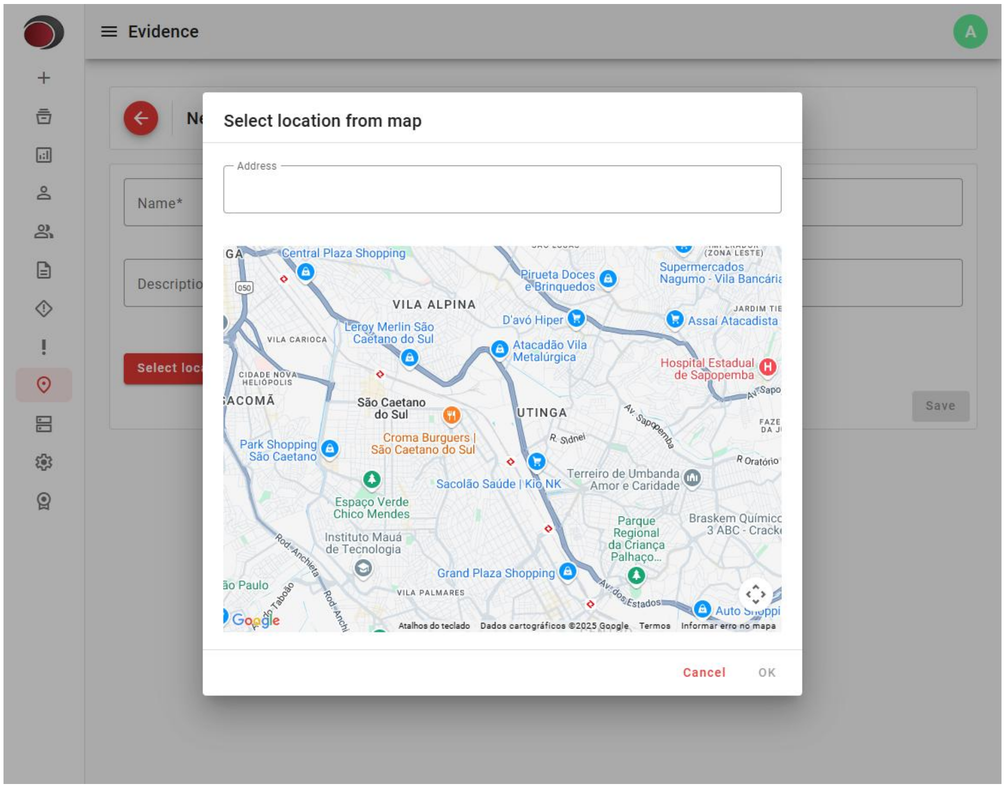
12.2 Adicionando locais

To add locations, click the button ⊕.



- **Name:** Name of the location
- **Descrição:** Optional description for the location

If this location can be associated with an address, click the **Select location from map** button.

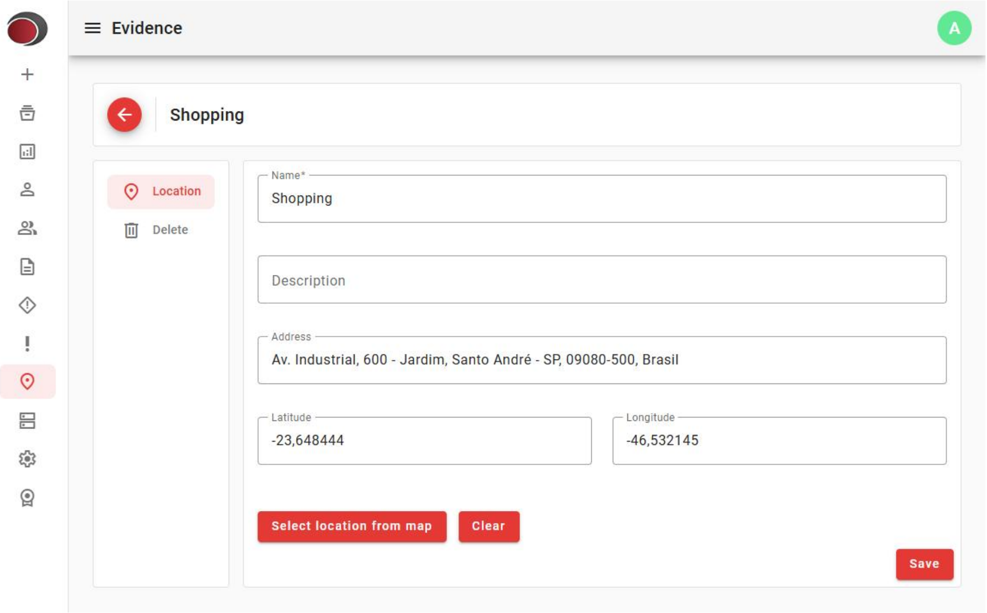


Enter the address in the **Address** field. Some suggestions will be displayed as you type the address. Select the desired option. You can also select an address directly on the map by dragging the map with the left mouse button, using the mouse scroll button to zoom in or out. Finally, double-click on the desired location so that the address is automatically selected.

Important
For the map to work, you need to add a valid API key in the system settings. See topic Map settings.

12.3 Alterando locais

To modify locations, click on the name of the location you want to modify.



Name*: Shopping

Description

Address: Av. Industrial, 600 - Jardim, Santo André - SP, 09080-500, Brasil

Latitude: -23,648444

Longitude: -46,532145

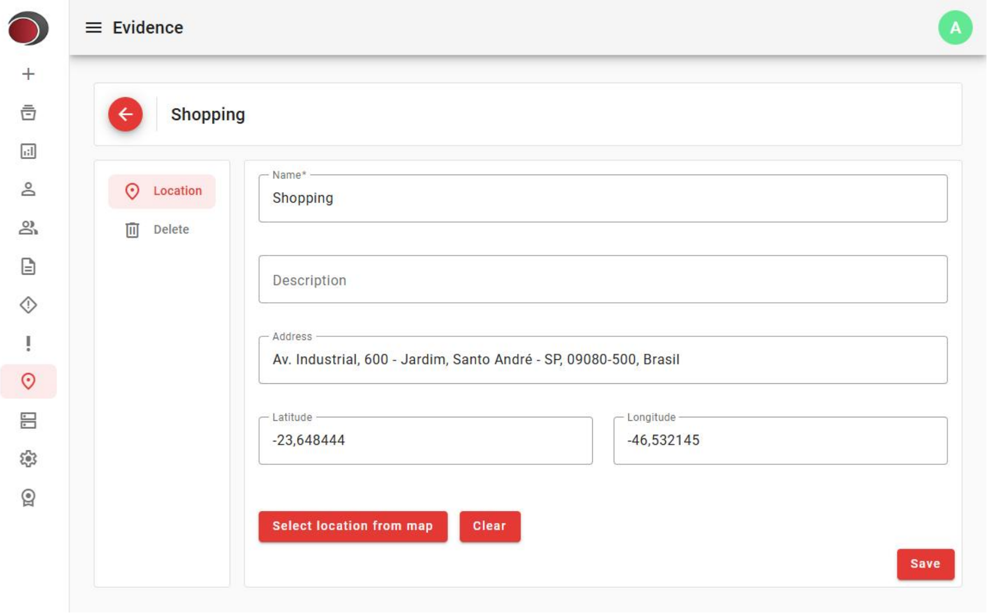
On the left side there is a menu where more settings can be made.

- **Location:** Allows you to modify the main location data.
- **Excluir:** Removes priority from the system. See the topic Excluindo locais.

12.4 Excluindo locais

When you delete a location, it will no longer be selectable when creating incidents. Even if deleted, locations associated with previously created incidents will be preserved.

To delete locations click the **Delete** button.



Name*: Shopping

Description

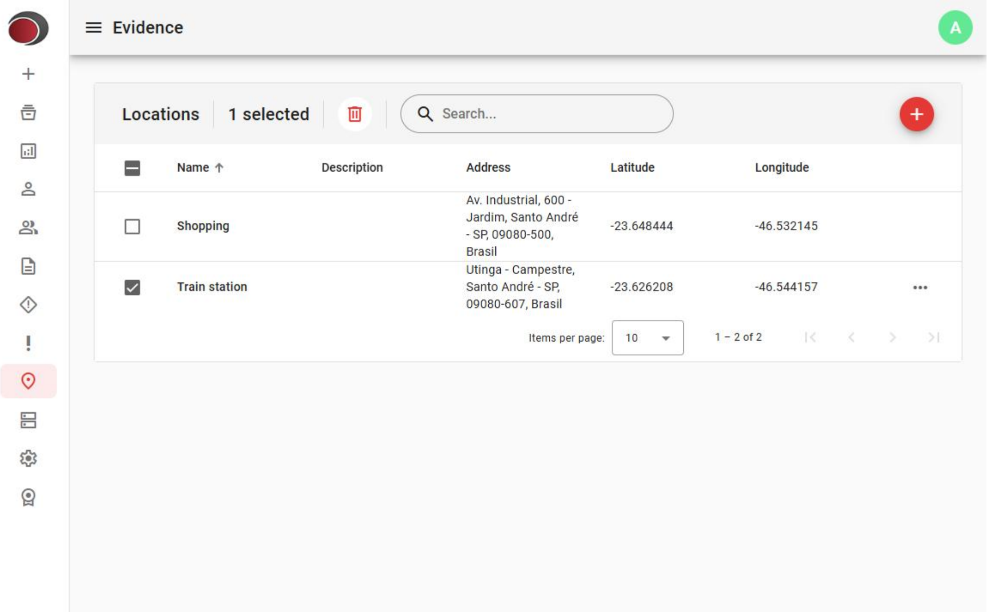
Address: Av. Industrial, 600 - Jardim, Santo André - SP, 09080-500, Brasil

Latitude: -23,648444

Longitude: -46,532145

Another way to delete locations is through the location registry. Next to each item there is a three-dot button with the option to remove it.

You can also use the checkboxes to remove more than one item at a time. Select the items you want to remove and then click 🗑.



▬	Name ↑	Description	Address	Latitude	Longitude	
□	Shopping		Av. Industrial, 600 - Jardim, Santo André - SP, 09080-500, Brasil	-23.648444	-46.532145	
☑	Train station		Utinga - Campestre, Santo André - SP, 09080-607, Brasil	-23.626208	-46.544157	•••

Items per page: 10 1 – 2 of 2

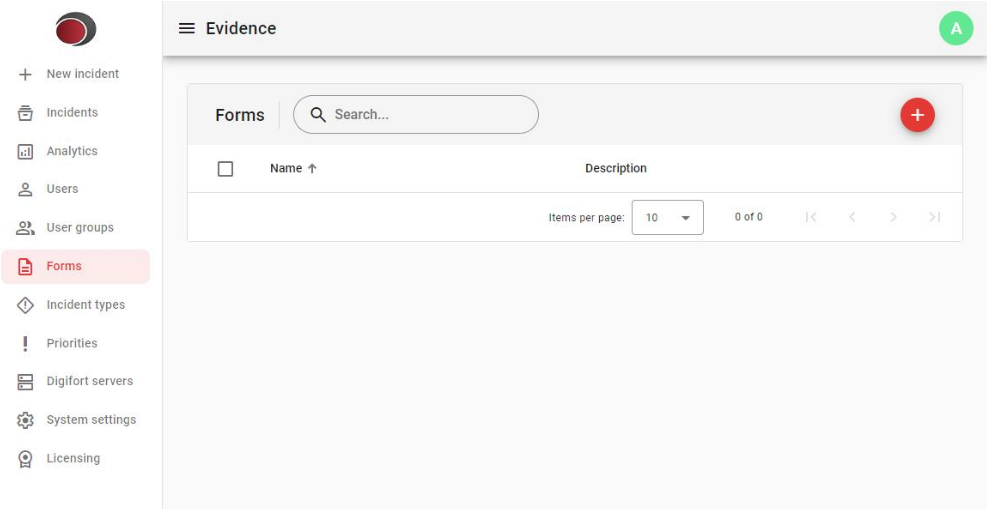
Chapter XIII

13 Forms

The forms module is a tool that allows the creation of forms adapted to the specific needs of each type of incident. This module is essential for capturing detailed and relevant information about each incident, ensuring that all necessary data is collected in a structured and efficient way.
With the forms module, administrators can create and manage custom forms with different types of fields, such as text, number, date, multiple selection, among others. These customized forms can be associated with different types of incidents, allowing for more accurate and appropriate data collection for each specific situation.

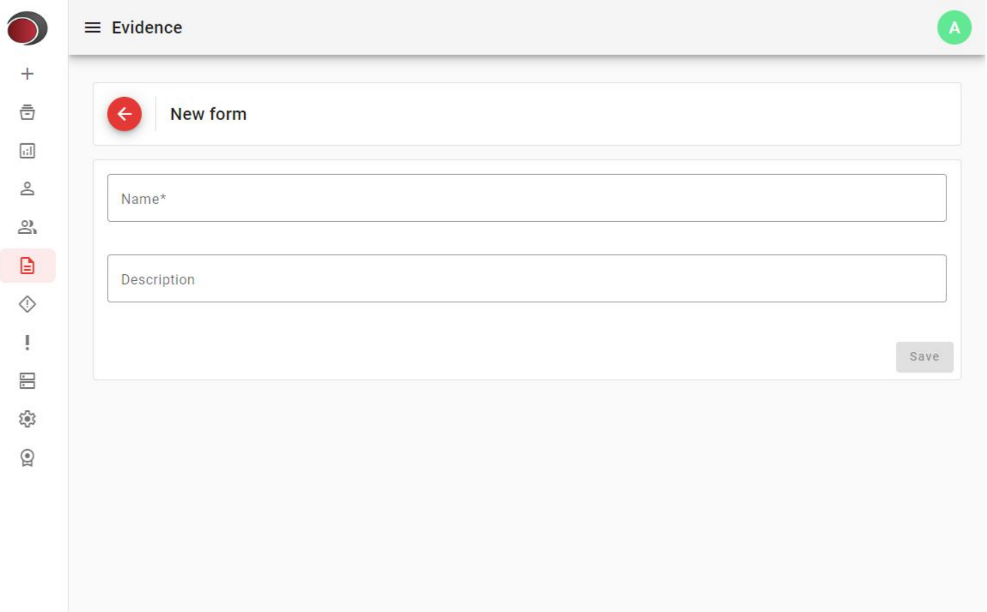
13.1 Accessing the forms module

In the side menu, click on the **Forms** option to access the module.



13.2 Adding forms

Para adicionar formulários, clique no botão ⊕.

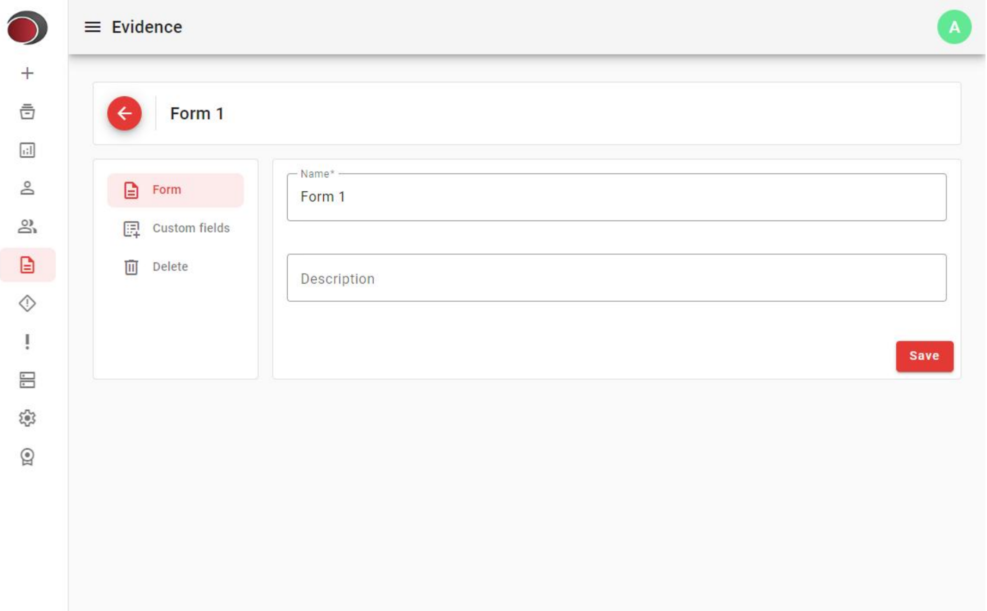


- **Name:** Name of the form.
- **Description:** An optional description for the form.

After filling in all the necessary data, click the Save button. You will automatically be redirected to the form change page. See the topic Modifying forms.

13.3 Modifying forms

To change forms, click on the name of the form you want to modify.



Name*
Form 1

On the left side there is a menu where more settings can be made.

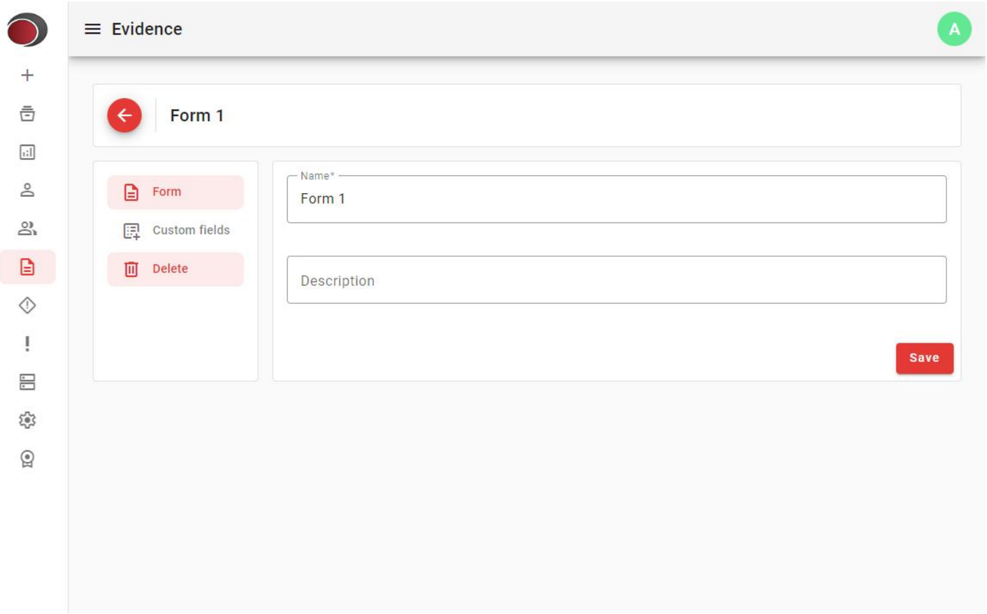
- **Form:** Allows you to modify the main data of the form.
- **Custom Fields:** Allows you to manage the form's custom fields. See the topic Custom fields.

- **Delete:** Removes the form from the system. See the topic Deleting forms.

13.4 Deleting forms

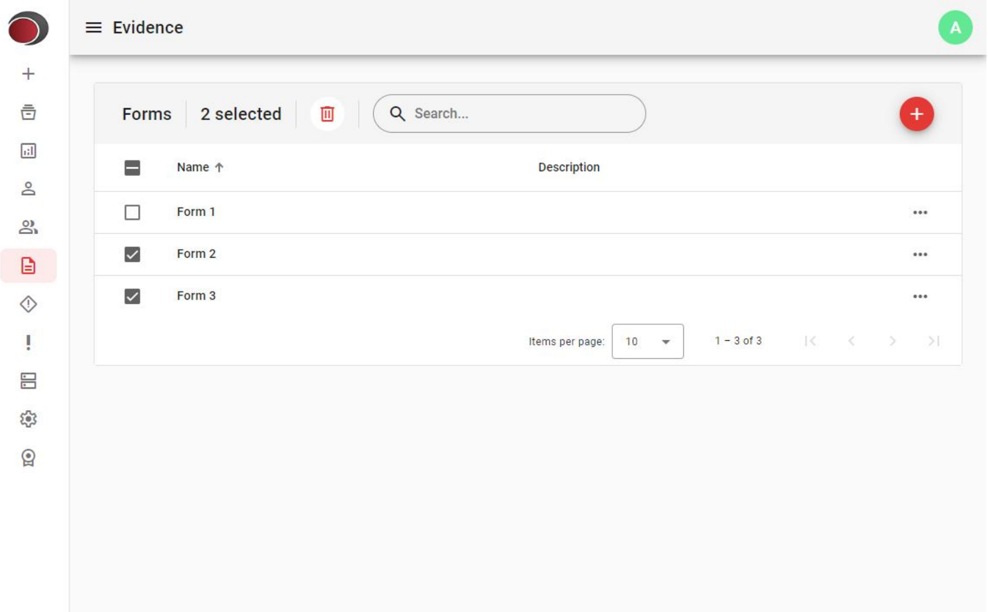
When you delete a form, it will no longer be available for filling out incidents, but all incidents created with this form will be preserved.

To delete forms, click the **Delete** button, as shown in the image below:



Name* Form 1

Another way to delete forms is through form registration. Next to each item there is a three-dot button with the option to remove it.
You can also use check boxes to remove more than one item at the same time. Select the items to be removed and then click 🗑.



Evidence

Forms 2 selected

Search...

▬	Name ↑	Description
☐	Form 1	
☑	Form 2	
☑	Form 3	

Items per page: 10

1 – 3 of 3

13.5 Custom fields

You can add custom fields to forms so that they can be filled in when an incident is added.

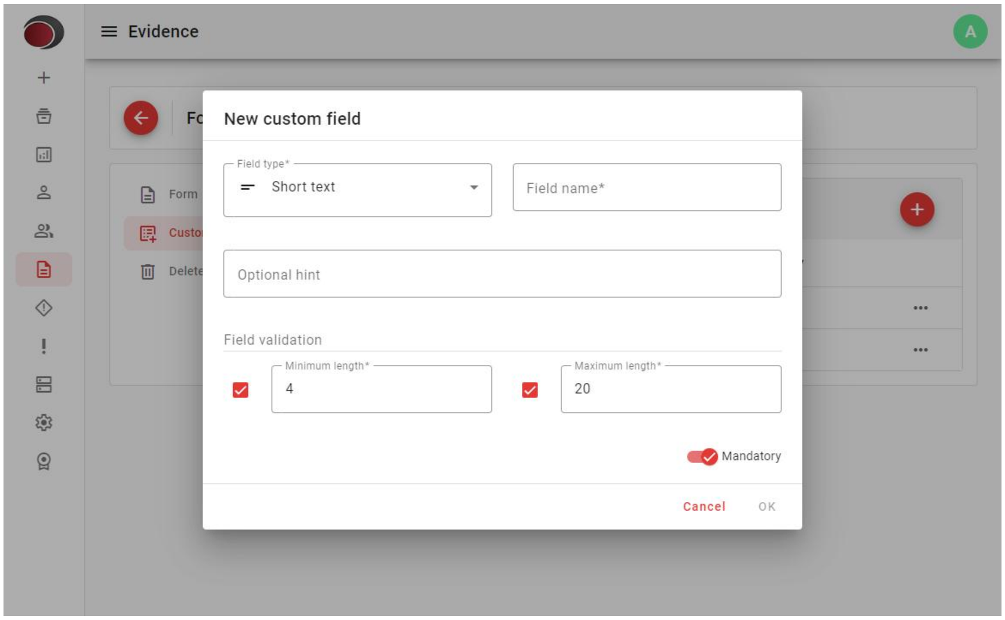
13.5.1 Custom field types

The following fields are available for use:

- **Short text:** A field for entering 1-line text.
- **Paragraph:** A field for entering multi-line text.
- **Number:** A field for entering numbers with maximum, minimum and scale validations.
- **Date:** A field for entering dates or selecting from a calendar.
- **Time:** A field for entering times.
- **Datetime:** A field that combines date and time.
- **Checkboxes:** A field where multiple options can be selected together.
- **Multiple choice:** A field with several options where only one of them can be selected.
- **Drop-down list:** A field with multiple options where only one of them can be selected from a drop-down list.
- **URL:** A field where a URL must be provided. When viewing an incident, links can be clicked to open in the browser.
- **Location:** A geographic location field. When filling out, the user can select the location on a map or search by address.

13.5.1.1 Short text

A simple 1-line text field.



New custom field

Field type*: Short text

Field name*

Optional hint

Field validation

☑ Minimum length*: 4

☑ Maximum length*: 20

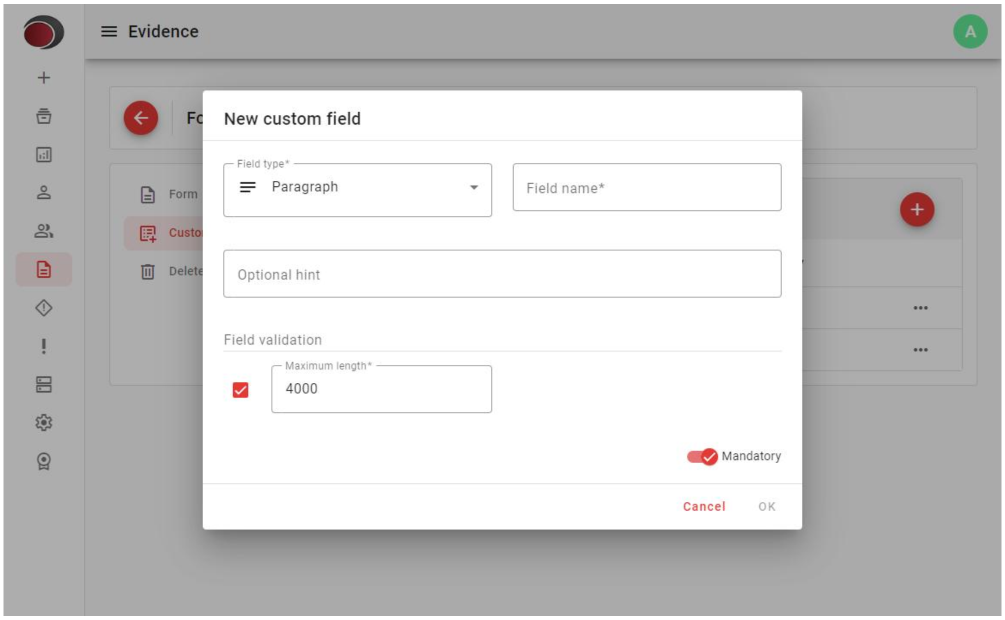
Mandatory

Validations:

- **Minimum length:** The minimum length of the text.
- **Maximum length:** The maximum length of the text.

13.5.1.2 Paragraph

A multi-line text field.



New custom field

Field type*: Paragraph

Field name*

Optional hint

Field validation

☑ Maximum length*: 4000

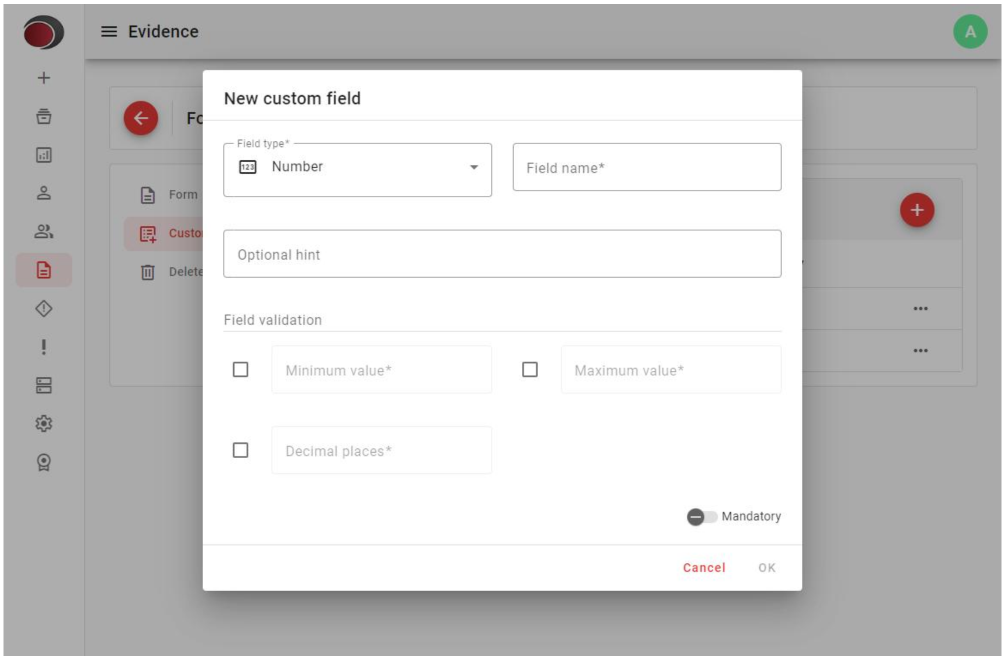
Mandatory

Validations:

- **Maximum length:** The maximum length of the text.

13.5.1.3 Number

A numeric field.



New custom field

Field type*: Number

Field name*

Optional hint

Field validation

□ Minimum value*   □ Maximum value*

□ Decimal places*

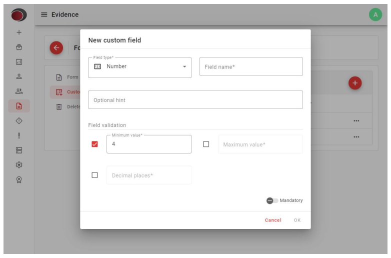
Mandatory

Cancel   OK

Validations:

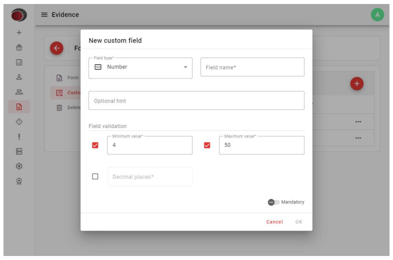
- **Minimum value:** The minimum value of the number.
- **Maximum value:** The maximum value of the number.
- **Decimal places:** Number of decimal places.

13.5.1.3.1 Examples



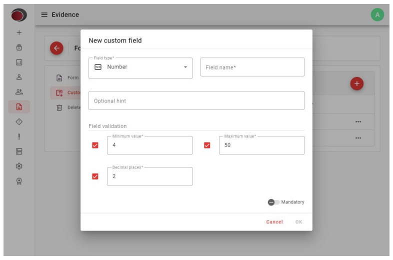
☑ Minimum value*: 4   □ Maximum value*   □ Decimal places*

The value of the number must be at least 4 and no maximum value



☑ Minimum value*: 4   ☑ Maximum value*: 50   □ Decimal places*

The value of the number must be between 4 and 50

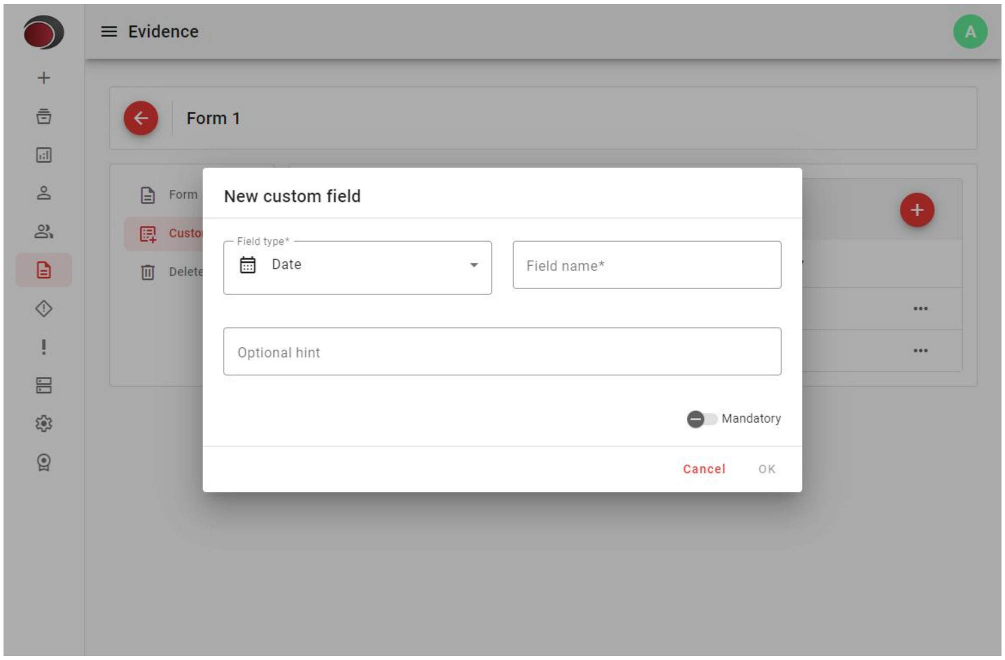


☑ Minimum value*: 4   ☑ Maximum value*: 50   ☑ Decimal places*: 2

The value of the number must be between 4 and 50 and 2 decimal places

13.5.1.4 Date

A field that allows you to select a date from a calendar.

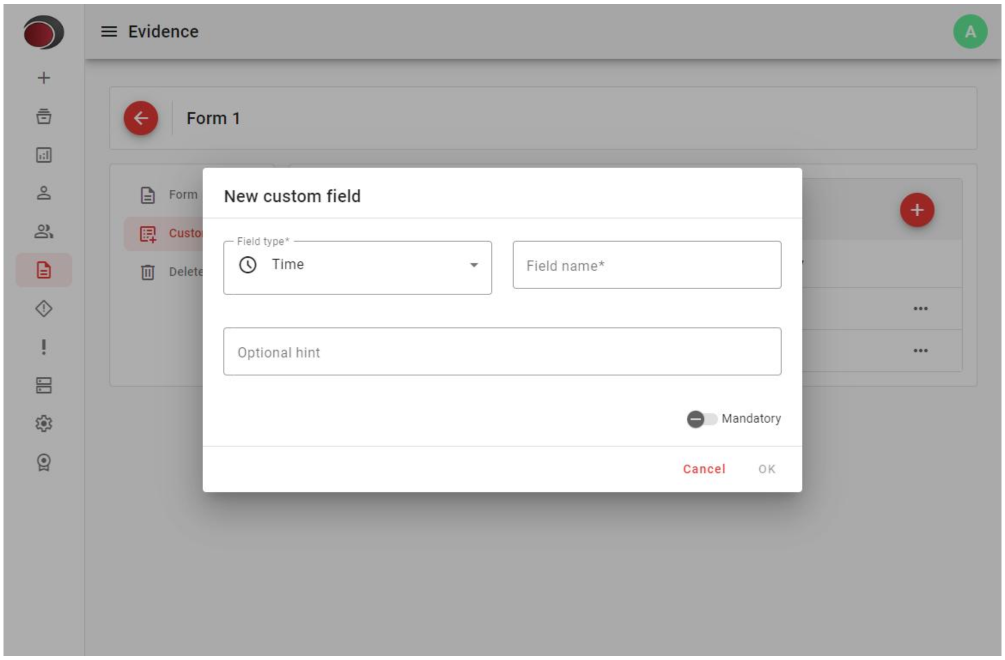


New custom field

Field type*: Date

13.5.1.5 Time

A time field.

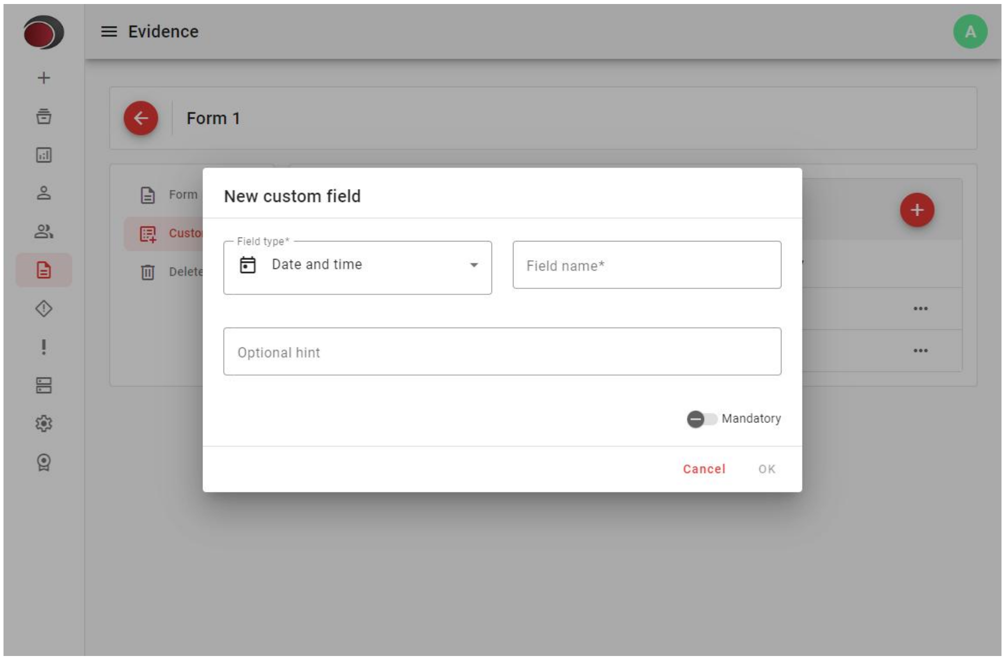


New custom field

Field type*: Time

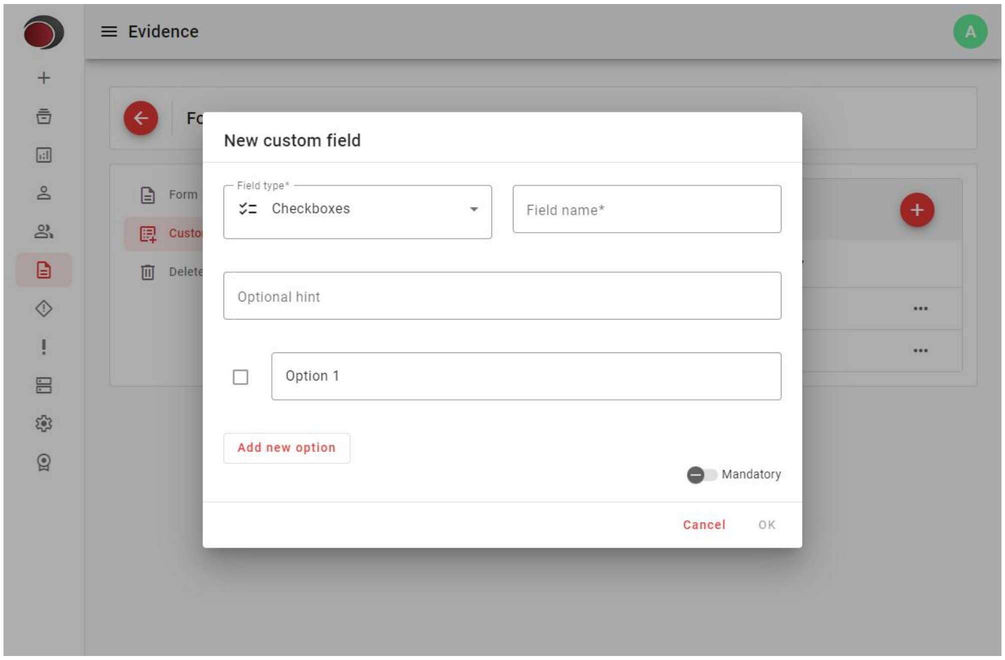
13.5.1.6 Date and time

A field with date, selectable by a calendar, and time.

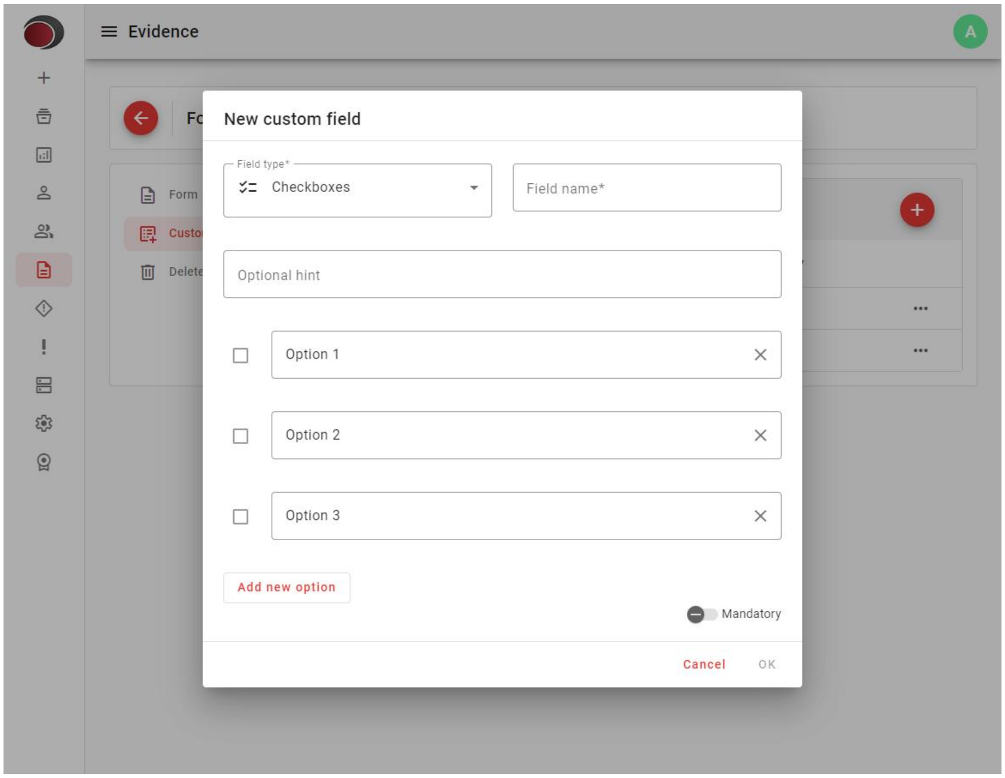


13.5.1.7 Checkboxes

A field where several options can be selected together when filling out the incident.

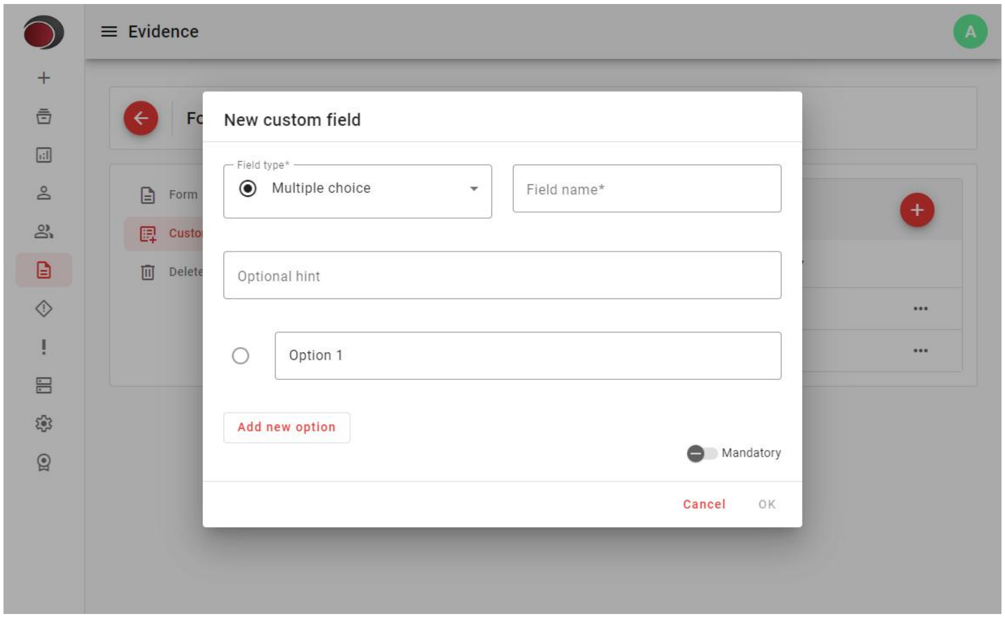


To add new options, click the **Add option** button and type the text for this option.

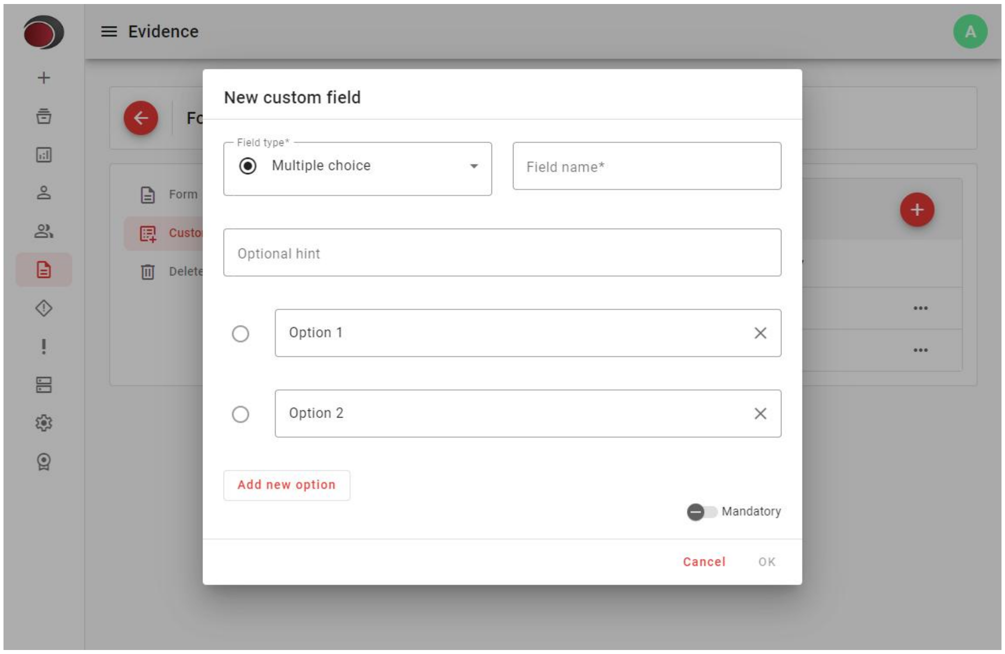


13.5.1.8 Multiple choice

A field with several options where only one of them can be selected.

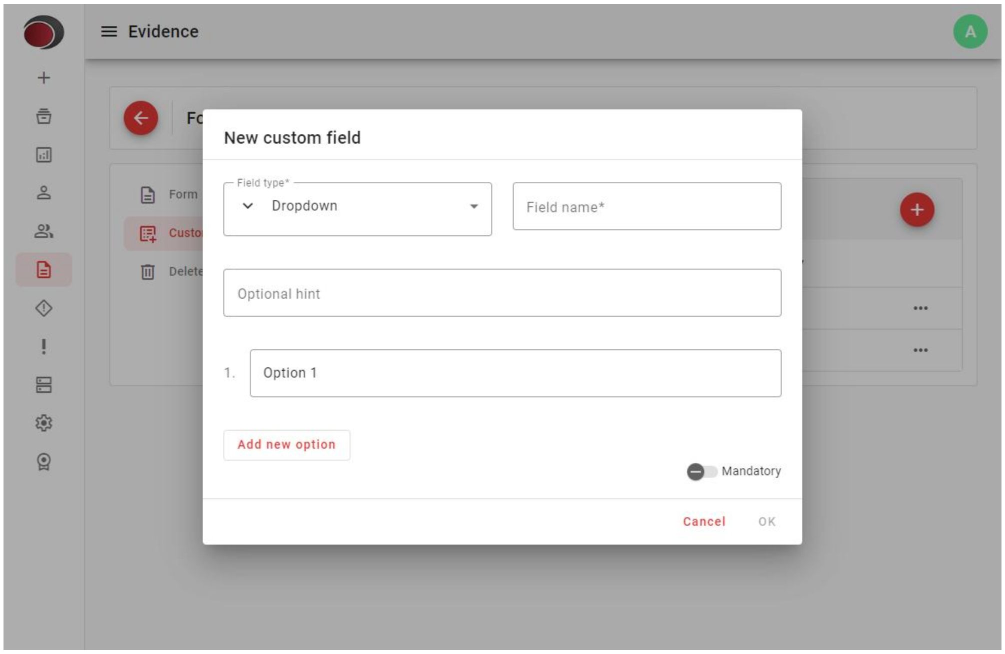


To add new options, click the **Add option** button and type the text for this option.

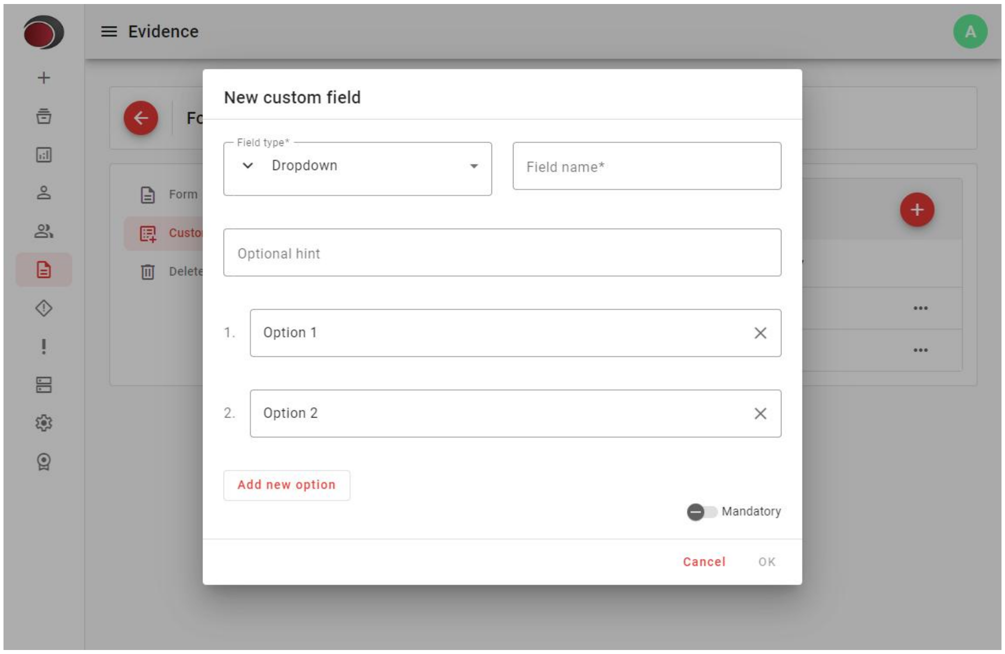


13.5.1.9 Dropdown

A field with multiple options where only one of them can be selected from a drop-down list.



To add new options, click the **Add option** button and type the text for this option.



New custom field

Field type*: Dropdown

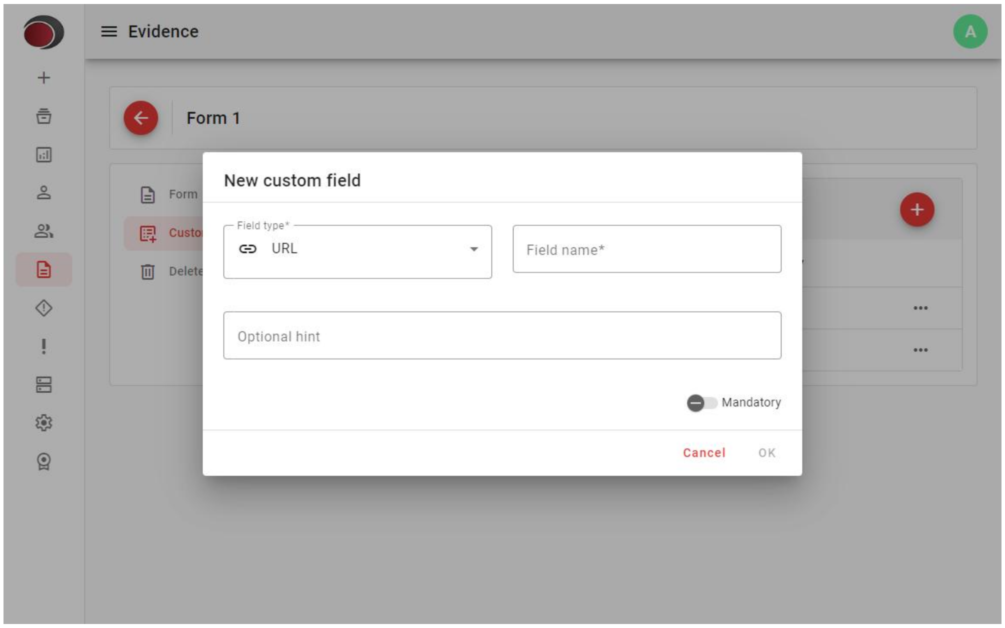
Field name*

Optional hint

1. Option 1
2. Option 2

13.5.1.10 URL

A field where a URL must be provided. When viewing an incident, links can be clicked to open in the browser.



New custom field

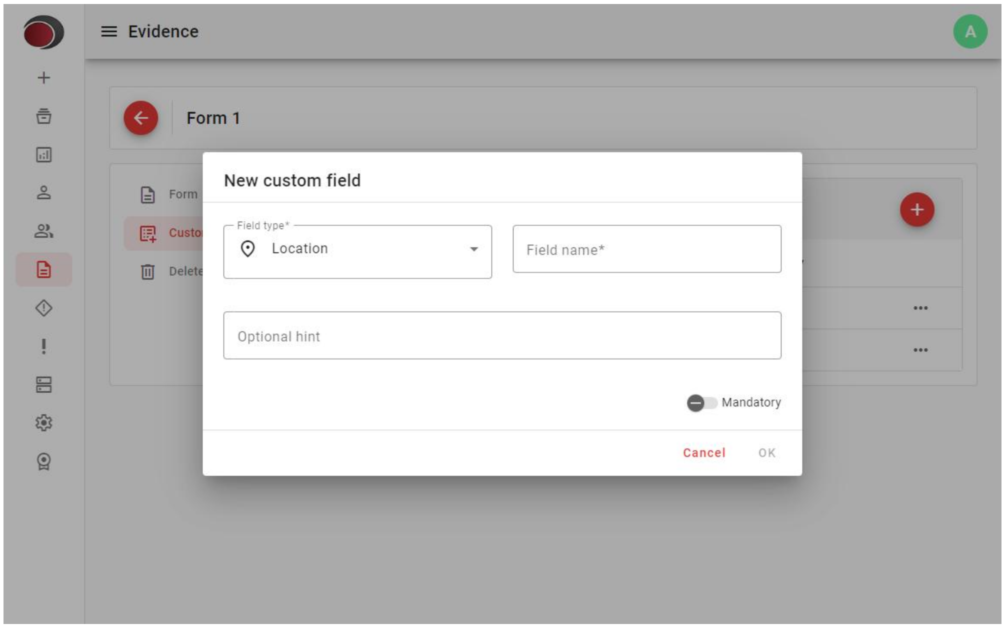
Field type*: URL

Field name*

Optional hint

13.5.1.11 Location

A geographic location field. When filling out, the user can select the location on a map or search by address.



New custom field

Field type*: Location

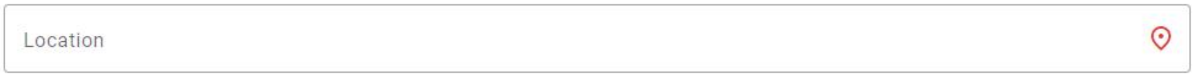
Field name*

Optional hint

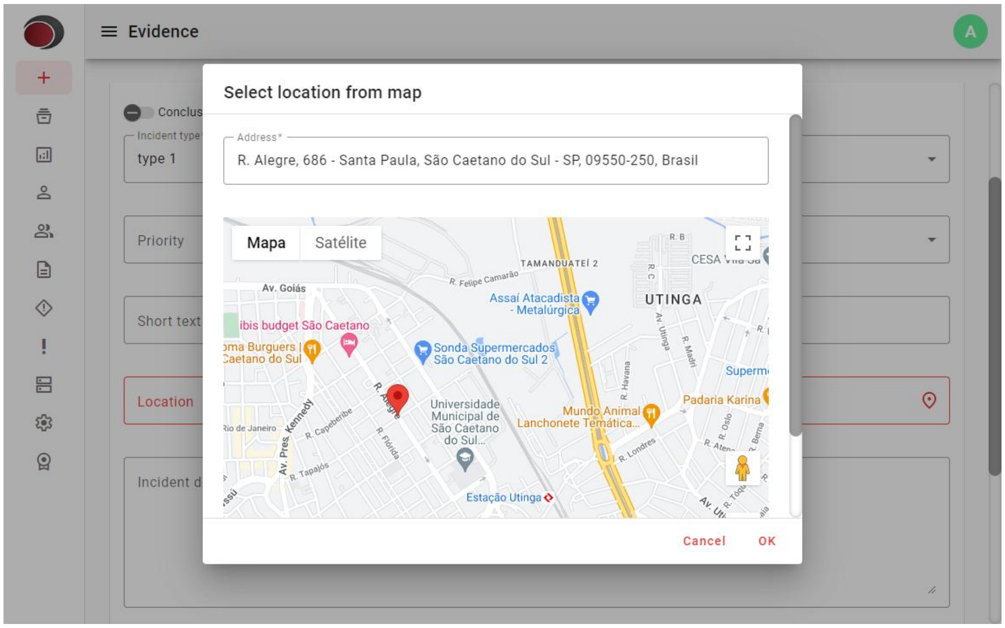
Mandatory

13.5.1.11.1 Filling in the location field

When filling out an incident, if this field is available, it will be displayed as follows:



To select a location, click the button 📍.



Select location from map

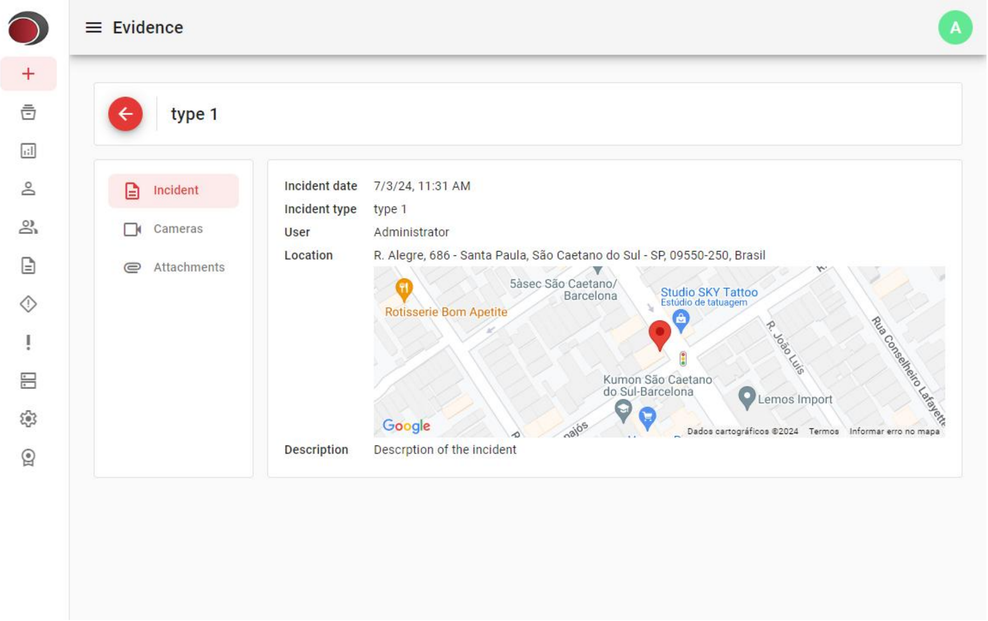
Address*: R. Alegre, 686 - Santa Paula, São Caetano do Sul - SP, 09550-250, Brasil

You can search for an address in the text field. With the auto-complete feature you can complete the address selection with the up or down arrows on the keyboard or by clicking on a suggestion with the

mouse.
You can also select an address by double-clicking on the map. The corresponding address will be automatically filled in.

13.5.1.11.2 Viewing a location field

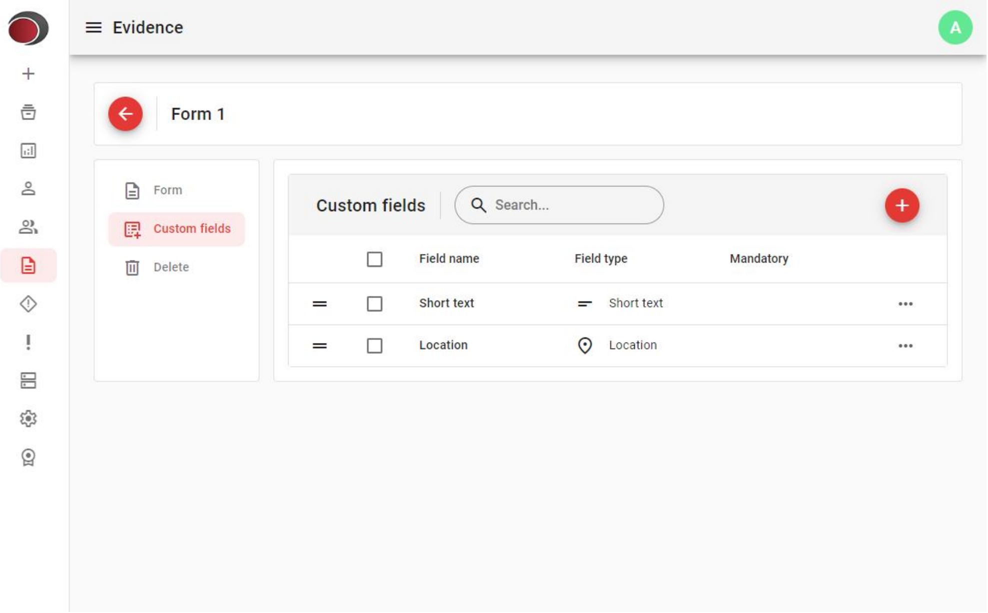
Location custom fields appear in an incident view as follows:



Incident date 7/3/24, 11:31 AM
Incident type type 1
User Administrator
Location R. Alegre, 686 - Santa Paula, São Caetano do Sul - SP, 09550-250, Brasil
Description Descrption of the incident

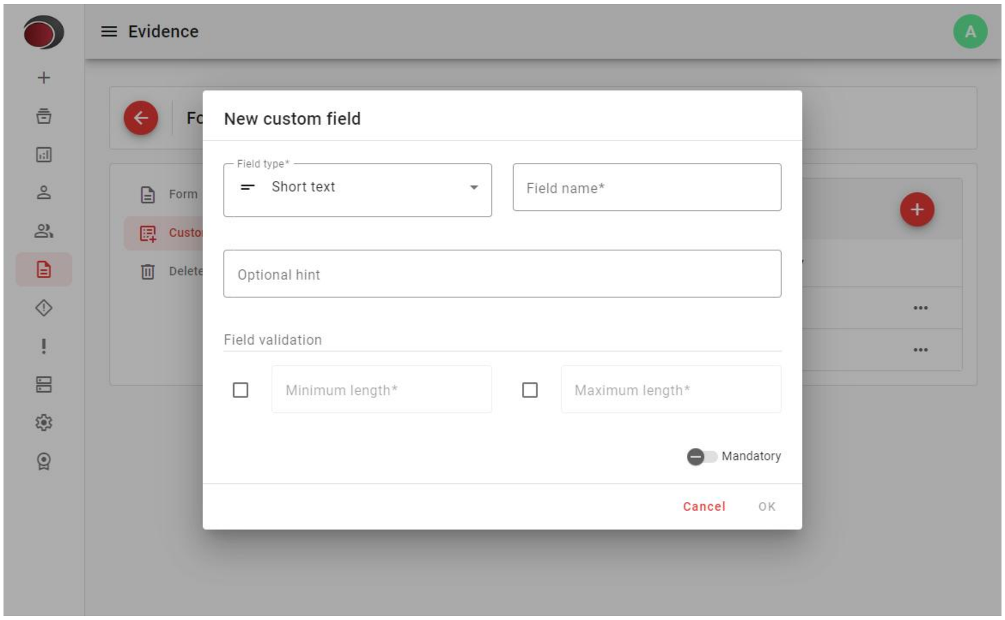
13.5.2 Adding custom fields

To add custom fields, first click the **Custom Fields** button located in the side menu of a form.



	□	Field name	Field type	Mandatory	
═	□	Short text	Short text		•••
═	□	Location	Location		•••

Once done, click the button ⊕ to add a new custom field.



New custom field

Field type*: Short text

Field name*

Optional hint

Field validation

□ Minimum length*

□ Maximum length*

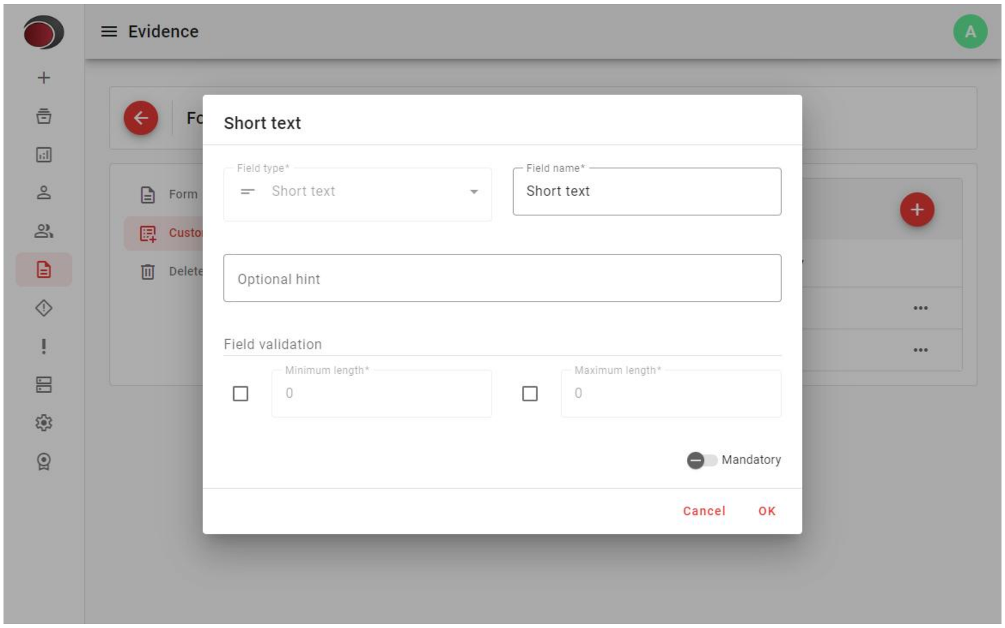
Mandatory

Cancel OK

- **Field type:** See the topic Custom fields.
- **Field Name:** This will be the text that identifies this field when filling out the incident.
- **Optional hint:** An optional text that describes the purpose of the field. This text will be displayed to the operator when completing the incident.
- **Field validation:** Some field types allow you to add validations. See the topic Custom fields.
- **Mandatory:** Mark the field as mandatory. A field marked as mandatory must be filled in by the operator when adding an incident. If it is not filled in, the incident cannot be saved.

13.5.3 Modifying custom fields

To change custom fields, click the name of the field you want to modify.



Short text

Field type*: Short text

Field name*: Short text

Optional hint

Field validation

□ Minimum length*: 0

□ Maximum length*: 0

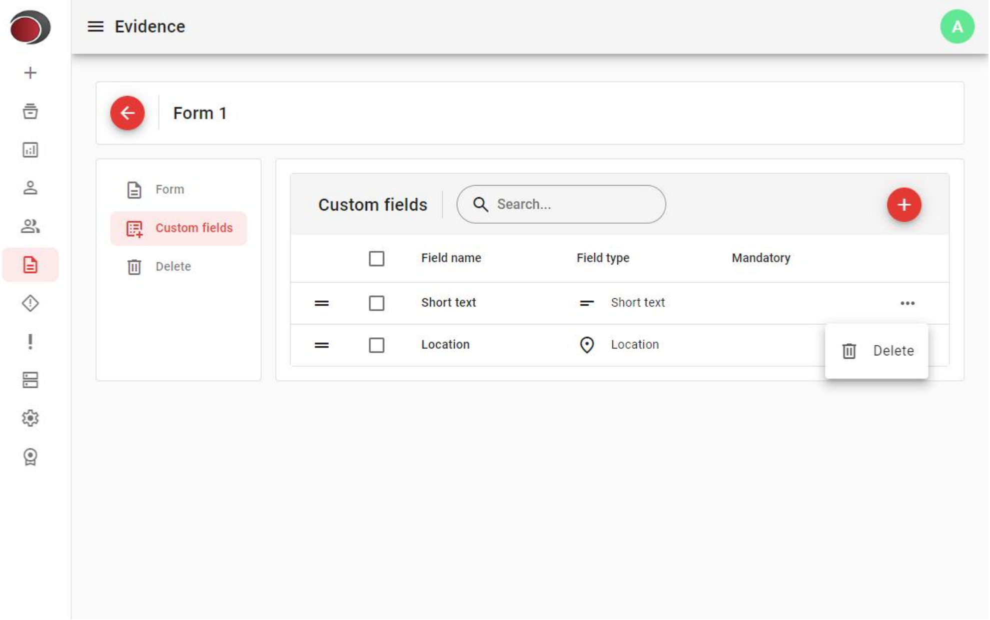
Mandatory

Cancel OK

13.5.4 Deleting custom fields

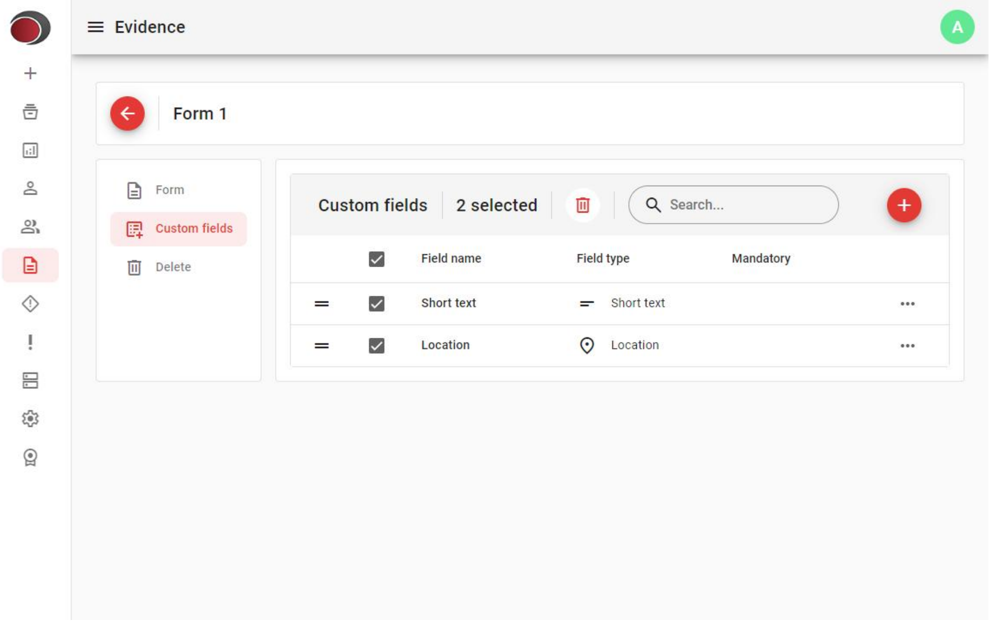
When deleting a custom field, it will no longer be available for filling incidents, but all incidents created with this field will be preserved.

To delete custom fields, click the 3-dot button on the right and then the **Delete** button.



	□	Field name	Field type	Mandatory	
═	□	Short text	Short text		•••
═	□	Location	Location		

You can also use checkboxes to remove more than one field at the same time. Select the fields to remove and then click 🗑.



	☑	Field name	Field type	Mandatory	
═	☑	Short text	Short text		•••
═	☑	Location	Location		•••

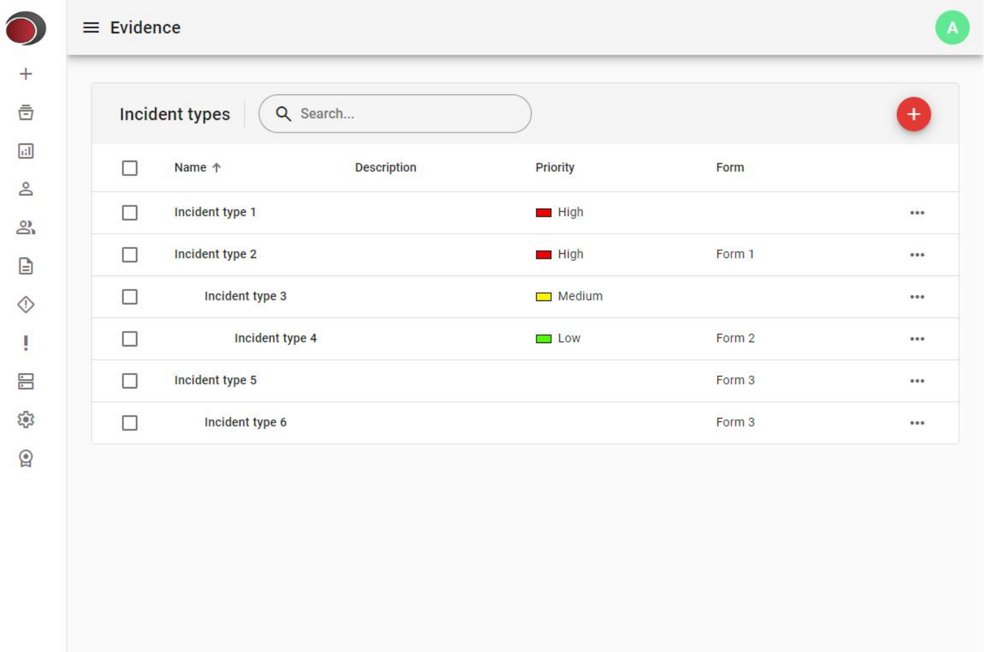
Chapter XIV

14 Incident types

Incident types are used to categorize incidents and provide functionality while filling in the incident form. Incident types can be chained hierarchically, working as categories, and have associated forms. This configuration will determine which items can be selected by the user when filling out incidents, according to the rules below:

- Items that have children can only be selected if there is an associated form. Otherwise, the user must select an available child.
- Items at the last levels of the hierarchy can always be selected, whether there is an associated form or not.

See the example below:

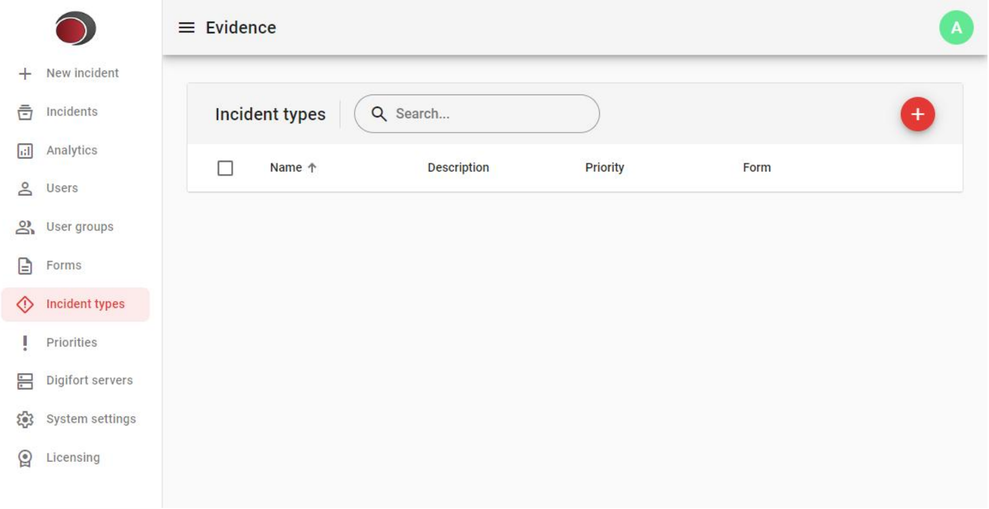


□	Name ↑	Description	Priority	Form	
□	Incident type 1		🟥 High		•••
□	Incident type 2		🟥 High	Form 1	•••
□	Incident type 3		🟨 Medium		•••
□	Incident type 4		🟩 Low	Form 2	•••
□	Incident type 5			Form 3	•••
□	Incident type 6			Form 3	•••

- **Incident type 1** can be selected as it does not have children. As there is no associated form, only the standard fields will be displayed for filling in the incident form.
- **Incident type 2** can be selected, because despite having children, it has an associated form. The custom fields from the **Form 1** will be displayed for you to fill out.
- **Incident type 3** cannot be selected because it has children and does not have an associated form.
- **Incident type 4** can be selected as it does not have children. The custom fields from the **Form 2** will be displayed for you to fill out.
- **Incident type 5** can be selected, because despite having children, it has an associated form. The custom fields from the **Form 3** will be displayed for you to fill out.
- **Incident type 6** can be selected as it does not have children. The custom fields from the **Form 3** will be displayed for you to fill out.

14.1 Accessing the incident types module

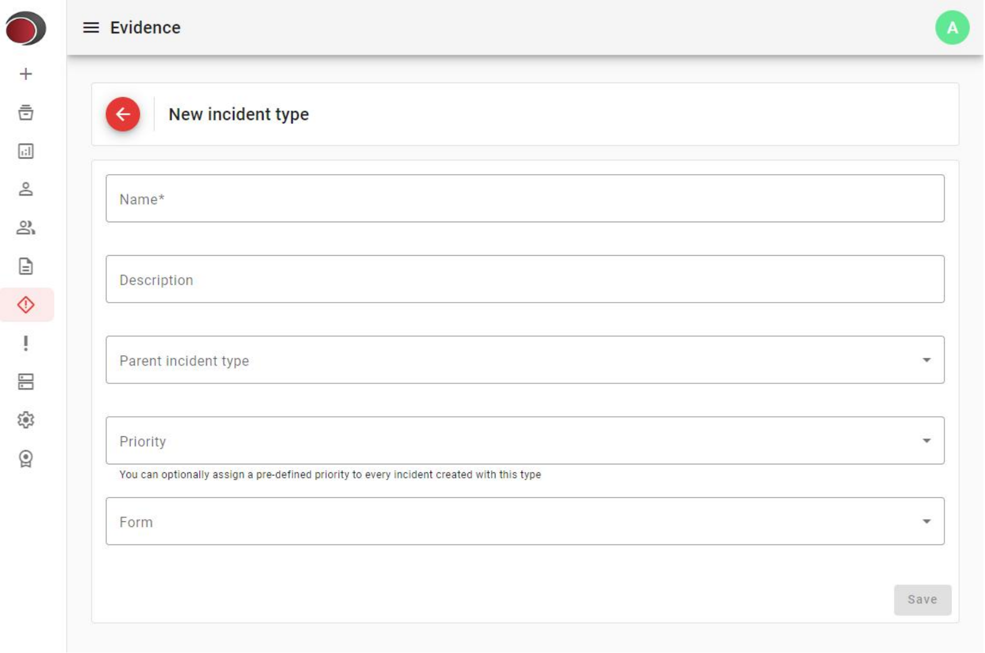
In the side menu, click on the **Incident types** option to access the module.



☐	Name ↑	Description	Priority	Form

14.2 Adding incident types

Para adicionar tipos de incidentes, clique no botão ⊕.



Name*

Description

Parent incident type

Priority

You can optionally assign a pre-defined priority to every incident created with this type

Form

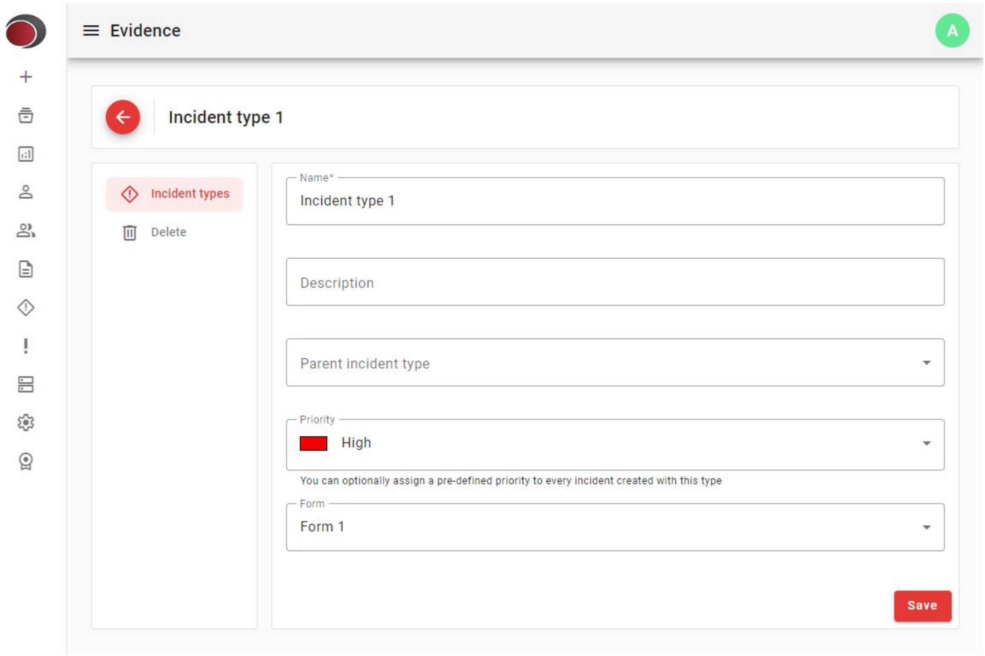
- **Name:** Name of the incident type.
- **Description:** An optional description.
- **Parent incident type:** Incident types can be chained together to help in categorizing and organizing incidents.
- **Priority:** You can optionally associate a priority for each incident created with this type. If a priority is not associated with the incident type, the user can choose a priority when filling out the incident.
- **Form:** You can optionally associate a form with the incident type. If a form is associated, the form's custom fields will be displayed for completion.
- **Allow selection of a location from the location registry:** By enabling this option, the user will be able to select a previously registered location to be associated with the incident. See the topic Locations. The following values ?determine the behavior of this feature:

- ○ **None:** The field to select the location will not be displayed for this type of incident.
- ○ **Optional:** The field to select the location will be displayed, but the user can fill in this field or not.
- ○ **Mandatory:** The field to select the location will be displayed and the user will be required to select a location.

After filling in all the necessary data, click the **Save** button. You will be automatically redirected to the change page. See the topic Modifying incident types.

14.3 Modifying incident types

To change incident types, click the name of the incident type you want to modify,



Name* Incident type 1

Description

Parent incident type

Priority 🟥 High

You can optionally assign a pre-defined priority to every incident created with this type

Form Form 1

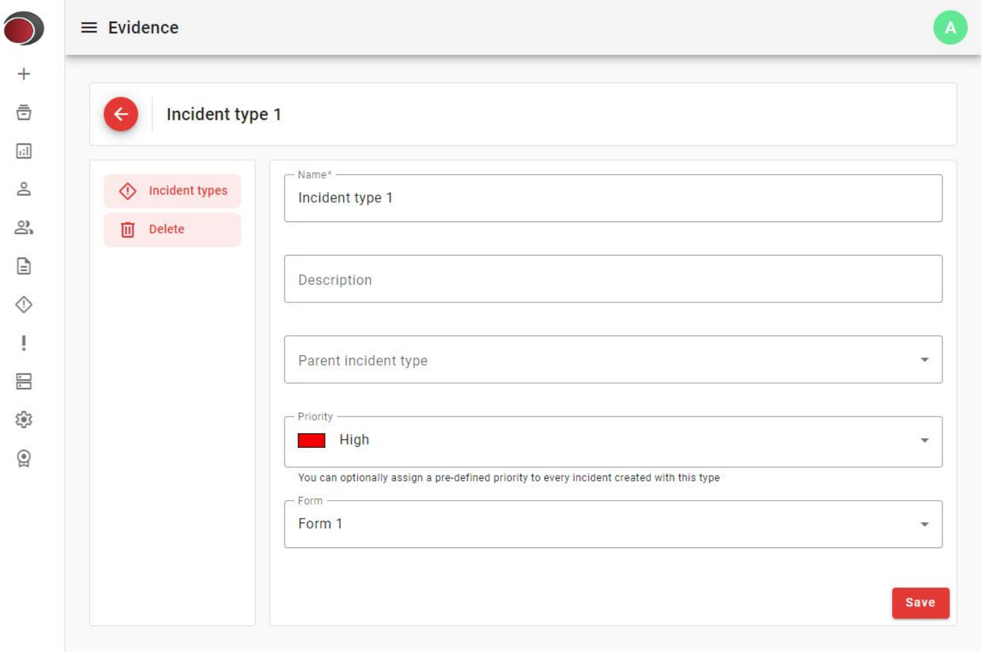
On the left side there is a menu where more settings can be made.

- **Incident type:** Allows you to modify the main data of the incident type.
- **Delete:** Removes the incident type from the system. See the topic Deleting incident types.

14.4 Deleting incident types

When you delete an incident type, it will no longer be available for selection when populating incidents, but all incidents created with that incident type will be preserved.

To delete, click the **Delete** button, as shown in the image below:



Incident type 1

Name*: Incident type 1

Description

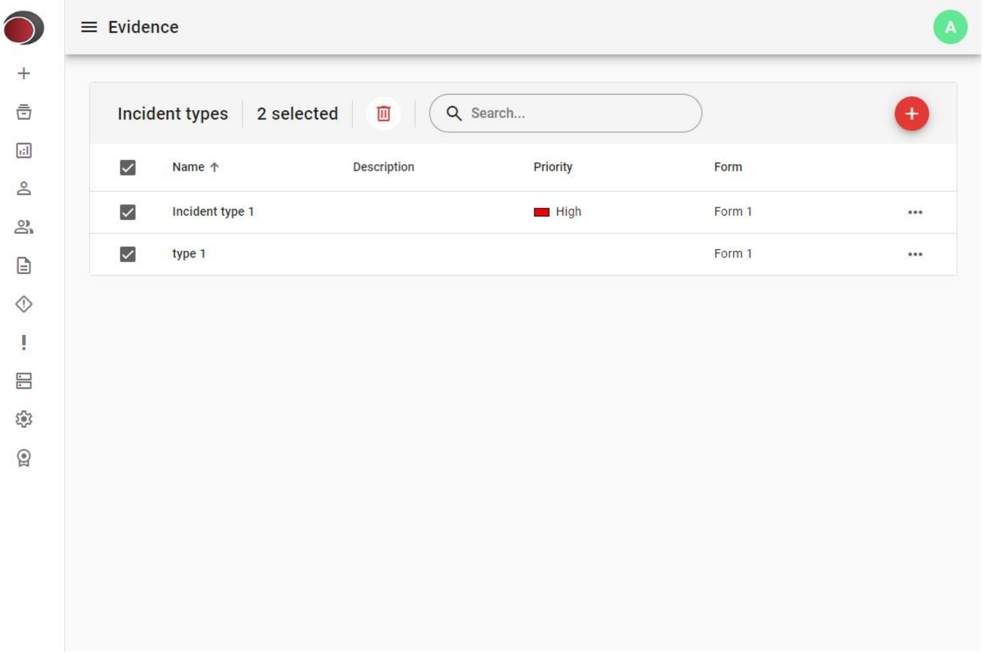
Parent incident type

Priority: 🟥 High

You can optionally assign a pre-defined priority to every incident created with this type

Form: Form 1

Another way to exclude is by registering incident types. Next to each item there is a three-dot button with the option to remove it.
You can also use check boxes to remove more than one item at the same time. Select the items to be removed and then click 🗑.



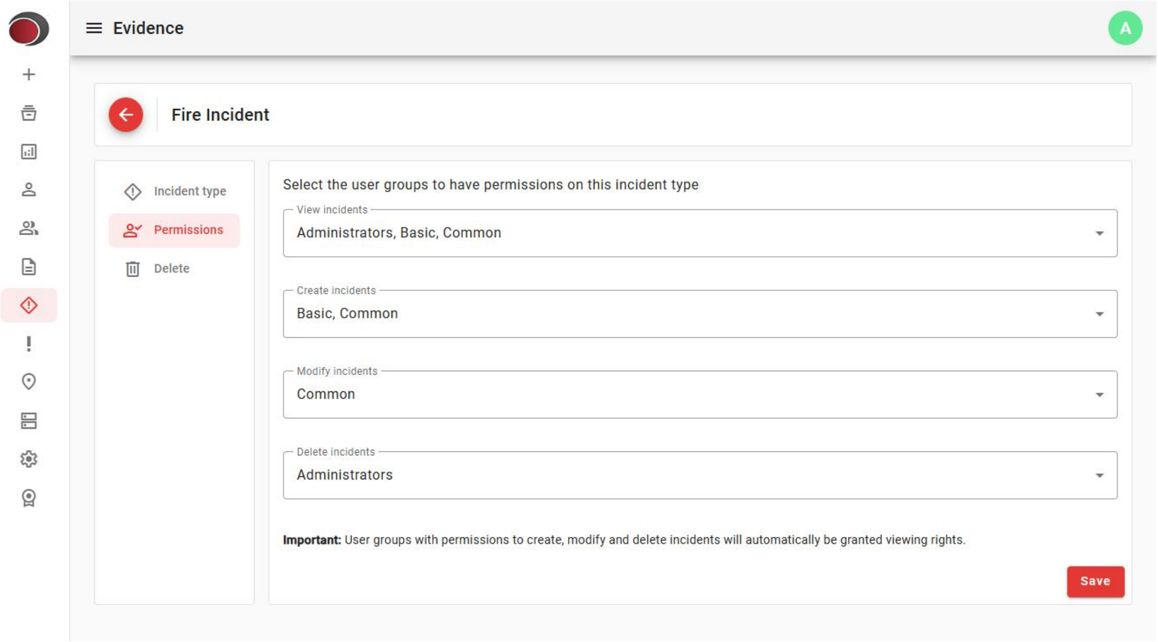
☑	Name ↑	Description	Priority	Form	
☑	Incident type 1		🟥 High	Form 1	•••
☑	type 1			Form 1	•••

Importante

! Incidents already created with this incident type will be preserved. All users will lose permission to view incidents associated with that type. Only the admin user will be able to view, edit, or delete these incidents. To avoid this effect, you can change the incident type of the incidents before performing this action.

14.5 Setting permissions to incident types

For users to be able to manage incidents, you need to define permissions for each incident type. This feature allows you to assign groups of users to tasks such as viewing, creating, modifying, and deleting incidents.
To access the permissions settings, click the **Permissions** button.



Select the user groups to have permissions on this incident type

View incidents: Administrators, Basic, Common

Create incidents: Basic, Common

Modify incidents: Common

Delete incidents: Administrators

Important: User groups with permissions to create, modify and delete incidents will automatically be granted viewing rights.

View Incidents: Select the user groups that will be allowed to view incidents of this type.
Create Incidents: Select the user groups that will be allowed to create incidents of this type.
Modify Incidents: Select the user groups that will be allowed to modify incidents of this type. To add or remove attachments and cameras, the user also needs this permission.
Delete Incidents: Select the user groups that will be allowed to delete incidents of this type

To create user groups, see the topic User groups.

Importante
! User groups with permissions to create, modify or delete incidents will automatically be granted viewing rights.

.

Chapter XV

15 Incidents

O módulo de incidentes é o recurso que será utilizado no dia a dia pela maioria dos usuários. É neste módulo onde formulários de incidentes serão preenchidos.

15.1 Overview

Incident Forms and Reviews Structure

When saving an incident, the system records not only the data filled in by the user, but also the entire **form structure** associated with the selected **incident type**. This means that custom fields, their settings, and positions in the form are stored along with the incident information.

Importance of Understanding Structure

To fully understand this functionality, it is important that the user is familiar with two main concepts:

- **Forms with custom fields:** created to allow flexibility in collecting information, with fields of text, number, coordinates, among others. See the topic Forms.
- **Incident Types:** configurable categories that organize incidents. Each type can have an associated form, which defines the fields that will be displayed when creating an incident. See the topic Incident types.

Revision-Immutable Structure

Since forms can be modified at any time by administrators, it is essential to ensure that the data entered into an incident remains consistent over time. Therefore, the original structure of the form associated with the incident **is saved at the time of registration** and remains **unchanged** even if the form associated with the incident type is subsequently changed.

This saved structure will be used in two situations:

- **Preview:** When viewing an incident, the system renders the form based on the saved structure, preserving the fields exactly as they were at the time of registration.
- **Edit:** When modifying an incident, this same structure is reused, ensuring that the original data is kept in the correct context.

! **Important**
Even if the user changes the incident type while editing, the form associated with the new type **will not be loaded.** The system will continue to use the original saved structure to maintain data consistency.

! **Important**
Even if the incident type has a fixed priority, the user **can change** the priority while editing the incident.

Editing Behavior and Revisions

When you edit an incident, the system **does not overwrite existing data.** Instead, it creates a **new**

revision that is linked to the previous revision of the incident. This new revision will contain the changes you made and will be considered the **latest version**.

- Only the most recent revision can be edited.
- Previous revisions are preserved as **read-only**, allowing full tracking of changes.
- A complete change history is available so the user can see how the incident has evolved over time. See the topic Viewing Incident Modification History.

Attachments and cameras

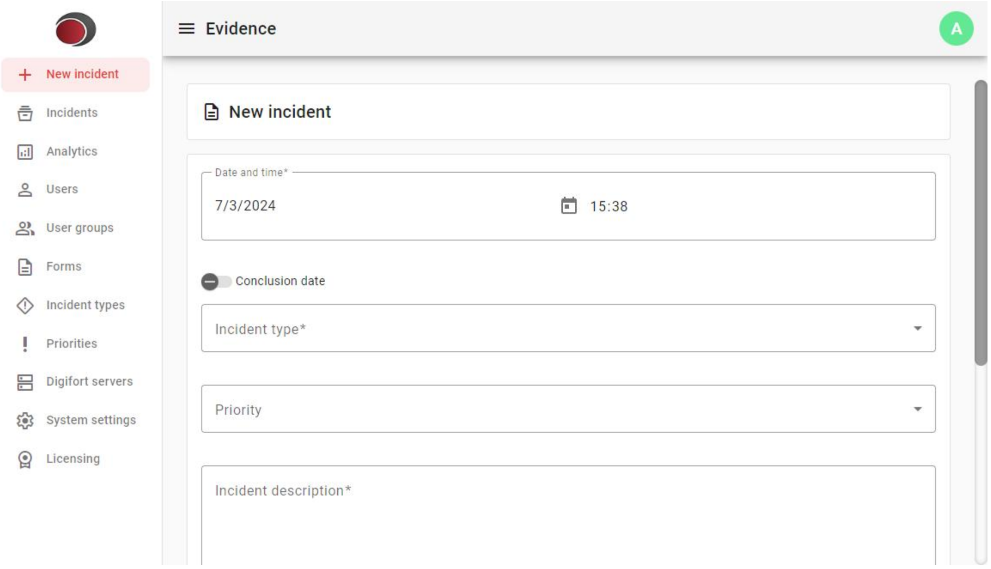
When viewing any revision of an incident, the user can add **attachments and cameras**. Even if the revision viewed is not the most recent, the system will always associate these new resources with the **latest revision** of the incident.

- Files and images are stored in the **first revision folder**, centralizing data in a single location for easy management.
- When an attachment, a camera, or even an entire incident is deleted, which also removes all associated attachments and cameras, the physical files are not deleted immediately. Instead, they are marked for deletion, and a background process will attempt to remove them as many times as necessary. This ensures that if a file is in use and cannot be deleted at that moment, the system will keep trying to delete it later until the operation succeeds.

Important
❗ For a user to add and remove attachments or cameras, they must have incident editing permission. See the topic Setting permissions to incident types.

15.2 Registering incidents

To register incidents, locate the **New incident** item in the side menu.



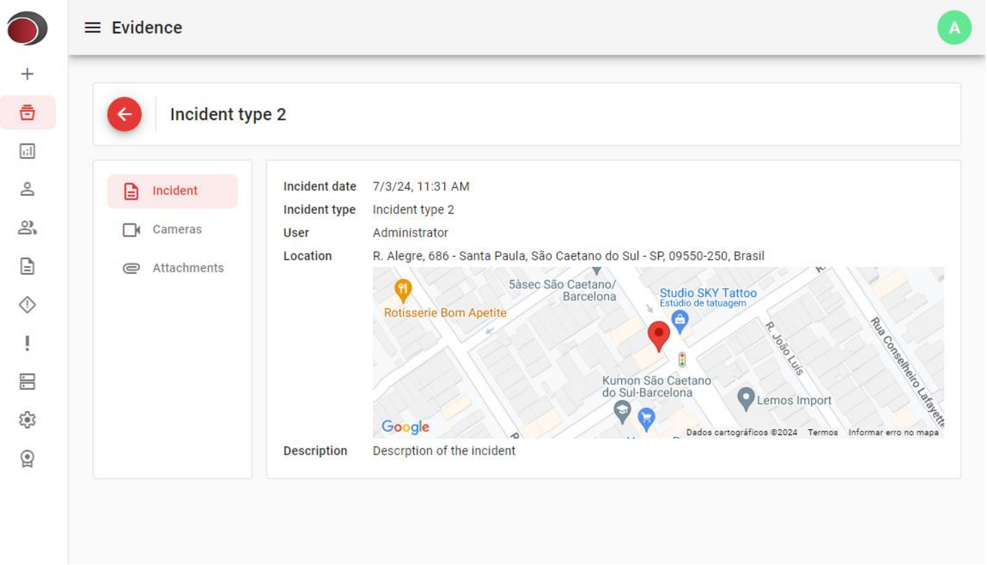
The incident form has some standard fields, which will always be displayed for completion regardless of whether there is a form associated with the type of incident to be selected:

- **Date and time:** Select the date and time of the incident. This date should represent the actual date of the incident. T
- **Conclusion date:** You can optionally assign the incident conclusion date during completion, if it is known. Otherwis
- **Incident type:** When selecting an item, the custom form fields associated with the incident type, if any, will be displ
- **Location:** Allows you to select a location previously registered in the Locations registry. To make this field available
- **Priority:** Priority of the incident. This field will be disabled if a priority is associated with the selected incident type. S
- **Incident description:** Description of the incident.
- **Additional notes:** An optional auxiliary text.

After filling in all the necessary fields, click the **Save** button. You will be redirected to the incident view page. See the t

15.3 Viewing incidents

On the incident view page you will be able to see the completed form, add cameras to attachments.



Incident type 2

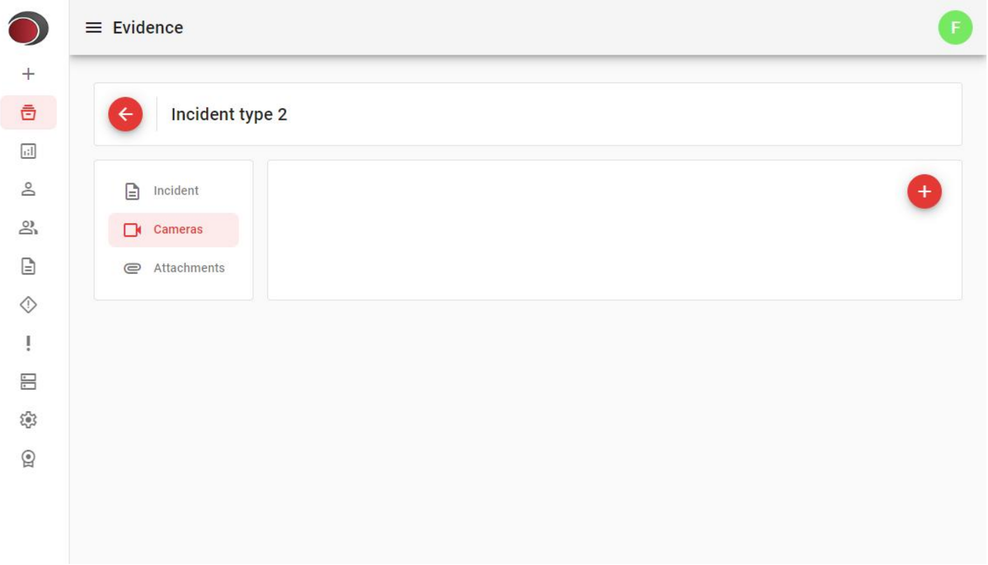
Incident date	7/3/24, 11:31 AM
Incident type	Incident type 2
User	Administrator
Location	R. Alegre, 686 - Santa Paula, São Caetano do Sul - SP, 09550-250, Brasil
Description	Descrption of the incident

15.3.1 Managing cameras

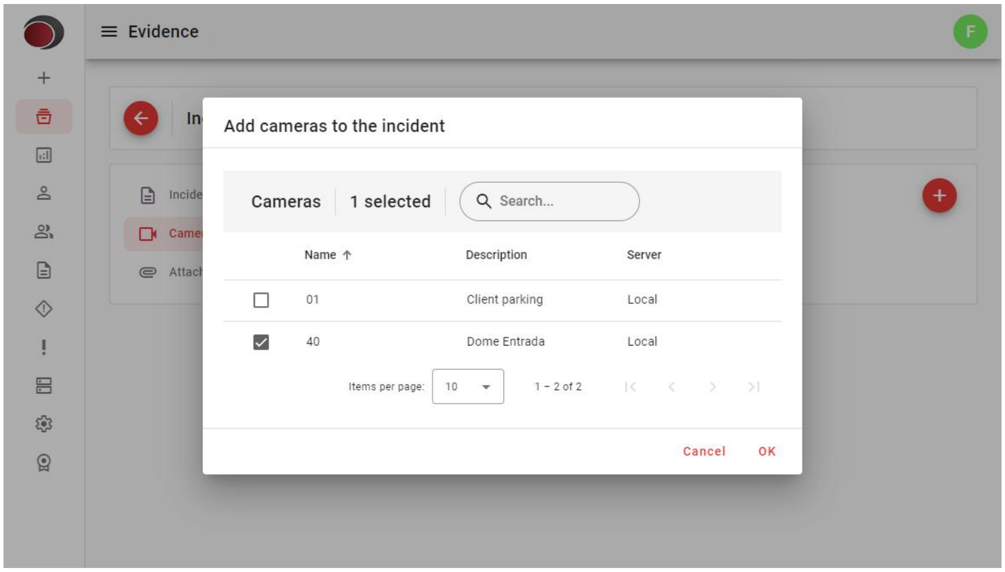
Videos of cameras can be imported from Digifort automatically by simply selecting the desired server and cameras.
The system will start a process of importing the camera video in parallel in .mp4 format. The user will be able to leave the page while the video is being imported.

15.3.1.1 Adding cameras to incidents

To add cameras to the incident, click the Cameras button in the side menu.



Once done, click the button ⊕ to add a camera. A screen listing cameras from all registered servers will be displayed. Servers must be previously registered. See the ser topic Digifort servers.

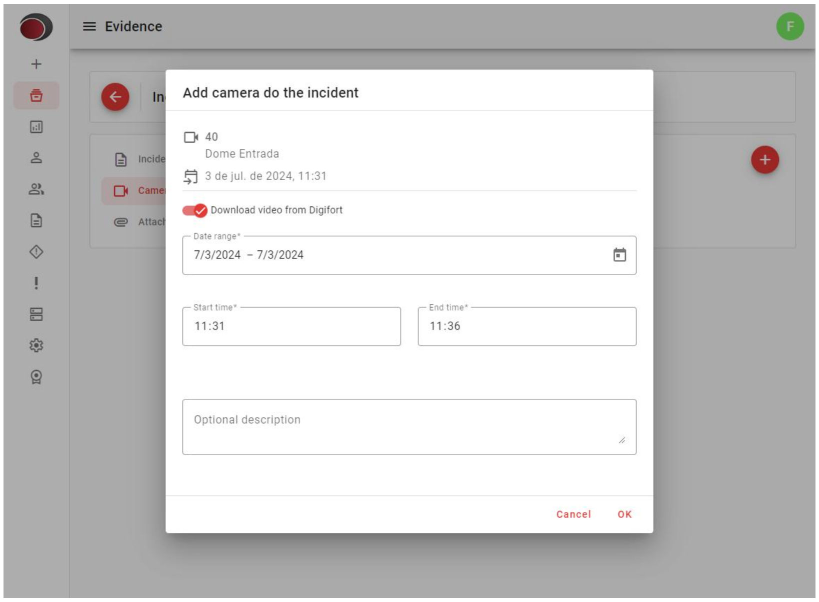


Add cameras to the incident

Cameras 1 selected

	Name ↑	Description	Server
□	01	Client parking	Local
☑	40	Dome Entrada	Local

Select the desired camera using the checkboxes and confirm. A second screen will appear to customize the video import:



Add camera do the incident

40
Dome Entrada
3 de jul. de 2024, 11:31

Download video from Digifort

Date range*: 7/3/2024 – 7/3/2024

Start time*: 11:31

End time*: 11:36

Optional description

Use the option **Download video from Digifort** to define whether the video should be imported or not. If this option is unchecked, the system will only add a link to the camera and the video will not be imported.

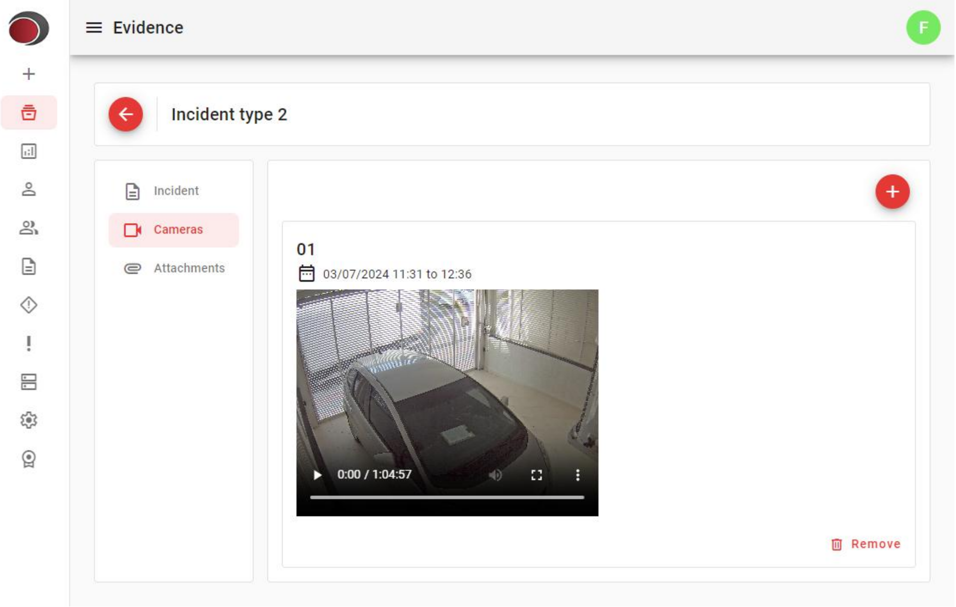
- **Date Range:** Select the date range of the video to be imported.
- **Start time:** Select the start time of the import.
- **End time:** Select the end time of the import.
- **Optional Description:** Add an optional description.

Important
The start date and time must be greater than or equal to the incident date.

Repeat this operation if you want to add more cameras.

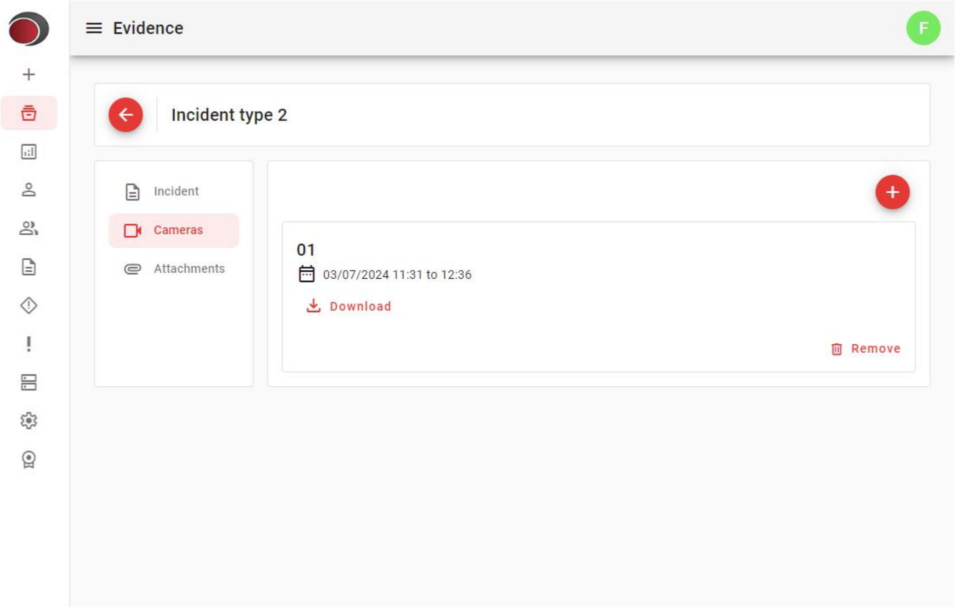
15.3.1.2 Viewing cameras

To view imported cameras, click the **Download** button. The file will be transferred and once complete, it will be played.

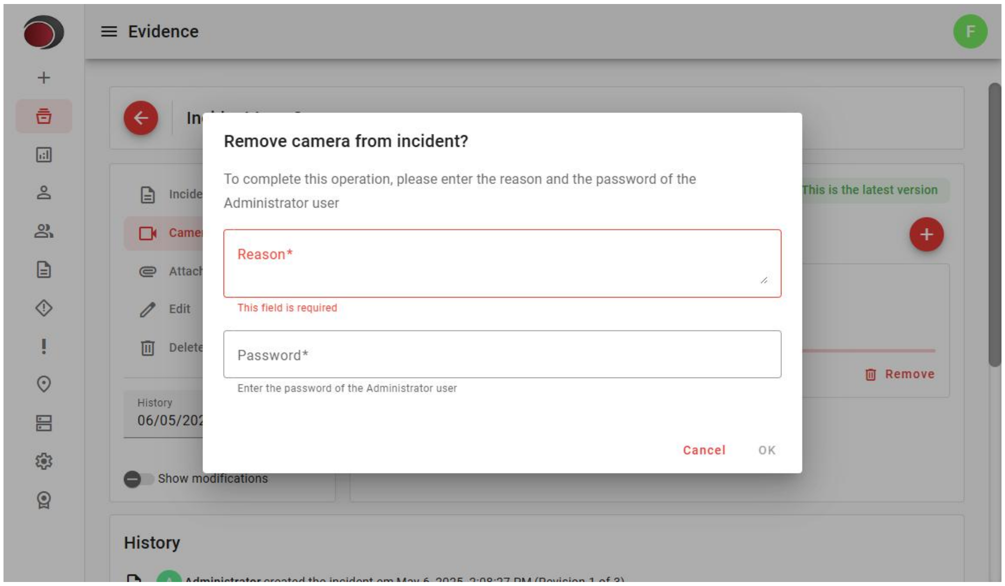


15.3.1.3 Deleting cameras

To remove incident cameras, click the **Delete** button.



The system will request the **reason and password** of the **Administrator** user. The reason will be stored and can be viewed in the incident modification history.


Evidence
F
Incide
Camer
Attach
Edit
Delete
History
06/05/202
Show modifications
This is the latest version
Remove
History
Administrator created the incident on May 6, 2025 2:08:27 PM (Revision 1 of 3)

Remove camera from incident?

To complete this operation, please enter the reason and the password of the Administrator user

Reason*

This field is required

Password*

Enter the password of the Administrator user

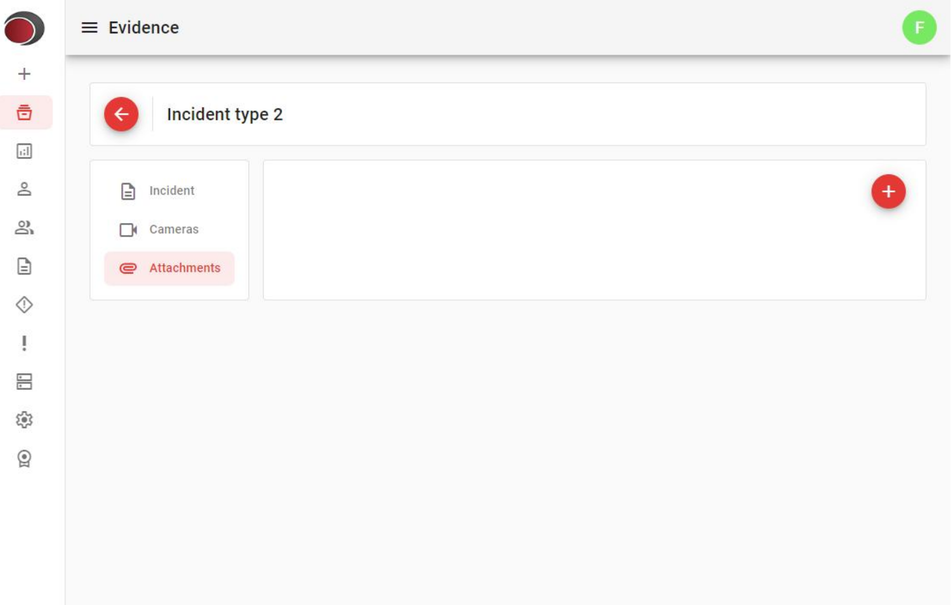
Cancel OK

15.3.2 Managing attachments

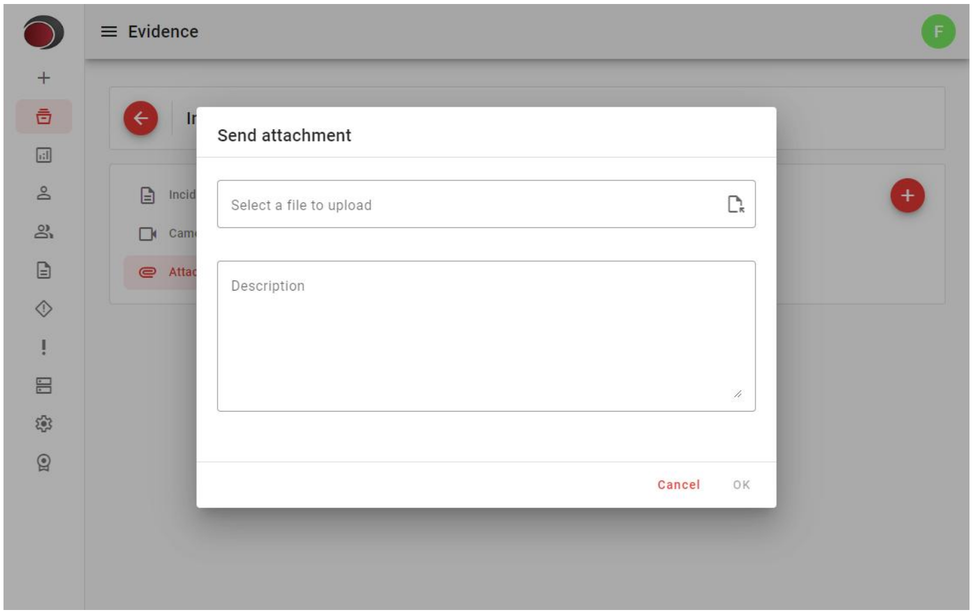
Attachments are files that can be added to incidents, such as documents, images and videos.

15.3.2.1 Adicionando anexos

To add attachments to the incident, click the **Attachments** button in the side menu.

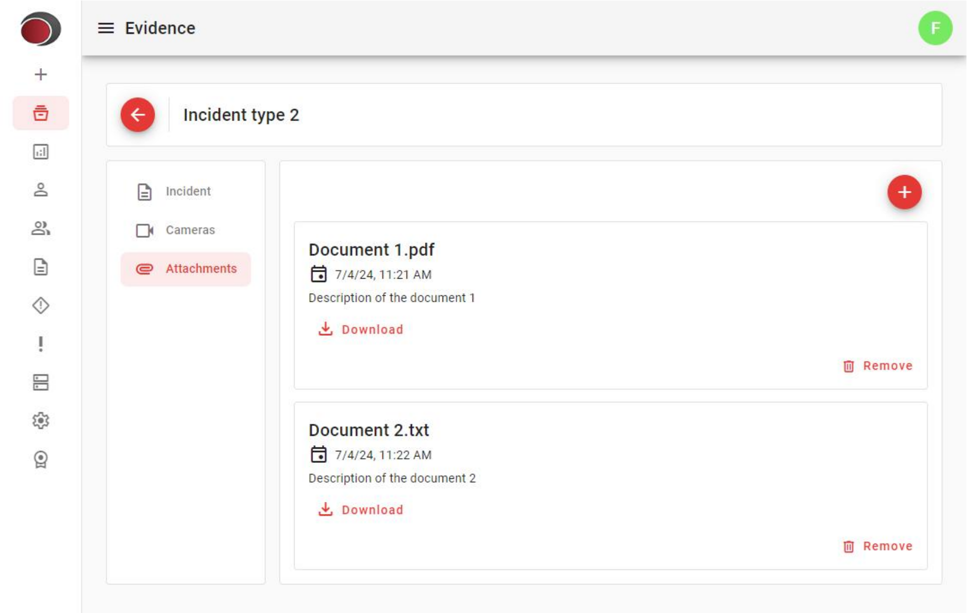


Once done, click the button. + . A screen will appear to select the file and add an optional description.



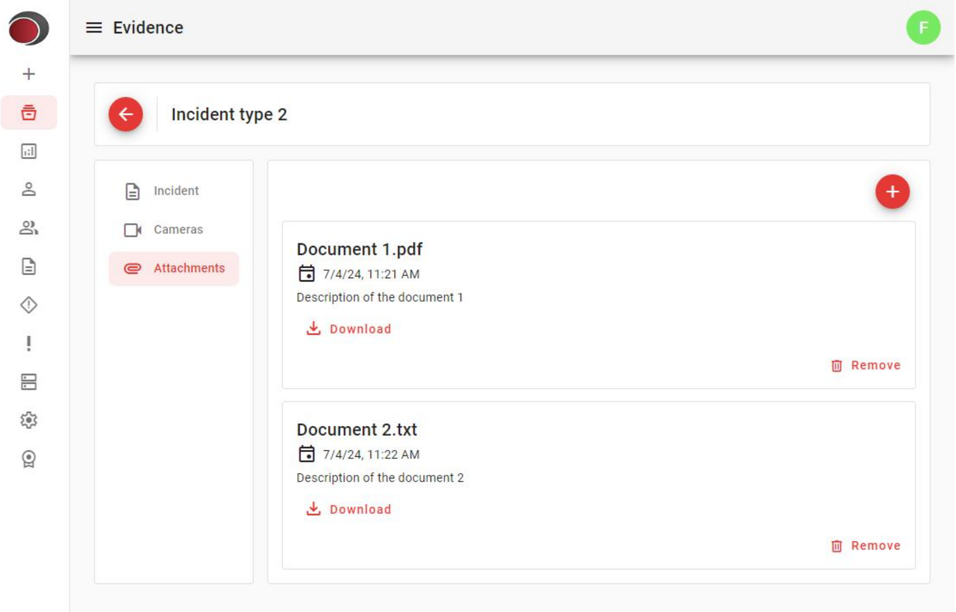
15.3.2.2 Downloading attachments

To download and view attachments, click the **Download** button.



15.3.2.3 Deleting attachments

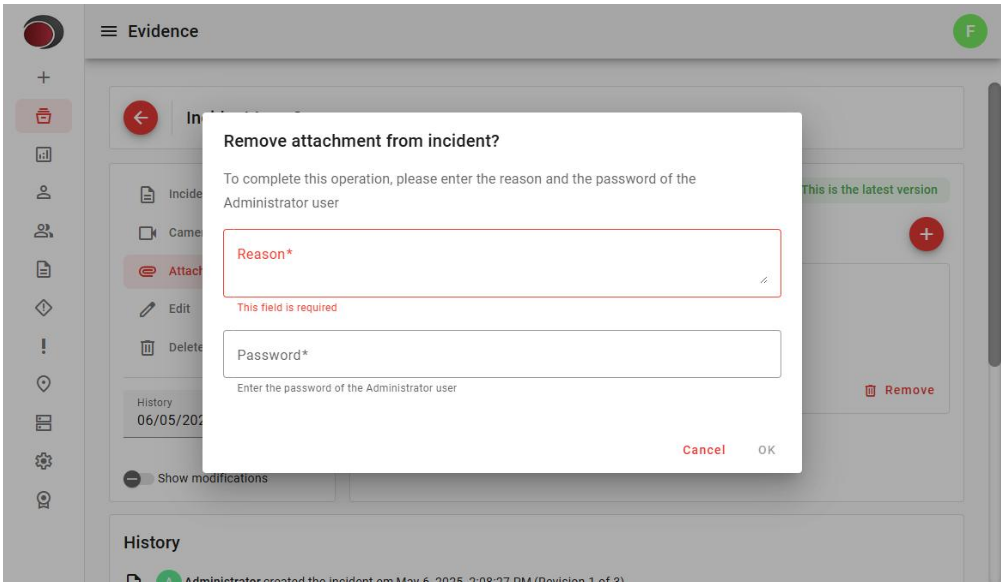
To remove incident attachments, click the **Delete** button.



Document 1.pdf
7/4/24, 11:21 AM
Description of the document 1

Document 2.txt
7/4/24, 11:22 AM
Description of the document 2

The system will request the **reason and password** of the **Administrator** user. The reason will be stored and can be viewed in the incident modification history.



Remove attachment from incident?

To complete this operation, please enter the reason and the password of the Administrator user

Reason*

This field is required

Password*

Enter the password of the Administrator user

Cancel OK

15.3.3 Editing incidents

To edit the incident, click the **Edit** button. The page for filling out the incident will be displayed with the currently valid values.
Change the necessary fields and click **Save**.

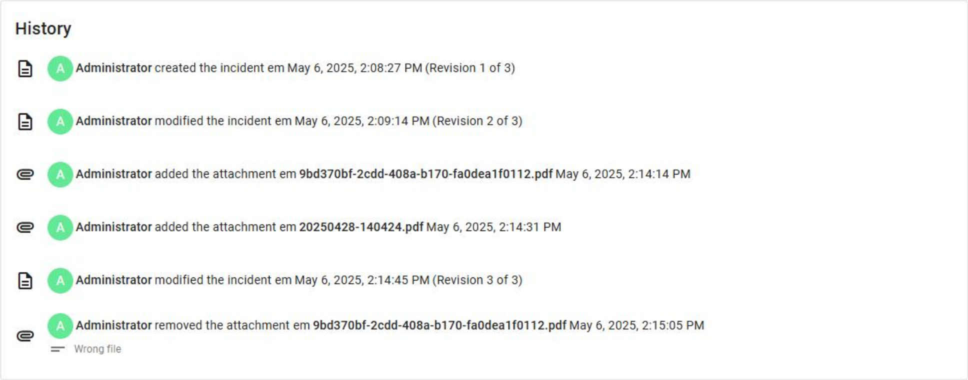
Dica

✓ The system will add a button like this ⮌ next to each field changed by the user. This button is intended to undo the edit, returning to the original value.

15.3.4 Viewing Incident Modification History

Just below the incident view pane, you'll see the **Change History**, an area that records all the changes made to the incident. This history contains the following information:

- **Date and time** of modification
- **User responsible** for the modification
- **Type of modification** performed: editing the incident form, adding or removing cameras and attachments



History

A **Administrator** created the incident em May 6, 2025, 2:08:27 PM (Revision 1 of 3)

A **Administrator** modified the incident em May 6, 2025, 2:09:14 PM (Revision 2 of 3)

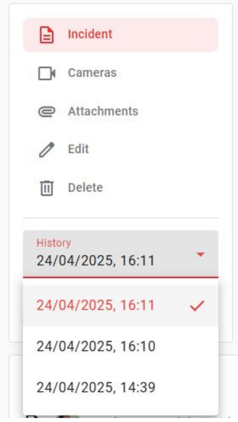
A **Administrator** added the attachment em **9bd370bf-2cdd-408a-b170-fa0dea1f0112.pdf** May 6, 2025, 2:14:14 PM

A **Administrator** added the attachment em **20250428-140424.pdf** May 6, 2025, 2:14:31 PM

A **Administrator** modified the incident em May 6, 2025, 2:14:45 PM (Revision 3 of 3)

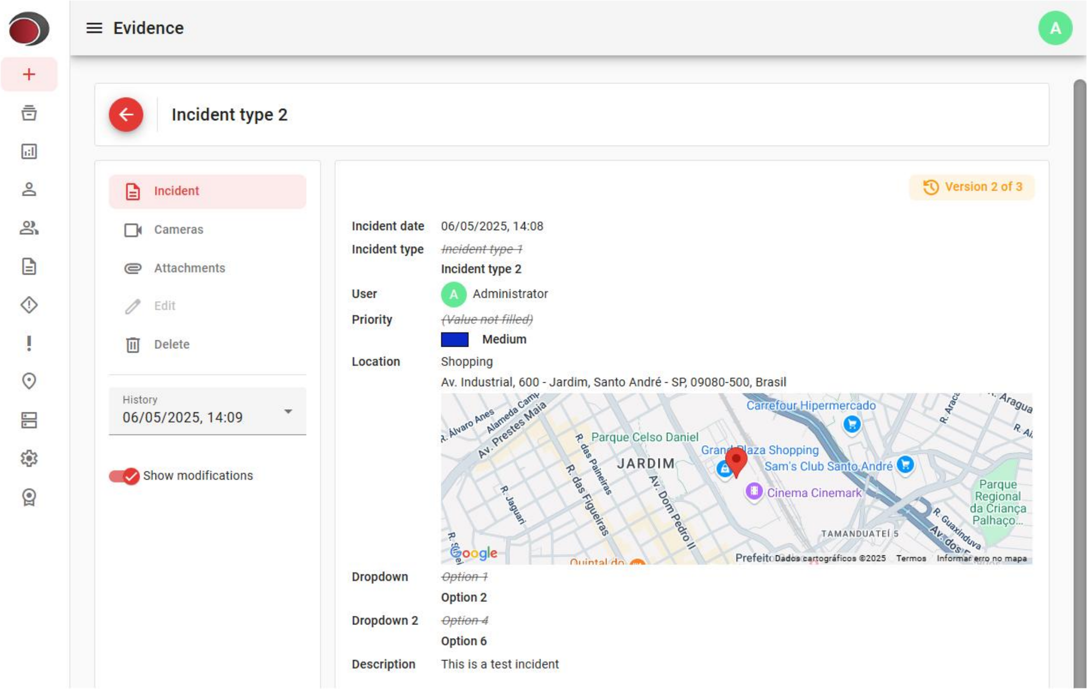
A **Administrator** removed the attachment em **9bd370bf-2cdd-408a-b170-fa0dea1f0112.pdf** May 6, 2025, 2:15:05 PM
Wrong file

On the left side of the incident actions menu, there is a **"History"** checkbox that displays a list of all revisions of the incident, identified by the modification date. When you select a revision, the system will load the corresponding view of the incident.



An informative badge like this Version 1 of 2 will be displayed in the upper right corner of the screen, indicating the revision number or whether the version being viewed is the most current.

Additionally, the **"Show modifications"** slider allows the user to compare the selected revision with the previous one, highlighting changes made to the form, cameras, or attachments.



Evidence

Incident type 2

- Incident
- Cameras
- Attachments
- Edit
- Delete

History
06/05/2025, 14:09

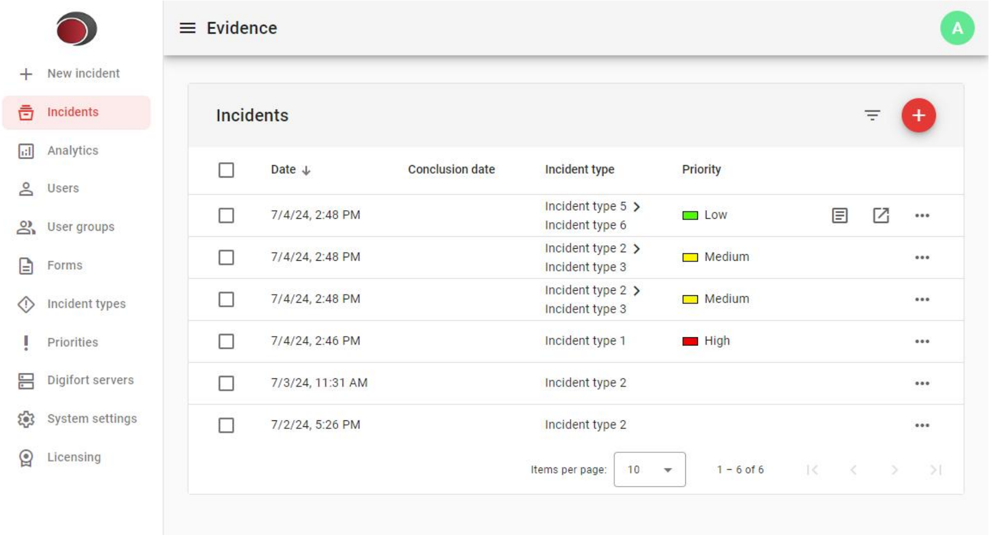
Show modifications

Version 2 of 3

Incident date	06/05/2025, 14:08
Incident type	~~Incident type 1~~ Incident type 2
User	A Administrator
Priority	~~(Value not filled)~~ Medium
Location	Shopping Av. Industrial, 600 - Jardim, Santo André - SP, 09080-500, Brasil
Dropdown	~~Option 1~~ Option 2
Dropdown 2	~~Option 4~~ Option 6
Description	This is a test incident

15.4 Searching for incidents

To search for incidents, click the **Incidents** button, located in the side menu.



Evidence

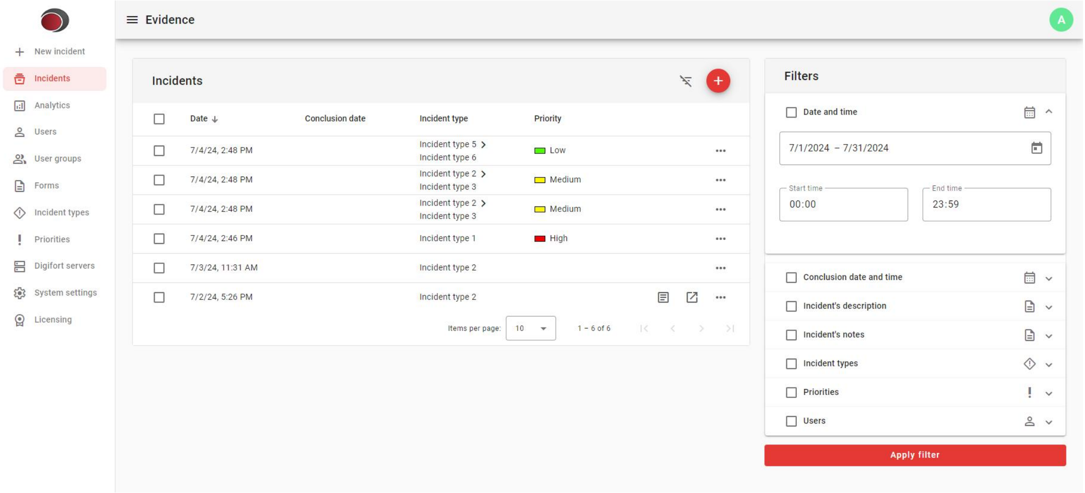
- New incident
- Incidents
- Analytics
- Users
- User groups
- Forms
- Incident types
- Priorities
- Digifort servers
- System settings
- Licensing

Incidents

☐	Date ↓	Conclusion date	Incident type	Priority
☐	7/4/24, 2:48 PM		Incident type 5 > Incident type 6	🟩 Low
☐	7/4/24, 2:48 PM		Incident type 2 > Incident type 3	🟨 Medium
☐	7/4/24, 2:48 PM		Incident type 2 > Incident type 3	🟨 Medium
☐	7/4/24, 2:46 PM		Incident type 1	🟥 High
☐	7/3/24, 11:31 AM		Incident type 2	
☐	7/2/24, 5:26 PM		Incident type 2	

Items per page: 10 1 – 6 of 6

This page lists all incidents created. You can filter the list of incidents by clicking the button . The filter menu will appear on the right. Select the desired filters and click the button **Apply filter.**



□	Date ↓	Conclusion date	Incident type	Priority	
□	7/4/24, 2:48 PM		Incident type 5 > Incident type 6	🟩 Low	•••
□	7/4/24, 2:48 PM		Incident type 2 > Incident type 3	🟨 Medium	•••
□	7/4/24, 2:48 PM		Incident type 2 > Incident type 3	🟨 Medium	•••
□	7/4/24, 2:46 PM		Incident type 1	🟥 High	•••
□	7/3/24, 11:31 AM		Incident type 2		•••
□	7/2/24, 5:26 PM		Incident type 2		•••

Items per page: 10 1 – 6 of 6

□ Date and time
7/1/2024 – 7/31/2024
Start time 00:00
End time 23:59

□ Conclusion date and time
□ Incident's description
□ Incident's notes
□ Incident types
□ Priorities
□ Users

Apply filter

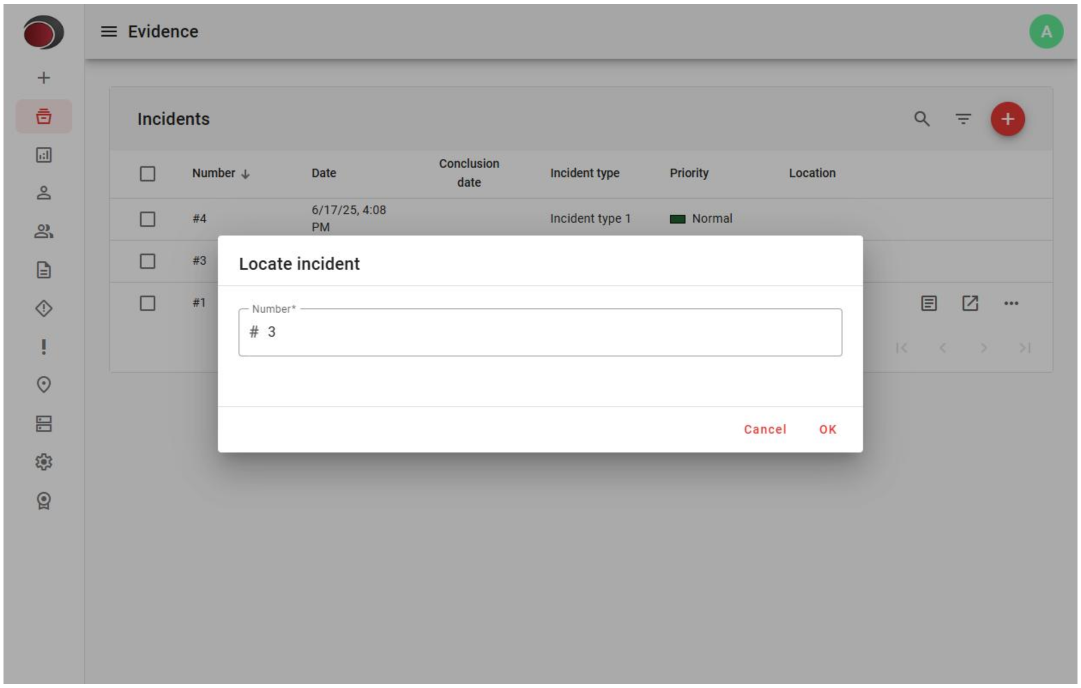
You can search using the fields from the forms filled out in the incidents. If there are any created forms, they will appear just below the filters menu. You can search across fields from multiple forms at the same time. To do this, simply fill in the desired fields and click the **Apply Filter** button.
To learn more about forms, see the Forms topic.

Important
Fields from the same form are combined with the **"AND"** condition. This means that if more than one field is filled in, the system will restrict the search results based on all the criteria entered. Different forms are combined with the **"OR"** condition, which broadens the results by including records that meet at least one of the criteria from any form used.

To view an incident, position the mouse over the desired item and click the button ☰, or the button ↗ to open in a new browser window. See the topic Viewing incidents.

15.4.1 Searching incidents by its number

To search for incidents by their number, click the button 🔍.



	Number	Date	Conclusion date	Incident type	Priority	Location
□	#4	6/17/25, 4:08 PM		Incident type 1	Normal	
□	#3					
□	#1					

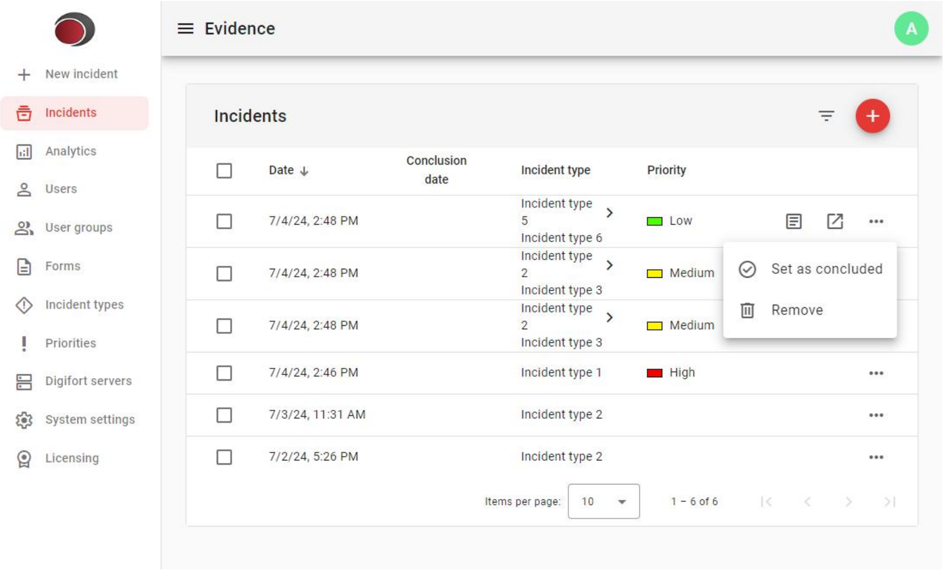
Locate incident

Number* # 3

Enter the incident number of the incident you want to locate and click OK. If the incident is located, the browser will redirect to the incident view page.

15.5 Marking incidents as concluded

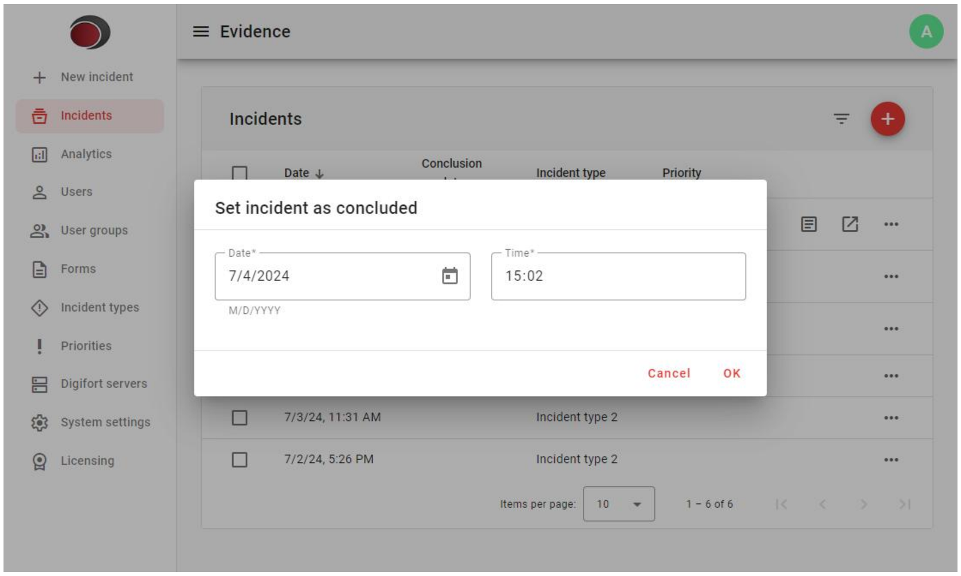
Incidents can be marked as concluded to help with traceability.
An incident can be created with its completion date already filled in, see the topic Registering incidents.
If the incident does not yet have a completion date, position the mouse over the desired item, click on the 3 dots icon and then **Mark as concluded**.



	Date	Conclusion date	Incident type	Priority
□	7/4/24, 2:48 PM		Incident type 5 Incident type 6	🟩 Low
□	7/4/24, 2:48 PM		Incident type 2 Incident type 3	🟨 Medium
□	7/4/24, 2:48 PM		Incident type 2 Incident type 3	🟨 Medium
□	7/4/24, 2:46 PM		Incident type 1	🟥 High
□	7/3/24, 11:31 AM		Incident type 2	
□	7/2/24, 5:26 PM		Incident type 2	

Items per page: 10 1 – 6 of 6

A window will open to set the date and time.



Set incident as concluded

Date*: 7/4/2024 (M/D/YYYY)

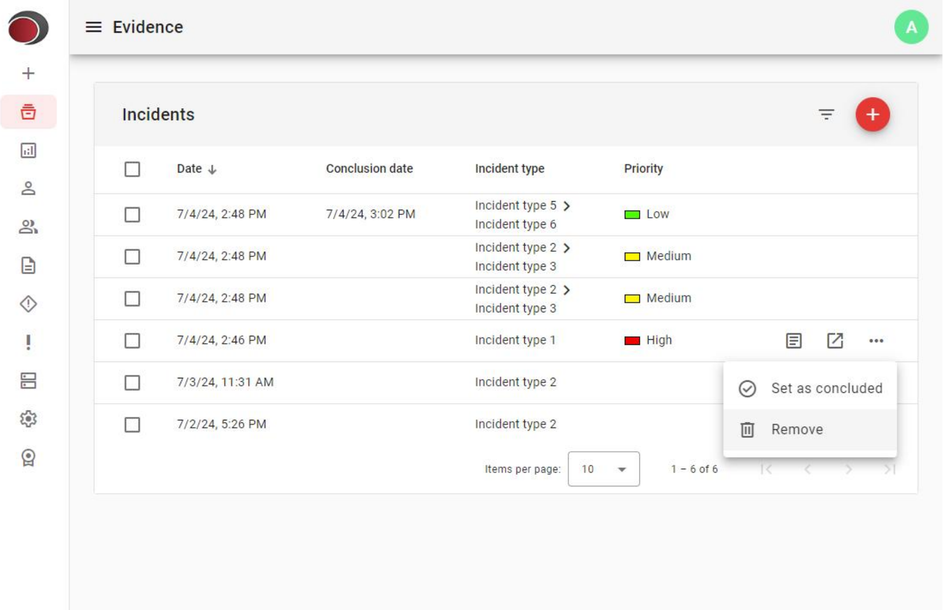
Time*: 15:02

□	Date ↓	Conclusion date	Incident type	Priority
□	7/3/24, 11:31 AM		Incident type 2	
□	7/2/24, 5:26 PM		Incident type 2	

Items per page: 10

15.6 Deleting incidents

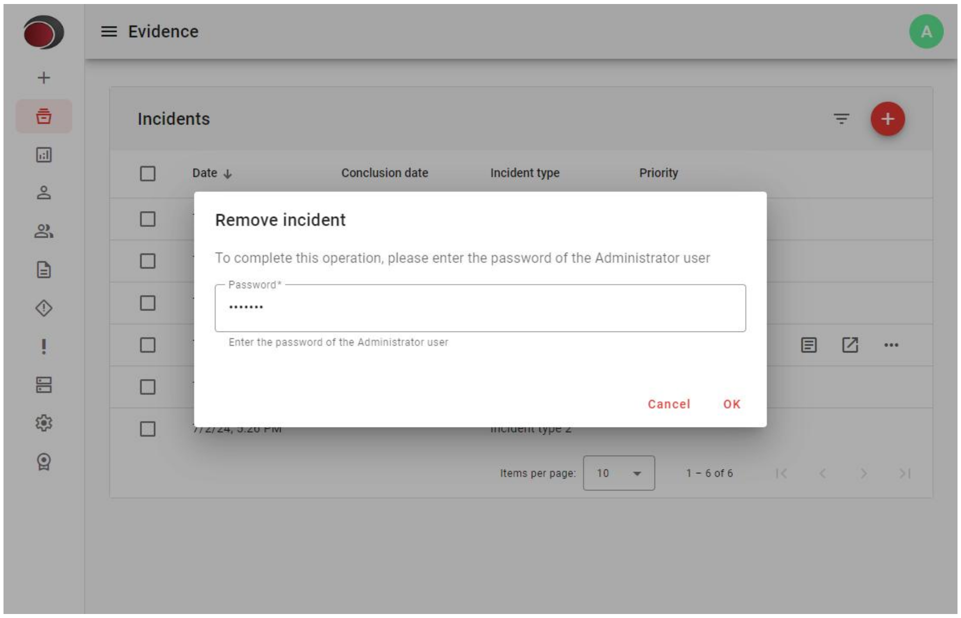
To delete incidents, position the mouse over the desired item, click the button ••• and then **Delete.**



□	Date ↓	Conclusion date	Incident type	Priority
□	7/4/24, 2:48 PM	7/4/24, 3:02 PM	Incident type 5 > Incident type 6	🟩 Low
□	7/4/24, 2:48 PM		Incident type 2 > Incident type 3	🟨 Medium
□	7/4/24, 2:48 PM		Incident type 2 > Incident type 3	🟨 Medium
□	7/4/24, 2:46 PM		Incident type 1	🟥 High
□	7/3/24, 11:31 AM		Incident type 2	
□	7/2/24, 5:26 PM		Incident type 2	

Items per page: 10

The system will request the **Administrator** user password.



Remove incident

To complete this operation, please enter the password of the Administrator user

Password*: •••••••

Enter the password of the Administrator user

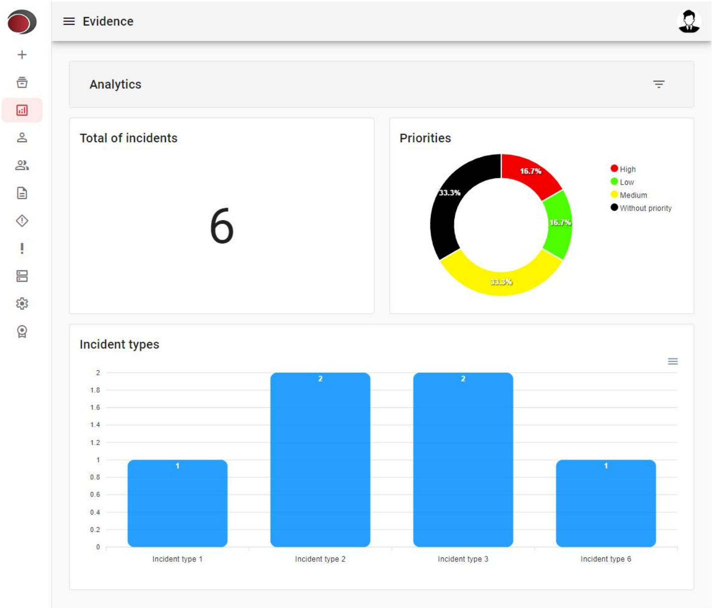
Chapter XVI

16 Analytics

The Analytics module is an essential tool for visualizing and analyzing incident data clearly and effectively. This module provides detailed statistical charts that help users understand trends, identify patterns, and make informed decisions based on the information collected.

16.1 Accessing the analytics module

In the side menu, click on the **Analytics** option to access the module.



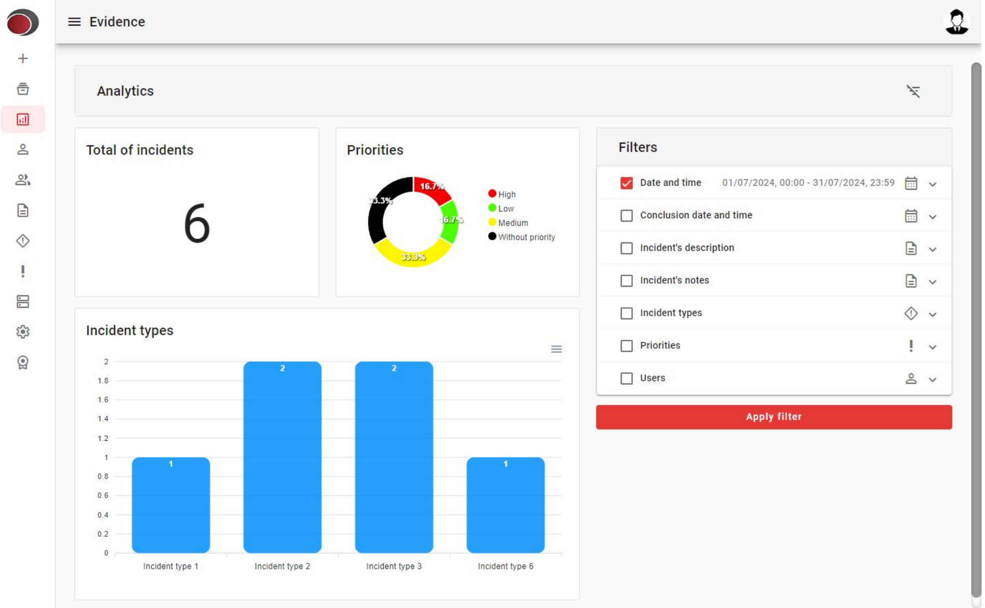
This dashboard is divided into 3 areas:

- **Total incidents:** Displays the total number of incidents created
- **Priorities:** Displays a pie chart with the percentage of incidents for each priority.
- **Incident types:** Displays a bar graph with the number of incidents of each type.

16.2 Filtering incidents

Various filters can be applied to personalize data display, allowing for more accurate and relevant analysis according to needs. This includes the ability to filter by dates, types of incidents, priorities, status, among other criteria.

To open the filters panel, click the button ☰ .



Filters

☑ Date and time 01/07/2024, 00:00 - 31/07/2024, 23:59

☐ Conclusion date and time

☐ Incident's description

☐ Incident's notes

☐ Incident types

☐ Priorities

☐ Users

Apply filter

You can filter using the fields from the forms filled out in the incidents. If there are any created forms, they will appear just below the filters menu. You can search across fields from multiple forms at the same time. To do this, simply fill in the desired fields and click the **Apply Filter** button.
To learn more about forms, see the Forms topic.

Important
Fields from the same form are combined with the **"AND"** condition. This means that if more than one field is filled in, the system will restrict the search results based on all the criteria entered. Different forms are combined with the **"OR"** condition, which broadens the results by including records that meet at least one of the criteria from any form used.

Select the desired filters and click the **Apply filter** button.