

Evidence 2.0.0
User manual
Rev. A

Index

Part I Welcome to the Digifort 2.0.0 manual	7
1 Screenshots.....	7
2 Who is this manual for.....	7
Part II Installing the system	9
Part III Managing services	13
1 Running the service manager.....	13
Part IV Accessing the system for the first time	15
1 First configuration steps.....	15
Part V System settings	17
1 Accessing system settings.....	17
2 Configuring the repository.....	17
3 Server settings.....	17
4 Configuring the SMTP server.....	18
5 Map settings.....	18
Part VI Licensing	20
1 Accessing the licensing module.....	20
2 Adding licenses.....	20
3 Removing licenses.....	21
4 Viewing licensed users.....	22
Part VII Digifort servers	24
1 Accessing the Digifort servers module.....	24
2 Adding Digifort servers.....	24
3 Modifying Digifort servers.....	25
4 Deleting Digifort servers.....	26
Part VIII Users	29
1 User types.....	29
Native user	29
Imported user	29
Differences between native and imported users	29
2 Accessing the users module.....	29
3 Adding users.....	30
Setting the user's first password	31

4	Modifying users.....	31
5	Deleting users.....	32
6	Managing groups.....	33
	Adicionando grupos à usuários	33
	Removing groups from users	34
7	Setting the profile picture.....	34
8	Modifying the user's password.....	34
9	Suspending users.....	35
10	Importing users.....	35
11	User authentication process.....	37
	Authentication of native users	37
	Authentication of imported users	37
12	Resetting the user's password.....	37
	Resetting the user's password on the login page	38
	Resetting the user's password from the users register	40
	Resetting user password in account management	40
Part IX User groups		42
1	Accessing the user groups module.....	42
2	Adding user groups.....	42
3	Modifying user groups.....	43
4	Deleting user groups.....	43
5	Managing users.....	44
	Adding users to groups	45
	Removing users from groups	45
6	Configuring access rights.....	46
Part X Managing the account of the logged user		48
1	Modifying the user's data.....	48
2	Modifying the user's settings.....	48
3	Modifying the profile picture.....	49
4	Resetting the password.....	50
Part XI Priorities		52
1	Accessing the priorities module.....	52
2	Adding priorities.....	52
3	Modifying priorities.....	53
4	Deleting priorities.....	53
5	Ordering priorities.....	54
Part XII Forms		57
1	Accessing the forms module.....	57
2	Adding forms.....	57

3	Modifying forms.....	58
4	Deleting forms.....	59
5	Custom fields.....	60
	Custom field types	60
	Short text	60
	Paragraph.....	61
	Number	62
	Examples	62
	Date	62
	Time	63
	Date and time.....	63
	Checkboxes.....	64
	Multiple choice.....	65
	Dropdown.....	66
	URL	67
	Location	67
	Filling in the location field.....	68
	Viewing a location field.....	69
	Adding custom fields	69
	Modifying custom fields	70
	Deleting custom fields	71

Part XIII Incident types 73

1	Accessing the incident types module.....	73
2	Adding incident types.....	74
3	Modifying incident types.....	75
4	Deleting incident types.....	75

Part XIV Incidents 78

1	Registering incidents.....	78
2	Searching for incidents.....	78
	Marking incidents as concluded	79
	Deleting incidents	80
3	Viewing incidents.....	81
	Managing cameras	82
	Adding cameras to incidents.....	82
	Viewing cameras.....	84
	Deleting cameras.....	84
	Managing attachments	85
	Adicionando anexos.....	85
	Downloading attachments.....	86
	Deleting attachments.....	86

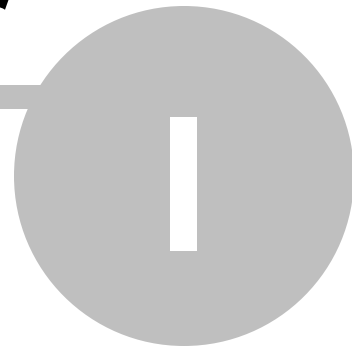
Part XV Analytics 89

1	Accessing the analytics module.....	89
2	Filtering incidents.....	89

Index

0

Chapter



1 Welcome to the Digifort 2.0.0 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 2.0.0. This manual is constantly updated and does not describe the features of the Beta or Dev versions of the system.

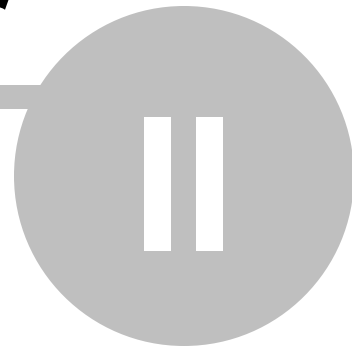
1.1 Screenshots

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

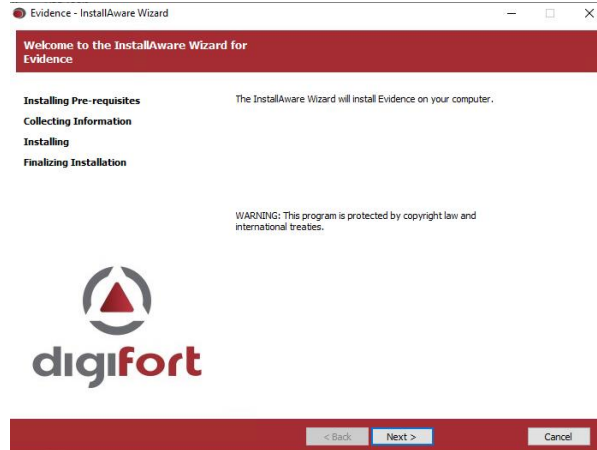
This manual is intended for system administrators and operators.

Chapter

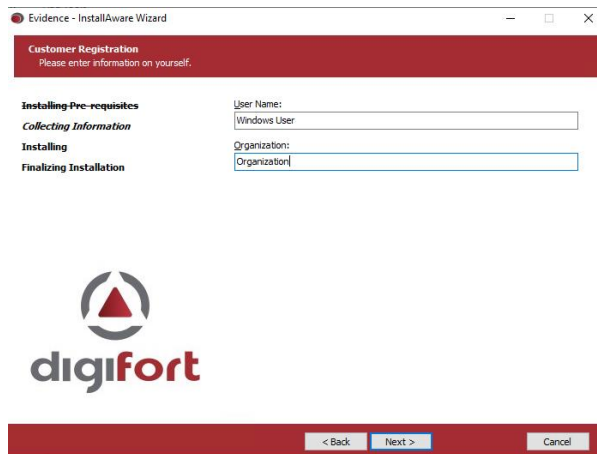


2 Installing the system

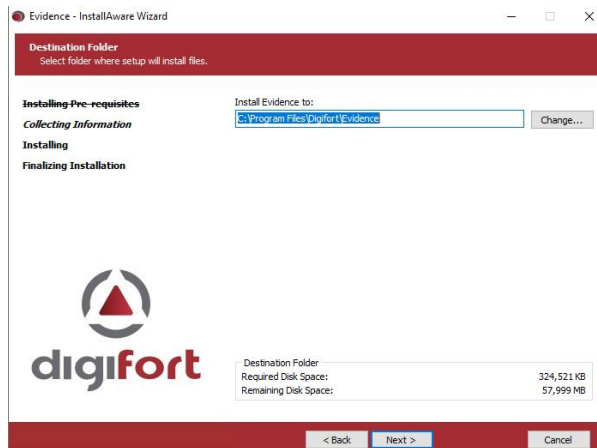
After running the installation program file, follow the steps below to install the system.



Click **Next**.



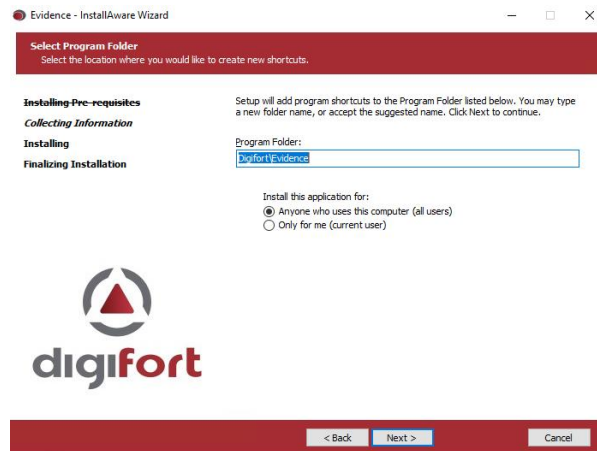
Enter your registration information and click **Next**.



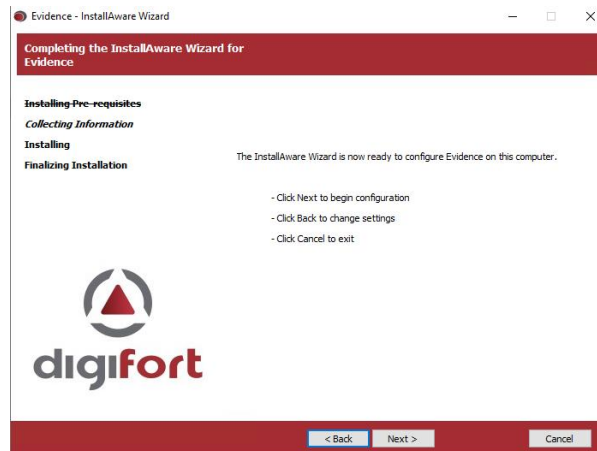
Select the location where the files will be installed and click **Next**.

Important

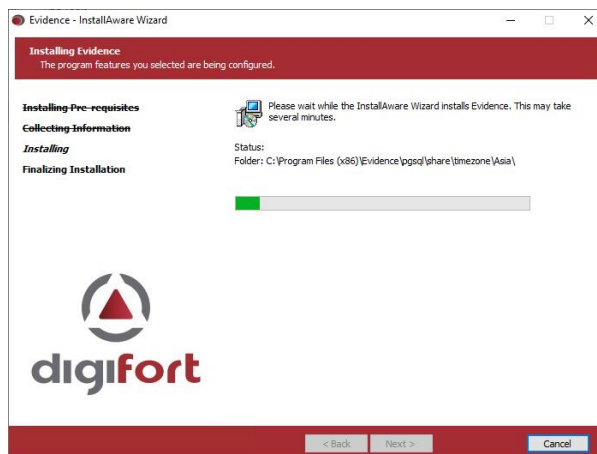
- ! In addition to the files necessary for the system to function, a database instance will be initialized in this folder. The database is responsible for storing all system data.



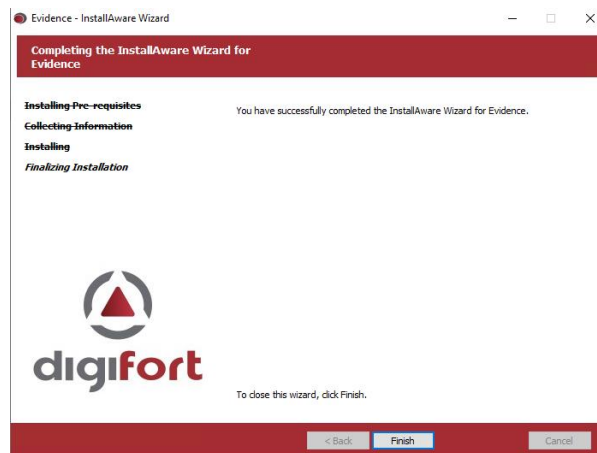
Select the Windows start menu folder where the shortcuts will be created and click **Next**.



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

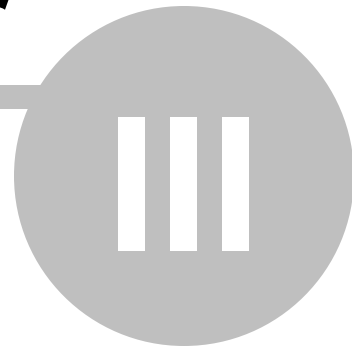


Wait for the installation process.



Click **Finish** to complete the installation.

Chapter



3 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.

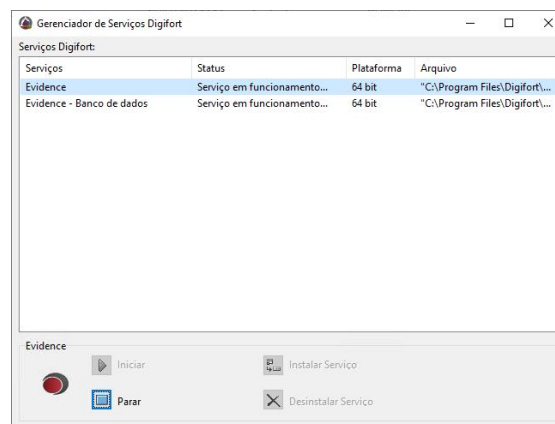
The Service Manager is the software responsible for controlling its execution, showing information about its operating state and providing service installation and startup controls.

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.

3.1 Running the service manager

To run the service manager, locate its icon on your Desktop or in the start menu and run it.



The service manager provides the following functionality:

- **Services Digifort:** Displays the list of available services that can be managed.
- **Start:** Starts the selected service. Only available if the service is installed and stopped.
- **Stop:** Stops the selected service. Only available if the service is installed and started.
- **Install Service:** Installs the selected service. Only available if the service is uninstalled.
- **Uninstall Service:** Uninstalls the selected service. Only available if the service is installed and stopped.

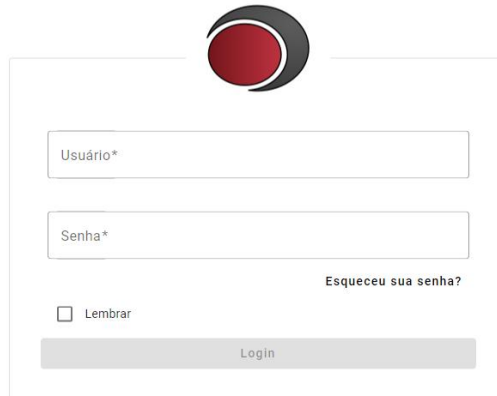
Chapter



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

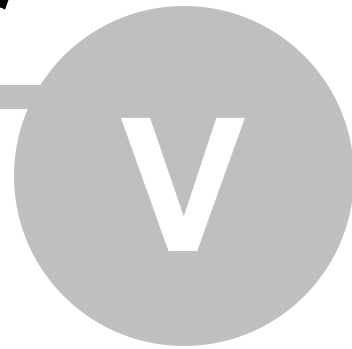
- ! For security reasons, we recommend changing the admin user password upon first access.

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

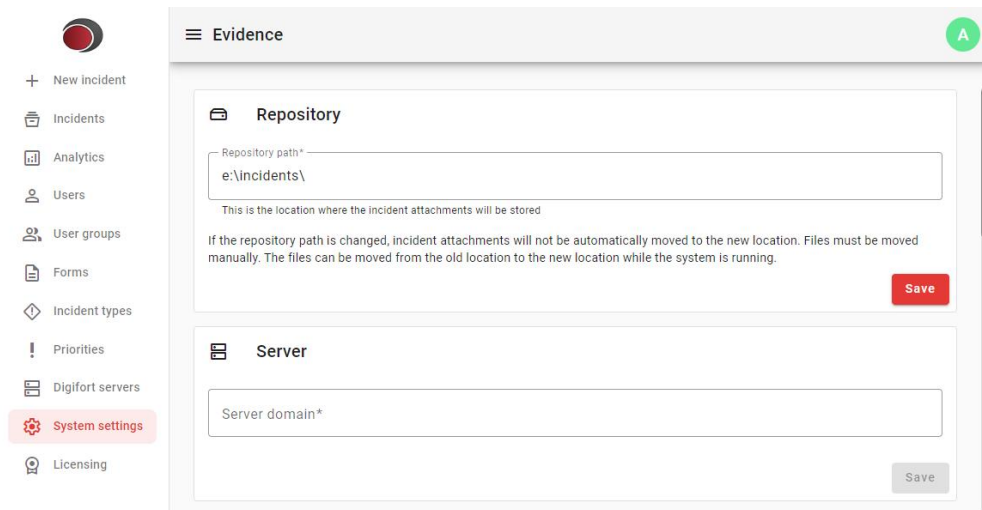


5 System settings

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.

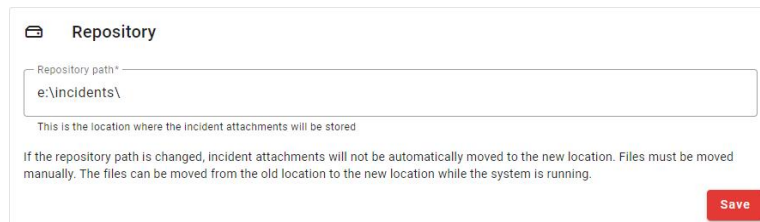


5.2 Configuring the repository

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.



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>. Points to the server's IP address.

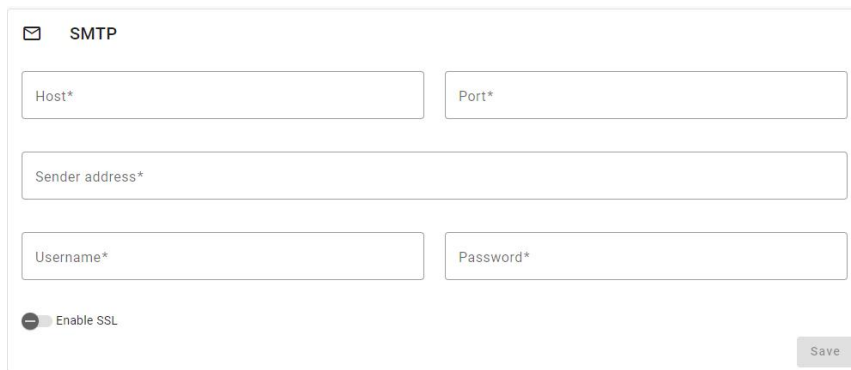
- <https://evidence-server>. Points to the server name.
- <https://www.company-name>. Points to the FQDN of the server where the system is hosted.



The screenshot shows a configuration form titled "Server". It contains a single text input field labeled "Server domain*" and a "Save" button in the bottom right corner.

5.4 Configuring the SMTP server

SMTP configuration, used by the system to send emails.




The screenshot shows an "SMTP" configuration form. It includes several input fields: "Host*", "Port*", "Sender address*", "Username*", and "Password*". There is also a toggle switch for "Enable SSL" and a "Save" button in the bottom right corner.

- **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. Search the Internet for how to generate your Google API key.



The screenshot shows a "Map" configuration form. It features a text input field labeled "Google Maps API key" with the placeholder text "Enter your API Key" and a red "Save" button in the bottom right corner.

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.

The screenshot shows the Evidence 2.0.0 interface. On the left is a sidebar menu with 'Licensing' highlighted. The main content area is titled 'Evidence 2.0.0' and contains the following sections:

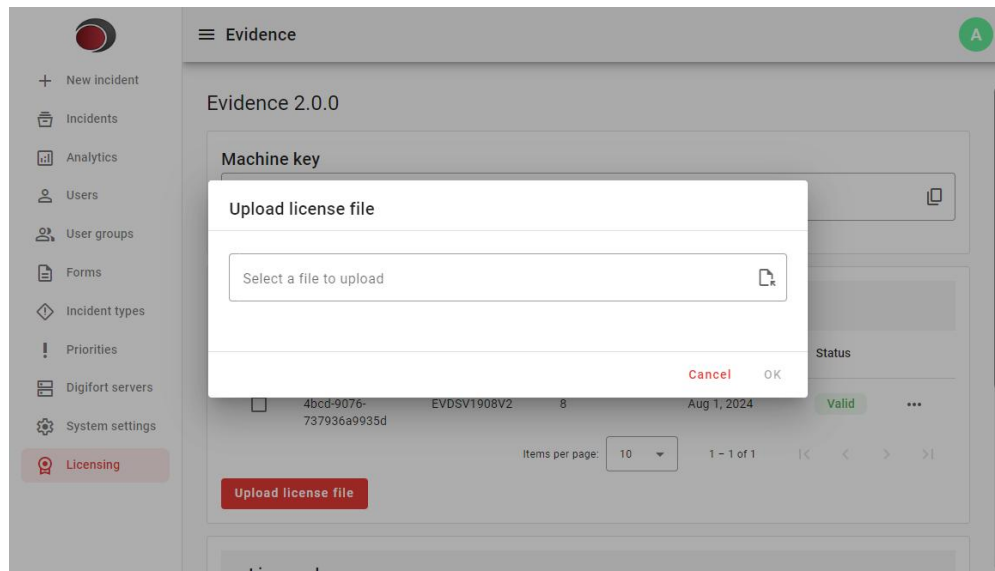
- Machine key:** A text box containing the unique ID: D9C0-EVD-1A54A86-04928*CBCF96/2CCF-MKEY-4748D0.
- Installed Licenses - 8 licensed users:** A table with columns: id, Part number, Licensed users, Expiration date, and Status. One license is listed with a status of 'Valid'.
- Licensed users:** A list of users: Administrator, User 1, and User 2.

Machine key

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

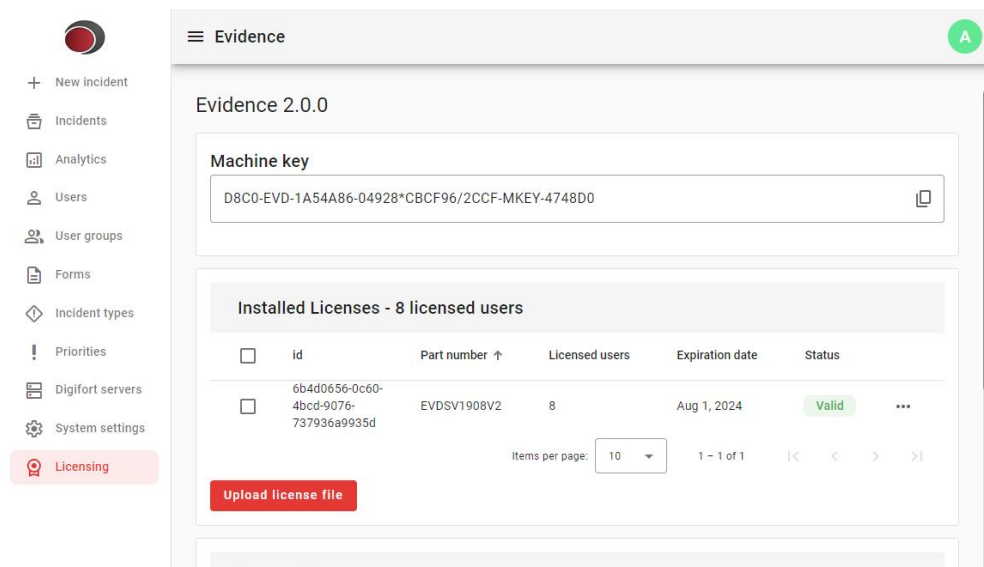
6.2 Adding licenses

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



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.



- **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**.

6.3 Removing licenses

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

The screenshot shows the Evidence 2.0.0 interface. On the left is a navigation menu with options: New incident, Incidents, Analytics, Users, User groups, Forms, Incident types, Priorities, Digifort servers, System settings, and Licensing (highlighted in red). The main content area is titled "Evidence 2.0.0" and contains a "Machine key" field with the value "D8C0-EVD-1A54A86-04928*CBCF96/2CCF-MKEY-4748D0". Below this is a section titled "Installed Licenses - 8 licensed users" which contains a table with the following data:

<input type="checkbox"/>	id	Part number ↑	Licensed users	Expiration date	Status	
<input type="checkbox"/>	6b4d0656-0c60-4bcd-9076-737936a9935d	EVDSV1908V2	8	Aug 1, 2024	Valid	...

Below the table is a red "Upload license file" button and a "Delete" button. The interface also shows "Items per page: 10" and "1 - 1 of 1".

6.4 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](#).

The screenshot shows the Evidence 2.0.0 interface with the "Licensed users" section expanded. The navigation menu is the same as in the previous screenshot. The main content area shows the "Licensed users" section with a table listing the users:

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

Below the table is a "Delete" button and "Items per page: 10" and "1 - 3 of 3".

Chapter



VII

7 Digifort servers

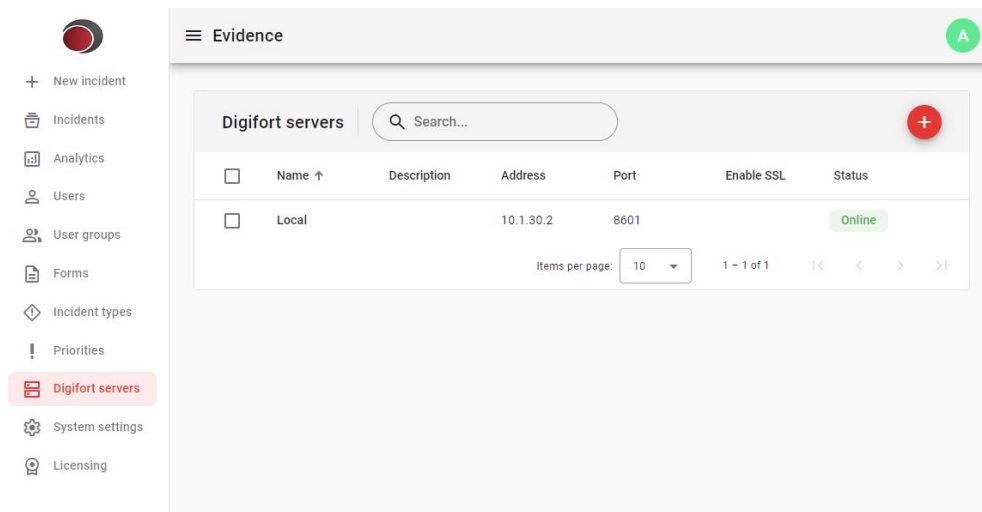
Evidence can be integrated with Digifort to add some functionality to both systems:

- 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**.

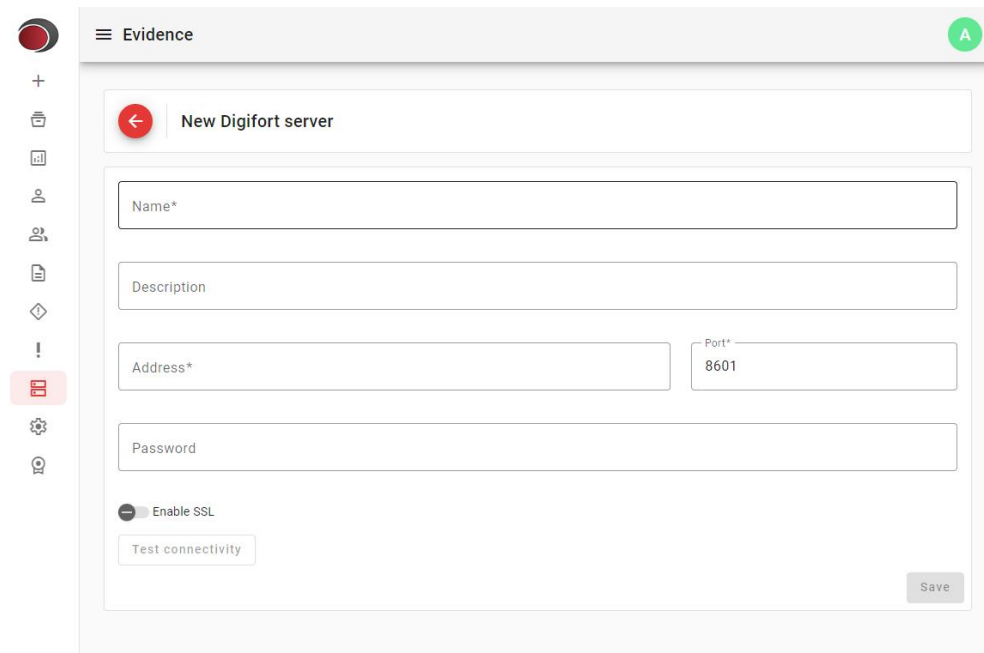


The screenshot displays the Evidence application interface. On the left is a side menu with various options, including 'Digifort servers' which is highlighted in red. The main content area shows the 'Digifort servers' module with a search bar and a table of servers. The table has columns for Name, Description, Address, Port, Enable SSL, and Status. One server named 'Local' is listed with address '10.1.30.2' and port '8601', and its status is 'Online'. A red '+' button is visible in the top right corner of the table area.

<input type="checkbox"/>	Name ↑	Description	Address	Port	Enable SSL	Status
<input type="checkbox"/>	Local		10.1.30.2	8601		Online

7.2 Adding Digifort servers

To add servers, click the button .



The screenshot shows a web interface titled 'Evidence' with a sidebar on the left containing various icons. The main content area is titled 'New Digifort server' and contains the following fields and controls:

- Name***: A text input field.
- Description**: A text input field.
- Address***: A text input field.
- Port***: A text input field with the value '8601' pre-filled.
- Password**: A text input field.
- Enable SSL**: A toggle switch currently turned off.
- Test connectivity**: A button.
- Save**: A button in the bottom right corner.

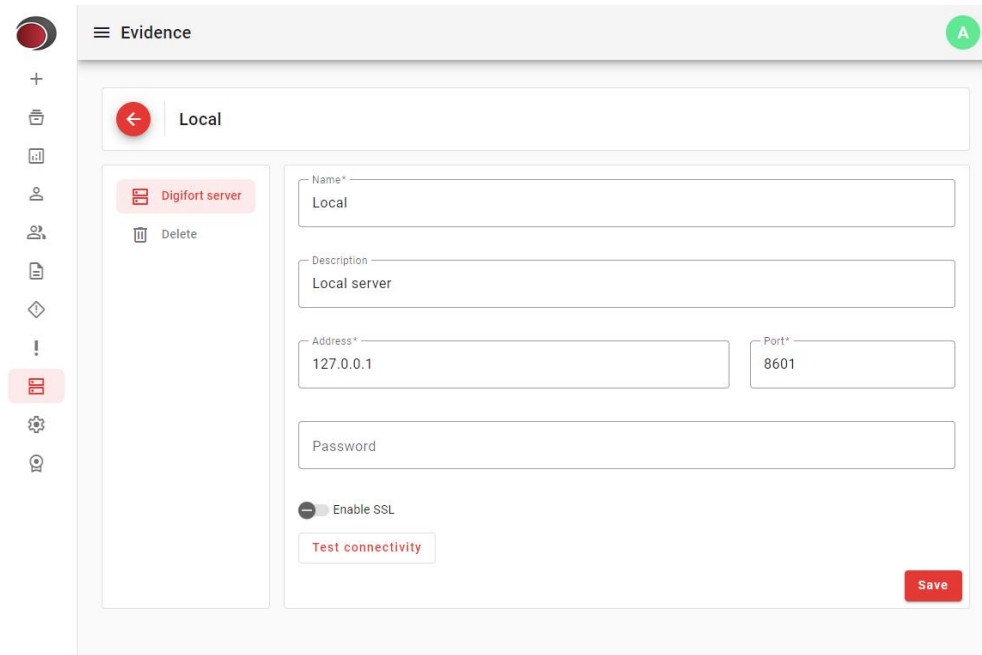
- **Name:** Server name.
- **Description:** An optional description.
- **Address:** IP address, computer name, or FQDN of the server.
- **Port:** TCP port
- **Password:** Password of the Digifort **admin** user.
- **Enable SSL:** Enables communication using SSL.

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.



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:

The screenshot shows the 'Evidence' application interface. On the left is a vertical sidebar with various icons. The main content area is titled 'Evidence' and contains a sub-section for 'Local' server configuration. This section includes a 'Name*' field with the value 'Local', a 'Description' field with 'Local server', an 'Address*' field with '127.0.0.1', and a 'Port*' field with '8601'. There is also a 'Password' field, an 'Enable SSL' toggle switch, and a 'Test connectivity' button. A 'Save' button is located at the bottom right of the form. On the left side of the form, there are two buttons: 'Digifort server' and 'Delete'.

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  .

The screenshot shows the 'Evidence' application interface displaying a list of 'Digifort servers'. The list has a search bar and a '+ Add' button. Two items are selected, indicated by checkmarks in the first column. The table has columns for Name, Description, Address, Port, Enable SSL, and Status. The 'Local' server is 'Online' and the 'Remote' server is 'Offline'. At the bottom, there is a pagination control showing 'Items per page: 10' and '1 - 2 of 2'.

<input checked="" type="checkbox"/>	Name ↑	Description	Address	Port	Enable SSL	Status
<input checked="" type="checkbox"/>	Local	Local server	127.0.0.1	8601		Online
<input checked="" type="checkbox"/>	Remote		189.24.24.56	8601		Offline

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

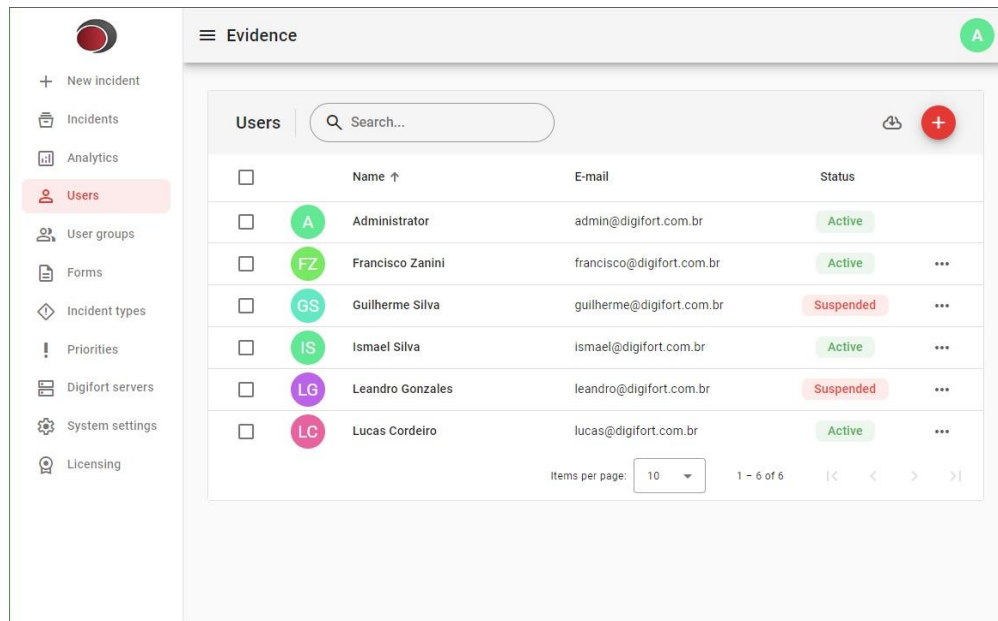
Imported users can use all system functions, including the functionality to import videos from Digifort cameras to incidents. See the topic [Managing cameras](#).

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.



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.

The screenshot shows a user management interface for 'Ismael Silva' (email: ismael@digifort.com.br). The interface includes a sidebar menu with options: Personal data, Groups, Profile picture, Reset password, Suspend user, and Delete. The main form contains input fields for First name (Ismael), Last name (Silva), Username (ismael), and E-mail (ismael@digifort.com.br), along with a red 'Save' button.

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](#).

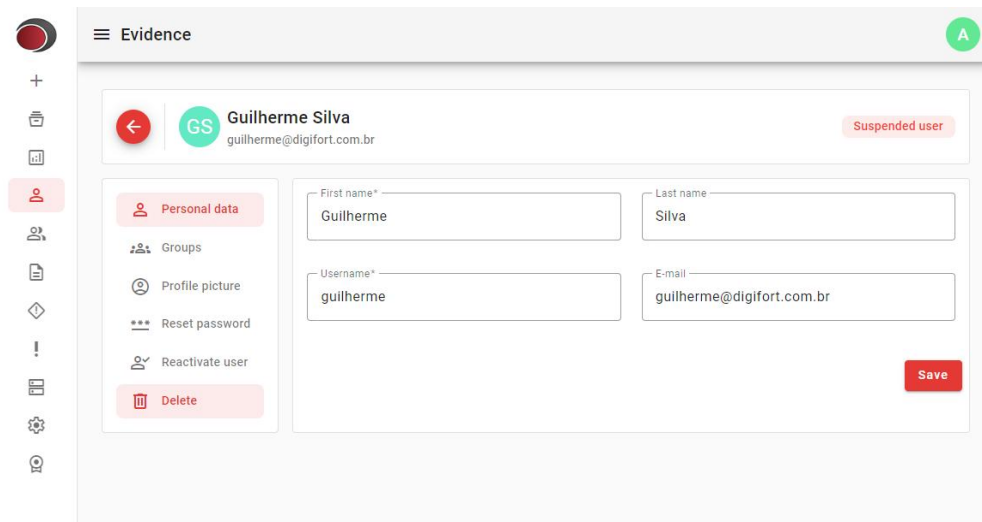
- **Delete:** Removes the user from the system. See the topic [Deleting users](#).

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.

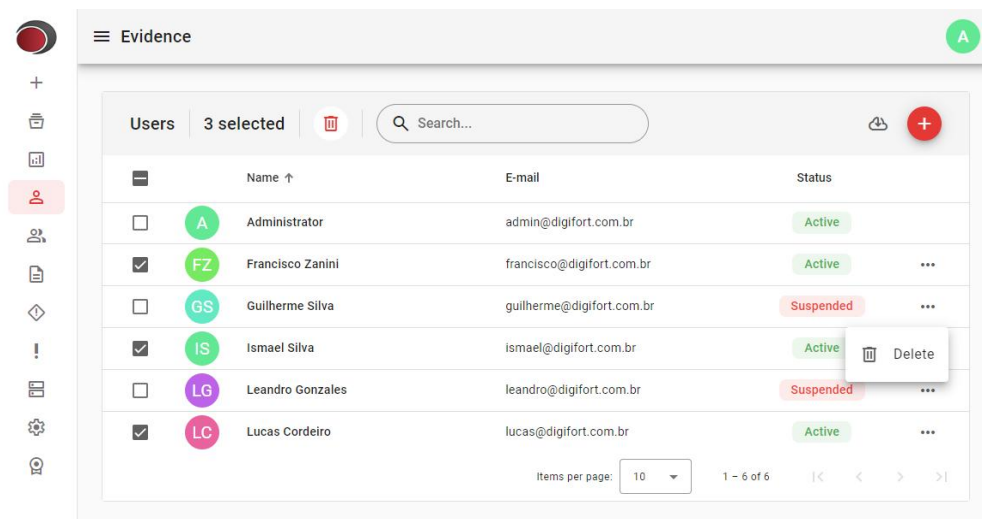
Although the user's data is preserved when removing it, a user with the same data may be created in the future.

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



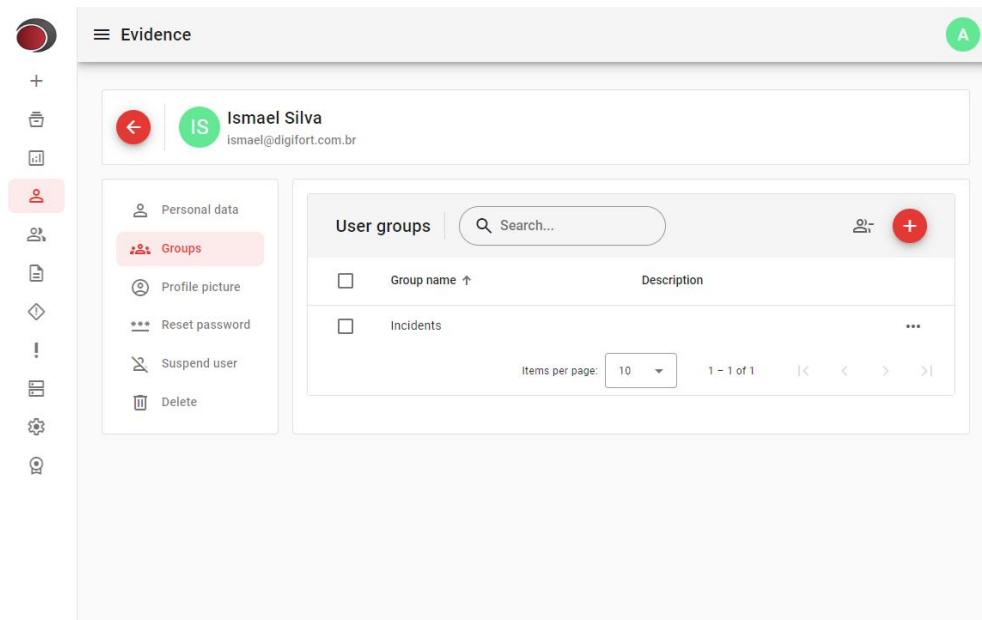
Another way to exclude users is through user registration. Next to each item there is a three-dot button with the option to remove it.

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  .



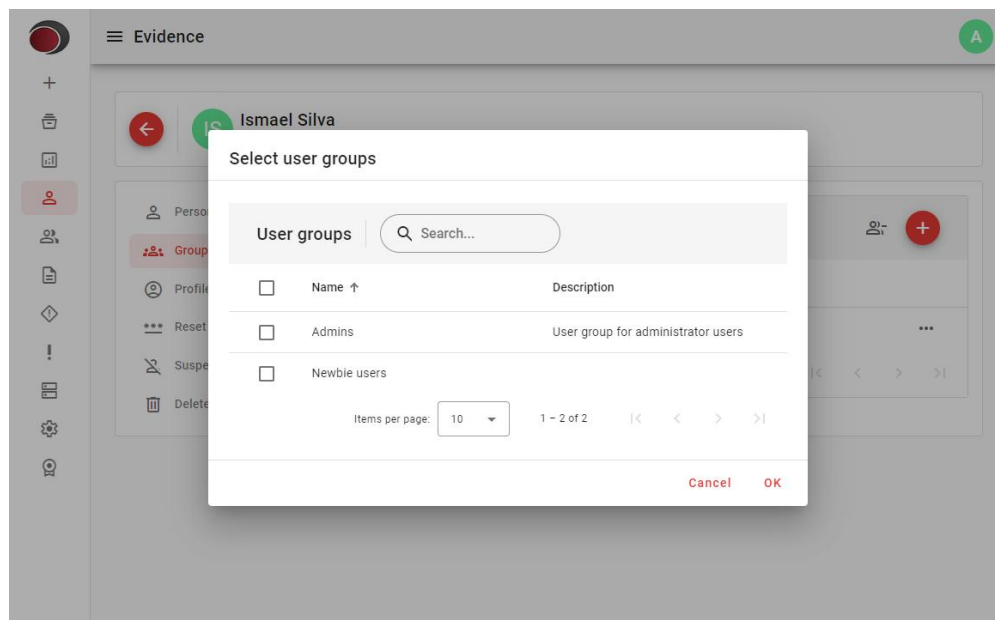
8.6 Managing groups

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.




8.6.1 Adicionando grupos à usuários

To add groups to the user, click the button .



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

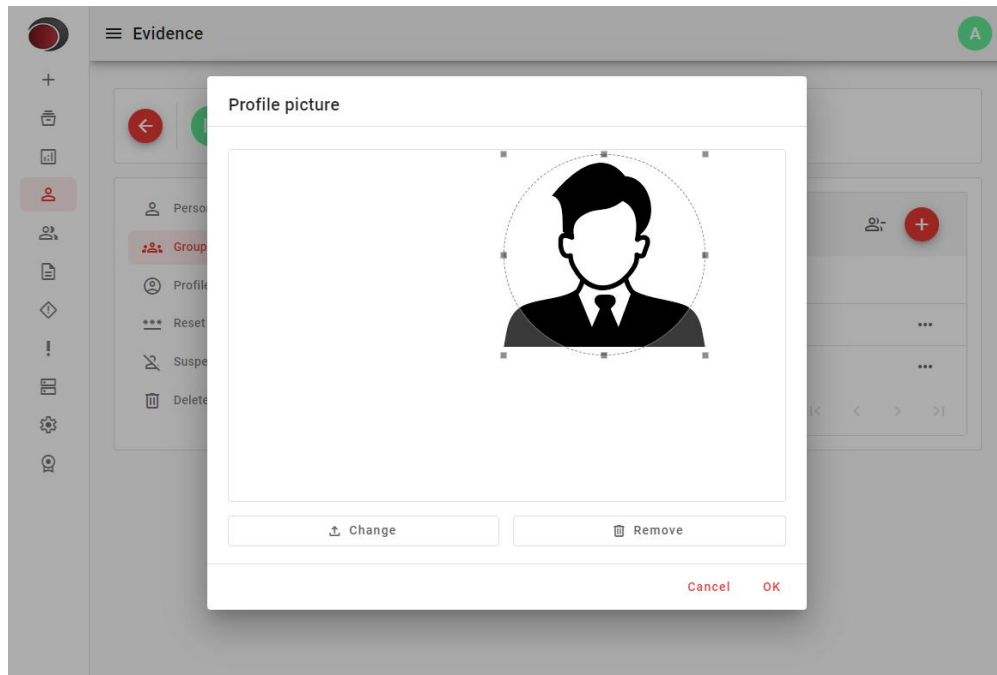
8.6.2 Removing groups from users

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.

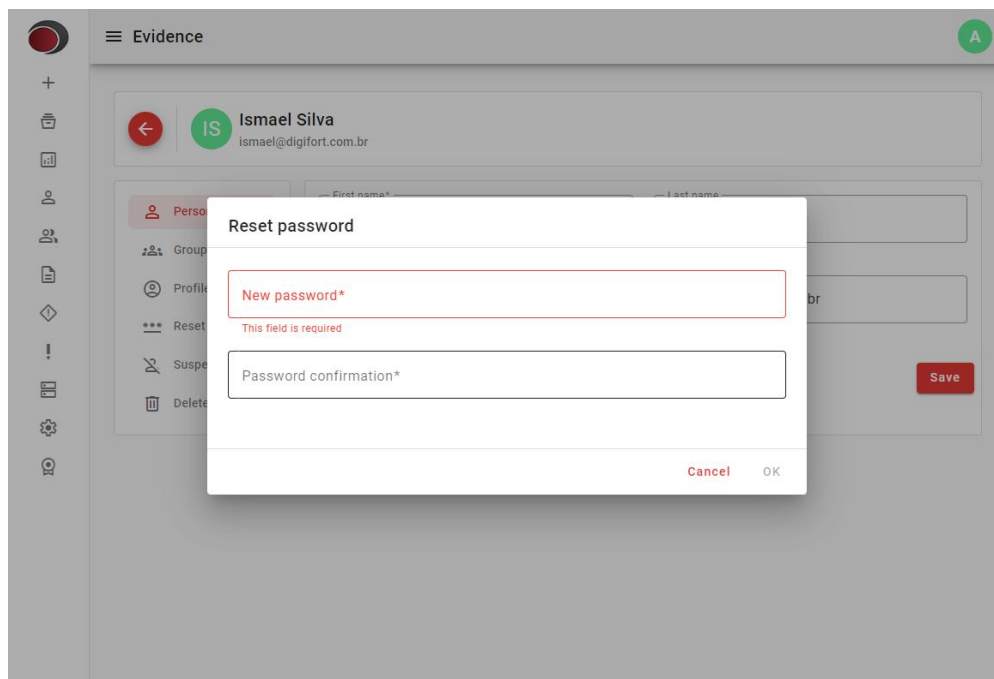
To set your profile picture, click the **Profile picture** button.



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.



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

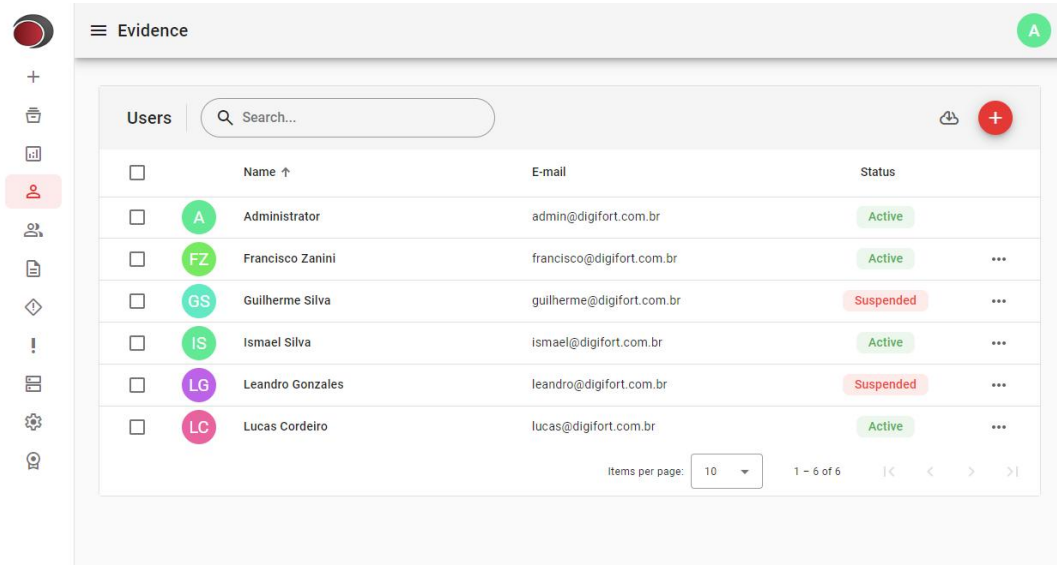
To suspend a user, click the **Suspend user** button.
A suspended user will have their access blocked until they are reactivated again.

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 .



The screenshot shows the 'Evidence' application interface. On the left is a sidebar with various icons, including a user icon. The main content area is titled 'Evidence' and contains a section for 'Users'. At the top of this section is a search bar labeled 'Search...'. Below the search bar is a table with the following columns: 'Name ↑', 'E-mail', and 'Status'. The table lists six users:

Name ↑	E-mail	Status
Administrator	admin@digifort.com.br	Active
Francisco Zanini	francisco@digifort.com.br	Active
Guilherme Silva	guilherme@digifort.com.br	Suspended
Ismael Silva	ismael@digifort.com.br	Active
Leandro Gonzales	leandro@digifort.com.br	Suspended
Lucas Cordeiro	lucas@digifort.com.br	Active

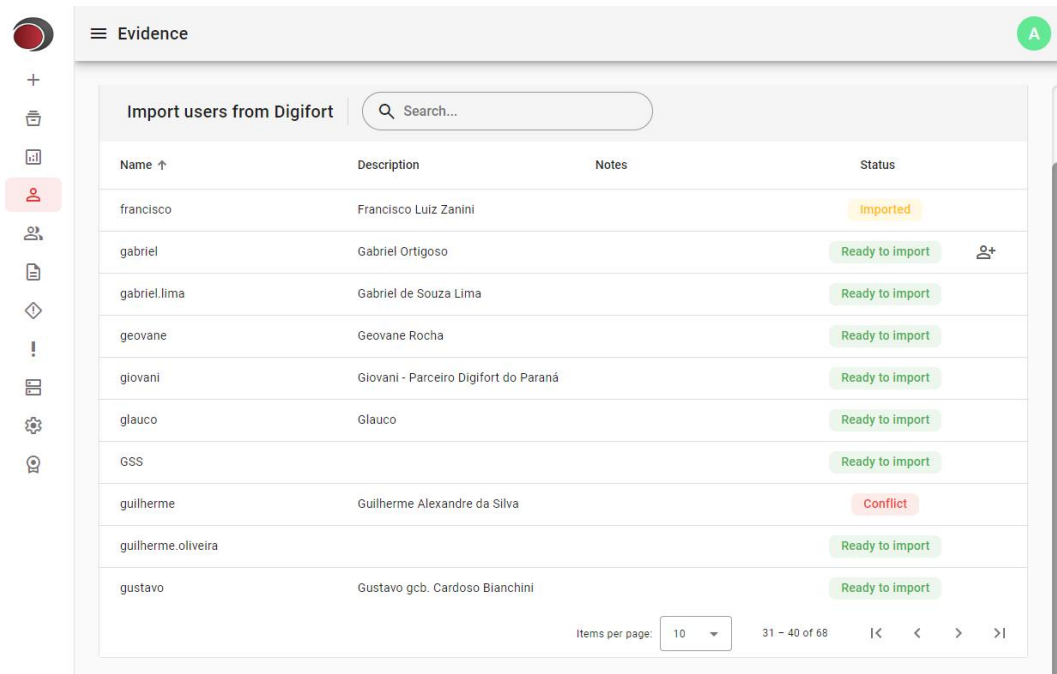
At the bottom of the table, there is a pagination control showing 'Items per page: 10' and '1 - 6 of 6'.

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.



The screenshot shows the 'Evidence' application interface. On the left is a sidebar with various icons, including a user icon. The main content area is titled 'Evidence' and contains a section for 'Import users from Digifort'. At the top of this section is a search bar labeled 'Search...'. Below the search bar is a table with the following columns: 'Name ↑', 'Description', 'Notes', and 'Status'. The table lists ten 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

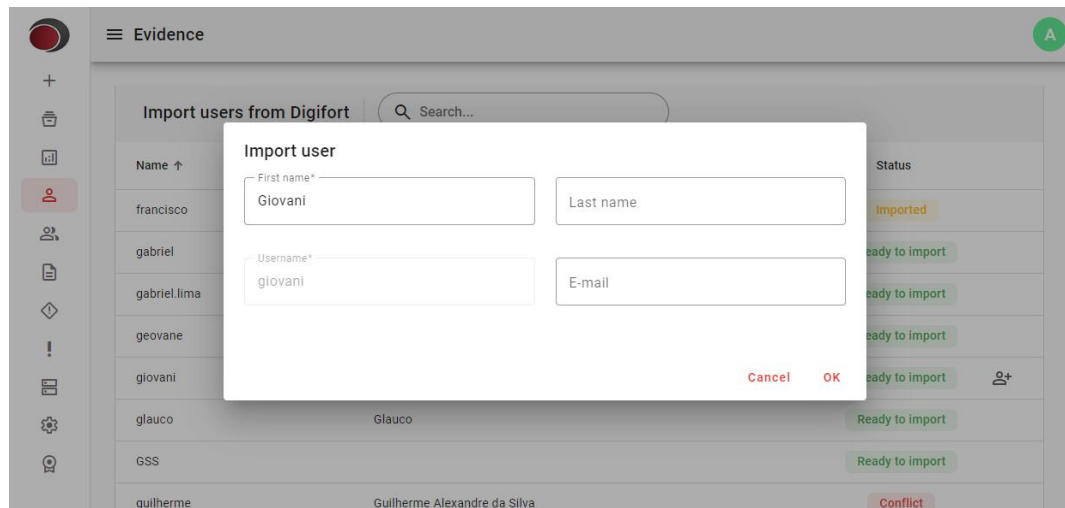
At the bottom of the table, there is a pagination control showing 'Items per page: 10' and '31 - 40 of 68'.

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 .



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

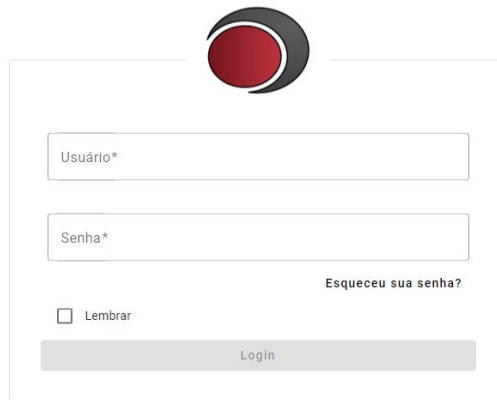
- Through user account management

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.

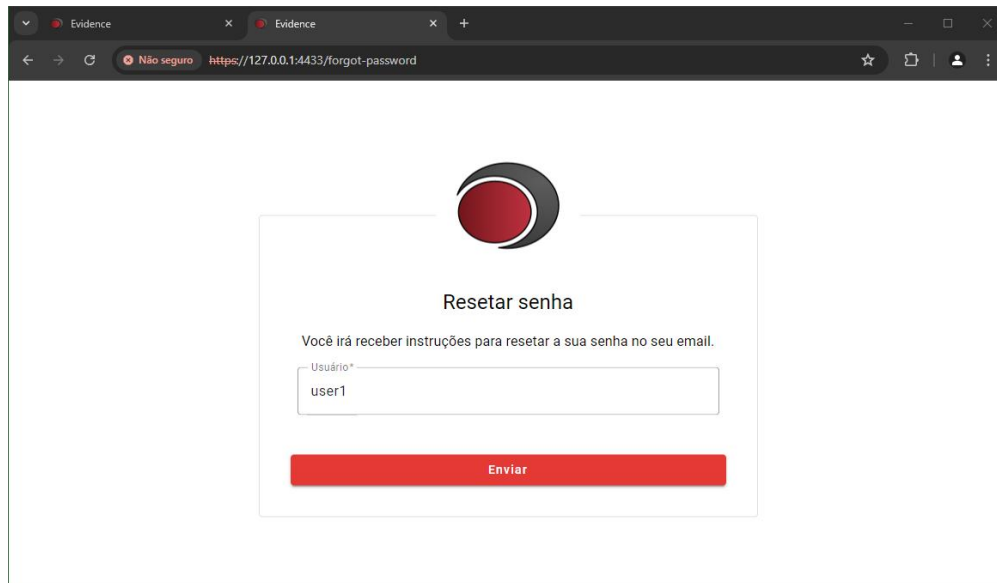
This email has a link that will take the user to the password reset page.

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



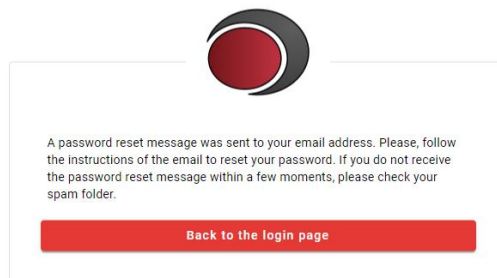
The screenshot shows a login form with a red and black circular logo at the top. Below the logo are two input fields: 'Usuário*' and 'Senha*'. To the right of the 'Senha*' field is a link that says 'Esqueceu sua senha?'. Below the input fields is a checkbox labeled 'Lembrar' and a 'Login' button.

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

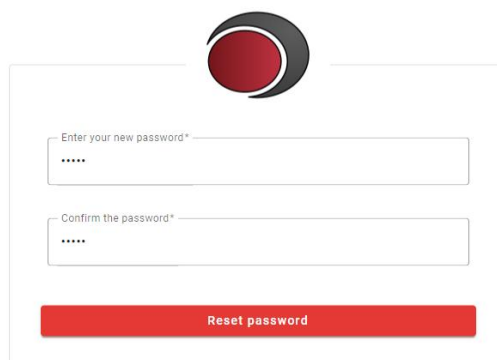


The screenshot shows a browser window with the URL 'https://127.0.0.1:4433/forgot-password'. The page has a red and black circular logo at the top. Below the logo is the title 'Resetar senha' and the text 'Você irá receber instruções para resetar a sua senha no seu email.' Below this text is an input field labeled 'Usuário*' with the value 'user1'. At the bottom of the form is a red 'Enviar' button.

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



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

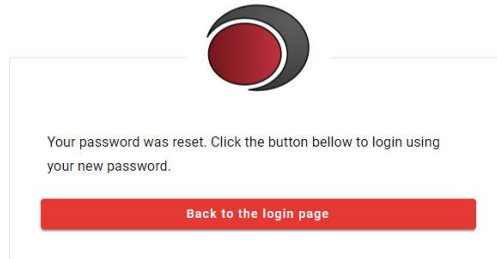


Enter your new password*

Confirm the password*

[Reset password](#)

Enter the new password and confirm.

**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

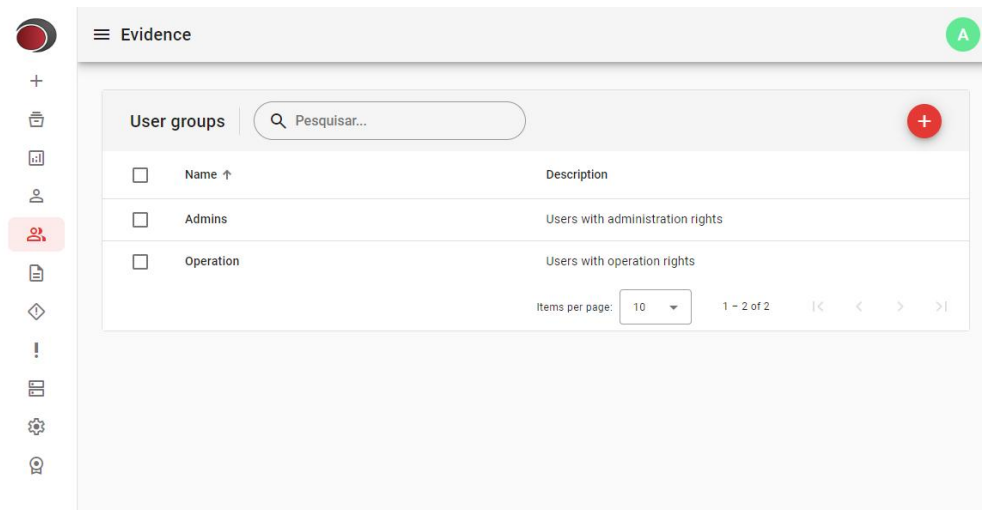
9 User groups

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.

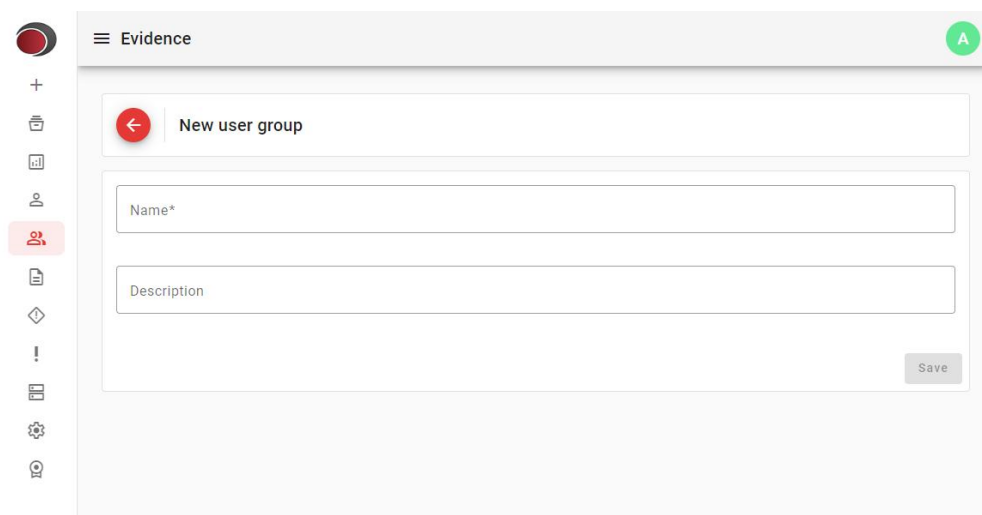
9.1 Accessing the user groups module

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



9.2 Adding user groups

To add user groups, click the button .

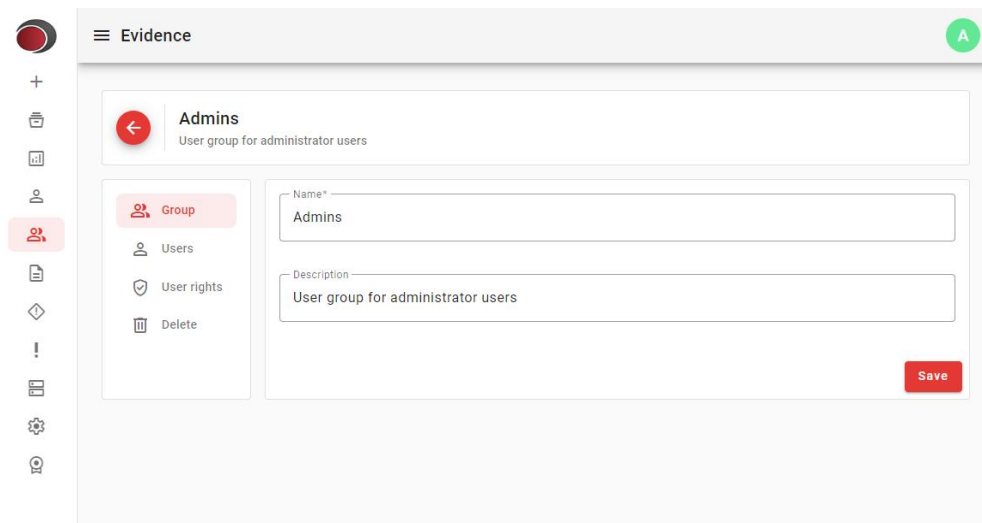


- **Name:** The name of the group
- **Description:** Optional description of the group

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.



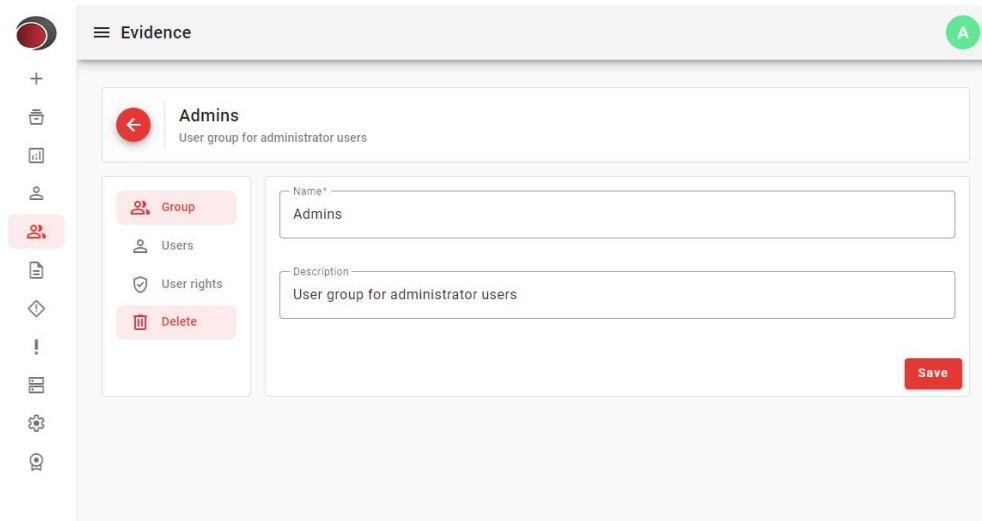
On the left side there is a menu where more group settings can be made.

- **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

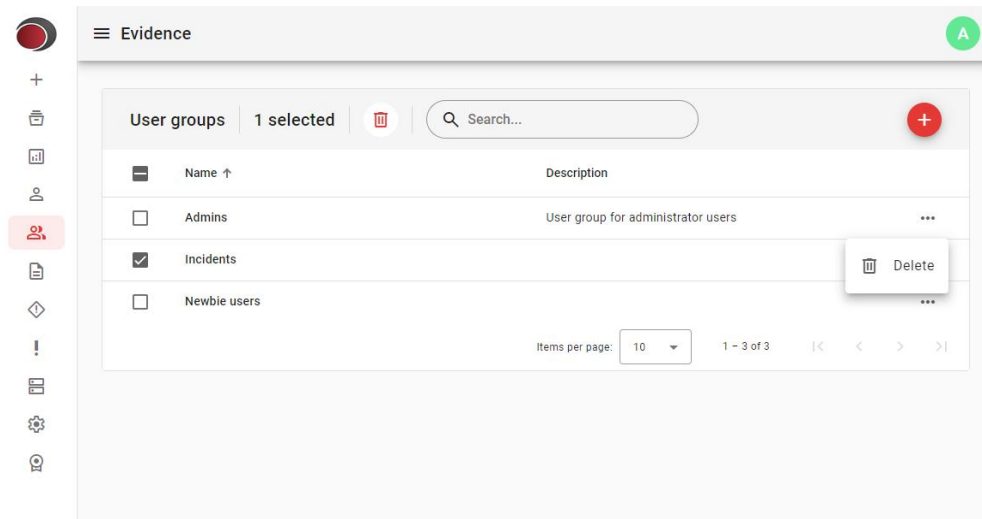
When deleting an user group, users belonging to the group will not be removed from the system, only their access rights will be removed.

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



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.

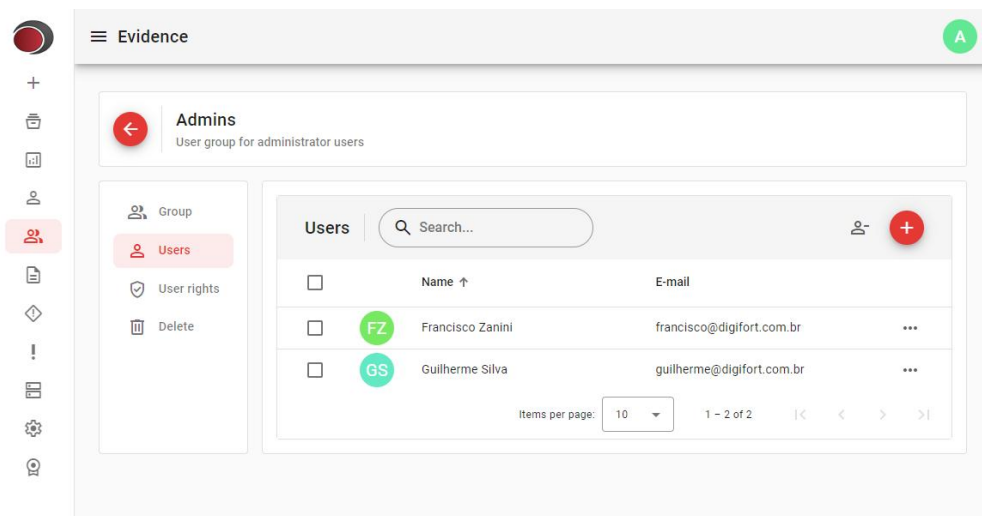
You can also use check boxes to remove more than one item at the same time. Select the items to be removed and then click  .



9.5 Managing users

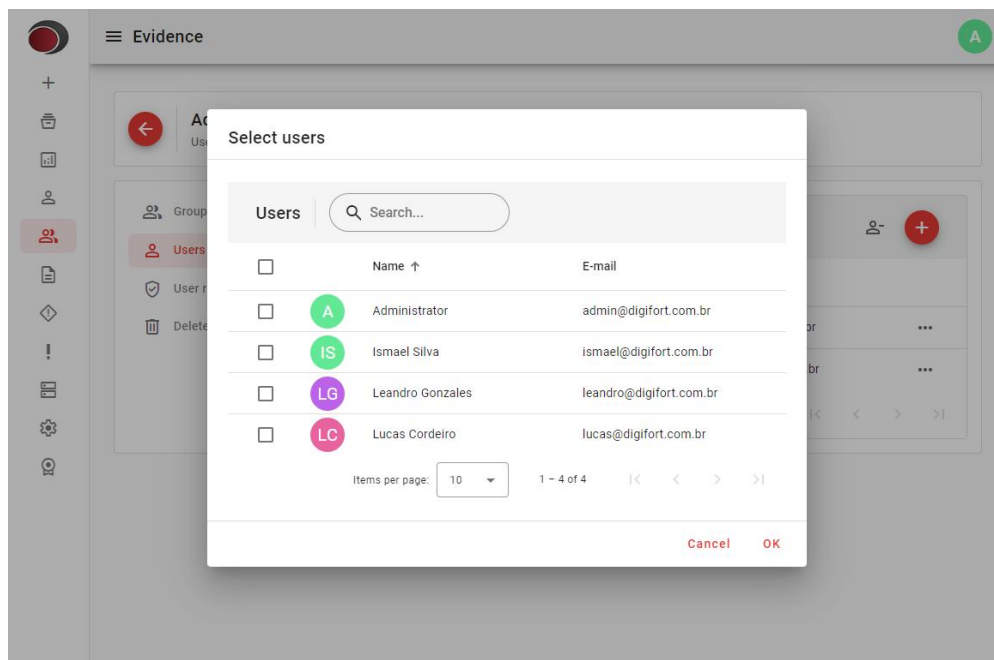
To add or remove users from the group, click the **Users** button.

A list of users will be displayed containing all users belonging to this group as shown in the image below:




9.5.1 Adding users to groups

To add users to the group, click the button .



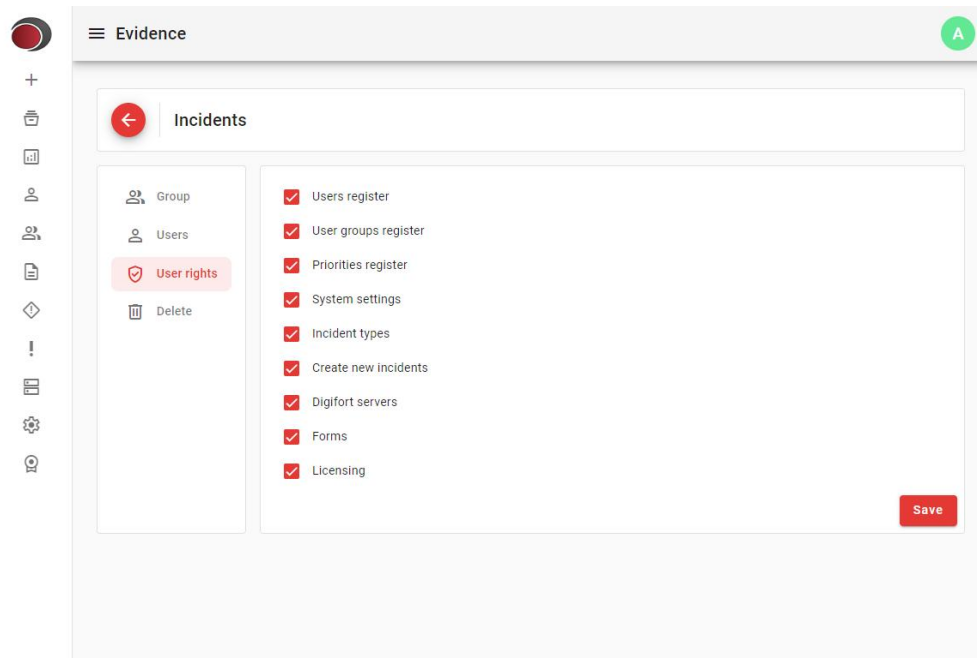
Select the desired users and click **OK**.

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 .

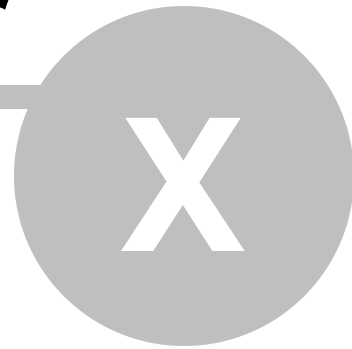
9.6 Configuring access rights

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



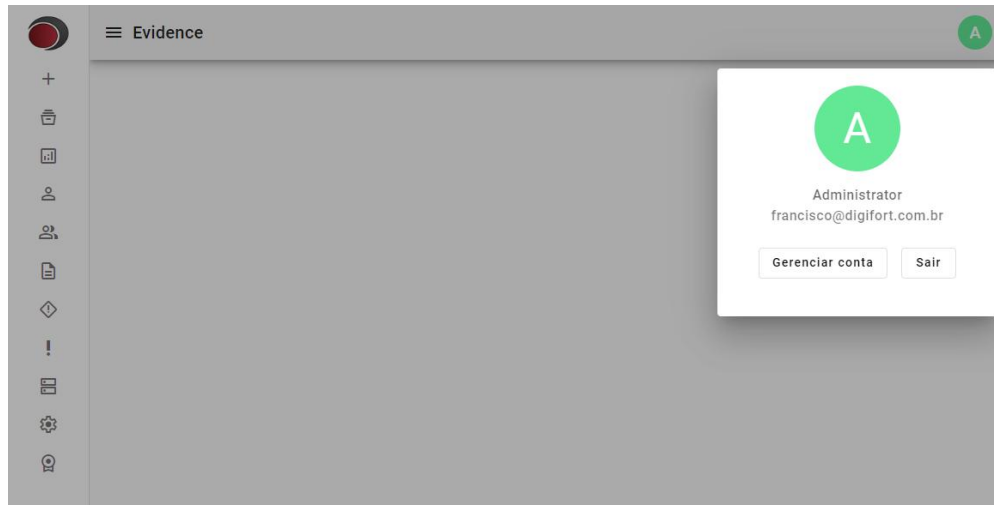
- **Users register:** Allows you to access registration, import, add, change and delete users.
- **User groups register:** Allows you to access the registration, add, change and delete user groups.
- **Priorities register:** Allows you to access the registration, add, change and delete priorities.
- **System Settings:** Allows you to modify system settings.
- **Incident types:** Allows you to access the registration, add, change and delete incident types.
- **Create new incident:** Allows the creation of incidents.
- **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



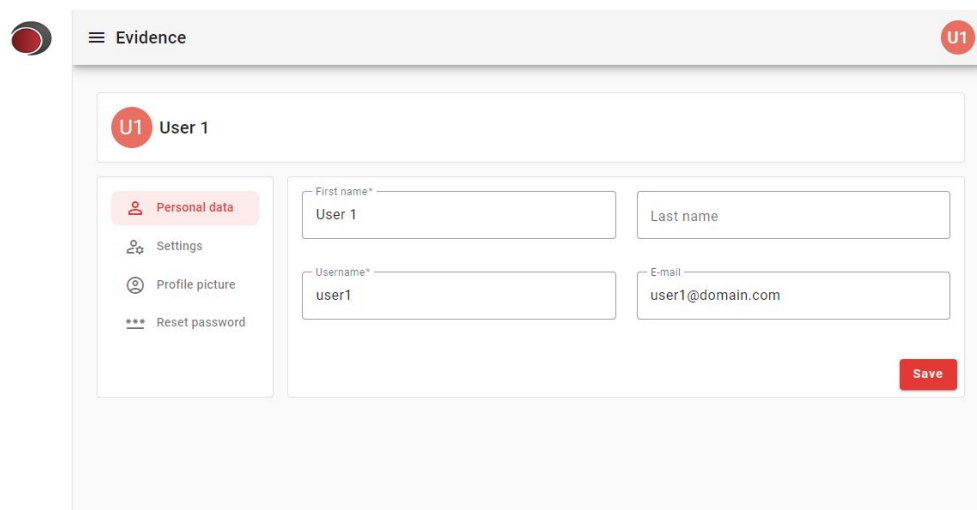
10 Managing the account of the logged user

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

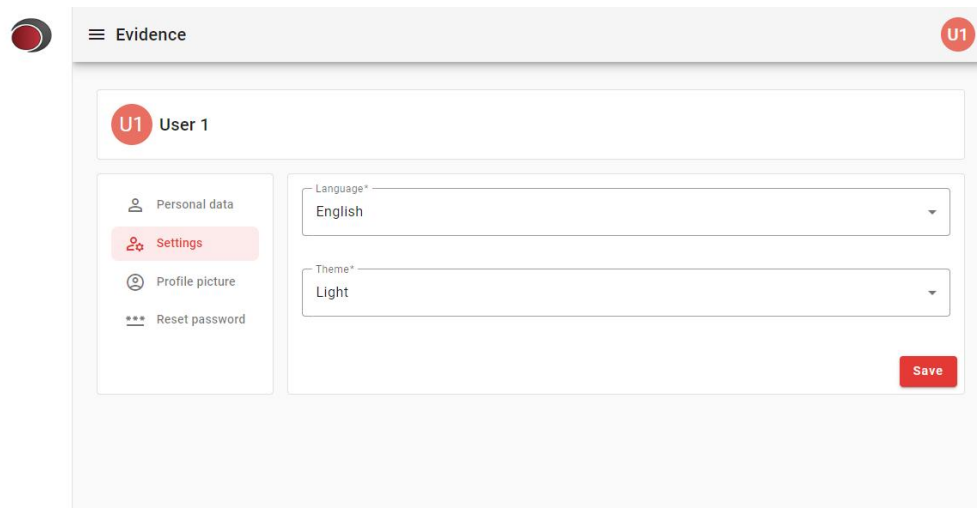
To change the logged in user's personal data, click the **Personal data** button.



- **First name:** User'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.

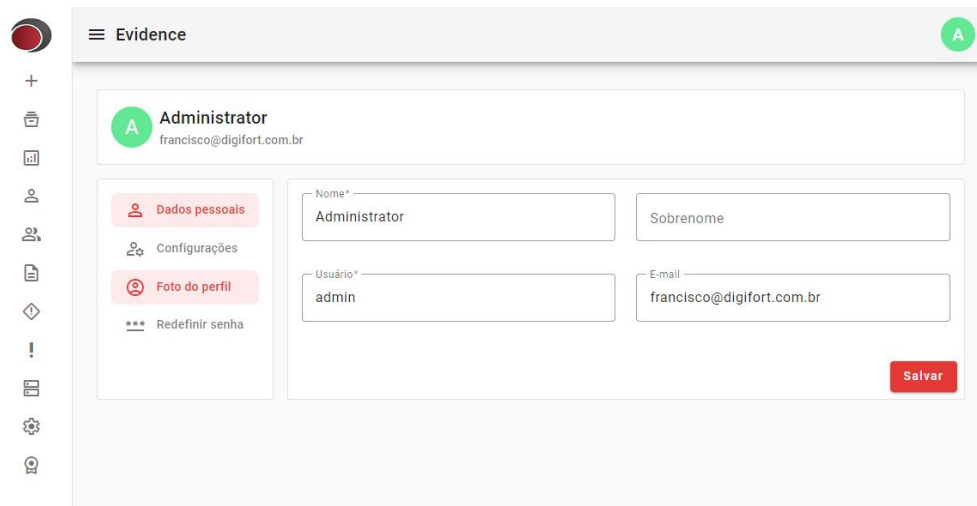


The screenshot shows the 'Evidence' application interface for a user named 'User 1'. The user's profile is displayed at the top. Below the profile, there is a sidebar menu with options: 'Personal data', 'Settings' (highlighted in red), 'Profile picture', and 'Reset password'. The main content area shows two dropdown menus: 'Language*' set to 'English' and 'Theme*' set to 'Light'. A red 'Save' button is located at the bottom right of the settings area.

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

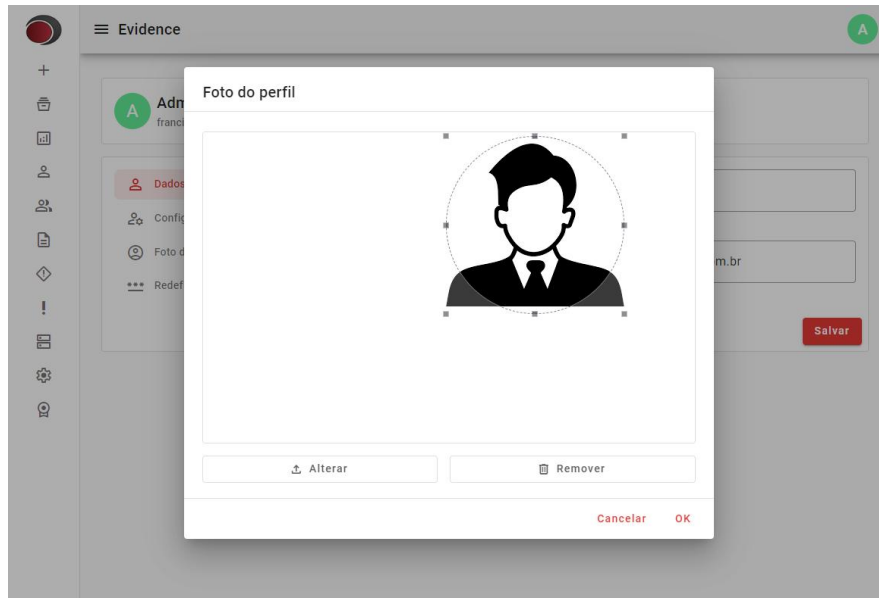
10.3 Modifying the profile picture

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



The screenshot shows the 'Evidence' application interface for a user named 'Administrator'. The user's profile is displayed at the top with the email 'francisco@digifort.com.br'. Below the profile, there is a sidebar menu with options: 'Dados pessoais', 'Configurações', 'Foto do perfil' (highlighted in red), and 'Redefinir senha'. The main content area shows four input fields: 'Nome*' (Administrator), 'Sobrenome', 'Usuário*' (admin), and 'E-mail' (francisco@digifort.com.br). A red 'Salvar' button is located at the bottom right of the settings area.

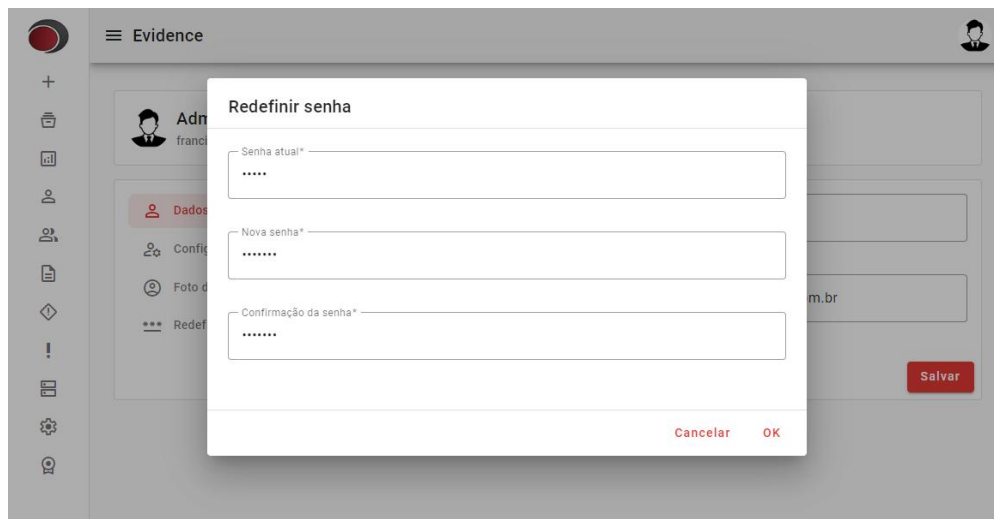
Select an image from your computer by clicking the **Change** button. You can use the framing controls to crop the image as needed.



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.



- **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



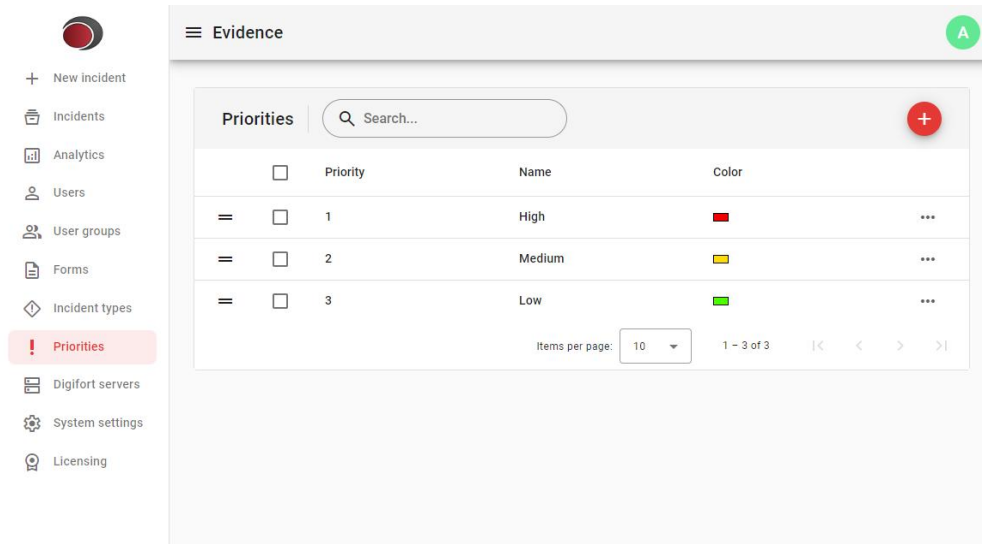
XI

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.

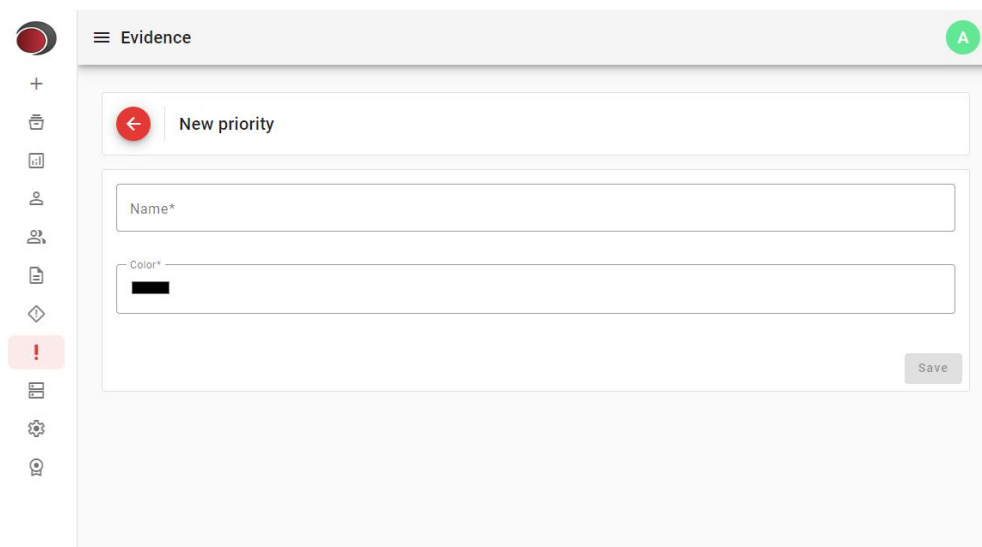
11.1 Accessing the priorities module

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



11.2 Adding priorities

To add priorities, click the button .



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

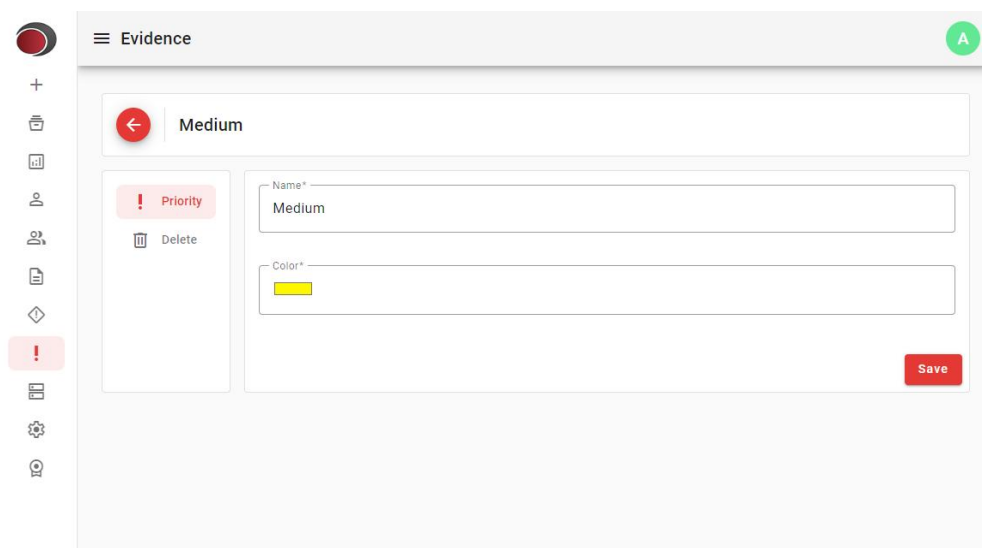
To select a color, click the black rectangle. A color selection window will appear as shown in the image below.



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.



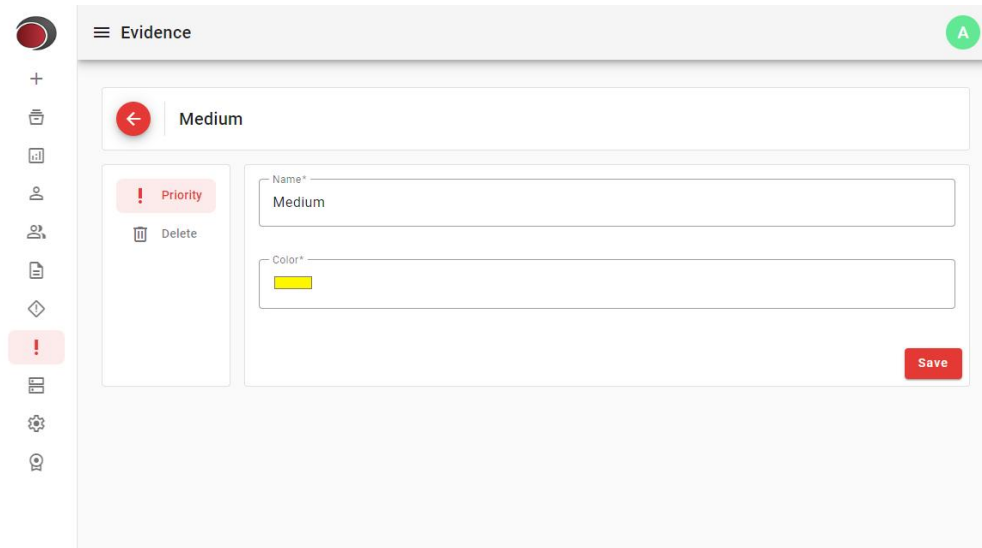
On the left side there is a menu where more settings can be made.

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


11.4 Deleting priorities

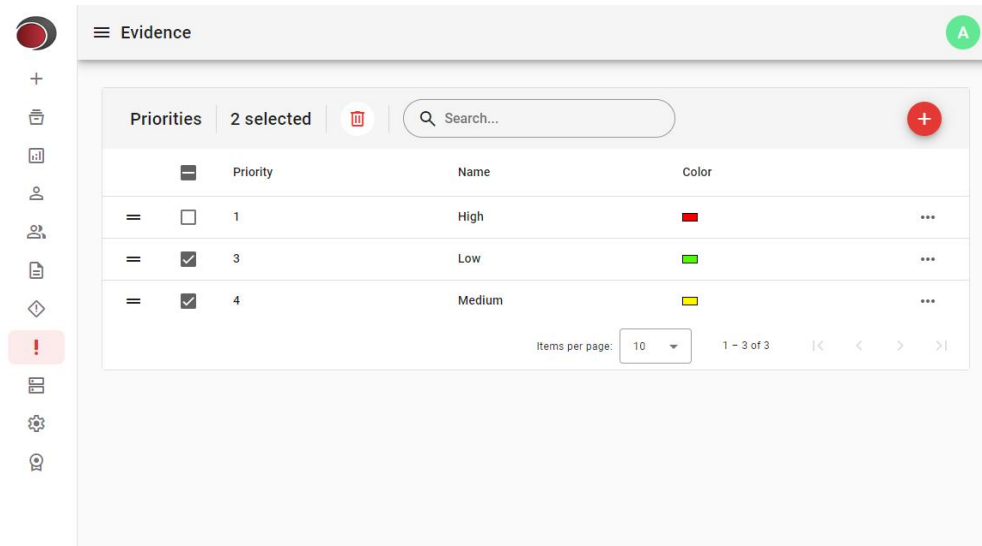
When you delete a priority, it will be disconnected from all incidents that were added with that priority. This way these incidents will not be prioritized.

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




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 .



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.

The screenshot shows a web application interface for managing priorities. On the left is a vertical sidebar with icons for home, add, delete, view, user, document, diamond, warning, list, settings, and help. The main content area is titled "Evidence" and contains a "Priorities" section. This section has a search bar and a red "+" button. Below is a table with three rows:

Priority	Name	Color
0	High	Red
1	Medium	Yellow
2	Low	Green

At the bottom of the table, there are pagination controls: "Items per page: 10" (with a dropdown arrow), "1 - 3 of 3", and navigation arrows (< > <>).

Chapter



XII

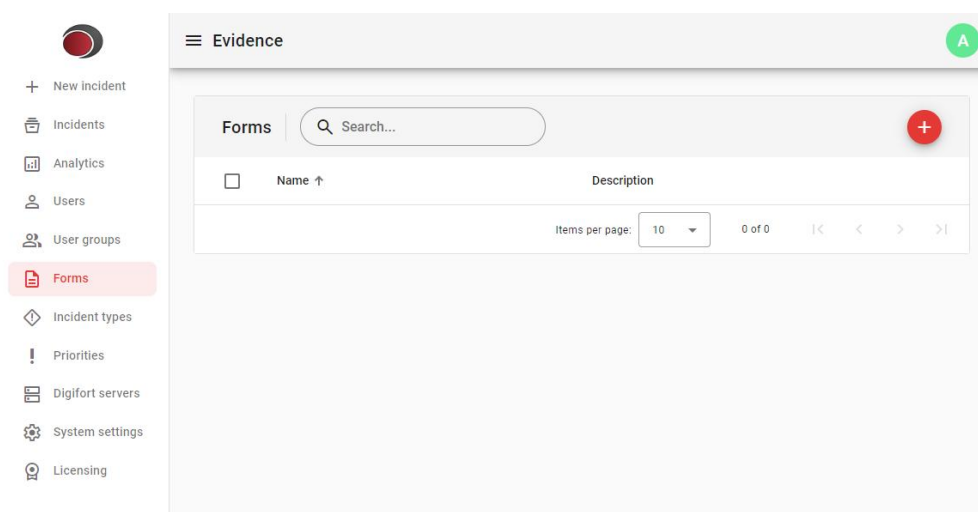
12 Forms

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.

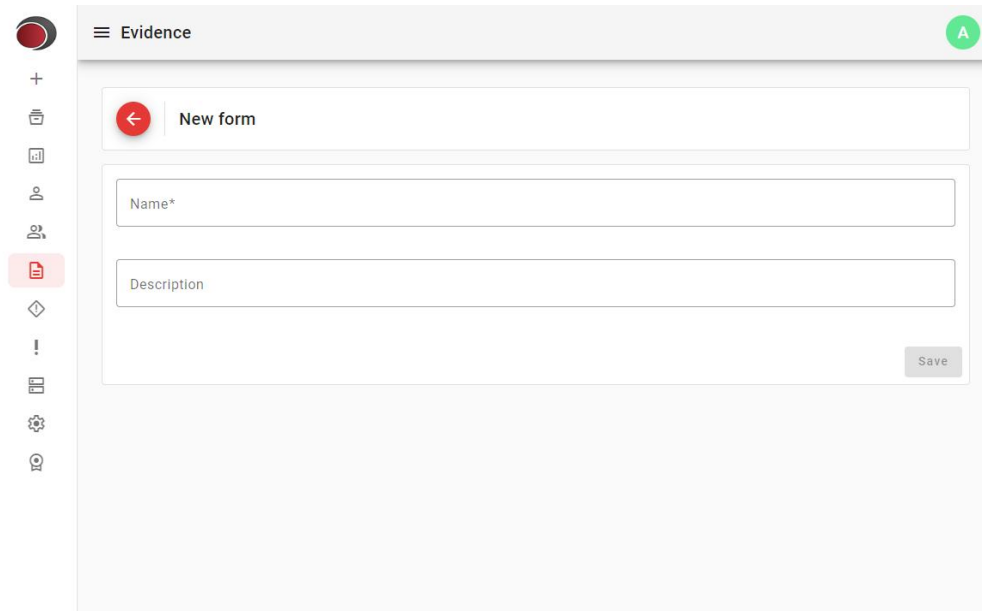
12.1 Accessing the forms module

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



12.2 Adding forms

Para adicionar formulários, clique no botão .

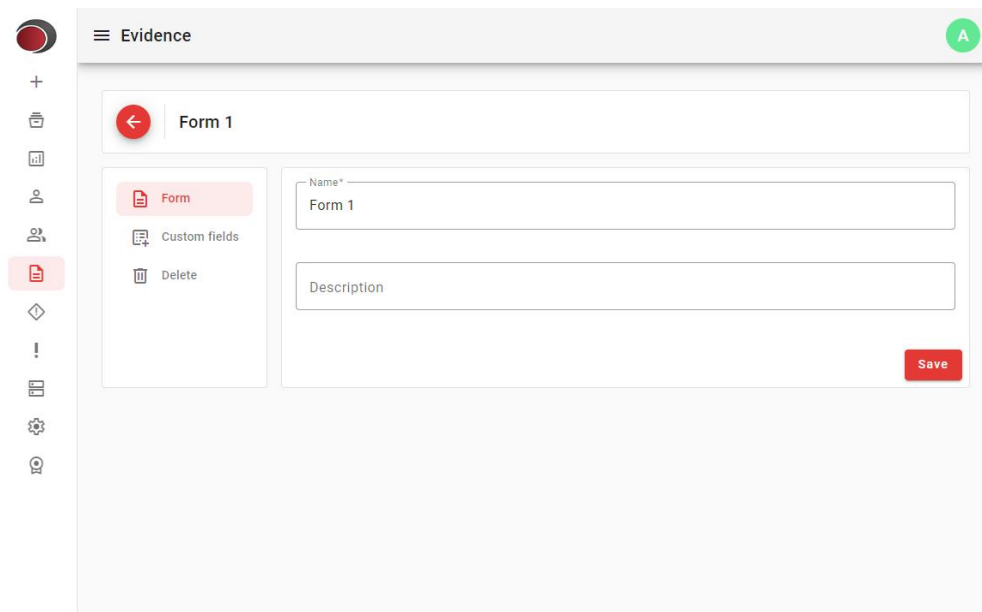


- **Name:** Name of the form.
- **Description:** An optional description for the form.

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](#).

12.3 Modifying forms

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



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

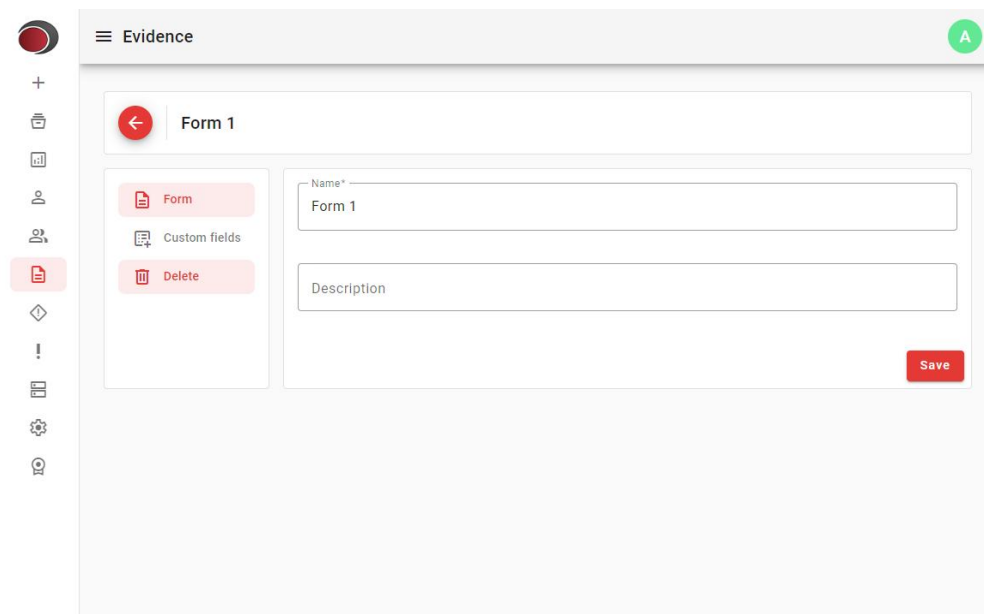
- **Form:** Allows you to modify the main data of the form.
- **Custom Fields:** Allows you to manage the form's custom fields. See the topic [Custom fields](#).

- **Delete:** Removes the form from the system. See the topic [Deleting forms](#).


12.4 Deleting forms

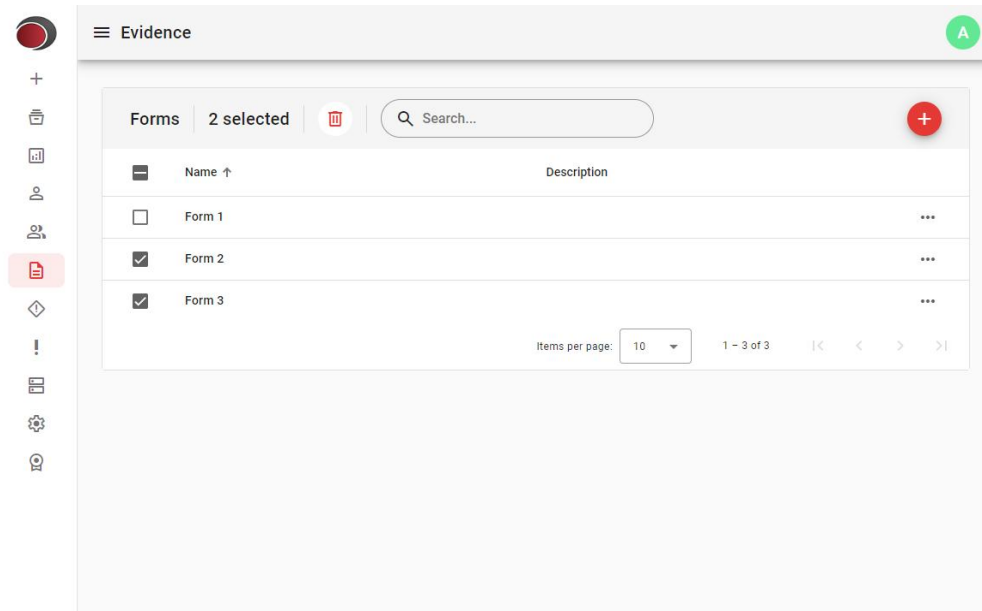
When you delete a form, it will no longer be available for filling out incidents, but all incidents created with this form will be preserved.

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



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 .



12.5 Custom fields

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

12.5.1 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.

12.5.1.1 Short text

A simple 1-line text field.

The screenshot shows the 'New custom field' dialog in the Evidence system. The dialog is titled 'New custom field' and has a 'Field type*' dropdown menu set to 'Short text'. To the right of the dropdown is a 'Field name*' input field. Below the dropdown is an 'Optional hint' input field. Under the 'Field validation' section, there are two checkboxes, both checked. The first checkbox is next to a 'Minimum length*' input field containing the value '4'. The second checkbox is next to a 'Maximum length*' input field containing the value '20'. At the bottom right of the dialog, there is a 'Mandatory' toggle switch, which is also checked. At the very bottom of the dialog are 'Cancel' and 'OK' buttons.

Validations:

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

12.5.1.2 Paragraph

A multi-line text field.

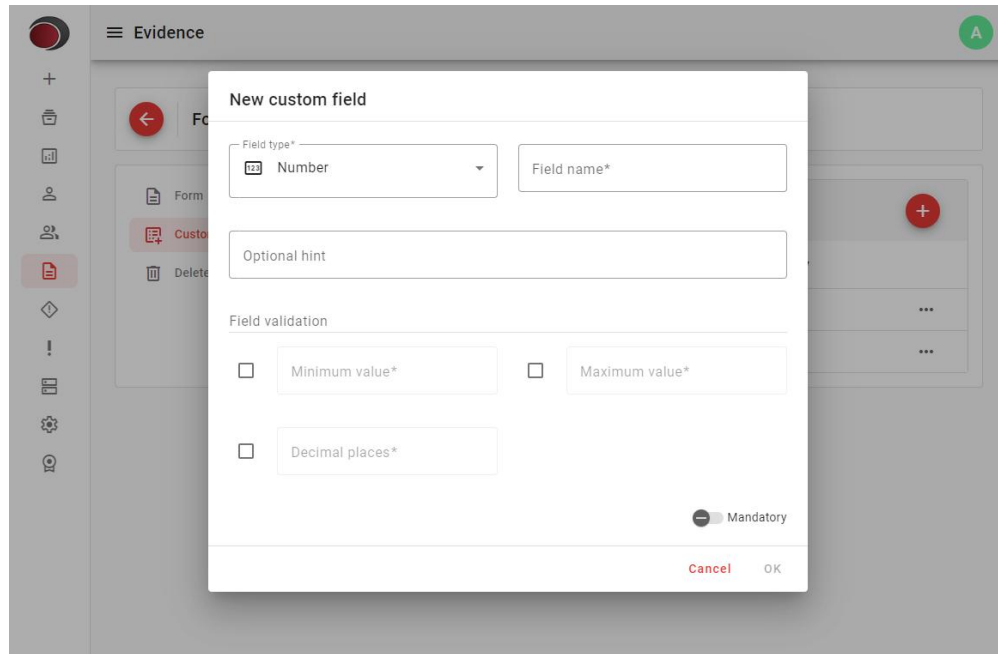
The screenshot shows the 'New custom field' dialog in the Evidence system. The dialog is titled 'New custom field' and has a 'Field type*' dropdown menu set to 'Paragraph'. To the right of the dropdown is a 'Field name*' input field. Below the dropdown is an 'Optional hint' input field. Under the 'Field validation' section, there is one checked checkbox next to a 'Maximum length*' input field containing the value '4000'. At the bottom right of the dialog, there is a 'Mandatory' toggle switch, which is also checked. At the very bottom of the dialog are 'Cancel' and 'OK' buttons.

Validations:

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

12.5.1.3 Number

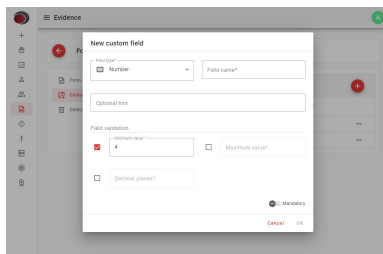
A numeric field.



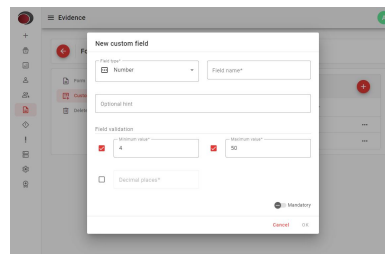
Validations:

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

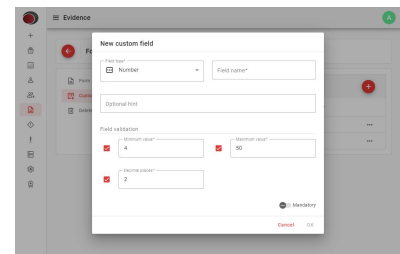
12.5.1.3.1 Examples



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



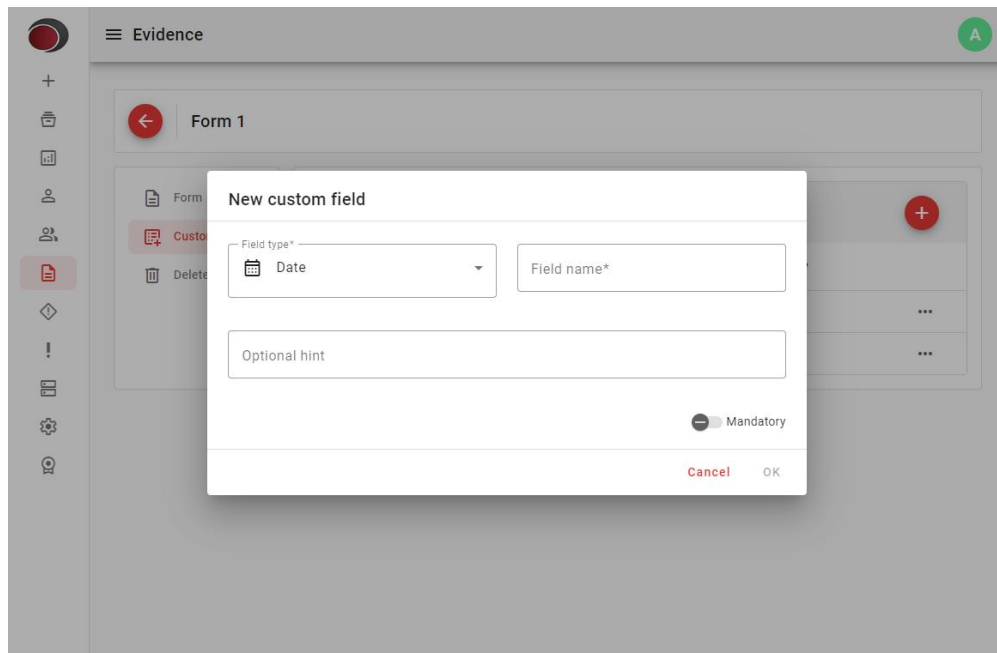
The value of the number must be between 4 and 50



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

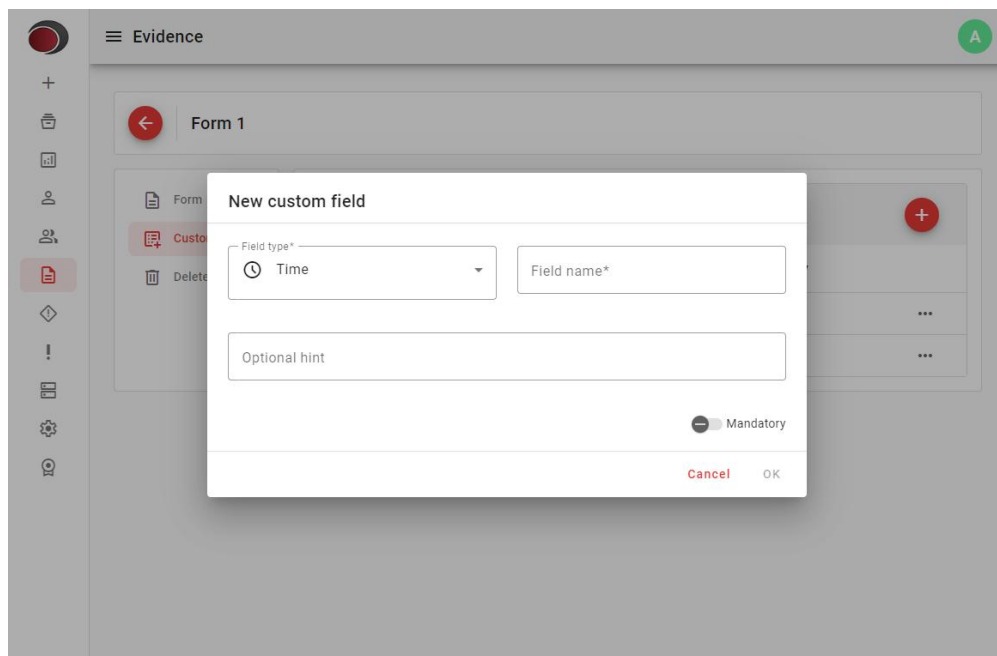
12.5.1.4 Date

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



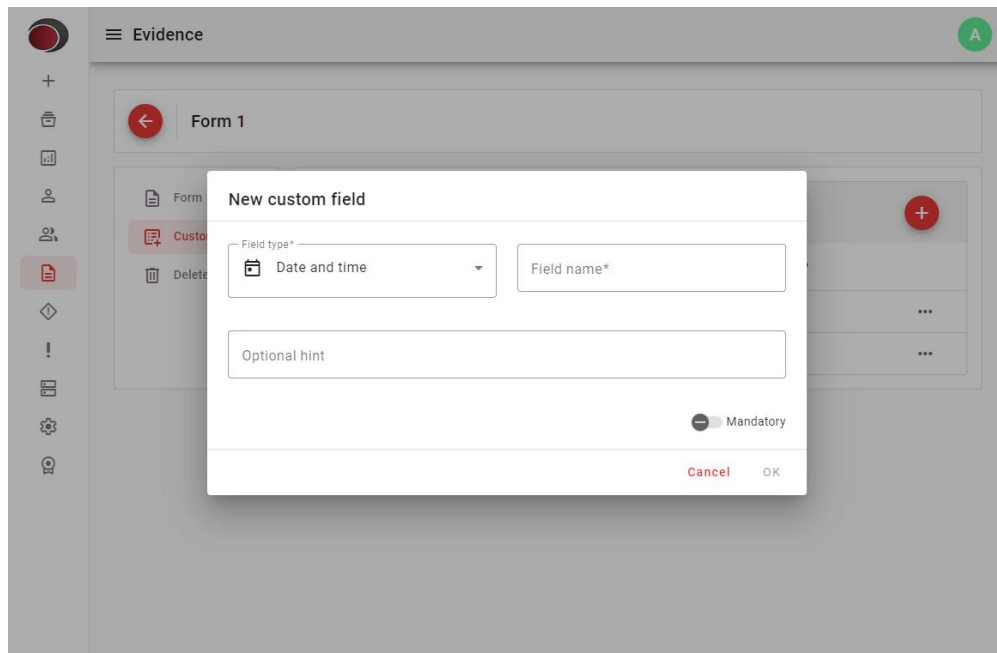
12.5.1.5 Time

A time field.



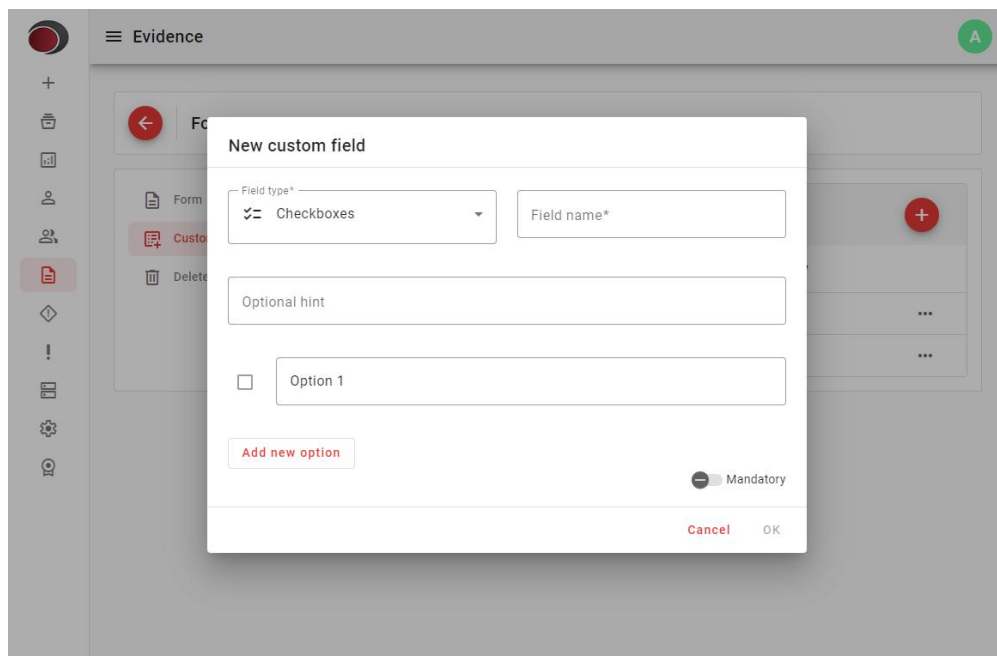
12.5.1.6 Date and time

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

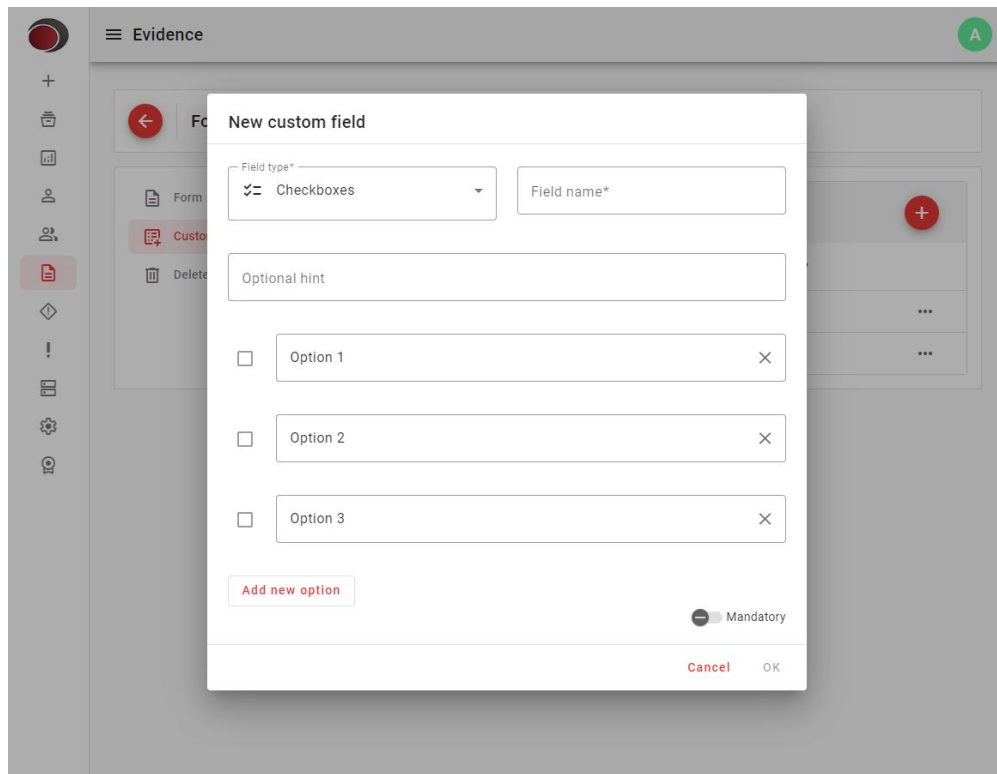


12.5.1.7 Checkboxes

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



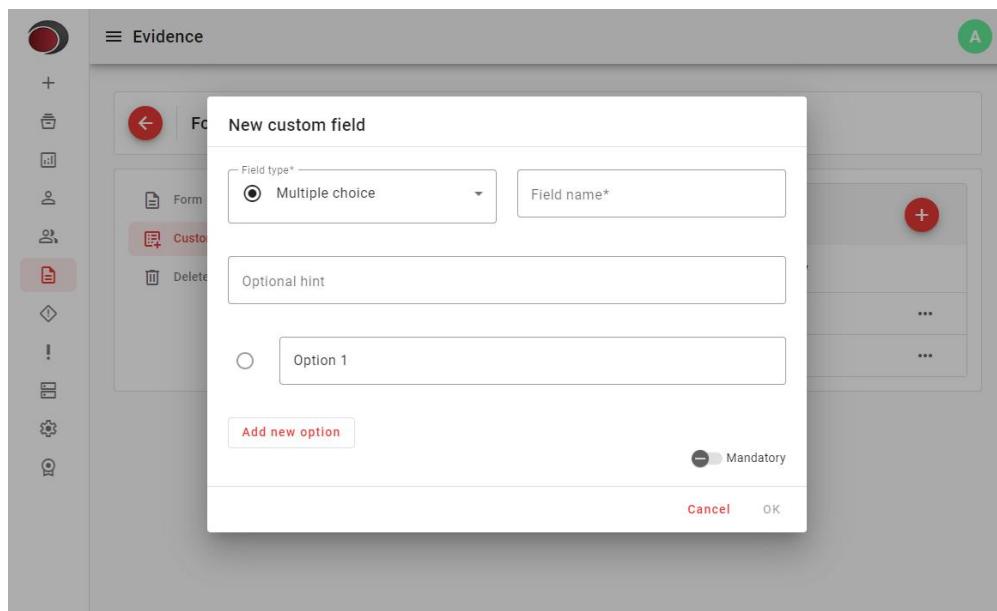
To add new options, click the **Add option** button and type the text for this option.



The screenshot shows the 'New custom field' dialog box in the Evidence system. The 'Field type*' dropdown is set to 'Checkboxes'. The 'Field name*' field is empty. Below the dropdown is an 'Optional hint' text box. There are three option rows, each with a checkbox, a text input field, and a close button (X). The options are labeled 'Option 1', 'Option 2', and 'Option 3'. At the bottom left is an 'Add new option' button. At the bottom right is a 'Mandatory' toggle switch, which is currently turned off. The dialog has 'Cancel' and 'OK' buttons at the bottom right.

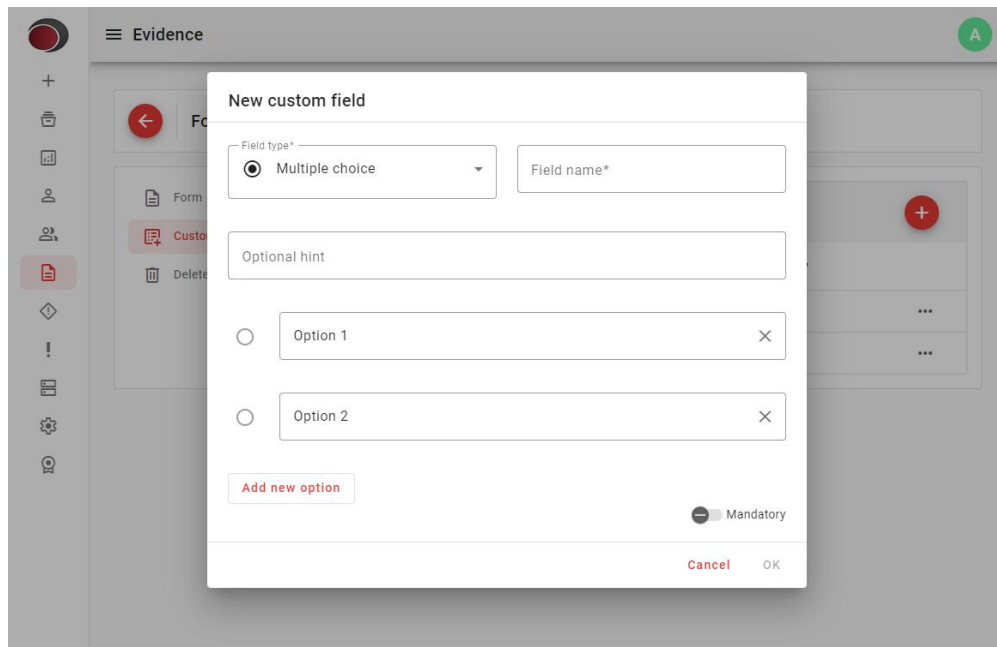
12.5.1.8 Multiple choice

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



The screenshot shows the 'New custom field' dialog box in the Evidence system. The 'Field type*' dropdown is set to 'Multiple choice'. The 'Field name*' field is empty. Below the dropdown is an 'Optional hint' text box. There is one option row with a radio button, a text input field, and a close button (X). The option is labeled 'Option 1'. At the bottom left is an 'Add new option' button. At the bottom right is a 'Mandatory' toggle switch, which is currently turned off. The dialog has 'Cancel' and 'OK' buttons at the bottom right.

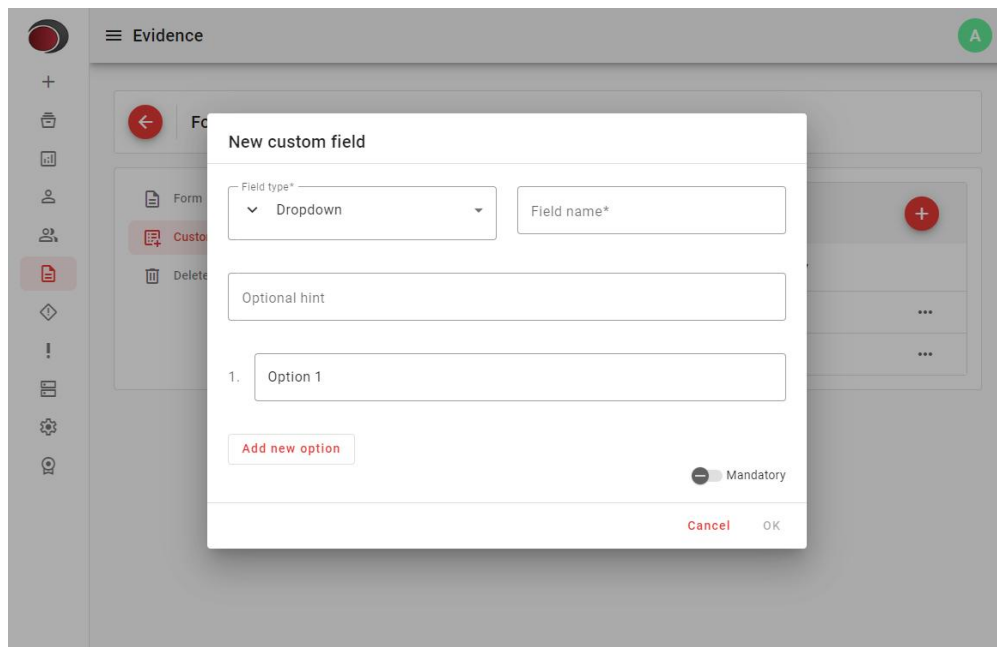
To add new options, click the **Add option** button and type the text for this option.



The screenshot shows the 'New custom field' dialog box in the Evidence application. The 'Field type*' dropdown is set to 'Multiple choice'. The 'Field name*' field is empty. Below the dropdown is an 'Optional hint' text box. There are two radio button options: 'Option 1' and 'Option 2', each with a delete 'X' button. An 'Add new option' button is located below the options. At the bottom right, there is a 'Mandatory' toggle switch, and 'Cancel' and 'OK' buttons.

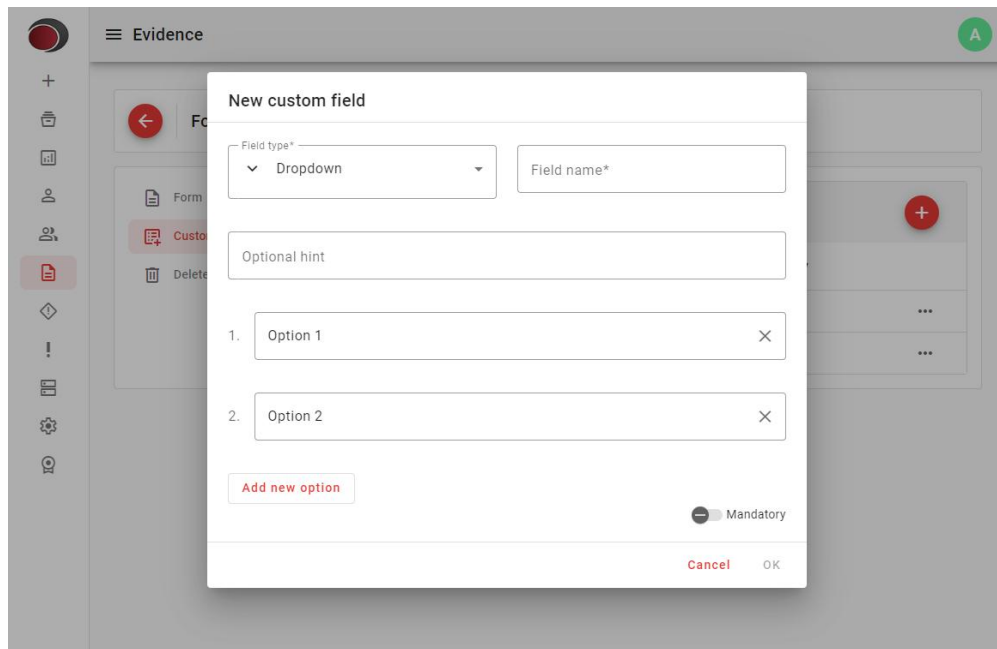
12.5.1.9 Dropdown

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



The screenshot shows the 'New custom field' dialog box in the Evidence application. The 'Field type*' dropdown is set to 'Dropdown'. The 'Field name*' field is empty. Below the dropdown is an 'Optional hint' text box. There is one radio button option: '1. Option 1'. An 'Add new option' button is located below the option. At the bottom right, there is a 'Mandatory' toggle switch, and 'Cancel' and 'OK' buttons.

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

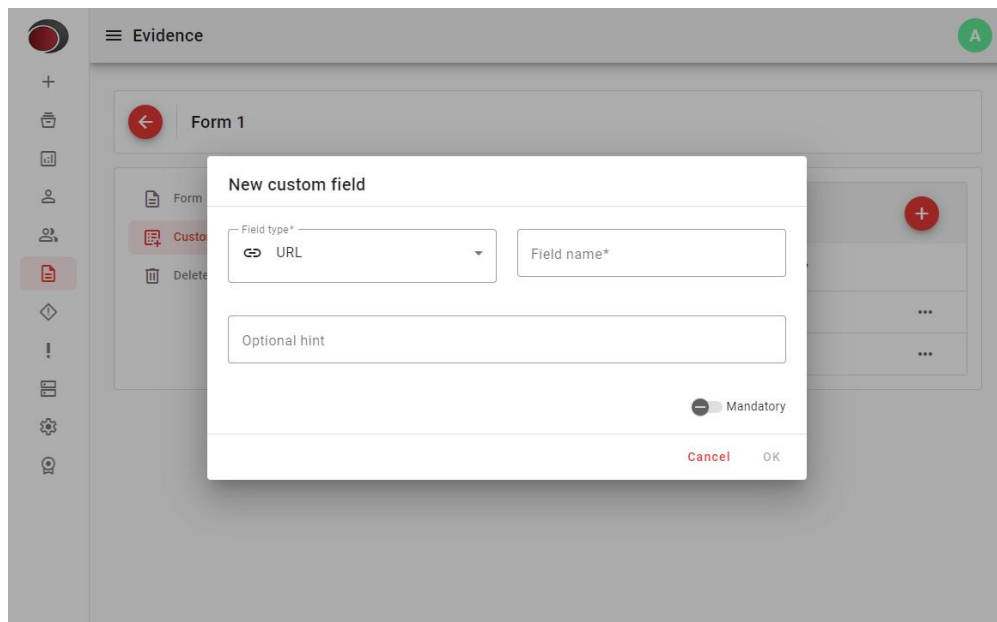


The screenshot shows the 'New custom field' dialog in the Evidence system. The dialog is titled 'New custom field' and contains the following elements:

- Field type*:** A dropdown menu set to 'Dropdown'.
- Field name*:** A text input field.
- Optional hint:** A text input field.
- Options:** A list of two options: '1. Option 1' and '2. Option 2', each with a close button (X).
- Add new option:** A button to add a new option.
- Mandatory:** A toggle switch currently turned off.
- Buttons:** 'Cancel' and 'OK' buttons at the bottom right.

12.5.1.10 URL

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

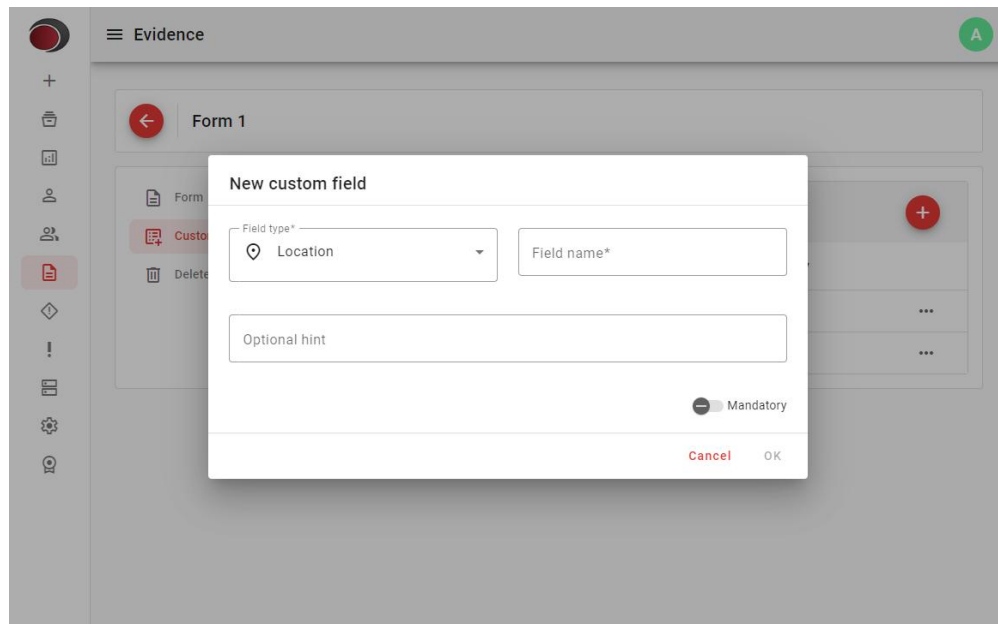


The screenshot shows the 'New custom field' dialog in the Evidence system, with the 'URL' field type selected. The dialog contains the following elements:

- Field type*:** A dropdown menu set to 'URL'.
- Field name*:** A text input field.
- Optional hint:** A text input field.
- Mandatory:** A toggle switch currently turned off.
- Buttons:** 'Cancel' and 'OK' buttons at the bottom right.


12.5.1.11 Location

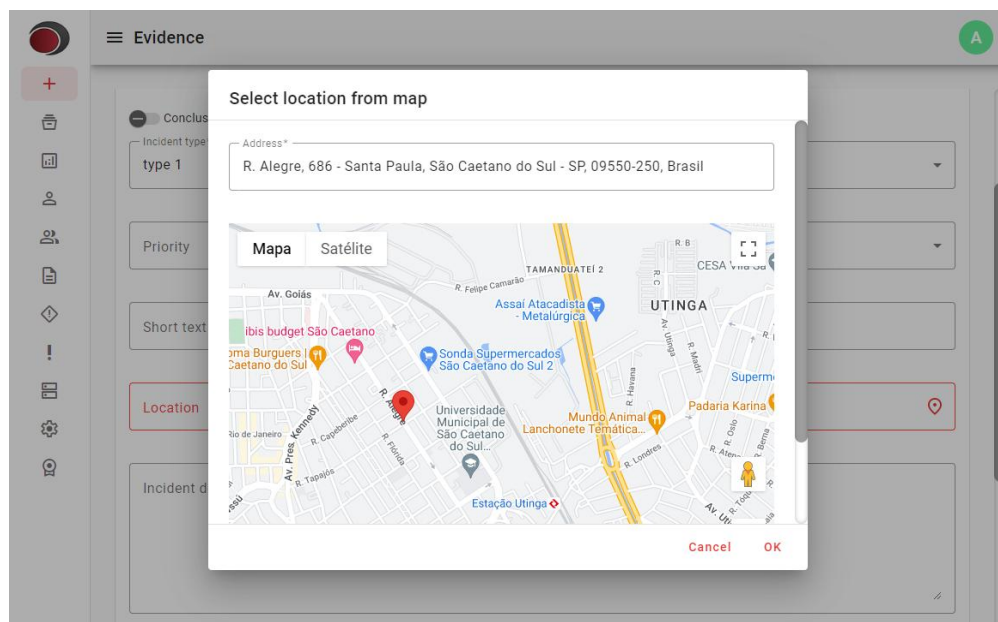
A geographic location field. When filling out, the user can select the location on a map or search by address.



12.5.1.11.1 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 .



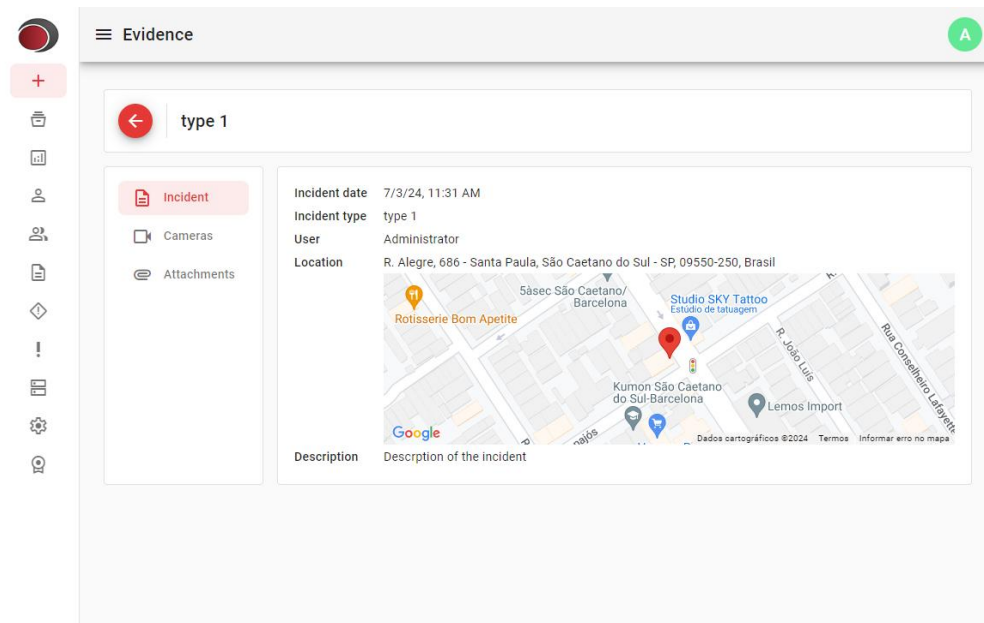
You can search for an address in the text field. With the auto-complete feature you can complete the address selection with the up or down arrows on the keyboard or by clicking on a suggestion with the

mouse.

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

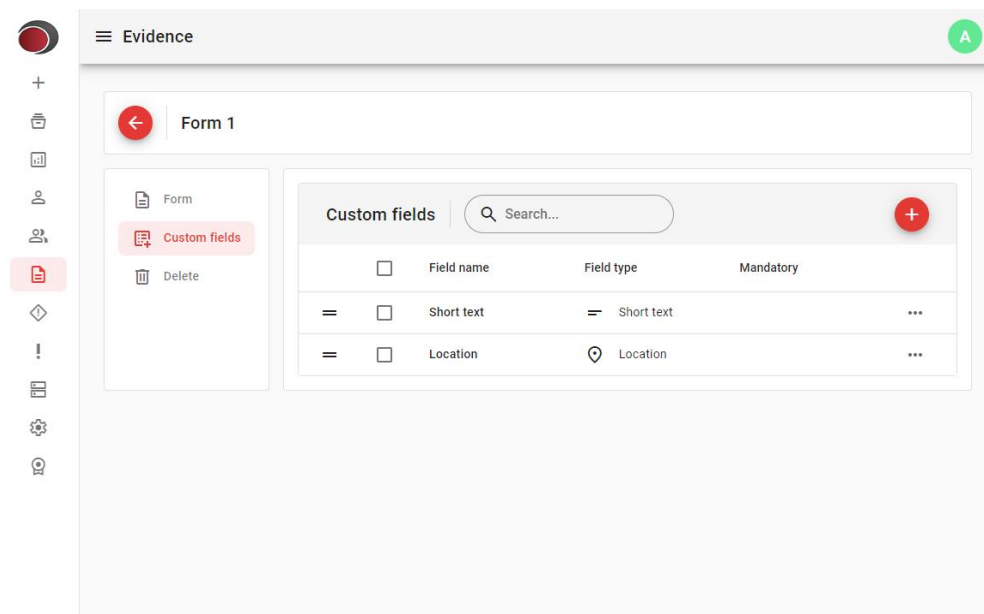
12.5.1.11.2 Viewing a location field

Location custom fields appear in an incident view as follows:

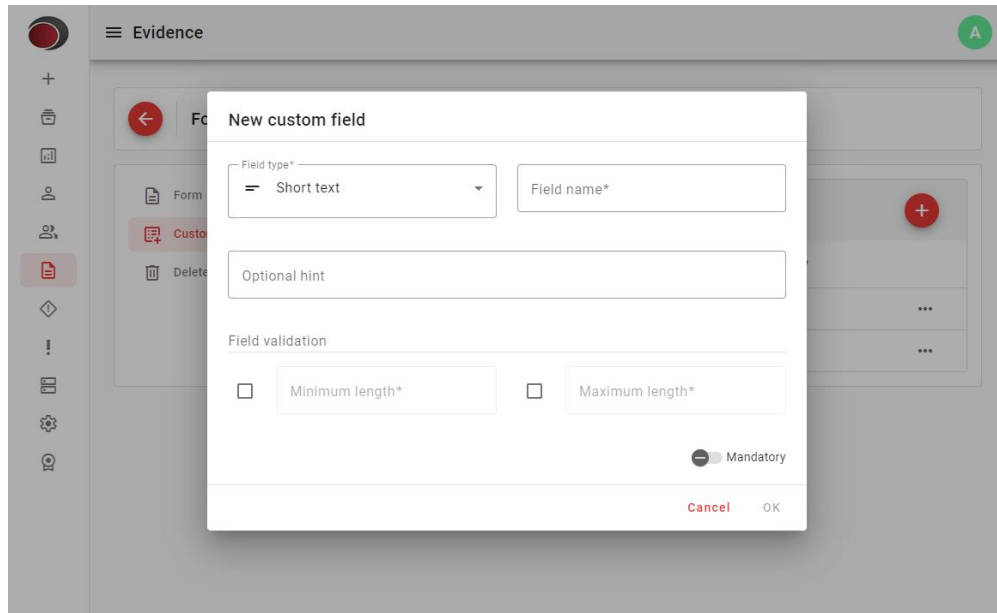


12.5.2 Adding custom fields

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



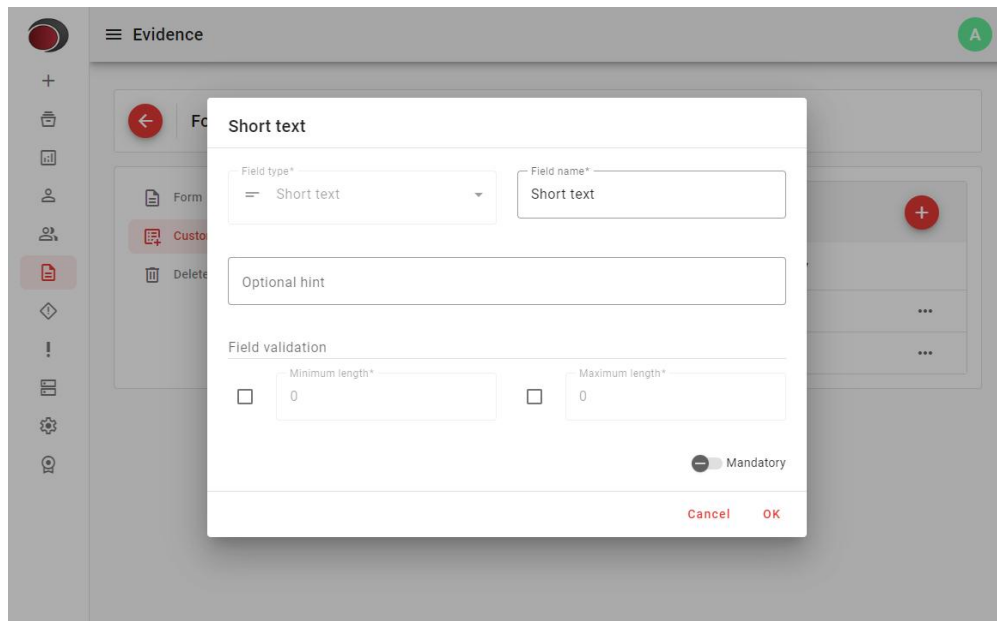
Once done, click the button  to add a new custom field.



- **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.

12.5.3 Modifying custom fields

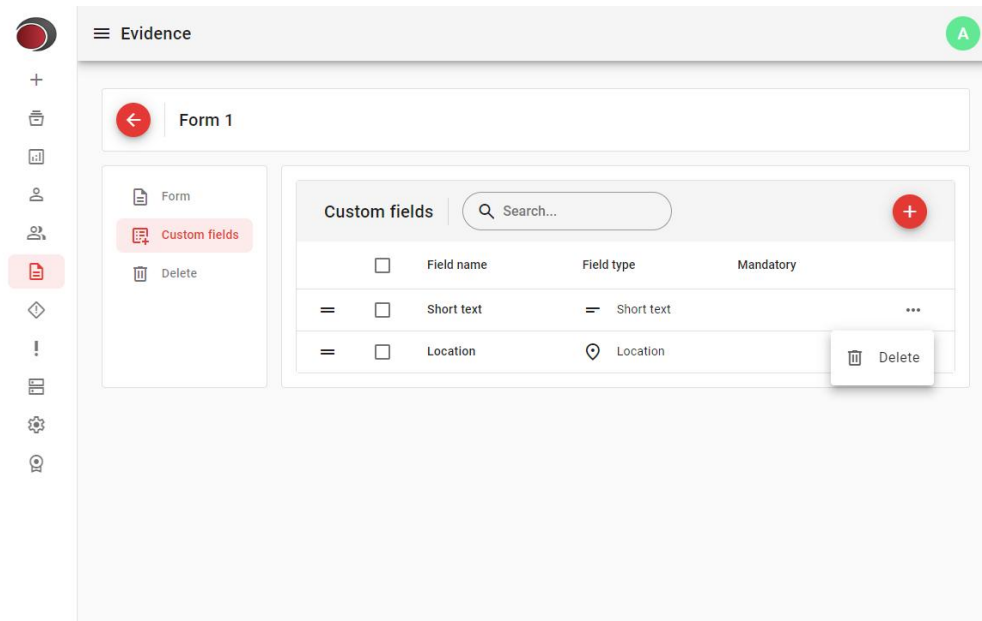
To change custom fields, click the name of the field you want to modify.




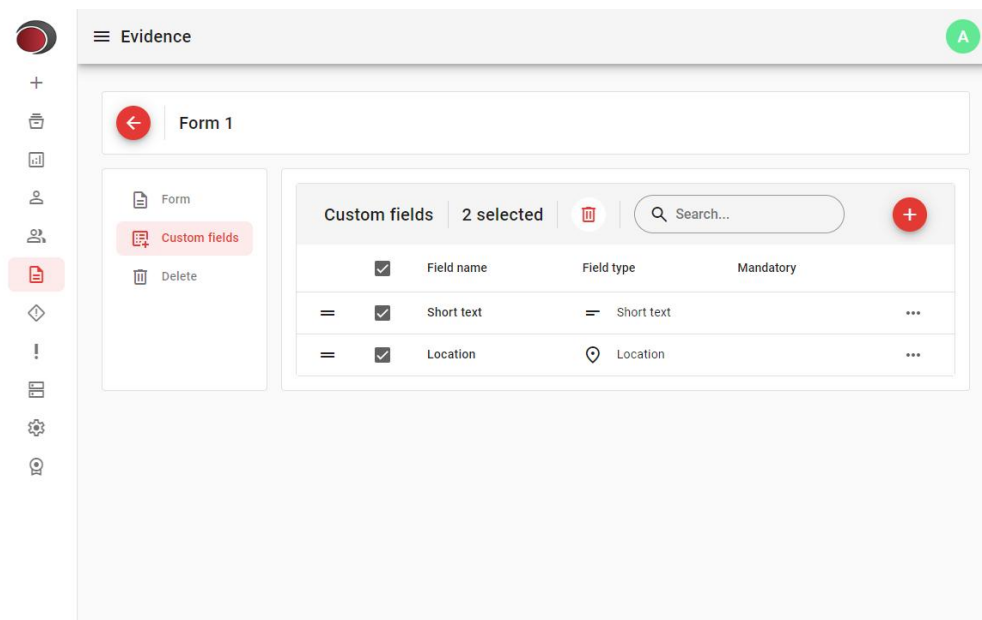
12.5.4 Deleting custom fields

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.



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



Chapter



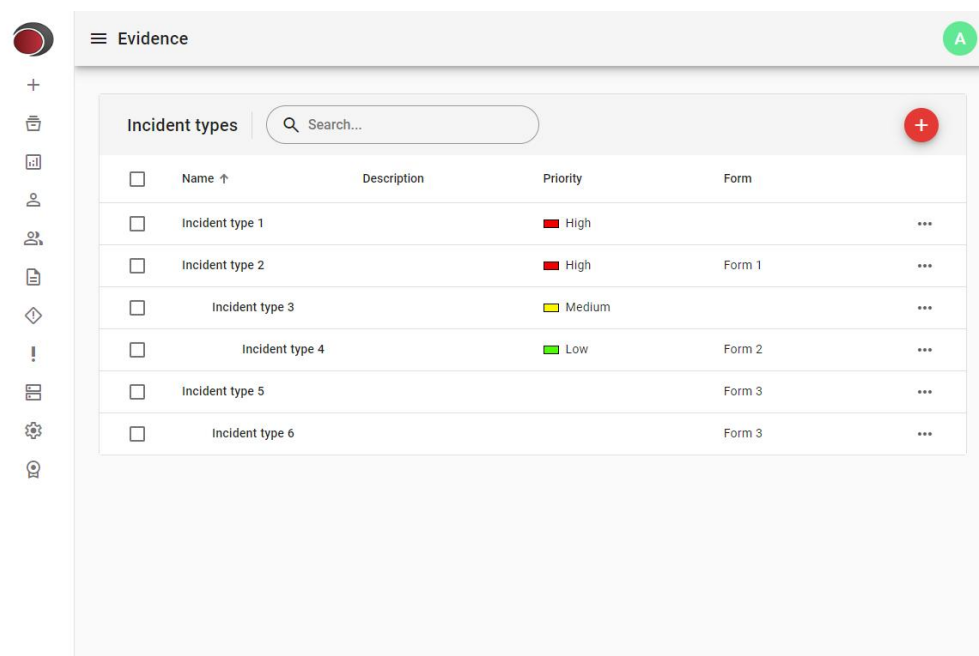
XIII

13 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.

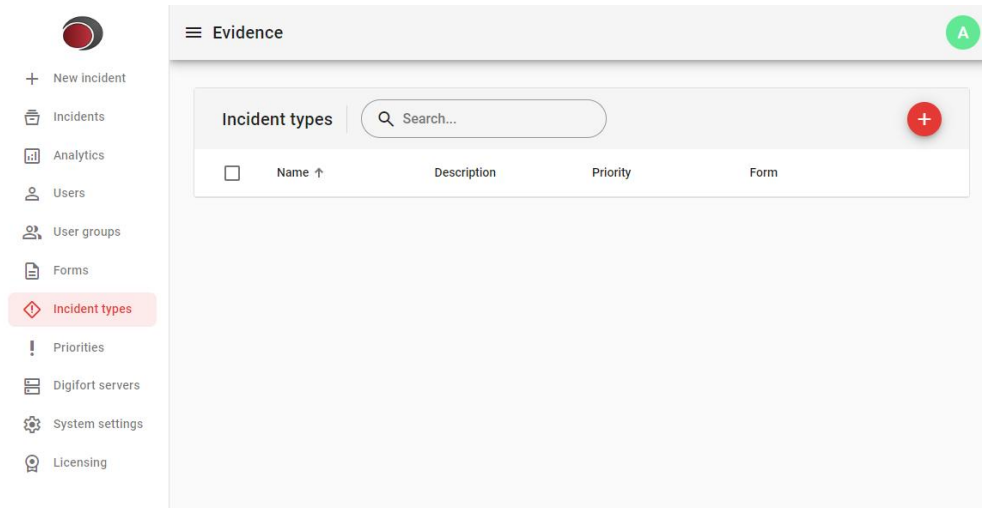
See the example below:




- **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.

13.1 Accessing the incident types module

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



13.2 Adding incident types

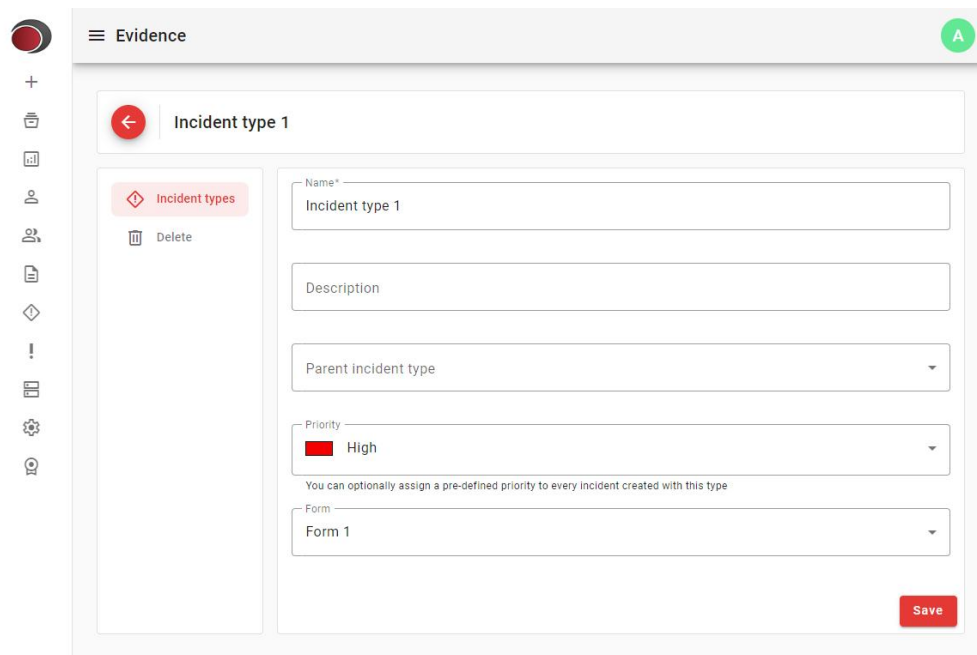
Para adicionar tipos de incidentes, clique no botão .

- **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.

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](#).

13.3 Modifying incident types

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



The screenshot shows the 'Evidence' application interface. At the top, there is a header with a hamburger menu icon, the text 'Evidence', and a green circle with the letter 'A'. Below the header is a navigation bar with a red back arrow and the text 'Incident type 1'. The main content area is divided into two sections. On the left, there is a sidebar menu with a red diamond icon and the text 'Incident types', and a 'Delete' button with a trash icon. On the right, there is a form with the following fields: 'Name*' (text input with value 'Incident type 1'), 'Description' (text input), 'Parent incident type' (dropdown menu), 'Priority' (dropdown menu with value 'High' and a red square icon), and 'Form' (dropdown menu with value 'Form 1'). Below the 'Priority' dropdown, there is a small text note: 'You can optionally assign a pre-defined priority to every incident created with this type'. At the bottom right of the form, there is a red 'Save' button.

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](#).

13.4 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:

The screenshot shows the 'Evidence' management interface. On the left is a vertical sidebar with various icons. The main content area is titled 'Incident type 1' and contains a form for editing an incident type. The form fields are:

- Name:** Incident type 1
- Description:** (empty text field)
- Parent incident type:** (dropdown menu)
- Priority:** High (with a red square icon)
- Form:** Form 1

Below the 'Priority' field, there is a note: "You can optionally assign a pre-defined priority to every Incident created with this type". A red 'Save' button is located at the bottom right of the form. On the left side of the form, there are two buttons: 'Incident types' and 'Delete'.

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 .

The screenshot shows the 'Evidence' management interface displaying a list of incident types. The table has the following columns: Name, Description, Priority, and Form. Two items are selected, indicated by checkmarks in the first column. A search bar and a '+ Add' button are visible at the top right of the table area.

<input checked="" type="checkbox"/>	Name ↑	Description	Priority	Form	
<input checked="" type="checkbox"/>	Incident type 1		High	Form 1	...
<input checked="" type="checkbox"/>	type 1			Form 1	...

Chapter

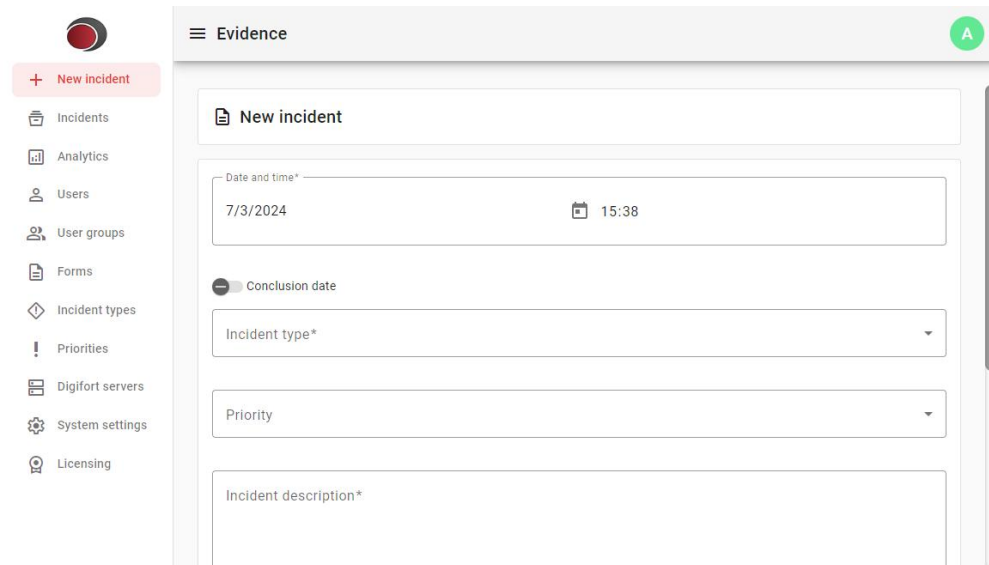
XIV

14 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.

14.1 Registering incidents

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

The screenshot shows the 'Evidence' application interface. On the left is a side menu with various options, including 'New incident' which is highlighted in red. The main content area is titled 'Evidence' and contains a 'New incident' form. The form has several fields: 'Date and time*' with a date picker set to '7/3/2024' and a time picker set to '15:38'; 'Conclusion date' with a toggle switch; 'Incident type*' with a dropdown menu; 'Priority' with a dropdown menu; and 'Incident description*' with a text area. A green 'A' icon is visible in the top right corner of the application header.


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.
- **Conclusion date:** You can optionally assign the incident conclusion date during completion, if it is known. Otherwise, it will be empty.
- **Incident type:** When selecting an item, the custom form fields associated with the incident type, if any, will be displayed.
- **Priority:** Priority of the incident. This field will be disabled if a priority is associated with the selected incident type.
- **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 [Incident view page](#).

14.2 Searching for incidents

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

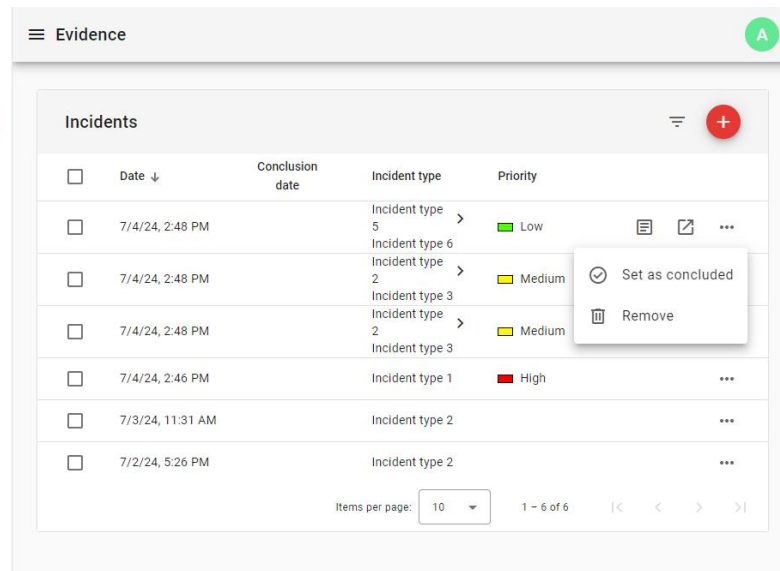
This page lists all incidents created. You can filter the list of incidents by clicking the button . The filter menu will appear on the right. Select the desired filters and click the button **Apply filter**.

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](#).

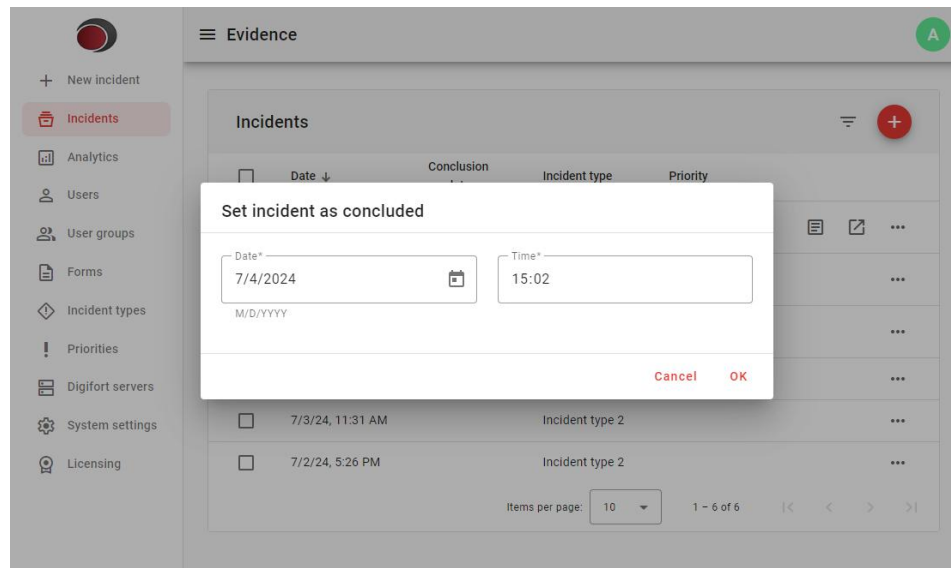
14.2.1 Marking incidents as concluded

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**.

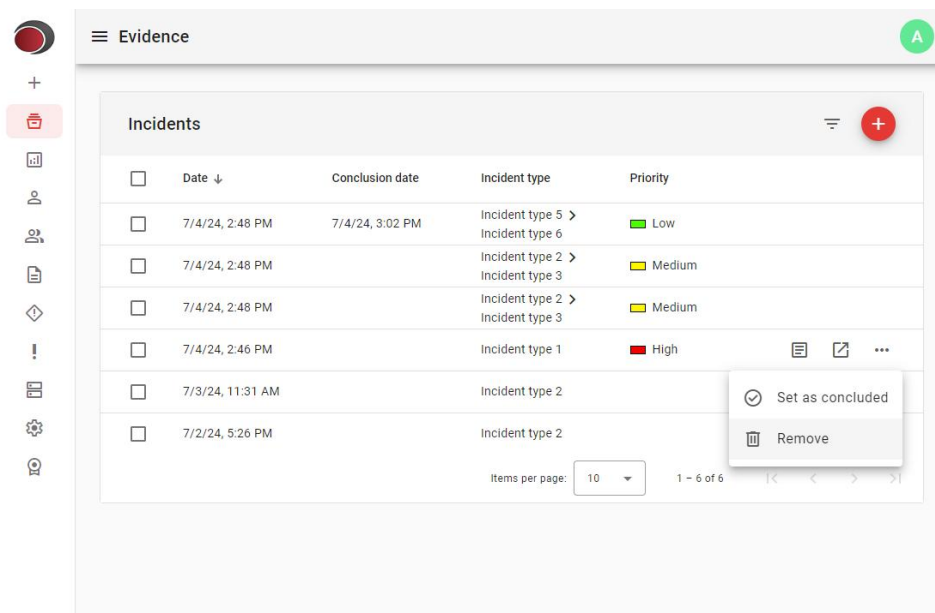


A window will open to set the date and time.

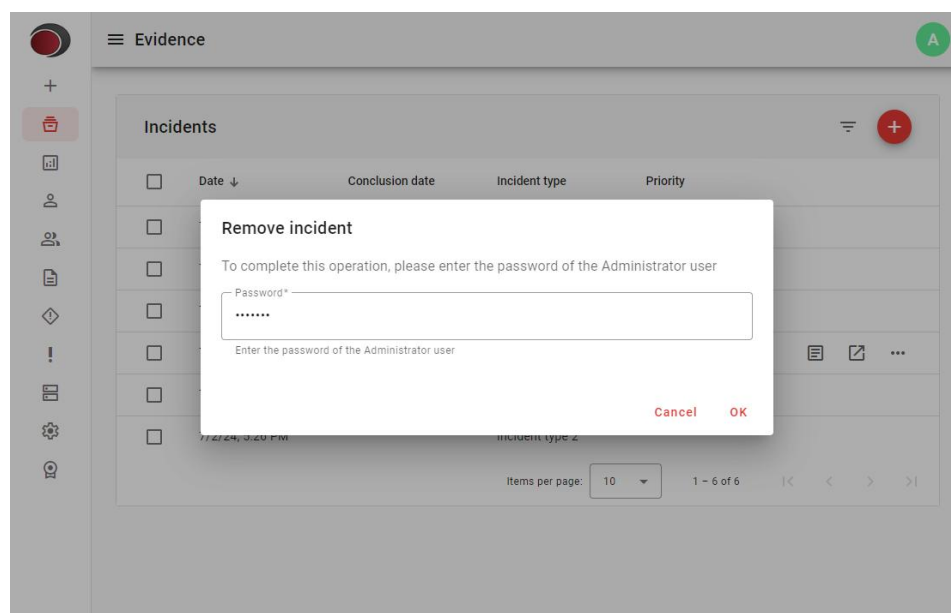


14.2.2 Deleting incidents

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

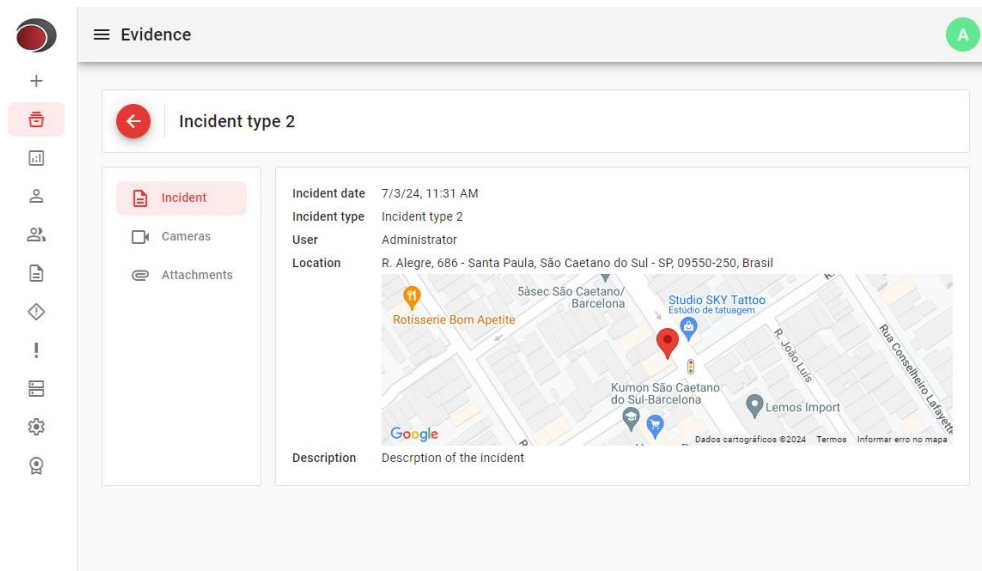


The system will request the **Administrator** user password.



14.3 Viewing incidents

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



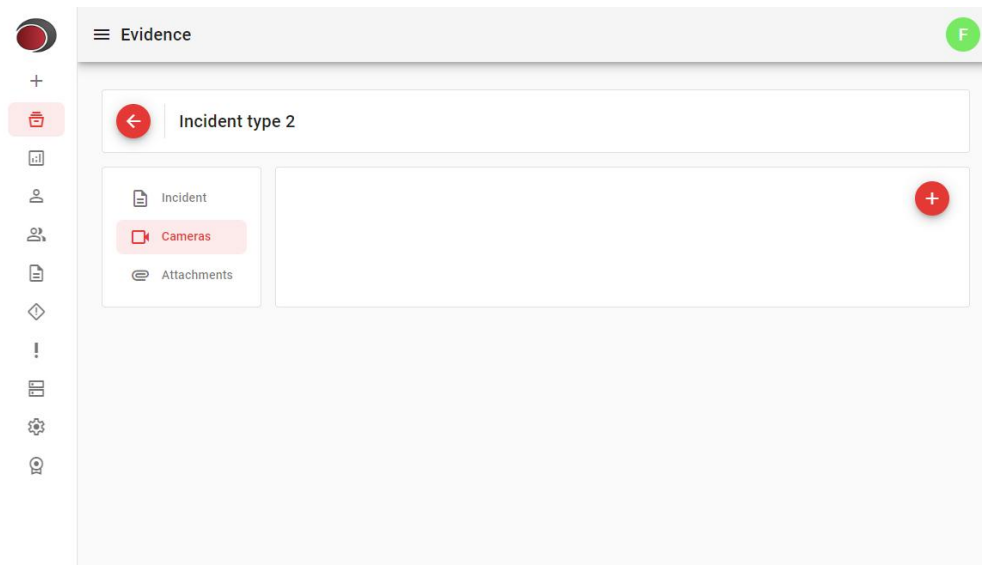
14.3.1 Managing cameras


Videos of cameras can be imported from Digifort automatically by simply selecting the desired server and cameras.

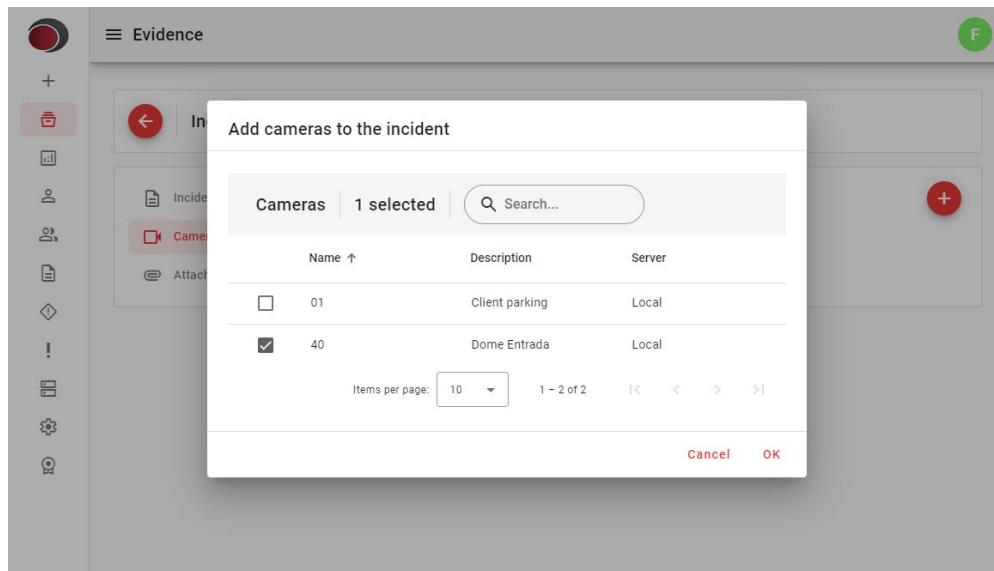
The system will start a process of importing the camera video in parallel in .mp4 format. The user will be able to leave the page while the video is being imported.

14.3.1.1 Adding cameras to incidents

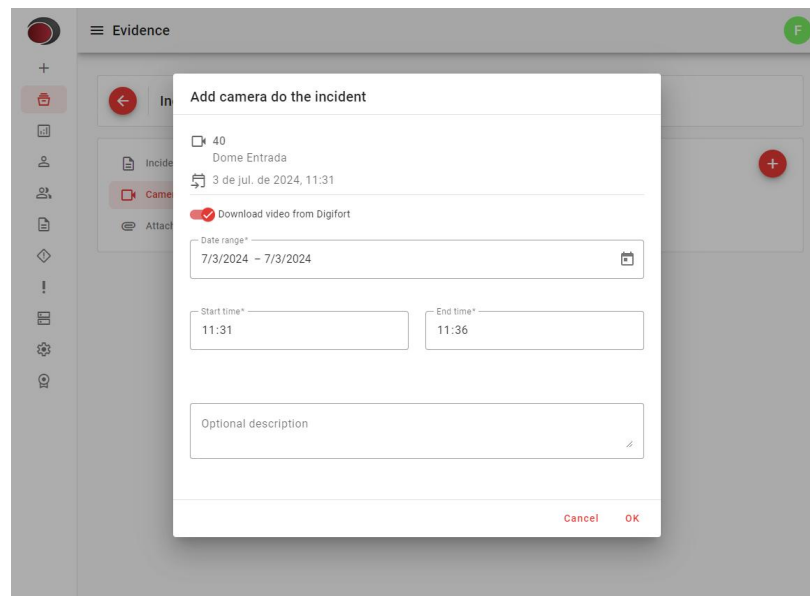
To add cameras to the incident, click the Cameras button in the side menu.



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](#).



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



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.

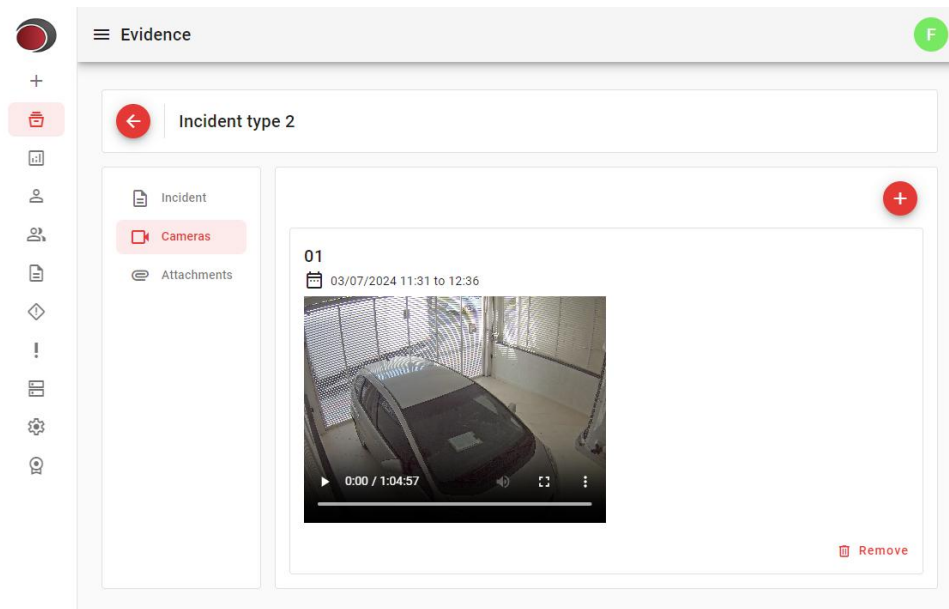
! Important

- 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.

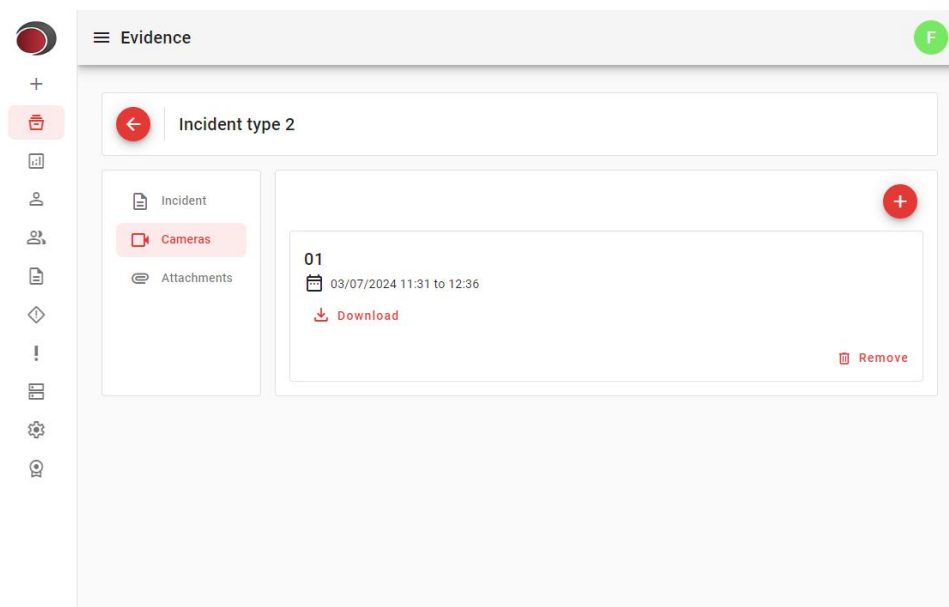
14.3.1.2 Viewing cameras

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

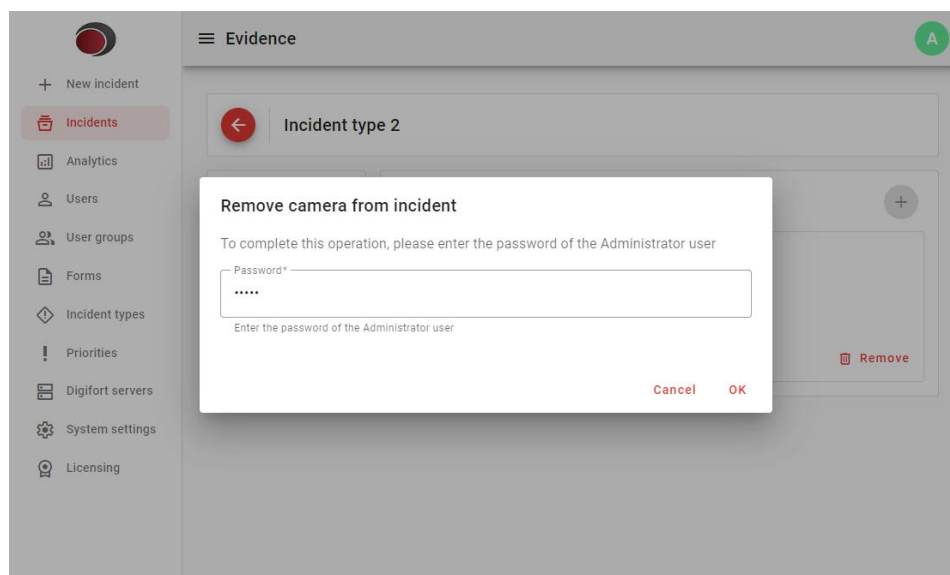


14.3.1.3 Deleting cameras

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



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

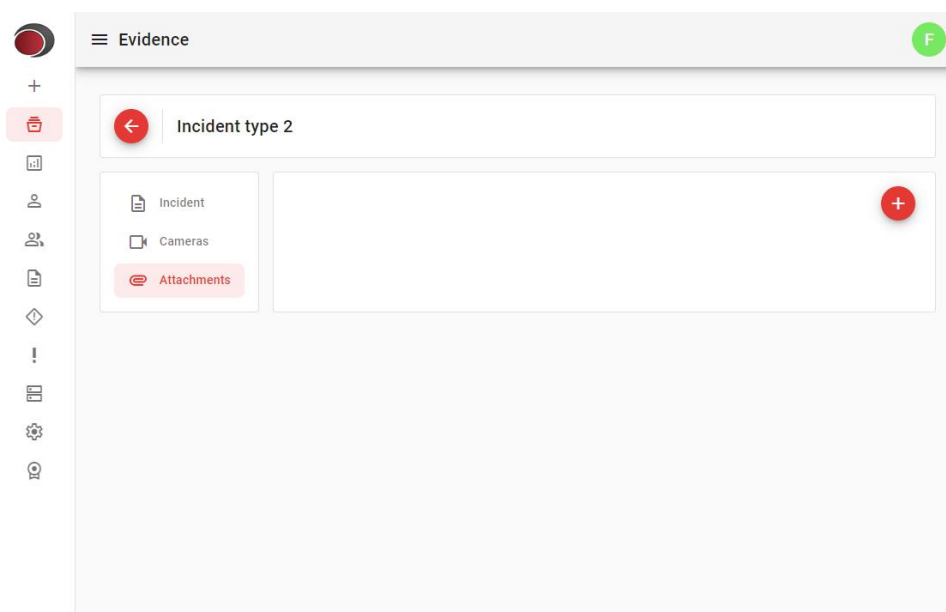


14.3.2 Managing attachments

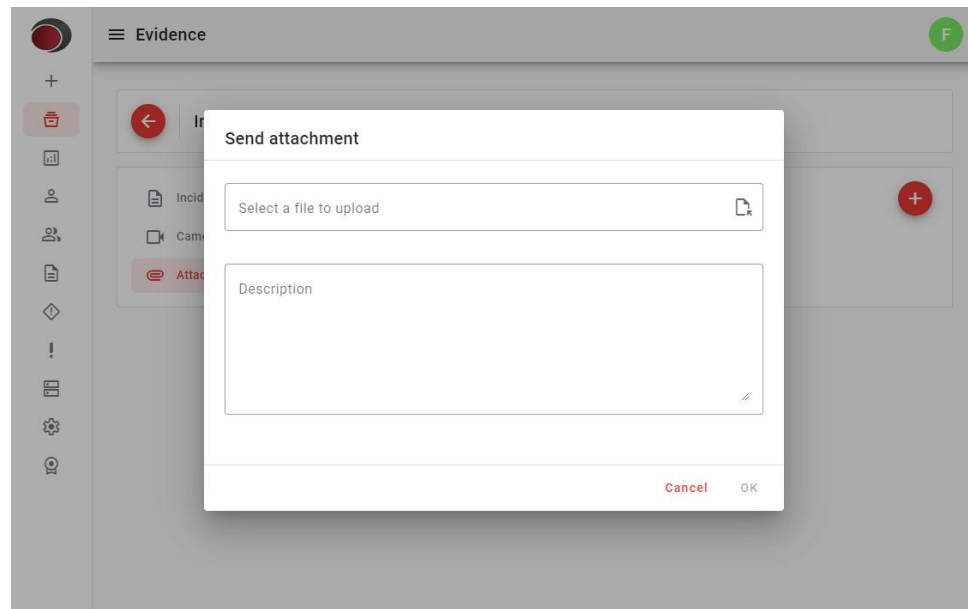
Attachments are files that can be added to incidents, such as documents, images and videos.

14.3.2.1 Adicionando anexos

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

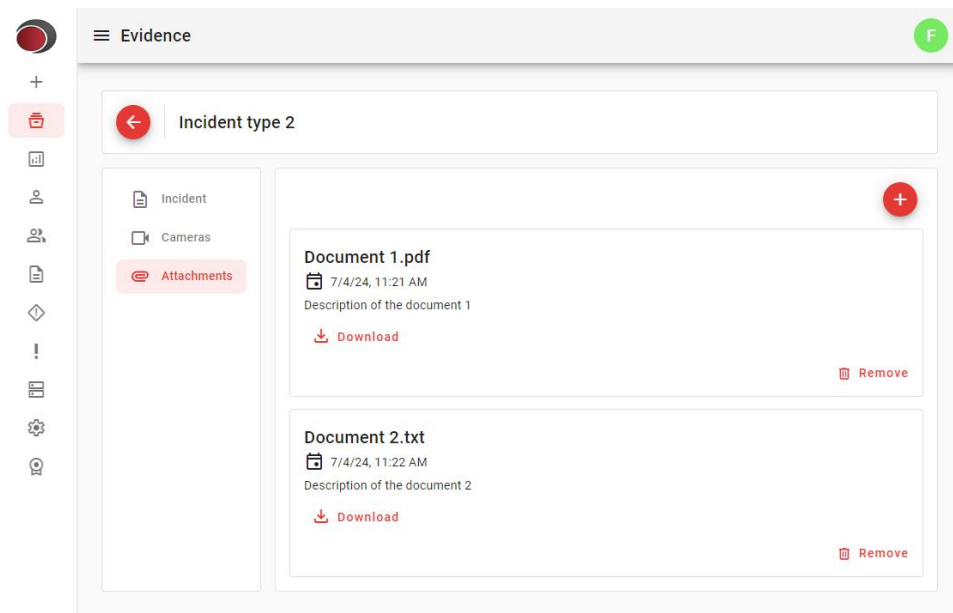


Once done, click the button. . A screen will appear to select the file and add an optional description.



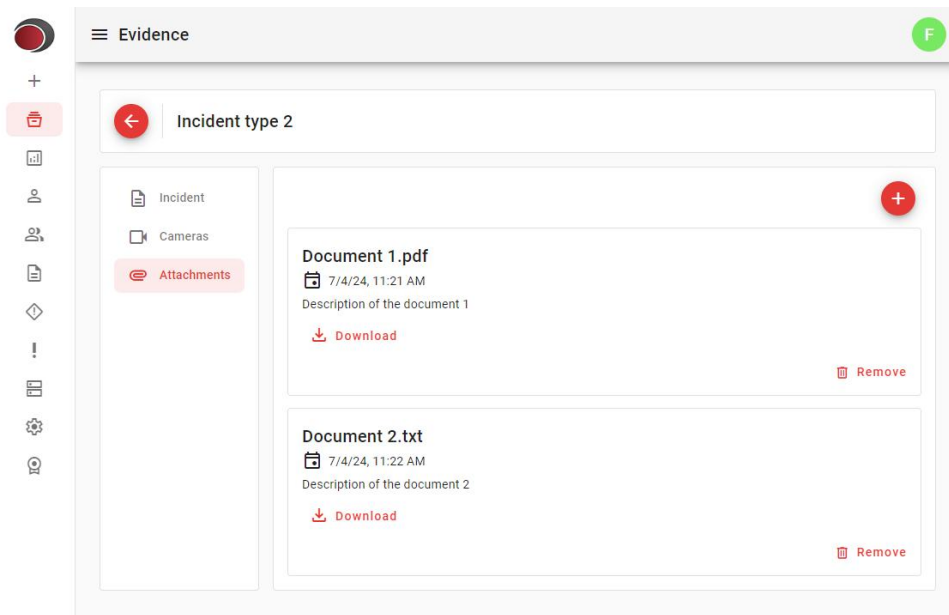
14.3.2.2 Downloading attachments

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

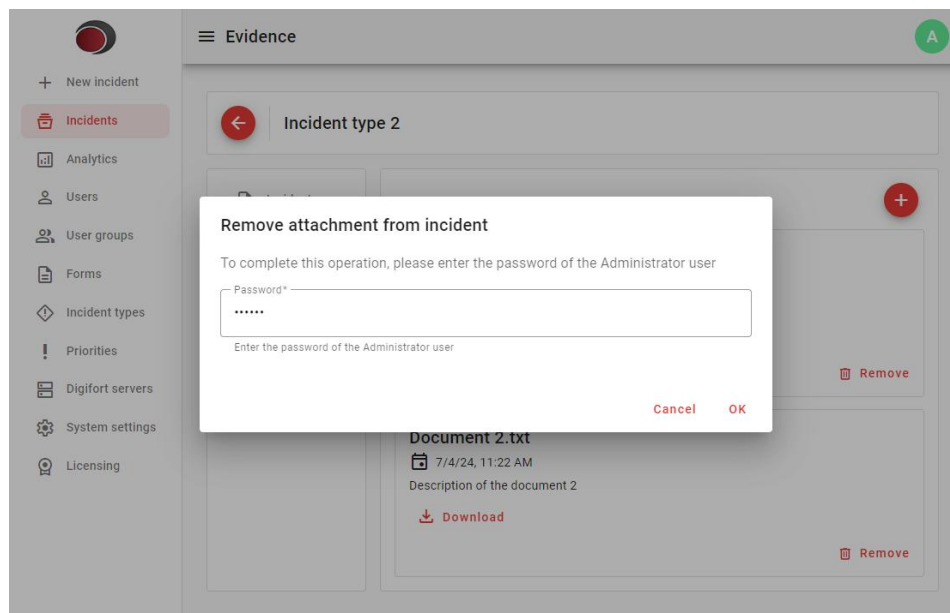


14.3.2.3 Deleting attachments

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



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



Chapter



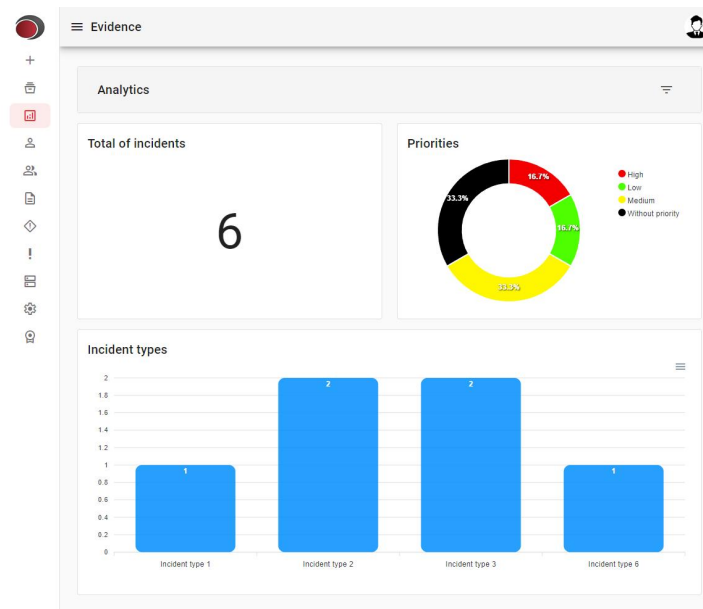
XV

15 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.

15.1 Accessing the analytics module

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



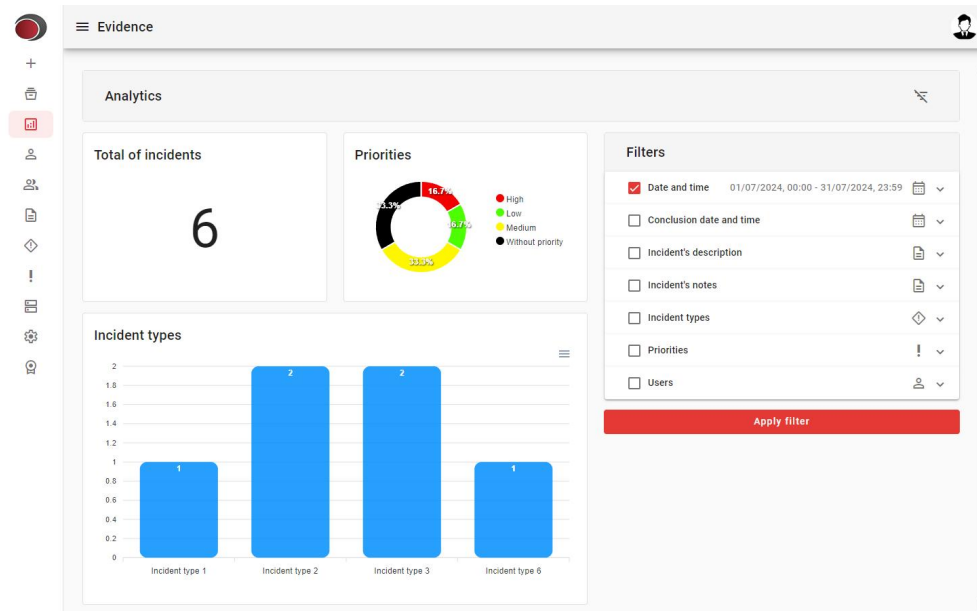
This dashboard is divided into 3 areas:

- **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.

15.2 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  .



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