NIS Incident Notification Platform

Release 0.5.15

NC3-LU

Jun 08, 2026

Technical considerations

1 Prerequisites

1.1 Software

Generally speaking, requirements are the following:

- A GNU/Linux distribution. Tested on Debian Bookworm and Ubuntu 22.04.3 LTS;
- Python version >= 3.10. Tested with Python 3.11 and 3.12;
- A PostgreSQL server for persistent storage. Tested with PostgreSQL 15.3 and 15.5;
- An email server — outgoing email;
- A cron daemon — scheduled tasks.

Postfix, or an equivalent software, is required for the email notifications.

For the Web server you can use Gunicorn, uWSGI, Apache or Nginx.

1.2 Hardware

The Django application is designed to operate efficiently, and it can run seamlessly on a Raspberry Pi when paired with Gunicorn and either Nginx or Apache to handle request proxying. It is advisable to allocate ample memory and disk space, particularly for the database, especially when it shares the same server. This proactive approach ensures smoother performance and mitigates potential resource constraints.

A decent configuration for a server would be:

- number of vCPU: 4;
- RAM (GB): 4;
- HDD (GB): 20.

The application will function seamlessly with these settings. Moreover, these values are relatively low when considering the capacity of modern servers.

1.3 Network

The deployment on the different servers requires an Internet connection since the updates are retrieved from the GitHub repository.

2 Installation

This section covers the installation steps of the sofware.

2.1 Containerized installation

You can, optionnally, create a LXC container.

```
$ lxc launch ubuntu:23.10 SERIMA --storage your-storage
$ lxc exec SERIMA -- /bin/bash
```

2.2 System packages

```
$ sudo apt install gettext curl npm postfix
```

2.3 Poetry

```
$ curl -sSL https://install.python-poetry.org | python3 -
```

at the end of the *~/.bashrc* file add the line:

```
$ export PATH="/root/.local/bin:$PATH"
```

2.4 PostgreSQL

Install PostgreSQL, the version provided by default for your GNU/Linux distribution.

```
$ sudo apt-get install postgresql
```

Create a database, database user:

```
$ sudo -u postgres createuser <username>
$ sudo -u postgres createdb <database>
$ sudo -u postgres psql
psql (15.6 (Debian 15.6-0+deb12u1))
Type "help" for help.
postgres=# alter user <username> with encrypted password '<password>';
ALTER ROLE
postgres=# grant all privileges on database <database> to <username>;
GRANT
postgres=# ALTER DATABASE <database> OWNER TO <username>;
GRANT
```

2.5 SERIMA

```
git clone https://github.com/informed-governance-project/SERIMA.git
cd SERIMA
git submodule update --init --recursive
npm install
# Copy the config and adjust the DB connection and the other settings:
cp governanceplatform/config_dev.py governanceplatform/config.py
poetry install
poetry shell
python manage.py migrate
python manage.py collectstatic
python manage.py compilemessages
```

2.5.1 Theme

In this case, the theme (CSS, icons, etc.) of the sofware will be under the `theme` folder as a Git submodule. You can replace it by your own. Currently two themes are available:

- https://github.com/informed-governance-project/default-theme (default theme, used for ILR Luxembourg)
- https://github.com/informed-governance-project/serimabe-theme (theme for IBPT.be)

If you do not want to use the default theme, do not clone the main repository with the submodule.

2.5.2 Configuration

In the configuration file `governanceplatform/config.py` , ensures that you have configured:

- `PUBLIC_URL`
- `ALLOWED_HOSTS`
- `OPERATOR_CONTACT` and `REGULATOR_CONTACT`
- `DATABASES`
- `HASH_KEY` and `SECRET_KEY`
- `DEBUG`: must be set to `False` in a production environment
- `CSRF_TRUSTED_ORIGINS`
- `EMAIL_SENDER`
- etc.

If `DEBUG` is set to `True` emails generated by SERIMA won't be sent but stored in a dedicated folder at the root of the project.

You **must really** set **your** secret keys.

Here is an example for the Fernet hash key (`HASH_KEY`):

```
$ python -c 'from cryptography.fernet import Fernet; print(Fernet.generate_key())'
b'Xaj5lFGAPiy2Ovzi4YmlWh-s4HHikFV4AswilOPPYN8='
```

For the Django secret key (`SECRET_KEY`), you can for example do:

```
$ python -c 'import secrets; print(secrets.token_hex())'
9cf5c7b13e469e6f6a9403b33410589031cfe927df6471a1cbdef1d4deb57c37
```

2.6 Create the PlatformAdmin user

```
$ python manage.py createsuperuser
```

This user will be able to create RegulatorAmin users via the Web interface of SERIMA.

The first PlatformAdmin user will also have to configure the `domain name` and `display name` of the application:

This step is essential for ensuring the proper functioning of the platform's email sending, such as for password recovery purposes, as well as for generating QR codes for two-factor authentication (2FA).

2.7 Launch the Django application

```
poetry run python manage.py runserver 127.0.0.1:8000
```

Of course, do not do that for a production environment.

2.8 Scheduled tasks

Configure the cron tasks:

```
0 * * * * cd /<-application-path->/SERIMA/  ; python manage.py runscript workflow_update_
↪status
0 * * * * cd /<-application-path->/SERIMA/  ; python manage.py runscript email_reminder
```

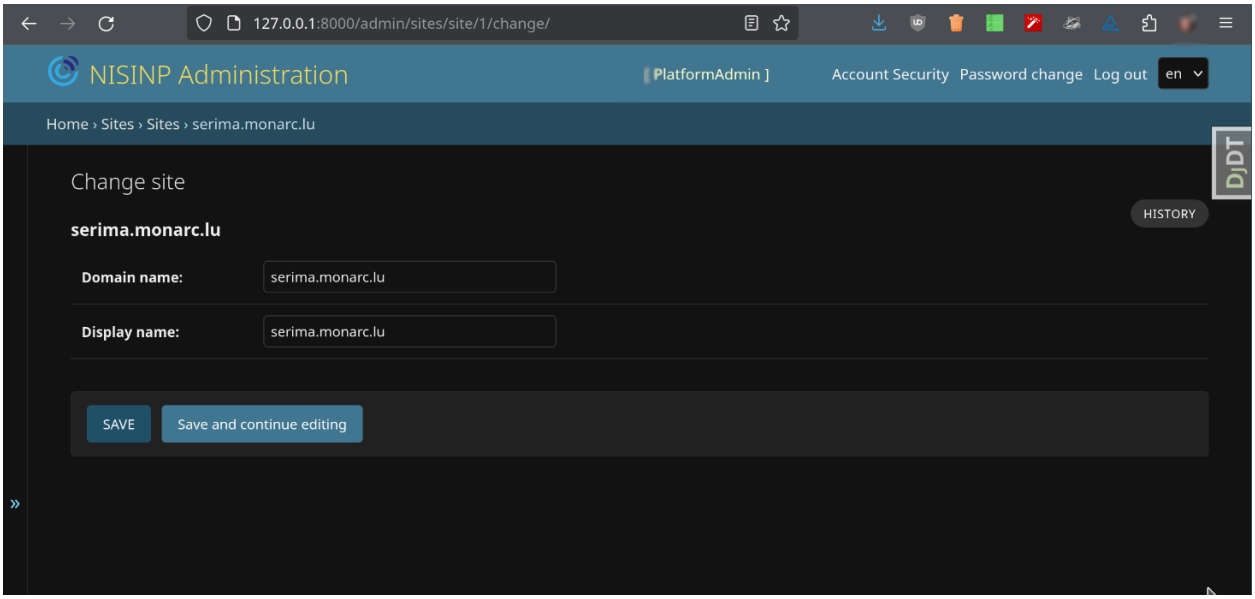


Fig. 2.1: Django application - Sites configuration.

The best is to use the Python executable in the virtual environment.

2.9 Apache

The `mod_wsgi` package provides an Apache module that implements a WSGI compliant interface for hosting Python based web applications on top of the Apache web server. Install Apache and this module.

```
$ sudo apt install apache2 libapache2-mod-wsgi-py3
```

Note

Only in the case you can not use the version of mod_wsgi from your GNU/Linux distribution:

```
$ sudo apt install apache2 apache2-dev # apxs2
$ wget https://github.com/GrahamDumpleton/mod_wsgi/archive/refs/tags/5.0.0.tar.gz
$ tar -xzvf 5.0.0.tar.gz
$ cd mod_wsgi-5.0.0/
$ ./configure --with-apxs=/usr/bin/apxs2 --with-python=/home/<user>/.pyenv/shims/
↪python
$ make
$ sudo make install
```

Then in `/etc/apache2/apache2.conf` add the lines:

```
LoadFile /home/<user>/.pyenv/versions/3.11.0/lib/libpython3.11.so
LoadModule wsgi_module /usr/lib/apache2/modules/mod_wsgi.so
```

Restart Apache:

```
sudo systemctl restart apache2.service
```

For the next steps you must have a valid domain name.

2.9.1 Example of VirtualHost configuration file

VirtualHost for a reverse proxy server:

```
<VirtualHost *:80>
    ServerAdmin info@incidents.serima.lu
    ServerName incidents.serima.lu

    DocumentRoot /var/www/html
    RewriteEngine on
    RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI} [END,NE,R=permanent]
</VirtualHost>

<VirtualHost *:443>
    ServerAdmin info@incidents.serima.lu
    DocumentRoot /var/www/html
    ServerName incidents.serima.lu

    # main configuration
    RewriteEngine On
    RewriteCond %{REQUEST_METHOD} !^(GET|POST|PUT|PATCH|DELETE|HEAD)
    RewriteRule .* - [R=405,L]

    SSLProxyEngine On
    ProxyPreserveHost On
    ProxyTimeout 1800

    CustomLog ${APACHE_LOG_DIR}/incidents.serima.lu_access.log combined
    ErrorLog ${APACHE_LOG_DIR}/incidents.serima.lu_error.log

    SSLEngine on
    SSLCertificateFile /etc/ssl/private/incidents_serima_lu/incidents_serima_lu.cer
    SSLCertificateChainFile /etc/ssl/private/incidents_serima_lu/incidents_serima_lu_
↪interm.cer
    SSLCertificateKeyFile /etc/ssl/private/incidents_serima_lu/incidents.serima_lu.key

    ProxyPass / http://web01.private.serima.lu/
    ProxyPassReverse / http://web01.private.serima.lu/
</VirtualHost>
```

Then configure HTTPS properly. If you want to use Let's Encrypt:

```
sudo apt install certbot python3-certbot-apache
sudo certbot certonly --standalone -d incidents.serima.lu
sudo a2enmod rewrite
sudo systemctl restart apache2.service
```

Verify that the certificate will be automatically updated:

```
$ cat /etc/letsencrypt/renewal/incidents.serima.lu.conf
# Options used in the renewal process
[renewalparams]
account = <-account-id->
authenticator = apache
server = https://acme-v02.api.letsencrypt.org/directory
```

VirtualHost for the application:

```
<VirtualHost *:80>
    ServerName web01.private.serima.lu
    ServerAdmin info@incidents.serima.lu

    WSGIDaemonProcess serima python-path=/home/USER/SERIMA:/home/USER/.cache/pypoetry/
↪virtualenvs/governanceplatform-AGxECetm-py3.10/lib/python3.10/site-packages/
    WSGIProcessGroup serima
    WSGIScriptAlias / /home/USER/SERIMA/governanceplatform/wsgi.py

    <Directory "/home/USER/SERIMA/governanceplatform/">
        <Files "wsgi.py">
            Require all granted
        </Files>
        WSGIApplicationGroup %{GLOBAL}
        WSGIPassAuthorization On

        Options Indexes FollowSymLinks
        Require all granted
    </Directory>

    Alias /static /home/USER/SERIMA/governanceplatform/static
    <Directory /home/USER/SERIMA/static>
        Require all granted
    </Directory>

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    LogLevel warn
    CustomLog ${APACHE_LOG_DIR}/incidents.serima.lu_access.log combined
    ErrorLog ${APACHE_LOG_DIR}/incidents.serima.lu_error.log
</VirtualHost>
```

3 Updating the application

All you have to do is:

```
$ cd SERIMA/
$ ./contrib/update.sh {APP_TAG} {THEME_TAG}
```

Replace *{APP_TAG}* and *{THEME_TAG}* with the Git tag or branch you want to deploy for the application and theme respectively. If omitted, both default to *master*.

Or manually:

```
$ cd SERIMA/
$ git pull origin master --tags
$ npm ci
$ poetry install
$ poetry run python manage.py collectstatic
```

(continues on next page)

(continued from previous page)

```
$ poetry run python manage.py migrate
$ poetry run python manage.py compilemessages
$ poetry run python manage.py update_group_permissions
```

Finally, restart Apache:

```
$ sudo systemctl restart apache2.service
```

4 Modules

Main components of the software:

- the governance platform (settings, administration panel and core components). The governance platform provides access to the various modules hosted on the platform;
- the Incident Notification module (models and views related to the incidents notifications);
- the API.

4.1 Incident Notification

The Web interface used to report and track incidents.

4.2 API

See the section dedicated to the API (*OpenAPI specicification* (page 10)).

5 Architecture

5.1 High level architecture

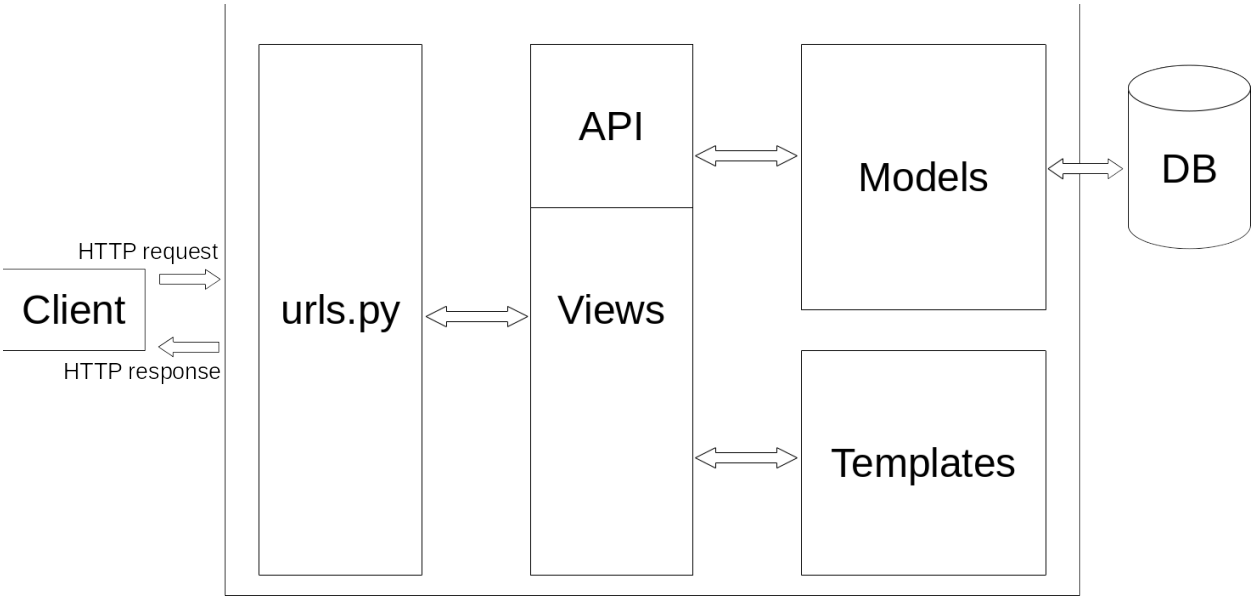


Fig. 5.1: High level architecture of a Django application.

5.2 Models

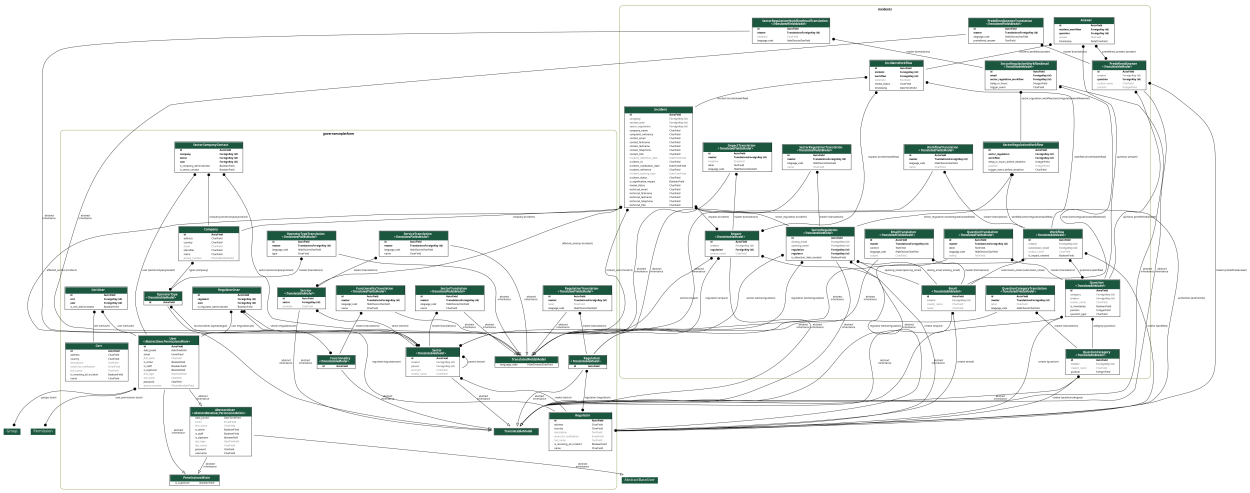


Fig. 5.2: Business related models for the *incidents* and *governance* modules.

6 API v1

The OpenAPI specicification should be avaible with Swagger UI at the address: http://127.0.0.1:8000/api/v1/swagger-ui/

6.1 OpenAPI specicification

7 Security Model

First, an overview of the security policy.

7.1 Security policy

7.1.1 Supported Versions

Last stable version of this software always provides security updates. There will be no security patches for other releases (tagged or not).

7.1.2 Reporting a Vulnerability

If you think you have found a potential security issue, do not open directly a public GitHub issue. Please email us. You can contact opensource@nc3.lu

You can also specify how you would like to be credited for your finding (commit message or release notes for the new release). We will respect your privacy and will only publicize your involvement if you grant us permission.

7.2 Source code

CodeQL is used to discover vulnerabilities across the **codebase**.

Tools such as *pyupgrade*, *pip-audit*, *GitHub Dependabot* and secret scanning are used to check for vulnerabilities in project **dependencies**. Each commit is checked on GitHub. The same kind of tests are performed locally thanks to pre-commit (https://pre-commit.com).

Code **quality** is verified with tools such as *black*, *flake8* and *mypy*.

Public security issues are listed here (https://github.com/informed-governance-project/SERIMA/issues?q=is%3Aissue+label%3Asecurity+).

7.3 Audit on the source code

7.4 Authentication

Two factor authentication is available and mandatory for the admin access.

8 Permissions and roles

8.1 Summary

The available roles are:

- PlatformAdmin (Django super admin)
- RegulatorAdmin
- RegulatorUser
- ObserverAdmin
- ObserverUser
- OperatorAdmin
- OperatorUser

8.2 Permissions

8.2.1 PlatformAdmin (Django super admin)

The first platform administrator must be created with the Django command:

```
$ python manage.py createsuperuser
```

The platform administrator is able to configure the `Site` section of the Django application. The platform administrator is able to create and manage other platform administrators. The platform administrator grants access to the governance platform to regulators and observers. A regulator, also known as competent authority, is a public organisation responsible as per the law for the supervision of a or multiple regulations. An observer is an organisation having a role defined by the law. He gets information to conduct his missions on a read only modus. The platform administrator defines the rules used by the automatic information forward to the observers. The platform administrator creates the regulations on the platform and assign them to the regulators. The platform administrator defines the operator categories. These are characteristics of the operators e.g. public/private. These categories are made available to the regulators, who can use them to sort the operators.

Each regulator, who wants to use the incident notification module, should ask the platform administrator to configure: - the regulator (as organization) - the first regulator administrator - the regulations he is responsible for. - the modules from the platform to be made available.

Each observer, who wants to use the incident notification module, should ask the platform administrator to configure: - the observer (as organization) - the first observer administrator - the logic for the automatic information forward.

8.2.2 RegulatorAdmin

The regulator administrator can create other regulator administrator but also regulator users for his organization. The regulator administrator has the responsibility to configure the regulations he is responsible for. A regulation is configured using a workflow containing various reports. Each report is a collection of questions structured using the question categories. The regulator administrator has access to any item of his organization. (Unlimited view).

8.2.3 RegulatorUser

The regulator administrator, when creating a regulator user, can limit his field of responsibilities to a or various sectors. (Limited view) The regulator user can create company and create an operator administrator who is the administrator of the company (operator). The regulator user is responsible to review the deliverables sent by the operators of his sectors.

8.2.4 ObserverAdmin

The observer administrator can create other observer administrators but also observer users for his entity. The observer administrator has a read only access to the items sent to his organization.

8.2.5 ObserverUser

The observer user has a read only access to the items sent to his organization.

8.2.6 OperatorAdmin

When creating a company, the regulator has to associate it to an operator administrator. An operator administrator can create other operator administrators but also operator users for his organization.

8.2.7 OperatorUser

An operator user is responsible to deliver the required documents and information to the regulators, who are supervising him.

9 User interface

9.1 The login page

On this page you can log in or create an account in case you have to notify an incident and you don't have credentials.

If you already have an account, please use the left pane and enter your credentials (email address and password) to log in.

In case you have forgotten your password or username, please click on the link below the 'Log in' button that says '**Forgotten your password or username?**'.

If you do not have an account, please click on the '**Sign Up**' link on the left pane, or use the right pane and click on the '**Create an account**' button. Both options will take you to the account creation page.

9.2 Create an account

If you do not have an account yet, create one by using the '**Sign Up**' link on the left or the '**Create an account**' button on the right. Populate the required fields and provide a password you would like to use.

Please note that the following password restrictions apply:

- Your password can't be too similar to your other personal information.
- Your password must contain at least 8 characters.
- Your password can't be a commonly used password.

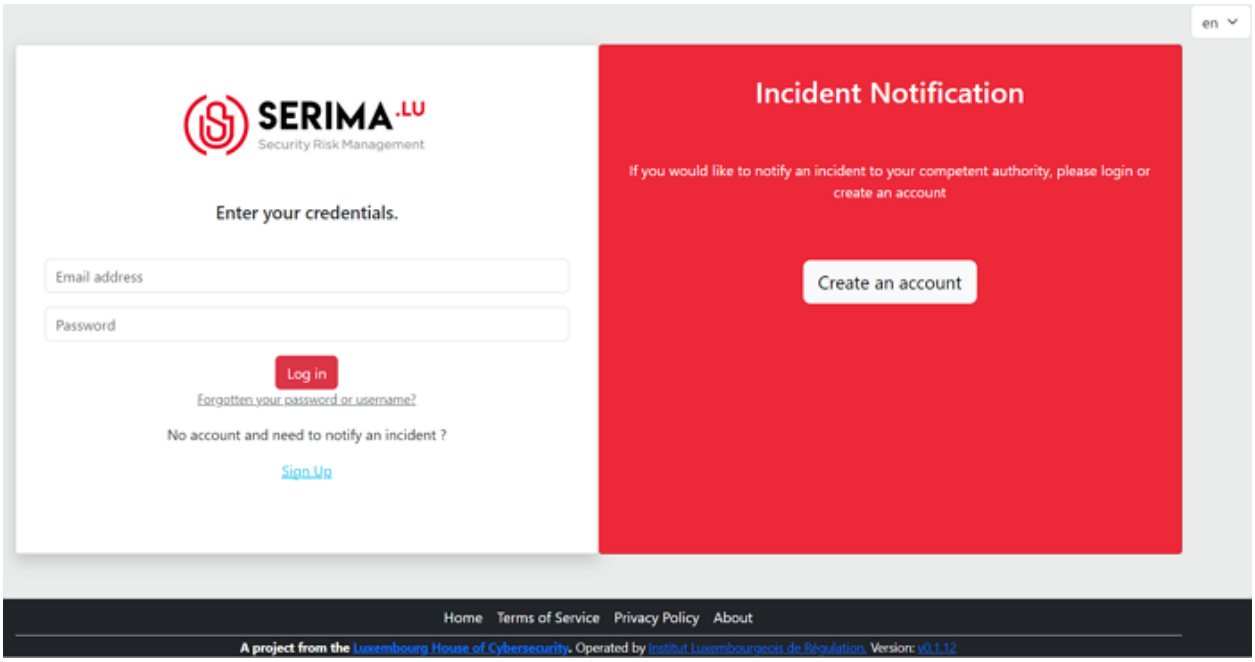


Fig. 9.1: Screenshot of the login page.

- Your password can't be entirely numeric.

9.3 Enable two-factor authentication

Once you click on '**Register**', you are logged into the SERIMA Platform. Since this is your first login, the system suggests you to enable the two-factor authentication. Click on the button '**Enable Two-Factor Authentication**'.

Follow the steps in the wizard to enable 2FA: first, click on the '**Next**' button.

Then either use your smartphone and scan the QR code from the screen or use the long character set called TOTP Secret to set up TOTP in your authenticator or password manager manually. As the last step, please enter the token (a six-digit number) into the Token field and click '**Next**'.

In case you have successfully enabled two-factor authentication, you are greeted with the below screen:

Please click on the grey button and log in again. Provide your email address and password and click on '**Log in**'. Then, open your authenticator app on your smartphone and type in the randomly generated Token and click '**Log in**'.

As an '**Operator**' or '**User**', this is your main page where you land whenever you open this application. Since this is your first login, there is no incident displayed in the incident dashboard.

The Platform is straightforward. Use the '**ILR SERIMA Platform**' link in the top-left corner to come back to the main page at any time.

In the top right-hand corner, you can see your name with a drop-down menu. If you click on the down-pointing arrow, the following dropdown menu appears:

- **Account**: you may change your first name, last name, and phone number.
- **Security**: you can change your security settings. You can create backup tokens in case you do not have any device with you (you can access your account using backup tokens). You can also disable two-factor authentication, but this is strongly not recommended.
- **Password**: you can change your password here. You must enter your old password and type in twice the new one you would like to use (please observe the restrictions on creating a new password).

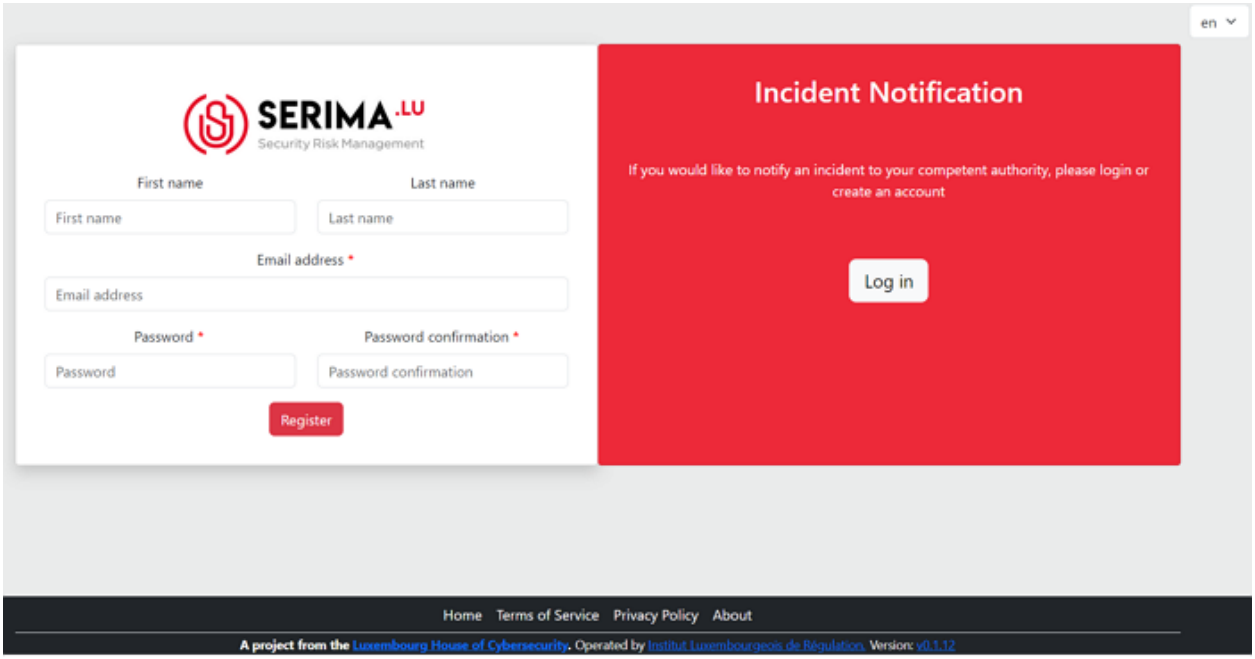


Fig. 9.2: Create an account

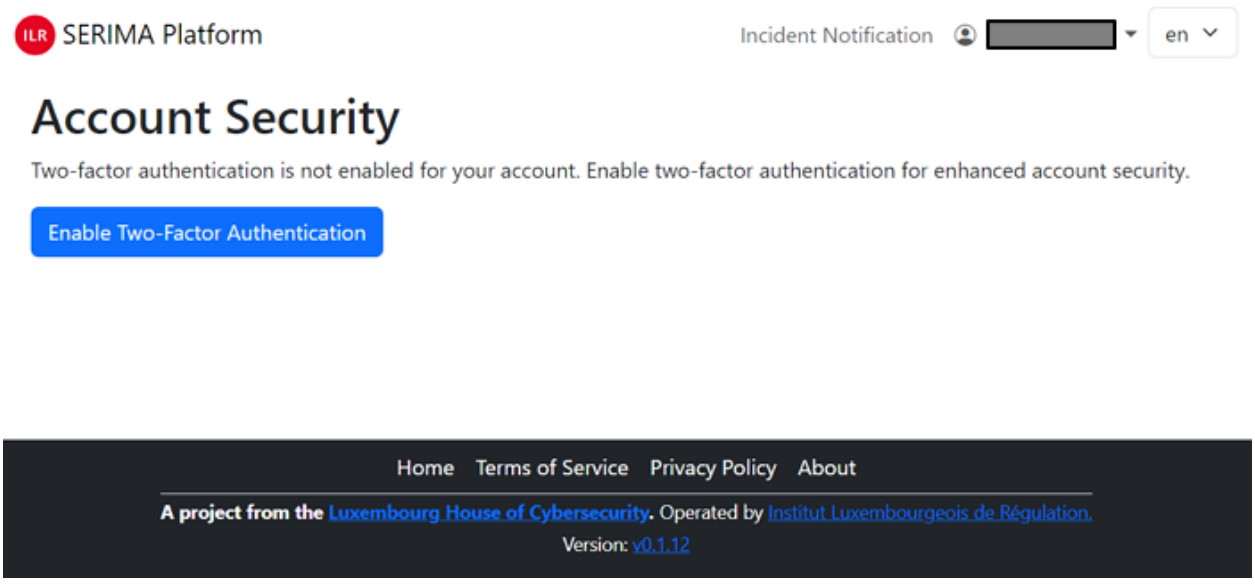


Fig. 9.3: 2FA

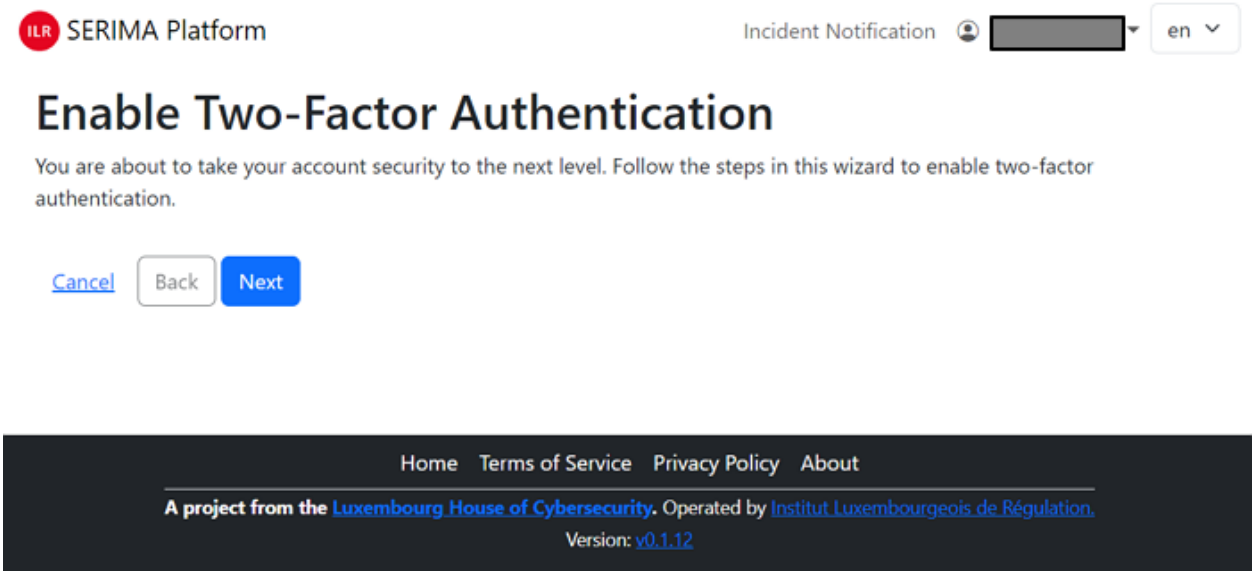


Fig. 9.4: 2FA

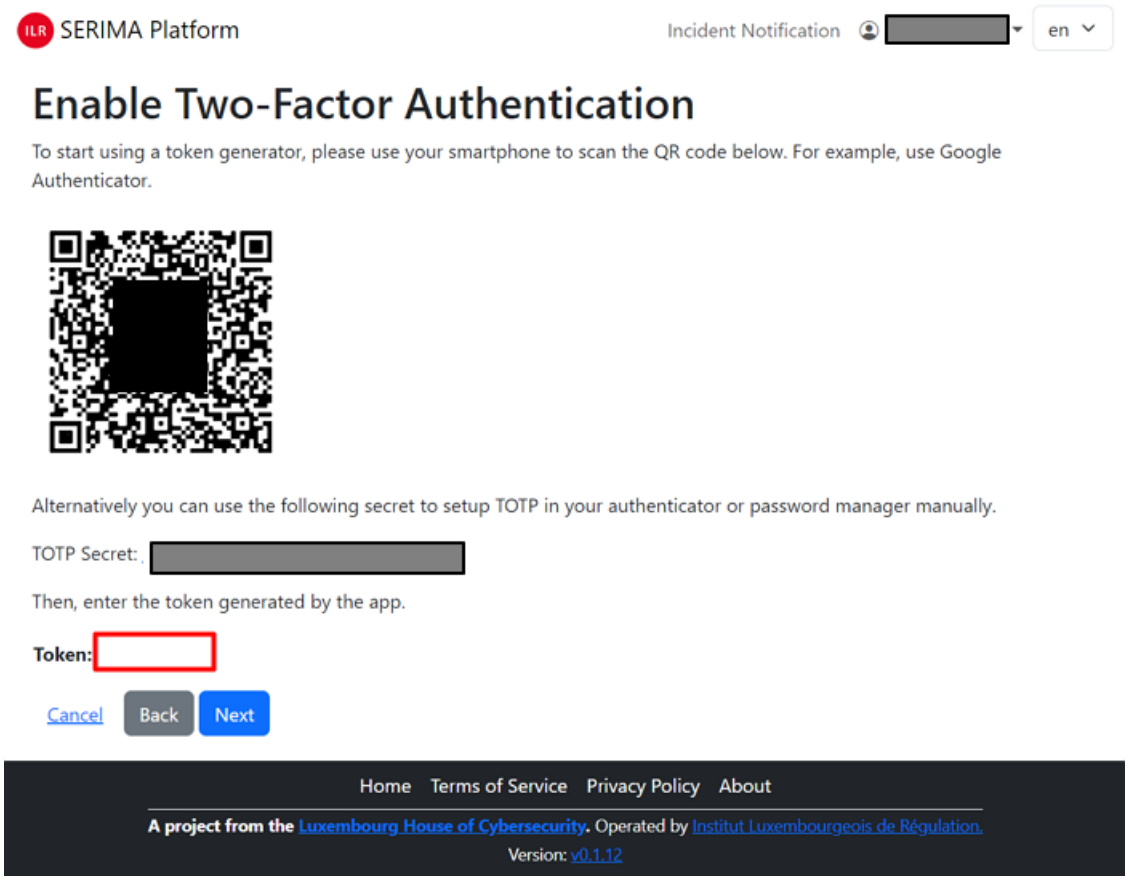


Fig. 9.5: 2FA

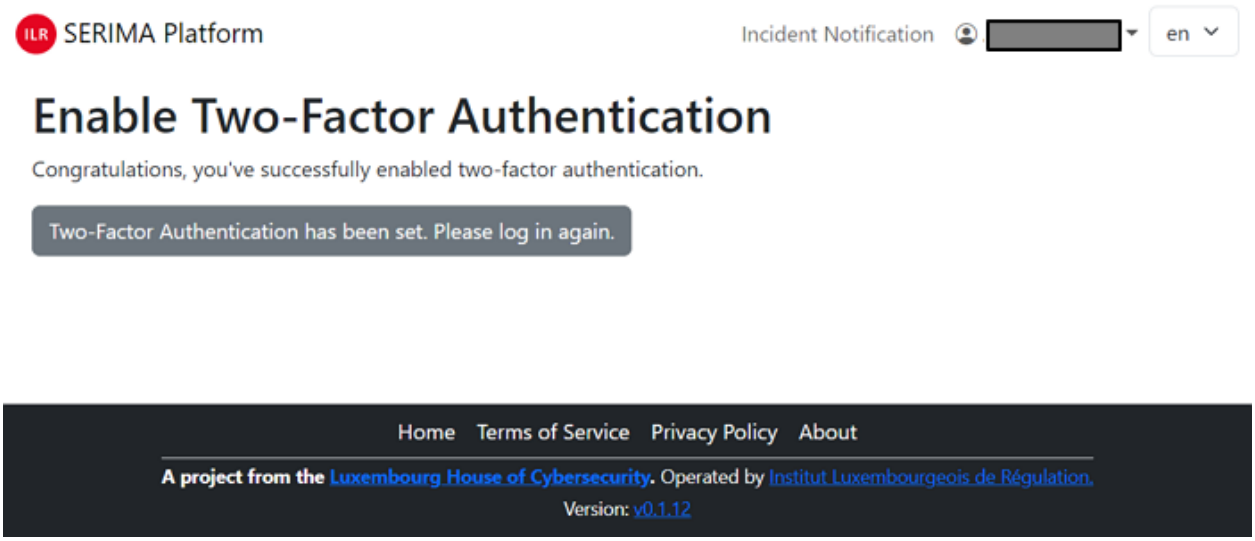


Fig. 9.6: 2FA

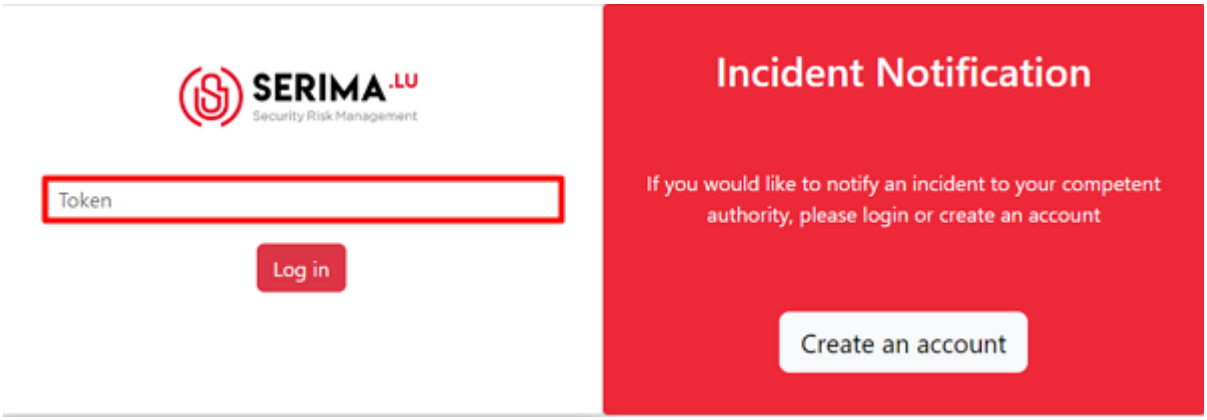
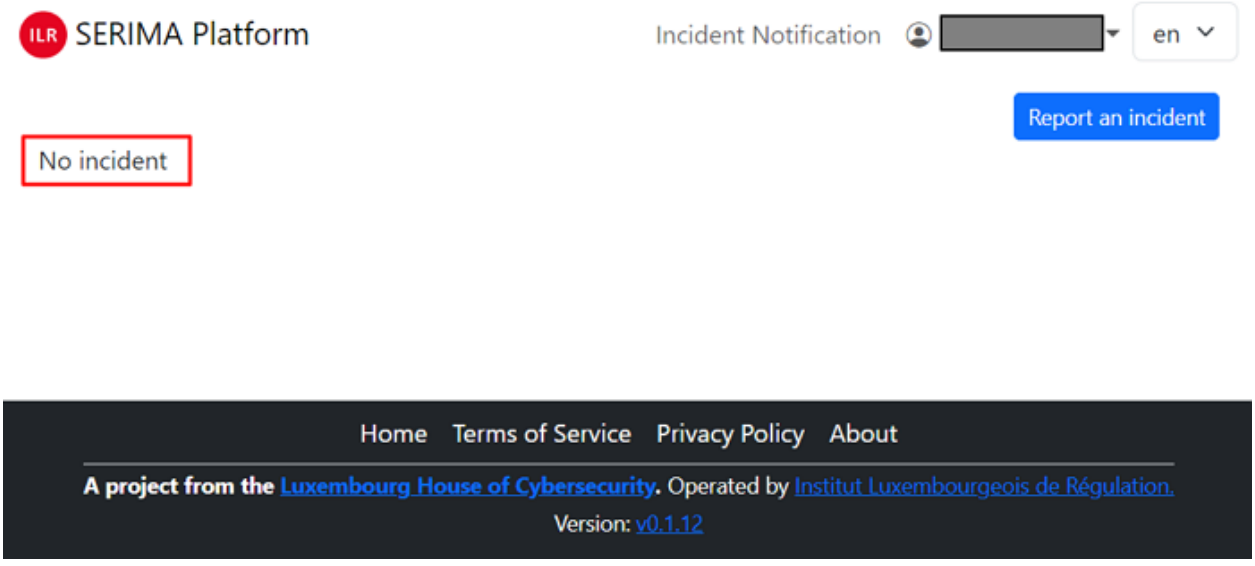
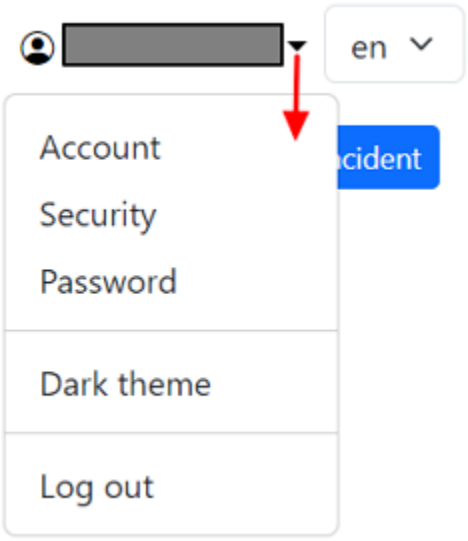
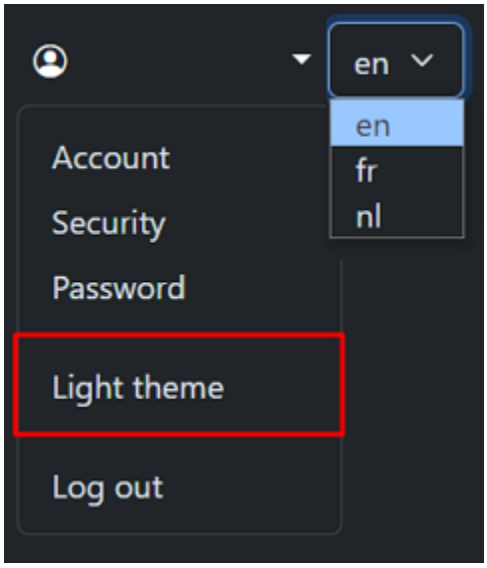


Fig. 9.7: 2FA



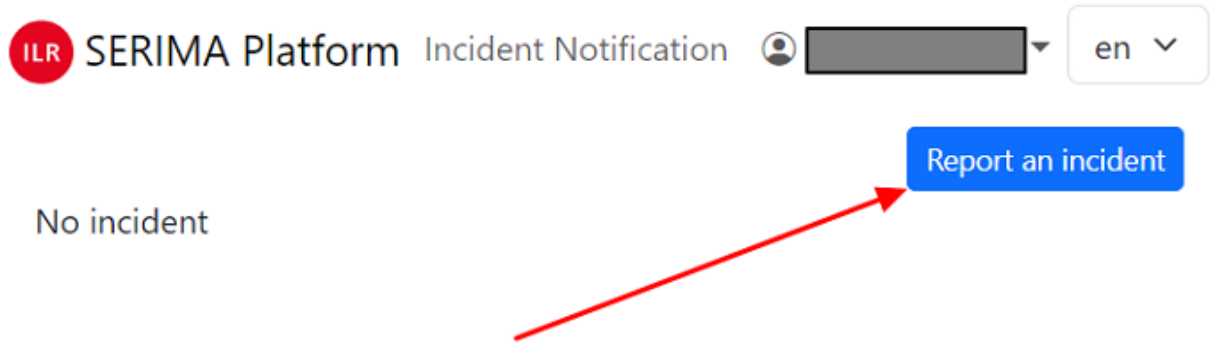

en
Account
Security
Password
Dark theme
Log out


en
en
fr
nl
Account
Security
Password
Light theme
Log out

- **Dark theme/Light theme**: you can switch between a dark and light background by using this link.
- **Log out**: use this link to log out from the application. In case you are not active, the system will log you out for security reasons.
- **Language separator**: in the top right-hand corner, you can switch between English (en), French (fr) and Dutch (nl) languages.

9.4 Report an incident

The main function of this module is to make it possible for you to report incidents. To report an incident, click on the 'Report an incident' button in the top right-hand corner:



9.4.1 Contact

The '**Contact**' form appears. Please fill in the required fields, so the authorities to whom you are sending the incident report can get back to you. The form has three main parts:

1. **Person in charge of the incident notification**: name, job title, email, telephone
2. **Technical contact** (if the same person, please activate the slider, so it will be blue)
3. **References** (Optional): Incident reference, Complaint reference

The below screenshot is only a fictitious example for demonstration purposes:

9.4.2 Regulators

The next page is the '**Regulators**'. Here, you can choose among the list items to which regulator you want to report the incident. You may choose several regulators by putting a tick mark in the checkboxes in front of the list items:

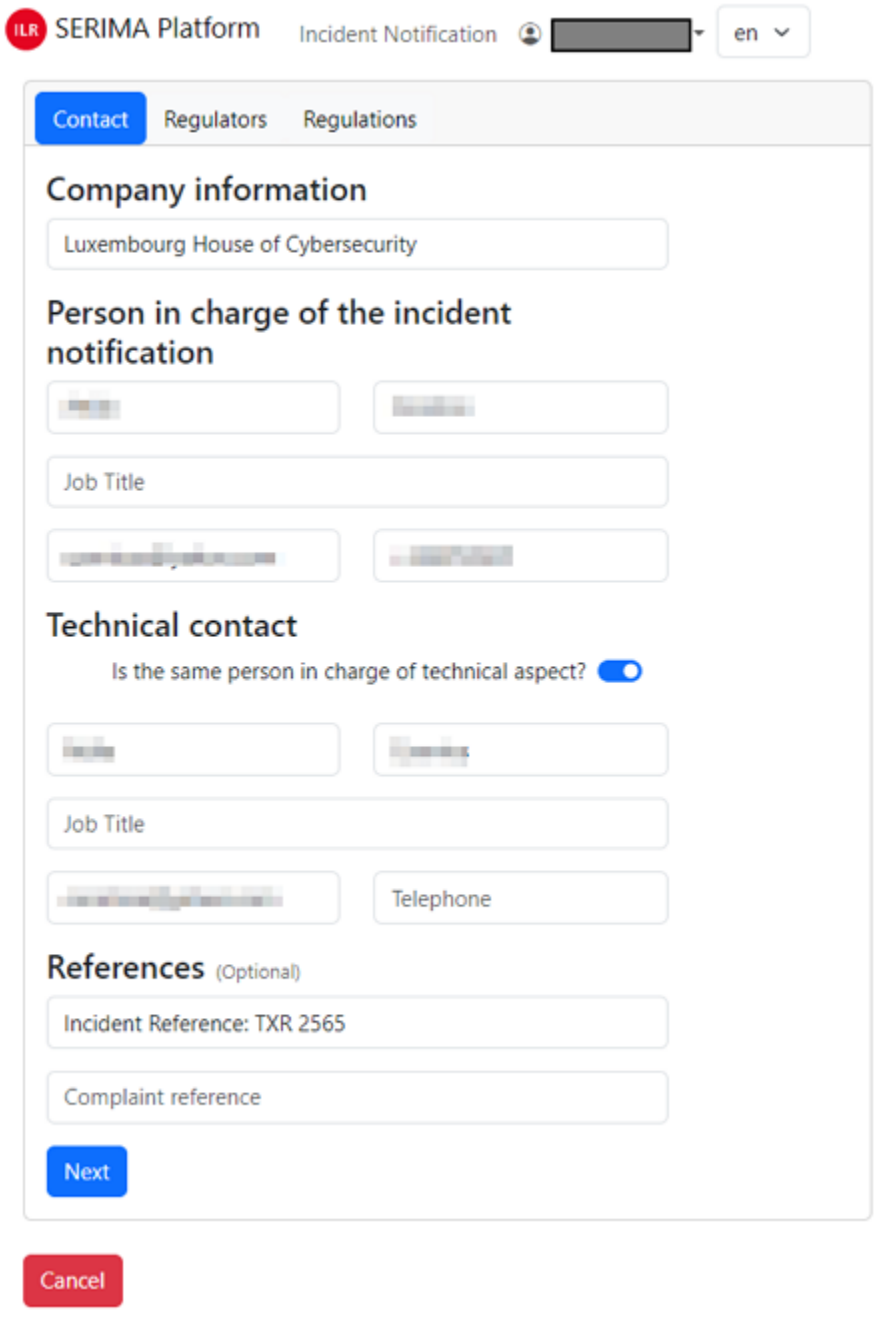
9.4.3 Regulations

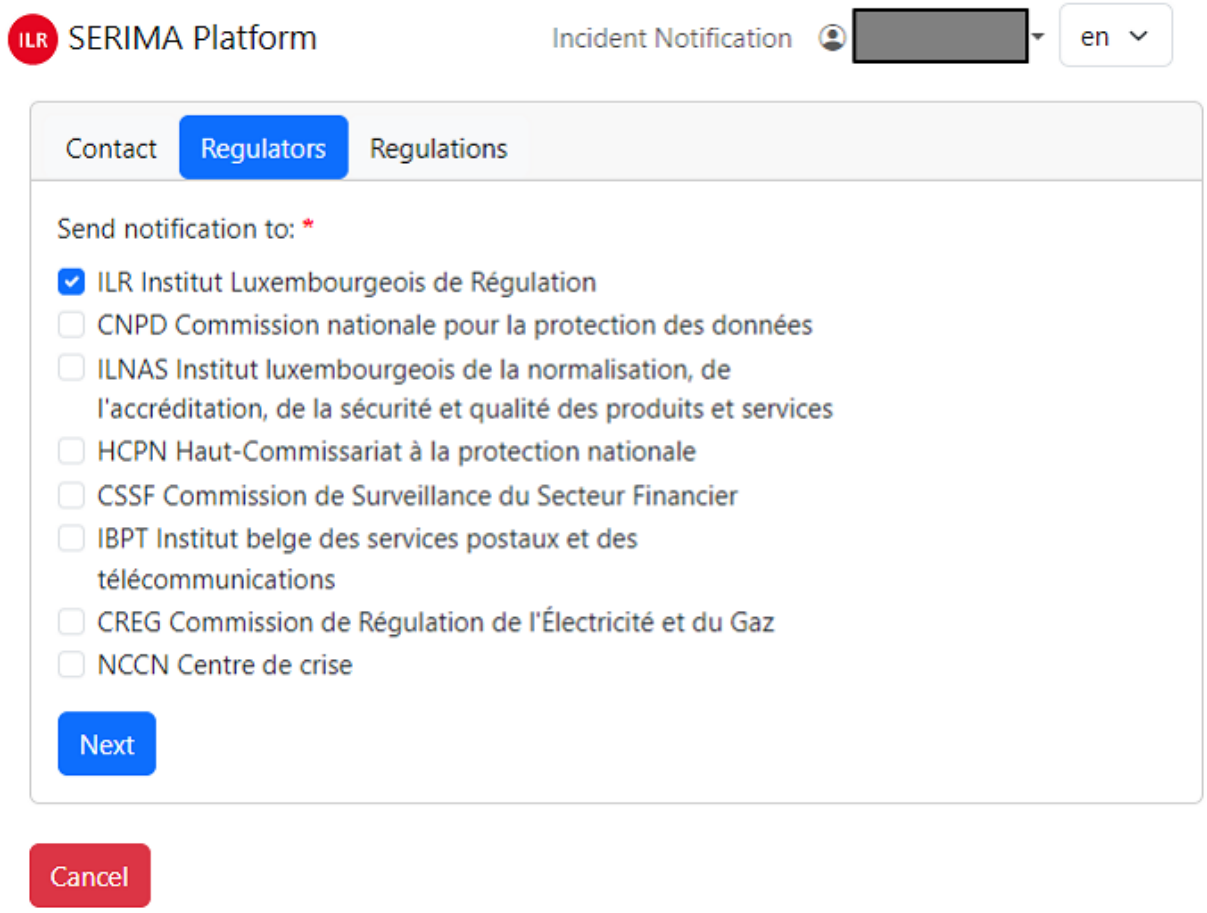
The following step is to define which regulation/s you want to refer to. Again, you may choose both.

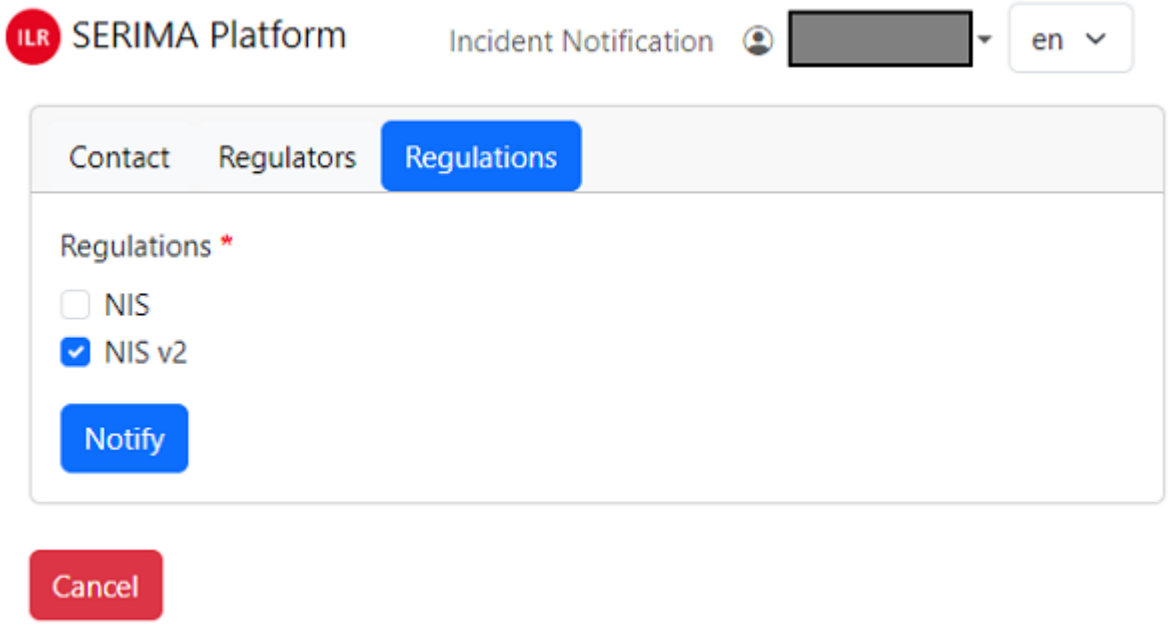
9.4.4 Sectors

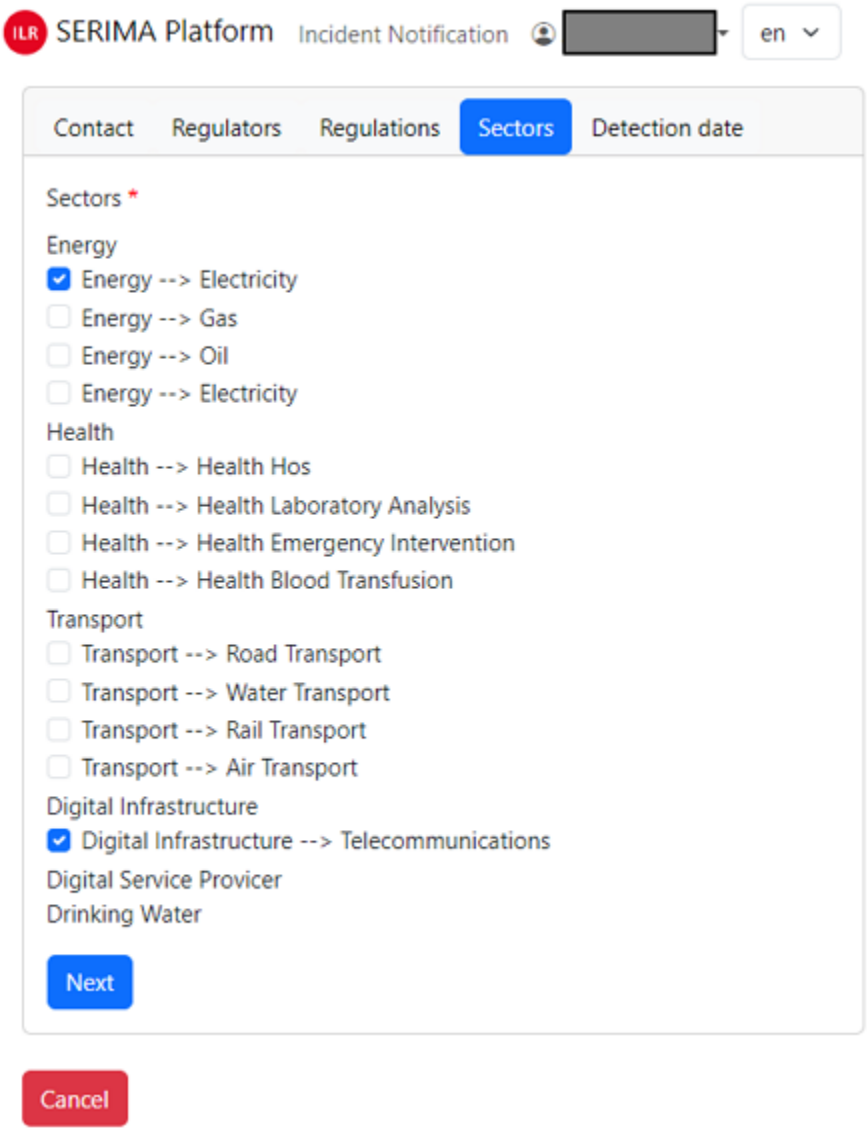
Then you should define which sector is affected by the incident. The options are very straightforward and you may choose more sectors. As many sectors as you have marked, as many incidents will be created in the system.

For demonstration purposes, let's choose two sectors (Energy-Electricity and Digital Infrastructure Telecommunications):


SERIMA Platform
Incident Notification
en
Contact
Regulators
Regulations
Company information
Luxembourg House of Cybersecurity
Person in charge of the incident notification
Job Title
Technical contact
Is the same person in charge of technical aspect?
Job Title
Telephone
References (Optional)
Incident Reference: TXR 2565
Complaint reference
Next
Cancel

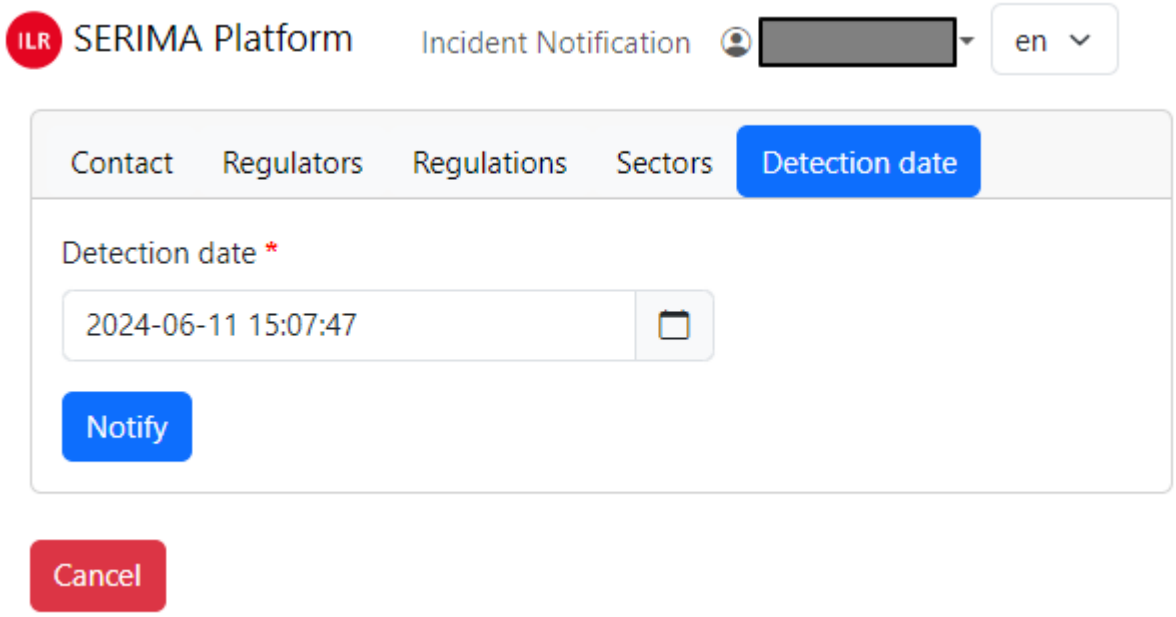

SERIMA Platform
Incident Notification
[redacted]
en
Contact
Regulators
Regulations
Send notification to: *
ILR Institut Luxembourgeois de Régulation
CNPD Commission nationale pour la protection des données
ILNAS Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services
HCPN Haut-Commissariat à la protection nationale
CSSF Commission de Surveillance du Secteur Financier
IBPT Institut belge des services postaux et des télécommunications
CREG Commission de Régulation de l'Électricité et du Gaz
NCCN Centre de crise
Next
Cancel


SERIMA Platform
Incident Notification
[redacted]
en
Contact
Regulators
Regulations
Regulations *
NIS
NIS v2
Notify
Cancel


SERIMA Platform
Incident Notification
en
Contact
Regulators
Regulations
Sectors
Detection date
Sectors *
Energy
Energy --> Electricity
Energy --> Gas
Energy --> Oil
Energy --> Electricity
Health
Health --> Health Hos
Health --> Health Laboratory Analysis
Health --> Health Emergency Intervention
Health --> Health Blood Transfusion
Transport
Transport --> Road Transport
Transport --> Water Transport
Transport --> Rail Transport
Transport --> Air Transport
Digital Infrastructure
Digital Infrastructure --> Telecommunications
Digital Service Provicer
Drinking Water
Next
Cancel

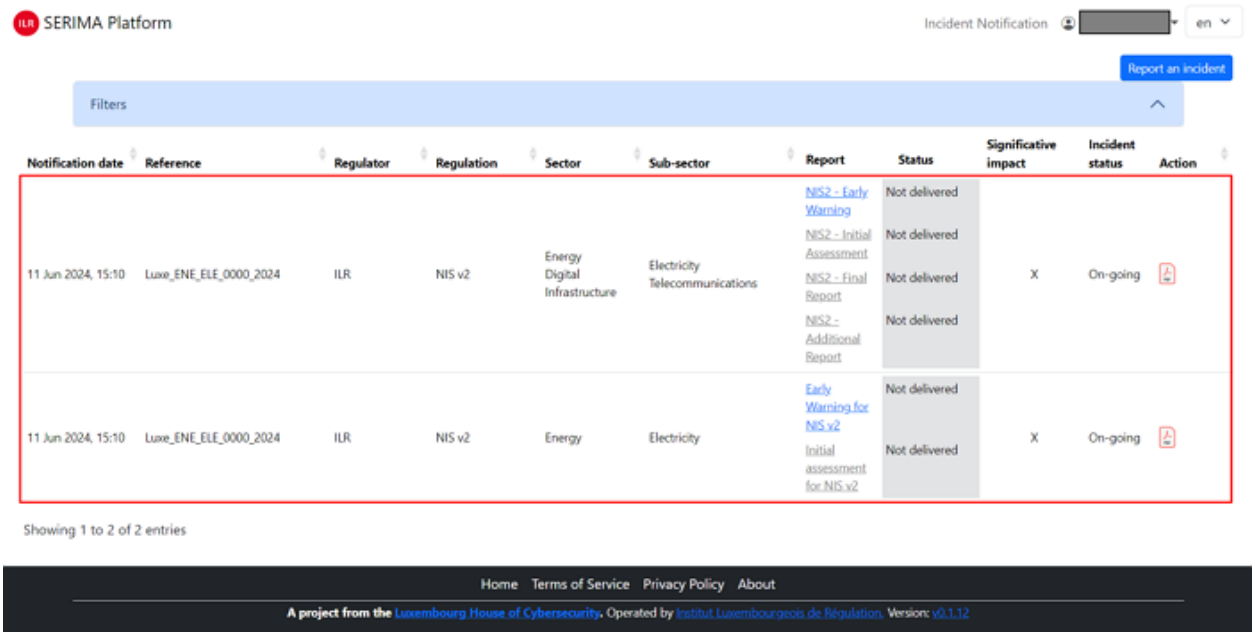
9.4.5 Detection date

As the final step in the incident reporting process, you should provide the date and time of the incident. The easiest way to populate the required field is to click on the calendar icon (the field will be automatically populated with the date and time of detection).



If the detection date field is filled in correctly, click the '**Report**' button to complete the incident reporting process. You will be directed back to the main screen (Incident List View) where you can see the newly created incident reports.

The table contains, on the one hand, the items that you filled in during the preparation of the incident report, as well as new columns: for example, the Significant impact, the Incident status, or the Action columns.



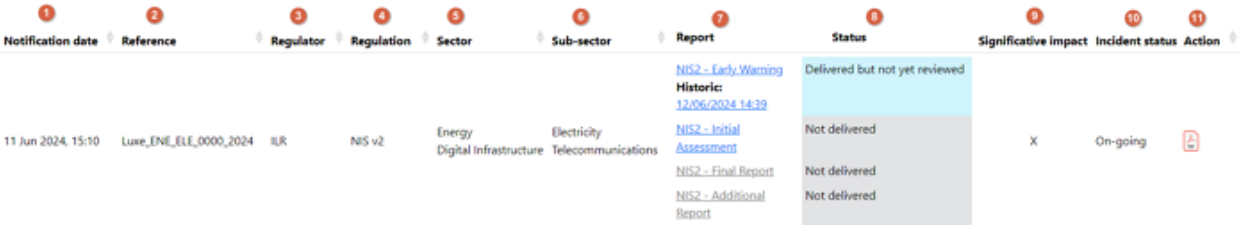
This is the page (**Incident List View**) where you can see the incident reports you sent and the information about them.

If there are many incidents in the table, you can sort them in alphabetical order using the arrows at the top of the columns. Only one sorting criteria can be activated at a time and the active sorting criteria is shown by a darker grey triangle:

In case you see clickable links in the table (for instance 'NIS2 – Early Warning' in the above screenshot), you may click on them for further information.

9.4.6 Incident list view

The **Incident List View** is the main screen of the application: this is the view that summarizes the list of incidents created by the operator (or end user). It is in a table format with the following columns:



The description of the columns is as follows:

	Column name	Description
1	Notification date	The creation date of the incident (when the operator notified the regulator)
2	Reference	The reference number generated by the system when an incident is reported
3	Regulator	The name of the regulator selected by the operator when creating the incident report
4	Regulation	The name of the regulation (NIS and/or NIS v2) the operator selected during the creation of the incident report
5	Sector	The name of the sector the operator selected when the incident report was created
6	Sub-sector	The name of the sub-sector the operator selected when the incident report was created
7	Report	Reports are different steps of the incident handling
8	Status	The status of the report (step of the incident)
9	Significative impact	Each incident can be significative or non-significative – calculated by the system
10	Incident status	The status of the incident (On-going, ...)
11	Action	Certain actions can be taken in different steps of an incident (for example PDF download)

When you submit an incident, the system creates a reference. It is a human readable reference number editable by the regulator regarding the incident.

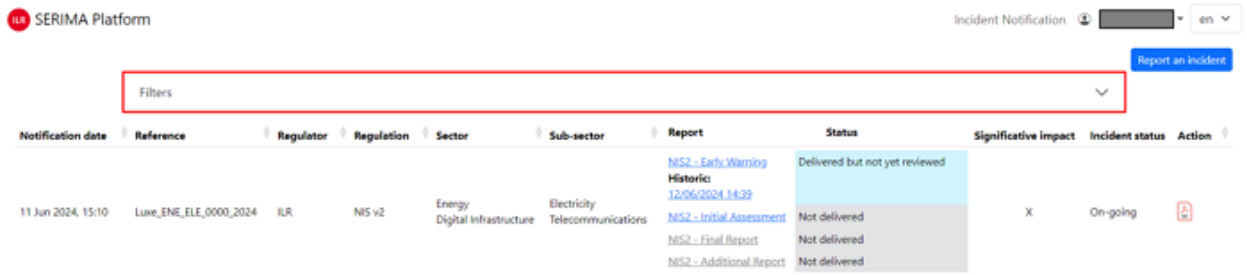
Each incident is composed of one or several reports. Reports are different steps, depending on the options you choose when creating the incident. You have to fill in the first report and after you can unlock the second. Please note that once you fill in a report, you can see all the historic steps.

Each report has a status: '**Not delivered**', '**Delivered but not yet reviewed**', '**Review passed**', '**Review failed**' and '**Not delivered and deadline exceeded**'.

9.4.7 Search among incidents

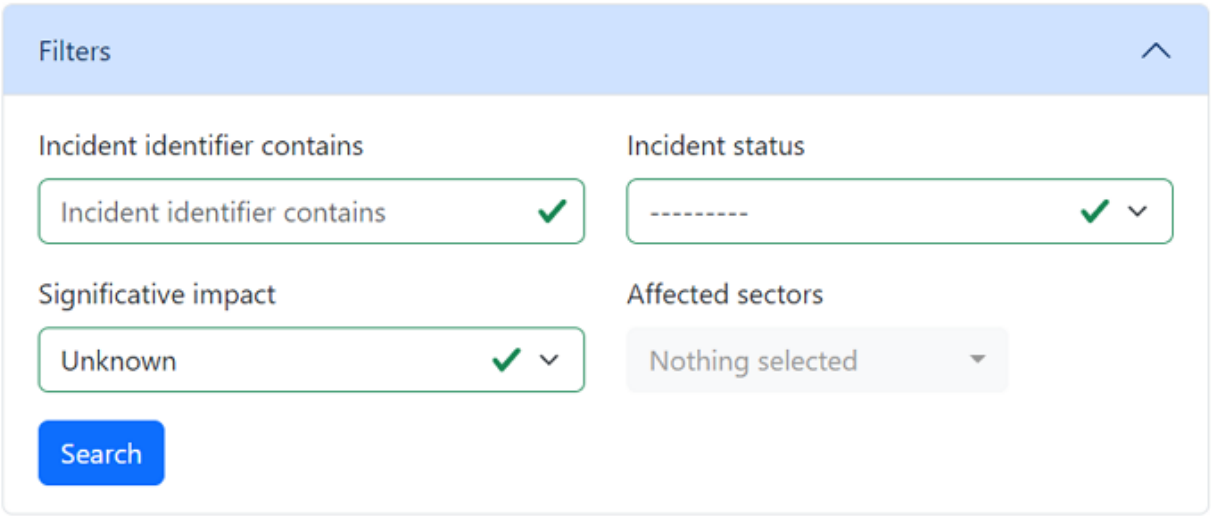
The filter function of the platform can be very useful if there are many incidents and you want to filter among them according to different criteria to find the incident you are looking for.

To make the filters visible, click on the down-pointing arrow at the right end of the filter field:



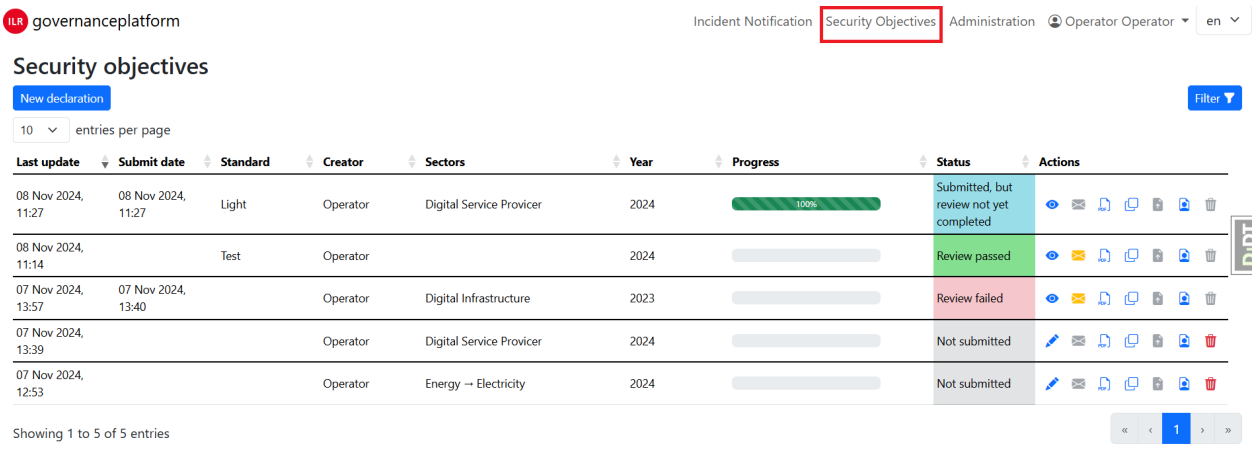
You can filter all your incidents and expand/collapse the filter area. The filter can be used with the following search fields:

- **Incident identifier contains**: this is a free-word search engine that can be used to search among incident identifiers by character strings.
- **Significative impact**: this field searches among the values of the Significative impact, which can have two values (yes or no). The '**X**' in the screenshot above corresponds to the value '**NO**' in the Significative Impact column.
- **Incident status**: The Incident status is also a Boolean data type, it can take only two values: '**Closed**' or '**On-going**'.
- **Affected sectors**: you can search among the affected sectors here, by clicking on the down-pointing arrow (a list of possible sectors appears, so you can search for a specific sector).



9.5 Security Obejctives

The security objective self-assessment is accessible by clicking on the menu at the top of the page.



If you already had some security objective reported, you can have a list like the above. Else you need to declare a new one by clicking on the blue button **New declaration**

The list is similar to the incident one. The only difference is that you have to submit your declaration by clicking on the green icon in the action menu.

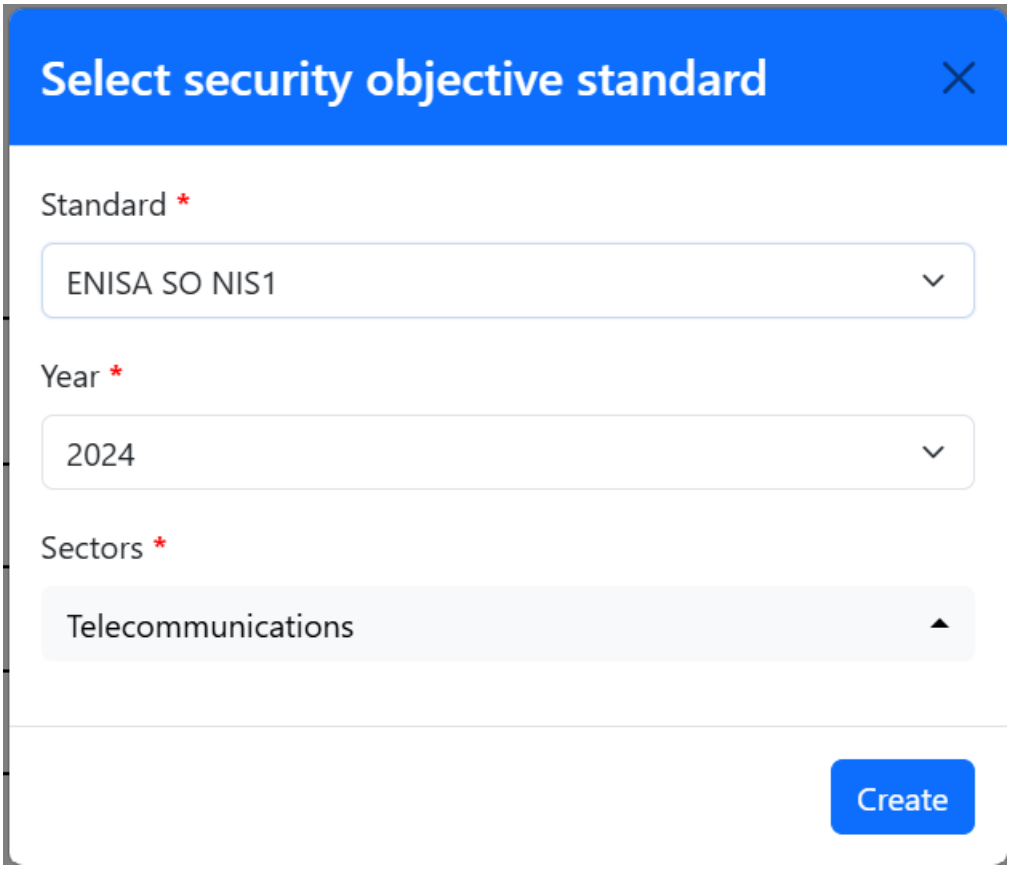
The action menu above is the one before the submission:

- The **blue pen** is to fill the security objective. It goes to an eye to see the security objectives when the security objectives are submitted
- The **envelope** is going to orange when you get a message from the competent authority
- The **PDF file** is here to generate a PDF file
- The **fourth icon** is here to duplicate a security objective. It allows us to start a new evaluation from a previous one
- The **file with the arrow** is here to submit the evaluation. When the evaluation is submitted, it's impossible to resubmit or edit
- The **icon with the portrait** is here to see who has accessed to the evaluation
- The **garbage icon** is to delete an evaluation while it's not submitted

9.5.1 Declare a new security objective

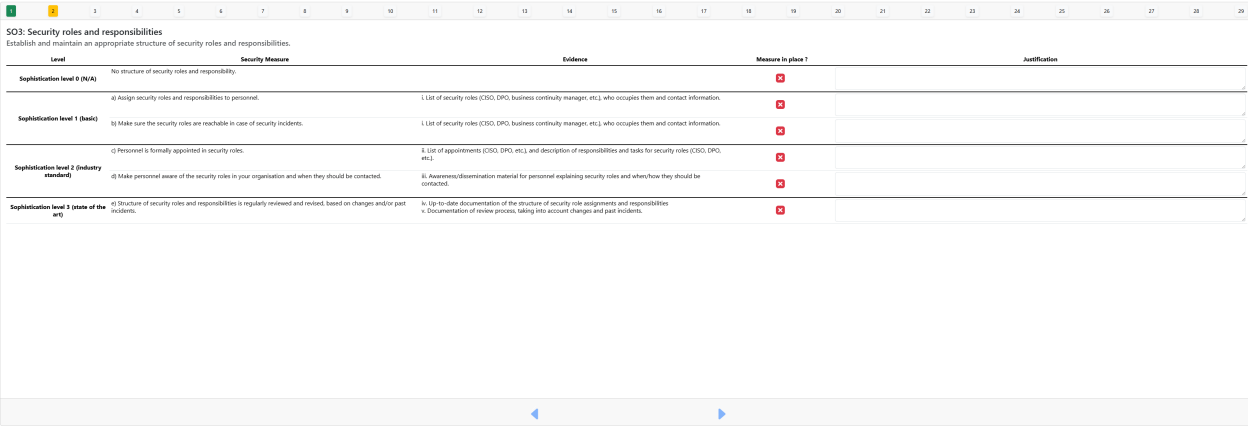
After clicking, a nice pop-up appears, you have to choose the referential, the sectors and the year.

Click on the blue button **create** and the standard is created and you are redirected to the page to fill all the security objectives. If you want to go back to the list view of all your creations, please use the menu at the top.



9.5.2 Fill a security objective (SO)

This is the page to fill a SO. At the top you have the list of all the security objectives.



As you can see, security objectives can have 3 states:

- **Green** correctly filled
- **Orange** filled but some information are missing
- **Blank** not filled

You have to tick the “measure in place” and put a justification to go to the green, you can switch between the different SO by clicking on the number or using the blue arrow at the bottom of the page.

10 Administration interface

10.1 Access to the administration page

Through the “Administration” link, left of the profile icon, above on the Incidents page, the following roles have access to the `site administration` interface, that allows to create and modify some database objects :

- PlatformAdmin : can create regulations, regulators, observers, other platform administrators
- RegulatorAdmin : can create workflows for incidents, RegulatorUser for its regulator, other regulator administrators
- RegulatorUser : can create companies and operator administrators
- OperatorAdmin : can create OperatorUser for its company and other operator administrators
- ObserverAdmin : can create ObserverUser for its Observer entity

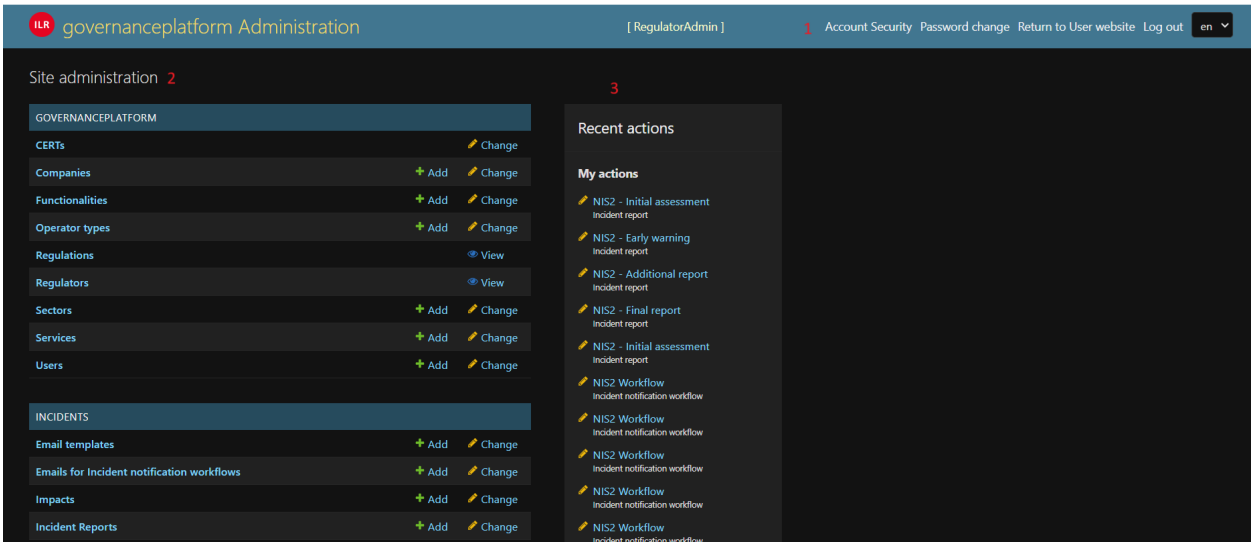


Fig. 10.1: Screenshot of an administrator page (Dark Theme).

The administrator page is composed of 3 parts:

1. The navigation bar, above, where you can change your account settings, language, also leave the website and return to the user website that shows incidents
2. A list of modules on the left, where you can select one type of objects related to incidents or users, and add or modify those
3. A list of your recent actions on the platform, on the right

10.2 Standard list view

When clicking on a module, e.g. “Impacts” as illustrated below, you see a list of the objects of that type, and you have different possible actions. The proposed actions may differ depending on the object type and your role.

1. Above the list is a search field, that allow to narrow the list to objects including that string,
2. On the right, you can filter the list according to some attributes,
3. Just above the filter box, some buttons if present allow you to import or export the list in several formats (JSON, CSV, etc.),

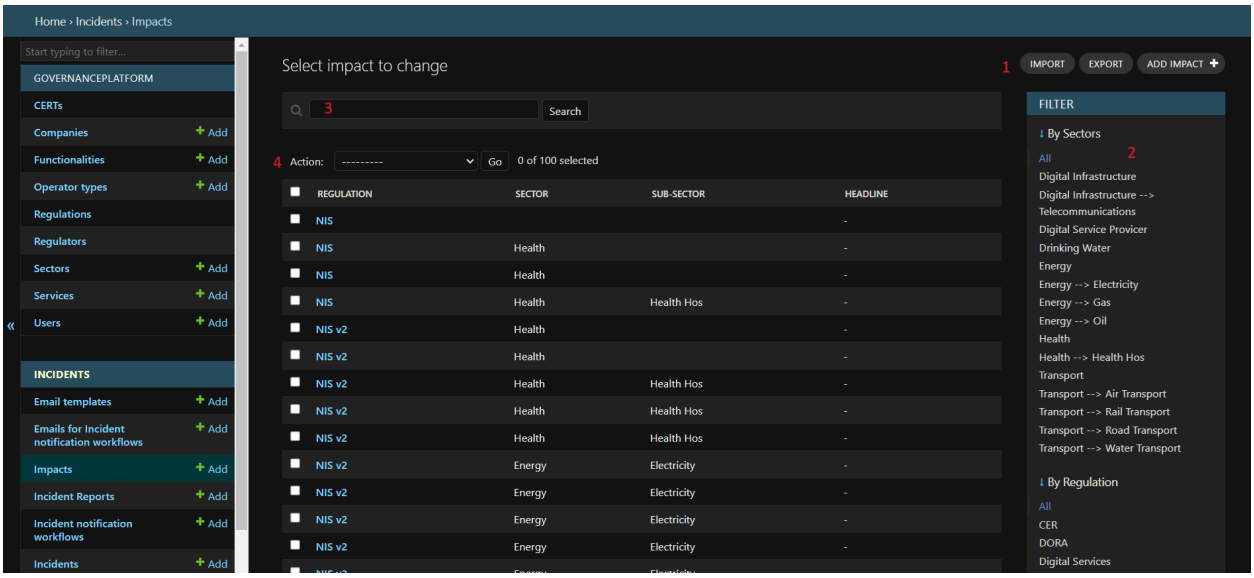


Fig. 10.2: Screenshot of a list page.

4. A button in the same zone allows to add a new object,
5. Some group actions are also available, for that you need to tick the case corresponding to the entries you want to modify and select the appropriate action above the list.

10.3 Standard add / change function

When clicking on the “Add” button or the first field of an object, you are directed to the “change” page, like shown below. When editing an existing object, the values are prefilled with the current properties of the object. When adding a new object, the form is blank.

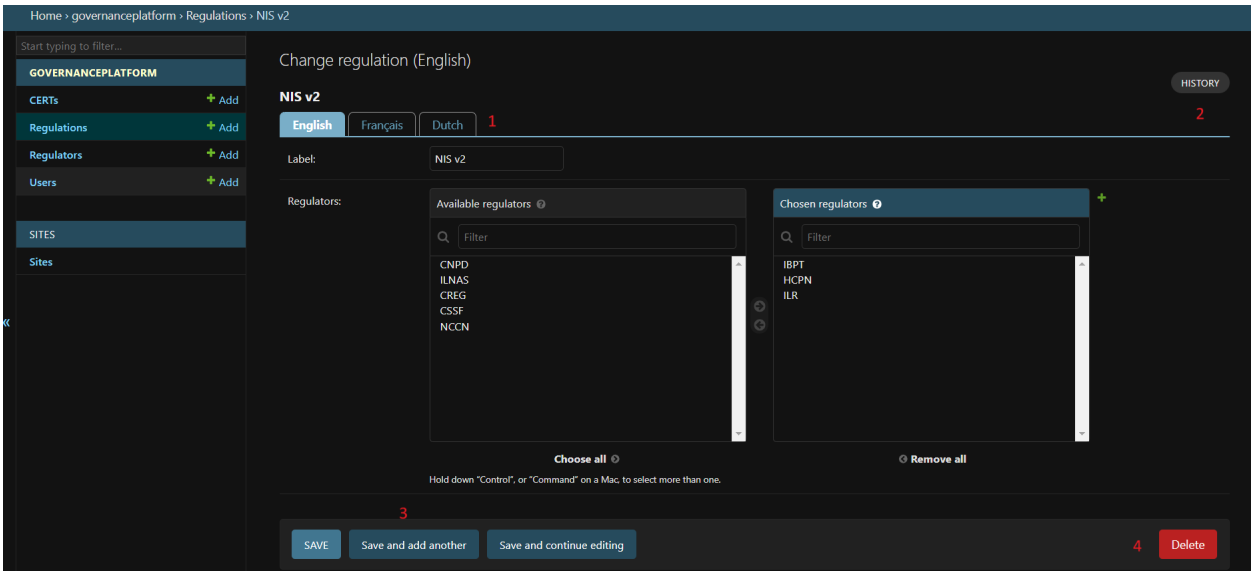


Fig. 10.3: Screenshot of an edition page.

1. Above the form, language tabs allow you to input several alternative versions of the object, since the platform is multi-linual. Note that you always need to fill at least the first language, as it is used as fallback, would some

fields be left blank in the other languages. **Also note that you need to save each language separately**. You can do that using the "Save and continue editing" button.

2. In the upper right part of the window, an "History" button allows you to see the history of the object (all the modifications done)
3. In the lower part of the window, different possibilities are proposed to save the object. You may also be able to delete the object. If you choose to delete the object, a confirmation message will be shown with the impacts on other entities.

10.4 Creation of workflow for incident notification

10.4.1 Creation of workflow

The RegulatorAdmin role is the one who defines the workflows for incident notification.

Here, the standard way to create a workflow:

1. First create an item in the `Incident notification workflows` module corresponding to the regulation (e.g. NIS2, CER, GDPR, etc.).
2. Then create the different steps of your workflow, that are called `incident reports` (e.g. Early Warning, Final Report, etc.).
3. Now link the `incident reports` with the `incident notification workflow`, for that go on `incident notification workflow` and choose the incident reports. The position defines the order of the reports.
4. Each incident report is made of a list of `questions`, organised in tabs called `question category`. The `question category` can be created directly in the question form. You have to create the category only one time, after you can reuse it. For a question, the `question category` should never remain blank.

> **Note**
>
> The `question category` helps for the rendering of the form for the user who submits the notification. There are different types of questions, such as FreeText or Multiple choice. Some can have `predefined answers`.

> **Caution**
>
> **It's important to use one answer only for one question**. You can create the predefined answer directly in the question form.**If you want to translate in several languages, you must first fill one language, click on "save and continue editing" and go to the other language, if you don't do that you will loose the content of the predefined answer**.

5. Your incident workflow is now done.

The workflow system also includes an automatic emailing system. The templates of the emails have to be defined in the `Email templates` entity. Each email has a name, subject, and content. The content can be personalized with data from the database, using the following tags:

- #INCIDENT_NOTIFICATION_DATE# : first notification of the incident
- #INCIDENT_DETECTION_DATE# : detection date of the incident
- #INCIDENT_STARTING_DATE#: starting date of the incident
- #INCIDENT_ID# : reference of the incident

Each `incident notification workflow` has:

- opening email : Email sent when the incident is created
- closing email : email sent when the incident is closed (by the regulator)
- Report status changed email : when there is a change in the lifecycle of the incident, for example a submission of a new report.

The three elements above reference an `Email template` that has to be defined.

Those emails can be completed by clicking on the `Emails for incident notification workflows`. For each incident reports (e.g. Early Warning), it's possible to send further emails like reminder, for that in the `Emails for incident notification workflows` you can define emails which are sent with delay, the delay can start from the Notification Date of the report or the date of the previous incident report.

For each couple regulation/sector(s), it's possible to define an `impact`, the impacts are here to qualify the incident as significative. If at least one impact is ticked by the person who submits the incident, the incident is qualified as "significative".

10.4.2 Modification of workflow

During the lifecycle of a workflow, it can evolve. For that you can change the questions of each incident reports. The application is keeping the history of questions and answer. So it will show the correct value in the history of the incident and in the PDF.

The admin part only show the last version of the report.

11 Platform Administrator interface

11.1 log-in

On this page you can log in or create an account in case you have to notify an incident and you don't have credentials.

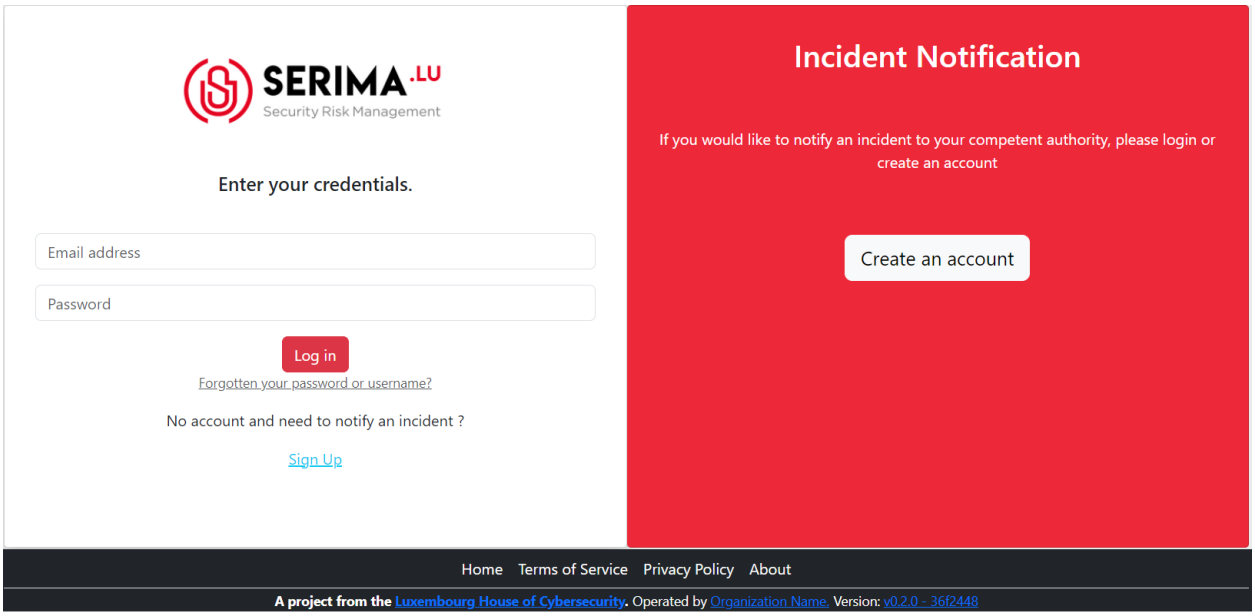


Fig. 11.1: Screenshot of the login page.

If you have credentials and don't remember the password please use the link: 'Forgotten your password or username?'

At the first login, you need to activate the 2FA.

11.2 Standard functionnality

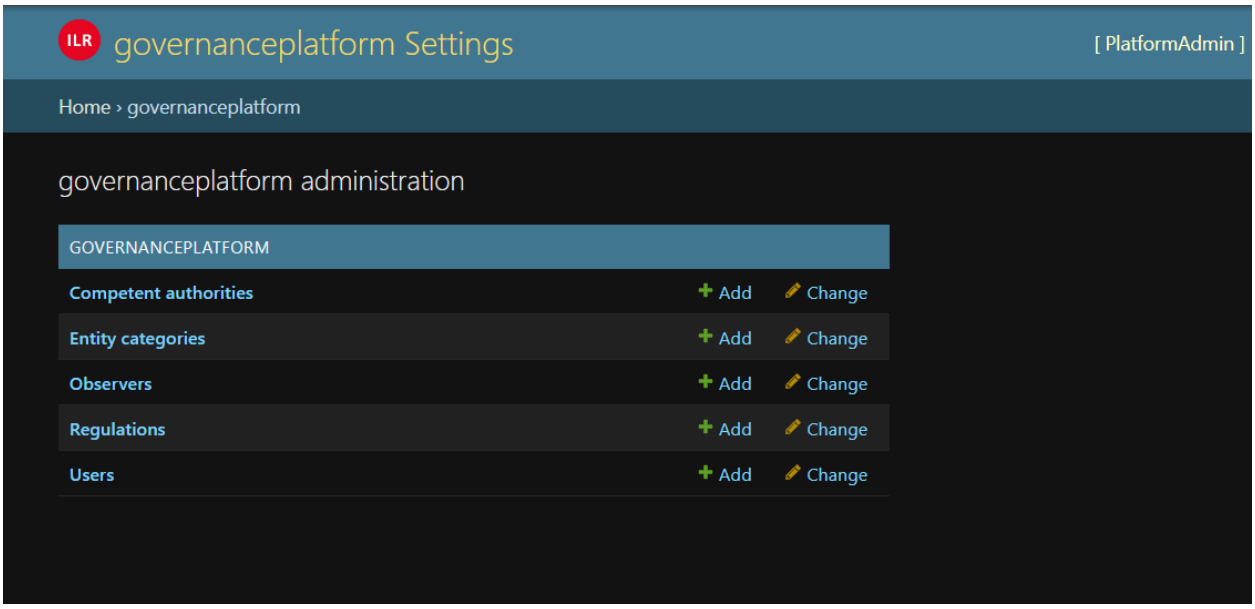


Fig. 11.2: Main page.

To see the standard function, have a look to the Administrator interface.

11.3 Definition of observers

To define the rules of incident reception for observer, you need firt to create `Entity categories` (e.g. Private, Public, Critical infrastructure, etc.).

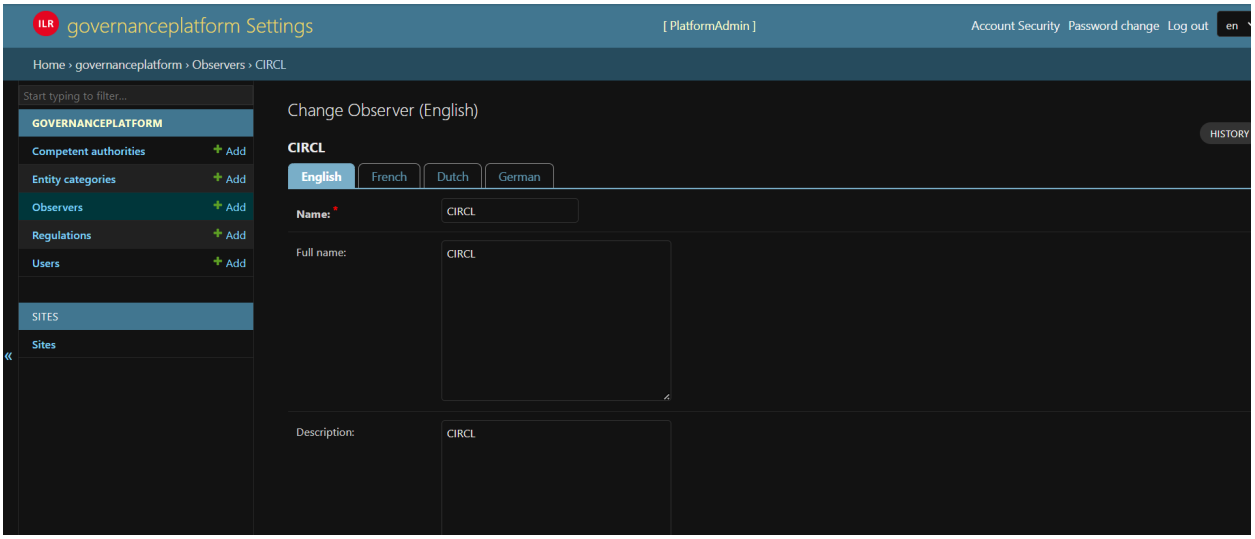


Fig. 11.3: Definition of an observer.

- The checkbox `Receives all incidents`, if it's checked the observer will receive all incidents, **no matter of the regulation**. If you need specific rules you have to define `observer regulations`

For observer regulation you need to define:

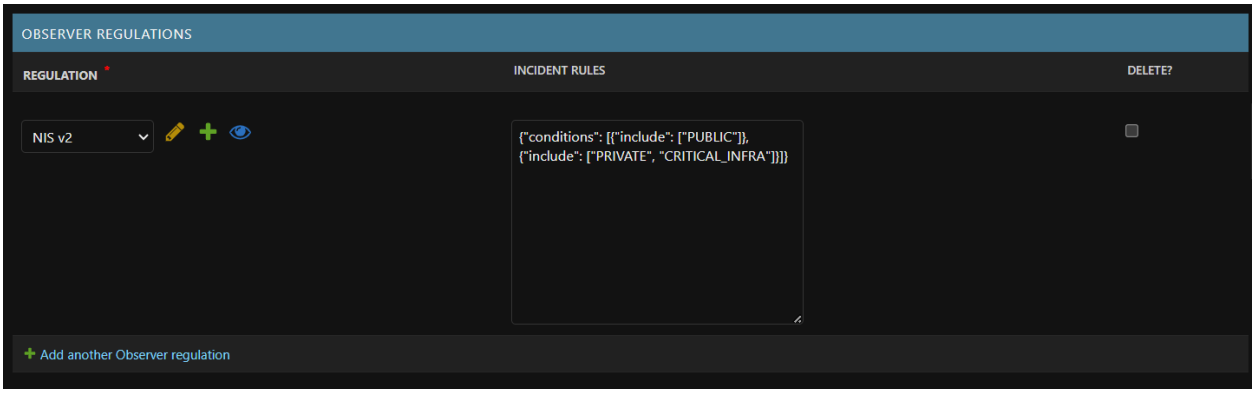


Fig. 11.4: Observer regulation.

1. The regulation concerned by the rules
2. The incident rules. The incident rules has to be defined as a JSON format following this structure:

```
{
    "conditions":[
        {
            "include":[
                "PUBLIC"
            ]
        },
        {
            "include":[
                "PRIVATE",
                "CRITICAL_INFRA"
            ]
        }
    ]
}
```

In the case above the regulation receive the incident which are `PUBLIC` **OR** the incidents which are `PRIVATE` and `CRITICAL_INFRA` (e.g. NIS2 AND (PUBLIC OR(PRIVATE AND NOT CRITICAL_INFRA))). PRIVATE, CRITICAL_INFRA and PUBLIC are `code` from `Entity Category`.

If the observer should receive all incidents of a regulation the `incident rules` should be {}.

Fig. 11.5: Observer regulation.

If incidents should be excluded, the tag exclude can be used in the JSON

```
{
    "conditions":[
        {
            "include":[
                "PRIVATE"
            ],
            "exclude":[
                "CRITICAL_INFRA"
            ]
        }
    ]
}
```

In the case above if we link to the regulation NIS2 we receive the incident from PRIVATE only and PRIVATE which are not CRITICAL_INFRA (e.g. NIS2 AND PRIVATE AND NOT CRITICAL_INFRA).

12 Presentation

The Incident Notification Module is developed and maintained by NC3-LU (https://github.com/NC3-LU) team in the framework of the Informed Governance Project (https://github.com/informed-governance-project).

The incident notification module is designed to be used as a national incident notification tool. It is multi-regulator, i.e. any regulator or competent authority of the country can use it and receive the incident notifications. It is multi-regulation, i.e. it can completely be configured, and each regulator is responsible to configure the regulations he is responsible for. The operators under supervision can use it to notify their incidents.

This project is lead by NC3-LU (https://www.nc3.lu). Developed in partnership with ILR.lu (https://web.ilr.lu) and IBPT.be (https://www.ibpt.be).

This document is intended to be a documentation for operators and users of the module. If you find errors or omission, please don't hesitate to submit an issue (https://github.com/informed-governance-project/SERIMA/issues/new?labels=documentation&template=bug_report.md) or open a pull request with a fix.

13 Contact

NC3 Luxembourg (https://www.nc3.lu) - info@nc3.lu

14 License

The Governance Platform is licensed under GNU Affero General Public License version 3 (https://www.gnu.org/licenses/agpl-3.0.html).

- Copyright (C) 2023-2026 Cédric Bonhomme <cedric.bonhomme@nc3.lu>
- Copyright (C) 2023-2026 Jérôme Lombardi <jerome.lombardi@nc3.lu>
- Copyright (C) 2023-2026 Juan Rocha <juan.rocha@nc3.lu>
- Copyright (C) 2023-2026 NC3 Luxembourg (https://www.nc3.lu)
- Copyright (C) 2023-2026 Ruslan Baidan <ruslan.baidan@nc3.lu>

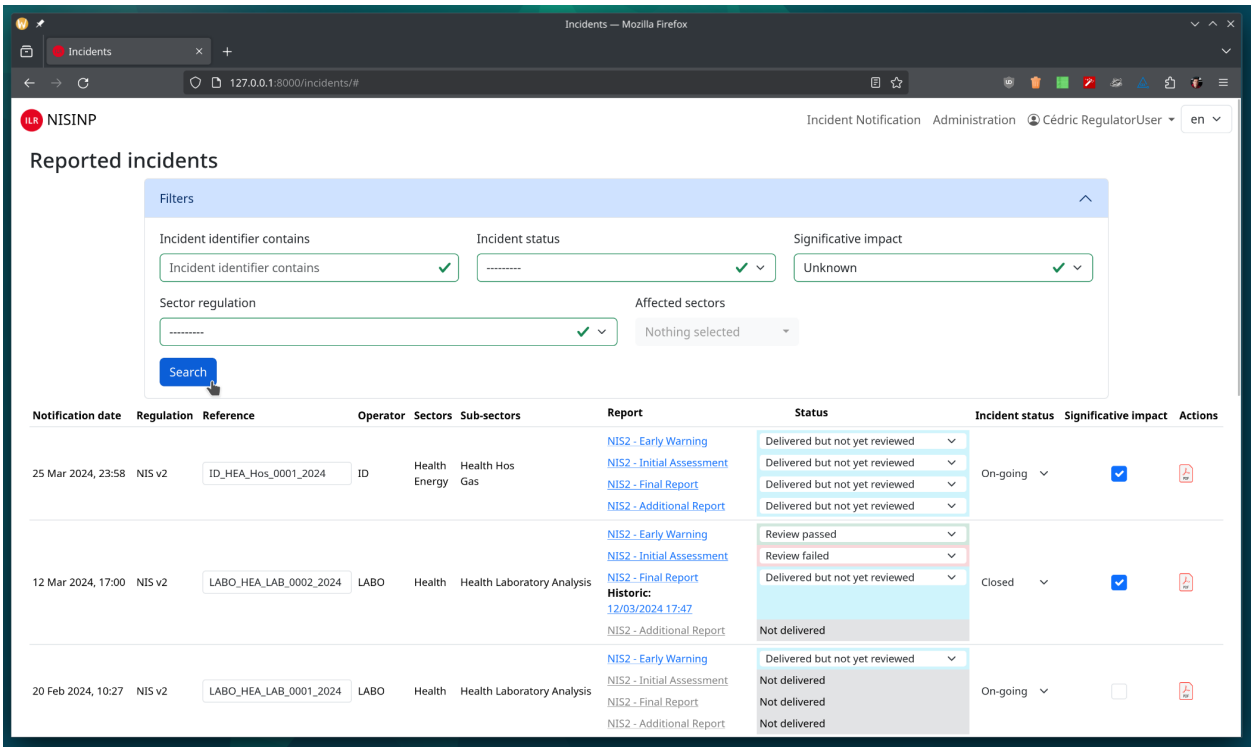


Fig. 12.1: Screenshot of the list of incidents from the regulator view.