



Documentation

Release 4

Jul 08, 2023

CONTENTS

1	Getting Started	3
1.1	Glossary	3
1.2	Features	4
1.3	Requirements	6
1.4	Supported Browsers	6
2	Setup	7
2.1	Installation Guide	7
2.2	Platform Wizard	7
3	Security	11
3.1	Threat Model	11
3.2	Application Security	16
3.3	Encryption Protocol	27
3.4	Security Audits	29
4	User Documentation	31
4.1	Common to All Users	31
4.2	For Administrators	35
4.3	For Recipients	63
4.4	For Whistleblowers	65
5	Project Roadmap	69
5.1	Introduction	69
5.2	Development Areas	69
5.3	Multisite Users	71
6	Developer Documentation	73
6.1	Development Environment	73
6.2	Software Libraries	75
6.3	Database Schema	75
6.4	Release Procedure	75
6.5	Continuous Integration	76
6.6	Code Documentation	77
	Index	79

[GlobaLeaks](#) is an open-source, free software intended to enable anyone to easily set up and maintain a secure whistle-blowing platform.

Note: This documentation is thank to the support of our community. Join us and contribute with your additions and suggestion. In any of the page you find a link that enables you to provide suggestions and corrections. We remind you that in case of any software issue or bug you may always report on the [ticketing system](#).

GETTING STARTED

1.1 Glossary

This is a list of jargon used in GlobaLeaks, defined in a way so as to be unambiguous and uniform across all references.

Administrator

The user that has set up and is maintaining the platform. An Administrator does not have access to Whistleblowers' reports.

Channel

The reporting channel intended as a container for reports. Channels can be configured in terms of questionnaire, recipients and policies. They are typically used to organize the reporting procedure.

Notification

An email sent to notify a recipient of a new report, or an update of an existing report.

Platform

A system running the GlobaLeaks software.

Questionnaire

A questionnaire is a set of questions that the whistleblower should fill to file a report.

Receipt

A 16-digits random secret code generated by the system and provided to whistleblowers upon the submission of their report, enabling them to anonymously access and update their report by adding comments and new files.

Recipient

The user enabled to read whistleblowers' reports. Recipients may also communicate with whistleblowers via the GlobaLeaks platform.

Report

The object of the submission by a whistleblower including answers to a questionnaire and attached material.

Submission

The action performed by the whistleblower when filing a report.

Whistleblower

The person who files a report.

1.2 Features

1.2.1 User Features

- Multi-user system with customizable user roles (whistleblower, recipient, administrator)
- Entirely manageable from a web administration interface
- Support for [more than 90 languages](#) with support for Right-to-Left (RTL)
- Let whistleblowers decide if and when to confidentially declare their identity
- Exchange multimedia files with whistleblower
- Secure management of files' access and visualization
- Chat with Whistleblower to discuss the report
- Unique 16-digit receipt for the whistleblower to log back in anonymously
- Simple recipient interface for receiving and analyzing reports
- Support for the categorization of the reports with labels
- Support for the user search of reports
- Support for assigning and creating case management statuses
- Customizable look and feel (logo, colour, styles, font, text)
- Define multiple reporting channels (e.g. per-topic, per-department)
- Create and manage multiple whistleblowing site (e.g for subsidiaries or third party clients)
- Advanced questionnaire builder
- Whistleblowing system statistics

1.2.2 Legal Features

- Designed in adherence with [ISO 37002:2021](#) and [EU Directive 2019/1937](#)
- Bidirectional anonymous communication (comments/messages)
- Customizable case management workflow (statuses/sub-statuses)
- Whistleblower identity conditional reporting workflow
- Manage conflict of interest in the reporting workflow
- Custodian functionality to authorize access to whistleblower identity
- GDPR privacy by design and by default
- GDPR configurable data retention policies
- GDPR compliant subscriber module for new users of SaaS services
- No logs of IP addresses
- Audit log
- Integratable with existing enterprise case management platform
- Free Software OSI Approved [AGPL 3.0 License](#)

1.2.3 Security Features

- Designed in adherence with [ISO 27001:2022](#)
- Full data encryption of whistleblower reports and recipient communication
- Digital anonymity support with [Tor](#) integration
- Built-in HTTPS support with [TLS 1.3](#) standard ([SSLabs A+](#) rating)
- Automatic free digital certificate enrollment ([Let's Encrypt](#))
- Multiple penetration tests with full public reports
- Conform to industry standards and best practices for application security ([OWASP](#))
- Two-Factor authentication (2FA) support compliant with standard [TOTP RFC 6238](#)
- Integrated network sandboxing with iptables
- Integrated application sandboxing with [AppArmor](#)
- Complete protection against automated submissions (spam prevention)
- Subject to continuous peer-review and periodic security audits
- PGP support for encrypted email notifications and encrypted file downloads
- Does not leave traces in browser cache

1.2.4 Technical Features

- Multi-site support enabling to run multiple virtual site on the same setup
- Responsive user interfaces made with [Bootstrap](#) CSS Framework
- Built-in Accessibility Support with [WAI-ARIA](#) compliance
- Automated Software Quality Measurement and Continuous Integration Testing
- Long-Term Support plan (LTS)
- Built with lightweight framework technologies ([AngularJS](#) and [Python Twisted](#))
- Integrated [SQLite](#) database
- Automatic setup of [Tor Onion Services Version 3](#)
- Support for self-service signup for whistleblowing SaaS service setup
- Support for Linux operating system ([Debian/Ubuntu](#))
- Debian packaging with repository for update/upgrades
- Fully self-contained application
- Easy integration of the platform with existing websites
- Rest API

1.3 Requirements

Make sure you understand and satisfy each of the following technical requirements.

1.3.1 Hardware Requirements

Requirements:

- CPU: Dual core 2.0GHz
- RAM: 1GB
- STORAGE: 20GB
- I/O: 10Mbit/s (shared)

Please note that GlobaLeaks is designed to run on servers even smaller than the above configuration.

The storage size should be defined based on your data retention policies and the expected use of the platform.

1.3.2 Software Requirements

GlobaLeaks is designed to run on GNU/Linux and developed and tested specifically for Debian based systems.

The software lifecycle of the platform includes full support for all Debian and Ubuntu LTS versions starting from [Debian 11](#) and [Ubuntu 20.04](#).

On these platforms the support is guaranteed following the official long term support timelines:

- [Release End of Life Timeline](#) defined by Debian;
- [Release End of Life Timeline](#) defined by Ubuntu.

Support for more distributions is planned.

1.4 Supported Browsers

GlobaLeaks has been designed to fully support commonly used browsers running on desktop PCs, laptops, tablets and phones.

We recommend the usage of the [Tor Browser](#) that protects users' anonymity and includes various privacy and security enhancements not present in other browsers.

Other supported browsers are:

Browser	Version
Mozilla Firefox	>= 38
Google Chrome	>= 45
Brave	>= 1.20.110
Edge	any
Safari	>= 8
iOS	>= 9
Android	>= 4.4

2.1 Installation Guide

The following is intended to guide you through the installation of GlobaLeaks.

Before starting the installation, make sure that your system satisfy the [Requirements](#).

Warning: GlobaLeaks is built to give the best technical anonymity to the Whistleblower. In addition the software with specific configurations enables the possibility to protect the identity of the platform administrator and the server's location but this requires advanced setup procedures not considered in this simplified installation guide. By executing the commands below your IP address and the location of your system could be tracked by the network providers and as well our systems will be receiving the same information in order to satisfy the provisioning of the software.

Install GlobaLeaks

In order to install GlobaLeaks run the following commands:

```
wget https://deb.globaleaks.org/install-globaleaks.sh
chmod +x install-globaleaks.sh
./install-globaleaks.sh
```

At the end of the installation follow the instruction provided that should guid through accessing the [Platform wizard](#).

2.2 Platform Wizard

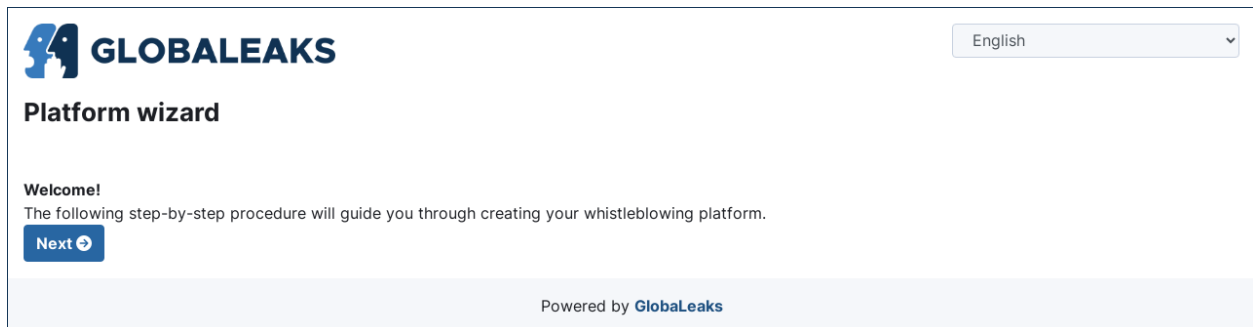
After installing of GlobaLeaks you can proceed with the platform wizard.

Open a browser at port 80 or port 8082 on your remote or local IP respectively.

We recommend you to to perform the wizard either by using the using Tor address provided at the end of the setup or on localhost via a VPN.

2.2.1 Choose the Primary Language for Your Site

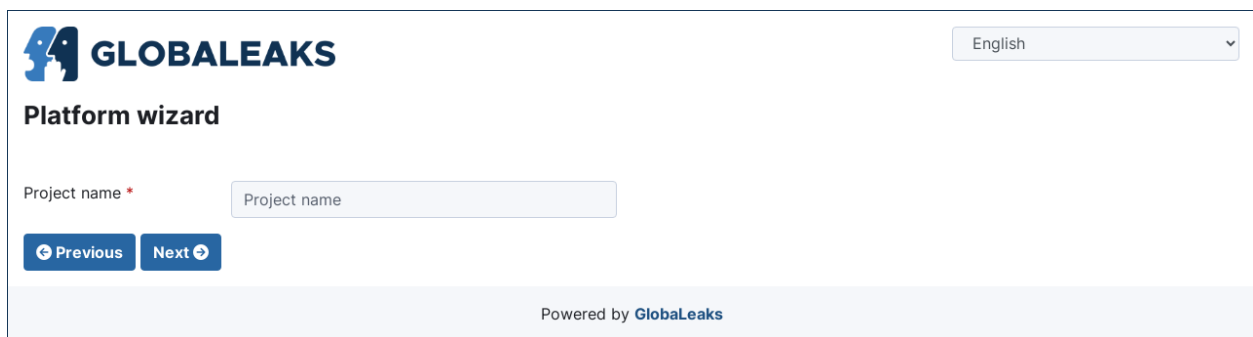
In the first page of the wizard you are invited to select the language of your site. Default choice is English, but many others languages are available and more are expected to be available in the future.



The screenshot shows the first step of the Globaleaks Platform wizard. At the top left is the Globaleaks logo. At the top right is a language selection dropdown menu currently set to 'English'. Below the logo, the text 'Platform wizard' is displayed. A 'Welcome!' message states: 'The following step-by-step procedure will guide you through creating your whistleblowing platform.' Below this message is a blue 'Next' button with a right arrow. At the bottom center, it says 'Powered by Globaleaks'.

2.2.2 Choose a Name for Your Project

In the second section of the wizard configure the name of your project.




The screenshot shows the second step of the Globaleaks Platform wizard. It features the same logo and language dropdown as the previous step. Below the 'Platform wizard' title, there is a label 'Project name' with a red asterisk, followed by a text input field containing the placeholder 'Project name'. Below the input field are two blue buttons: 'Previous' with a left arrow and 'Next' with a right arrow. At the bottom center, it says 'Powered by Globaleaks'.

2.2.3 Configure the Account for the Administrator of Your Whistleblowing Site

In the third section of the wizard configure the account details of the administrator of your project.

Keep in mind to choose a strong password in order to protect this sensitive account; an indication of the strength of the chosen password is shown to guide you in this task.



English ▾

Platform wizard

Admin

Username *

Name *

Email address *

Password *


Password (Confirm) *

☒ Make it possible for this admin to reset user passwords.
 We advise selecting this option if you would like to protect data from being lost in the situation where recipients lose their passwords. On the other hand, we would not advise using this feature if you want to setup a system where only recipients are able to access submissions.

Powered by **GlobaLeaks**

2.2.4 Configure the Account for the First Recipient of Reports

In the forth section of the wizard configure the account details of the first recipient for the reports sent to your project.



English ▾

Platform wizard

Recipient

Username *

Name *

Email address *

Password *


Password (Confirm) *

☐ Skip the recipient account creation.

Powered by **GlobaLeaks**

2.2.5 Read and Accept the License

In the fifth section of the wizard you are invited to read and accept the License of GlobaLeaks

 **GLOBALEAKS**

English

Platform wizard

License

Copyright (c) 2011-2023 - GlobaLeaks

This program is free software: you can redistribute it and/or modify it under the terms of the GNU Affero General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Affero General Public License for more details.

You should have received a copy of the GNU Affero General Public License along with this program. If not, see .

☒ I have read and agree to the terms of the license.

☐ Notify developers of software problems


By enabling this feature, you will contribute to the development and security of the platform.

[< Previous](#) [Next >](#)

Powered by **GlobaLeaks**

2.2.6 Complete the Wizard

The sixth section of the wizard notifies you the completion of the wizard.

 **GLOBALEAKS**

English

Platform wizard

Congratulations!

You have completed the platform wizard.

[Proceed](#)

Powered by **GlobaLeaks**

3.1 Threat Model

GlobaLeaks is an free and open source whistleblowing software that can be used in many different usage scenarios that may require very different approaches to obtain at the same time strong security and high usability. This two requirements are necessary to safely handle a whistleblowing procedure by protecting whistleblowers and at the same time achieve specific project goals. For this reasons considering the variety of different use cases and risks the software supports the possibility to be configured o respond to the specific threat model here detailed.

This document is intended to be used by organizations that want to implement a whistleblowing procedure based on Globaleaks and support the analysis and comprehension of the specific threat model of their context of use and of the risks involved and guide users through the selection of the best practices to be used within their own project.

3.1.1 Users Matrix

As a first step we define the type of users that can interact with a GlobaLeaks platform.

User	Definition
Whistleblower	The user who submits an anonymous report through the platform. Whistleblowers are persons operating in a wide range of different threat models depending on the usage scenario and the nature of information being submitted.
Recipient	The user receiving anonymous reports submitted by Whistleblowers and responsible for their analysis. Recipients act reasonably in good faith and have to be considered in all scenarios described as trusted party with reference to the protection of Whistleblowers' and the confidentiality of the information by them communicated.
Administrator	The users supporting the setup, the management and monitoring the security of the platform. Administrator may not represent the same entity running, promoting and managing the whistleblowing initiatives (e.g., hosted solutions, multiple stakeholders projects, etc). The Administrator has to be considered in all scenarios described as a trusted entity. They do not have direct access to reports and they are responsible for advising Recipients on the best practices to be adopted in their work.

It's highly relevant to apply each of the security measures always in relationship to the users using the plattform, trying to identify an adequate security and usability tradeoff.

3.1.2 Anonymity Matrix

The anonymity of different users must be differentiated and classified depending on the context of use represented by the following definitions:

User	Definition
Anonymous	The user has accessed the platform via the Tor Browser and following the best practices for protecting their identity reducing to the maximum the possibility that a system involved in the operation has tracked their activities and their own IP address. The user has not provided any information about their own identity to Recipients.
Confidential	The user has used the platform by using a common browser. In this case, third parties could have logged their IP address during their operations but the platform has protected the content of their communication. The user may have possibly opted for disclosing confidentially their own identity to Recipients.

The platform always reports to users their current anonymity state and inform them about the best practices for accessing anonymously via the Tor Browser. Depending on the use case Administrators could possibly enforce the requirement that Whistleblowers could file reports only by using the Tor Browser.

3.1.3 Communication Security Matrix

The security of communication with respect to third party transmission monitoring may have different requirements depending on its context of use.

Identity disclosure is a highly relevant topic, because even in an Anonymous High security environment, identity disclosure may be an valuable option for specific whistleblowing initiative workflows.

If a user starts dealing with an Anonymity set “Anonymous” and with an “Undisclosed Identity” they can always decide, at a later stage, to disclose their identity. The opposite is not possible. This is one of the key considerations to provide users protection around GlobaLeaks.

Voluntary identity disclosure may be required in certain whistleblowing procedures because, generally:

- A tip off MAY receive a follow-up and can be anonymous;
- Formal reports MUST receive a follow-up and in that case cannot be anonymous.

The “MAY” vs. “MUST” is with respect to the actions of recipients and is a fundamental element of the guarantee provided to whistleblowers in many initiatives (e.g., a corporate or institutional whistleblowing platform should not follow a MUST approach for Anonymous submission follow-up, considering such submissions just tip offs and not formal reports).

3.1.4 Usage Scenarios Matrix

In this section you will find examples that show how different anonymity levels of different users can be mixed together depending on the context of use.

Use case	Description
Media outlet	A Media outlet, whose identity is disclosed, decides to start a Whistleblowing initiative. The outlet's recipients are disclosed to Whistleblowers, so that they can trust a specific journalist rather than the outlet itself. Full anonymity must be assured to whistleblowers and their identity cannot be disclosed in connection with anonymous submissions. The whistleblower MAY choose to willingly disclose their identity (e.g. when the journalist's source-protection record is trusted).
Corporate compliance	A Corporation needs to implement transparency, or anti-bribery law compliance, by promoting its initiatives to employees, consultants and providers. The recipients are part of a division of the company (e.g. Internal Audit office). The Whistleblower is guaranteed full anonymity, but they can optionally disclose their identity.
Human Rights Activism Initiative	A Human Rights Group starts a Whistleblowing initiative to spot human rights violations in a dangerous place. The organization requires anonymity to avoid retaliations and takedowns, and operates under a pseudonym. The Recipients MUST not be disclosed to the Whistleblowers, but a Partial Disclosure by pseudonym can be acceptable in order to give proper trust to "Who the whistleblower is submitting to". The Whistleblower MUST be guaranteed anonymity and their identity cannot be disclosed.
Citizen media initiative	A Citizen media initiative with its own public identity wants to collect reports on a specific topic (political, environmental malpractice, corruption, etc) in a medium-low risk operational context. The recipients could be public or use Pseudonym in order to avoid complete exposure. The Whistleblower, if the topic is not life-threatening, can be allowed to submit also in a Confidential way to lower the entrance barrier.

Below we show how different usage scenarios can require different anonymity levels, communication security requirements and identity disclosures for different users.

GlobaLeaks, through its user interface, will enable each user with appropriate security awareness information, and will enforce specific requirements to specific users by the application of clear configuration guidelines.

Scenario	User	Anonymity level	Identity disclosure	Communication security
Media outlet	Whistle-blower	Anonymous	Undisclosed	High security
	Recipient	No anonymity	Disclosed	Medium security
	Admin	No anonymity	Disclosed	Medium security
Corporate compliance	Whistle-blower	Anonymous	Optionally disclosed	High security
	Recipient	No anonymity	Partially disclosed	Medium security
	Admin	No anonymity	Disclosed	Medium security
Human Rights Activism initiative	Whistle-blower	Anonymous	Undisclosed	High security
	Recipient	Anonymous	Partially disclosed	High security
	Admin	Anonymous	Partially disclosed	High security
Citizen media initiative	Whistle-blower	Confidential	Optionally disclosed	Medium security
	Recipient	Confidential	Confidential	Medium security
	Admin	No anonymity	Disclosed	Medium security

3.1.5 Data Security Matrix

This section highlights the data that is handled by GlobaLeaks and how different protection schemes are applied to GlobaLeaks handled data.

The following information types are the one involved within GlobaLeaks:

Information type	Description
Questionnaire answers	The data associated with a submission such as the filled forms and selectors provided by the Whistleblower.
Submission attachments	The files associated with a submission.
Platform configuration	The data for the configuration and customization of the platform.
Software files	All the files that the software requires to work, including configuration defaults.
Email notifications	Data sent to notify recipients of a new report via email

Below a matrix showing different security measures applied on data.

Information type	Encryption	Filters	Sanitization
Questionnaire answers	Encrypted on the database with per-user / per-submissions keys	Keyword filters	Antispam, Anti XSS
Submission attachments	Encrypted on the filesystem with per-user / per/submissions keys	Extension blocking, Antivirus	N/A
Email notifications	Encrypted with PGP when recipients keys are available	Antispam to prevent flooding	N/A

3.1.6 Threats to Anonymity and Confidentiality

In this section we highlight several threats that require specific explanation.

Browser History and Cache

GlobaLeaks tries to avoid, by using properly crafted HTTP headers and other techniques, leaking information into any user's browser history or cache. This privacy feature cannot guarantee the safety of the user against a forensics analysis of their browser cache and/or history, but it is provided as an additional safety measure.

Metadata

Every file can contain metadata related to the author or the whistleblower. The cleanup of metadata of submitted files is a particular topic that attempts to protect an “unaware” whistleblower from including information in a document that may put their anonymity at risk. In the context of GlobaLeaks, by default no automatic metadata cleanup is implemented because metadata is considered fundamental part of the original evidence that shall be preserved and not invalidated. For this reason metadata cleanup is an optional operation that could be suggested to Whistleblowers or operated by Recipients when sharing the document with other persons. When sharing files to external third parties Recipients are invited to print the document and provide a hard copy. This process is helpful to ensure that recipients only share what they see without risking to share sensitive information contained in the metadata of the files of which they may not be aware of. To get to know more about metadata and the best practices on redacting metadata from digital files we recommend reading the article [Everything you wanted to know about media metadata, but were afraid to ask](#) by Harlo Holmes. A valuable tool supporting these advanced procedures is the [Metadata Anonymization Toolkit](#)

Malware and Trojans

GlobaLeaks could not prevent an attacker to use the platform maliciously trying to target recipients users with malware and trojans in general. Considering this and in order to be less vulnerable to risks of data exfiltration perpetrated with trojans, Recipients should always implement proper operation security by possibly using a laptop dedicated to reports visualization and open file attachments on computers disconnected from the network and other sensible information. Wherever possible in their operation they should adopt specialized secure operation systems like [QubesOS](#) or [Tails](#) or and at least run an up-to-date Anti-Virus software.

Network and Reverse Proxies

GlobaLeaks is intended to be used by end users with a direct Tor or TLS connection from the browser of the user to the application backend. Any use of Network and Reverse Proxies in front of the application is discouraged; those appliances could significantly interfere with the application and lower its security vanishing any confidentiality and anonymity measure implemented within GlobaLeaks.

Data Stored Outside the Platform

GlobaLeaks does not provide any kind of security for data that is stored outside the GlobaLeaks system. Is responsibility of Recipients to protect the data they download from the platform on their personal computer or that they share with other persons with external usb drives. The operatin system used or the pen drive adoptet should offer encryption and guarantee that in case of device loss or stealing no one could access the data therein contained.

Environmental Factors

GlobaLeaks does not protect against environmental factors related to actors' physical locations and/or their social relationships. For example if a user has a video bug installed in their house to monitor all their activity, GlobaLeaks cannot protect them. Likewise, if a whistleblower, who is supposed to be anonymous, tells their story to friends or coworkers, GlobaLeaks cannot protect them.

Incorrect Data Retention Policies

GlobaLeaks implements by default a strict data retention policy of 90 days to enable users to operate on the report for a limited time necessary for the investigations. If the platform is configured to retain every report for a long time and Recipients do not manually delete the unnecessary reports, the value of the platform data for an attacker increases and so too does the risk.

Human Negligence

While we do provide the Administrator the ability to fine tune their security related configurations, and while we do continuously inform the users about their security related context at every step of interactions, GlobaLeaks cannot protect against any major security threats coming from human negligence. For example, if a Whistleblower submits data that a third party (carrying on an ex-post facto investigation) can use to identify them as the unique owner or recent viewer of that data, then the Whistleblower cannot be protected by GlobaLeaks.

Advanced Traffic Analysis

An attacker monitoring HTTPS traffic, with no ability to decrypt it, can still identify the role of the intercepted users, because the Whistleblower, Recipient and Administrator interfaces generate different network traffic patterns. GlobaLeaks does not provide protection against this threat. We suggest using [Tor pluggable transports](#) or other methods that provide additional protection against this kind of attack.

3.2 Application Security

The GlobaLeaks software tries to conform with industry standard best and practices and its security is a result of applied research.

This document tries to detail every aspect implemented by the application in relation to the security design.

3.2.1 Architecture

The software is made up of two main components: a **Backend** and a **Client**:

- The Backend is a python backend that runs on a physical backend and exposes a [REST API](#).
- The Client is a JavaScript client-side web application that interacts with Backend only through [XHR](#).

3.2.2 Anonymity

Users's anonymity is protected by means of the [Tor](#) technology.

The entire application considers to avoid logging of sensible metadata that could lead to identification of whistleblowers.

3.2.3 Authentication

The confidentiality of the authentication is protected by either [Tor Onion Services v3](#) or [TLS version 1.2+](#).

This section describes the authentication methods implemented by the system.

Password

By accessing the login web interface, **Administrators** and **Recipients** need to insert their respective **Username** and **Password**. If the password submitted is valid, the system grants access to the functionality available to that user.

Receipt

Whistleblowers access their **Reports** by using an anonymous **Receipts**, which are random generated 16 digits sequences created by the Backend when the Report is first submitted. The reason of this format of 16 digits is that it resembles a standard phone number, making it easier for the whistleblowers to conceal their receipts.

3.2.4 Password Security

The following password security measures implemented by the system.

Password Storage

Password are never stored in plaintext but the system maintain at rest only an hash. This apply to every authentication secret included whistleblower receipts.

The platform stores Users' passwords hashed with a random 128 bit salt, unique for each user.

Passwords are hashed using [Argon2](#), a key derivation function that was selected as the winner of the [Password Hashing Competition](#) in July 2015.

The hash involves a per-user salt for each user and a per-system salt for whistleblowers.

Password Complexity

The system enforces the usage of complex password by implementing a custom algorithm necessary for ensuring a reasonable entropy of each authentication secret.

Password are scored in three levels: Strong, Acceptable, Insecure.

- Strong: A strong password should be formed by capital letters, lowercase letters, numbers and a symbols, be at least 12 characters long and include a variety of at least 10 different inputs.
- Acceptable: An acceptable password should be formed by at least 3 different inputs over capital letters, lowercase letters, numbers and a symbols, be at least 10 characters and include a variety of at least 7 different inputs.
- Insecure: A password ranked below the strong or acceptable levels is marked as insecure and not accepted by the system.

We encourage each end user to use [KeePassXC](#) to generate and retain strong and unique passphrases.

Two Factor Authentication

The system implements Two Factor Authentication (2FA) based on TOTP based on [RFC 6238](#) algorithm and 160 bits secrets.

Users are enabled to enroll for 2FA via their own preferences and administrators can optionally enforce this requirement.

We recommend using [FreeOTP](#) available [for Android](#) and [for iOS](#).

Password Change on First Login

The system enforces users to change their own password at their first login.

Administrators could as well enforce password change for users at their next login.

Periodic Password Change

By default the system enforces users to change their own password at least every year.

This period is configurable by administrators.

Proof of Work on Login and Submissions

The system implements an automatic [Proof of Work](#) on every login that requires every client to request a token, solve a computational problem before being able to perform a login or file a submission.

Rate Limit on Anonymous Sessions

The system implements rate limiting on whistleblowers' sessions preventing to execute more than 5 requests per second.

Slowdown on Failed Login Attempts

The system identifies multiple failed login attempts and implement a slowdown procedure where an authenticating client should wait up to 42 seconds to complete an authentication.

This feature is intended to slow down possible attacks requiring more resources to users in terms of time, computation and memory.

Password Recovery

In case of password loss users could request a password reset via the web login interface clicking on a [Forgot password?](#) button present on the login interface.

When this button is clicked, users are invited to enter their username or an email. If the provided username or the email correspond to an existing user, the system will provide a reset link to the configured email.

By clicking the link received by email the user is then invited to configure a new email different from the previous.

In case encryption is enabled on the system, a user clicking on the reset link would have first to insert their [Account Recovery Key](#) and only in case of correct insertion the user will be enabled to set a new password.

3.2.5 Web Application Security

This section describes the Web Application Security implemented by the software in adherence with the [OWASP Security Guidelines](#).

Session Management

The session implementation follows the [OWASP Session Management Cheat Sheet](#) security guidelines.

The system assigns a Session to each authenticated user. The Session ID is 256bits long secret generated randomly by the backend. Each session expire accordingly to a timeout of 60 minutes. Session IDs are exchanged by the client with the backend by means of an header ([X-Session](#)) and do expire as soon that users close their browser or the tab running [GlobaLeaks](#). Users could explicitly log out via a logout button or implicitly by closing the browser.

Cookies and XSRF Prevention

Cookies are not used intentionally to minimize XSRF attacks and any possible attack based on them. Instead than using Cookies authentication is based on a custom HTTP Session Header sent by the client on authenticated requests.

HTTP Headers

The system implements a large set of HTTP headers specifically configured to improve the software security and achieves [score A+](#) by [Security Headers](#) and [score A+](#) by [Mozilla Observatory](#).

Strict-Transport-Security

The system implements strict transport security by default.

```
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```

The default configuration of the application see this feature disabled.

Content-Security-Policy

The backend implements a strict [Content Security Policy \(CSP\)](#) preventing any interaction with resources of third parties and restricting execution of untrusted user input:

```
Content-Security-Policy: base-uri 'none'; default-src 'none'; form-action 'none'; frame-  
-ancestors 'none'; sandbox;
```

On this default policy are then implemented specific policies in adherence to the principle of least privilege.

For example:

- the index.html source of the app is the only resource enabled to load scripts from the same origin;
- every dynamic content is strictly sandboxed on a null origin;
- every untrusted user input or third party library is executed in a sandbox limiting its interaction with other application components.

Cross-Origin-Embedder-Policy

The backend implements the following [Cross-Origin-Embedder-Policy \(COEP\)](#):

```
Cross-Origin-Embedder-Policy: require-corp
```

Cross-Origin-Opener-Policy

The backend implements the following [Cross-Origin-Opener-Policy \(COOP\)](#):

```
Cross-Origin-Resource-Policy: same-origin
```

Cross-Origin-Resource-Policy

The backend implements the following [Cross-Origin-Resource-Policy \(CORP\)](#):

```
Cross-Origin-Resource-Policy: same-origin
```

Permissions-Policy

The backend implements the following Permissions-Policy header configuration to limit the possible de-anonymization of the user by disabling dangerous browser features:

```
Permissions-Policy: camera=('none') display-capture=('none') document-domain=('none')  
↪ fullscreen=('none') geolocation=('none') microphone=('none') speaker=('none')
```

X-Frame-Options

In addition to the implement Content Security Policy of level 3 that prevent the application to be included into an IFrame, the backend implements the outdated X-Frame-Options header to ensure that iframes are always prevented in any circumstance also on outdated browsers:

```
X-Frame-Options: deny
```

Referrer-Policy

Web-browsers usually attach referrers in their http headers as they browse links. The platform enforces a referrer policy to avoid this behaviour.

```
Referrer-Policy: no-referrer
```

X-Content-Type-Options

When setting up Content-Type for the specific output, we avoid the automatic mime detection logic of the browser by setting up the following header:

```
X-Content-Type-Options: nosniff
```


Cache-Control

To prevent or limit the forensic traces left on the device used by whistleblowers and in the devices involved in the communication the platform, as by section 3. [Storing Responses in Caches of RFC 7234](#) the platform uses the `Cache-control` HTTP header with the configuration `no-store` to instruct clients and possible network proxies to disable any sort of data cache.

```
Cache-Control: no-store
```

Crawlers Policy

For security reasons the backend instructs crawlers to avoid any caching and indexing of the application and uses the `Robots.txt` file to enable crawling only of the home page; indexing of the home page is in fact considered best practice in order to be able to widespread the information about the existence of the platform and ease access to possible whistleblowers.

The configuration implemented is the following:

```
User-agent: *
Allow: /$
Disallow: *
```

As well the platform instruct crawlers to not keep any cache by injecting the following HTTP header:

```
X-Robots-Tag: noarchive
```

For high sensitive projects where the platform is intended to remain hidden and communicated to possible whistleblowers directly the platform could be as well configured to disable indexing completely.

The following is the HTTP header injected in this case:

```
X-Robots-Tag: noindex
```

Anchor Tags and External URLs

The client opens external urls on a new tab independent from the application context by setting `rel='noreferrer'` and `target='_blank'` on every anchor tag.

```
<a href="url" rel="noreferrer" target="_blank">link title</a>
```

Input Validation

The application implement strict input validation both on the backend and on the client

On the Backend

Each client request is strictly validated by the backend against a set of regular expressions and only requests matching the expression are then processed.

As well a set of rules are applied to each request type to limit possible attacks. For example any request is limited to a payload of 1MB.

On the Client

Each server output is strictly validated by the Client at rendering time by using the angular component `ngSanitize.$sanitize`

Form Autocomplete OFF

Form implemented by the platform make use of the HTML5 form attribute in order to instruct the browser to do not keep caching of the user data in order to predict and autocomplete forms on subsequent submissions.

This is achieved by setting `autocomplete="off"` on the relevant forms or attributes.

3.2.6 Network Security

Connection Anonymity

Users's anonymity is offered by means of the implementation of the [Tor](#) technology. The application implements an Onion Service v3 and advices users to use the Tor Browser when accessing to it.

Connection Encryption

Users' connection is always encrypted, by means of the [Tor Protocol](#) while using the Tor Browser or by means of [TLS](#) when the application is accessed via a common browser.

The use of the Tor is recommended over HTTPS for its advanced properties of resistance to selective interception and censorship that would make it difficult for a third party to selectively capture or block access to the site to specific whistleblower or company department.

The software enables as well easy setup of HTTPS offering both automatic setup via [Let'sEncrypt](#) and manual setup.

TLS Certificates are generated using using [NIST Curve P-384](#).

The configuration enables only TLS1.2+ and is fine tuned and hardened to achieve [SSL Labs grade A+](#).

In particular only following ciphertexts are enabled:

```
TLS13-AES-256-GCM-SHA384
TLS13-CHACHA20-POLY1305-SHA256
TLS13-AES-128-GCM-SHA256
ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-CHACHA20-POLY1305
ECDHE-RSA-CHACHA20-POLY1305
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256
```

Network Sandboxing

The GlobaLeaks backend integrates [iptables](#) by default and implements strict firewall rules that restrict network incoming network connection to HTTP and HTTPS connection on ports 80 and 443.

In addition the application makes it possible to anonymize outgoing connections that could be configured to be sent through Tor.

3.2.7 Data Encryption

Submissions data, file attachment, messages and metadata exchanged between whistleblowers and recipients is encrypted using the GlobaLeaks [Encryption Protocol](#).

In addition to this GlobaLeaks implements many other encryption components and the following is the set of the main libraries and their main usage:

- [Python-NaCL](#): is used for implementing data encryption
- [PyOpenSSL](#): is used for implementing HTTPS
- [Python-Cryptography](#): is used for implementing authentication
- [Python-GnuPG](#): is used for encrypting email notifications and file downloads by means of `PGP`

3.2.8 Application Sandboxing

The GlobaLeaks backend integrates [AppArmor](#) by default and implements a strict sandboxing profile enabling the application to access only the strictly required files. As well the application does run under a dedicated user and group “globaleaks” with reduced privileges.

3.2.9 Database Security

The GlobaLeaks backend implements an hardened local SQLite database accessed via the SQLAlchemy ORM.

This design choice is selected in order to ensure that the application could fully control its configuration implementing a large set of security measures in adherence to the [security recommendations by SQLite](#)

Secure Deletion

The GlobaLeaks backend enables a SQLite capability for secure deletion that automatically makes the database overwrite the data upon each delete query:

```
PRAGMA secure_delete = ON
```

Auto Vacuum

The platform enables a SQLite capability for automatic vacuum of deleted entries with automatic recall of unused pages:

```
PRAGMA auto_vacuum = FULL
```

Limited Database Trust

The GlobaLeaks backend utilizes the SQLite [trusted_schema](#) pragma to limit the trust put on the database in order to limit exploitation on which the database could be maliciously corrupted by an attacker.

```
PRAGMA trusted_schema = OFF
```

Limited Database Functionalities

The GlobaLeaks backend runs specific SQLite functionalities to reduce the types of queries to the ones necessary to run the application and reduce the possibilities of exploitation in case of successful SQL injection attacks.

This is implemented by using the ``conn.set_authorizer`` API and using a strict authorizer callback that authorizes the execution of a limited set of SQL instructions:

```
SQLITE_FUNCTION: count, lower, min, max
SQLITE_INSERT
SQLITE_READ,
SQLITE_SELECT
SQLITE_TRANSACTION
SQLITE_UPDATE
```

3.2.10 DoS Resiliency

To avoid applicative and database denial of service, GlobaLeaks apply the following measures:

- It tries to limit the possibility of automating any operation by implement a proof of work on each unauthenticated request (hashcash)
- It applies rate limiting on any authenticated session
- It is written to limit the possibility of triggering CPU intensive routines by an external user (e.g. by implementing limits on queries and jobs execution time)
- It implements monitoring of each activity trying to implement detection of attacks and implement proactively security measures to prevent DoS (e.g. implementing slowdown on fast-operations)

3.2.11 Other Measures

Browser History and Forensic Traces

The whole application is designed keeping in mind to try to avoid or reduce the forensic traces left by whistleblowers on their devices while filing their reports.

When the accessed via the Tor Browser, the browser guarantees that no persistent traces are left on the device of the user.

In order to prevent or limit the forensic traces left in the browser history of the users accessing the platform via a common browser, the application avoids to change URI during whistleblower navigation. This has the effect to prevent the browser to log the activities performed by the user and offers high plausible deniability protection making the whistleblower appear as a simple visitor of the homepage and avoiding an actual evidence of any submission.

Secure File Management

Secure File Download

Any attachment file uploaded by anonymous whistleblowers could possibly contain malware that could be provided intentionally or not. It is always recommended if possible to download files and access them on an air-gapped machine disconnected from the network and other sensible devices. In order to safely download files and move them using a USB stick the application offers the possibility to perform a report export enabling the download of a ZIP archive including all the report content and thus reducing risks of executing files on-click during the file transfer from a device to one other.

Safe File Opening

For conditions where the whistleblower trustworthiness has been validated or in projects subject to a low risk threat model, the application offers an integrated file viewer that benefiting of modern browser sandboxing capabilities enable opening of a limited set of file types that are considered more safe and in a way that is better than accessing files directly through the operation system. This option is disabled by default and it is recommended that administrators of the project enable this feature only after proper evaluation and only in conditions in which it possible to ensure that recipients' browsers are always maintained up-to-date. Among the advantages of this novel viewer is the fact that access to files is performed within a controlled sandbox, via a set of controlled libraries and avoiding usage of any permanent storage and thus limiting the the exposure of the opened file.

The set of file formats supported by this viewer are:

- AUDIO
- CSV
- IMAGE
- PDF
- VIDEO
- TXT

The default configuration of the application see this feature disabled.

PGP Encryption

The system offers an optional PGP encryption feature.

When enabled, users could possibly enable a personal PGP key that will be used by the system to encrypt email notifications and encrypt downloaded files on-the-fly.

This is a recommended feature for high risk threat models in association with the usage of air-gapped systems for the visualization of the reports.

The default configuration of the application see this feature disabled.

Encryption of Temporary Files

Files being uploaded and temporarily stored on the disk during the upload process are encrypted with a temporary, symmetric AES-key in order to avoid writing any part of an unencrypted file's data chunk to disk. The encryption is done in "streaming" by using AES 128bit in CTR mode. The key files are stored in memory and are unique for each file being uploaded.

Secure File Delete

Every file deleted by the application is overwritten before releasing the file space on the disk.

The overwrite routine is performed by a periodic scheduler and acts as following:

- A first overwrite writes 0 on the whole file;
- A second overwrite writes 1 on the whole file;
- A third overwrite writes random bytes on the whole file.

Exception Logging and Redaction

In order to quickly diagnose potential problems in the software when exceptions in clients are generated, they are automatically reported to the backend. The backend temporarily caches these exceptions and sends them to the backend administrator via email.

In order to prevent inadvertent information leaks the logs are run through filters that redact email addresses and uuids.

Entropy Sources

The main source of entropy for the platform is `/dev/urandom`.

UUIDv4 Randomness

Resources in the system like submissions and files are identified by a UUIDv4 in order to not be guessable by an external user and limit possible attacks.

TLS for SMTP Notification

All of the notifications are sent through SMTP over TLS encrypted channel by using SMTP/TLS or SMTPS, depending on the configuration.

3.3 Encryption Protocol

GlobaLeaks implements an encryption protocol specifically designed for anonymous whistleblowing applications.

The protocol has been developed and validated in collaboration with the [Open Technology Fund](#) and represents a tradeoff between security and usability intended to provide easy use by whistleblowers and reasonable security from attackers seizing the backend and attempting brute-force decryption.

Encryption is implemented for each submission protecting questionnaire's answers, comments, attachments and involved metadata. The keys involved in the encryption are per-user and per-report and this guarantees that only whistleblowers and their recipients could access the reports. Such an implementation implies that in case users forget their password, they would lose any possibility of access to the data contained in their accounts.

In order to enable users to be able to recover their own account in case of loss of their password, the system implements an [Key Recovery](#) mechanism and make available to every user an Account Recovery Key. This measure ensures that users in possession of their own Account Recovery Key could always restore their own access to their own account and the data contained therein.

In order to protect the system from data loss in case of users' loss of both the password and the account recovery key, the system could be configured enabling a [Key Escrow](#) mechanism and delegating to administrators the role and responsibility to support users recovering access to their own accounts and the data contained therein. Such a capability has the value to add resiliency to the project protecting from any data loss in case of users' death or in condition of conflict of interest inside the recipient team. The same capability has the drawback that users with access to escrow keys could possibly access others users accounts and the data contained therein. Project owners are invited to wisely choose if enabling this feature depending on the project's threat model and to document the choice on the project's privacy policies.

3.3.1 Encryption's Workflow

- Users choose a personal secure password at first login done using an account activation link;
- The system creates a personal user asymmetrical keypair and stores the private key symmetrically encrypted with a secret derived from the personal user password;
- The private key of each user is protected with the Key Recovery mechanism and if enabled with the Key Escrow mechanism;
- The whistleblower files a report;
- The system assigns personal numeric 16-digits receipt for the whistleblower;
- The system generates an asymmetrical keypair for the whistleblower and stores the private key symmetrically encrypted with a secret derived from the receipt of the whistleblower;
- The system generates an asymmetrical keypair for the encryption of the report, the attached files, the comments and the involved metadata and stores a copy of the private key encrypted for each involved user by using their own public key;
- The system encrypts the report, the attached files, the comments and the metadata with the public key generated for the report;

- The system grants every involved user access to their reports and enable them to communicate by automatically locking and unlocking involved keys when a report is accessed or new communication is performed.

3.3.2 Encryption's Details

Algorithms

Type	Implementation
Asymmetric encryption	Libsodium SealedBoxes , an encryption implementation that combines Curve25519, XSalsa20 and Poly1305 algorithms.
Symmetric encryption	Libsodium SecretBoxes , an encryption implementation that combines XSalsa20 and Poly1305.

Users' Credentials

The system used two different type of credentials depending on the user role:

Credentials type	User role
Passwords	Passwords are used for authenticating users identified by a username
Receipts	Receipts are 16-digits random secrets used for authenticating anonymous whistleblowers

Assumptions:

- The system enforces strong password complexity;
- The system enforces expiration of receipts according to a strict data retention policy limiting the concurrent number of active receipts;

Users' Keys

Type	Generation	Storage
ECC Curve25519 key-pair	Generated by the backend at first user login for authenticated users and on submission for whistleblowers	Keys are stored on the backend encrypted using symmetric encryption. The symmetric key used for encrypting users' keys is derived from the users' credentials using the KDF function Argon2ID . The parameters for Argon2ID used for KDF are chosen stronger than the parameters one used for authentication of related user which the hash is stored. The parameters are chosen to require 128MB per Login and 1 second of computation.

Data Encryption's Keys

Type	Generation	Storage
256 bit keys	Generated by the backend for each report	Keys and stored on backend filesystem encrypted using asymmetric encryption by means of Users' and Whistleblower's keys respectively

3.3.3 Key Generation

Users' encryption keys are automatically generated during the first user login and secured by means of the user passphrase used for login. This simple but effective key generation policy requires users to perform their first login before being enabled to receive reports.

3.3.4 Key Recovery

The system implements a key recovery system by means of a recovery key and symmetric encryption.

Upon generation of a user key, the private key is symmetrically encrypted with a randomly generated recovery key.

For usability reasons, this recovery is kept as well encrypted on the backend making it possible for logged users in possession of their password to retrieve and print their own account recovery key.

3.3.5 Key Escrow

The system implements an optional key escrow mechanism in order to limit data loss in case of users' password loss.

Key escrow can be enabled during the initial application wizard or alternatively could be enabled in the advanced settings of the software.

We advise enabling this option if you would like to protect whistleblowers' submissions from being lost in the situation where recipients lose their passwords. On the other hand, we would not advise using this feature if you want to setup a system where only recipients are able to access submissions.

When the option is enabled the system will generate and assign an escrow key and assign it to the administrator that has enabled the feature; the key will be furtherly used by the system to encrypt every system key preserving a copy that could be unlocked by any administrator in the availability of the escrow key.

Administrators with access to the escrow key will be able to support any internal user in case of password loss and issue password reset. As well they will be able to grant this same privilege to other administrators or disable the feature completely.

3.4 Security Audits

GlobaLeaks is periodically subject to independent security audits in order to verify and improve the security of the system.

We try to get it audited at least every 2 years thanks to funding opportunities. Each user and adopter as well sometimes is able to fund additional audits.

This page lists the currently publicly available reports.

If you have carried or have the possibility to sponsor a security audit please email us at info@globaleaks.org. This would be particularly important for the general software security. When asking a company to audit the software please always remember to ask for the possibility to publish the report before this is performed; many auditors in fact may not agree with publishing afterwards and this happened many times with waste of project resources.

We additionally invite independent security researchers to apply to our [Bug Bounty](#) initiative, which it's hosted on [HackerOne](#).

Date	Auditor	Goal	Report
2013	iSecPartners	Architecture Audit	Report
2013	Cure53	Web Security Audit	Report
2014	LeastAuthority	Source Code Audit	Report
2018	SubGraph	Overall Audit	Report
2019	RadicallyOpenSecurity	Crypto Audit, Multi-tenancy Audit, Overall Audit	Report
2022	RadicallyOpenSecurity	Server Source Code Audit, Client Pentest, OpSec for Whistleblowers, OpSec for Server Administrators	Report

USER DOCUMENTATION

4.1 Common to All Users

4.1.1 Login

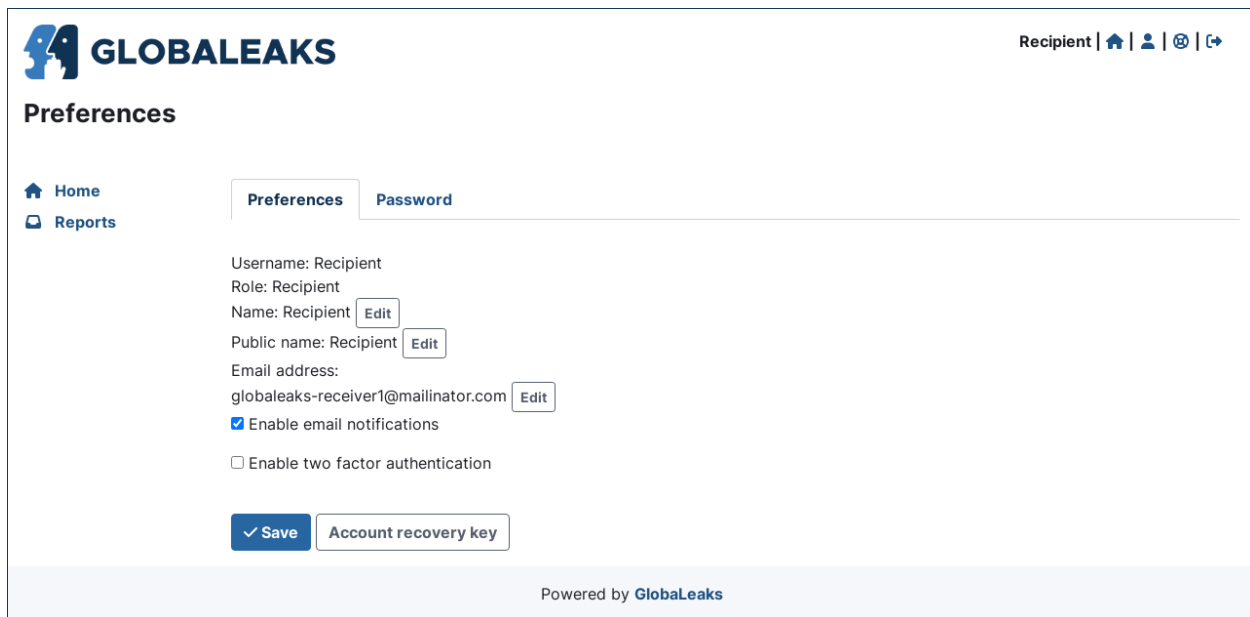
Users could login by accessing the `/#/login` page.



The screenshot shows the login interface for Globaleaks. At the top left is the Globaleaks logo, which consists of a stylized blue 'G' with a white face and the word 'GLOBALEAKS' in bold blue capital letters. Below the logo is the text 'Log in'. There are two input fields: the first is labeled 'Username' with a person icon, and the second is labeled 'Password' with a lock icon. Below these fields are two buttons: a blue button with a white arrow and the text 'Log in', and a white button with a grey border and the text 'Forgot password?'. At the bottom of the form, there is a light grey footer bar with the text 'Powered by [GlobaLeaks](#)'.

4.1.2 Access the User Preferences

After login Users could access their preferences by clicking the **Preferences** link present in the login status bar.



The screenshot shows the GLOBALEAKS web interface. At the top left is the GLOBALEAKS logo. At the top right, the user is identified as 'Recipient' with icons for home, user profile, settings, and a share icon. Below the logo is the 'Preferences' title. On the left is a sidebar with 'Home' and 'Reports' links. The main content area has two tabs: 'Preferences' (active) and 'Password'. Under the 'Preferences' tab, the following information is displayed: Username: Recipient, Role: Recipient, Name: Recipient (with an 'Edit' button), Public name: Recipient (with an 'Edit' button), Email address: globaleaks-receiver1@mailinator.com (with an 'Edit' button), a checked checkbox for 'Enable email notifications', and an unchecked checkbox for 'Enable two factor authentication'. At the bottom of the form are a 'Save' button and an 'Account recovery key' button. The footer of the page states 'Powered by GLOBALEAKS'.

4.1.3 Change Your Password

Users could change their own password by accessing the Password tab present in the Preferences page.



This screenshot shows the 'Password' tab within the GLOBALEAKS 'Preferences' section. The interface is identical to the previous screenshot, but the 'Preferences' tab is inactive, and the 'Password' tab is active. The main content area contains three password input fields: 'Current password *', 'New password *', and 'Type your new password again *'. Each field is followed by a light blue input box. At the bottom of the form is a 'Save' button. The footer of the page states 'Powered by GLOBALEAKS'.

4.1.4 Reset Your Password

Users could request a password reset via the `/#/login` page by clicking the `Forgot password?` button.

After clicking the button users are requested to type their own username or email address.

The first screenshot shows the login page with the 'Forgot password?' button. The second screenshot shows the password reset request form. The third screenshot shows the confirmation message after a password reset request is submitted.

Log in

Username

Password

Log in Forgot password?

Powered by [GlobaLeaks](#)

Password reset

Enter your account's username or your email address to request a password reset.

Submit

Powered by [GlobaLeaks](#)

Password reset

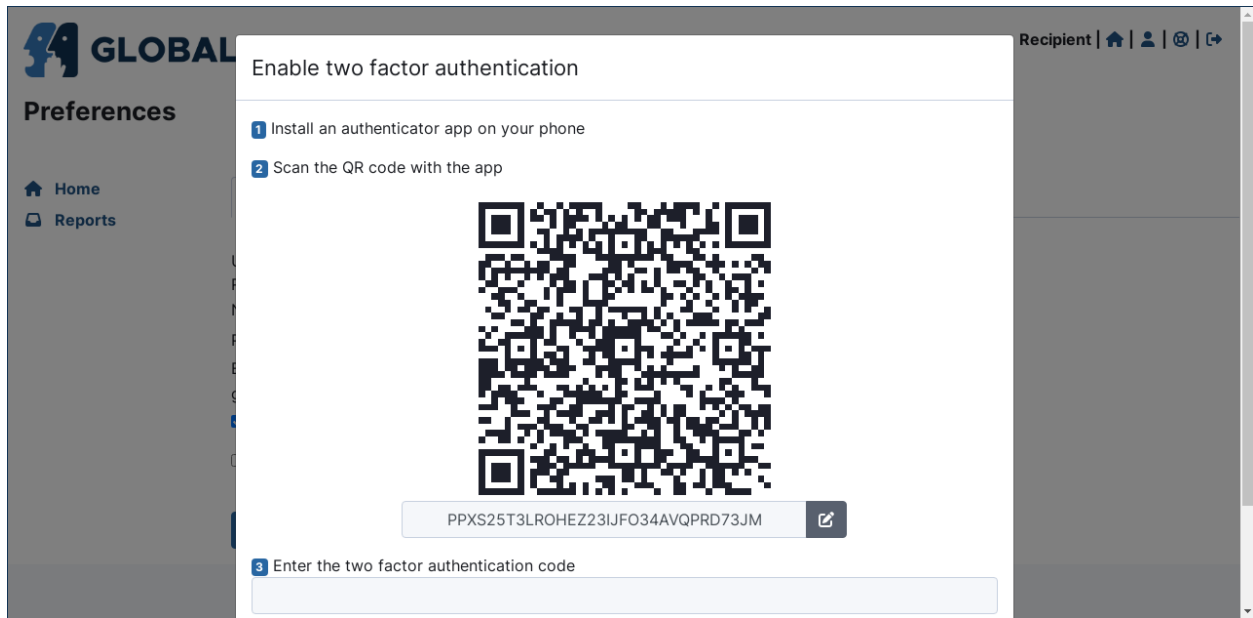
Password reset requested. Please check your inbox for further instructions.

Powered by [GlobaLeaks](#)

4.1.5 Enable Two-Factor-Authentication (2FA)

Users could enable Two-Factor-Authentication by clicking the `Enable two factor authentication` option inside the `Preferences` page.

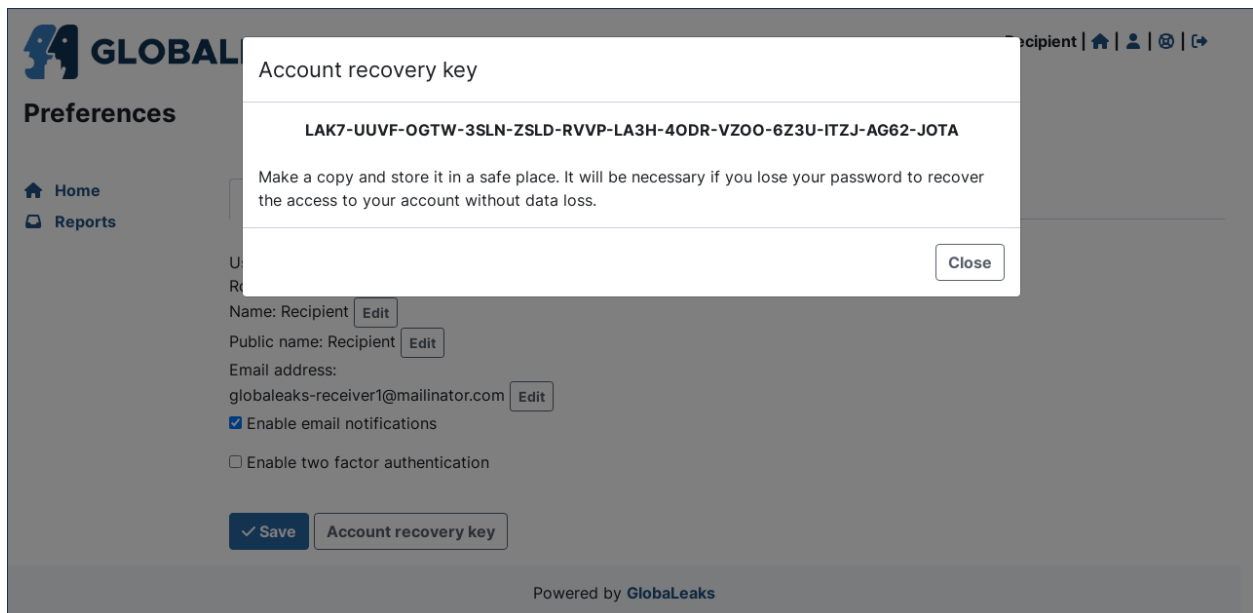
To enable the feature the user requires to have a phone with installed a common `Authenticator APP` implementing the TOTP standard as by [RFC 6238](#)



4.1.6 Access and Save Your Account Recovery Key

Users could access their own Account Recovery key by clicking the Account Recovery Key button present in the Preferences page.

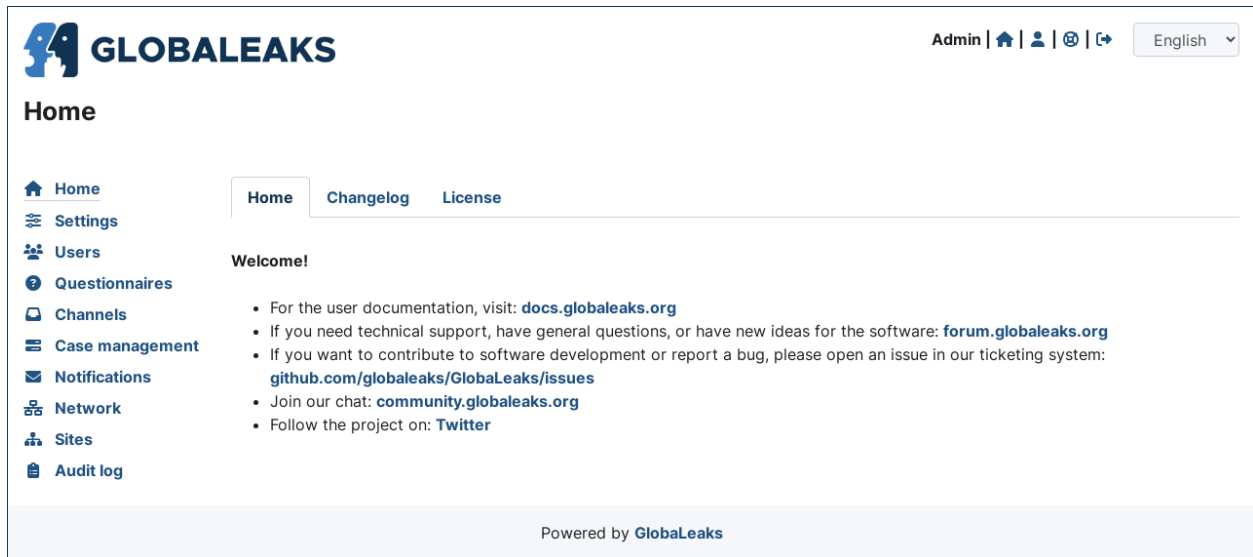
This is a fundamental step that any user should do at their first login after activating their own account in order to backup their own account recovery key and get sure to not incur in data loss due to password loss.



4.2 For Administrators

4.2.1 User Interface

This section offers you a summary of the user interface offered to Admin users.



Through the menu you could access the following administrative sections:

1. Settings
2. Users
3. Questionnaires
4. Channels
5. Case management
6. Notification
7. Network
8. Sites
9. Audit log

Settings


This is the section that offers you all the main customization possibilities necessary for implementing a basic and functional whistleblowing site.






This section is furtherly divided in:

1. Settings
2. Theme customization
3. Languages
4. Text customization
5. Advanced settings


Settings


In this section is configurable the logo and all the texts of the main user interfaces.


 **GLOBALEAKS**


Admin |  |  |  |  | English 


Site settings


 Home


 Settings


 Users


 Questionnaires


 Channels

 Case management

 Notifications

 Network

 Sites

 Audit log

Settings


Theme customization

Languages

Text customization

Advanced

Logo



Project name

GLOBALEAKS

Description

Secure whistleblowing platform based on GlobaLeaks free and open-source software.

Homepage title

Presentation

Question to solicit possible whistleblowers

Whistleblowing button

File a report

Disclaimer

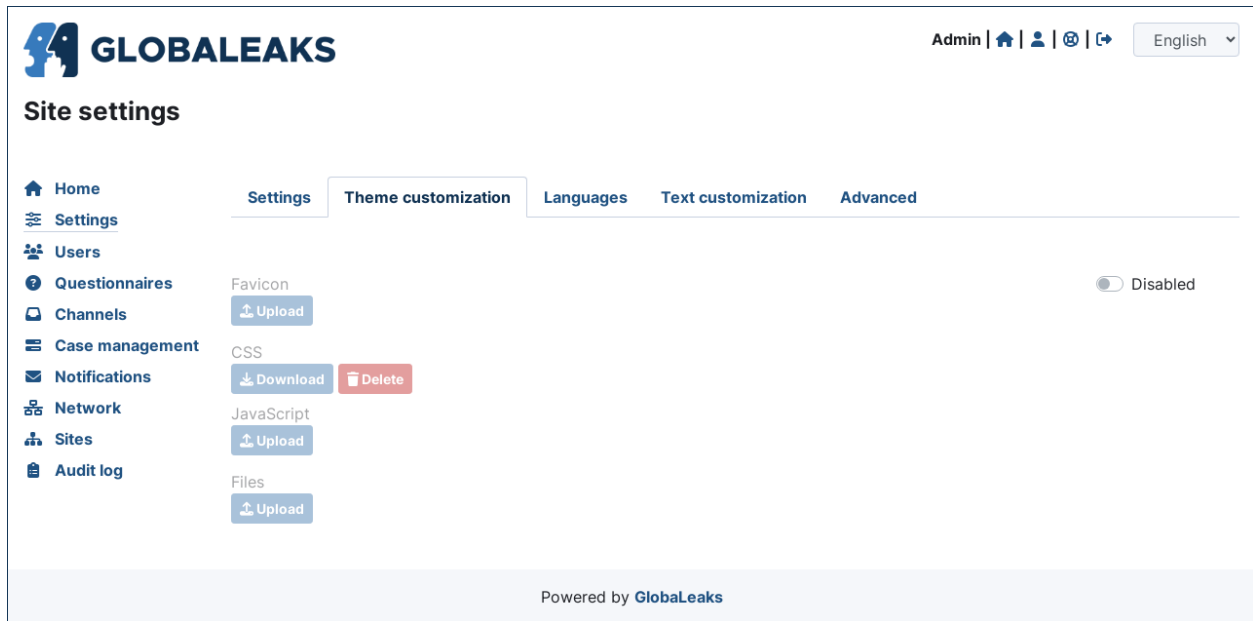
Footer

✓ Save

Powered by **GlobaLeaks**

Theme Customization

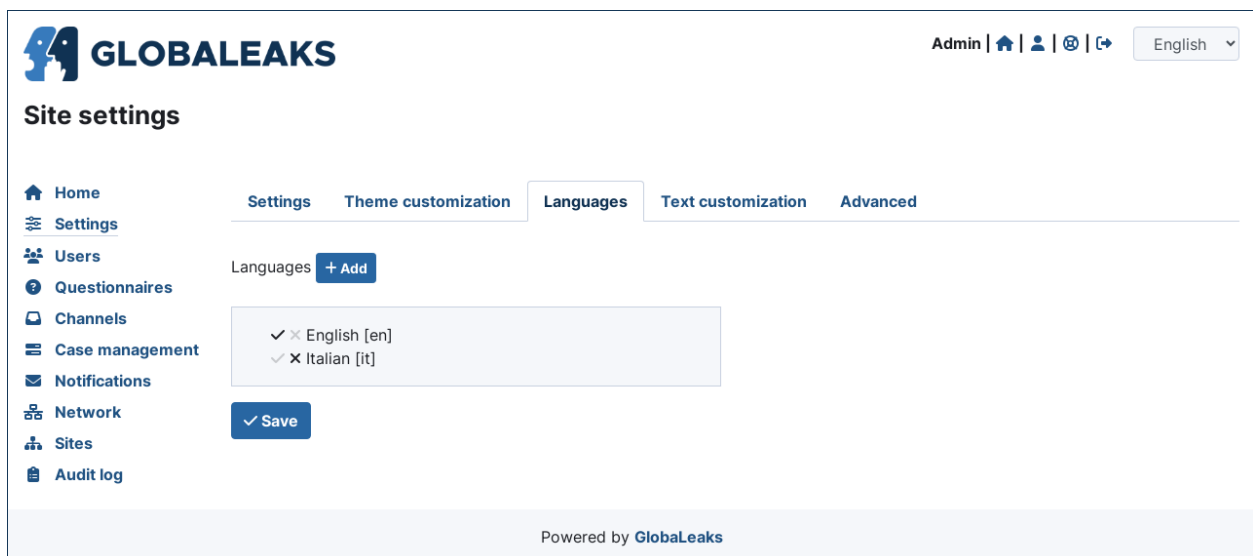
In this section could be loaded CSS and Javascript files necessary to customize the interface.



Languages

In this section you could enable all the languages required by your project and configure the default language.

Note: Thanks to the [Localization Lab](#) and our great volunteer community, the software is already available and continuously made available in a lot of languages. This aspect of internationalization is crucial in many projects. In case you are starting a project and the required languages are not available we strongly invite you to register on our [web translation platform](#) offered by [Transifex](#) and support yourself the translation. Internationalization and Localization is in fact are crucial for the success of a whistleblowing project. Thank you!



Text Customization







Here could be configured overrides for any of the texts of the platform and of their translation.

The screenshot shows the 'Text customization' settings page in the GLOBALEAKS admin interface. The page has a sidebar on the left with navigation links: Home, Settings, Users, Questionnaires, Channels, Case management, Notifications, Network, Sites, and Audit log. The main content area has tabs for Settings, Theme customization, Languages, Text customization (selected), and Advanced. Under the 'Text customization' tab, there is a 'Language:' dropdown menu set to 'English'. Below it is an 'Add custom text' dropdown menu. A '+ Add' button is located below the dropdown. At the bottom, there is a table with three columns: 'Original text', 'Original translation', and 'Custom translation'. The footer of the page states 'Powered by GLOBALEAKS'.











Original text	Original translation	Custom translation
---------------	----------------------	--------------------

Advanced Settings

In this section could be configured a set of advanced settings.


Admin |  |  |  |  | English 

Site settings

 Home
  Settings
  Users
  Questionnaires
  Channels
  Case management
  Notifications
  Network
  Sites
  Audit log

Settings
 Theme customization
 Languages
 Text customization
 Advanced

☐ Disable submissions

☒ Enable encryption

☒ Enable administrators to change user passwords

 Administrators authorized to change user passwords:

Admin

☒ Enable file viewer

☐ Enable PGP

☐ Enable simplified login

☒ Enable search engines indexing

 Default questionnaire

GLOBALEAKS

 Text shown on top of the interface for selecting channels

Select a reporting channel:

☒ Show contexts in alphabetical order

 Size limit for file attachments (megabytes)

30

☐ Require two factor authentication

 Password change interval

365

 For security reasons, password changes are required at regular intervals.
 Set the value to 0 to disable this feature.

 Number of days till notifying unread reports to users

7

 Custom support URL

☒ Disable the privacy panel

☒ Enable custodian user role

☐ Enable scoring system

 Logging level

ERROR

 Anomaly detection thresholds



	Low	High
Available disk space (megabytes)	1000	200
Available disk space (percentage)	10	3


☒ Log accesses of internal users

☐ Notify administrators of software problems

☐ Notify developers of software problems

 By enabling this feature, you will contribute to the development and security of the platform.

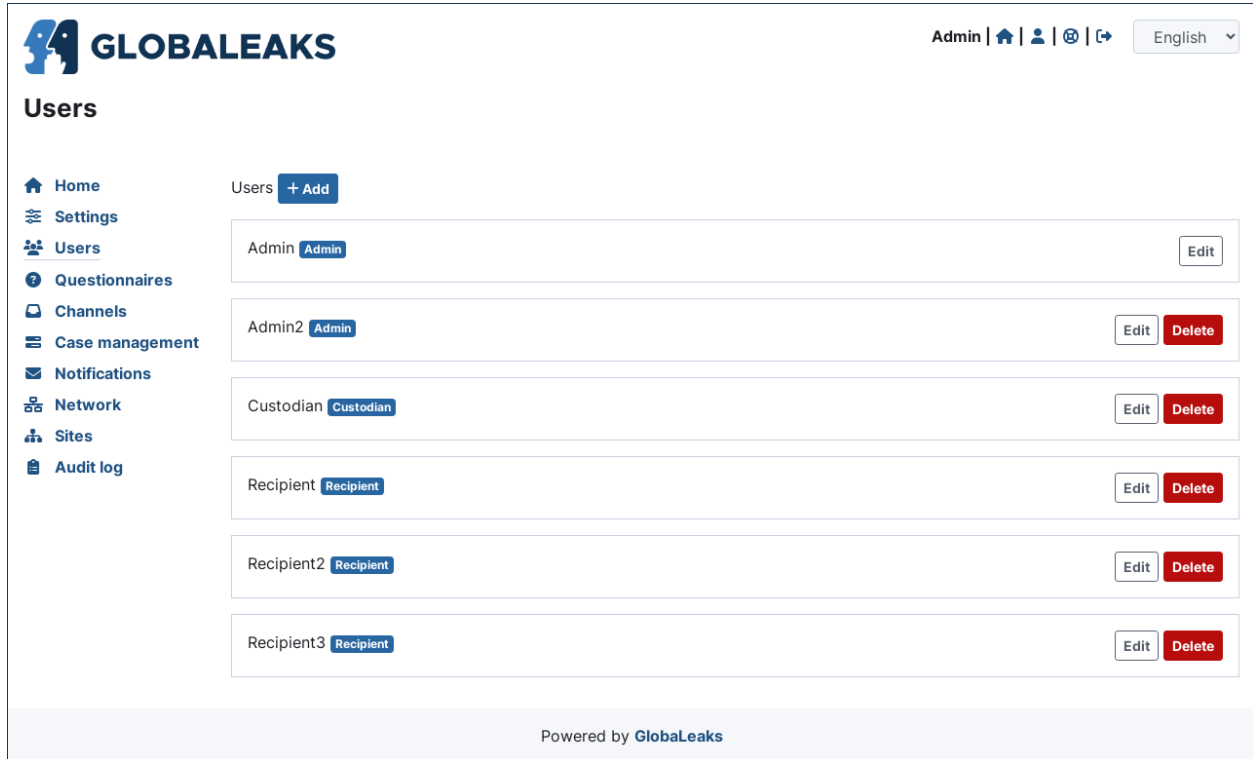
 Save
  Reset reports

Powered by 

Users

This sections is where users could be created and managed. The system with the basic configuration completed with the initial Platform wizard is configured with an Administrator and a Recipient.

Depending on your project needs here you could create users with different roles and manage their respective privileges.



User Roles

The software offers the possibility to create users with the following roles:

1. Administrators
2. Recipients

Questionnaires


The software implements a standard default questionnaire that is proposed as a good base for a generic whistleblowing procedure. This questionnaire is the current result of the research performed by the project team with the organizations that have adopted the solution and especially with anticorruption and investigative journalism NGOs.






As every organization has different needs, risks and goals globaleaks has been designed considering to implement an advanced questionnaire builder offering the possibility to design custom questionnaires.

The following sections present the questionnaire builder and its capabilities.











The screenshot shows the GLOBALEAKS web application interface. At the top left is the GLOBALEAKS logo. To the right of the logo is the text "Admin" followed by icons for home, user, settings, and a share icon, and a language dropdown menu set to "English". Below the logo is the heading "Questionnaires". On the left side is a vertical sidebar menu with the following items: Home, Settings, Users, Questionnaires (highlighted), Channels, Case management, Notifications, Network, Sites, and Audit log. The main content area has two tabs: "Questionnaires" (active) and "Question templates". Below the tabs, there is a section labeled "Questionnaires" with a "+ Add" button and an "Import" button. Below this, there is a list of questionnaires. The first entry is "GLOBALEAKS" with "Export" and "Duplicate" buttons. The second entry is "Questionnaire 1" with "Edit", "Export", "Duplicate", and "Delete" buttons. At the bottom of the page, it says "Powered by GLOBALEAKS".

Depending on your project needs you may evaluate defining some questions once as Question Templates and reuse the same question in multiple questionnaires.






Admin |  |  |  |  | English 


Questionnaires


 Home
 Settings
 Users
 Questionnaires
 Channels
 Case management
 Notifications
 Network
 Sites
 Audit log


QuestionnairesQuestion templates


Question templates  Add  Import


Attachment 


Edit  Export Delete


Checkbox 


Edit  Export Delete


Date 


Edit  Export Delete


Date range 


Edit  Export Delete


Group of questions 


Edit  Export Delete


Multi-line text input 


Edit  Export Delete


Multiple choice input 


Edit  Export Delete


Selection box 


Edit  Export Delete

Single-line text input 

Edit  Export Delete

Terms of service 

Edit  Export Delete

Powered by 

Steps

The software enables to organize questionnaire in one or multiple steps. For example the default questionnaire is organized with a single step including all the questions.

Questions Types

The software enables you to create questions of the following types:

1. Single-line text input
2. Multi-line text input
3. Selection box
4. Multiple choice input
5. Checkbox
6. Attachment
7. Terms of service
8. Date
9. Date range
10. Question group

Common Question Properties

Each of the software question types make it possible to configure the following properties:

Question: The text of the question

Hint: A hint that will be shown via an popover and a question mark near the question.

Description: A description text that will be shown below the question

Required: Set this field if you want this question to be mandatory

Preview: Set this field if you want the answers to this question to appear in the preview section of the list

Channels

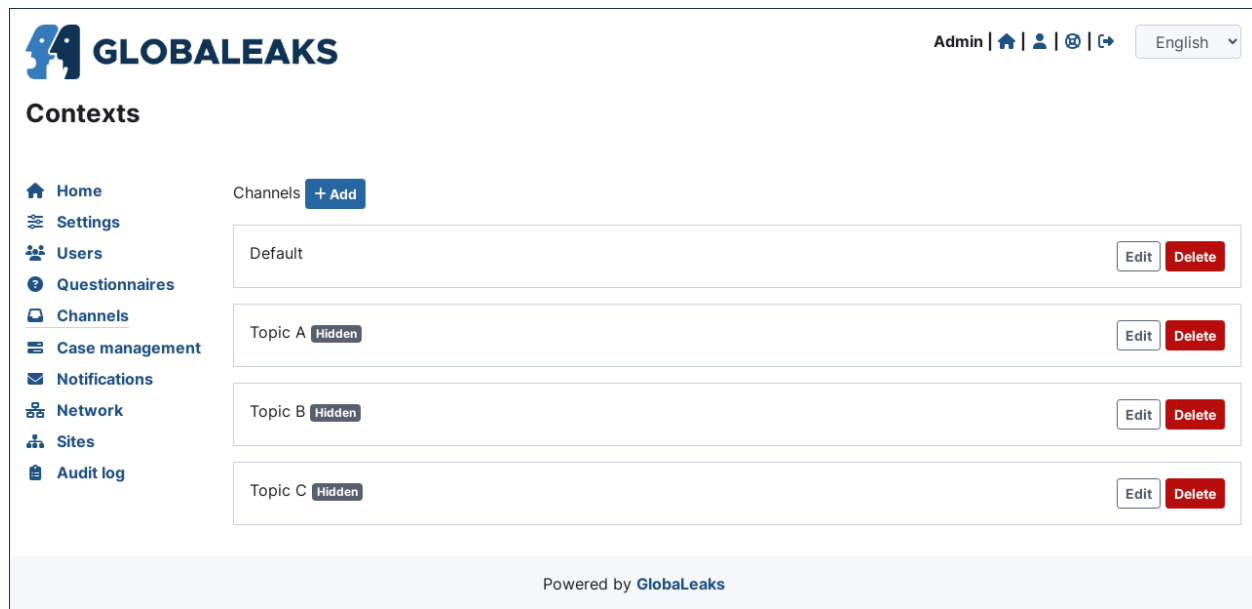
This section is where whistleblowing channels could be created and managed.

A whistleblowing channel is typically defined by the following main characteristics

Name: the name of the channel Image: an image to identify the channel Description: a description of the channel Recipients: the set of recipients that will receive reports sent to this channel Questionnaire: the questionnaire that will be proposed to whistleblowers selecting this channel Submission expiration: the data retention policy for the channel

The system with the basic configuration completed with the initial platform wizard is configured with a single Channel called Default, on which is associated a recipient and the default questionnaire.

Depending on your project needs here you could create additional Channels and configure their respective properties.



Submissions Expiration

The software enables to configure a data retention policy for each channel. This is a fundamental property of the whistleblowing channel that makes it possible to configure automatic secure deletion of reports after a certain period of time. This setting should be configured in relation to the risk of the channel in order to limit unneeded exposure of the reports received therein.

By default a channel is configured with a report expiration of 90 days.

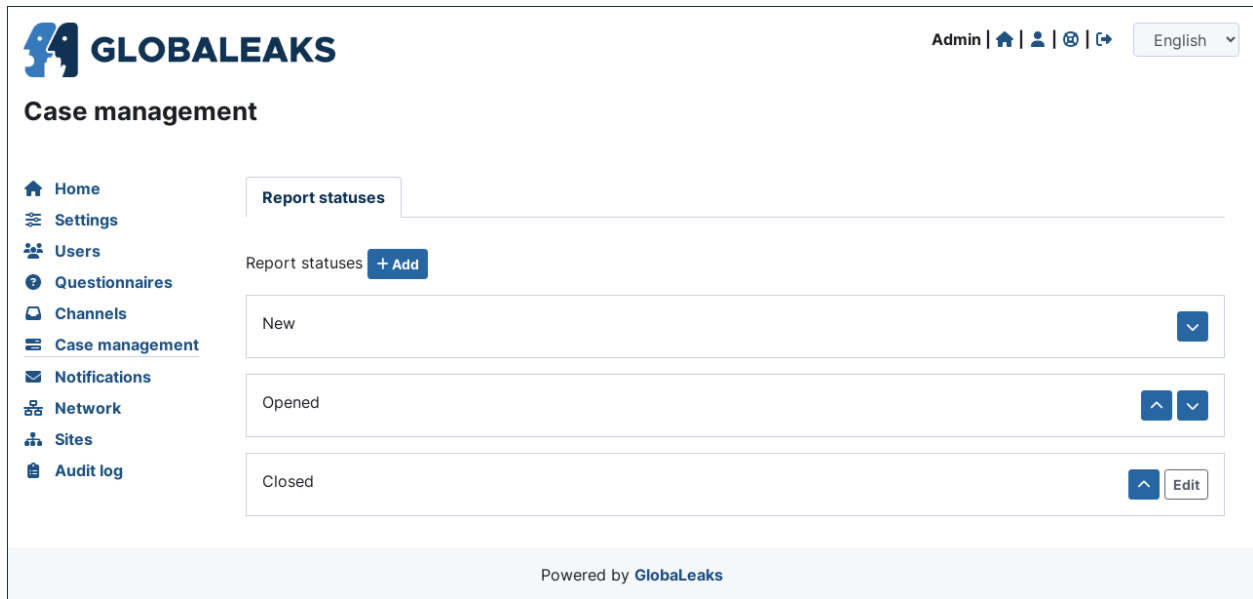
Case Management

This section is intended to host all the main case management feature that will be offered by the software. Currently it hosts the possibility to define reports statuses and sub-statuses intended to be used by Recipients while working on the reports.

By default the system includes the following report statuses:

1. New
2. Open
3. Closed

Within this section you may add additional Statuses between the State Open and Closed and you can furtherly define Sub-statuses for the Closed status (e.g. Archived / Spam)



Notification

This is the section where are configured all the aspects related to the mail notifications sent by the software.







The section is furtherly divided in:

1. Main configuration
2. Notification templates

Main configuration

Here are configured the technical details about SMTP.

Note: By default GlobaLeaks comes with a working configuration that is based on systems offered by the GlobaLeaks developers to the community of users and testers; even though this configuration is designed by their owners with special care in relation to security and privacy you are invited to consider using alternative systems for your production environment.



Admin |  |  |  |  | English 

Notification settings

- Home
- Settings
- Users
- Questionnaires
- Channels
- Case management
- Notifications
- Network
- Sites
- Audit log

Settings

Templates

 Default mail configuration in use. Please consider using a private mail server.

SMTP email address

notifications@globaleaks.org

SMTP server address

mail.globaleaks.org

SMTP server port

587

Security

SMTP/TLS

☒ Require authentication

Username

globaleaks

Password

.....

☐ Disable notifications to administrators

☐ Disable notifications to recipients

☐ Disable notifications to custodians

Number of hours before sending a report expiration alert

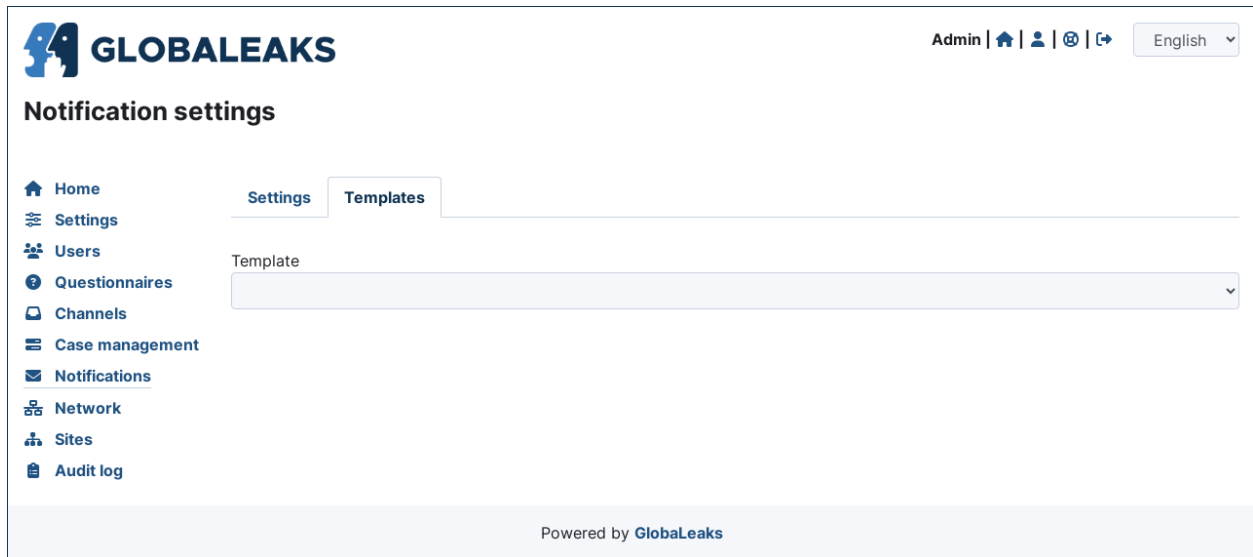
24

Powered by [Globleaks](#)

Notification Templates

In this section are configured the notification templates.

By default globaleaks includes text and translations for each of the templates that are provided to be fully functional and studied with particular care in relation to security and privacy. Depending on your project needs you may override the default text with your customized texts.



Network

In this section are configured the network settings.

The section is furtherly divided in:

1. HTTPS
2. Tor
3. IP Access control
4. URL Redirects

HTTPS

Here you can configure all the aspects related to the access of the platform via the HTTPS Protocol.

GLOBALEAKS Admin | Home | User | Settings | English

Network settings

- Home
- Settings
- Users
- Questionnaires
- Channels
- Case management
- Notifications
- Network**
- Sites
- Audit log

HTTPS Tor Access control URL redirects

Hostname: domain.tld Save

Status: Disabled

The platform supports the configuration of HTTPS through this interface.

Automatic configuration

Using automatic HTTPS configuration will handle the entire process of requesting, enabling and renewing certificates from the Let's Encrypt Certificate Authority. The platform must be reachable through a public IP address and the selected hostname must have a DNS record referencing that address.

Proceed

Manual configuration

The manual configuration wizard will guide you through the setup of HTTPS from an alternative Certificate Authority.

Proceed

Powered by **GlobalLeaks**


In particular here are configured:

1. The domain name used by your project
2. The HTTPS key and certificates

To ease the deployment and the maintenance and reduce the costs of your project, consider using the software includes support for the Let's Encrypt HTTPS certificates.

Tor

Here you can configure all the aspects related to the access of the platform via the Tor Protocol.


Admin | [Home](#) | [Users](#) | [Settings](#) | [Help](#) | [Logout](#)
English ▾

Network settings

- Home
- Settings
- Users
- Questionnaires
- Channels
- Case management
- Notifications
- Network**
- Sites
- Audit log

HTTPS
Tor
Access control
URL redirects

Tor Onion Service
naaofywcfyomcx3e6rcneep2dwwh6vhpy6wnslwuhpbwz63khncznqd.onion
Regenerate

☐ Anonymize outgoing connections
☒ Let the platform be reachable without Tor
Roles enabled to use the platform without Tor


Role	Enabled
Admin	<input checked="" type="checkbox"/>
Recipient	<input checked="" type="checkbox"/>
Whistleblower	<input checked="" type="checkbox"/>

Save

Powered by **GlobaLeaks**

IP Access Control

Here you can configure IP based Access Control.


Admin | [Home](#) | [Users](#) | [Settings](#) | [Help](#) | [Logout](#)
English ▾

Network settings

- Home
- Settings
- Users
- Questionnaires
- Channels
- Case management
- Notifications
- Network**
- Sites
- Audit log

HTTPS
Tor
Access control
URL redirects

Restrict access to specific IP addresses

Role	Enabled	Allowed IP addresses
Admin	<input type="checkbox"/>	
Recipient	<input type="checkbox"/>	

Each entry must be separated with a comma.
Example: 212.35.212.87,192.0.2.0/24,2001:db8::/32

Save

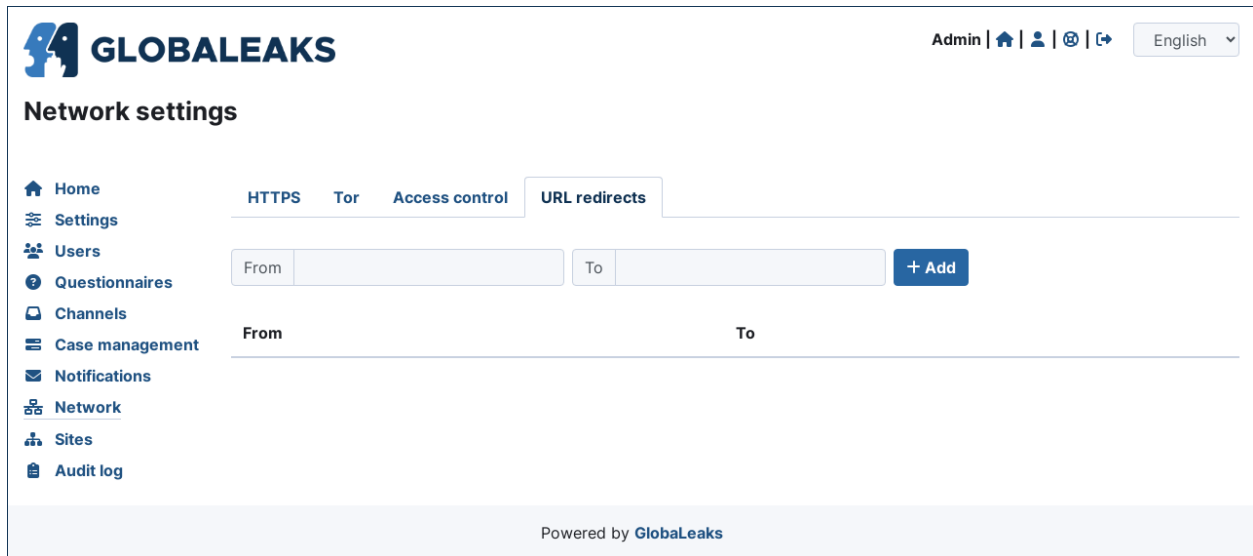
Powered by **GlobaLeaks**

Suggested configurations are:

1. Prevent Whistleblowers to report from within their respective work space.
2. Restrict Recipients access to their intranet.

URL Redirects

Here you can configure URL Redirects.



The screenshot shows the GLOBALEAKS administration interface. At the top, there's a header with the GLOBALEAKS logo, user information (Admin), and a language dropdown set to English. Below the header, the 'Network settings' section is active, with tabs for HTTPS, Tor, Access control, and URL redirects. The URL redirects tab is selected, showing a table with columns 'From' and 'To'. Above the table, there are input fields for 'From' and 'To', and a '+ Add' button. A sidebar on the left lists various settings categories: Home, Settings, Users, Questionnaires, Channels, Case management, Notifications, Network (highlighted), Sites, and Audit log. The footer indicates the system is 'Powered by GLOBALEAKS'.

Sites

The site section enables organization to create and manage multiple secondary whistleblowing sites.

Sites Management

Secondary whistleblowing platforms with independent configurations can be manually created and managed through the Sites interface.

Organizations have typically need for creating a secondary site when dealing with subsidiaries or third party clients.

GLOBALEAKS

Admin | Home | User | Settings | English

Sites management

Home Settings Users Questionnaires Channels Case management Notifications Network Sites Audit log

Sites Options

Sites [+ Add](#)

- GLOBALEAKS**
naafywcfyomcx3e6rcneep2dwwh6vhhpy6wnslwuhpbwz63khncznqd.onion
domain.tld
- Platform A**
rq12ygrrru25ovzy6c5a3zjguixp8cm6wli2h7maqkdrovg7m3p7xnad.onion [Enabled](#) [Configure](#) [Edit](#) [Delete](#)
- Platform B**
hvdye6c7gfn3fkx4rw74jgl2ue2w2vo53kvbshr3ah4h7epzedf44yad.onion [Enabled](#) [Configure](#) [Edit](#) [Delete](#)
- Platform C**
esclehs465aa2zjqos2y6kdnkeaf3k5gkub6hwa3zvr7faazte6a5ad.onion [Enabled](#) [Configure](#) [Edit](#) [Delete](#)

Powered by GLOBALEAKS

After creating a secondary site an administrators of the main site could simply enter on that system by clicking a “Configure” button.

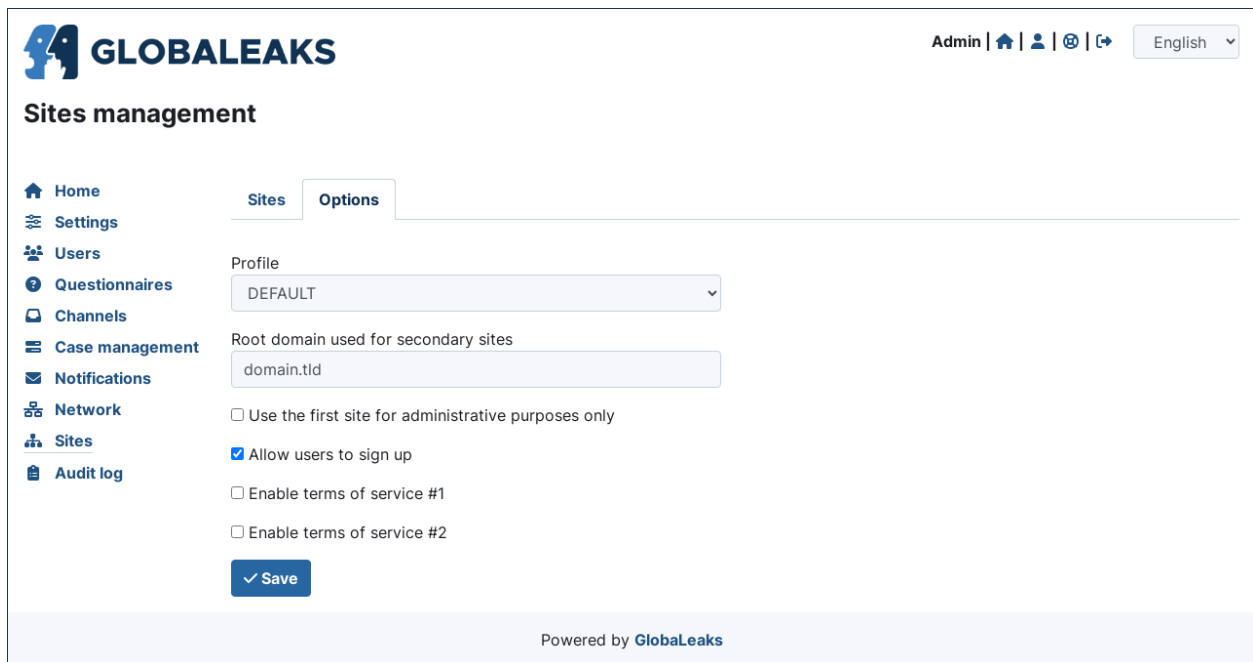
After clicking on the button the administrator will be logged in on the the administrative panel of the site.

Signup Module

The software features a signup module that can be enabled and used to offers others users the possibility to register their secondary site.


Organizations have typically need for a signup module when offering the platform to other subsidiaries or third party clients where they want users to have the possibility to self subscribe.

The signup feature can be enabled in the Options tab of the Sites section.



The screenshot shows the 'Sites management' page in the GlobaLeaks admin interface. The top navigation bar includes the GlobaLeaks logo, 'Admin' link, and user icons. The left sidebar lists various management sections: Home, Settings, Users, Questionnaires, Channels, Case management, Notifications, Network, Sites (highlighted), and Audit log. The main content area has two tabs: 'Sites' and 'Options'. Under the 'Options' tab, there is a 'Profile' dropdown menu set to 'DEFAULT', a text input for 'Root domain used for secondary sites' with 'domain.tld', and three checkboxes: 'Use the first site for administrative purposes only' (unchecked), 'Allow users to sign up' (checked), 'Enable terms of service #1' (unchecked), and 'Enable terms of service #2' (unchecked). A 'Save' button is at the bottom. The footer says 'Powered by GlobaLeaks'.







When the signup module is enabled the submission module of the main site is automatically disabled and the home page will be featuring the following signup form:



The screenshot shows the 'Sign up' form in the GlobaLeaks interface. The top navigation bar includes the GlobaLeaks logo and a language dropdown set to 'English'. The main heading is 'Sign up'. Below it, the 'Sign up' section contains a 'Site' field with a dropdown menu showing '.domain.tld'. There are four input fields: 'Name', 'Surname', 'Email address', and 'Email address (Confirmation)'. Each field has a red asterisk indicating it is required. A 'Proceed' button is at the bottom left. The footer says 'Powered by GlobaLeaks'.

Audit Log

The software features a privacy precerving audit log enabling administrators of the system to supervise on projects operations.


Admin |  |  |  |  |  English




Audit log

- Home
- Settings
- Users
- Questionnaires
- Channels
- Case management
- Notifications
- Network
- Sites
- Audit log**


Audit log
Users
Reports
Scheduled jobs

Date	Type	Severity	User	Object
03-07-2023 18:07	login	0	89dbf9f9-b0ec-468c-8ddb-25179e977309	
03-07-2023 18:07	logout	0	22979ffe-a2a7-45fb-bb86-620aa2616843	
03-07-2023 18:07	access_report	0	22979ffe-a2a7-45fb-bb86-620aa2616843	f87889b4-5d88-45ed-b0f7-3cb6dca06532
03-07-2023 18:07	login	0	22979ffe-a2a7-45fb-bb86-620aa2616843	
03-07-2023 18:06	logout	0	22979ffe-a2a7-45fb-bb86-620aa2616843	
03-07-2023 18:06	access_report	0	22979ffe-a2a7-45fb-bb86-620aa2616843	f87889b4-5d88-45ed-b0f7-3cb6dca06532
03-07-2023 18:06	login	0	22979ffe-a2a7-45fb-bb86-620aa2616843	
03-07-2023 18:06	whistleblower_logout	0		
03-07-2023 18:06	whistleblower_login	0		
03-07-2023 18:06	logout	0	22979ffe-a2a7-45fb-bb86-620aa2616843	
03-07-2023 18:06	access_report	0	22979ffe-a2a7-45fb-bb86-620aa2616843	f87889b4-5d88-45ed-b0f7-3cb6dca06532
03-07-2023 18:06	update_report_status	0	22979ffe-a2a7-45fb-bb86-620aa2616843	f87889b4-5d88-45ed-b0f7-3cb6dca06532
03-07-2023 18:06	login	0	22979ffe-a2a7-45fb-bb86-620aa2616843	
03-07-2023 18:06	whistleblower_new_report	0		
03-07-2023 18:06	whistleblower_new_report	0		
03-07-2023 18:06	whistleblower_new_report	0		
03-07-2023 18:05	logout	0	89dbf9f9-b0ec-468c-8ddb-25179e977309	
03-07-2023 18:05	login	0	89dbf9f9-b0ec-468c-8ddb-25179e977309	
03-07-2023 18:05	logout	0	89dbf9f9-b0ec-468c-8ddb-25179e977309	
03-07-2023 18:05	login	0	89dbf9f9-b0ec-468c-8ddb-25179e977309	

<< First
< Previous
1
2
3
4
Next >
Last >>

 Export
 globaleaks.log
 access.log

Powered by **GlobaLeaks**


Admin | [Home](#) | [Users](#) | [Reports](#) | [Scheduled jobs](#)
English ▾

Audit log


[Home](#)
[Settings](#)
[Users](#)
[Questionnaires](#)
[Channels](#)
[Case management](#)
[Notifications](#)
[Network](#)
[Sites](#)
[Audit log](#)

[Audit log](#)
[Users](#)
[Reports](#)
[Scheduled jobs](#)

ID	Username	Role	Name	2FA	Creation date	Last access
89dbf9f9-b0ec-468c-8ddb-25179e977309	admin	admin	Admin	×	03-07-2023 18:02	03-07-2023 18:07
3ac20b6a-7ef6-436e-9baa-84b6a5b0559a	Admin2	admin	Admin2	×	03-07-2023 18:03	03-07-2023 18:04
b2714f60-a425-434c-9fe6-bd6196b5f278	Custodian	custodian	Custodian	×	03-07-2023 18:03	03-07-2023 18:04
22979ffe-a2a7-45fb-bb86-620aa2616843	Recipient	receiver	Recipient	×	03-07-2023 18:03	03-07-2023 18:07
3837cdfb-932d-4716-9b59-4724ba3dc065	Recipient2	receiver	Recipient2	×	03-07-2023 18:03	03-07-2023 18:04
e47dc80d-3318-45e8-9468-e4548db02c02	Recipient3	receiver	Recipient3	×	03-07-2023 18:03	01-01-1970 01:00

[Export](#)

Powered by **GlobaLeaks**


Admin | [Home](#) | [Users](#) | [Reports](#) | [Scheduled jobs](#)
English ▾

Audit log








[Home](#)
[Settings](#)
[Users](#)
[Questionnaires](#)
[Channels](#)
[Case management](#)
[Notifications](#)
[Network](#)
[Sites](#)
[Audit log](#)

[Audit log](#)
[Users](#)
[Reports](#)
[Scheduled jobs](#)











#	Date	Last update	Expiration date	Channel	Status	Tor	Comments	Messages	Files	Whistleblower's last access
3	03-07-2023 18:06	03-07-2023 18:06	02-10-2023	Default	Opened		2	0	2	03-07-2023 18:06
2	03-07-2023 18:06	03-07-2023 18:06	02-10-2023	Default	New		0	0	2	03-07-2023 18:06
1	03-07-2023 18:06	03-07-2023 18:06	02-10-2023	Default	New		0	0	2	03-07-2023 18:06

[Export](#)

Powered by **GlobaLeaks**



Admin |  |  |  |  |  | English 

Audit log

 Home
  Settings
  Users
  Questionnaires
  Channels
  Case management
  Notifications
  Network
  Sites
  Audit log

[Audit log](#)
[Users](#)
[Reports](#)
[Scheduled jobs](#)

	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	
Anomalies	0s 18:02:14 03-07- 2023	0s 18:03:14 03-07- 2023	0.001s 18:04:14 03-07- 2023	0s 18:05:14 03-07- 2023	0s 18:06:14 03-07- 2023	0s 18:07:14 03-07- 2023					
CertificateCheck											
Cleaning											
Delivery	0.082s 18:02:14 03-07- 2023	0.006s 18:02:19 03-07- 2023	0.005s 18:02:24 03-07- 2023	0.019s 18:02:29 03-07- 2023	0.018s 18:02:34 03-07- 2023	0.006s 18:02:39 03-07- 2023	0.006s 18:02:44 03-07- 2023	0.006s 18:02:49 03-07- 2023	0.006s 18:02:54 03-07- 2023	0.005s 18:07:19 03-07- 2023	
ExitNodesRefresh	0.687s 18:02:14 03-07- 2023										
Notification	0.055s 18:02:14 03-07- 2023	0.016s 18:02:24 03-07- 2023	0.056s 18:02:34 03-07- 2023	0.082s 18:02:44 03-07- 2023	1.795s 18:02:54 03-07- 2023	0.102s 18:03:04 03-07- 2023	2.714s 18:03:14 03-07- 2023	0.013s 18:03:24 03-07- 2023	0.015s 18:03:34 03-07- 2023	0.014s 18:07:14 03-07- 2023	
PGPCheck											
SessionManagement	0.001s 18:02:14 03-07- 2023	0s 18:03:14 03-07- 2023	0s 18:04:14 03-07- 2023	0s 18:05:14 03-07- 2023	0s 18:06:14 03-07- 2023	0s 18:07:14 03-07- 2023					
Statistics											
UpdateCheck											

 Export

Powered by **GlobaLeaks**

4.2.2 Common Configurations

Configure the Logo

The first thing you want to give to your whistleblowing site is a branding identity; this could be done by loading a logo in section Site settings / Main configuration.

Settings	Theme customization	Languages	Text customization	Advanced
<p>Logo</p> <div style="border: 1px dashed gray; height: 80px; width: 100px; margin: 0 auto; display: flex; align-items: center; justify-content: center;"> </div>				
<p>Project name</p> <input type="text" value="GLOBALEAKS"/>				
<p>Description</p> <input type="text" value="Secure whistleblowing platform based on GlobaLeaks free and open-source software."/>				
<p>Homepage title</p> <input type="text"/>				
<p>Presentation</p> <input type="text"/>				
<p>Question to solicit possible whistleblowers</p> <input type="text"/>				
<p>Whistleblowing button</p> <input type="text" value="File a report"/>				
<p>Disclaimer</p> <input type="text"/>				
<p>Footer</p> <input type="text"/>				
<input type="button" value="✓ Save"/>				

Scroll down along the page to reach the “Save” button, click on it and have your logo and favicon applied.

Enable Languages

You may want your GlobaLeaks installation served on more than one language

To do so, in the section “Site settings / Languages” select the languages you would like and add them.

Note that in the same interface you can mark the default application language.

Settings	Theme customization	Languages	Text customization	Advanced
Languages + Add				
<div> <input checked="" type="checkbox"/> × English [en] <input checked="" type="checkbox"/> × Italian [it] </div>				
<div>✓ Save</div>				

Configure Notification Settings

GlobaLeaks sends out notifications of different events to different receivers and to admins. In order to have this working, you have to select “Notification Settings” in the “Administration Interface - General Settings” page and set up email account and related server parameters.

We suggest you to setup an email account dedicated to sending out notifications from your initiative.

Settings	Templates
<div> Default mail configuration in use. Please consider using a private mail server. </div>	
SMTP email address <input type="text" value="notifications@globaleaks.org"/>	
SMTP server address <input type="text" value="mail.globaleaks.org"/>	
SMTP server port <input type="text" value="587"/>	
Security <input type="text" value="SMTP/TLS"/>	
<input checked="" type="checkbox"/> Require authentication	
Username <input type="text" value="globaleaks"/>	
Password <input type="password" value="....."/>	
<input type="checkbox"/> Disable notifications to administrators <input type="checkbox"/> Disable notifications to recipients <input type="checkbox"/> Disable notifications to custodians	
Number of hours before sending a report expiration alert <input type="text" value="24"/>	
<div> <div>✓ Save</div> <div>✉ Test the configuration</div> <div>Reset SMTP configuration</div> <div>Reset notification templates to default</div> </div>	

Enter the followings:

- SMTP name: the name of your GlobaLeaks project or something that equally descriptive
- SMTP email address: the email address used to send notifications
- Username: the username corresponding to the just inserted “SMTP email address”; this is needed to authenticate to the SMTP server and send emails
- Password: Password of the above corresponding “SMTP email address”
- SMTP Server Address: it is the hostname of the SMTP server you are using to send notification emails
- SMTP Server Port: Port used to send outgoing emails. It is usually 465 or 587 (SMTP with TLS is at TCP port 587; SMTP with SSL is at 465)
- Transport Security: from the drop down menu select the opportune security level

It is better to leave untouched the pre-defined settings pertaining the notification to admins and to recipients, but in the case you want to disable them, it is possible to check the corresponding checkboxes.

You can then set the value for the time at which the notification alert of expiring report; this value is set at 72hours to give time to the recipient(s) to check and manage the pending submissions.

It is possible to tweak the maximum number of emails allowed in an hour, before email will be suspended in order to avoid flooding the system. It is advised to keep the pre-defined value, and eventually change it accordingly with mail server capabilities.

Once configured all the parameters for notifications, it is possible to test them by just clicking on the “Test the configuration” button.

If all is working as expected, click on the “Save” button to keep the configured parameters.

Configure Recipients

The Recipient is the person that will receive and process the data that whistleblowers input in the platform. You can have one or multiple Recipients per Context, and also have one Recipient that can access to multiple Contexts. The platform is very flexible on this and allows you to define in very detail your whistleblowing system and procedure.

Customize the Graphic Layout

Example 1: Custom Background

This CSS example shows how to customize the Background Color of the application.

```
body
{
    background-color: blue;
}
```

Example 2: Custom Font

This CSS example shows how to customize the font of the application.

```
@font-face {  
  font-family: 'Antani';  
  src: url('s/antani.woff2') format('woff2');  
  font-weight: normal;  
  font-style: normal;  
}  
  
body {  
  font-family: 'Antani', Inter, sans-serif;  
  font-size: 16px;  
}
```

4.2.3 Upgrade Guide

Regular Update

To safely upgrade a GlobaLeaks installation please proceed with a backup of your setup by following the [Backup and restore](#) guide.

This is necessary so that if something goes wrong and you need to rollback, you will be able to just uninstall the current package, then install the same version of globaleaks that was previously installed and working.

In order to update GlobaLeaks perform the following commands:

```
apt-get update && apt-get install globaleaks
```

Upgrade of the Distribution Version

For security and stability reasons it is recommended to not perform a distribution upgrade.

GlobaLeaks could be instead easily migrated to a new up-to-date Debian system with the following recommended instructions:

- create an archive backup of /var/globaleaks
- instantiate the latest Debian available
- log on the new server and extract the backup in /var/globaleaks
- follow the [Installation Guide](#); GlobaLeaks while installing will recognize the presence of an existing data directory and will use it

In Case of Errors

The above commands should allow you to perform regularly updates. On some conditions due to special updates it could be possible that those commands result in a failure. Consult this page for knowing specific FAQs on precise failures.

In case you do not find any specific documented solution for your failure, you could run the GlobaLeaks install script. The installation script in fact is designed to allow the update of GlobaLeaks and it includes fixes for the most common issue.

To run the install script for updating globaleaks perform the following commands:

```
wget https://deb.globaleaks.org/install-globaleaks.sh
chmod +x install-globaleaks.sh
./install-globaleaks.sh
```

4.2.4 Backup and Restore

The following bash script could be used in order to perform a backup manually:

```
#!/bin/sh
set -e

if [ -d "/var/globaleaks" ]; then
    timestamp=$(date +%s)
    version=`dpkg -s globaleaks | grep '^Version:' | cut -d ' ' -f2`
    filepath=/var/globaleaks/backups/globaleaks-$version-$timestamp.tar.gz
    echo "Creating backup of /var/globaleaks in $filepath"
    mkdir -p /var/globaleaks/backups
    chown globaleaks:globaleaks /var/globaleaks/backups
    tar --exclude='/var/globaleaks/backups' -zcvf $filepath /var/globaleaks
fi
```

After the completion of the command you will find a tar.gz archive within the /var/globaleaks/backups. The file will have the format: globaleaks-\$version-\$timestamp.tar.gz

GlobaLeaks does automatically perform a backup at each platform update and the backup is kept under data retention policy and is deleted 15 days after the update.

To restore an existing backup:

- be sure globaleaks is not running; globaleaks can be shut down with “service globaleaks stop”;
- identify the version of globaleaks required for restoring globaleaks. the version is written in the backup filename;
- extract the content of the archive in /var/globaleaks with the command tar -zxvf backup.tar.gz
- install the required version of globaleaks with: apt-get install globaleaks=version (e.g. globaleaks=3)

4.2.5 Troubleshooting

Issues and Bug Reporting

If you encounter any issue and you are not able to run GlobalLeaks:

- Be sure to strictly follow the Installation Guide for installation
- Be sure to satisfy the Technical Requirements for hardware and operating system version.
- Search on the support forum to check if a user has already encountered your issue: <https://forum.globaleaks.org>
- Report the issue on the official software ticking system: <https://github.com/globaleaks/GlobalLeaks/issues>

Useful Debugging Commands

Depending on your setup. There are a few things that are usually the first things to check to see if GlobalLeaks is working.

- Is the service running?

```
service globaleaks status
```

- Is the service responding on the loopback interface?

```
curl -vvv localhost:8082
```

- Is the service listening on external interfaces?

```
netstat -tap
```

- Are exceptions being generated?

```
less /var/globaleaks/log/globaleaks.log
```

Log Files

There are a few useful logs and corresponding log files when GlobalLeaks is installed.

GlobalLeaks process:

```
/var/globaleaks/log/globaleaks.log
```

The verbosity is configurable via the web interface of the software inside Advanced Settings.

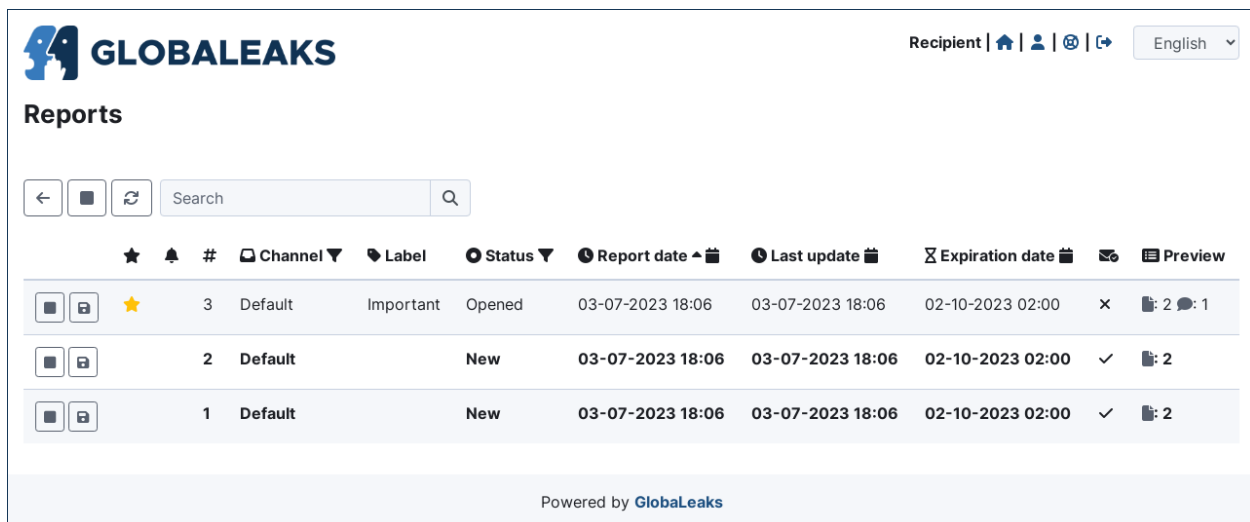
Tor:

```
/var/log/tor/log iptables: /var/log/syslog AppArmor: /var/log/kern.log
```

4.3 For Recipients

4.3.1 Access the List of the Existing Reports


The lists of the existing reports can be accessed via the link **Reports** on the sidebar of the Recipient's Homepage.








4.3.2 Access a Report










A report can be accessed in two ways:


- By clicking on it like on a mailbox system from the **Reports** page
- By clicking on the link received on a mail notification and entering own credentials








Recipient |  |  |  |  | English 


Report


Important 

Status: Opened 

#	Channel	Date	Last update	Expiration date	Reminder date	 	Tor	Status
3	Default	03-07-2023 18:06	03-07-2023 18:06	02-10-2023 02:00	—			Opened

Recipients 

Recipient
Recipient2
Recipient3

Questionnaire answers 

Please summarize your report in a few words.
summary

Describe your report in detail.
detail

Where did the facts happen?
...

When did the facts happen?
...


How are you involved in the reported facts?
I witnessed the facts in person





Do you have evidence to support your report?
Yes


Please describe the evidence in detail.
...

Have you reported the facts to other organizations and/or individuals?
No


What is the outcome you want to achieve with our support?
...


Attachments 

Filename	View	Download	Upload date	Type	File size
evidence-1			03-07-2023 18:06	application/octet-stream	11 B
evidence-2			03-07-2023 18:06	application/octet-stream	11 B


Files attached by recipients 

Upload a file:

Description  Upload

Comments 

0/4096


 Send

Whistleblower
comment reply

03-07-2023 18:06

Recipient
comment

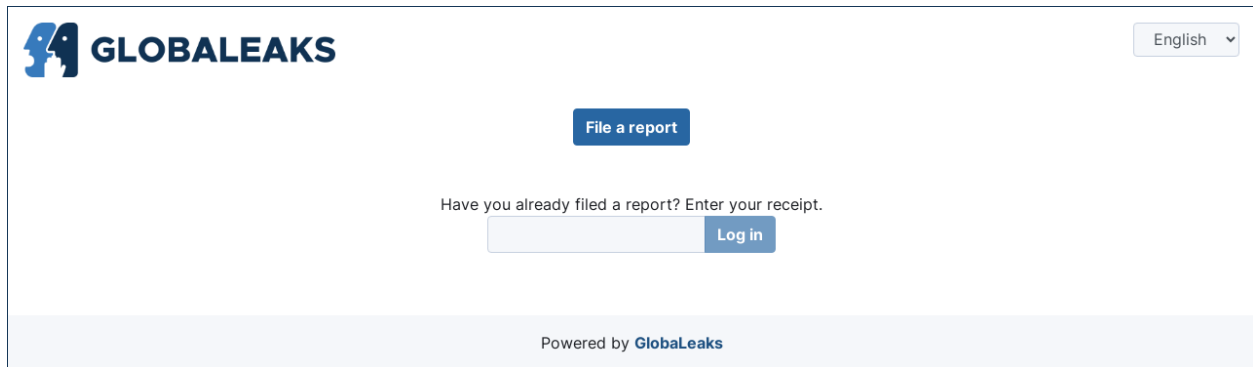
03-07-2023 18:06

Powered by 


4.4 For Whistleblowers

4.4.1 File a New Report

A new report can be filed by accessing the homepage of the platform and clicking the **File a report** button.



The screenshot shows the GlobalLeaks homepage. In the top left corner is the GlobalLeaks logo, which consists of a blue icon of two puzzle pieces forming a head and the word "GLOBALEAKS" in blue capital letters. In the top right corner is a language dropdown menu with "English" selected. In the center of the page is a blue button labeled "File a report". Below this button is the text "Have you already filed a report? Enter your receipt." followed by a light blue input field and a blue button labeled "Log in". At the bottom of the page is a light blue footer bar with the text "Powered by GlobalLeaks".

English ▾

Please summarize your report in a few words. *

summary

Describe your report in detail. *

detail

Where did the facts happen? * When did the facts happen? *

... ...


How are you involved in the reported facts? *



I witnessed the facts in person ▾

Do you have evidence to support your report? *



Yes ▾

Please attach the evidence to support your report.

 Upload Select a file or drag it here.



evidence-1
Size: 11 B



evidence-2
Size: 11 B

Please describe the evidence in detail. *

A thorough description of the submitted evidence enhances our ability to evaluate claims and investigate. Please take care to reference significant portions of any videos, images or documents submitted.

...

Have you reported the facts to other organizations and/or individuals? *

No ▾


What is the outcome you want to achieve with our support? *

...

Submit

Powered by [GlobalLeaks](#)

After filing a new report the systems provides to the user a 16-digit receipt.

Logout English

Your report was successful.

Thank you. Your report was successful. We will try to get back to you as soon as possible.

Remember your receipt for this report.

7142 6363 6973 2809


Use the 16 digit receipt to log in. It will allow you to view any messages we sent you, and also to add extra info.

View your report

Powered by **GlobaLeaks**

4.4.2 Access an Existing Report

An existing report can be accessed by entering the 16-digit receipt obtained at the end of the submission on the login interface present on the home page of the platform.

English


File a report

Have you already filed a report? Enter your receipt.


7142 6363 6973 2809






Log in

Powered by **GlobaLeaks**

 **GLOBALEAKS**

[Logout](#) English



 Channel	 Date	 Last update	 Expiration date	 Status
Default	03-07-2023 18:06	03-07-2023 18:06	02-10-2023 02:00	Opened

Questionnaire answers

Please summarize your report in a few words.
summary

Describe your report in detail.
detail

Where did the facts happen?
...

When did the facts happen?
...

How are you involved in the reported facts?
I witnessed the facts in person

Do you have evidence to support your report?
Yes


Please describe the evidence in detail.
...

Have you reported the facts to other organizations and/or individuals?
No

What is the outcome you want to achieve with our support?
...

Attachments

Filename	Upload date	Type	File size
evidence-1	03-07-2023 18:06	application/octet-stream	11 B
evidence-2	03-07-2023 18:06	application/octet-stream	11 B

 Upload Select a file or drag it here.

Comments

0/4096

Send

Whistleblower
comment reply

03-07-2023 18:06

Recipient
comment

03-07-2023 18:06

Powered by [Globleaks](#)

PROJECT ROADMAP

Note: This tentative roadmap is built by the GlobaLeaks team in order to try to respond to main users' needs. Please get sure that the needs of your projects and users are well represented on the project [Ticketing System](#). If your organization could fund the development of parts of this roadmap please write us at info@globaleaks.org

5.1 Introduction

[GlobaLeaks](#) is free, open source software enabling anyone to easily set up and maintain a secure whistleblowing platform.

Started in 2011, the software is now widely used worldwide by more than 3000 organizations working in the fields of anti-corruption activism, human rights violations reporting, investigative journalism, and corporate compliance.

This document details the main areas of research development and represents the actual tentative readmap of consolidation planned for 2023-2025 based on the analysis of the large set of user needs collected within the official [Ticketing System](#).

5.2 Development Areas

5.2.1 Application Client Update

GlobaLeaks client is still based on Angular 1 and on other stable but outdated components. Considering the maturity of the technology and of the libraries adopted, this does not currently represent any security risk but as the time passes by, it significantly impacts the possibility of growth of the application, especially in relation to the set of planned project extensions.

Within this project idea we propose to rewrite the current application client pursuing the following set of goals:

- Bump of the core client library from AngularJS to Angular;
- Bump of Bootstrap library from Bootstrap 4 to Bootstrap 5;
- General optimization and modularization of the client

5.2.2 Statistics and Reporting

GlobaLeaks still misses the implementation for any generation of statistics and reports. Such features are considered fundamental in order to properly support users in analysis, investigation and reporting.

E.g:

- Recipients should be able to visually see statistics about the received reports received and the data contained; these statistics should empower users in their work providing relevant information out of the data collection that could help users analyze and study social problems like corruption and be able to organize and export automatic reporting;
- Administrators should be able to visually see a dashboard in order to monitor the system and assure that all is working well (e.g. that recipients are receiving submissions and are able to access them and that no attacks are performed on the system).

Ideas:

- A client library could be adopted to generate reports directly on the client (e.g. Chart.js)
- The implementation should support the possibility of exporting the report in PDF; in relation to this aspect it should be considered the advantages of a possible backend implementation.

Reference tickets:

- <https://github.com/globaleaks/GlobaLeaks/issues/1959>
- <https://github.com/globaleaks/GlobaLeaks/issues/2254>

5.2.3 Audit Log

GlobaLeaks still misses the implementation of a complete audit logit. This is considered a fundamental feature in order to achieve full accountability of the whistleblowing process and increase security.

Ideas:

- Software audit log should be improved
- The software could exposes a standard log interfaces in CEF/LEEF/Syslog format to foster integration with third party SIEM software.

Reference tickets:

- <https://github.com/globaleaks/GlobaLeaks/issues/2579>
- <https://github.com/globaleaks/GlobaLeaks/issues/2580>
- <https://github.com/globaleaks/GlobaLeaks/issues/2651>

5.2.4 GDPR compliance

GlobaLeaks implements by-design many best practices in matters of privacy and security. In order to be effectively accepted and competitive beside commercial proprietary solutions and to guarantee the sustainability of the project, the software needs to achieve some market “standards” (e.g. GDPR compliance / ISO certifications / etc.); among all we selected that GDPR compliance is a first step where the software could implement best practices (e.g. procedures for self signup should present appropriate legal notices, terms of services, and contractualization). Within the software, there should be implemented an automatic contract generation via PDF or other suitable formats in respect with the GDPR requirements.

Reference tickets:

- <https://github.com/globaleaks/GlobaLeaks/issues/2145>
- <https://github.com/globaleaks/GlobaLeaks/issues/2658>
- <https://github.com/globaleaks/GlobaLeaks/issues/2866>
- <https://github.com/globaleaks/GlobaLeaks/issues/2767>
- <https://github.com/globaleaks/GlobaLeaks/issues/3011>
- <https://github.com/globaleaks/GlobaLeaks/issues/3012>

5.2.5 Backup and Restore

GlobaLeaks currently misses any feature for performing backup and restoring of its setup. These duties are currently performed by its users following typical best manual practices (e.g. archiving the data directory of the application). This project idea is to research the best practices to be applied in this context and to identify suitable strategies for implementing periodic, secure and encrypted backups to be restored upon necessity.

Reference tickets:

- <https://github.com/globaleaks/GlobaLeaks/issues/528>
- <https://github.com/globaleaks/GlobaLeaks/issues/2149>

5.2.6 Multitenancy

5.2.7 Import and Export of Tenants

Part of the software is a recent feature of Multitenancy, first implemented in 2018 and stabilized during 2019. Through this feature, GlobaLeaks makes it possible to create multiple setups of itself via virtual sites (similarly to Wordpress multisite feature). In order to make it more easy for an administrator to migrate a platform from a system to an other or to enable users to require data portability from a globaleaks provider to an other, for example in relation to GDPR it has been evaluated necessary to improve the multi tenancy implementation by implementing support for import-export of tenants. In the context of a whistleblowing application, involving encryption and logging this poses important challenges on how to best handle this process.

Reference tickets:

- <https://github.com/globaleaks/GlobaLeaks/issues/2632>
- <https://github.com/globaleaks/GlobaLeaks/issues/2631>

5.3 Multisite Users

(To be further researched)

Important requirement at the base of the Multitenancy expansion is the possibility to enable users to be administrators and recipients of two or multiple instances running on the same multi-site setup. This is useful for example when a lawyer takes part as a recipient on multiple projects; as well it is useful when an ICT consultant joins consultancy on multiple projects.

This could significantly simplify user access enabling the user to have a single set of username and password and associated keys.

References tickets:

- <https://github.com/globaleaks/GlobaLeaks/issues/2302>

DEVELOPER DOCUMENTATION

6.1 Development Environment

This guide describe how to set up an environment in order to contribute to the development of GlobaLeaks.

6.1.1 Requirements

The guide assumes you run a Debian based system and that the following software is installed on your system:

- debhelper
- devscripts
- dh-apparmor
- dh-python
- git
- grunt-cli
- node
- npm
- python3
- python3-dev
- python3-pip
- python3-setuptools
- python3-sphinx
- python3-virtualenv

6.1.2 Setup

The repository could be cloned with:

```
git clone https://github.com/globaleaks/GlobaLeaks.git
```

Client dependencies could be installed by issuing:

```
cd GlobaLeaks/client
npm install -d
grunt copy:sources
```

Backend dependencies could be installed by issuing:

```
cd GlobaLeaks/backend
python3 -menv env
source ./env/bin/activate
pip3 install -r requirements.txt
```

This will create for you a python virtualenv in the directory env containing all the required python dependencies.

Then, anytime you will want to activate the environment to run globaleaks you will just need to issue the command:

```
cd GlobaLeaks/backend && source ./env/bin/activate
```

Setup the client:

```
cd GlobaLeaks/client
npm install -d
grunt build
```

Setup the backend and its dependencies:

```
cd GlobaLeaks/backend
python3 -menv env
source env/bin/activate
pip3 install -r requirements.txt
```

6.1.3 Run

To run globaleaks from sources within the development environment you should issue:

```
cd GlobaLeaks/backend
source ./env/bin/activate
./bin/globaleaks -z -n
```

GlobaLeaks will start and be reachable at the following address <http://127.0.0.1:8082>

6.2 Software Libraries

The software libraries used by GlobaLeaks are listed in the following files:

- Backend: [backend/requirements.txt](#)
- Client: [client/package.json](#)
- Packaging: [debian/control](#)

6.3 Database Schema

Here could be found the [Schema and the ER Model of GlobaLeaks database](#)

6.4 Release Procedure

This is the procedure followed to publish a new GlobaLeaks release.

A release is represented by:

- A version bump;
- An updated CHANGELOG;
- A commit titled “Bump to version \$number”;
- A tag commit \$version signed by a core developer with its own key;
- An updated package on [deb.globaleaks.org](#);
- A signed repository.

6.4.1 Release Tagging

The release is represented by a tag commit on Github performed via:

```
export DEBFULLNAME="GlobaLeaks software signing key"
export DEBEMAIL="info@globaleaks.org"
dch -i
git commit -a -m "commit before new tag message"
git push origin
git tag -s v0.1 -m 'GlobaLeaks version 0.1'
git push origin --tags
```

6.4.2 Release Packaging

The package is built by means of the official official build script by issuing:

```
cd GlobaLeaks && ./script/build -d all
```

This command builds a package for each supported distribution and version.

6.4.3 Package Publishing

The package is published on deb.globalekas.org by issuing:

```
dput globaleaks ../globaleaks_${version}_all.changes
```

6.4.4 Repository Signing

The release is then signed by a core developer by using the official project key via:

```
gpg --detach-sign --digest-algo SHA512 -o Release.gpg Release
```

6.5 Continuous Integration

The GlobaLeaks codebase is continuously tested for bug within a complete continuous integration lifecycle implemented.

Testes are performed at every commit by:

- performing static and dynamic testing on [TravisCI](#);
- tracking tests coverage and code quality with [Codacy](#).

6.5.1 Unit Tests

Unit tests are implemented by means of python-twisted and trial

Tests can be run manually by issuing:

```
cd GlobaLeaks/backend  
trial globaleaks
```

6.5.2 E2E Tests

End to end tests are implemented by means of the Protractor AngularJS library.

Tests can be run manually by issuing:

```
cd GlobaLeaks/client  
./node_modules/protractor/bin/webdriver-manager update  
./node_modules/protractor/bin/protractor tests/protractor.config.js
```


6.6 Code Documentation

- `modindex`

INDEX

A

Administrator, [3](#)

C

Channel, [3](#)

N

Notification, [3](#)

P

Platform, [3](#)

Q

Questionnaire, [3](#)

R

Receipt, [3](#)

Recipient, [3](#)

Report, [3](#)

S

Submission, [3](#)

W

Whistleblower, [3](#)