GlobaLeaks Documentation

Release 3

Hermes Center for Transparency and Digital Human Rights

Mar 09, 2020
# Contents

## 1 Getting started
- **1.1 Glossary** ................................................................. 3
- **1.2 Features** ................................................................. 3
- **1.3 Encryption** ............................................................... 4
  - 1.3.1 Account recovery .................................................. 4
  - 1.3.2 Key escrow ............................................................. 5
- **1.4 Requirements** ............................................................ 5
  - 1.4.1 Hardware requirements ........................................... 5
  - 1.4.2 Software requirements ............................................ 5

## 2 Setup
- **2.1 Installation guide** ..................................................... 7
- **2.2 Platform wizard** ....................................................... 7
  - 2.2.1 Choose the primary language for your site ..................... 8
  - 2.2.2 Configure the name of your project ............................. 8
  - 2.2.3 Configure the account for the administrator of your whistleblowing site .................................................. 9
  - 2.2.4 Configure the account for the first recipient of your whistleblowing site .................................................. 10
  - 2.2.5 Read and accept the license of GlobaLeaks ..................... 11
  - 2.2.6 Complete the wizard ............................................... 12

## 3 User documentation
- **3.1 For all users** ............................................................. 15
  - 3.1.1 Login ................................................................. 15
  - 3.1.2 Access the user preferences ...................................... 15
  - 3.1.3 Change your password ............................................ 15
  - 3.1.4 Reset your password .............................................. 15
  - 3.1.5 Enable Two-Factor-Authentication (2FA) ..................... 15
- **3.2 For administrators** .................................................... 16
  - 3.2.1 User interface ....................................................... 16
    - 3.2.1.1 Site settings ................................................. 17
    - 3.2.1.2 Users .......................................................... 20
    - 3.2.1.3 Questionnaires ............................................. 21
    - 3.2.1.4 Contexts .................................................... 23
    - 3.2.1.5 Case management ........................................... 24
    - 3.2.1.6 Notification settings ...................................... 25
    - 3.2.1.7 Network settings ........................................... 27
    - 3.2.1.8 Advanced settings ......................................... 30
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2.1.9</td>
<td>System overview</td>
<td>32</td>
</tr>
<tr>
<td>3.2.2</td>
<td>Common configurations</td>
<td>33</td>
</tr>
<tr>
<td>3.2.2.1</td>
<td>Configure the logo</td>
<td>33</td>
</tr>
<tr>
<td>3.2.2.2</td>
<td>Enable languages</td>
<td>33</td>
</tr>
<tr>
<td>3.2.2.3</td>
<td>Configure HTTPS</td>
<td>34</td>
</tr>
<tr>
<td>3.2.2.4</td>
<td>Configure notification settings</td>
<td>38</td>
</tr>
<tr>
<td>3.2.2.5</td>
<td>Configure recipients</td>
<td>40</td>
</tr>
<tr>
<td>3.2.2.6</td>
<td>Configure questionnaires</td>
<td>40</td>
</tr>
<tr>
<td>3.2.2.7</td>
<td>Configure contexts</td>
<td>40</td>
</tr>
<tr>
<td>3.2.2.8</td>
<td>Customize the graphic layout</td>
<td>41</td>
</tr>
<tr>
<td>3.2.3</td>
<td>Integration guide</td>
<td>41</td>
</tr>
<tr>
<td>3.2.3.1</td>
<td>Main components to integrate</td>
<td>41</td>
</tr>
<tr>
<td>3.2.3.2</td>
<td>Integration modes</td>
<td>41</td>
</tr>
<tr>
<td>3.2.3.3</td>
<td>URL parameters</td>
<td>42</td>
</tr>
<tr>
<td>3.2.4</td>
<td>Upgrade guide</td>
<td>43</td>
</tr>
<tr>
<td>3.2.4.1</td>
<td>Regular update</td>
<td>43</td>
</tr>
<tr>
<td>3.2.4.2</td>
<td>Upgrade of the distribution version</td>
<td>43</td>
</tr>
<tr>
<td>3.2.4.3</td>
<td>In case of errors</td>
<td>43</td>
</tr>
<tr>
<td>3.2.5</td>
<td>Backup and restore</td>
<td>44</td>
</tr>
<tr>
<td>3.2.6</td>
<td>Troubleshooting</td>
<td>44</td>
</tr>
<tr>
<td>3.2.6.1</td>
<td>Issues and bug reporting</td>
<td>44</td>
</tr>
<tr>
<td>3.2.6.2</td>
<td>Useful debugging commands</td>
<td>44</td>
</tr>
<tr>
<td>3.2.6.3</td>
<td>Log files</td>
<td>45</td>
</tr>
<tr>
<td>3.3</td>
<td>For recipients</td>
<td>45</td>
</tr>
<tr>
<td>3.3.1</td>
<td>Access the list of the existing submissions</td>
<td>45</td>
</tr>
<tr>
<td>3.3.2</td>
<td>Access a submission</td>
<td>45</td>
</tr>
<tr>
<td>3.3.3</td>
<td>Label a submission</td>
<td>45</td>
</tr>
<tr>
<td>3.3.4</td>
<td>Change the state of a submission</td>
<td>45</td>
</tr>
<tr>
<td>3.3.5</td>
<td>Exchange comments with the whistleblower</td>
<td>45</td>
</tr>
<tr>
<td>3.3.6</td>
<td>Export a submission</td>
<td>46</td>
</tr>
<tr>
<td>4</td>
<td>Source code documentation</td>
<td>47</td>
</tr>
</tbody>
</table>

Index

49
GlobaLeaks is an open-source, free software intended to enable secure and anonymous whistleblowing projects developed by the Hermes Center for Transparency and Digital Human Rights.

**Note:** This documentation is thanks to the support of the GlobaLeaks Community. Join us and contribute with your additions and suggestions. 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 GlobaLeaks Ticketing System.
CHAPTER 1

Getting started

1.1 Glossary

This is a list of jargon that is used inside of the GlobaLeaks software. Here we define it in a way to be unambiguous and uniform across all of their references.

**Admin**  The user that has setup and is maintaining the Platform.

**Context**  A topic covered by a Globaleaks based project (ex. Corruption).

**GlobaLeaks**  Our project, a FLOSS, security focused and flexible whistleblowing framework.

**Notification**  Method used to notify a Recipient that a new Submission or an update of an existing Submission is available.

**Platform**  A system running the GlobaLeaks framework.

**Questionnaire**  A questionnaire is a set of questions that the whistleblower should fill out for completing a Submission to a Platform.

**Receipt**  An access token that allows the Whistleblower to be authenticated to the secret (it effectively acts as a password) generated by the Platform and returned to the Whistleblower when a Submission has been completed. It enables the Whistleblower to modify and update the submission eventually uploading new files, adding comments to the Tip, and reading Receivers’s comments about the submitted materials.

**Recipient**  It is the receiver of an anonymous Submission sent by the Whistleblower.

**Submission**  The action performed by the Whistleblower to submit a Tip to the Platform. This action is performed by the Whistleblower in respect to the Context requirement.

**Whistleblower**  A user that is reporting to the Platform by uploading material and filling out the submission form.

1.2 Features

- Configurable submission contexts and questionnaires
• Single and multiple recipients capabilities
• Integrated Multi-Tenancy support
• Support for anonymous submissions (via Tor) and confidential submissions (via HTTPS)
• Integrated optimized HTTPS capability with support for Let'sEncrypt Certification Authority
• Rich configuration options and defaults
• Optimized UI with advanced User Experience (UX)
• Accessible Rich Internet Application compliant to WAI-ARIA
• Embedded internationalization and localization support
• Fully translated in more than 30 languages
• Support for Right-to-Left (RTL) design
• Integrated support for PGP and AES encryption
• Ongoing development for clientside encryption
• Configurable mail templating system for each notification
• All-in-one solution including embedded webserver and SQLite database
• Integrated network sandboxing (IPTables)
• Integrated application sandboxing (AppArmor)
• Two-Factor Authentication (2FA) support compliant to standard TOTP RFC 6238
• Support for multi-tenancy and multi-site
• Fully unit-tested and end2end tested on commit with test code coverage over 90%
• Strong security with 5 independent audits
• Including Whistleblower Identity Management features compliant with Italian Anticorruption Authority Specs ANAC
• Compliant with recent whistleblowing protection laws in the fields of whistleblowing protection like Italian 190/2012 and 231/2001, French Sapin II and International ISO 37001

1.3 Encryption

By default GlobaLeaks implements encryption for each submission protecting answers to the questionnaire, comments, attachments and involved metadata. The keys involved in the encryption are per-user and per-submission and only users to which the data was destinated could access the data. Keys are generated for each user at the first login and the keys are kept securely encrypted with a secret derived; This mechanism guarantees that only the user could access the data. Please note that user would forget the password the data won’t be accessible anymore. In order to know about the features involved in account recovery and key escrow see the two specific sections on the topic.

1.3.1 Account recovery

To protect from possible password loss and corresponding data loss, users are entitled to download or print a personal recovery key and they could make this anytime via their profile section. It is highly recommended to include this manual procedure in any user documentation requiring users to perform this operation before actually starting using the system.
1.3.2 Key escrow

A key escrow mechanism is implemented by default and enables the admin user to restore user account on behalf of users in case of data loss. This feature is automatically enabled on the first admin user created by the system and depending on the threat model and the organizational aspects of the projects this user is entitled to disable the feature or to enable it for other admin users.

1.4 Requirements

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

1.4.1 Hardware requirements

Requirements:

- CPU: Dual core 2.0GHz
- RAM: 2GB (Does not impact the maximum filesize that a platform installation can handle in upload)
- STORAGE: 20GB Allocate more based on data retention policy and (expected) traffic.
- I/O: 10Mbit/s (shared)

1.4.2 Software requirements

GlobaLeaks is designed to run on GNU/Linux and developed and tested specifically for Debian 10 (Buster)

The software lifecycle of the platform includes full support for all Debian and Ubuntu LTS versions starting from Debian 10 and Ubuntu 18.04.

On these platforms the support is guaranteed following the Release End of Life defined by Ubuntu.

Support for more distributions is planned.
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 Copy & Paste the following commands in your terminal:

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

At the end of the process a web interface will be reachable locally on port 8082 and remotely on port 80 and you will be able to proceed with 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 local or remote IP respectively.
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.

Welcome!

The following step-by-step procedure will guide you through creating your whistleblowing platform.

2.2.2 Configure the name of your project

In the second section of the wizard configure the name of your project.
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.
2.2.4 Configure the account for the first recipient of your whistleblowing site

In the forth section of the wizard configure the account details of the first recipient for the submissions to your project. Note that the recipient’s password is set to a pre-defined value “password”.

Powered by GlobalLeaks
2.2.5 Read and accept the license of GlobaLeaks

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

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

You have completed the platform wizard.
CHAPTER 3

User documentation

3.1 For all users

3.1.1 Login

TODO

3.1.2 Access the user preferences

TODO

3.1.3 Change your password

TODO

3.1.4 Reset your password

TODO

3.1.5 Enable Two-Factor-Authentication (2FA)

TODO
3.2 For administrators

3.2.1 User interface

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

Anytime you log in as administrator via the Login page the application takes you to your personal administrative Homepage: This page includes some documentation about GlobaLeaks that is intended to clarify you all the up-to-date documentation in matter of software security, best practices and community support.

From this Home page you may access all the common user facilities already described in the general User Documentation.

A menu on the right offers you links to the different administrative sections:

1. Site settings
2. Users
3. Questionnaires
4. Contexts
5. Case management
6. Notification settings
7. Network settings
8. Advanced settings
9. System overview

3.2.1.1 Site 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. Main configuration
2. Theme customization
3. Files
4. Languages
5. Text customization

Main configuration

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

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

In this section could be loaded any file that need to be served via the platform to whistleblowers (e.g. a policy in PDF) or that are required by your CSS and Javascript customization.

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!
3.2.1.2 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

Administrators

TODO

Recipients

TODO

3.2.1.3 Questionnaires

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

By default the software implements a Default Questionnaire with a single Step and the following three questions:

One question “Short description” of type “Multi-line text input” enabling whistleblower to provide a short summary of the fact reported;

One question “Full description” of type “Multi-line text input” enabling whistleblowers to describe the fact reported in detail;

One question “Attachments” of type “Attachment” enabling users to load one or more attachments.

The system with its basic configuration completed with the initial Platform wizard is also already configured with this Default Questionnaire pre-associated to the Default Context.

Depending on your project needs you could create specific questionnaire for each of your different submissions’ contexts.
Depending on your project needs you may evaluate defining some questions once as Question Templates and reuse the same question in multiple questionnaires.

**Steps**

The software enables to organise 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. Map
11. Question group

General 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 submission list

Question properties by question type

**Single and Multi line text input**

TODO

**Selection box, Multiple choice input, Checkbox**

TODO

**Question groups**

TODO

**Conditional questions**

TODO

3.2.1.4 Contexts

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

A whistleblowing channel is typically defined by the following main characteristics

3.2. For administrators
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 submissions 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 Context called Default, on which is associated a recipient and the default questionnaire.

Depending on your project needs here you could create additional Contexts and configure their respective recipients and 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 submissions 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 submissions received therein.

By default a context is configured with a submission expiration of 30 days.

3.2.1.5 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 submissions statuses and substatuses intended to be used by Recipients while working on the submissions.

By default the system includes the following submission 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 Substatuses for the Closed status (e.g. Archived / Spam)
3.2.1.6 Notification settings

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 enviroment.
In this section are configured the notification templates.

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.

3.2.1.7 Network settings

In this section are configured the network settings.

The section is furtherly divided in:

1. HTTPS
2. Tor
3. IP Access control

HTTPS

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

**Tor**

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

### IP Access Control

- **Tor Onion Service**: 54zmr3s3wlruf54gfcdkijfsglbtcbuiqrlmtzpe5h5gfta42pkmqd.onion
- **Tor Browser download link**: https://www.torproject.org/download/download-easy.html

- **Anonymize outgoing connections**: Check
- **Let the platform be reachable without Tor**: Check

<table>
<thead>
<tr>
<th>Role</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>✔️</td>
</tr>
<tr>
<td>Custodian</td>
<td>✔️</td>
</tr>
<tr>
<td>Recipient</td>
<td>✔️</td>
</tr>
<tr>
<td>Whistleblower</td>
<td>✔️</td>
</tr>
</tbody>
</table>

[Save]

3.2. For administrators
Suggested configurations are:

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

3.2.1.8 Advanced settings

TODO
Main configuration | URL redirects | Anomaly detection thresholds

- Disable submissions
- **Enable encryption**
- **Enable encryption’s keys recovery**
- **Enable multisite feature**
- **Allow recipients to delete submissions**
- **Allow recipients to postpone expiration date of the submission**
- **Allow recipients to grant permissions to whistleblowers on specific submissions**
- **Enable search engines indexing**

**Description**

Allow the following websites to embed the platform inside iframes

```
domain, domain, domain
```

- **Enable custom privacy panel**
- **Disable the privacy panel**
- **Enable the receipt hint**
- **Enable the Ricochet panel**

**Amount of days till whistleblower access expires**

```
365
```

For security reasons the whistleblower access is subject to expiration.
Tweak this setting only if you know what you are doing.

- **Require two factor authentication**

**Password change interval**

```
90
```

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

**Landing page**

```
home
```

**Default questionnaire**

```
Default
```

3.2. For administrators

**Title of the submission page**

```
Blow the whistle
```
3.2.1.9 System overview

**TODO**

<table>
<thead>
<tr>
<th>Low risk</th>
<th>High risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available disk space (in megabytes)</td>
<td>1000</td>
</tr>
<tr>
<td>Available disk space (in percentage)</td>
<td>10</td>
</tr>
</tbody>
</table>
3.2.2 Common configurations

3.2.2.1 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.

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

3.2.2.2 Enable languages

You may want your GlobaLeaks installation served on more than one language, other the one selected as primary during First Configuration (todo: insert cross reference).

To do so, in the “Administration Interface - General Settings” page, select the “Languages” tab: a list of all available languages is shown. Select the alternative chosen language(s) and scroll down through the page to the “Save” button, click it to save your choices.

Note that in the same interface you can change, through a drop down menu, the default language in which GlobaLeaks installation is served.
3.2.2.3 Configure HTTPS

It is quite important to configure HTTPS for your GlobaLeaks installation. Nowadays, every website should protect its users with HTTPS, and this is so much true for a whistleblowing system. HTTPS helps prevent malicious actors from tampering the communications between your GlobaLeaks installation and the browser of the users.

To configure HTTPS, go to “Administration interface - Network settings” and select the “HTTPS Settings” tab. If not already filled with the hostname of the GlobaLeaks installation you are configuring, just fill the “Hostname” field with the FQDN and click on the “Verify” button.

If the verification process is successful, just click on the “Proceed” button; otherwise, you have to verify that the domain name you choose is correctly set up.

Note: Keep in mind that domain name propagation over DNS can take some time.
You then have to choose among two proposed options:

- **Automatic**: the entire process of requesting, enabling and renewing certificates will be handled from the Let’s Encrypt Certificate Authority. The parent organization, the Internet Security Research Group, is committed to providing the service for free. (You can read more about this on [https://letsencrypt.org](https://letsencrypt.org))

- **Manual**: if you already have a certificate from a Certificate Authority, this is your option. A wizard will guide you through the process of installing said certificate

**Automatic HTTPS Configuration**

To configure HTTPS the easy way, with free certificate from Let’s Encrypt ([https://letsencrypt.org](https://letsencrypt.org)), just click on the “Proceed” button in the “Automatic” box
This can take a little and the “loading” symbol is shown
When ready, the system will prompt you to read the Term of Service from the Let’s Encrypt site by clicking on the button “Read the Term of Service”. If you agree to accept said TOS, check the checkbox “I agree to the Term of Service” and click on the “Proceed” button, this will start the automatic generation and installation of the Certificate. .. image:: imgs/HTTPS_Config_Automatic_Option_3.png

When this process is completed, you will be prompted to immediately activate the configuration by clicking on the “Enable” button, or review the configuration by clicking on “Review” button. .. image:: imgs/HTTPS_Config_Automatic_Option_4.png

By clicking on “Enable”, the system will provide to configure entirely the feature and you will be shown this alert box: .. image:: imgs/HTTPS_Automatic_Conf_Ongoing.png

When finished you will be disconnected ad an admin and your browser redirected to the https version of the platform, where you can login to follow up with configuration.

3.2. For administrators
Manual HTTPS Configuration

The interface can generate the Private Key and the Certificate Signing Request. The Certificate Signing Request has to be provided to a Certificate Authority (usually, your ISP can help you with this) to retrieve a Certificate. After having validated your request and your ownership of the hostname, the Certificate Authority will issue you a Certificate and provide a file containing Intermediate Certificates. Load the Certificate and the file containing the Intermediate Certificates to complete the HTTPS setup. .. HINT: Please note that the file format expected for all files uploaded is PEM. Sometimes Certificate Authorities will provide certificates in DER format which must be converted to PEM.

3.2.2.4 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.
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 submission; 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.

3.2.2.5 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.

3.2.2.6 Configure questionnaires

TODO

3.2.2.7 Configure contexts

The context is sort a conceptual container of your whistleblowing initiative. To better understand this, just think about a whistleblowing initiative devoted to gather information about ethical misconducts infringing the ethical code of a governmental agency or of a company. When you configure the Context you will assign to it a name that can be evocative of the mission related to this context so that the whistleblowers know that this is the right place where to communicate their data. Then you would like to describe in more detail the context itself, so that whistleblower are informed that this is part of a whole process in which specific persons, the receivers, will receive and follow up on the data they’re submitting.

To configure a Context, log in as an admin, go to the administration interface, select “Context configuration” in the menu on the left of the page and fill the text field with the name choosen for the Context, then click on “Add” button. .. image:: imgs/Context_conf_1.png

Then you will see that the new Context is added to the page and to access the configuration interface for this context, click on the “Edit” button. .. image:: imgs/Context_conf_2.png

The configuration interface specific of the selected context is shown and you can proceed with filling of the various field. .. image:: imgs/Context_conf_3.png

The most important field in this section at this stage of the configuration process is surely the “Text shown on top of the interface for selecting recipients”: this text will be shown in the interface exposed to the whistleblowers. So
be sure to use suitable and appealing terms and phrases and be clear in explaining which data are accepted, who will be the recipients, which is the follow up of the submitted data. Just think of this text as the main tool to convince your source to submit data through this channel. Once completed this task, click on “Save” button. You can verify the appearance by visiting ...

### 3.2.2.8 Customize the graphic layout

#### Example 1: custom background

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

```css
body {
    background-color: red;
}
```

#### Example 2: custom font

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

```css
@font-face {
    font-family: 'Antani';
    src: url('static/antani.ttf') format('truetype');
    font-weight: normal;
    font-style: normal;
}

body {
    font-family: 'Antani', Helvetica, Arial, Sans;
    font-size: 16px;
}
```

### 3.2.3 Integration guide

This guide illustrates how GlobaLeaks can be integrated into an existing website.

#### 3.2.3.1 Main components to integrate

There are two main components that need to be integrated into an initiative’s website. They are:

- **Submission interface** (this lets a whistleblower make a new submission): /#/submission
- **Receipt interface** (this lets a whistleblower interact with an existing submission): /#/receipt

These are the main examples which are typically required. In general, though, every URL in GlobaLeaks can be embedded on the host’s website. If the URL Parameter ?embedded=true is appended to a GlobaLeaks URL, the page’s header and footer is removed and the page becomes embeddable within another page.

#### 3.2.3.2 Integration modes

Depending on the integration requirements, the following configurations are possible:
• Plugin based integration (suggested)
• iframe based integration

Plugin based integration

GlobaLeaks provides a specific Javascript plugin to be used for integration. The platform makes it available at /js/plugin.js. The plugin can be included on a website with a script tag like:

```
<script type="text/javascript" src="https://PublicWebsite/globaleaks/js/plugin.js"></script>
```

The plugin safely loads the platform as a widget by calling the function StartGlobaLeaks(). This function can be used to embed specific platform resources. In the following example the submission interface is loaded when the link is clicked.

```
<a href="javascript:startGlobaLeaks('https://PublicWebsite/globaleaks/#/submission')" style="text-decoration: none;">Blow the Whistle!</a>
```

Iframe based integration

Using iframes to integrate GlobaLeaks into a website is not recommended because browsers are known to leak information about a whistleblowers browsing activity. However, they have been used in the past in low-risk environments and are worth mentioning. Including the two main components is similar to the plugin based solution discussed above.

Submission interface

```
<iframe width="100%" height="100%" frameborder="0" src="https://PublicWebsite/#/submission?embedded=true"></iframe>
```

Receipt Interface

```
<iframe width="100%" height="100%" frameborder="0" src="https://PublicWebsite/#/receipt?embedded=true"></iframe>
```

3.2.3.3 URL parameters

There are several URL parameters that a web developer can use to change the GlobaLeaks platform’s behaviour when integrating the platform into a website.

Language selection

The lang URL parameter pre-selects the language used in the interface. The example below loads the submission interface in English.

```
/#/submission?lang=en
```

Context selection

The context URL parameter selects a specific submission context to load by passing a UUID. For example:
Note that a context’s UUIDs can be found on the platform in the context configuration section of the administration interface.

### 3.2.4 Upgrade guide

#### 3.2.4.1 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
```

#### 3.2.4.2 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

#### 3.2.4.3 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
```
3.2.5 Backup and restore

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

```bash
#!/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)

3.2.6 Troubleshooting

3.2.6.1 Issues and bug reporting

If you encounter any issue and you are not able to to run GlobaLeaks h

- 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/GlobaLeaks/issues

3.2.6.2 Useful debugging commands

Depending on your setup. There are a few things that are usually the first things to check to see if GlobaLeaks 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? Is Tor2Web service listening on 443?

netstat -tap

• Are exceptions being generated?

less /var/globleaks/logs/globaleaks.log

3.2.6.3 Log files

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

GlobaLeaks process:

/var/globaleaks/logs/globaleaks.log

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

Tor:


3.3 For recipients

3.3.1 Access the list of the existing submissions

TODO

3.3.2 Access a submission

TODO

3.3.3 Label a submission

TODO

3.3.4 Change the state of a submission

TODO

3.3.5 Exchange comments with the whistleblower

TODO
3.3.6 Export a submission

TODO
CHAPTER 4

Source code documentation

- modindex
Index

A
Admin, 3

C
Context, 3

G
GlobaLeaks, 3

N
Notification, 3

P
Platform, 3

Q
Questionnaire, 3

R
Receipt, 3
Recipient, 3

S
Submission, 3

W
Whistleblower, 3