Install the software.

Extract the archive in a cool/dry place, `/var/www/OSSEC-WUI` or `/var/www/html/OSSEC-WUI` are good places !
Your web server must use PHP 7, previous versions were working with PHP 5 but I can't do any more testing with PHP 5 which is already « end of life ».
The following PHP extensions are mandatory :

```
php7 curl
php7 json
pho7 mbstring
php7 mysql
php7 xml
```

The installation should work with Postgresql but I didn't test it.
In the first step we install the software without authentication.

Connection with the database.
The database conmection is defined in the file "db_ossec.php" :

```
...
if ( ! defined('DB_USER_O') )
     {    define ('DB_USER_O', 'User name');
          define ('DB_PASSWORD_O', 'Password');
          define ('DB_HOST_O', 'IP Address');
          define ('DB_NAME_O', 'Database name');
          define ('DB_TYPE_O', 'running');
#         define ('DB_TYPE_O', 'history');
     }
....
```

The constant "DB_TYPE_O" is used to define the "type" of the installation :
"running" for the database fed directly by Ossec.
"history" for the "history" database.
The standard use is the "running" mode with only one database.

Adapt the functionnal parameters.
Some parameters are stored in the file "config.php".
You can adjust some functions eg:
- $google_api_key = string
Used for accessing the maps (for IP inspection), get a new one as it is mine !
- $glb_indexgraphlogarithmic = "true"
You can use "false", but "true" gives often a better view ...
- $glb_autorefresh = integer (seconds)
Self explanatory.

Some "default" values used for the first use of "index.php" for example
- $glb_level = 1 .. 15
Default level at launch
- $glb_hours = 1..144
Number of hours displayed.
- $glb-graphbreakdown = (source|path|level|rule_id)
Mode used for the "index.php" graph

Some values to use to set the height for some graphs it can be handy for rather small screens :
- $glb_height_index = 380;
For the "index.php" graph
- $glb_height_detail = 300;
For the "detail" graph
- $glb_height_stat_rules = 500;
For statistics by rule
- $glb_height_stat_level = 500;
For statistics by level
- $glb_height_mass_left = 600;
  $glb_height_mass_right_high = 300;
  $glb_height_mass_right_low = 300;
For adjusting size for the three graphs for massmonitorig.

Look in that file to see other parameters.

Two « modes » are avaliables.
The standard mode is called "running" and uses directly the ossec database.
You can split the datas between 2 databases :
- the "running" feeded by Ossec.
- the "history" feeeded by all alerts deleted from the "running" database.
The method is efficient, you delete alerts from "running" when alert are proceded but all deleted alerts are inserted in the "history" database for statistical needs and other reasons.
So the "running" part is rather small and it is esay to look into data but all information remain in the history.

For the history database you need to :
- create a new database
- give rights to the owner of the running database to insert into that new base.
- create a new user with insert/delete/select/update on the new base (or use the standard user with enough rights on the new database. The new user must, at lesast, have a right to select in the running database.
- create an "alert" table in the new base
- create basic views giving access to the other tables in the running user.
  example : create view category as select * from running.category;
- add a trigger on the running tale "alert" to insert deleted rows in the history alert table.
Models of all actions are provided in the SQL directory.

For the software you need to create a new directory near /var/www/OSSEC-WUI, for example /var/www/OSSEC-WUI-HIS... and create links.
cd OSSEC-WUI-HIS
ln -s ../OSSEC-WUI/* ./
rm db_ossec.php
rm config.php
cp ../OSSEC-WUI/db_ossec.php ./
cp ../OSSEC-WUI/config.php./

So you can access the history database with the right mode "history".

```
if ( ! defined('DB_USER_O') )
        {       define ('DB_USER_O', 'User name');
                define ('DB_PASSWORD_O', 'Password');
                define ('DB_HOST_O', 'IP Address');
                define ('DB_NAME_O', 'History Database name');
#               define ('DB_TYPE_O', 'running');
                define ('DB_TYPE_O', 'history');
        }
```

If you run with the authentication facility the file « db_auth.php » has the same structure for the « auth » database, There is a small doc for using the auth facility.
And adjust some parameters in the config.php to your needs.

The « authenticated » mode is not enabled by default.
To enable it you will have to « link » amilogged.php_auth to amilogged.php et look the AUTH_INIT doc.
That's all.