Enable the log-out feature for GestióIP >= 3.5

GestióIP 3.5 comes with and log-out mechanism. For installations which where upgraded to v3.5 from an older version, the log-out feature must be enabled manually.

To enable log-out you need to

- Enable the Apache modules mod_session and mod_session_crypto.
- Edit the Apache configuration file gestioip.conf.
- Restart the Apache web server.

After restarting the Apache web server there will appear the log-out button within the GestióIP front end.

1 Enable the required Apache modules

1.1 Ubuntu

All required packages should be installed by default. Just enable the required packages with the following commands.

```
sudo a2enmod request
sudo a2enmod rewrite
sudo a2enmod session
sudo a2enmod session_cookie
sudo a2enmod session_crypto
sudo a2enmod auth_form
```

1.2 Redhat

Install the required packages:

```
sudo yum install mod_session apr-util-openssl
```

To enable the required packages open the following two files with an editor:

/etc/httpd/conf.modules.d/01-session.conf:

Make sure that the following two lines are uncommented.

```
LoadModule auth_form_module modules/mod_auth_form.so
LoadModule session_crypto_module module/mod_session_crypto.so
```

/etc/httpd/conf.modules.d/00-base.conf:

Make sure that the following line is uncommented.

```
LoadModule request_module modules/mod_request.so
```

2 Edit the Apache configuration

GestióIP's Apache configuration file is called gestioip.conf.

You find the Apache configuration gestioip.conf, depending in the Linux distribution in

/etc/apache2/sites-available/gestioip.conf (Ubuntu)
/etc/httpd/conf.d/gestioip.conf (RH, CentOS)
/etc/apache2/conf.d/gestioip.conf (Suse)

First make a backup of the old configuration file. Change to the directory where the file gestioip.conf is located and execute the following command:

```
sudo cp gestioip.conf gestioip.conf.orig
```

If there occur problems with the new configuration, you can restore the old configuration at any moment with the command.

```
sudo cp gestioip.conf.orig gestioip.conf
```

Now edit the Apache configuration: open the file gestioip.conf with an editor, comment out the line "AuthType Basic":

```
#AuthType Basic
```

and add the blue lines of the sample configuration.

Replace the lines **[DOCUMENT_ROOT]** with the Apache document root:

Apache document root:
/var/www/gestioip (Ubuntu <18)
/var/www/html/gestioip/ (Ubuntu >= 18)
/var/www/html/ (Redhat)
/srv/www/htdocs (Suse)

Replace **MY_SECRET_CHANGE_ME** by a random string.

Replace **[APACHE_CONF_DIR]** with the Apache configuration base directory:

/etc/apache2/ (ubuntu)

/etc/httpd/ (RH, CentOS)
/etc/apache2/ (Suse)

Sample configuration file with mod_session enabled:

```
# Apache 2.4 configuration file for GestioIP

<Directory "[DOCUMENT_ROOT]">

        RewriteEngine On
        RewriteBase /
        RewriteCond %{ENV:REDIRECT_STATUS} ^401$
        RewriteRule .* - [E=REMOTE_USER:%{ENV:REDIRECT_REMOTE_USER}]

        AddHandler cgi-script .cgi
        AddDefaultCharset utf8
        AllowOverride None
        DirectoryIndex index.cgi
        Options +ExecCGI +FollowSymLinks

        #AuthType Basic
        AuthFormProvider file
        AuthType form
        AuthName GestioIP
        Session On
        SessionEnv On
        SessionCookieName session path=/
        SessionCryptoPassphrase MY_SECRET_CHANGE_ME

        AuthUserFile [APACHE_CONF_DIR]/users-gestioip
        Require user gipadmin

        ErrorDocument 401 /gestioip/login/login.html
        ErrorDocument 403 /gestioip/errors/error403.html
        ErrorDocument 404 /gestioip/errors/error404.html
        ErrorDocument 500 /gestioip/errors/error500.html
</Directory>

<Directory "[DOCUMENT_ROOT]/login">
    Order deny,allow
    Allow from All
    Satisfy Any
</Directory>

<Directory "[DOCUMENT_ROOT]/logout">
        SetHandler form-logout-handler
        AuthFormLogoutLocation "/gestioip/login/logout.cgi"
        Session On
        SessionMaxAge 1
        SessionCookieName session path=/
</Directory>

<Directory "[DOCUMENT_ROOT]/css">
    Order deny,allow
    Allow from All
    Satisfy Any
</Directory>

<Directory "[DOCUMENT_ROOT]/api">
    AuthType Basic
</Directory>

<Directory "[DOCUMENT_ROOT]/priv">
        AddDefaultCharset utf8
        AllowOverride None
        Require all denied
```

```
</Directory>

<Directory "[DOCUMENT_ROOT]/modules">
        AddDefaultCharset utf8
        AllowOverride None
        Require all denied
</Directory>

<Directory “[DOCUMENT_ROOT]/errors”>
        AddDefaultCharset utf8
        AllowOverride None
        Order deny,allow
        Allow from All
        Satisfy Any
</Directory>
```

3 Restart the Apache webserver

Restart the Apache web server to make the changes take effect.

Execute a syntax check against the new configuration first:

```
sudo apachectl -t

Syntax OK
```

If there appear the output “Syntax OK”, restart the web server:

Ubuntu:

```
sudo systemctl restart apache2
```

If the service is not starting correctly execute the following command to search for errors

```
sudo systemctl status apache2
```

And check the log files under /var/log/apache2.

Redhat/Centos:

```
sudo service httpd restart
```

If the service is not starting correctly execute the following command to search for errors

```
sudo service httpd status
```

And check the log files under /var/log/httpd.