Issues / Problems

Let's Encrypt Setup & Troubleshooting

EHCP & Let's Encrypt

EHCP integrates with Let's Encrypt allowing users and administrators to configure their domains and websites to use HTTPS using free SSL certificates.

To enable Let's Encrypt support, the web server mode must be set to SSL or SSLOnly in the advanced settings of EHCP. To get to the advanced settings page, on the EHCP panel home page, click on "Options" under "System Operations". On the next page, click on the link that says "Advanced Settings". Here, you can change whether or not the server should run apache2 or nginx. This is also where you can configure the HTTP mode the server should use. You can use non-ssl, ssl mixed mode (both non-ssl and ssl supported), or ssl only. Enable SSL mixed or only mode in order to enable Let's Encrypt certificate support.

Here's how Let's Encrypt works in EHCP:

Each domain configured in the EHCP panel can be configured to use a Let's Encrypt or custom SSL certificate. To configure the domain to use a Let's Encrypt SSL certificate, select the domain in the panel, and then click on "Add SSL Certificate". If your server is running mixed SSL mode, you will have the option to enable "Redirect All HTTP Requests to HTTPS" for each domain. If this option is selected, non-SSL requests will be automatically redirected to SSL HTTPS requests. If this option is not selected, standard HTTP requests will not be redirected to HTTPS requests automatically.

If you are logged in as the admin account, there are additional advanced settings that allow you to request additional domains and subdomains that the panel may not have automatically configured for special setups. To see these options, click on the "Show Advanced Admin Options" button.

Click on the "Use FREE SSL" button to request a SSL certificate from Let's Encrypt for your domain. EHCP will now request a SSL certificate from Let's Encrypt using Certbot. This process may fail due to a variety of reasons. The most common error is that the user's account has been configured in EHCP with an invalid email address. Make sure each user has a valid email address set in the panel, and that includes the admin account & the panel's default email address (which can be adjusted in the options page - adminemail option). If EHCP fails to retrieve a SSL certificate from Let's Encrypt, the default EHCP SSL certificate will be used for the domain, which won't technically be valid. To see what went wrong, look at the log file in /var/log/letsencrypt/letsencrypt.log on the server.

If something goes wrong, you can re-initiate the Let's Encrypt request for the domain by going to the "Add SSL Certificate" page. Here, click on the "Remove and Reset SSL Configuration for Domain" link and then click on the "Remove Certificate & Reset SSL Settings" button. Then, repeat the initial steps for requesting a certificate from Let's Encrypt to try again. Again, reasons for failure will show up in the /var/log/letsencrypt/letsencrypt.log log file on the server. After you correct each issue, you will need to begin the request again by first removing any SSL configuration for the domain and then re-requesting a Let's Encrypt certificate.

Default Certificate Request

Issues / Problems

By default, EHCP will request a SSL certficiate for the domain and all of its EHCP configured sub-domains. However, alias subdomains depending on the web server mode such as cp.domain.com or webmail.domain.com will NOT be protected by default. The **root domain itself must be configured to use Let's Encrypt** before any subdomains can also use Let's Encrypt.

However, the advanced admin options can be used to request additional custom domain and sub-domain Let's Encrypt certificates. If you do use the advanced admin options to request custom certificates, you must configure the domain to use them manually. This can be done by selecting the domain in the EHCP panel. Now, click on "Edit Apache Template". This page will show the apache2 or nginx site template for the domain. Here, you can configure, set, and use manual paths to custom Let's Encrypt certificates. You must make manual changes and edits here, or they will be overwritten when the EHCP panel next syncs everything.

Final Notes

Let's Encrypt issues certificates for working domains only. If your domain isn't reacheable to the outside world, a certificate will not be issued, and the default EHCP certificate will be used locally on the server. Make sure your name servers are set up properly on the domain to point to the EHCP web server before requesting to use Let's Encrypt for SSL.

The user requesting a certificate **must have a valid email address associated with his EHCP account** in order to retrieve and use a Let's Encrypt SSL certificate.

Unique solution ID: #1010
Author: Eric
Last update: 2018-01-22 22:17