SSL configuration

In order for EZproxy to give remote users access to resources with secure URLs, you must obtain, install, and configure an SSL Certificate.

Overview

Secure URLs begin with https instead of http. For example, a URL that would require an SSL certificate and configuration in EZproxy would look like this:

https://www.researchdb.com

If you have any resources with URLs beginning with https, you will need to configure EZproxy to run with an SSL Certificate.

This page will guide you through the steps required to create an SSL certificate and activate it for use by EZproxy.

OpenSSL

These features of EZproxy use the OpenSSL Toolkit. The EZproxy program files contain the OpenSSL routines required by EZproxy; no separate library files need to be downloaded to provide this functionality.

Certificate renewal

If you are already using an SSL certificate with EZproxy and need to renew that certificate, refer to SSL Certificate Renewal for more information.

Watch a video

Using an SSL Certificate with EZproxy (11:23)

This video will help you understand SSL Certificates, and your options when it comes to choosing what kind of SSL Certificate to use with EZproxy.

Media, iframe, embed and object tags are not supported inside of a PDF.
Choose your certificate

EZproxy allows you to generate self-signed certificates or to request certificates from a certificate authority such as VeriSign, Thawte, etc. You must decide whether you want to use a self-signed certificate or purchase a certificate from a certificate authority.

- A self-signed certificate is free, but will cause a browser warning when people access your EZproxy server. Users can choose to ignore the browser warning and move on to the resource.
- A certificate purchased from a Certificate Signing Authority will allow a user to access https URLs without browser warnings.

You must also determine whether to use a wildcard certificate.

- If you are using Proxy by Port, you do not need a wildcard certificate.
- If you are using Proxy by Hostname, a wildcard certificate will ensure your users do not see browser warnings during login or when proxying https web sites.

For more information on differences in browser behavior, consult [SSL Certificate Options](#).

If you purchase a certificate, make certain that you are backing up your EZproxy installation, and particularly the ssl subdirectory because if you lose these files, you may have to pay to replace the certificate.

Clean up config.txt

Before you begin configuration, you will need to clean up config.txt.

1. Check config.txt to see if it contains the following directive:

   ```
   Option IgnoreWildcardCertificate
   ```

   If you find this directive, it indicates that your EZproxy server may be using a wildcard certificate that was created outside of EZproxy and imported manually. This option can interfere with certificates created within EZproxy. If you find this directive and you are planning to create a certificate from within EZproxy, you should delete this directive.

2. If you have not already done so, edit user.txt and add the following line:

   ```
   someuser:somepass:admin
   ```

   Replace someuser and somepass with the username and password you will use to log in to EZproxy with administrative access. You will use these login credentials to enable your SSL certificate in EZproxy.

Configure

The following instructions explain how to configure EZproxy to enable https support. In all of these examples, in any location where `http://ezproxy.yourlib:2048` appears, you should substitute your own EZproxy server name and port.

1. If you are using proxy by hostname, or if you are using proxy by port and want to use https to encrypt user login processing, edit config.txt and add the line:
LoginPortSSL 443

443 is the preferred number as this is the standard port for use with https. If you already have a secure web server running on the same system as EZproxy, it will already be using port 443. In this case, you will need to either set up two separate IP addresses on your server, or you will need to pick an alternate number such as:

LoginPortSSL 2443

If you use a firewall, you may also need to configure it to allow access to the port you select.

2. Login to your EZproxy server at your admin URL:

http://ezproxy.yourlib.org:2048/admin

using the admin username and password entered in your config.txt. If you use CAS, CGI, or Shibboleth for user authentication, please consult EZproxy Administration for additional steps that are required to access the administration page.

3. From the EZproxy administration page, under the Miscellaneous heading, click on Manage SSL (https) certificates. This page is referred to as the SSL management page throughout the rest of this document.

4. On the SSL management page, click Create New SSL Certificate.

5. In the Create New SSL Certificate form, when creating a new certificate for both Proxy by Port and Proxy by Hostname configurations, you must fill in the following required information.

   a. Country: your two-letter country code
   b. State or Province: your unabbreviated state or province (e.g. Ohio, not OH)
   c. Organization: your organization
   d. Administrator email: your email address

Wildcard Certificates and EZproxy V6.1 and Later

If EZproxy is configured to Proxy by Hostname and you are running EZproxy V6.1 or later, you will also see the following options.

   • Certificate name: The name that will appear in the CN field of your certificate.
   • Subject Alternate Name: The name(s) that will appear in the SAN field of your certificate.

The options you select in these fields will depend upon the requirements of your Certificate Signing Authority (CSA). For details about these fields and other optional fields, refer to your certificate authority's documentation. If your CSA requires you to enter your server's wildcard name in the SAN field, you must be running EZproxy V6.1 or later.

If you are generating a self-signed certificate, you can select any combination of entries for these fields because all self-signed certificates generate browser warnings.

Wildcard Certificates and EZproxy V6.0.8 and Earlier

If you are using EZproxy V6.0.8 or earlier, EZproxy will not use the SAN field when looking for domains. Your certificate must contain the following:

   • Certificate name: Must be a wildcard entry containing ".*", for example, *.ezproxy.college.edu
   • Subject Alternate Name: Must contain the non-wildcard domain, for example, if the wildcard domain looks as
above, the SAN must be ezproxy.college.edu

All EZproxy URLs that are in websites or publicized to users must use the following syntax: http://ezproxy.college.edu/login?url=http://www.somedb.com

6. If you have decided to create a self-signed certificate, click Self-Signed Certificate. Once you see the Certificate Details page, skip to step 11.

7. If you have decided to purchase a certificate, click Certificate Signing Request. You will be taken to a page with Certificate Signing Request (CSR) Details.

8. EZproxy will display a Certificate Signing Request (CSR), which is a block of lines that looks like this:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBxTCCAS4CAQAwgYQxHjAcBgNVBAMUFSoUZXpwcm9m94eS55b3VybGliLm9yZzEL
MAkGA1UEBhMCVVMxEDAOBgNVBAgTB0FyaXpvbmExGTAXBgNVBAoTEFVzZWZ1bCBV
-----END CERTIFICATE REQUEST-----
```

You will need to submit this text to your certificate authority.

While your certificate request is being processed, do not delete the certificate signing request. When you receive your certificate, it must be applied against the original request. This information will be saved on and accessible from the SSL management page.

9. Visit the web site of your certificate authority and follow their procedure for purchasing a certificate. When purchasing, if you are asked for your web server type, select Apache+ModSSL or just Apache as either is directly compatible with EZproxy.

When you are asked for your certificate signing request, you will need to copy and paste everything from the certificate signing request created in step 7, starting with the BEGIN CERTIFICATE REQUEST line through the END CERTIFICATE REQUEST line, including all the hyphens. If you have logged out of EZproxy, you can log back in and access your CSR details from SSL management page. From there click on the ID number for the appropriate CSR to view this information.

10. Depending on the policies of your certificate authority, it may take a few minutes or a few days to receive your certificate. The certificate will look similar to:

```
-----BEGIN CERTIFICATE-----
MIIF5jCCBU+gAwIBAgIDAJAYMA0GCSqGSIb3DQEBBQUAMIGjMQswCQYDVQQGEwJF
zESmBAGA1UECMBMJQxOT5BMRiwEAYDVQQHEwICQVJDRUxPTkExGTAxBgNV
-----END CERTIFICATE-----
```

In addition to the certificate for your server, the certificate authority may also provide intermediate or chained certificates. At this point, you should only be working with the certificate that has been issued for your server.

Once you receive your certificate, return to the SSL management page and click on your certificate signing request. Paste in all of the lines from BEGIN CERTIFICATE through END CERTIFICATE from the Certificate Signing Authority, including all the hyphens, into the certificate box, and click Save. EZproxy should accept the certificate. If it does not accept the certificate, ensure that you are copying the certificate for your server and not an intermediate certificate, then try pasting and saving again.
Two common mistakes that could prevent you from saving a certificate

<table>
<thead>
<tr>
<th>YOU WILL BE UNABLE TO SAVE A CERTIFICATE IF YOU:</th>
<th>WHY THIS IS A PROBLEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>• create a CSR</td>
<td>A certificate is bound to a key that is created as part of the original CSR and cannot be applied to any other CSR. If you make this mistake, you will need to resubmit the new CSR to your certificate authority and ask them to use it to replace your certificate.</td>
</tr>
<tr>
<td>• submit this original to your certificate authority</td>
<td></td>
</tr>
<tr>
<td>• delete the original request</td>
<td></td>
</tr>
<tr>
<td>• receive the certificate from your authority</td>
<td></td>
</tr>
<tr>
<td>• recreate the request</td>
<td></td>
</tr>
<tr>
<td>• try to apply the certificate from the original request to the recreated request</td>
<td></td>
</tr>
<tr>
<td>• get an error</td>
<td></td>
</tr>
<tr>
<td>• create a CSR</td>
<td>Again, certificates are bound to their original CSR, so this process will fail. If you have an existing certificate that was not requested using the EZproxy CSR request generator, click Import Existing SSL Certificate on the SSL management page to enter existing certificates.</td>
</tr>
<tr>
<td>• try to apply an existing certificate that was create outside of EZproxy to that newly created CSR</td>
<td></td>
</tr>
<tr>
<td>• get an error</td>
<td></td>
</tr>
</tbody>
</table>

11. If your certificate authority provides a intermediate certificate file or a chained certificate authority file, you need to enter this on the **CSR Details** page. Open up the **CSR Details** page from the SSL management page, and paste the intermediate certificate into the box toward the end of the page. You will only see this box once you have installed your certificate. Click **Save Certificate**. Changes to intermediate certificates take effect immediately, with no need to restart EZproxy.

12. On the Certificate Details page, find the line of text that states **To make this the active certificate for this server, type ACTIVE in this box --- then click activate**. Follow these instructions to activate your certificate.

13. Once the certificate is active, click **Administration** in the upper left corner of the screen to return to the main administration page.

14. On the EZproxy Administration page, click **Restart EZproxy**, and follow the instructions on **Restart EZproxy**.

15. You can confirm that the correct certificate is active by clicking on the SSL management page from the EZproxy Administration screen after EZproxy has restarted.

16. Add the following directive to your config.txt file to enable secure login:

   ```
   Option ForceHTTPSLogin
   ```

   This directive will redirect any requests for the login page to the secure, https URL for your EZproxy server. For more information about this directive see **Option ForceHTTPSLogin**.