Options for securing your EZproxy server

Last updated: Wed, 08 May 2019 19:33:54 GMT

EZproxy config.txt directives can be entered in many combinations to secure your EZproxy server. The most common security configurations employ encryption settings, limits, and monitoring/logging directives to record and limit users’ activity. The following tables provide lists of commonly used security, monitoring, and logging directives available to secure your server.

Login encryption

One step you can take to increase the security of your users’ credentials and limit the potential for illicit logins with legitimate credentials is to encrypt communication between your users and your EZproxy server. The following directives will allow you to create a secure login page using https and an SSL port. This means, for example, that whenever a user logs in to your EZproxy server, their username and password will be encrypted before transmission instead of being sent in clear text, making it more difficult for those credentials to be stolen.

Before using these directives, you must create an SSL certificate and apply it to your EZproxy server. For more details on how to do this, please see SSL Configuration.

<table>
<thead>
<tr>
<th>DIRECTIVE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LoginPortSSL</strong></td>
<td>this directive enables you to specify the port on which EZproxy should listen for incoming login, menu, and administration requests using https. This directive is necessary if you want to require your users to login using https as defined by the Option ForceHTTPSLogin directive.</td>
</tr>
<tr>
<td><strong>Option ForceHTTPSLogin</strong></td>
<td>When present, this directive will specify that the user login page always be presented using https, making it a more secure page for logins. Any attempts to access the page using http will be redirected to the https page.</td>
</tr>
<tr>
<td><strong>Option ForceHTTPSAdmin</strong></td>
<td>When present, this directive will specify that the admin login page always be presented using https, making it a more secure page for logins. Any attempts to access the admin page using http will be redirected to the https page.</td>
</tr>
</tbody>
</table>

Additional encryption options

Secure Socket Layer (SSL) is a cryptographic security protocol used to encrypt network information transmissions. SSL has generally been replaced with Transport Layer Security (TLS). EZproxy can support two SSL security options--SSL 2
and SSL 3; however, you can disable these weaker protocols so that only TLS is used. For more details about what version of TLS is currently supported, please see EZproxy release notes.

Note: In all supported EZproxy versions, SSL 3 is disabled by default.

When entered in your config.txt file, any Option DisableSSL directives that you enter must come before the LoginPortSSL directive.

<table>
<thead>
<tr>
<th>DIRECTIVE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option DisableSSL40bit</td>
<td>Disables the use of SSL encryption algorithms that use only 40-bits. This directive also disables SSL 2.</td>
</tr>
<tr>
<td>Option DisableSSLv2</td>
<td>Disables the use of SSL 2 handshakes.</td>
</tr>
<tr>
<td>SSLCipherSuite</td>
<td>This directive allows you to define security settings using SSL Cipher Suite strings.</td>
</tr>
</tbody>
</table>

For more details about each of these security options, please see Secure your EZproxy server.

### Additional limits configuration options

The following directives provide additional security for your EZproxy server, not related to encryption.

Note: Each of the directives below is defined in terms of security. For a more complete definition and discussion of how these directives work for both security and other purposes, please click on the name of the directive.

<table>
<thead>
<tr>
<th>DIRECTIVE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxLifetime</td>
<td>This directive closes sessions that remain inactive for longer than a given period of time. This can help minimize the likelihood that a valid session left open on a public computer be taken over by an illegitimate user.</td>
</tr>
<tr>
<td>MaxSessions</td>
<td>This directive limits the maximum number of EZproxy sessions that can exist at one time. This helps protect against denial of service attacks that could overwhelm your EZproxy server with traffic and shut it down. Setting a limit appropriate to your server will also help maintain your server’s health.</td>
</tr>
<tr>
<td>Option BlockCountryChange</td>
<td>Using the Location directive as a reference, this directive disconnects any user whose IP address changes from one country to another during a session.</td>
</tr>
<tr>
<td>UMask</td>
<td>This directive provides a numeric value that controls the</td>
</tr>
</tbody>
</table>
permissions on files created by the Linux version of EZproxy, using the same syntax and the Linux command umask.

Monitoring security

Once you have configured the above options, OCLC suggests you input the following options in your config.txt to monitor use of your EZproxy resources and help you deal with security breaches if they occur. Monitoring security and your security settings are directly related to log configuration. The list below provides a brief overview of log-related directives that can be useful in monitoring your EZproxy server’s security. For a more detailed discussion of EZproxy log options, please see Log Files Overview and the related directives pages linked there.

Note: Each of the directives below is defined in terms of security. For a more complete definition and discussion of how these directives work for both security and other purposes, please click on the name of the directive.

<table>
<thead>
<tr>
<th>DIRECTIVE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Most</td>
<td>This directive enables you to access use details from your admin page and identify potential problem users.</td>
</tr>
<tr>
<td>IntruderIPAttempts</td>
<td>This directive allows you to identify and automatically block users who repeatedly attempt to access your EZproxy server from a specific IP address with invalid credentials. A record of each failed attempt will be recorded in your Audit log if you have Audit Most configured.</td>
</tr>
<tr>
<td>IntruderUserAttempts</td>
<td>This directive allows you to identify and automatically block users who repeatedly attempt to access your EZproxy server with an invalid password for a given username. A record of each failed attempt will be recorded in your Audit log if you have Audit Most configured.</td>
</tr>
<tr>
<td>Location</td>
<td>When used in combination with Audit Most, this directive enables you to determine where your users are located based on their IP address. This can be useful information in identifying problem use and users.</td>
</tr>
<tr>
<td>Option StatusUser</td>
<td>This directive causes EZproxy to display the username associated with a login session on the Server Status page, accessible from the admin page. This makes it easier to determine if the same username is being used by many users to gain access to your server.</td>
</tr>
<tr>
<td>DIRECTIVE</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Option LogSession</strong></td>
<td>This directive causes EZproxy to record the session identifier as part of entries in the ezproxy.log or spu.log file when %u is entered as a qualifier with LogFormat or LogSPU. This allows you to cross-reference a user with a user’s browsing activity if needed. The link between user and session is stored in the audit file; this link is automatically broken after the number of days specified in AuditPurge, when the audit file is deleted.</td>
</tr>
<tr>
<td><strong>Option LogUser</strong></td>
<td>This directive causes EZproxy to record the username as part of entries in the ezproxy.log or spu.log file when %u is entered as a qualifier with LogFormat or LogSPU. This allows you to quickly identify the username used to initiate a problem-session and follow up with the appropriate steps necessary to limit that users’ access to resources. Note: Special configurations in LogFormat and LogSPU are necessary to record BOTH session ID and username. For more information see the Fields to Customize Log Data table on the LogFormat directive page.</td>
</tr>
<tr>
<td><strong>UsageLimit</strong></td>
<td>This directive provides multiple options for monitoring and then enforcing limits on usage. When entered as UsageLimit Global, this directive allows you to watch users’ activity and see how much data is being transferred to them, which can be helpful in identifying potentially problematic users. Adding additional options to the directive can allow you to enforce specific content transfer limits for specific periods of time.</td>
</tr>
</tbody>
</table>