Learn how to use the UsageLimit config.txt directive to set limits on EZproxy usage. **UsageLimits** allow you to set limits on EZproxy usage to comply with content provider requests, minimize the potential for the illicit download of large amounts of content, and limit reductions in access speed.

Content providers will sometimes place limits on the amount of content that users can download during a given time period due to licensing agreements they have with content owners. These limits can be enforced with the *UsageLimit* directive, which allows you to apply limits to individual resources without altering the amount of content your users can access from other resources.

You can also proactively impose usage limits to keep intruders from downloading large quantities of information with compromised credentials. If content providers detect unusually large quantity downloads, they may block your access to their resources, causing interruptions for your legitimate users. To avoid this, you can set appropriate limits on users’ ability to access all resources as a preventative measure. As described in the example tab, it is best to monitor usage before setting these limits so you do not inadvertently prevent legitimate users from having appropriate levels of access to resources.

Finally, if you put appropriate limits in place, high volume users who could potentially slow down access speeds for other users will be limited in how much they can download at one period of time, and thus free up bandwidth for other users to access resources.

**UsageLimit** is a position-dependent config.txt directive that interacts with database definitions. Any database following an open UsageLimit statement will be limited by the parameters set by this directive unless the directive is selectively applied. For more details about how to apply limits *globally* and *selectively*, see below.

**UsageLimit** is used to detect when a user is downloading an excessive amount of content and automatically suspend the user’s access. When a user's access is suspended and that user tries to access content through EZproxy, EZproxy sends the file suspend.htm, from the docs directory in the EZproxy installation directory, to the remote user. If you are going to enforce limits, you should create a suspend.htm file and provide information to tell users what to do if they have encountered this limit, particularly during early configuration when your limits may be too strict to meet the actual needs of your users.

A **UsageLimit** is evaluated based on the username used to log into EZproxy and applied across all user sessions.

The basic form for **UsageLimit** consists of the directive followed by parameters specifying the types of limits you are implementing, whether those limits will be enforced, and ending with a name you assign to that limit. A limit with all parameters would look as follows:

```
UsageLimit -enforce -expires=120 -interval=60 -local -MB=100 -transfers=100 All
```

Where you enter the specific numerical values for the limit options you would like to implement, and provide a unique name in place of "All" for the limit. The options each have a hyphen (-) in front of their names. You can include or omit
any option. The only required component of a UsageLimit is that you provide a name at the end of the statement.

Note: If you use CGI authentication, your CGI authentication must be configured to provide username information to EZproxy for UsageLimits to work properly.

**Global UsageLimit**

You can apply a global limit that will impact all databases by placing the directive statement at the beginning of your database configurations. The limits specified by this statement will apply to all databases that follow. The directive statement could look as follows:

```
UsageLimit -enforce -MB=100 Global
```

You can add as many limiting options as you want and enter any numerical value to define that limit. The name Global can be replaced with any name to identify this limit. For more details about how to construct a Global limit, see the Examples.

**Selective UsageLimit**

You can also apply limits so that they apply only to certain databases.

```
UsageLimit -enforce -expires=120 -interval=60 -transfers=100 Selective
Title Some Database
URL http://www.somedb.com
D somedb.com
UsageLimit -end Selective
```

Where you enter specific numerical values for the limit options. You can provide any name to designate the resources that will be controlled by this limit. For more details about how to construct a Selective limit, see the Example tab.
# Options

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-end</code></td>
<td>Specifies that this UsageLimit should not impact any of the databases that follow in config.txt. Use this only if you want the limit to apply to certain databases as this works as a bracket to enclose the databases controlled by the given limit.</td>
</tr>
<tr>
<td><code>-enforce</code></td>
<td>Specifies that any user account that exceeds set limit thresholds should be suspended. If this option is not specified, usage is monitored, but users who exceed the thresholds are not denied access. As a safety precaution, access for EZproxy administrators is never suspended.</td>
</tr>
<tr>
<td><code>-expires</code></td>
<td>Specifies that any suspension to a user's account should automatically clear after the given number of minutes specified have elapsed. If -expires is not specified, a suspended account remains suspended until the EZproxy administrator clears the suspension. See EZproxy Administration for information on how to access the EZproxy administration page.</td>
</tr>
<tr>
<td><code>-interval</code></td>
<td>Specifies the interval over which to consider the -MB or -transfers limits. If no -interval is specified, the default is 1440 minutes, which is one day.</td>
</tr>
<tr>
<td><code>-local</code></td>
<td>Specifies access limits to local EZproxy pages, including the menu page or pages served from the /public, /limited, or /loggedin directories.</td>
</tr>
<tr>
<td><code>-MB</code></td>
<td>Specifies limits to the number of megabytes of data transferred.</td>
</tr>
<tr>
<td><code>-transfers</code></td>
<td>Specifies limits to the number of page requests.</td>
</tr>
</tbody>
</table>

# Examples

The UsageLimit directive can be customized in a number of ways as necessary to monitor or enforce limits on your users' use of EZproxy.

**Monitoring use**

To start out, you can simply monitor EZproxy by adding:
UsageLimit Global

The choice of global for the usage limit name is arbitrary, and you can assign any name that will help you identify why you created this particular limit or which databases to control. As configured, this limit will monitor usage information over the past 1440 minutes (day). Accounts will not be suspended. Requests for information that come directly from EZproxy will not be included. All information gathered from this directive statement will be recorded in the messages.txt log.

Data transfer limit

If you decide to apply limits, for example a user should not transfer more than 100MB per day, you can start by using:

UsageLimit -MB=100 Global

This will only monitor use, not suspend access. If user exceeds this limit, a message like this will be recorded in messages.txt:

2005-08-01 09:00:00 Global 0.001MB usage limit exceeded by rdoe

Once you are ready to enforce a limit, you need to add the -enforce option, such as:

UsageLimit -enforce -MB=100 Global

With this statement in place, if a user exceeds the 100MB limit, that user will be unable to access EZproxy until you clear his/her suspension through the EZproxy administration page. If you want the suspension to expire automatically after 360 minutes (six hours), you could use:

UsageLimit -enforce -expires=360 -MB=100 Global

When you specify an expiration period, you can still manually clear the suspension at any time using the administration page.

Multiple usage limits

In a more complicated example, we will impose two separate limits, one arbitrarily named Global and the other arbitrarily named Selective. Global will impose a 100MB limit on all databases. Selective will impose a limit allowing only a total of 500 transfers total from Some Database and Another Database. Some Database and Another Database are not adjacent. The Global limit will require manual resetting, but the Selective limit will automatically reset after 180 minutes (three hours). For this, you could use:

UsageLimit -enforce -MB=100 Global

UsageLimit -enforce -expires=180 -transfers=500 Selective

Title Some Database
URL http://www.somedb.com/
D somedb.com
UsageLimit -end Selective
In this configuration, users who transfer more than 100MB of data from any combination of databases, or users who transfer more than 500 pages from a combination of Some Database and Another Database, will have their access suspended. The Selective limit will only apply to Some Database and Another Database, but not to Other Database, nor will it apply to additional databases that appear further down in config.txt.

If you want to apply a limit selectively to more than one database, you only need to enter the specific options for the usage limit the first time you enter it in config.txt. For all subsequent databases that you would like to limit with those parameters, you only need to add UsageLimit with the name of the limit to set a starting point for the limit and UsageLimit -end with the name of the limit to close the limit.

Advanced example

An example of how to combine all of the security features of EZproxy can be found in Secure your EZproxy server.

Related directives

Audit