ExcludeIP

Last updated: Mon, 21 May 2018 20:41:41 GMT

Learn how to use the ExcludeIP config.txt directive to identify computers that have IP addresses known by your database vendors in EZproxy.

**ExcludeIP** (also written as E) is a position-dependent config.txt directive that interacts with AutoLoginIP and IncludeIP directives; database definitions; and other ExcludeIP directives.

ExcludeIP is used to identify computers that have IP addresses that are known by your database vendors and thus do not need to be proxied. It accepts a single parameter that is either an IP address or an IP address range.

AutoLoginIP and ExcludeIP are normally used to modify EZproxy's behavior for computers you manage, with ExcludeIP as the recommended and more commonly used option. AutoLoginIP is used in instances where a computer or group of computers must be proxied to be able to access a database, but where you do not need to challenge the user to authenticate first. ExcludeIP is used in instances where a computer or group of computers do not need to be proxied and the user should be redirected to the real URL, without a challenge for user authentication and without the user being proxied.

**CIDR Notation**

ExcludeIP accepts IP address ranges in CIDR notation. For example:

```
ExcludeIP 192.168.0.0/16
```

**Examples**

**Example: local users bypass EZproxy**

In this example, all machines in the IP address range of 192.168.0.0-192.168.255.255 are known to the vendor and users from these machines should be redirected to the real database URLs, bypassing EZproxy.

```
ExcludeIP 192.168.0.0-192.168.255.255
```

<table>
<thead>
<tr>
<th>Title Some Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL <a href="http://www.somedb.com/">http://www.somedb.com/</a></td>
</tr>
<tr>
<td>Domain somedb.com</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title Other Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL <a href="http://www.otherdb.com/">http://www.otherdb.com/</a></td>
</tr>
<tr>
<td>Domain otherdb.com</td>
</tr>
</tbody>
</table>

**Example: everyone logs into e-reserves, local users bypass EZproxy for everything else**

This example demonstrates setting up a local server with e-reserves where you want all users, both local and remote, to be required to authenticate before they can access the e-reserves server, but all other databases will bypass EZproxy. The key to this behavior is placing the e-reserves database definition prior to the first ExcludeIP directive.
Title E-reserves
URL http://ereserves.yourlib.org/
HJ ereserves.yourlib.org
ExcludeIP 192.168.0.0-192.168.255.255

Title Some Database
URL http://www.somedb.com/
Domain somedb.com

To make this configuration truly effective, the resource must be configured not to allow local users access, or else users can simply manipulate the URL and take EZproxy out of the path. When making such a change, you may want to allow select machines direct access, such as staff machines, but insure that all other computers are blocked except for your EZproxy server.

Related directives

AutoLoginIP, ExcludeIPBanner, IncludeIP, Option RequireAuthenticate, RejectIP