


Restricting Access by IP Address

For increased protection, if your staff uses fixed IP addresses, you can restrict access to a specific set of IP addresses. This will help to prevent access by hackers and other malicious users.

 We recommend performing this task and other security measures immediately after installing WHMCS. For a full list, see [More Ways to Secure Your WHMCS Installation](#).


Restricting Access

To restrict access, create a `.htaccess` file in your WHMCS admin directory.

Add the correct content for your version of Apache to the new `.htaccess` file:

Apache 2.2


```
order deny,allow
allow from 12.34.5.67
allow from 98.76.54.32
deny from all
```

 Click to copy

Apache 2.4

```
Require ip 12.34.5.67
Require ip 98.76.54.32
```

 Click to copy

 You can specify as many different `allow from` or `Require ip` lines as you require. You can allow entire IP subnets by specifying just the first part of an IP address (for example, `12.34.`). This is `.htaccess` IP restriction.