Redirector IP bypass zones

Jump to: how to configure IP ranges

When using redirector links, you can optionally add redirector IP bypass zones which will allow you to bypass OpenAthens authentication at locations where the resources will allow access via IP authentication. This is very useful if you have to maintain separate links to resources in your library catalogue, portal or link resolver tool depending on when account holders are inside or outside of your network. Redirector bypass zones will work with any resource that has either an access URL (bypassable) or a redirector configuration (redirectable).

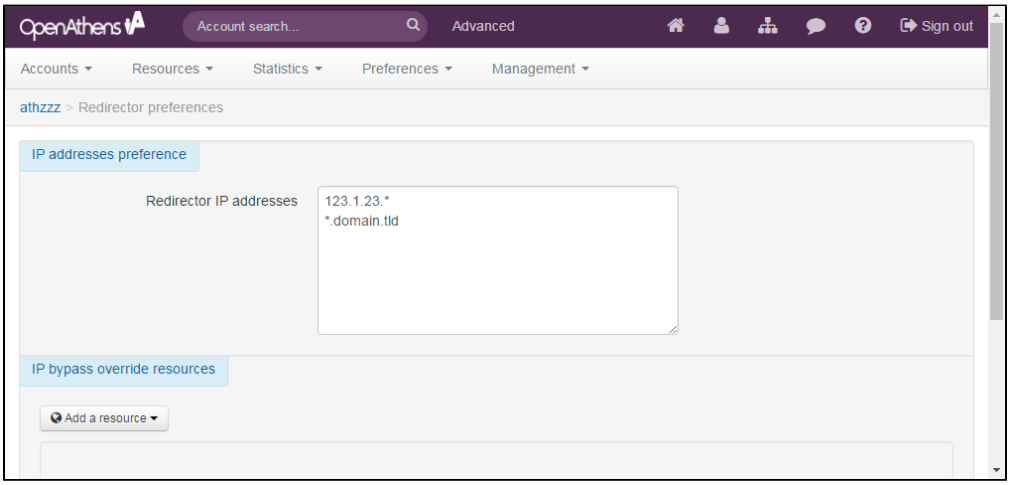
When a user follows a redirector link, the redirector will decide whether to pass the user straight to the service provider, or pass the user to the OpenAthens authentication point where the user would be challenged for username and password if they were not already signed in.

A high level version of the user journey would go something like this:

User follows Redirector link		
Location recognised		Location not recognised
Passed directly to resource for IP authentication		OpenAthens authentication Stats recorded
Access		

Configuring IP ranges

Menu: ***Preferences > Redirector***



Enter the IP addresses or ranges that are covered by IP authentication for your resources and save preferences.E.g:

```
123.3.23.12
123.3.23.*
123.3.22-23.*
```

Ranges may only be specified within the last two octets. If you have a range expressed with a slash it will need to be translated into an accepted format.

In most cases it will be sufficient to specify these ranges at the domain level, but additional ranges can be added per organisation to cater for local circumstances - for example where a local organisation has additional IP ranges, especially if they are connected with local resource subscriptions. You should ensure that local administrators are aware of the impact of mistakes though; see below.

At the domain level you also have the option to specify resources that should ignore this bypass zone and always use the OpenAthens access route, for example where IP authentication is not available on a particular resource. To set this up click the add resource button and start typing the name of the resource. Select the resource and then save. Only resources compatible with IP bypass will be listed.

Anything to watch out for?

Locations covered by Redirector IP addresses rely on a resource's IP authentication for access. You need to take care to match the ranges you specify with what your resources will IP authenticate.

- If you specify a range of addresses that is too big - i.e. includes addresses that are not IP authenticated by your resources - then users may find themselves in a location where they cannot gain access.
- If you specify a range of addresses that is too small - i.e. does not cover all the addresses that are IP authenticated by your resources - then users may find themselves asked for OpenAthens credentials when they do not expect to be.

Changes to bypass zones or resource exceptions do not apply immediately and it can take up to 14 hours for changes to go live.

When access does not go though the OpenAthens authentication point, we cannot record statistics.