

About restrictive mode

A question that often comes up is about restrictive mode - what is it for and do I need it on or off?

- [What is restrictive mode?](#)
- [Do I need it on or off?](#)
- [How to turn it on or off](#)

What is restrictive mode?

Restrictive mode was developed as a means of dealing with the occasional federated resource that, due to loopholes in some federations' rules, decided that the onus was on the Identity Provider (IdP) to only respond for users that should have access - what the SP was meant to do was make that decision themselves based on the attributes they were passed.

That's what restrictive mode was *built* for but it has other applications:

- Adding insurance against a publisher blaming you for their mistake if they let users in when they shouldn't
- Making the 'no access' message the same for all the resources you don't subscribe to - the user gets a consistent message from OpenAthens instead of whatever the publisher says.
- Removing resources you do not subscribe to from statistics - because of how federated access works, we cannot tell if the resource let the user in or not, so we count that the user was transferred to the resource

Do I need it on or off?

New customers

If you are a brand new customer then you should leave it off (the default) until you have got access to your subscriptions sorted out - this is to make it as easy as possible to get access to the resource set up without added restrictions. Once access to your resources is arranged you can set it on or leave it off as suits your preference.

The insurance angle

Off: you depend on publishers not letting your users in if you don't have a subscription

Advantages:

- You do not need to manage permission sets or their allocation beyond the default set for the role attribute

Disadvantages:

- None?

On: you can make sure it that it can't happen

Advantages:

- You have more control

Disadvantages:

- You need to manage resource allocation to permission sets (in each of your sub-organisations)
- You need to manage permission set allocation to accounts (in each of your sub-organisations)

The statistics angle

Off: you will be able to see which resources your users are trying to access alongside those that you subscribe to.

Advantages:

- You will be able to monitor and respond to how your users want to access content
- The resources you don't subscribe to can be counted as turnaways
- You do not need to manage permission sets or their allocation beyond the default set for the role attribute

Disadvantages:

- You may see 'stats' for resources that you do not subscribe to in your reports
- You need to manually filter these resources in statistics reports

On: you will not see statistics for resources that have not been allocated to permission sets

Advantages:

- You only see stats for the resources you have allocated

Disadvantages:

- You need to manage resource allocation to permission sets (in each of your sub-organisations)
 - You need to manage permission set allocation to accounts (in each of your sub-organisations)
-

The error message angle

Off: Users will get a 'no access' message from the resource

Advantages:

- You do not need to manage permission sets or their allocation beyond the default set for the role attribute

Disadvantages:

- Some error messages are better than others

On: Users will get a 'no access' message from OpenAthens

Advantages:

- Consistent error message for resources you have not allocated

Disadvantages:

- Only works for resources in the same federation(s) as you
 - You need to manage resource allocation to permission sets (in each of your sub-organisations)
 - You need to manage permission set allocation to accounts (in each of your sub-organisations)
-

How to turn it on or off

First make sure that all of your users have permission sets assigned and that those sets contain the relevant resources. Don't forget to include MyAthens. If you are using local accounts you'll want to do this a day or more before.

Restrictive mode is a per-organisation setting so is set on the organisation preferences page (**Preferences > Organisation**). The setting is at the bottom of the page. Once you save the page the change will take a few minutes to propagate to our authentication points. Repeat for any sub-organisations where you want it to apply.

The advantage of this being a per-organisation setting is that you do not need to have restrictive mode turned on (or off) for all the users across your domain - a mix is possible if that would suit you better.