# Setting up and Managing ACLs in oneye 0.8

So you're curious about the ACL facility in oneye, but are unsure about how to use it? Be unsure no longer! Read on.

In this guide, we're going to see how we can use ACLs to deny access to a program installed by default on all oneye systems - Public Board. We're going to create the ACL rule, and then target it at a specific user. After that, we'll look at editing it and retargeting it at a group. For the purposes of this guide, I've created a user called exampleUser, and assigned him to a group called exampleGroup.

**What are ACLs?**

ACLs, or to give them their full name, Access Control Lists, define user- or group-specific restrictions to system functions.

**Why use ACLs?**

If you wanted to prevent users from performing a certain task, you could use an ACL to do that. If you wanted to restrict use of a program, you could set an ACL. Yes, you could simply remove the program, but then nobody could use it. ACLs permit the restriction to be placed on specific users.

**Important**

Before we go any further, please make sure that your installation is up-to-date. At the time of writing, there have been several fixes to ACL functionality that the methods in this guide rely on. Go to http://lars-sh.de/2011/09/22/how-to-download-the-latest-oneye-svn/ for a guide to downloading and installing the latest svn revision.

## Creating an ACL rule

First, login as root. For the time being, ACLs can only be set by root.

Now you've logged in, let's have a look at the application we're going to block. Open it up and have a good look (figure 1). *Public Board* provides an IRC-style chat facility to your users.

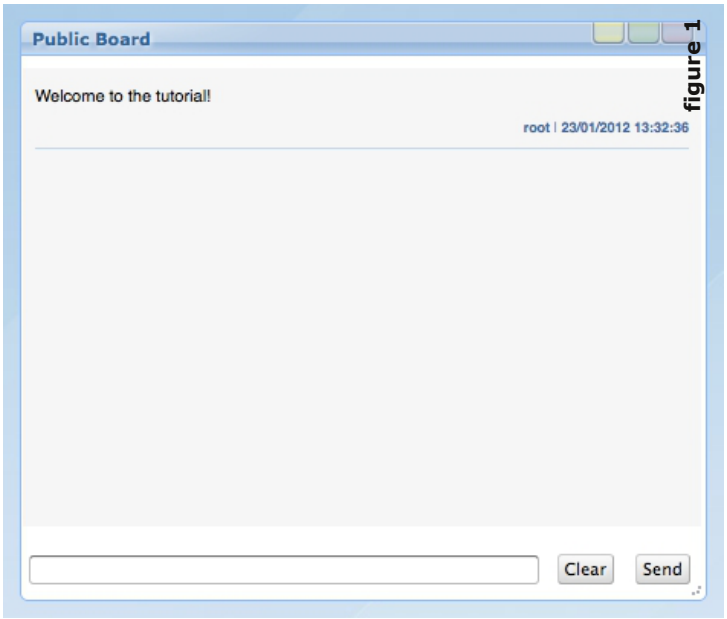

figure 1

Anyhow, you don't need *Public Board* running to set up ACL rules for it, so close it for now. What you do need is to know its package name. This is the real name of the app, rather than the user friendly label assigned to it in the UI. For *Public Board*, the package name is *eyeBoard*.

With this in mind, open *System Preferences*.

If we go to *Access Control* under the heading *Administration*, we can see a list of all the ACLs in the system (figure 2).

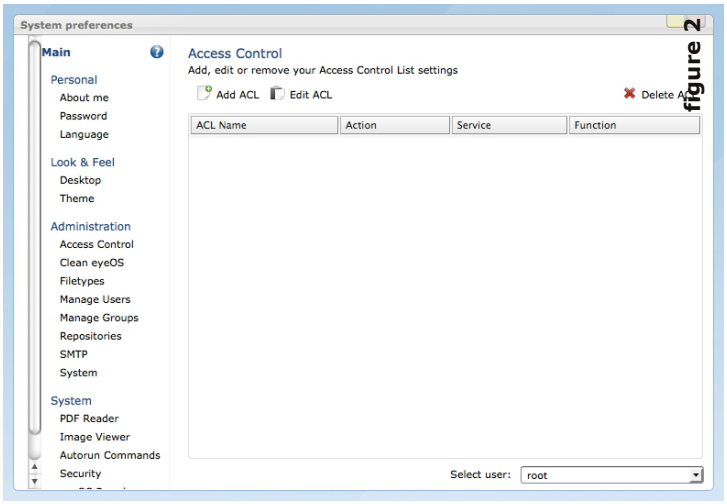

figure 2

To create a new ACL, select *Add ACL*. You'll be presented with four boxes that all need to be filled in (figure 3).

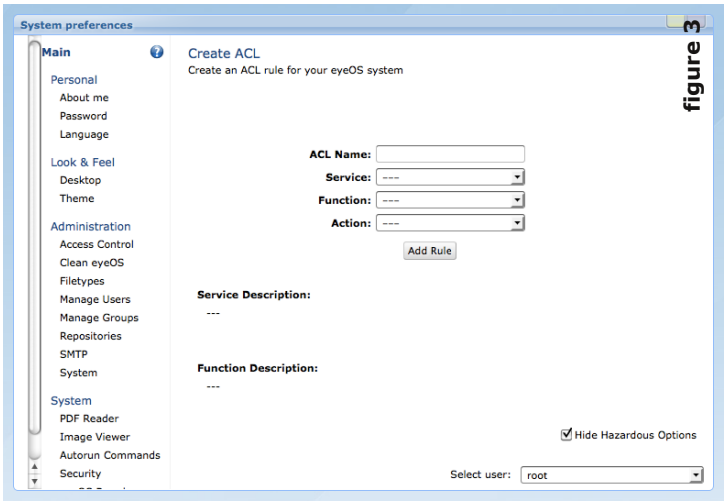


figure 3

In the first box, *ACL Name*, type a name for your ACL. This is the name that the system will use in the ACL list, so make sure it means something to you. I'm going to name my new ACL "Block Board".

The second box, *Service*, is a list of system services available in the system. If you select one, a brief description is provided for you to read. For now, select *proc*.

The third box, *Function*, automatically repopulates itself depending on what you select in Service, as the functions differ between services. Again, selecting an option from this box causes a brief description to appear. For now, select *launch*.

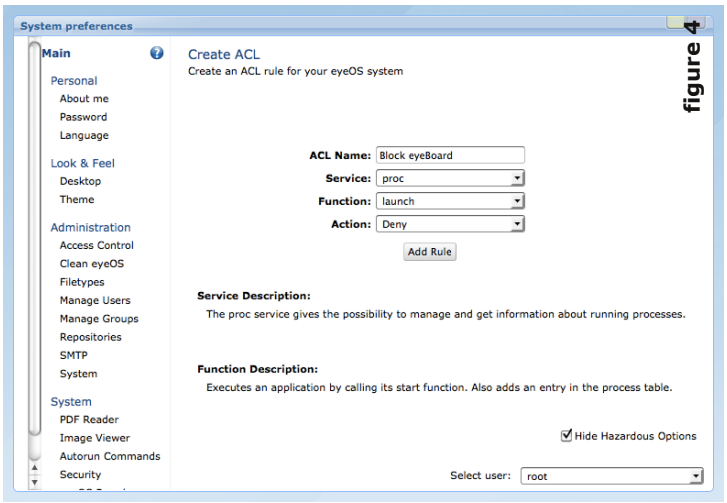


figure 4

The fourth box, *Action*, is a simple boolean choice: *Accept* or *Deny*. Essentially, do you want to permit or deny access to the function chosen in Function. For this example, we want *Deny* (figure 4).

Before moving on, I want to just mention the checkbox in the lower-right corner. Many of the functions selectable on this page are critical to the operation of oneye. If they are denied, it could cause some serious problems. To prevent this happening by accident, these particular functions are hidden by default. Unchecking this box causes them to reappear. **Please be very careful with this.**

Having filled in the boxes, select *Add Rule*.

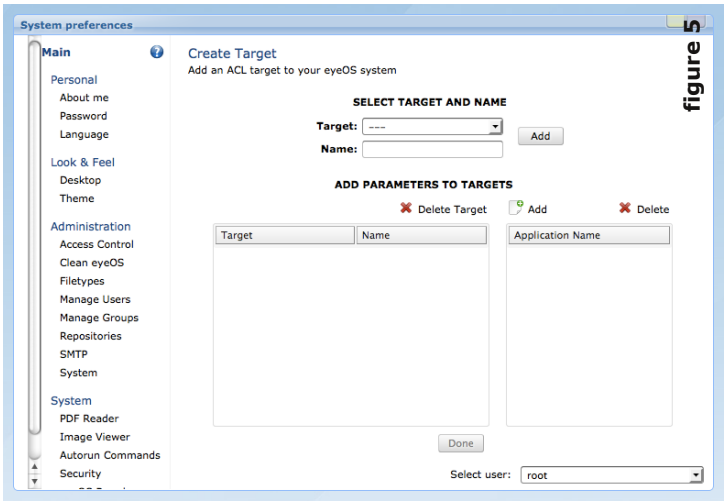


figure 5

## Targeting a user

The next screen (figure 5) presents more options and these can be a little obscure.

These options permit you to target the rule at someone, be it a user or a group. Without setting these, the rule is fairly useless.

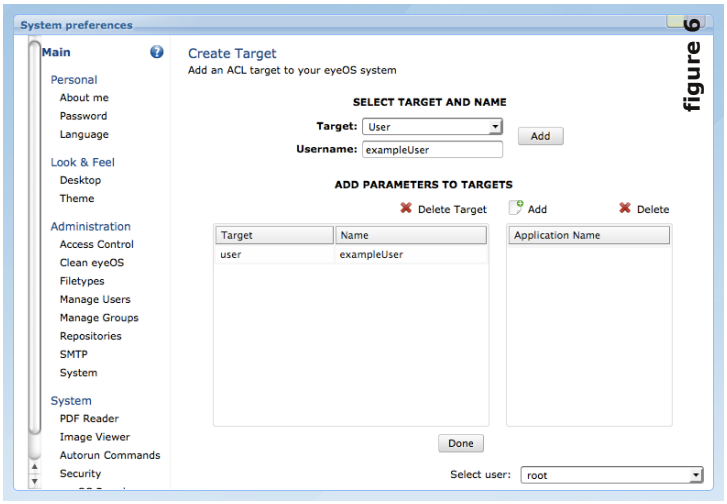


figure 6

The first option, *Target*, permits you to select between *User*, *Group*, and *Admin*. We want *User*.

You'll notice that as you chose an option, the label of the next box changes. Now, it says Username. So, write in the username of the user you wish to apply the rule to and press *Add* to the right of it. You'll notice that it is added to the left-hand table below (figure 6).

Now at the moment, this rule is setup up to deny the launch of **all** applications to the user "exampleUser". This also includes the applications required for core operation of oneye. Because of this, and the fact that we want to block "eyeBoard" specifically, we turn our attention to the right-hand table. As you might expect from the "Application Name" written at the top, this is a list of Applications to be blocked.

To create an entry, select the newly created entry in the left-hand table, then press *Add* immediately above the right-hand table. A dialog box will popup asking for a parameter. The 'parameter' is the package name of the application. So type in "eyeBoard" and press *Add* (figure 7).

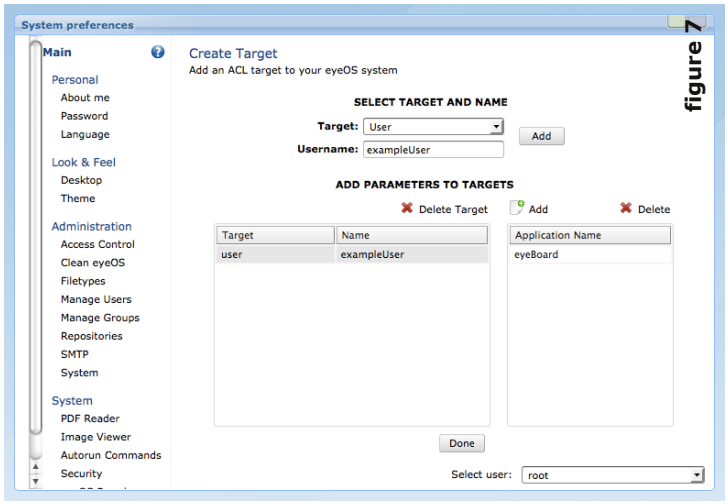

figure 7

With that, now press *Done*, and you'll return to the ACL list.

**Problem?**

A problem can arise here. If you login successfully, but you end up staring at the wallpaper without any docks or desktop icons, you may have forgotten to set any params for the target. I'm afraid you'll have to delete your session cookie and refresh the page manually. This will return you to the login screen. Login as root, and have a look at your ACL rule. Editing ACL rules is looked at next.

## Testing it

Let's test it! Close your session and return to the login screen. This time, login as the user you've just targeted.

Upon logging in, you'll find that everything should work normally. Unless you try to run *Public Board* at which point... nothing happens. Which is as it should be. After all, you've just denied access to it!

Feel free to login as any other user to make sure that no other user is denied access to Public Board, but for the purposes of this guide, we'll move on to editing the ACL rule.

**Program still runs**

If the program still runs, please, first make sure that you have set the rule correctly. If that still doesn't work, make sure that you are running an up-to-date system.

## Editing an ACL rule

So, what happens if we want to edit an ACL rule?

Let's log back in as root and return to our ACL rule list.

Selecting the ACL rule we want to edit and pressing *Edit ACL* takes us to a screen that permits us to edit it (figure 8).

From here we can use *ACL Name* to rename the rule or *Action* to change whether the rule Accepts or Denies the Function. We don't need to do either of these things, so we shall instead choose to select the

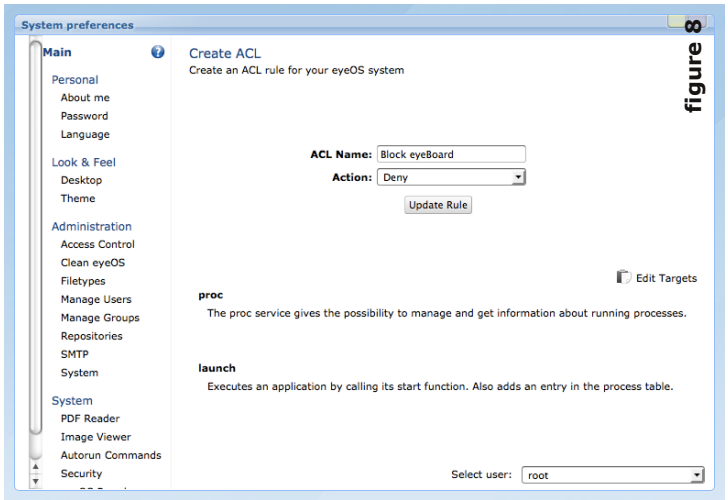

figure 8

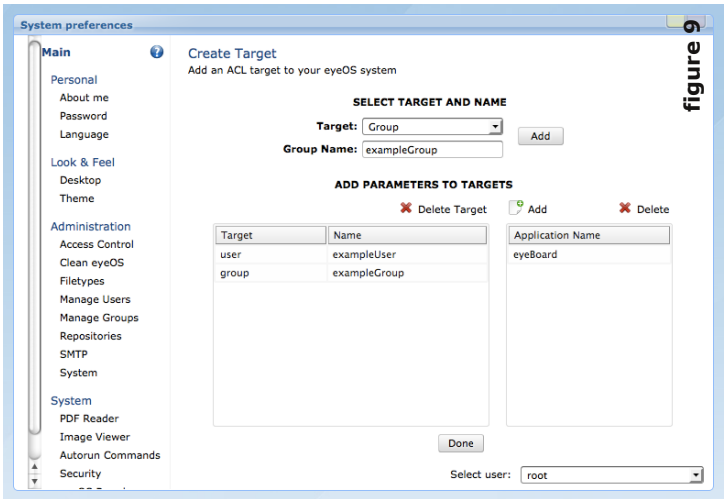


figure 9

option above the table entitled *Edit Target*.

## Targeting a Group

This takes us to screen that looks somwehat familiar. This time round, we go to *Target* and select *Group*. The box below automatically relabels itself to "Group Name". We write in "exampleGroup" and press *Add* (figure 9).

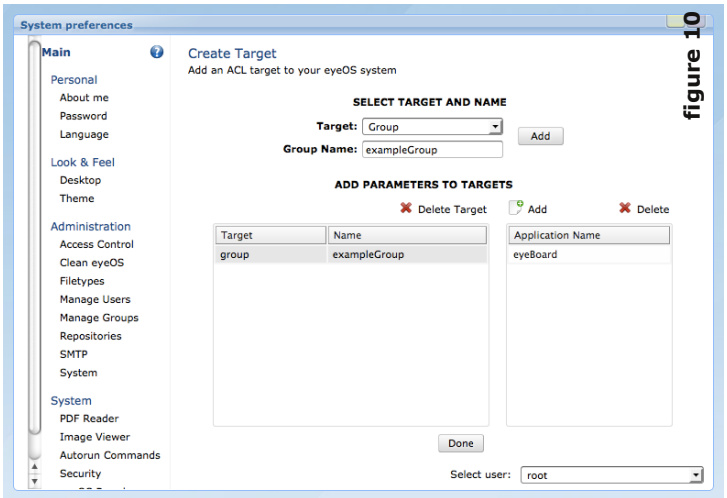


figure 10

Two things are important to note here. The first is that we still have the original target "exampleUser", so we select it and select the nearest *Delete* button. The second thing to notice is that when you select our newly created target, it has no parameters set under "Application Name".

The reason for this is so you can use the same function on different users and groups but specifying different parameters for each target. (For example I could use this very rule to prevent another user from launching *eyeNav* whilst preventing exampleUser from launching *eyeBoard*, - exampleUser can still run *eyeNav* and the other user can still run *eyeBoard*).

With that in mind, we select our new target, choose *Add* and write "eyeBoard" into the dialog provided.

After double-checking that everything is as we wish it (figure 10), we hit *Done*, and so return to the main ACL table.

## Testing it

Time to test our new rule! Logging out of root and back in as any user in the group "exampleGroup", we can launch any apps – except *Public Board* – as expected.

**A note about Root**

Don't worry if root happens to be a member of any group targeted by an ACL - root is immune to them. This also means that attempting to specifically target root as a user will also fail. This is how it should be and will never change.

**How do I find the package name?**

The simplest (but not the quickest) way is, with the app closed, open Process Manager and go to the Processes tab. Start the app you're interested in and note the value of Process Name of the line that's just been added to Process Manager (it's typically the bottom most one, just below eyeProcess).

**Important**

Please be very, very careful with ACLs. Many of the functions capable of being blocked are critical to the smooth operation of oneye. If you block any of these for a user, it means that oneye is unable to use that function - even in the background - during that user's session. This will not only disrupt the functionality of oneye, it may also drive your user-base away.