### **Trac Permissions**

Error: Macro TracGuideToc(None) failed

```
'NoneType' object has no attribute 'find'
```

Trac uses a simple permission system to control what users can and can't access.

Permission privileges are managed using the <u>trac-admin</u> tool.

Non-authenticated users accessing the system are assigned the name "anonymous". Assign permissions to the "anonymous" user to set privileges for anonymous/guest users. The parts of Trac that a user does not have the privileges for will not be displayed in the navigation.

In addition to these privileges, users can be granted additional individual rights in effect when authenticated and logged into the system. All logged in users belong to the virtual group "authenticated", which inherits permissions from "anonymous".

# **Available Privileges**

To enable all privileges for a user, use the TRAC\_ADMIN permission. Having TRAC\_ADMIN is like being root on a \*NIX system, it will allow you perform any operation.

Otherwise, individual privileges can be assigned to users for the various different functional areas of Trac (note that the privilege names are case-sensitive):

### **Repository Browser**

BROWSER\_VIEW View directory listings in the repository browser

LOG VIEW View revision logs of files and directories in the repository browser

FILE\_VIEW View files in the <u>repository browser</u>

CHANGESET VIEW View repository check-ins

### **Ticket System**

TICKET\_VIEW View existing <u>tickets</u> and perform <u>ticket queries</u>

TICKET\_CREATE Create new tickets

TICKET\_APPEND Add comments or attachments to tickets

TICKET\_CHGPROP Modify ticket properties (priority, assignment, keywords, etc.) except description field

TICKET\_MODIFY

Includes both TICKET\_APPEND and TICKET\_CHGPROP, and in addition allows

resolving tickets

TICKET\_ADMIN All TICKET\_\* permissions, plus the deletion of ticket attachments and modification of the

description field

### Roadmap

MILESTONE\_VIEW View a milestone
MILESTONE\_CREATE Create a new milestone

MILESTONE\_MODIFY Modify existing milestones

MILESTONE\_DELETE Delete milestones

Trac Permissions 1

MILESTONE\_ADMIN All MILESTONE\_\* permissions
ROADMAP\_VIEW View the roadmap page

### Reports

REPORT\_VIEW View reports

REPORT\_SQL\_VIEW View the underlying SQL query of a report

REPORT\_CREATE Create new reports

REPORT\_MODIFY Modify existing reports

REPORT\_DELETE Delete reports

REPORT\_ADMIN All REPORT\_\* permissions

#### Wiki System

WIKI\_VIEW View existing wiki pages

WIKI\_CREATE Create new wiki pages

WIKI\_MODIFY Change wiki pages

WIKI\_DELETE Delete wiki pages and attachments

WIKI\_ADMIN All WIKI\_\* permissions, plus the management of readonly pages.

#### **Others**

TIMELINE\_VIEW View the timeline page

SEARCH\_VIEW View and execute search queries

CONFIG\_VIEW Enables additional pages on About Trac that show the current configuration or the list of installed plugins

# **Granting Privileges**

You grant privileges to users using <u>trac-admin</u>. The current set of privileges can be listed with the following command:

```
$ trac-admin /path/to/projenv permission list
```

This command will allow the user bob to delete reports:

```
$ trac-admin /path/to/projenv permission add bob REPORT_DELETE
```

The permission add command also accepts multiple privilege names:

```
\ trac-admin /path/to/projenv permission add bob REPORT_DELETE WIKI_CREATE
```

# **Permission Groups**

Permissions can be grouped together to form roles such as developer, admin, etc.

```
$ trac-admin /path/to/projenv permission add developer WIKI_ADMIN
$ trac-admin /path/to/projenv permission add developer REPORT_ADMIN
$ trac-admin /path/to/projenv permission add developer TICKET_MODIFY
$ trac-admin /path/to/projenv permission add bob developer
$ trac-admin /path/to/projenv permission add john developer
```

Group membership can be checked by doing a permission list with no further arguments; the resulting

Roadmap 2

output will include group memberships. Use lowercase for group names, as uppercase is reserved for permissions.

# **Removing Permissions**

Permissions can be removed using the 'remove' command. For example:

This command will prevent the user *bob* from deleting reports:

```
$ trac-admin /path/to/projenv permission remove bob REPORT_DELETE
```

Just like permission add, this command accepts multiple privilege names.

You can also remove all privileges for a specific user:

```
$ trac-admin /path/to/projenv permission remove bob *
```

Or one privilege for all users:

```
$ trac-admin /path/to/projenv permission remove * REPORT_ADMIN
```

### **Default Permissions**

Granting privileges to the special user *anonymous* can be used to control what an anonymous user can do before they have logged in.

In the same way, privileges granted to the special user *authenticated* will apply to any authenticated (logged in) user.

See also: <u>TracAdmin</u>, <u>TracGuide</u> and <u>?FineGrainedPermissions</u>

Permission Groups 3