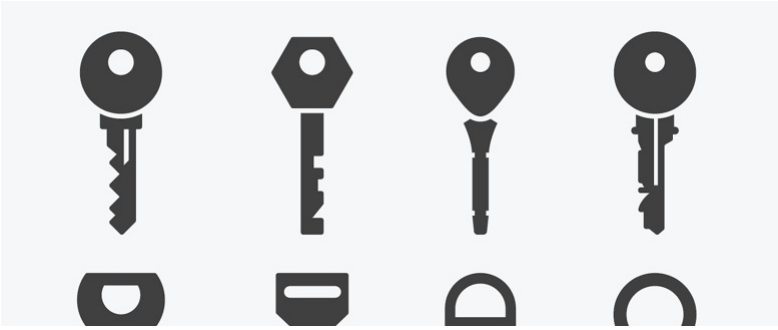
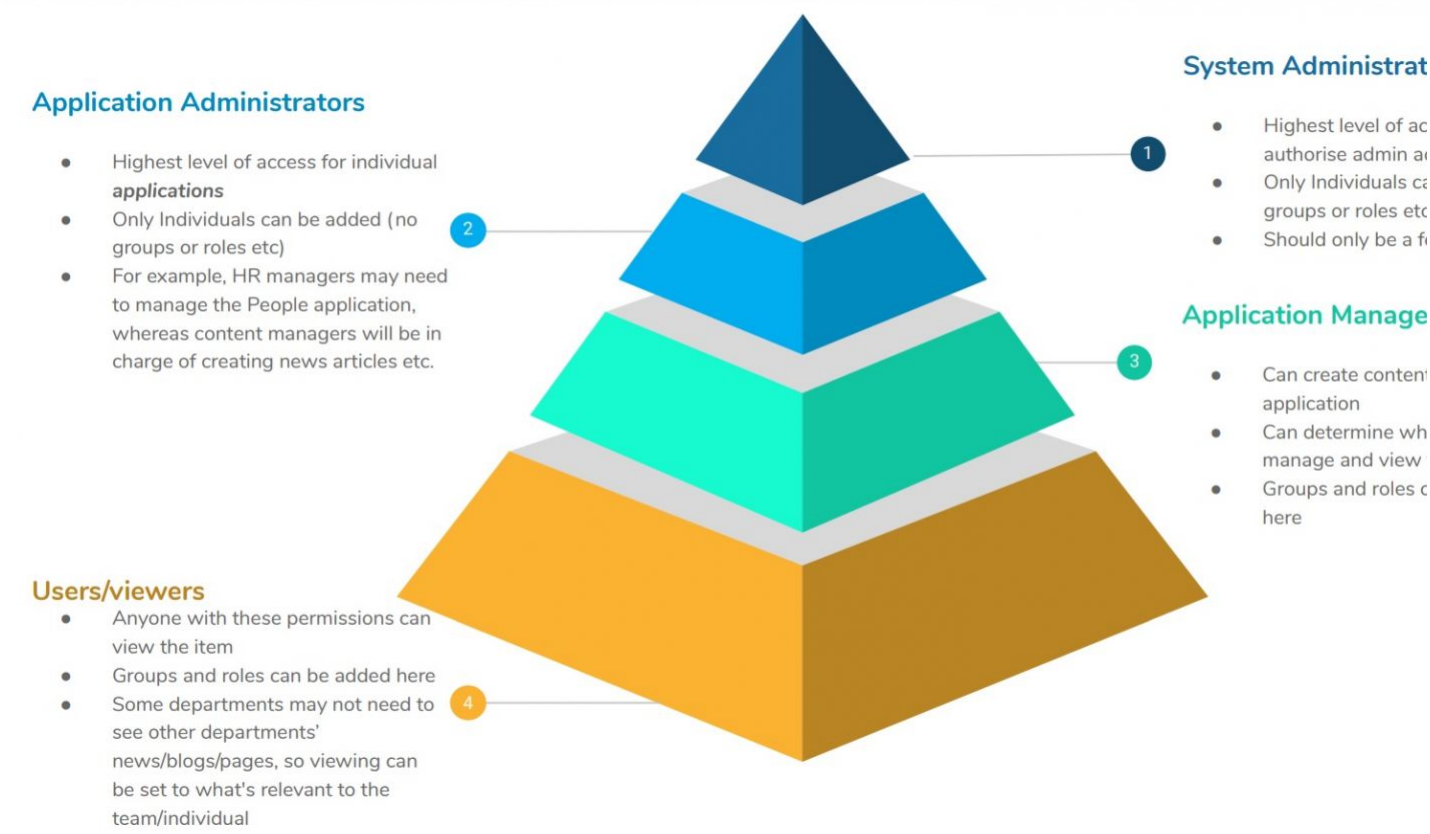
Link to article: https://discover.claromentis.com/knowledgebase/articles/707/assigning-permissions-and-management



Assigning permissions and Management

Click on the below image to see it enlarged in a new window:

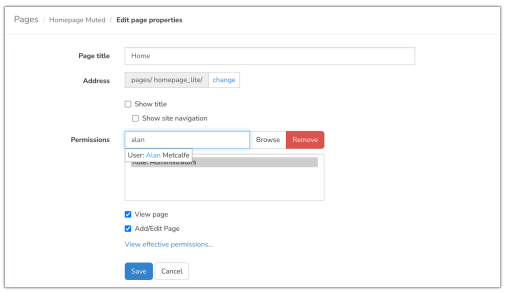


Assigning permissions to users as an administrator

Permission dialogues will appear in each application and may look a little different across them, but the fundamental function is the same.

In each, the system asks who can access this content and what additional actions (if applicable) can they perform.

This is how different access is created across the site and between users.



Start typing a user's name to see them appear and click on to add them to the box.

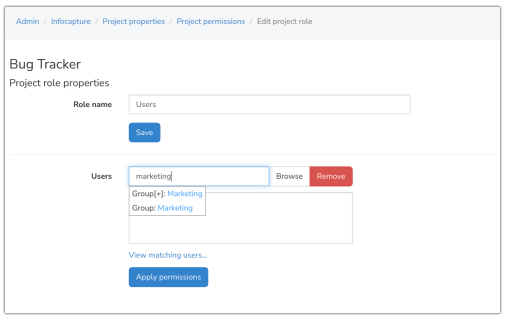
Check the boxes against any additional rights you wish them to have.

Once saved that user can now perform the actions you have determined.

Use Roles and Groups where possible and not individual users

The system will also offer Roles and Groups in permissions, which will have been created by People administrators on your site.

Enter these in permissions boxes to give all its members the same rights in one fell swoop.



It is best practice to add new users to as many Roles and/or Groups as possible to diversify the access you can give them.

Do not enter specific user names where possible and instead use a Role or Group, this means when a new user joins you can simply add them to the Roles/Groups in People so they instantly gain the desired access across applications where they have been entered into permissions.

Entering user names into permissions dialogues only means over time and for any new account every user's access has to be updated individually which is laborious and not the best way to use the system.

In some cases specific user names are required only, however for the majority of the site Roles/Groups should be used instead.

Management

Once you begin using your site, over time permissions dialogues across applications will become filled out with the appropriate users/roles/groups.

Maintaining these over time falls to system and application administrators as they have the access to ensure that users entered are relevant and appropriate for the content.

Due to the nature of the Intranet, there is no way to carry out a permissions audit or report to see which user/role/group is entered across all applications.

There is a report for documents specifically to check user permissions across your structure.

For all other applications, this is a manual process instead, with their permissions dialogues checked to ensure the correct user/role/group entries have been made or for changes to be carried out.

If all administrators are working together to cover all applications and perform regular access checks, this task can be maintained comprehensively as well and any changes to the entries easily be orchestrated.

Created on 6 April 2020 by Hannah Door. Last modified on 30 November 2023
Tags: admin, permissions, users, pyramid, group, role, assign