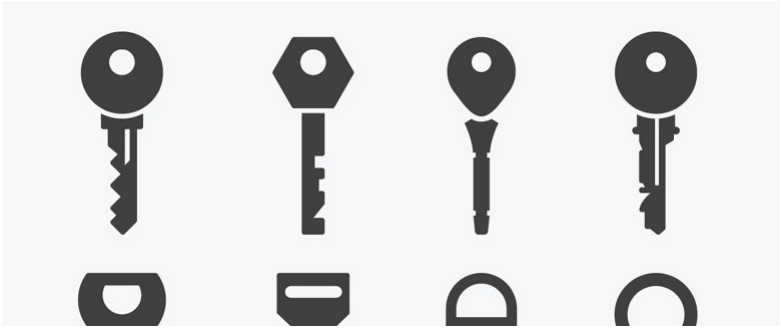
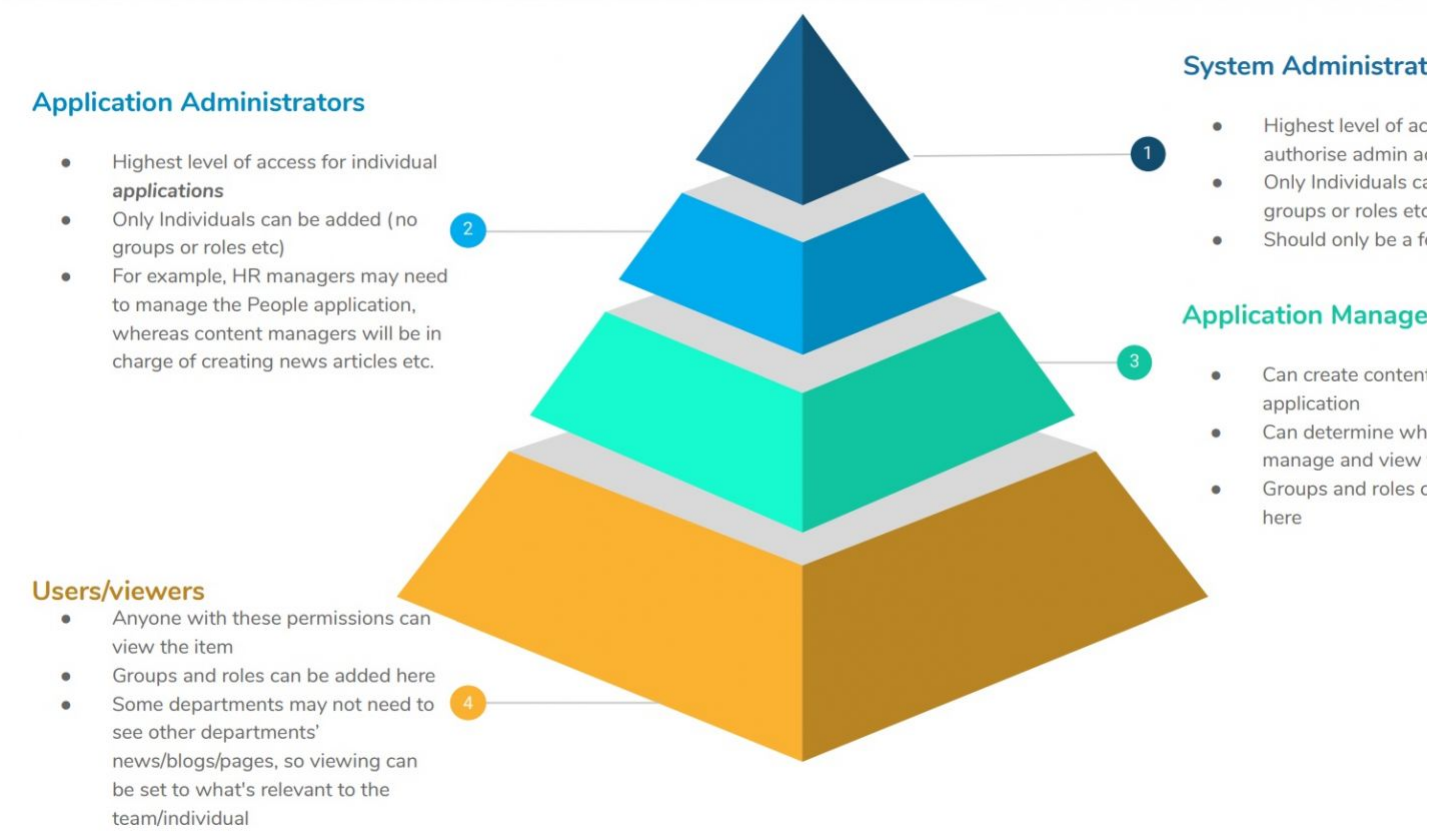
Link to article: https://discover.claromentis.com/knowledgebase/articles/707/assigning-permissions-ongoing-management



Assigning permissions & ongoing management

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

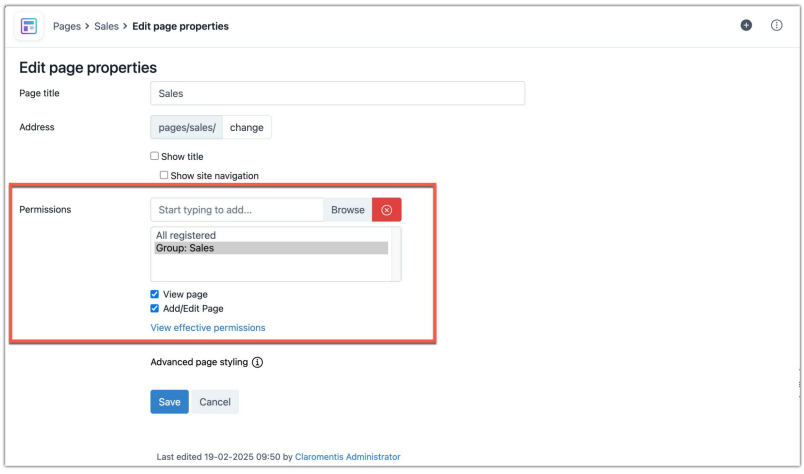


Assigning permissions as an administrator

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

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

This is how Intranet administrators build different access levels across the site and between users.



Start typing a user/role/group and select them from the drop-down.

Check the boxes against any additional abilities you wish this user or members, or that role/group to have.

Once saved, those users can now perform the actions you have determined.

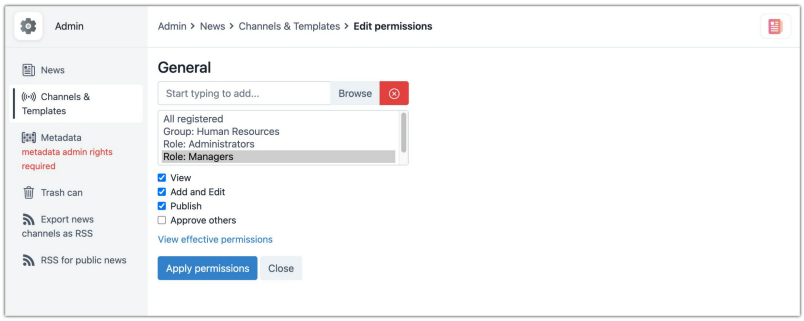
Always use Roles & Groups where possible and not individual users

Roles and Groups are created by People administrators (Groups can be created by a user sync if this is in use)

It is best practice to add users to as many Roles and/or Groups as possible to simplify and diversify their access.

Use Roles & groups in all permissions boxes to encapsulate the users within them and give permission in one fell swoop.

This means easier management over time, as when a new user joins your company, the administrator can simply add them to all relevant Roles/Groups, and they will instantly get the access where those have been entered in permissions boxes across the site.



Deleting a Role or a group

Only application administrators of People can delete Roles or Groups from Admin > People

Deleting a Role or Group will remove it from any/all permissions boxes that it was placed in.

If this is done without consideration of the other users/roles/groups left in permissions boxes in applications, access issues can occur.

Vigilance should be exercised around deleting roles and groups for this reason and avoided until a review has been carried out to ensure no access loss.

Ongoing management

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

Maintaining the permissions entered, the Roles & groups that exist and user membership in them falls to system and application administrators.

They should work in collaboration with People administrators (if they do not have these rights themselves) and your IT team if a user sync is in use to ensure the necessary adjustments can be applied.

Due to the nature of the Intranet, there is no way to carry out a permissions audit to see which user/role/group is entered where and with which permissions.

There is a report for documents specifically to check user permissions across the structure, but for all other applications, a review of who can access what is a manual process.

If all administrators work together to review all applications and perform regular access checks, this task can be maintained comprehensively, and any changes to the entries can be easily orchestrated.

Created on 7 January 2026 by Hannah Door. Last modified on 30 June 2026
Tags: admin, permissions, users, pyramid, group, role, assign