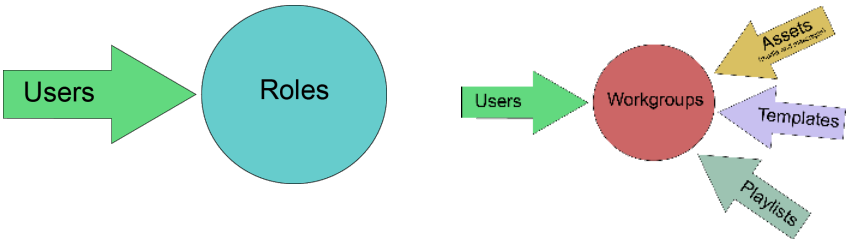
Workgroups

About Workgroups

Workgroups are a collection of users, assets (media and messages), templates, and playlists that rely on a permission structure for sharing and utilization. The basic relationships between roles, users, workgroups, and content is:

- Users are assigned to roles and workgroups separately.
- Roles are assigned to users.
- Roles determine users' permissions to perform functions in Content Manager.
- Assests, templates, and playlists are assigned to users.
- Workgroups are assigned to users.
- Workgroups determine users' privileges to content.
- Workgroup roles determine permissions to assets, templates, and playlists. Depending upon configured permissions, users may have add, edit, delete, and/or view privileges.

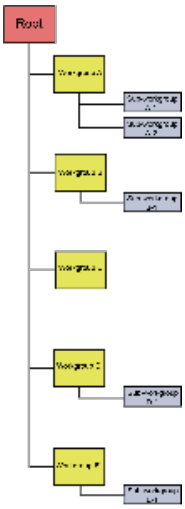
Users can have any combination of permissions to add, delete, edit, and view content. Content can be shared between workgroups or maintained for use by a single workgroup. The following diagram demonstrates the relationship between roles, users, assets, templates, playlists, and workgroups.



Workgroup Structure

In Content Manager, workgroups have hierarchical dependencies. This means that workgroups can have sub-workgroups associated with them. Permissions to assets, templates, and playlists are controlled using this structure. All workgroups are sub-workgroup of the "Root" workgroup. This workgroup has access to add, edit, delete, and view every asset, playlist, and template in COntent Manager. Association with this workgroup is typically reserved for administrators without workgroups and super administrators. The Workgroup Hierarchy diagram below demonstrates workgroup structure.

Workgroup Hierarchy

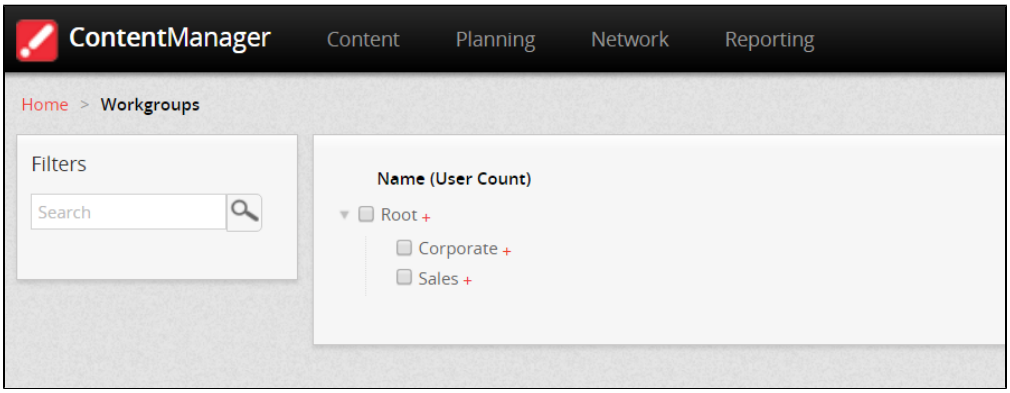


For an example of how workgroup view privileges work, see the chart in Sharing Content Between Workgroups.

Workgroup Structure in Content Manager

> **Note**
>
> Before creating and administering workgroups, think about the structure of your content and the needs of your business. Understanding how your content is structured and how users access it is key to figuring out how to best create and associate workgroups with users and content.

In Content Manager, workgroups are part of a hierarchical structure in which there is a root followed by nested workgroups. Workgroups can be nested as many levels down as needed to support your business needs.



Workgroups and Status

Content in workgroups is also identified by its state. It can be in one of three state, or a combination of owned and shared:

State	Description
Owned	Content that belongs to a particular workgroup. Depending on the user's role, this content can be viewed, edited, or deleted.
Shared	Content that is owned by one workgroup, but available to another workgroup. Users with whom the content is shared have view privileges.

No Workgroup	Content that is accessible to all users. Depending on role permissions, this content can have edit, view, or delete privileges.

For information about how workgroups, content items, and user privileges operate with view permissions see the User View Privileges table in the Workgroups and Users section.

Workgroups and Users

Administrators or super administrators define permissions. The needs of your business determine the best way to define your permissions structure. In many organizations, users have multiple roles in the Scala suite of products.

There are five basic types of user permissions in Content Manager:

User Type	Availability of Content
Super Administrator	• Has access to all assets, templates, and playlists within Content Manager. • Can delete, add, view, and edit all assets, templates, and playlists.
Administrator *without* a user workgroup	• Has access to all assets within Content Manager. • Can delete, add, view, and edit all assets, templates, and playlists.
Administrator *with* a user workgroup	• Can only see the assets in assigned workgroup and without an owner workgroup. • Can delete, add, view, and edit all assets, templates, playlists in assigned workgroup and without an owner workgroup. • Can view assets, templates, and playlists from other workgroup, if shared.
Non-administrative user *without* a user workgroup	• Can only see assets, playlists, and templates without an owner workgroup. • Depending on role permissions, may or may not have delete, add, and edit privileges. • Can view assets, templates, and playlists from other workgroup, if shared.
Non-administrative user *with* a user workgroup	• Can only see assets, playlists, and templates in assigned workgroup and assets, templates, and playlists without an owner workgroup. • Depending on role permissions, may or may not have delete, add, and edit privileges in assigned workgroup. • Can view assets, templates, and playlists from other workgroup, if shared.

Because of the way roles and permissions are created in Content Manager, there can be variants of each of these user roles.

Owner Workgroups versus Shared With Workgroups

An *owner workgroup* is the workgroup of the user who uploaded an asset, template, or playlist. If the owner workgroup is a parent workgroup, ownership can also be assigned to any, or all, of the children.

Shared with workgroups are the workgroups which have permission to view and utilize the content in playlists.

The following list describes what a user can do with each workgroup permission:

- **Add** - upload additional data to the workgroup.

- **Edit** - make changes to the asset, template, or playlist.
- **Delete** - remove the asset, template, or playlist.
- **View** - see the asset, template, or playlist and use.

Assets

The following table demonstrates the relationships between assets, owner workgroups, and shared workgroups.

Asset				
Workgroup Permission	**Add**	**Edit**	**Delete**	**View**
Owner Workgroup	✓	✓	✓	✓
Shared with Workgroup	✗	✗	✗	✓

Templates

The following table demonstrates the relationships between templates, owner workgroups, and shared workgroups.

Templates				
Workgroup Permission	**Add**	**Edit**	**Delete**	**View**
Owner Workgroup	✓	✓	✓	✓
Shared with Workgroup	✗	✗	✗	✓

Playlists

The following table demonstrates the relationships between playlists, owner workgroups, and shared workgroups. Users in shared workgroups can use the playlist, but cannot make any changes to it.

Playlists				
Workgroup Permission	**Add**	**Edit**	**Delete**	**View**
Owner Workgroup	✓	✓	✓	✓
Shared with Workgroup	✗	✗	✗	✓

Managing Workgroups

Create workgroups, users, and roles directly in Content Manager or using Lightweight Directory Access Protocol (LDAP). For more information about using LDAP to manage workgroups, users, and roles, see LDAP and Active Directory: Managing Authentication and Authorization.

> **Note**
>
> If using Active Directory/LDAP to manage roles and users, any changes to users, roles, and workgroups must be performed in LDAP, not in Content Manager.

Sharing Content Between Workgroups

Users are added to workgroups and have access to the content in associated workgroups. When assets, playlists, or templates are shared, those with whom the content is shared have view only privileges, regardless of their role. This means that users with whom content is shared can view and use assets, templates and playlists, but cannot edit or delete them.

Examples

- Users in workgroup A can see all of the content associated with workgroup A and sub-workgroups A-1 and A-2. Sub-workgroup A-1 can only see the content associated with A-1. Sub-workgroup A-2 can only see the content associated with A-2.
- Users in workgroup B cannot see any content from workgroup A, unless it is shared with them. Users in workgroup B can see all of the content in workgroup B.
- If content is associated with the root level, all users can see it.
- If content is not associated with a workgroup, all users can see it.

The following chart depicts how user view privileges function in Content Manager when content is owned, global, and/or shared:

			User View Privileges													
Media Item	Owned by Workgroup	Shared with Workgroup(s)	User in Workgroup A	User in Workgroup A-1	User in Workgroup A-2	User in Workgroup B	User in Workgroup B-1	User in Workgroup C	User in Workgroup D	User in Workgroup D-1	User in Workgroup E	User in Workgroup E-1	User with No Workgroup	Admin in Workgroup A	Admin with No Workgroup	Super Admin
m01	A	Not shared	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓
m02	A	B	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓
m03	A	C	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓
m04	A	B,C	✓	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓
m05	B	Not shared	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
m06	B	A	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓
m07	B	Not shared	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
m08	B	A,C	✓	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓
m09	C	E-1	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✗	✗	✓	✓
m10	C	A	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓
m11	C	B	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓
m12	C	Not shared	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓
m13	No owner	Not shared	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
m14	D	Not shared	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓
m15	E	Not shared	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✓
m16	E	B	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗	✓	✓
m17	A-1	Not shared	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓
m18	A-1	B-1	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓
m19	A-2	Not shared	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓
m20	B-1	A	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓
m21	E-1	A-2	✓	✗	✓	✗	✗	✗	✗	✗	✓	✓	✗	✓	✓	✓

User View Privileges Demonstrated

The User View Privileges chart (above) and the Workgroup Hierarchy diagram (above) will help visually explain the following examples.

1. Media item 02 (m02) is owned by workgroup A and shared with workgroup B. This means that:
    a. Only workgroup A can edit or delete it.
    b. Workgroup B has view privileges,which means they can see and use m02, but edit or delete it.
    c. Sub-workgroups A-1, A-2, and B-1 cannot view m02 because workgroup rules require that they are granted permissions by the owner workgroup A to view.
    d. The administrator to workgroup A can view the content because they are part of the workgroup and have administrative access. Additionally, they can edit or delete the m02.
    e. The administrator without a workgroup has access to view, edit, or delete m02 because s/he is an administrator and not bound to a workgroup.
    f. The super administrator is able to add, view, edit, and delete m02 because of the role permissions associated with a super administrator.
2. Media item 13 (m13) is neither owned nor shared by a workgroup. Based on workgroup rules, this means that:
    a. All users can view the media item.
3. Media item 21 (m21) is owned by workgroup E-1 and shared with workgroup A-2. Based on workgroup rules, this means that:
    a. Parent workgroup E can view m21 because it is the parent to E-1.
    b. Workgroup A-2 can view the item because the item is shared with them.
    c. Workgroup A can view the media item because it is the parent to A-1.
    d. The administrator for workgroup A can view it because s/he is an administrator for the workgroup and is a part of workgroup A.

e. The administrator with no workgroup can view, edit, or delete m21 because s/he is an administrator and is not associated with a workgroup.
f. The super administrator can view, edit, or delete m21 because of his/her role permissions.