

Restricted Delivery

One of the aspects of central asset governance is to restrict access to assets. Restriction of assets is established by having the DAM Admin/Brand Manager, set the “roles” on assets which are approved. This is done on the authoring side, on AEMaaCS author instance.

The end-users who would be searching or consuming delivered asset binary, will be able to access restricted assets, upon passing the Authorization.

Restricted Delivery via IMS

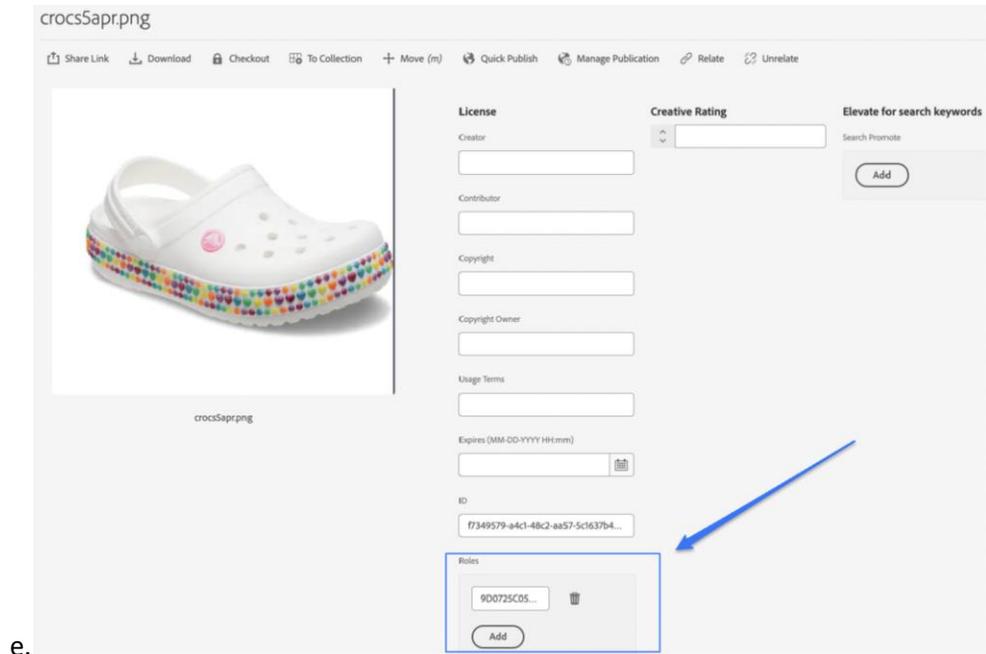
Steps:

- Authoring:

Restricting assets’ delivery is done by setting roles on the assets. The roles are set in AEMaaCS instance.

The instructions to do the same are as following:

1. DAM Admin should go to (Touch UI)
2. Make sure "Roles" field exists in Advanced Metadata of Asset, else add following field in metadata schema((Touch UI) Tools → Assets → Metadata Schemas → edit):
 - a. Add a Multi Value Text Field : Field Label → "Roles", Map to property → ".jcr:content/metadata/dam:roles"
3. Fetch IMS groups to be added in Asset's **Roles** Metadata:
 - b. Login to <https://adminconsole.adobe.com/> → <Go to your respective organisation> → User Groups
 - c. Select User Group you intend to add and extract orgID and userGroupID from URL, OR use
 - d. <Your respective Org Id>@AdobeOrg:<your respective user group ID>(i.e OrgID:userGroupID)
4. Add Group ID in Asset's **Roles** Metadata:



e.

- Delivery:

Delivery of restricted assets, require a valid IMS token. The instructions are as following:

5. Get access token (as described in the [help document](#)):
 - f. login to your AEMaaCS environment's Dev Console, for e.g. <https://dev-console-ns-team-aem-cm-stg-n25271.ethos14-stage-va7.dev.adobe.com/#release-cm-p47604-e144858>
 - g. Switch to Environment → Integrations → Local Token → Get Local Development Token → copy accessToken value
 - h. Please refer to the linked help document, to understand the lifetime of access token, and related aspects.
6. Pass the access token acquired in previous step in the "Authorization" header. Ensure its value is prefixed with "Bearer ". (This is Bearer Authentication)
7. it should return 404 without IMS access token or with access token which does not have same principals/groups as added in asset's metadata