# Viewing security audit report

The Resource application allows you to generate a security audit report in a spreadsheet format.

The report shows all users with access or who are assigned to a selected resource, when the access was granted, who granted the access, and the scope of user assignment, whether the access covers the entire resource (global scope) or only the package level (resource-specific scope). The report provides visibility for  management should they want to review resource access or remove it from some users.

| | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| 1 | Resource: | **Magic Library** | | | | | |
| 2 | | | | | | | |
| 3 | Assigned users by roles | | | | | | |
| 4 | | | | | | | |
| 5 | | | | | | | |
| 6 | | Role: **Administer Projects[Custom]** | | | | | |
| 7 | | **Name** | **Type** | **Date Access Granted** | **Granted by** | **Scope** | |
| 8 | | **c1 [Administer Projects]** | User | 31/08/2017 11:18 AM | Administrator | Global | |
| 9 | | **group1** | User Group | 16/11/2017 01:47 PM | book | Global | |
| 10 | | | | | | | |
| 11 | | Role: **Edit Project Properties[Custom]** | | | | | |
| 12 | | **Name** | **Type** | **Date Access Granted** | **Granted by** | **Scope** | |
| 13 | | **c2 [Edit Project Properties]** | User | 31/08/2017 11:18 AM | Administrator | Global | |
| 14 | | **group1** | User Group | 16/11/2017 01:47 PM | book | Global | |
| 15 | | | | | | | |
| 16 | | Role: **Edit Projects[Custom]** | | | | | |
| 17 | | **Name** | **Type** | **Date Access Granted** | **Granted by** | **Scope** | |
| 18 | | **c3 [Edit Projects]** | User | 31/08/2017 11:19 AM | Administrator | Global | |
| 19 | | **group1** | User Group | 16/11/2017 01:47 PM | book | Global | |
| 20 | | | | | | | |
| 21 | | Role: **Manage Model Permissions[Custom]** | | | | | |
| 22 | | **Name** | **Type** | **Date Access Granted** | **Granted by** | **Scope** | |
| 23 | | **c4 [Manage Model Permissions]** | User | 31/08/2017 11:19 AM | Administrator | Global | |
| 24 | | **group1** | User Group | 16/11/2017 01:47 PM | book | Global | |
| 25 | | | | | | | |
| 26 | | Role: **Manage Owned Project Access Right[Custom]** | | | | | |
| 27 | | **Name** | **Type** | **Date Access Granted** | **Granted by** | **Scope** | |
| 28 | | **c5 [Manage Owned Project Access Right]** | User | 31/08/2017 11:19 AM | Administrator | Global | |
| 29 | | **group1** | User Group | 16/11/2017 01:47 PM | book | Global | |
| 30 | | | | | | | |
| 31 | | Role: **Project Contributor** | | | | | |
| 32 | | **Name** | **Type** | **Date Access Granted** | **Granted by** | **Scope** | |
| 33 | | **group1** | User Group | 16/11/2017 01:47 PM | book | Global | |
| 34 | | **p1 [Project Contributor]** | User | 31/08/2017 11:15 AM | Administrator | Global | |
| 35 | | | | | | | |

An example of a security audit report containing all assigned users (grouped by role) who have access to a particular resource.

Only a **Security Manager** or a user with **Manage User** permission will be able to view the report.

**Note**

- The role assignment grant log capability is available in MagicDraw 18.5. Earlier versions do not provide information about the users who granted a role to other users in the project.
- When you migrate Teamwork Cloud to 18.5 or 19.0, a user with a username (i.e., "Migration_18.4To18.5") will be printed in the **Granted by** column. It is considered the grantor of the access at the time you migrated TWCloud.

To generate a security audit report

---

- Go to the **Resource** application, select a resource and click ⋮.

- From the list select to **View security audit report.** A security audit report for the selected resource will be generated and downloaded to your local machine.