



Free Training Transcript:
Permissions

Welcome to this Permissions video. To follow along, you'll need administrator access to Tableau Online or Tableau Server. There are four main components of Tableau Server and Tableau Online security: authentication, authorization, data security, and network security. This video focuses on the second piece, authorization.

Permissions & Site Roles

Authorization determines who can see content and how they can interact with it. In Tableau, authorization is determined by a combination of Permissions and Site Roles. Permissions are things like the capability to save to a project, web edit a workbook, connect to a data source, etc. They apply to a specific piece of content (project, data source, workbook, or view) for a given group or user. The capabilities of a permission are not given to a group or user in a vacuum, it's always in the context of the content.

Site roles, on the other hand, are assigned to a given user and are the foundational level of authorization. I've named all my users by their site role, so we can see the interaction of permissions and site roles. Site roles are established at the time a user is created, but can be updated later.

Site roles determine the maximum level of permissions a user can have. A user with a site role of Viewer will never be able to web edit even if that capability is explicitly granted to them. However, site roles do not inherently grant any permissions in and of themselves. The exception is Administrator site roles—administrators always have all permissions.

For more information about the specific site roles and the limits each puts on possible permissions, refer to the related resources under this video.

Groups and Users

When it comes to permissions, a common practice is to put users into groups and only assign content permissions to those groups. By adding users who should have the same access to the same content to a group, permissions can be managed in bulk. "All Users" is a default group that every user is automatically added to.

Let's add a new group. Click New Group. This group will be for Marketing Managers—it will contain users who should all have the same permissions on the same content. Once the group is created, click into it and click Add Users. Now we can pick who should be in the group. I'll add Interactor, Publisher, and Viewer.

Projects & Project Permissions

Clicking back on to the content tab, we can see the types of content in the toolbar at the top. Just as groups allow for bulk management of user permissions, projects act as folders, holding workbooks, views, and data sources, simplifying organization and permissions management for that content. Click on the Default project, then click permissions. (Remember, permissions are assigned from the content itself.) Project permissions come in two types—the capabilities for the project itself, and permissions for the content inside them. When a new project is created, it inherits all permissions from the Default project. As such, the default project can be thought of as a permissions template for all projects.

Assigning Permissions

Let's set permissions on the Default project. What are we looking at, here? If we expand the Project area, we see the capabilities for the project itself: view, save, or be a project leader. View allows a user see that a project exists. Save allows a user to save content to that project, essentially allowing publishing to that project. Project leader is a more complicated capability. If a user has the project leader capability, some things they can do include: access all content in the project, edit the default permissions for workbooks and data sources in the project, and lock or unlock permissions to the project.

Before we start, notice that the All Users group is already present. In order to minimize confusion, it's often easiest to completely clear all capabilities for the All Users group. This lets us start from a blank slate where no users can do anything with this content. Then, we can add in the explicit group rules we want and have clear control over exactly what's happening.

Click the ellipses next to All Users and select Edit. In the drop downs, change the template to None. These options roughly align with the site roles, but here we're talking about sets of permission capabilities that often go together. We can customize once we've picked a basic template, or, in this case, clear everything with one click by picking None. When None is selected, we need to click "Delete" to apply that change.

Now we have our clean slate. Down at the bottom of the screen, we can see the resulting permissions grid. This can be useful because it shows the combined permissions for all users in the group. Note that when All Users have no permissions, user with admin site roles still have full permissions.

Adding a Group Rule

Ok, let's add permissions for our Marketing Managers. Click "add a user or group rule" and select the Marketing Managers group. We'll change the project template to Viewer and click save. The resulting permissions grid only shows the users in the group we've selected up top—to see everything, click All Users, but we're ok with just these.

What if we want to change the template? Click the ellipses next to Marketing Manager again, and select Edit. If we pick the Project Leader template, only that capability is allowed. Click save. What the heck happened below? Well, the Project Leader capability automatically comes with the View and Save capabilities, so those are added, too. Except for the Viewer site role—even though the group rule explicitly allows them the project leader capability, their site role of viewer limits the maximum permissions available, and they're denied Project Leader. If we hover over a box, we get a tool tip explaining how the resulting permissions were computed.

Editing Permissions

Let's modify the permissions for workbooks in this project. Expand out the workbook area, and we're met with a host of new, workbook-specific capabilities. These options are the same as if we navigated to a particular workbook and clicked Permissions. Hovering over each icon tells us what it is.

To change the permissions, click the ellipses next to the group we want to edit, and click Edit. If we click through the templates, each set of capabilities being added in. Let's leave it on interact. Then in the Edit area, click to allow downloading a workbook. And click twice to toggle the ability to delete from allowed to denied. The template has changed to custom because we've modified it. Click save.

What happened in the resulting permissions grid? The interactor and publisher site roles have the whole suit of editing capabilities—even deleting. Hovering shows us this is because they're project leaders. The viewer site role user, though, only has the view capabilities—they're not a project leader, and they cannot be granted interact capabilities because of their site role. But let's turn off the project leader capability. Click the ellipses. Click edit. Change the project template to viewer. Now the interactor and publisher capabilities are what we expected.

If we hover over the grey box for delete box for interactor, we see that they're denied by group rule. Contrast this to the grey box for move, where they're denied because

the capability is not allowed by any rule. Tableau permissions are restrictive—that is, a capability must be explicitly granted or it will be denied. Additionally, individual permissions trump group level permissions. This means that if an individual is specifically denied a right, but is also a member of a group that is allowed the same right, the individual deny will win out. For more information on how permissions are evaluated, check out the online help.

Web Edit and Save/Save As

Finally, it's worth noting that certain actions require a specific combination of site role and permission. For a user to be able to web edit, they must: be at least an Interactor or Publisher Site Role and have the web edit capability allowed on that workbook. However, to be able to save their changes as a new workbook they must: be at least a publisher site role, and have the save capability for the project—as well as the capability to: download/save as for the workbook (if they should be able to overwrite the original workbook with their changes, they ALSO need the save capability on the workbook). As a note, an interactor can be given the capability to download/save as, but it only lets them download the workbook. Save-as during web-edit is only possible for users with a publisher site role (or admin).

Locking Permissions to the Project

If we're happy with our permissions and don't want to add in the complexity of different workbooks and data sources in the project having different permissions, we can lock the permissions to the project. On the right side of the screen, this button either says "Managed by the owner" or "Locked to the project" depending on which configuration is currently applied. Only administrators and project leaders can toggle this setting. Click on the button and select Locked to the project. The permissions we're setting here will now apply to all content published to this project. The publisher (owner) will retain all access to their own content, but they won't be able to override these permission settings.

Conclusion

Permissions and site roles together offer robust authorization in Tableau Online and Tableau Server. For more in-depth coverage of the nuances of authorization, refer to the resources below this video. Thank you for watching this permissions training video. We invite you to continue with the Free Training videos to learn more about using Tableau.