Understanding user access, roles, and best practices for collaborative project management

Overview

In EXFO Exchange, the structural hierarchy is made up of **organizations** and **workspaces**. While both are essential to managing users and test data, understanding their differences is key to avoiding access issues, improving efficiency, and managing large projects across teams or contractors.
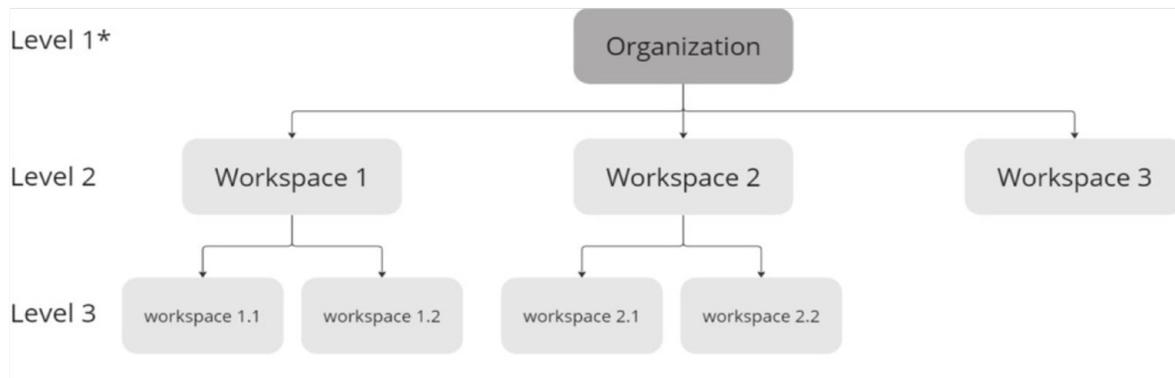

Figure 1. How Organization and Workspace levels are structured

Key concepts

Organization

An **organization** in EXFO Exchange represents a company, a division or a business unit, regardless of size. It is the top-level structure that controls access, administrative rights, and configuration-level actions, but does not store jobs or results. The latter is done at the workspace level.

Key characteristics:

• Represents the company or main business entity.

• Enables the editing of key parameters (e.g., test configurations and result properties).

• Grants control over permissions (e.g., user management and workspace deletion).

• Requires **Org Admin** access for critical actions.

• Must be shared explicitly with users who need full access.

Best practice

Invite managers and key users to the **organization level**, not just the workspace. This ensures that they can access essential tools, such as test configuration import.

Workspace

A **workspace** is a substructure under an organization. It is typically used to organize work by region, contractor, build partner, project or team.

Key characteristics:

- Used to manage jobs and test results.
- Level at which most technicians are invited.
- Where most field activity happens.
- Inherits visibility from the parent organization or workspace, if user is invited at a higher level in the hierarchy.

Best practice

Avoid inviting users to multiple workspaces if they already have access via the parent workspace or organization. It creates redundancy and confusion. Also, workspaces can be mistakenly duplicated if users are unaware of inherited visibility.

A user can have access to multiple organizations and/or multiple workspaces under different or the same organizations.

Real-world scenarios to learn from

Scenario 1: Missing permissions

A QA manager had access to a workspace but couldn't import test configurations. The issue? They weren't invited to the organization level, where configuration rights are managed.

Scenario 2: Access attribution inefficiencies

A contractor created multiple workspaces and invited users to each workspace individually, not realizing access to the parent workspace or organization automatically grants access to all sub-workspaces.

Scenario 3: Deletion issues

A director tried to delete a workspace but was unable to. Reason: they were not granted organization-level permissions. Workspace-level access isn't enough to manage or delete substructures.

Org admin-only permissions

Only users invited as **Org Admins** can:

- Import or manage test configurations.
- Manage user roles across all workspaces.
- Delete workspaces.
- Create and manage result properties.

Summary

Understanding the distinction between organizations and workspaces is essential for:

- Preventing permission issues.
- Simplifying user management.
- Proper organization configuration and management.
- Clear data visibility.

When in doubt, ensure that key personnel have organization-level access, not just workspace-level visibility.

Advice: Always invite managers, analysts and configuration leads to the organization.