Changes to Authorization

Contents:

This section covers changes between release on the following topics:

- Authorization to the platform
  - User roles
  - Permissions of roles
- User management

Release 7.1

Release 7.1 introduces **role-based access controls (RBAC)**, in which access to Trifacta resources are managed at finer-grained levels. This release introduces the basic RBAC framework and the following key changes.

> **NOTE:** Over the next few releases, additional capabilities will be added to the basic RBAC framework, enabling administrators to provide better and more closely defined access to objects. Check back to this section with each upgrade.

Workspace admin is a super user

Beginning in Release 7.1, the workspace admin is a super-user of the product.

> **NOTE:** In this release, the workspace admin user has owner access to user-created objects, such as flows and connections, within the workspace.

A **workspace** is a set of users and their objects, such as flows and connections. For more information, see *Workspace Admin Permissions*.

All upgraded Trifacta admins are now workspace admins

> **NOTE:** If you are upgrading Trifacta Self-Managed Enterprise Edition, any Trifacta admin users are now workspace admin users. A single workspace is supported in your instance of Trifacta Self-Managed Enterprise Edition. Additional workspaces are not supported.

> **NOTE:** In Trifacta Self-Managed Enterprise Edition, any user who is granted the admin role is also granted the workspace admin role, which enables owner-level access to user-created objects in the workspace.

Admin can edit any global connection

After an administrator has made a connection global (available to all users):

- Any administrator can edit the connection.
- All users can use the connection (existing functionality)
- The connection cannot be made private again (existing functionality). Connection must be deleted and recreated.

Menu items unavailable due to account roles

Beginning in this release, menu items may not be displayed to specific users because of their current role assignments.

> **NOTE:** This behavior had existed in previous releases. In this release and future releases, workspace admins may receive inquiries about menu option availability. A user's assigned roles could be a likely source for why a menu option is not available to the user.

Logging

Logs from the authorization service may provide insight into access problems. These logs are available for download through the support bundle. For more information, see *Support Bundle Contents*.

Authorization changes to APIs

Some API endpoints now include information that is specific to the changes in this release for authorization. See *Changes to the APIs*.