Data Access Control

Overview

Data access controls what users can see in Zuora, such as a U.S regional sales person viewing only customer accounts in the U.S. This article introduces key features and explains how to implement data access control.

What is Data Access Control?

Data Access Control gives customers the ability to customize and control what areas their users can access within Zuora.

Data Access Control allows you do the following:

• Restrict what products and accounts your users can see within Zuora.
• Configure multiple business units under a single tenant.

Access to this feature requires a specific edition of Zuora. See Zuora Editions for details. Get in touch with our sales team through zuora.com for specific terms and pricing.
You must have Zuora Platform Administrator permission to manage Data Access Control. See Zuora Platform Roles for more information.

**Data Access Control Versus Permissions**

Data access controls differ from permissions in the following:

- Data Access Control is what users can see within Zuora. For example, U.S. users should only be allowed to see U.S accounts.
- Permissions are what users can do within Zuora. For example, having the ability to create a bill run.

**Hierarchy**

A hierarchy is a set of tags created by your Zuora administrator to enforce access rights on a Zuora object. Both hierarchies and tags are organized in a tree structure.

Currently, the following applies to a hierarchy:

- Each tenant can only have one hierarchy
- Each hierarchy has a maximum of one hundred tags
- Each hierarchy has a maximum of ten levels

**Tags**

A tag is a value within a hierarchy that is assigned to users and objects. Tags are organized in a tree structure. The following are examples of tag values:

- Roles
- Product lines
- Business units
- Regions
- Verticals

**How Tags are Applied to Objects**

When you tag an object, you are tagging an account or product. For example, if you apply a "West Coast" tag on an account, all subscriptions under that account will inherit the same tag. Take into account that transaction objects, such as subscriptions, invoices, payments, and refunds are restricted because they inherit tag of the account, but not the product.

See Zuora API Object Basics for more information on objects.
How Tags are Applied to Users

When you apply tags to users:

- Each user can only be assigned one tag
- Users can view objects within their role and below them
- Users will not be able to view objects above or across them within the hierarchy
- Users can also be reassigned tags

Unrestricted Access

Unrestricted access are objects that can be viewed by any user. Regardless of where a user resides in the tag hierarchy, unrestricted objects can be accessed by all users. Any user can change an object to or from Unrestricted.

Complete Data Access Control

Complete data access control is the top level of the Data Access Control hierarchy. Users tagged at this root level have access to all objects within Zuora. Users that have not been tagged, will automatically be tagged at the root level.

Call Zuora APIs with Data Access Control Enabled

To allow users to make API calls with data access control enabled, you must assign them the top-level tag in the access hierarchy. Otherwise, they will get an error indicating that they do not have the access right when they make API calls.