Zones, Users, Groups, Roles and Permissions

YOUnite can group an organization's resources to mirror the organization's structure (e.g. divisions, departments, districts, etc) and uses these groupings to create relationships within the organization. With YOUnite these groupings are called **zones.**

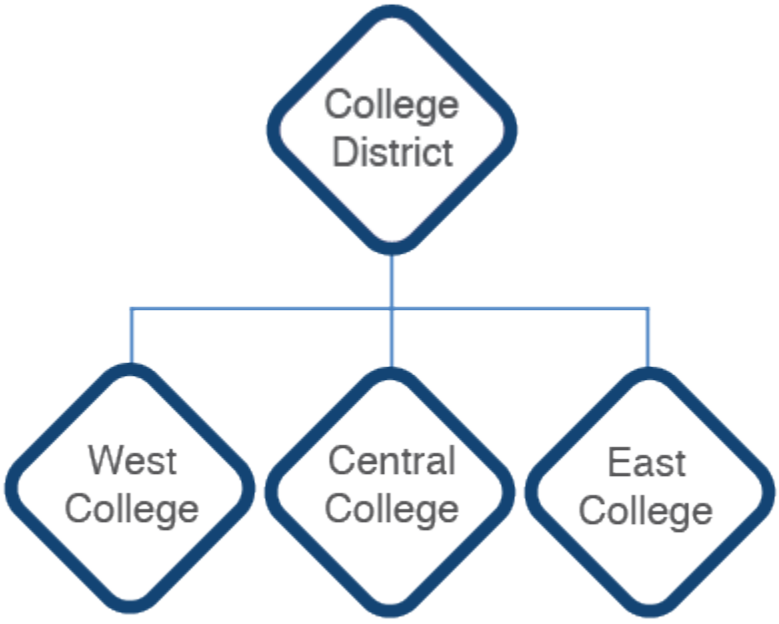
It's important to understand the distinction permissions and ACLs:

- Permissions grant access to resources in the YOUnite ecosystem
- ACLs manage access to inbound and outbound data (which is covered in the Governance page).

Zones

As mentioned above, YOUnite provides zones so an organization can group master data resources along its organization structure.

Zones are associated with each other in a hierarchical structure with parent, child and sibling zones. For example, the following diagram illustrates a college district as the parent zone with three child college zones (which, of course, are siblings of each other):



Zone characteristics:

- Zones generally have two types of users associated with them:
    - **Zone admin** is responsible for general zone management. A zone admin is defined when the zone is created.
    - **Zone data steward** is responsible for the data, data domains and data governance.

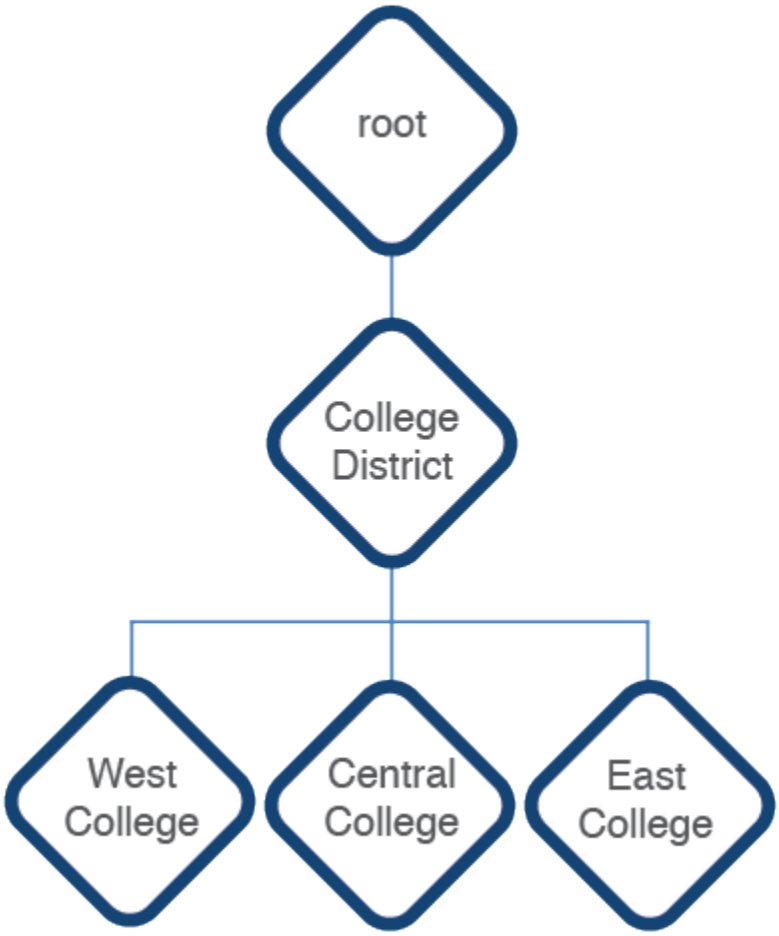
    User types are defined by polices. Polices are covered below.

- Zones receive notifications of data record changes and operational events.
- Zones can have zero, one or more adaptors that map entities stored in services to federated data domains.
- The Zone Admin controls access to zone resources with the exception of the data associated with the adaptors
- The Zone Data Steward controls access to the data entities associated with a zone's adaptors

- The Zone Data Steward can restrict either out-bound or in-bound data shared with or from other zones.
- Centralized YOUnite logs are indexed on a per-zone basis
- A Zone Data Steward can define and share data domains (domains) but generally a single top-level domain creates domains for the entire YOUnite deployment.

The Ultimate Root Zone

Upon initial deployment, YOUnite creates a root zone called **root** with a zone admin user **mdmadmin**. All zones created are subordinate to it. The `UUID` of the root zone is always `6c5a754b-6ce0-4871-8dec-d39e255eccc3`. The root zone's UUID was necessary when creating the "College District" zone below:

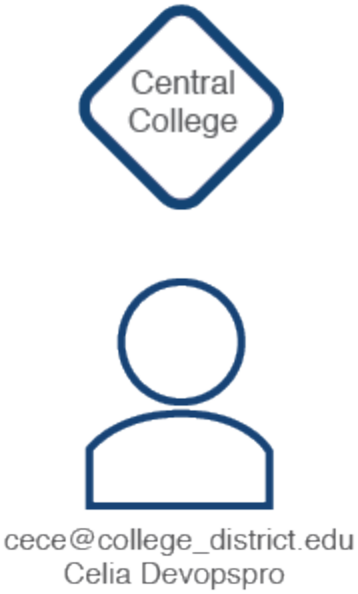


Zone Users

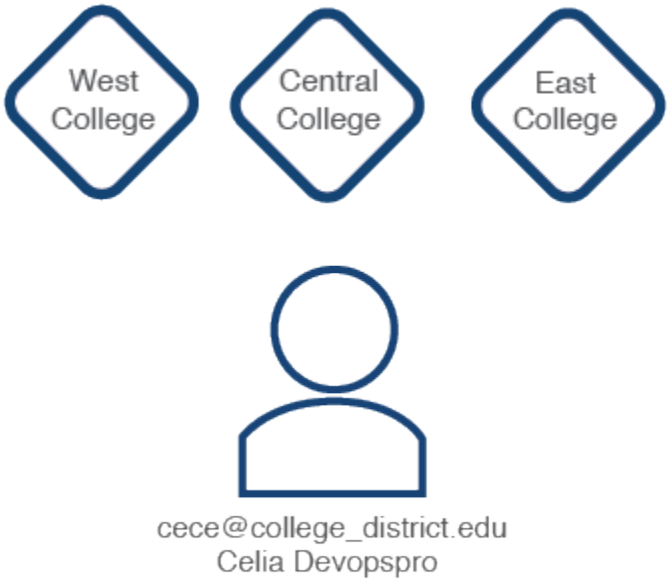
A zone is created by associating a new or existing user with an SSO ID to the zone (TODO See YOUnite and SSO Providers). A zone can not be created without the necessarily associated SSO ID. The first zone user associated with this zone becomes the zone's **Zone Admin** (more on user types and permissions to follow). The Zone Admin has full administrative privileges for the zone.

If this is the first zone associated to a SSO ID, a **YOUnite User** (User) is created that is tied to the associated SSO ID.

For example, if the IT admin created above for the college district zone (senor_jefe@college_district.edu) creates a zone called "Central College" and assigns Cece Jones SSO ID to it as the IT admin for the zone, then a new YOUnite User (cece@college_district.edu) is created and she will be associated with the "Central College" zone:



If two more zone's are created and Cece is associated with them, the same YOUnite User name is used for all associated zones. So now the one YOUnite User (with SSO ID cece@college_district.edu) is associated with three zones:



The YOUnite User's permissions are specific to the zone they are logged into so the YOUnite User's permissions can be different from one zone to another. This is accomplished using permissions, roles and groups.

Permissions

YOUnite users can be granted or denied access to resources by setting appropriate permissions. Permissions do not stand on their own but are grouped into Polices (which are explained below). Permissions are managed by the Zone Admin or other users that have been given control over a zone's permissions. It is better to think of permissions as being grouped together into *roles*, which are explained below.

Permissions are broken out into two properties:

1. Resource URI: The YOUnite resource that is part of the user's zone. If the zone user has the appropriate permissions, they can allow other users to access a resource such as a domain, logs, adaptors, etc.
2. Actions: These are the actions the user can perform on the resource. They include GET, PUT, POST, DELETE, PATCH (and ALL).

Permission Example

In this example a user is granted full access to all domains in the zone except for:

- staff: The user has no access to the staff domain
- students: The user has full access except DELETE to the students zone

	Actions			
Resource	**GET**	**PUT**	**POST**	**DELETE**
/domains/*	YES	YES	YES	YES
/domains/staff/*	NO	NO	NO	NO
/domains/students/*	YES	YES	YES	NO

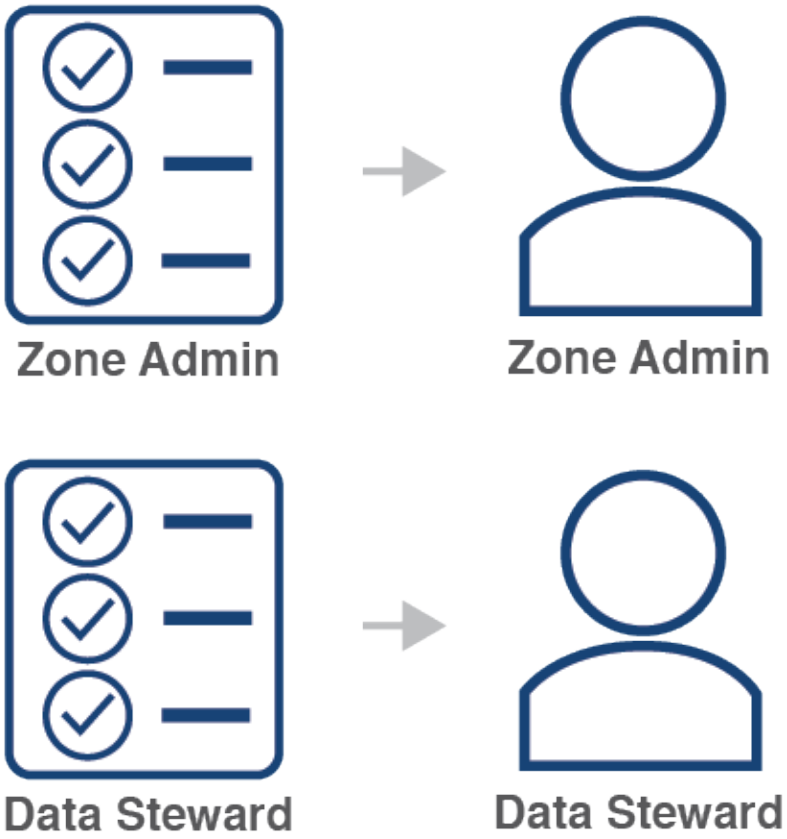
Any user with this permission can create, modify, delete and view all other user's for a zone.

Roles

A role is a group of permissions that can be used to manage user access to resources. YOUnite has two default **managed roles.** These two managed roles are visible to all zones and can not be deleted.

Typically there are two types of users associated with a zone that leverage these roles:

1. **Zone Admin**: These users have zone admin privileges. As mentioned above, the first Zone Admin has full administrative privileges for the zone but additional roles and permissions can be configured that restrict access to other Zone Admins. The Zone Admin has general zone management responsibilities such as creating subordinate zones, adding adaptors, creating/managing groups and Users and attaching Roles to Groups and individual Users.
2. **Zone Data Steward** (ZDS): Zone Admins can create additional Users with data steward permissions. These Users have access and manage control (governance) to the data records (covered in the Scopes & Metadata and Metadata pages). (TODO need to fix the link. I think should be to Governance now.)



See the YOUnite API documentation for more specific on roles.

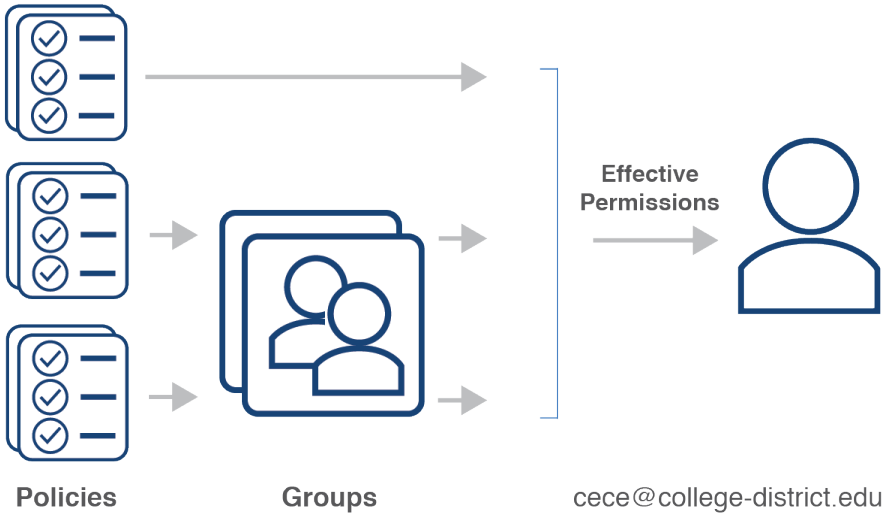
Groups

A Group is a collection of Users in a zone that has roles associated with it. A Group can have multiple roles associated with it and Users can belong to more than one group.

Effective Permissions

In particular zone, the User's effective permissions are a union of all the permissions associated with all of the groups that he or she is in and any roles directly associated with them.

The following diagram pulls all of the above topics together and shows how the user's effective permissions are calculated (TODO graphic below needs to be fixed to say roles instead of policies.)



See the YOUnite API documentation for more specifics on zones, users, groups and roles.