About Organizations, Zones & Users

Data on Asset Manager is segregated by an enterprise-grade user management facility that controls who can see Asset Manager system options, components, and zones. Access to individual zones is controlled by an administrator who assigns users to organizations and zones. User-defined system configurations can be reused in all zones to which the user has access.

Organizations

In the context of Asset Manager and for the purpose of linking users to zones, an Organization is a set of Zones with a common set of permissions. There can be many organizations and these are associated with one another in a single layer without hierarchy. Organizations do not nest within other organizations.

Each organization has three fully defined roles belonging to it: **SysAdmin**, **Manager**, and **Viewer**. The organization segregates users and controls what information they can see and manipulate. You can add, edit, and delete most organizations. The default organization, called Organization 1, can be renamed but not deleted.

This structure of access control enables you to restrict zone access to particular users. Now, New York Asset Manager users can have access to the New York Zone and not the London Zone, for example. London users can be granted access to London Asset Manager Zone and blocked from New York Asset Manager Zone.

About Organizations

- Each zone is assigned to a single organization
- Each role is specific to an organization
- Each user can have multiple roles and the roles can be associated with different organizations

Example: **User Sally**

- Has two roles: Manager/Organization1 and Viewer/Organization2
- Can view and modify all of Organization1's zones
- Can create new zones in Organization1
- Can view but not create zones in Organization2

Example: **User Bob**

- Has one role: Viewer/Organization1
- Can view zones in Organization1
- Cannot view zones in Organization2
- Cannot modify or create new zones in either organization

Zones

Available Zones are sets of network devices you want to monitor as a unit. For example, a zone might describe a subnet, an enclave, boxes containing classified financial data, machines belonging to a particular business unit, devices affiliated by region or purpose, machines over which a security or operations professional is responsible.

A zone may also describe a set of network devices that are to be monitored using defined indexing methods. In the screencap on the left, several zones have been set up to target the same IPs/CIDRs. The indexing methods each zone uses to explore the area, however, vary. The zones have been named to indicate the indexing methods that have been configured to perform. Host+Port+DP, for example, contains collectors configured to identify host, port, and device profiling information. This method is especially useful when you want to find out or better understand what Asset Manager can discover using one indexing technique versus another.

Typically, one organization contains several zones.

- The zone that comes with Asset Manager by default is called Zone1. This default zone can be renamed but not deleted.
- You can add, edit, or delete zones. Select the zone you want to manage before clicking Edit Zone or Delete Zone.
- You may add as many zones as you need.

When you add a zone, consider giving it a name that's associated with its user base such as Corporate Zone, Guest Zone, or Wi-Fi Zone. Or give it a name with geographical or business significance such as Manufacturing, Finance, West Coast Office, or New York Office.

See Adding & Managing Zones for step-by-step procedures on how to add, edit, view, monitor, and map zones.

Users

A ***user*** is a login and password combination that identifies individuals entitled to use Asset Manager.

Valid usernames:

- Use this set of characters: A-Za-z0-9_.-
- Are one or more characters (but not a single dot, digit or hyphen)
- Do not start with a hyphen
- If the id starts with a dot, then there has to be at least one non-dot character afterwards
- If the id starts with a number, then there must be one non-numeric character afterwards

A ***superuser*** is not a role but a flag that allows a user to manage all aspects of the system regardless of zone affiliation. The entire system is accessible to a user with superuser privileges. CRUD operations can only be performed by a superuser. Also, the superuser can see the Support menu option.

The superuser permission is required to grant superuser status to another user. It is also required to add the first user to an organization. At least one user must have this superuser flag set. Any attempt to delete the last superuser is ignored by the system and a message is returned to the user. The password for this user is "admin". See Managing Asset Manager via the CLI for the "Adding a superuser" command. The superuser can oversee the complete Asset Manager system. This role is equivalent to the root user of linux or the Administrator of Windows.

Asset Manager comes with two default users: *admin* and *manager* - The admin has the SysAdmin role and superuser privileges.

User	Role	Description
admin	SysAdmin Viewer	Has SysAdmin role and superuser privileges
manager	Manager Viewer	Has Manager role of the default Organization 1. Has Viewer role of the default Organization 1.

About configuring users . . .

- The "superuser" is a flag associated with a user, and not with a Role or Organization. It provides complete access to the Asset Manager system. The *superuser* can access everything. The *superuser* flag is set via the CLI only. Multiple superusers can be created. Superusers can be deleted as long as there is more than one of them. The last superuser cannot be deleted.
- You can add, edit, and delete usernames.
- You can add, edit, and delete user accounts.

Browse to **Settings** > **Users** to set up user accounts and system access.

Roles

Roles define the system features and commands users can access. Each user is assigned a set of permissions, or *role*.

Username	Full Name	Roles
admin	Default administrative user	Organization1(SysAdmin)
manager	Default management user	Organization1(Manager,Viewer)
manager2	Manager2	Organization2(Manager)
mgr_all	mgr_all	Organization3(Manager) Organization1(Manager) Organization2(Manager)
org3_mgr	org3_mgr	Organization3(Manager)
org3_sysadmin	org3_sysadmin	Organization3(SysAdmin)
org3_viewer	org3_viewer	Organization3(Viewer)
viewer1	Viewer1	Organization1(Viewer)
viewer2	Viewer2	Organization2(Viewer)
vw_all	vw_all	Organization1(Viewer) Organization3(Viewer) Organization2(Viewer)

Asset Manager comes with three pre-defined roles that you can assign to a user. You can assign all three rolls to a user, two of the roles to a user, or none of the rolls to a user.

SysAdmin - Manages the system. Is concerned with details at device level (i.e., software and hardware). Can manage the Asset Manager System (Installation of License, Upgrading the System, Configuring CEF, Resetting the IP, Restarting services or system). The SysAdmin cannot log in to the Asset Manager GUI *unless* he or she has also been given the Viewer role, the Manager role, or has been flagged as a superuser.

```
sysadmin@QE-TB-CC-3320>
  authentication  Manage licenses, SSL certificates and authentication
  certificate     Manage licenses and SSL certificates
  collector       View and edit collectors
  exit            Logout of the current CLI session
  help            Display an overview of the CLI syntax
  history         Display the current session's command line history
  log             View and edit system log settings
  logout          Logout of the current CLI session
  organization    View and edit organizations
  role            View and edit roles
  spectre         View and connect to Lumeta Spectre systems
  system          View, edit system parameters; shutdown/reboot system
  top             Exit sub-command mode and return to top level
  user            View and edit users
  zone            View and edit zones
```

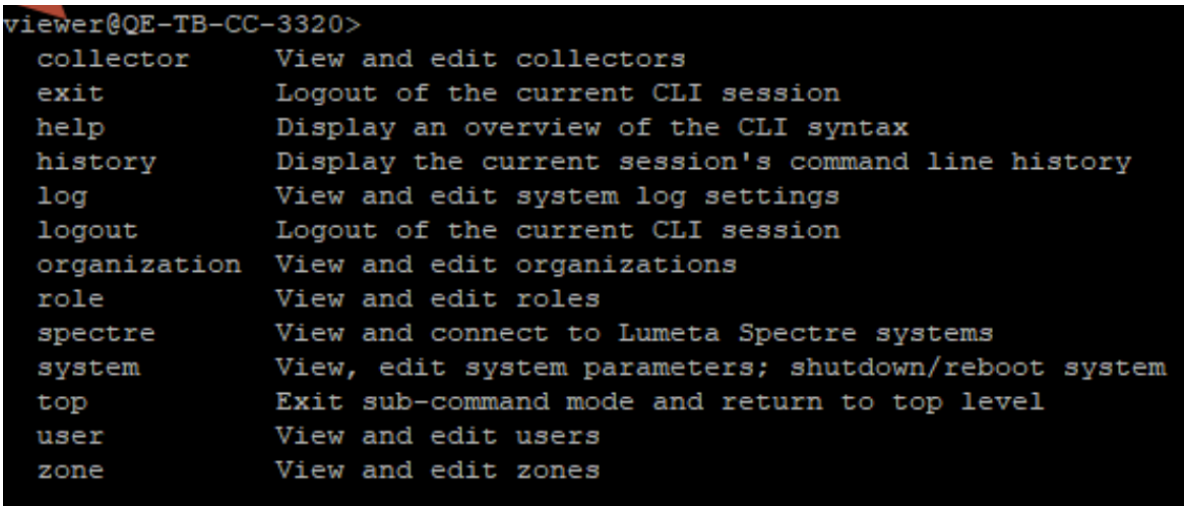
Manager - Concerned with Asset Manager-specific details. Manages the Organization to which he/she belongs. Creates zones and collectors, assigning roles to users, subscribes to notifications, configures dashboards.
Manager can access GUI for the following functionality:

- Can modify users – can edit the roles and password of a user.
- Can add/modify/delete zones
- Can add/modify collectors (and all its sub functionality)
- Can configure notifications
- Can not configure CEF notifications
- Can view reports, maps and zones

Manager can access the following commands in CLI:

```
mal@QE-TB-CC-3320>
  collector     View and edit collectors
  exit          Logout of the current CLI session
  help          Display an overview of the CLI syntax
  history       Display the current session's command line history
  log           View and edit system log settings
  logout        Logout of the current CLI session
  organization  View and edit organizations
  role          View and edit roles
  spectre       View and connect to Lumeta Spectre systems
  system        View, edit system parameters; shutdown/reboot system
  top           Exit sub-command mode and return to top level
  user          View and edit users
  zone          View and edit zones
```

Viewer - Read only. User cannot manipulate zones or Asset Manager system software or hardware. Views the organization to which he/she belongs. Can view zones, collectors, maps, and dashboards.



User Roles

Every GUI and CLI command calls an API. Every API call has either a single permission associated with it, or no permissions at all. If no permission, or the permission NONE, anyone can use that API.

Permission	Notes
NO_ACCESS	API is disabled
NONE	No permission required (default) – Anyone can use the API
VIEW_ZONE	Viewing reports and dashboards
MANAGE_USERS	Adding and deleting users, assigning roles
MANAGE_ZONES	Adding/deleting/configuring zones and collectors
MANAGE_SYSTEM	All system-wide functions, like importing configs, starting/stopping services, etc.
MANAGE_SCOUT	Interpreted as "manage remote" for adding and deleting remote systems
BYPASS_ACCESS	Only superuser may use this API

Every role has a group of permissions. If a user has a role, then that role's permissions define which APIs the user can call, and in turn which GUI and CLI commands. Superuser is not a role; it's a flag. When a user has the superuser flag enabled, the system bypasses (ignores) the roles and allows the user to run any API, and therefore any command.Some APIs require BYPASS_ACCESS permission, which means that only a superuser can use those APIs.

Role	Permissions
Manager	MANAGE_USERS, MANAGE_ZONES, VIEW_ZONE
SysAdmin	MANAGE_SCOUTS, MANAGE_SYSTEM
Viewer	VIEW_ZONE
PortalUser	MANAGE_SCOUTS, VIEW_ZONE

FAQs

If a user needs access to all zones, view only, what access would they need?
This user would need the "Viewer" role for each organization.

A user has admin right access, why can't that user see all zones?
Assuming the user has the "SysAdmin" role, this role is focused on managing the Asset Manager appliance. It does not provide view access.

Is there any conflict or issue with multiple users logging into the same CC at the same time, under the default admin account?
This is not recommended as a standard operation as there is no individual accountability in such a process. As to conflict, the only area where there would be an issue is around the map. The map automatically saves changes for the user. This means that if User Bob goes to the map, moves stuff around, and makes certain display choices; these get saved. Bob then goes off duty, and Mary logs in. Mary goes to the map and makes changes. Mary goes off duty, Bob logs in, goes to the map and the map is different than what he expects from his last save because Mary's (more recent) choices have overwritten Bob's.