Universal Control Plane Beta 0.8 Access Control Mini Guide

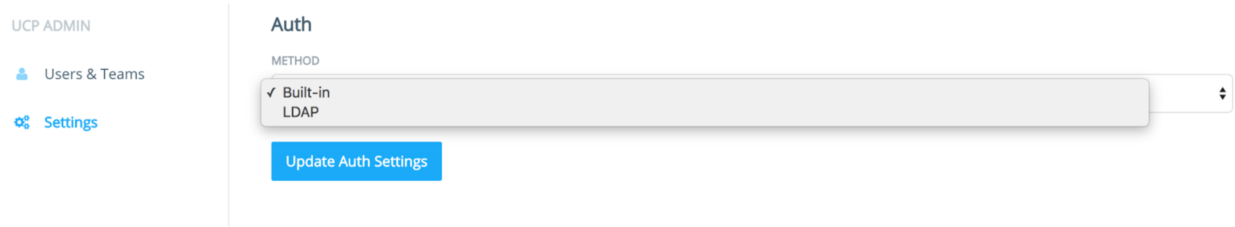
In the latest version of the UCP Beta we've added some features around LDAP integration and role-based access control. You can expect more rigorous documentation on this in the 1.0 release, but for now here's a quick guide to get you started.

Managed vs LDAP

In UCP you can authenticate user accounts in one of two ways: **Built-in** and **LDAP**. In **Built-in** mode, an admin can create new users and set relevant information (**Name**, **Password**, etc.). The account information is stored in UCP.

In **LDAP** mode, UCP can integrate with your organization's existing LDAP user and authentication database. To switch to **LDAP** mode:

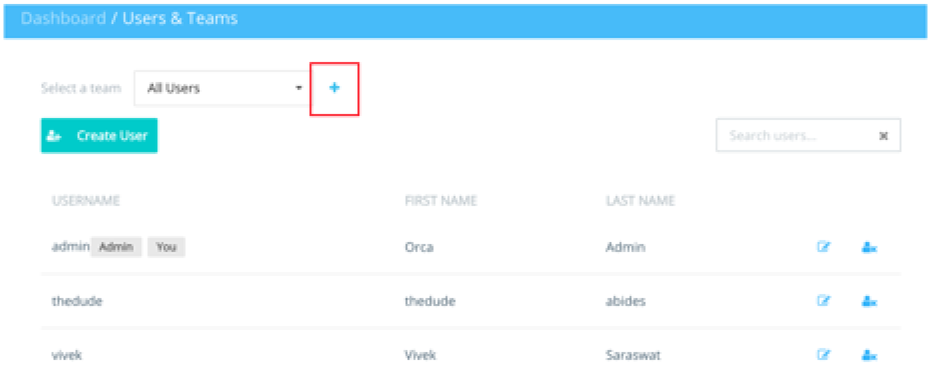
1. Log in as a user with admin privileges.
2. Choose **Settings** page.
3. Scroll down to the **Auth** section.
4. Choose **LDAP** mode for the method.



Switching to LDAP mode causes UCP to display several options required to configure the integration between UCP and your LDAP database. Though we won't go into this process in detail here, it is similar to the process outlined in the Docker Trusted Registry documentation (https://docs.docker.com/docker-trusted-registry/configuration/#ldap-authentication).

Users and Teams

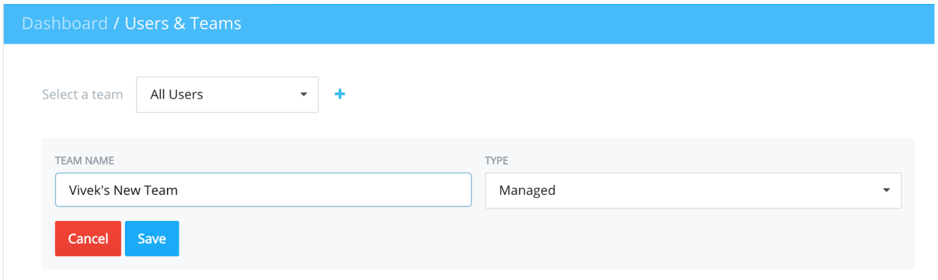
New to UCP 0.8 is the ability to create **Teams**. A team groups users for access control purposes. A team can be manually created via UCP or can be synced through LDAP system integration. UCP admins can manually create a new team by going to the **Users & Teams** page clicking the **+** (plus sign) on the **Select a Team** page (see below).



Select a team: All Users

USERNAME	FIRST NAME	LAST NAME
admin Admin You	Orca	Admin
thedude	thedude	abides
vivek	Vivek	Saraswat

This will open up a new set of dialog boxes for creating a new team (either Managed via UCP or synced to an LDAP group).

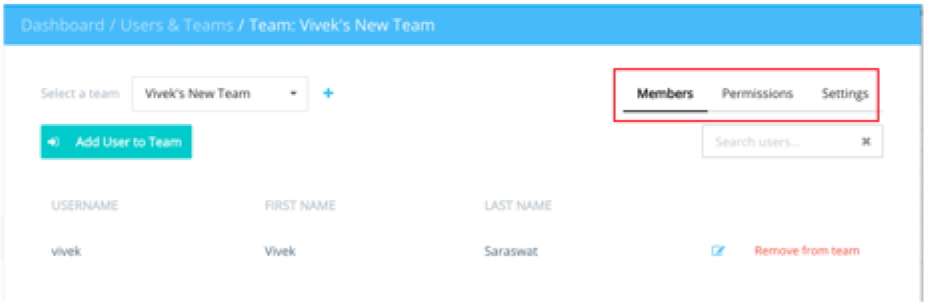


Select a team: All Users

TEAM NAME: Vivek's New Team

TYPE: Managed

Once you have created a new team, you'll see a couple of options (see below). **Members** allows you to add and remove users to the team. Settings allows you to rename or delete the team. Permissions allows you to enforce access control to containers. More on that below.



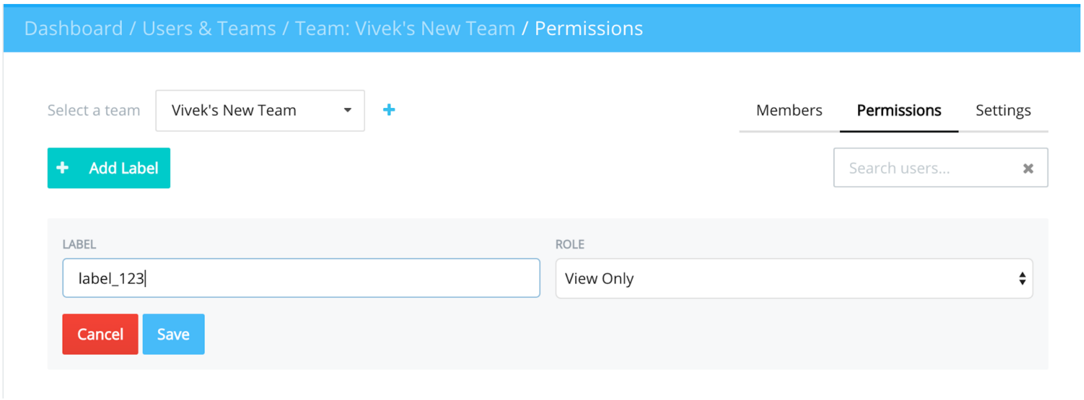
Select a team: Vivek's New Team

USERNAME	FIRST NAME	LAST NAME	
vivek	Vivek	Saraswat	Remove from team

Access Control

In UCP 0.8, access control is enforced through the use of labels. Using UCP you can assign a team a specific "role" (level of access) relative to that label. When you apply that label to a container, members of that team gain that role's level of access to the container. In the current UCP 0.8 beta, these roles are:

Total Control: Can view, inspect, run, delete, and exec into containers
Restricted Control: Can view, inspect, run, and delete containers
View Only: Can view and inspect containers
No Access: Cannot view containers


Dashboard / Users & Teams / Team: Vivek's New Team / Permissions
Members
Permissions
Settings
+ Add Label
Search users...
Cancel
Save

Select a team: Vivek's New Team

LABEL: label_123

ROLE: View Only

A team can have multiple labels; similarly, multiple teams can have different roles for the same label. If a user is a part of two or more teams which have different roles for a specific label, that user gets the highest level of access out of those roles. By default, a non-admin user who is not part of any teams will not see any containers at all (because they have no roles and thus no levels of access). Also by default, an admin user has access to all containers.

One note--we've seen some potential issues around using access control on non-admin user accounts that were created in previous versions of the UCP Beta. If you have upgraded to 0.8.0 from an earlier version, you must recreate the non-admin accounts if you would like to test out the access control features. You can expect these issues to be sorted out prior to the 1.0 release of UCP.

This concludes our quick-and-dirty guide to using access control with UCP 0.8. Please feel free to ask any questions or troubleshoot issues in the forums.