



# Hedvig RBAC User Guide

# Table of Contents

Hedvig RBAC overview .....	4
Concepts of RBAC .....	4
Default tenant and roles .....	5
Built-in system users .....	5
Using the Hedvig WebUI to set up and manage RBAC .....	6
Logging into the Hedvig WebUI .....	6
Selecting a Tenant .....	7
Accessing the RBAC (User Administration) menu.....	7
User Management.....	8
Primary tenant defined .....	8
Adding a new user to a tenant .....	9
Adding a user manually (locally).....	9
Adding an LDAP/AD user or group .....	10
Deleting multiple users.....	12
Managing CHAP users.....	13
Working with a specific user .....	14
Changing roles for a user .....	14
Deleting a user from a tenant .....	15
Role Management.....	16
Hedvig default roles (SuperUser, PowerUser, Admin, Monitor).....	17
Types of permissions (Own, Tenant, All).....	18
Permissions for Hedvig default roles.....	18
Adding custom roles .....	20
Example of adding custom roles.....	21
Removing custom roles .....	22
Tenant Management.....	23
Adding a tenant.....	23
Working with a specific tenant.....	24
Showing the users of a tenant .....	24
Removing a tenant .....	25
Adding a user to a tenant.....	25
Edit Profile .....	26
Appendix A: Connecting/editing preconfigured LDAP/AD server .....	28
Appendix B: Glossary .....	32

# List of Figures

Figure 1: Hedvig WebUI login screen.....	6
Figure 2: User menu - Select Tenant .....	7
Figure 3: Four areas of RBAC management.....	7
Figure 4: User Management dialog.....	8
Figure 5: Add User dialog - Adding a user manually.....	9
Figure 6: Add User dialog - Adding an LDAP/AD user.....	10
Figure 7: Add User dialog - Listing of LDAP/AD users .....	10
Figure 8: Add User dialog - LDAP/AD user information .....	11
Figure 9: Add User dialog - Add LDAP/AD Group .....	11
Figure 10: Add User dialog - Add LDAP/AD Group - Listing of users.....	12
Figure 11: Deleting multiple users.....	12
Figure 12: Delete Users dialog.....	12
Figure 13: Manage CHAP Users dialog - Current Users tab.....	13
Figure 14: Manage CHAP Users dialog - Add User tab .....	13
Figure 15: User Management dialog - User tasks.....	14
Figure 16: Change Roles dialog .....	14
Figure 17: Delete User dialog .....	15
Figure 18: Role Management dialog.....	16
Figure 19: Add Role dialog.....	20
Figure 20: Role Management dialog - Setting up a custom role .....	21
Figure 21: Remove Role dialog.....	22
Figure 22: Tenant Management dialog.....	23
Figure 23: Add Tenant dialog.....	23
Figure 24: Tenant Management dialog - Tenant tasks .....	24
Figure 25: Tenant Users dialog.....	24
Figure 26: Remove Tenant dialog.....	25
Figure 27: Add Users to Tenant dialog .....	25
Figure 28: Edit Profile dialog.....	26
Figure 29: Edit Profile dialog - LDAP/AD user message .....	27
Figure 30: User menu - LDAP/AD Configuration.....	28
Figure 31: LDAP/AD Configuration dialog.....	29
Figure 32: Group/Role Mapping dialog.....	31

# Hedvig RBAC overview

Hedvig's role-based access control (RBAC) has been implemented primarily for the administration of *multitenancy*. RBAC lets you assign permissions using *roles*, a process that is more flexible and persistent than assigning permissions directly to *users*.

Hedvig RBAC has been applied to the following aspects of the Hedvig environment: *Hedvig clusters*, *Hedvig virtual disks*, and *Hedvig user administration*.

The following sections contain additional information about the features of Hedvig RBAC:

- [Concepts of RBAC](#)
- [Default tenant and roles](#)
- [Built-in system users](#)

## Concepts of RBAC

Hedvig RBAC is based on the concepts of:

- *tenants*, which are *groups* of users:
    - You can set up multiple tenants per cluster.
    - You can set up multiple LDAP/AD servers per tenant.
  - *users* assigned to these tenants:
    - You can set up multiple users per tenant.
    - Each user can belong to more than one tenant.
    - Each user has a *primary tenant* — the tenant to which they are first assigned (see also [Primary tenant defined](#)).
- Note:** You do not have to set up *LDAP/AD users* as *Hedvig users* — they can log in directly if you give them permission. However, for LDAP/AD users to use Hedvig S3, you must save them as Hedvig users in order to use the Security Token service.
- *user roles*, which give users *permission* to perform specific tasks:
    - Each user has one role per tenant.
    - Roles can be Hedvig default roles (*SuperUser*, *PowerUser*, *Admin*, or *Monitor*) or custom roles that you have created.
  - *tenant attributes*, which are defined in the context of other tenants.

## Default tenant and roles

Hedvig RBAC is set up with one default tenant, *Hedvig*.

There are four Hedvig default roles, which cannot be edited or deleted. You can assign these Hedvig default roles to your users, and/or you can create new *custom* roles for your users (see also [Role Management](#)).

- *SuperUser*
- *PowerUser*
- *Admin*
- *Monitor*

## Built-in system users

There are five *built-in system users*, which cannot be edited or deleted. You may notice them as the *creator* of some of your virtual disks.

- *HedvigAdmin*, which is used by the Hedvig support team for general troubleshooting. This user has a default password of *hedvig*, which you should change after login, to customize it for your cluster (see also [Edit Profile](#)).
- *Hedvig CLI*, which is displayed for certain actions performed in the Hedvig CLI.
- *Hedvig WebUI*, which is displayed for certain actions performed by Hedvig REST APIs.
- *Openstack*, which is displayed for certain actions performed with OpenStack.
- a built-in system user that is the *name of your cluster*

# Using the Hedvig WebUI to set up and manage RBAC

- [Logging into the Hedvig WebUI](#)
- [Selecting a Tenant](#)
- [Accessing the RBAC \(User Administration\) menu](#)

## Logging into the Hedvig WebUI

The Hedvig WebUI provides visual real-time monitoring of Hedvig Storage Clusters and runs on any HTML5-compatible web browser, including mobile devices.

To access a Hedvig Storage Cluster using the Hedvig WebUI, enter:

`http://cluster_node_name` or `https://cluster_node_name`

You will see a login screen. Enter your **Username** (which is case sensitive) and **Password**, and optionally a **Domain or LDAP/AD Server Name**, and select **Log in**.

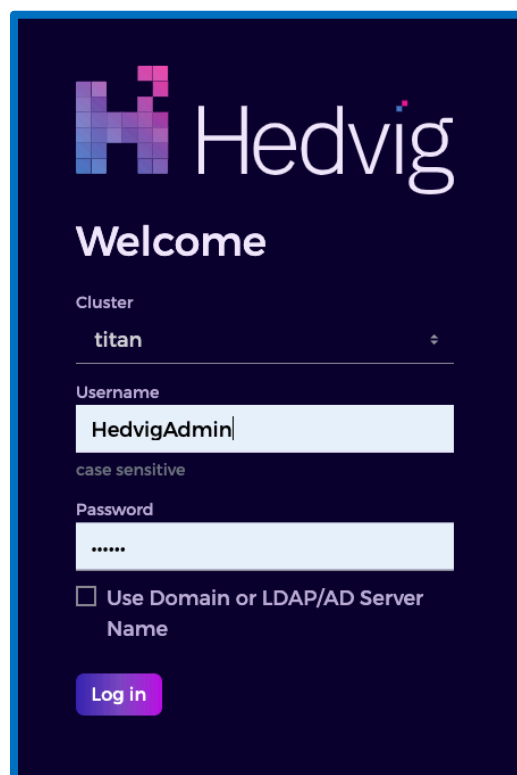


Figure 1: Hedvig WebUI login screen

## Selecting a Tenant

In the Hedvig WebUI, you should first select a Tenant, if you have more than one. Choose **Select Tenant** from the **User** menu. As aforementioned, the default tenant is *Hedvig*.

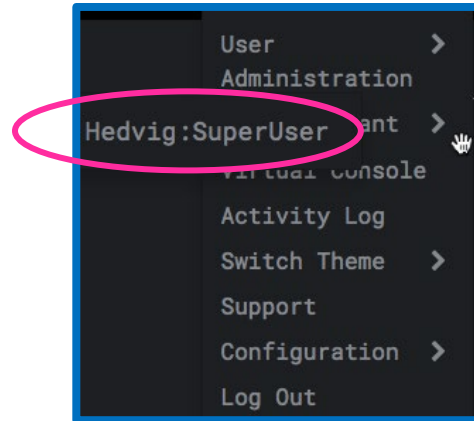


Figure 2: User menu - Select Tenant

## Accessing the RBAC (User Administration) menu

To access the RBAC functions, select **User Administration** from the **User** menu. You will see the following menu.

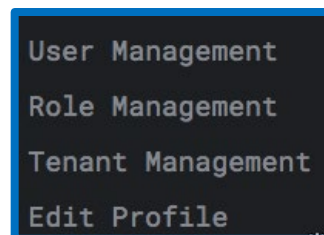


Figure 3: Four areas of RBAC management

The four areas of RBAC management will be explained in detail in this guide:

- [User Management](#)
- [Role Management](#)
- [Tenant Management](#)
- [Edit Profile](#)

# User Management

User Management lets you add users to a tenant, as well as edit tenants or delete existing users from a tenant. You also manage CHAP Users in this area.

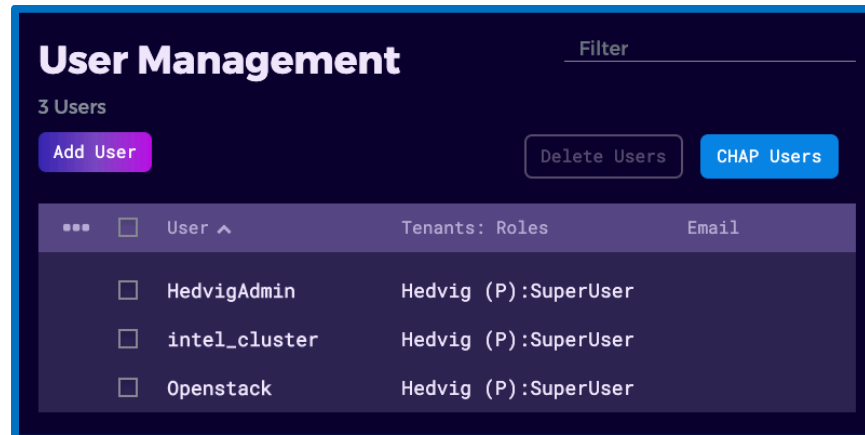


Figure 4: User Management dialog

## Primary tenant defined

In the **Tenants: Roles** column, the **(P)** indicates the *primary tenant* of a user. The first time a user is added to a Hedvig Cluster, the tenant to which they are added is their primary tenant.

When a user has multiple tenants, the user's primary tenant will not change unless that specific tenant is deleted using the **Change Roles** page for that user. And this can be done only by a PowerUser of that tenant, or a SuperUser.

**Note:** See also [Changing roles for a user](#).

This section has the following subsections:

- [Adding a new user to a tenant](#)
- [Deleting multiple users](#)
- [Managing CHAP users](#)
- [Working with a specific user](#)



## Adding a new user to a tenant

To add a new user to a tenant, on the **User Management** page, select **Add User**. There are several choices for adding a user:

- [Adding a user manually \(locally\)](#)
- [Adding an LDAP/AD user or group](#) (if you are connected to an LDAP/AD server)

### Notes:

- A PowerUser can add (to their specific tenant) only those users who do not already have a primary tenant.
- A SuperUser can add all types of users, including another SuperUser.
- For any user addition, if you do not specify a password, one will be generated and emailed to the user.

## Adding a user manually (locally)

To add a user manually (that is, *locally*), complete the requested information in the **Add User** dialog. You can, but do not have to, enter a password. If you do not, a random password will be emailed to the specified email address. Then, select **Run**.

The screenshot shows a dark-themed 'Add User' dialog box. At the top, there are three radio buttons: 'Enter Manually' (selected), 'Add LDAP/AD User', and 'Add LDAP/AD Group'. Below these are several input fields: 'Display Name', 'User Name', 'Tenant' (with a dropdown menu showing 'Hedvig'), 'Role' (with a dropdown menu showing 'PowerUser'), 'Email', 'Mobile', 'Password', and 'Confirm Password'. At the bottom, there is a note: 'Note: If a password is not entered, a random password will be generated and sent to the email address specified.' and a 'Run' button.

Figure 5: Add User dialog - Adding a user manually

## Adding an LDAP/AD user or group

An LDAP/AD configuration is on a per Tenant basis.

**Note:** If you are trying to add an LDAP/AD user, but have not connected your LDAP/AD server to the Hedvig WebUI, you will get a message to that effect.

To set up a LDAP server, see [Appendix A: Connecting a preconfigured LDAP/AD server](#).

1. Choose whether to **Add LDAP/AD User** or to **Add LDAP/AD group**.
2. To **Add LDAP/AD User** (for a group, skip to step 3):

**Add User**

Enter Manually
  Add LDAP/AD User
  Add LDAP/AD Group

Tenant  
Hedvig

Server  
192.168.108.17

User Search Filter  
(objectclass=person)

Next

Figure 6: Add User dialog - Adding an LDAP/AD user

- a. Select a **Tenant**.
- b. Select an LDAP/AD **Server**.
- c. Enter a search filter in **User Search Filter**, for example:  
(objectclass=InetOrgPerson)
- d. Select **Next**.
- e. In the resulting screen, select the desired user's id.

**Add User** ✕

Adding LDAP/AD User - Click on user's id to select.

5 Users Filter

User	Display Name	Email	Mobile
euclid@ldap.forumsys...		euclid@ldap.forumsys...	
euler@ldap.forumsys...		euler@ldap.forumsys...	
gauss@ldap.forumsys...		gauss@ldap.forumsys...	
riemann@ldap.forumsy...		riemann@ldap.forumsy...	
test@ldap.forumsys.c...			

Back

Figure 7: Add User dialog - Listing of LDAP/AD users

- f. In the resulting screen, complete the user's information, and select **Run**.

The screenshot shows a dark-themed dialog box titled "Add User" with a close button (X) in the top right corner. At the top left is a "Back" button. Below it are several input fields: "Display Name" with the value "sqladmin", "User Name" with "sqladmin@192.168.108.17", "Tenant" with a dropdown menu showing "Hedvig", and "Group" with a dropdown menu showing "CN=Enterprise Admins,CN=Users,DC=corp,DC=hedviginc,DC=com". Below these are fields for "Role" (containing "SuperUser"), "Email", and "Mobile". At the bottom left is a "Run" button.

Figure 8: Add User dialog - LDAP/AD user information

3. To add all of the users in an LDAP/AD Group:

The screenshot shows a dark-themed dialog box titled "Add User" with a close button (X) in the top right corner. At the top, there are three radio buttons: "Enter Manually", "Add LDAP/AD User", and "Add LDAP/AD Group", with the third one selected. Below are several input fields: "Tenant" with a dropdown menu showing "Hedvig", "Server" with a dropdown menu showing "192.168.108.17", and "Group" with a dropdown menu showing "CN=Denied RODC Password Replication Group,CN=Users,DC=corp,DC=hedviginc,DC=com". At the bottom left is a "Next" button.

Figure 9: Add User dialog - Add LDAP/AD Group

- Select a **Tenant**.
- Select an LDAP/AD **Server**.
- Select a **Group**.
- Select **Next**.

- e. In the resulting screen, all displayed users will be added when you select **Run**.

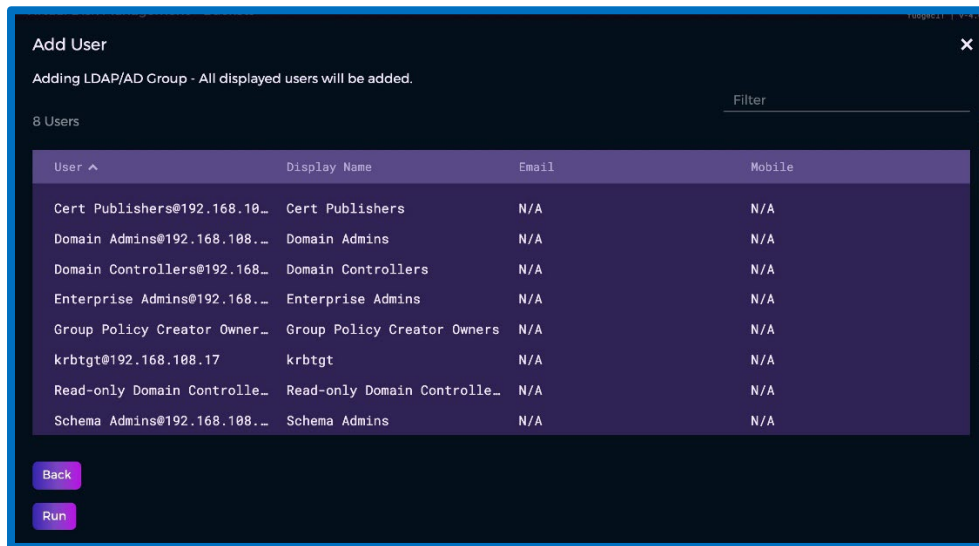


Figure 10: Add User dialog - Add LDAP/AD Group - Listing of users

**Note:** LDAP/AD users are named <user name>@<LDAP/AD server name>.

## Deleting multiple users

On the **User Management** page, to delete selected (or all) users, check the boxes to the left of the desired users (or check the top box to select all), and select **Delete Users** at the top right. In the **Delete Users** dialog, select **Run**.

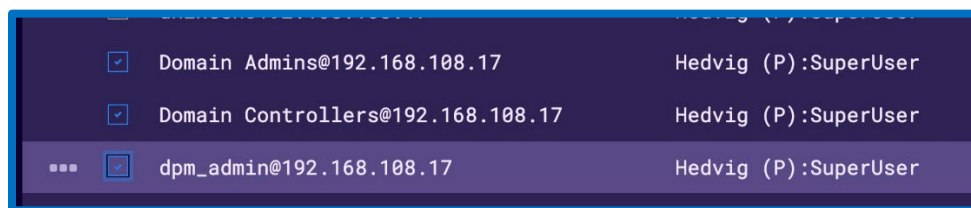


Figure 11: Deleting multiple users

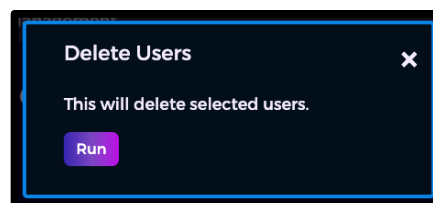


Figure 12: Delete Users dialog

**Note:** When deleting LDAP users that have been added as a group to a tenant, you must manually select all of these users to schedule them for deletion.

## Managing CHAP users

On the **User Management** page, to manage CHAP (Challenge-Handshake Authentication Protocol) users, select **CHAP Users** at the top right.

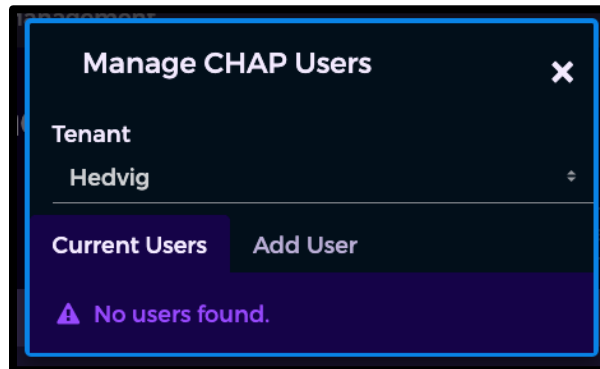


Figure 13: Manage CHAP Users dialog - Current Users tab

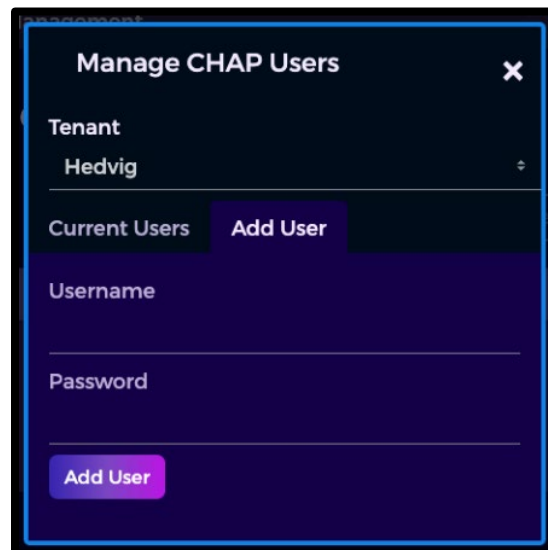


Figure 14: Manage CHAP Users dialog - Add User tab

In the **Manage CHAP Users** dialog, to add a CHAP user, select the **Add User** tab, and enter the **Username** and **Password**, noting the following requirements:

- CHAP usernames can be from 1 to 128 bytes. Username cannot be null.
- CHAP passwords can be from 1 to 512 bytes. Password cannot be null.
- Microsoft iSCSI Initiator requires both the initiator and target CHAP passwords to be at least 12 bytes if IPsec encryption is not used. The maximum password length is 16 bytes.

Select the **Add User** button at the bottom of the dialog to complete the process.

## Working with a specific user

When you select the ellipsis (...) to the left of each user on the **User Management** page, you will see a list of tasks that you can perform.

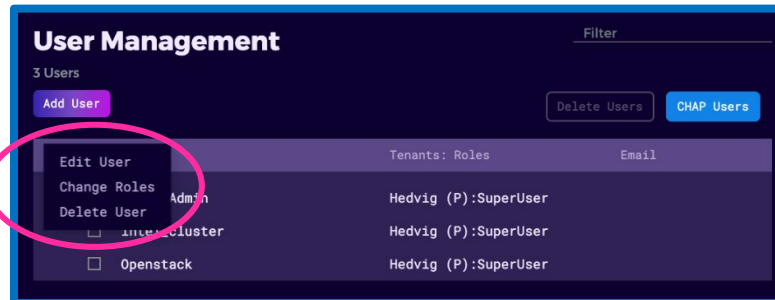


Figure 15: User Management dialog - User tasks

- **Edit User** - see [Edit Profile](#). This task is usually done by a user for his or her own profile. However, a SuperUser can edit all user profiles, and a PowerUser can edit the user profiles of the users in their specific tenant.
- Change Roles - see [Changing roles for a user](#).
- Delete User - see [Deleting a user from a tenant](#).

## Changing roles for a user

To change the roles for a user, select **Change Roles**. In the **Change Roles** dialog, you can change both the tenant and/or the role. You can also add tenants and roles.

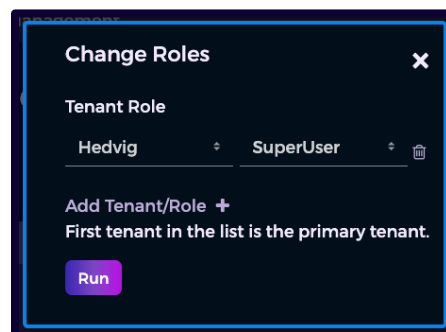


Figure 16: Change Roles dialog

Only a SuperUser can change the primary tenant, which is the first tenant in the list.

- If the user has more than one tenant, you must delete the current primary tenant.
- If the user has only one tenant, you can simply change the primary tenant.

**Note:** See also [Primary tenant defined](#).

## Deleting a user from a tenant

A SuperUser can delete any user. A PowerUser can delete only users whose primary tenant is their specific tenant.

To delete a user from a tenant, select **Delete User**. The **Delete User** dialog gives you an opportunity to confirm the deletion of the selected user. Select **Run** if you are sure you want to delete the user.

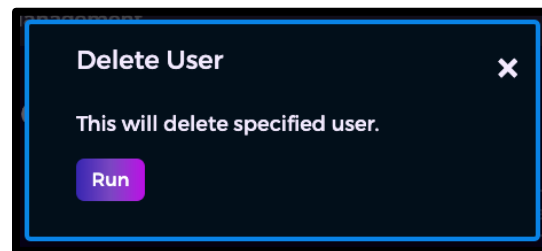


Figure 17: Delete User dialog

**Note:** To quickly delete multiple (or all) users, you can use the **Delete Users** button on the **User Management** page. See [Deleting multiple users](#).

# Role Management

Role Management lets you see the specific permissions for the four Hedvig default roles. You can also add and remove custom roles.

## Notes:

- Deletions are considered a special type of administration and are delineated separately from basic management tasks.
- The **View Vdisk Management - Own** permission is implicit for all users, and therefore it is not explicitly listed in the Permissions table.

The screenshot shows the 'Role Management' dialog for the 'Hedvig' tenant. It features a table with 14 rows of permissions and 4 columns of roles. Each cell contains a checkbox, with blue indicating a checked permission and pink indicating an unchecked permission.

Permissions	Admin	Monitor	PowerUser	SuperUser
View Cluster & Alerts	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
View Vdisk Management - Tenant	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
View Vdisk Management - All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Manage Vdisks and Snapshots - Own	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Manage Vdisks and Snapshots - Tenant	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Manage Vdisks and Snapshots - All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Delete Vdisks and Snapshots - Own	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Delete Vdisks and Snapshots - Tenant	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Delete Vdisks and Snapshots - All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Manage Users - Tenant	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Manage Users - All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Manage Roles and Tenants	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
CLI and Log Access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Cluster and VDM Debug Access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 18: Role Management dialog



This section has the following subsections:

- [Hedvig default roles \(SuperUser, PowerUser, Admin, Monitor\)](#)
- [Types of permissions \(Own, Tenant, All\)](#)
- [Permissions for Hedvig default roles](#)
- [Adding custom roles](#)
- [Removing custom roles](#)

## Hedvig default roles (SuperUser, PowerUser, Admin, Monitor)

There are four Hedvig default roles in the Hedvig RBAC system. They cannot be edited or deleted.

- **SuperUser:** A SuperUser role, by default, belongs to the default tenant, *Hedvig*. A SuperUser is similar to a Hedvig Cluster administrator and has all permissions to manage and delete tenants, roles, users, virtual disks, and snapshots. In addition, you can also assign a SuperUser role to another user.
- **PowerUser** (tenant-specific): A PowerUser role is essentially a SuperUser for a specific tenant. This user can manage users and virtual disks for that tenant, and can delete user profiles for users for whom this is the primary (P) tenant. A PowerUser can assign roles only equal to, or below, his or her own permissions.
- **Admin** (tenant-specific): An Admin role has all permissions for managing and deleting virtual disks, but no permissions for managing or deleting users.
- **Monitor** (tenant-specific): A Monitor role can view clusters, view his or her own data, and manage his or her own virtual disks. This role does not have any delete permissions.

**Note:** The only roles that can administer users are the built-in SuperUser and PowerUser roles. All custom roles (that is, roles you have added), as well as the Admin and Monitor roles, can manage only virtual disks, not users.

## Types of permissions (Own, Tenant, All)

There are three types of permissions in the Hedvig RBAC system:

- **User with Own permissions:** With Own permissions, a user can manage and delete tenants, roles, users, virtual disks, and snapshots only for the virtual disks and snapshots *that he or she created*. For example, you could create a custom role to administer your *own* virtual disks.
- **User with Tenant permissions:** With Tenant permissions, a user can manage and delete tenants, roles, users, virtual disks, and snapshots for all virtual disks and users *in the same specific tenant*.
- **User with All permissions:** With All permissions, a user can manage and delete tenants, roles, users, virtual disks, and snapshots for *all virtual disks and users*.

## Permissions for Hedvig default roles

Permission	Admin	Monitor	PowerUser	SuperUser
<b>View cluster &amp; alerts:</b> <ul style="list-style-type: none"> <li>• view Cluster Watch</li> <li>• view cluster and node visualizations</li> <li>• view cluster and node metadata</li> <li>• view alerts</li> <li>• view alert history</li> <li>• view data and metadata nodes</li> <li>• view Hedvig Storage Proxies (controllers)</li> <li>• view cluster metrics</li> <li>• view node activities – Storage Pool Migration, re-replication</li> </ul>	√	√	√	√
<b>View virtual disk management - Tenant</b> <i>(for virtual disks of the same tenant):</i> <ul style="list-style-type: none"> <li>• view virtual disk metadata</li> <li>• view containers</li> <li>• view snapshot information</li> <li>• view clone information</li> <li>• browse NFS</li> </ul>	√		√	√
<b>View virtual disk management - All</b> <i>(for virtual disks of all tenants):</i> <ul style="list-style-type: none"> <li>• view virtual disk metadata</li> <li>• view containers</li> <li>• view snapshot information</li> <li>• view clone information</li> <li>• browse NFS</li> </ul>				√
<b>Manage virtual disks &amp; snapshots – Own</b> <i>(for a user's own virtual disks &amp; snapshots):</i> <ul style="list-style-type: none"> <li>• create and manage virtual disks and snapshots</li> <li>• clone new virtual disks from viewable snapshots</li> <li>• revert viewable virtual disks to snapshot</li> <li>• add tags to virtual disks</li> <li>• add LUN to virtual disks</li> <li>• unmap LUN from virtual disks</li> <li>• mount virtual disks</li> <li>• unmount virtual disks</li> <li>• add export to virtual disks</li> <li>• remove export from virtual disks</li> <li>• resize virtual disks</li> <li>• view virtual disk metrics</li> </ul>	√	√	√	√

Permission	Admin	Monitor	PowerUser	SuperUser
<b>Manage virtual disks &amp; snapshots – Tenant</b> <i>(for virtual disks &amp; snapshots of the same tenant):</i> <ul style="list-style-type: none"> <li>• create and manage virtual disks and snapshots</li> <li>• clone new virtual disks from viewable snapshots</li> <li>• revert viewable virtual disks to snapshot</li> <li>• add tags to virtual disks</li> <li>• add LUN to virtual disks</li> <li>• unmap LUN from virtual disks</li> <li>• mount virtual disks</li> <li>• unmount virtual disks</li> <li>• add export to virtual disks</li> <li>• remove export from virtual disks</li> <li>• resize virtual disks</li> <li>• view virtual disk metrics</li> </ul>	√		√	√
<b>Manage virtual disks and snapshots – All</b> <i>(for virtual disks &amp; snapshots of all tenants):</i> <ul style="list-style-type: none"> <li>• create and manage virtual disks and snapshots</li> <li>• clone new virtual disks from viewable snapshots</li> <li>• revert viewable virtual disks to snapshot</li> <li>• add tags to virtual disks</li> <li>• add LUN to virtual disks</li> <li>• unmap LUN from virtual disks</li> <li>• mount virtual disks</li> <li>• unmount virtual disks</li> <li>• add export to virtual disks</li> <li>• remove export from virtual disks</li> <li>• resize virtual disks</li> <li>• view virtual disk metrics</li> </ul>				√
<b>Delete virtual disks and snapshots - Own</b> <i>(for a user's own virtual disks &amp; snapshots):</i> <ul style="list-style-type: none"> <li>• delete virtual disks</li> <li>• delete snapshots</li> </ul>	√		√	√
<b>Delete virtual disks and snapshots - Tenant</b> <i>(for virtual disks &amp; snapshots of same tenant):</i> <ul style="list-style-type: none"> <li>• delete virtual disks</li> <li>• delete snapshots</li> </ul>	√		√	√
<b>Delete virtual disks and snapshots – All</b> <i>(for virtual disks &amp; snapshots of all tenants):</i> <ul style="list-style-type: none"> <li>• delete virtual disks</li> <li>• delete snapshots</li> </ul>				√
<b>Manage users – Tenant</b> <i>(for users of the same tenant):</i> <ul style="list-style-type: none"> <li>• view user management</li> <li>• view activity log for viewable users</li> <li>• add users to viewable tenants</li> <li>• delete users</li> <li>• modify display name</li> <li>• modify email</li> <li>• modify mobile phone</li> <li>• modify inactivity timeout</li> <li>• modify password</li> </ul>			√	√
<b>Manage users – All</b> <i>(for users of all tenants):</i> <ul style="list-style-type: none"> <li>• delete users</li> <li>• modify display name</li> <li>• modify email</li> <li>• modify mobile phone</li> <li>• modify inactivity timeout</li> <li>• modify password</li> </ul>				√
<b>Manage roles &amp; tenants:</b> <ul style="list-style-type: none"> <li>• create tenants</li> <li>• create role types</li> <li>• delete role types</li> <li>• change role permissions</li> <li>• assign tenant for all users</li> <li>• assign role for all users</li> </ul>				√
<b>CLI &amp; log access:</b> <ul style="list-style-type: none"> <li>• access the Hedvig CLI through the Hedvig WebUI</li> <li>• view logs through Virtual Console</li> </ul>				√
<b>Cluster &amp; VDM debug access:</b> <ul style="list-style-type: none"> <li>• view debug data and commands for viewable virtual disks</li> </ul>				√

## Adding custom roles

A SuperUser can add a custom role to any tenant, including the default tenant, *Hedvig*.

To add a new role:

1. Select **Add Role** to the right of **User Administration -> Role Management**.
2. In the **Add Role** dialog, enter the **New Role Name**.



Figure 19: Add Role dialog

3. To use the same permissions as another role, select **Copy Permissions From Role**, and you will be prompted to select that role.
4. Select **Run**.
5. Back on the main **Role Management** page, notice that the new custom role has been added to the table.
6. Select the desired permissions for this role. Notice that if you select a permission, other permissions that are *inherently* part of that permission will also be applied.
7. Select **Save** to save *all* the permissions for this new role.

## Example of adding custom roles

An example of adding custom roles is shown in *Figure 19: Role Management dialog - Setting up a custom role.*

**Note:** When the *Manage Vdisks and Snapshots - Tenant* permission is selected, both the *Manage Vdisks and Snapshots - Own* and the *View Vdisk Management - Tenant* permissions are also automatically selected, because they are basically subsets of the selected permission.

Permissions	Admin	Monitor	PowerUser	SuperUser	customrole
View Cluster & Alerts	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
View Vdisk Management - Tenant	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
View Vdisk Management - All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Manage Vdisks and Snapshots - Own	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Manage Vdisks and Snapshots - Tenant	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Manage Vdisks and Snapshots - All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Delete Vdisks and Snapshots - Own	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Delete Vdisks and Snapshots - Tenant	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Delete Vdisks and Snapshots - All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Manage Users - Tenant	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Manage Users - All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Manage Roles and Tenants	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
CLI and Log Access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Cluster and VDM Debug Access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Configuration	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Figure 20: Role Management dialog - Setting up a custom role

## Removing custom roles

A SuperUser can remove a custom role, but cannot remove any of the Hedvig default roles.

To remove a custom role, select **Remove Role** to the right of **Add Role**. Then, select the role you wish to remove.

The **Remove Role** dialog gives you an opportunity to confirm the deletion of the selected role. Select **Run** if you are sure you want to remove the role.

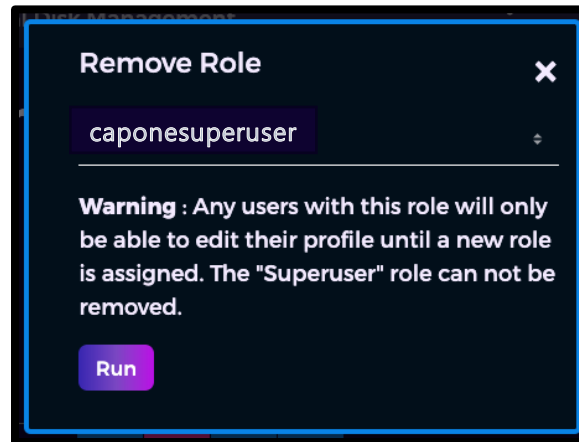


Figure 21: Remove Role dialog

# Tenant Management

Selecting **User Management -> Tenant Management** lets you add tenants, add users to tenants, remove tenants, and manage roles.



Figure 22: Tenant Management dialog

This section has the following subsections:

- [Adding a tenant](#)
- [Working with a specific tenant](#)

## Adding a tenant

To add a tenant, select **Add Tenant** under **Tenant Management**. Enter the **Name**, and select **Run**.

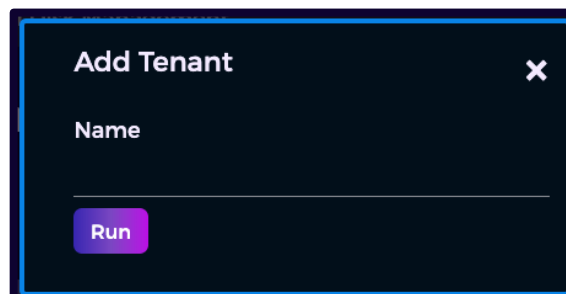


Figure 23: Add Tenant dialog

## Working with a specific tenant



- **Show Users** - see [Showing the users of a tenant](#)
- **Resize** - To resize a tenant, see: [https://documentation.commvault.com/cds/126292\\_configuring\\_tenant\\_upper\\_quota\\_limit.html](https://documentation.commvault.com/cds/126292_configuring_tenant_upper_quota_limit.html)
- **Remove** - see [Removing a tenant](#)
- **Add Users** - see [Adding a user to a tenant](#)
- **Manage Roles** - see [Role Management](#)

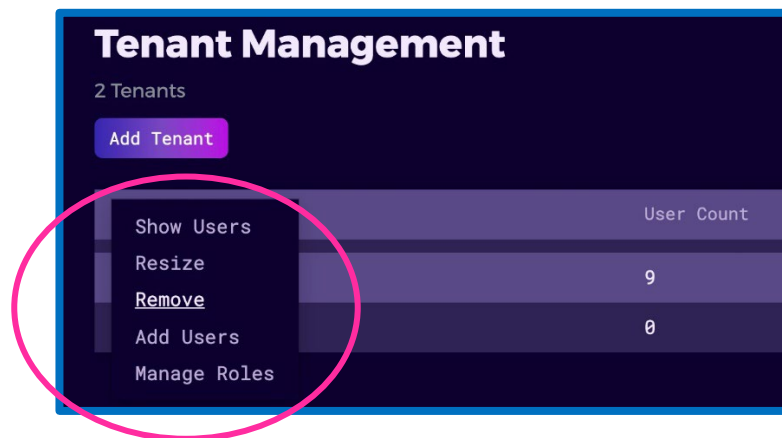


Figure 24: Tenant Management dialog - Tenant tasks

## Showing the users of a tenant

To see all the users, and their corresponding roles, of a specified tenant, select **Show Users**. The **Tenant Users** dialog is displayed.

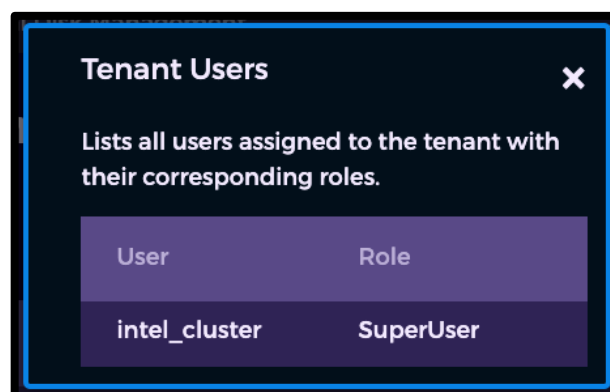


Figure 25: Tenant Users dialog



## Removing a tenant

Only a SuperUser can remove a tenant, and that tenant must not have any users.

To remove a tenant, select **Remove**. The **Remove Tenant** dialog gives you an opportunity to confirm the deletion of the selected tenant. Select **Run** if you are sure you want to remove the tenant.



Figure 26: Remove Tenant dialog

## Adding a user to a tenant

To add a user(s) to a tenant, select **Add Users**.

Select the **Users** (you can select one or more) and the **Role**, and select **Run**.

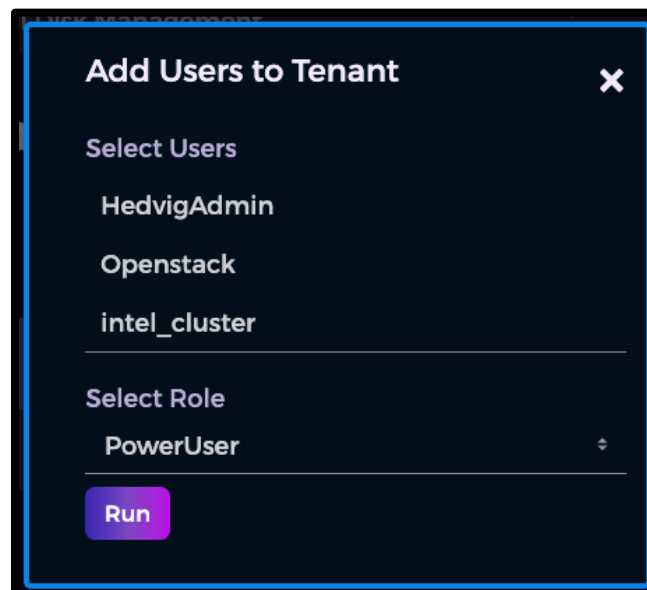


Figure 27: Add Users to Tenant dialog

# Edit Profile

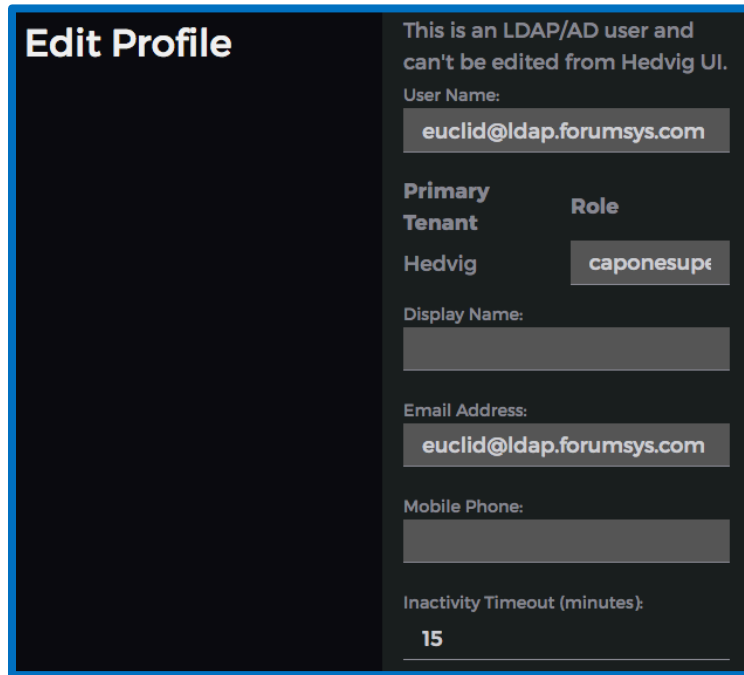
Edit Profile lets you change the stored information for a specified user, depending on where you launch it, your role, and the type of user:

- When you launch this dialog from **User Administration > Edit Profile**, you will be editing the profile of the user name under which you logged in.
- When you launch this dialog from **User Administration > User Management > “...” for user > Edit User**, you will be editing the profile of the user you selected on the **User Management** page.
- If you are a SuperUser, you can change the **password** and the **Inactivity Timeout**.

Primary Tenant	Role
Hedvig	SuperUser

Figure 28: Edit Profile dialog

- If you have selected an LDAP user, you can edit only the **Inactivity Timeout** in the Hedvig WebUI. All other fields must be changed using your LDAP server.



**Edit Profile**

This is an LDAP/AD user and can't be edited from Hedvig UI.

User Name:  
euclid@ldap.forumsys.com

Primary Tenant	Role
Hedvig	caponesup€

Display Name:  
[Empty field]

Email Address:  
euclid@ldap.forumsys.com

Mobile Phone:  
[Empty field]

Inactivity Timeout (minutes):  
**15**

Figure 29: Edit Profile dialog - LDAP/AD user message

## Appendix A: Connecting/editing preconfigured LDAP/AD server

To connect or edit a preconfigured LDAP/AD server to the Hedvig WebUI, select **LDAP/AD Configuration** from the **Configuration** entry on the **User** menu in the Hedvig WebUI.

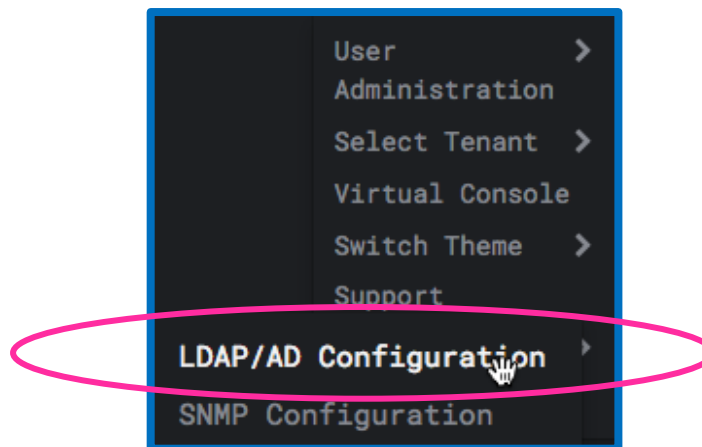


Figure 30: User menu - LDAP/AD Configuration

In the **LDAP/AD Configuration** dialog (shown on the next page), complete the information as desired, and select **Save Changes** when done.

## LDAP/AD Configuration

Tenant: ▾  
Hedvig

---

Server : ▾  
Configure New Server/Dor

*Each tenant/server pair allows to set up a separate LDAP configuration.*

Use Domain Name

Server: \_\_\_\_\_

Port: \_\_\_\_\_

Use SSL

Naming Attribute: \_\_\_\_\_

Admin Distinguished Name: \_\_\_\_\_

Admin Password: \_\_\_\_\_  
\*\*\*\*\*

User Search Base: \_\_\_\_\_

User Search Filter: \_\_\_\_\_

Group Search Base: \_\_\_\_\_

Group Search Filter: \_\_\_\_\_

Group Member Attribute: \_\_\_\_\_

### User Attribute Names

*Customize LDAP/AD attributes for users.*

Display Name: \_\_\_\_\_

Email: \_\_\_\_\_

Mobile: \_\_\_\_\_

[Configure Group/Role Mapping](#)

*You'll be able to configure Group/Role mapping after saving this configuration.*

Copy/Paste configuration

[Save Changes](#)

Figure 31: LDAP/AD Configuration dialog

**LDAP/AD Configuration:**

- **Tenant:** You can set up a separate LDAP/AD configuration for each tenant/server pair.
- **Server:** Select an existing server, or select **Configure New Server/Domain Name**.
- **Use Domain Name:** Select this when you want to use a **Domain Name**, rather than a server port.
- **Server:** Displays the name of the existing server you selected, or is blank to enter a new server name.
- **Port:** Enter a port number for a new server, or, if needed, change the port number for an existing server. The default for LDAP is 389 and for LDAPS (LDAP over SSL) is 636.
- **Use SSL:** To enable LDAP over SSL (LDAPS).
- **Naming Attribute:** The attribute that is used to identify a user in LDAP.
- **Admin Distinguished Name:** The distinguished name (DN) of the admin account.
- **Admin Password:** The password of the admin account.
- **User Search Base:** The base used to search for users.
- **User Search Filter:** The filter used to search for users.
- **Group Search Base:** The base used to search for groups.
- **Group Search Filter:** The filter used to search for groups.
- **Group Member Attribute:** The attribute name for specifying group members.
- **User Attribute Names:** To customize LDAP/AD attributes:
  - **Display Name:** The LDAP attribute for a user's Display Name.
  - **Email:** The LDAP attribute for a user's email address.
  - **Mobile:** The LDAP attribute for a user's mobile phone number.

**LDAP/AD Configuration (continued):**

- **Configure Group/Role Mapping** brings up the **Group/Role Mapping** dialog, in which you can add more groups and roles. You can also use the **Filter** function to select only certain groups. Note that the default role for groups is **Not Mapped**.



Figure 32: Group/Role Mapping dialog

- **Copy/Paste configuration:** To copy a configuration to a clipboard or to paste it from a clipboard.
- **Delete Server:** To delete this LDAP/AD server from this tenant's configuration.
- **Save Changes:** To save the changes you have made for this tenant/server combination.

# Appendix B: Glossary

Table 3: Glossary of terms

term	definition
<b>AD</b>	Microsoft <i>Active Directory</i> is a directory service developed for Windows domain networks. Active Directory uses LDAP versions 2 and 3, Microsoft's version of Kerberos, and DNS.
<b>CHAP</b>	The <i>Challenge-Handshake Authentication Protocol</i> authenticates a user or network host to an authenticating entity.
<b>CN</b>	The <i>Common-Name</i> attribute represents an object and is used to perform searches in LDAP.
<b>DC</b>	<i>Domain Component</i> objects represent the top of an LDAP tree that uses DNS to define its namespace.
<b>DN</b>	A <i>distinguished name</i> includes an object's entire path to the root of the LDAP namespace.
<b>DNS</b>	The <i>domain name system</i> is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network.
<b>Hedvig Storage Cluster</b>	A <i>Hedvig Storage Cluster</i> is an elastic cluster, formed by using any type of commodity server(s).
<b>Hedvig Storage Cluster Node</b>	A <i>Hedvig Storage Cluster Node</i> is an individual commodity server running <i>Hedvig Storage Service</i> software.
<b>Hedvig Storage Pool</b>	A <i>Hedvig Storage Pool</i> is a logical grouping of multiple physical disks that are presented as a single entity.
<b>Hedvig Storage Proxy</b>	A <i>Hedvig Storage Proxy</i> is a lightweight software component that deploys at the application tier as a VM or Docker container, or on bare metal, to provide storage access to any physical host or virtual machine in the application tier. The storage proxy presents block, file, and object storage access to app hosts, accelerates read performance with flash caching, drives efficiency with deduplication, and secures data with encryption.
<b>inode</b>	An <i>inode</i> is a data structure used to represent a file system object, which can be one of various things including a file or a directory.



term	definition
<b>LDAP</b>	The <i>Lightweight Directory Access Protocol</i> is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an IP network.
<b>multitenancy</b>	<i>Multitenancy</i> is an architecture in which a single instance of software runs on a server and serves multiple tenants. In multitenancy, every tenant is provided a dedicated share of the instance - including its data, configuration, user management, tenant individual functionality, etc.
<b>primary tenant</b>	The first time a user is added to a Hedvig Cluster, the tenant to which they are added is their <i>primary tenant</i> .
<b>RAID</b>	<i>Redundant array of independent disks</i> is a data storage virtualization technology that combines multiple physical disk drive components into a single logical unit for the purposes of data redundancy, performance improvement, or both.
<b>RBAC</b>	<i>Role-based access control</i> is an approach to restricting system access to authorized users.
<b>SSL</b>	<i>Secure Sockets Layer</i> is a cryptographic protocol that provides communications security over a computer network.
<b>tenant</b>	A <i>tenant</i> is a group of users who share a common access with specific privileges to a software instance.
<b>virtual disk</b>	A <i>virtual disk</i> is an abstracted logical disk volume presented to a computer or application for read/write use.
<b>VM</b>	A <i>virtual machine</i> is a software computer that, like a physical computer, runs an operating system and applications.

Commvault Systems, Inc., believes the information in this publication is accurate as of its publication date. The information is subject to change without notice. The information in this publication is provided as is. Commvault Systems, Inc., makes no representations or warranties of any kind with respect to the information in this publication and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any Commvault Systems, Inc., software described in this publication requires an applicable software license. All trademarks are the property of their respective owners. Revision date: 020822.

Software-defined AES-256, FIPS compliant encryption of data in flight and at rest.