

# Access Provisioning

Unizin Data Warehouse (UDW) is a **full-service product**. To provision access for a new user, a [Member's UDW Sponsor team](#) must submit a [Support Ticket](#) with the necessary information (see below).

## Security measures

Unizin applies a number of security measures to user access to each Member's UDW. The following measures are taken for all new user access to an UDW:

1. An Institution's UDW [Sponsor Team](#) must submit UDW access.
2. Usernames and passwords are randomly generated strings.
3. An IP Whitelist filters traffic to Member UDWs.

During UDW implementation, Members identify individuals who constitute the UDW [Sponsor team](#). Sponsor team members "own" the UDW service at their institution and submit requests for access provisioning on their users' behalf.

## User provisioning process

Sponsor team members at a Member institution may request access to their UDW for themselves or for non-Sponsor team individuals.

If a non-Sponsor team individual requests access to their UDW, Unizin will refer that individual back to the Sponsor team.

All requests for access submitted via a [Support Ticket](#) must include:

- For Individual Access:
  - Full name and email address of the individual whose access Unizin will provision.
- For Application Access:
  - If the account is for another application to access the UDW, include the name or a description of the application.
  - The name and email address of the primary contact for that application.

Personal information for the user allows for tracking of user accounts for later de-provisioning.

When access for the user is approved, Unizin Support will send the requestor a set of credentials that can be downloaded a single time from a generated URL. This URL may be forwarded to the user if desired.

## IP whitelisting process

During an implementation of the UDW, a Member will provide a set of IP address ranges to whitelist. If this set needs to be modified at any time, a Sponsor team member may submit a [Support Ticket](#).

All requests for IP whitelisting changes must include:

- IP range in [CIDR](#) format.
- An indication if the IP range should be whitelisted or removed from the whitelist.

When the IP whitelisting change has occurred, Unizin Support will send the requestor a confirmation.