Manage User Access And Security

There are two ways to create and manage user accounts and user authentication credentials: create and manage user accounts in AtScale's local directory service, or configure AtScale to authenticate users via an external directory service.

> **Restriction:** Use AtScale's local directory service for testing only. Do not use it in production environments. This directory service is not meant to support the types of workloads that are common to production environments. Before using AtScale in production, configure your AtScale organization to use an external directory service, such as Microsoft Active Directory, another LDAP service, or Google G Suite Directory.

Users and authentication settings are configured per organization in AtScale. A user must be assigned a role in an organization in order to be a member of an organization.

Only AtScale super users and organization administrators can manage users and authentication preferences in AtScale. AtScale recommends creating user accounts for each person who needs access to AtScale.

AtScale ships with an embedded directory service, which is the initial directory service configured for the default organization. If you use AtScale with its default configuration, you can create and delete users in the Design Center, and the users are automatically synchronized with the embedded directory service.

If you configure AtScale to use an external directory service (such as LDAP or Microsoft Active Directory), you administer users in your directory service tools, not in AtScale. Users are then synchronized on demand, or whenever they successfully authenticate to AtScale. You can map directory groups to AtScale roles and groups so that users are assigned the appropriate permissions in AtScale. Supported external directory services are Google G Suite Directory, LDAP servers, and Microsoft Active Directory.

> **Attention:** When you are administering user access and security for an AtScale cluster, you must use an external directory service.

A user must be assigned a role in an organization in order to access AtScale. A role grants system-level permissions to a user and controls what they can do in the AtScale application. Every organization should have at least one user who is a member of the Organization Admin role (this makes the user a super user within that organization only).

Users can also be organized into groups for the purpose of assigning runtime (query access) permissions to AtScale projects and cubes. Users, roles, and groups are configured per organization. Each organization can also be configured to use a different directory service to authenticate users if needed.