Manage User Access and Security

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

Restriction: Use AtScale's local directory service for testing only. Do not use it in production environments service is not meant to support the types of workloads that are common to production environments. Bef AtScale in production, configure your AtScale organization to use an external directory service, such as M 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 *r* organization in order to be a member of an organization.

Only AtScale super users and organization administrators can manage users and authentication preferenc 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 organization. If you use AtScale with its default configuration, you can create and delete users in the Des 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), users in your directory service tools, not in AtScale. Users are then synchronized on demand, or whenever successfully authenticate to AtScale. You can map directory groups to AtScale roles and groups so that us the appropriate permissions in AtScale. Supported external directory services are Google G Suite Director and Microsoft Active Directory.

Attention: When you are administering user access and security for an AtScale cluster, you must use an e service.

A user must be assigned a *role* in an organization in order to access AtScale. A role grants system-level p user and controls what they can do in the AtScale application. Every organization should have at least on 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 t projects and cubes. Users, roles, and groups are configured *per organization*. Each organization can also b use a different directory service to authenticate users if needed.