Using External Authentication

Every organization in AtScale requires a directory service for managing AtScale users. For evaluation purposes AtScale uses its own embedded directory service. However, production installations must use an external directory service. To manage user authentication through an external directory service, you need to:

- Configure AtScale to connect to the external directory, like LDAP server, Azure Active Directory, or Google's G Suite Directory
- Assign AtScale roles to directory groups, grant runtime permissions on cubes to directory groups, and synchronize the user accounts to AtScale.
- Disable user management in AtScale. When managing users in AtScale you cannot write to external directory services.

Before You Start

Note the following:

- 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.

- When you are administering user access and security for an AtScale cluster, you must use an external directory service.

More Information

- Connecting to an LDAP Server or Microsoft Active Directory and Azure AD
- Connecting to AtScale Using Windows Authentication
- Connecting to Active Directory that uses LDAP Channel Binding
- Connecting to Okta Using OAuth 2.0
- Connecting to Auth0
- Connecting to Azure Active Directory
- Connecting to Google G Suite Directory
- Assigning Roles to Directory Groups
- Granting Runtime Permission on Cubes to Groups of Externally-Authenticated Users
- Setting Up Impersonation of Data Warehouse Accounts by Directory Groups
- Setting Up Impersonation for Google BigQuery
- Bulk Synchronization of User Accounts to AtScale