LDAP Active Directory

This guide assumes you already have a forest/domain configured and that your environment is properly secured.

This is a basic configuration. You may want to set additional options or permissions in your forest/domain.

See also Delegated Authentication for single sign-on (SSO) integration.

Setup

To enable authentication with LDAP and Active Directory, the following needs to be done:

- Configure secure LDAP in your domain.
- Create a user and optionally an UO to use for LDAP authentication.

Configure Your EMS Server

- Set up an Element Cloud Enterprise server.
- Click the Integrations tab.
- Select LDAP from the list of available Advanced Authentication methods.
- Set the following configuration parameters:

```
Bind URI: ldaps://ldap.example.com:636
Base: OU=matrix,DC=example,DC=com
Bind DN: CN=emsadmin,CN=Users,DC=example,DD=com
Bind Password: supersecret
UID: SamAccountName
Display Name: See below
Email: mail
```

- For Display Name, you have a few options based on your preference. For example:
  - displayName
  - GivenName
  - Name
  - sn
- For a full list, open PowerShell on your domain controller and enter

```
Import-Module ActiveDirectory
Get-ADUser test_user -Properties *
```

- Save your LDAP settings and wait for your EMS server to reprovision.
- Authentication in Element should now be working. If not, please look in the logs for your firewall or domain controllers or contact EMS support from our support form

---

Revision #3
Created 18 April 2022 14:19:51 by Karl Abbott
Updated 4 May 2023 14:44:39 by Twilight Sparkle