Usage Scenarios

Usage Scenarios

With LDAP bridge as an example data source.

Onboarding

- User logs in to Element, either using OpenID or with a user+password with LDAP integration
- User automatically gets invited to spaces matching their LDAP Organizational Unit memberships, which are nested the way they are nested in LDAP
- For each space they're in, user gets invited to every room that's configured to be joinable by space members
- **Result**: user learns their place in the company structure, discovers their peers and becomes aware of all the public conversations happening in the company

For the following sections, we assume a hierarchy of LDAP Organizational Units:

- Employees
  - Engineering
  - Support

Restructuring

- In the previously described OrgUnit hierarchy, assume a user Evan belonging to Engineering
- Evan is being moved from Engineering to the more generic Employees
- GS kicks evan from the Engineering space and from all the public rooms in it
- Evan is added to the Support OrgUnit
- GS invites Evan to the Support Matrix space and all its space-public rooms
- **Result**: Moving users around within the company hierarchy is represented by moving them around in the Matrix space.

Offboarding

- In the previously described OrgUnit hierarchy, assume a user Evan belonging to Engineering
- Evan is being removed from LDAP entirely, or moved outside of Employees, which is the root space managed by GS
- Evan's Matrix account is being deactivated, preventing them from logging in.

- Evan is subject to the user deletion flow.
- **Result**: GS will automatically erase a user from Matrix if they no longer belong to the LDAP space managed by it.

Permission management

- GS is configured to assign a power level of 50 to every user in groups called moderators or engineering-moderators
- In the previously described OrgUnit hierarchy, we have users Evan and Brenda belonging to Engineering (and therefore also to Employees).
- We create two LDAP Security Groups: moderators in Employees and engineering-moderators in Engineering
- We make Evan a member of moderators, and Brenda a member of engineering-moderators
- GS assigns a power level of 50 to Evan in the Employees Matrix space and all rooms contained within it – except its subspaces (including Engineering) where Evan's power level is still the default 0
- GS assigns a power level of 50 to Brenda in the Engineering and all its child rooms. Brenda still has a default power level of 0 in Employees
- The spaces managed by GS allow its moderators (PL 50) to create child rooms and spaces
- **Result**: LDAP Security Groups can be used to manage Matrix power levels in a granular and configurable manner

LDAP as a source of truth

- In a space hierarchy managed by GS, a user acquires a power level higher than the one described in their LDAP security group
- In response to that, GS demotes the user back to the power level that they should have according to LDAP. If the user is currently an Admin, GS will temporarily take over their account and make them demote themselves.
- A user, for any reason, ends up in a room that they shouldn't be in – for example, a room they were a member of now becomes a part of the company Space.
- In response to that, GS immediately kicks them from the room they weren't supposed to be in.
- **Result**: LDAP is the source of truth, and any changes in Matrix that don't conform to the rules established in LDAP get automatically corrected.

Revision #2
Created 2025-05-15 09:24:23 UTC by Gaël Goinvic
Updated 2025-05-27 13:12:00 UTC by Gaël Goinvic