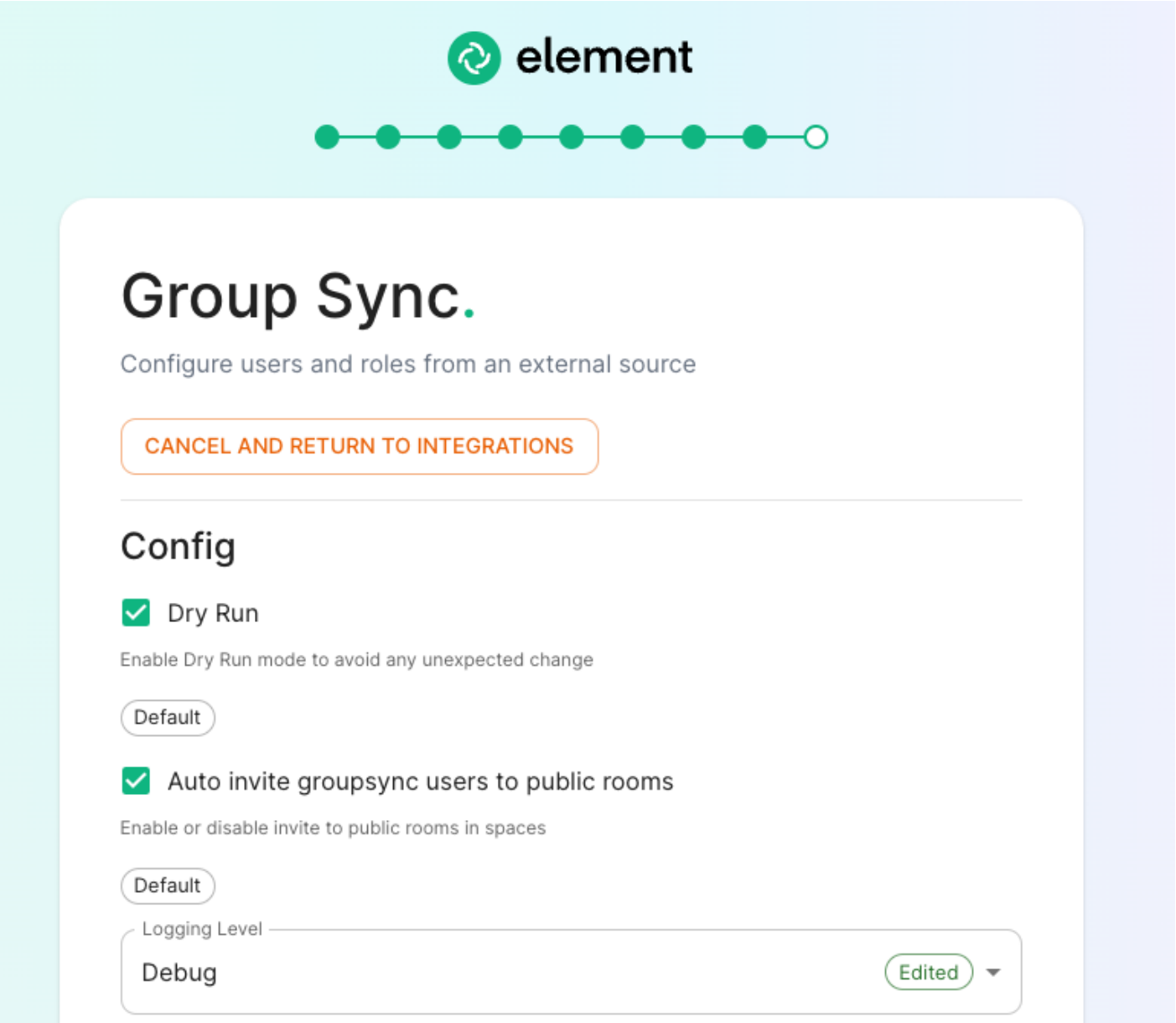
Setting up Group Sync with the Installer

What is Group Sync?

Group Sync allows you to use the ACLs from your identity infrastructure in order to set up permissions on Spaces and Rooms in the Element Ecosystem. Please note that the initial version we are providing only supports a single node, non-federated configuration.

Configuring Group Sync

From the Installer's Integrations page, click "Install" under "Group Sync".



- Leaving `Dry Run` checked in combination with `Logging Level` set to `Debug` gives you the ability to visualize in the pod's log file what result group sync will produce without effectively creating spaces and potentially corrupting your database. Otherwise, uncheck `Dry Run` to create spaces according to your spaces mappings defined in the `Space mapping` section.
- `Auto invite groupsync users to public room` determines whether users will be automatically invited to rooms (default, public and space-joinable). Users will still get invited to spaces regardless of this setting.

Configuring the source

LDAP Servers

- You should create a LDAP account with read access.
- This account should use password authentication.

Select source

(•) LDAP ( ) Azure (MSGraph) ( ) SCIM

LDAP

Mapping attribute for room name

name

The LDAP attribute to request space names

Mapping attribute for username

sAMAccountName

The LDAP attribute to requiest user id

LDAP Base DN

OU=Demo corp,DC=olivier,DC=sales-demos,DC=element,DC=io

The LDAP base DN

LDAP Bind DN

CN=gsync,CN=Users,DC=olivier,DC=sales-demos,DC=element,DC=i

The LDAP bind DN

Check interval in seconds

60 Default

the ldap check in seconds

LDAP Filter

An additional ldap filter

LDAP URI

ldap://3.75.187.130

The LDAP URI groupsync will use to request users

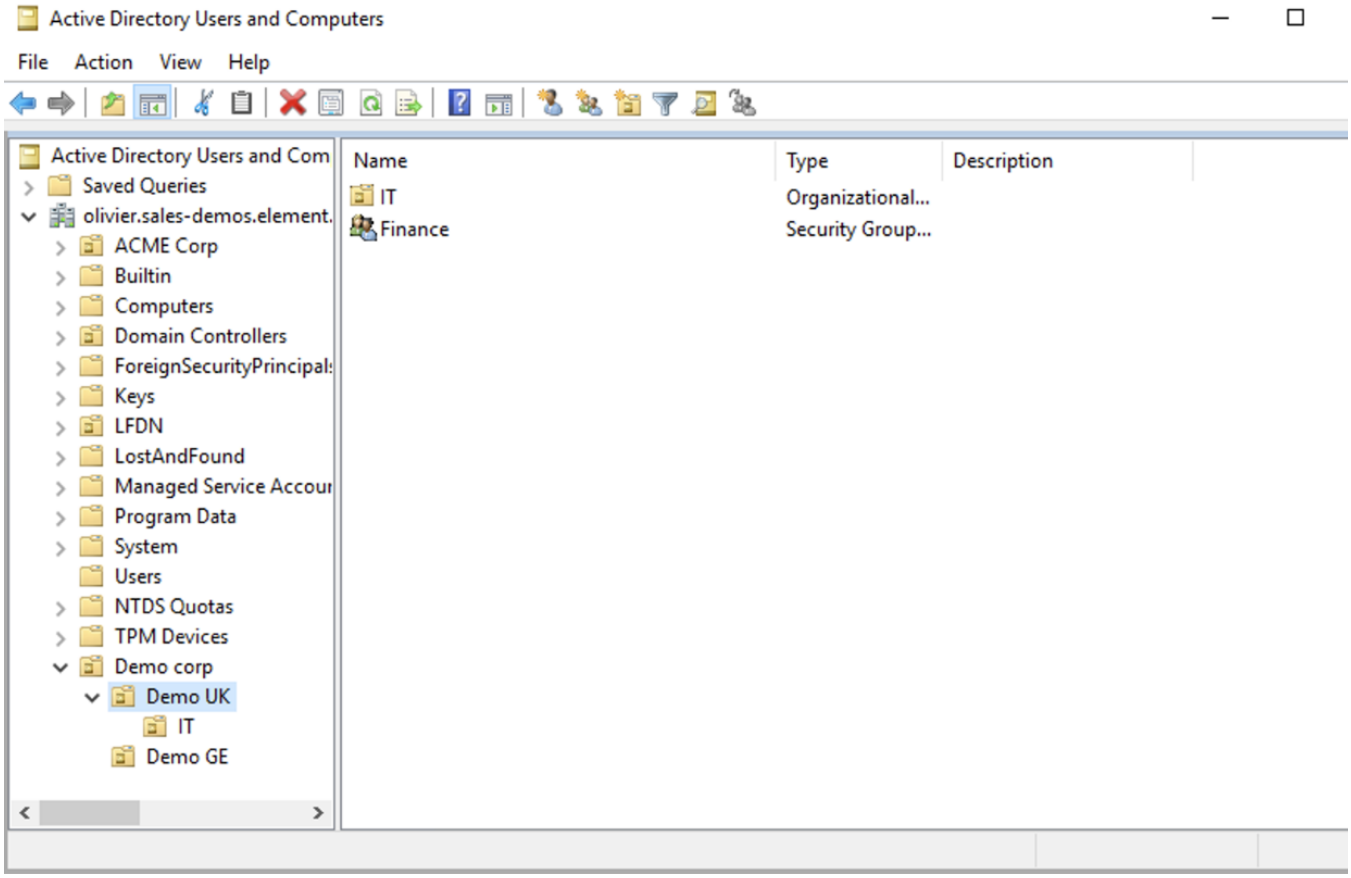
Secrets / Group Sync / LDAP Bind Password

LDAP Password

••••••••••••

LDAP Bind password

- `LDAP Base DN`: the distinguished name of the root level Org Unit in your LDAP directory. In our example, `Demo Corp` is our root level, spaces are mapped against Org Units , but you can map a space against any object (groups, security groups,..) belonging to this root level. **The root level must contain all the Users, Groups and OUs used in the space mapping.**



The distinguished name can be displayed by selecting `View` / `Advanced Features` in the Active Directory console and then, right-clicking on the object, selecting `Properties` / `Attributes Editor`.

The DN is `OU=Demo corp,DC=olivier,DC=sales-demos,DC=element,DC=io`.

- `Mapping attribute for room name`: LDAP attribute used to give an internal ID to the space (visible when setting the log in debug mode)
- `Mapping attribute for username`: LDAP attribute like `sAMAccountName` used to map the localpart of the mxid against the value of this attribute.
  If `@bob:my-domain.org` is the mxid, `bob` is the localpart and groupsync expects to match this value in the LDAP attribute `sAMAccountName`.
- `LDAP Bind DN`: the distinguished name of the LDAP account with read access.
- `Check interval in seconds`: the frequency Group sync refreshes the space mapping in Element.
- `LDAP Filter`: an LDAP filter to filter out objects under the LDAP Base DN. **The filter must be able to capture Users, Groups and OUs used in the space mapping.**
- `LDAP URI`: the URI of your LDAP server.
- `LDAP Bind Password`: the password of the LDAP account with read access.

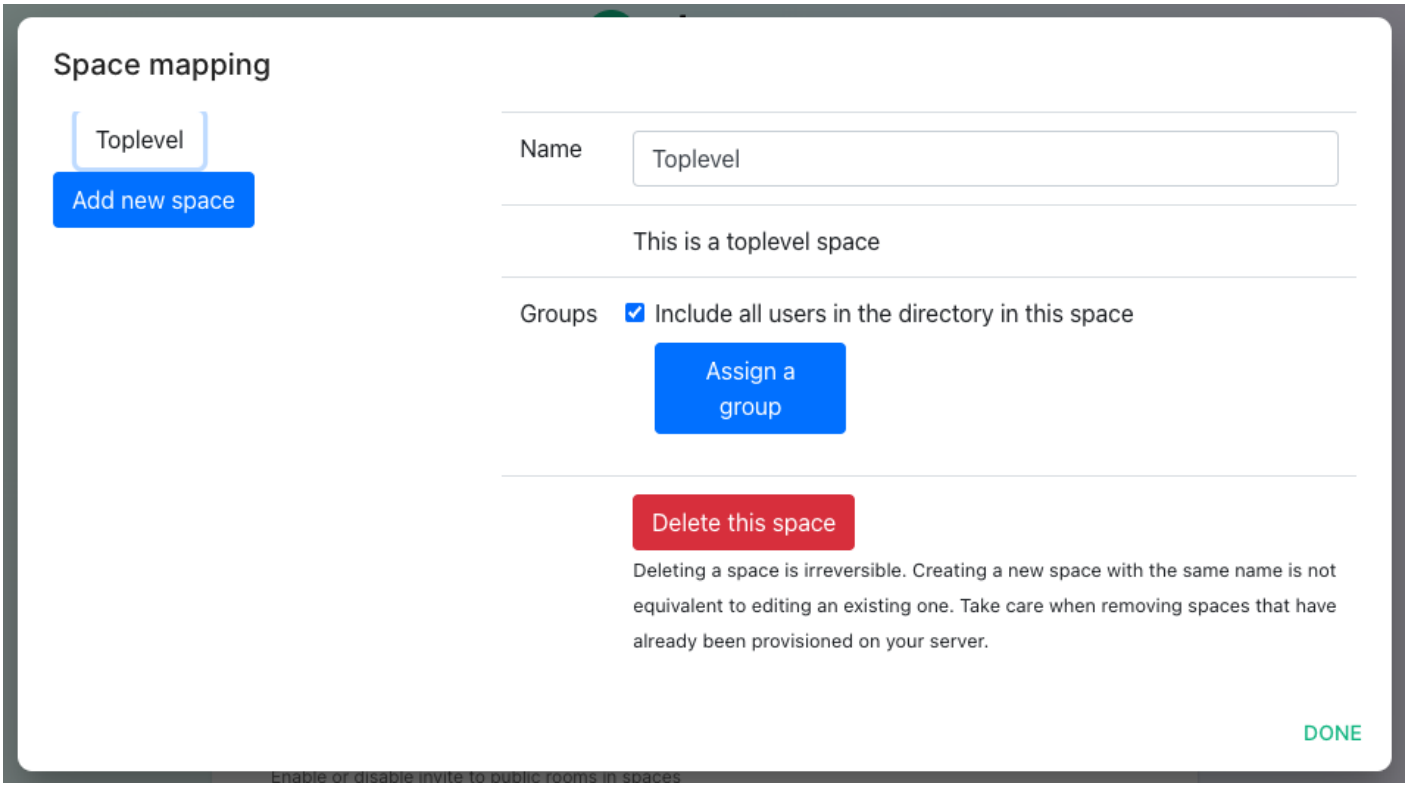
MS Graph (Azure AD)

- You need to create an `App registration`. You'll need the `Tenant ID` of the organization, the `Application (client ID)` and a secret generated from `Certificates & secrets` on the app.
- For the bridge to be able to operate correctly, navigate to API permissions and ensure it has access to Group.Read.All, GroupMember.Read.All and User.Read.All. Ensure that these are Application permissions (rather than Delegated).
- Remember to grant the admin consent for those.
- To use MSGraph source, select MSGraph as your source.
  - `msgraph_tenant_id`: This is the "Tenant ID" from your Azure Active Directory Overview
  - `msgraph_client_id`: Register your app in "App registrations". This will be its "Application (client) ID"
  - `msgraph_client_secret` : Go to "Certificates & secrets", and click on "New client secret". This will be the "Value" of the created secret (not the "Secret ID").

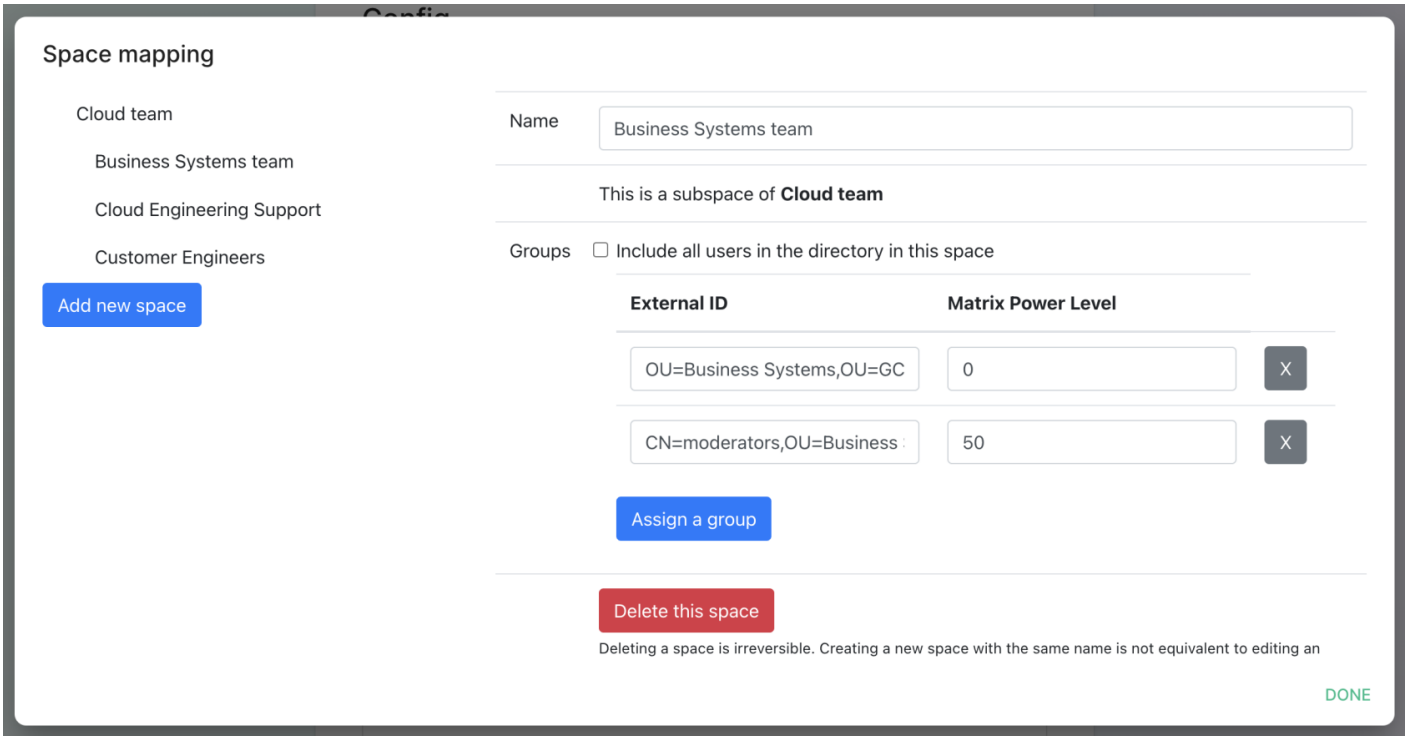
Space Mapping

The space mapping mechanism allows us to configure spaces that Group Sync will maintain, beyond the ones that you can create manually.

It is optional – the configuration can be skipped but if you enable Group Sync, you have to edit the Space mapping by clicking on the `EDIT` button and rename the `(unnamed space)` to something meaningful.



`Include all users in the directory in this space`: all available users, regardless of group memberships join the space. This option is convenient when creating a common subspace shared between all users.



When clicking on `Add new space`, you can leave the space as a top level space or you can drag and drop this space onto an existing space, making this space a subspace of the existing space.

You can then map an external ID (the LDAP distinguished name) against a power level. Every user belonging to this external ID is granted the power level set in the interface. This external ID that can be any LDAP object like an OrgUnit, a Group or a Security Group. **The external ID is case-sensitive**

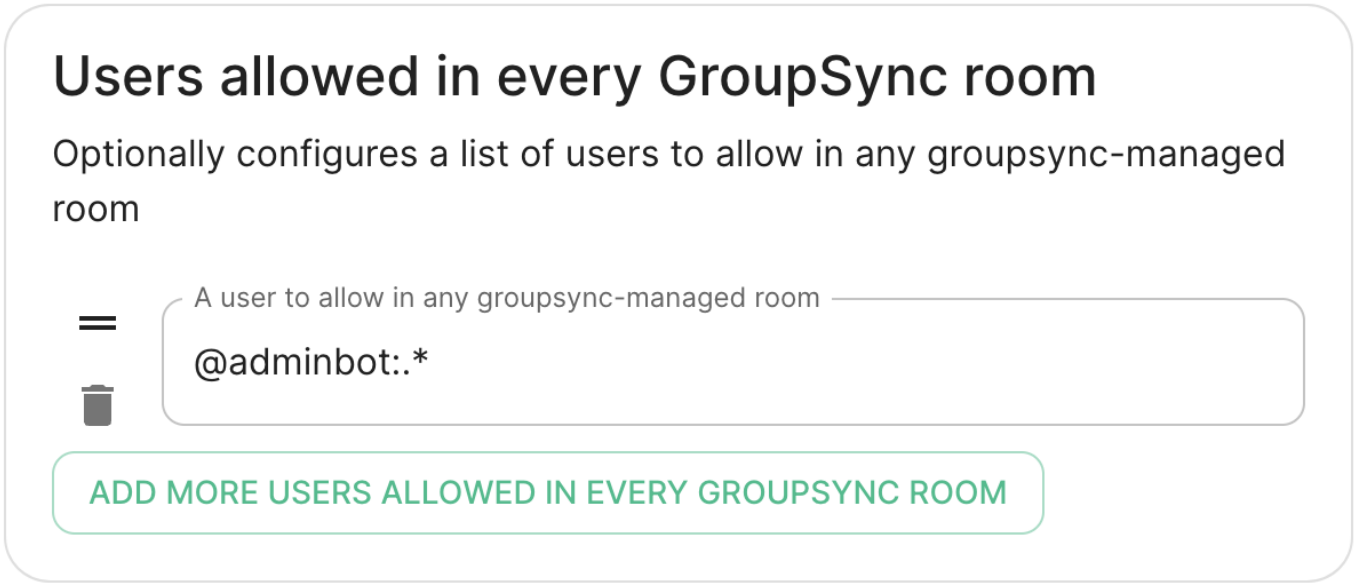
A power level 0 is a default user that can write messages, react to messages and delete his own messages.

A power level 50 is a moderator that can creates rooms, delete messages from members.

A power level 100 is an administrator but since GroupSync manages spaces, invitations to the rooms, it does not make sense to map a group against a power level 100.

Custom power levels other than 0 and 50 are not supported yet.

Users allowed in every GroupSync room

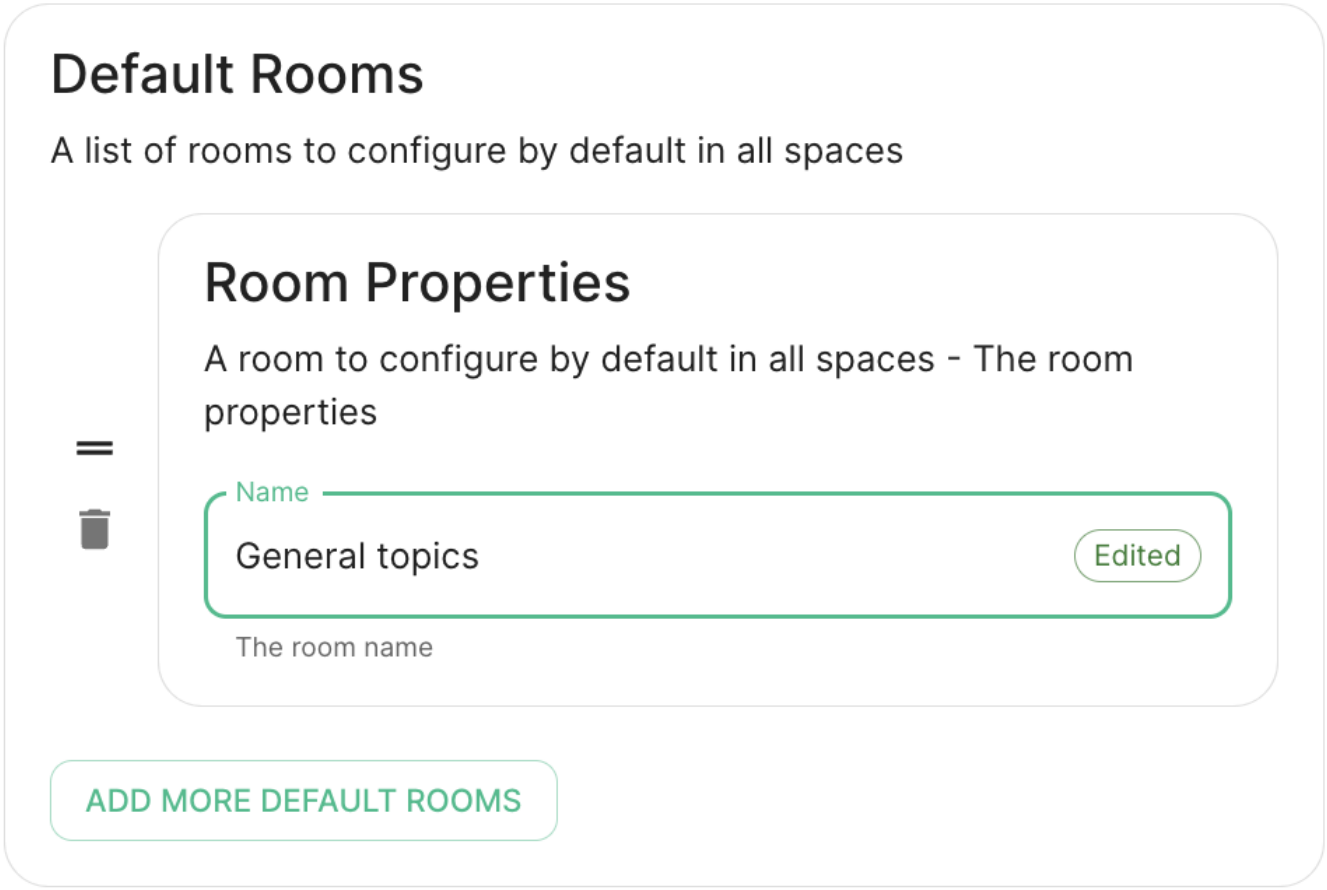


A list of userid patterns that will not get kicked from rooms even if they don't belong to them according to LDAP.

This is useful for things like auditbot if Audibot has been enabled.

Patterns listed here will be wrapped in ^ and $ before matching.

Defaults Rooms



A list of rooms added to every space

H

Revision #3
Created 2024-11-06 10:22:24 UTC by Kieran Mitchell Lane
Updated 2024-11-06 13:22:29 UTC by Kieran Mitchell Lane