

1. deletion

cannot delete users in both AD & Authentik.

- if only deleted in authentik on next sync the deleted user created because it still remains in LDAP.

2.unique names

both users and groups must have unique names.

two clients may have admins groups in that senerio we have to create admin groups with unique names. eg.(example@admin...)

3.auto-sync

by default auto sync is set for an hour.

- either we can set it too few minuets and build it from the source.
- or run sync with a script when new user is added to LDAP.

4.rename

if the username changed in ldap authentik considers it as a new user entry not an update of old user. results in multiple accounts for the same user.

Is there are any ways to deactivate users that was deleted from AD (i'm syncing all users to authentik from our active directory) automatically?

<https://github.com/goauthentik/authentik/issues/3986>



rissson last month

Member ...

We are planning on implementing this for 2025.6 (unconfirmed release name) as an optional toggle on the source. However, the LDAP source doesn't have a specific way of hard-linking authentik users to LDAP users. Because of this, we need to go through a two-step migration process to allow detecting which users should be deleted. The first step will be included in the upcoming 2025.4 as part of [#13796](#), and the actual implementation will be for 2025.6.

For the time being, we recommend deactivating users in LDAP, and running a sync so that they also get deactivated in authentik.