

# LDAP Provider Generic Setup (Authentik)

## Create User/Group?

1. Create a new user account to bind with under *Directory* -> *Users* -> *Create*, in this example called `ldapservice`.

Note the DN of this user will be `cn=ldapservice,ou=users,dc=ldap,dc=goauthentik,dc=io`

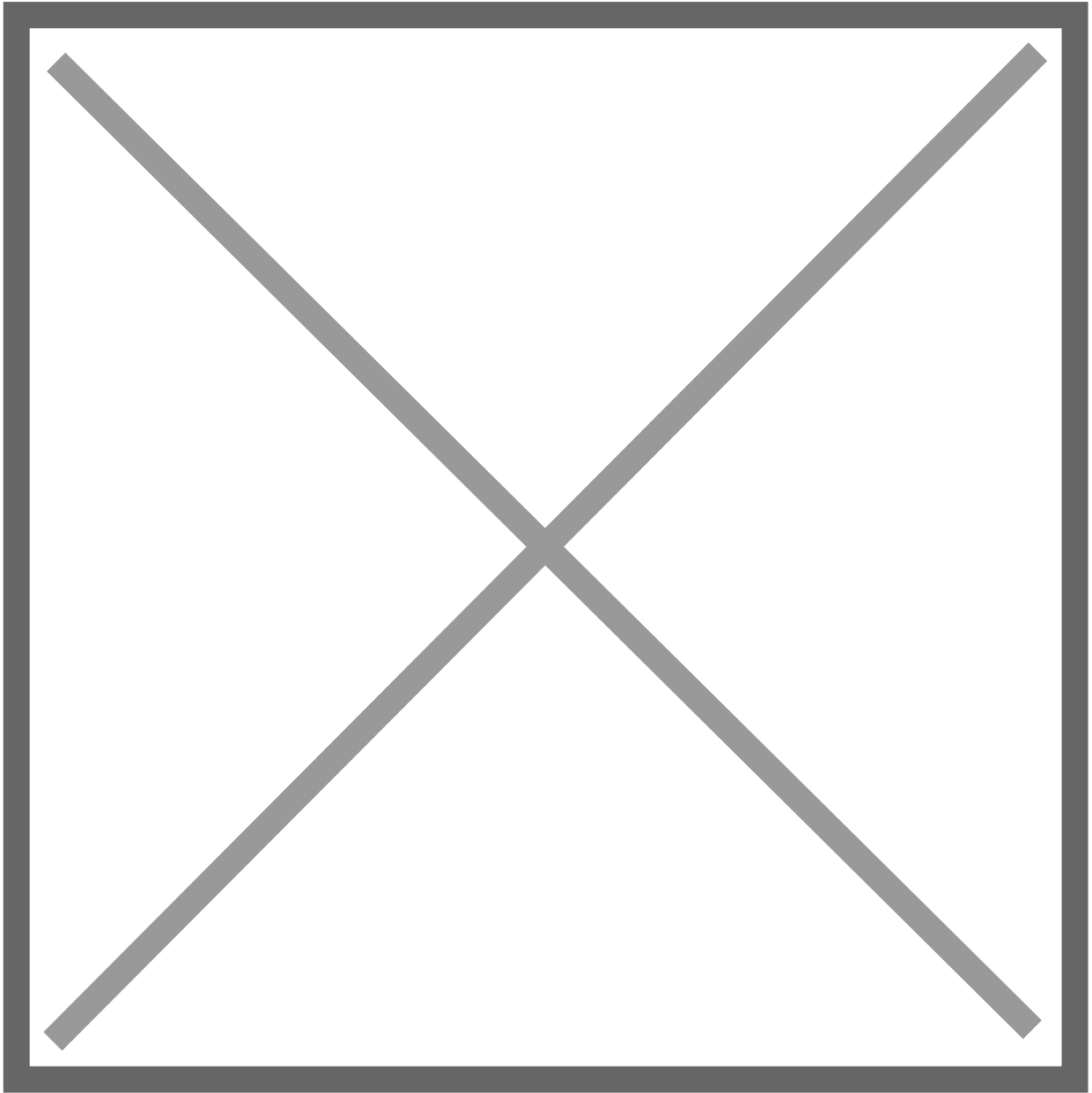
2. Create a new group for LDAP searches. In this example `ldapsearch`. Add the `ldapservice` user to this new group.NFO

Note: The `default-authentication-flow` validates MFA by default, and currently everything but SMS-based devices are supported by LDAP. If you plan to use only dedicated service accounts to bind to LDAP, or don't use SMS-based authenticators, then you can use the default flow and skip the extra steps below and continue at [Create LDAP Provider](#)

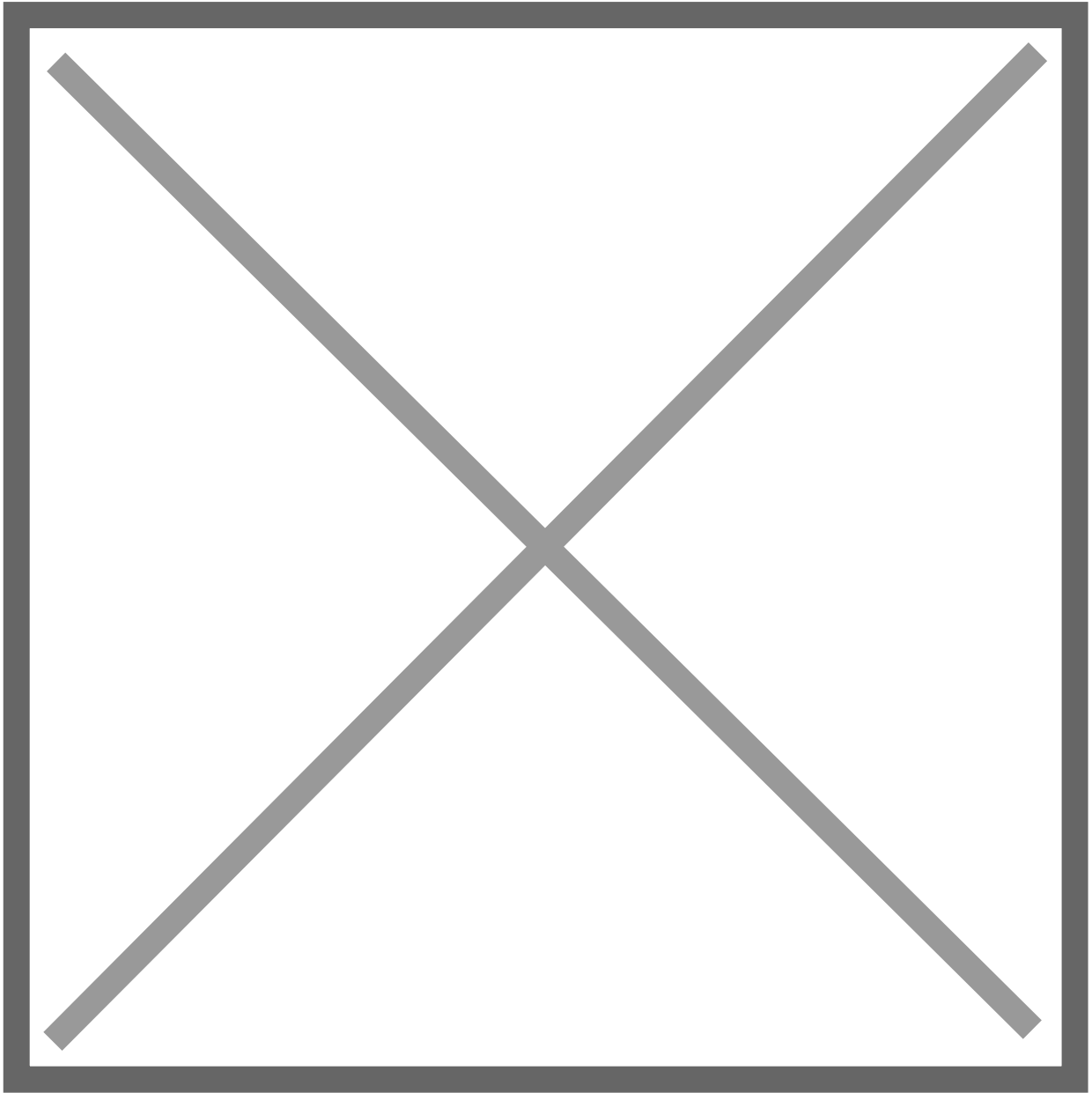
## LDAP Flow?

### Create Custom Stages?

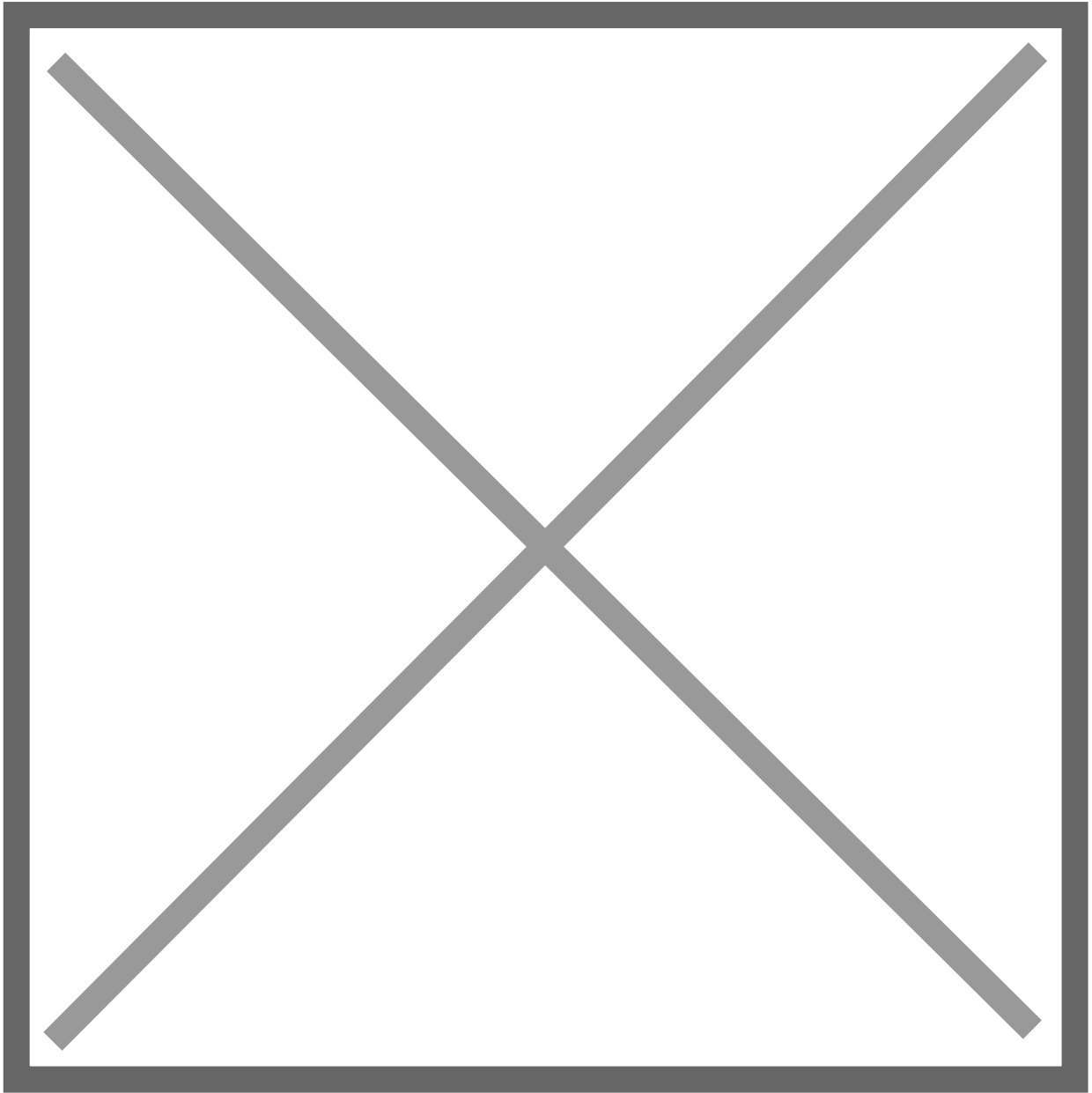
1. Create a new identification stage. *Flows & Stage* -> *Stages* -> *Create*



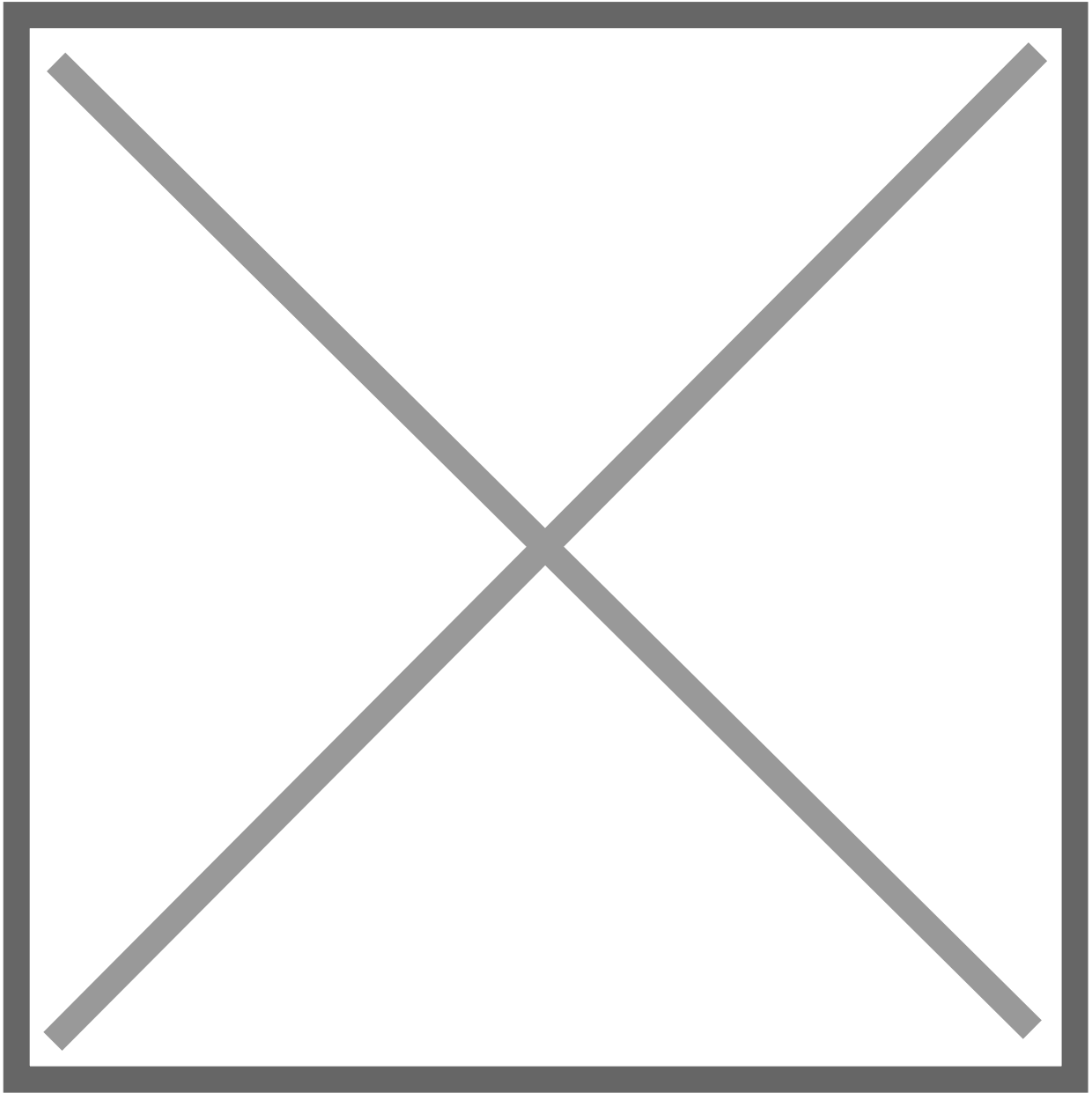
2. Name it something meaningful like `ldap-identification-stage`. Select User fields Username and Email (and UPN if it is relevant to your setup).



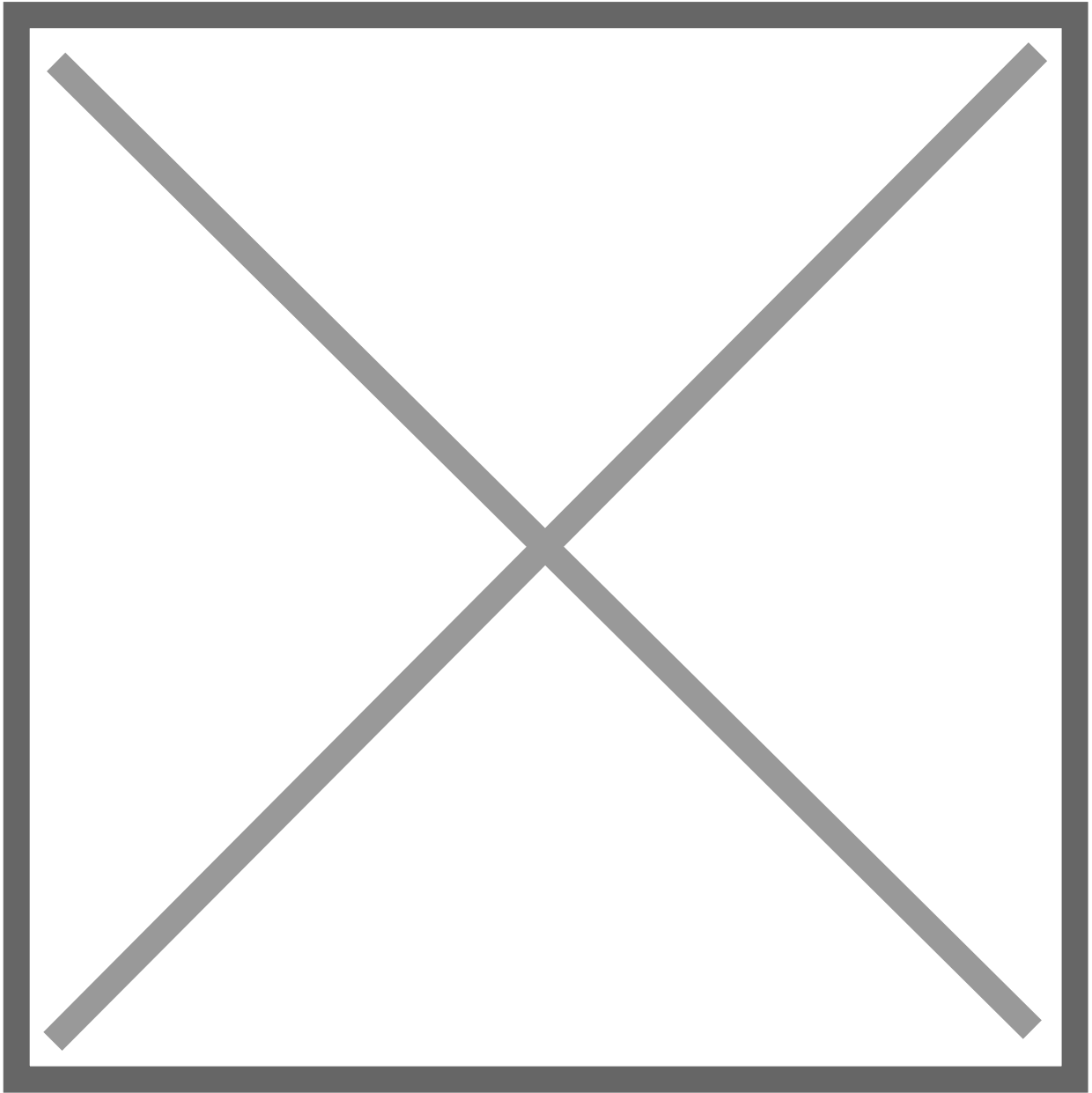
3. Create a new password stage. *Flows & Stage -> Stages -> Create*



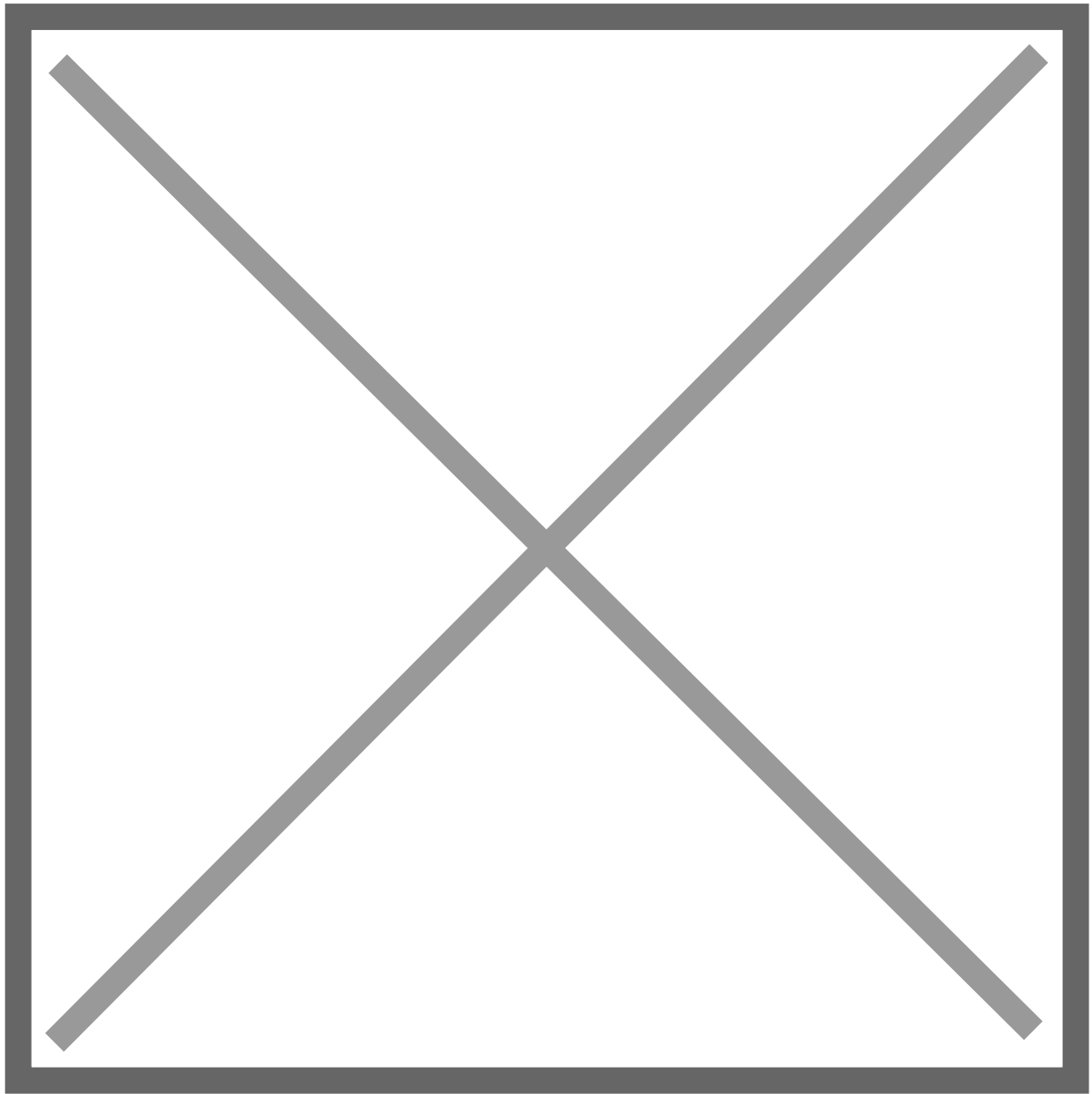
4. Name it something meaningful like `ldap-authentication-password`. Leave the defaults for Backends.



5. Create a new user login stage. *Flows & Stage -> Stages -> Create*

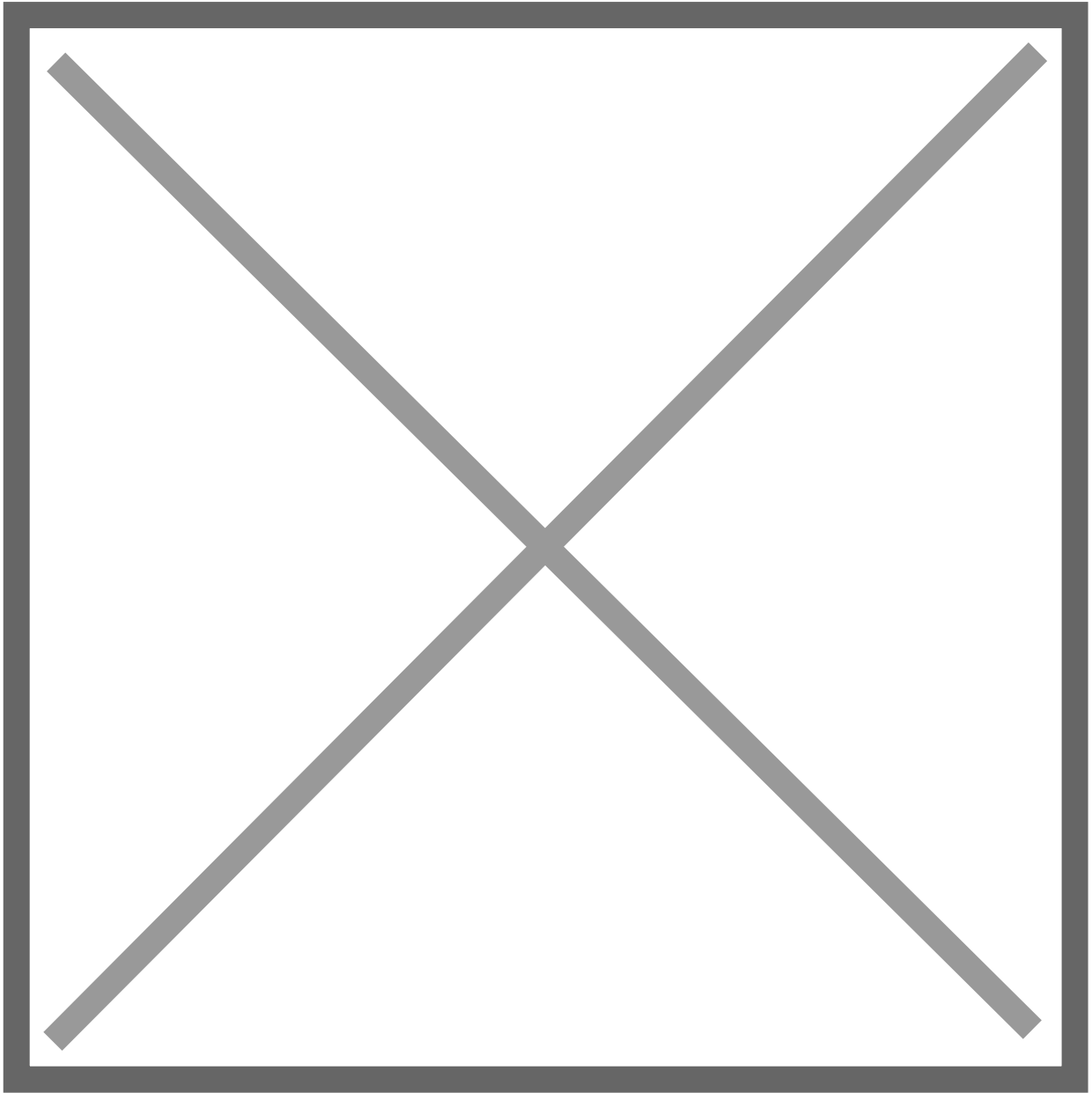


6. Name it something meaningful like `ldap-authentication-login`.



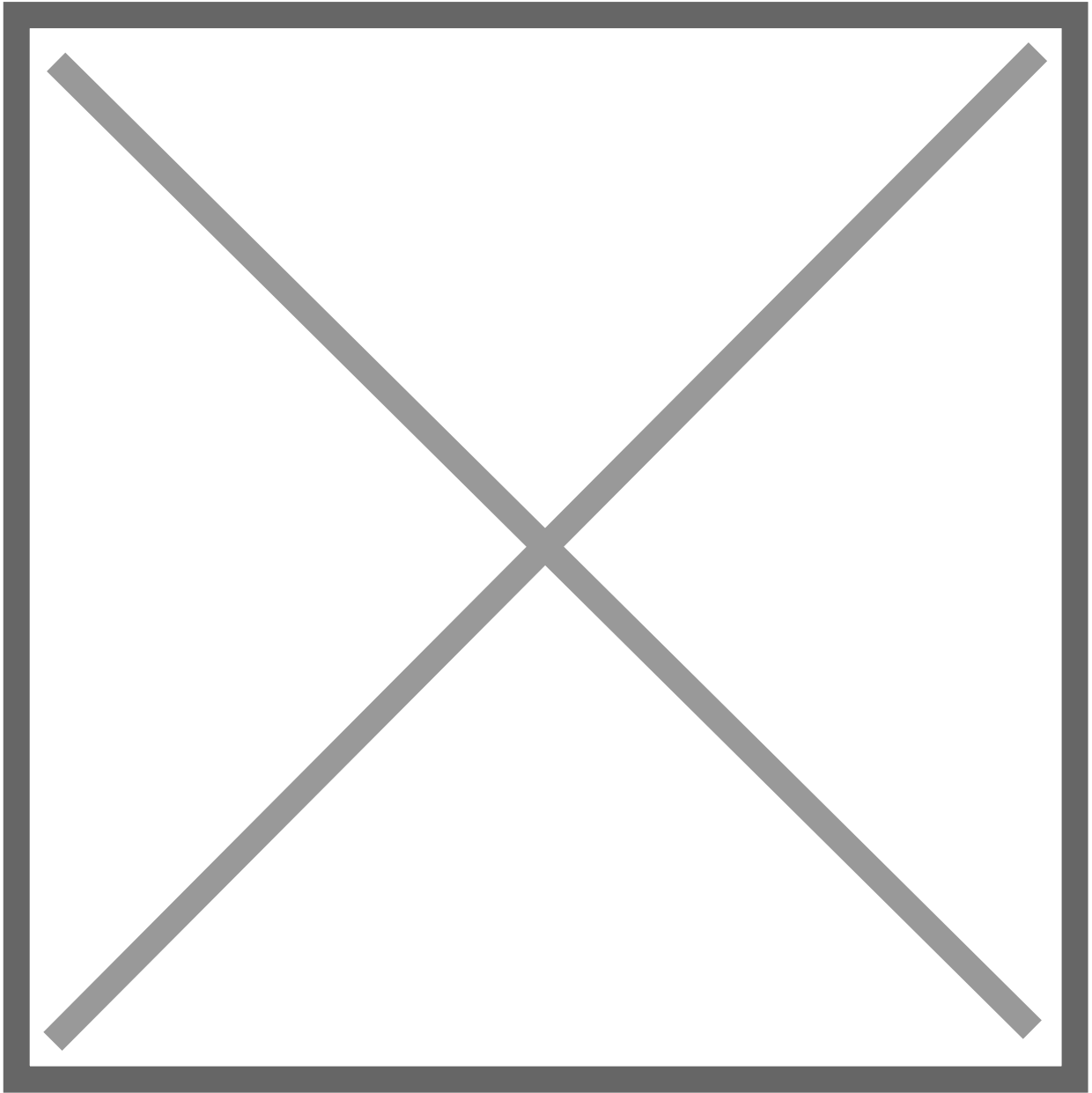
## Create Custom Flow?

1. Create a new authentication flow under *Flows & Stage* -> *Flows* -> *Create*, and name it something meaningful like `ldap-authentication-flow`

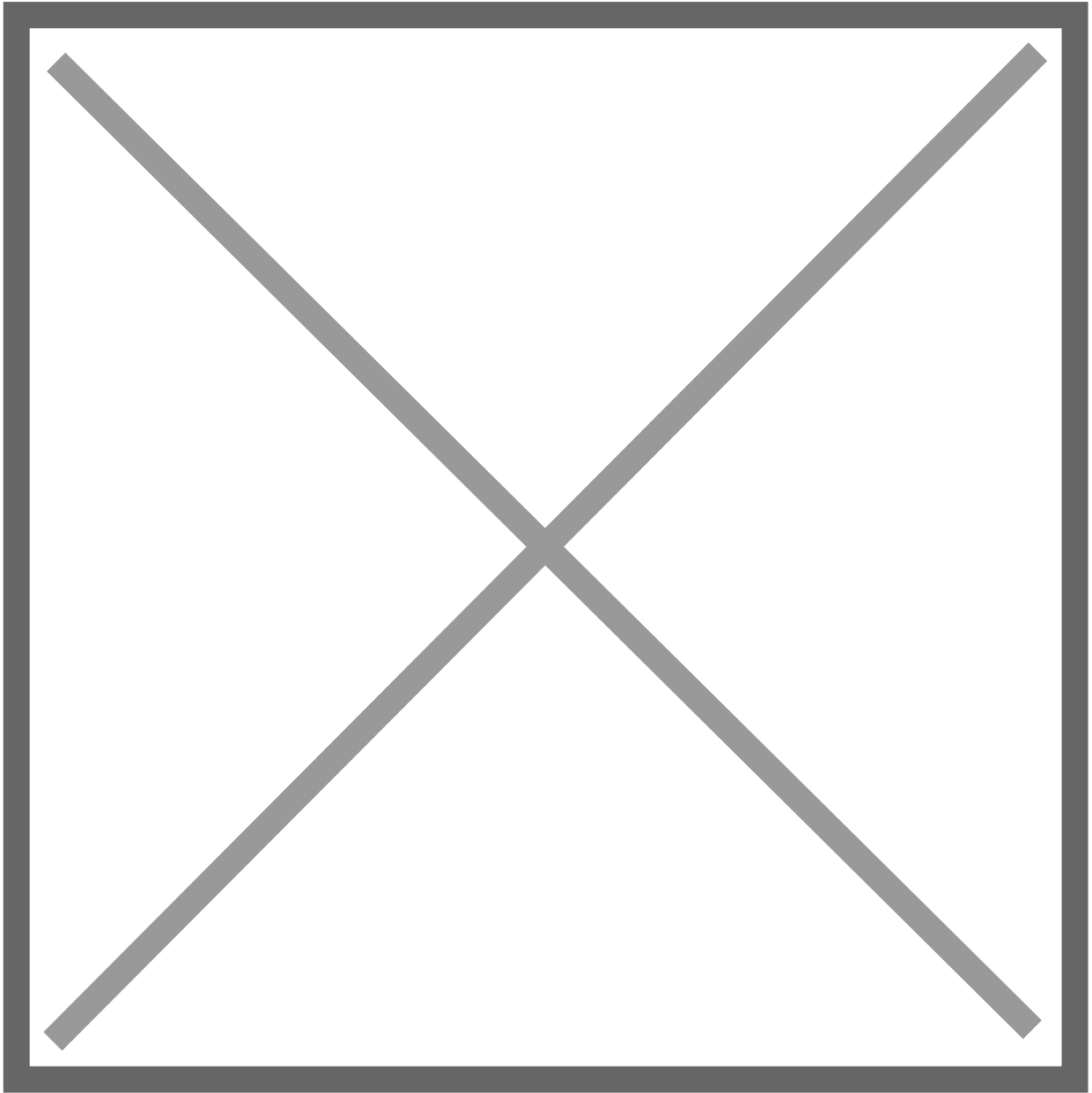


2. Click the newly created flow and choose *Stage Bindings*.

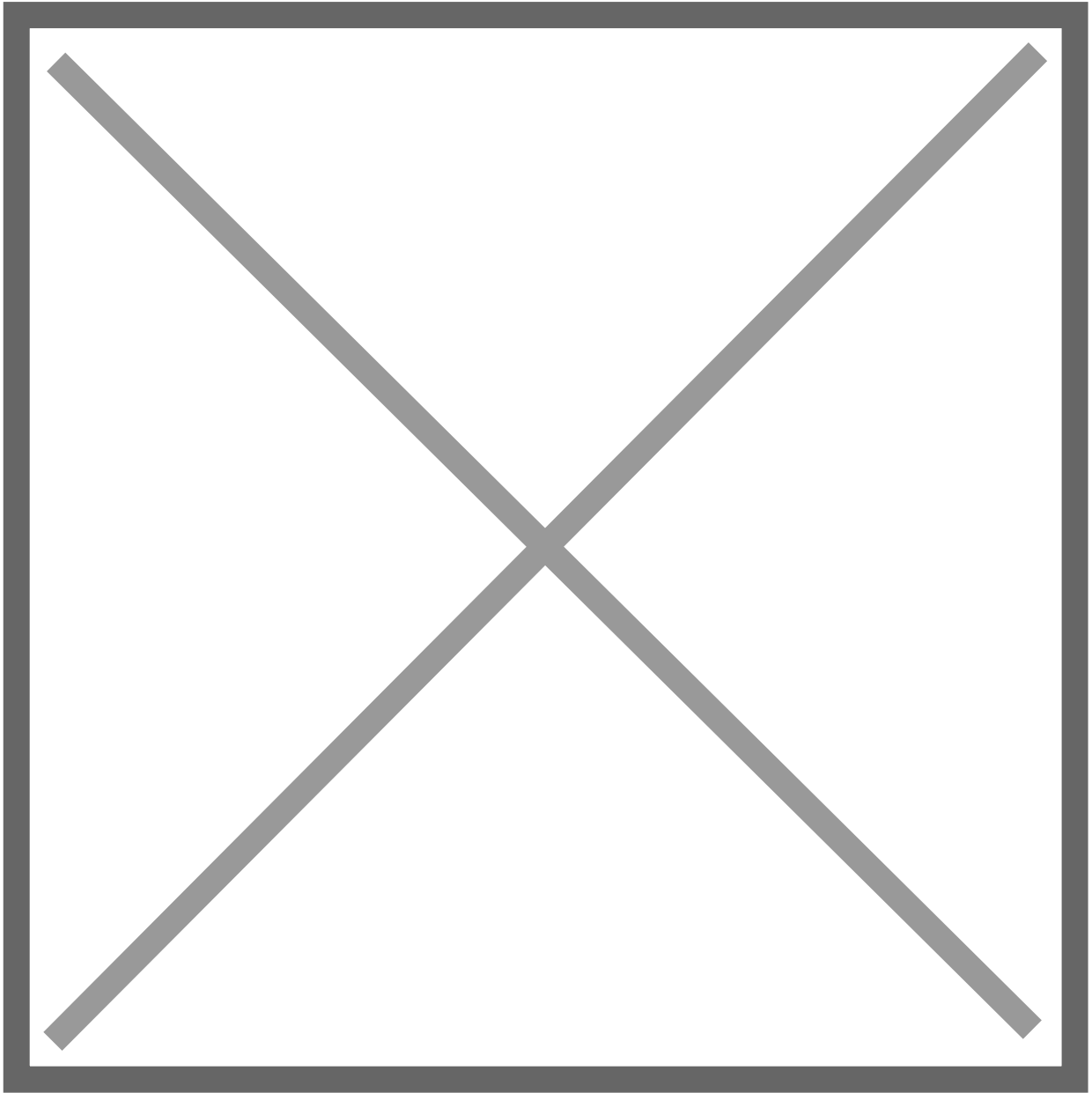




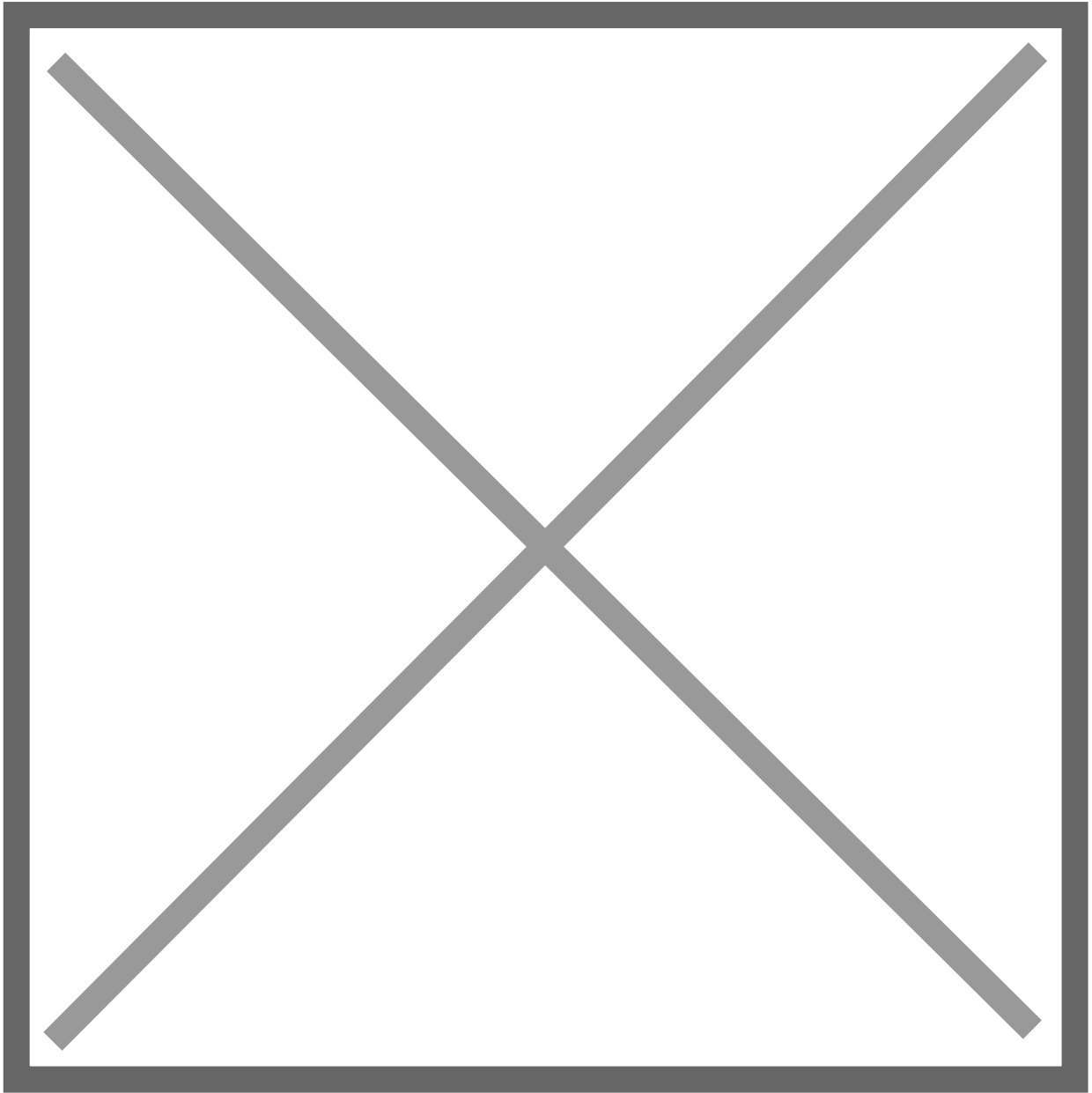
3. Click `Bind Stage` choose `ldap-identification-stage` and set the order to `10`.



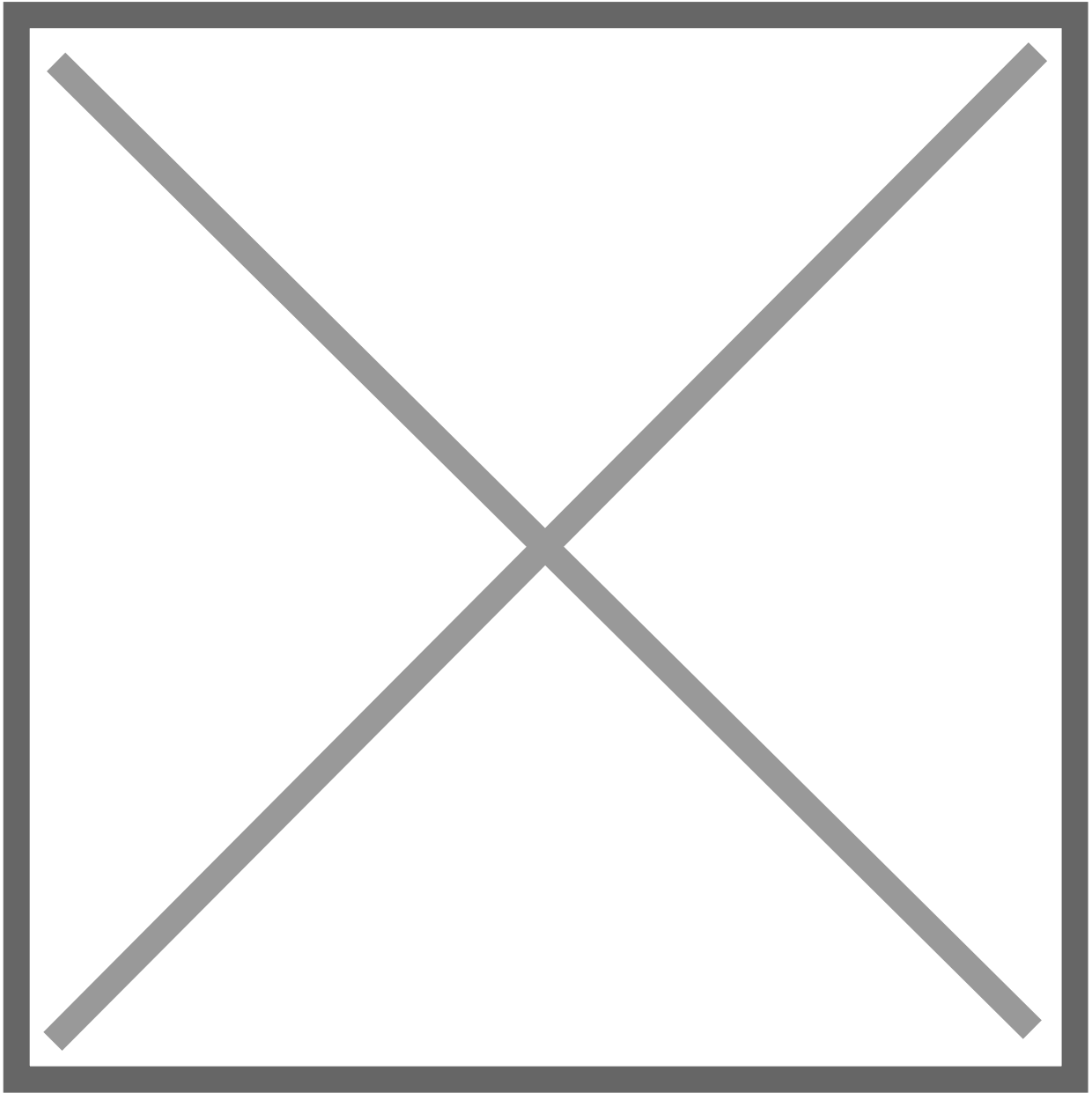
4. Click `Bind Stage` choose `ldap-authentication-login` and set the order to `30`.



5. Edit the `ldap-identification-stage`.

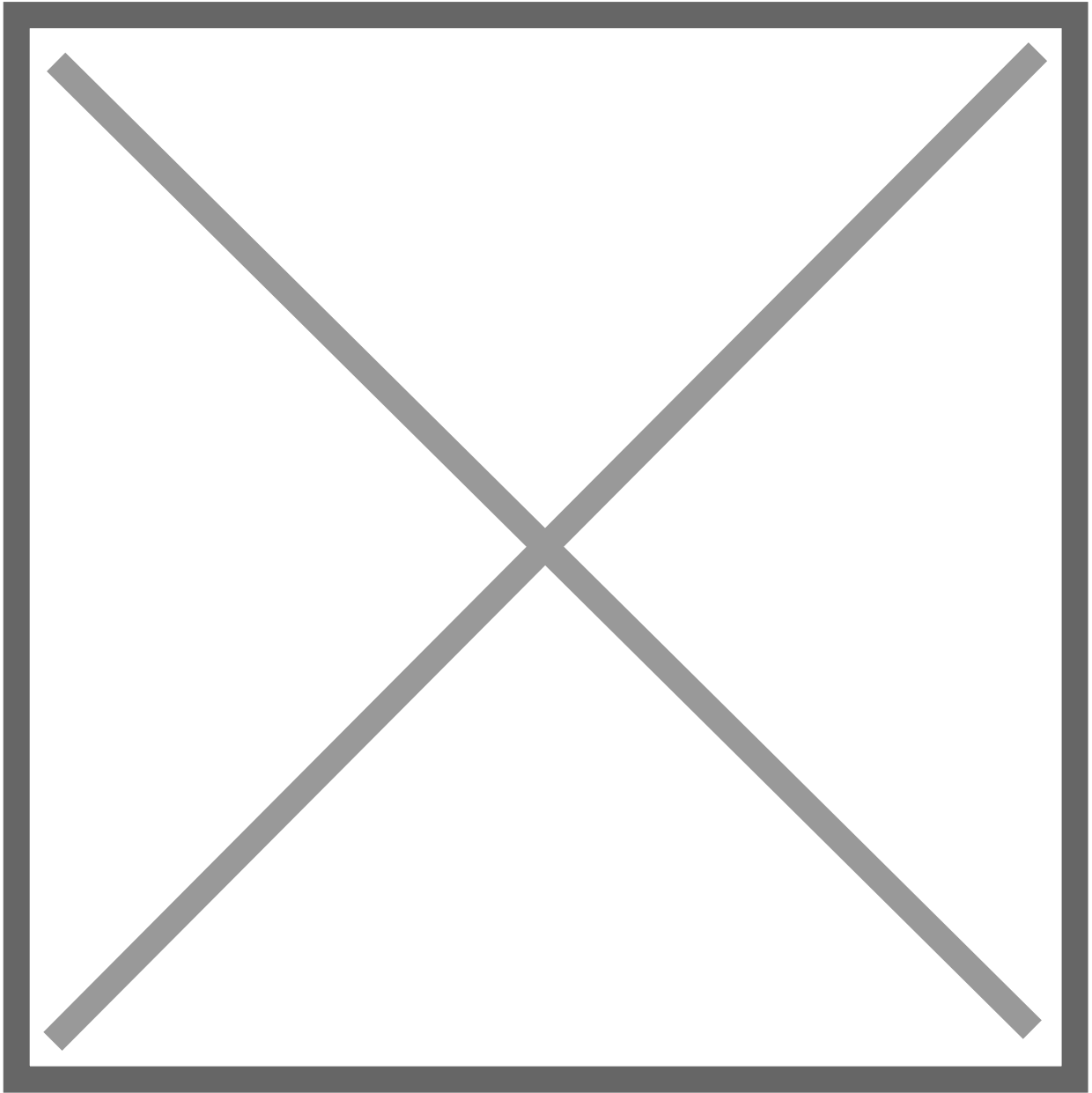


6. Change the Password stage to `ldap-authentication-password`.

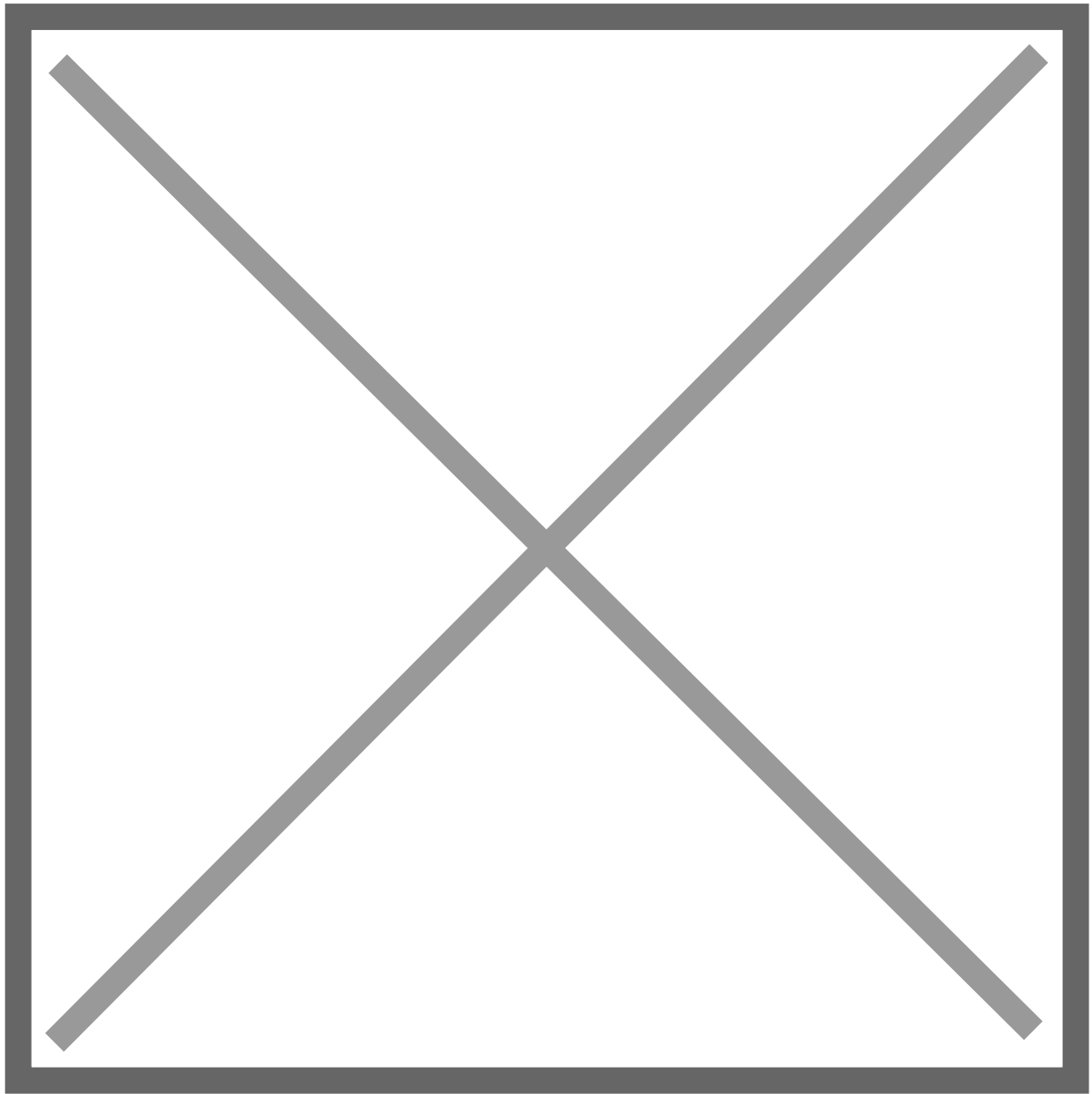


## Create LDAP Provider?

1. Create the LDAP Provider under *Applications* -> *Providers* -> *Create*.

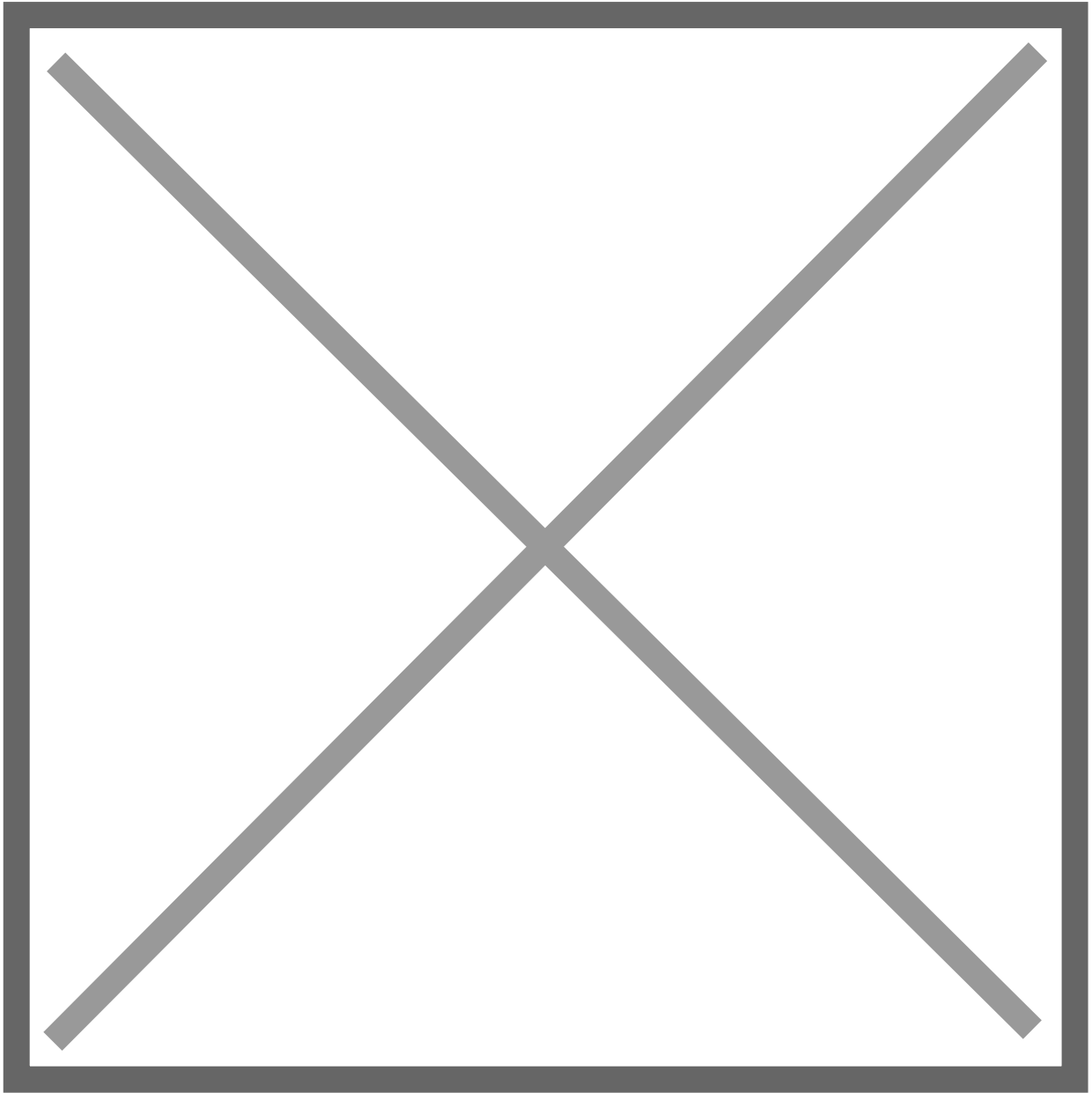


2. Name is something meaningful like `LDAP`, bind the custom flow created previously (or the default flow, depending on setup) and specify the search group created earlier.



## Create LDAP Application?

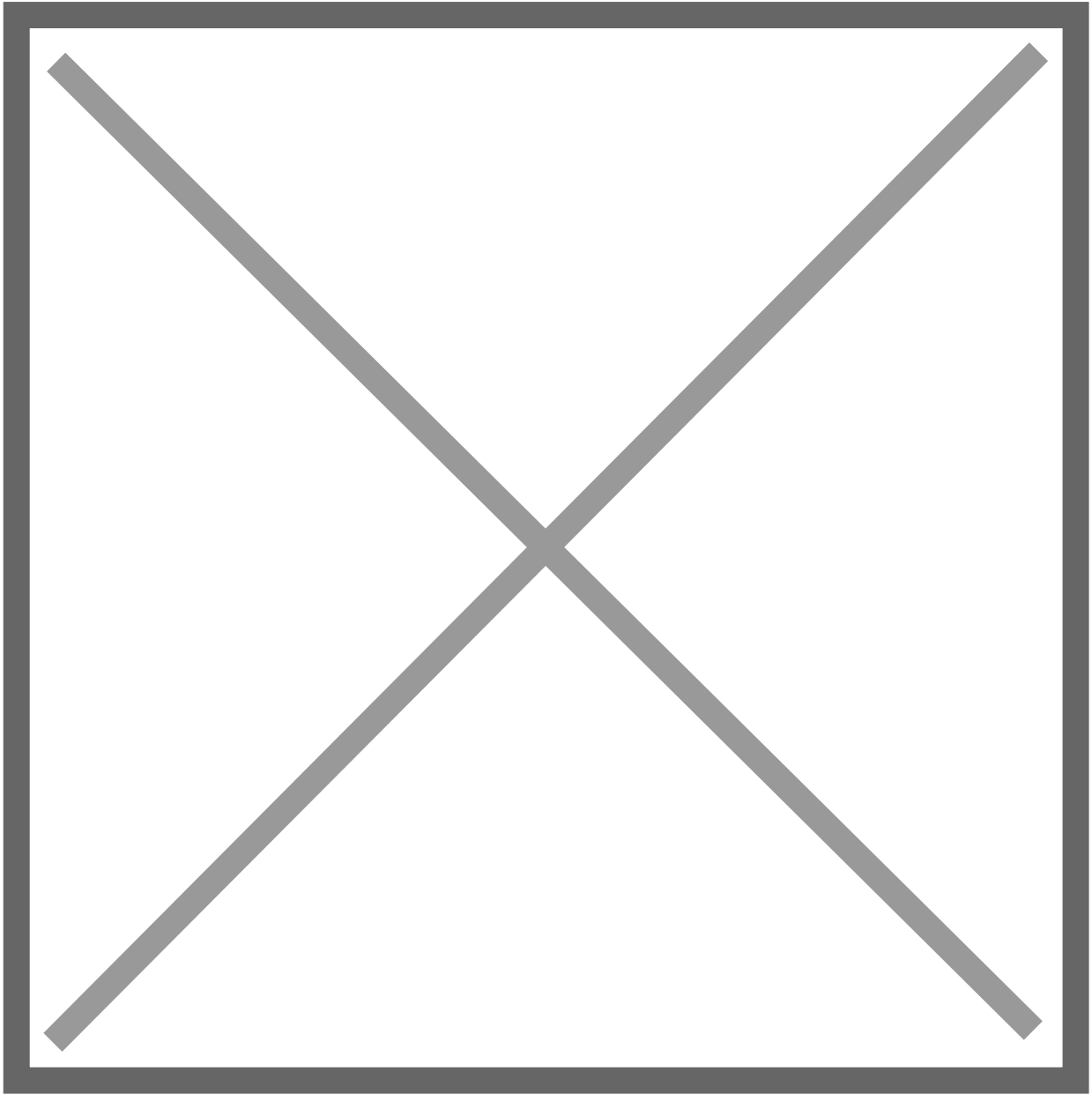
1. Create the LDAP Application under *Applications* -> *Applications* -> *Create* and name it something meaningful like `LDAP`. Choose the provider created in the previous step.



## Create LDAP Outpost?

1. Create (or update) the LDAP Outpost under *Applications -> Outposts -> Create*. Set the Type to  and choose the  application created in the previous step.





INFO

The LDAP Outpost selects different providers based on their Base DN. Adding multiple providers with the same Base DN will result in inconsistent access

## Idapsearch Test?

Test connectivity by using Idapsearch.

INFO

Idapsearch can be installed on Linux system with these commands

```
sudo apt-get install ldap-utils -y # Debian-based systems
sudo yum install openldap-clients -y # CentOS-based systems
```

```
ldapsearch \
  -x \
  -h <LDAP Outpost IP address> \
  -p 389 \ # Production should use SSL 636
  -D 'cn=ldapservice,ou=users,DC=ldap,DC=goauthentik,DC=io' \
  -w '<ldapuserpassword>' \
  -b 'DC=ldap,DC=goauthentik,DC=io' \
  '(objectClass=user)'
```

■

INFO This query will log the first successful attempt in an event in the *Events* -> *Logs* area, further successful logins from the same user are not logged as they are cached in the outpost.

# Manual Outpost deployment in docker-compose

To deploy an outpost with docker-compose, use this snippet in your docker-compose file.

You can also run the outpost in a separate docker-compose project, you just have to ensure that the outpost container can reach your application container.

## Proxy outpost?

```
version: "3.5"

services:
  authentik_proxy:
    image: ghcr.io/goauthentik/proxy
    # Optionally specify which networks the container should be
    # might be needed to reach the core authentik server
    # networks:
    #   - foo
```

```
ports:
  - 9000:9000
  - 9443:9443

environment:
  AUTHENTIK_HOST: https://your-authentik.tld
  AUTHENTIK_INSECURE: "false"
  AUTHENTIK_TOKEN: token-generated-by-authentik
  # Starting with 2021.9, you can optionally set this too
  # when authentik_host for internal communication doesn't match the public URL
  # AUTHENTIK_HOST_BROWSER: https://external-domain.tld
```

■

## LDAP outpost?

```
version: "3.5"

services:
  authentik_ldap:
    image: ghcr.io/goauthentik/ldap
    # Optionally specify which networks the container should be
    # might be needed to reach the core authentik server
    # networks:
    #   - foo
    ports:
      - 389:3389
      - 636:6636
    environment:
      AUTHENTIK_HOST: https://your-authentik.tld
      AUTHENTIK_INSECURE: "false"
      AUTHENTIK_TOKEN: token-generated-by-authentik
```

---

Revision #4

Created 21 January 2024 19:08:21 by joliveira

Updated 21 January 2024 19:23:47 by joliveira