Authentik LDAP Provider

LDAP Provider: Link: https://docs.goauthentik.io/add-secure-apps/providers/ldap/

Create LDAP Provider: Link: https://docs.goauthentik.io/add-secure-apps/providers/ldap/create-ldap-provider/

Outposts: Link: https://docs.goauthentik.io/add-secure-apps/outposts/

Outposts Compose: link: https://docs.goauthentik.io/add-secure-apps/outposts/

Create an LDAP provider

Creating an authentik LDAP provider requires the following steps:

1. Create an LDAP authentication flow *(optional)*
2. Create an LDAP application and provider
3. Create a service account and assign the LDAP search permission
4. Create an LDAP Outpost

Create an LDAP authentication flow *(optional)*

The `default-authentication-flow` validates MFA by default. Duo, TOTP, and static authenticators are supported by the LDAP provider. WebAuthn and SMS are not supported.

If you plan to use only dedicated service accounts to bind to LDAP, or only use LDAP supported MFA authenticators, then you can use the default authentication flow and skip this section and continue with the Create an LDAP application and provider section.

Refer to Code-Based MFA support for more information on LDAP and MFA.

Create custom stages

You'll need to create the stages that make up the flow.

1. Log in to authentik as an administrator and open the authentik Admin interface.

2. Navigate to **Flows and Stages** > **Stages**, and click **Create**.

Password Stage

First, you'll need to create a Password Stage.

3. Select **Password Stage** as the stage type, click **Next**, and set the following required configurations:
   - Provide a **Name** for the stage (e.g. `ldap-authentication-password-stage`).
   - For **Backends**, leave the default settings.
4. Click **Finish**

Identification Stage

Next, you'll need to create an Identification Stage.

5. On the **Stages** page, click **Create**.
6. Select **Identification Stage** as the stage type, click **Next**, and set the following required configurations:
   - Provide a **Name** for the stage (e.g. `ldap-identification-stage`).
   - For **User fields**, select `Username` and `Email` (and UPN if it is relevant to your setup).
   - Set **Password stage** to the Password Stage created in the previous section (e.g. `ldap-authentication-password-stage`)
7. Click **Finish**

User Login Stage

Finally, you'll need to create a User Login Stage.

8. On the **Stages** page, click **Create**.
9. Select **User Login Stage** as the stage type, click **Next**, and set the following required configurations:
   - Provide a **Name** for the stage (e.g. `ldap-authentication-login-stage`).
10. Click **Finish**

Create an LDAP authentication flow

Now you'll need to create the LDAP authentication flow and bind the previously created stages.

1. Log in to authentik as an administrator and open the authentik Admin interface.
2. Navigate to **Flows and Stages** > **Flows**, click **Create**, and set the following required configurations:
   - Provide a **Name**, **Title** and **Slug** for the flow (e.g. `ldap-authentication-flow`).
   - Set **Designation** to `Authentication`.
3. Click **Create**.

4. Click the name of the newly created flow, open the **Stage Bindings** tab, and click **Bind existing stage**.
5. Select the previously created LDAP Identification Stage (e.g. `ldap-identification-stage`), set the order to `10`, and click **Create**.
6. Click **Bind existing stage**.
7. Select the previously created LDAP User Login Stage (e.g. `ldap-authentication-login-stage`), set the order to `30`, and click **Create**.

Create an LDAP application and provider

The LDAP application and provider can now be created.

1. Log in to authentik as an administrator and open the authentik Admin interface.
2. Navigate to **Applications** > **Applications**, click **Create with Provider** to create an application and provider pair.
3. On the **New application** page, define the application details, and then click **Next**.
4. Select **LDAP Provider** as the **Provider Type**, and then click **Next**.
5. On the **Configure LDAP Provider** page, provide the configuration settings and then click **Submit** to create both the application and the provider.

INFO

If you followed the optional Create an LDAP authentication flow section, ensure that you set **Bind flow** to newly created authentication flow (e.g. `ldap-authentication-flow`).

Create a service account

Create a service account to bind to LDAP with.

1. Log in to authentik as an administrator and open the authentik Admin interface.
2. Navigate to **Directory** > **Users** and click **New User**.
3. Provide a name for the service account (e.g. `ldapservice`) and click **Create**.
4. Click the name of the newly created service account.
5. Under **Recovery**, click **Set password**, provide a secure password for the account, and click **Update password**.

Default DN of service account

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

Assign the LDAP search permission to the service account

The service account needs permissions to search the LDAP directory. You'll need to create a role with the permission and assign the service account to that role.

1. Log in to authentik as an administrator and open the authentik Admin interface.
2. Navigate to **Directory** > **Roles** and click **Create**.
3. Provide a name for the role (e.g. `LDAP search`) and then click **Create**.
4. Click on the newly created role and open the **Users** tab.
5. Click **Add existing user**, select the service account, and then click **Assign**.
6. Navigate to **Applications** > **Providers**.
7. Click on the name of the newly created LDAP provider and open the **Permissions** tab.
8. Click **Assign Object Permissions**.
9. Select the role that you created (e.g. `LDAP search`), enable the **Search full LDAP directory** permission, and then click **Assign**.

Create an LDAP Outpost

The LDAP provider requires the deployment of an LDAP Outpost.

1. Log in to authentik as an administrator and open the authentik Admin interface.
2. Navigate to **Applications** > **Outposts**, click **Create** and set the following required configurations:
   - Provide a **Name** for the outpost (e.g. `LDAP Outpost').
   - Set the **Type** as `LDAP`.
   - Set **Integration** to match your deployment method or manually deploy an outpost via Docker-Compose or Kubernetes. For more information, refer to the Outpost documentation.
   - Under **Applications**, select the LDAP application created in the previous section.
   - Under **Advanced settings**, set the required outpost configurations. For more information, refer to Outpost Configuration
3. Click **Create**.

Multiple LDAP providers

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

Configuration verification

You can test the LDAP provider by using the `ldapsearch` tool on Linux and macOS, or the `dsquery` tool on Windows.

- ldapsearch
- dsquery

To install the `ldapsearch` tool, use one of the following commands:

```
sudo apt-get install ldap-utils -y # Debian-based systems
sudo yum install openldap-clients -y # CentOS-based systems
brew install openldap #macOS based systems (requires Homebrew to be installed)
```

To search the LDAP directory using the previously created `ldapservice` service account, use the following command:

```
ldapsearch \
  -x \
  -H ldap://<LDAP outpost IP address>:389 \
  -D 'cn=ldapservice,ou=users,DC=ldap,DC=goauthentik,DC=io' \
  -w '<ldapuserpassword>' \
  -b 'DC=ldap,DC=goauthentik,DC=io' \
  '(objectClass=user)'
```

This example query will return all users and log the first successful attempt in an event in **Events** > **Logs**. Subsequent successful logins from the same user are not logged by default, as they are cached in the outpost. For more details see Bind modes.

LDAPS

In production it is recommended to use LDAPS, which requires `ldaps://` as the protocol, and port number `636` rather than `389`. See LDAPS for more information.

Revision #3
Created 11 April 2026 01:07:52 by Administrador
Updated 11 April 2026 14:24:40 by Administrador