

Integração do Nextcloud com Authentik LDAP

Link: <https://integrations.goauthentik.io/chat-communication-collaboration/nextcloud/>

Em 09/04/2026

What is Nextcloud

“ Nextcloud is a suite of client-server software for creating and using file hosting services. Nextcloud is free and open-source, which means that anyone is allowed to install and operate it on their own private server devices.

-- <https://nextcloud.com/>

WARNING

If you require [server side encryption](#), you must use LDAP. OpenID and SAML will cause **irrevocable data loss**. Nextcloud server side encryption requires access to the user's cleartext password, which Nextcloud has access to only when using LDAP because the user enters their password directly into Nextcloud.

CAUTION

This setup only works when Nextcloud is running with HTTPS enabled. See [here](#) on how to configure this.

INFO

If there's an issue with the configuration, you can log in using the built-in authentication by visiting <http://nextcloud.company/login?direct=1>.

Configuration methods

It is possible to configure Nextcloud to use OIDC, SAML, or LDAP for authentication. Below are the steps to configure each method.

- OIDC

- SAML
- LDAP

LDAP Configuration

Preparation

The following placeholders are used in this guide:

- `nextcloud.company` is the FQDN of the Nextcloud installation.
- `authentik.company` is the FQDN of the authentik installation.

INFO

This documentation lists only the settings that you need to change from their default values. Be aware that any changes other than those explicitly mentioned in this guide could cause issues accessing your application.

Create an application and provider in authentik

1. Log in to authentik as an administrator and open the authentik Admin interface.
2. Navigate to **Applications > Applications** and click **Create with Provider** to create an application and provider pair. (Alternatively you can first create a provider separately, then create the application and connect it with the provider.)
 - **Application:** provide a descriptive name, an optional group for the type of application, the policy engine mode, and optional UI settings.
 - **Choose a Provider type:** select **LDAP** as the provider type.
 - **Configure the Provider:** provide a name (or accept the auto-provided name) and the bind flow to use for this provider
 - **Configure Bindings (optional):** you can create a [binding](#) (policy, group, or user) to manage the listing and access to applications on a user's **My applications** page.
3. Click **Submit** to save the new application and provider.

Create an LDAP outpost

1. Log in to authentik as an admin, and open the authentik Admin interface.
2. Navigate to **Applications > Outposts** and click **Create**.
 - **Name:** provide a suitable name for the outpost.
 - **Type:** `LDAP`
 - Under applications, add the newly created Nextcloud application to **Selected Applications**.
3. Click **Create**.

Nextcloud configuration

1. In Nextcloud, ensure that the **LDAP user and group backend** app is installed.
2. Log in to Nextcloud as an administrator.
3. Navigate to **Settings > LDAP user and group backend** and configure the following settings:
 - On the **Server** tab:
 - Click the **+** icon and enter the following settings:
 - **Host:** enter the hostname/IP address of the authentik LDAP outpost preceded by `ldap://` or `ldaps://`. If using LDAPS you will also need to specify the certificate that is being used.
 - **Port:** `389` or `636` for secure LDAP.
 - Under **Credentials**, enter the **Bind DN** of the authentik LDAP provider and the associated user password.
 - Under **Base DN**, enter the **Search base** of the authentik LDAP provider.
 - On the **Users** tab:
 - Set **Only these object classes** to `Users`.
 - On the **LDAP/AD integration** tab:
 - Uncheck **LDAP/AD Username**.
 - Set **Other Attributes** to `cn`.
 - Click **Expert** in the top right corner and enter these settings:
 - **Internal Username Attribute:** `uid`
 - **UUID Attribute for Users:** `uid`
 - **UUID Attribute for Groups:** `gidNumber`
 - Click **Advanced** in the top right corner and enter these settings:
 - Under **Connection Settings:**
 - **Configuration Active:** checked
 - Under **Directory Settings:**
 - **User Display Name Field:** `name`
 - **Base User Tree:** enter the **Search base** of the authentik LDAP provider.
 - **Group Display Name Field:** `cn`
 - **Base Group Tree:** enter the **Search base** of the authentik LDAP provider.
 - **Group-Member Association:** `gidNumber`
 - Under **Special Attributes:**
 - **Email Field:** `mailPrimaryAddress`
 - On the **Groups** tab:
 - Set **Only these object classes** to `groups`.
 - Select the authentik groups that require Nextcloud access.

INFO

If Nextcloud is behind a reverse proxy, force HTTPS by adding `'overwriteprotocol' =>`
`'https'` to the Nextcloud `config/config.php` file. See [the Nextcloud admin manual](#) for more details.

Configuration verification

To confirm that authentik is properly configured with Nextcloud, log out and log back in using LDAP credentials. If successful you will then be redirected to the Nextcloud dashboard.

Resources

- [Nextcloud docs - User authentication with LDAP](#)
- [Nextcloud OIDC App - User Documentation](#)

Help us improve this content

We welcome your knowledge and expertise. If you see areas of the documentation that you can improve (fix a typo, correct a technical detail, add additional context, etc.) we would really appreciate your contribution.

- [Edit on GitHub](#)
- [Contributor Guide](#)
- [Open an issue](#)
- [Get Enterprise Support](#)

Revision #1

Created 9 April 2026 20:06:25 by Administrador

Updated 9 April 2026 20:13:52 by Administrador