Authentik

- Installing Authentik on CasaOS (Big Bear Template)
- Linking Authentik SSO to Nextcloud (OIDC)

Installing Authentik on CasaOS (Big Bear Template)

Overview

This article outlines the successful installation of **Authentik** on an Ubuntu server running **CasaOS** (192.168.0.152). Authentik is a complex application consisting of four separate containers that must communicate over a shared internal network.

---

1. Pre-Installation Cleanup

To prevent database corruption or "ghost" network conflicts, start with a clean environment.

- **Remove Existing Apps:** Uninstall any previous Authentik or Postgres attempts via the CasaOS dashboard.
- **Clear AppData:** Use the Files app to delete the `AppData/big-bear-authentik` folder.
- **Prune Ghost Networks:** If an installation fails with a "Label" or "Network" error, use a terminal to run:

```
docker network prune
```

*(Enter '*y*' when prompted to remove unused custom networks.)*

---

2. Installation via Big Bear App Store

Navigate to the App Store in CasaOS and select **Authentik** from the Big Bear repository. Before clicking "Install," you must adjust the settings for all four components.

A. Component: big-bear-authentik (Server)

- **Network:** Select `big-bear-authentik` (or the longest available big-bear network name).
- **Ports:** Add a new port mapping:
  - **Host:** 9000
  - **Container:** 9000

    - **Protocol:** TCP
- **Web UI:** Ensure the URL is set to `http://[IP]:9000`.

B. Components: DB, Redis, and Worker

Navigate to the tabs for `big-bear-authentik-db`, `big-bear-authentik-redis`, and `big-bear-authentik-worker`.

- **Crucial Step:** Change the **Network** on every single tab to match the one selected for the Server (`big-bear-authentik`).
- **Internal Communication:** Do **not** map host ports for the DB or Redis; they communicate internally over the shared bridge network.

---

3. Post-Installation & Troubleshooting

The "Authentik Starting" Screen

Upon first boot, the server will display a black screen stating "authentik starting."

- **Cause:** The server is running initial database migrations and building internal tables.
- **Action:** Wait **3–5 minutes**. Do not restart the containers during this phase.

Database "Unhealthy" Status

If the DB is marked unhealthy, it is usually due to a password mismatch in the environment variables.

- **Fix:** Ensure `POSTGRES_PASSWORD` in the DB tab matches the `AUTHENTIK_POSTGRESQL__PASSWORD` in both the Server and Worker tabs.

---

4. Initial Admin Account Setup

Authentik does not ship with a default password for the `akadmin` user. You must trigger the initial setup flow.

1. Navigate to: `http://192.168.0.152:9000/if/flow/initial-setup/`
2. Set a strong master password for the **akadmin** account.
3. Log in at the standard portal using:
    - **Username:** akadmin
    - **Password:** (The one you just created)

Summary of "What Worked"

Requirement	Value / Selection
Shared Network	big-bear-authentik (Set on all 4 tabs)
Primary Port	9000 (Mapped for HTTP access)
Worker Command	worker
Setup URL	/if/flow/initial-setup/

Linking Authentik SSO to Nextcloud (OIDC)

> **Purpose:** This guide outlines the steps to enable Single Sign-On (SSO) for Nextcloud using Authentik via the OpenID Connect (OIDC) protocol. This allows users to log in to Nextcloud using their central Authentik credentials.

Prerequisites

- A working **Authentik** instance (e.g., `auth.goonersnas.com`).
- A working **Nextcloud** instance (e.g., `nc.goonersnas.com`).
- Administrator access to both platforms.

Step 1: Create the Authentik Provider

The Provider acts as the authentication engine for the handshake.

1. Navigate to **Applications > Providers** in the Authentik Admin interface.
2. Click **Create** and select **OAuth2/OpenID Provider**.

3. Set the following values:

Field	Value
Name	Nextcloud
Authentication flow	default-authentication-flow
Authorization flow	default-provider-authorization-implicit-consent
Client Type	Confidential

4. In the **Redirect URIs** section, add the following (adjust domain as needed):

```
https://nc.goonersnas.com/index.php/apps/sociallogin/custom_oidc/authentik
```

Click **Finish** and then copy your **Client ID** and **Client Secret** from the provider details page.

Step 2: Create the Authentik Application

The Application links the Provider to a user-facing icon.

1. Navigate to **Applications > Applications**.
2. Click **Create**.
3. **Name:** Nextcloud | **Slug:** nextcloud
4. **Provider:** Select the "Nextcloud" provider created in Step 1.
5. Click **Finish**.

Step 3: Configure Nextcloud Social Login

Install the **Social Login** app from the Nextcloud App Store, then navigate to **Settings > Administration > Social login**.

3.1 General Settings

Check the following boxes at the top of the page:

- **Uncheck:** "Disable auto-create new users" (to allow SSO to create accounts).
- **Check:** "Allow users to connect social logins with their account".
- **Check:** "Update user profile every login".

3.2 Custom OpenID Connect

Click the + button under Custom OpenID Connect and fill in the following:

Nextcloud Field	Authentik URL Path
Internal name	authentik
Authorize URL	https://auth.goonersnas.com/application/o/authorize/
Token URL	https://auth.goonersnas.com/application/o/token/
User info URL	https://auth.goonersnas.com/application/o/userinfo/
Scope	openid profile email

> **Important:** Ensure there are no leading or trailing spaces in the Client ID or Client Secret fields.

Step 4: Final Testing

1. Open an **Incognito Window**.
2. Navigate to your Nextcloud URL.

3. Click the large **Authentik** button at the bottom of the login form.
4. Log in with your Authentik credentials.

> **Success!** If redirected to your Nextcloud dashboard, the SSO link is active. New users created in Authentik will now automatically have Nextcloud accounts provisioned on their first login.