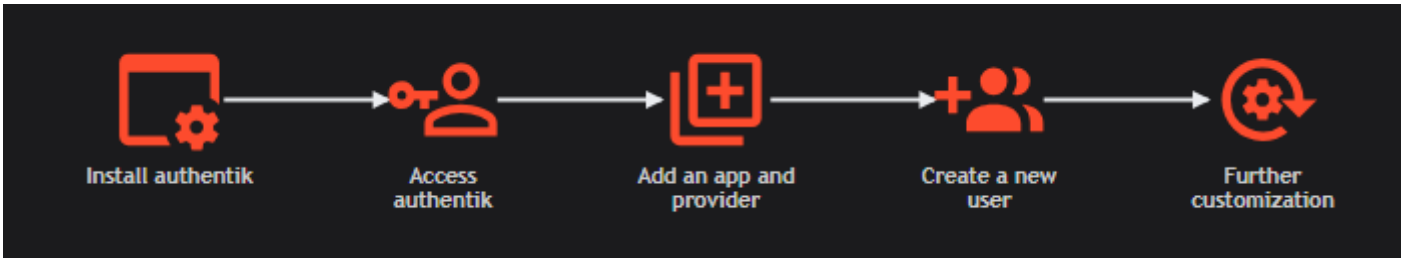
Configurações iniciais do Authentik

Link: https://docs.goauthentik.io/install-config/first-steps/

First steps

After you have installed and started authentik, you are now ready to add your first application and provider, add some users, and get started with using authentik as your Identity provider.



Where are we now, and what's next?

The following tutorial assumes that you have already:

1. Installed authentik on either Docker Compose, Kubernetes, or AWS CloudFormation and confirmed that the server, worker, and the PostgreSQL database are started and running.
2. Opened authentik in your browser to the `initial-setup` flow and added credentials for a default Admin account. (Docker, Kubernetes), or AWS CloudFormation.

Initial setup in browser
You will get a `Not Found` error if the initial setup URL doesn't include the forward slash `/` at the very end of the URL. Also verify that the authentik server, worker, and PostgreSQL database are running and healthy. Review additional tips in our troubleshooting docs.

Other optional pre-installation configurations that you might have already completed include:

- Configured your global email address.
- Configured your PostgreSQL settings (read-replica, connections, etc.).
- Configured a reverse proxy.
- Configured your media storage settings or optionally AWS S3 file storage.

- Added additional custom configurations environment variables.
- Verified your configuration settings.

Install your first application and provider

Now that you have your authentik instance installed and configured with the required settings, you can add your first application and provider. After that, we'll walk through how to add your first user.

Security Best Practice

In a production environment, best practice is to first create a group, then create the user(s), and then add the application. Then you can configure the application to have a binding to a specific group or user. The binding controls the access to the application (whether or not it is displayed on a user's My Applications page).

authentik supports integration with any application; refer to our Integrations documentation to view integrations guides for over 180 of the most common ones.

In this guide we'll be setting up Grafana as an example application.

Why Grafana?

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

A. In the Admin interface, navigate to **Applications** > **Applications** and click **Create with Provider** to create an application and provider pair.

About application and provider pairs

Every application that you add to authentik requires a provider, which is used to configure the specific protocol between the application and authentik, for example OAuth2/OIDC, SAML, LDAP, or others.

B. Provide the details for the application (Grafana) and provider (OAuth2/OIDC).

- **Configure the Application**:
  - **Name**: provide a descriptive name (such as Grafana).
    - **Group**: select an optional group for the application; groups are used to visually separate applications. For example, you can choose to group applications that you use for coding from those you use for internal communication.
  - **Policy engine mode**: select **Any** for this tutorial; the mode determnes how strictly policies are adhered to.

    - **TIP**: in authentik, policies are used in authentik to fine-tune access to applications, flows, stages and many other authentik components. It is not required to use a policy at all, though. The *policy engine mode* setting of **Any** means that as long as a single policy passes (or if there are no policies bound to the application), then access to the application is granted. The mode **ALL** means that every one of any policies bound to the application must pass in order for a user to have access to the application.
  - **UI Settings**: optional UI settings that are displayed about the application, including the launch URL, and three settings to display extra information about the application on the **My Applications** page: an optional icon, the publisher of the application, and a brief description.
- **Choose a Provider type**: select **OAuth2/OpenID Connect** as the provider type.
- **Configure the Provider**:
  - **Name**: Provide a name (or accept the auto-provided name).
  - **Authorization flow**: Select the default `implicit` authorization flow to use for this provider.
    - **TIP**: The authorization flow is where the various steps, or *stages* of authorization are defined and executed. The defined set of stages construct the workflows of authentication, authorization, etc.
  - **Protocol settings** provide the following required configurations:
    - Note the **Client ID**, **Client Secret**, and **Slug** values because they will be required later when you configure Grafana to use authentik.
    - Set a `Strict` redirect URI to `https://grafana.company/login/generic_oauth`.
      - **TIP**: The Redirect URI is where the application will go as soon as authentik's authorization flow is successfully completed.
  - **Logout URI**: set to `https://grafana.company/logout`.
  - **Logout Method**: set to `Front-channel`.
    - **TIP**: With OAuth2, front-channel logout is considered the default because most application (including Grafana) do not support back-channel logout.
  - **Signing key**: select any available signing key.
    - **TIP**: authentik generates a key that you can use, called the `authentik Self-signed Certificate`, if you do not have a specific signing key for an application.
- **Configure Bindings** *(optional)*: for this tutorial, skip this step because you do not yet have a user. Later, after you create your first user, you can create a binding to manage the display and access to applications on a user's **My applications** page.
  - **TIP**: By creating a binding between an application and a specific user, you are ensuring that the application is accessible only to that user and any other users or groups for whom you created a binding. Learn more about how bindings are used in authentik in our Bindings overview.

  For any fields not mentioned above, you can leave the default value.

C. Click **Submit** to save the new application and provider.

2. Configure Grafana to use authentik as its IdP

For some applications, you log into the application and configure settings there; with Grafana you simply edit your Grafana Docker Compose file. Here you add basic configuration settings as well as the **Client ID**, **Client Secret**, and the **Slug** values that you obtained when you configured the application and provider in authentik in Step 1. above.

A. In the Grafana Docker Compose file, set the following environment variables:

Tips

These values below are for a Grafana instance running in Docker; for standalone or Helm Chart instances refer to our Grafana integration guide.

Note that `authentik.company` is a placeholder that we use in our example settings; replace this with the domain that authentik is running on in your environment.

```
environment:
    GF_AUTH_GENERIC_OAUTH_ENABLED: "true"
    GF_AUTH_GENERIC_OAUTH_NAME: "authentik"
    GF_AUTH_GENERIC_OAUTH_CLIENT_ID: "<Client ID from above>"
    GF_AUTH_GENERIC_OAUTH_CLIENT_SECRET: "<Client Secret from above>"
    GF_AUTH_GENERIC_OAUTH_SCOPES: "openid profile email"
    GF_AUTH_GENERIC_OAUTH_AUTH_URL: "https://authentik.company/application/o/authorize/"
    GF_AUTH_GENERIC_OAUTH_TOKEN_URL: "https://authentik.company/application/o/token/"
    GF_AUTH_GENERIC_OAUTH_API_URL: "https://authentik.company/application/o/userinfo/"
    GF_AUTH_SIGNOUT_REDIRECT_URL:
"https://authentik.company/application/o/<application_slug>/end-session/"
    # Optionally enable auto-login (bypasses Grafana login screen)
    GF_AUTH_OAUTH_AUTO_LOGIN: "true"
    # Optionally map user groups to Grafana roles
    GF_AUTH_GENERIC_OAUTH_ROLE_ATTRIBUTE_PATH: "contains(groups[*], 'Grafana Admins') &&
'Admin' || contains(groups[*], 'Grafana Editors') && 'Editor' || 'Viewer'"
    # Required if Grafana is running behind a reverse proxy
    GF_SERVER_ROOT_URL: "https://grafana.company"
```

B. Save your Grafana Docker Compose file, and then launch the stack and access Grafana via your browser at the configured URL.

C. To confirm that authentik is properly configured with the new application, log out of Grafana and then log back in using the **Sign in with authentik** button. You should be redirected to authentik to provide credentials.

Add your first user

Now that you can access the authentik Admin interface, and you have added an application and provider, let's add a new user.

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

A. Navigate to **Directory > Users**, and click **New User**.

B. Fill in the ***required*** fields:

- **Username**: This value must be unique across all users.
- **TIP**: With OAuth2, front-channel logout is considered the default because most application (including Grafana) do not support back-channel logout.
- **Path**: The path where the user will be created. By default the new user is created in the `users` directory, but you can change that later by editing the user.
  - **TIP**: Paths are basically directories, that are used to organize your users (for example HR vs Sales, etc.). Paths do not ipoact access; they are purely organizational. Note that the top-level **users** directory displays all users in that directory and all sub-directories.

For information about the ***optional*** fields below, refer to our documentation on managing users.

- **Name**: The display name of the user.
- **Email**: The email address of the user. This is required for many integrations.
- **Is active**: Define the newly created user account as active.
- **Attributes**: You can leave this empty for this tutorial. This field can be used to store custom attributes for the user, in YAML or JSON format. These attributes can then be used within property mappings and policies.

C. Click **Create**.

2. Verify that the new user was created

- Look for the new user in the list on the **Directory** > **Users** page.

What's next?

Now that you have added your first application, and a new user, here are some typical next steps:

- Assign your new user to appropriate groups and roles.
- Configure federated or external sources (an existing source of user credentials and other user data).
- Set up MFA
- Define property mappings.
- Create a custom flow.

- Install an Enterprise license
- Create a policy to control access, force MFA use, etc..

Things to know and troubleshooting tips

Review the following information to learn more about the basics of setting up authentik and for troubleshooting tips.

Modifying the Docker Compose file

Especially when you are just starting out with authentik, we recommend that you use the default `docker-compose.yml` file that comes with the download, instead of trying to write the file from scratch. After you have successfully installed, configured, and accessed authentik, you can edit the file to do more advanced configurations, as documented in the Configuration section.

Reverse proxy

Typically authentik is set up with a reverse proxy in front of it. If you already have a reverse proxy that you are using to handle your incoming network traffic, you can simply use that same reverse proxy for authentik, by adding a few configuration values. For more details see the Reverse proxy guide.

The `latest` tag is deprecated

The `:latest` tag has been deprecated and will never be updated from the 2025.2 release. Instead, use a specific version tag for authentik instances' container images, such as `:2025.12`.

Using bindings to allow or restrict access to applications

Note that if you do not define any bindings, then all users have access to the application. To control access, you can create a binding. For more information about user access, refer to our documentation about authorization and hiding an application.

Upgrades

When you are ready to upgrade to the latest version, be sure to read our Upgrade documentation and refer to the Release Notes for the specific version.

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
-

Revision #1
Created 11 April 2026 00:11:41 by Administrador
Updated 11 April 2026 00:19:05 by Administrador