# Configure basic authentication


- Disable basic authentication
- Password policy
- Disable login form


Grafana provides a basic authentication system with password authentication enabled by default. This document details configuration options to manage and enhance basic authentication.

# Disable basic authentication

To disable basic authentication, use the following configuration:

```
[auth.basic]
enabled = false
```

# Password policy

By default, Grafana's password policy requires a minimum of four characters for basic auth users. For a stronger password policy, enable the `password_policy` configuration option.

With the `password_policy` option enabled, new and updated passwords must meet the following criteria:

- At least 12 characters
- At least one uppercase letter
- At least one lowercase letter
- At least one number
- At least one special character

```
[auth.basic]
password_policy = true
```

{{< admonition type="note" >}} Existing passwords that do not comply with the new password policy will not be affected until the user updates their password. {{< /admonition >}}

# Disable login form

To hide the Grafana login form, use the following configuration setting:

```
[auth]
disable_login_form = true
```

This can be helpful in setups where authentication is handled entirely through external mechanisms or single sign-on (SSO).

---

□□□ #2
□ □□□ □□□ 2026-10-31 16:12:51 UTC
□ □□□ □□□ 2026-10-31 16:12:53 UTC