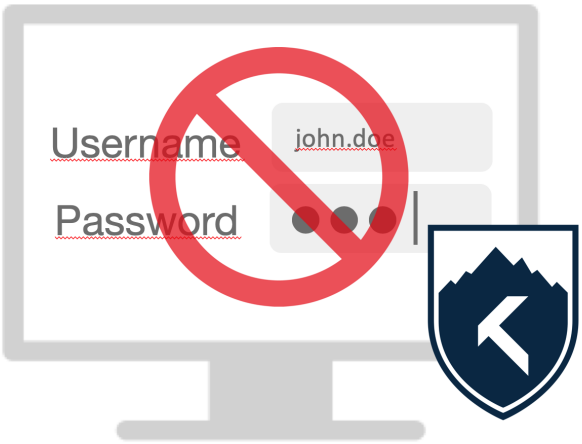
Common settings

These settings applies to both SAML and Windows Integrated Authentication (Kerberos), and are found under the Common menu.

Disable traditional username / password login

Kantega Single Sign-on does not prevent the usage of traditional username / password login by default. Any user can cancel SSO and log in manually, provided they are provisioned in a way that gives them passwords in the first place. This can sometimes be undesirable, for example when users are provisioned through AD/LDAP where passwords are available - but the organization wishes to require the use of 2FA or SmartCard.



By disabling traditional login:

- Username and password fields will be removed from login pages, making it impossible for users to authenticate through the standard login forms.
- BasicAuth is disabled for REST endpoints; any integrations you have must use OAuth.

Enabling this will no longer let you log in to an administrator account with username and password. Even so, retaining an admin account and password in the Internal directory is highly recommended as a backup in case you need to restore SSO functionality. If necessary, you may re-enable password login by deleting the following file on your Atlassian product server:

```
<atlassian_home_folder>/kerberos/disable_username_password_login.txt
```

It takes up to one minute for change to have effect if you disable by removing the file, and on other cluster nodes if applicable.

⚠ Please note that only the standard login forms are disabled, not the core password/directory system. As such, username and password login may still be usable through third party plugins/applications etc. if these run their own password validation.

Forced SSO URLs

Kantega Single Sign-on will by default only authenticate users where your Atlassian product would otherwise require them to log in with a username and password.

By activating Forced SSO URLs, users may be logged in also on pages that normally do not require this.