

Configure Password Criteria

By default, the Trifacta® application enforces very few requirements on password length, capitalization, or special characters. Users who are setting or resetting their passwords are permitted to create a password of one character in length with no additional requirements.

NOTE: When passwords are set or reset, the platform does perform an assessment of the quality of the password and reports it to the user before saving. For more information, see *User Profile Page*.

Before you permit users to create accounts, you should review the password requirements for your enterprise and, where needed, apply them to the Trifacta application.

Enable

To enable enforcement of password criteria, please enable the following parameter.

Steps:

You can apply this change through the *Admin Settings Page* (recommended) or `trifacta-conf.json`. For more information, see *Platform Configuration Methods*.

Locate the following parameter and set it to `true`:

```
"feature.enablePasswordCriteria": true,
```

When enabled, submitted changes to user passwords are evaluated based on the configuration settings defined below.

Configure

The following parameters govern the password criteria enforced by the Trifacta application when the feature is enabled.

Parameter	Description	Default
<code>webapp.passwordCriteria.length.min</code>	Minimum length of a password to Trifacta application	0
<code>webapp.passwordCriteria.length.max</code>	Maximum length of a password to Trifacta application	100
<code>webapp.passwordCriteria.description</code>	Text describing the criteria that a password must meet. Specify this value last.	
<code>webapp.passwordCriteria.contains.uppercase</code>	Defines whether the password must contain uppercase characters	undefined
<code>webapp.passwordCriteria.contains.symbols</code>	Defines whether the password must contain symbols	undefined
<code>webapp.passwordCriteria.contains.spaces</code>	Defines whether the password must contain space characters	undefined
<code>webapp.passwordCriteria.contains.lowercase</code>	Defines whether the password must contain lowercase characters	undefined
<code>webapp.passwordCriteria.contains.letters</code>	Defines whether the password must contain letters (a-z)	undefined
<code>webapp.passwordCriteria.contains.digits</code>	Defines whether the password must contain digits (0-9)	undefined

Criteria settings:

Some of the criteria settings support the following options:

Setting	Description
enforce	Each password must pass this requirement.
forbid	Passwords cannot have this requirement.
undefined	(default) This requirement is disabled. Users may choose to include or not include this requirement in their passwords.