Configuring the Team Server lockout policy

> ⚠ Only available in the BiZZdesign on-premise solution. If you are working with the cloud solution, you can contact BiZZdesign Support to submit a change request for these settings.

The Team Server lockout policy can be used to create a more secure Team Server for your organization.

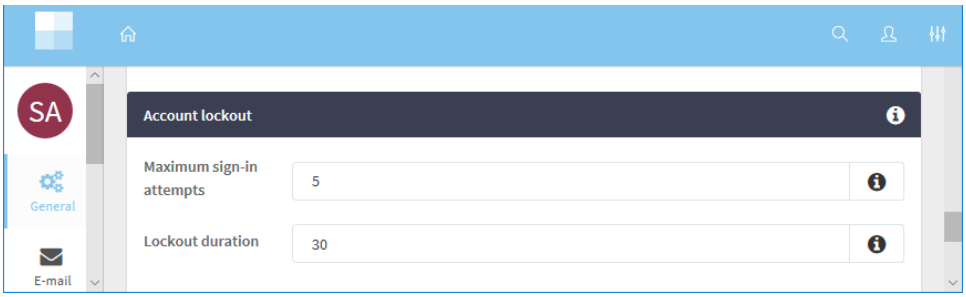
> ⓘ Changing the lockout policy should only be done by application administrators who are familiar with installing and configuring software and databases.

Required roles

System Administrator

Steps:

1. In the sidebar menu, click **Settings > General**.
2. On the general settings page, in **Account lockout**, specify the desired lockout settings.



Maximum sign-in attempts: Set the maximum allowed number of attempts a user can perform before being blocked from the Team Server for the amount of time set at the lockout duration. Initial value is set to 5. Minimum allowed is 1 .

Lockout duration: Set the amount of time (in seconds) that a user must be blocked from the Team Server after exceeding the allowed number of unsuccessful sign-in attempts. Initial value is set to 30 seconds. Minimum allowed is 1 second.

3. Click **Apply** to save the changes.

Related articles

- Team Server configuration options