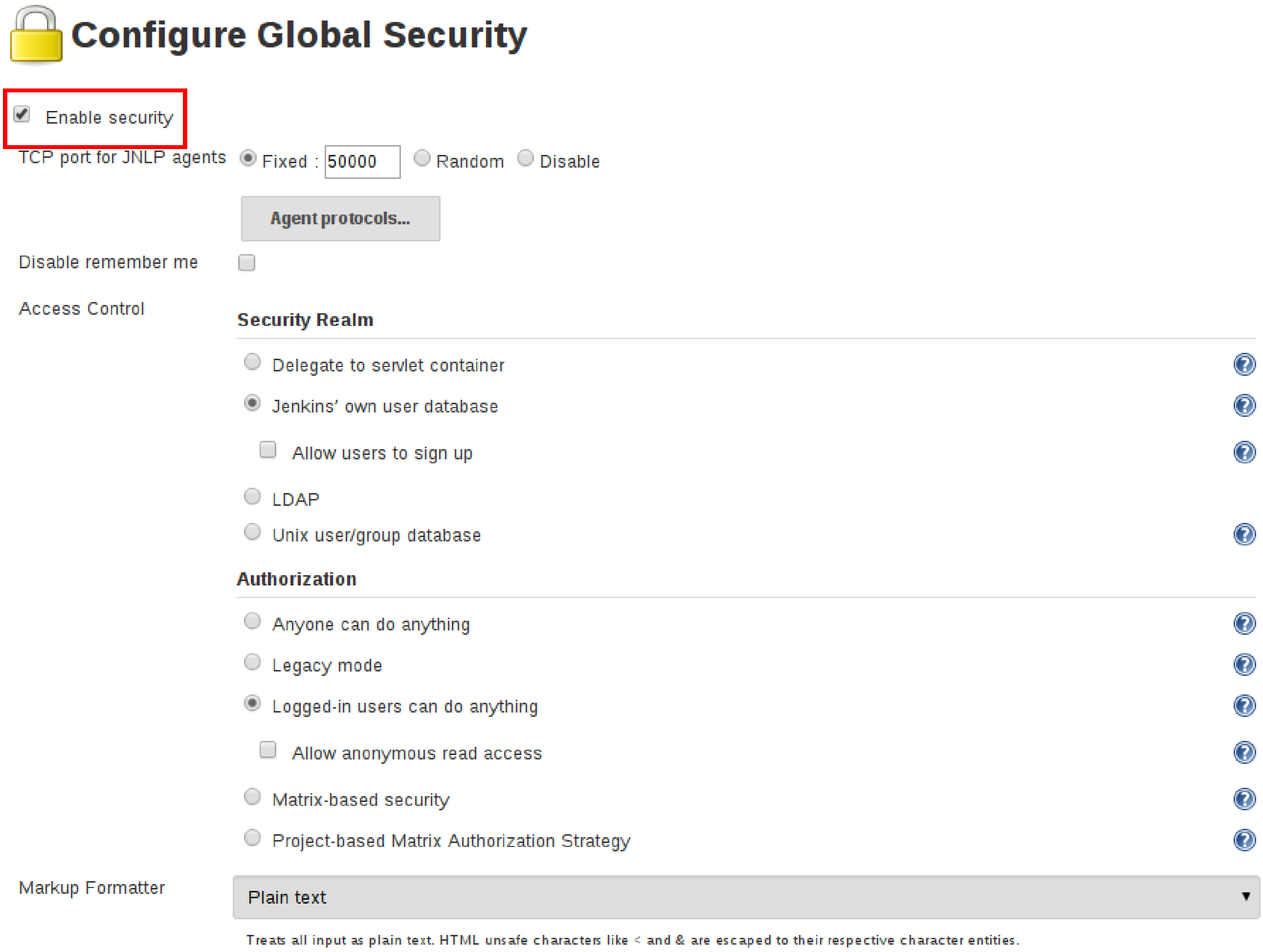
Enabling Security

When the **Enable Security** checkbox is checked, which has been the default since Jenkins 2.0, users can log in with a username and password in order to perform operations not available to anonymous users. Which operations require users to log in depends on the chosen authorization strategy and its configuration; by default anonymous users have no permissions, and logged in users have full control. This checkbox should **always** be enabled for any non-local (test) Jenkins environment.

The Enable Security section of the web UI allows a Jenkins administrator to enable, configure, or disable key security features which apply to the entire Jenkins environment.



Configure Global Security

☑ Enable security

TCP port for JNLP agents ● Fixed : 50000 ○ Random ○ Disable

Agent protocols...

Disable remember me □

Access Control

Security Realm

○ Delegate to servlet container

● Jenkins' own user database

□ Allow users to sign up

○ LDAP

○ Unix user/group database

Authorization

○ Anyone can do anything

○ Legacy mode

● Logged-in users can do anything

□ Allow anonymous read access

○ Matrix-based security

○ Project-based Matrix Authorization Strategy

Markup Formatter: Plain text

Treats all input as plain text. HTML unsafe characters like < and & are escaped to their respective character entities.

JNLP TCP Port

Jenkins uses a TCP port to communicate with agents launched via the JNLP protocol, such as Windows-based agents. As of Jenkins 2.0, by default this port is disabled.

For administrators wishing to use JNLP-based agents, the two port options are:

1. **Random**: The JNLP port is chosen random to avoid collisions on the Jenkins master. The downside to randomized JNLP ports is that they're chosen during the boot of the Jenkins master, making it difficult to manage firewall rules allowing JNLP traffic.
2. **Fixed**: The JNLP port is chosen by the Jenkins administrator and is consistent across reboots of