



Configure Global Security

☒ Enable security [?](#)

Disable remember me ☐ [?](#)

Access Control

Security Realm

☐ Delegate to servlet container [?](#)

☒ Jenkins' own user database [?](#)

☐ Allow users to sign up [?](#)

☐ LDAP [?](#)

Authorization

☐ Anyone can do anything [?](#)

☐ Legacy mode [?](#)

☒ Logged-in users can do anything [?](#)

☐ Allow anonymous read access [?](#)

☐ Role-based matrix authorization strategy [?](#)

Markup Formatter

Markup Formatter

Plain text [?](#)

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

Agents

TCP port for JNLP agents ☒ Fixed : ☐ Random ☐ Disable [?](#)

Agent protocols...

CSRF Protection

☒ Prevent Cross Site Request Forgery exploits [?](#)

Crumbs

Crumb Algorithm

☒ Default Crumb Issuer [?](#)

☐ Enable proxy compatibility

Client master on-master executors

☐ Enforce

Client master security

Security Setting Enforcement [?](#)

Policy

☒ Enforce Cross Site Request Forgery exploits prevention settings [?](#)

☒ Enforce markup formatter

☒ Enforce slave → master

Save

Apply

Authentication mapping

Trusted master with equivalent security realm

?

Operations Center		Client Master
SYSTEM	↔	SYSTEM
ANONYMOUS	↔	ANONYMOUS
user	↔	user

☐ Allow per-master configuration of authentication mapping

?

CLI

☐ Enable CLI over Remoting

?

Plugin Manager

☐ Use browser for metadata download

?

Access Control for Builds

Add ▼

API Token

☐ Generate a legacy API token for each newly created user (Not recommended)

?

☐ Allow users to manually create a legacy API token (Not recommended)

?

☒ Enable API Token usage statistics

?

☒ Enable Agent → Master Access Control

?

Rules can be tweaked [here](#)

SSH Server

SSHD Port

☐ Fixed :

☐ Random

☒ Disable

?