Jenkins　　**Configure Global Security**

🔒 Configure Global Security

Authentication

Security Realm	
	☐ Disable remember me

Security Realm

- ○ Active Directory
- ○ Delegate to servlet container
- ⦿ Jenkins' own user database
  - ☐ Allow users to sign up
- ○ LDAP
- ○ Unix user/group database
- ○ None

Authorization

Strategy

Authorization

- ○ Anyone can do anything
- ○ Legacy mode
- ○ Logged-in users can do anything
- ○ Matrix-based security
- ⦿ Project-based Matrix Authorization Strategy

User/group	Overall			Credentials					Agent							Job										Run			View				SCM	Lockable Resources		
	Administer	Read	SystemRead	Create	Delete	ManageDomains	Update	View	Build	Configure	Connect	Create	Delete	Disconnect	ExtendedRead	Build	Cancel	Configure	Create	Delete	Discover	ExtendedRead	Move	Read	Workspace	Delete	Replay	Update	Configure	Create	Delete	Read	Tag	Reserve	Unlock	View
👥 Anonymous Users	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
👥 Authenticated Users	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
👤 admin	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

> **Add user or group...**

- ○ Role-Based 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 inbound agents	⦿ Fixed : 50000 　 ○ Random ○ Disable

> **Agent protocols...**

CSRF Protection

Crumb Issuer	Default Crumb Issuer
	☐ Enable proxy compat

> **Save**　　**Apply**

☑ Enable script security for Job DSL scripts

Jenkins　　**Configure Global Security**

Strategies　☑ Run as Specific User

☑ Run as User who Triggered Build

☑ Run as anonymous

☐ Run as SYSTEM

Delete

Per-project configurable Build Authorization

Strategies　☑ Run as Specific User

☑ Run as User who Triggered Build

☑ Run as anonymous

☐ Run as SYSTEM

Delete

[Add ▾]

Hidden security warnings

This section allows you to suppress warnings, applicable to your Jenkins configuration, provided by the updates sites. If you do, they won't be shown by the Update Site Warnings administrative monitor. Checked warnings are reported (the default), unchecked warnings are hidden.

Security warnings　　☑ Matrix Project Plugin: Stored XSS vulnerability in single axis builds tooltips
https://jenkins.io/security/advisory/2020-07-15/#SECURITY-1924

☑ Matrix Authorization Strategy Plugin: Stored XSS vulnerability
https://jenkins.io/security/advisory/2020-07-15/#SECURITY-1909

☑ Jenkins core: Multiple security vulnerabilities in Jenkins 2.244 and earlier, LTS 2.235.1 and earlier
https://jenkins.io/security/advisory/2020-07-15/

☑ Matrix Project Plugin: Stored XSS vulnerability in multiple axis builds tooltips
https://jenkins.io/security/advisory/2020-07-15/#SECURITY-1925

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

Agent → Master Security

☑ Enable Agent → Master Access Control

Rules can be tweaked here

SSH Server

SSHD Port　　○ Fixed : [　　　　　　　 ⇕]　○ Random　◉ Disable

[**Save**]　[Apply]