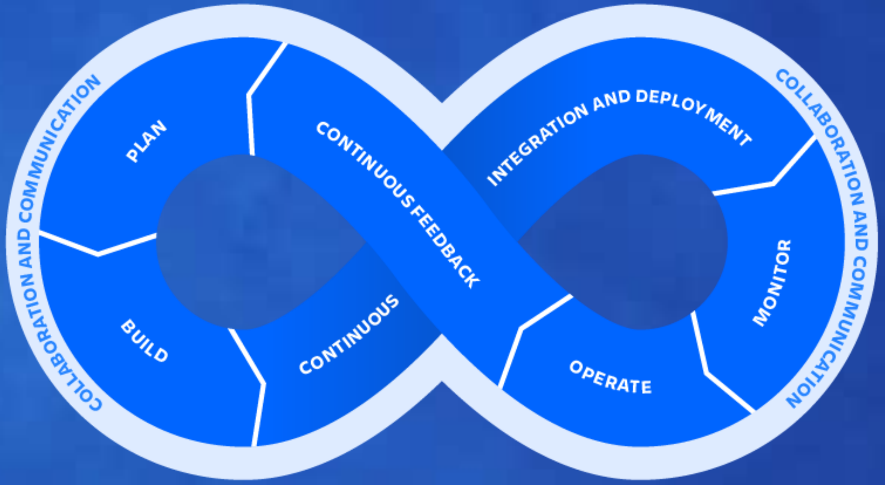

PLAN
CONTINUOUS FEEDBACK
INTEGRATION AND DEPLOYMENT
MONITOR
OPERATE
CONTINUOUS
BUILD
COLLABORATION AND COMMUNICATION
COLLABORATION AND COMMUNICATION

Session 9. Securing Jenkins

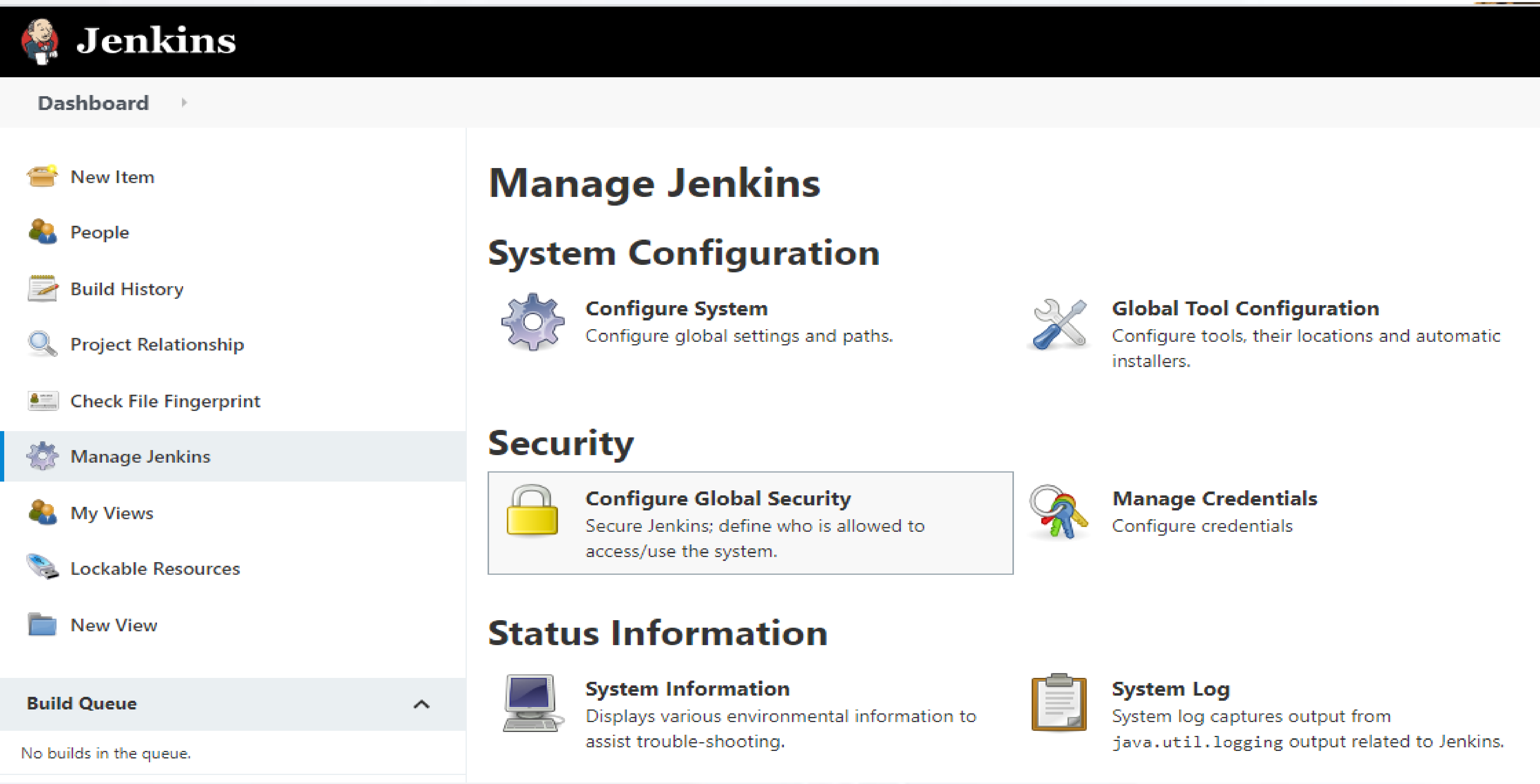
Ram N Sangwan

Agenda

- Authentication
- Jenkins Plugin
- Authorization
- Creating users

Jenkins Security

- Securing Jenkins has two aspects to it.
  - Access control, which ensures users are authenticated when accessing Jenkins and their activities are authorized.
  - Protecting Jenkins against external threats



No builds in the queue.

Manage Jenkins

System Configuration

Configure System
Configure global settings and paths.

Global Tool Configuration
Configure tools, their locations and automatic installers.

Security

Configure Global Security
Secure Jenkins; define who is allowed to access/use the system.

Manage Credentials
Configure credentials

Status Information

System Information
Displays various environmental information to assist trouble-shooting.

System Log
System log captures output from `java.util.logging` output related to Jenkins.

Access Control

- You should lock down the access to Jenkins UI so that users are authenticated and appropriate set of permissions are given to them.
- This setting is controlled mainly by two axes:
  - **Security Realm**, which determines users and their passwords, as well as what groups the users belong to.
  - **Authorization Strategy**, which determines who has access to what.
- These two axes are orthogonal, and need to be individually configured. For example, you might choose to use external LDAP or Active Directory as the security realm, and you might choose "everyone full access once logged in" mode for authorization strategy.
- Or you might choose to let Jenkins run its own user database, and perform access control based on the permission/user matrix.

Security Realm

By default Jenkins includes support for a few different Security Realms:

- Delegate to servlet container
  - For delegating authentication a servlet container running the Jenkins controller, such as Jetty.
- Jenkins’ own user database
  - Use Jenkins’s own built-in user data store for authentication instead of delegating to an external system. This is enabled by default and is suitable for smaller environments.
- LDAP
  - Delegate all authentication to a configured LDAP server, including both users and groups. This option is more common for larger installations in organizations which already have configured an external identity provider such as LDAP. This also supports Active Directory installations.

Security Realm

- Unix user/group database
  - Delegates the authentication to the underlying Unix OS-level user database on the Jenkins controller.
  - This mode will also allow re-use of Unix groups for authorization.
  - For example, Jenkins can be configured such that "Everyone in the developers group has administrator access." To support this feature, Jenkins relies on PAM which may need to be configured external to the Jenkins environment.

Jenkins Plugins

Plugins can provide additional security realms which may be useful for incorporating Jenkins into existing identity systems, such as:

- Active Directory - https://plugins.jenkins.io/active-directory
- GitHub Authentication - https://plugins.jenkins.io/github-oauth
- Atlassian Crowd 2 - https://plugins.jenkins.io/crowd2

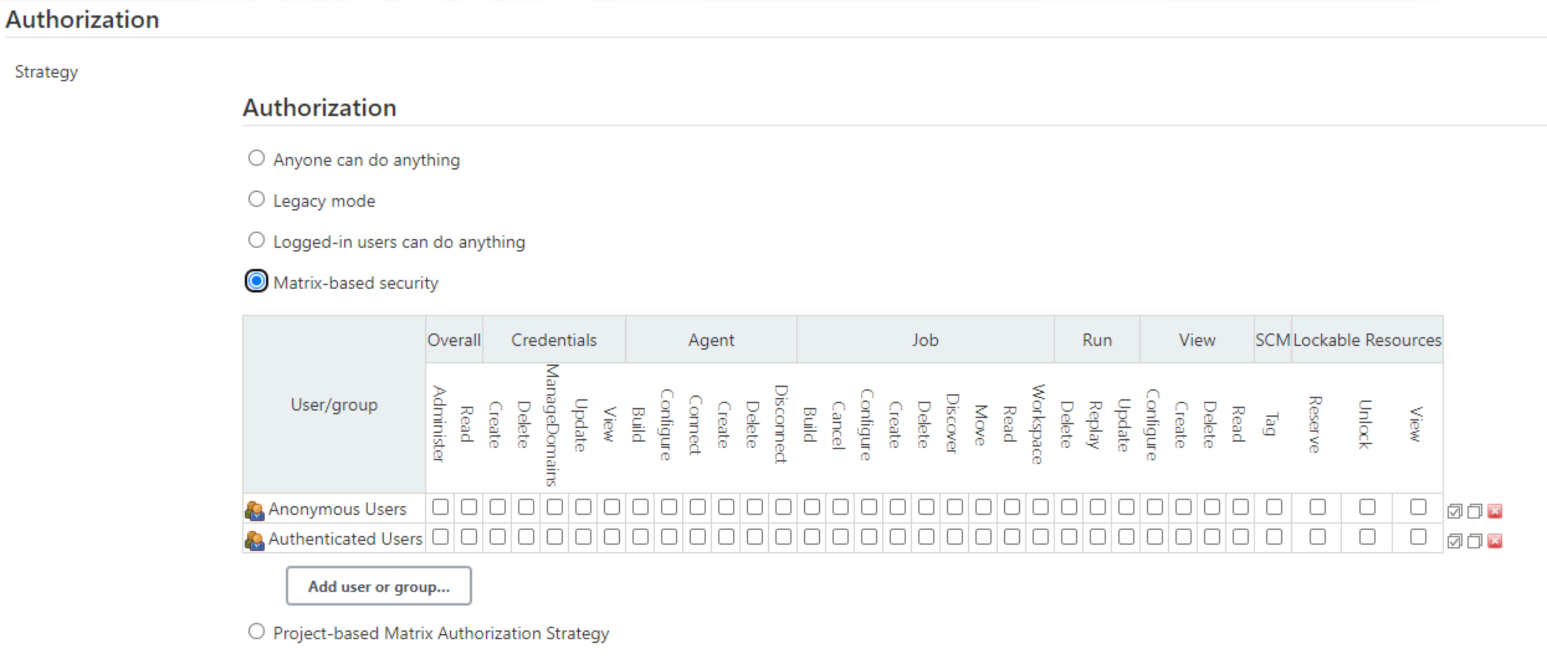
Authorization

The Security Realm, or authentication, indicates who can access the Jenkins environment. Authorization indicates what they can access in the Jenkins environment. By default Jenkins supports a few different Authorization options:

- Anyone can do anything
    - Everyone gets full control of Jenkins, including anonymous users who haven’t logged in. Do not use this setting for anything other than local test Jenkins controllers.
- Legacy mode
    - If a user has the "admin" role, they will be granted full control over the system, and otherwise (including anonymous users) will only have the read access. Do not use this setting for anything other than local test Jenkins controllers.

Matrix-based security

- Logged in users can do anything
  - In this mode, every logged-in user gets full control of Jenkins.
- Matrix-based security
  - This authorization scheme allows for granular control over which users and groups are able to perform which actions in the Jenkins environment.



Authorization

Strategy

Authorization

○ Anyone can do anything

○ Legacy mode

○ Logged-in users can do anything

● Matrix-based security

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

Add user or group...

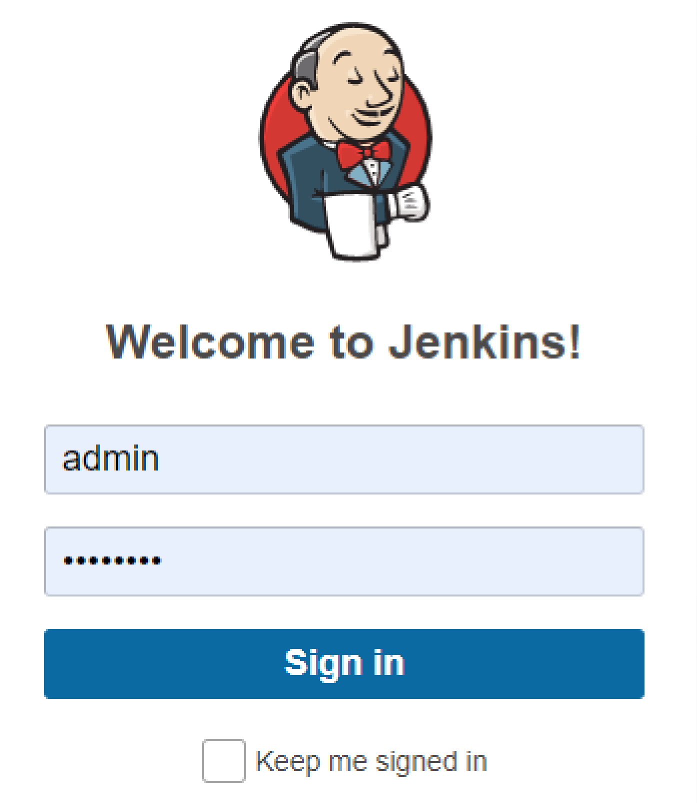
○ Project-based Matrix Authorization Strategy

Enabling Security

- In Jenkins you have the ability to setup users and their relevant permissions on the Jenkins instance.
- By default you will not want everyone to be able to define jobs or other administrative tasks in Jenkins.
- So Jenkins has the ability to have a security configuration in place.
- The "Configure Global 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.

Create/Add a User

- Login to your Jenkins dashboard by visiting http://10.10.0.100:8080/



Welcome to Jenkins!

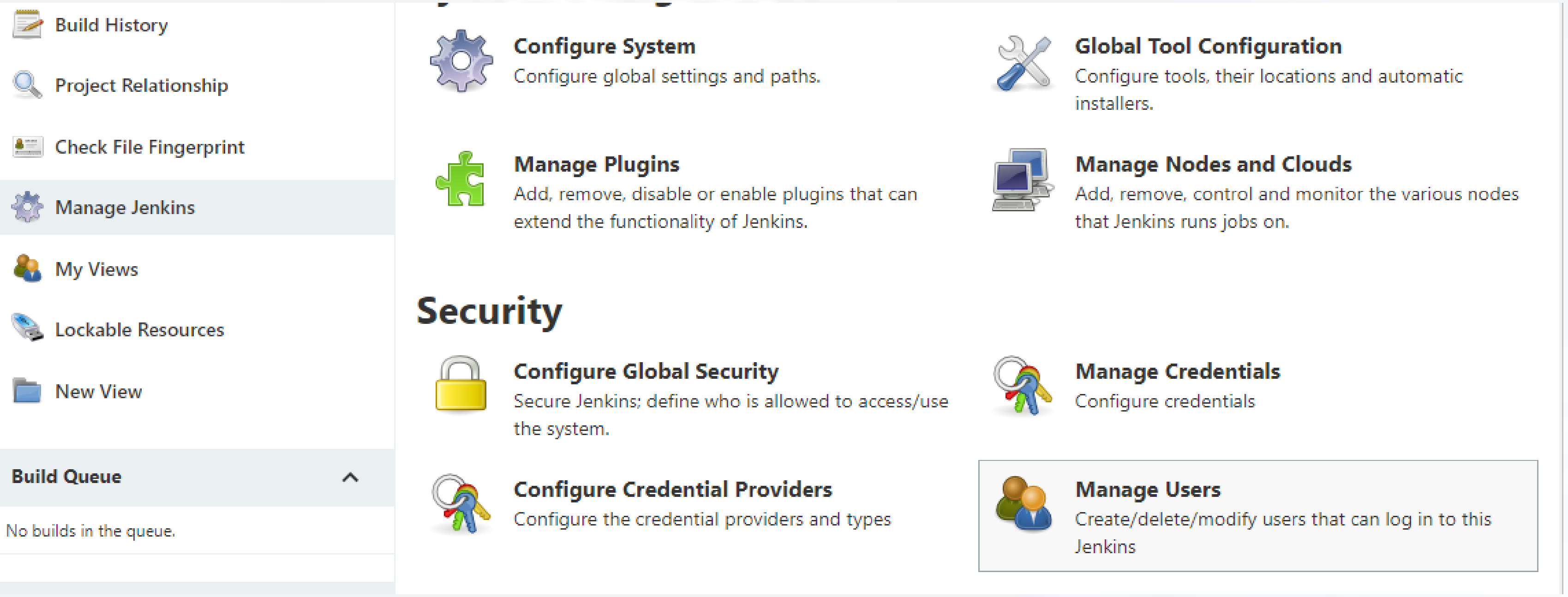
admin

•••••••••

□ Keep me signed in

Create Users

- Under Manage Jenkins, Click ***Manage Users***
- Click Create User
- Enter User details like password, name, email etc.



Configure System
Configure global settings and paths.

Global Tool Configuration
Configure tools, their locations and automatic installers.

Manage Plugins
Add, remove, disable or enable plugins that can extend the functionality of Jenkins.

Manage Nodes and Clouds
Add, remove, control and monitor the various nodes that Jenkins runs jobs on.

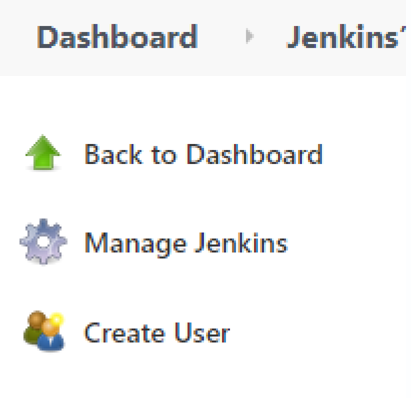
Security

Configure Global Security
Secure Jenkins; define who is allowed to access/use the system.

Manage Credentials
Configure credentials

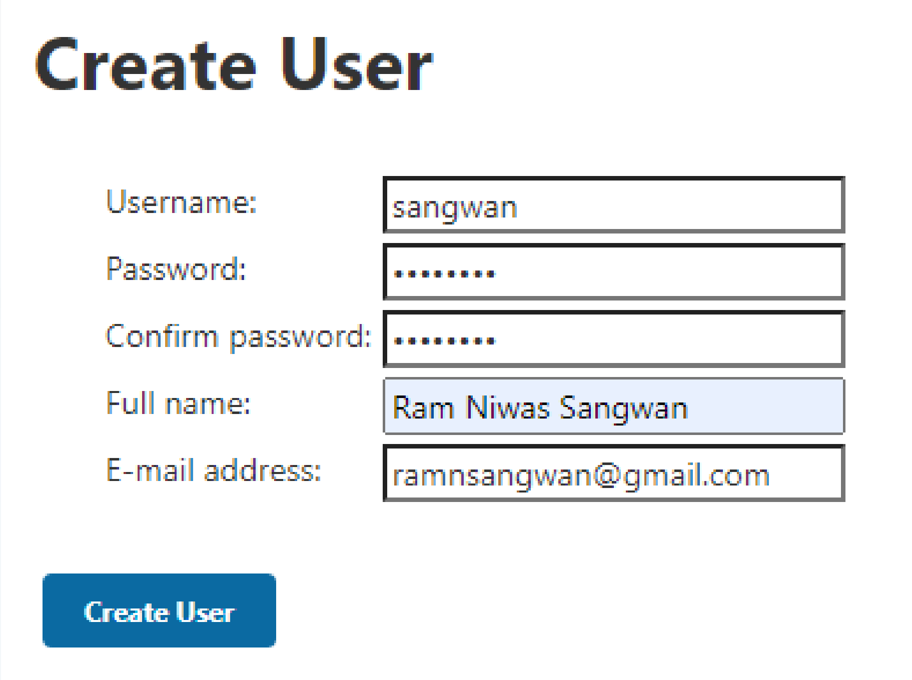
Configure Credential Providers
Configure the credential providers and types

Manage Users
Create/delete/modify users that can log in to this Jenkins



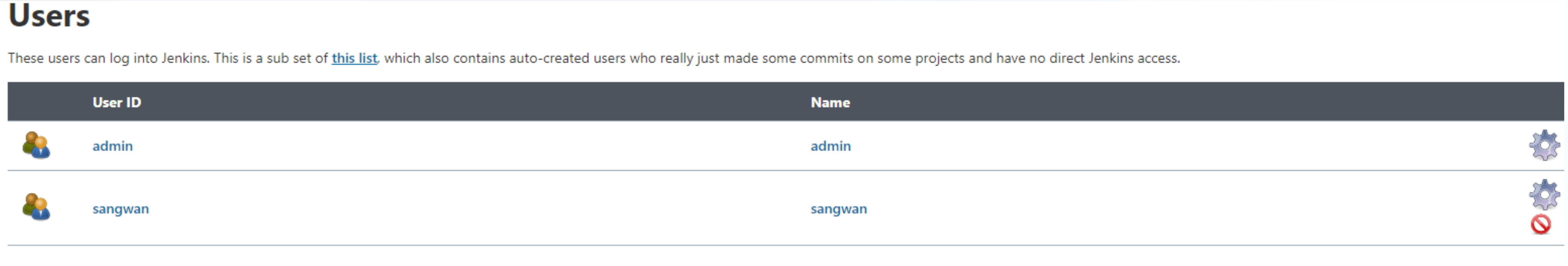
Enter User Details

- Fill in the details and click on create user.
- User will be created and appear in the list.



Create User

Username:	sangwan
Password:	••••••••
Confirm password:	••••••••
Full name:	Ram Niwas Sangwan
E-mail address:	ramnsangwan@gmail.com



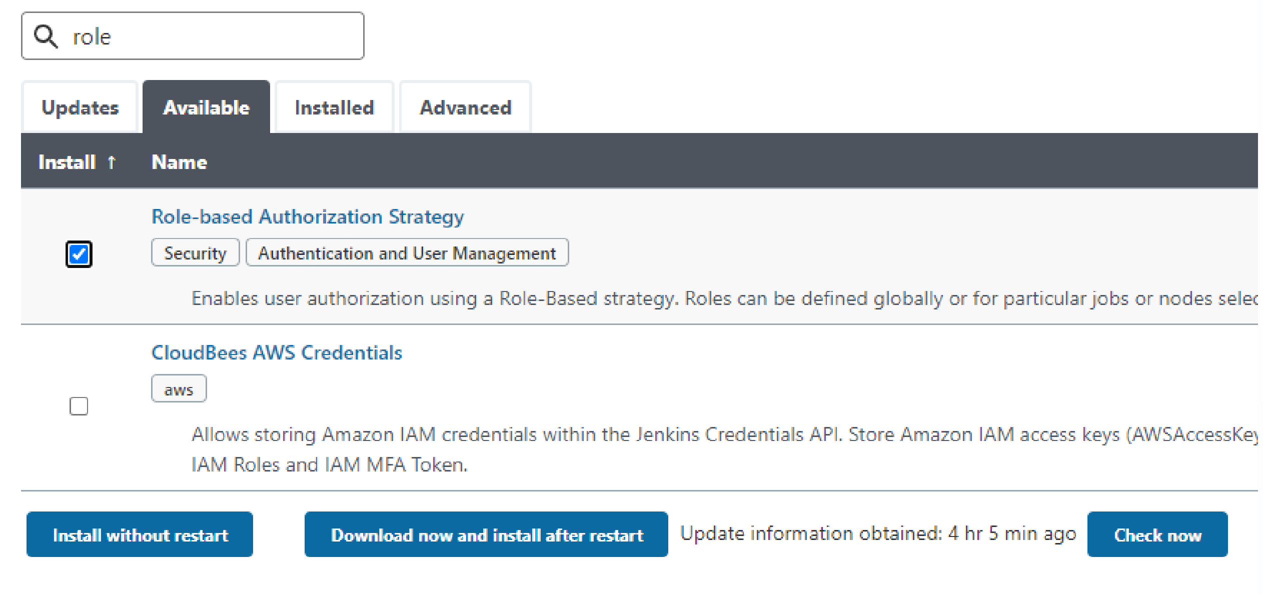
Users

These users can log into Jenkins. This is a sub set of this list, which also contains auto-created users who really just made some commits on some projects and have no direct Jenkins access.

	User ID	Name
	admin	admin
	sangwan	sangwan

Install Role Strategy Plugin

- Visit http://10.10.0.100:8080/pluginManager/available directly.
- OR
  - Go to **Manage Jenkins**
  - Click on the Manage Plugins option.
  - In available section, screen Search for "role".
  - Select **Role-based Authorization Strategy** plugin
  - Click on "**Install without restart**“

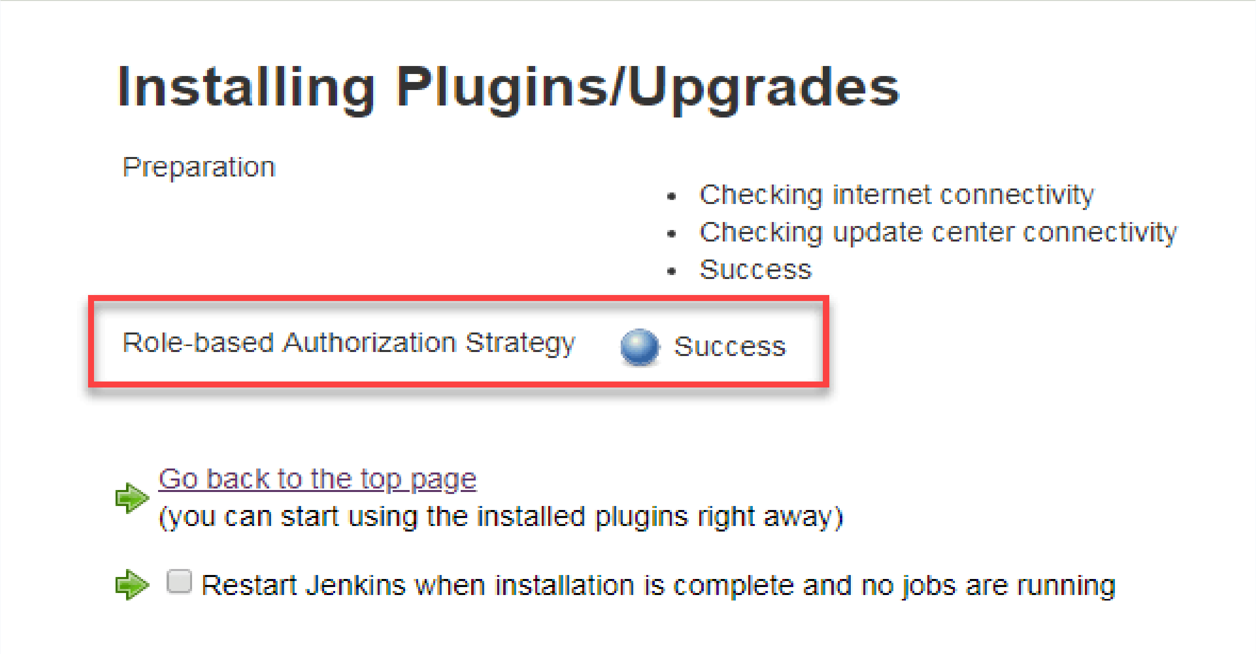


Install ↑	Name
☑	Role-based Authorization Strategy Security · Authentication and User Management Enables user authorization using a Role-Based strategy. Roles can be defined globally or for particular jobs or nodes selec
□	CloudBees AWS Credentials aws Allows storing Amazon IAM credentials within the Jenkins Credentials API. Store Amazon IAM access keys (AWSAccessKey IAM Roles and IAM MFA Token.

Update information obtained: 4 hr 5 min ago

Plugin Installation

Once the plugin is installed, a "success" status will be displayed



Installing Plugins/Upgrades

Preparation

- Checking internet connectivity
- Checking update center connectivity
- Success

Role-based Authorization Strategy ● Success

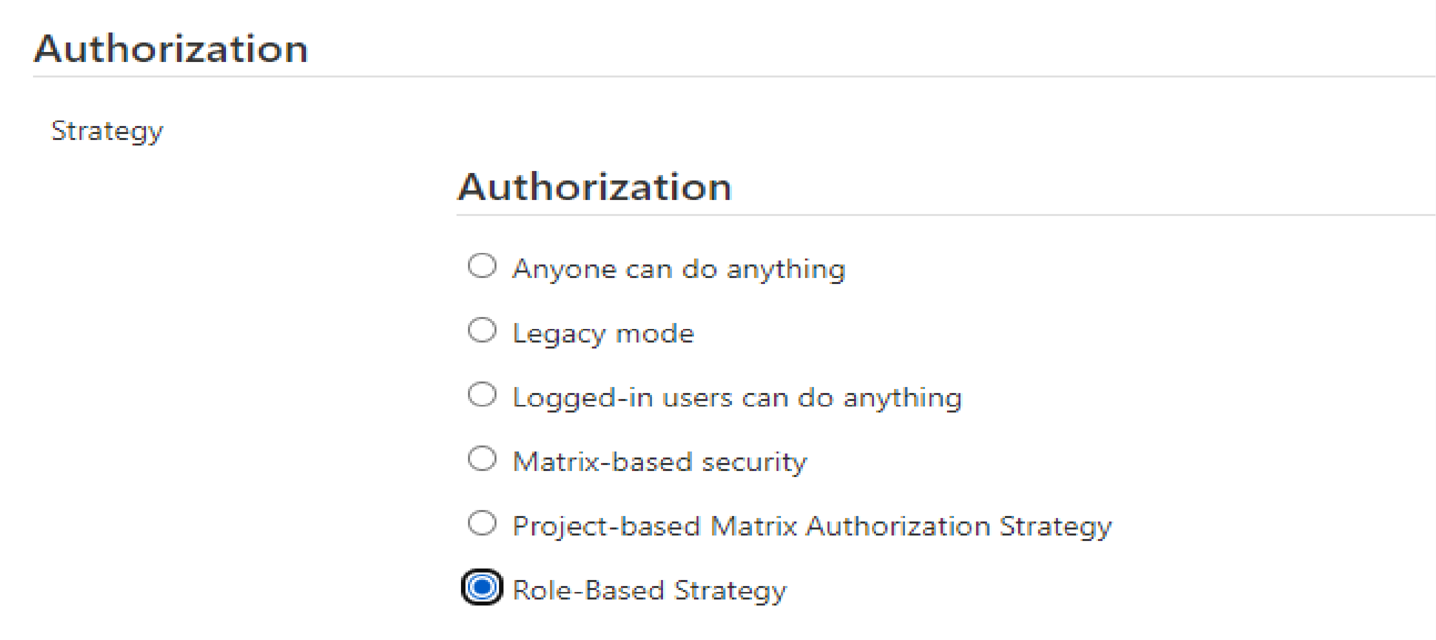
Go back to the top page
(you can start using the installed plugins right away)

□ Restart Jenkins when installation is complete and no jobs are running

Click on **Go back to the top page.**

Select Role Based Strategy

- Go to **Manage Jenkins ->** Configure Global Security -> Under **Authorization,** select **Role Based Strategy**. Click on **Save**.



Authorization

Strategy

Authorization

○ Anyone can do anything

○ Legacy mode

○ Logged-in users can do anything

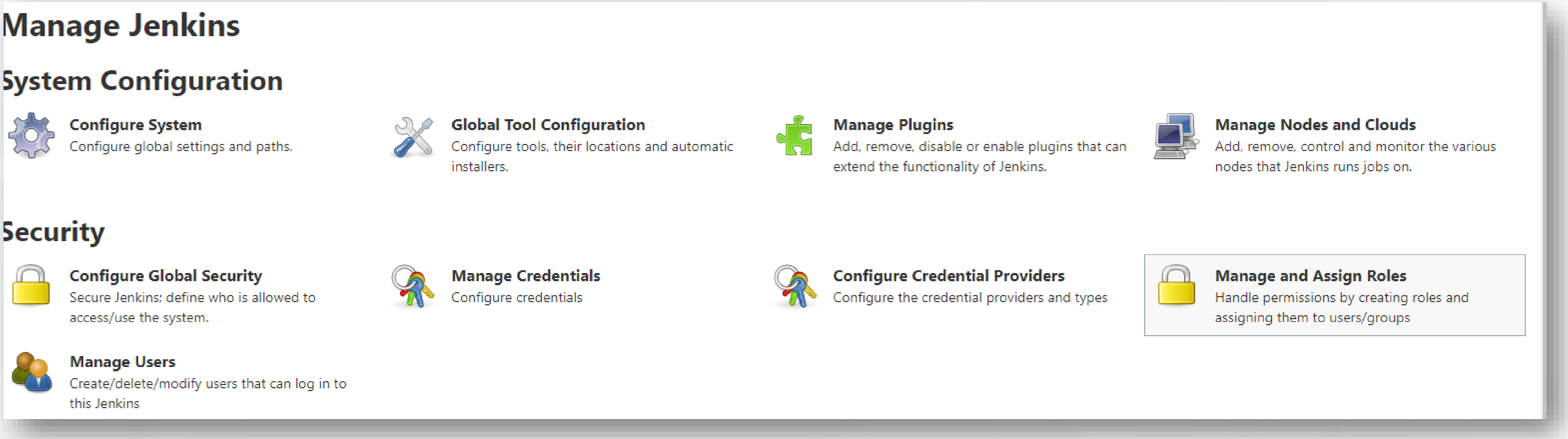
○ Matrix-based security

○ Project-based Matrix Authorization Strategy

● Role-Based Strategy

Create Roles

- Go to **Manage Jenkins**
- Select **Manage and Assign Roles**



Manage Jenkins

System Configuration

Configure System
Configure global settings and paths.

Global Tool Configuration
Configure tools, their locations and automatic installers.

Manage Plugins
Add, remove, disable or enable plugins that can extend the functionality of Jenkins.

Manage Nodes and Clouds
Add, remove, control and monitor the various nodes that Jenkins runs jobs on.

Security

Configure Global Security
Secure Jenkins; define who is allowed to access/use the system.

Manage Credentials
Configure credentials

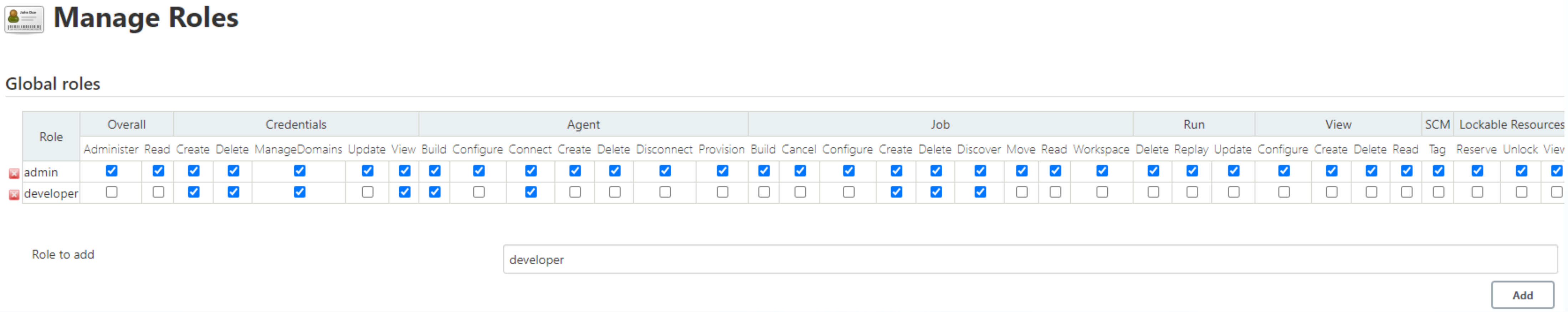
Configure Credential Providers
Configure the credential providers and types

Manage and Assign Roles
Handle permissions by creating roles and assigning them to users/groups

Manage Users
Create/delete/modify users that can log in to this Jenkins

Manage Roles

- Click on **Manage Roles** to add new roles based on your organization
- To create a new role called "developer",
- Type "developer" under "role".
- Click on "Add" to create a new role.
- Now, select the permissions you want to assign to the "Developer" role.
- Click Save



Manage Roles

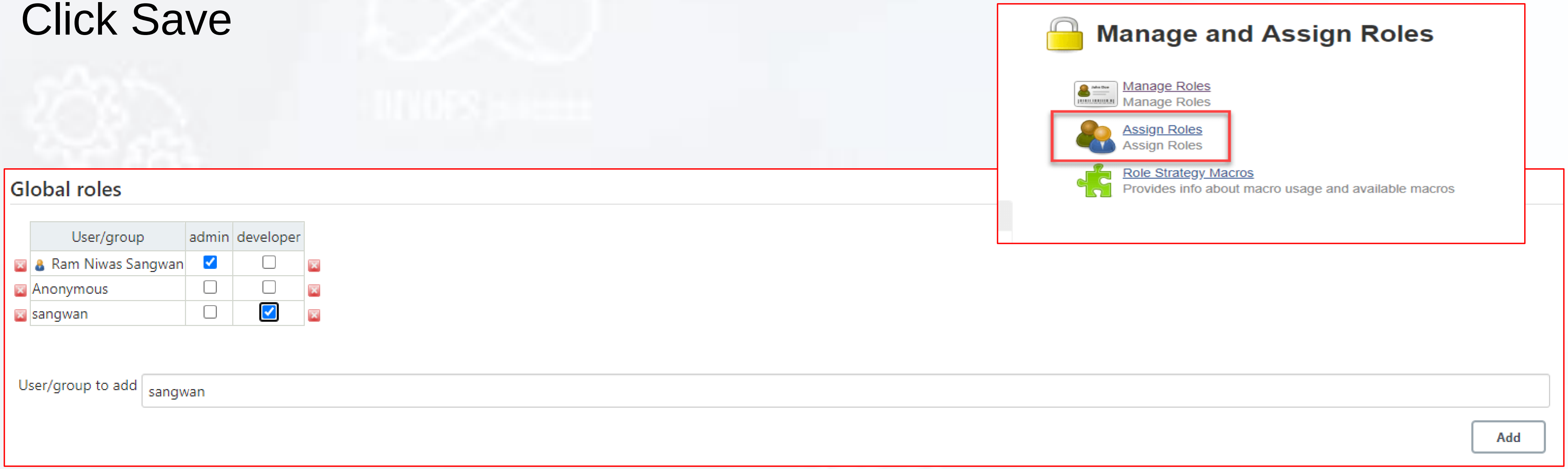
Global roles

Role	Overall		Credentials					Agent							Job									Run			View				SCM	Lockable Resources		
	Administer	Read	Create	Delete	ManageDomains	Update	View	Build	Configure	Connect	Create	Delete	Disconnect	Provision	Build	Cancel	Configure	Create	Delete	Discover	Move	Read	Workspace	Delete	Replay	Update	Configure	Create	Delete	Read	Tag	Reserve	Unlock	Viev
☒ admin	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
☒ developer	□	□	☑	☑	☑	□	☑	☑	□	☑	□	□	□	□	□	□	□	☑	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Role to add: developer

Assign the Role to User Created Earlier

- Go to **Manage Jenkins**
- Select Manage and Assign Roles
- We shall add the new role "developer" to user "**sangwan**"
- Selector developer role checkbox
- Click Save



Manage and Assign Roles

Manage Roles
Manage Roles

Assign Roles
Assign Roles

Role Strategy Macros
Provides info about macro usage and available macros

Global roles

User/group	admin	developer
Ram Niwas Sangwan	☑	□
Anonymous	□	□
sangwan	□	☑

User/group to add: sangwan

Thank You