**To set up authentication in Jenkins, follow these steps:**

1. Launch the Jenkins web interface: Open a web browser and navigate to http://<Jenkins\_host>:8080 (replace <Jenkins\_host> with the hostname or IP address of your Jenkins server).
2. Log in as an administrator: If you haven't already logged in as an administrator, log in now. You will need administrator privileges to set up authentication.
3. Access the Configure Global Security page: From the Jenkins main page, click on the Manage Jenkins link in the left-side navigation menu, then click on the Configure Global Security link.
4. Choose an authentication method: On the Configure Global Security page, select an authentication method from the Security Realm section. Jenkins supports several authentication methods, including:
   1. Jenkins own user database
   2. LDAP
   3. Active Directory
   4. OpenID
   5. SAML
   6. OAuth
5. Configure the chosen authentication method: Depending on the authentication method you chose, you will need to configure various settings. For example, if you chose Jenkins own user database, you may need to create new users and grant them privileges. If you chose LDAP, you will need to specify the hostname and port of the LDAP server, as well as the base DN and bind DN.
6. Save the authentication settings: Once you have configured the authentication method, click the Save button to apply the changes and return to the Jenkins main page.
7. Test the authentication: Log out of Jenkins and then log back in with a user account that you have set up for authentication. Ensure that the user can log in and that the authentication settings are working as expected.