Security

Out of the box, SonarQube comes with a complete mechanism to manage security (authentication + authorization). Configuring security allows you to cover two main use cases:

- Manage access rights to components, information, etc.
- Enable customization (custom dashboards, notifications, etc.) of SonarQube for users

Here are examples of security restrictions you can enforce by configuring security in SonarQube:

- Secure a SonarQube instance by forcing authentication prior to accessing any page
- Make a given project invisible to anonymous users
- Restrict access to a project to a given group of users
- Restrict access to a project's source code to a given set of users
- Define who can administer a project (setting exclusion patterns, tuning plugins configuration for that project, etc.)
- Define who can administer a SonarQube instance

For detailed explanations on how to configure the built-in security mechanism, browse Authentication and Authorization.

Authentication and authorization can also be delegated to an external system: LDAP or Active Directory with the SonarQube LDAP Plugin, PAM with the SonarQube PAM Plugin or Crowd with the SonarQube Crowd Plugin. SSO is also supported through the SonarQube OpenID plugin.

Another aspect of security is the encryption of settings such as passwords. SonarQube provides a built-in mechanism to encrypt settings.