SonarQube Integration with SIAM for Access Control

This document outlines the steps to integrate SonarQube with SIAM (Service Integration and Management) to enforce controlled access. Every new user will be required to raise a Request Item (RITM) to gain access to SonarQube. Once the request is approved, the user will be provisioned to the default group, `sonar-users`, which grants them access.

# Steps to Onboard SonarQube to SIAM

1. \*\*Confirm Default Group Configuration\*\*:  
 - Log in to SonarQube as an admin.  
 - Go to \*\*Administration\*\* > \*\*Security\*\* > \*\*Groups\*\*.  
 - Verify that the \*\*`sonar-users`\*\* group exists and is set as the \*\*default group\*\* for all authenticated users.

2. \*\*Coordinate with SIAM Team\*\*:  
 - Instruct the SIAM team to:  
 - Create a \*\*Role Entitlement\*\* for the \*\*`sonar-users`\*\* group.  
 - Link the entitlement to the default group \*\*`sonar-users`\*\* in SonarQube.

3. \*\*Define Approval Workflow in SIAM\*\*:  
 - Ensure that users must raise an \*\*RITM (Request Item)\*\* to request access to the \*\*SonarQube Role\*\*.  
 - Configure the approval flow for the entitlement in SIAM (e.g., manager approval).

4. \*\*Provision Access to Approved Users\*\*:  
 - Once the request is approved in SIAM, users will automatically be added to the \*\*`sonar-users`\*\* group.  
 - This grants them default permissions in SonarQube.

5. \*\*Disable Anonymous Access\*\*:  
 - Go to \*\*Administration\*\* > \*\*Security\*\* > \*\*Global Permissions\*\*.  
 - Remove permissions for anonymous or deprecated groups to ensure only authenticated users can access SonarQube.

6. \*\*Test the Process\*\*:  
 - Raise a test RITM in SIAM to verify:  
 - Approval flow works correctly.  
 - Users are provisioned to the \*\*`sonar-users`\*\* group.  
 - They can log in to SonarQube and access resources.

7. \*\*Communicate to Users\*\*:  
 - Notify teams that all new SonarQube access requests must go through SIAM.  
 - Document the process and share the RITM workflow for clarity.

By following these steps, SonarQube access will be efficiently managed and controlled through SIAM, ensuring that only authorized users can access SonarQube services.

# Steps to Onboard SonarQube Administrator Role to SIAM

In addition to managing access via the default `sonar-users` group, a dedicated \*\*admin role\*\* will be created in SIAM for the `sonar-administrators` group. This ensures centralized control and governance over administrative privileges.

1. \*\*Verify Existing Admin Users\*\*:  
 - Log in to SonarQube as an admin.  
 - Go to \*\*Administration\*\* > \*\*Security\*\* > \*\*Users\*\*.  
 - Identify all client users with individual admin privileges.

2. \*\*Coordinate with SIAM Team\*\*:  
 - Instruct the SIAM team to create a \*\*Role Entitlement\*\* for the \*\*`sonar-administrators`\*\* group.  
 - Map all existing client users with admin privileges to this new role.

3. \*\*Define Approval Workflow in SIAM\*\*:  
 - Ensure that any request for administrative access to SonarQube goes through the RITM process.  
 - Configure approval workflows (e.g., manager or admin approvals) for granting access.

4. \*\*Provision Approved Users to Admin Group\*\*:  
 - Once the RITM is approved, provision the user to the \*\*`sonar-administrators`\*\* group.  
 - Verify that the user has the required administrative access in SonarQube.

5. \*\*Monitor and Communicate\*\*:  
 - Periodically review users with `sonar-administrators` privileges to ensure compliance.  
 - Notify teams that administrative access requests must follow the SIAM approval process.

By implementing this approach, administrative privileges in SonarQube will be centrally managed through SIAM, ensuring proper governance and approval workflows.