# CloudBees CI (Jenkins) Onboarding into SIAM

## Overview

This document outlines the steps to onboard CloudBees CI (Jenkins) into the SIAM (Service Integration and Access Management) system. It ensures that users and roles in CloudBees CI are properly mapped to SIAM-managed roles and that necessary permissions are granted for each role.  
  
CloudBees CI (Jenkins) uses a system of roles and groups to manage access to different resources. The following roles and groups are available across different controllers in CloudBees CI.

## CloudBees CI Roles

### DevOps Internal Controller:

* System Administrator: Full access to manage all configurations, users, and system settings.
* Administrator: Administrator access to manage CloudBees CI configurations and users, but with limited system control.
* DevOps Run: Access to manage and run builds, deployments, and releases.
* DevOps Build: Access to create, manage, and execute builds and related processes.

### Other Controllers (e.g., CloudBees CD):

* Administrator: Full administrative control, including user management and system configurations.
* ReadOnly: Limited access with read-only permissions to view configurations, jobs, and builds without making changes.

These roles must be mapped to SIAM roles for ensuring proper access control and compliance.

## SIAM Integration Process

### 1. Creating SIAM Roles for CloudBees CI

Before associating users to roles, the following roles must be created in the SIAM system for each CloudBees CI controller:

* CloudBees CI System Administrator: Mapped to the System Administrator role in the DevOps internal controller.
* CloudBees CI Administrator: Mapped to the Administrator role in the DevOps internal controller or other controllers.
* CloudBees CI DevOps Run: Mapped to the DevOps Run role.
* CloudBees CI DevOps Build: Mapped to the DevOps Build role.
* CloudBees CI ReadOnly: Mapped to the ReadOnly role in other controllers.

Note: Each role in SIAM should be assigned with appropriate permissions according to the responsibilities of the CloudBees CI role.

### 2. User Creation Process in CloudBees CI

CloudBees CI users can be created manually or through LDAP integration. SIAM should ensure that every user who requires access to CloudBees CI creates a Request Item (RITM) for role approval.

#### API to Create a User in CloudBees CI

Endpoint:  
POST /createItem?name=USERNAME

Example:  
curl -X POST "https://cloudbees-ci-url/createItem?name=newusername" \  
-u "admin:password" \  
-d '<user><fullName>New User</fullName><email>newuser@example.com</email></user>'

### 3. Mapping Users to Roles in CloudBees CI

CloudBees CI uses roles to manage access. These roles need to be mapped to SIAM roles. The Role-based Authorization Strategy Plugin in CloudBees CI can be used to assign users to specific roles.

### 4. Fetching Groups and Users in CloudBees CI

To onboard CloudBees CI users into SIAM, it's necessary to fetch the groups and their associated users.

### 5. Adding Users to Internal Groups

To add users directly to an internal group in CloudBees CI.

### 6. Mapping CloudBees CI Roles to SIAM Roles

This section defines the mapping between CloudBees CI roles and SIAM roles for DevOps controllers and other controllers.

### 7. SIAM Workflow for User Access

Steps include User Request, Approval Process, Mapping Role in CloudBees CI, and granting access.

### 8. Removing Access for Users

To remove access from a user, revoke roles in CloudBees CI and SIAM, ensuring access is completely disabled.

### 9. Auditing and Logging

All access requests, approvals, and changes must be logged for compliance and auditing purposes.

## Conclusion

This process ensures that CloudBees CI (Jenkins) is properly integrated with the SIAM system for access management. By mapping roles between CloudBees CI and SIAM, access control is centralized and managed securely. Users must raise an RITM for role approval before being granted access to CloudBees CI, and the necessary permissions will be enforced for each role.