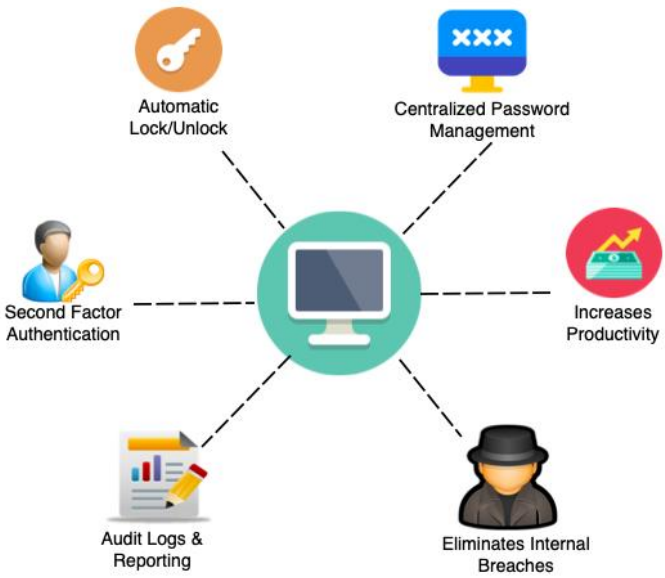
Why a Centralized Identity and Access Management System?

Businesses are becoming more and more complex day-by-day in terms of; systems being added, applications developed or acquired for various operations, more and more users coming on to IT platforms, Open API Systems, Thousands of entitlements getting generated from enterprise applications and last but not the least is the users with privileged accounts.

This leads to IT managers, especially security managers, being asked following questions:

1. What determines your employee's access to an application and with what privileges? Who authorizes them? Are they policies driven? Can they be easily verified/audited?
2. Where do your employees keep their passwords for various systems and applications they are entitled to use? What constitutes their identity? Given the mobile access to enterprise applications (or cloud-based applications), are the identities federated in a secured and controlled manners?
3. How much manpower efforts are you utilizing in servicing requests related with password change requests, adding/deleting users in Organization, provisioning new users to applications or modifying their existing entitlements (due to reasons like role change in the organization), managing entitlement changes in your applications?
4. How do you ensure Segregation of Duties in your Organization? Does your organization face rogue accounts issues? Have you checked/audited your system(s) for rogue or orphan accounts?
5. Do you have full control of Privileged Accounts? Who and why people have privileged access? When and why privileged accounts are being accessed and by whom?

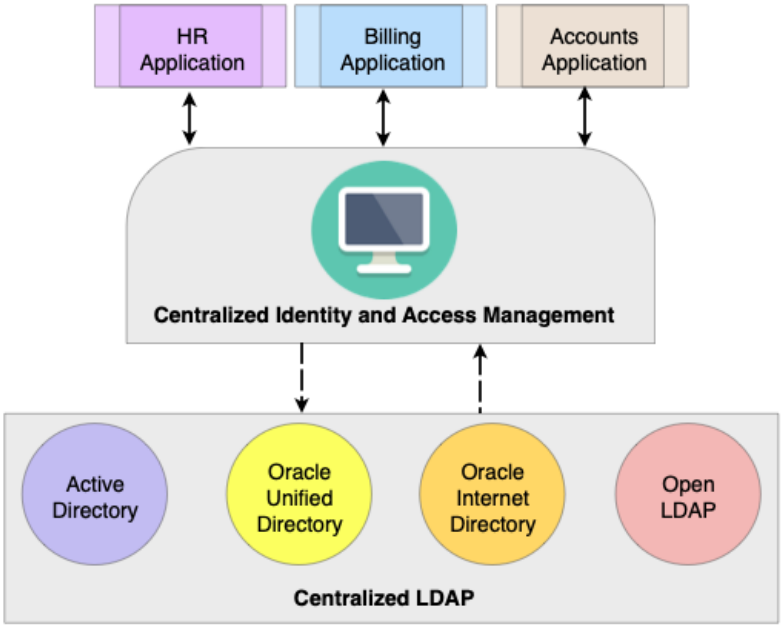


The answers to all these questions lie in implementing a Centralized Identity and Access Management System (CIAMS). In a centralized system, rather than having multiple accounts to use various work resources, each

employee, partner, or customer can reach all the applications, services, and resources they need through a single profile. A centralized access management for customer and partner-facing applications can also provide a big opportunity to set your company apart. CIAMS manages the followings:

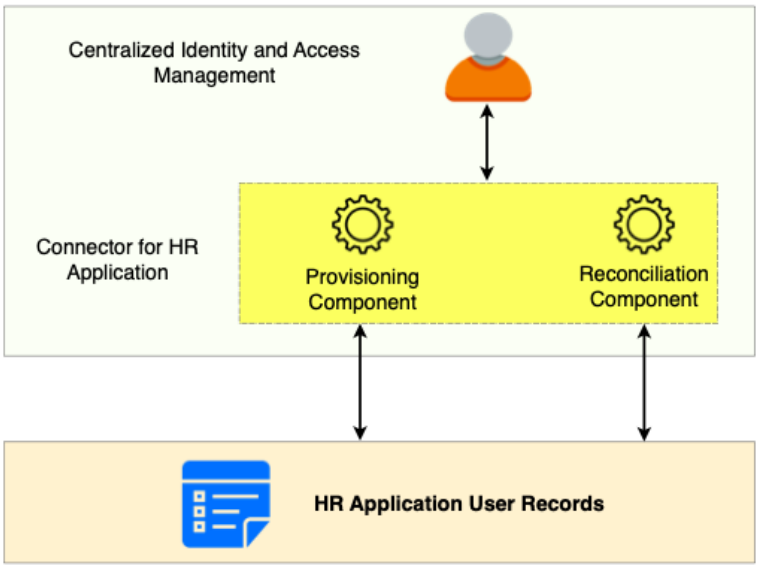
1. A central LDAP based directory of users and password.

   CIAMS uses its own central LDAP based directory to store user profile information along with user's credentials. Central LDAP repository can be synced with other LDAP repositories using LDAP connectors if required.



2. On-boarding a new user into the Organization. Organizations needs to synchronize this to the HR System since HR is the first organization to know when a person is entering and leaving the organization.

   New user can be created on both systems either in Centralized Identity Management System or HR Application. Using CIAMS Connectors user information sync between CIAMS and HR Application.



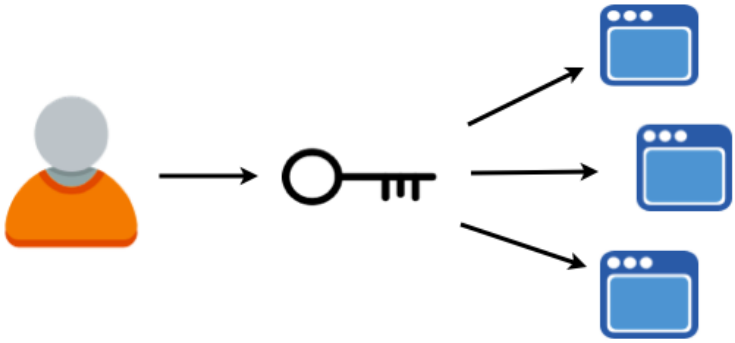
3. Defining password policies and retention rules.

   Password policy help/force users to create strong passwords. Administrators can set password expiration time, user lockout (permanent/temporary), automatic unlocking etc. Common configurations for password policy are listed below:

   - Minimum/Maximum Uppercase Characters
   - Warn After
   - Expire After
   - Disallow Last Passwords
   - Maximum Attempts
   - Permanent Lockout
   - Lockout Duration

4. Enabling Single-Sign-On across all applications.

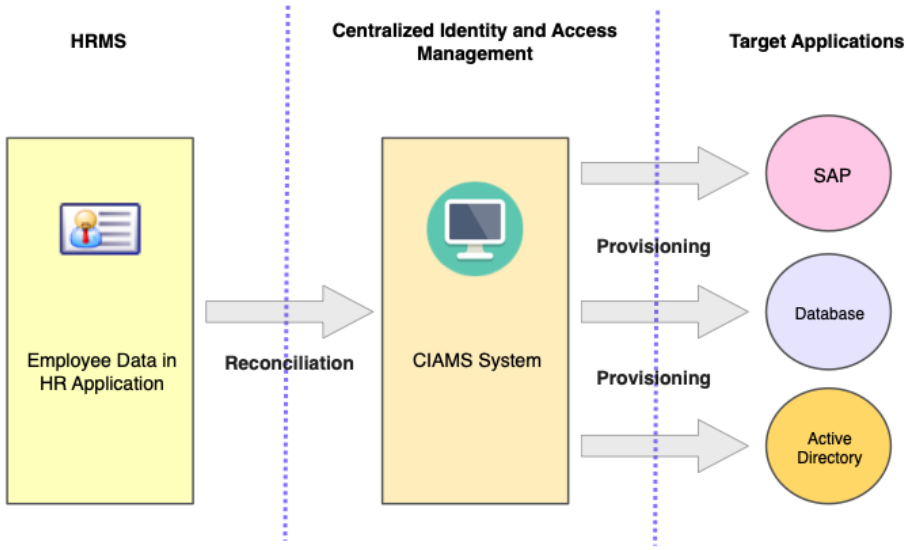
   Single sign-on (SSO) allows access control of multiple related, independent applications to be accessed by logging in just once and access all required resources within applications without logging in again.



5. Provisioning a user across all required applications based on either policies or requests workflows.

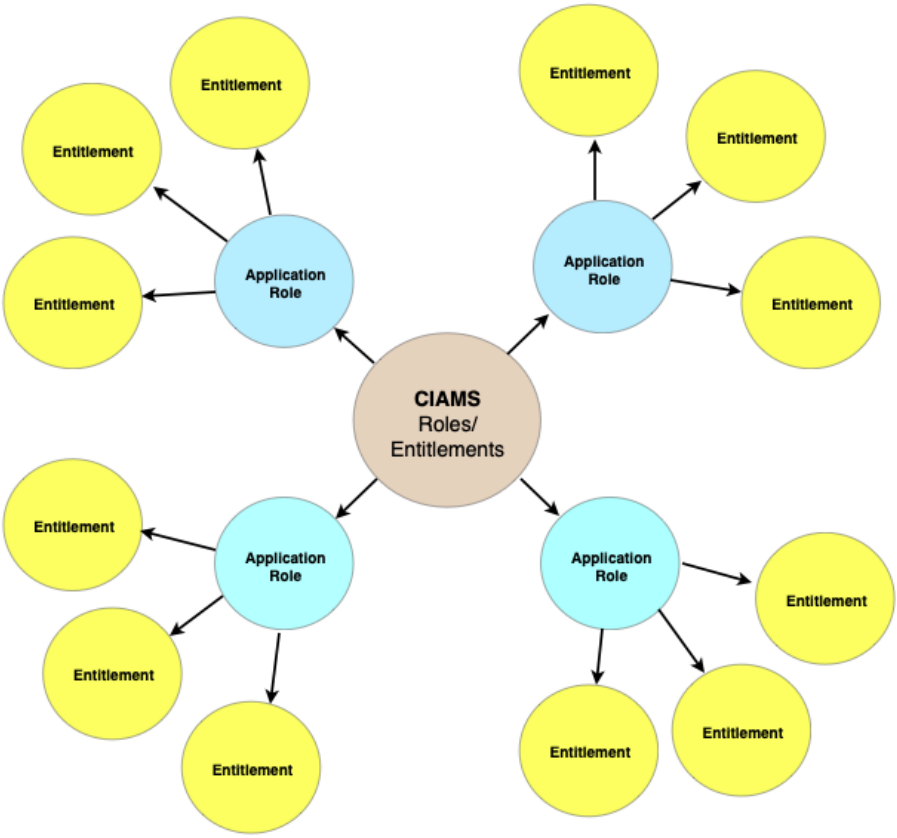
   CIAMS provides out-of-the box connectors and framework to develop custom connector. These connectors can be configured with CIAMS to handle provisioning and reconciliation operations.

   For example, CIAMS can reconcile existing users from HR system and provision these users to multiple target applications. Administrator can configure rule base access policy which trigger user provisioning to different applications based on configured rules.



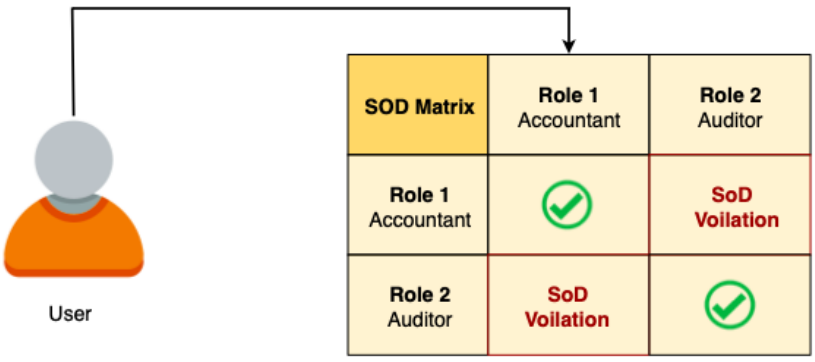
6. Defining centralized roles and assigning them to users and aligning them with Applications entitlements.

   CIAMS Administrator can define centralized roles which can be assigned to different users and applications. A role with an application can contain set of entitlements which can be managed through CIAMS. Different applications can have different set of Roles and Entitlements which can be reconciled from target system using connectors. If new Role/Entitlement is added through CIAMS then it can be provisioned to target application using CIAMS connectors.



7. Maintaining rules for managing conflicting roles and entitlements.

   CIAMS Administrator can define rules for conflicting roles and entitlements. For example, a rule can be defined for Role1 (Accountant) and Role2 (Auditor) which are mutually exclusive and should trigger an alarm for SoD violation if requested together. If a user generate request for both Roles (Accountant & Auditor) then his approval authority (manager) will see SoD violation.



8. Providing ready-to-use audit reports on authorizations and entitlements.

CIAMS provide audit logs for different system events like authentication, authorization, user profile create/update, password policy, approvals, entitlement assignment etc. Audit logs are provided in terms of file system and database. CIAMS reporting tool directly capture audit data from audit database for reporting purpose. Reports can be customized for end-user perspective and exported into different required formats (xls, pdf, html etc.).

9. De-provisioning users from all applications after he resigns.

   CIAMS rule base access policy (attached with connector) can be configured for provisioning and de-provisioning operations. After user resigns from organization, its status in HR application is marked as de-activated. Based on user status marked in HR application, CIAMS rule triggers access policy to de-provision user from attached target applications.

10. Defining privileged accounts/accesses and provisioning them to privileged users. A privileged user is someone who has administrative access to critical systems. For instance, anyone who can set up and delete user accounts and roles on Oracle database is a privileged user. The CIAMS also monitors and logs the actions carried out by such users.

    To access critical systems in organization, privileged user need to login into privileged account manager and checkout application to get its credentials. Every checkout generates different password. Once privileged user completes work then he check-in (release) application which invalidate credentials generated after checkout.

11. CIAMS works on standards like SAML 2.0 and federates the identity across cloud-based applications.
12. In addition to CIAMS, Cloud Access Security Brokers can be deployed to enforce security, compliance, and governance policies for cloud applications. CASBs help organizations extend the security controls of their on-premises infrastructure to the cloud.