ORSUS
LIFECYCLE MANAGER

ORSUS LIFECYCLE MANAGER

Management of digital indentities plays a critical role in maintaining relationships between employees, customers and clients. Due to the increasing number of business applications today, many organizations need to attain granular visibility into what users have access to, as far as governance, risk, and compliance are concerned. Without an automated and simplified way to manage discrete identities and their access, managing IAM (Identity and Access Management) landscape becomes more complex, posing challenges to secure identities and access control. This may leave an organization's digital infrastructure vulnerable, generate compliance issues, security risks, and result in potential gaps due to a siloed approach.

ORSUS Lifecycle Manager (OLM) is a secure and modern platform that supports your digital strategy to manage identities and access to disparate applications and data across several environments. The capabilities of this platform help you cover business, technical and organizational aspects of IAM, while reducing the complexity inherited from the dynamic nature of identities, processes and applications.

"A Modern Identity, Access And Security Management Platform"

OLM FEATURES AND FUNCTIONALITIES

Lifecycle Management

Automate the entire identity lifecycle management process based on attribute/rule-based provisioning policies, multi-source synchronization, reconciliation and orphan account management.

Account Management

OLM ensures that any given identity has access to the right resources (applications, systems, etc.) and within the correct context. We offer a high degree of integration between identity management and access management, allowing stronger control and audit over all accounts and access.

Non-User Account Management capitalize Shared accounts for consistency

OLM provides a comprehensive governance model to efficiently manage non-user identities across Admin accounts, Service accounts, Test accounts, Training accounts, Exchange accounts, Impersonation accounts and shared accounts. As non-user accounts require specialized onboarding, access and target resources, the OLM platform simplifies and streamlines the processes that include self-service-based onboarding, policy-based provisioning, automated recertifications, extensive logging and monitoring techniques.

Role Management

Using OLM, you can efficiently govern role-based access control for multiple systems and applications within a single console, reducing the workload of administrative staff and IT support in permission assignment.

Group Management

IAM involves various critical roles across an organization's security "stack," but these roles are frequently overlooked because they are distributed across various groups such as all employees, application admins, etc. OLM helps you with all group access controls including handling exceptions, policies, reconciliations, recertifications, reports and more.

Applications & Entitlements

OLM establishes fine-grained level access management through entitlements. It simplifies the application access by supporting both group-level and role-level entitlements, offering authorized users the flexibility to add one or more groups and/or

OLM streamlines the process of assigning entitlements to the users via on-demand, self-service based requests, while having custom workflows in place to apply appropriate scrutiny for authorizing the requests. Similar to group and role management, users' application entitlements can be recertified, monitored, and audited using governance and compliance controls.

Access Recertifications

OLM gives authorized users the power to review and manage internal and external users' access rights. Using OLM, you can create adhoc based recertifications as well as campaign-based review schedules to validate accounts, groups, roles, entitlements and their assignments within an intuitive UI.

Workflow Management

Customize, construct and automate your business processes through intuitive drag-and-drop workflows for setting up new accounts, roles, and groups to assign memberships and certify access rights.

Self-Service

OLM allows users to request accounts & access, respond to approvals, track the status of various requests submitted, manage delegations and reset passwords.

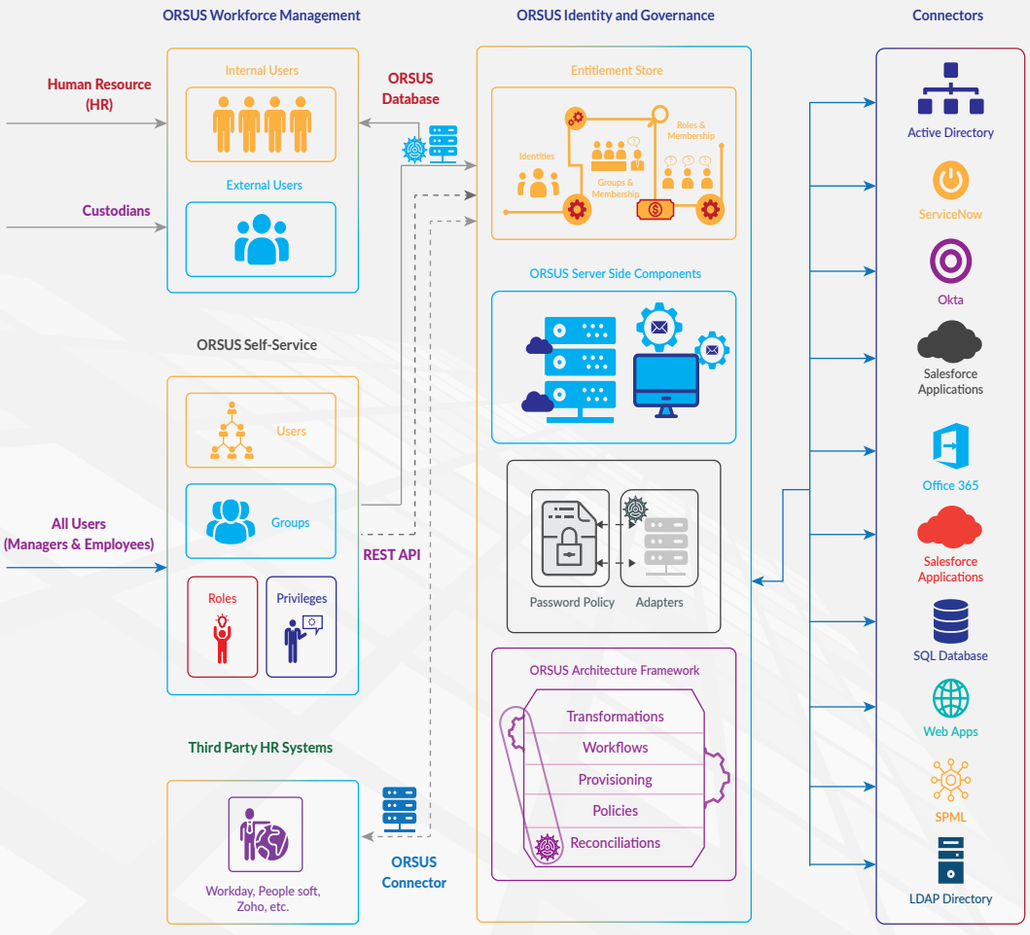
Integrations and APIs

OLM helps you leverage out-of-the-box connectors to integrate with leading applications to manage identities and security across all lines of your business.

Access Policies

OLM helps you automate the entire lifecycle of identities using a policy-driven approach. You can create and enforce policies based on granular and contextual information that defines how individual users can access applications, such as birth right policies, user's attributes change related policies, etc. This automated approach comes with customizations to add enforcement rules for each policy to manage groups, roles, entitlements, and application/systems access to identities.

OLM ARCHITECTURE



WHY OLM?

Integrated Solution

Get a 'best-fit' IAM controlled architecture to streamline, automate and simplify all your business processes involved in managing identities and their access.

Simplified Security and Compliance

Deliver smarter security and meet your increasingly stringent compliance requirements through governance controls and access policies.

Save Time

Use automated workflows and save time to onboard/off-board users with minimal human error, save audit review time to validate access, and accelerate time to market.

Scalability

The solution has been developed and tested to meet the size criteria for any type of market and to support growing usage.

Lower Costs

Achieve significant cost savings by reducing operational and support costs, automating manual workflows for administrative business processes, such as identity administration, password resets, etc.