ORACLE
FUSION MIDDLEWARE
IDENTITY MANAGEMENT

Oracle Identity Cloud Service

A Business Overview

ORACLE WHITE PAPER | SEPTEMBER 2016

ORACLE

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Table of Contents

Executive Overview

In new competitive business landscape organizations are trying to launch new services in a quickest timeframe to take early bird advantage. They want to reach out to more people and endorse their brand through social media. They want to launch mobile applications to give better services to their customers and get competitive advantage. Most of these organizations are developing and hosting these services using PaaS/SaaS model so that can avoid hassles of developing or managing them in-house.

Security is one of the most critical and important aspects for every new initiative. Data loss & leakage risks, unauthorized access through misuse of credentials and improper access controls, hijacking of accounts and malicious insiders are some of the biggest concerns that are always present in the ever faster delivery of these new services.

Identity & Access Management (IAM) can provide a single aggregated view of identities to all systems, it enables multi channel access and provides a platform to define and enforce policies at one layer to ensure consistency. An important consideration for these organizations is to define how IAM is implemented for these new initiatives/services. They can implement security for each application in a monolithic, distinct and unique fashion for that application or they can leverage a platform approach which can give them a shared single identity across multiple applications, shared services, shared policies across multiple applications and provide cross channel visibility.

The ability to enable business and drive new opportunities through a solid secure infrastructure and a platform designed for this kind of business agility is where the new business opportunity lies today.

This white paper discusses how Oracle's Identity Cloud Service can be used to enable organizations to rapidly develop fast, reliable and secure services for their new business initiatives.

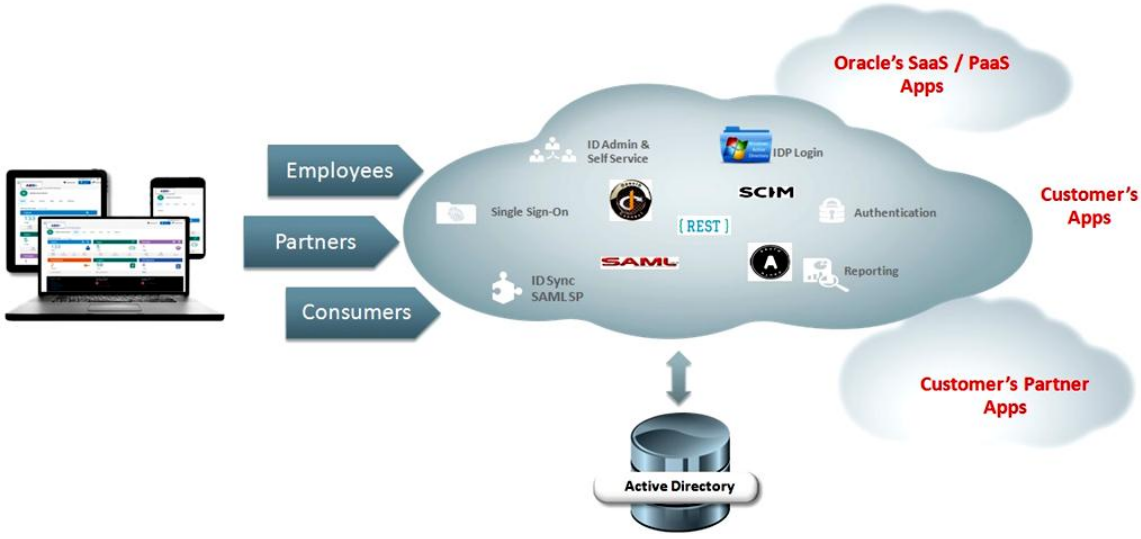
Market Trends and Business Drivers for Cloud IAM

- **Increasing SaaS Adoption**
  - More and more sales, IT and Business functions are moving to the cloud. Enterprises want to manage access to these SaaS applications as an extension to their on-premise applications.
- **Strong Security**
  - As data moves from on-premise to cloud and more corporate data is exposed via multiple channels, there is a critical requirement of strong authentication for user's access, channel security to ensure data is secure in transit and authorization controls to ensure only authorized users access the data.
  - Enterprises need a platform that can act as a security broker for OAuth and Federation to enable service to service communication and support Identity propagation.

- **Single Sign On**
  - With the adoption of a SaaS application, providing SSO between SaaS apps and Enterprise apps has become even more challenging.
  - Companies want to enable access to partners and consumers and allow them to use their social identity
  - Demand for SAML and Open ID Connect is increasing
- **Co-exist with Existing IAM Infrastructure**
  - Controlling access to cloud applications is one challenge but there are still a plethora of legacy on-premise applications.
  - Only a hybrid solution that can connect the cloud and on-premise can provide a complete solution to extended enterprise control.
- **Connect Enterprise Directory to Cloud**
  - Customers don't want their existing users to remember new passwords to enable Cloud access.
  - Enterprises want to connect their directory infrastructure to the Cloud to re-use their investments in directory infrastructure and create a near seamless incorporation of Cloud services into their business.
  - On-Premise AD is the most widely used IDP for employee populations.
- **Hybrid Multi Channel Access**
  - Any device, anywhere, anytime access is the key ask from customers which requires enabling multichannel access for the services
  - Only a security platform that is built on open standards, which is context aware can enable customer's services on motile channels while ensuring security and consistency.
- **Simplicity and Performance**
  - Get users productive faster through immediate access to key applications and systems.
  - Enhanced User Productivity and experience by providing self-service and SSO solutions.
  - Scale up to millions of users.

Core Solution Components

Oracle Identity Cloud Service provides a number of core services, each of which solves a unique challenge faced by many enterprises.



Elastic, Multi Tenant Platform based on Microservice Architecture

Oracle Identity Cloud Service Management provides an innovative, fully integrated service that delivers all the core identity and access management capabilities through a multi-tenant Cloud platform. The design of the next generation Identity Cloud Service (IDCS) is based on the microservice architecture which is naturally aligned with Cloud principles of Scalability, Elasticity, Resilience, Ease of Deployment, Functional Agility, Technical Adoption and Organization Alignment.

Reduces complexity

Traditionally on-premise IAM implementations can be costly as they provide greater flexibility for customizations. Oracle Identity Cloud Service is designed to provide maximum configuration to support customer business processes and reduce the burden of implementation costs. It is designed with the following key considerations:

- More configuration and less customization
- Business Friendly UI
- Focus on simplicity and easy of usage

Pay As You Go Model

- The business does not need to buy hardware to install the product. There is no upfront perpetual license cost.
- Customers need to pay only for what they use. They can scale the number of users and applications up or down as needed during their contract.
- Security teams need only manage configurations and policies. They are no longer required to do the operational activities of maintaining the solution itself. They need less specific technical skills and resources to manage the solution.
- Ideal solution for small businesses that can't afford on-premise IAM solution

Support for Open Standards

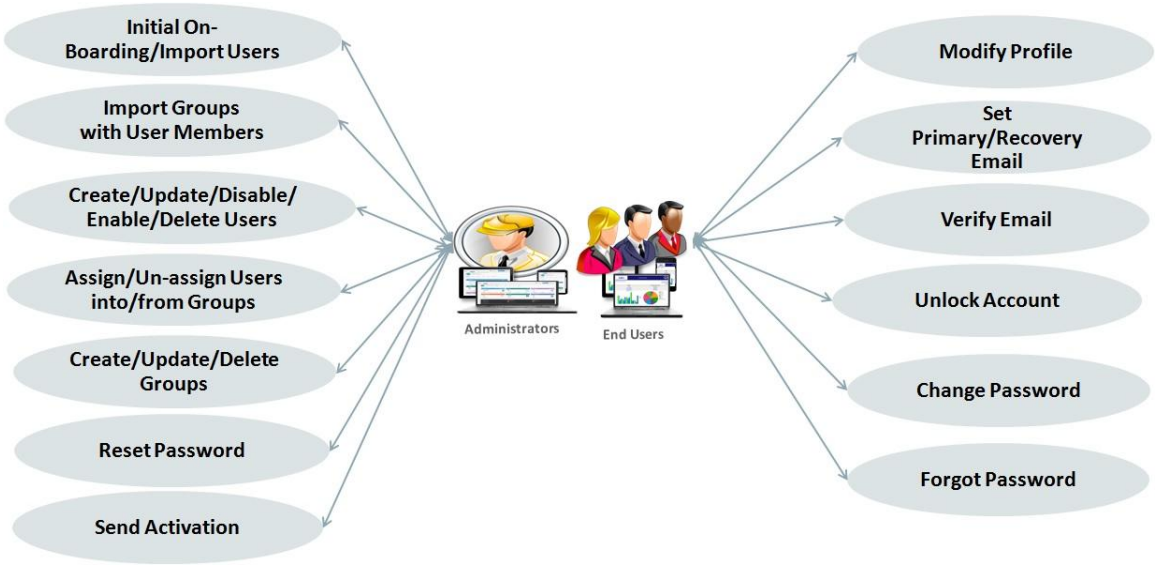
All components of IDCS are built on modern Cloud principles and use standard open stack protocols.

- **OpenID Connect** for browser-based user authentication
- **OAuth2** for securing REST API calls
- **HTTP cookies** for tracking user's active sessions
- **JWT-based tokens** for applications to map authenticated Cloud identities to local application identities
- **SAML** for providing Single Sign on for Cross Domain applications using Federation
- **SCIM** for simplified user management in the Cloud by defining a schema for representing users and groups
- **RESTful APIs** for all identity functions for customization and headless operations

Identity Administration across SaaS Apps and On-Premise Active Directory

As businesses are adopting more SaaS applications with the intent to extend or leverage their on-premise infrastructure, management of identities across these hybrid environments has become more challenging. IDCS provides a unified view of user access to SaaS applications and On-Premise AD. It provides administrative interfaces to manage these identities and also provides self service interfaces to end users so that they can manage their own profile and password and reduce administrative/help desk burden.

Oracle Identity Cloud Service seamlessly integrates with On-Premise Active directory to provide single sign on between Cloud and On-Premise applications. Through its Identity Bridge component IDCS can synchronize all the identities and groups from Active Directory into its own ID Store. Through ID Bridge it can also delegate the Authentication service to on-premise AD without the need of having a federation infrastructure in place. This will allow Organizations to leverage their existing investment in Active Directory and they can extend their services to Oracle Public Cloud and external SaaS applications.



List of some of the core capabilities are as follows:

- **User and Group Lifecycle Management –** One click management for your users through an easy to use self service interface across all your on-premise and Cloud applications.
- **Self Service Profile Management** – Manage profile, Set recovery address
- **Password Management** – Change password, reset password, Account unlock
- **Integration with On-Prem AD** – Sync users and Groups from On-premise AD

Identity Federation

Oracle Identity Cloud Service acts as a Federation hub that can be used to allow secure access to corporate resources by partners by exchanging identity information securely. It significantly reduces the need to manage unnecessary or additional accounts in the enterprise directory and lowers the cost of integrations through support of industry federation standards. With federation organizations can do more business online by allowing their business partners secure access to protected applications. Advantages of the federation service are as follows:

- Integration with On-Prem AD and OAM/OIF as IDP
- Supports Transient Federation, Account Mapping, Account Linking and Attribute Sharing.
- Accelerated SaaS adoption and faster service by providing a complete, end-to-end federation solution
- Reduced cost of integration projects through support of industry federation standards
- Eliminated burden of identity ownership by reducing the number of unnecessary user accounts in the enterprise directory
- Quick and high return on investment through supporting a wide variety of authentication providers/ IDPs and applications/SPs

Single Sign On

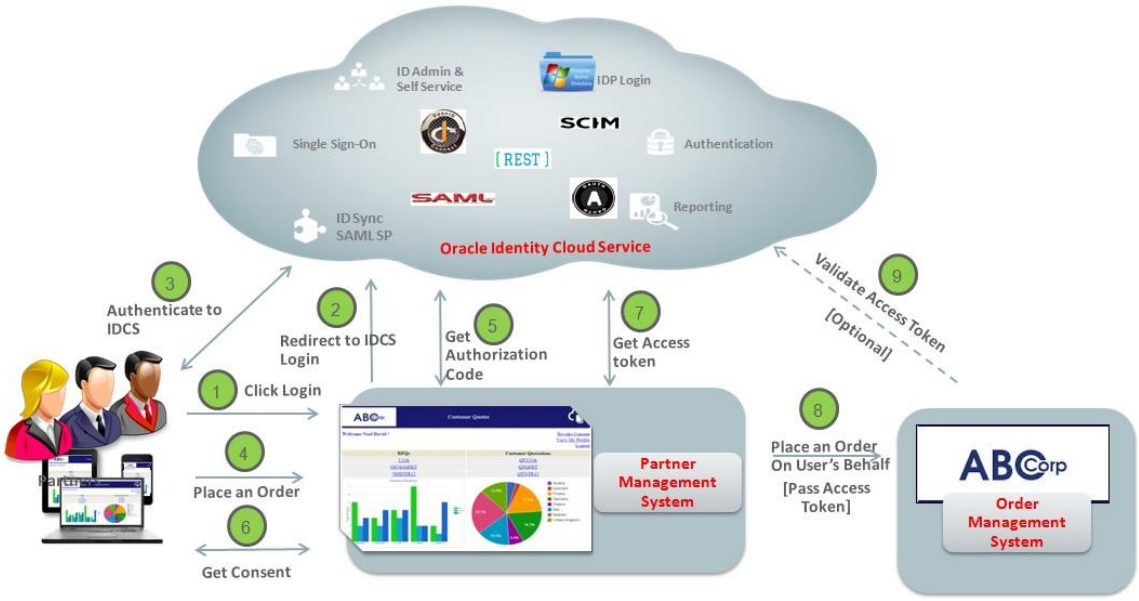
IDCS supports both SAML and OpenID Connect standards to provide SSO capabilities. It acts as a hub to provide SSO between cross platform applications that support SAML and OpenID Connect. Some of the core capabilities are listed below:

- Provide a cloud-based portal for employees to access SaaS applications
- IDBridge as an optional on-premises agent to use a corporate AD as user store.
- Support for Bi-directional SAML SSO (IDP Initiated & SP Initiated) and single logout
- Support for Bi-directional OpenID Connect SSO (IDP Initiated & RP Initiated) and single logout
- Support Cloud Gate to provide out of the box SSO support for OPC Applications

Security using OAuth2

A business has to provide access to its resource for its employees, partners and consumers for B2E, B2B and B2C scenarios. They want to ensure that these resources are accessed with maximum security but without having to manage all types of security infrastructure.

IDCS provides OAuth2 implementation to deliver a highly-scalable, multi-tenant OAuth2 compliant token service for securing programmatic (REST) access to applications (Resource Servers) by other apps (Clients). Customers can register their protected resources as an OAuth Resources in IDCS and register OAuth clients that are allowed to access those resources with proper scopes.



Some of the advantages of the OAuth service are as follows:

- Provides design time Admin interfaces to register OAuth Resources/Clients and Polices
- Provides run time life cycle management of OAuth Tokes and enforcement of security policies
- It provides a standards compliant token based service that can be leveraged by third-party services including Oracle Public Cloud hosted applications and services.

» It supports identity propagation use cases where application clients are required to impersonate end users and standards based tokens are the natural choice.

Seamless Access to Oracle Public Cloud Applications

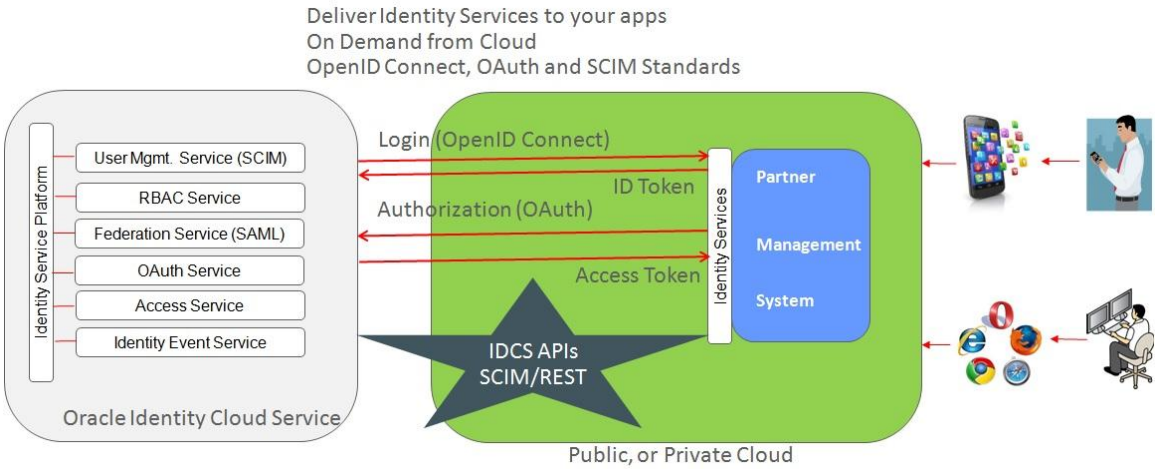
Identity Cloud Service provides native integration to all public Cloud applications. Customers who have bought any SaaS or PaaS application from Oracle public cloud will get basic IDCS services such as User Management, Self Profile Management, Password Management, Group Management, and Application Role management, Single Sign On, Application Registration and Reporting. Oracle public cloud applications will be auto configured in IDCS when a customer buys these services. No additional configuration is required by the administrators to configure these services for user management and single sign on.

Bring your own Apps – Build Applications using IDCS

Customers who want to build consumer facing applications and host external Identities in the cloud can leverage Identity Cloud Platform as their external IDP. These customers can build applications rapidly and secure it with cloud IDM in minutes, not months.

These applications can allow users to login through Self service registration or with a Social Identity such as FaceBook, Twitter and Google+. IDCS will pre-integrate these apps with popular providers. This will save integration time and effort in maintaining these applications.

With capabilities like self profile management and self password management, businesses can keep their helpdesk costs low while maintaining or improving the quality of their end user experience.



IDCS Advantages

- » Application Developers focus on core business logic and **delegate IAM responsibilities to IDCS**.
- » IDCS **Enables multi-channel access** by providing REST enabled APIs that can be consumed by any platform or language. It's fully context aware so that a policy decision can be made depending on where and when an application is being accessed.
- » Businesses can take advantage of **IDCS elasticity** during peak load. Capabilities like self registration and password reset can experience low and high volume activity because of promotions or during certain periods of the year depending on the type of service industry.

- Businesses can **reduce cost** by providing self service based profile and password management thus reducing help desk calls
- **Extend the capability** as an when needed rather than building it in the application

  Example – At some point the business feels that they need Multi Factor authentication for the application; it's simply a matter of switching a button "ON" in IDCS and configure the policy.

Conclusion – IDCS enables business for secure and faster adoption of services

Oracle identity Cloud Service provides a comprehensive IAM platform that is fully integrated with its own Oracle Public Cloud platform; built on modern cloud principles that can be used by organizations to simplify the interaction with business partners and customers. It allows running IAM services for the internal IT infrastructure on standardized cloud solutions, avoiding costly and complex implementation projects. IDCS enables businesses to roll out faster services with maximum security with low integration and maintenance cost.

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US


blogs.oracle.com/oracle


facebook.com/oracle


twitter.com/oracle


oracle.com

Hardware and Software, Engineered to Work Together

Identity Cloud Service -A Business White Paper
September 2016
Author: [Atul Goyal]
Contributing Authors: [OPTIONAL]


Oracle is committed to developing practices and products that help protect the environment