
ORACLE
IDENTITY CLOUD SERVICE
Secure Your Enterprise and Enable Your Users
ORACLE

Take on the challenges of an **extended enterprise.**

Cloud Adoption

IT organizations everywhere are using on-premises software together with cloud services. To access applications, users must keep track of multiple URLs, user names, and passwords.

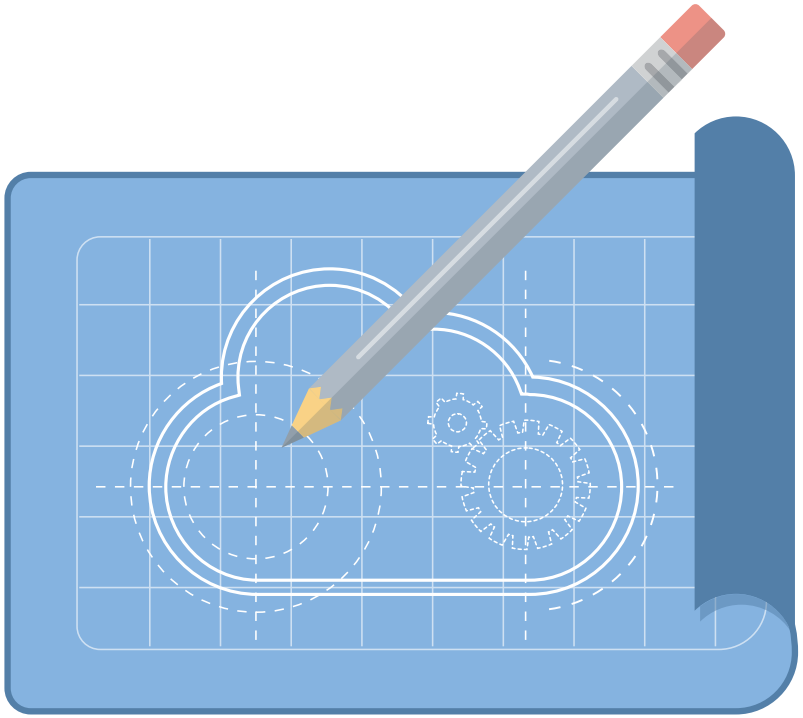
BYOD Policy Implementation

Because workers use their own devices to access enterprise resources, companies are scrambling to implement bring-your-own-device (BYOD) policies to maintain company security.

SSO for Application Access

Users access applications from everywhere, at any time. Using single sign-on (SSO) provides consistency across cloud, mobile, and enterprise applications, which improves usability while reducing implementation costs.

Benefit from Oracle's **next-generation IDaaS platform.**



Modern cloud applications require modern identity and access management (IAM) architectures. According to all major industry analysts, there is a huge need for IAM solutions offered as identity cloud services (IDaaS). As enterprises use more software applications as services (SaaS), they must provision users and oversee the rights that are assigned to them, quickly and easily.

Oracle Identity Cloud Service is Oracle's next-generation IDaaS platform built on modern cloud principles using open identity standards to address these challenges.

This platform delivers innovative and fully integrated IAM capabilities through a multitenant cloud that can be leveraged by other cloud-based services.

WATCH
Oracle Identity Cloud Service Product Tour

Take advantage of all of the capabilities of **Oracle Identity Cloud Service.**

Open Standards

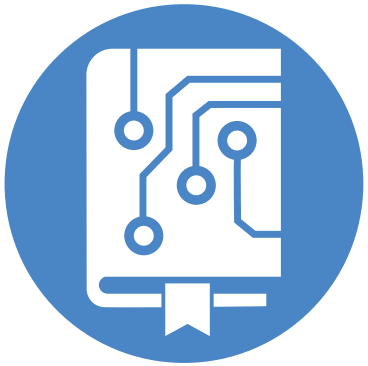
Leverage the power of open standards to deliver highly flexible integrations with other applications.

Identity Management

Manage user credentials across cloud, mobile, and on-premises applications—quickly, easily, and from only one place.

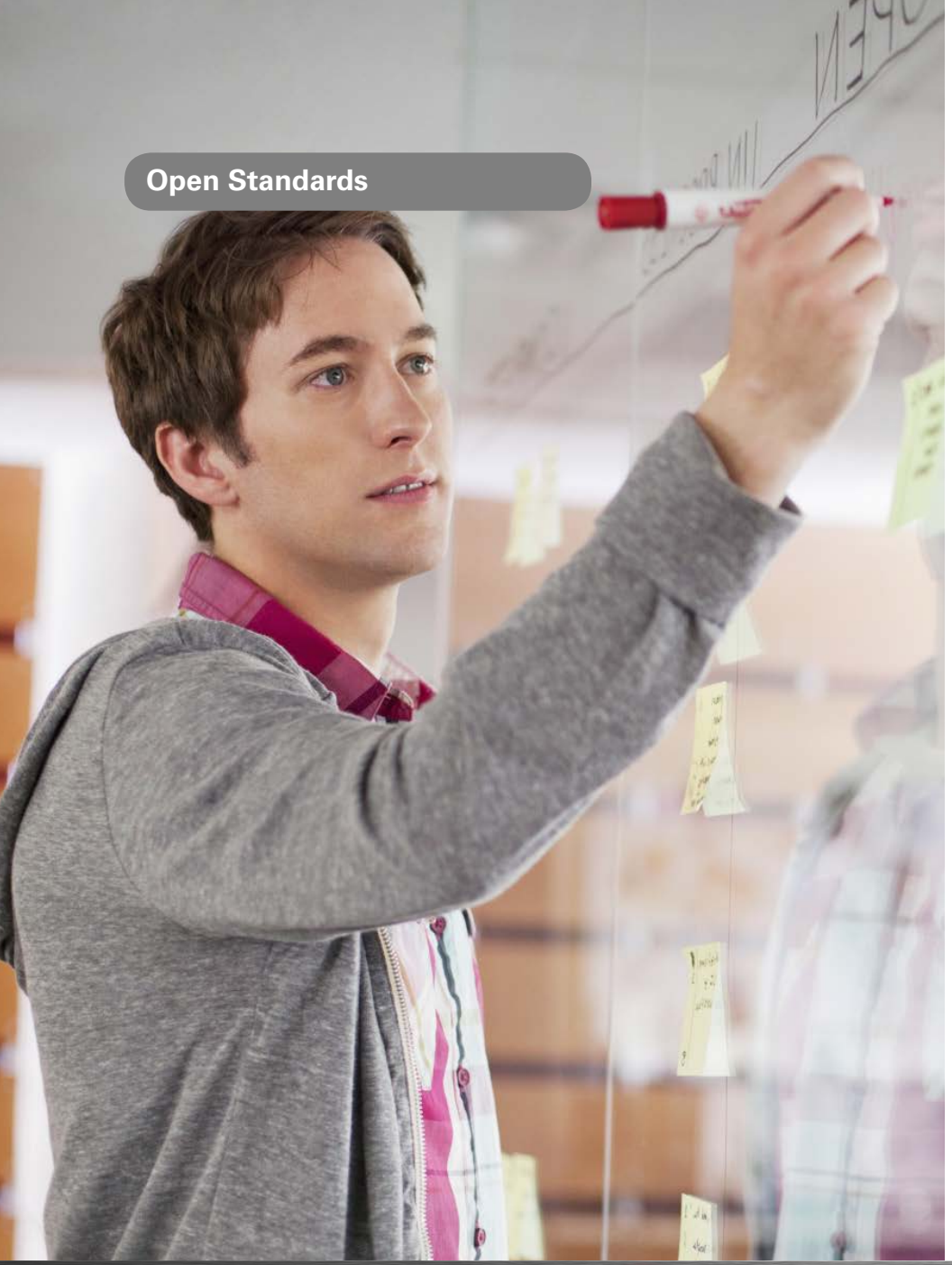
SSO and Authorization

Use SSO and authorization to access applications on-premises and in the cloud from any device, everywhere.



Hybrid Identity Management

Synchronize your users and SSO between Microsoft Active Directory or your Oracle Identity Management Suite and the cloud.



Leverage an **API-first and open-standards solution.**

Oracle Identity Cloud Service is built on an API-first architecture that leverages the power of open standards to deliver highly flexible and portable integrations:

- **SAML 2.0:** Security Assertion Markup Language (SAML) is an XML-based standard that provides federated SSO compatibility with most on-premises identity management applications.
- **OAuth 2.0:** A REST-based standard that provides authorization between cloud services. OAuth is implemented by most of the cloud services to securely delegate authorizations via tokens.
- **OpenID Connect:** An identity layer standard that sits on top of OAuth 2.0 to provide federated SSO. OpenID Connect is compatible with most of the social identity providers in the cloud.
- **SCIM:** System for Cross-domain Identity Management (SCIM) is a REST-based standard that defines schemas for managing identities across cloud services. With SCIM, you can synchronize identities between different IAM services without converting messages.

Identity Management

Manage your identities with **robust tools.**

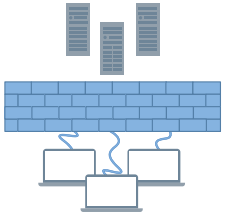
With Oracle Identity Cloud Service, you have a robust set of tools to manage your identities in the cloud:

- **REST APIs:** Use the SCIM-based REST APIs for managing identities and configurations from custom applications.
- **Administrative user interface:** Use this interface for user, group, application, and policy lifecycle management, to bulk load identities, and to download software development kits (SDKs).
- **Self-service user interface:** End users can leverage this interface to request access to groups and applications, manage their applications, profiles, and passwords, set their primary and recovery email addresses, activate and unlock their accounts, and link their social login accounts to their Oracle Identity Cloud Service user accounts through social identity providers, such as LinkedIn, Facebook, Twitter, Google, and Microsoft. This improves their efficiency and user experience while reducing help desk costs.

Use policy controls for **flexible and secure access to resources.**

Identity Provider Policies

Use these policies to specify which identity providers are available when someone is trying to sign into Oracle Identity Cloud Service, either when they're accessing a specific app or attempting to access resources that are protected by Oracle Identity Cloud Service. You can also use identity provider policies to determine whether users authenticate into Oracle Identity Cloud Service with their local credentials or by using credentials associated with SAML or social identity providers.



Network Perimeters

Define network perimeters and use them to prevent users from signing into Oracle Identity Cloud Service if they use one of the IP addresses in the network perimeter, or allow users to log in, using only IP addresses contained in the network perimeter.

Sign-on Policies

Use these policies to define criteria that Oracle Identity Cloud Service uses to determine whether to allow a user to sign into Oracle Identity Cloud Service or prevent a user from accessing Oracle Identity Cloud Service.

Secure your applications in the cloud **quickly.**

With SSO and authorization, you can secure applications in the cloud and integrate with other cloud services in minutes independent of the development platform or language.

This integration can consume identities, SSO, and authorization that is provided by Oracle Identity Cloud Service via open standards, like SAML, OAuth, OpenID Connect, and SCIM. The App Catalog contains pre-built integrations with major cloud services, making the integration with them simple and convenient. If you don't find the secure form fill application that you need in the App Catalog, or you simply want to create your own, you can do so with Oracle Identity Cloud Service.

If your applications are hosted at Oracle, then you can leverage native integrations with other Oracle Cloud Services.

By delegating these features to Oracle Identity Cloud Service, developers can focus on the core business logic, which saves you time and money.

WATCH
Integrate Applications with REST APIs

WATCH
Integrate Applications with OAuth

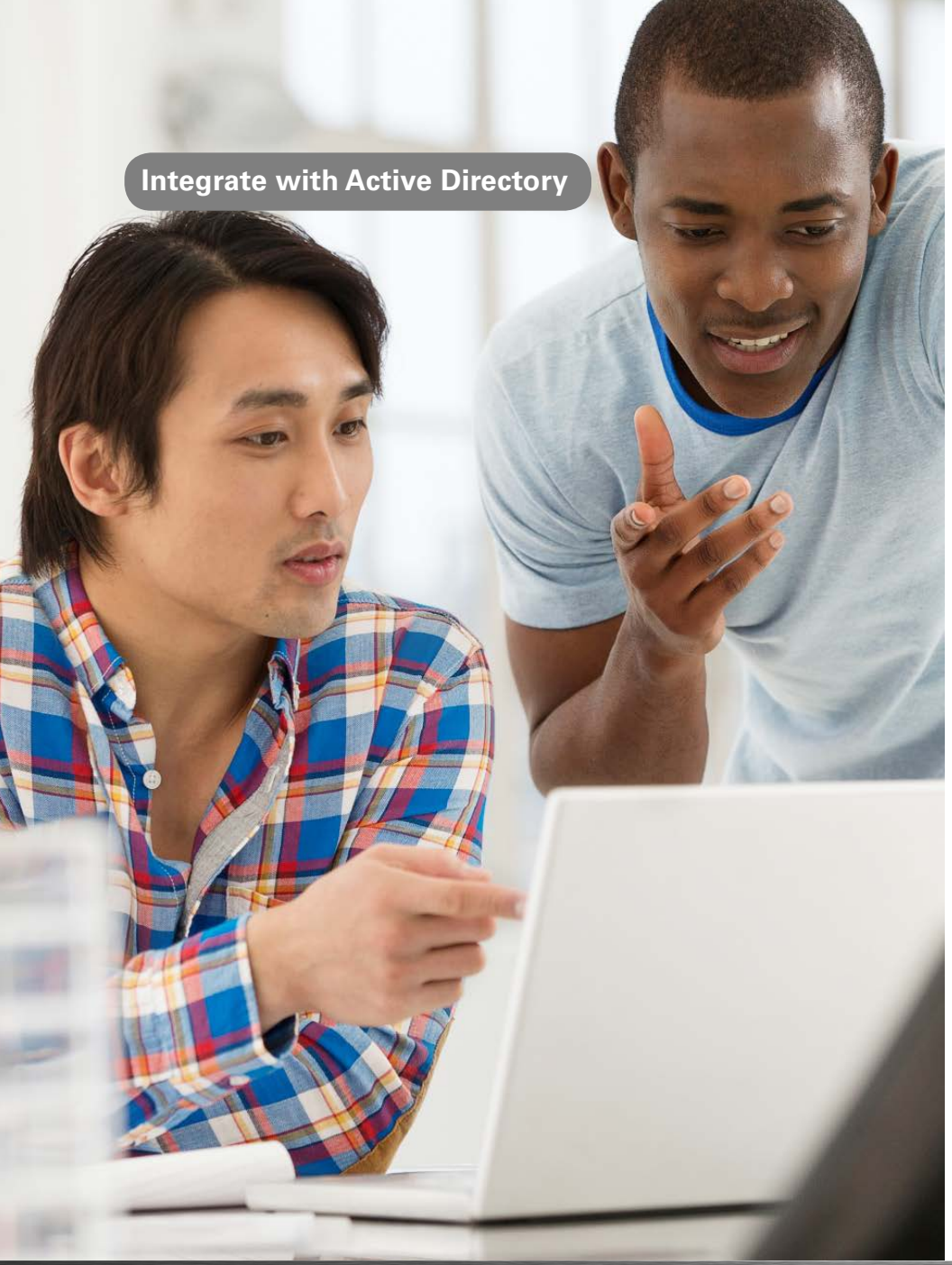
Access all applications with a single login.

With Oracle Identity Cloud Service, you can implement federated SSO with other solutions. With this integration, your on-premises users, partners, and cloud users can access on-premises and cloud applications with a single login from anywhere, at any time:

- **SAML SSO:** Implement federated SSO with SAML Identity Providers located on your premises or on your partners' premises.
- **OpenID Connect SSO:** Configure OpenID Connect and OAuth 2.0-based SSO with trusted cloud providers.
- **Social Account SSO:** Use federated SSO and social identity providers to link social accounts with user accounts in Oracle Identity Cloud Service.

Oracle Identity Cloud Service supports its native authentication in parallel with federated SSO. You can take advantage of this feature to implement heterogeneous authentication for each type of user.

WATCH
Integrate with Social Networks



ORACLE

Integrate with your **Microsoft Active Directory platform.**

Oracle Identity Cloud Service provides tools for a seamless integration with your Microsoft Active Directory (AD) platform:

- **Bridge:** The bridge continuously reconciles your AD users and groups to Oracle Identity Cloud Service, so you don't need to propagate entries manually.
- **Federated SSO with ADFS:** The SAML integration provides SSO between your Active Directory Federation Services (ADFS) users and Oracle Identity Cloud Service.

With your AD platform fully integrated to Oracle Identity Cloud Service, you can keep your AD users in the cloud without additional synchronization or management effort.

WATCH
Integrate with Active Directory

Control your **on-premises** assets.

If you're an on-premises customer, then you can keep your investment. You have full control of when and how you want to move your assets from the on-premises world to the cloud.

If you want to implement hybrid identity management between Oracle Identity Cloud Service and Oracle Identity Management Suite or Oracle E-Business Suite, then you can use:

- **Oracle Identity Manager (OIM) Connector:** This connector continuously reconciles OIM users and roles with Oracle Identity Cloud Service so you don't need to propagate entries manually. You can also apply the OIM certifications and segregation of duties to the Oracle Identity Cloud Service user accounts.
- **Federated SSO with Oracle Access Manager:** This SAML integration provides SSO between your Oracle Access Manager users and Oracle Identity Cloud Service.
- **Oracle E-Business Suite (EBS) Asserter:** Use this lightweight Java application to integrate your EBS environment with Oracle Identity Cloud Service for authentication and password management purposes.

With the hybrid integration between Oracle Identity Cloud Service and Oracle Identity Management Suite or Oracle E-Business Suite, you enforce identity governance in the cloud from a single cloud service.

WATCH
Integrate with
Oracle Identity Manager

WATCH
Integrate with
Oracle Access Manager

Get Started

Learn More

- View data sheets, FAQs, pricing, and additional resources on the **Identity Cloud Service** product page.
- Purchase a subscription and get started with using Oracle Identity Cloud Service by visiting the **Oracle Help Center.**

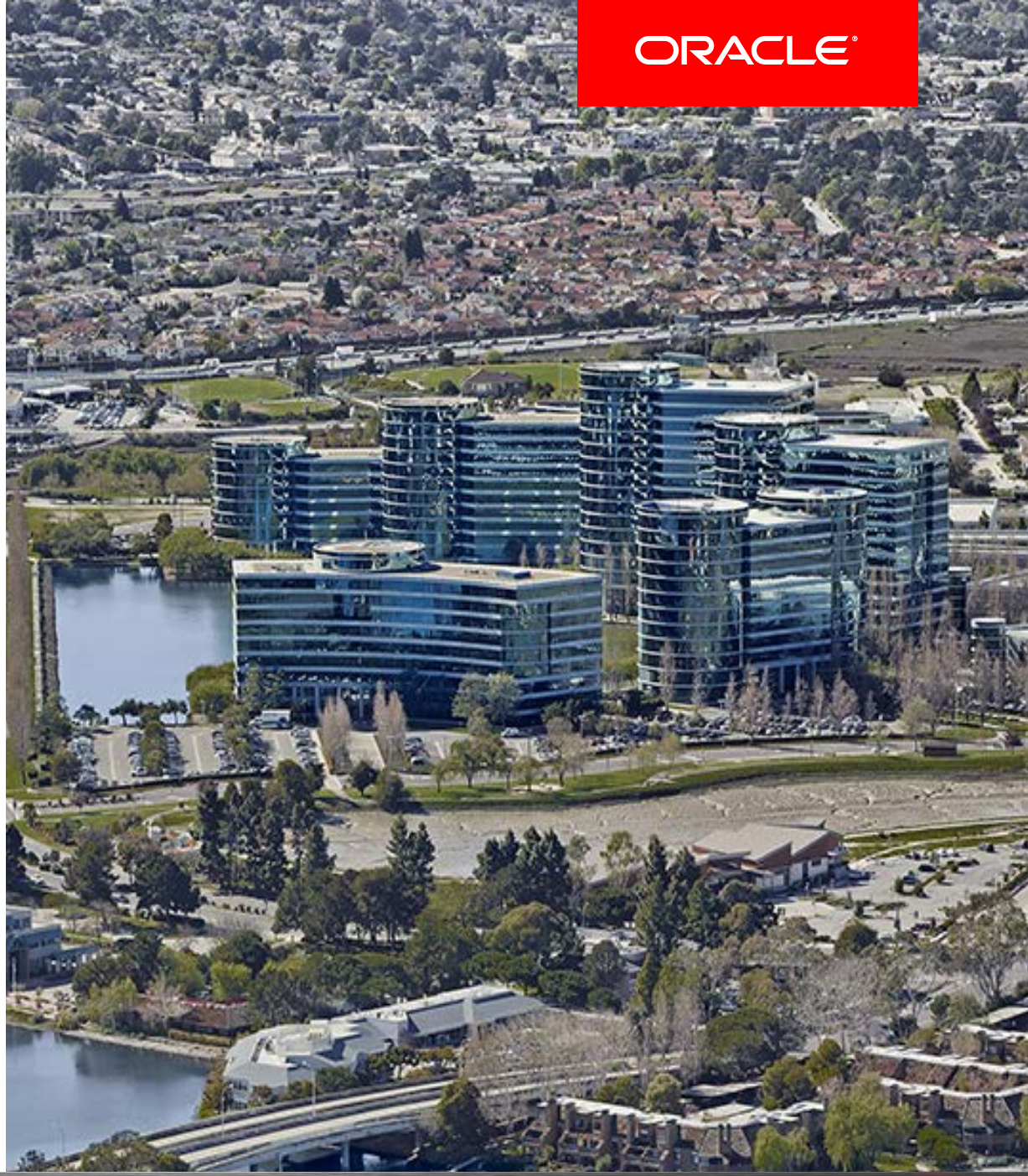
Connect

Twitter: **@OracleCloud**
Facebook: **Oracle Cloud**
LinkedIn: **Official Oracle Cloud Group**
YouTube: **Oracle Cloud Channel**

Visit

Visit our Oracle Cloud community.

Oracle Events
Oracle Cloud Solutions Blog



Safe Harbor

The preceding 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.

v. Jan 29, 2018