ORACLE

OCI IAM Identity Domains: What Oracle IDCS customers need to know

Oracle recently merged the capabilities of Oracle Identity Cloud Service (IDCS) into the native Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) service. IDCS is no longer offered as a separate service, but all features and functionality continue to exist as part of OCI IAM. As a native OCI service, customers will see improved performance and scale, immediate availability in more global regions, and a new cross-region disaster recovery feature.

What is OCI IAM?

OCI IAM is the access control plane for Oracle Cloud. It's the OCI-native authentication service and policy engine for OCI and Oracle Cloud Applications that has been used to manage access to OCI resources such as networking, compute, storage, and analytics.

What changed for IDCS and OCI IAM?

Oracle recently made available new capabilities for the OCI IAM service offering broader IAM features and capabilities. As part of this upgraded service release, all features and functionality of the existing Oracle Identity Cloud Service (IDCS) have been merged into OCI IAM. IDCS is no longer offered as a separate service, but all its features and capabilities will continue to function as part of the updated OCI IAM service.

OCI IAM will support the following core functions:

- OCI IAM will continue to serve as the critical access control plane for Oracle Cloud.
- Oracle Cloud applications are expected to standardize over time on OCI IAM as the native IAM service for the application.
- OCI IAM will support a wide range of enterprise Identity and Access Management (IAM) use cases for complex, hybrid IT environments.
- OCI IAM will provide a developer friendly IAM engine for custom and consumer applications.

By unifying administration and user experiences across these key IAM functions, the new service helps simplify administration, reduce cost of ownership, and improve time to value. The service spans cloud and on-premises, providing the flexibility to handle a wide variety of IAM use cases across employee, partner,
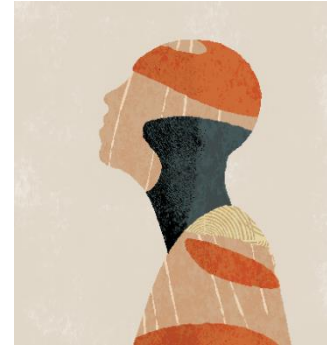
Additional Resources
To learn more about OCI IAM, please visit:

- Oracle Cloud Infrastructure Identity and Access Management documentation
- OCI Identity and Access Management Solution Page
- Identity Cloud Service Documentation
- Oracle Cloud Security Blog

ORACLE

and consumer scenarios. As a native service of OCI, customers can use the diverse feature set of OCI IAM across use cases in any geography. The new service will be delivered on OCI infrastructure for trusted performance and stability.

All OCI tenancies have been migrated to the upgraded OCI IAM service with identity domains. Previously existing IDCS instances (stripes) are now available in the OCI Console as identity domains. Because IDCS instances were migrated into OCI tenancies, most OCI customers will see the auto-federated IDCS instance is now an identity domain in the root compartment named IdentityCloudService. There are no required changes to applications, users, or groups in domains that formerly existed as IDCS instances or to local users in OCI tenancies.

The updated OCI IAM service introduces i*dentity domains*.

- Identity domains are the next generation of IDCS instances (stripes). Each existing IDCS instance is now an identity domain.
- Each OCI IAM identity domain represents a stand-alone identity and access management solution.
- Each identity domain represents a different user population, but certain use cases may require users to exist in multiple domains.
- Identity domains each have their own settings, configurations, and security policies to ensure optimal security.
- OCI IAM is an Identity-as-a-Service (IDaaS) solution with the flexibility to cover virtually any IAM use cases across employees, partners, and consumers.

How does this impact existing Identity Cloud Service (IDCS) instances?

Oracle Identity Cloud Service (IDCS) customers should be familiar with the level of enterprise IAM functionality IDCS provides. None of the existing IDCS features or functionality will change as part of this migration. IDCS will become an integral component of Oracle Cloud Infrastructure Identity and Access Management (OCI IAM).

As a native service of OCI, OCI IAM will take advantage of infrastructure that offers consistently high performance, enterprise scalability, availability in all the Oracle global cloud regions, and an extensive set of regulatory compliance and security certifications.

The OCI IAM service will continue to serve all current IDCS use cases including providing a stand-alone Identity-as-a-Service (IDaaS) solution for managing access across numerous third-party applications. IDCS customers migrating to OCI IAM do not need to consume any other OCI services to continue using the services previously provided by IDCS.

As noted above, previously existing IDCS instances are now available in the OCI Console as identity domains.

ORACLE

What's new in OCI IAM for IDCS customers?

The migration to OCI IAM and the introduction of identity domains adds IDCS features natively to the OCI IAM service. Here's what you need to know:

- **Improved Administration Experience:** Identity administration is now available through the OCI admin console under a navigation menu item called Identity & Security > Domains. Administrators will see the same set of features and functionality that they're used to in IDCS for managing users, groups, applications, security settings, and other configurations.

- **No Impact for Existing Users, Policies, Configuration, or Access:** Existing security controls and policies will continue to function as expected. Functionality is not being removed nor any policy configurations changing. There should be no impact to security settings or to the user experience.

- **Disaster Recovery:** In most regions, OCI IAM now has a cross-region disaster recovery feature that will recover identity domain data in the unlikely event that an entire OCI region becomes unavailable. This is included and does not require any changes or updates to existing applications.

Post-Upgrade Guidance

- **Administrative Access:** As IDCS instances have become part of OCI via identity domains, members of the OCI *Administrators* group will have full access to manage OCI IAM identity domains. Customers should confirm that use of this group is consistent with their security policies.

  Each OCI tenancy includes an *Administrator* account that is, by default, a member of the tenancy *Administrators* group. The *Administrators* group grants full access to the entire tenancy. It is therefore best practice not to use the *Administrator* account for day-to-day administration and the tenancy *Administrators* group should be reserved for emergency scenarios.

  It's good practice to discontinue use of the account after initial setup and instead set a complex password on the account and then store the credentials safely in a secure location such as a physical safe.

- **Firewall Configuration:** To take advantage of the new Disaster Recovery (DR) feature which establishes a DR region outside of the primary region, customers may need to update their firewall policies to enable communication with the additional (DR) regions. Refer to OCI documentation for details.

Where can I get more information?

For more information, please review the OCI IAM product documentation or visit the Oracle Identity and Access Management Webpage.

ORACLE

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

📝 blogs.oracle.com   f facebook.com/oracle   🐦 twitter.com/oracle

ORACLE