ORACLE

OCI IAM Identity Domains: What OCI IAM 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. This enables OCI customers with a rich, enterprise-class set of identity and access management (IAM) features for use with OCI and Oracle Cloud applications.

What is OCI IAM?

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

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

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

IAM is also flexible enough to handle a wide variety of IAM use cases across employee, partner, and consumer scenarios.

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*.

- 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 OCI tenancies?

OCI administrators should already be familiar with the OCI IAM service which enables authentication into OCI and management of access entitlements for OCI resources via OCI IAM policies. Today, many customers choose to additionally use IDCS to enable more advanced IAM deployments. This creates an additional layer of IAM to manage and sometimes incurs additional cost.

The introduction of identity domains adds these features natively to the OCI IAM service simplifying administration and operational management. Here's what you need to know:

- **Powerful IAM functionality at no additional cost:** Oracle brought all the enterprise IAM capabilities of IDCS into OCI IAM natively. IAM functionality such as advanced authentication techniques and user lifecycle management is now natively available and included in your existing OCI tenancies for use with your subscribed* Oracle services.
  ** Upgrades are available to provide IAM support beyond subscribed Oracle services.*
- **Single Point of Authentication:** The OCI sign-on screen is simplified with fewer options to reduce confusion for users.
- **Single Point of IAM Management:** Customers who previously used IDCS with OCI tenancies will now enjoy simplified administration via a single pane of glass for all users. Identity domains are accessible in the OCI Console navigation menu under Identity & Security.
- **No Impact for Existing Users, Policies, Configuration, or Access:** This upgrade will maintain all existing security policies, configurations, and user populations. There should be no impact to security settings or to

the user experience. We're did not remove functionality or change any policy configurations.

- **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.