

Migrating to OCI IAM: What Oracle IDCS customers need to know

Oracle is merging the capabilities of Oracle Identity Cloud Service (IDCS) into the native Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) service. All IDCS features and functionality will 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. Best of all, the migration to OCI IAM will be seamless and automatic without any loss of existing capabilities or features, including managing access across numerous third-party applications.

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 is changing for IDCS and OCI IAM?

Oracle will soon be announcing new service capabilities for the OCI IAM service offering broader IAM features and capabilities. As part of this new service release, all features and functionality of the existing Oracle Identity Cloud Service (IDCS) will be merged into OCI IAM as *identity domains*. IDCS will no longer exist as a separate service, but all its features and capabilities will continue to function as part of the new 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 supports a wide range of enterprise Identity and Access Management (IAM) use cases for complex, hybrid IT environments.
- OCI IAM provides a developer friendly IAM engine for custom and consumer applications.



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](#)

By unifying administration and user experiences across these key IAM functions, the new service will help simplify administration, reduce cost of ownership, and improve time to value. The service will span cloud and on-premises, providing the flexibility to handle a wide variety of IAM use cases across employee, partner, 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.

The conversion from IDCS to OCI IAM identity domains is expected to be largely transparent with no anticipated down time or service interruption. There are no required changes to applications, users, or groups in existing IDCS stripes or to local users in OCI tenancies.

When this process completes, existing IDCS stripes will be available in the OCI Console as identity domains. Because IDCS stripes will be 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.

- Identity domains are the next generation of IDCS instances (stripes). Each existing IDCS instance will become 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 identity 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.

What changes with an existing Identity Cloud Service (IDCS) deployment?

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. As part of this change, the backend IDCS service becomes 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.

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:** The migration will apply changes to the administrative console. Identity administration will be available through the OCI admin console under a navigation menu item called Identity & Security > Identity 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.

When will this happen?

The updated OCI IAM service, with *identity domains*, was made generally available (GA) for new customers across all global regions in late 2021. This did not impact existing tenancies. We expect to begin introducing identity domains into existing tenancies in the coming months. Once all tenancies have been migrated, identity domains will be enabled for all customers.

Post-Upgrade Guidance

- **Administrative Access:** As IDCS instances migrate to become part of OCI via identity domains, members of the OCI tenancy *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.

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](#).

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

 facebook.com/oracle

 twitter.com/oracle

Copyright © 2022, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0120

Disclaimer: If you are unsure whether your data sheet needs a disclaimer, read the revenue recognition policy. If you have further questions about your content and the disclaimer requirements, e-mail REVREC_US@oracle.com.