

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

What do I need to know?

- In the coming months, Oracle Identity Cloud Service (IDCS) instances will become [OCI IAM identity domains](#).
- You will receive a notification approximately two weeks before the process begins for your tenancy.
- This process will not introduce any service downtime.
- No changes are required for applications, users, groups, or IDCS configurations.
- All existing IDCS administration and My Profile functionality remains the same but will be moved to the [Oracle Cloud Console](#).
- The Oracle Cloud sign-in page will have an updated design to match the latest Oracle Cloud design guidelines.

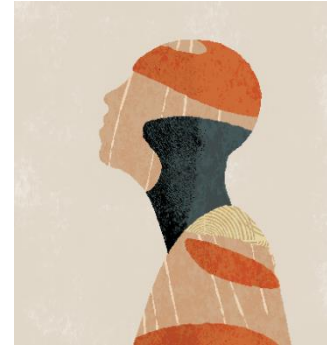
What happens when identity domains are introduced into my Oracle Cloud tenancy?

When this process completes, all existing IDCS instances will be available in the Oracle Cloud Console as identity domains. For OCI tenancies with an auto-federated IDCS instance, that instance will become an identity domain in the OCI tenancy root compartment named `OracleIdentityCloudService`.

Three more important changes will occur:

1. **Oracle Cloud sign-in page:** will be updated with a new design.
2. **Identity Cloud Service administration** functionality will be moved to the Oracle Cloud Console.
3. **My Profile** functionality will be merged with Oracle Cloud Console user profile.

See below for more information and Frequently Asked Questions related to these changes.



What is OCI IAM?

[OCI IAM](#) is the access control plane for Oracle Cloud. It's the authentication service and policy engine used to manage access to Oracle Cloud resources such as networking, compute, storage, and analytics.

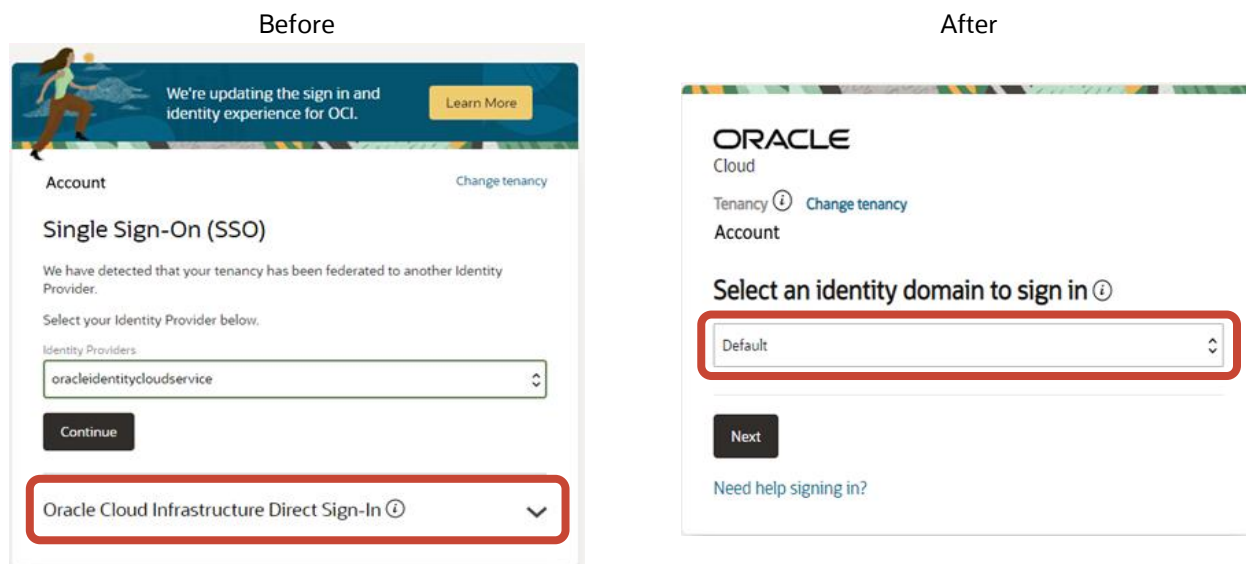
Additional Resources

- [Oracle Cloud Infrastructure Identity and Access Management documentation](#)
- [What is the Oracle Cloud Console?](#)
- [OCI Identity and Access Management Solution Page](#)
- [Oracle Cloud Security Blog](#)

1. Oracle Cloud sign-in page will be updated with a new design

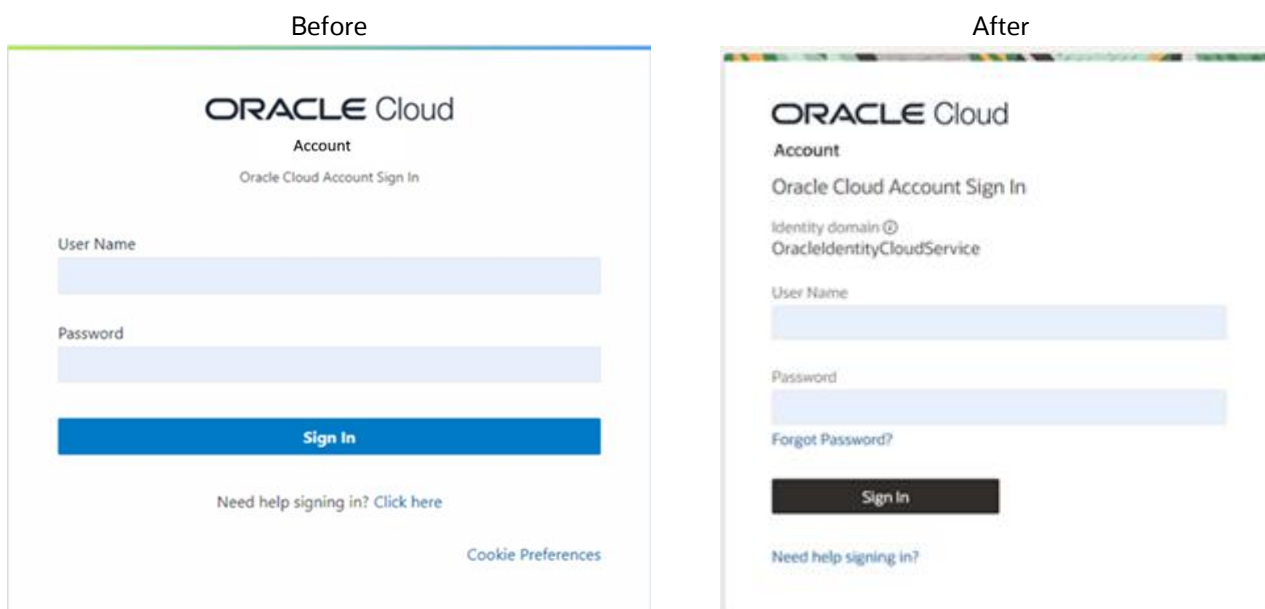
The Oracle Cloud sign-in page will be refreshed to match the latest Oracle Cloud design guidelines. Instead of two sign in options (identity providers and OCI direct sign-in), all users will select an identity domain to sign in.

Users who currently select the **Direct Sign-In** option, should select the **Default** identity domain from the updated sign-in page.

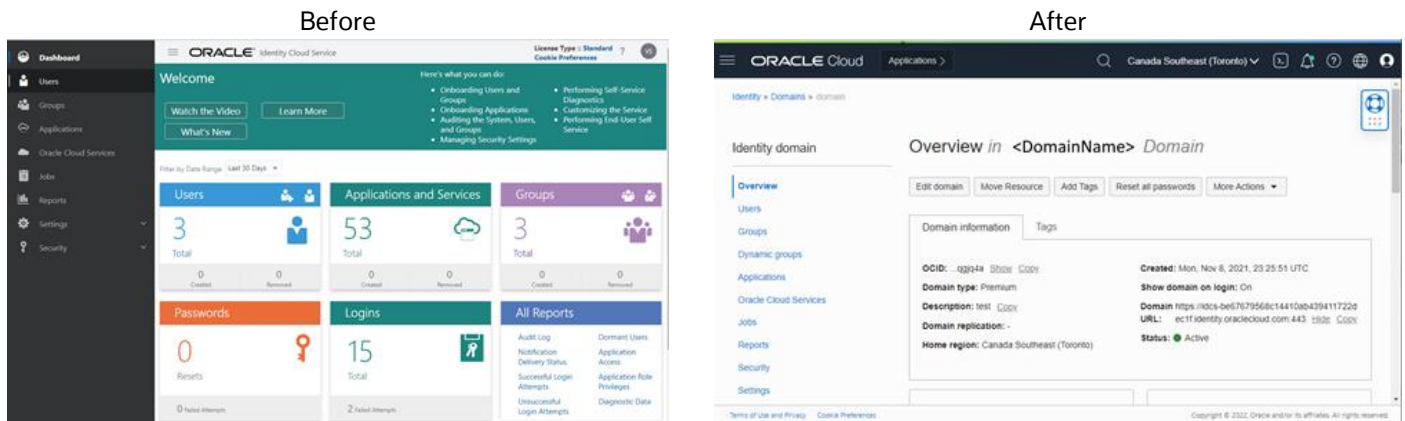


2. Identity Cloud Service administration functionality will be moved to the Oracle Cloud Console

Customers who use IDCS to authenticate users for applications will notice minor style changes to the IDCS sign-in page. The added "identity domain" attribute is the name of the identity domain that matches the IDCS instance name



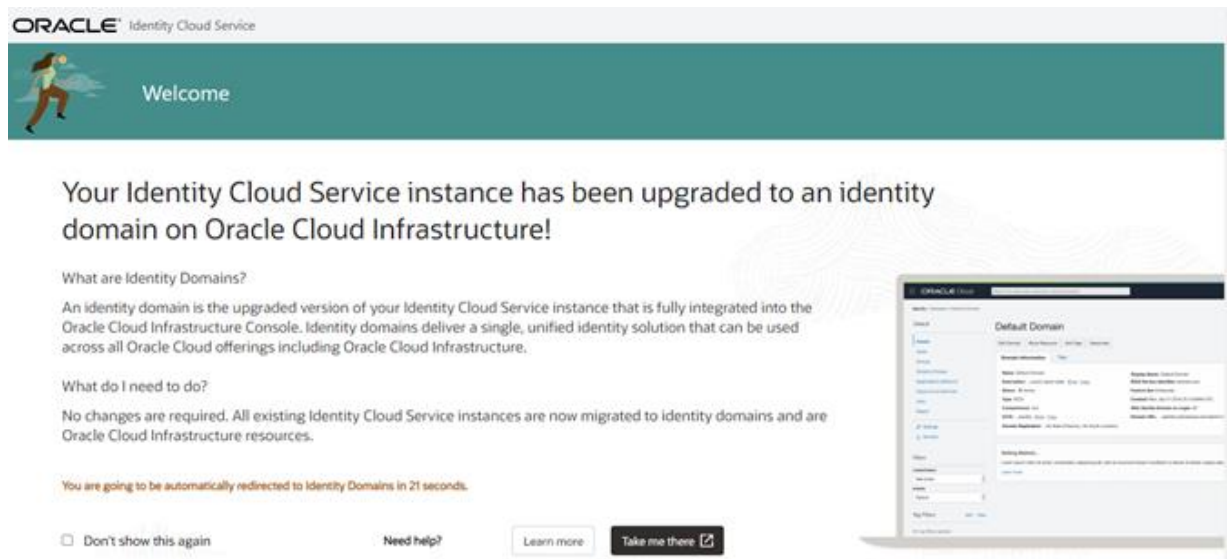
The Identity Cloud Service administration console now redirects to the Oracle Cloud Console. The same set of administrative functions is available in the new console.



To navigate to Identity domains in the Oracle Cloud Console, Select **Identity & Security** in the navigation menu, then select **Domains** under the **Identity** heading.

Will my existing bookmarks work?

Yes, they will work, and a redirection page will welcome you to the new experience.



For example:

<https://idcs-<instanceid>.identity.oraclecloud.com/ui/v1/adminconsole>

will be redirected to:

<https://console.<region>.oraclecloud.com/identity/domains/<DomainOCID>>

3. My Profile functionality will be merged with Oracle Cloud Console user profile

Customers who use the IDCS My Profile pages will notice style changes to the My Profile pages, which will now be delivered via the Oracle Cloud Console.

Before

The screenshot shows the Oracle My Profile page for user Brian Rogers. The page is divided into three main sections: Account Information, Work Information, and Other Information. The Account Information section includes fields for User Name, Email, Prefix, Instant Messaging Address, First Name, Home Phone Number, Middle Name, Mobile Phone Number, Last Name, and Suffix. The Work Information section includes fields for Title, Country, Street Address, Time Zone, City, Locale, Postal Code, and Work Phone Number. The Other Information section includes fields for User Type, Division, Employee Number, Department, Organization Name, Cost Center, Set Once, testName, test, and Read Only. A Save button is located in the top right corner of the Account Information section.

Section	Field Name	Value / Type
Account Information	User Name	brian.rogers@mycompany.com
	Email	brian.rogers@mycompany.com
	Prefix	<input type="text"/>
	Instant Messaging Address	<input type="text"/>
	First Name	Brian
	Home Phone Number	<input type="text"/>
	Middle Name	<input type="text"/>
	Mobile Phone Number	<input type="text"/>
	* Last Name	Rogers
	Suffix	<input type="text"/>
Work Information	Title	<input type="text"/>
	Country	<input type="text"/>
	Street Address	<input type="text"/>
	Time Zone	<input type="text"/>
	City	<input type="text"/>
	Locale	<input type="text"/>
	Postal Code	<input type="text"/>
	Work Phone Number	<input type="text"/>
Other Information	User Type	<input type="text"/>
	Division	<input type="text"/>
	Employee Number	<input type="text"/>
	Department	<input type="text"/>
	Organization Name	<input type="text"/>
	Cost Center	<input type="text"/>
	Set Once	<input type="text"/>
	testName	<input type="text"/>
	test	<input type="text"/>
	Read Only	<input type="text"/>

After

ORACLE Cloud Search for resources, services, and documents

Identity - My profile

Brian Rogers
This is a sample description field

Email: brian.rogers@mycompany.com | Organization name: My Company | Department: Sales | Last updated: Tues, Sep 1, 2023 00:00 UTC

My profile

- Access my catalog
- Change my password
- Security preferences
- Edit my profile

My requests

My groups

My applications

My consents

My approvals

My social accounts

Auth. tokens and keys

- API keys
- Customer secret keys
- OAuth 2.0 client credentials
- My access tokens

Saved passwords

- SMTP credentials
- MyAuth2.0 credentials
- Database passwords

Profile details [Edit profile](#) [Change password](#)

OCID: ..254ny54

User name: brian.rogers@mycompany.com | Email: brian.rogers@mycompany.com [Edit](#)

Created: Tue, Sep 1, 2020, 16:36:14 UTC | Instant messaging address: None

Prefix: | Home Phone number: -

First name: Brian | My Oracle support account: -

Middle name: | Multi-factor authentication: Disabled [Link account](#)

Last name: Rogers:

Work information

Title: Product Manager | User type: None

Street address: - | Employee number: -

City: Seattle | Organization name: -

Postal code: 98101 | Division: -

State: Washington | Department: -

Country: USA | Cost center: -

Time zone: brian.rogers@mycompany.com

Preferred language: None

Other information

Title: Product Manager

Street address: -

City: Seattle

Capabilities

Local password: Yes | SMTP credentials: Yes

API keys: Yes | Customer secret keys: Yes

Auth tokens: Yes | OAuth 2.0 client credentials: Yes

Database passwords: Yes

Tags [Add tags](#)

Defined tags (1)

Oracle-Tags CreatedBy: This_user

[Terms of User and Privacy](#) [Cookie Preferences](#) Copyright © 2023, Oracle and/or its affiliates. All rights reserved.

Frequently Asked Questions about OCI IAM identity domains

- General FAQs
- FAQs for existing OCI administrators
- FAQs for existing IDCS administrators
- FAQs for Oracle SaaS and Application administrators

General FAQs

What are the benefits of introducing OCI IAM identity domains?

Identity domains add several IAM features natively to the OCI IAM service which simplifies administration and operational management:

- Oracle is bringing all the enterprise IAM capabilities of IDCS into OCI IAM natively. IAM functionality such as advanced authentication techniques and user lifecycle management will be natively available in your existing OCI tenancies.
- The Oracle Cloud sign-in page will be simplified with fewer options to reduce confusion for users.
- Customers who currently use IDCS with their OCI tenancies will now enjoy simplified administration via a single pane of glass for all user management. Identity domains are accessible in the Oracle Cloud Console navigation menu under Identity & Security.
- OCI IAM is an Identity-as-a-Service (IDaaS) solution with the flexibility to cover virtually any IAM use cases across employee, partner, consumer, and developer scenarios.
- By unifying administration and user experiences across key IAM functions, identity domains will 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 optimized performance and stability. OCI IAM is also flexible enough to handle a wide variety of IAM use cases across employee, partner, and consumer scenarios.

When will this happen?

We expect to introduce identity domains into all remaining OCI tenancies in 2023. You will receive a notification approximately two weeks before the process begins for your tenancy. In all Oracle Cloud commercial regions, new tenancies and child tenancies are already being provisioned with OCI IAM identity domains.

How does this impact my end-users who aren't technically savvy?

General system users will notice an upgrade to the design of the sign-in page. If you are using a custom sign-in page, the design will not be impacted. They will continue to use the My Profile and Catalog pages from their IDCS instance. They can continue to reset their own passwords. In general, most users will see this update as a design update.

FAQs for existing OCI administrators

How will this impact existing OCI tenancies?

- Local OCI users and groups will become part of the *Default* identity domain. Users that sign in using "Direct Sign-In" should use the Default domain on their next sign in.
- Existing external federations will continue to operate. However, new federation relationships will need to be configured in an identity domain.
- There is no impact for existing users, policies, configuration, or access. This update will maintain all existing security policies, configurations, and user populations. We're not removing functionality or changing any policy configurations.
- All IDCS instances associated with your cloud account are now administered via the Oracle Cloud Console as identity domains.

Will this update maintain provisioning to OCI IAM security groups for use in OCI policies?

- To preserve existing OCI policies and security configurations, this update will maintain group mapping from the federated IDCS instance to the Default identity domain.

How is administrative access impacted for existing OCI tenancies?

- Granting a user or a group the Identity Domain Administrator role in the Default domain is equivalent to granting them full administrator permissions for the tenancy. This behavior applies to the Default domain only. Granting users or groups the Identity Domain Administrator role for domains other than the Default domain, grants them full administrator permissions only for that domain. You should confirm that the membership of the Identity Domain Administrator role in the Default identity domain is consistent with your security policies.
- An OCI_Admistrators group has also been added to the IDCS instance that was provided during tenancy creation (usually called the IdentityCloudService). This group is mapped to the *Default* identity domain's Administrators group, which does not have any users assigned at creation time. If you want users to have full access to the entire tenancy, you can add them to the OCI_Admistrators group in the IdentityCloudService domain.
- Each OCI tenancy includes an Administrator account that is created as a member of the tenancy Administrators group. The tenancy Administrators group grants full access to all resources in the tenancy. This now includes the ability to manage identity domains. Any member of this group should be carefully examined.

What is changing in the existing OCI IAM service?

- OCI IAM is being updated with additional IAM features and capabilities. 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 serve additional and expanded use cases:
 - OCI IAM continues to serve as the critical access control plane for Oracle Cloud.
 - Over time, Oracle Cloud applications will standardize on OCI IAM as the native IAM service.
 - OCI IAM supports a wide range of enterprise IAM use cases for complex, hybrid environments.
 - OCI IAM provides a developer friendly IAM engine for custom and consumer applications.

FAQs for existing IDCS administrators

How does this impact my existing IDCS instances?

- All existing configurations, security settings, user and group populations, and access assignments will continue to exist with no interruption.
- Custom sign-in pages will not be modified. Users who authenticate via a custom sign-in page will not experience any changes.
- IDCS administrators will be redirected from the existing IDCS administrative console to the Oracle Cloud Console where updated IDCS instances will be listed as OCI IAM identity domains.
- There are no changes to pricing, metering, or included features for existing IDCS instances. Customers will continue to use their existing IDCS service SKUs.

Will this update allow my organization to leverage the new Identity Domain license types?

- Yes. After IDCS instances become identity domains, administrators will have the ability to change the domain type from the current IDCS license to any of the available identity domain types. This will require that the domain resources do not exceed the limits of the target domain type.

How is administrative access impacted for existing IDCS instances?

For all existing IDCS instances, ensure that you validate the group membership of the **OCI Administrators** group(s). This group will have full access to your OCI tenancy and all your identity domains. To do this:

- Go to the MyServices console or the Identity Cloud Service console.
- Locate the **OCI Administrators** group.
- Add and/or remove users to that group to be consistent with your security policies.
- [Learn more](#) about IAM administrator roles.

FAQs for Oracle SaaS and Application administrators

How does this impact the My Services console?

My Services will still be available. However, the identity and access functionality will be found under identity domains in the Oracle Cloud Console. There are no changes to the provisioning mechanisms for SaaS services. These will continue to work the same way. All existing IDCS instances will appear in the Oracle Cloud Console instead of MyServices and all identity domain management will occur in the Oracle Cloud Console. Customers may still use the MyServices console and links for users, groups, and My Profile but these links will redirect to the Oracle Cloud Console along with the *Identity Application* tile, overview, and status links. Billing metric information will also be in the Oracle Cloud Console.

Connect with us

Call +1.800.ORACLE1 or visit [oracle.com](https://www.oracle.com). Outside North America, find your local office at: [oracle.com/contact](https://www.oracle.com/contact).

 blogs.oracle.com

 facebook.com/oracle

 twitter.com/oracle

Copyright © 2023, 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.