ORACLE

Introducing OCI IAM Identity Domains: What customers need to know

Oracle merged the capabilities of Oracle Identity Cloud Service (IDCS) into the native Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) service. This enables 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?

- Oracle Identity Cloud Service (IDCS) instances are now OCI IAM identity domains.
- All existing IDCS administration and My Profile functionality remains the same but is now available in the Oracle Cloud Console.
- The Oracle Cloud sign-in page has an updated design to match the latest Oracle Cloud design guidelines.

What changes were introduced into my Oracle Cloud tenancy?

All existing IDCS instances are now available in the Oracle Cloud Console as identity domains. For OCI tenancies that previously had an auto-federated IDCS instance, that instance is now an identity domain in the OCI tenancy root compartment named `OracleIdentityCloudService`.

Three more important changes have occurred:

1. **Oracle Cloud sign-in page:** has been updated with a new design.

2. **Identity Cloud Service administration** functionality has been moved to the Oracle Cloud Console.

3. **My Profile** functionality has been merged with Oracle Cloud Console user profile.

See below for more information and Frequently Asked Questions related to these changes.
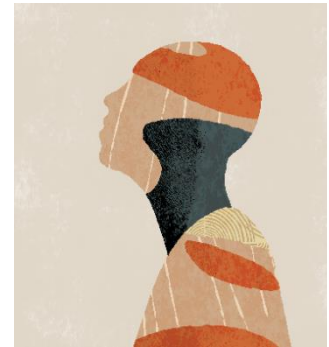
What is OCI IAM?

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

ORACLE

## 1. Oracle Cloud sign-in page has been updated with a new design

The Oracle Cloud sign-in page has been 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 now select an identity domain to sign in.

Users who previously selected the **Direct Sign-In** option, should now select the **Default** identity domain from the updated sign-in page.
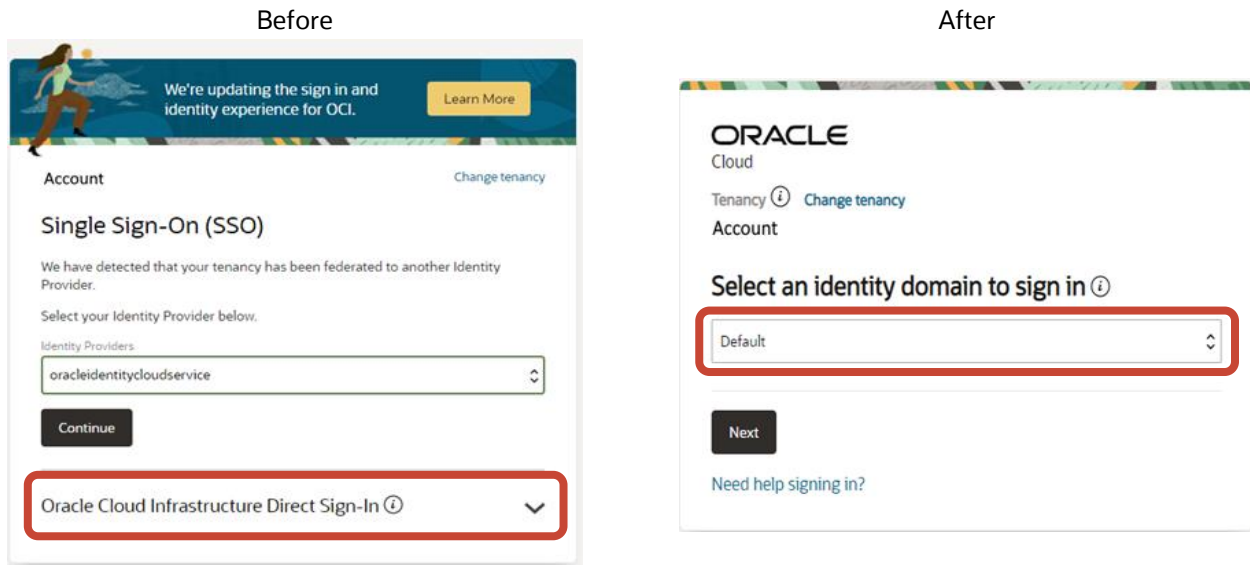
Before · After

2. Identity Cloud Service administration functionality has been moved to the Oracle Cloud Console

Customers who used 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.

Before · After
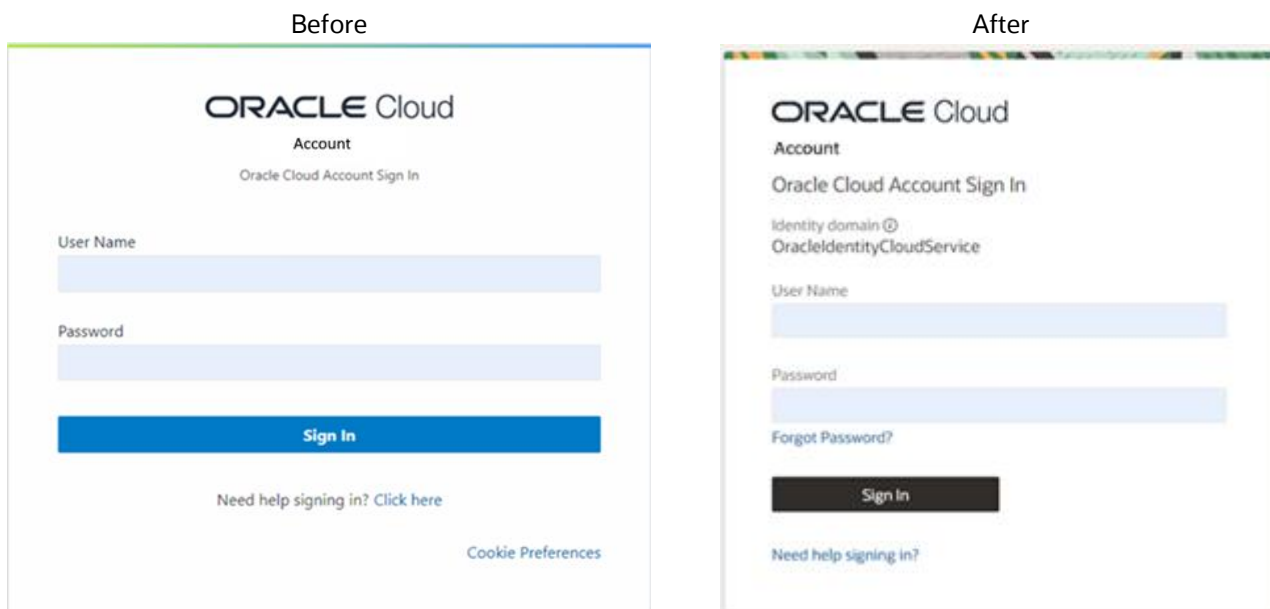
ORACLE

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.

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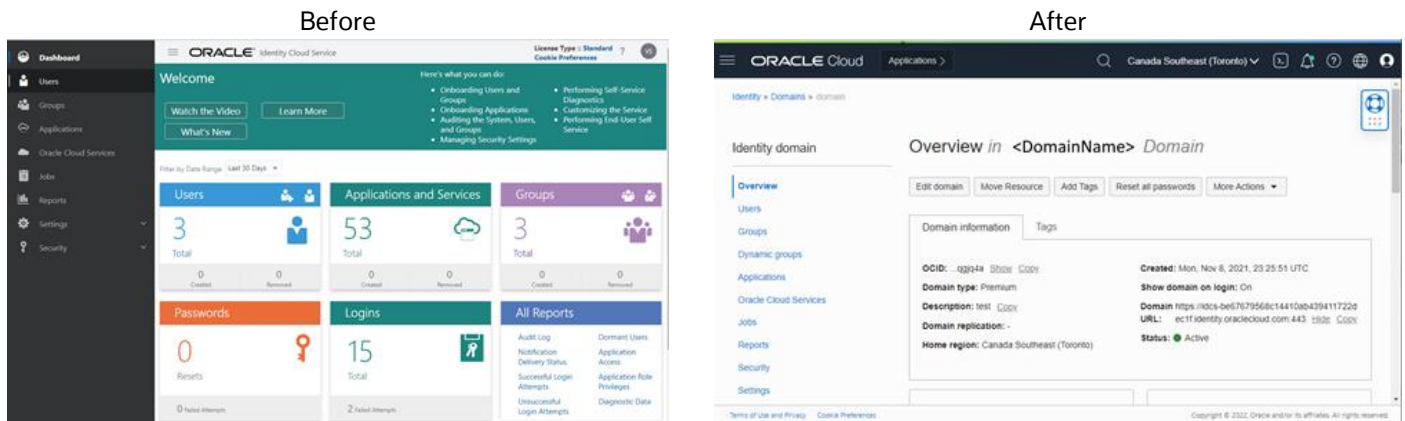
To navigate to Identity domains in the Oracle Cloud Console, Select **Identity & Security** in the navigation menu, then select **Domains** under the **Identity** heading.

Will my existing bookmarks work?

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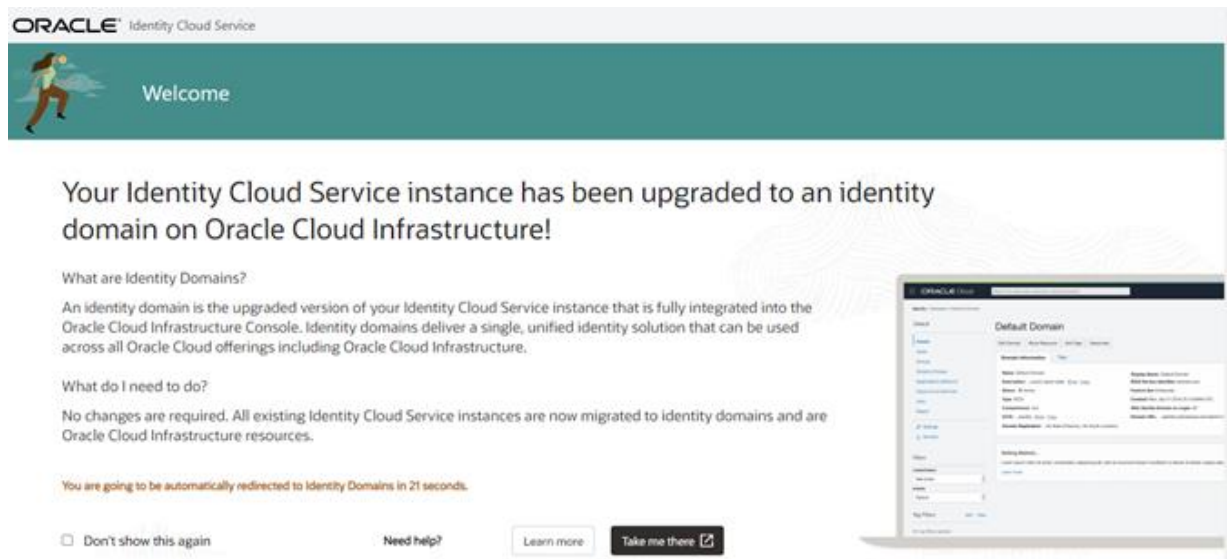
For example:

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

will be redirected to:

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

ORACLE

3. My Profile functionality has been 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

After

ORACLE

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 merged all the enterprise IAM capabilities of IDCS into OCI IAM natively. IAM functionality such as advanced authentication techniques and user lifecycle management are now natively available in your OCI tenancy.
- The Oracle Cloud sign-in page has been simplified with fewer options to reduce confusion for users.
- Customers who previously used 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 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 is 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.

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 same My Profile and Catalog pages. 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 does this impact existing OCI tenancies?

- Local OCI users and groups are now 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.

ORACLE

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 maintains 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_Administrators 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_Administrators 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 changed in the existing OCI IAM service?

- OCI IAM has been 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 have not been 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.

ORACLE

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 is still available. However, the identity and access functionality is now 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**. Outside North America, find your local office at: **oracle.com/contact**.

  blogs.oracle.com   facebook.com/oracle   twitter.com/oracle