Oracle® Cloud

Known Issues for Oracle Identity Cloud Service

Release 21.2.1

E55915-40

April 2021

Feature Limitations

This guide documents the complete set of Oracle Identity Cloud Service features. Your localized version of Oracle Identity Cloud Service might contain a subset of these features. Therefore, you might find features in this documentation that are not available in your localized version of Oracle Identity Cloud Service.

Delegated Authentication Limitations

Note the following limitations with delegated authentication in Oracle Identity Cloud Service.

Topics:

Changing the Password of a Microsoft Active Directory User

If you're changing the Microsoft Active Directory password of a user, then both the old and new passwords will be valid for a brief time. After an hour or two, have the user supply their username and old password. This password should no longer work.

Can’t Configure Delegated Authentication

If you see **The Delegated Authentication feature hasn't been activated because it's in the Beta phase.** message on the **Delegated Authentication** page, then delegated authentication hasn't been activated for your Oracle Identity Cloud Service instance. Contact DevOps to activate it.

Notification Template Limitations

Note the following limitations with Oracle Identity Cloud Service notification templates.

Topics:

Notification Template Customizations

Oracle Identity Cloud Service provides you with email templates for user and administrator notifications. You can tailor the recipients and content of these templates to meet the business and security requirements for your enterprise applications.

Note that customizations to any notification templates won't be upgraded with new content or email variables associated with future versions of the templates. This also applies to notification templates that you don't customize.

Update the Domain Name of an Email Address

If the domain name of the email address that appears in the **From Email** field for all notifications isn’t valid, then you can change it. To do so:

1. In the Identity Cloud Service console, expand the **Navigation Drawer**, click **Settings**, and then click **Notifications**.
2. Update the domain name that appears in the **From Email Address** field.
3. Click **Save**, and then in the **Confirmation** window, click **Yes**.

> **Tip:**
>
> You can revert back to the default email address of **no-reply@oracle.com**.

Microsoft Active Directory (AD) Bridge Limitations

The following section describes known limitations with the Microsoft Active Directory (AD) Bridge for Oracle Identity Cloud Service.

Topics:

- The AD server password has changed or expired, but I can't enter the new password in the client for the AD Bridge.
- The client for the AD Bridge crashes or stops synchronizing after upgrading Oracle Identity Cloud Service.
- Removing the domain for the AD Bridge may take time.
- After regenerating the Client Secret for the AD Bridge, the bridge doesn’t work.
- The AD Bridge can’t import users from AD into Oracle Identity Cloud Service.
- AD Bridge configured to synchronize users in a particular group do not synchronize immediately.

Restoring an old backup in AD affects identity synchronization.

Please clean up the users in Oracle Identity Cloud Service and start over.

The client for the AD Bridge operates on a Microsoft Windows environment only.

With the AD Bridge, Oracle Identity Cloud Service can connect to your AD enterprise directory structure.

For version 18.3.6 of Oracle Identity Cloud Service, use a Windows 7+ or Windows Server 2008 R2+ operating system, and version 4.6+ (this supports TLS 1.2) of the Microsoft .NET software framework (which is required for the bridge to run).

For more information about the certified versions for Oracle Identity Cloud Service, your operating system, and the Microsoft .NET software framework, refer to Understand the Microsoft Active Directory (AD) Bridge in *Administering Oracle Identity Cloud Service*.

When configuring an AD Bridge and selecting OUs, if I select a parent OU, then none of the children OUs are selected.

This issue has been seen intermittently and a fix is planned for a future release. If you experience this issue, then first expand the parent OU, deselect it, and then select the parent OU again. All visible child OUs are now selected.

The AD server password has changed or expired, but I can't enter the new password in the client for the AD Bridge.

To prevent this behavior from happening, before you use the AD Bridge to import any AD user accounts into Oracle Identity Cloud Service, enable the **Password Never Expires** option for the accounts in AD. Otherwise, the passwords for the accounts expire. If this occurs, then you can change the passwords using the following steps.

1. Go to the **Service MMC Console** on the host machine where the AD Bridge is running.
2. Select **Identity Cloud Service Microsoft Active Directory Bridge Service**, click **Properties**, click the **Log On** tab, and then change the account credentials.
3. Restart the service.
4. Go to the **Directory Integrations** page and ensure that the AD Bridge has an **Active** status.

> **Note:**
>
> The status of the service can also be checked in the configuration UI installed with the bridge.

The client for the AD Bridge crashes or stops synchronizing after upgrading Oracle Identity Cloud Service.

After an Oracle Identity Cloud Service upgrade, the AD Bridge client might crash because of new features implementation.

To resolve this issue:

1. Uninstall the client for the AD Bridge from your Microsoft Windows machine.
2. Go to the Identity Cloud Service console, click **Settings**, and then click **Directory Integrations**. Remove the AD Bridge.
3. Add a new bridge.
4. Download the new version of the client for the bridge and install it on your Microsoft Windows machine.

Users previously synchronized to the Oracle Identity Cloud Service are not affected by the recreation of the AD Bridge and new installation of the client software, if you use the same configuration for the new bridge as for the deleted one.

Removing the domain for the AD Bridge may take time.

If you have an AD server with a large amount of organizational units (OUs), and you then attempt to remove the domain for the AD Bridge from the **Directory Integrations** page of the Identity Cloud Service console, it may take several minutes for this to occur.

After regenerating the Client Secret for the AD Bridge, the bridge doesn't work.

If you're using the 17.2.6 version of the client for the AD Bridge, then you must upgrade your client to the latest version. See Create a Microsoft Active Directory (AD) Bridge to install the updated client for the bridge.

The AD Bridge can't import users from AD into Oracle Identity Cloud Service.

The AD Bridge must be able to access the AD organizational units (OUs) and the parent OUs that contain the users you want to import into Oracle Identity Cloud Service. To ensure that the bridge can access the OUs:

1. Launch Active Directory Users and Computers.
2. Right-click the OU that contains the users you want to import into Oracle Identity Cloud Service, and select **Properties** from the drop-down menu.
3. In the **Properties** window, click the **Security** tab.
4. In the **Advanced Security Settings** window, click the **Security** tab, and click **Advanced**.
5. Click **Add**.
6. In the **Permission Entry** window, click the **Select a Principal** link.
7. In the **Select User, Computer, Service Account, or Group** window, search for the user with which the AD Bridge is configured, and click **OK**.
8. In the **Permission Entry** window:
    a. From the **Type** drop-down menu, select **Allow**.
    b. From the **Applies to** drop-down menu, select **This Object and all descendant objects**.
    c. From the **Permissions** pane, select the **List contents**, **Read all properties**, and **Read permissions** check boxes.
    d. Click **OK**.
9. In the **Advanced Security Settings** window, click **OK**.

10. In the **Properties** window, click **OK**.
11. Close Active Directory Users and Computers.

AD Bridge configured to synchronize users in a particular group do not synchronize immediately.

The user synchronization from Microsoft Active Directory to Oracle Identity Cloud Service relies on the USN-Changed attribute value in Active Directory. The USN-Changed attribute is the update sequence number (USN) assigned by the local directory for the latest change. Active Directory increments this number for each change made to a user.

Assigning a user to a group modifies the group and not the user, so the USN-Changed attribute is not incremented in Active Directory for that user. Therefore, the user may not appear in Oracle Identity Cloud Service at the next user synchronization cycle - even though that user is now a candidate for synchronization. You can only synchronize the candidate user to Oracle Identity Cloud Service after you make a change to the user, which results in the USN-Changed attribute being incremented in Active Directory.

Identity Provider Limitations

Note the following identity provider limitations with Oracle Identity Cloud Service.

Topics:

Issue with SAML Identity Providers

If you have activated only one SAML identity provider and you don't want this identity provider to appear in the **Sign In** page, then don't assign the identity provider to either the default identity provider policy or to any app-specific identity provider policies.

Network Perimeter Limitations

Note the following network perimeter limitations with Oracle Identity Cloud Service

Topics:

English Translation Issues for Network Perimeters

Any errors related to adding, modifying, or removing network perimeters are for the English translation only. These errors will not appear for other translations. This issue can be fixed by applying the patch for 18.1.2.01.

Safari Browser Limitations

Learn about the Safari browser limitations.

The Safari client is not supported in Oracle Identity Cloud Service at this time. Safari Mobile is supported to launch the enrollment URL for the OMA app. See Add an Account to the OMA App by Using the Enrollment URL.

Interface Limitations

Note the following limitations and their solutions when using the Oracle Identity Cloud Service interfaces.

Topics:

Account Form Fields Are Not Translated

The Account Form that is used to assign custom apps to users or to assign users to custom apps that support identity provisioning is not translated this release.

Unable to Cancel a Service Instance

You cannot cancel a service instance after you have created it.

To remove a service instance, wait until Oracle Cloud notifies you that your service instance is active and ready to use. Then, delete the service instance.

My export job reports that it was successful. But my completion percentage is not 100%. How can that be?

During the execution of an export job, if some of the resources have been deleted (for example, resources that were eligible for export, but still not picked up by export job), the job status reports the export was successful, but it won't show a 100% completion percentage.

For example, assume that the tenant administrator submits a job to export 1000 users. However, during job execution, someone has deleted 50 users (which were about to be exported). In this example, the job status reports that the export was successful but the completion percentage will be 95%.

Unable to Delete Users from the Identity Cloud Service console if the User is Federated

Users synced from Active Directory (AD) and marked federated can't be deleted from Identity Cloud Service console. Removed these users from AD directly.

Chrome Auto-fill Causing Errors on the My Profile Details Page

This issue has been noted in Google Chrome. If you have signed-in to an Oracle Identity Cloud Service instance on one tab in Google Chrome and then open **My Profile Details** in a second tab within the same browser instance, and the **Work Phone Number** field is empty, the **Work Phone Number** field is being populated with an email address.

This is an improper format for the Work Phone Number field and any changes you try to save to the profile will fail because of this error.

To work around this issue:

- Only use one tab when accessing the Oracle Identity Cloud Interface UI.
- Ensure that all fields on the My Profile Details are correct before saving.

The 'isAuthoritative setting always shows as 'true' even if the 'isAuthoritative' attribute value is set to false.

If the On-premise Oracle Internet Directory Application is created via the REST API using the /Apps end-point, the POST payload or a subsequent PATCH must set the `isAuthoritative` attribute value to `true`. Note: The Oracle Identity Cloud Service user interface always displays the 'authoritative' check box as 'true' for such applications irrespective of the value set for `isAuthoritative`. You can't edit this setting from the user interface.

To work around this issue ensure that when creating the On-premise Oracle Internet Directory Application via the REST API using the /Apps end-point, the POST payload or a subsequent PATCH must set the `isAuthoritative` attribute value to `true`.

API Limitations

Note the following API limitations with Oracle Identity Cloud Service.

Topics:

OAuth 2.0 Limitation

The OAuth 2.0 implementation in Oracle Identity Cloud Service does not support getting scopes from multiple resource servers in a single token request.

Embedded Cloud Cache (ECC)

`/KerberosRealmUsers` endpoint. The >= and <= attributes, when used in a search filter, are not supported with this endpoint.

Job Imports

The **View Details** button in the **Jobs** page of the Identity Cloud Service console doesn't work for jobs that are imported using REST APIs.

Apps Limitation

If the On-premise 'Oracle Internet Directory' App is created via the back-end using the `/Apps` endpoint, the POST payload or a subsequent PATCH should set `isAuthoritative` attribute value to `true`. The IDCS UI always display **authoritative** checkbox as checked for such Apps irrespective of the value.

Endpoints without Examples

Some of the newly added REST API endpoints do not have examples.

Identity Cloud Service Application Catalog Limitation

Learn about the issues you may encounter when using the instructions for integrating Identity Cloud Service.

Topics

Accessibility Limitations

At this time, the instructions for integrating Identity Cloud Service are not fully Section 508 compliant. Specifically, many images are missing alternative text and the use of the > character must be removed in future releases.

Application Limitations

Note the following limitations and their solutions when managing applications.

Topics:

Max numbers settings for application synchronization inaccurate

There is an issue when enabling synchronization for an app catalog application. The number specified in **Max. number of creates** and **Max. number of deletes** syncs the number entered +10. For example, in a *create scenario*, set **Max. number of creates** to 10 and sync 25 new accounts without any owner match. The sync must stop anywhere between 10-20 accounts. Run the job again until all new accounts with unmatched owners are synced completely. This approach is primarily useful when

syncing batches that have many creates, updates, and deletes. The same behavior also occurs for numbers set in the **Max. number of deletes** field.

Re-granting the Office 365 app to the same user fails

Problem: After performing a revoke operation, re-granting the Office 365 App to the revoked user in Office 365 fails as the revoked user account is present in the Office 365 recycle bin and not permanently deleted. Solution: Ensure that you log in to Azure PowerShell and run the following command: `Remove-MsolUser -UserPrincipalName "user.idcs@fed-domain.com" -RemoveFromRecycleBin\`

User Field Missing Information on Import

If an administrator performs a parallel provisioning and synchronization (Import) operation, the User column might be missing the user name and email fields for the returned data on the Import tab.

Home Email is Displayed When Work Email Is Expected

When provisioning and synchronization are enabled for an Oracle Cloud app and you import users, the User column of the import table sometimes lists the Home Email Address instead of listing the Work Email Address even if the setting is Primary Email Type=work.

Adaptive Security Limitations

The following section describes known limitations with the Adaptive Security feature for Oracle Identity Cloud Service.

Topics:

I can’t set the speed for the Impossible travel between locations event.

For the **Impossible travel between locations** event, click the menu twice to set the speed to miles per hour (MPH) or kilometers per hour (KPH).

MFA Limitations

Note the following Multi-Factor Authentication (MFA) limitations with Oracle Identity Cloud Service.

Topic

Cannot Log In When Only PHONE_CALL Is Enabled

When MFA is enabled and you are enrolled just in PHONE_CALL using REST APIs, you cannot log in using IDCS UI.

Break Glass Limitation

When MFA is enabled, an identity domain administrator must enroll in more than one factor. If an identity domain administrator gets locked out of the MFA-enabled environment and has not enrolled in multiple factors, it can’t be unlocked further.

Internet Explorer v11 Compatibility Mode

When using Microsoft Internet Explorer version 11 in compatibility mode with the Windows 10 operating system, Oracle Identity Cloud Service supports only simple log in. In simple login mode, Multi-Factor Authentication (MFA) fails. To turn off compatibility mode in Internet Explorer:

1. Select **Tools,** and then **Compatibility View settings.**
2. Clear the **Display intranet sites in Compatibility View** check box.
3. Select the required websites from the list of websites that have been added to Compatibility View and click **Remove.**

Limit to the Number of Security Questions That Display

When defining security questions for MFA, you can add as many as you want. However, only 48 security questions can appear in the Oracle Identity Cloud Service administration console.

Oracle® Cloud Known Issues for Oracle Identity Cloud Service, Release 21.2.1
E55915-40

Documentation that describes new features available in Oracle Identity Cloud Service.