ORACLE

Authenticating Oracle DB with Azure AD

Inge Os
Cloud Security Advisor
inge.os@oracle.com

Create Enterprise Application within AzureAD

Configuration steps
- Register secure APP with AzureAD App Registration
- Configure shadow app for user mapping and group/db role mapping

For Non Autonomous Database
- Enable TLS for Oracle Net
- Configure database for AzureAZ AuthN

For Autonomous Database
- Configure database for AzureAZ AuthN

Configure Client

Create AzureAD confidential App

Default Directory - Microsoft Azu

https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/Overview

Oracle favorites folder | Oracle Applications | Cloud Sign In | Home | Oracle Clou...

Microsoft Azure | Search resources, services, and docs (G+/) | m DEFAULT DIRECTORY

Home >

Default Directory | Overview

Azure Active Directory

Add | Manage tenants | What's new | Preview features | Got feedback?

Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center!

Overview | Monitoring | Properties | Recommendations | Tutorials

Search your tenant

Basic information

Name	Default Directory	Users	17
Tenant ID	9bad	Groups	5
Primary domain	microsoft.com	Applications	6
License	Azure AD Free	Devices	0

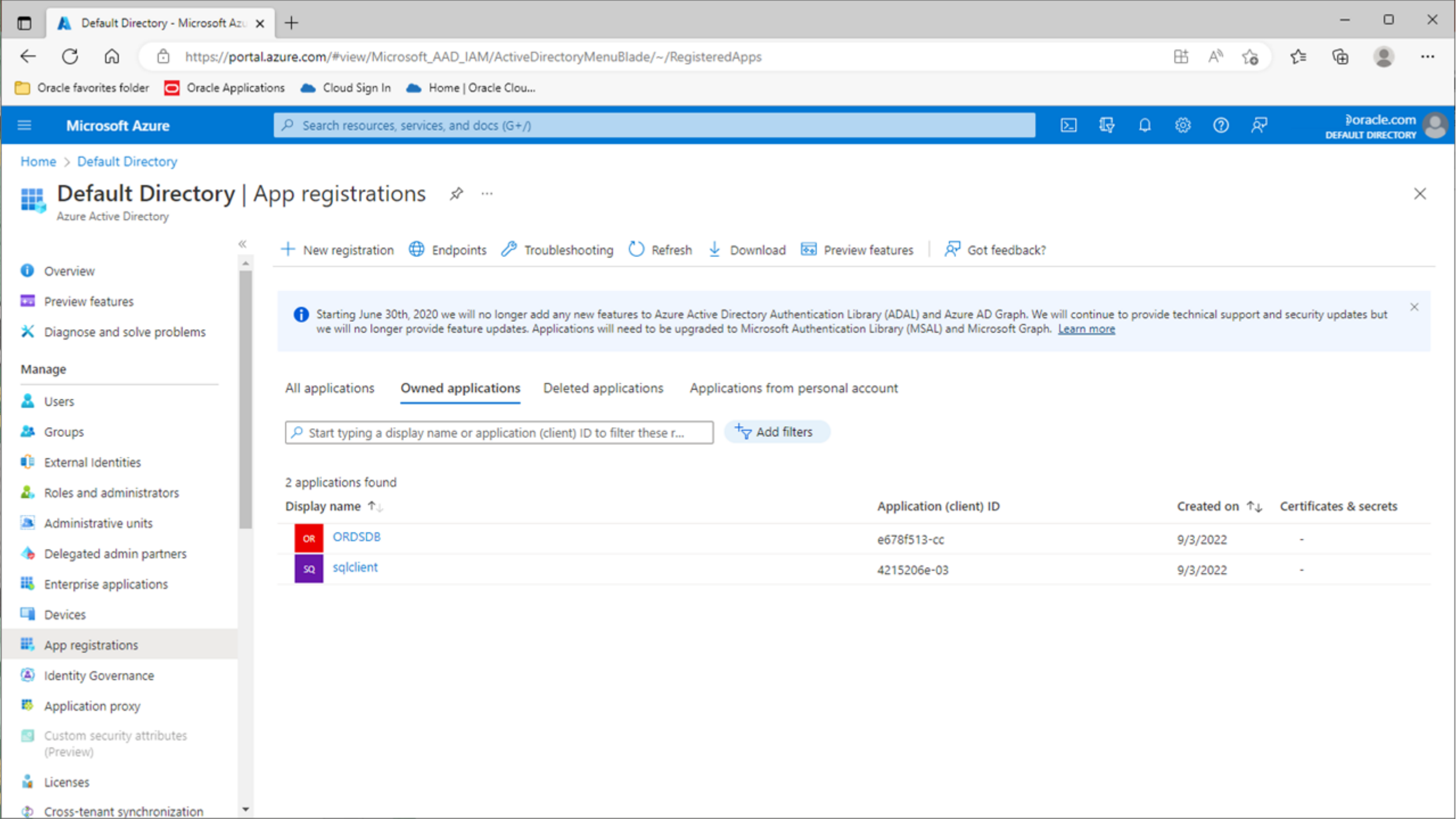
Alerts

Upcoming Authenticator number matching enforcement

Microsoft Authenticator number matching admin controls will be removed after February 27, 2023. Number matching will be enforced for all Microsoft Authenticator users after this date.

Upcoming MFA Server deprecation

Please migrate from MFA Server to Azure AD Multi-Factor Authentication by September 2024 to avoid any service impact.


Default Directory - Microsoft Azu
https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/RegisteredApps
Oracle favorites folder
Oracle Applications
Cloud Sign In
Home | Oracle Clou...
Microsoft Azure
Search resources, services, and docs (G+/)
oracle.com
DEFAULT DIRECTORY
Home > Default Directory
Default Directory | App registrations
Azure Active Directory
New registration
Endpoints
Troubleshooting
Refresh
Download
Preview features
Got feedback?
Overview
Preview features
Diagnose and solve problems
Manage
Users
Groups
External Identities
Roles and administrators
Administrative units
Delegated admin partners
Enterprise applications
Devices
App registrations
Identity Governance
Application proxy
Custom security attributes (Preview)
Licenses
Cross-tenant synchronization
Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more
All applications
Owned applications
Deleted applications
Applications from personal account
Start typing a display name or application (client) ID to filter these r...
Add filters
2 applications found
Display name
Application (client) ID
Created on
Certificates & secrets
OR
ORDSDB
e678f513-cc
9/3/2022
-
SQ
sqlclient
4215206e-03
9/3/2022
-

Register an application - Microsc

https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/CreateApplicationBlade/quickStartType~/null/isMSAApp~/false

Oracle favorites folder | Oracle Applications | Cloud Sign In | Home | Oracle Clou...

Microsoft Azure

Search resources, services, and docs (G+/)

oracle.com
DEFAULT DIRECTORY

Home > Default Directory | App registrations >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

ios3db19c

Supported account types

Who can use this application or access this API?

- (•) Accounts in this organizational directory only (Default Directory only - Single tenant)
- ( ) Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ( ) Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ( ) Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform | e.g. https://example.com/auth

By proceeding, you agree to the Microsoft Platform Policies

Register

ios3db19c - Microsoft Azure

https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/Overview/quickStartType~/null/sourceType/Microsoft_AAD_IAM/appId/98...

Oracle favorites folder | Oracle Applications | Cloud Sign In | Home | Oracle Clou...

Microsoft Azure | Search resources, services, and docs (G+/) | @oracle.com DEFAULT DIRECTORY

Home > Default Directory | App registrations >

ios3db19c

Collect these values for DB configuration

Search

- Overview
- Quickstart
- Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Delete | Endpoints | Preview features

Essentials

Display name	: ios3db19c	Client credentials	: Add a certificate or secret
Application (client) ID	: 986986539865986986539898698653986 5	Redirect URIs	: Add a Redirect URI
Object ID	: 42cl42cf5-42cf542cl42cf5-4242cl42cf5-42cf5	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: 9ba9bad-9bad9ba9bad-9b9ba9bad-9bad	Managed application in l...	: ios3db19c
Supported account types	: My organization only		

Get Started | Documentation

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

Call APIs

Build more powerful apps with rich user and

Sign in users in 5 minutes

Use our SDKs to sign in users and call APIs in a few

Configure for your organization

Assign users and groups, apply conditional access

ios3db19c | Expose an API

Search

Overview
Quickstart
Integration assistant

Manage

Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest

Support + Troubleshooting

Troubleshooting
New support request

Got feedback?

Application ID URI ⓘ Set

Scopes defined by this API

Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.

Adding a scope here creates only delegated permissions. If you are looking to create application-only scopes, use 'App roles' and define app roles assignable to application type. Go to App roles.

+ Add a scope

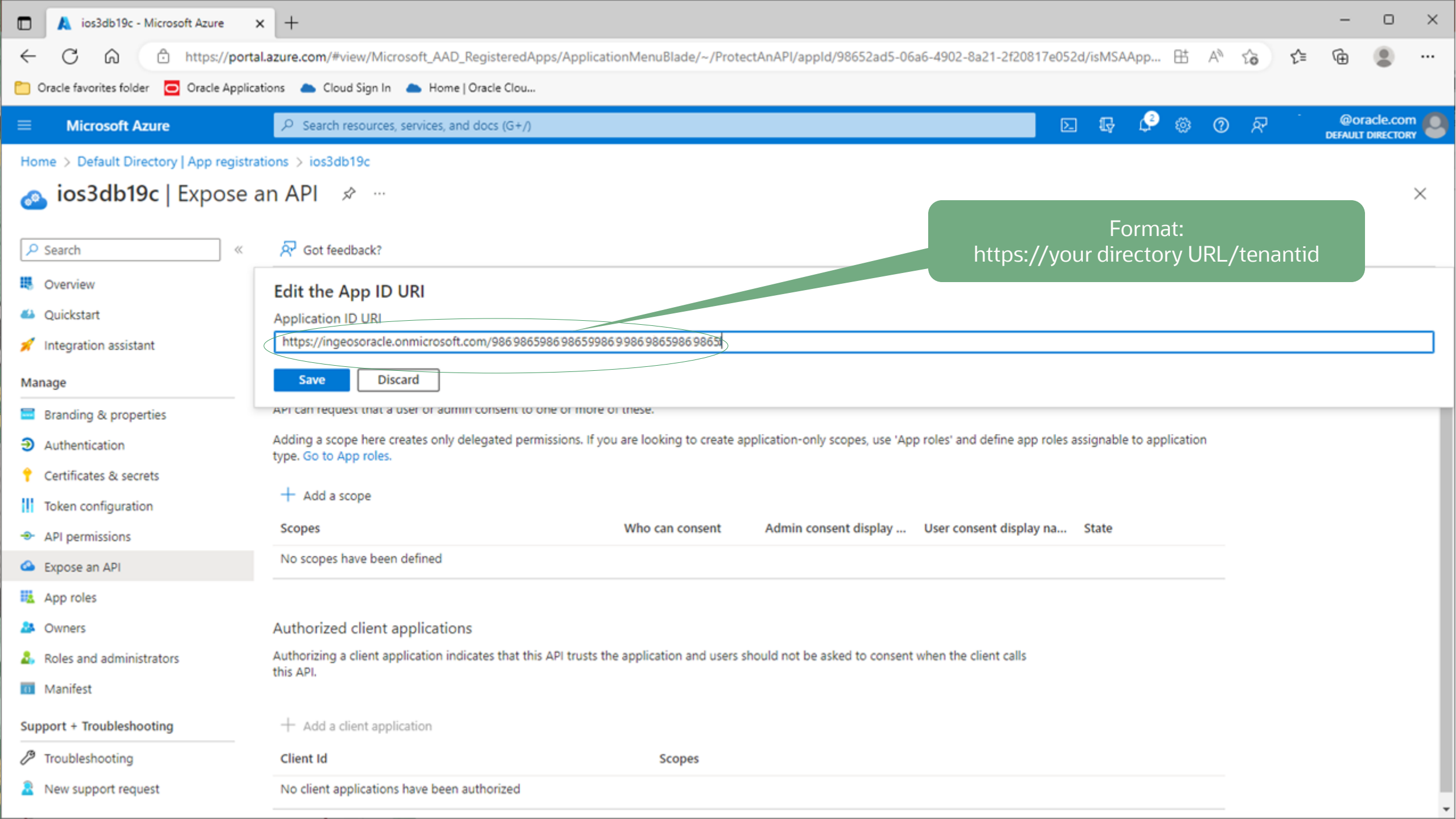
Scopes	Who can consent	Admin consent display ...	User consent display na...	State
No scopes have been defined				

Authorized client applications

Authorizing a client application indicates that this API trusts the application and users should not be asked to consent when the client calls this API.

+ Add a client application

Client Id	Scopes
No client applications have been authorized	


ios3db19c - Microsoft Azure
https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/ProtectAnAPI/appId/98652ad5-06a6-4902-8a21-2f20817e052d/isMSAApp...
Oracle favorites folder
Oracle Applications
Cloud Sign In
Home | Oracle Clou...
Microsoft Azure
Search resources, services, and docs (G+/)
@oracle.com
DEFAULT DIRECTORY
Home > Default Directory | App registrations > ios3db19c
ios3db19c | Expose an API
Search
Got feedback?
Overview
Quickstart
Integration assistant
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
Troubleshooting
New support request
Edit the App ID URI
Application ID URI
https://ingeosoracle.onmicrosoft.com/986 9865986 98659986 9 986 9865986 9865
Save
Discard
Format:
https://your directory URL/tenantid
Adding a scope here creates only delegated permissions. If you are looking to create application-only scopes, use 'App roles' and define app roles assignable to application type. Go to App roles.
Add a scope
Scopes
Who can consent
Admin consent display ...
User consent display na...
State
No scopes have been defined
Authorized client applications
Authorizing a client application indicates that this API trusts the application and users should not be asked to consent when the client calls this API.
Add a client application
Client Id
Scopes
No client applications have been authorized

ios3db19c | Expose an API

Search

Overview
Quickstart
Integration assistant

Manage

Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest

Support + Troubleshooting

Troubleshooting
New support request

Got feedback?

Application ID URI: https://ingeosoracle.onmicrosoft.com/98659865986598698659865986986598659865

Scopes defined by this API

Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.

Adding a scope here creates only delegated permissions. If you are looking to create application-only scopes, use 'App roles' and define app roles assignable to application type. Go to App roles.

Add a scope

Scopes	Who can consent	Admin consent display ...	User consent display na...	State
No scopes have been defined				

Authorized client applications

Authorizing a client application indicates that this API trusts the application and users should not be asked to consent when the client calls this API.

Add a client application

Client Id	Scopes
No client applications have been authorized	

Add a scope - Microsoft Azure

https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/ProtectAnAPI/appId/98652ad5-06a6-4902-8a21-2f20817e052d/isMSAApp...

Oracle favorites folder | Oracle Applications | Cloud Sign In | Home | Oracle Clou...

Microsoft Azure | Search resources, services, and docs (G+/) | @oracle.com DEFAULT DIRECTORY

Home > Default Directory | App registrations > ios3db19c

ios3db19c | Expose an API

Search

- Overview
- Quickstart
- Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Got feedback?

Application ID URI: https://oracle.oracle.onmicrosoft.com/98652986529865286528652986529865 98652

Scopes defined by this API

Define custom scopes to restrict access to data and functionality protected by the API. An application that requires API can request that a user or admin consent to one or more of these.

Adding a scope here creates only delegated permissions. If you are looking to create application-only scopes, use ' type. Go to App roles.

+ Add a scope

Scopes	Who can consent	Admin consent display
No scopes have been defined		

Authorized client applications

Authorizing a client application indicates that this API trusts the application and users should not be asked to cons this API.

+ Add a client application

Client Id	Scopes
No client applications have been authorized	

Add a scope

Scope name * e.g. Files.Read

https://ioracleoracle.onmicrosoft.com/98652986529865986529865298652 98652/

Who can consent? Admins and users | Admins only

Admin consent display name * e.g. Read user files

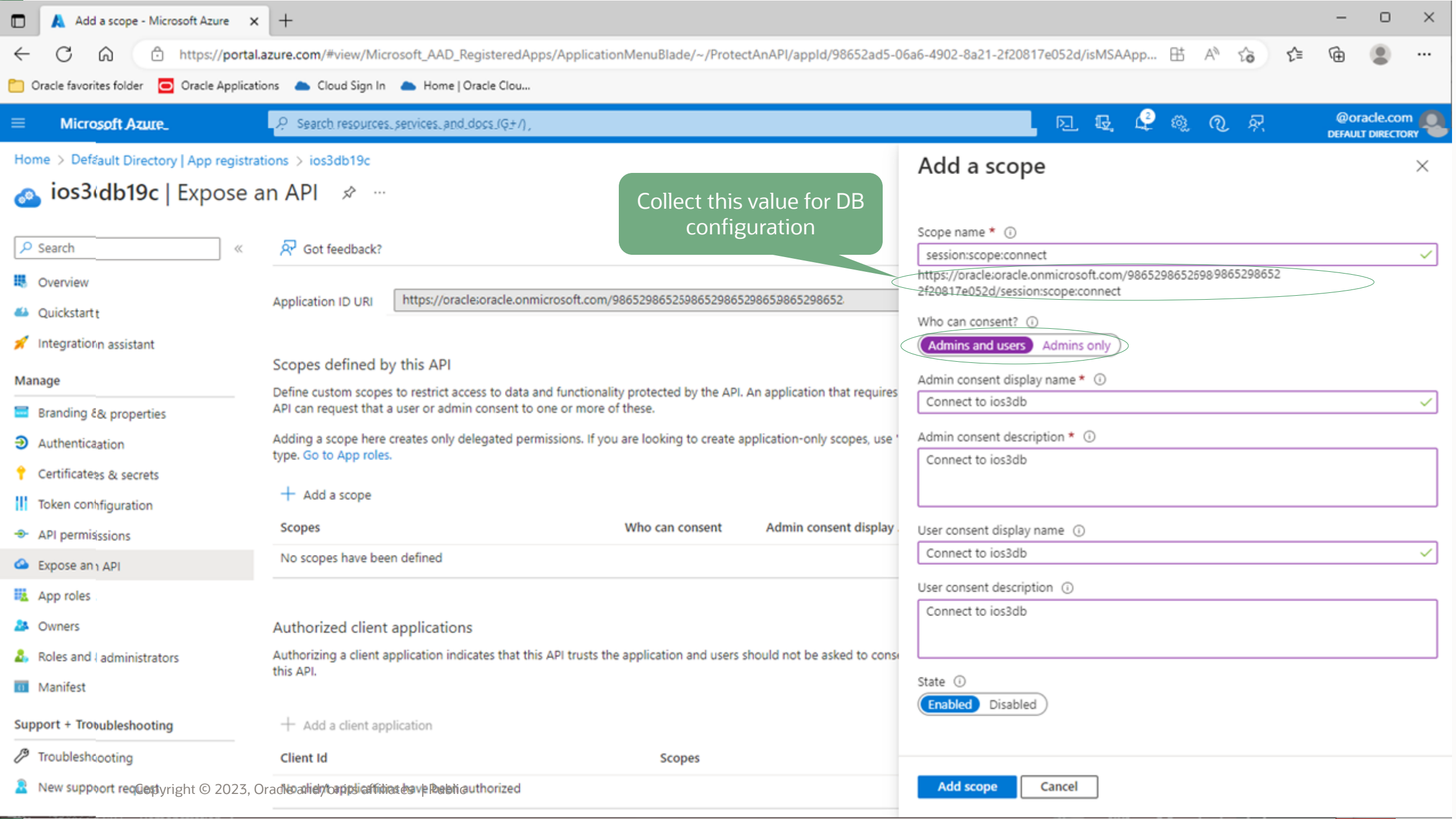
Admin consent description * e.g. Allows the app to read the signed-in user's files.

User consent display name e.g. Read your files

User consent description e.g. Allows the app to read your files.

State: Enabled | Disabled

Add scope | Cancel



ios3db19c | Expose an API

Update application Authentication
Successfully added Scope

Search

Overview
Quickstart
Integration assistant

Manage

Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest

Support + Troubleshooting

Troubleshooting
New support request

Got feedback?

Got a second to give us some feedback? →

Application ID URI: https://ingeosoracle.onmicrosoft.com/98652986529865298652986598652986521

Scopes defined by this API

Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.

Adding a scope here creates only delegated permissions. If you are looking to create application-only scopes, use 'App roles' and define app roles assignable to application type. Go to App roles.

+ Add a scope

Scopes	Who can consent	Admin consent display ...	User consent display na...	State
https://oracleoracle.onmicrosoft.com/9865298/98652...	Admins and users	Connect to ios3db	Connect to ios3db	Enabled

Authorized client applications

Authorizing a client application indicates that this API trusts the application and users should not be asked to consent when the client calls this API.

+ Add a client application

Collect data for the database

Take note of:

- Client-id
- Tenant ID
- Application URI
- Scope definition

These data will be used later for configuration of the database

Create global users and global roles

For the mapping scheme to work some actions needs to be taken on the Azure side:

- Create the role name in the app
- Assign the roles to users
- Assing the user(s) to the shadow Enterprise application
  - Note: For free tier AzureAD, only users, not groups can be assigned to an enterprise application

ios3db19c | App roles

Search

Overview
Quickstart
Integration assistant

Manage

Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest

Support + Troubleshooting

Troubleshooting
New support request

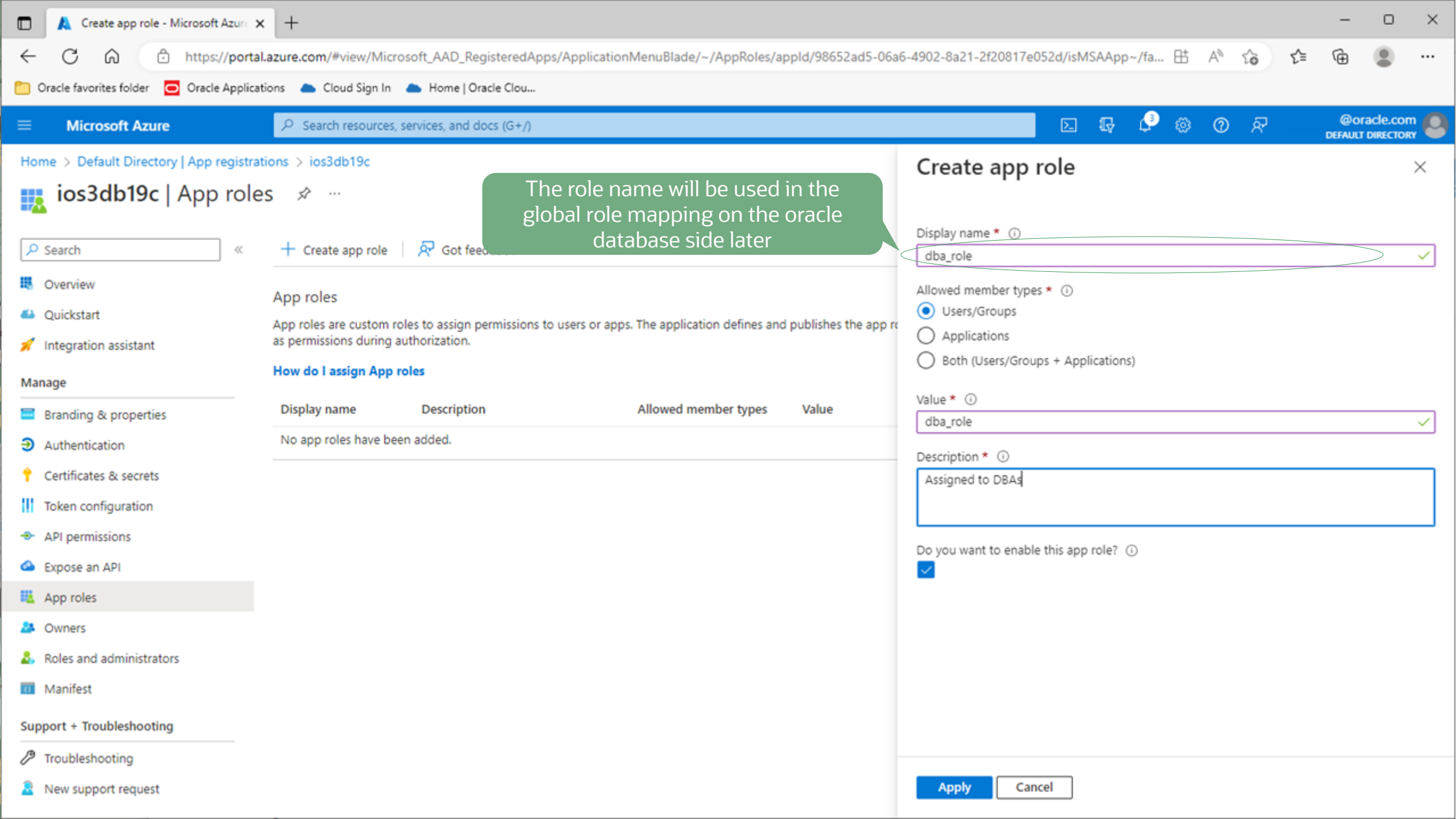
Create app role | Got feedback?

App roles

App roles are custom roles to assign permissions to users or apps. The application defines and publishes the app roles and interprets them as permissions during authorization.

How do I assign App roles

Display name	Description	Allowed member types	Value	ID	State
No app roles have been added.					


Create app role - Microsoft Azure
https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/AppRoles/appId/98652ad5-06a6-4902-8a21-2f20817e052d/isMSAApp~/fa...
Oracle favorites folder
Oracle Applications
Cloud Sign In
Home | Oracle Clou...
Microsoft Azure
Search resources, services, and docs (G+/)
@oracle.com
DEFAULT DIRECTORY
Home > Default Directory | App registrations > ios3db19c
ios3db19c | App roles
Search
Overview
Quickstart
Integration assistant
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
Troubleshooting
New support request
Create app role
Got feedback?
App roles
App roles are custom roles to assign permissions to users or apps. The application defines and publishes the app roles as permissions during authorization.
How do I assign App roles
Display name
Description
Allowed member types
Value
No app roles have been added.
The role name will be used in the global role mapping on the oracle database side later
Create app role
Display name *
dba_role
Allowed member types *
Users/Groups
Applications
Both (Users/Groups + Applications)
Value *
dba_role
Description *
Assigned to DBAs
Do you want to enable this app role?
Apply
Cancel

ios3db19c | App roles

Create new app role
Successfully updated ios3db19c

Search

Overview
Quickstart
Integration assistant

Manage

Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest

Support + Troubleshooting

Troubleshooting
New support request

Create app role | Got feedback?

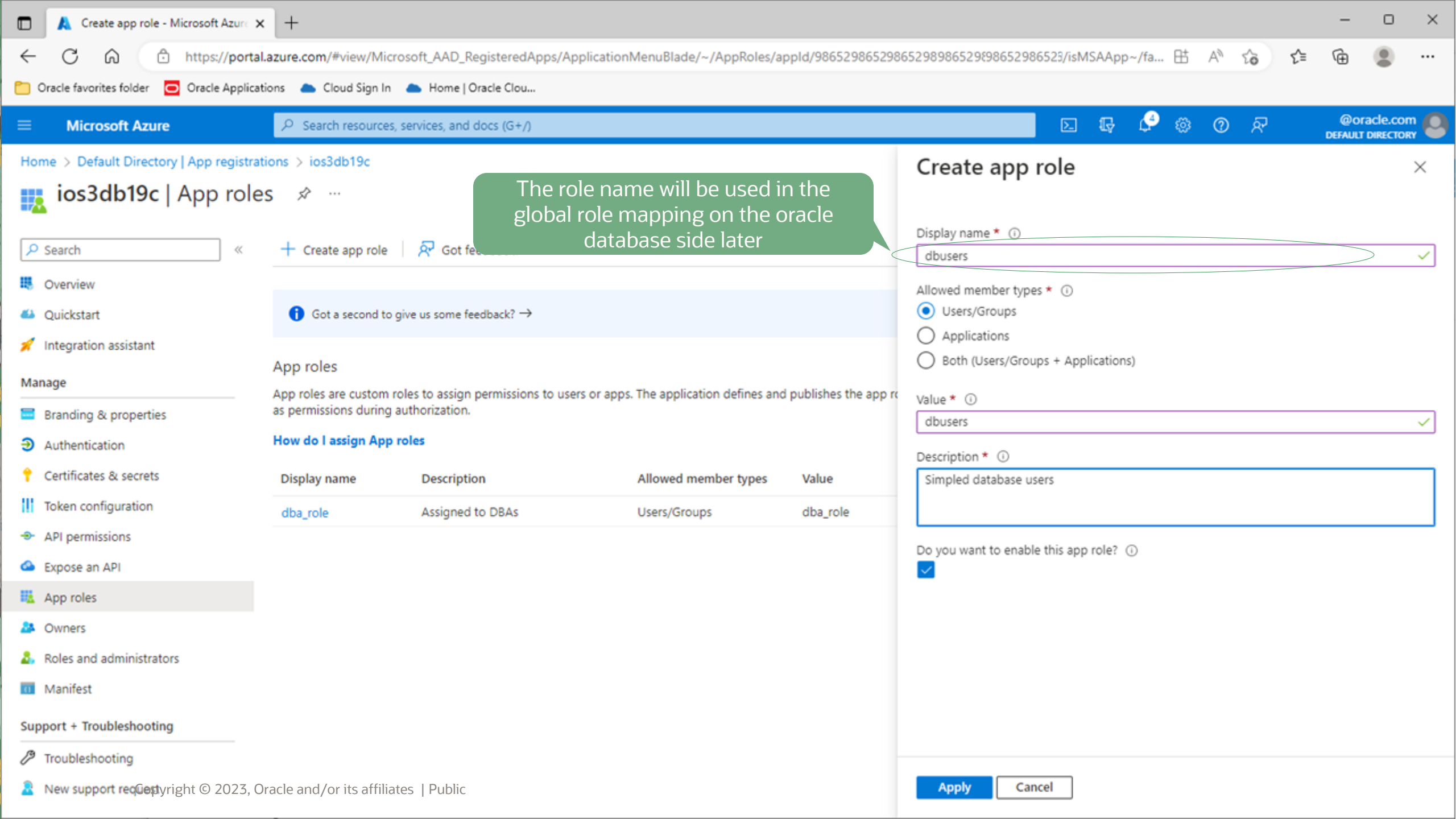
Got a second to give us some feedback? →

App roles

App roles are custom roles to assign permissions to users or apps. The application defines and publishes the app roles and interprets them as permissions during authorization.

How do I assign App roles

Display name	Description	Allowed member types	Value	ID	State
dba_role	Assigned to DBAs	Users/Groups	dba_role	f8f2427d-02a5-4abe-9...	Enabled



ios3db19c | App roles

Create new app role
Successfully updated ios3db19c

Search

Overview
Quickstart
Integration assistant

Manage

Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest

Support + Troubleshooting

Troubleshooting
New support request

Create app role | Got feedback?

Got a second to give us some feedback? →

App roles

App roles are custom roles to assign permissions to users or apps. The application defines and publishes the app roles and interprets them as permissions during authorization.

How do I assign App roles

Display name	Description	Allowed member types	Value	ID	State
dba_role	Assigned to DBAs	Users/Groups	dba_role	f8f2427d-02a5-4abe-9...	Enabled
dbusers	Simpled database users	Users/Groups	dbusers	e4b465a7-a11e-4d29-...	Enabled

ios3db19c | Authentication

Search

Overview
Quickstart
Integration assistant

Manage

Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest

Support + Troubleshooting

Troubleshooting

Got feedback?

Got a second to give us some feedback? →

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Supported account types

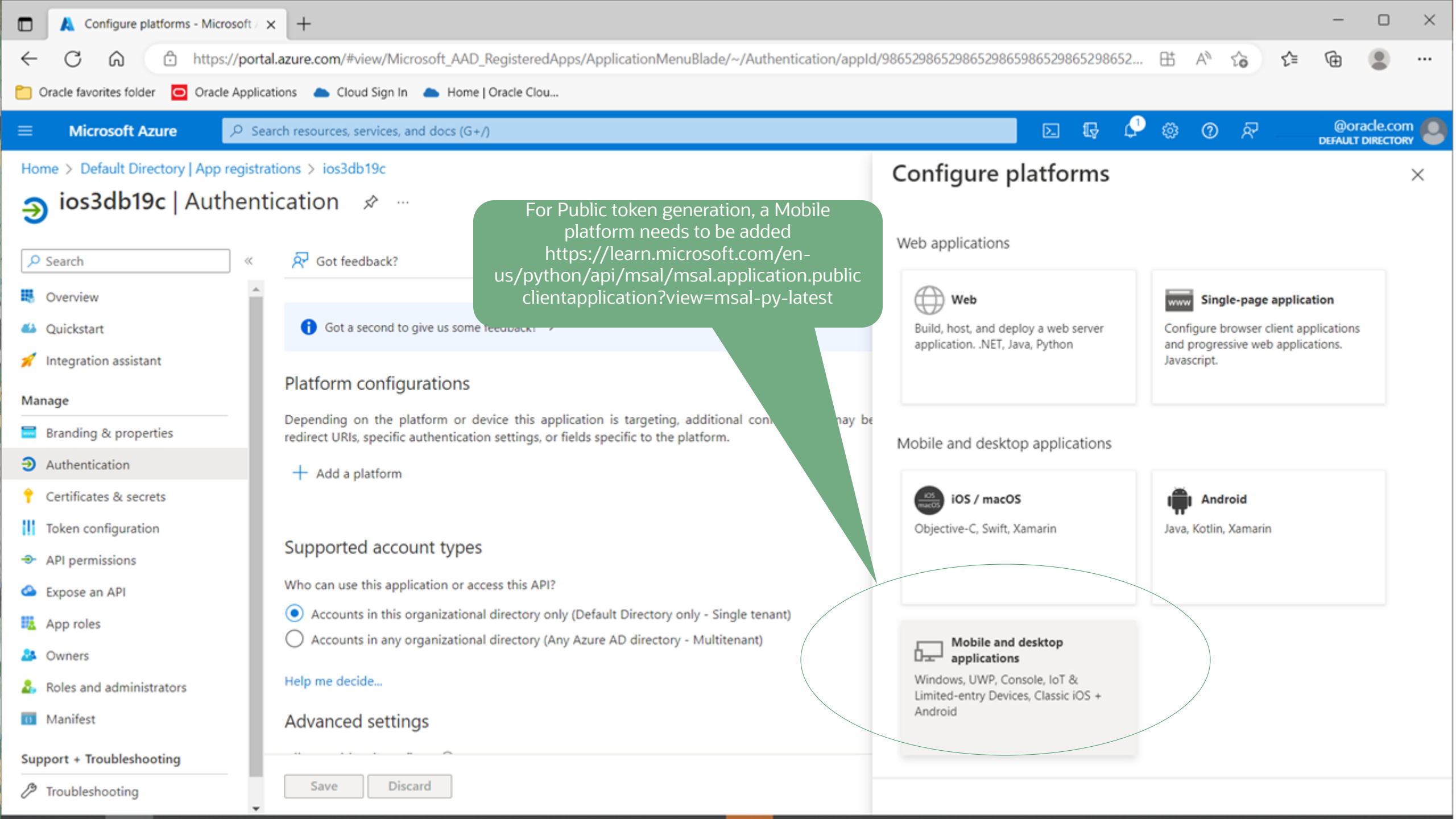
Who can use this application or access this API?

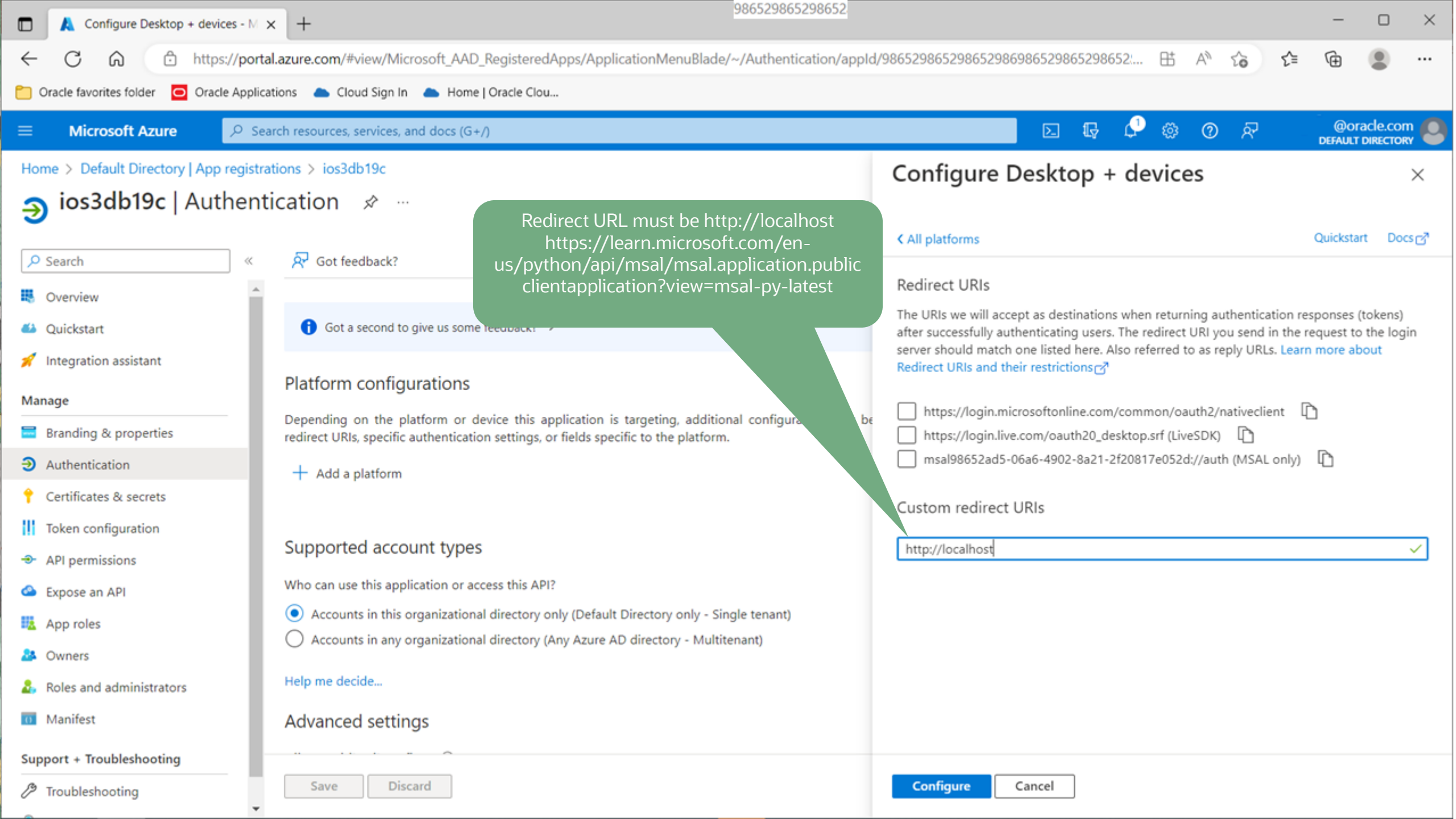
- (●) Accounts in this organizational directory only (Default Directory only - Single tenant)
- ( ) Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Help me decide...

Advanced settings

Save | Discard


Configure platforms - Microsoft
https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/Authentication/appId/9865298652986529865986529865298652...
Oracle favorites folder
Oracle Applications
Cloud Sign In
Home | Oracle Clou...
Microsoft Azure
Search resources, services, and docs (G+/)
@oracle.com
DEFAULT DIRECTORY
Home > Default Directory | App registrations > ios3db19c
ios3db19c | Authentication
Search
Got feedback?
Overview
Quickstart
Integration assistant
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
Troubleshooting
Got a second to give us some feedback?
Platform configurations
Depending on the platform or device this application is targeting, additional con... may be
redirect URIs, specific authentication settings, or fields specific to the platform.
Add a platform
Supported account types
Who can use this application or access this API?
Accounts in this organizational directory only (Default Directory only - Single tenant)
Accounts in any organizational directory (Any Azure AD directory - Multitenant)
Help me decide...
Advanced settings
Save
Discard
For Public token generation, a Mobile platform needs to be added https://learn.microsoft.com/en-us/python/api/msal/msal.application.publicclientapplication?view=msal-py-latest
Configure platforms
Web applications
Web
Build, host, and deploy a web server application. .NET, Java, Python
Single-page application
Configure browser client applications and progressive web applications. Javascript.
Mobile and desktop applications
iOS / macOS
Objective-C, Swift, Xamarin
Android
Java, Kotlin, Xamarin
Mobile and desktop applications
Windows, UWP, Console, IoT & Limited-entry Devices, Classic iOS + Android


986529865298652
Configure Desktop + devices - M
https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/Authentication/appId/986529865298652986986529865298652...
Oracle favorites folder
Oracle Applications
Cloud Sign In
Home | Oracle Clou...
Microsoft Azure
Search resources, services, and docs (G+/)
@oracle.com
DEFAULT DIRECTORY
Home > Default Directory | App registrations > ios3db19c
ios3db19c | Authentication
Search
Got feedback?
Overview
Quickstart
Integration assistant
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
Troubleshooting
Got a second to give us some feedback?
Platform configurations
Depending on the platform or device this application is targeting, additional configura be
redirect URIs, specific authentication settings, or fields specific to the platform.
Add a platform
Supported account types
Who can use this application or access this API?
Accounts in this organizational directory only (Default Directory only - Single tenant)
Accounts in any organizational directory (Any Azure AD directory - Multitenant)
Help me decide...
Advanced settings
Save
Discard
Redirect URL must be http://localhost
https://learn.microsoft.com/en-us/python/api/msal/msal.application.publicclientapplication?view=msal-py-latest
Configure Desktop + devices
All platforms
Quickstart
Docs
Redirect URIs
The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions
https://login.microsoftonline.com/common/oauth2/nativeclient
https://login.live.com/oauth20_desktop.srf (LiveSDK)
msal98652ad5-06a6-4902-8a21-2f20817e052d://auth (MSAL only)
Custom redirect URIs
http://localhost
Configure
Cancel

ios3db19c | Authentication

Search

Overview
Quickstart
Integration assistant

Manage

Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest

Support + Troubleshooting

Troubleshooting

Got feedback?

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

Add a platform

Mobile and desktop applications

Quickstart | Docs

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

- https://login.microsoftonline.com/common/oauth2/nativeclient
- https://login.live.com/oauth20_desktop.srf (LiveSDK)
- msal98652ad5-06a6-4902-8a21-2f20817e052d://auth (MSAL only)
- http://localhost

Add URI

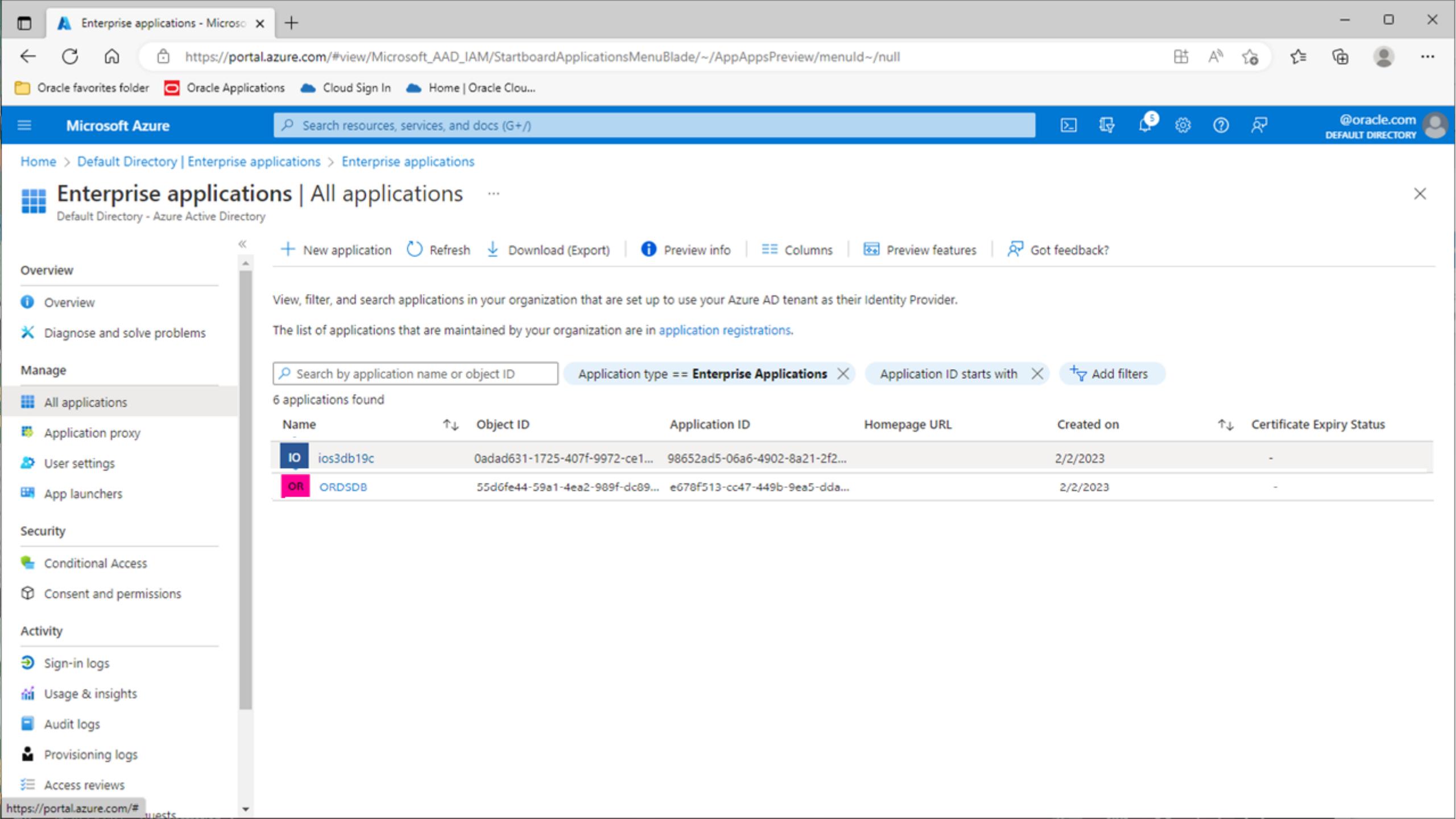
Save | Discard

Configure AzureAD Shadow Enterprise Application

In Azure, the app registration will create a shadow Enterprise application.

In this application assign the groups (require subscribed AzureAD) or users to the application.

These users will then be assigned the Oracle DB enterprise user and enterprise roles required for mapping to Oracle Database


Enterprise applications - Microso
https://portal.azure.com/#view/Microsoft_AAD_IAM/StartboardApplicationsMenuBlade/~/AppAppsPreview/menuId~/null
Oracle favorites folder
Oracle Applications
Cloud Sign In
Home | Oracle Clou...
Microsoft Azure
Search resources, services, and docs (G+/)
@oracle.com
DEFAULT DIRECTORY
Home > Default Directory | Enterprise applications > Enterprise applications
Enterprise applications | All applications
Default Directory - Azure Active Directory
New application
Refresh
Download (Export)
Preview info
Columns
Preview features
Got feedback?
Overview
Overview
Diagnose and solve problems
Manage
All applications
Application proxy
User settings
App launchers
Security
Conditional Access
Consent and permissions
Activity
Sign-in logs
Usage & insights
Audit logs
Provisioning logs
Access reviews
View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider.
The list of applications that are maintained by your organization are in application registrations.
Search by application name or object ID
Application type == Enterprise Applications
Application ID starts with
Add filters
6 applications found
Name
Object ID
Application ID
Homepage URL
Created on
Certificate Expiry Status
IO
ios3db19c
0adad631-1725-407f-9972-ce1...
98652ad5-06a6-4902-8a21-2f2...
2/2/2023
-
OR
ORDSDB
55d6fe44-59a1-4ea2-989f-dc89...
e678f513-cc47-449b-9ea5-dda...
2/2/2023
-
https://portal.azure.com/#

ios3db19c | Overview

Enterprise Application

Overview
Deployment Plan
Diagnose and solve problems

Manage

Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Custom security attributes (preview)

Security

Conditional Access
Permissions
Token encryption

Properties

IO

Name

ios3db19c

Copy to clipboard

Application ID

98652ad5-06a6-4902-8a21-...

Object ID

0adad631-1725-407f-9972-...

Getting Started

1. Assign users and groups

Provide specific users and groups access to the applications

Assign users and groups

2. Provision User Accounts

You'll need to create user accounts in the application

Learn more

3. Conditional Access

Secure access to this application with a customizable access policy.

Create a policy

4. Self service

Enable users to request access to the application using their Azure AD credentials

Get started

ios3db19c | Users and groups

Enterprise Application

Overview
Deployment Plan
Diagnose and solve problems

Manage

Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Custom security attributes (preview)

Security

Conditional Access
Permissions
Token encryption

Add user/group | Edit assignment | Remove | Update credentials | Columns | Got feedback?

The application will not appear for assigned users within My Apps. Set 'visible to users?' to yes in properties to enable this. →

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration.

First 200 shown, to search all users & gro...

Display Name	Object Type	Role assigned
No application assignments found		

Add Assignment - Microsoft Azu

https://portal.azure.com/#view/Microsoft_AAD_IAM/AddAssignmentBlade/objectId/0adad631-1725-407f-9972-ce1ecb59fe42

Oracle favorites folder | Oracle Applications | Cloud Sign In | Home | Oracle Clou...

Microsoft Azure

Search resources, services, and docs (G+/)

@oracle.com
DEFAULT DIRECTORY

Home > Default Directory | Enterprise applications > Enterprise applications | All applications > ios3db19c | Users and groups >

Add Assignment

Default Directory

Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

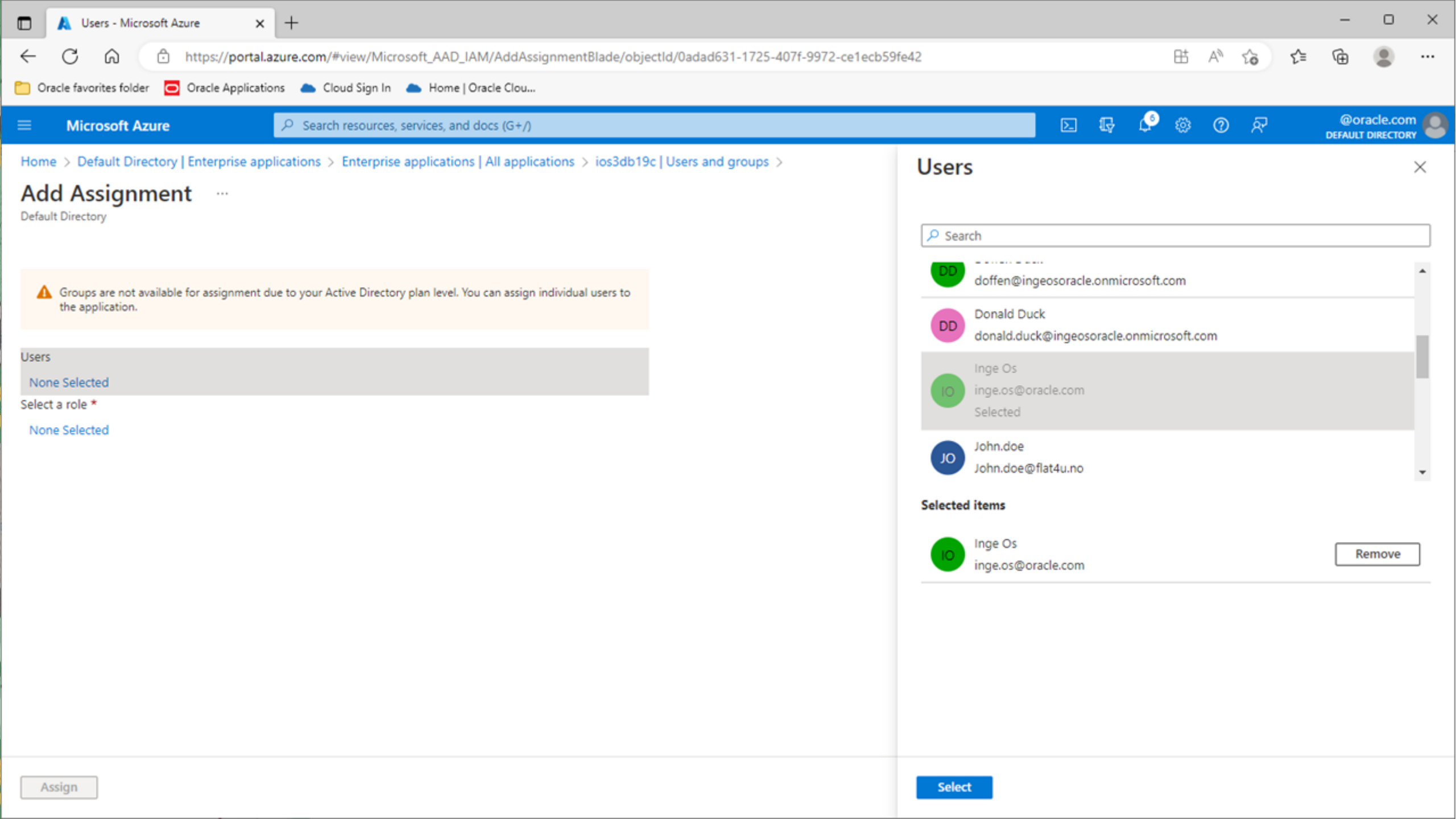
Users

None Selected

Select a role *

None Selected

Assign


Users - Microsoft Azure
https://portal.azure.com/#view/Microsoft_AAD_IAM/AddAssignmentBlade/objectId/0adad631-1725-407f-9972-ce1ecb59fe42
Oracle favorites folder
Oracle Applications
Cloud Sign In
Home | Oracle Clou...
Microsoft Azure
Search resources, services, and docs (G+/)
@oracle.com
DEFAULT DIRECTORY
Home > Default Directory | Enterprise applications > Enterprise applications | All applications > ios3db19c | Users and groups >
Add Assignment
Default Directory
Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.
Users
None Selected
Select a role *
None Selected
Assign
Users
Search
DD
doffen@ingeosoracle.onmicrosoft.com
DD
Donald Duck
donald.duck@ingeosoracle.onmicrosoft.com
IO
Inge Os
inge.os@oracle.com
Selected
JO
John.doe
John.doe@flat4u.no
Selected items
IO
Inge Os
inge.os@oracle.com
Remove
Select

Select a role - Microsoft Azure

https://portal.azure.com/#view/Microsoft_AAD_IAM/AddAssignmentBlade/objectId/0adad631-1725-407f-9972-ce1ecb59fe42

Oracle favorites folder | Oracle Applications | Cloud Sign In | Home | Oracle Clou...

Microsoft Azure

Search resources, services, and docs (G+/)

@oracle.com
DEFAULT DIRECTORY

Home > Default Directory | Enterprise applications > Enterprise applications | All applications > ios3db19c | Users and groups >

Add Assignment

Default Directory

Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

Users

1 user selected.

Select a role *

None Selected

Assign

Select a role

Only a single role can be selected

Enter role name to filter items...

dba_role

dbusers

Selected Role

dba_role

Select

ios3db19c | Users and groups

Enterprise Application

Overview
Deployment Plan
Diagnose and solve problems

Manage

Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Custom security attributes (preview)

Security

Conditional Access
Permissions
Token encryption

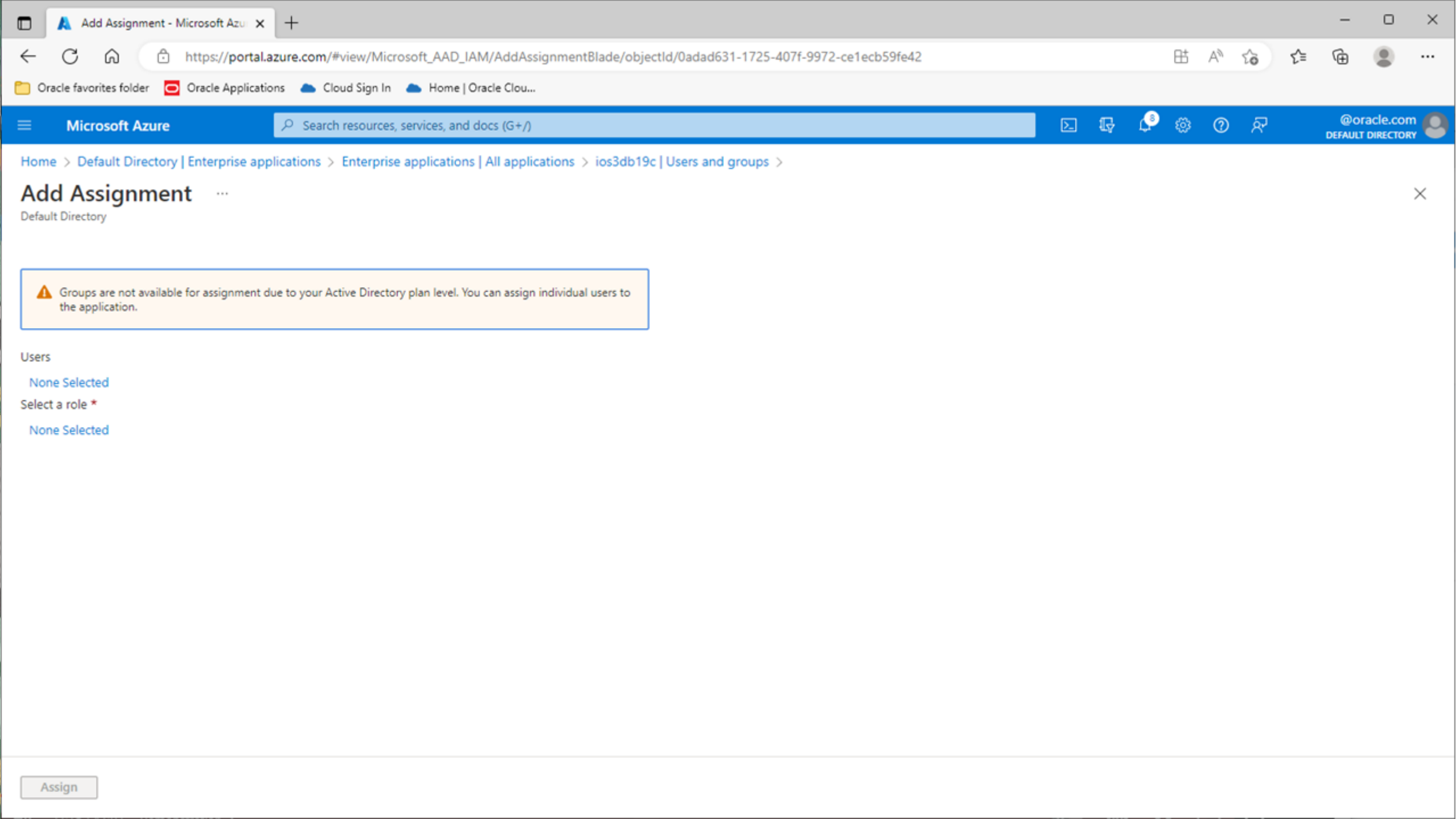
Add user/group | Edit assignment | Remove | Update credentials | Columns | Got feedback?

The application will not appear for assigned users within My Apps. Set 'visible to users?' to yes in properties to enable this. →

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration.

First 200 shown, to search all users & gro...

Display Name	Object Type	Role assigned
IO Inge Os	User	dba_role


Add Assignment - Microsoft Azu
https://portal.azure.com/#view/Microsoft_AAD_IAM/AddAssignmentBlade/objectId/0adad631-1725-407f-9972-ce1ecb59fe42
Oracle favorites folder
Oracle Applications
Cloud Sign In
Home | Oracle Clou...
Microsoft Azure
Search resources, services, and docs (G+/)
@oracle.com
DEFAULT DIRECTORY
Home > Default Directory | Enterprise applications > Enterprise applications | All applications > ios3db19c | Users and groups >
Add Assignment
Default Directory
Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.
Users
None Selected
Select a role *
None Selected
Assign

Select a role - Microsoft Azure

https://portal.azure.com/#view/Microsoft_AAD_IAM/AddAssignmentBlade/objectId/0adad631-1725-407f-9972-ce1ecb59fe42

Oracle favorites folder | Oracle Applications | Cloud Sign In | Home | Oracle Clou...

Microsoft Azure

Search resources, services, and docs (G+/)

@oracle.com
DEFAULT DIRECTORY

Home > Default Directory | Enterprise applications > Enterprise applications | All applications > ios3db19c | Users and groups >

Add Assignment

Default Directory

Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

Users

1 user selected.

Select a role *

None Selected

Assign

Select a role

Only a single role can be selected

Enter role name to filter items...

dba_role

dbusers

Selected Role

dbusers

Select

ios3db19c - Microsoft Azure

https://portal.azure.com/#view/Microsoft_AAD_IAM/ManagedAppMenuBlade/~/Users/objectId/0adad631-1725-407f-9972-ce1ecb59fe42/appId/98652ad5-06a6-49...

Oracle favorites folder | Oracle Applications | Cloud Sign In | Home | Oracle Clou...

Microsoft Azure | Search resources, services, and docs (G+/) | @oracle.com DEFAULT DIRECTORY

Home > Default Directory | Enterprise applications > Enterprise applications | All applications > ios3db19c

ios3db19c | Users and groups

Enterprise Application

Application assignment succeeded
1 user & 0 groups have been assigned access

Add user/group | Edit assignment | Remove | Update credentials | Columns | Got feedback?

The application will not appear for assigned users within My Apps. Set 'visible to users?' to yes in properties to enable this. →

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration.

First 200 shown, to search all users & gro...

Display Name	Object Type	Role assigned
IO Inge Os	User	dba_role
IO Inge Os	User	dbusers

Configure a database for AzureAD Authorization

Configuration of a Database

- Configure TLS communication between the client and the server for oracle.net. (this is not in the scope of this presentation)
- Enable azureAD as identity provider
- Create global user
- Create global role

Create global user and global role

```
create user AZADUSER identified globally as 'AZURE_ROLE=dbusers';
create role azuread_dba identified globally as 'AZURE_ROLE=dba_role';
grant create session to AZADUSER;
grant pdb_dba to azuread_dba;
```

Enable azureAD as identity provider

```
ALTER SYSTEM SET IDENTITY_PROVIDER_TYPE=AZURE_AD SCOPE=BOTH;
ALTER SYSTEM SET IDENTITY_PROVIDER_CONFIG =
'{
   "application_id_uri" :"https://demooracle.onmicrosoft.com/1111122222-
2222-5703-8b12-3a029130b25c"  ,
   "tenant_id" : "8ce0a0e-1111-2222-8888-abababcdcdcd",
}' SCOPE=BOTH;
```

Configure Automous for AzureAD Authorization

Enable azureAD as identity provider

```
BEGIN
  DBMS_CLOUD_ADMIN.ENABLE_EXTERNAL_AUTHENTICATION(
      type   =>'AZURE_AD',
      params => JSON_OBJECT('tenant_id' VALUE
                            '1111122222-2222-5703-8b12-3a029130b25c "',
                            'application_id' VALUE
                            'e678f513-cc47-449b-9ea5-dda54a7e912a',
                            'application_id_uri' VALUE
                            'https://demooracle.onmicrosoft.com/ 1111122222-
2222-5703-8b12-3a029130b25c '),
      force => TRUE
  );
END;
```

Create global user and global role

```
create user AZADUSER identified globally as 'AZURE_ROLE=dbusers';
create role azuread_dba identified globally as 'AZURE_ROLE=dba_role';
grant create session to AZADUSER;
grant pdb_dba to azuread_dba;
```

Configure tnsnames.ora

Sample TNS entry for the connection

```
atp_tp_adaz =
(description=
   (retry_count=20)(retry_delay=3)
   (address=(protocol=tcps)(port=1522)(host=adb.eu-frankfurt-1.oraclecloud.com))
   (connect_data=
      (service_name=xxyyzzdemoservice_atp_tp.atp.oraclecloud.com))
      (security=(ssl_server_cert_dn="CN=adwc.eucom-central-1.oraclecloud.com,
            OU=Oracle BMCS FRANKFURT, O=Oracle Corporation, L=Redwood City,
            ST=California, C=US")
      (TOKEN_AUTH=OAUTH)
      (TOKEN_LOCATION="/home/oracle/azad/azadtoken.jwt")
   )
)
```

This is the file where the generated token will be stored

Simple Python example, generates tokencode

Token generation sample app based on msal Python SDK

https://msal-python.readthedocs.io/en/latest/

```
# pip install msal
# Python 3.x
#
#  (c) Inge Os, Oracle Norway 3/2-2023
#
from msal import PublicClientApplication
import sys
import os
import json
import platform

# Default values
client_id = None
tenant_id = None
scopes = None

#
# Retrieve CMD line arguments
#
if platform.system().lower() == 'linux':
    configFile="/home/oracle/azuread-demo/config.json"
else:
    configFile="azadconfig.json«
# Load configuration
#
with open(args.configfile) as f:
    configText = f.read()
try:
    cfg=json.loads(configText)
except (Exception, ValueError) as ex:
    print('invalid configuration in configfile: ' + str(ex))
    exit(1)
```

```
app = PublicClientApplication(
    client_id = client_id,
    authority = "https://login.microsoftonline.com/" +tenant_id
)

acquire_tokens_result = app.acquire_token_interactive(
    scopes = scopes
)

if 'error' in acquire_tokens_result:
    print("Error: " + acquire_tokens_result['error'])
    print("Description: " +
acquire_tokens_result['error_description'])
else:
    print("Access token:\n")
    print(acquire_tokens_result['access_token'])
    with open(args.tokenfile+'.jwt', 'w') as f:
        f.write(acquire_tokens_result['access_token'])
    print("\nRefresh token:\n")
    print(acquire_tokens_result['refresh_token'])
    with open(args.tokenfile+'.rjwt', 'w') as f:
        f.write(acquire_tokens_result['refresh_token'])
```

Token generation

```
(base) G:\demo_projects\cloud_labs\azuread_19c>python getazadtokenV3.py
Access token:

eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNROW5OUjdiUm9meG1lW
…
-o807nJEWtNEkIwPXTSdmy4lSv_cg_18DQZQZ6Grys0AsdG2xX9lFPNnjA

Refresh token:

0.AXMADvCtm5q4CkmXG73faHz-uRP1eOZHzJtEnqXdpUp-kSpzADk.AgABAAEAAAD—
…
pslJGWiV1nibOSc5EFTaqMDYoZHEpWqFbZMz8eCk_94K3lwL8kXGDylqrQofxJDxfDCGKkFx-B8a1YOBfrA
```

Upload the generated token to the tokenfile pointed at in the tnsnames.ora file

Sample SQL script

```
cat rundemo.sql
connect /@iosp_tp_azad
set feedback off
set heading off
prompt logged on user
select user from dual;
prompt
prompt sys_context('userenv','CURRENT_USER')
pause press any key
 select sys_context('userenv','CURRENT_USER') from dual;
prompt
prompt sys_context('userenv','AUTHENTICATED_IDENTITY')
pause press any key
 select sys_context('userenv','AUTHENTICATED_IDENTITY') from dual;
prompt
prompt sys_context('userenv','ENTERPRISE_IDENTITY')
pause press any key
prompt
 select sys_context('userenv','ENTERPRISE_IDENTITY') from dual;
prompt
```


Run of test script

```
SQL> @rundemo
Connected.
logged on user

AZADUSER

sys_context('userenv','CURRENT_USER')
press any key


AZADUSER

sys_context('userenv','AUTHENTICATED_IDENTITY')
press any key


live.com#somebody@oracle.com

sys_context('userenv','ENTERPRISE_IDENTITY')
press any key



e678f513-cc47-449b-9ea5-dda54a7e912a
```


References

https://blogs.oracle.com/cloudsecurity/post/azure-active-directory-can-authenticate-database-users
https://www.youtube.com/watch?v=GkrulRzlNYI

https://msal-python.readthedocs.io/en/latest/