Custom claims in AzureAD to adjust unique name id

IDCS Federation

Inge Os

Master Principal Cloud Specialist

Updated 30/12-2021

The challenge, Azure AD as IdP, IDCS as SP, with different mail domains

When federation from Azure, the unique nameid is with the domain name of Azure Domain you federate from, and the AzureAD domainname does not always match the unique name in IDCS

AzureAD principal username is matched to IDCS username

The solution is to create a custom claim that strips off the domain name from the username that is mapped to IDCS username

A claim can be conditional, ie. Linked to group membership

Example, Azure AD users and groups

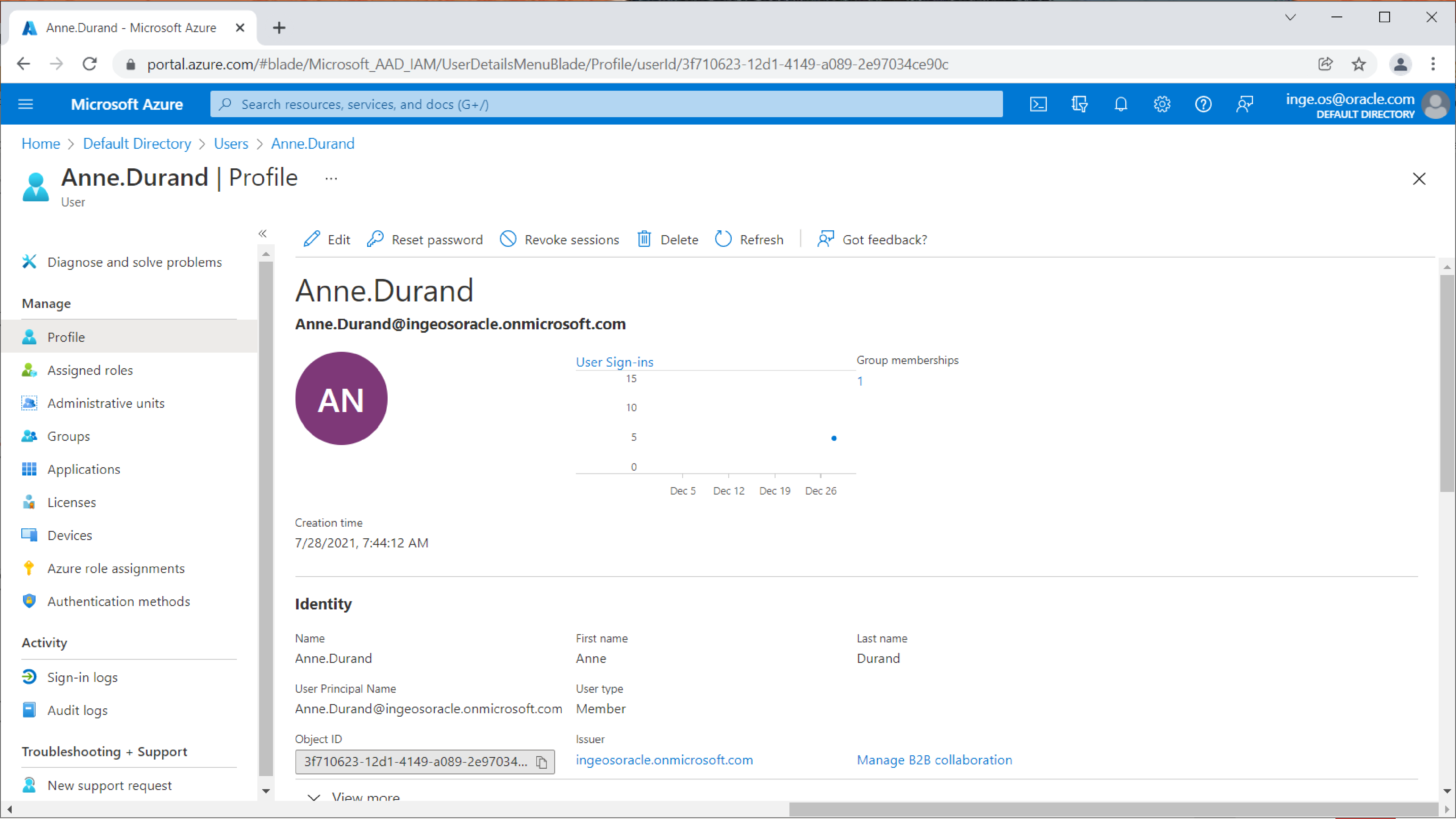
Azure AD Name	Azure AD User Prinipal name	Azure AD Group membership
Anne Durand	Anne.Durand@ingeosoracle.onmicrosoft.com	ebsuser
Casey Brown	casey.brown@ingeosoracle.onmicrosoft.com	ebsuser
Dart Vader	Dvader@ingeosoracle.onmicrosoft.com	ociuser

Example, IDCS users

IDCS Display Name	IDCS User name	IDCS Mailid
Anne Durand	anne.durand	anne.durand@gmail.com
Casey Brown	casey.brown	casey.brown@gmail.com
Dart Vader	Dvader@ingeosoracle.onmicrosoft.com	inge.os@oracle.com

In IDCS username does not need to be the same as mail address

Azure AD users and groups



Anne.Durand

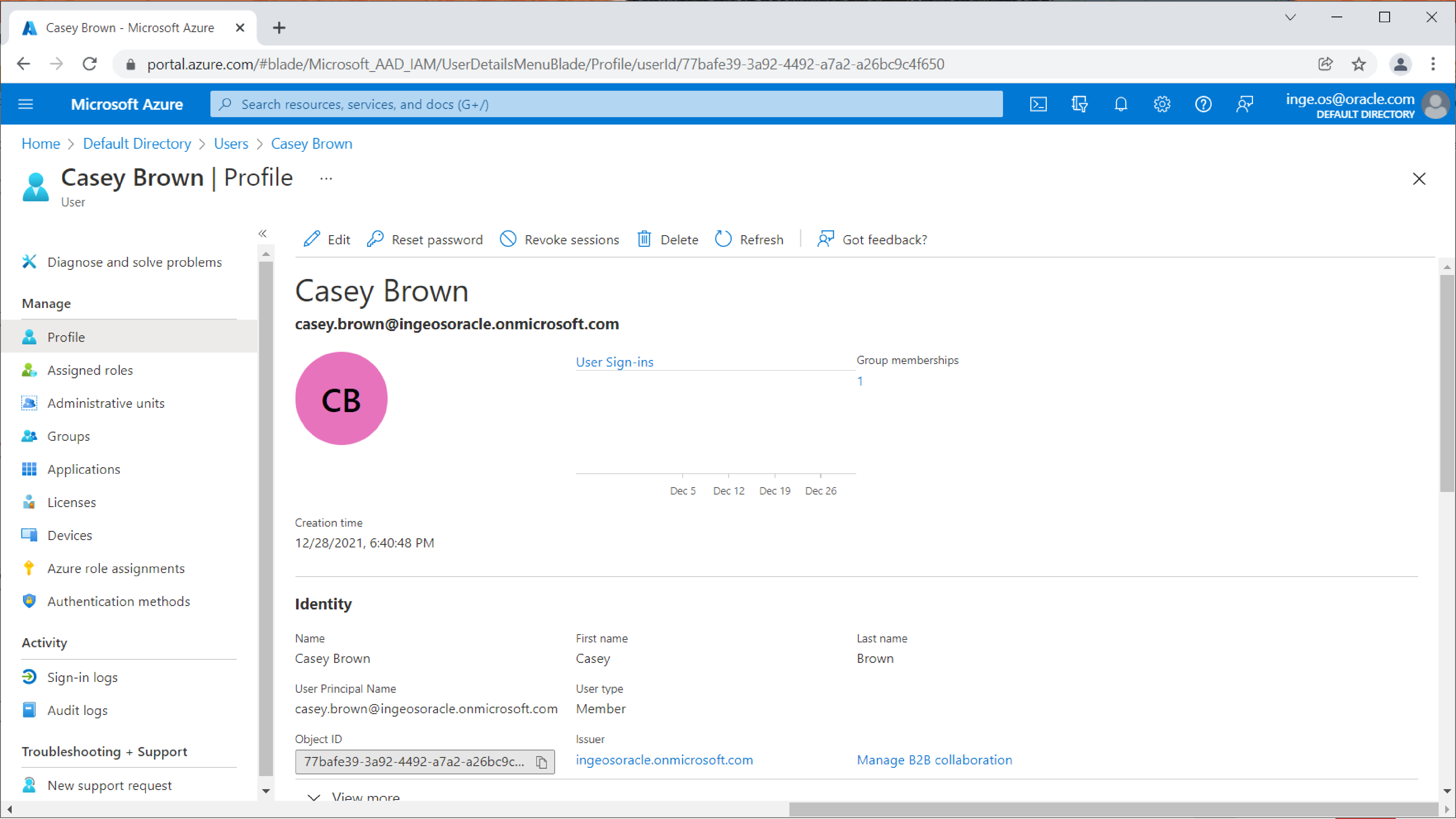
Anne.Durand@ingeosoracle.onmicrosoft.com

Group memberships
1

Creation time
7/28/2021, 7:44:12 AM

Identity

Name Anne.Durand	First name Anne	Last name Durand
User Principal Name Anne.Durand@ingeosoracle.onmicrosoft.com	User type Member	
Object ID 3f710623-12d1-4149-a089-2e97034...	Issuer ingeosoracle.onmicrosoft.com	Manage B2B collaboration



Casey Brown | Profile

User

Casey Brown

casey.brown@ingeosoracle.onmicrosoft.com

User Sign-ins

Group memberships
1

Creation time
12/28/2021, 6:40:48 PM

Identity

Name	First name	Last name
Casey Brown	Casey	Brown

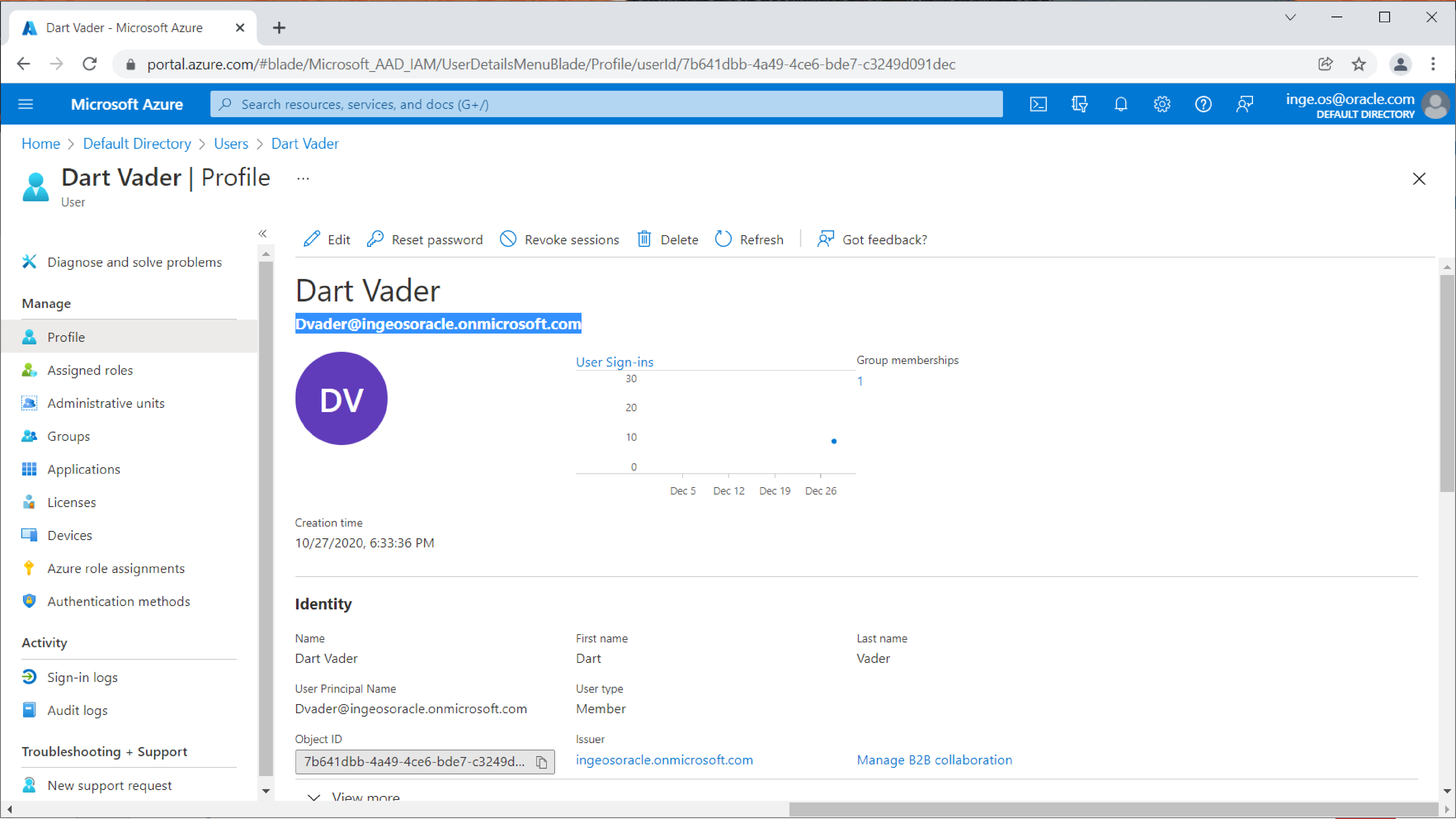
User Principal Name
casey.brown@ingeosoracle.onmicrosoft.com

User type
Member

Object ID
77bafe39-3a92-4492-a7a2-a26bc9c...

Issuer
ingeosoracle.onmicrosoft.com

Manage B2B collaboration



Dart Vader

Dvader@ingeosoracle.onmicrosoft.com

Group memberships
1

Creation time
10/27/2020, 6:33:36 PM

Identity

Name
Dart Vader

First name
Dart

Last name
Vader

User Principal Name
Dvader@ingeosoracle.onmicrosoft.com

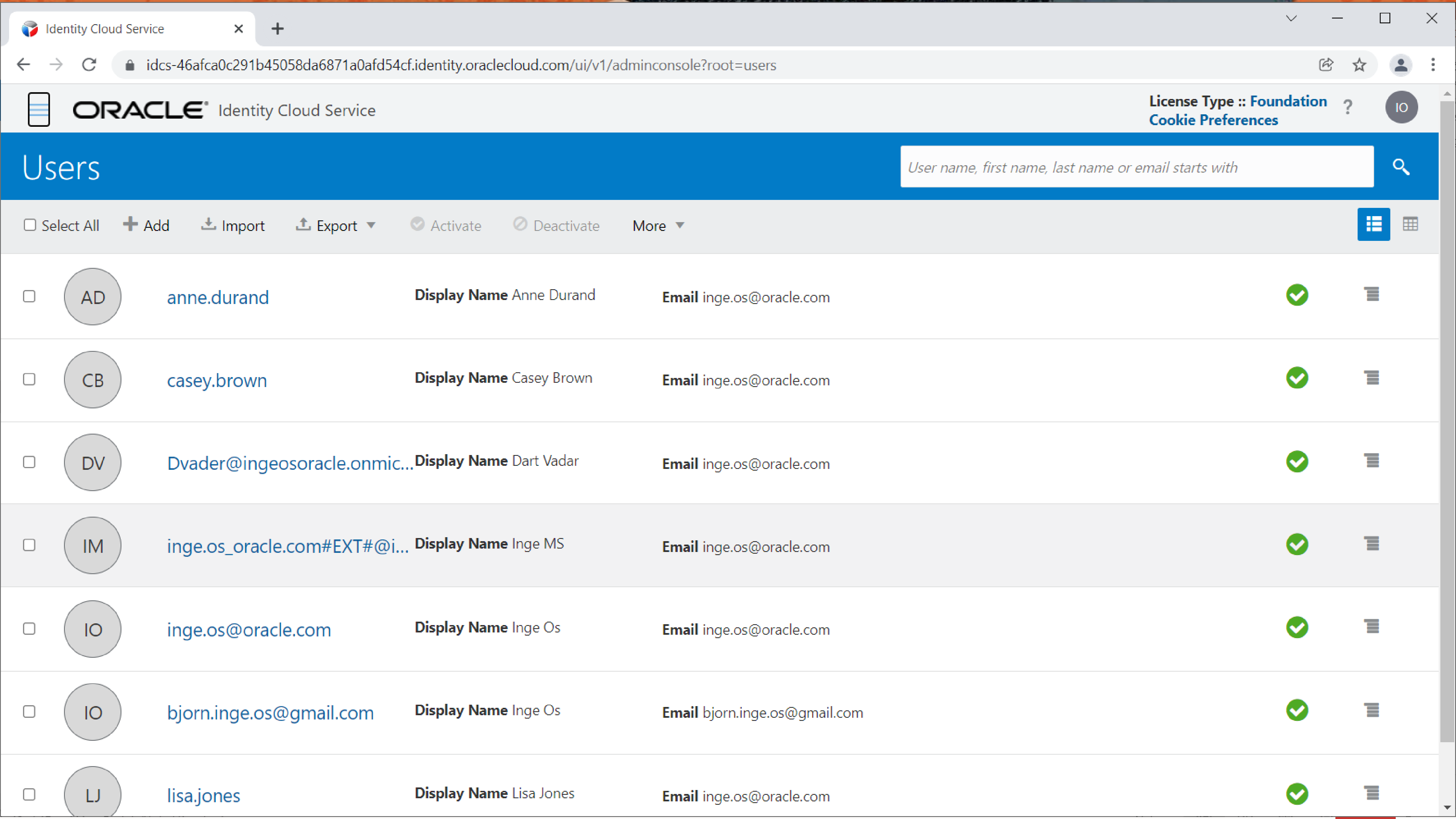
User type
Member

Object ID
7b641dbb-4a49-4ce6-bde7-c3249d...

Issuer
ingeosoracle.onmicrosoft.com

Manage B2B collaboration

IDCS users



Identity Cloud Service
idcs-46afca0c291b45058da6871a0afd54cf.identity.oraclecloud.com/ui/v1/adminconsole?root=users
ORACLE Identity Cloud Service
License Type :: Foundation
Cookie Preferences
?
IO
User name, first name, last name or email starts with
□ Select All
Add
Import
Export
Activate
Deactivate
More

Users

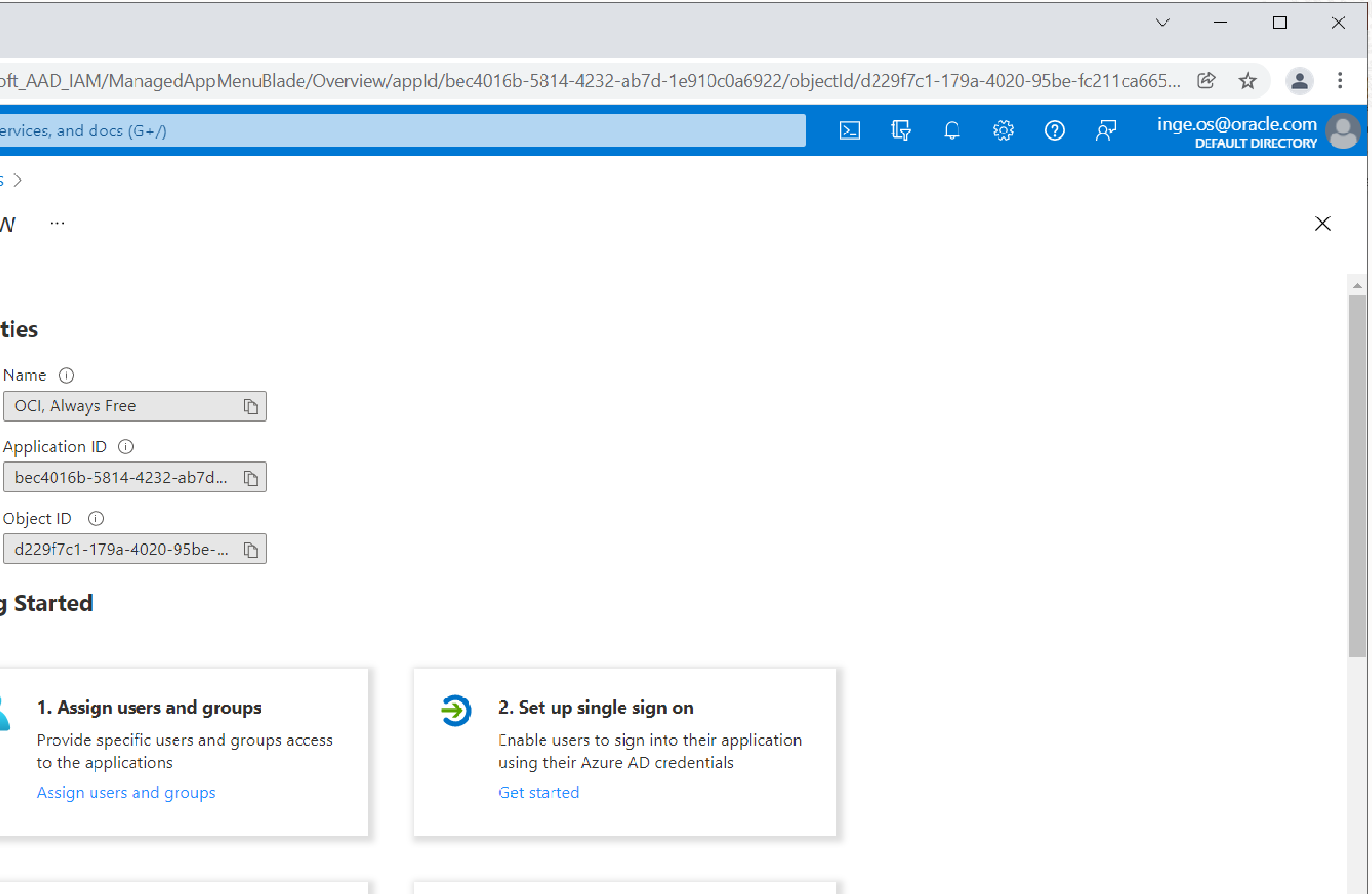
□	AD	anne.durand	**Display Name** Anne Durand	**Email** inge.os@oracle.com
□	CB	casey.brown	**Display Name** Casey Brown	**Email** inge.os@oracle.com
□	DV	Dvader@ingeosoracle.onmic...	**Display Name** Dart Vadar	**Email** inge.os@oracle.com
□	IM	inge.os_oracle.com#EXT#@i...	**Display Name** Inge MS	**Email** inge.os@oracle.com
□	IO	inge.os@oracle.com	**Display Name** Inge Os	**Email** inge.os@oracle.com
□	IO	bjorn.inge.os@gmail.com	**Display Name** Inge Os	**Email** bjorn.inge.os@gmail.com
□	LJ	lisa.jones	**Display Name** Lisa Jones	**Email** inge.os@oracle.com

Azure AD Claim for federation

Members of group ebsusers, mail domain is stripped off

Members of ociusers keeps mail domain

Only members of thse two groups federates successfully



oft_AAD_IAM/ManagedAppMenuBlade/Overview/appId/bec4016b-5814-4232-ab7d-1e910c0a6922/objectId/d229f7c1-179a-4020-95be-fc211ca665...

inge.os@oracle.com
DEFAULT DIRECTORY

W ···

ties

Name
OCI, Always Free

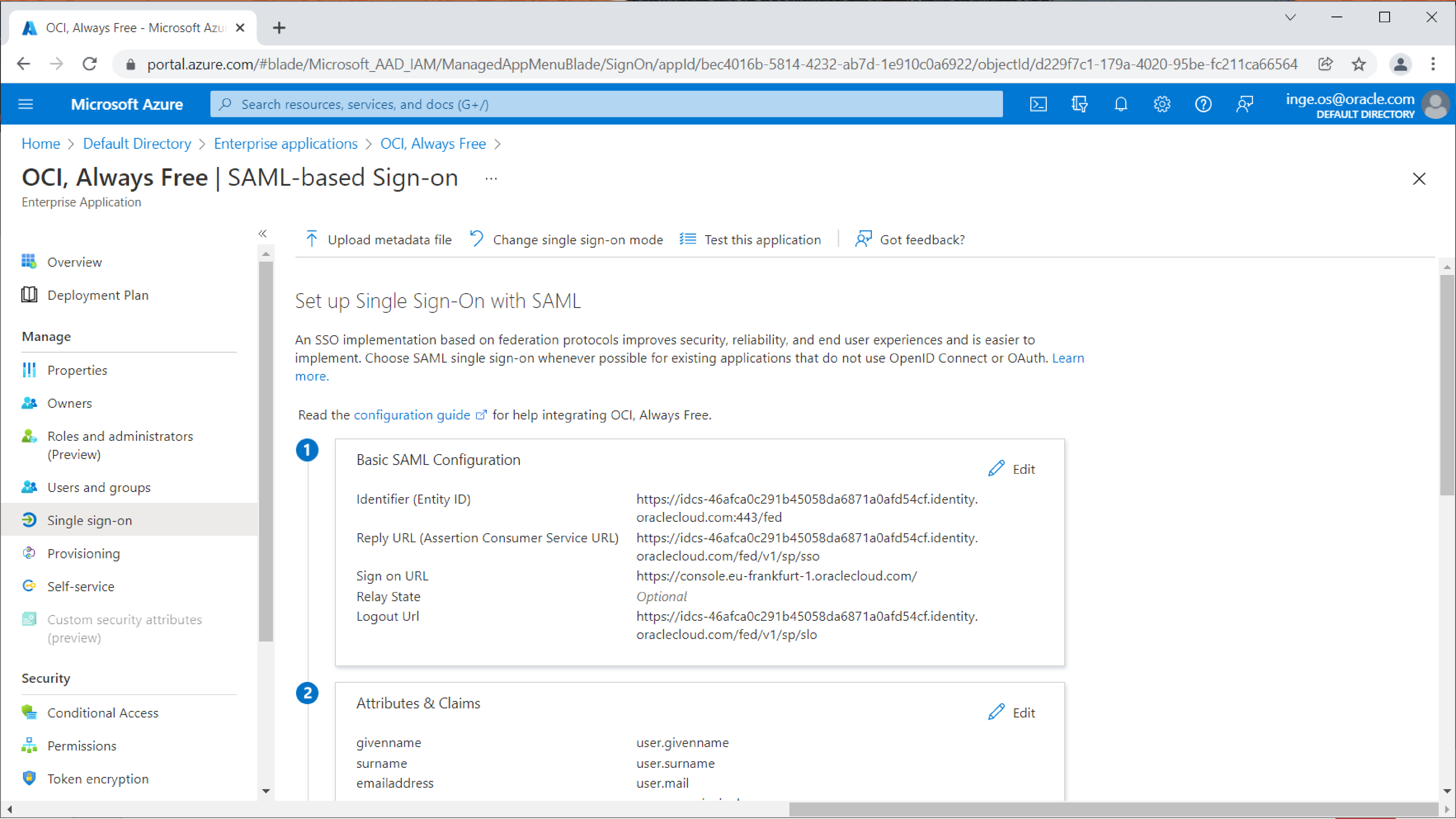
Application ID
bec4016b-5814-4232-ab7d...

Object ID
d229f7c1-179a-4020-95be-...

g Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started



OCI, Always Free - Microsoft Azu
portal.azure.com/#blade/Microsoft_AAD_IAM/ManagedAppMenuBlade/SignOn/appId/bec4016b-5814-4232-ab7d-1e910c0a6922/objectId/d229f7c1-179a-4020-95be-fc211ca66564
Microsoft Azure
Search resources, services, and docs (G+/)
inge.os@oracle.com
DEFAULT DIRECTORY
Home > Default Directory > Enterprise applications > OCI, Always Free >

OCI, Always Free | SAML-based Sign-on

Enterprise Application

Overview
Deployment Plan
Manage
Properties
Owners
Roles and administrators (Preview)
Users and groups
Single sign-on
Provisioning
Self-service
Custom security attributes (preview)
Security
Conditional Access
Permissions
Token encryption
Upload metadata file
Change single sign-on mode
Test this application
Got feedback?

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

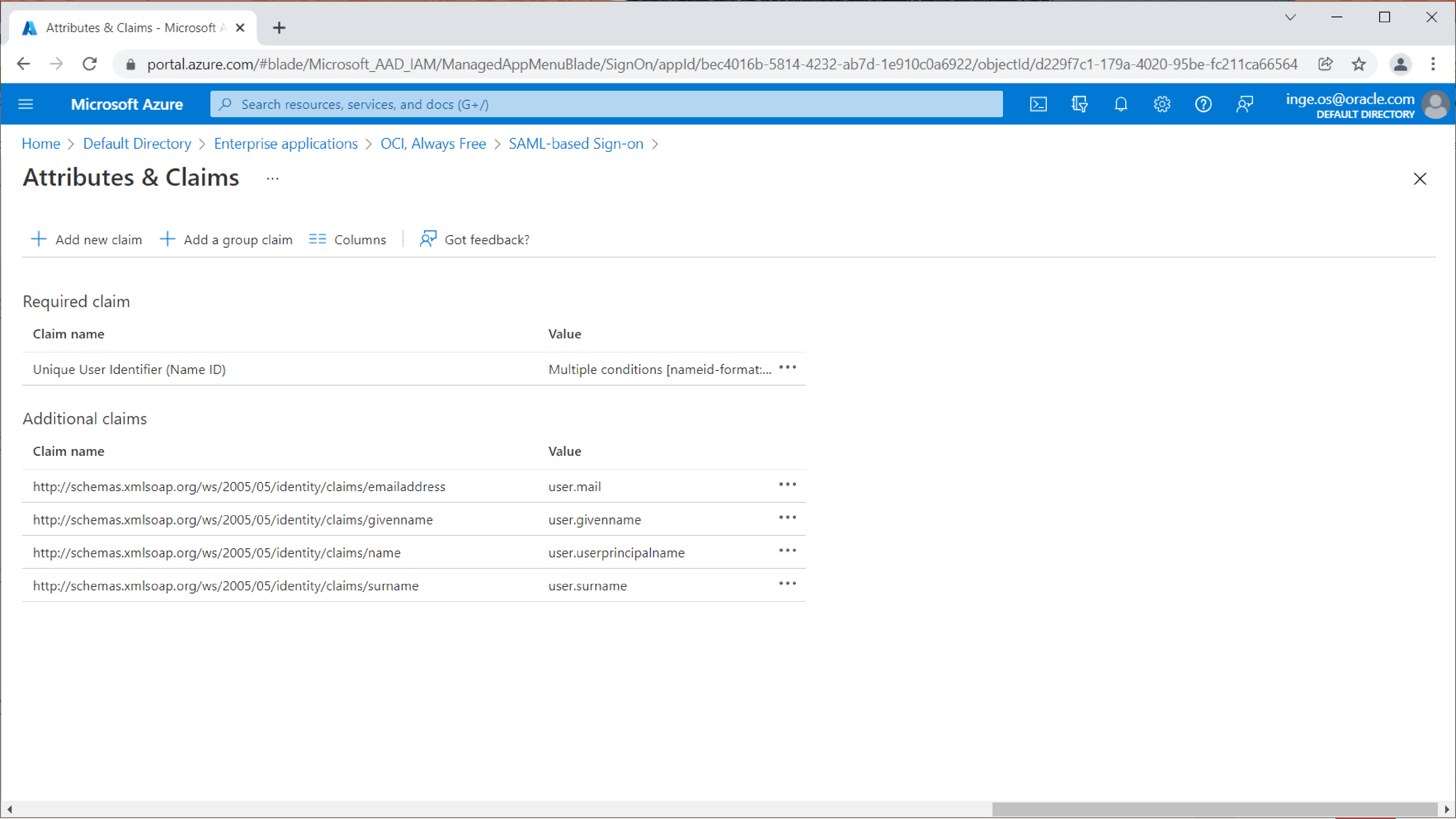
Read the configuration guide for help integrating OCI, Always Free.

1 Basic SAML Configuration — Edit

Identifier (Entity ID)	https://idcs-46afca0c291b45058da6871a0afd54cf.identity.oraclecloud.com:443/fed
Reply URL (Assertion Consumer Service URL)	https://idcs-46afca0c291b45058da6871a0afd54cf.identity.oraclecloud.com/fed/v1/sp/sso
Sign on URL	https://console.eu-frankfurt-1.oraclecloud.com/
Relay State	*Optional*
Logout Url	https://idcs-46afca0c291b45058da6871a0afd54cf.identity.oraclecloud.com/fed/v1/sp/slo

2 Attributes & Claims — Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail


Attributes & Claims - Microsoft A
portal.azure.com/#blade/Microsoft_AAD_IAM/ManagedAppMenuBlade/SignOn/appId/bec4016b-5814-4232-ab7d-1e910c0a6922/objectId/d229f7c1-179a-4020-95be-fc211ca66564
Microsoft Azure
Search resources, services, and docs (G+/)
inge.os@oracle.com
DEFAULT DIRECTORY
Home > Default Directory > Enterprise applications > OCI, Always Free > SAML-based Sign-on >
Add new claim
Add a group claim
Columns
Got feedback?

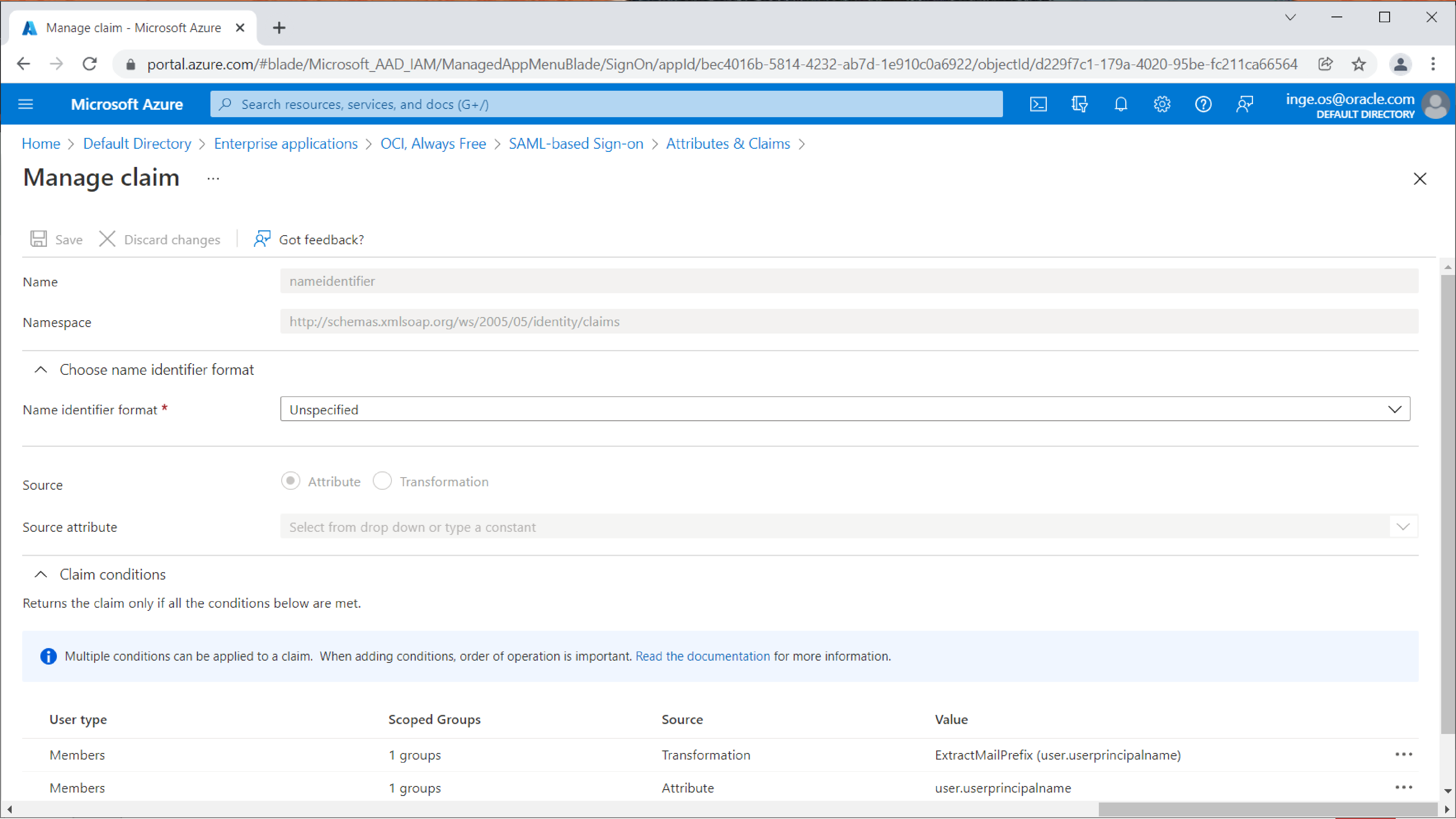
Attributes & Claims

Required claim

Claim name	Value
Unique User Identifier (Name ID)	Multiple conditions [nameid-format:...

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname


Manage claim - Microsoft Azure
portal.azure.com/#blade/Microsoft_AAD_IAM/ManagedAppMenuBlade/SignOn/appId/bec4016b-5814-4232-ab7d-1e910c0a6922/objectId/d229f7c1-179a-4020-95be-fc211ca66564
Microsoft Azure
Search resources, services, and docs (G+/)
inge.os@oracle.com
DEFAULT DIRECTORY
Home > Default Directory > Enterprise applications > OCI, Always Free > SAML-based Sign-on > Attributes & Claims >
Save
Discard changes
Got feedback?

Manage claim ...

Name	nameidentifier
Namespace	http://schemas.xmlsoap.org/ws/2005/05/identity/claims

^ Choose name identifier format

Name identifier format *	Unspecified
Source	● Attribute ○ Transformation
Source attribute	Select from drop down or type a constant

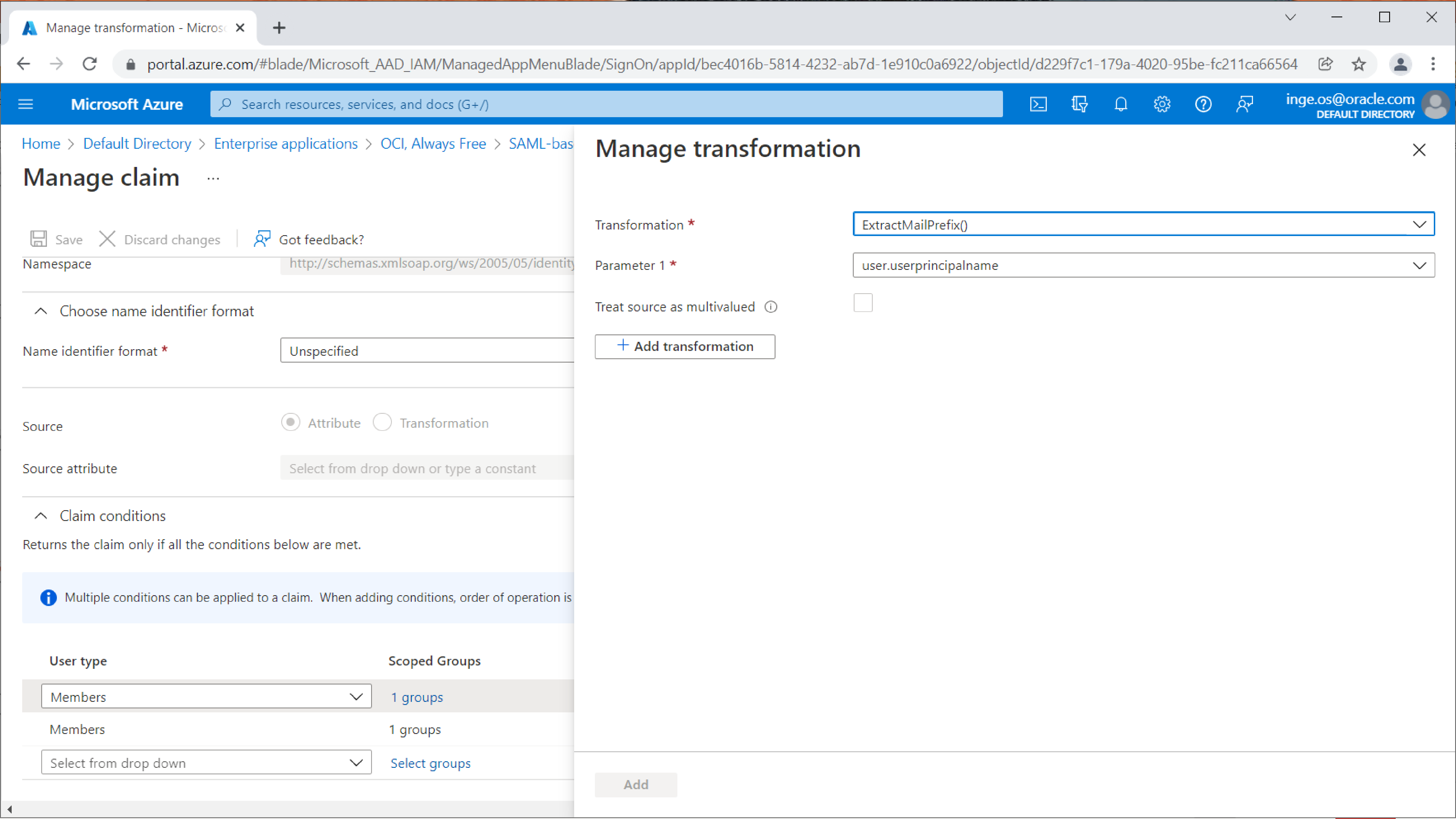
^ Claim conditions

Returns the claim only if all the conditions below are met.

Multiple conditions can be applied to a claim. When adding conditions, order of operation is important. Read the documentation for more information.

User type	Scoped Groups	Source	Value	
Members	1 groups	Transformation	ExtractMailPrefix (user.userprincipalname)	•••
Members	1 groups	Attribute	user.userprincipalname	•••

Claim for ebsusers group



Manage transformation - Micros

portal.azure.com/#blade/Microsoft_AAD_IAM/ManagedAppMenuBlade/SignOn/appId/bec4016b-5814-4232-ab7d-1e910c0a6922/objectId/d229f7c1-179a-4020-95be-fc211ca66564

Microsoft Azure

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

inge.os@oracle.com
DEFAULT DIRECTORY

Home > Default Directory > Enterprise applications > OCI, Always Free > SAML-bas

Manage claim ...

Save | Discard changes | Got feedback?

Namespace: http://schemas.xmlsoap.org/ws/2005/05/identity

Choose name identifier format

Name identifier format *: Unspecified

Source: ● Attribute ○ Transformation

Source attribute: Select from drop down or type a constant

Claim conditions

Returns the claim only if all the conditions below are met.

Multiple conditions can be applied to a claim. When adding conditions, order of operation is

User type	Scoped Groups
Members	1 groups
Members	1 groups
Select from drop down	Select groups

Manage transformation

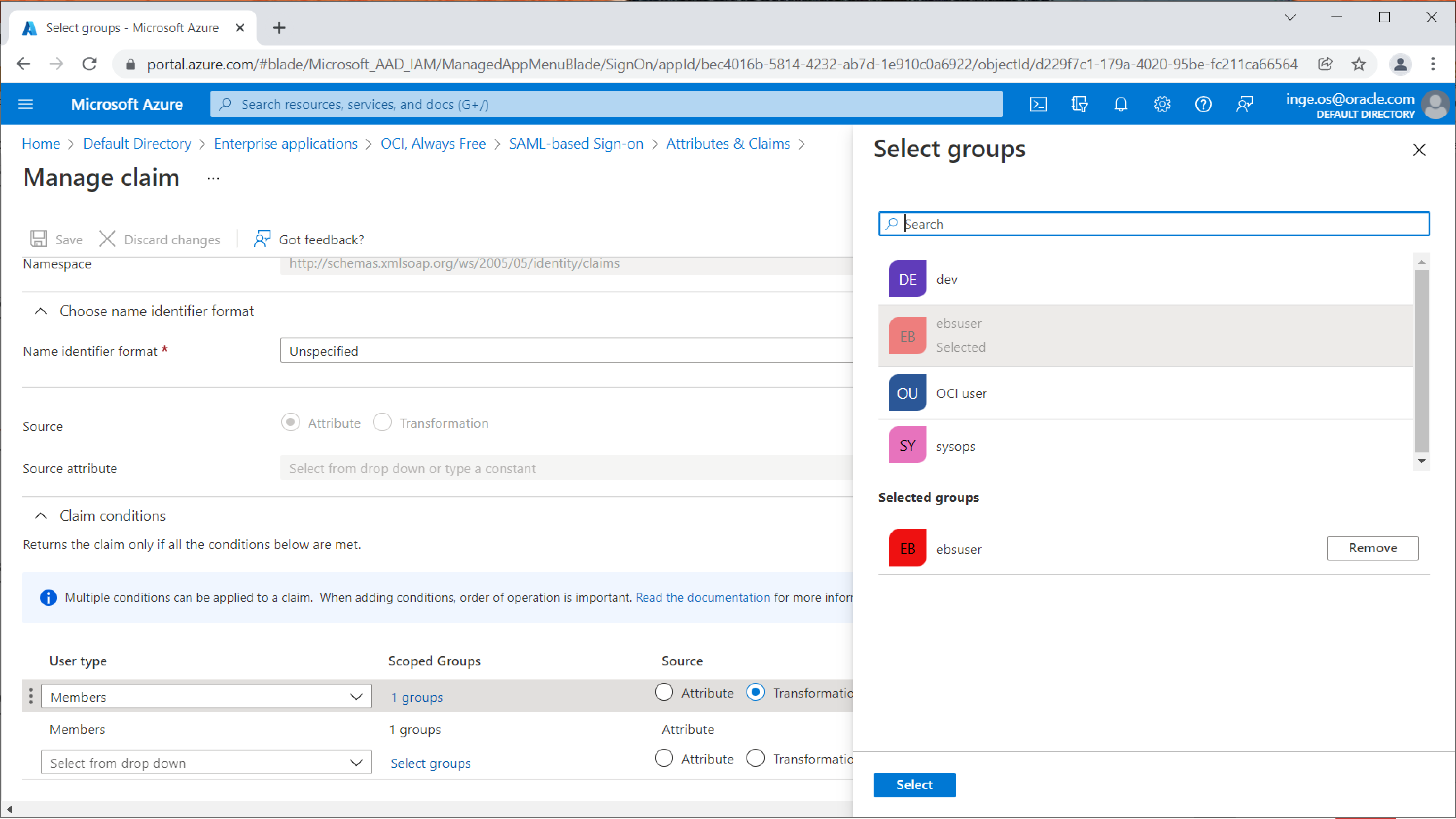
Transformation *: ExtractMailPrefix()

Parameter 1 *: user.userprincipalname

Treat source as multivalued ⓘ □

+ Add transformation

Add


Select groups - Microsoft Azure
portal.azure.com/#blade/Microsoft_AAD_IAM/ManagedAppMenuBlade/SignOn/appId/bec4016b-5814-4232-ab7d-1e910c0a6922/objectId/d229f7c1-179a-4020-95be-fc211ca66564
Microsoft Azure
Search resources, services, and docs (G+/)
inge.os@oracle.com
DEFAULT DIRECTORY
Home > Default Directory > Enterprise applications > OCI, Always Free > SAML-based Sign-on > Attributes & Claims >
Save
Discard changes
Got feedback?

Manage claim ...

Namespace: http://schemas.xmlsoap.org/ws/2005/05/identity/claims

Choose name identifier format

Name identifier format *: Unspecified

Source: ● Attribute ○ Transformation

Source attribute: Select from drop down or type a constant

Claim conditions

Returns the claim only if all the conditions below are met.

Multiple conditions can be applied to a claim. When adding conditions, order of operation is important. Read the documentation for more inform

User type	Scoped Groups	Source
Members	1 groups	○ Attribute ● Transformatio
Members	1 groups	Attribute
Select from drop down	Select groups	○ Attribute ○ Transformatio

Select groups

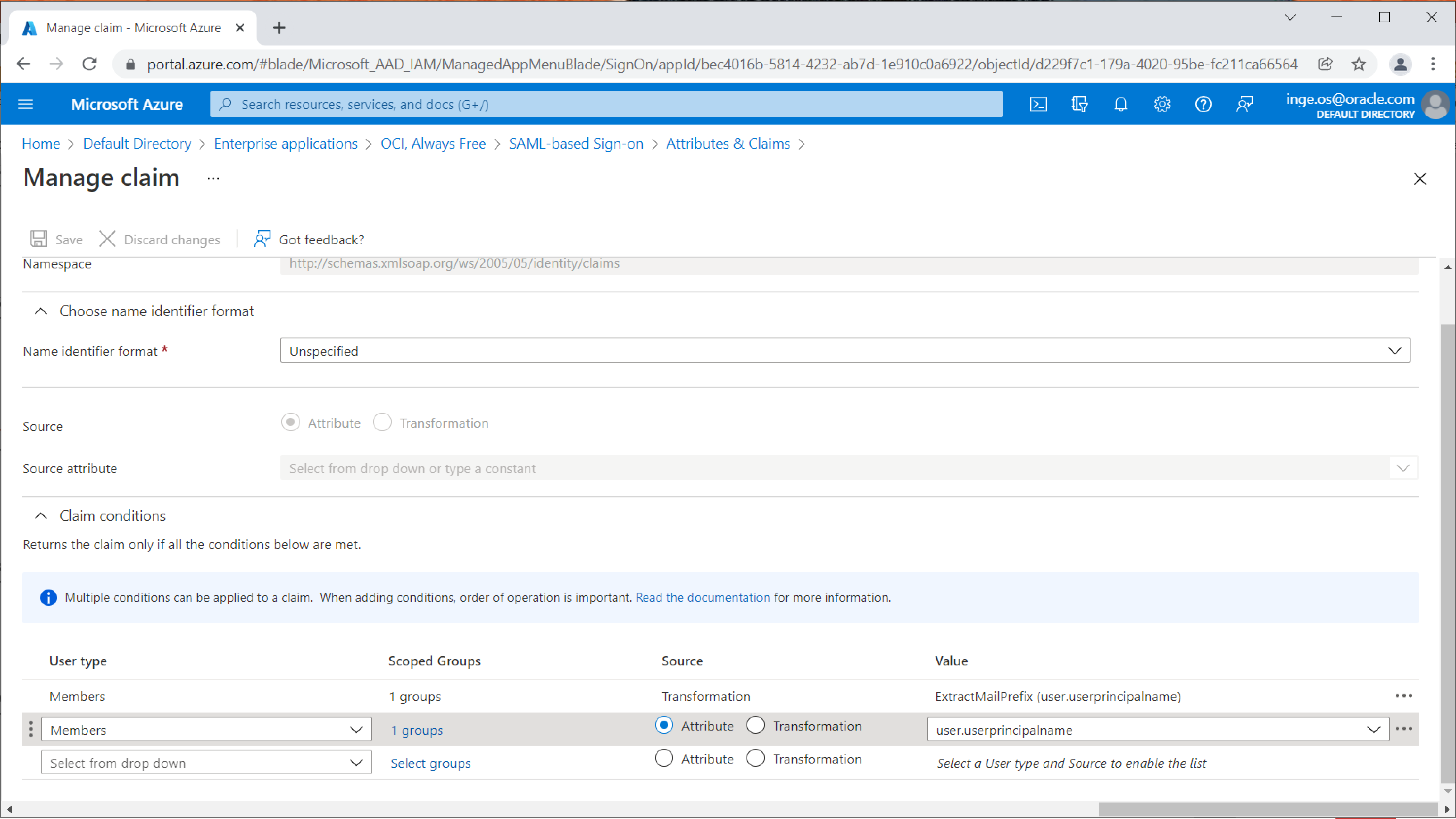
Search

DE	dev
EB	ebsuser Selected
OU	OCI user
SY	sysops

Selected groups

EB	ebsuser	Remove

Claim for ociusers gorup



Manage claim - Microsoft Azure
portal.azure.com/#blade/Microsoft_AAD_IAM/ManagedAppMenuBlade/SignOn/appId/bec4016b-5814-4232-ab7d-1e910c0a6922/objectId/d229f7c1-179a-4020-95be-fc211ca66564
Microsoft Azure
Search resources, services, and docs (G+/)
inge.os@oracle.com
DEFAULT DIRECTORY
Home > Default Directory > Enterprise applications > OCI, Always Free > SAML-based Sign-on > Attributes & Claims >
Save
Discard changes
Got feedback?

Manage claim

Namespace: http://schemas.xmlsoap.org/ws/2005/05/identity/claims

Choose name identifier format

Name identifier format *: Unspecified

Source: ● Attribute ○ Transformation

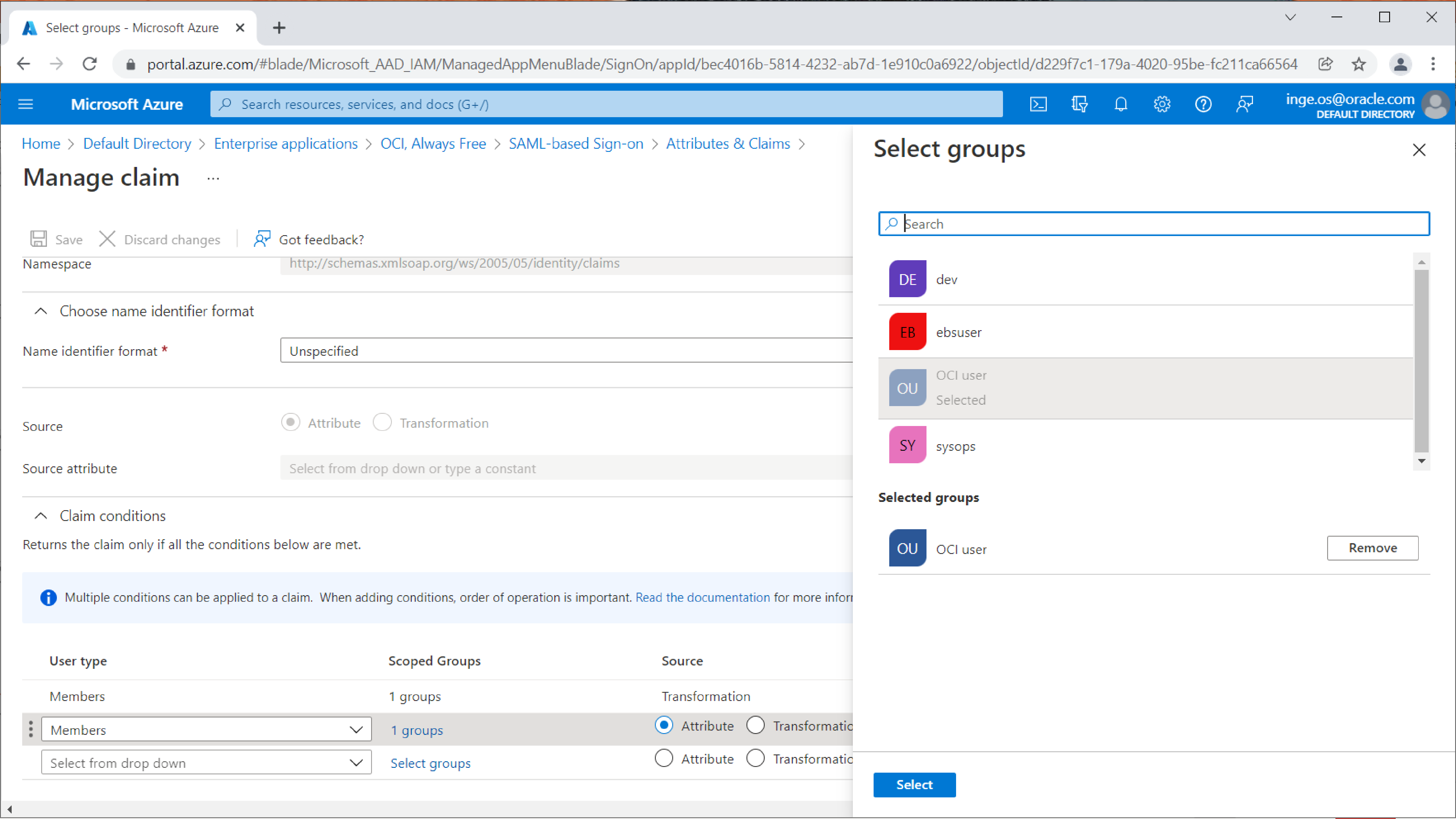
Source attribute: Select from drop down or type a constant

Claim conditions

Returns the claim only if all the conditions below are met.

Multiple conditions can be applied to a claim. When adding conditions, order of operation is important. Read the documentation for more information.

User type	Scoped Groups	Source	Value
Members	1 groups	Transformation	ExtractMailPrefix (user.userprincipalname)
Members	1 groups	● Attribute ○ Transformation	user.userprincipalname
Select from drop down	Select groups	○ Attribute ○ Transformation	*Select a User type and Source to enable the list*



portal.azure.com/#blade/Microsoft_AAD_IAM/ManagedAppMenuBlade/SignOn/appId/bec4016b-5814-4232-ab7d-1e910c0a6922/objectId/d229f7c1-179a-4020-95be-fc211ca66564

Home > Default Directory > Enterprise applications > OCI, Always Free > SAML-based Sign-on > Attributes & Claims >

Manage claim

Namespace: http://schemas.xmlsoap.org/ws/2005/05/identity/claims

Choose name identifier format

Name identifier format *: Unspecified

Source: ● Attribute ○ Transformation

Source attribute: Select from drop down or type a constant

Claim conditions

Returns the claim only if all the conditions below are met.

Multiple conditions can be applied to a claim. When adding conditions, order of operation is important. Read the documentation for more infor

User type	Scoped Groups	Source
Members	1 groups	Transformation
Members	1 groups	● Attribute ○ Transformatio
Select from drop down	Select groups	○ Attribute ○ Transformatio

Select groups

Search

- DE dev
- EB ebsuser
- OU OCI user
Selected
- SY sysops

Selected groups

OU OCI user — Remove

Documentation reference

MS AD, Claims customization reference

https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-saml-claims-customization