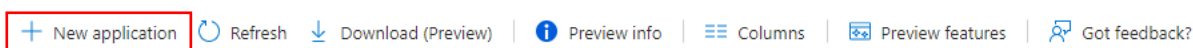


Federando Azure para IDCS

Passo 1: Criando uma aplicação para Federação na Azure

Na Azure, clique em Enterprise Applications e crie uma aplicação (+ New application)

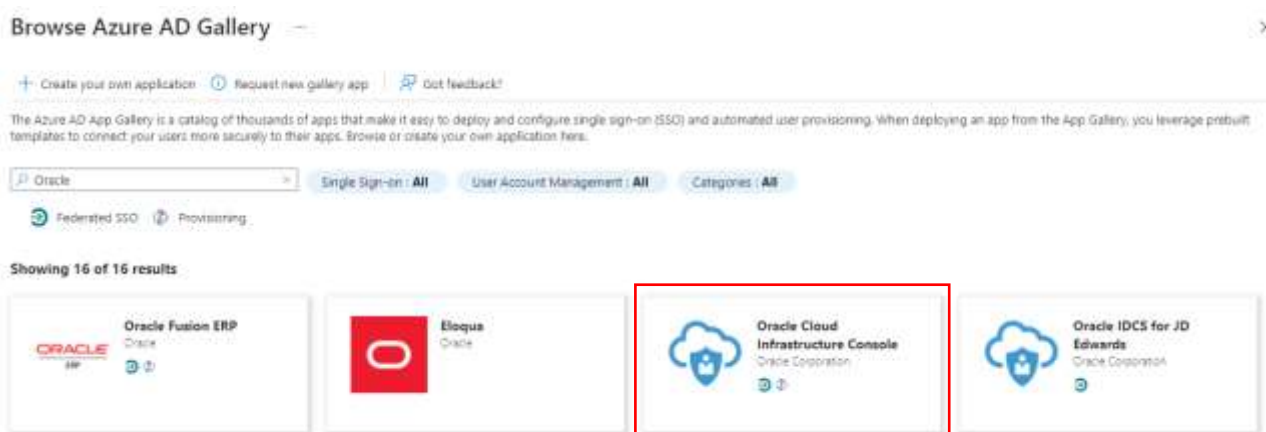


Want to switch back to the legacy Enterprise Apps search experience? Click to leave the preview. →

View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider.

Search by application name or object ID

Busque por Oracle na caixa de pesquisa e selecione **Oracle Infrastructure Console**

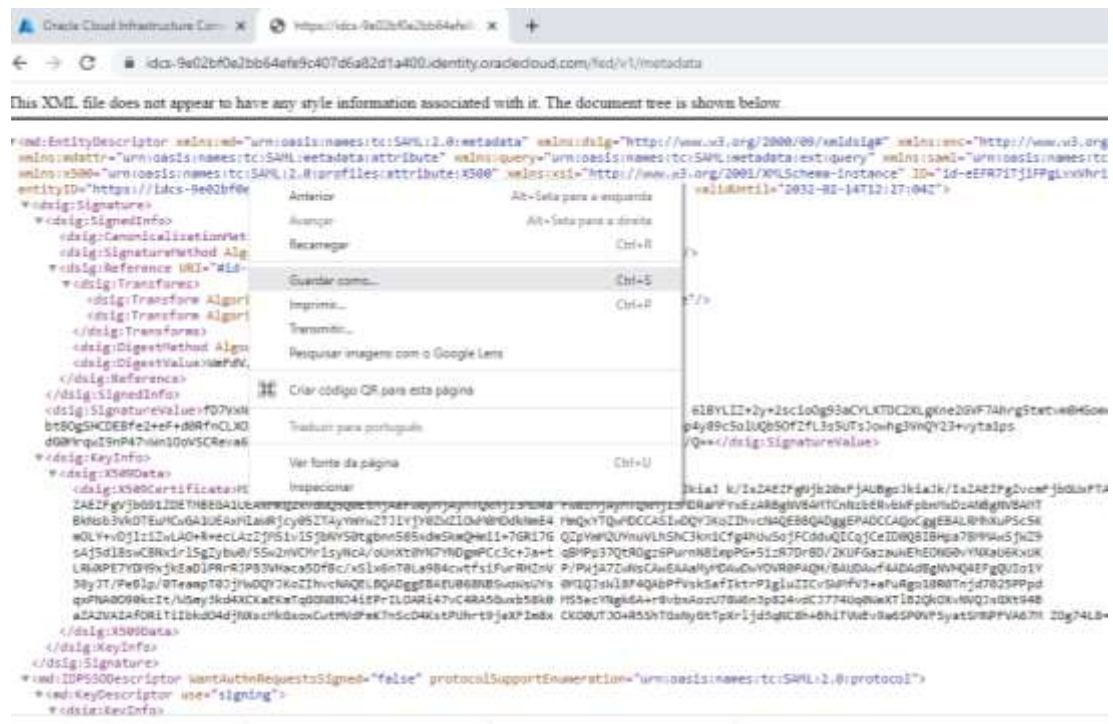


Dê um nome para aplicação e clique em Create



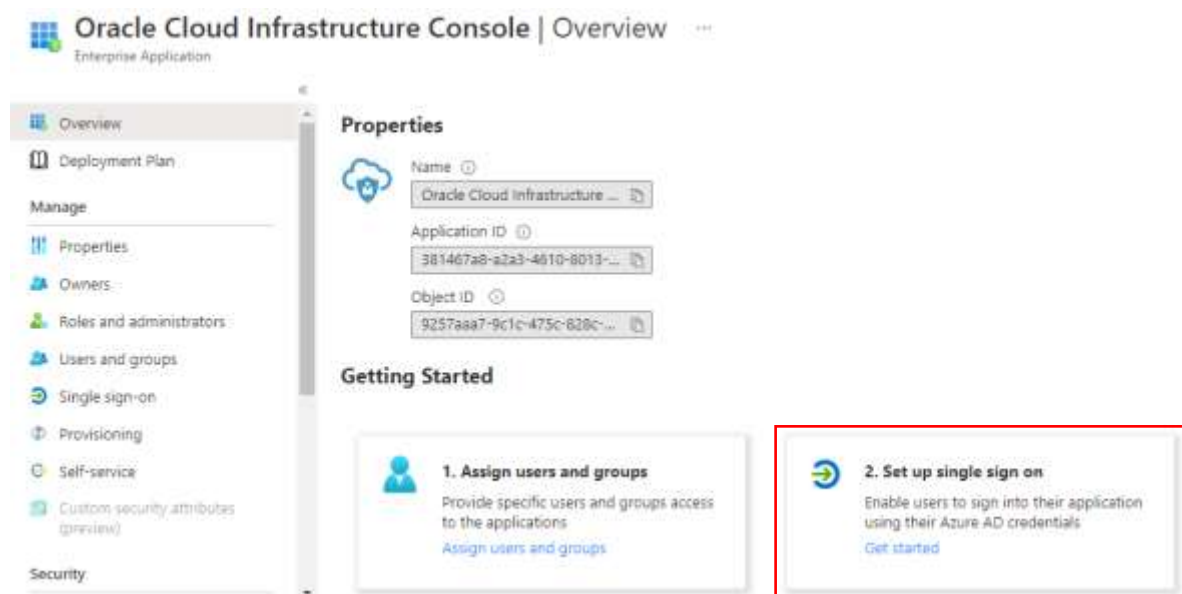
Baixe o arquivo de Metadata do seu IDCS através do link abaixo, troque os xxx pelo id do seu IDCS

<https://idcs-xxxxxxx.identity.oraclecloud.com/fed/v1/metadata>




Com a aplicação criada, iremos iniciar a configuração da autenticação via SAML.


Em Overview, selecione a opção **(2. Set up sign on)**



Depois selecione a opção **SAML**

Select a single sign-on method [Help me decide](#)

**Disabled**
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

**SAML**
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Na página do SAML-based Sign-on, faça o upload do seu arquivo de metadata do IDCS baixado anteriormente através da url do IDCS

[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 Oracle Cloud Infrastructure Console.

1 Basic SAML Configuration [Edit](#)

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Required
Relay State (Optional)	<i>Optional</i>
Logout Url (Optional)	<i>Optional</i>

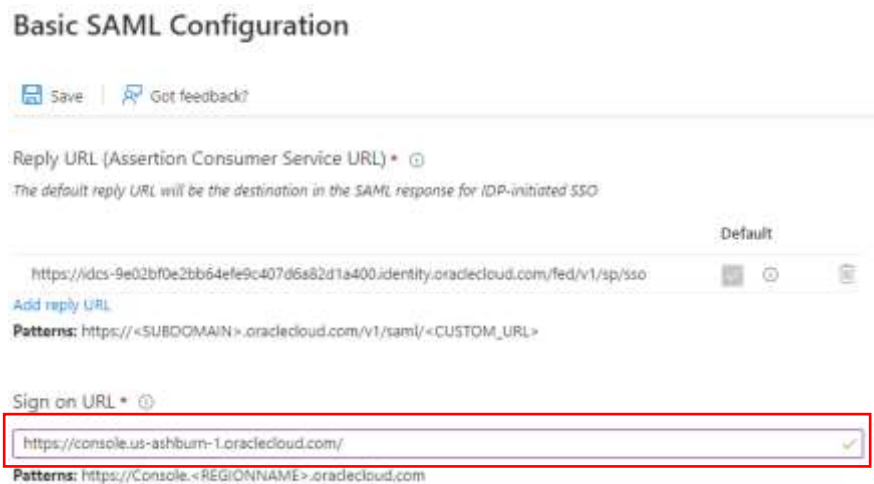
Upload metadata file.

Values for the fields below are provided by Oracle Cloud Infrastructure Console. file if provided by Oracle Cloud Infrastructure Console.

[Add](#) [Cancel](#)

Após fazer o download, preencha o campo de Sign on URL com o endereço de acesso do seu tenancy, exemplo:

<https://console.<REGIONNAME>.oraclecloud.com>



Basic SAML Configuration

Save | Got feedback?

Reply URL (Assertion Consumer Service URL) * ⓘ
The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

<https://idcs-9e02bf0e2bb64efe9c407d6s82d1a400.identity.oraclecloud.com/fed/v1/sp/sso>

[Add reply URL](#)

Patterns: https://<SUBDOMAIN>.oraclecloud.com/v1/saml/<CUSTOM_URL>

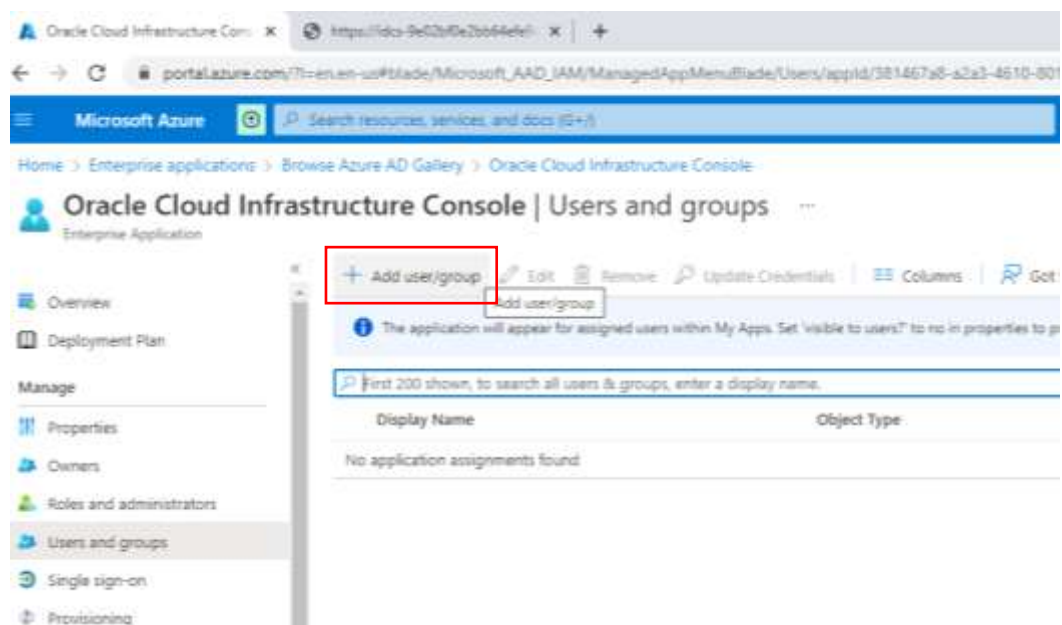
Sign on URL * ⓘ

<https://console.us-ashburn-1.oraclecloud.com/>

Patterns: <https://Console.<REGIONNAME>.oraclecloud.com>

Faça a atribuição dos usuários e grupos que deseja para a aplicação

(Esse grupo ou usuário deve ser criado anteriormente na Azure)



Oracle Cloud Infrastructure Console | Users and groups

Enterprise Application

Overview | Deployment Plan | Manage | Properties | Owners | Roles and administrators | **Users and groups** | Single sign-on | Provisioning

+ Add user/group | Edit | Remove | Update Credentials | Columns | Got feedback?

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to p

First 200 shown, to search all users & groups, enter a display name.

Display Name	Object Type
No application assignments found	

Nos atributos de conta de usuário, altere o Unique User Identifier (Name ID) de user.userprincipalname para user.mail

Manage claim ...

 Save  Discard changes |  Got feedback?

Name	nameidentifier
Namespace	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
^ Choose name identifier format	
Name identifier format *	Email address
Source *	<input checked="" type="radio"/> Attribute <input type="radio"/> Transformation
Source attribute *	DE: <input type="text" value="user.userprincipalname"/>
v Claim conditions	

Manage claim ...

 Save  Discard changes |  Got feedback?

Name	nameidentifier
Namespace	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
^ Choose name identifier format	
Name identifier format *	Email address
Source *	<input checked="" type="radio"/> Attribute <input type="radio"/> Transformation
Source attribute *	PARA: <input type="text" value="user.mail"/>
v Claim conditions	

Para o próximo passo será necessário fazer o download do metadado da Azure, navegue até Overview, selecione Set up Single Sign On, navegue até o Item 3 e faça download do arquivo Federation Metadata XML

SAML Signing Certificate		Edit
Status	Active	
Thumbprint	FF28860CD685724A6714149DE5593E0636CABAAF	
Expiration	2/25/2025, 11:55:11 AM	
Notification Email	weltonjesus2022@outlook.com	
App Federation Metadata Url	https://login.microsoftonline.com/cc91cd1e-f769-...	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	

Passo 2: Criando um provedor de identidade externa para o IDCS

No IDCS, navegue até **Security** e depois selecione **Identity Providers**

Clique em **Add SAML IDP**

Dê um nome para a aplicação e clique em Next

Add Identity Provider

Back

1 Details

2 Configure

3 Map

4 Export

5 Test

6 Activate

Next

Provide the name and description, and upload an icon for the Identity Provider.

* Name

AzureIDP

Description

Icon

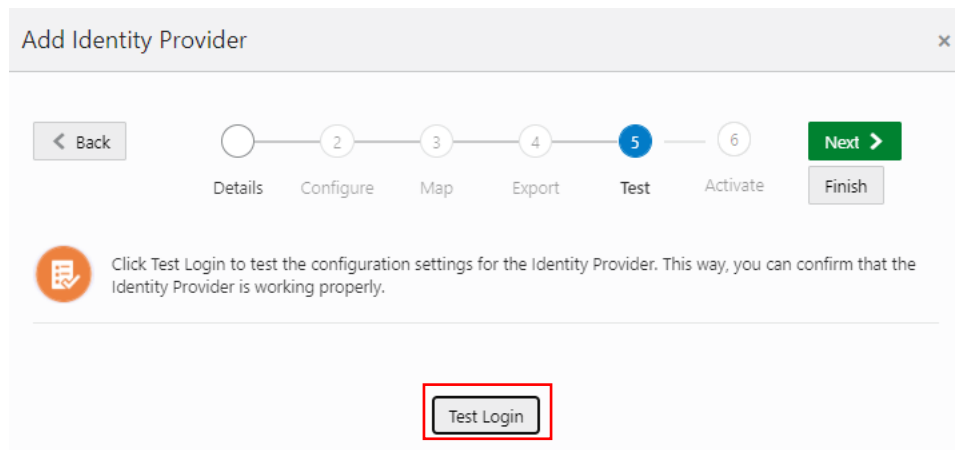
Upload

Em configure, selecione o arquivo Metada que foi feito download do Azure, marque a opção Include Signing Certificate e clique em Next

Na página de mapeamento de usuários, altere para as configurações abaixo, alterando a opção Oracle Identity Cloud Service User Attribute para Email Address e clique em Next

Na próxima página, não precisa fazer o download do Service Provider Metadata, somente clique em Next

Após configurar, clique em Test Login



The 'Add Identity Provider' dialog box features a progress bar with six steps: Details, Configure, Map, Export, Test, and Activate. The 'Test' step is currently selected and highlighted in blue. Navigation buttons include 'Back', 'Next', and 'Finish'. An orange icon with a checkmark and a document symbol is positioned to the left of an instructional message. At the bottom center, a 'Test Login' button is highlighted with a red rectangular border.

Add Identity Provider

Details Configure Map Export **Test** Activate

Click Test Login to test the configuration settings for the Identity Provider. This way, you can confirm that the Identity Provider is working properly.

Test Login

Se estiver tudo correto, a mensagem abaixo será apresentada

Your connection is successful.

You may close this window and go back to the admin console.

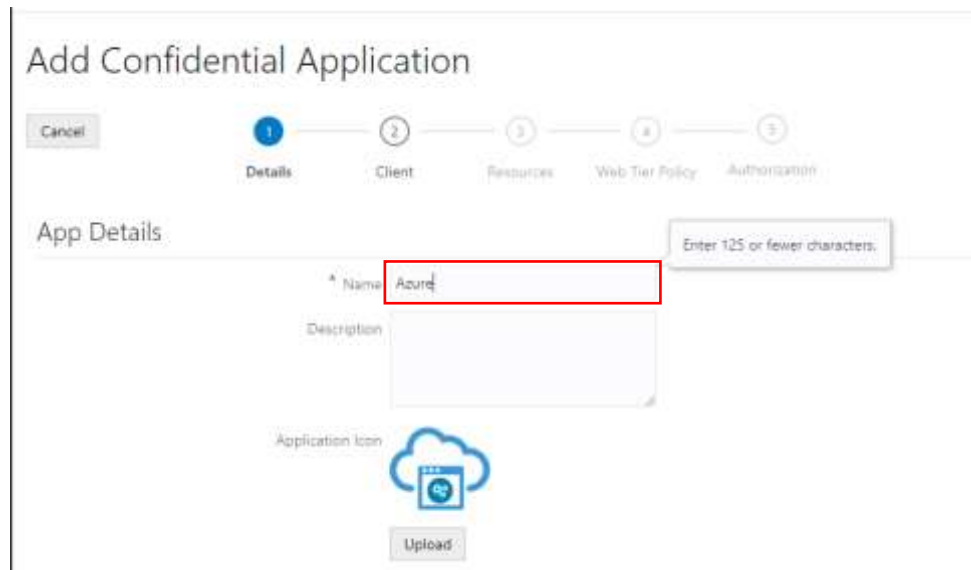
Habilite o Provedor de identidade antes de prosseguir para o próximo passo.

AzureAD	SAVE		Activate
Email	Local		Edit
			Test

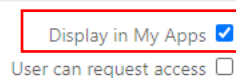
Passo 3: Criando a sincronização dos usuários e grupos da Azure para o IDCS

Antes de fazer essa configuração, caso o usuário seja o mesmo criado para validação da federação, delete o usuário em Users para conseguir que ele seja sincronizado via Application

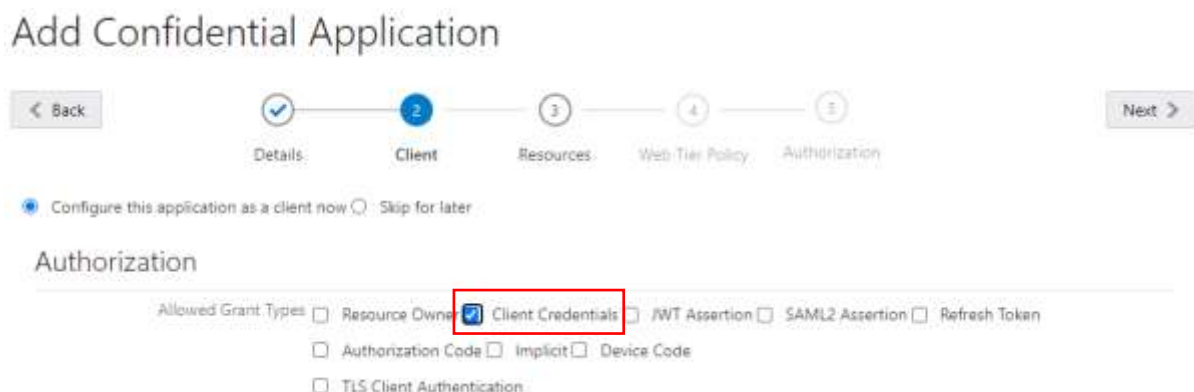
No IDCS navegue até **Applications** e selecione a opção **Add Confidential Application**, dê um nome para ela e depois marque a opção no final **Display in My Apps**



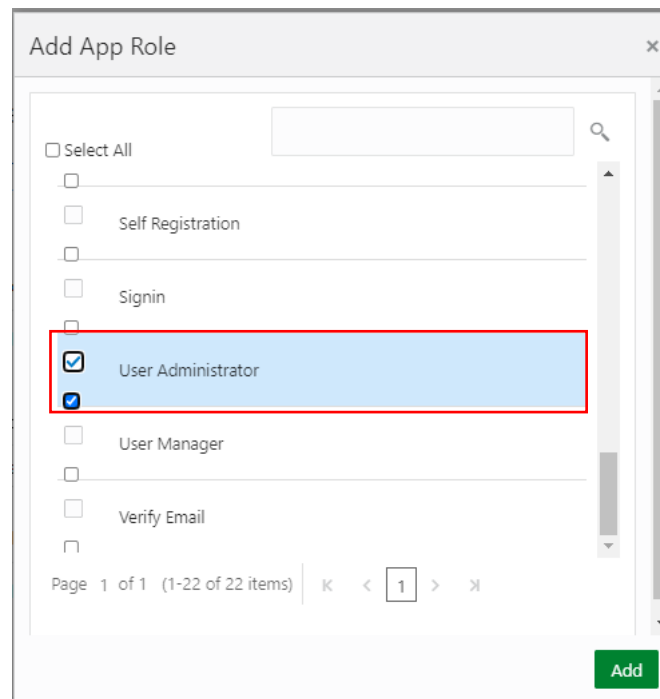
Display Settings



Selecione **Configure this application as a client now**, e em **Allowed Grant Types**, selecione **Client Credentials**



Adicione uma função para o usuário em App Roles, selecione User Administrator



Grant the client access to Identity Cloud Service Admin APIs

<div>+ Add</div>		
App Roles	Protected	
User Administrator	No	X

Em Resources, deixe como está e clique em Next



Expose APIs to Other Applications

Specify the APIs that need to be protected.

☐ Configure this application as a resource server now ☒ Skip for later

No Resources are protected by OAuth

Em Web Tier Policy deixe como está e clique em Next

Add Confidential Application

< Back

4

DetailsClientResourcesWeb Tier PolicyAuthorization

Next >

Web Tier Policy

Use this page to configure, edit, and validate a web tier policy. Additionally, you can import and export existing policies.

☐ Configure Web Tier Policy for this application ☒ Skip for later

Em Authorization, deixe desmarcada a opção e clique em Finish

Add Confidential Application

< Back

5

DetailsClientResourcesWeb Tier PolicyAuthorization

Finish

Authorization

Enforce Grants as Authorization ☐

Anote a chave e o Client ID, você irá usar na sincronização com a Azure

Application Added

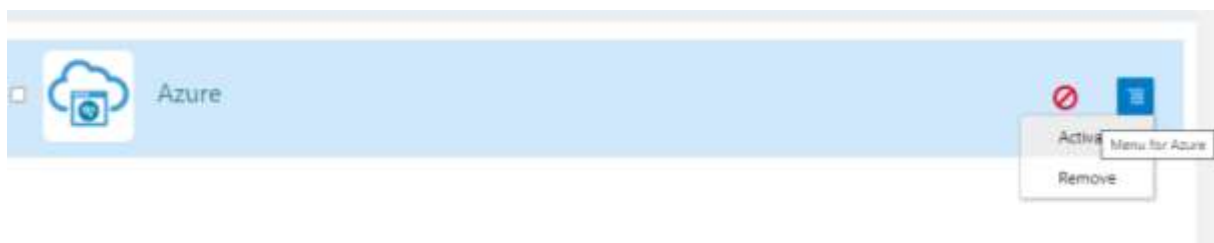
Below is the new Client ID and Client Secret for your application.

This information also appears on the Configuration tab in the Details section for the application.

Client ID	3556f6b60e294d1bb572f4f830374e34
Client Secret	[REDACTED]

Close

Ative a aplicação ao final do processo



Volte para a Azure, navegue até Enterprise Applications e selecione a aplicação da Oracle criada anteriormente

View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider.

Search by application name or object ID


Application type == Enterprise Applications X Applications status == Any X Application visibility == Any X Add filters


1 application found


Name	Object ID	Application ID	Homepage URL	Created on
Oracle Cloud Infrastruc	9257aaa7-9c1c-475c-828c-b2...	381467a8-a2a3-4610-8013-fa...	https://*.oraclecloud.com/v1/s...	2/25/2022


Navegue até Provision User Accounts

Getting 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](#)

**3. Provision User Accounts**
Automatically create and delete user accounts in the application.
[Get started](#)

**4. Conditional Access**
Secure access to this application with a customizable access policy.
[Create a policy](#)

Clique em Get Started e troque o modo para Automatic

Save X Discard

Provisioning Mode

Automatic

Use Azure AD to manage the creation and synchronization of user accounts in Oracle Cloud Infrastructure Console based on user and group assignment.

Em Admin Credentials, preencha os campos com o Tenant URL e a Secret Token,

A tenant URL você deve alterar da seguinte forma:

https://<IdP ID>.identity.oraclecloud.com/admin/v1

Onde: <idP ID> é seu **idcs-xxxxxxxxxxxxxxxx**

Cole a Client Secret

Admin Credentials

Admin Credentials

Azure AD needs the following information to connect to Oracle Cloud Infrastructure Console's API and synchronize user data.

Tenant URL * ⓘ

Secret Token

DICA! Durante a tentativa de conexão caso aconteça um erro de permissão será necessário converter a chave

Acesse: <https://www.base64encode.org/>

Cole a chave da seguinte forma:

<client-id>:<secret-id>

Mude as opções conforme a imagem abaixo, clique em Encode e copie a chave que será gerada

Encode to Base64 format

Simply enter your data then push the encode button.

Cole a chave <client-id>:<secret-id>

To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Destination character set.

CRLF (Windows) Destination newline separator.

☒ Encode each line separately (useful for when you have multiple entries).

☐ Split lines into 76 character wide chunks (useful for MIME).

☐ Perform URL-safe encoding (uses Base64URL format).

☒ Live mode OFF Encodes in real-time as you type or paste (supports only the UTF-8 character set).

Encodes your data into the area below.

Clique em ENCODE

MjhlhMWlxYjEwYjM0NGQ4NDg tNDE5MC00MTZlTikNmEtYjQxYzk5NGNlZjli

Copie essa chave

Altere os valores

Clique em Test Connection e em caso de sucesso, salve as configurações

The screenshot shows the 'Provisioning' configuration page. At the top, there is a 'Save' button (highlighted with a red box) and a 'Discard' button. A success message box at the top right states: 'Testing connection to Oracle Cloud Infrastructure Console. The supplied credentials are authorized to enable provisioning.' Below this, the 'Admin Credentials' section is visible, containing a 'Tenant URL' field with a value and a 'Secret Token' field. At the bottom of this section, a 'Test Connection' button is highlighted with a red box.

Volte para provisionamento e selecione a opção **Edit Provisioning**

This screenshot shows the provisioning controls and status. At the top, there are buttons for 'Start provisioning', 'Stop provisioning', 'Restart provisioning', 'Edit provisioning' (highlighted with a red box), 'Provision on demand', and 'Refresh'. Below these, the 'Current cycle status' section shows 'Initial cycle not run' and '0% complete'. To the right, under 'Statistics to date', there are links for 'View provisioning details' and 'View technical information'. A link for 'View provisioning logs' is also present.

Vá até Mappings e verifique se as 2 opções estão como Yes, os usuários e grupos atrelados a aplicação serão sincronizados para federação para Oracle Cloud.

The screenshot shows the 'Mappings' configuration page. It includes a description: 'Mappings allow you to define how data should flow between Azure Active Directory and OracleIDCS.' Below this is a table with two columns: 'Name' and 'Enabled'. The table contains two rows: 'Provision Azure Active Directory Groups' and 'Provision Azure Active Directory Users', both with 'Yes' in the 'Enabled' column. These two rows are highlighted with a red box. At the bottom, there is a checkbox for 'Restore default mappings'.

Name	Enabled
Provision Azure Active Directory Groups	Yes
Provision Azure Active Directory Users	Yes

Acesse Provision Azure Active Directory Users e verifique se a sincronização está ativa

This screenshot shows the configuration for 'Provision Azure Active Directory Users'. It includes a 'Name' field with the value 'Provision Azure Active Directory Users'. Below this, there is an 'Enabled' section with a toggle switch set to 'Yes' (highlighted with a red box) and a 'No' option.

Faça o ajuste para que os usuários sejam federados da forma correta.

Navegue até o Provisioning, depois em Mappings, edite o Provisioning Azure Active Directory Users

Provisioning

Save Discard

Mappings

Mappings allow you to define how data should flow between Azure Active Directory and OracleIDCS.

Name	Enabled
Provision Azure Active Directory Groups	Yes
Provision Azure Active Directory Users	Yes

Adicione o seguinte atributo em Add New Mapping

Attribute Mapping

Save Discard

city	addresses[type eq "work"] locality	Delete
state	addresses[type eq "work"] region	Delete
postalCode	addresses[type eq "work"] postal...	Delete
country	addresses[type eq "work"] country	Delete
streetAddress	addresses[type eq "work"] streetA...	Delete
employeeId	urn:ietf:params:scim:schemas:exte...	Delete
department	urn:ietf:params:scim:schemas:exte...	Delete
Add New Mapping		

Altere para Constant, colote a Constant Value como True e coloque o Target attribute:
urn:ietf:params:scim:schemas:oracle:idcs:extension:user:User:isFederatedUser

Conforme abaixo

Edit Attribute



A mapping lets you define how the attributes in one class of Azure AD object (e.g. Users) should flow to and from this application.

Mapping type ⓘ

Constant

Constant Value * ⓘ

true

Target attribute * ⓘ

urn:ietf:params:scim:schemas:oracle:idcs:extension:user:U...

Match objects using this attribute

No

Matching precedence ⓘ

Ok

O intervalo de sincronização é de 40 minutos, caso queira forçar uma sincronização inicial, clique em Start Provisioning

Start provisioning

☐ Stop provisioning

Current cycle status

Incremental cycle completed.

100% complete

Users
1

Groups
1

Passo 4: Criando uma política de acesso a aplicação

Navegue até **Security** e depois selecione **Sign-On Policies**

Clique em **Add** e dê um nome para Policy

Add Sign-On Policy

Cancel

<

1

2

3

>

Details

Sign-On Rules

Apps

Details

* Policy Name

AzureIDP-Police

Description

No próximo passo, Adicione uma **Rule Sign-On**

Dê um nome, selecione o provedor de identidade da Azure e deixe a opção Access is como Allowed

Add Rule

* Rule Name Rule-AzureIDP

Conditions

If the user is authenticated by AzureIDP X

And is a member of these groups Enter or select one or more groups.

And is an administrator ☐

And is not one of these users Enter or select one or more user accounts.

And the user's client IP address is ☒ Anywhere ☐ In one or more of these network perimeters

Adaptive Security Conditions

And if the user's risk level is > >

And the risk provider name Default Risk Provider Risk Score > > +

Actions

Access is Allowed

No próximo passo selecione as aplicação configurada para Azure anteriormente

Add Sign-On Policy

Cancel < Details Sign-On Rules Apps > Finish

Apps

☐ Select All + Assign X Remove

☒ Azure

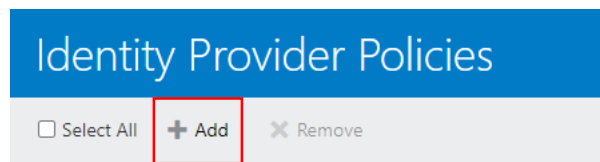
Clique em Finish

Habilite a política

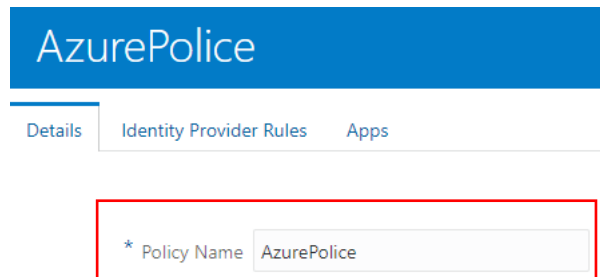
Passo 5: Cconfigurando uma IDP Policy para a aplicação federada

Navegue até Security, depois IDP Policy

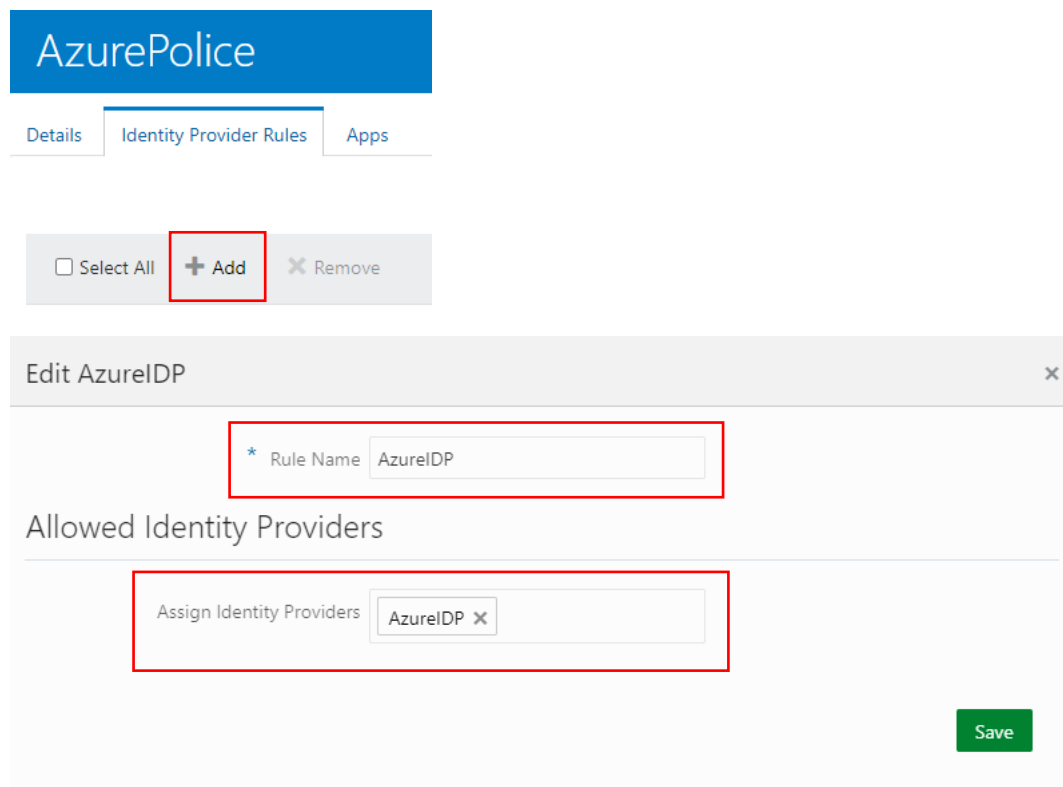
Clique em Add



Dê um nome para Police



Adicione um Identity Provider Rules, dê um nome e faça a associação do IDP criado para AzureIDP



Em APPs, faça a associação da aplicação desejada, no caso irei associar o OAC

AzurePolice

Details

Identity Provider Rules

Apps

☐ Select All

+ Assign

× Remove



ANALYTICSINST_oac-idpjqbyeiom-
ia

Ao fazer login na URL da aplicação você será redirecionado automaticamente para o provedor federado.