

Configurando SAML para autenticação do SmartDashboard

Helio Leite

Security Engineer

Dez - 2024

Este documento criado em Dez de 2024 serve como um guia de implementação de uma autenticação via SAML para o SmartDashboard não substituindo os guias oficiais para um melhor detalhamento.

Os documentos oficiais são sempre atualizados e podem ser localizados nos links abaixo:

R82 Whats New

https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_RN/Content/Topics-RN/Whats-New.htm

Check Point Quantum R82 Release

<https://support.checkpoint.com/results/sk/sk181127>

R82 Quantum Security Management Administration Guide

https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_SecurityManagement_AdminGuide/Content/Topics-SECMG/Welcome.htm

Criar uma conta de administrador com login de autenticação SAML

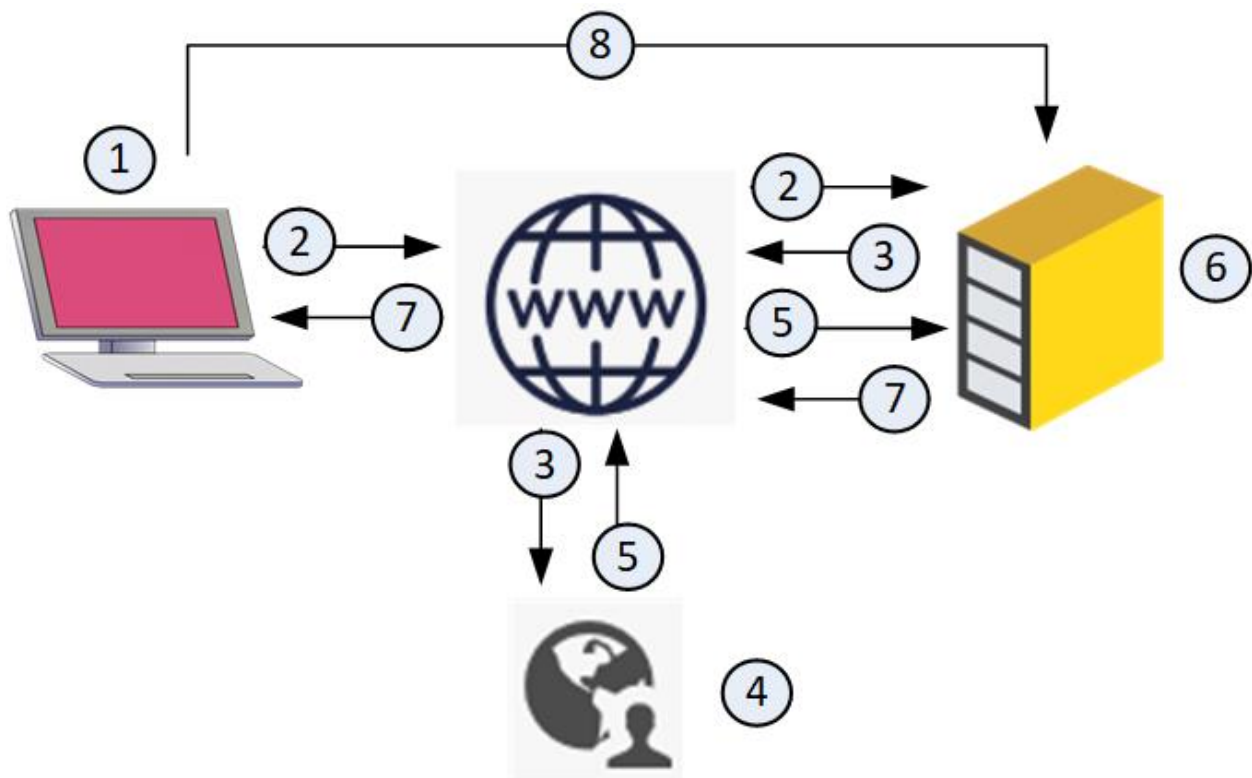
Com a autenticação SAML, os administradores iniciam sessão no SmartConsole através de um IDP ("Identity Provider") de terceiros com o protocolo SAML. O IDP detém as informações sobre os administradores, incluindo a capacidade de autenticar. A Check Point suporta estes IDPs: Okta, Ping Identity e Azure.

Caso de utilização

1. Os administradores com contas no Azure AD e que querem trabalhar com o SmartConsole.
2. Se cada administrador usar dois nomes e senhas diferentes, um para o Azure e outro para o SmartConsole, isso causará uma série de problemas:
3. Os administradores devem lidar com diferentes políticas de senha e expiração (além de outras senhas corporativas).
4. Os administradores têm de se lembrar de duas senhas diferentes, uma para o Azure e outra para a SmartConsole (além de outras senhas corporativas).
5. Requer manutenção adicional dos administradores. Por exemplo, quando um administrador sai da empresa, é necessário removê-lo de todas as aplicações em que está registado. Se utilizar um IDP, basta remover o administrador da base de dados do IDP.
6. A organização prefere que cada administrador use uma senha única para o Azure AD e a SmartConsole. Com o IDP, o administrador pode autenticar-se uma vez no Azure e, quando o administrador se conectar na SmartConsole, este já o reconhece e não tem de introduzir uma nova senha. Desta forma, o administrador também não revela a sua senha á (SMS) Security Management Server.

Fluxo do processo de autenticação SAML:

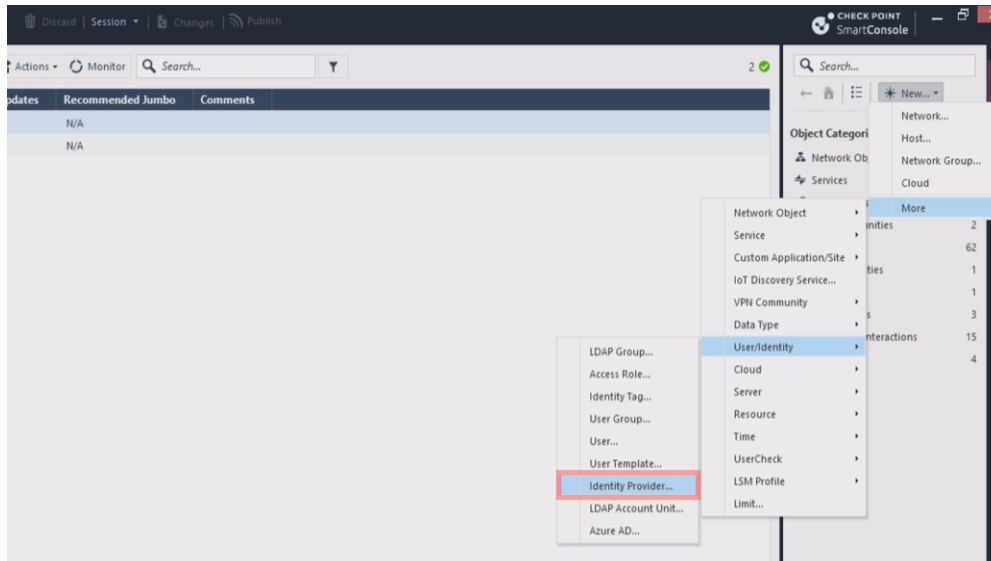
1. O administrador tenta iniciar sessão na SmartConsole.
2. A SmartConsole redirecciona o administrador de volta para o browser para uma URL que está pré-configurada na SMS.
3. A SMS redirecciona o browser com um pedido SAML para o IDP.
4. O IDP autentica o administrador.
5. O IDP gera uma sessão de autenticação SAML e envia-a de volta para o SMS através do browser.
6. O SMS valida a sessão autenticada SAML.
7. Se o administrador for autenticado, o SMS redirecciona o browser para a SmartConsole com os dados necessários para a autenticação.
8. A SmartConsole abre uma sessão para o SMS com estes dados de autenticação.



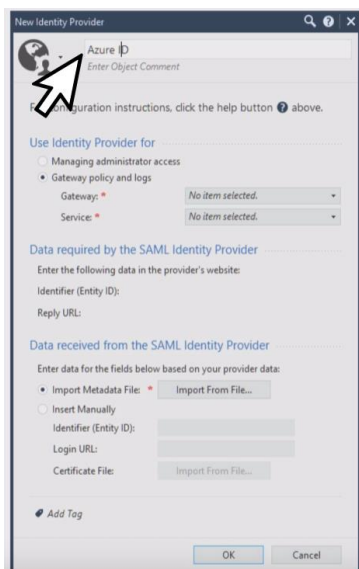
Login de autenticação via SAML

Nota - Por padrão, a autenticação SAML para login do SmartConsole exige que o Gaia Portal na SMS funcione na porta TCP 443. Se o Gaia Portal for executado em uma porta diferente, insira esse número de porta na janela de logon da SmartConsole (<IP_Address>:<Port>). Para obter mais informações, consulte sk182032.

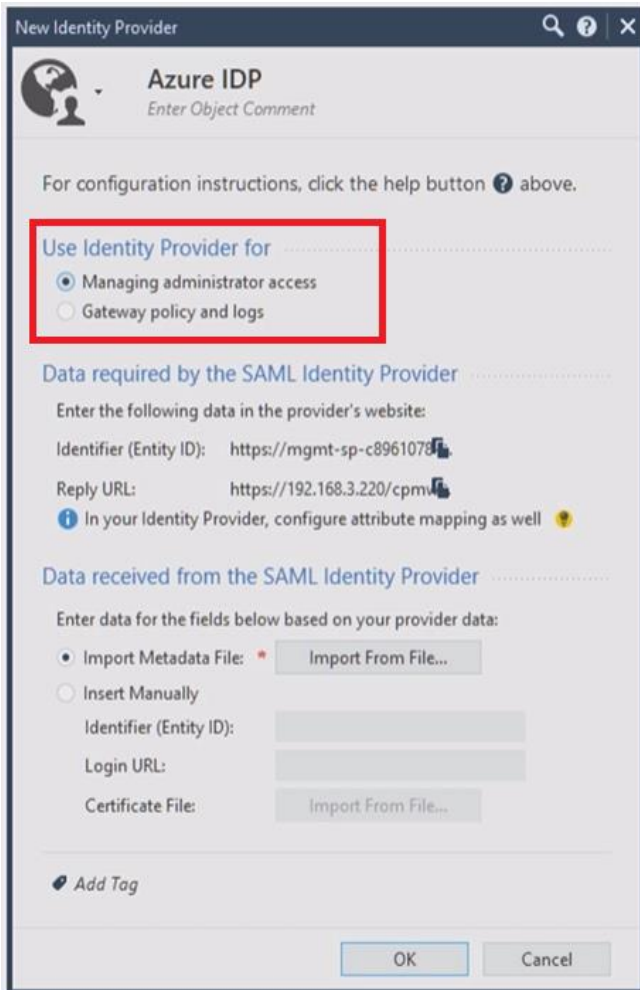
1. Abrir a SmartConsol e crie um objeto “Identity Provider” (IDP) e configure-o
2. No “Object Explorer” clique em “New” > “More” > “User/Identity” > “Identity Provider”



3. A janela de criação de um novo “Identity Provider” é aberta.



4. Configure estas propiedades para o objeto de “Identity Provider”:
 - a. “Name” (por exemplo: Azure).
 - b. Use “Identity Provider” for - Seleccione “Managing administrator access”.



New Identity Provider

Azure IDP
Enter Object Comment


For configuration instructions, click the help button ? above.


Use Identity Provider for



Managing administrator access
 Gateway policy and logs

Data required by the SAML Identity Provider

Enter the following data in the provider's website:

Identifier (Entity ID): 

Reply URL: 

 In your Identity Provider, configure attribute mapping as well 

Data received from the SAML Identity Provider

Enter data for the fields below based on your provider data:


Import Metadata File: *

Insert Manually

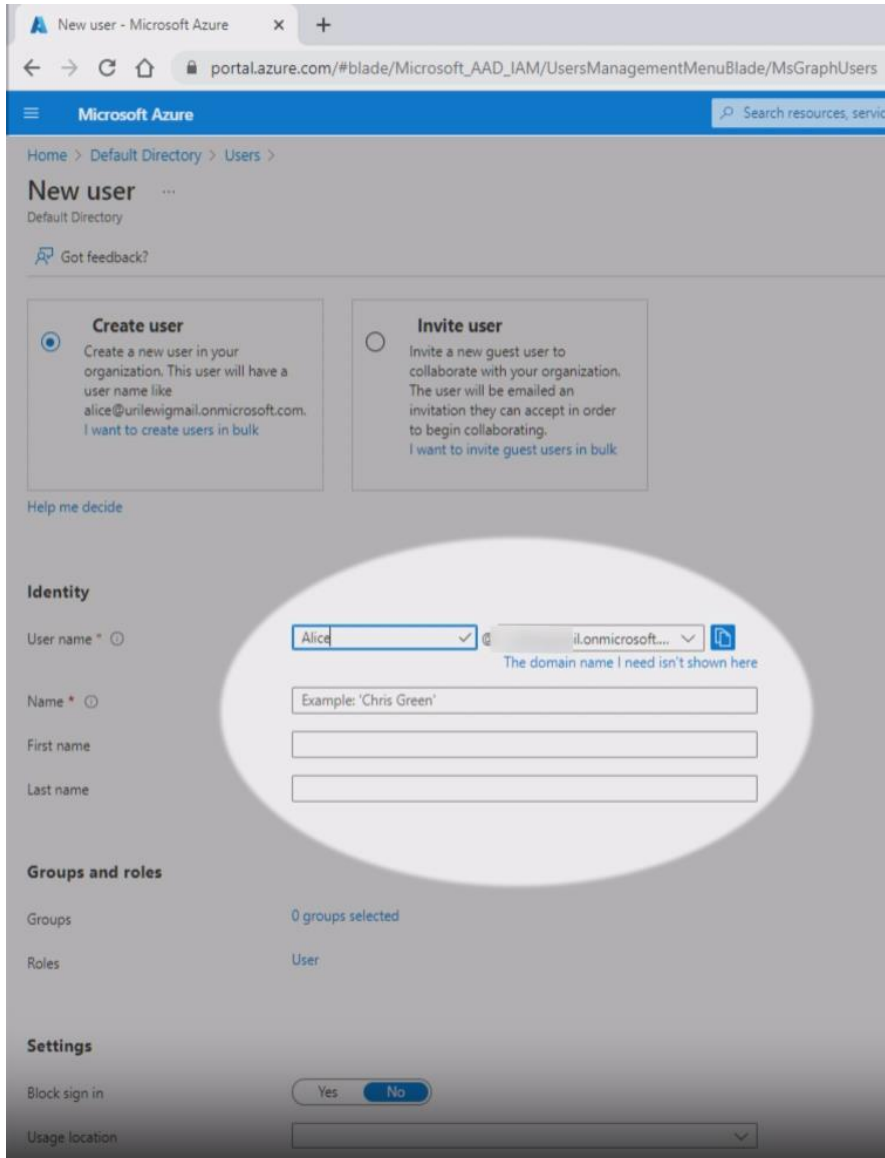
Identifier (Entity ID):

Login URL:

Certificate File:

 Add Tag

5. Primeiro passo a criação de usuários, por exemplo em “create user” preencha os campos necessários neste exemplo “User Name” Alice Palmer e Bob Alan



New user - Microsoft Azure

portal.azure.com/#blade/Microsoft_AAD_IAM/UsersManagementMenuBlade/MsGraphUsers

Microsoft Azure

Home > Default Directory > Users >

New user

Default Directory

Got feedback?

Create user


Create a new user in your organization. This user will have a user name like `alice@unilewigmil.onmicrosoft.com`.
I want to create users in bulk

Invite user

Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.
I want to invite guest users in bulk

[Help me decide](#)

Identity

User name * @ 
The domain name I need isn't shown here

Name *

First name

Last name

Groups and roles

Groups 0 groups selected

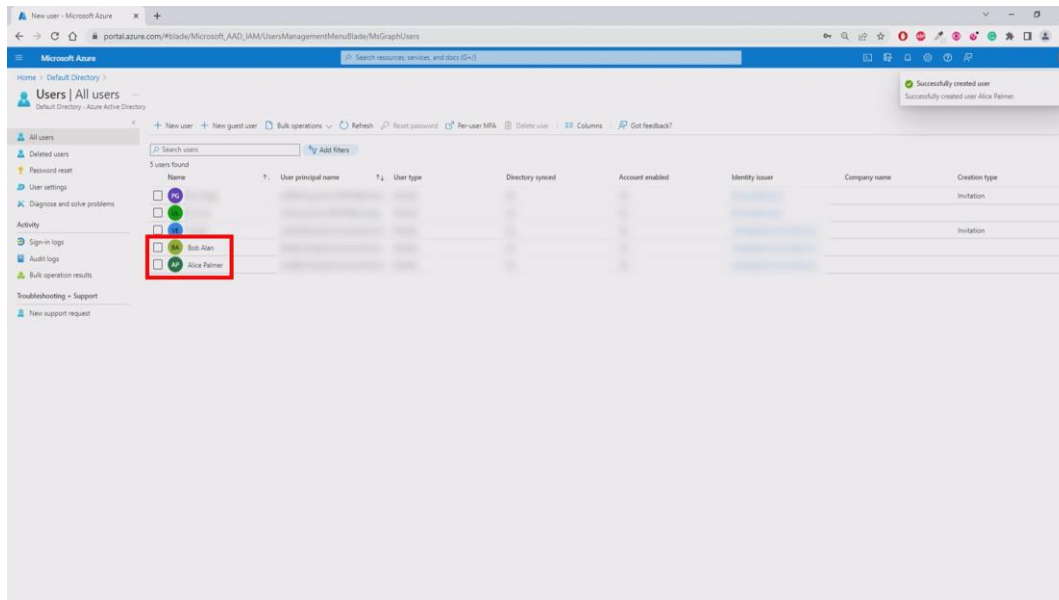
Roles User

Settings

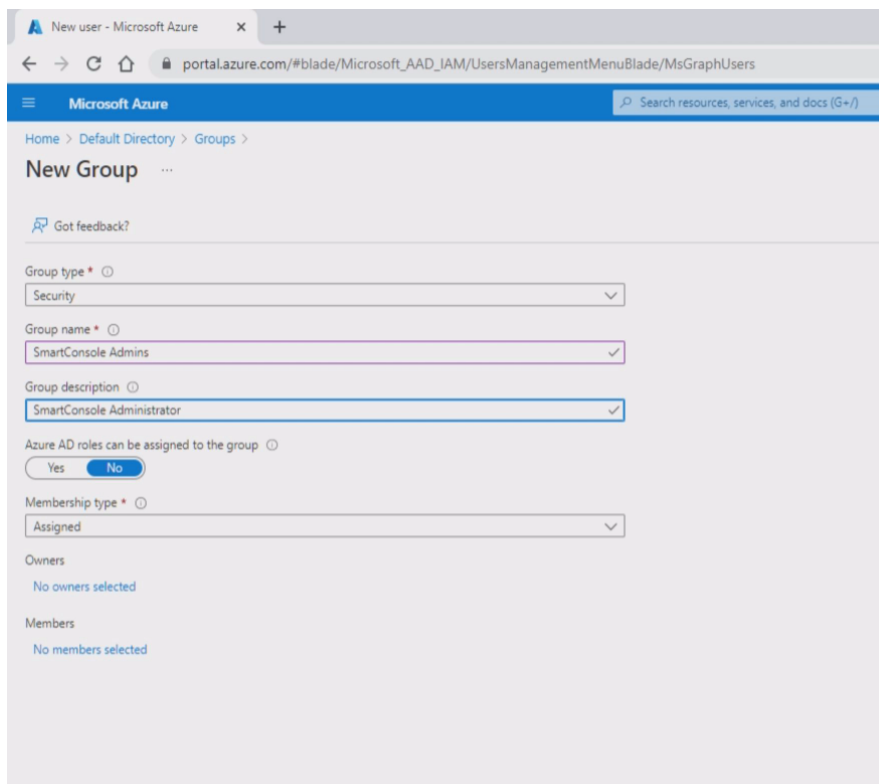
Block sign in Yes No

Usage location

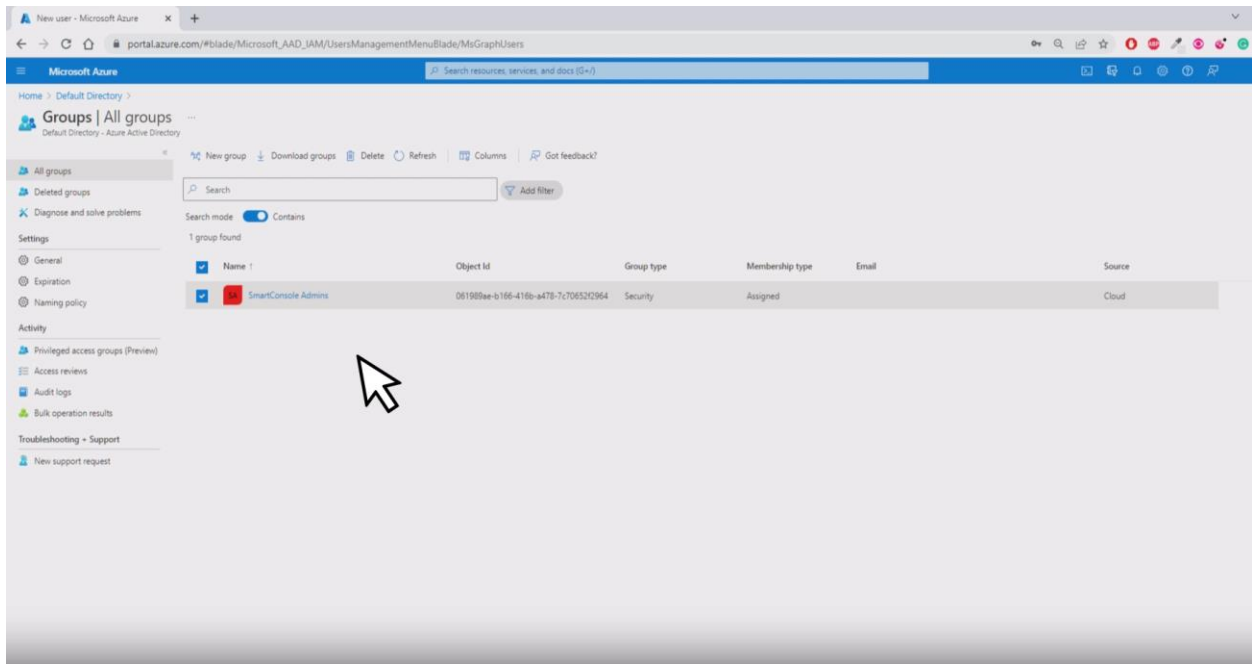
6. Após os usuários criados conforme abaixo crie um novo grupo em “New Group”.



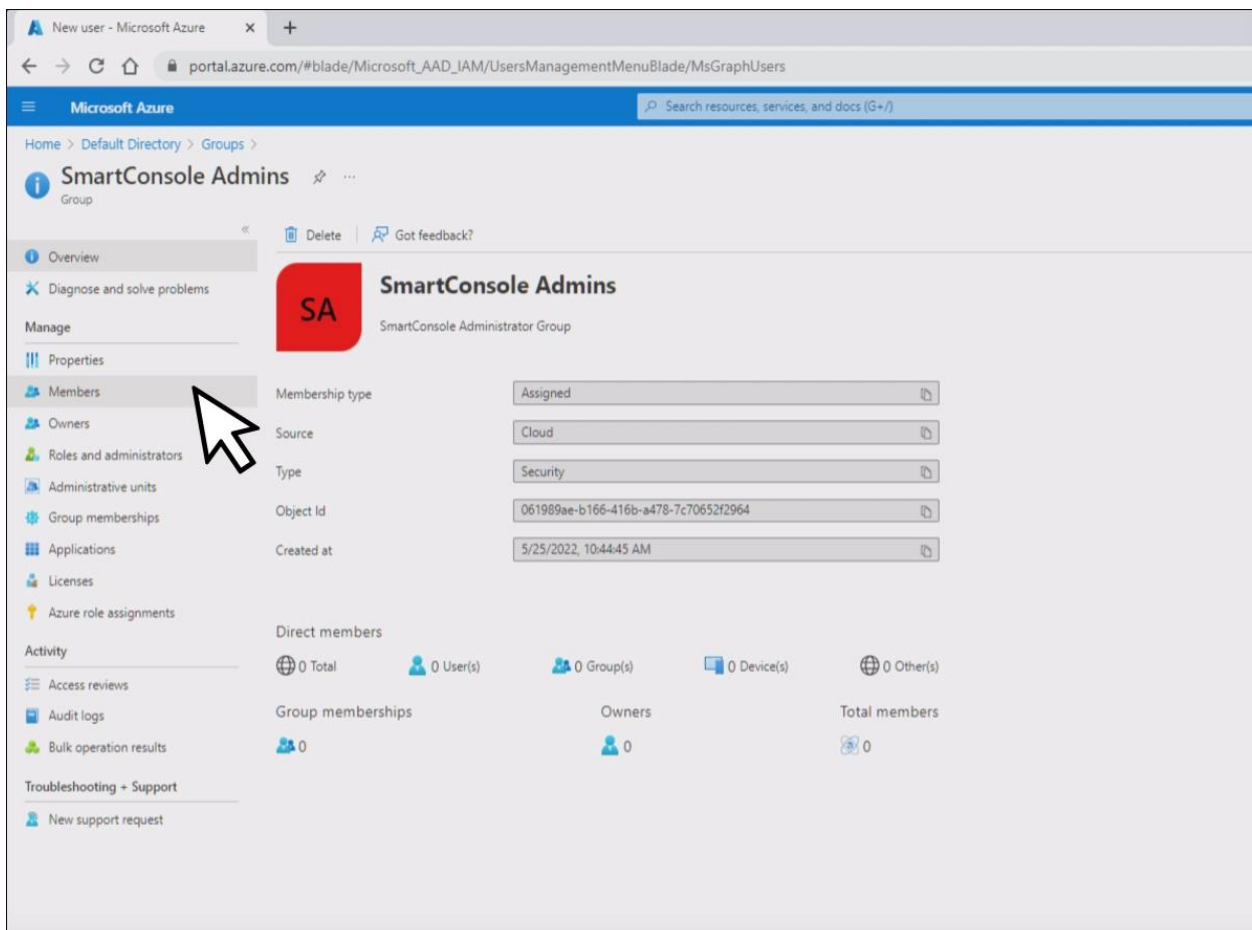
7. Em “New Group” criamos o grupo de exemplo smart console admins



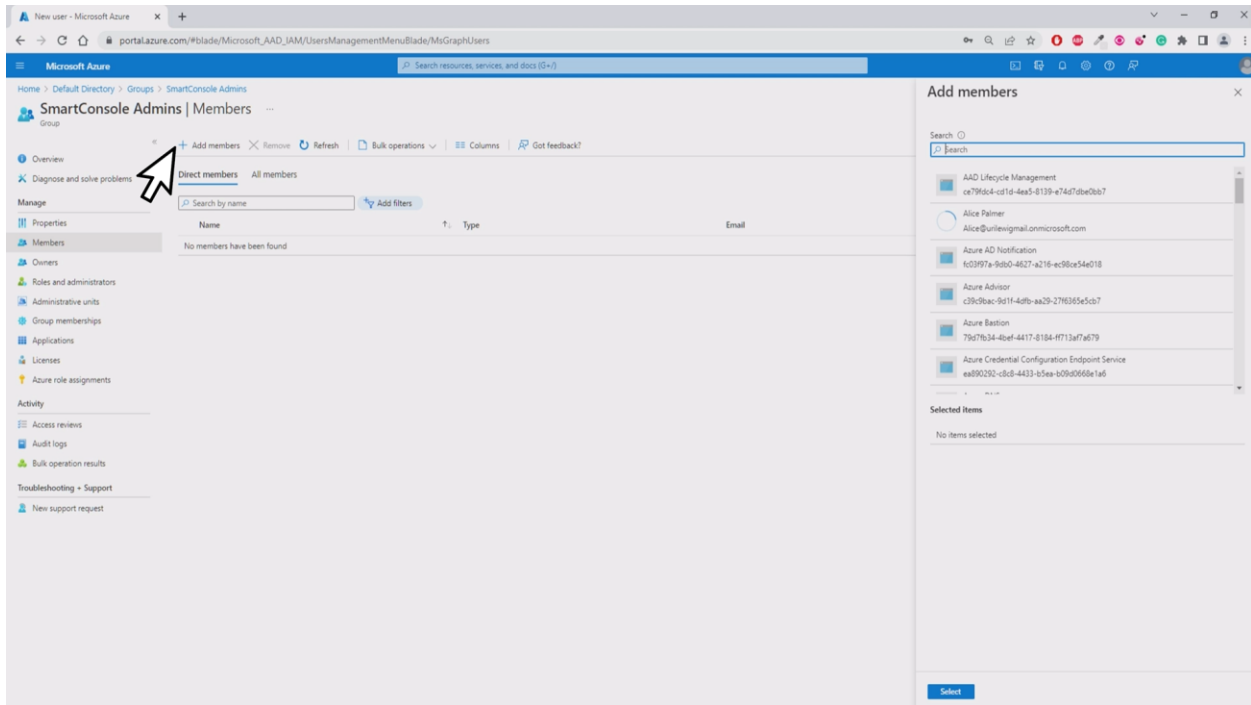
8. Após a criação do grupo clique no objeto criado.



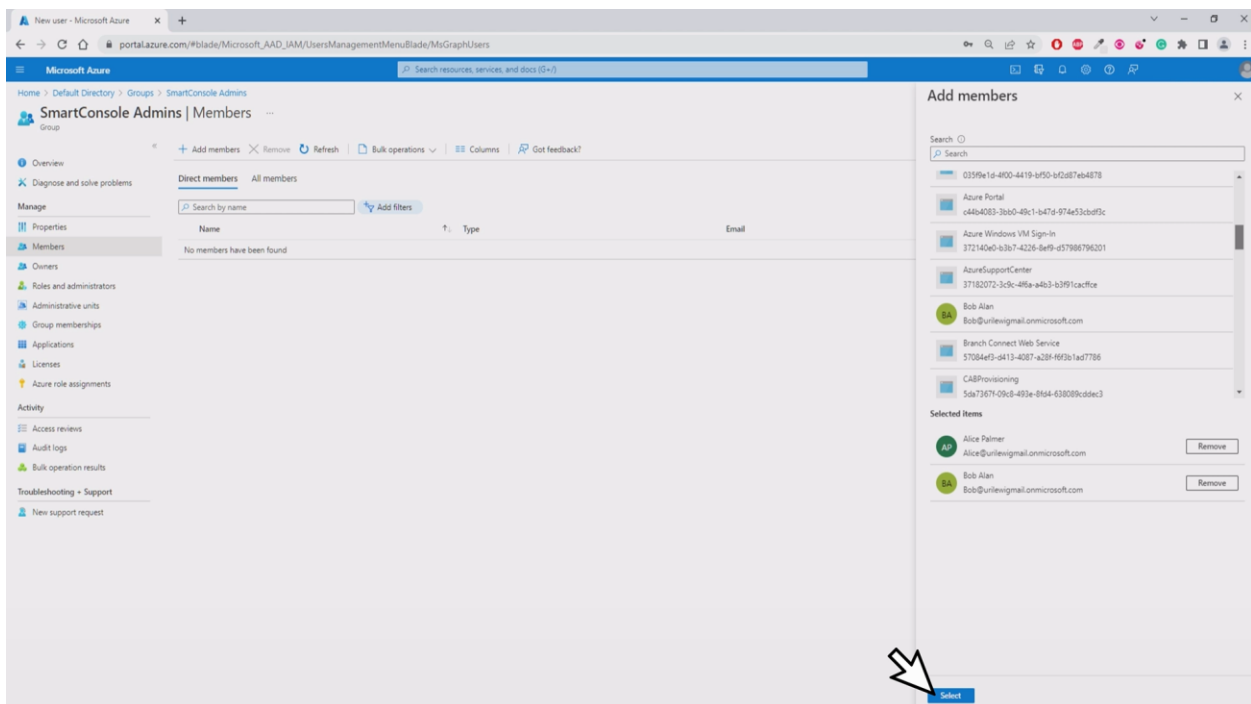
9. Vá até a guia “members” localizado no canto esquerdo



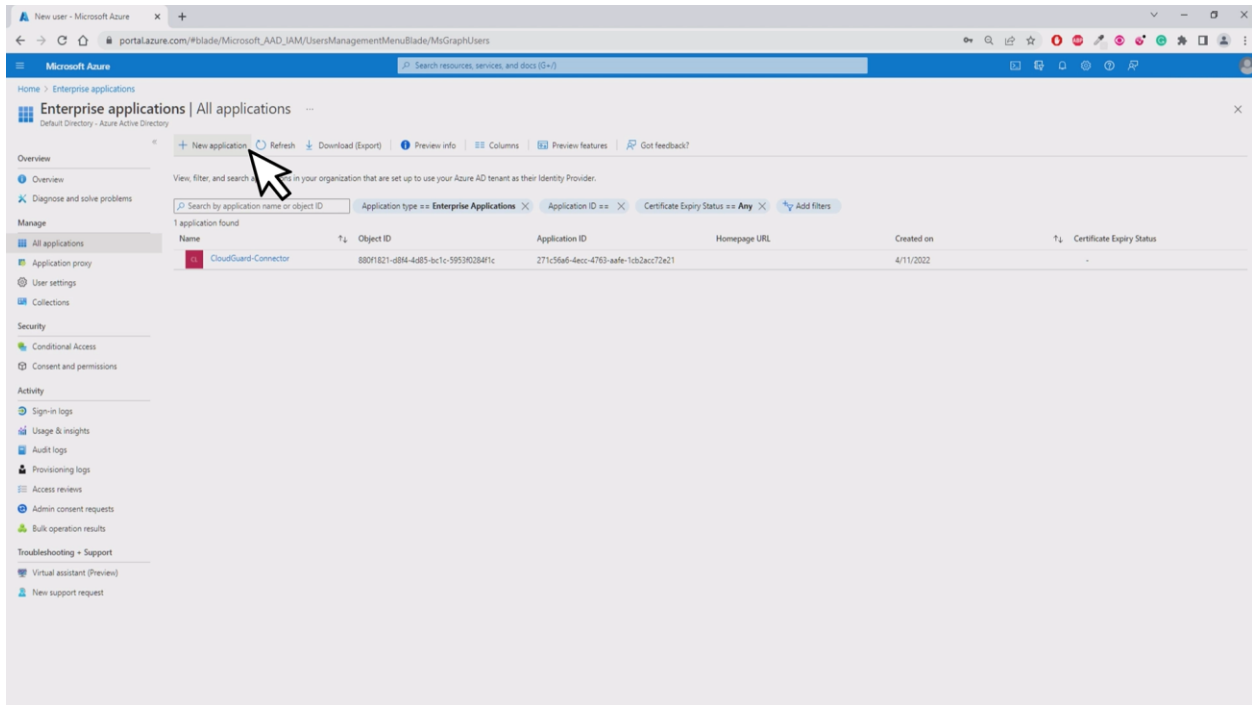
10. Clique em “add members” para adicionar membros no canto superior esquerdo, e ao lado direito aparecerá a tela de seleção de membros



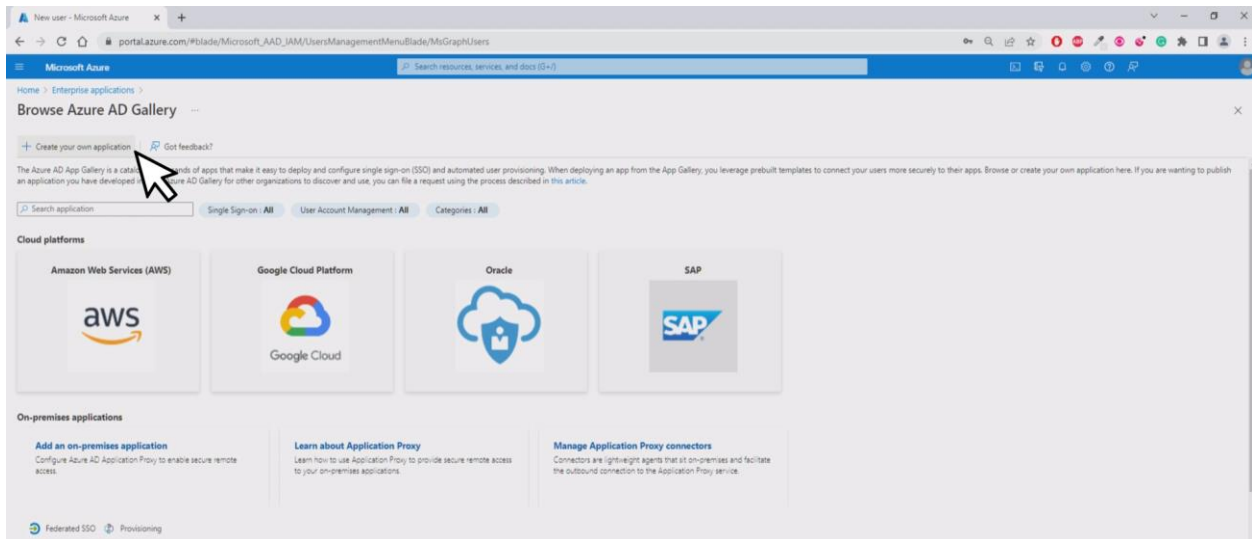
11. Selecione os membros desejados , em nosso caso Bob Alan e Alice Palmer e clique em selecionar.



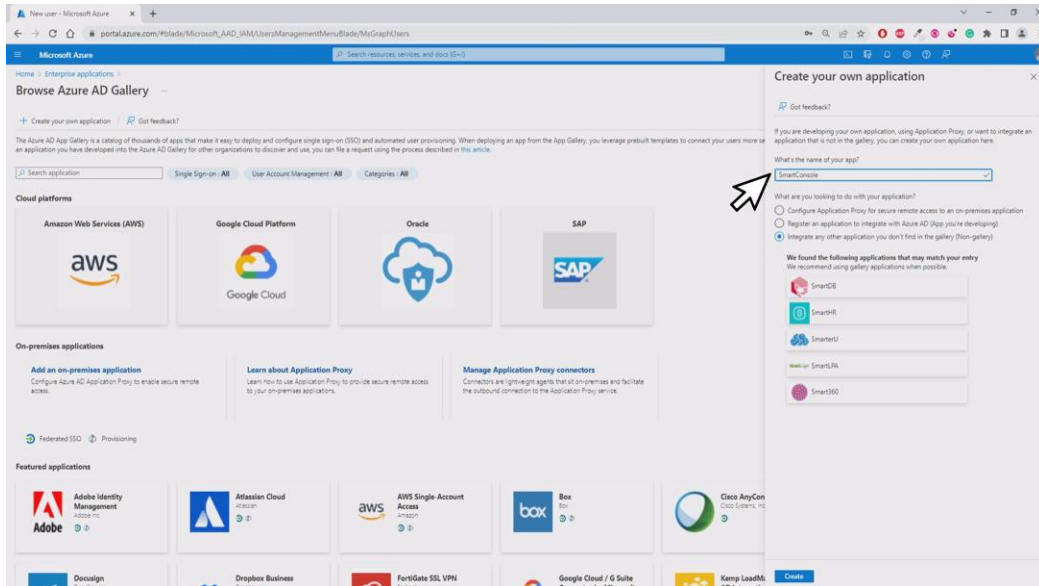
12. O próximo passo é criar uma “enterprise application”, clique em criar nova aplicação



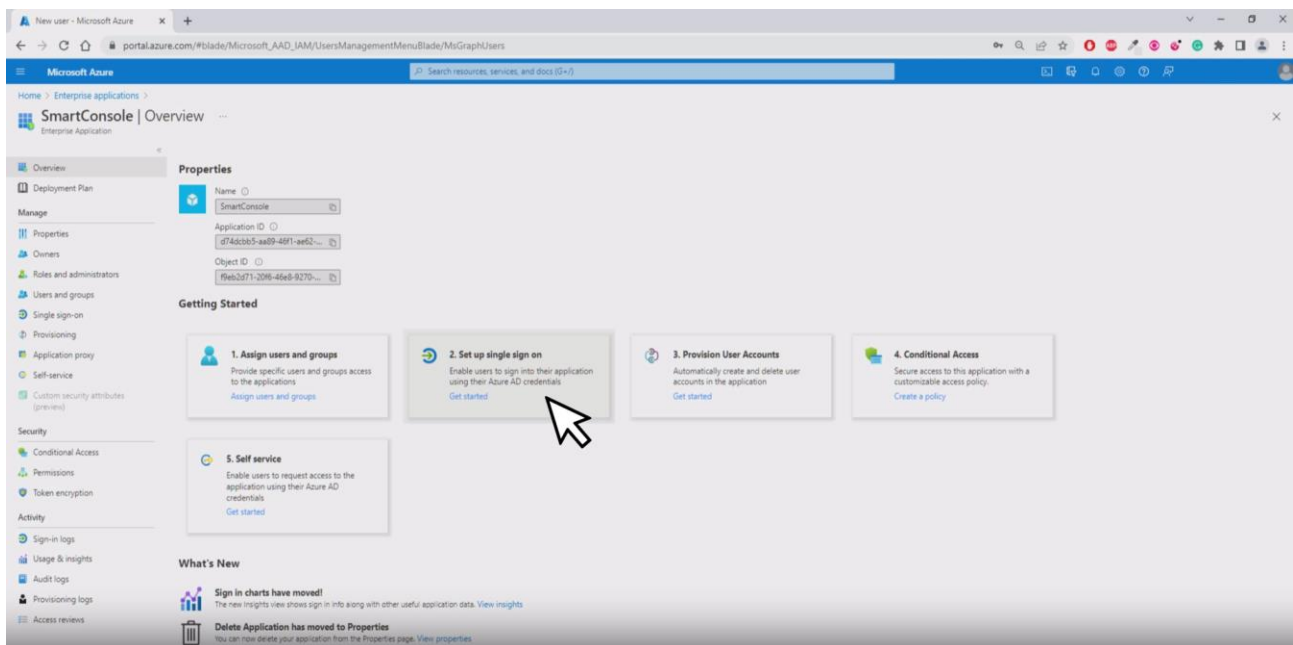
13. Selecione criar sua própria aplicação “Create your own application”



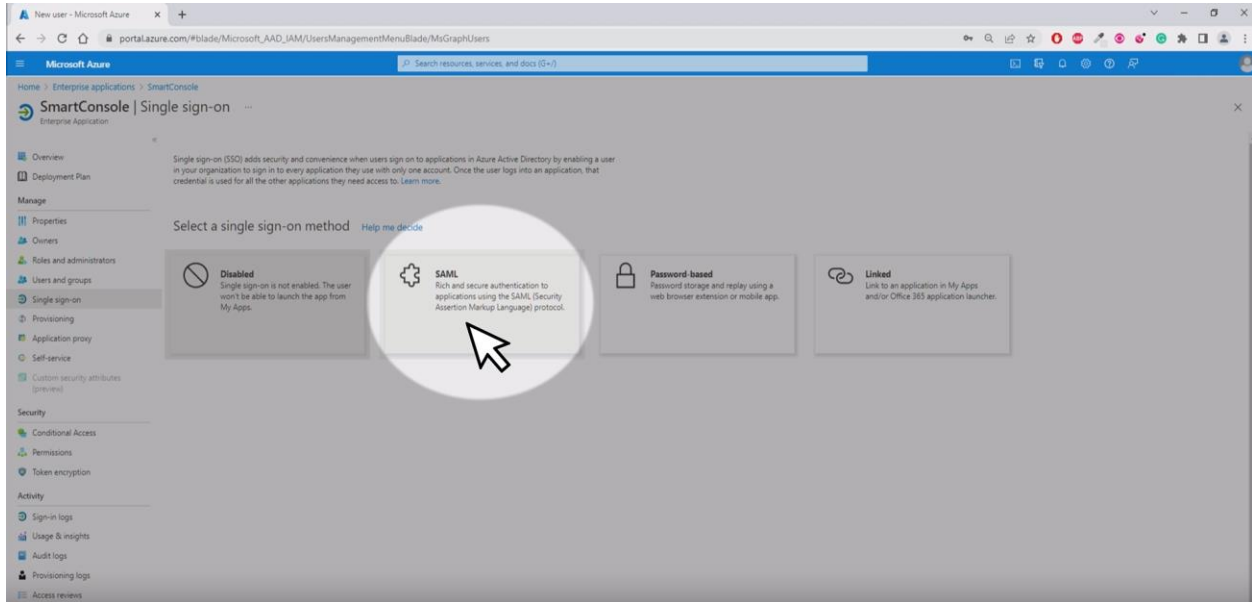
14. Coloque um nome para sua aplicação no nosso exemplo “SmartConsole” e selecione a opção “Integrate any other application you don’t find in the gallery (Non-Gallery)” e clique em “create”



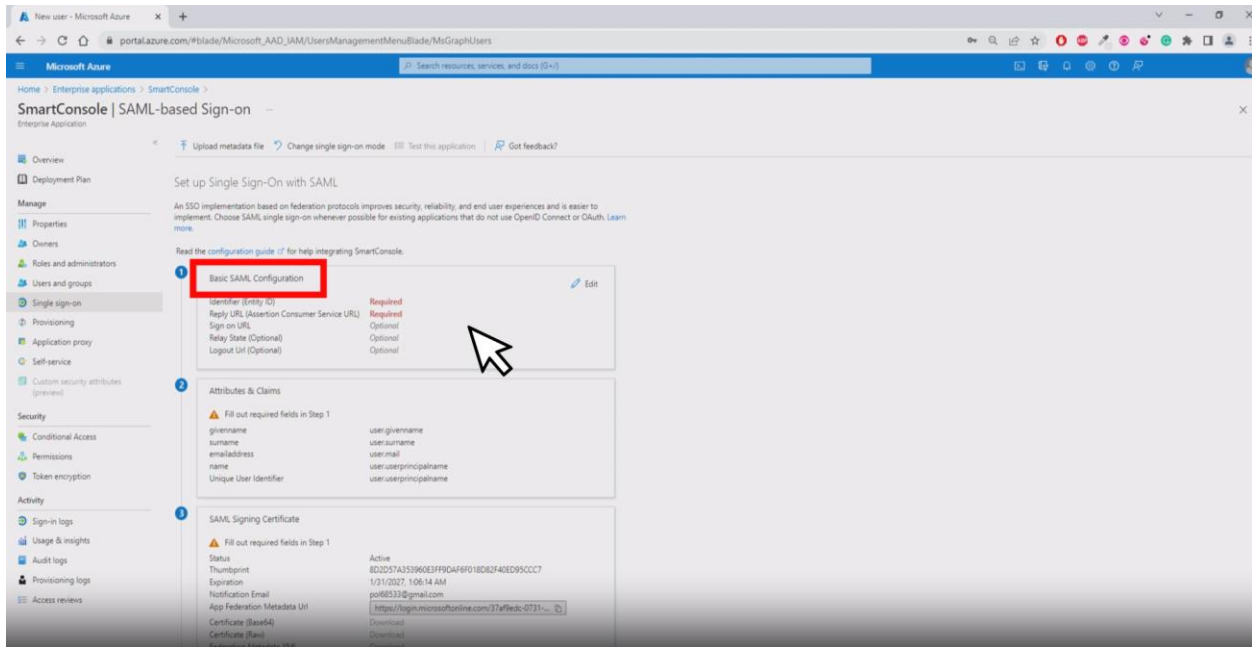
15. Dentro da aplicação criada vá em “2. set up single sign on”



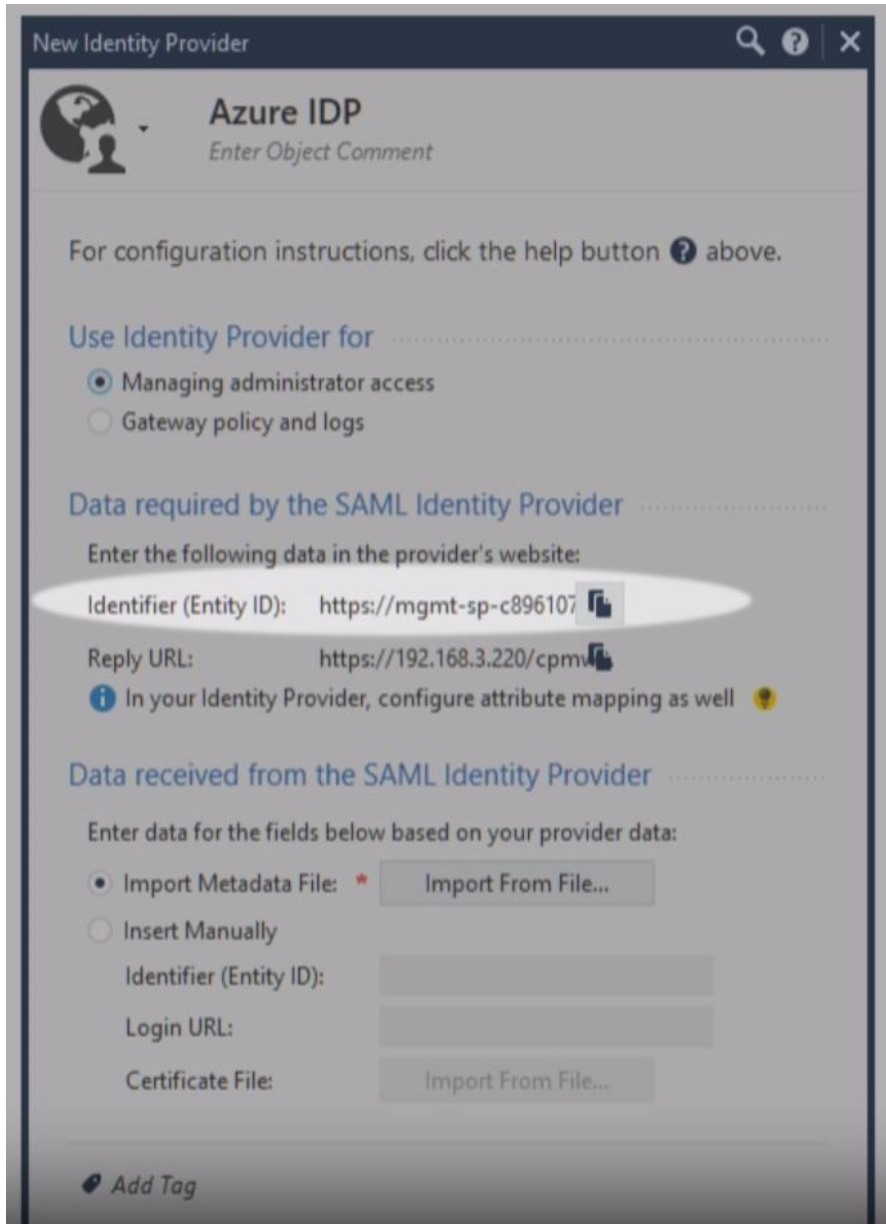
16. Seleccione a opção “SAML”



17. Clique em editar “Basic SAML Configuration”



18. Voltando a “Smart Console” na janela do novo IDP copie as seguintes informações “Identifier (Entity ID)”



New Identity Provider

Azure IDP
Enter Object Comment


For configuration instructions, click the help button ? above.


Use Identity Provider for



- Managing administrator access
- Gateway policy and logs

Data required by the SAML Identity Provider

Enter the following data in the provider's website:

Identifier (Entity ID): 

Reply URL: 

 In your Identity Provider, configure attribute mapping as well 

Data received from the SAML Identity Provider


Enter data for the fields below based on your provider data:

- Import Metadata File: *
- Insert Manually

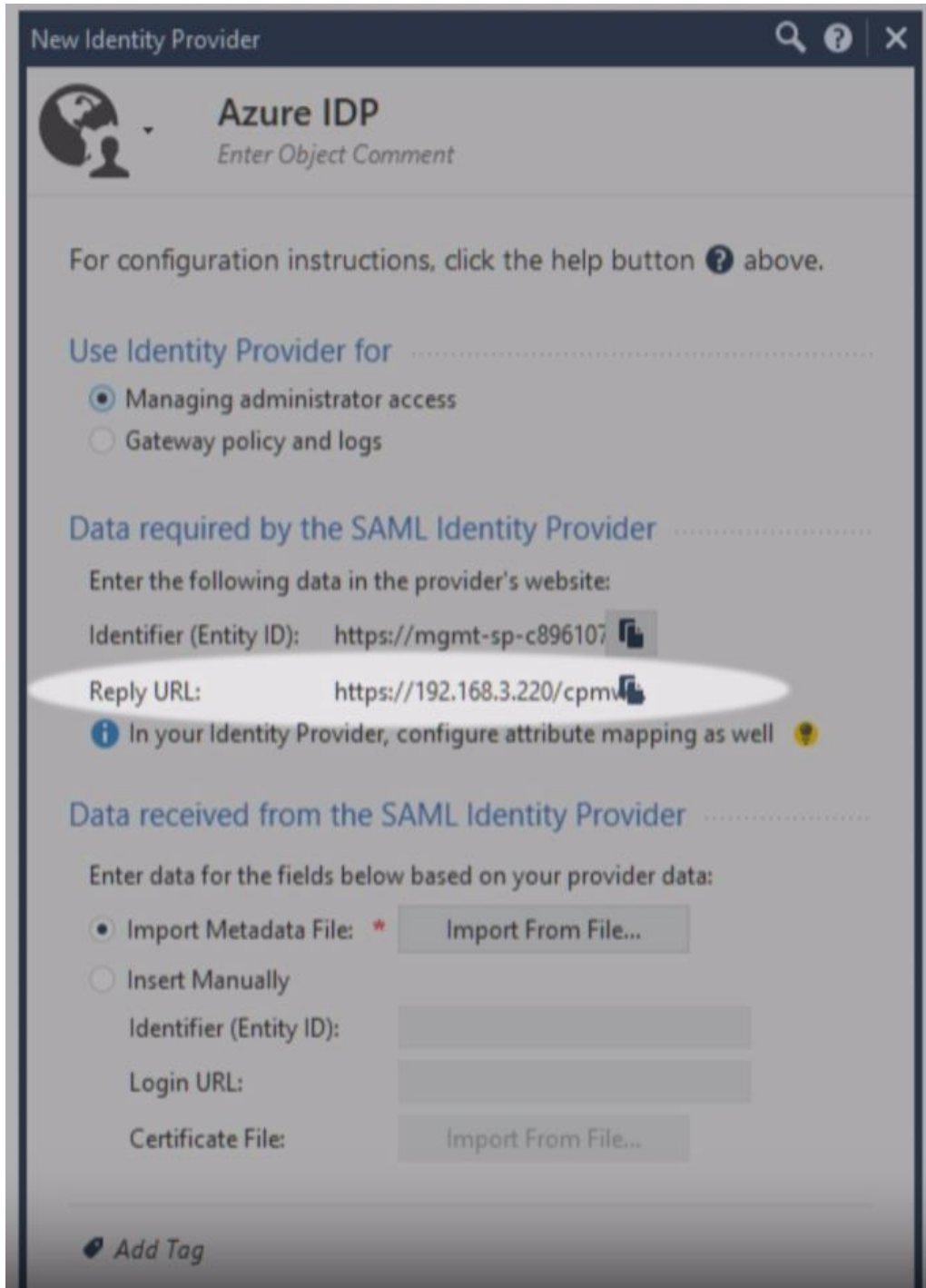
Identifier (Entity ID):

Login URL:

Certificate File:

 Add Tag

19. Copie também a informação “Reply URL”



New Identity Provider

Azure IDP
Enter Object Comment


For configuration instructions, click the help button ? above.


Use Identity Provider for



- Managing administrator access
- Gateway policy and logs

Data required by the SAML Identity Provider

Enter the following data in the provider's website:

Identifier (Entity ID): 

Reply URL: 

 In your Identity Provider, configure attribute mapping as well 

Data received from the SAML Identity Provider


Enter data for the fields below based on your provider data:

- Import Metadata File: *
- Insert Manually

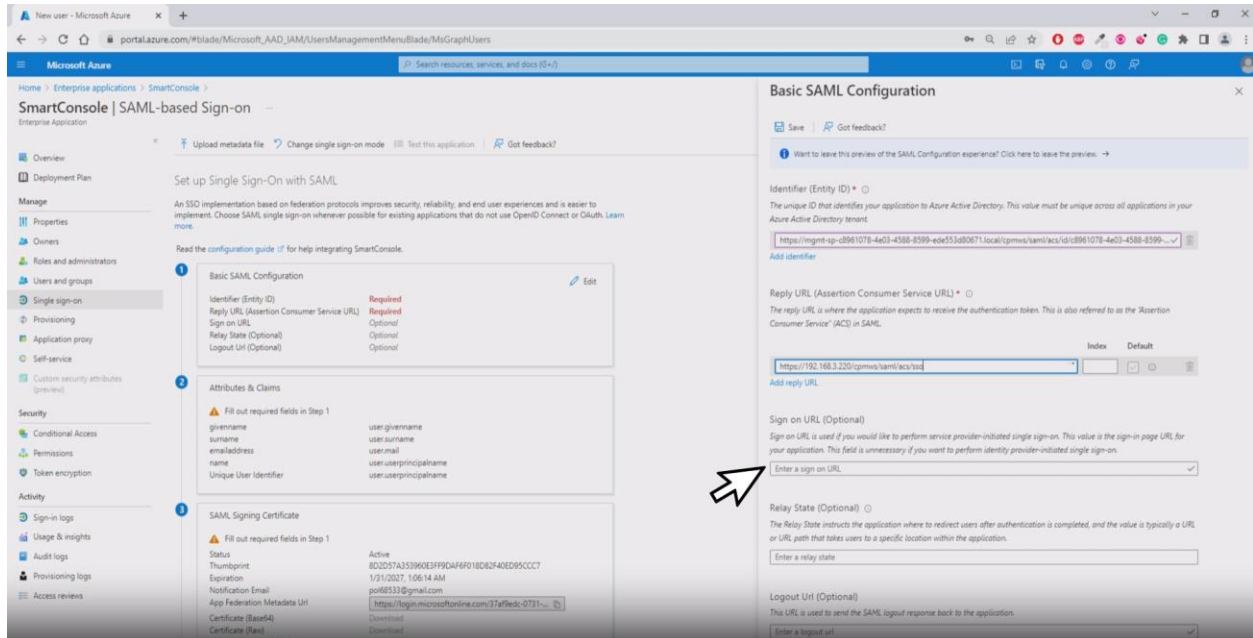
Identifier (Entity ID):

Login URL:

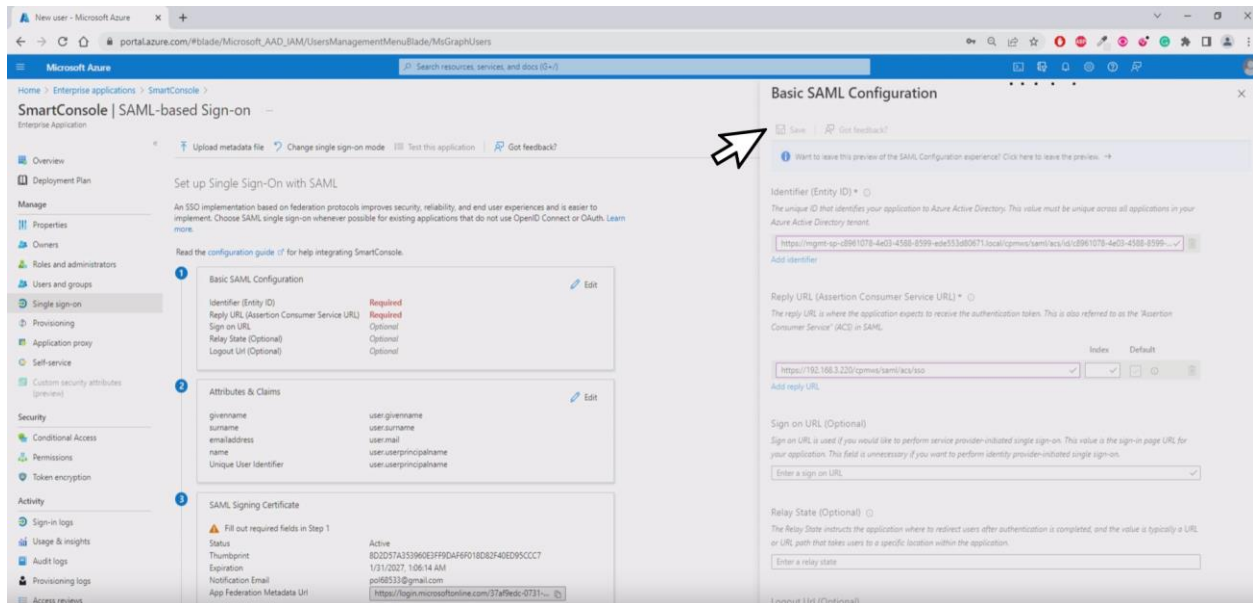
Certificate File:

 Add Tag

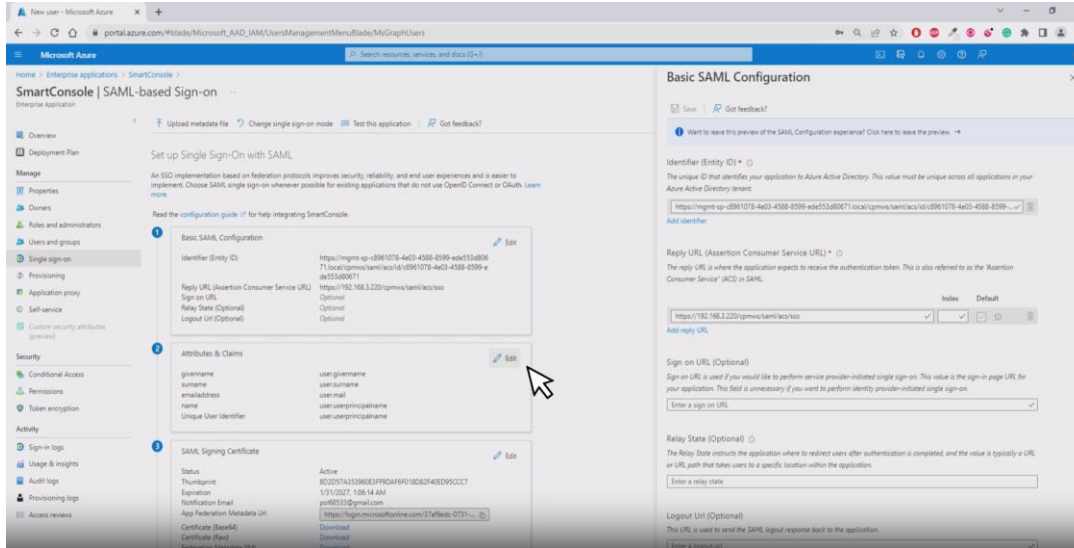
20. Volte a console do portal azure e cole as informações copiadas em seus respectivos campos “Identifier Entity ID” e “Reply URL”



21. Clique em “Save”



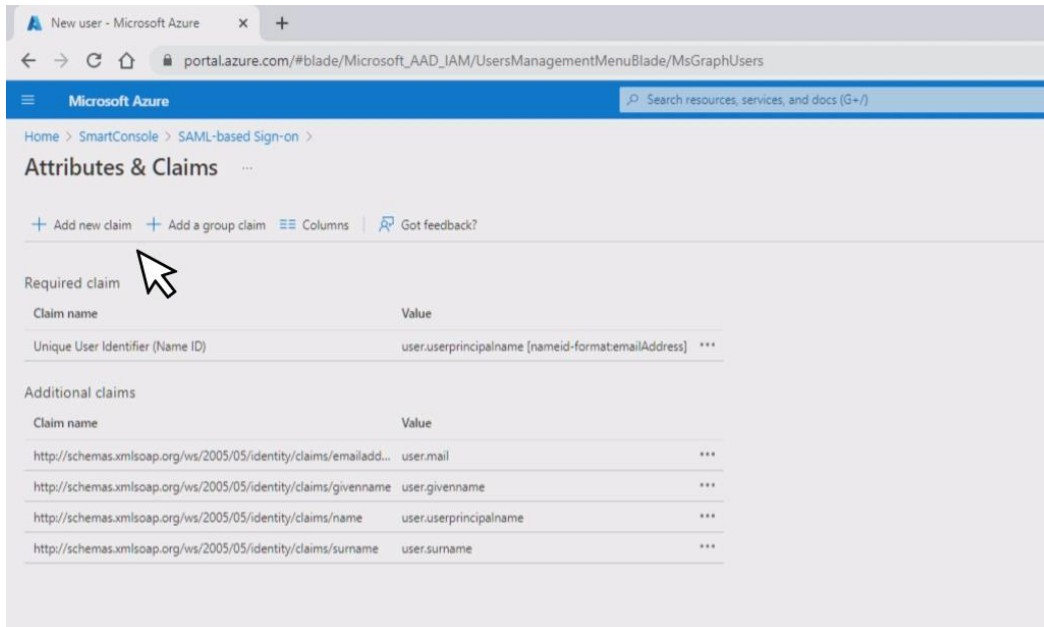
22. Clique em Editar “Attributes & Claims”



The screenshot shows the 'Basic SAML Configuration' page in the Microsoft Azure portal. The left sidebar contains navigation options like Overview, Deployment Plan, Manage, Properties, and Security. The main content area is titled 'SmartConsole | SAML-based Sign-on'. It includes a 'Basic SAML Configuration' section with fields for Identifier (Entity ID), Reply URL, and Sign-on URL. Below this is the 'Attributes & Claims' section, which is highlighted with a mouse cursor pointing to an 'Edit' button. The 'Attributes & Claims' section contains a table with columns for 'Claim name' and 'Value'.

Claim name	Value
givenname	user.givenname
surname	user.surname
emailaddress	user.email
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

23. Clique em “Add new Claim”

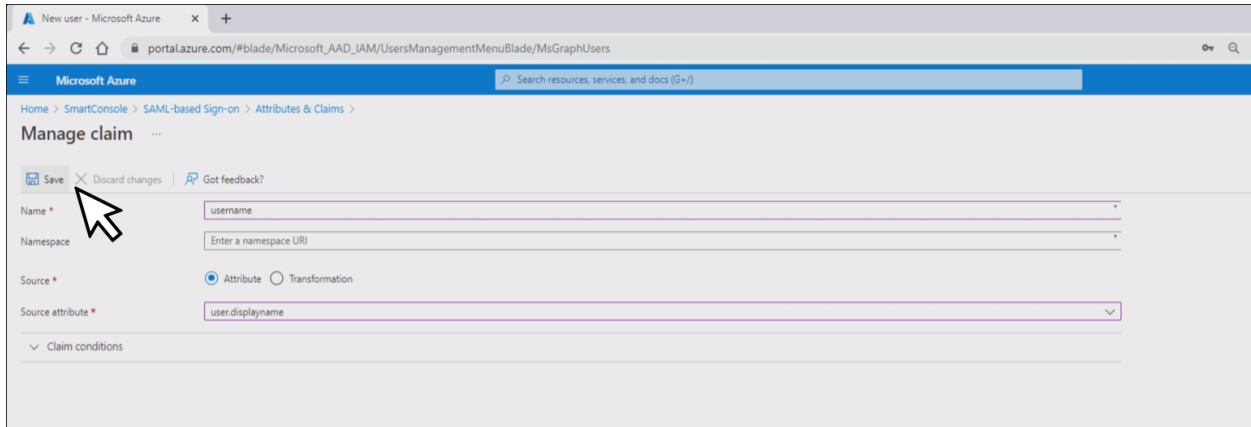


The screenshot shows the 'Attributes & Claims' page in the Microsoft Azure portal. The page title is 'Attributes & Claims'. Below the title, there are buttons for '+ Add new claim', '+ Add a group claim', 'Columns', and 'Got feedback?'. A mouse cursor is pointing to the '+ Add new claim' button. Below these buttons, there are two sections: 'Required claim' and 'Additional claims'. The 'Required claim' section contains a table with columns for 'Claim name' and 'Value'. The 'Additional claims' section contains a table with columns for 'Claim name' and 'Value'.

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-formatemailAddress] ***

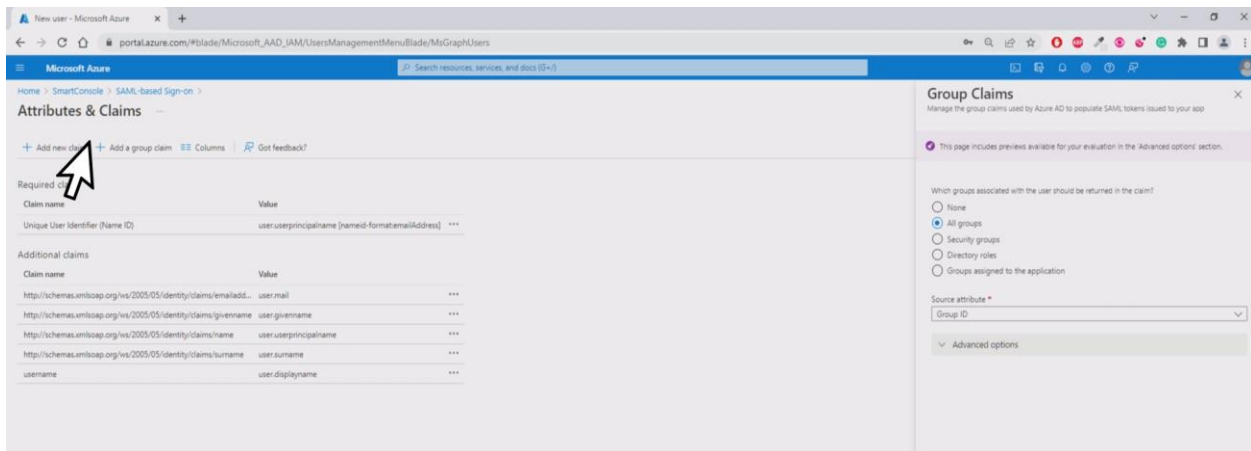
Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname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

24. Em name digite “username” em source selecione “attribute” e source attribute selecione “user.displayname” e clique em salvar



Microsoft Azure portal screenshot showing the 'Manage claim' configuration page. The 'Name' field is set to 'username'. The 'Source' is set to 'Attribute'. The 'Source attribute' is set to 'user.displayname'. A mouse cursor is pointing at the 'Save' button.

25. Clique em “add a group claim”

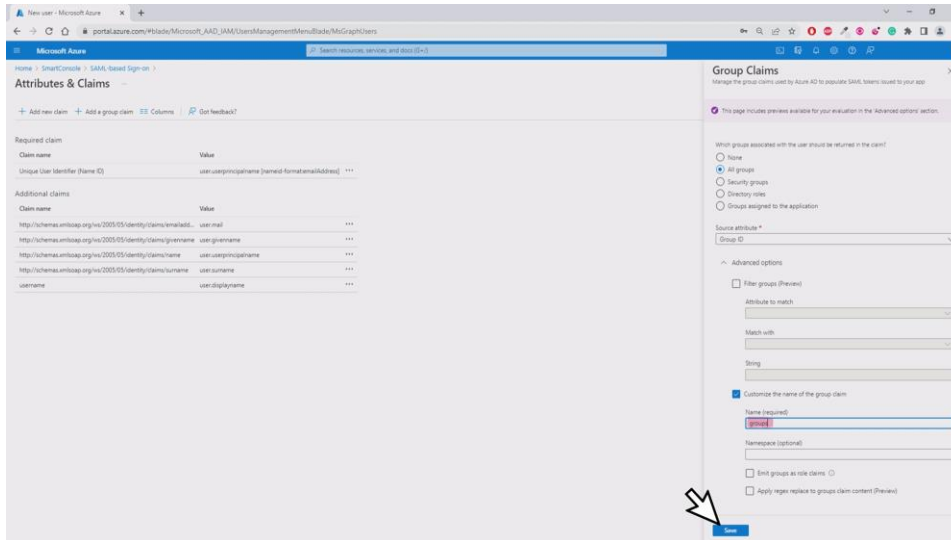


Microsoft Azure portal screenshot showing the 'Attributes & Claims' configuration page. The 'Add a group claim' button is highlighted with a mouse cursor. The 'Group Claims' panel on the right is visible, showing options for which groups should be returned in the claim.

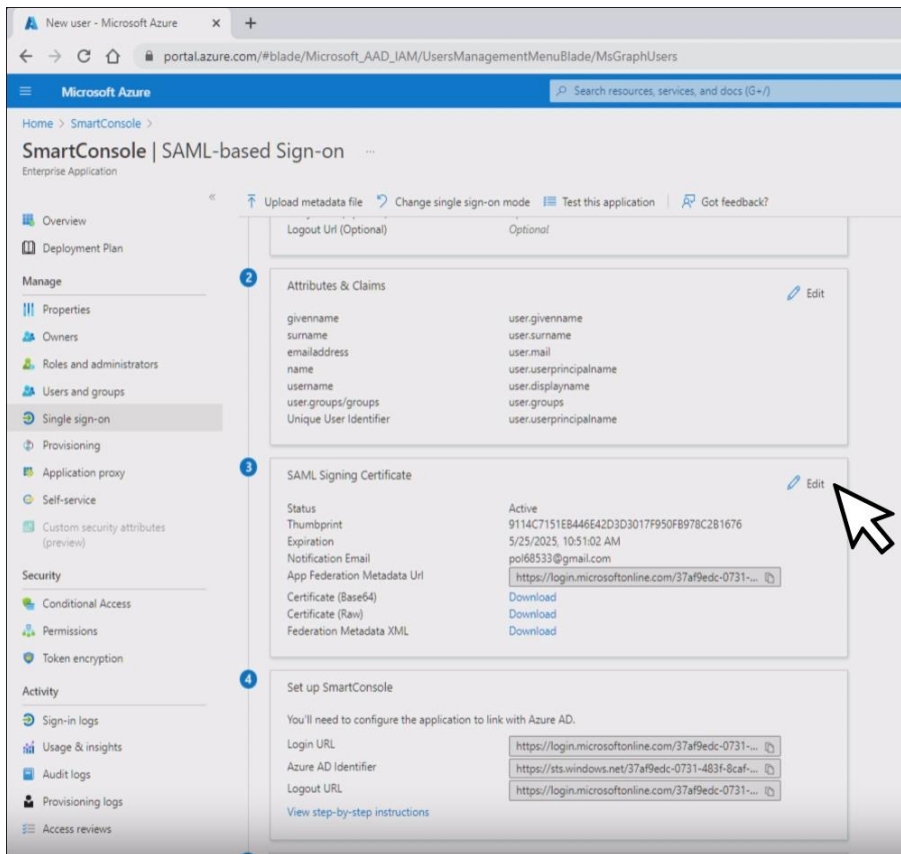
Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname (named-formatemailaddress) ***

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	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 ***
username	user.displayname ***

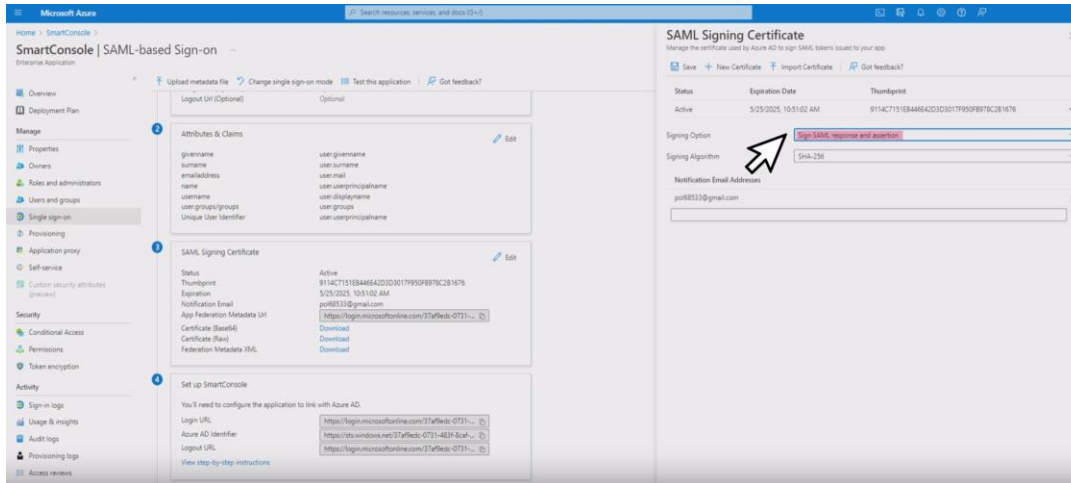
26. Selecione “All Groups” e selecione “Customize the name of the group claim” e digite o nome “groups”



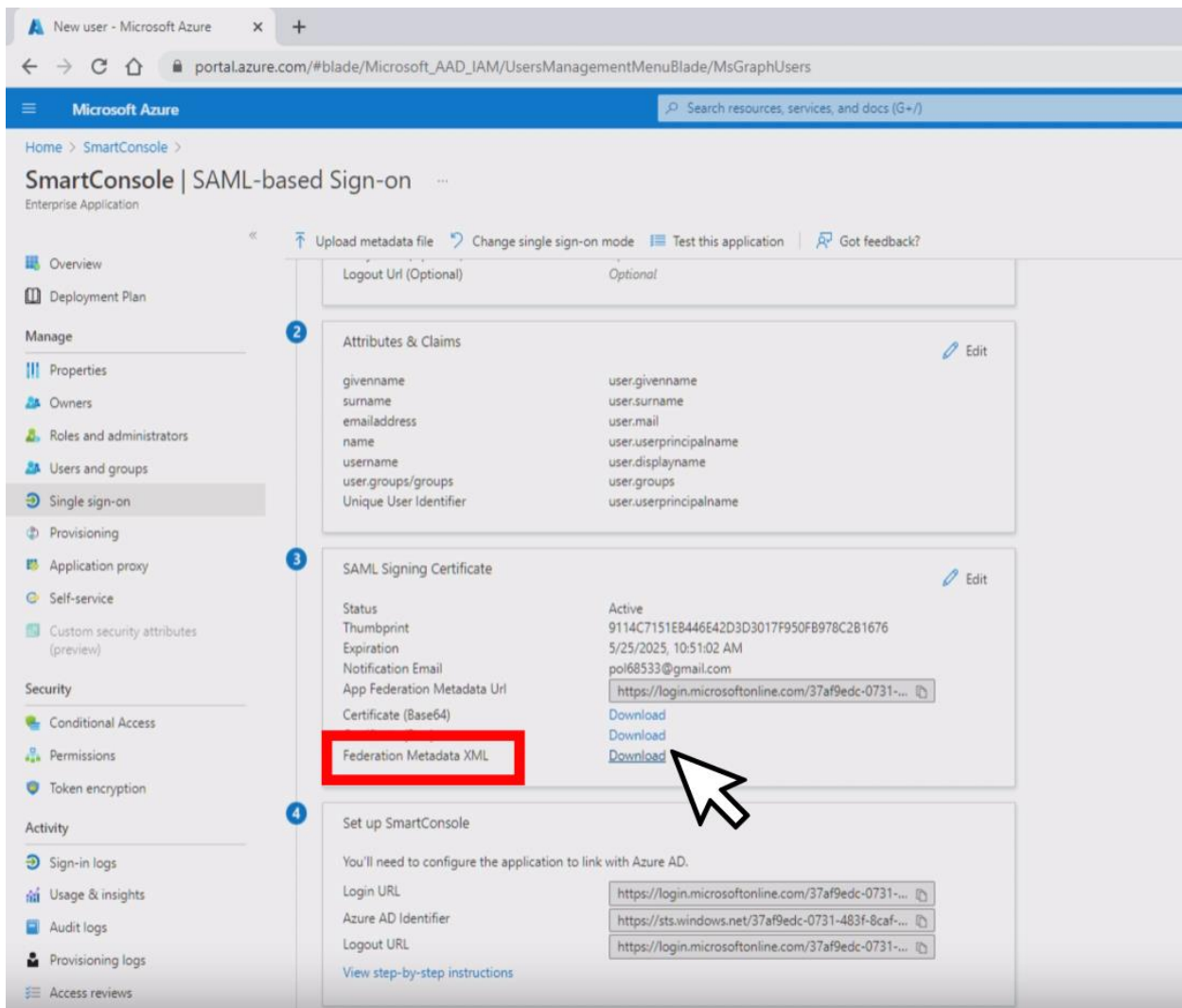
27. Clique em editar “SAML Sign Certificate”



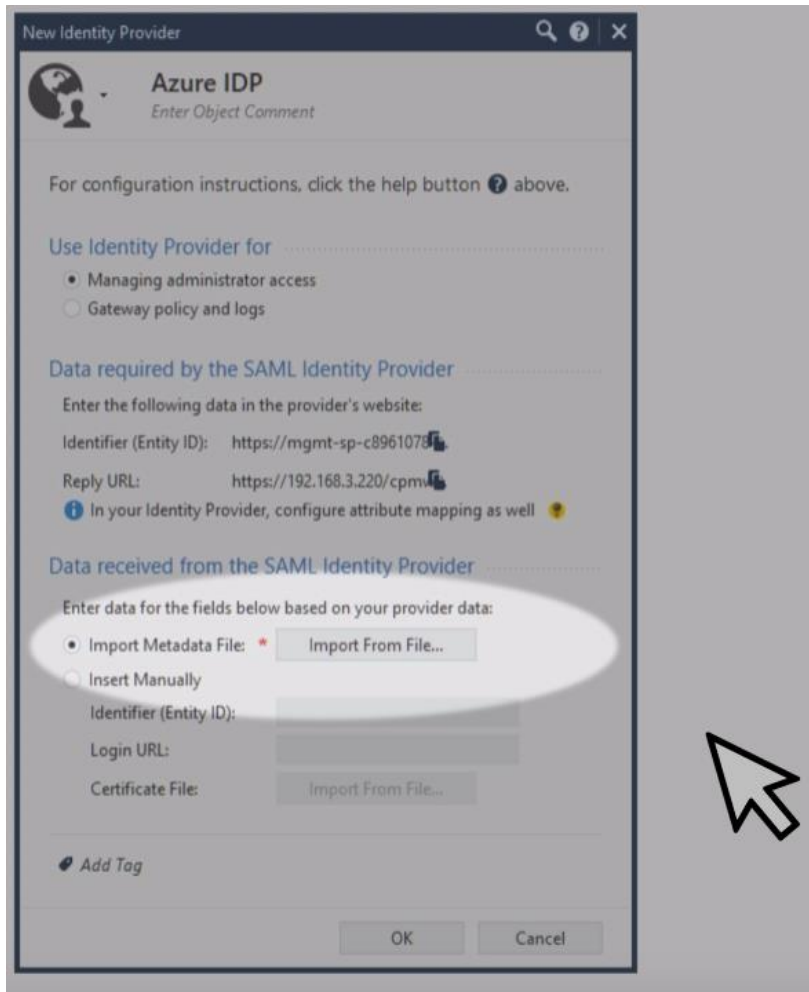
28. Em Signing option selecione “Sign SAML response and assertion” e salve a configuração



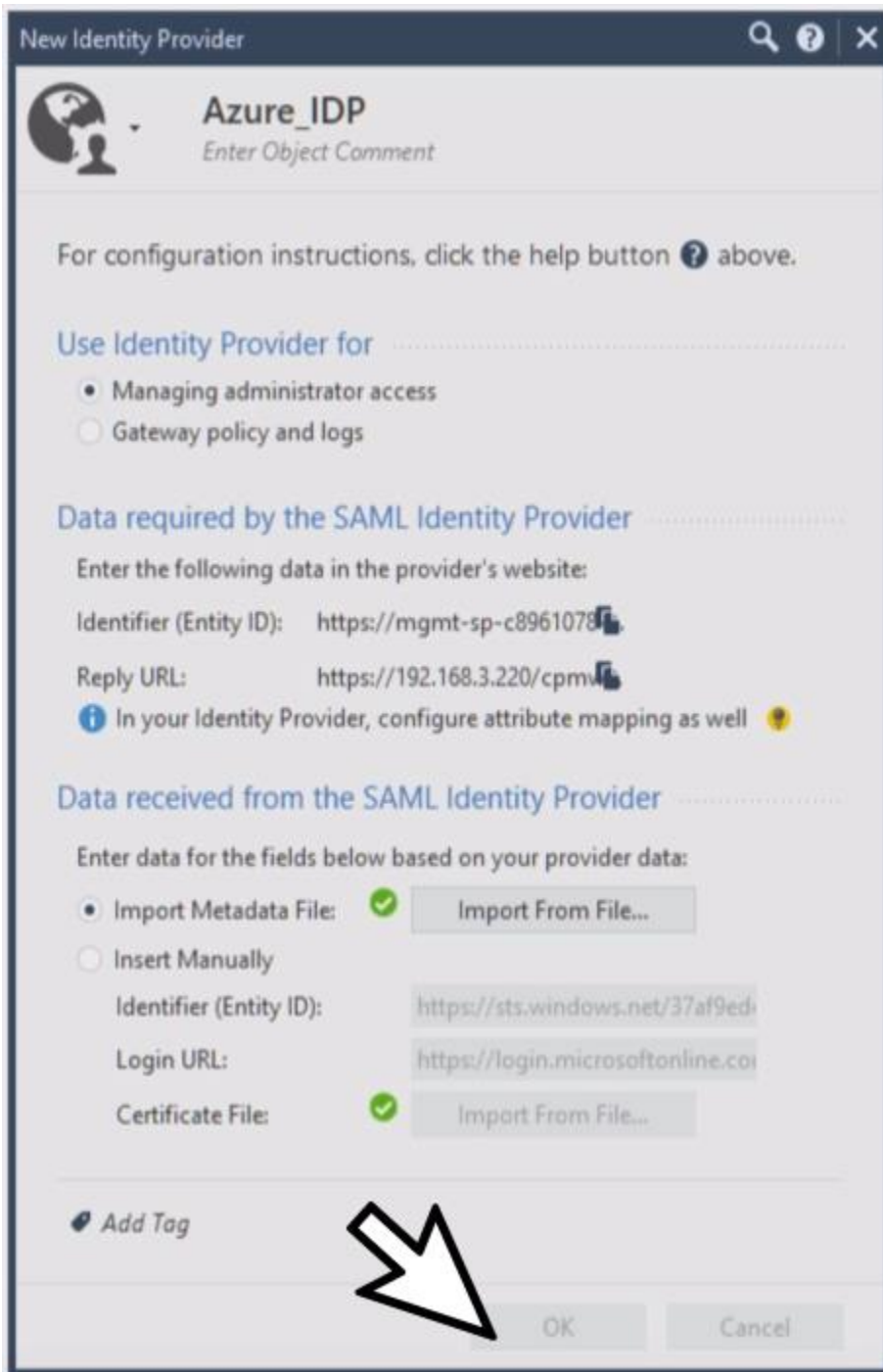
29. Voltando na tela de single sign-on faça o download do “Federation Metadata XML”



30. Volte ao Check Point no objeto do novo IDP e importe o arquivo que foi efetuado o download

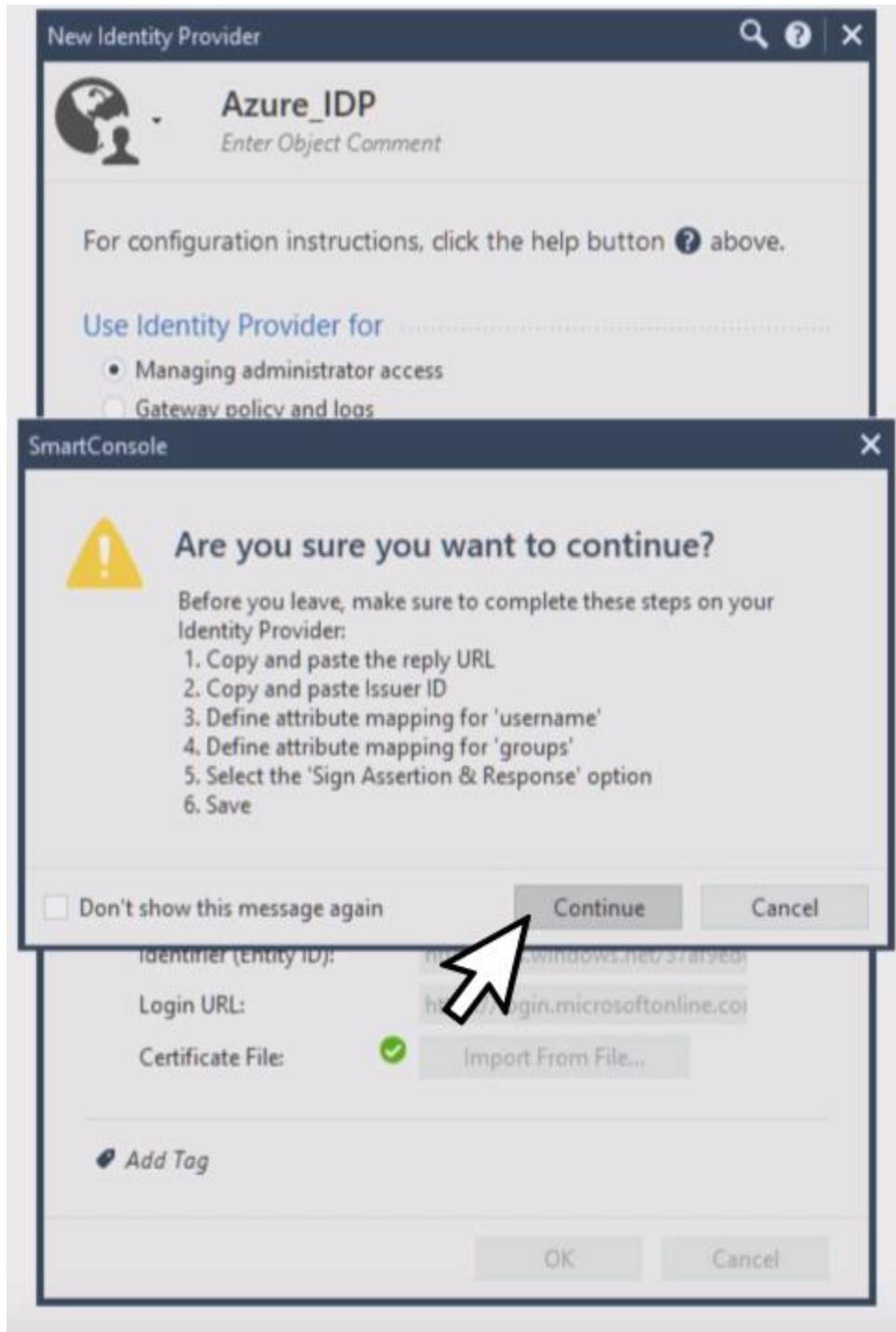


31. Após importar clique em OK

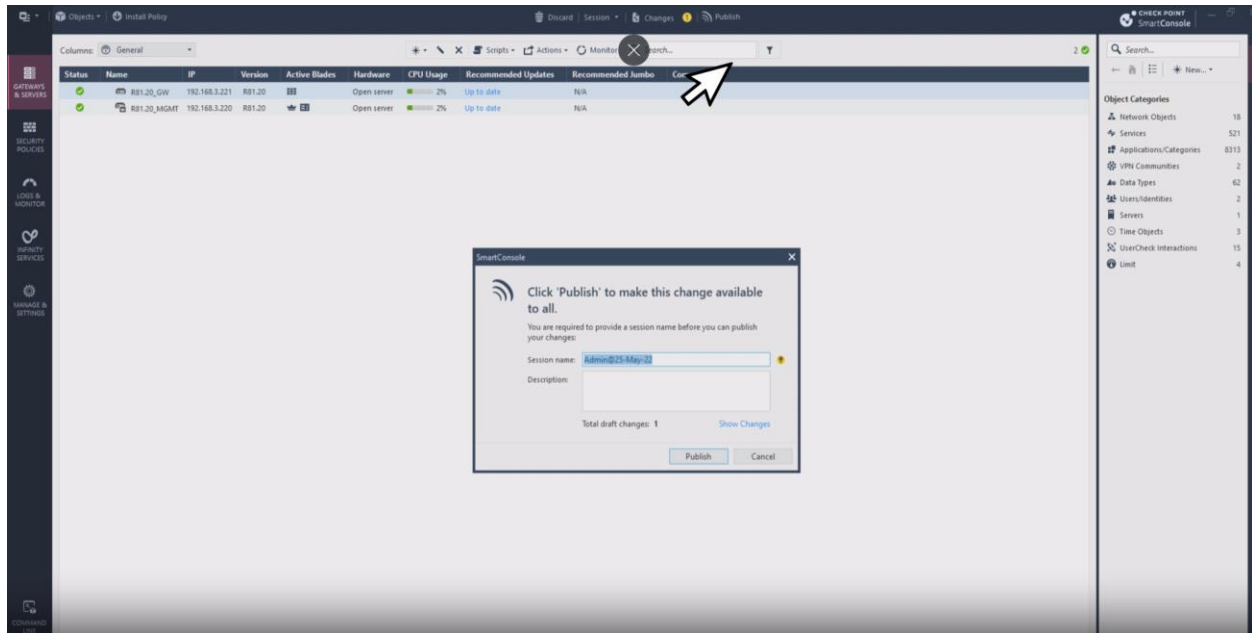


The screenshot shows a 'New Identity Provider' dialog box for 'Azure_IDP'. The window title is 'New Identity Provider'. The main heading is 'Azure_IDP' with a subtext 'Enter Object Comment'. Below this, there is a help message: 'For configuration instructions, click the help button ? above.' The 'Use Identity Provider for' section has two radio buttons: 'Managing administrator access' (selected) and 'Gateway policy and logs'. The 'Data required by the SAML Identity Provider' section includes fields for 'Identifier (Entity ID): https://mgmt-sp-c8961078' and 'Reply URL: https://192.168.3.220/cpmv'. A note below these fields says 'In your Identity Provider, configure attribute mapping as well'. The 'Data received from the SAML Identity Provider' section has a radio button for 'Import Metadata File' (selected) with a green checkmark and an 'Import From File...' button. Below this are fields for 'Identifier (Entity ID): https://sts.windows.net/37af9ed', 'Login URL: https://login.microsoftonline.coi', and 'Certificate File' (selected with a green checkmark) with an 'Import From File...' button. At the bottom left, there is an 'Add Tag' button. At the bottom right, there are 'OK' and 'Cancel' buttons. A large white mouse cursor arrow is pointing at the 'OK' button.

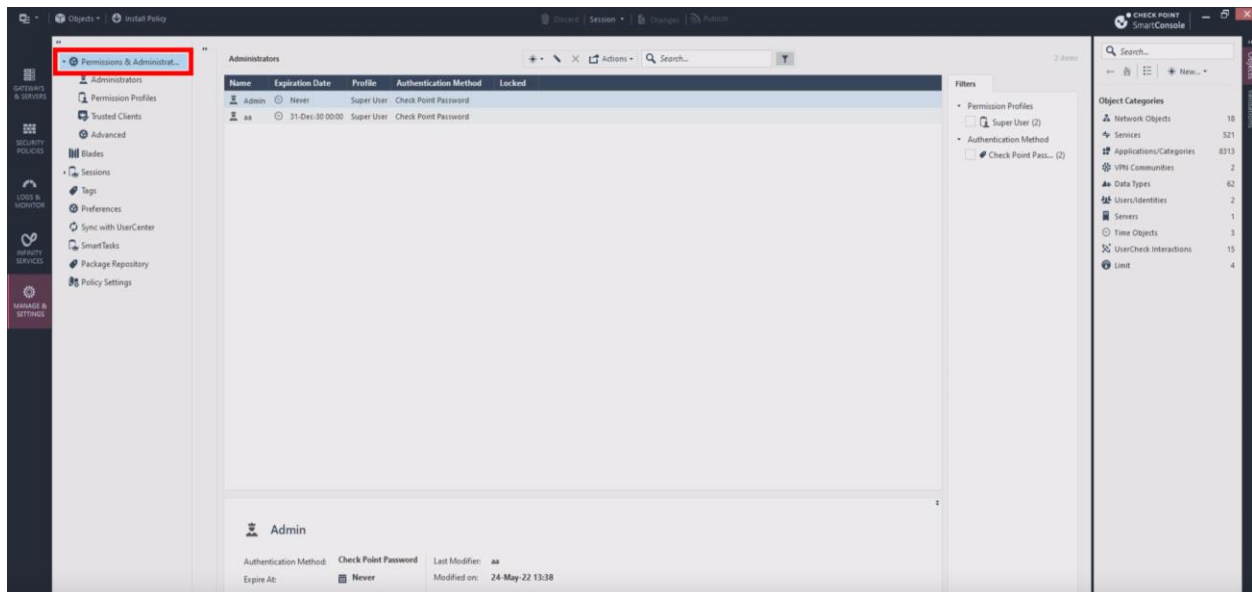
32. Você receberá alguns alertas sobre as configurações que devem ser feitas no provedor de identidade que já efetuamos clique em “Continue”



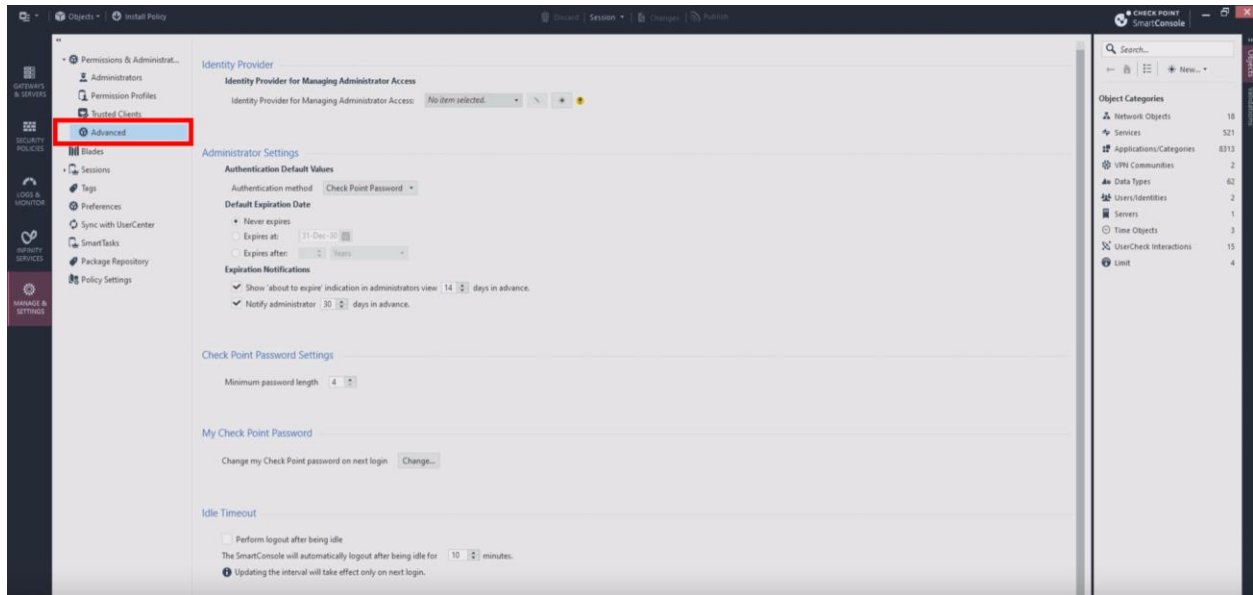
33. Clique em “publish”



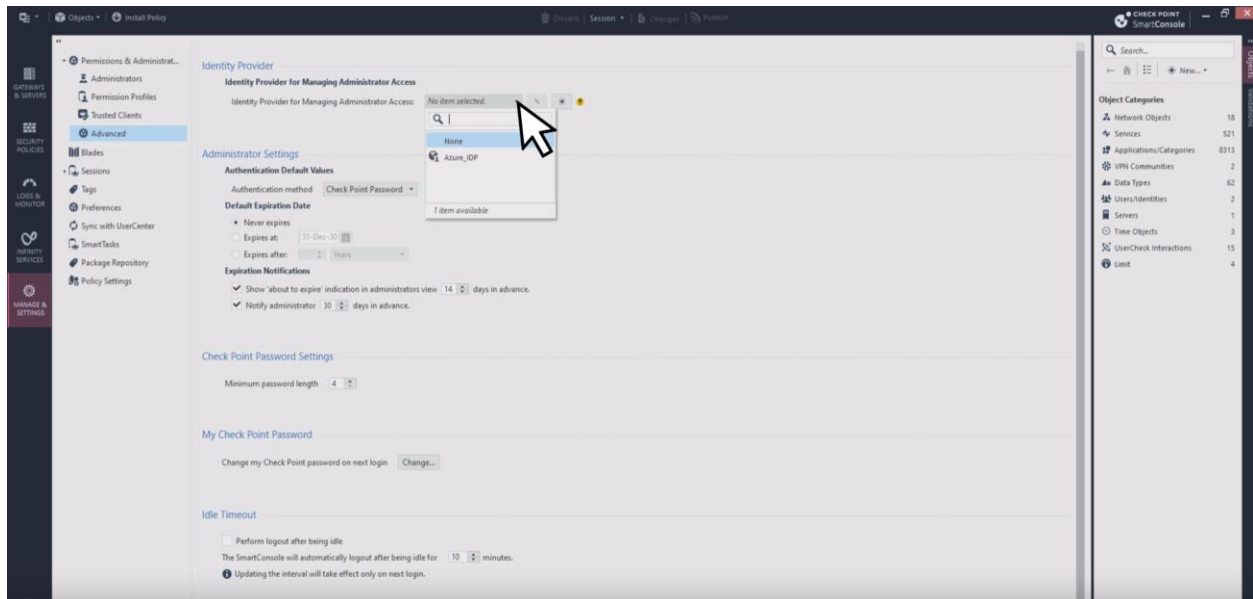
34. Va até “Permissions & Administrators”



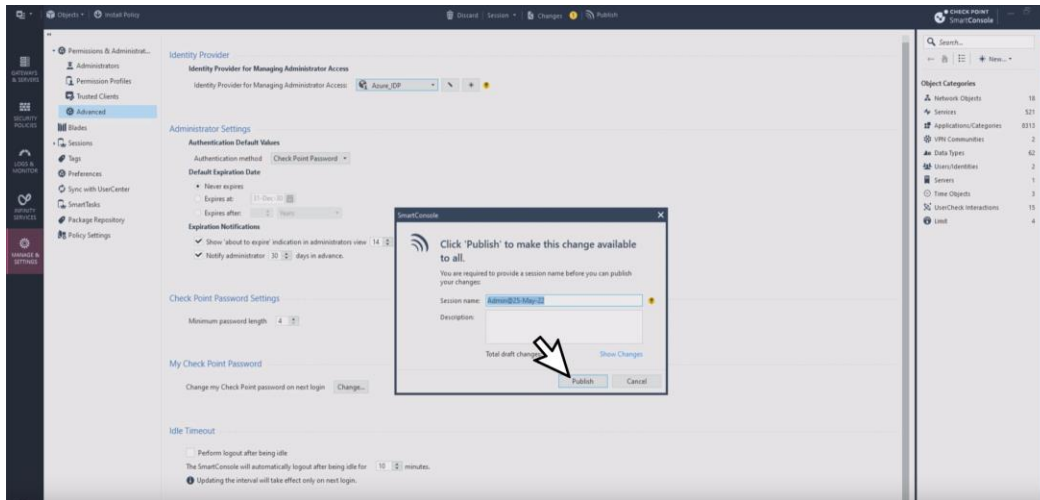
35. Vá até a guia “Advanced”



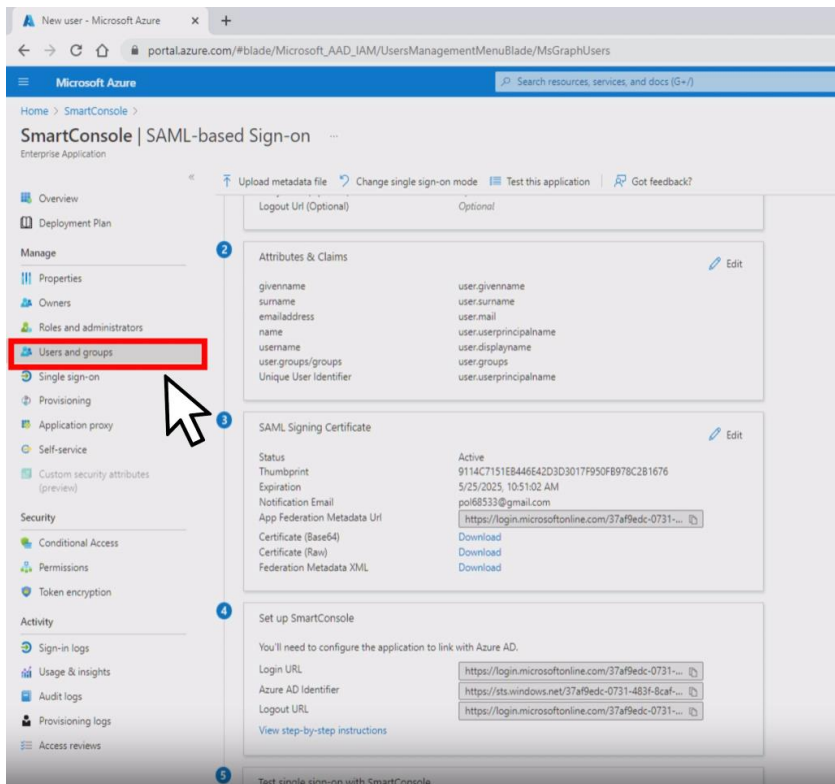
36. Em “Identity Provider” selecione o objeto que acabamos de criar em nosso caso “Azure_IDP”



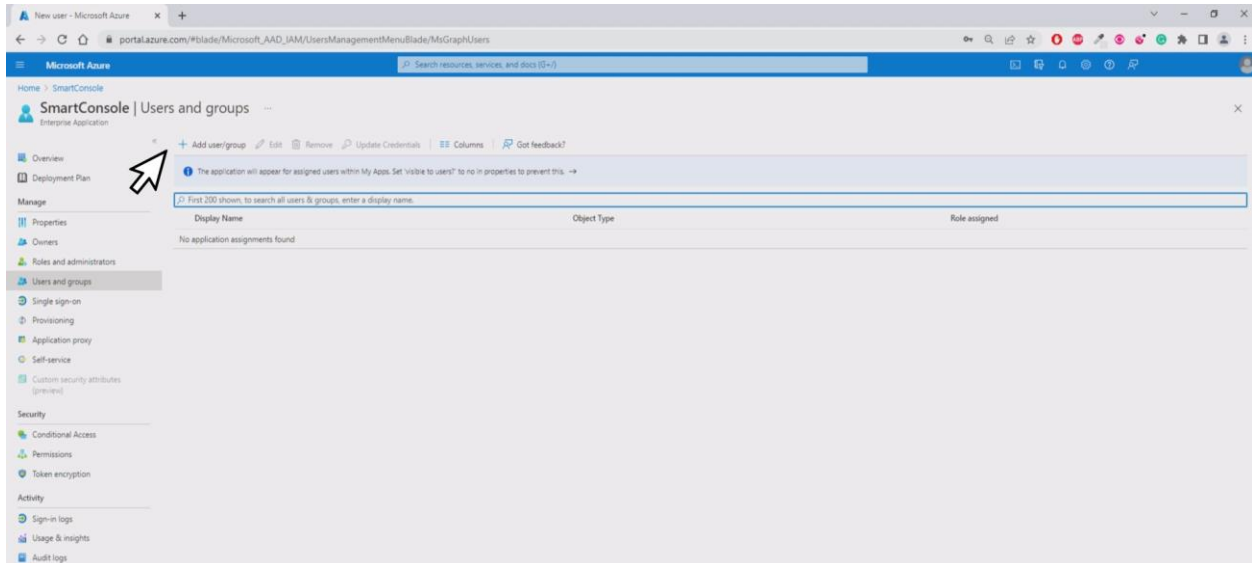
37. Publique a sessão novamente clicando em “Publish”



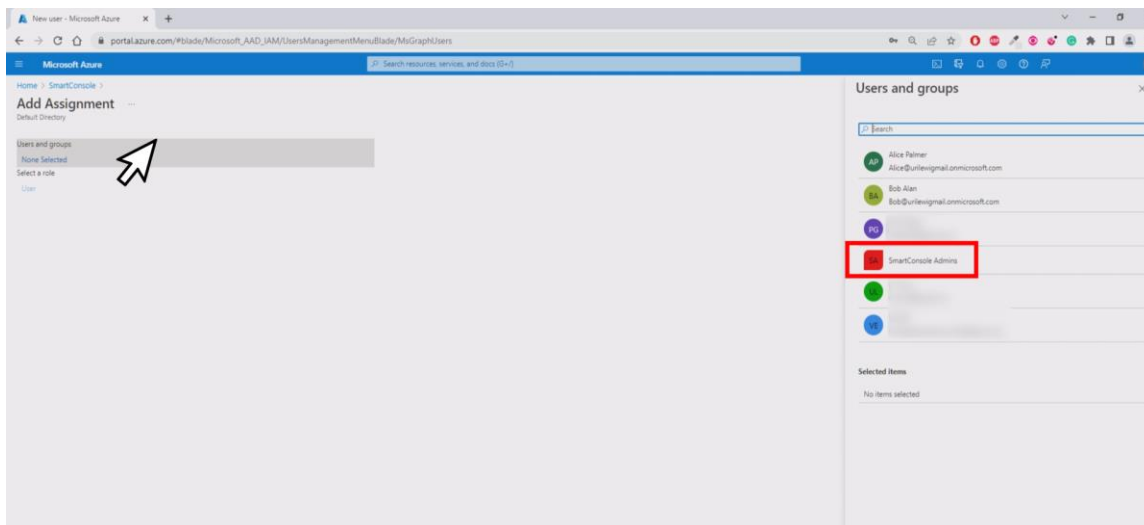
38. Volte ao portal Azure para dar o devido permissionamento dentro da aplicação criada “SmartConsole” vá até “Users and Groups”



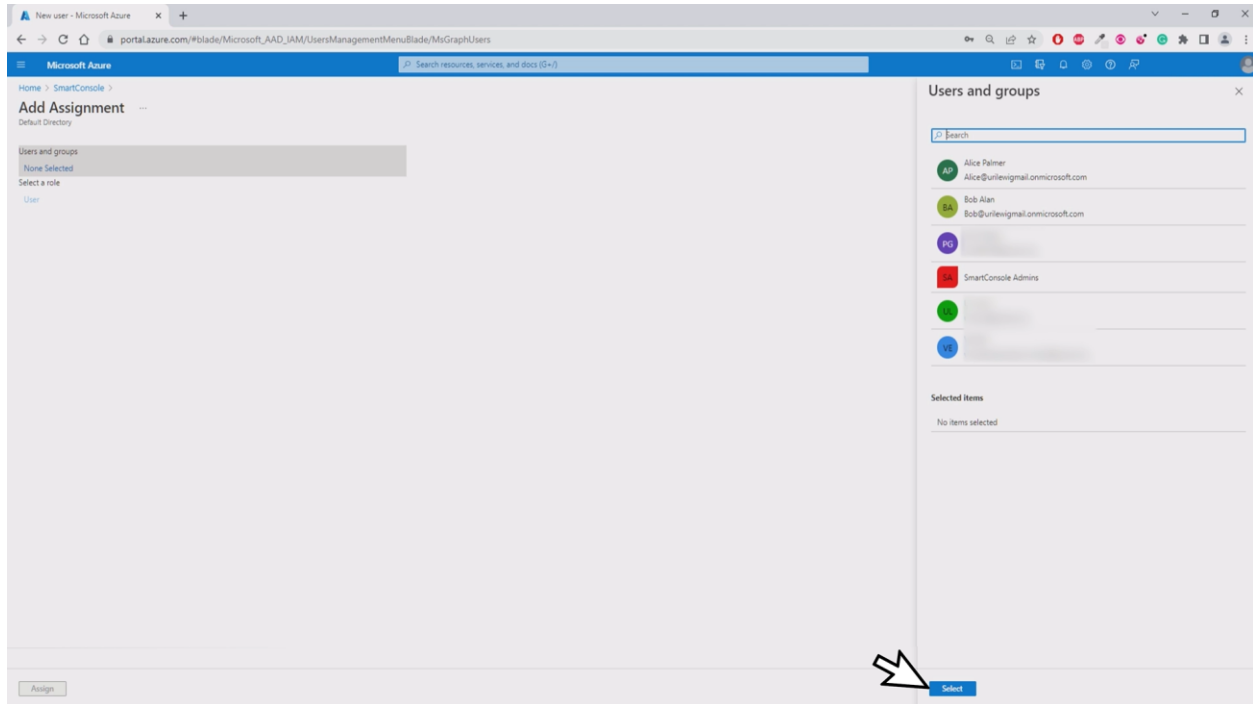
39. Clique em “Add user/group”



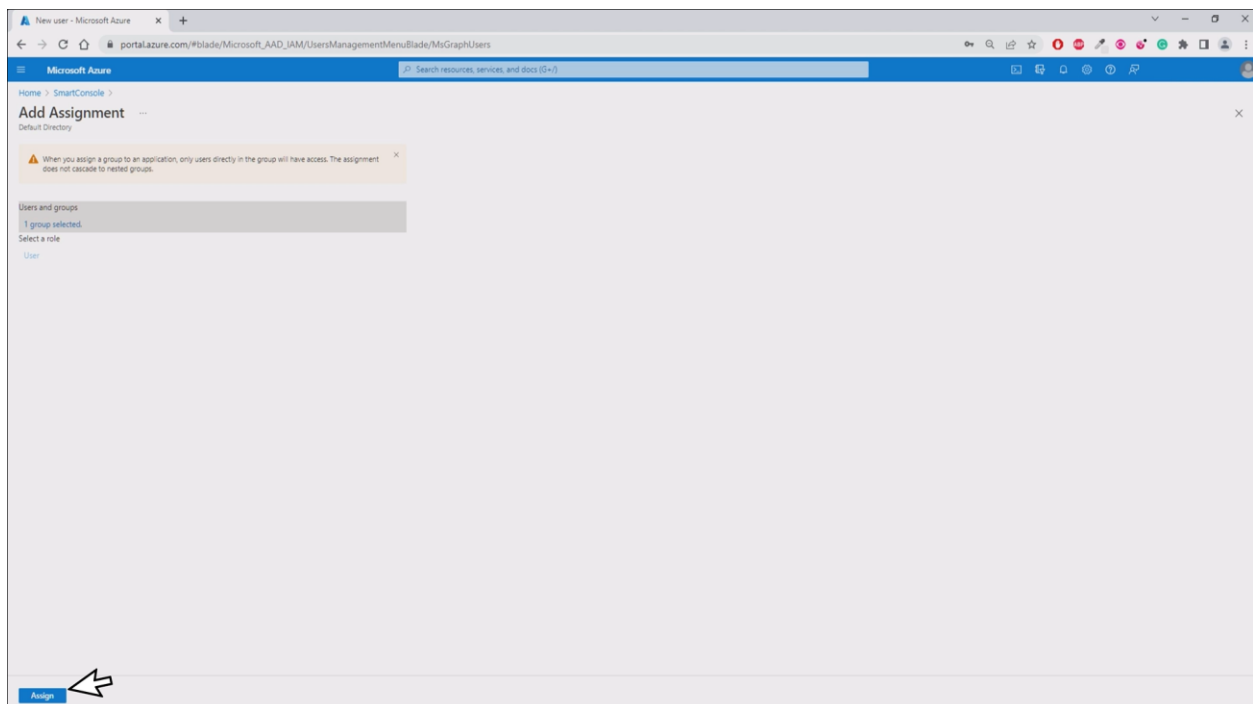
40. Selecione o grupo que criamos “SmartConsole Admins” que contem Alice Palmer e Bob Alan



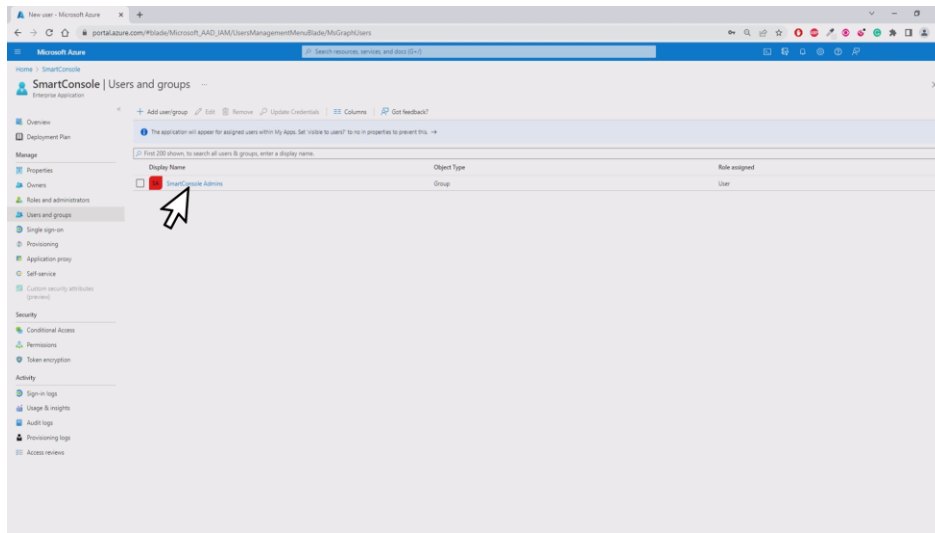
41. Clique em “Select”



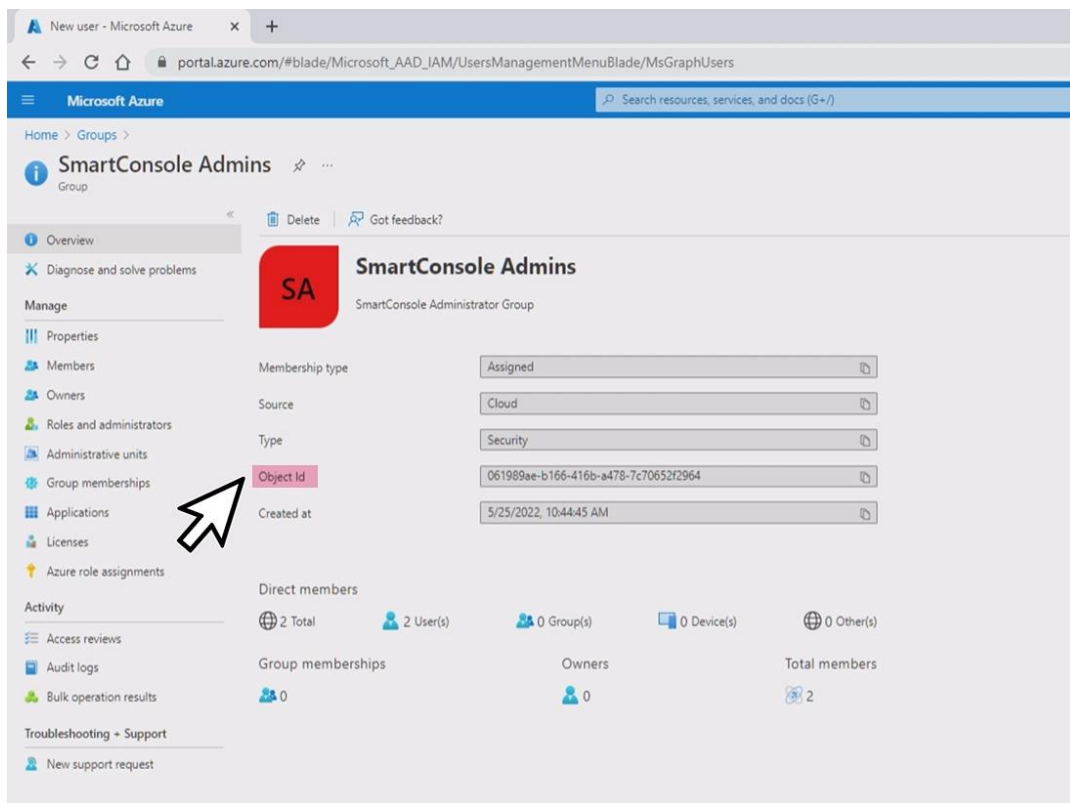
42. Clique em “Assign”



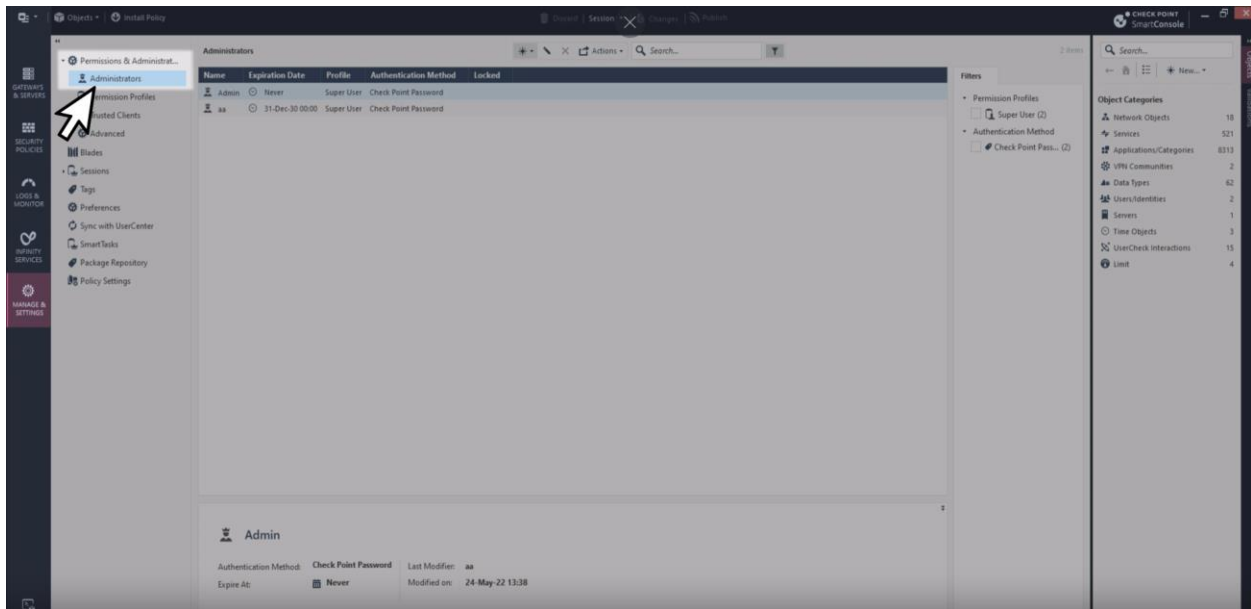
43. Após isso seria possível verificar usuários e grupos com este acesso



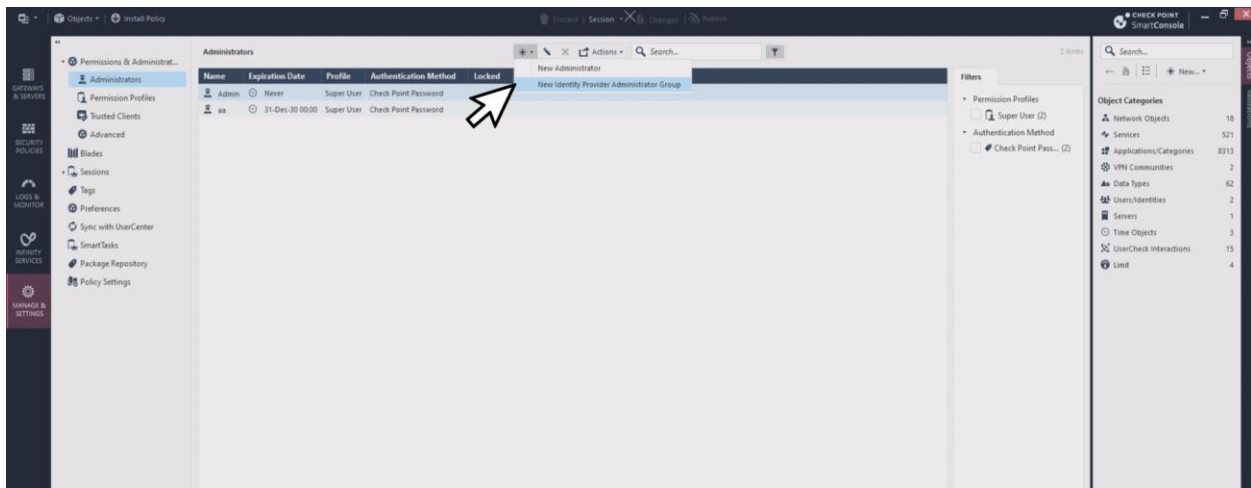
44. Clique em “Overview” dentro da grupo “SmartConsole Admins” e copie o “Object ID” deste grupo



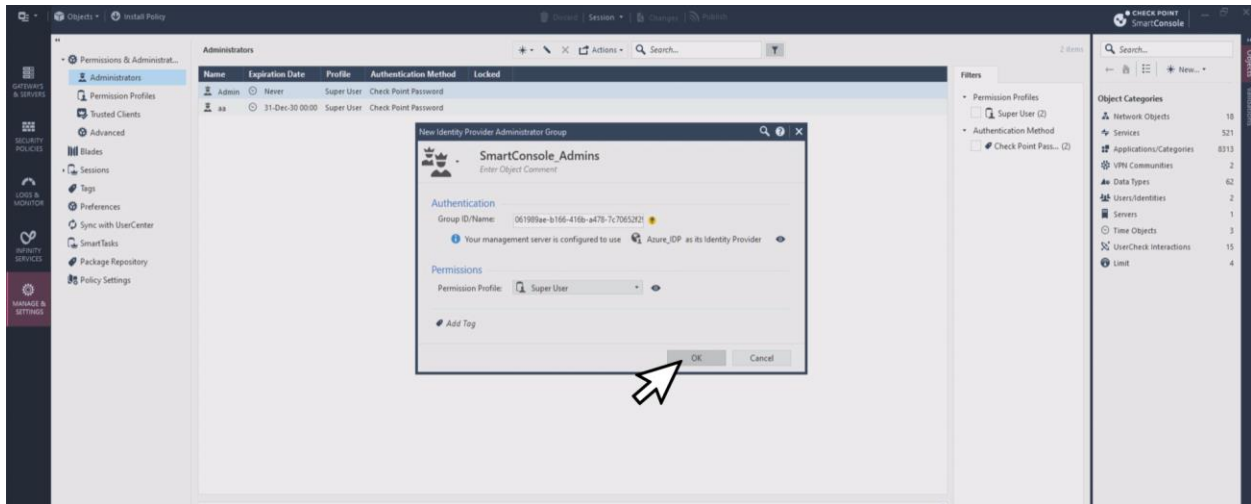
45. Volte para a console Check Point em “Administrators”



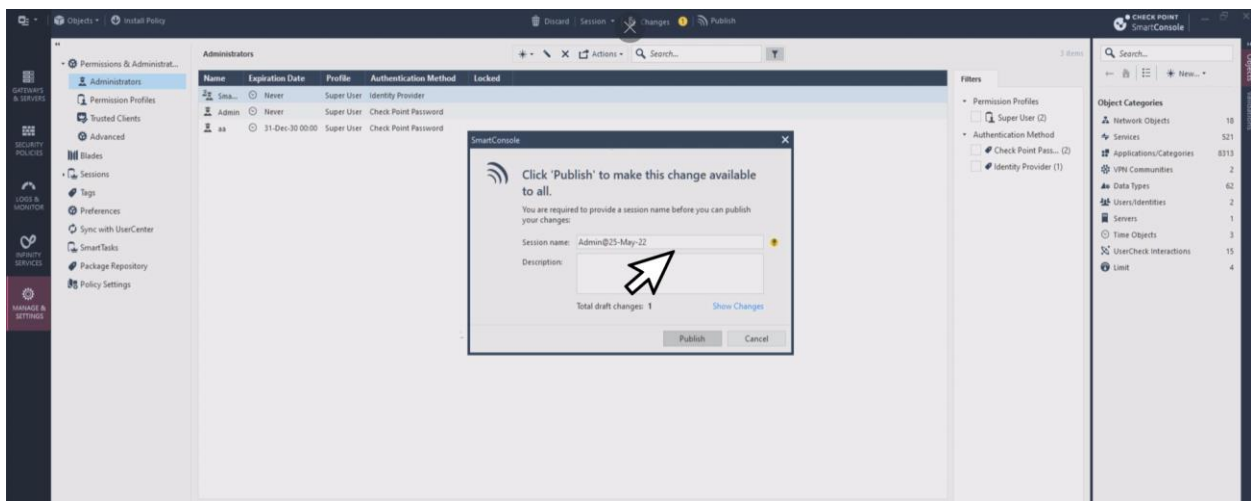
46. Clique em criar “New Identity Provider Administrator Group”



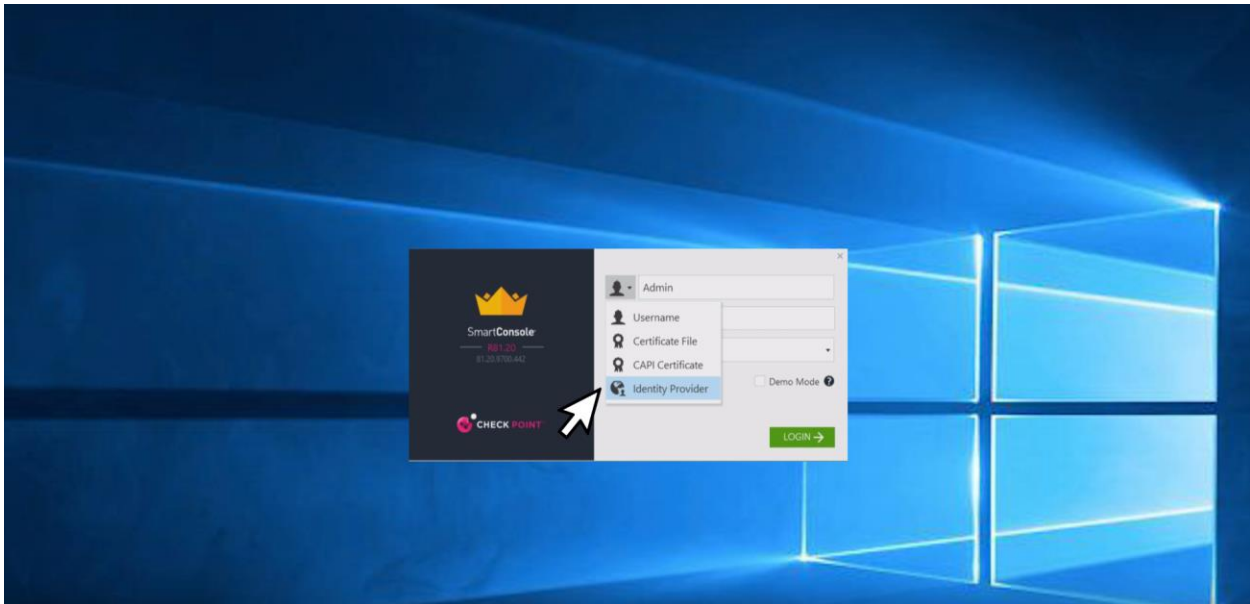
47. Digite o Nome para o grupo , cole o “object ID” copiado do portal azure e selecione a permissão em nosso caso super user



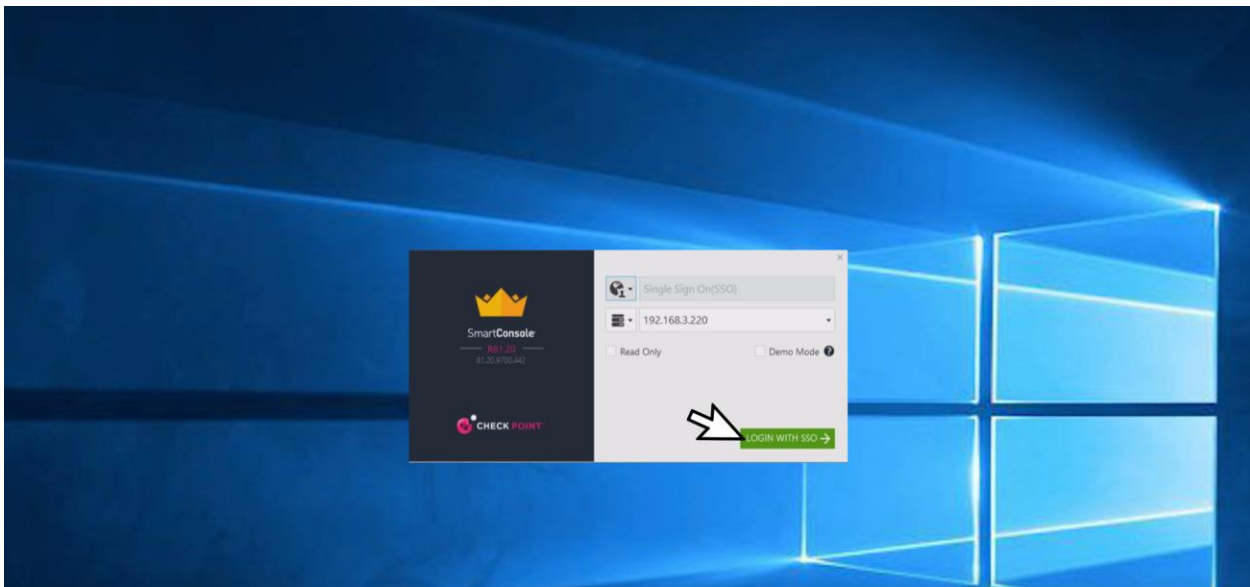
48. Publique a sessão em “Publish”



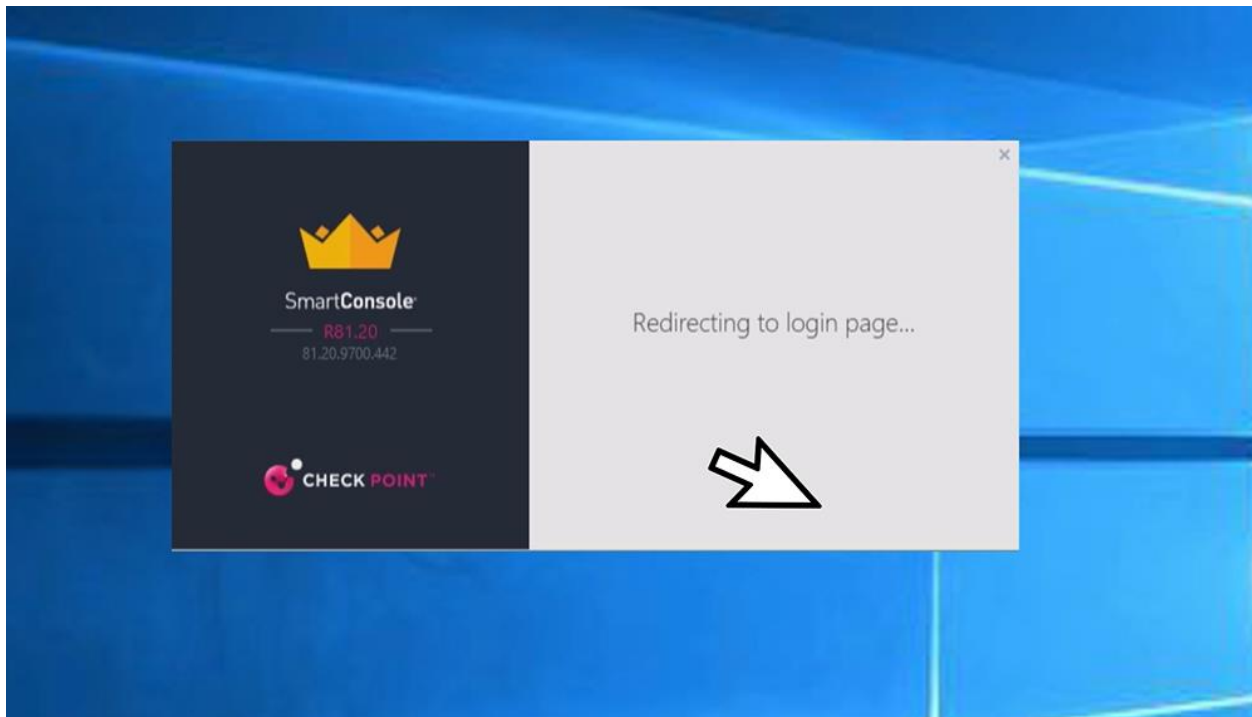
49. Para efetuar o login selecione “Identity Provider” na tela de autenticação



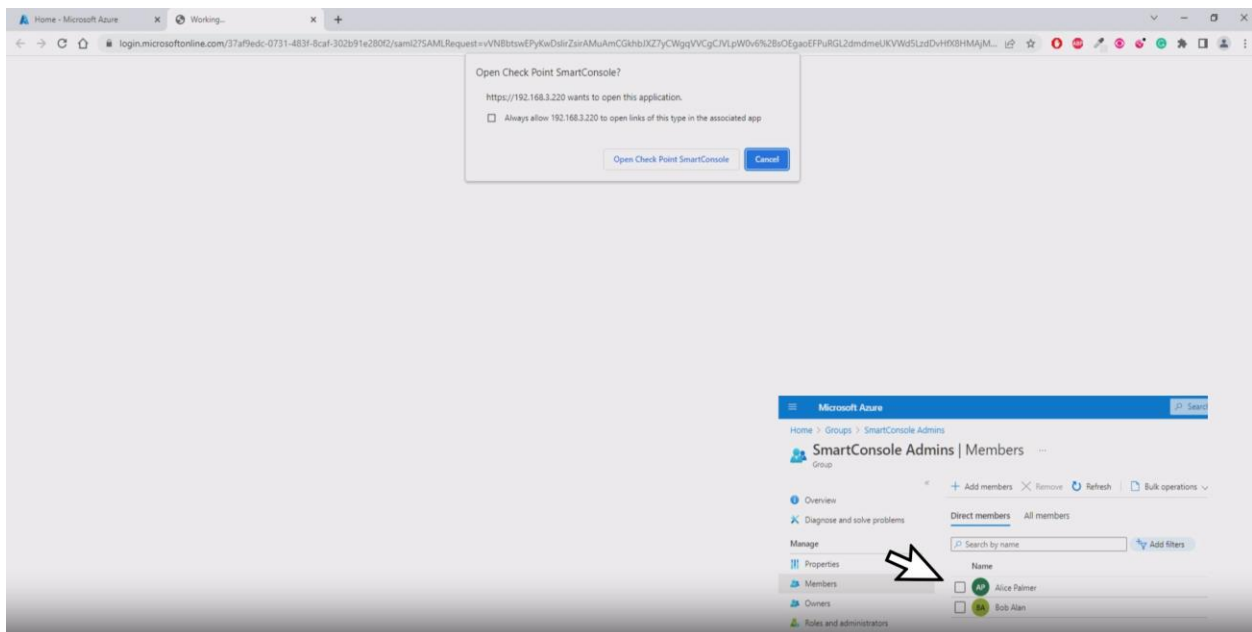
50. Digite o IP da SMS e clique em “LOGIN WITH SSO”



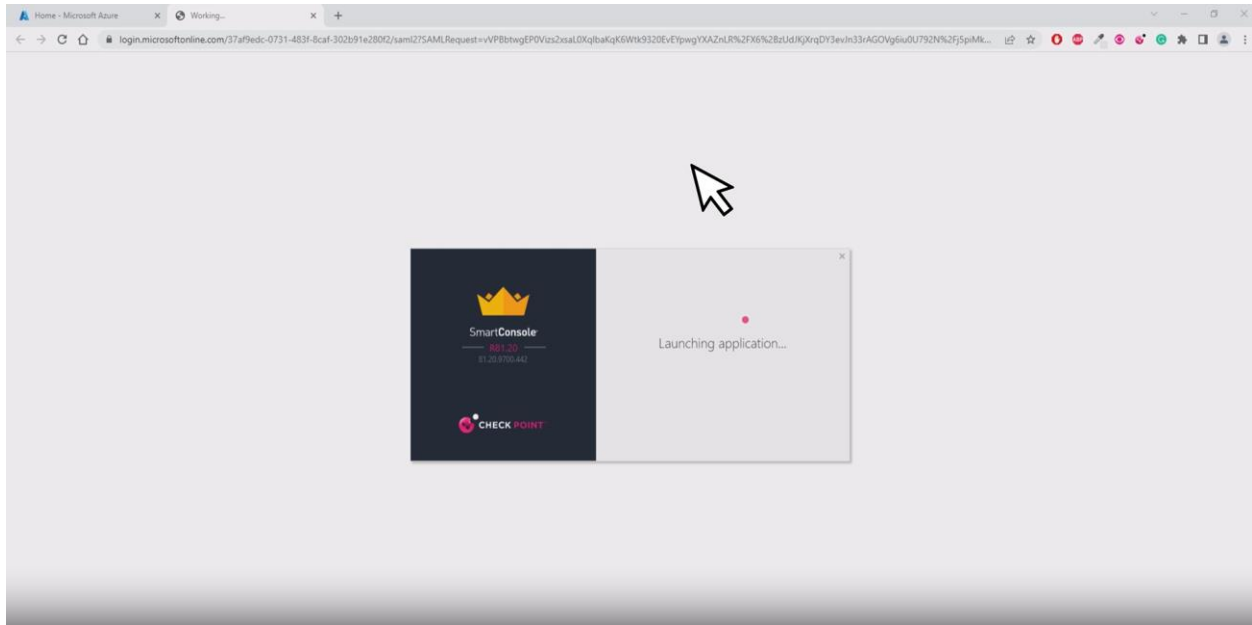
51. Você será redirecionado para uma tela de login



52. Após a autenticação pelo browser se você estiver contido no grupo “SmartConsole Admins” você será permitido a acessar a SMS via SSO



53. Abrindo a console após a autenticação



54. Através dos Logs é possível confirmar a autenticação correta e autorizada.

