



Azure AD SSO for Web console UI login

Key takeaway

- Native Azure AD integration for Web console UI login
- How to configure Azure and Firewall
- Troubleshooting & FAQs
- Security best practices

Customer problems prior to v19.5



Cannot integrate natively
with Azure AD



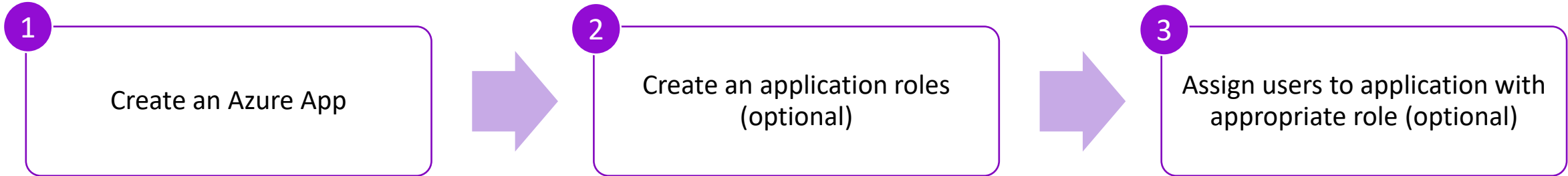
Difficult to manage multiple
administrators dynamically (via
Idp)



Cannot have centralized
security and access controls (
password policy, MFA, etc.)

How to configure

Azure Configuration



Display name : demoOAuth
Application (client) ID : 9108b000-1120-9203-5ecf05d05-
Object ID : 63c6206-425a-be94-c198beb-
Directory (tenant) ID : 605107e-c94e-180-e5-4f421-
Supported account types : My organization only

 Select **Web** App as option (Single Tenant)

App roles

App roles are custom roles to assign permissions to use as permissions during authorization.

[How do I assign App roles](#)


Display name	Description
CaptivePortal	captive portal
AdminRole	Admin role

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

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

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

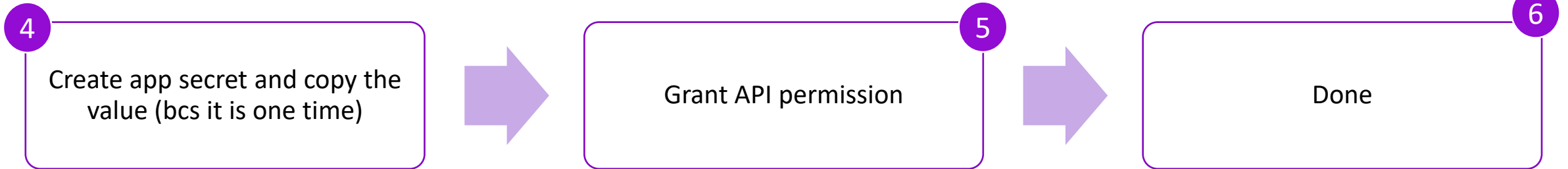
Display Name	Object Type	Role assigned
<input type="checkbox"/> AP Alok Patel	User	CaptivePortal
<input type="checkbox"/> DE demoOAuth	ServicePrincipal	AdminRole
<input type="checkbox"/> JA Jubin Aghara	User	AdminRole

 **Security best practice – Enable the user assignment (see below).**

Assignment required? ⓘ


Yes **No**

Azure Configuration



+ New client secret			
Description	Expires	Value	Secret ID
ssso	2/19/2023	PAI*****	2bc70056-8853-42ec-a39f-b7a2b3bc864a

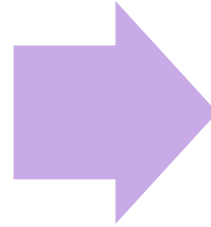
+ Add a permission <input checked="" type="checkbox"/> Grant admin consent for Default Directory		
API / Permissions name	Type	Description
Microsoft Graph (3)		
Group.Read.All	Delegated	Read all groups
User.Read	Delegated	Sign in and read user profile
User.Read.All	Delegated	Read all users' full profiles

 **Group permission is required only if a user is assigned to one or more group(s). If you don't set the API permission you will see 500 Internal Server Error due to Authorization Failure.**

Firewall configuration

1

Configure Azure AD SSO



2

Configure role mapping and profile you want to associate to Admin user

Servers Services **Groups** Users Multi-factor authentication Web authentication Guest users Clientless users STAS ...

Server type: Azure AD SSO
⚠ At present, you can use Azure AD authentication for administrator users only for signing in to the web admin console. User-based rules and policies, such as firewall rules and SD-WAN routes, don't work for users authenticated through Azure AD yet.

Server name *: Enter Server name

Application (client) ID *: Enter Application (client) ID ⓘ

Directory (tenant) ID *: admin ⓘ

Client secret *:

Redirect URI *: 172.16.16.16 ⓘ Use the current browser URL

Web admin console URL: <https://172.16.16.16:4444/webconsole/oauth2/callback> [Copy](#)

User portal URL: <https://172.16.16.16:4443/userportal/oauth2/callback> [Copy](#)

Role mapping ⓘ

User type * User Administrator

Identifier type	Value	Profile
roles	admin	Administrator

Note: groups and roles identifiers are group and role name respectively NOT uuid or oid of groups or roles.

Firewall configuration

3

Configure Admin Authentication Method
(Select SSO)

Administrator authentication methods

Set authentication methods same as firewall

Authentication server list

type to search...

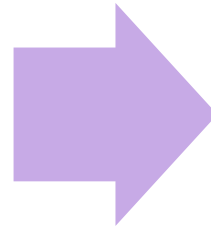
Local

Selected authentication server

Local

drag to change priority

Apply



4

Configure and Copy the return URI (from
firewall) and set this up in Azure AD

Redirect URI *

172.16.16.16

Use the current browser URL

Web admin console URL <https://172.16.16.16:4444/webconsole/oauth2/callback> [Copy](#)

Web

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (the URIs send in the request to the login server should match one listed here. Also referred to as

<https://172.16.16.16:4444/webconsole/oauth2/callback>

Add URI



Please note redirect URI is from where an admin is accessing the firewall – it can be public or private IP or domain. After successful authentication, Azure AD returns the ID/Access Token on this location.


Troubleshooting

- CLI

- /log/oauth_sso_webadmin.log

- Log viewer

- Admin module

	Time	Log comp	Status	Username	Src IP	Message	Message ID
 Admin	2022-08-23 11:51:04	GUI	Successful	live.com#agharajubin@gmail.com	172.16.16.250	User live.com#agharajubin@gmail.com logged in successfully to Web Admin Console through Azure AD SSO authentication mechanism	17507

FAQs

I am getting AADSTS50011 error from the Microsoft.

Please ensure Redirect URI is configured in Azure that matches with the firewall SSO server configuration.

I cannot sign in when I use guest user or personal account.

This is a known issue (NC-101912) in EAP0, fixed already in EAP1.

What is Redirect URI ?

A redirect URI, or reply URL, is the location where the authorization server sends the user once the app has been successfully authorized and granted an authorization code or access token.

FAQs

Is it fine to use the same App we used for Azure AD Sync in Central, or is this not recommended ?

Yes, you can use same azure app to protect multiple application. It is advised to use separate apps for better isolation and granular security control.

I am getting 500 Internal Server Error.

API permission is not properly configured in Azure AD. Configure **User.Read**, **User.ReadAll**, and **Group.Read.All** *delegated* permission. Note: Group.Read.All is only required if user is assigned to one or more groups.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Default Directory

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (3)				...
Group.Read.All	Delegated	Read all groups	Yes	✓ Granted for Default Dire... ...
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for Default Dire... ...
User.Read.All	Delegated	Read all users' full profiles	Yes	✓ Granted for Default Dire... ...

Best practices

- Create separate Azure application for Firewall SSO for better control and isolation.
- Ensure “Assignment required” is turned on in Azure AD to grant access to limited users (assigned to the Azure application).
- Grant only required API permissions (User.ReadAll and Group.ReadAll).
- Configure application roles and role-mapping in the firewall to allow required access.
- It is advised to enable multi-factor authentication for all users in Azure AD.
- App ownership configuration: Owners can manage all aspects of a registered application. It's important to regularly review the ownership of application.

Demo recording

Thank you!