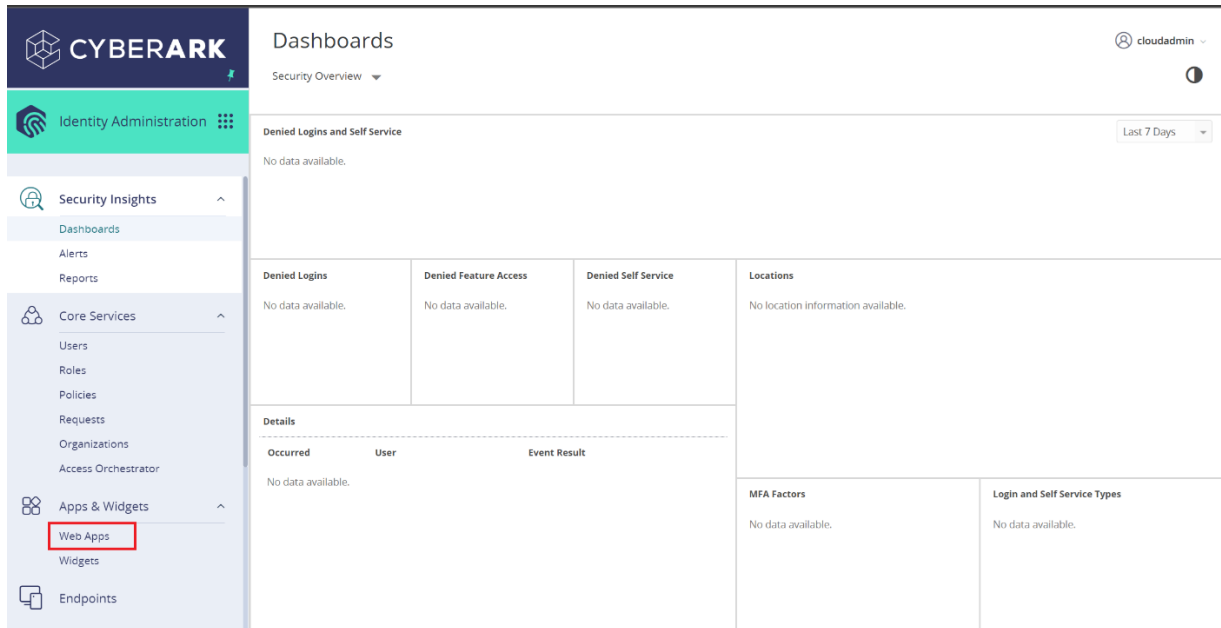


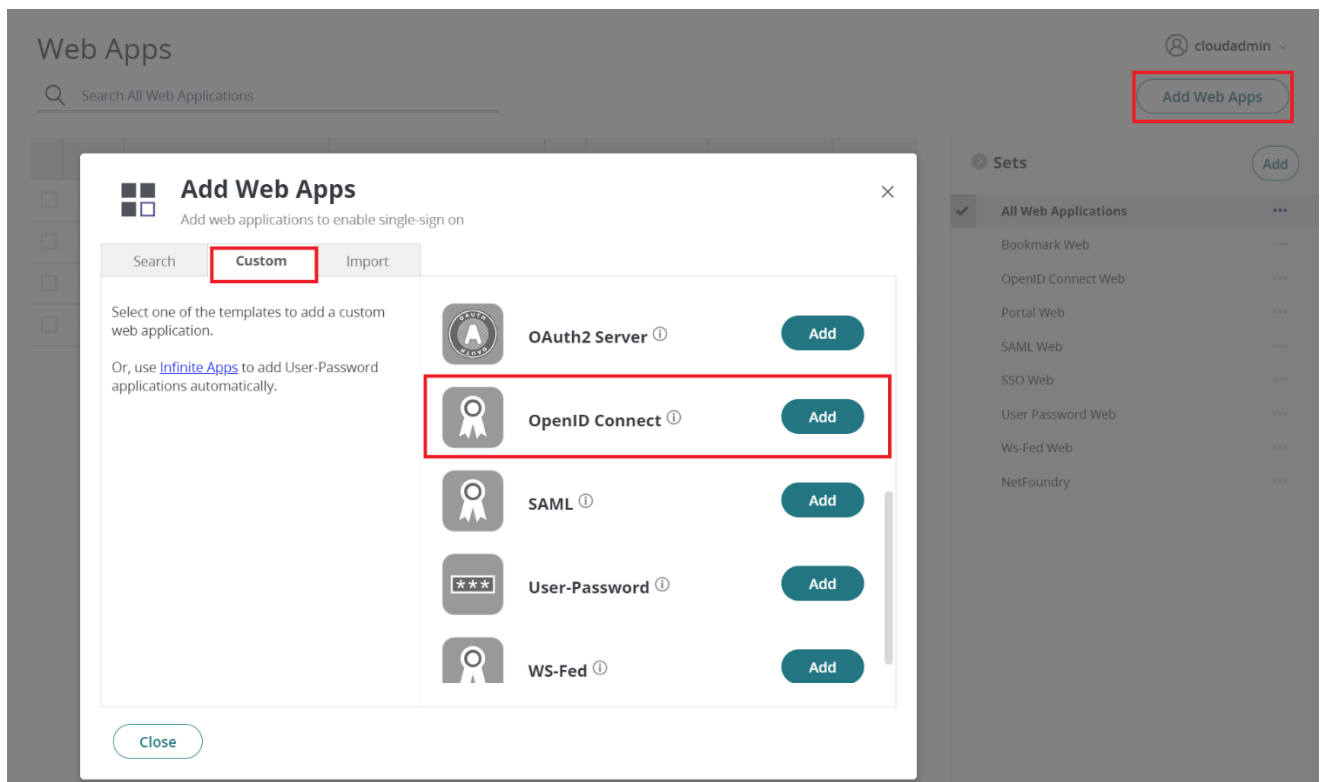
BrowZer - CyberArk

PART ONE - CyberArk Configuration

1. Login into the CyberArk Admin Console and Click on Web Apps.



2. From the Web Apps section, click on “Add Web Apps” and select “OpenID Connect”



3. If you have Organizations setup, select the one you'll assign this Application.

Add Web App ×

**OpenID Connect**

Description
This template enables you to provide single sign-on to a web application that uses OpenID Connect for authentication.

Organization

NetFoundry

NetFoundry

Do you want to add this application?

Yes

No

4. In the next session, we need to configure the initial settings of our application.
 - a. Select an ApplicationID.
 - b. Add a Name.
 - c. Select the appropriate Category based on your requirements and preferences.
 - d. Remember to Copy the AppKey as we'll use it later in the BrowZer configuration.

Settings

Trust

Tokens

Scope

Permissions

Policy

Account Mapping

Linked Applications

Provisioning

App Gateway

Workflow

Changelog

Secure Web Sessions

Additional Attributes

Settings

[Learn more](#)

Application ID * ⓘ

browzer

Description

☐ Customize Name and Description for each language ⓘ

Name *

BrowZer Authentication

Description

This template allows authenticate BrowZer users via CyberArk IDP.

Category *

ZeroTrust

Logo



[Browse](#)

Recommended image size is 180 x 180

Organization

NetFoundry

Advanced

App key ⓘ

b1afeb0e-538a-4bb3-b8c6-ffa4946b36c4

[Copy Key](#)

Widget ID ⓘ

[Copy Key](#)

[Save](#)

[Cancel](#)

5. Then click on “Trust” to configure the Service Provider and Authorized URLs.
 - a. Create a Client Secret (you may use a random value or a UUID4 value as well)
 - b. Take note of the Metadata URL and the Issuer URL, as we’ll use them later.
 - c. For Each BrowZer application you configure, you must add its URL into the Authorized Redirect URIs and Post-Logout Redirect URIs.

Trust

OpenID Connect client ID ⓘ
b1 [Copy](#)

OpenID Connect client secret * ⓘ
.....

OpenID Connect metadata URL ⓘ
https://.....cyberark.cloud/browser/.well-known/openid-confi [Copy](#)

OpenID Connect issuer URL ⓘ
https://.....id.cyberark.cloud/browser/ [Copy](#)

Service Provider Configuration

☒ Login initiated by the relying party (RP) ⓘ
☐ Login initiated by CyberArk Identity ⓘ

Authorized redirect URIs * ⓘ
[Add](#)

Name
☐ https://neuron.icslab.browser.cloudziti.io
☐ https://emqx.icslab.browser.cloudziti.io
☐ https://openplc.icslab.browser.cloudziti.io

☐ Enable full url match ⓘ

Post-logout redirect URIs ⓘ
[Add](#)

Name
☐ https://openplc.icslab.browser.cloudziti.io/
☐ https://emqx.icslab.browser.cloudziti.io/

6. In the Tokens Screen, you need to configure the script to set the Claims needed. By default, CyberArk won't send any Claim that hasn't been set in this section.

Tokens

Access and ID token lifetime * ⓘ
5 hours

☐ Issue refresh tokens ⓘ

Script to set custom claims and headers ⓘ
[Reset Script](#) [Test](#)

Script to generate OpenID Connect authorization and UserInfo responses for this application. [Learn more](#)

```
1 var mail = LoginUser.Get('mail');
2 setClaim('email', mail);
3 setClaim('mail', mail);
```

```
var mail = LoginUser.Get('mail');  
  
setClaim('email',mail);  
  
setClaim('mail',mail);
```

- Now, we need to configure the General Authentication settings, in particular for the API Security, allowing each Domina for each BrowZer Application needed.

Platform

- Authentication Profiles
- Certificate Authorities
- Security Questions
- Security Settings
- Signing Certificates

Authentication Tokens

- FIDO2 Authenticators
- OATH Tokens

Other

- RADIUS Connections
- Duo Configuration
- YubiKey Configuration

Security Settings

Use these settings to define security related settings.

[Learn more](#)

- ☐ Enable anti-phishing security image ①
- ☐ Securely capture users passwords at login ①
- ☐ Enable forgot username self-service at login ①
- ☐ Send email notification to users when password is changed
- ☐ Enable user interaction with email invitations ①
- ☐ Disable the force authentication at the Identity Provider for SAML login ①
- ☒ Don't use certificates for authentication on Android if prompt is required ①
- ☐ Hide login authentication method hints ①

8 Email and SMS passcode length ①

Additional Attributes for MFA ①

[Add](#)

Attribute	Type
No attributes specified	

CAPTCHA Settings

Off Number of consecutive failed login attempts allowed before showing a CAPTCHA (default Off)

API Security

Origin Validation ①

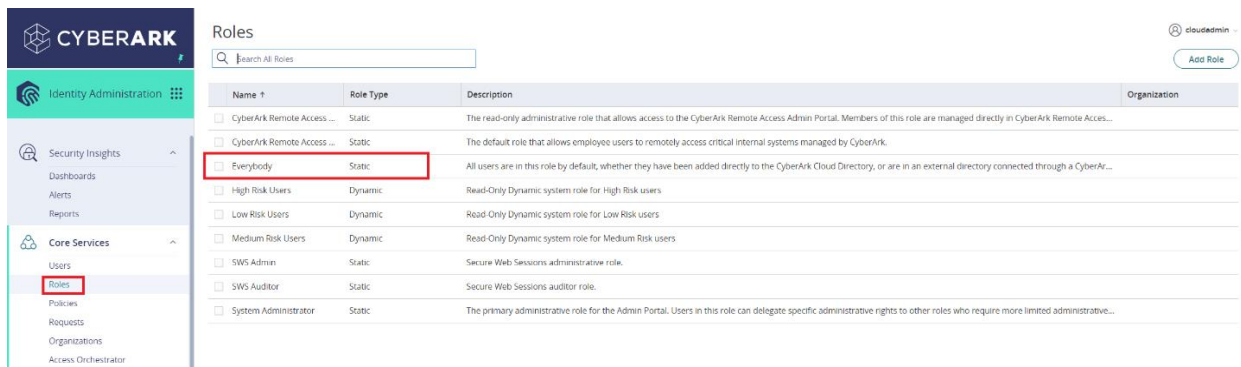
- ☐ Enable (recommended)
- ☒ Validate GET requests ①

Specify Trusted DNS Domains for API Calls ①

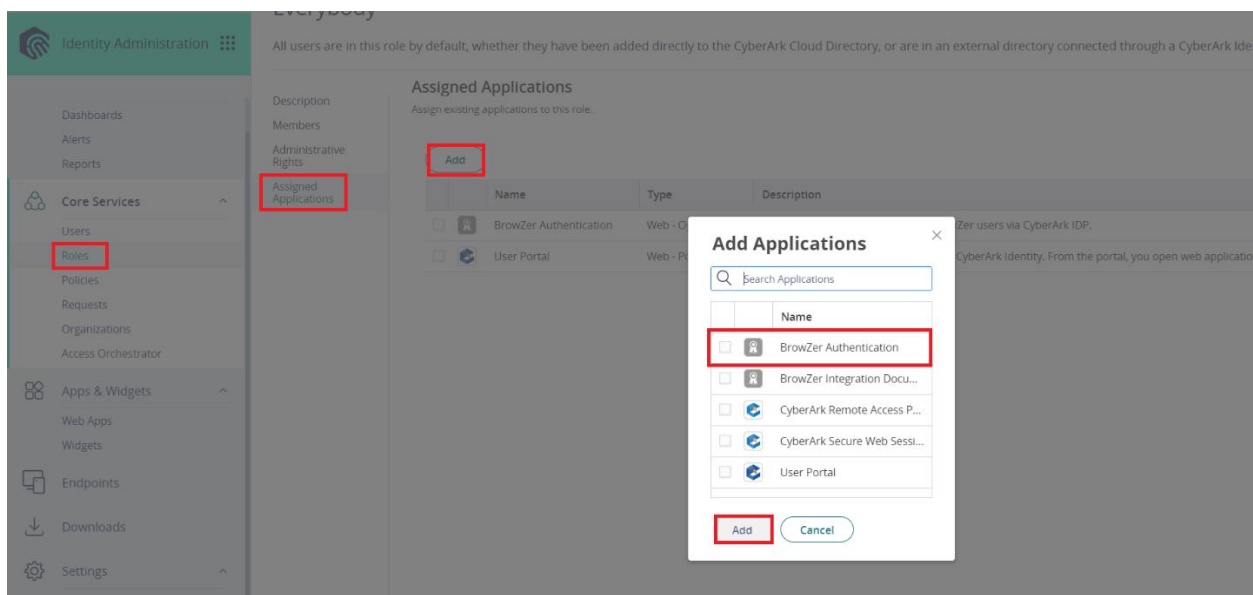
[Add](#)

Allowed Domain
☐ openpic.icslab.browzer.cloudziti.io
☐ emqx.icslab.browzer.cloudziti.io
☐ neuron.icslab.browzer.cloudziti.io

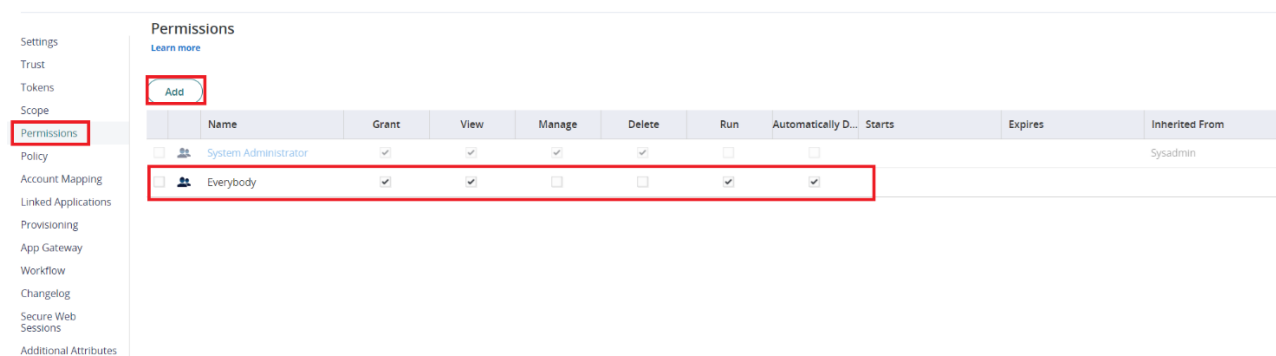
- Then, we need to assign the application to the appropriated Roles. For that Click on Core Services → Roles and click on the Role you want to assign the BrowZer Application. In this particular case for “Everyone”.



9. Now click on “Assigned Applications” → Add” then select your recently create Web App.



10. Finally, in order to deploy your new application. Return to the Web App and click on your recently created App. Then select “Permissions” and Grant the ones you required, basically “Grant”, “View” and “Automatically Deploy”.



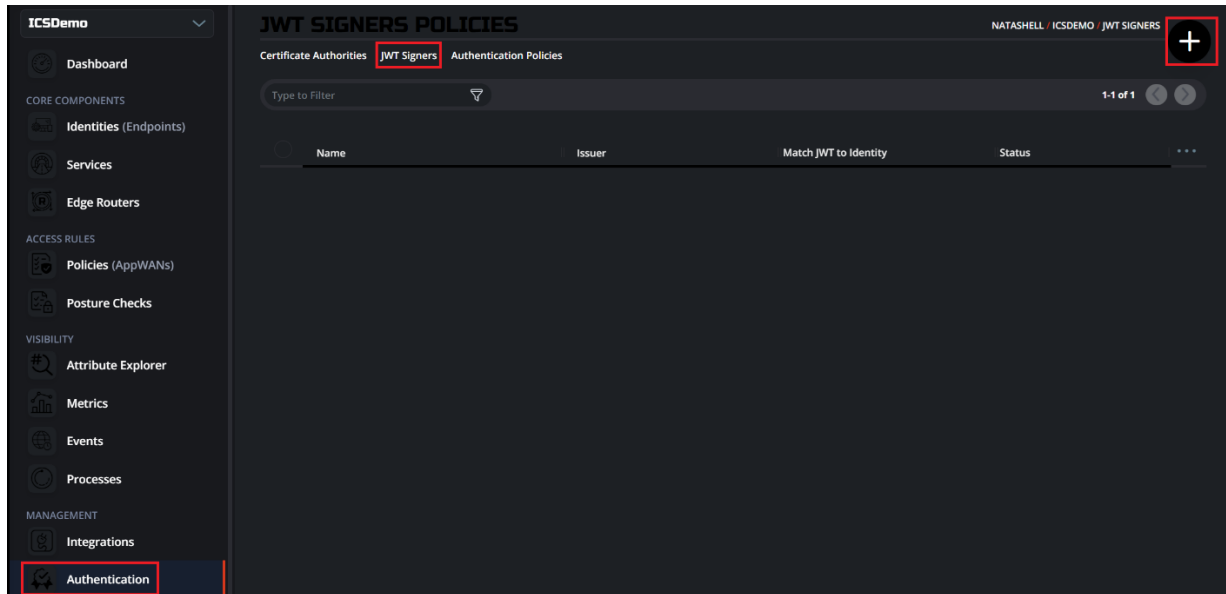
11. You can open the openID configuration and get the values for JWKS_URI and “Issuer” or get them from the step 5.

```
{
  "authorization_endpoint": "https://abm4626.id.cyberark.cloud/OAuth2/Authorize/browser",
  "code_challenge_methods_supported": [
    "plain",
    "S256"
  ],
  "jwks_uri": "https://abm4626.id.cyberark.cloud/OAuth2/Keys/browser",
  "response_types_supported": [
    "code",
    "id_token",
    "id_token token",
    "code id_token",
    "code token",
    "code id_token token"
  ],
  "introspection_endpoint": "https://abm4626.id.cyberark.cloud/OAuth2/Introspect/browser",
  "id_token_signing_alg_values_supported": [
    "RS256"
  ],
  "subject_types_supported": [
    "public"
  ],
  "issuer": "https://abm4626.id.cyberark.cloud/browser/",
  "userinfo_endpoint": "https://abm4626.id.cyberark.cloud/OAuth2/UserInfo/browser",
  "token_endpoint": "https://abm4626.id.cyberark.cloud/OAuth2/Token/browser",
  "scopes_supported": [
    "openid",
    "profile",
    "email",
    "address",
    "phone"
  ],
  "claims_supported": [
    "sub",
    "name",
    "family_name",
    "given_name",
    "picture",
    "preferred_username",
    "email",
    "email_verified",
    "phone_number",
    "phone_number_verified",
    "address",
    "auth_time",
    "aud",
    "iss",
    "exp",
    "iat"
  ],
  "end_session_endpoint": "https://abm4626.id.cyberark.cloud/OAuth2/EndSessionV2/browser"
}
```

PART TWO - THE JWT SIGNER

1. Login into the NetFoundry Console then in Authentication and select JWT Signers →

+



2. Fill the required information based on your application settings. Issuer and External Auth URL are the value as the “Issues” in your OpenID application.

SIGNER NAME REQUIRED

CyberArk-Identity YES ☒ ENABLED

ISSUER REQUIRED

https://.id.cyberark.cloud/browser/

AUDIENCE REQUIRED

b1afeb0e-

JWKS ENDPOINT REQUIRED

https://.id.cyberark.cloud/OAuth2/Keys/browser

MATCH JWT TO IDENTITY WHEN: REQUIRED

JWT CLAIMS

email

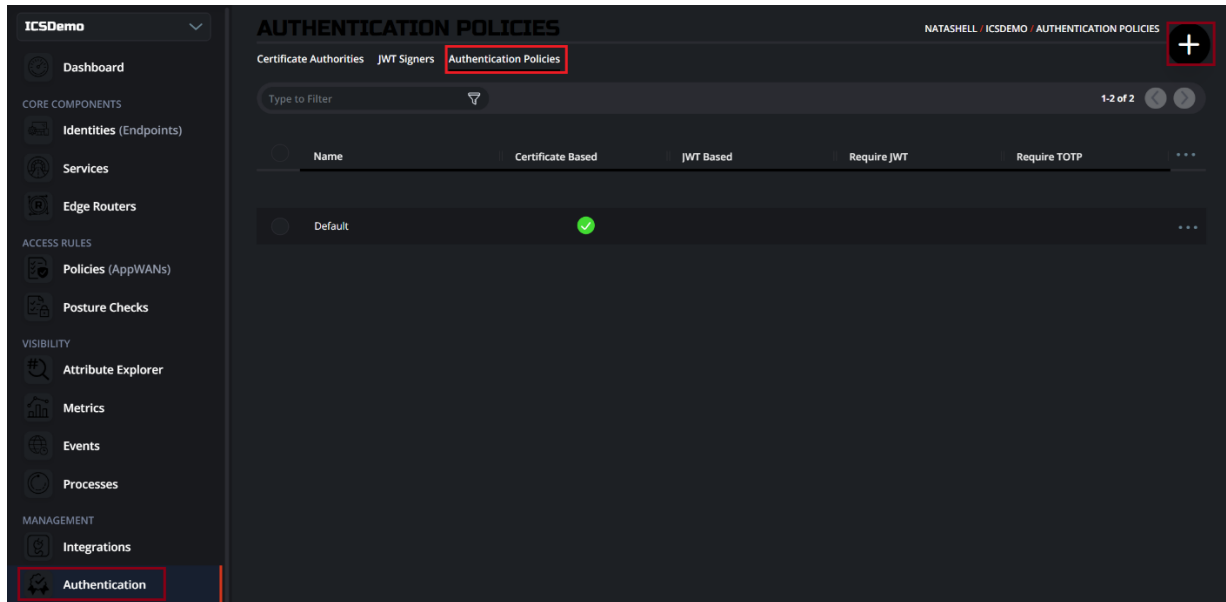
IDENTITY'S

☐ Id OR ☒ External Id

EXTERNAL AUTH URL OPTIONAL

https://.id.cyberark.cloud/browser/

3. Then, create new Authentication Policy.



4. Select your recently created JWT Signer and enable the JWT Based Authentication.

POLICY NAME REQUIRED

CyberArk-Identity

PRIMARY AUTHENTICATION ⓘ

CERTIFICATE BASED AUTHENTICATION NO

ALLOW EXPIRED CERTIFICATES NO

JWT BASED AUTHENTICATION YES

ALLOWED JWT SIGNERS

Choose JWT Signers

× CyberArk-Identity

SECONDARY AUTHENTICATION ⓘ

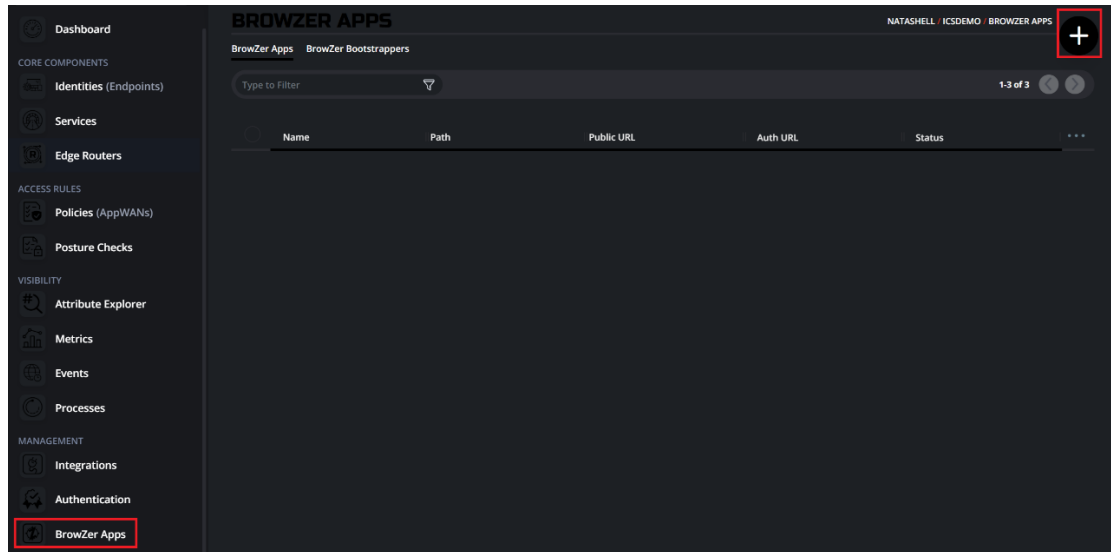
REQUIRE JWT FROM

Choose JWT Signers

REQUIRE TOTP CODE NO

PART THREE - THE BROWZER APP

1. Click on BrowZer Apps then add a new one.



2. Select your service and in case you require HTTPS, enable it.
 - a. The OIDC Base URL is the same as the Issuer of your OpenID Application.
 - b. The ClientID is the App ID or App Key.

The screenshot shows the 'ADD NEW APP' form with four sections, each marked as 'REQUIRED'.

- 1 APP NAME**: A text input field containing 'Neuron-App'.
- 2 PRIMARY SETTINGS**:
 - SELECT THE APP ENTRY POINT**: A dropdown menu showing 'ICS-Neuron-App'.
 - SERVICE REQUIRES HTTPS**: A toggle switch set to 'NO'.
 - PATH**: A text input field containing '/'. It is marked as 'OPTIONAL'.
- 3 PUBLIC ACCESS POINT SETTINGS**:
 - PUBLIC URL**: A text input field containing 'https://neuron' followed by a domain icon.
- 4 USER AUTHENTICATION SETTINGS**:
 - OIDC BASE URL**: A text input field containing 'https://.id.cyberark.cloud/browser/'.
 - CLIENT ID**: A text input field containing 'b1afeb0e-'.

3. Test your successful login, remember create the identity and associate your newly create Authentication Policy

1

IDENTITY NAME

REQUIRED

Marcos-CyberArk

2

IDENTITY ATTRIBUTES ⓘ

OPTIONAL

Add attributes to group identities

✕ #ICS-Operator

 REISSUE KEY 

4

Select an Installer for Your OS

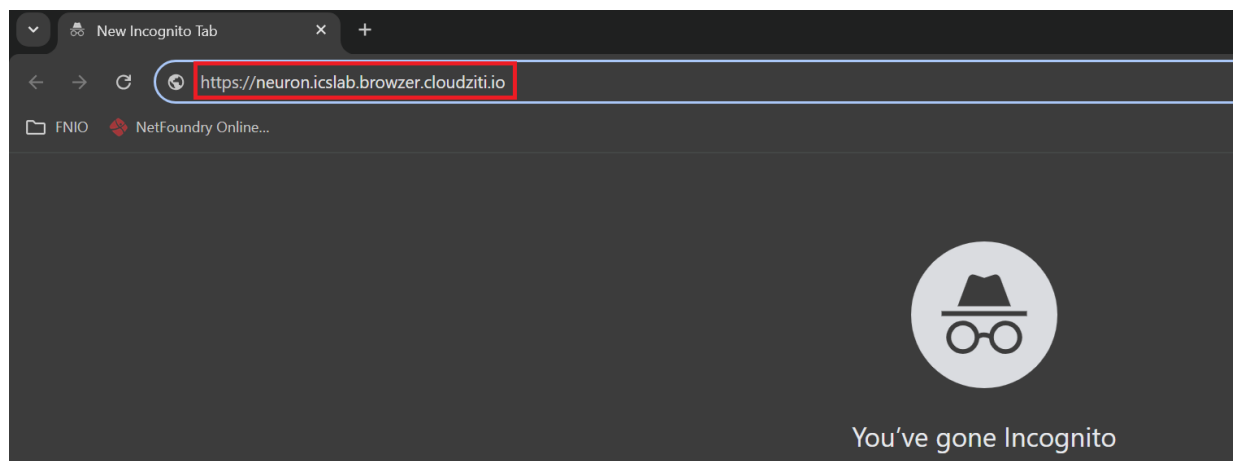
 SELECT AN INSTALLER 

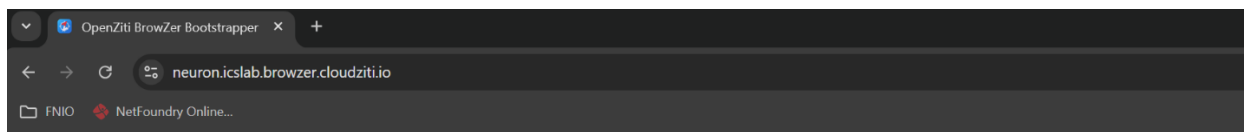
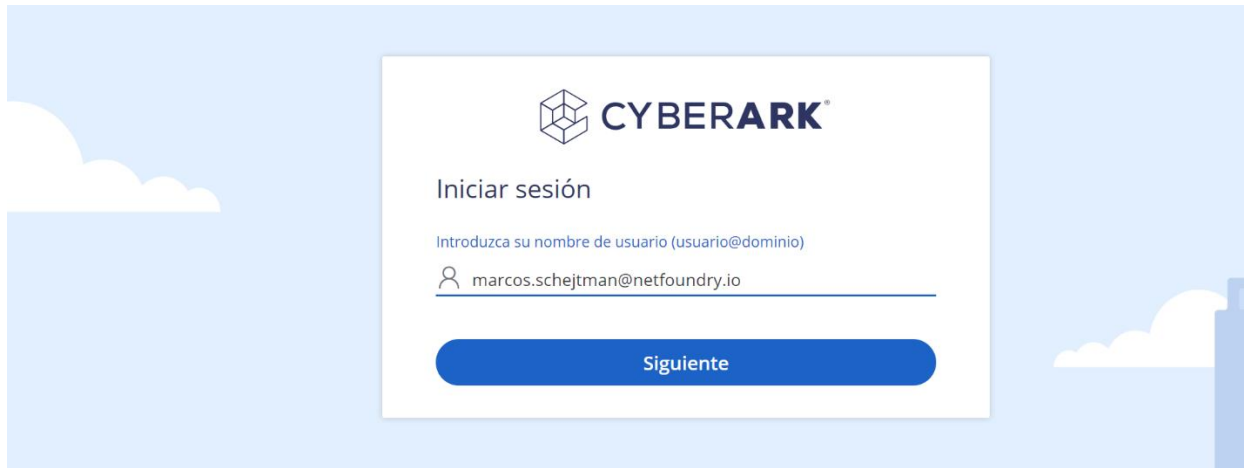
AUTHORIZATION POLICY ⓘ

OPTIONAL

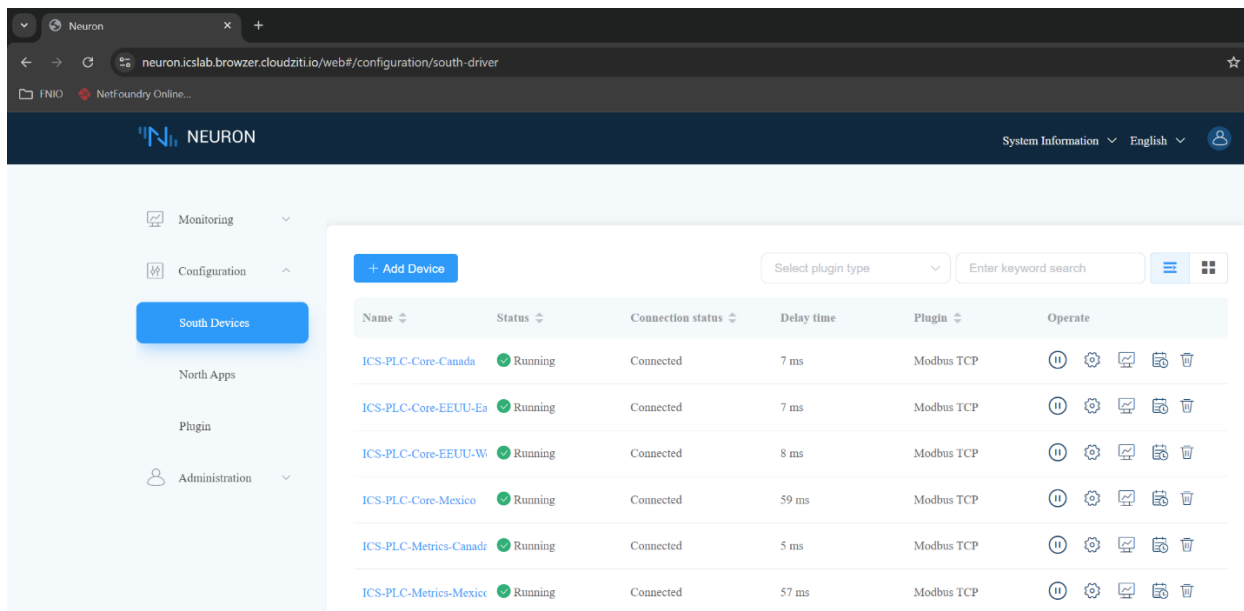
CyberArk-Identity

marcos.schejtman@netfoundry.io





OpenZiti BrowZer is Bootstrapping your web app

The main interface of the Neuron web application. It features a dark blue header with the "NEURON" logo and navigation links for "System Information", "English", and a user profile. A left sidebar contains a menu with "Monitoring", "Configuration", "South Devices" (highlighted in blue), "North Apps", "Plugin", and "Administration". The main content area displays a table of devices. At the top of the table is a blue "+ Add Device" button and a search bar. The table has columns for Name, Status, Connection status, Delay time, Plugin, and Operate. It lists six devices, all with a "Running" status and "Connected" connection status, using "Modbus TCP" as the plugin.

Name	Status	Connection status	Delay time	Plugin	Operate
ICS-PLC-Core-Canada	Running	Connected	7 ms	Modbus TCP	[Pause] [Settings] [Monitor] [Logs] [Delete]
ICS-PLC-Core-EEUU-Ea	Running	Connected	7 ms	Modbus TCP	[Pause] [Settings] [Monitor] [Logs] [Delete]
ICS-PLC-Core-EEUU-W	Running	Connected	8 ms	Modbus TCP	[Pause] [Settings] [Monitor] [Logs] [Delete]
ICS-PLC-Core-Mexico	Running	Connected	59 ms	Modbus TCP	[Pause] [Settings] [Monitor] [Logs] [Delete]
ICS-PLC-Metrics-Canada	Running	Connected	5 ms	Modbus TCP	[Pause] [Settings] [Monitor] [Logs] [Delete]
ICS-PLC-Metrics-Mexico	Running	Connected	57 ms	Modbus TCP	[Pause] [Settings] [Monitor] [Logs] [Delete]