

## My setup

Windows 10 Client with Checkpoint Remote Access (Client E87.20)

Checkpoint Single Gateway in Azure, running R81.20 Build 703, no other JHF installed

Checkpoint SMS in Azure, running R81.20, no other JHF installed

Azure Enterprise App (gallery app) „Check Point Remote Secure Access VPN“

Date of testing: 2023/04/05

## Intention

I wanted to setup a Remote Access environment where users can authenticate against a SAML Identity Provider and the authorization is also provided by that IdP, so that there is no need for a LDAP server to get the group memberships.

## Pre-configuration steps

I followed this configuration guide:

[https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP\\_R81.20\\_RemoteAccessVPN\\_AdminGuide/Content/Topics-VPNRG/SAML-Support-for-Remote-Access-VPN.htm?Highlight=saml](https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_RemoteAccessVPN_AdminGuide/Content/Topics-VPNRG/SAML-Support-for-Remote-Access-VPN.htm?Highlight=saml)

I have not configured these steps:

- Step 4 – point 11 – „On each Security Gateway of version R81.10 and lower, download a script that is required to use the feature.“ (because my setup uses R81.20)
- Step 5: Install and Configure Remote Access VPN Clients
- Everything that is related to a LDAP configuration to get group memberships through LDAP

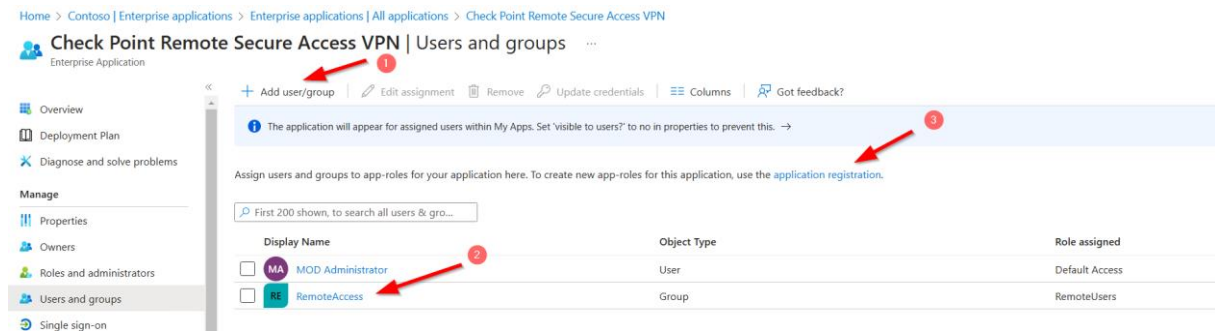
The following parts are only an additional piece, because the documentation is sometime not that good in describing the details of the required steps. So please use the mentioned guide above from Checkpoint and I hope that my additional information can help you to get it up and running.

# Checkpoint Remote Access SAML Authentication & Authorization with Azure AD

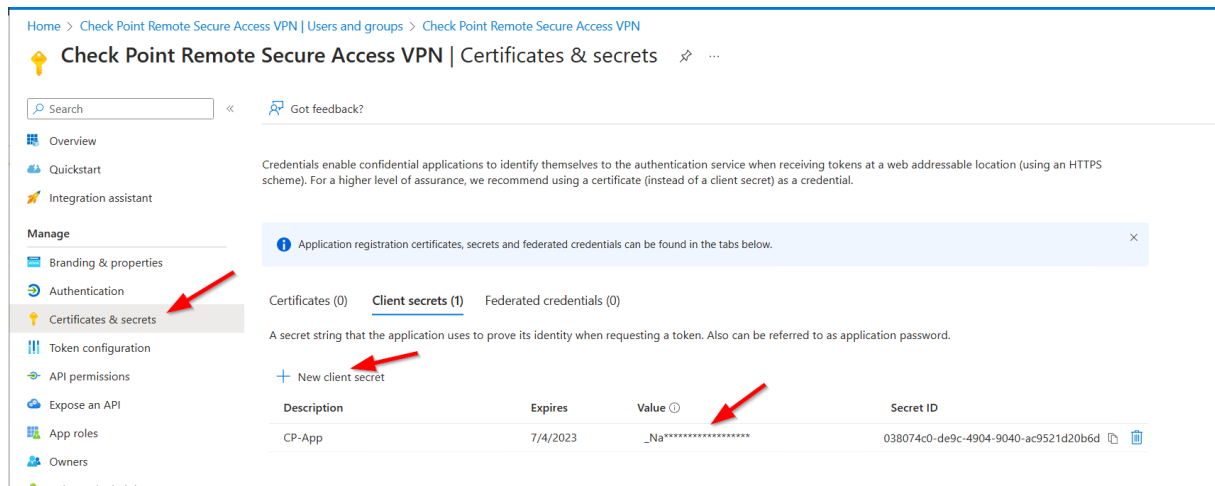
## Enterprise App – role and app registration

Create a AAD group for Remote Access users, add your users to that group.

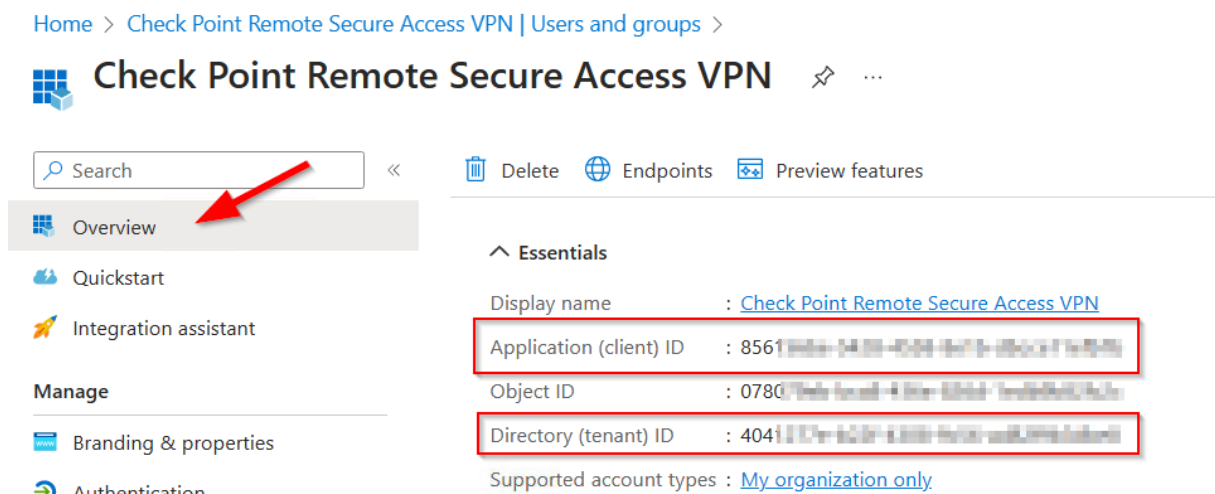
Use the link „application registration“ to define a role and App permissions.



Create an App secret so that Checkpoint Management + Gateway is able to read user and group details. Save the value in your password tresor.



You'll also need the Application ID & Directory ID



Add permission to this app registration, so that the App can read some user / group related data:

# Checkpoint Remote Access SAML Authentication & Authorization with Azure AD

Home > Check Point Remote Secure Access VPN | Users and groups > Check Point Remote Secure Access VPN

## Check Point Remote Secure Access VPN | API permissions

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value that will be used. [Learn more](#)

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 Contoso

API / Permissions name	Type	Description	Admin consent required	Status
Microsoft Graph (3)				
Device.Read.All	Application	Read all devices	Yes	Granted for Contoso
Group.Read.All	Application	Read all groups	Yes	Granted for Contoso
User.Read.All	Application	Read all users' full profiles	Yes	Granted for Contoso

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

## Create a new role:

Home > Contoso | Enterprise applications > Enterprise applications | All applications > Check Point Remote Secure Access VPN | Users and groups > Check Point Remote Secure Access VPN

## Check Point Remote Secure Access VPN | App roles

+ Create app role    Got feedback?

App roles

App roles are custom roles to assign permissions to users or apps. The application defines and publishes the app roles and interprets them as permissions during authorization.

**How do I assign App roles**

Display name	Description	Allowed member types	Value	ID	State
RemoteUsers	RemoteUsers	Users/Groups	RemoteUsers	fbea3299-1d8e-4b4a-...	Enabled
msiam_access	msiam_access	Users/Groups		6996bac3-b464-498c-...	Enabled

Go one step back to your Enterprise App, open „Users and Groups“.

Select your Remote User group and „Edit assignment“. Select the previous created role.

Home > Check Point Remote Secure Access VPN

## Check Point Remote Secure Access VPN | Users and groups

+ Add user/group    Edit assignment    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 prevent this. →

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the [application registration](#).

First 200 shown, to search all users & groups...

Display Name	Object Type	Role assigned
MA MOD Administrator	User	Default Access
RE RemoteAccess	Group	RemoteUsers

## Enterprise App - Single SignOn


You need to add a new claim:

Claim name: „group\_attr“

Value: „user.assignedroles“

[Home](#) > [Check Point Remote Secure Access VPN | SAML-based Sign-on](#) > [SAML-based Sign-on](#) >



### Attributes & Claims ...

 [+ Add new claim](#) [+ Add a group claim](#) [☰ Columns](#) | [🗨 Got feedback?](#)

#### Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]

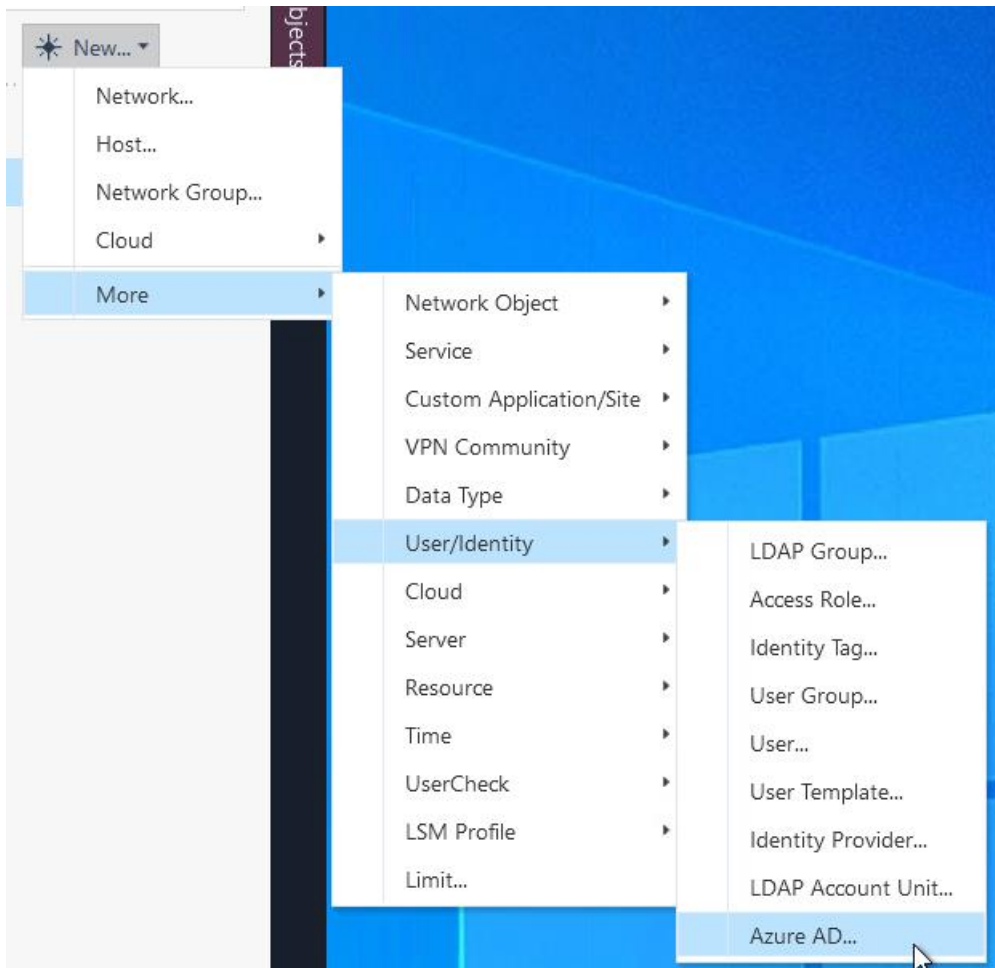
#### Additional claims

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

∨ Advanced settings

## Smart Console – object to read identities from AAD

Switch to Smart Console and add a new User/Identity, type „Azure AD“.



„Application Key“ is the secret value:

The connection needs to be successful, otherwise reload the browser from Azure AD (the secret value needs to be hidden by some „\*\*\*\*\*“).

Another possible fault can be, that the API permission is not set or granted.

## Checkpoint Remote Access SAML Authentication & Authorization with Azure AD

Azure AD

CP-App  
Enter Object Comment

⚠ Changes will be applied after publish.

Service Principal Authentication

Application ID: 856 [redacted]

Application Key: [redacted]

Directory ID: 404 [redacted]

Azure AD User Authentication

Username: [redacted]

Password: [redacted]

Test Connection **Connected**

Note: when using the Azure AD feature, each security gateway saves locally all the entities from the Azure repository, regardless of the gateway's region.

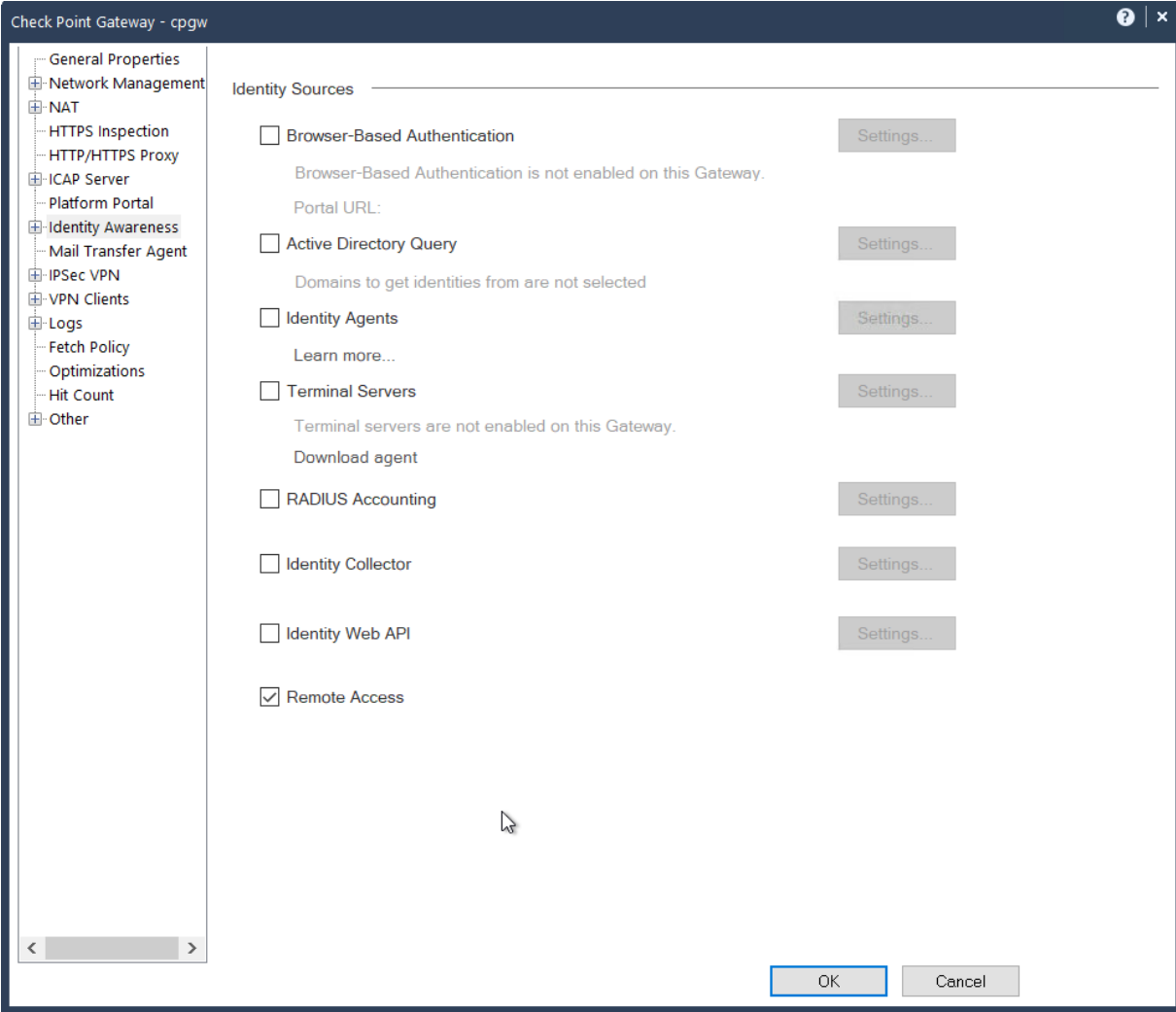
Add Tag

OK Cancel

Publish now your changes.

Open your gateway, blade Identity Awareness, check „Remote Access“.

Checkpoint Remote Access SAML Authentication & Authorization with Azure AD

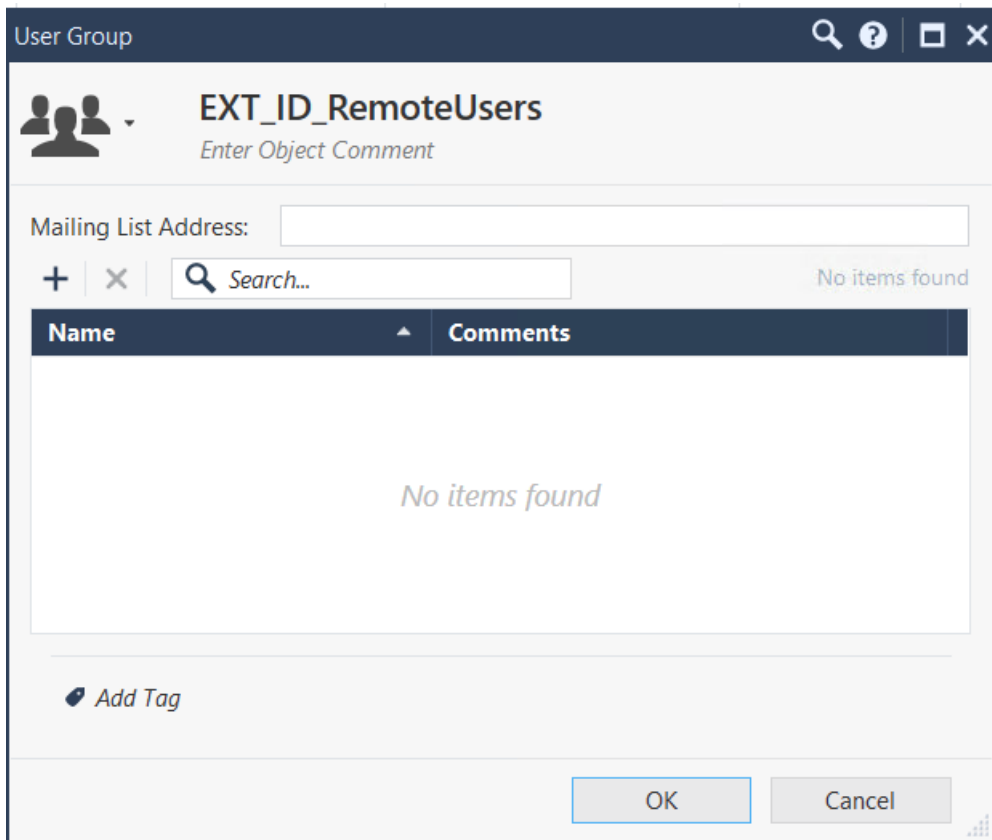


## Checkpoint Remote Access SAML Authentication & Authorization with Azure AD

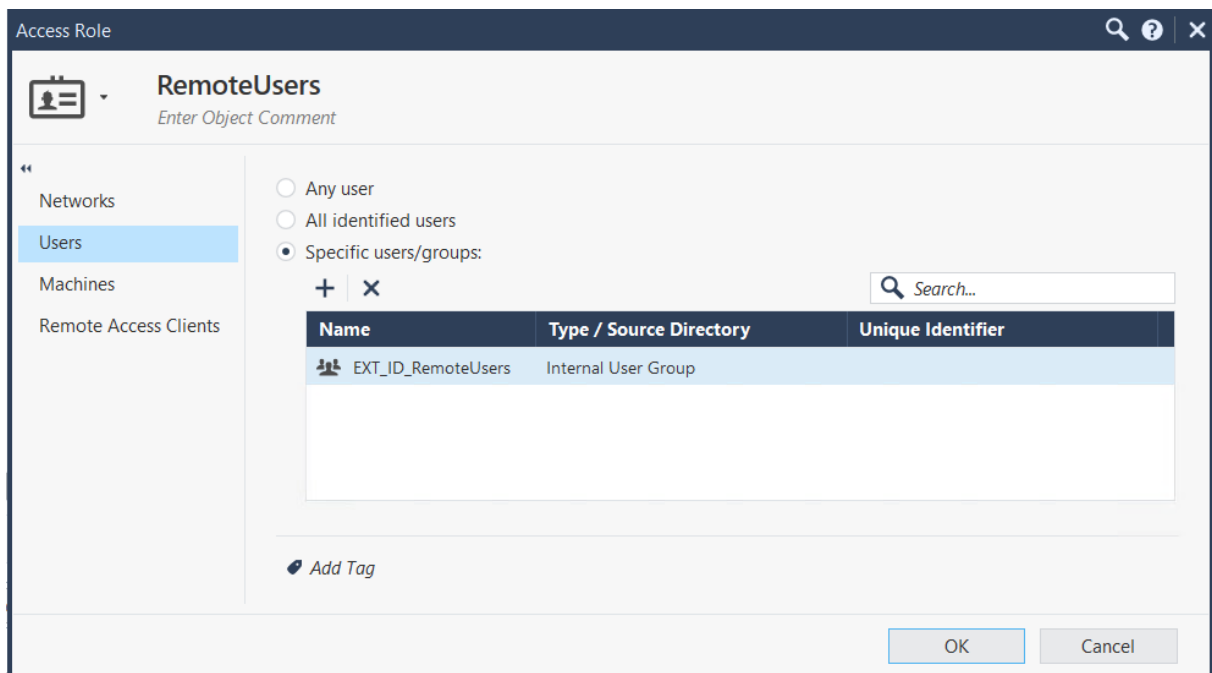
### Smart Console – Internal User Group / Access Role

Create an „Internal User Group“ and take care of the name.

The name needs this syntax: „EXT\_ID\_“ followed by your role name, leave the rest empty.



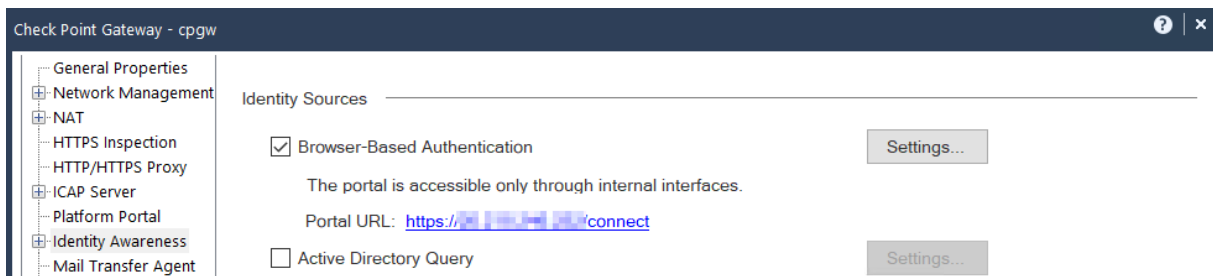
Use that internal group in your Access Role:





## Checkpoint Remote Access SAML Authentication & Authorization with Azure AD

In case for access without Remote Access, you can check „Browser-Based Authentication“.



Keep in mind, that you'll have to add in your access role the native user or group from Azure AD. The Internal User Group (starting with „EXT\_ID\_“ is only necessary for Remote Access).

Create a policy with that Access Role as the Source and whatever destination / service you will allow.

## Checkpoint Remote Access SAML Authentication & Authorization with Azure AD

### User is connected – PDP monitor

When the user is connected, you can view the details with „pdp monitor“ and check the assigned role and groups:

```
[Expert@cpgw:0]# pdp monitor all

Session: 0cfe0c18
Session UUID: {1A1A3A7F-DB65-638F-C47C-9E3D08F0537F}
Ip: 172.16.10.3
Users:
AlexW@M365x96201156.OnMicrosoft.com {f5750b79}
LogUsername: AlexW@M365x96201156.OnMicrosoft.com
Groups: All Users;EXT_ID_RemoteUsers
Roles: RemoteUsers
Client Type: Remote Access
Authentication Method: Trust
Distinguished Name:
Connect Time: Wed Apr 5 13:21:44 2023
Next Reauthentication: Wed Apr 5 14:59:53 2023
Next Connectivity Check: -
Next Ldap Fetch: -

Packet Tagging Status: Not Active
Published Gateways: Local
*****
[Expert@cpgw:0]#
```