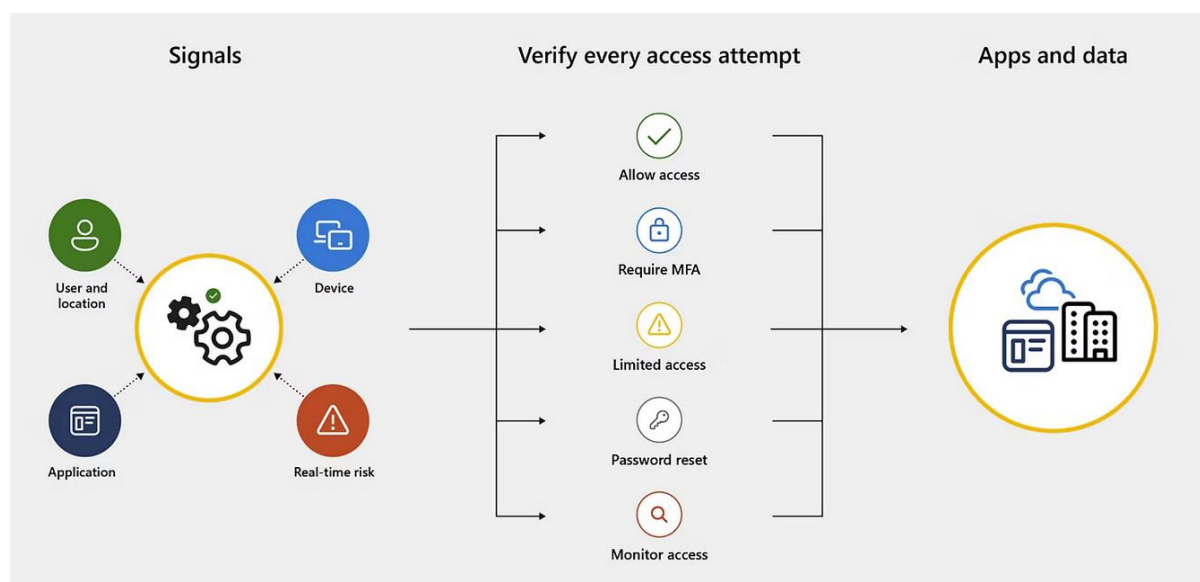


## Microsoft Entra admin centar - Conditional Access

Uvjetni pristup (Conditional Access) je skup konfiguracija pravila koji kontrolira koji uređaji i korisnici mogu imati pristup različitim aplikacijama. Konkretno govoreći o Microsoftovom okruženju, pravila uvjetnog pristupa rade s Office 365 i drugim aplikacijama softvera kao usluge (SaaS) konfiguriranim u Azure Active Directory.

Conditional access radi na principu ispunjenja uvijeta IF-THEN, tada se potrebne radnje mogu poduzeti za taj uvijet.

Npr. Korisnik želi pristupiti bilo kojoj Office 365 aplikaciji i mora izvršiti provjeru autentičnosti (MFA) da bi joj pristupio.



Conditional Access koristi se u Microsoft Entra ID okruženju. Koristi za objedinjavanje signala, donošenje odluka i primjenu pravilnika tvrtke ili ustanove. Riječ je o mehanizmu za provedbu sigurnosnih pravilnika koji analizira signale u stvarnom vremenu da bi na ključnim kontrolnim točkama donosio odluke o provedbi zaštite. Lijeva strana dijagrama predstavlja način na koji se objedinjuju signali korisnika, uređaja, lokacija, aplikacija, oznaka podataka i analize rizika; odluke se provode na temelju objedinjenih signala. U središnjem dijelu dijagrama prikazuju se uobičajene odluke na temelju signala, uključujući blokiranje, ograničavanje, dopuštanje pristupa ili traženje dodatnih koraka, kao što su provjera autentičnosti ili ponovno postavljanje lozinke. Desna strana dijagrama predstavlja način na koji se odluka provodi na aplikacijama i podacima kada uvjetni pristup odredi odgovarajuću radnju.

S Conditional Access možete kreirati pravila koja pružaju istu zaštitu kao zadane sigurnosne postavke (Security defaults), ali s granularnošću. Uvjetni pristup i sigurnosne zadane postavke ne smiju se kombinirati jer vas stvaranje pravila uvjetnog pristupa sprječava da omogućite sigurnosne zadane postavke.

#### **Dobre prakse:**

Dobro je isključujući tj. Izuzeti račune za koje ne želimo da se primjeni Conditional Access polica zbog mogućnosti komplikacija u radu za račune:

- **break-glass račun**
- **servisni računi**

#### **Ograničenja:**

Conditional Access ima ograničenje od 195 polica po tenantu. Ovo ograničenje pravila od 195 uključuje Conditional access pravila u bilo kojem stanju, uključujući način rada samo za izvješća (report-only mode), uključeno ili isključeno.

#### Načini postavke police

- Report-only mode
- On
- Off

-By default, svaka polica stvorena iz predložaka kreira se u report-only modu načina rada samo za izvješća kako bi se polica prvo mogla testirati.

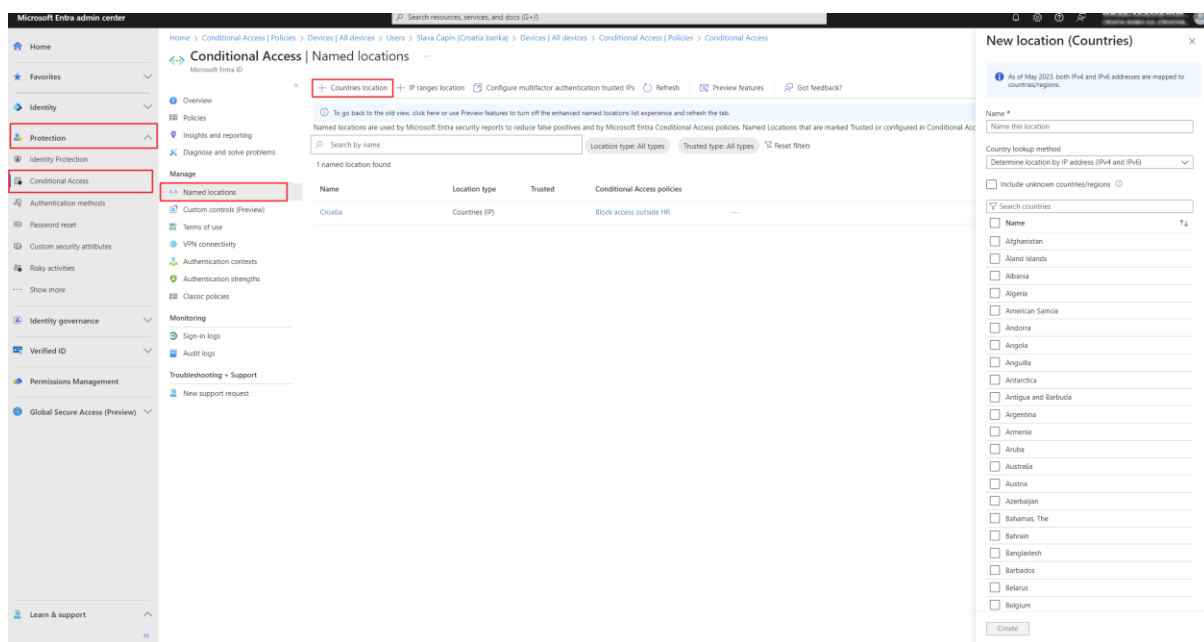
#### **Named Location**

Možemo ograničiti pristup s obzirom na zemlju. Restrikciju možemo postaviti i putem IP rangea. Npr dodamo sve poznate vanjske IP adrese putem koji će biti propušten pristup. Sve ostale IP adrese ili zemlje bit će automatski ograničene.

Za ograničavanje/dopuštanje pristupa iz zemlje, prvo ćemo otići na imenovane lokacije, a zatim kliknuti na "lokacija zemalja" za dodavanje zemalja.

Potrebno je:

Login Microsoft Entra admin centar -> Protection -> Conditional Access -> Named Location



Na drugom koraku potrebno je upisati Zemlju koju želimo dodati te odabrati „Create“

The screenshot shows the 'New location (Countries)' dialog box. At the top, there is an information message: 'As of May 2023, both IPv4 and IPv6 addresses are mapped to countries/regions.' Below this, the 'Name' field is filled with 'Croatia'. The 'Country lookup method' dropdown is set to 'Determine location by IP address (IPv4 and IPv6)'. The 'Include unknown countries/regions' checkbox is unchecked. A list of countries is shown with 'Croatia' selected. At the bottom, there is a 'Create' button.

## Conditional Access Policy

Nakon što smo dodali zemlju ili IP range, potrebno je konfigurirati policu

### New Policy

Protection -> Conditional Access -> Policies -> New policy

Postavljamo uvijete police.

[Home](#) > [Conditional Access | Policies](#) >

## New ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

[Learn more](#)

Name \*

Block access outside of croatia



### Assignments

Users ⓘ

All users included and specific users excluded

Target resources ⓘ

No target resources selected

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.

[Learn more](#)

Include

Exclude

Select the users and groups to exempt from the policy

☐

Guest or external users ⓘ

☐

Directory roles ⓘ

☒

Users and groups

Select excluded users and groups

1 user



test1  
test1@croatiabanka.hr



## Location

Na ovom koraku pod include sam postavio opciju Any Location tako da se blokiraju pravo pristupa sa svih lokacija osim Exclude – Hrvatska, tako da se može pristupiti samo iz geolokacije Hrvatske cloud aplikacijama.

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

Device platforms ⓘ

Not configured

Locations ⓘ

Any location

Client apps ⓘ

Not configured

Filter for devices ⓘ

Not configured

Authentication flows (Preview) ⓘ

Not configured

Control user access based on their physical location. [Learn more](#)

Configure ⓘ

Yes

No

**Include** Exclude

☒ Any location

☐ All trusted locations

☐ Selected locations

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

Device platforms ⓘ  
Not configured

Locations ⓘ  
Any location and 1 excluded

Client apps ⓘ  
Not configured

Filter for devices ⓘ  
Not configured

Authentication flows (Preview) ⓘ  
Not configured

Control user access based on their physical location. [Learn more](#)

Configure ⓘ  

YesNo

IncludeExclude

Select the locations to exempt from the policy

All trusted locations

Selected locations

Select

Croatia

Croatia...