Bezbednost i validacija

Sadržaj

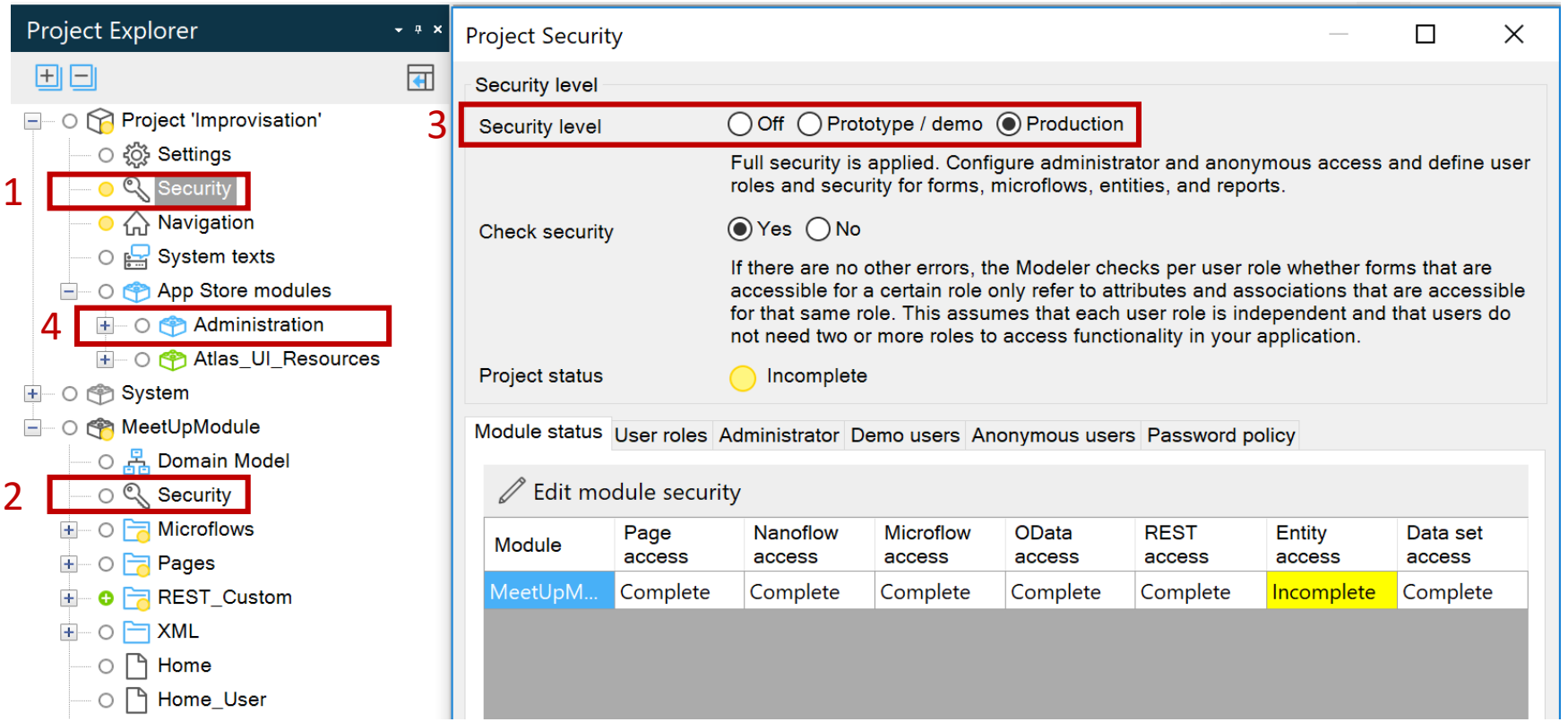
- Uvod
- Kontrola pristupa
  - Uloge
  - Mehanizam
  - Pravila pristupa
- Validacija podataka
- Dodatno
  - REST

Uvod

- U okviru Mendix-a, bezbednošću se rukuje na dva nivoa:
  - Na nivou projekta, odakle se upravlja stepenom (*level*) bezbednosti i podešavanjima vezanim za čitavu aplikaciju
  - Na nivou pojedinačnih modula, odakle se se upravlja pristupom entitetima, logici i stranicama (kroz funkcionalne uloge *(role)*)

- Kako bezbednost ne bi uticala na brzinu razvoja softvera, postoje tri stepena bezbednosti:
  - *Off* – bezbednost nije uključena, nema korisničkih naloga i uloga, slobodan pristup svim resursima. Ovo je podrazumevani nivo bezbednosti
  - *Prototype/Demo* - stepen bezbednosti namenjen za prototip aplikacije, koja nije još u produkciji. Postoje korisnici, i uloge. Pristup ograničen za stranice i logiku, ali ne i entitete
  - *Production* – Restriktivniji stepen bezbednosti od *Prototype/Demo,* zahteva i definisanje pravila pristupa na nivou entiteta

Uvod

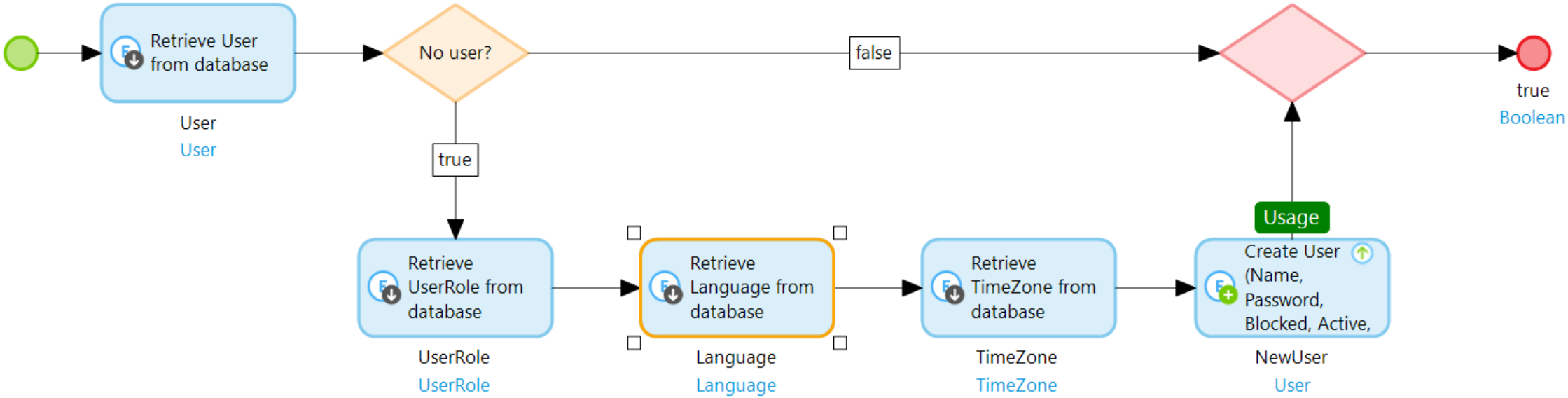


1. Podešavanje bezbednosti na nivou projekta
2. Podešavanje prava pristupa na nivou modula (ako stepen bezbednosti (3. *Security level)* nije *off)*
4. *Administration* modul, kojeg **možete** iskoristiti za rukovanje korisničkim nalozima

Uvod

- U produkcionom stepenu bezbednosti, *Modeler* vrši validaciju konzistentosti bezbednosnih pravila
- Na nivou projekta, moguće je:
  - Definisati korisničke uloge (*roles)* na nivou projekta, i povezati ih sa ulogama na nivou pojedinačnih modula
  - Dodati administratorski nalog (koji će biti kreiran samo u testnom okruženju na lokalu, dok se za *cloud* okruženje on mora drugačije kreirati)
  - Dodati testne korisničke naloge, što ubrzava testiranje aplikacije za različite uloge
  - Definisati politiku za anonimne korisnike – korisnike koji nisu autentifikovani, nisu odradili *log-in*
- Kada stepen bezbednosti više nije *off*, *log-in* stranica će automatski biti prikazana kao početna stranica za anonimne korisnike.
- Ulogovani korisnik se može odjaviti dugmetom tipa *"Sign out"*. Kroz *microflow* se to može učiniti pomoću java akcije.

Uvod



Kreiranje admin korisnika programski (*after startup*)

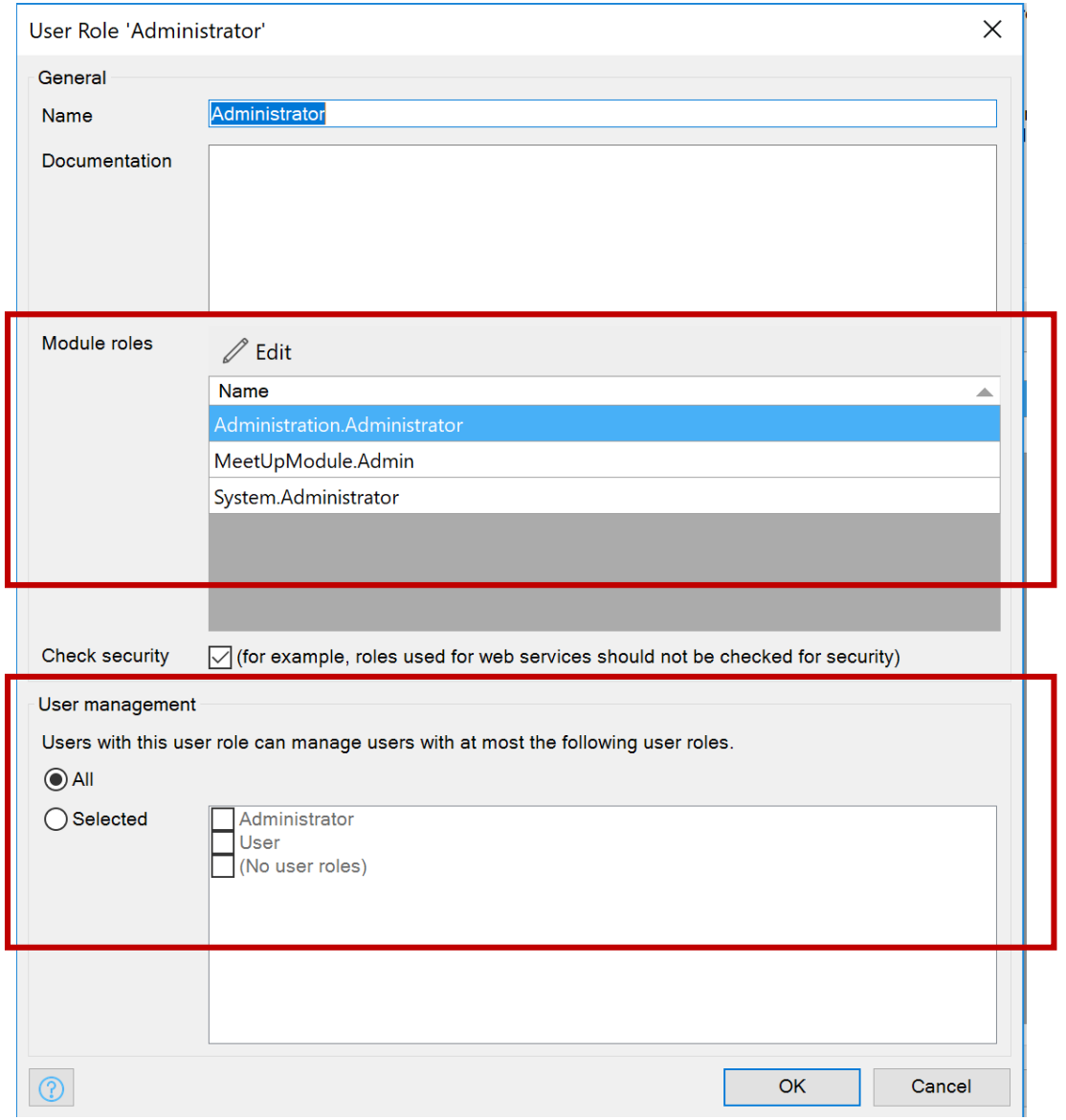
Kontrola pristupa - uloge

- Korisnicima aplikacije se dodeljuju uloge na nivou čitavog projekta (*User roles*)
- Za (funkcionalne) uloge na nivou pojedinačnih modula definišu se pravila pristupa entitetima, *microflow*-ovima i stranicama iz tog konkretnog modula

- Korisničkim ulogama na nivou projekta se dodeljuju uloge na nivou pojedinačnih modula (*Module roles*)
  - Jedna korisnička uloga na nivou projekta može biti uvezana sa više uloga definisanih na nivou jednog pojedačnog modula.
  - Ako, pak, nije ni sa jednom, korisnik koji ima tu korisničku ulogu, nema prava (**direktnog**) pristupa bilo kojim resursima definisanim u okviru tog modula

- Ako se dozvole anonimni korisnici, i njima se mora dodeliti korisnička uloga!

Kontrola pristupa - uloge

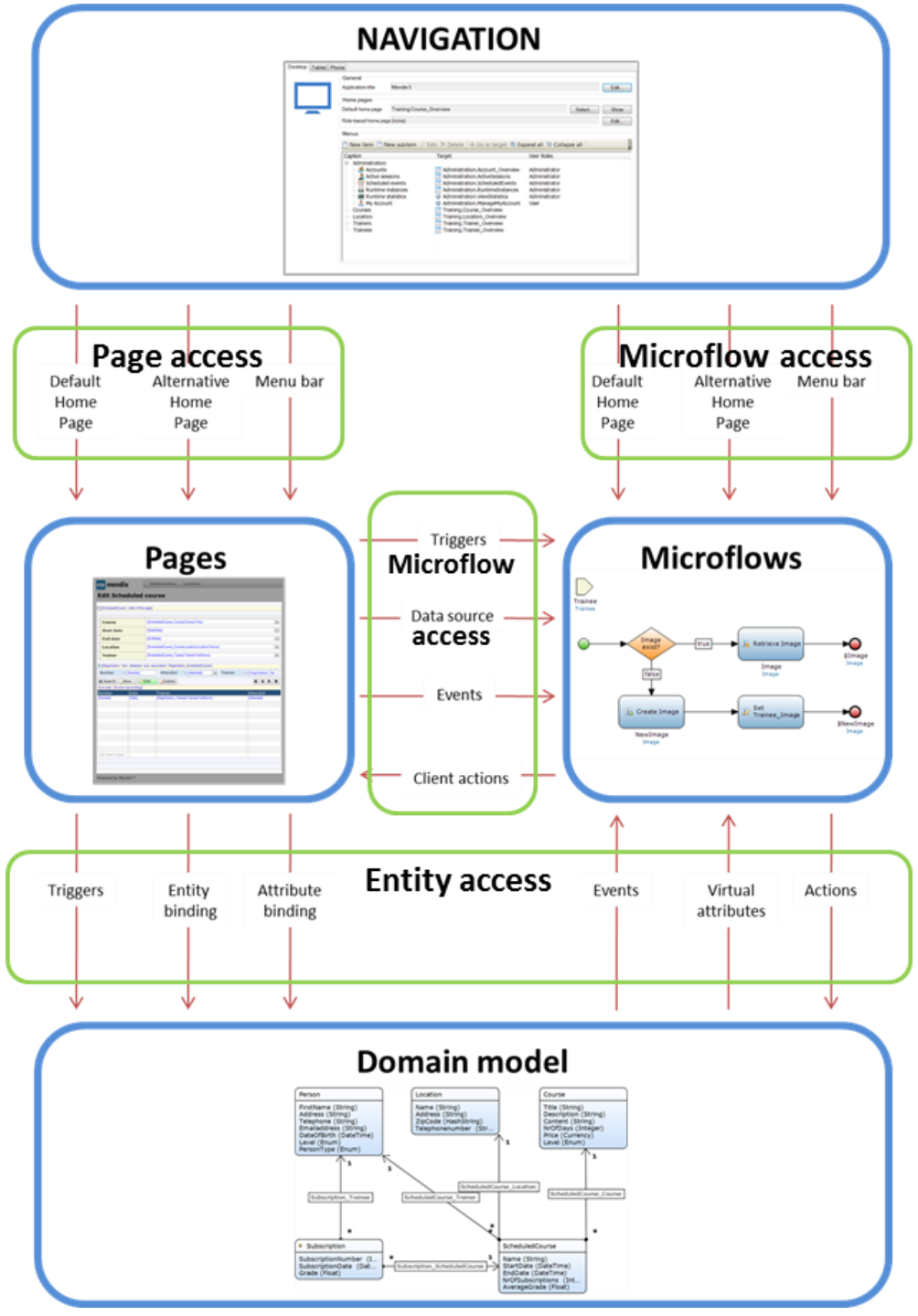


Dodeljivanje uloga na nivou modula korisničkoj ulozi

Kada stepen bezbednosti nije *off, Mendix* vodi računa o tome da se od korisnika sakrije ono čemu on nema (direktan) pristup:

- Ako nema pristup stranici, neće se prikazivati link u navigaciji, niti bilo koje dugme koje na tu stranicu vodi
- Ako nema pristup *microflow*-u, neće mu se prikazati dugme koje ga pokreće
- Neće mu se prikazati entiteti/atributi kojima nema pristup, ili će mu biti onemogućena izmena
- …

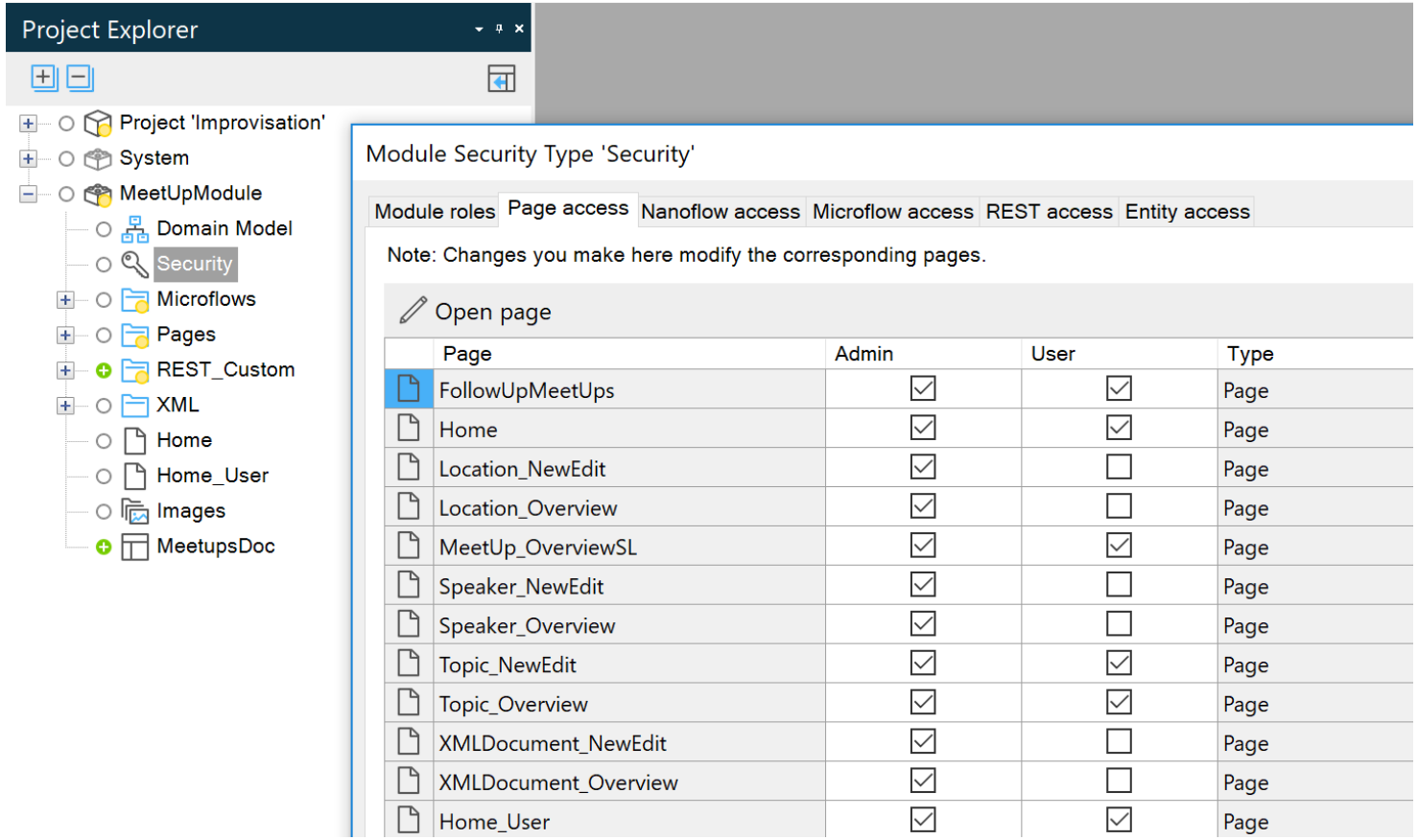
Indirektno, kroz logiku, korisnik može dobiti pristup, na šta bi trebalo obratiti pažnju (kroz submicroflow-ove, event handler-e...)



Kontrola pristupa

Za stranice i logiku, pravila pristupa se podešavaju na nivou modula, za svaku od uloga definisanih u okviru tog modula.

Podešavanje je u vidu matrice, ali je moguće i preko osobina (*properties*) *microflow*-ova (*allowed roles*), i stranica (*visible for*)

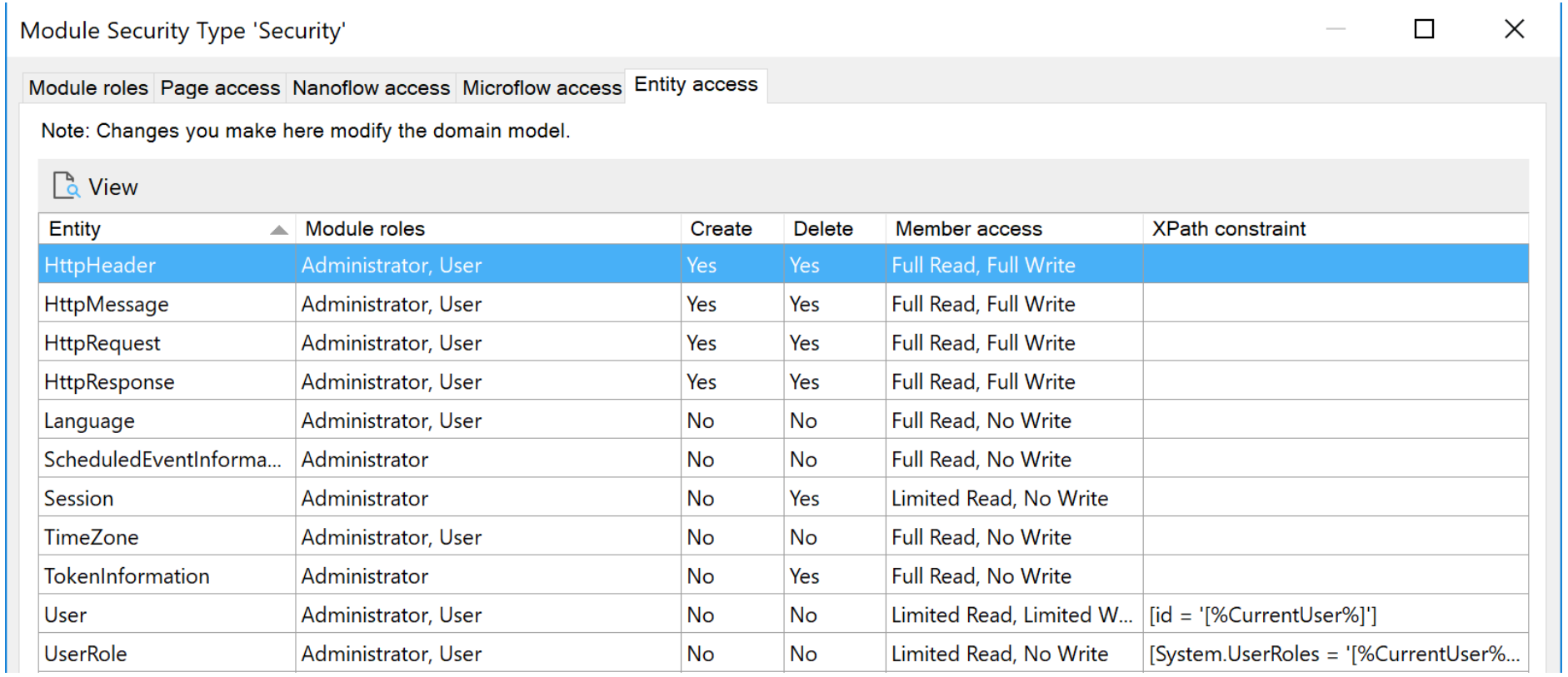


Podešavanje kontrole pristupa na nivou modula

Kontrola pristupa

- Kada su u pitanju pravila pristupa za entitete, definiše se pravo pristupa za CRUD operacije:
  - Definiše se pravo kreiranja i/ili da brisanja objekata entiteta
  - Za svaki atribut pojedinačno se definiše pravo pristupa (Read, Write, -), kao i podrazumevano pravo za svaki novi atribut
  - Pomoću XPath izraza se specificira kojim objektima entiteta je dozvoljen pristup (npr. Korisnik ima pristup samo svom objektu User entiteta); Kada je XPath deo prazan, dozvoljen je pristup svim objektima
  - Specificira se za koje uloge na nivou modula pravilo važi
  - Ova pravila su aditivna! Ako postoji više pravila pristupa istom entitetu za jednu ulogu na nivou modula, kombinovaće se

Kontrola pristupa



Entity	Module roles	Create	Delete	Member access	XPath constraint
HttpHeader	Administrator, User	Yes	Yes	Full Read, Full Write	
HttpMessage	Administrator, User	Yes	Yes	Full Read, Full Write	
HttpRequest	Administrator, User	Yes	Yes	Full Read, Full Write	
HttpResponse	Administrator, User	Yes	Yes	Full Read, Full Write	
Language	Administrator, User	No	No	Full Read, No Write	
ScheduledEventInforma...	Administrator	No	No	Full Read, No Write	
Session	Administrator	No	Yes	Limited Read, No Write	
TimeZone	Administrator, User	No	No	Full Read, No Write	
TokenInformation	Administrator	No	Yes	Full Read, No Write	
User	Administrator, User	No	No	Limited Read, Limited W...	[id = '[%CurrentUser%]']
UserRole	Administrator, User	No	No	Limited Read, No Write	[System.UserRoles = '[%CurrentUser%...

Podešavanje kontrole pristupa
za entitete na nivou modula

Kontrola pristupa

- Na slici ispod je prikazan XPath koji ograničava pravo pristupa samo na korisnika koji je kreirao objekat entiteta (preko *System.owner* atributa nad tim entitetom, koji se dodaje kroz domenski model)
- Pored toga, moguće je definisati da korisnik vidi samo objekte sa kojim je u vezi (ako je korisnik reprezentovan *User* entitetom, ili naslednikom, *Path to user* može da pomogne)

Kontrola pristupa

- Kada su u pitanju pravila pristupa za entitete kroz *microflow*-ove, situacija je malo kompleksnija – kada bi se išlo po pravilu da logika poslovnog procesa uvek ima prava pristupa samo podacima kojima uloga modula ima pristup, to bi potencijalno bilo previše restriktivno. Recimo, akcija pokrenuta od strane korisnika ne bi mogla da rezultuje kreiranjem objekta entiteta koji je za tog korisnika read-only
  - Primer: analitika prometa je primer kada korisnik ima samo pravo čitanja, a nastaje kao rezultat transakcija

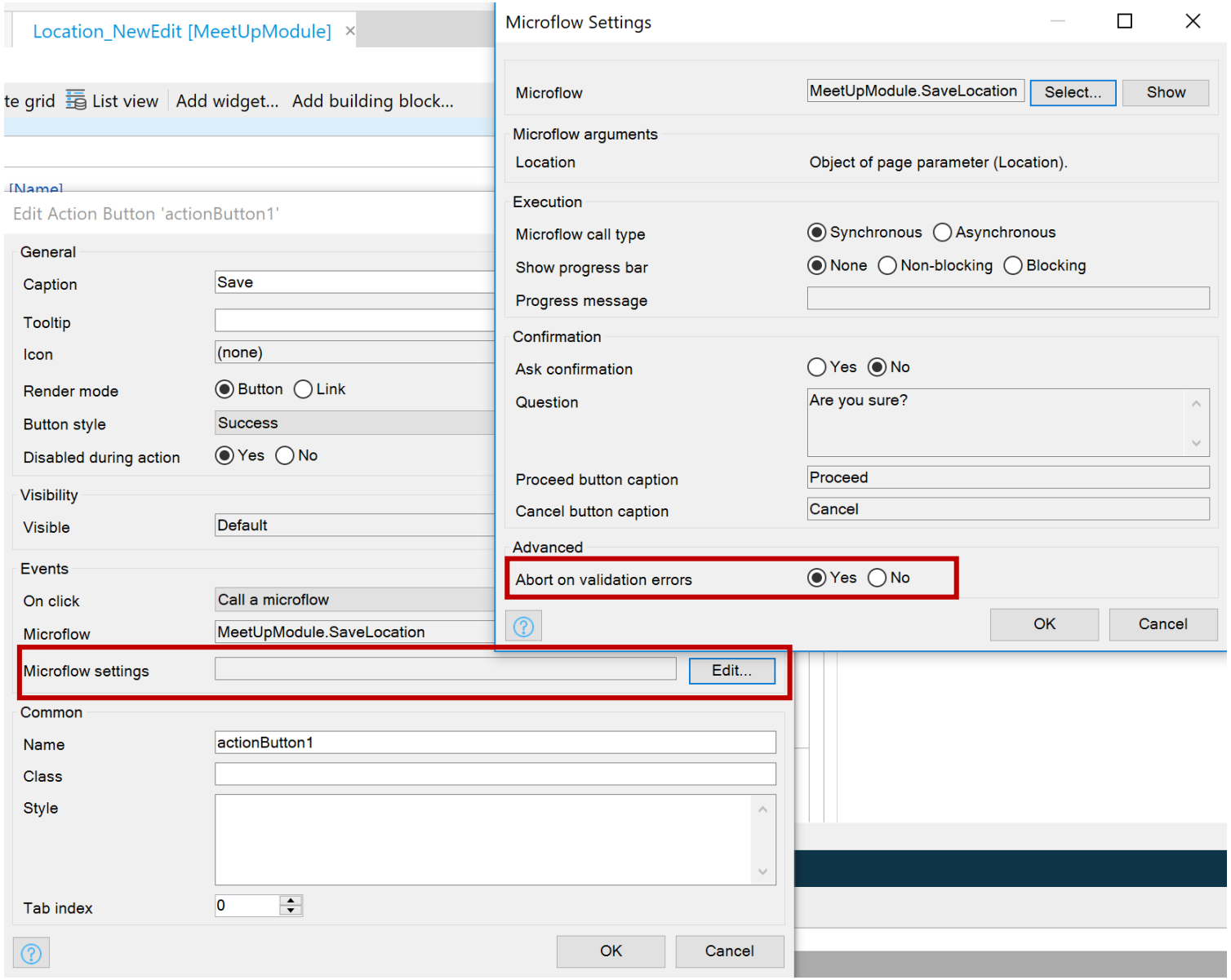
- *Microflow*-ovi imaju osobinu *Apply entity access,* koja je podrazumevano isključena (zbog gore navedenih razloga). Kada se uključi, na sve operacije nad bazom podataka u okviru procesa će biti primenjena pravila pristupa.
- Ovo pravilo se NE propagira u *submicroflow*-ove. Međutim, *microflow* koji ima uključeno ovo pravilo, može biti pozvan samo iz *microflow*-a koji takođe ima.

Validacija podataka

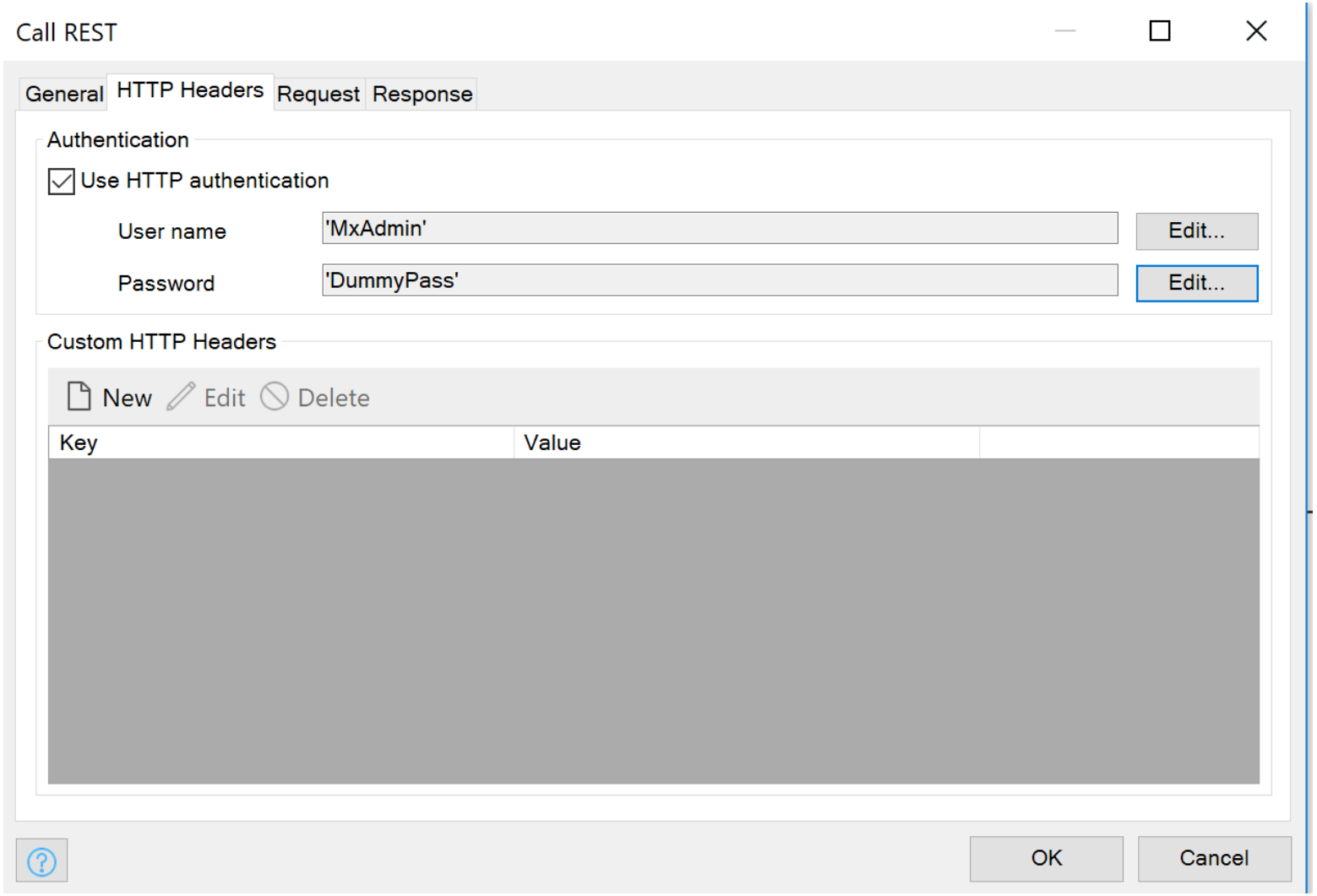
- Podatke je moguće validirati sledeće načine:
  - Ograničenja nad atributima entiteta
  - Validacija kroz logiku u *Before Commit Event Handler* (koji može da vrati *false* ako podaci nisu validni)
  - Validacija kroz poslovni proces *(microflow)* za čuvanje
  - Validacija na samoj formi

- Validacija na samoj formi se izvršava na klijentu
- Ponuđene su različite opcije u zavisnosti od *widget*-a koji se koristi, a moguće je prilagoditi i poruku
- Uglavnom je omogućena i *Custom* opcija za validaciju, pri čemu se specificira izraz za validaciju, u okviru kojeg je dostupan trenutni objekat i uneta vrednost
- Validacija se podrazumevano pokreće za *Save* dugme, ali i za onu što pokreću *Microflow* akcije. To je moguće isključiti (*Microflow settings* u *properties*)

Validacija podataka



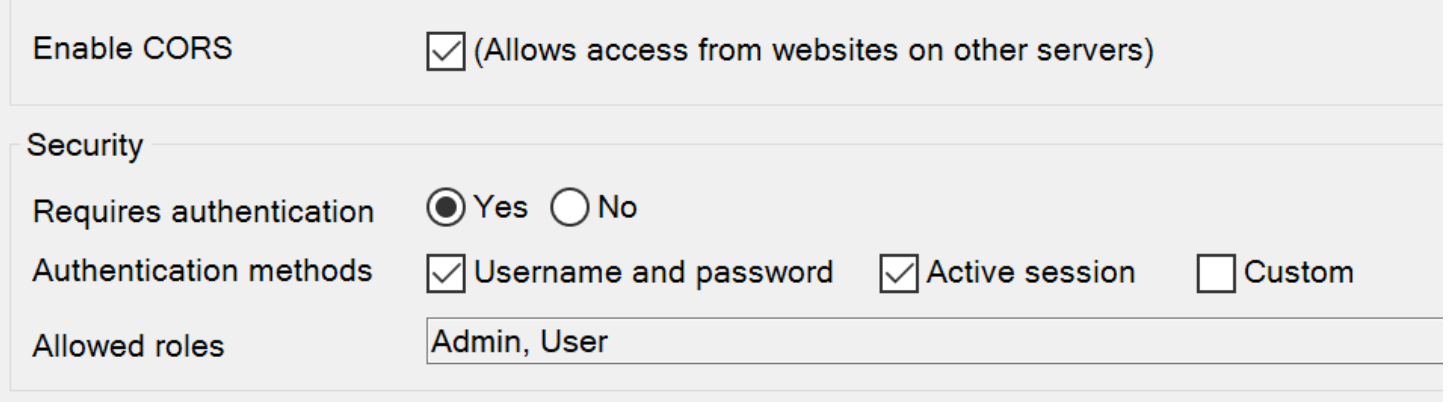
Dodatno - Kontrola pristupa - REST



Primer poziva ka Mx REST putanji za koju je uključena autentikacija – Call REST akcija

Dodatno - Kontrola pristupa - REST

- Za Published REST Service se mogu podesiti CORS pravila i pravila pristupa
- Za autentikaciju se koristi HTTP autentikacija, zasnovana na korisničkom imenu i šifri, mada se može iskoristiti i neka druga (npr. JWT)
- Definišu se uloge koje imaju pristup, i time se specificira pristup svim putanjama



Hvala na pažnji!