UNILAB ACCESS CONTROL SYSTEM v1.0

SISTEM KONTROLE PROLAZA

SADRŽAJ

1. O PROGRAMU

Unilab Access Control System predstavlja software-sko rješenje napredne kontrole prolaza. Sistem je baziran na hardware-u proizvođača IDTECK, koji od 1989. godine proizvodi sofisticiranu opremu kontrole prolaza i radnog vremena.

Unilab Access Control System je realiziran u obliku Microsoft Windows aplikacije, koja omogućava potpunu kontrolu nad hardware-om (kontrolerima prolaza, terminalima radnog vremena, citacima, bravama ...) odnosno, u krajnjem ishodu, ulascima u štićene prostore. Za pohranjivanje esencijalnih podataka o korištenoj opremi, kao i informacija koje se odnose na ulaske u štićene prostore, program koristi pouzdani i jako zastupljeni MySQL server relacionih baza podataka. Sistem nudi mogućnost automatskog backup-a korištene baze, što je jako bitno u incidentnim situacijama, kao što je nepredviđeni kvar na računaru na kojem je software korišten. Software podržava različite načine komunikacije sa hardware-om i to: Ethernet, RS232, RS485, RS422. Nudi se mogućnost kreiranja različitih vrsta izvještaja, kao i rad sa *mrežnim kamerama,* za vizuelnu potvrdu ulazaka u štićene prostore.

Budući da je Unilab Access Control System upotpunosti razvila firma Unilab d.o.o. to smo u mogućnosti odgovoriti na specifične zahtjeve naših klijenata.

2. INSTALIRANJE PROGRAMA

Unilab Access Control System za svoj rad koristi MySQL server, pa iz ovog razloga procesu instaliranja software-a najčešće prethodi instaliranje MySQL servera, kao i kreiranje odgovarajuće baze na serveru. Neophodni instalacioni program za MySQL server je smješten na instalacionom CD-u, u folderu **MySQL Server 5.0.24.** Tokom procesa instalacije, između ostalog, zahtjevaće se unos administratorske šifre **neophodne za rad sa serverom**.

Nakon što smo instalirali MySQL server, možemo preći na kreiranje baze neophodne za rad našeg software-a. Kreiranje baze obavlja se putem *MySQL Command Line Client*-a na slijedeći način:

1) Izvršiti kopiranje **db_uacs_empty.sql** fajla iz foldera **UACS v1.0** (instalacioni CD) na lokaciju C:\
2) Pokrenuti Windows Run dialog (Win + R) i otkucati **cmd**
3) U slučaju da je MySQL server instaliran na C: particiju HDD-a, tada je potrebno putem novootvorenog Windows Command Line Interpreter-a pozicionirati se na lokaciju C:\Program files\MySQL\MySQL Server 5.0\bin
4) Sada je potrebno pozvati MySQL Command Line Client kucanjem komande:
   mysql –u root –p
   Pri ovom pozivu klijent će od korisnika zahtjevati unos administratorske šifre MySQL servera.
5) U slučaju korektnog izvršavanja prethodne komande, uočićemo da daljni rad se obavlja u MySQL client-u. Nakon ovoga je potrebno otkucati komandu:
   CREATE DATABASE uacs;
   a potom i komandu:
   exit
6) U slučaju da su prethodne komande korektno izvršene, možemo se uvjeriti da naš rad se nastavlja u Window Command Line Interpreter-u.
7) Posljednja komanda se odnosi na rekonstrukciju baze iz fajla **db_uacs_empty.sql.** Za ovu rekonstrukciju je potrebno otkucati komandu:
   mysql –u root –p uacs < C:\db_uacs_empty.sql
   Za izvršavanje prethodne komande je neophodan unos administratorske šifra MySQL servera.

Sada kada je baza neophodna za rad našeg programa kreirana na serveru, potrebno je započeti instalaciju našeg programa smještenog u folderu **UACS v1.0** instalacionog CD-a. Po okončanju ove instalacije potrebno je startati program. Primjetićemo da sve kontrole u programu su blokirane, izuzev one koja se odnosi na aktivaciju programa. Proces aktivacije zahtjeva unos aktivacijskog ključa, kojeg generiše firma Unilab d.o.o. Pomenućemo da se radi o dinamičkoj zaštiti programa od neautoriziranog korištenja, što za krajnjeg korisnika znači da program može biti korišten samo sa onim korisničkim account-om, sa kojim je program instaliran. Promjena konfiguracije sistema može za posljedicu imati zaključavanje programa, te u ovom slučaju potrebno nas je kontaktirati radi ponovnog (besplatnog) otključavanja programa.

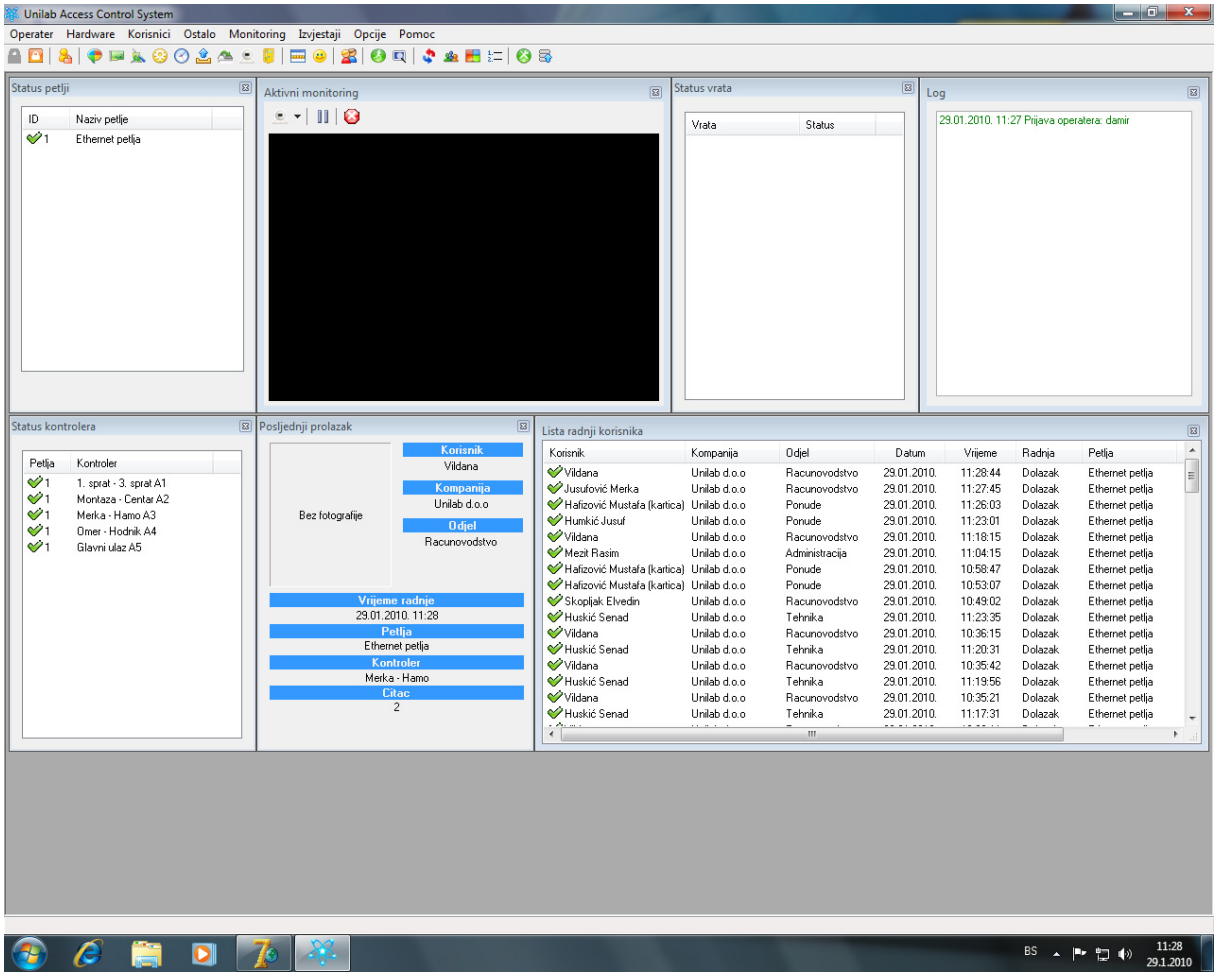
3. PODEŠAVANJE HARDWARE-a KONTROLE PROLAZA

3.1 UVOD

Kontroler prolaza, zajedno za pripadajućim čitačima, predstavlja osnovnu komponentu svakog sistema kontrole prolaza. U najvećem broju slučajeva jedan kontroler nije dovoljan za kontrolu ulazaka u veći broj štićenih prostora, te se iz tog razloga kontroleri vezuju u tkz. petlje kontrolera. U slučaju Unilab Access Control System-a radi se o mogućnosti definisanja do 8 petlji kontrolera, pri čemu u svakoj petlji može egzistirati do 32 kontrolera.

3.2 DEFINISANJE PETLJI KONTROLERA

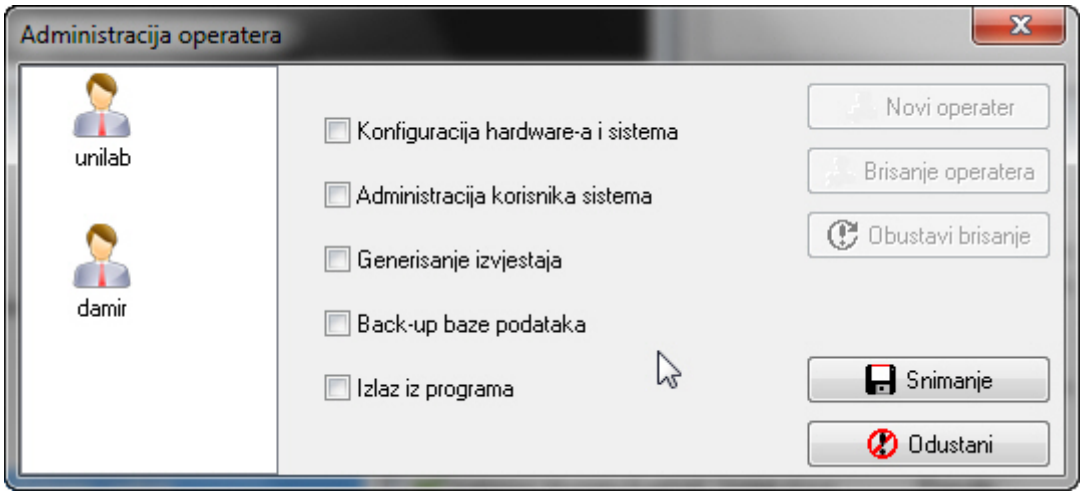
Prije nego što pređemo na razmatranje predmetnog problema upoznajmo se najprije sa glavnim dijelom grafičkog interfejsa aplikacije.



Slika 1. Glavni dio grafičkog interfejsa Unilab Access Control System-a

Kao što se to može vidjeti sa prethodne slike, grafički interfejs aplikacije čini veći broj prozora, jedan glavni meni kao i tkz. toolbar, za brzi pristup opcijama programa. Nakon pokretanja programa sve kontrole, izuzev one za prijavu u program, su blokirane. Na ovaj način se onemogućava neautorizirani rad sa programom. Dakle, da bi smo mogli raditi sa programom, najprije se potrebno prijaviti u program putem stavke "Prijava operatera", koja je smještena u "Operater" meniju. U procesu prijave,

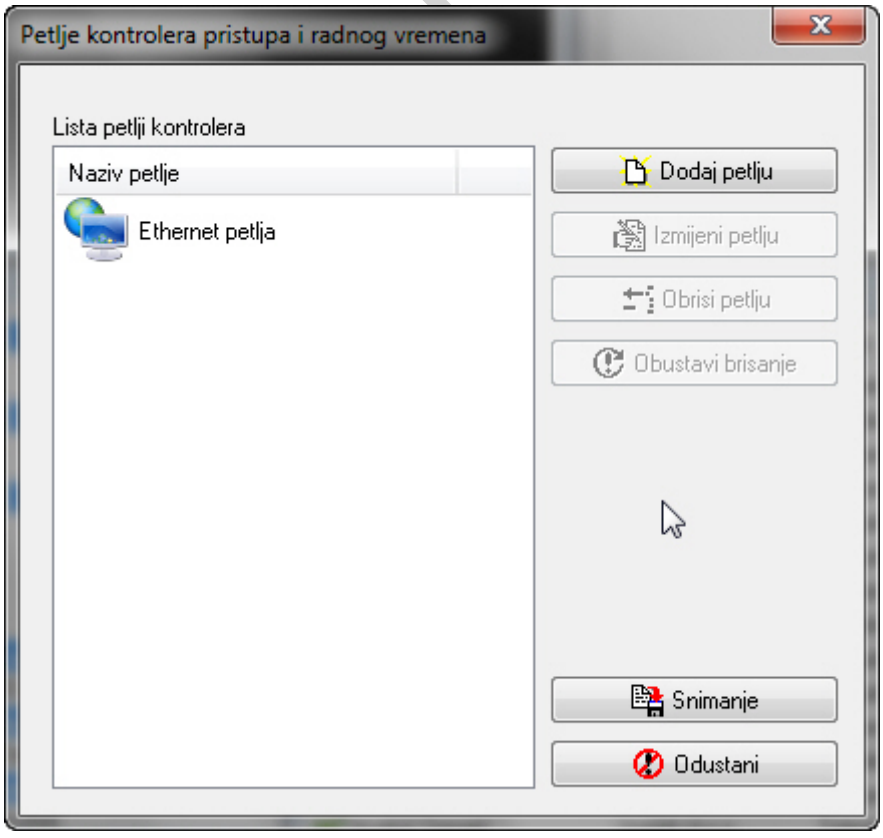
program će zatražiti validno korisničko ime i šifru, te na osnovu ponuđenih informacija omogućiti ili onemogućiti daljni rad. Napomenimo da za svako korisničko ime se vezuju i određena prava za rad sa programom, a koja mogu biti modifikovana putem stavke "Administracija operatera".



Slika 2. Administracija operatera programa

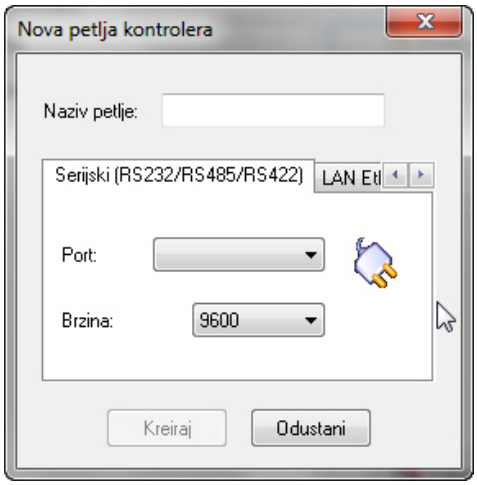
Inicijalno u programu egzistira korisnik "unilab" sa šifrom "unilab", koji ima potpuna prava za rad sa programom.

Sada kada nam je poznat način prijave operatera u program, kao i njihova administracija, pređimo na ažuriranje petlji kontrolera. Ažuriranje petlji kontrolera obavlja se putem stavke "Petlje kontrolera" smještene u "Hardware" meniju. Odabirom pomenute stavke pojavljuje se dialog, kojeg prikazuje slijedeća slika.



Slika 3. Ažuriranje petlji kontrolera pristupa i radnog vremena

Za dodavanje nove petlje potrebno je kliknuti na dugme sa nazivom "Dodaj petlju". Ovom radnjom će biti prikazan slijedeći dialog:

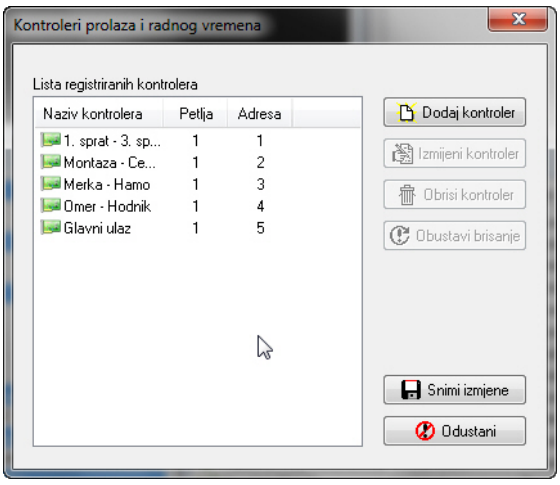


Slika 4. Dodavanje nove petlje kontrolera

Od operatera se zahtjeva unos naziva nove petlje, kao i način komunikacije software-a sa petljom. Nakon unosa zahtjevanih parametara, program će se ponovo vratiti na prethodni dialog (koji je izmjenjen dodavanjem nove petlje). Za konačnu potvrdu unosa potrebno je kliknuti na dugme sa nazivom "Snimanje" (Slika 3). Nakon pomenute potvrde program će pokušati uspostaviti vezu sa svim prijavljenim petljama. Ispravnost komunikacije moguće je verifikovati putem prozora sa nazivom "Status petlji" (slika 1). Ikona pored naziva petlje ukazuje na problem komunikacije sa petljom. Izmjenu parametara postojeće petlje moguće je obaviti klikom na dugme "Izmijeni petlju", dok brisanje petlje putem dugmeta "Obrisi petlju". Kao i u slučaju dodavanja nove petlje, konačna potvrda ivršenih radnji se obavlja klikom na dugme "Snimanje" (slika 3).

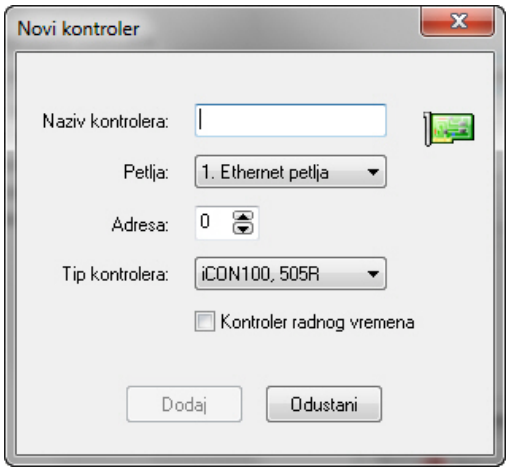
3.3 DEFINISANJE KONTROLERA PRISTUPA

Nakon što smo upoznati sa ažuriranjem petlji kontrolera, pređimo na ažuriranje liste samih kontrolera. Ovo ažuriranje se obavlja odabirom stavke "Kontroleri pristupa i radnog vremena" iz "Hardware" menija. Slijedeća slika prikazuje dialog, putem kojeg se vrše ova ažuriranja.



Slika 5. Ažuriranje kontrolera pristupa i radnog vremena

Za dodavanje novog kontrolera potrebno je kliknuti na dugme "Dodaj kontroler". Ovim će biti prikazan slijedeći dialog:

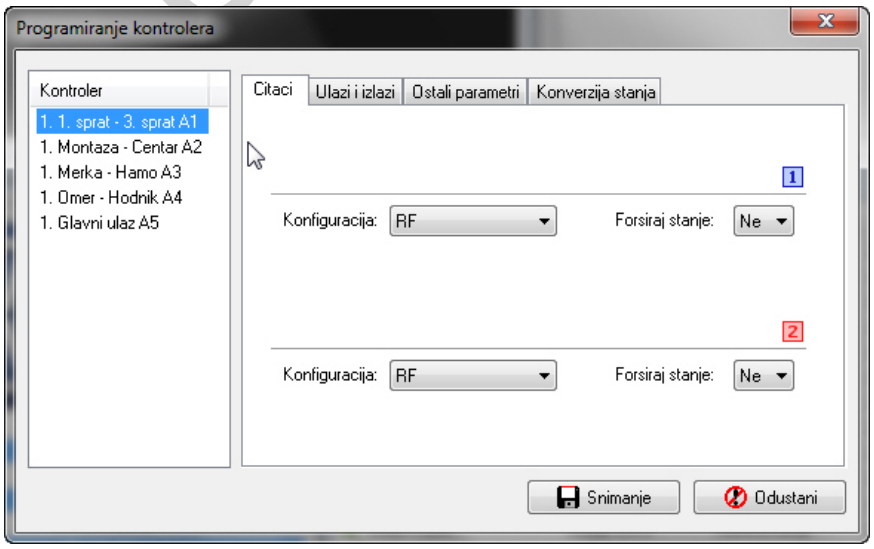


Slika 6. Dodavanje novog kontrolera

Kao što se to može vidjeti sa prethodne slike, od operatera se zahtjeva unos naziva kontrolera (poželjno je da naziv asocira na odgovarajući štićeni prostor), petlje u kojoj se kontroler fizički nalazi, adrese kontrolera kao i tipa kontrolera. U slučaju da se radi o terminalu radnog vremena, predviđenog za evidenciju radnog vremena uposlenika, potrebno je označiti stavku "Kontroler radnog vremena". Kao i u slučaju dodavanje petlji kontrolera, tako i u slučaju dodavanja novog kontrolera, za konačnu potvrdu poduzetih radnji potrebno je kliknuti na dugme "Snimi izmjene" (slika 5). Izmjenu parametara postojećeg kontrolera moguće je obaviti klikom na dugme "Izmijeni kontroler", dok brisanje kontrolera se obavlja klikom na dugme "Obriši kontroler" (slika 5). Ispravnost komunikacije software-a sa pojedinim kontrolerima je moguće verifikovati putem prozora "Status kontrolera" (slika 1).

3.4 PROGRAMIRANJE KONTROLERA

Programiranje kontrolera se obavlja putem posebnog dialoga, koji se poziva odabirom istoimene stavke u "Hardware" meniju. Slijedeća slika prikazuje pomenuti dialog:

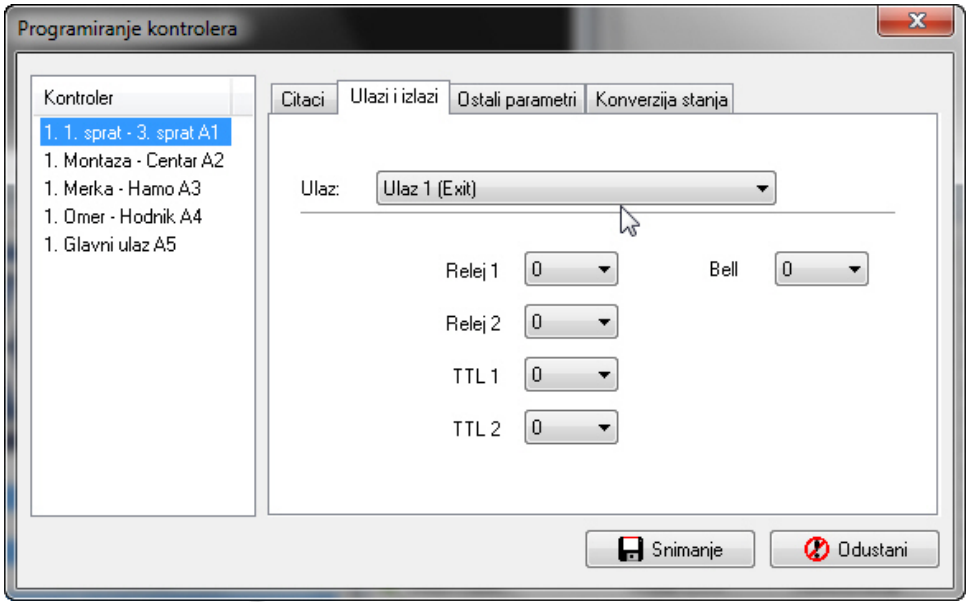


Slika 7. Programiranje kontrolera

Sa prethodne slike vidimo da na lijevoj strani dialoga se nalazi lista prijavljenih kontrolera, dok se na desnoj strani nalaze palete mogućih programskih opcija. Nakon što označimo željeni kontroler (klik na naziv kontrolera), potrebno je najprije odabrati željenu programsku paletu (Čitači, Ulazi i izlazi, Ostali parametri, Konverzija stanja). Putem palete sa nazivom "Čitači" vrši se podešavanje kontrolerskih ulaza, predviđenih za povezivanje čitača. Napomenimo da svaki kontroler ima dva ulaza predviđena za povezivanje čitača. Postoje različite implementacije čitača. Neki od njih pored što mogu vršiti očitanje bezkontaktnih kartica, sadrže i tastaturu putem koje je moguće unositi šifru ili PIN. Dakle, postoje tri načina rada kontrolera u pogledu čitača. Prvi način rada je vezan za čitače koji samo mogu vršiti očitanje RF kartica. Ovaj način rada je označen kao "RF" (pogledati sliku 7). Ukoliko je potrebno da kontroler pored kartice zahtjeva i unos odgovarajuće šifre, onda je potrebno odabrati "RF+PW" način rada kontrolera. Posljednja opcija se odnosi na korištenje PIN-a kao autentikacijskog parametra.

Sa slike 7 uočavamo polja koja su označena kao "Forsiraj stanje". Ova polja imaju važnu ulogu u evidenciji radnog vremena, obzirom da označavaju radnje koje uposlenici mogu obavljati (Dolazak na posao, Kraj radnog vremena, Pauza, Službeni odlazak, ...). Kada je u pitanju kontrola prolaza reći ćemo da stanje sa vrijednosti 1 označava radnju Dolaska/Ulaska, dok sva ostala stanja označavaju radnju Odlaska/Izlaska.

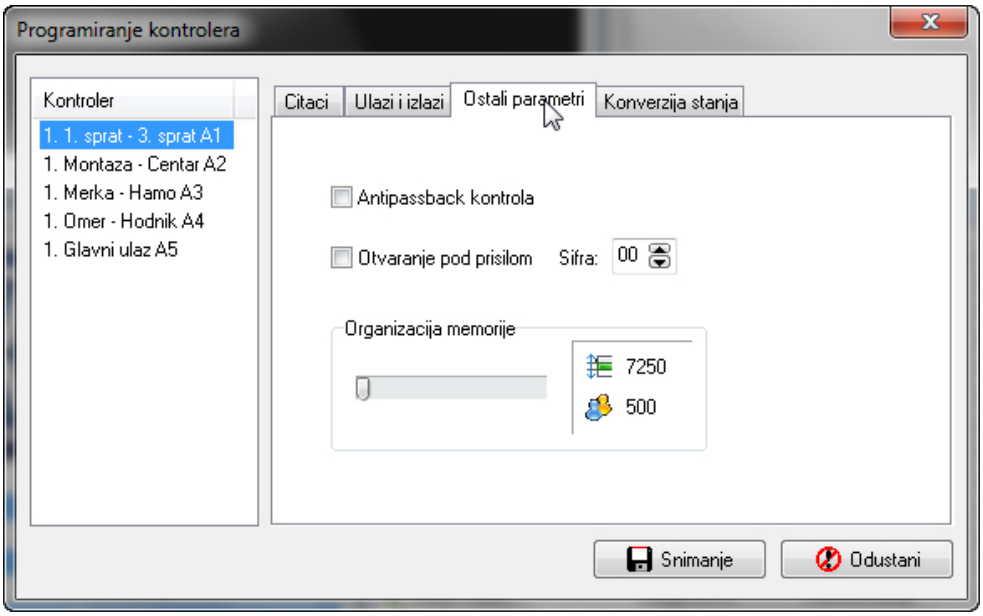
Veza između kontrolerskih ulaza i izlaza se obavlja putem palete "Ulazi i izlazi". Sadržaj ove palete je prikazan na slijedećoj slici:



Slika 8. Programiranje veza ulaza i izlaza kontrolera

Na ovoj paleti je bitno izdvojiti dvije cjeline (odvojene horizontalnom crtom). Gornja cjelina, koja je nazvana "Ulaz", sadrži listu mogućih ulaznih pobuda kontrolera, dok dornja cjelina sadrži vremenske vrijednosti reakcije izlaza kontrolera na ulaznu pobudu. Sa prethodne slike vidimo da promjene na digitalnom ulazu 1 nece biti pracene promjenama na izlazima kontrolera. Ukoliko bi neki od izlaza imao vrijednost različitu od 0, to bi značilo da će taj izlaz biti aktivan definisani broj sekundi, na njemu pripadajuću ulaznu pobudu. Putem ove palete se definiše vrijeme aktivnosti brave, neophodno za otvaranje vrata.

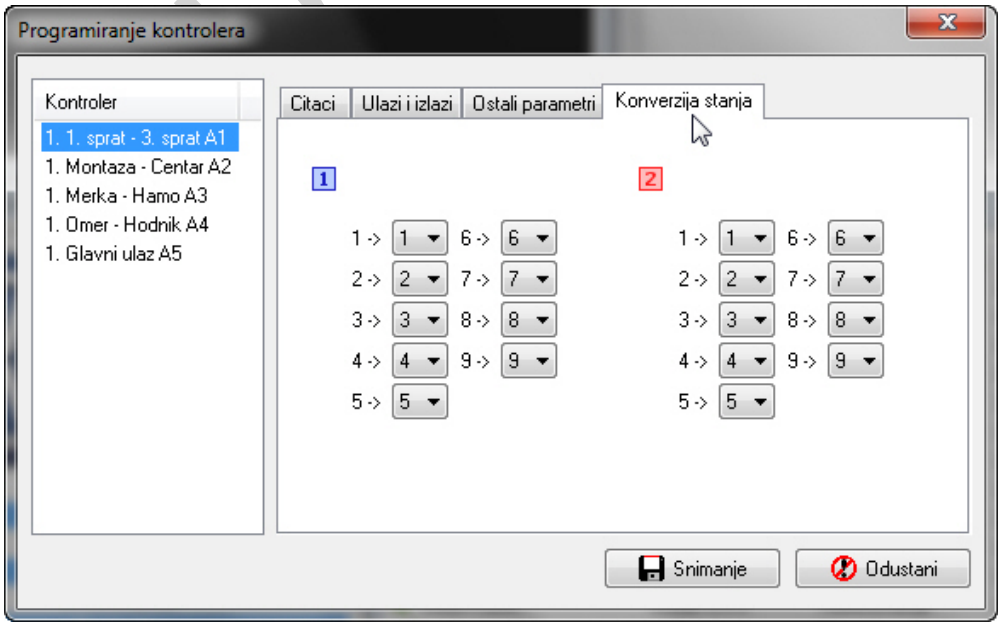
Paleta sa nazivom "Ostali parametri" sadrži opcije vezane za *Antipassback kontrolu,* otvaranje vrata pod prisilom, kao i konfigurisanje memorije kontrolera. Na slijedećoj slici se može vidjeti sadržaj razmatrane palete.



Slika 9. Podešavanje antipassback-a, memorije kontrolera te šifre otvaranja pod prisilom

Pod antipassback kontrolom se podrazumjeva funkcija blokade uzastopnog korištenja jednog čitača kontrolera. Naime, kada se aktivira ova opcija kontroler očekuje naizmjenično korištenje čitača. Ova opcija se često koristi pri kontroli ulazaka u prostorije od posebnog značaja. U ovakvim okolnostima jedan od čitača je namijenjen za ulaz u prostor, dok je drugi namijenjen za izlaz iz tog prostora. Ukoliko je kartica iskorištena za ulaz u prostor, antipassback kontrola određuje da njeno slijedeće korištenje može biti samo za izlaz iz prostora, a nikako za ponovni ulaz.
Za korištenje funkcije pod nazivom "Otvaranje pod prisilom" potrebno je da čitači posjeduju odgovarajuću tastaturu. Ukoliko korisnik unese šifru prisile, software će operatera o tome obavijestiti na poseban način. Također, moguće je podesiti hardware-sku reakciju kontrolera na unos šifre prisile. Naime, kontroler može aktivirati jedan ili više svojih izlaza ukoliko je bila unešena šifra prisile.

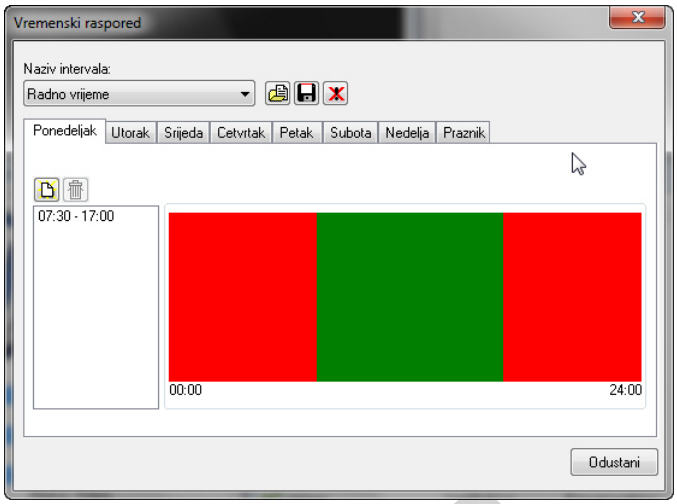
Paleta "Konverzija stanja" se odnosi isključivo na sistem evidencije radnog vremena. Budući da u samom kontroleru svaki funkcijski taster ima predefinisano stanje, koje nije moguće mijenjati, to ova paleta nudi software-sko rješenje ovog problema. Sadržaj palete prikazuje slijedeća slika.



Slika 10. Konverzija stanja kontrolera

3.5 VREMENSKI RASPOREDI

Čest zahtjev u sistemima kontrole prolaza je vremensko ograničavanje korisnika na korištenje sistema. Da bi smo nekog korisnika vremenski ograničili na korištenje sistema, potrebno je kreirati vremenski raspored koji odgovara pomenutom ograničenju. Ovi rasporedi se ažuriraju putem dialoga, koji je dostupan odabirom stavke "Vremenski raspored" u "Hardware" meniju.

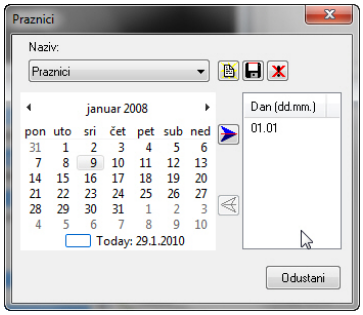


Slika 11. Vremenski rasporedi

Na operateru programa je da za svaki dan definiše validne vremenske intervale korištenja sistema (na prethodnoj slici zeleni segment) te da ovom rasporedu da odgovarajući naziv. Na prethodnoj slici uočavamo nekoliko dugmadi. Dugmadi pored naziva intervala se odnose na kreiranje novog rasporeda, spašavanje izmjena nad odabranim rasporedom te brisanje odabranog rasporeda, sukcesivno. Ispod ovog dijela nailazimo na dva nova dugmeta i to: dugme za dodavanje novog intervala i dugme za brisanje selektovanog intervala. Napomenimo da **svaki dan je moguće podijeliti na do 5 intervala i da je ukupno moguće kreirati do 10 vremenskih rasporeda**, što predstavlja hardware-sko ograničenje sistema.

3.6 PRAZNICI

Na prethodnoj slici je moguće uočiti paletu sa nazivom "Praznik". Putem ove palete je moguće napraviti posebno vremensko ograničenje korisnika u vrijeme praznika. Da bi smo koristili ovu opciju, potrebno je da najprije definišemo koji dani su praznici. Definisanje praznika se obavlja odabirom stavke "Praznici", smještene u "Hardware" meniju. Na slijedećoj slici je prikazan dialog za ažuriranje praznika.

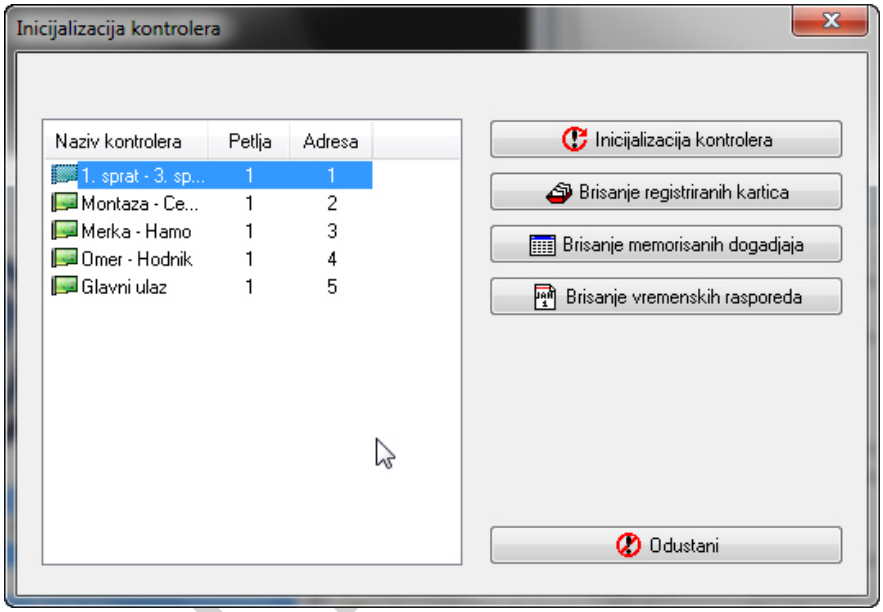


Slika 12. Ažuriranje praznika

Dodavanje novog dana u listu praznika se obavlja označavanjem željenog dana i klikom na dugme koje pokazuje desno od kalendara, dok brisanje dana iz liste praznika se obavlja označavanje tog dana u listi i klikom na dugme koje pokazuje lijevo od kalendara. Konačna potvrda napravljenih izmjena se obavlja putem dugmeta koje sadrži ikonicu sa disketom. Pored pomenutih kontrola postoje dva dugmeta, koja se koriste za dodavanje nove grupe praznika, kao i brisanje selektovane grupe praznika.

3.7 INICIJALIZACIJA KONTROLERA

Pod inicijalizacijom kontrolera podrazumijevamo vraćanje pojedinih opcija kontrolera na fabričke postavke. Inicijalizacija kontrolera se obavlja putem istoimenog dialoga, koji se aktivira odabirom stavke "Inicijalizacija kontrolera" u "Hardware" meniju. Na slijedećoj slici je prikazan dialog za inicijalizaciju kontrolera.

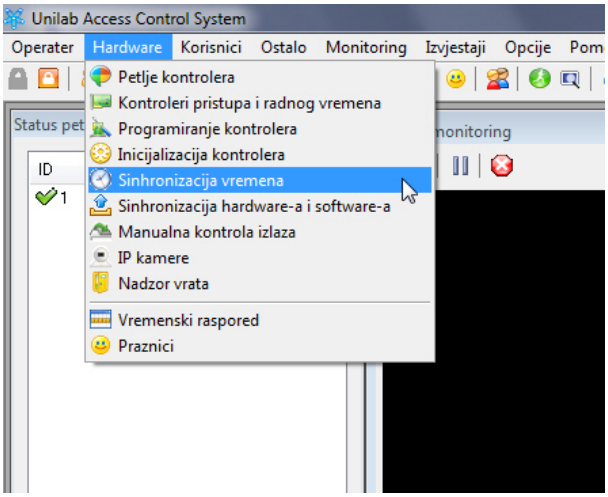


Slika 11. Inicijalizacija kontrolera

Sa prethodne slike uočavamo da lijevi dio sadrži listu kontrolera, dok desni moguće načine inicijalizacije. Dugme sa nazivom "Inicijalizacija kontrolera" se koristi za vraćanje svih postavki kontrolera na fabrički predefinisane vrijednosti. "Brisanje registriranih kartica", kao što i sam naziv upućuje, označava brisanje svih memorisanih kartica u kontroleru. Događaje smještene u memoriji kontrolera je moguće obrisati putem istoimene opcije, dok sve vremenske rasporede definisane u kontroleru, je moguće obrisati putem dugmeta sa nazivom "Brisanje vremenskih rasporeda".

3.8 PODEŠAVANJE SATA REALNOG VREMENA KONTROLERA

IDTECK kontroleri pristupa i radnog vremena su opremljeni satom realnog vremena, koji se koristi pri mnogim radnjama kontrolera. Tako npr. kontroler odluka o dozvoli ili odbijanju nekog korisnika da koristi sistem, donosi poredeći tekuće vrijeme sata realnog vremena sa dozvoljenim vremenom definisanim kroz prava tog korisnika. Svi događaji koje kontroleri generišu sadrže "vremenske pečate" generisane ovim satom. Iz navedenog je moguće zaključiti da ovaj sat, i njegova tačnost, imaju značajnu ulugu u cijelom sistemu kontrole prolaza. Podešavanje sata realnog vremena se obavlja odabirom stavke "Sinhronizacija vremena " smještene u "Hardware" meniju. Slijedeća slika prikazuje pomenutu stavku.

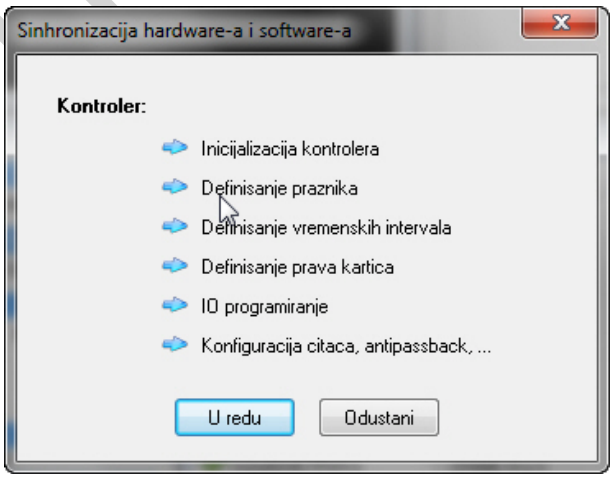


Slika 12. Sinhronizacija vremena kontrolera i računara

Odabirom ove stavke Unilab Access Control System će pokrenuti proces sinhronizovanja sata realnog vremena svih prijavljenih kontrolera sa satom računara na kojem je program pokrenut. Također je bitno napomenuti da je program opremljen mehanizmom automatske sinhronizacije vremena, koja se obavlja svaka 24 sata rada programa.

3.9 SINHRONIZACIJA HARDWARE-a I SOFTWARE-a

Proces sinhronizacije hardware i software-a podrazumijeva radnje koje poduzima Unilab Access Control System, kako bi održao jednakost konfiguracija spremljenih u samom software-u, kao i onih koje su smještene u harware-u (kontrolerima). Ova sinhronizacija se upotrebljava isključivo u situacijama gdje se mogu pojaviti pomenute razlike, kao što je fizička zamjena nekog od kontrolera. Da bi smo izvršili usaglašavanje konfiguracija potrebno je odabrati stavku "Sinhronizacija hardware-a i software" iz "Hardware" menija (pogledati prethodnu sliku). Ovom radnjom će biti prikazan slijedeći dialog:

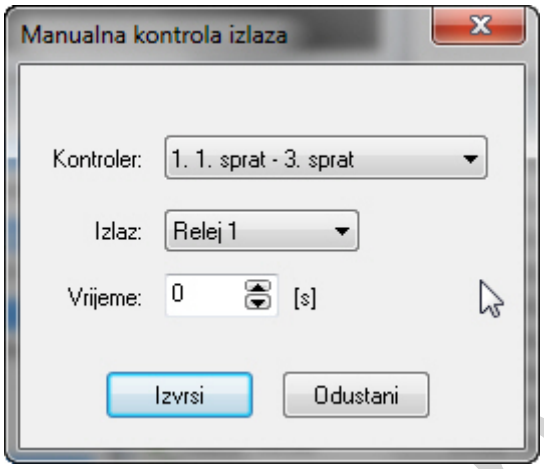


Slika 13. Sinhronizacija hardware-a i software-a

Proces sinhronizacije se odvija u šest koraka. Prvi korak je inicijalizacija kontrolera, kojim se obezbjeđuje vraćanje postavki kontrolera na fabrički definisane vrijednosti. Nakon ovog koraka slijedi definisanje praznika, vremenskih rasporeda, prava korisnika sistema, kao i programiranje veza ulaza i izlaza, konfigurisanje čitača, antipassback-a i sličnog. Važno je napomenuti da ovaj proces mora proći bez greške, kako bi sistem funkcionisao na željeni način.

3.10 MANUALNA KONTROLA IZLAZA

Opcija manualne kontrole izlaza obezbijeđuje direktno upravljanje izlazima kontrolera putem software-a. Ova opcija se nalazi u "Hardware" meniju, pod istoimenom stavkom (pogledati sliku 12). Slijedeća slika prikazuje dialog namijenjen upravljanju izlazima kontrolera.

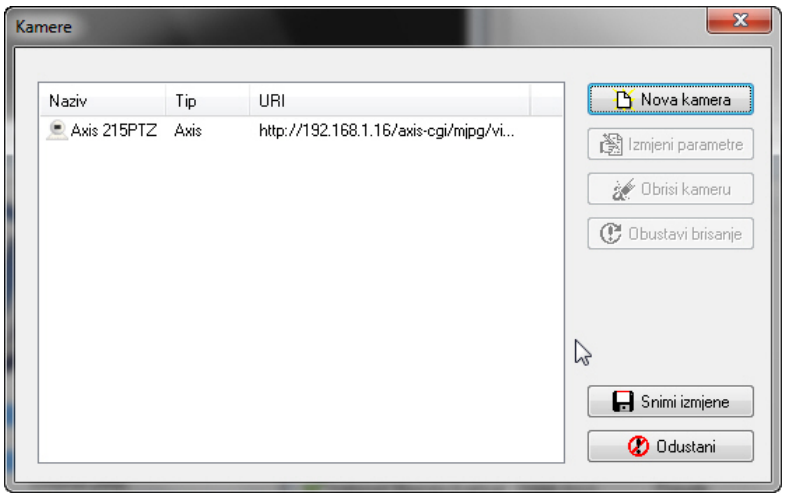


Slika 14. Manualna kontrola izlaza

Sa prethodne slike izdvojićemo tri bitne cjeline. Prva od njih se odnosi na kontroler, čije ulaze želimo direktno kontrolisati. Druga cjelina sadrži listu mogućih izlaza kontrolera (Relej 1, Relej 2, TTL1, ...). Putem ove liste se odabire izlaz na kontroleru, čije stanje želimo promijeniti. Na kraju dolazimo do cjeline koja se odnosi na vrijeme trajanja promjene izlaza kontrolera. Važno je napomenuti da **vrijednost od 99s označava trajnu promjenu stanja izlaza kontrolera**.

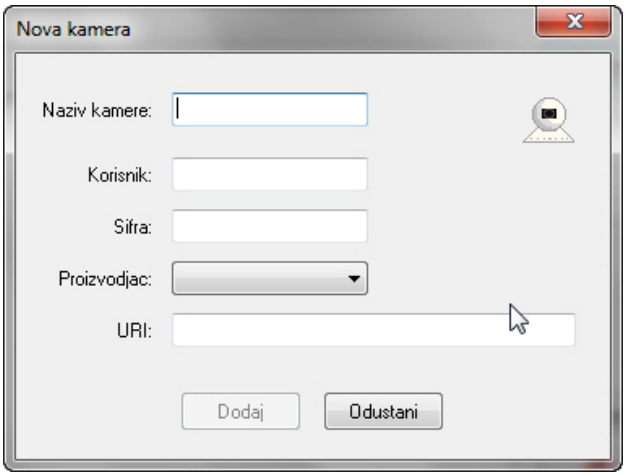
3.11 IP KAMERE

Unilab Access Control System nudi mogućnost rada sa mrežnim kamerama u cilju vizuelne potvrde nekih događaja u sistemu kontrole prolaza. Software trenutno podržava rad sa mrežnim kamerama proizvođača: Axis, Sony, Planet i TrendNET. Za ažuriranje mrežnih kamera potrebno je odabrati stavku "IP kamere" iz "Hardware" menija.



Slika 15. Ažuriranje mrežnih kamera

Dodavanje nove kamera se obavlja klikom na dugme sa nazivom "Nova kamera". Ovim će biti prikazan slijedeći dialog:

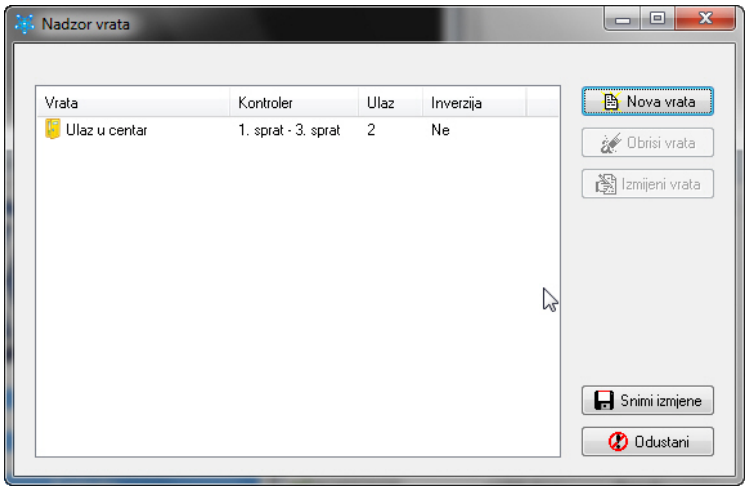


Slika 16. Dodavanje nove kamere

Od operatera se zahtjeva unos naziva kamere (poželjno da asocira na prostor koji kamera snima), korisničkog imena i šifre neophodnih za pristup kameri, proizvođača kamere kao i URI-a koji pokazuje na putanju do MJPEG stream-a (pogledati prilog B). Važno je napomenuti da URI direktno zavisi od IP adrese kamere, kao i proizvođača kamere. Kao što je to bio slučaj sa drugim opcijama programa, krajnja potvrda ažuriranja liste kamera se obavlja klikom na dugme sa nazivom "Snimi izmjene" (Slika 15).

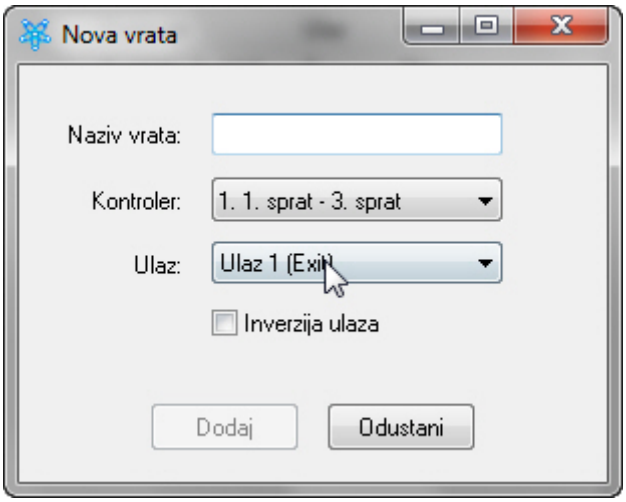
3.12 NADZOR OTVORENOSTI/ZATVORENOSTI VRATA

U sistemima kontrole prolaza nekad se nameće zahtjev monitoringa zatvorenosti/otvorenosti pojedinih vrata, koja su pod kontrolom samog sistema. Za realizaciju ove funkcije obično se koriste magnetni senzori povezani sa kontrolerima, koji govore o stanju vrata tj. da li su vrata otvorena ili zatvorena. Kada je u pitanju software, potrebno je označiti na kojim ulazima kontrolera su povezani magnetni senzori, a sam nadzor otvorenosti/zatvorenosti vrata se obavlja putem posebnog prozora, koji je nazvan "Status vrata" (pogledati sliku 1). Da bi smo odredili ulaze na koje su povezani pomenuti magnetni senzori odaberimo stavku "Nadzor vrata" u "Hardware" meniju. Ovim će biti prikazan slijedeći dialog:



Slika 17. Ažuriranje liste nadziranih vrata

Nova vrata možemo dodati klikom na istoimeno dugme, čime će biti prikaza slijedeći dialog:



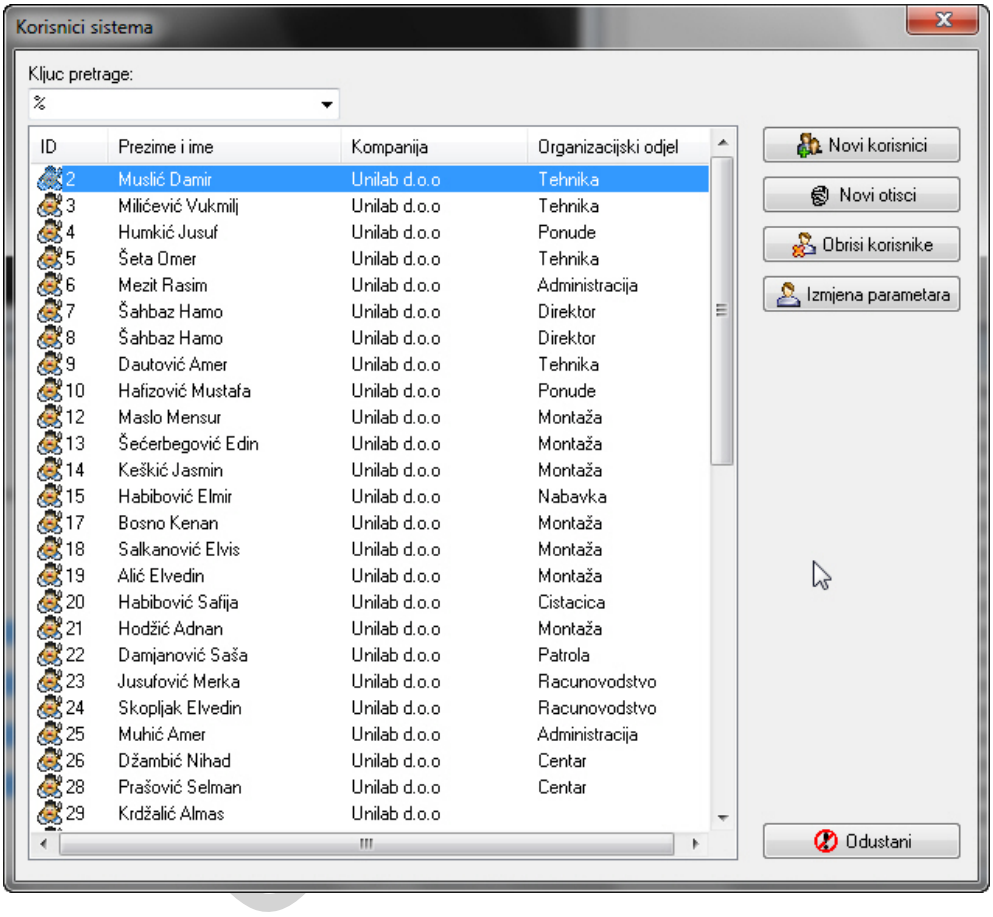
Slika 18. Dodavanje novih vrata u sistem nadzora

Kao što se to može vidjeti sa prethodne slike, potrebno je najprije odrediti naziv novim vratima, kontroler koji njima upravalja i na čiji je ulaz povezan magnetni senzor, te na kraju sam ulaz na koji je senzor povezan. Pored pomenutih parametara pojavljuje se i opcija sa nazivom "Inverzija ulaza", koja se koristi u slučaju potrebe invertovanja stanja ulaza kontrolera.

4. AŽURIRANJE KORISNIKA SISTEMA

4.1 DODAVANJE NOVIH KORISNIKA

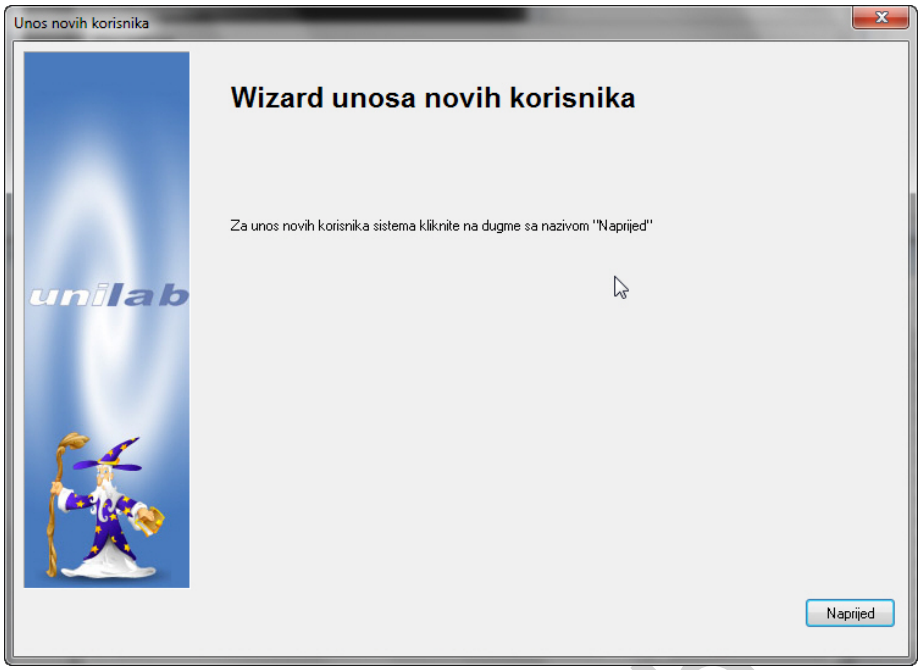
Ažuriranje liste korisnika sistema obavlja se putem posebnog dialoga, koji biva prikazan odabirom stavke "Korisnici sistema" u "Korisnici" meniju.



Slika 19. Ažuriranje korisnika sistema

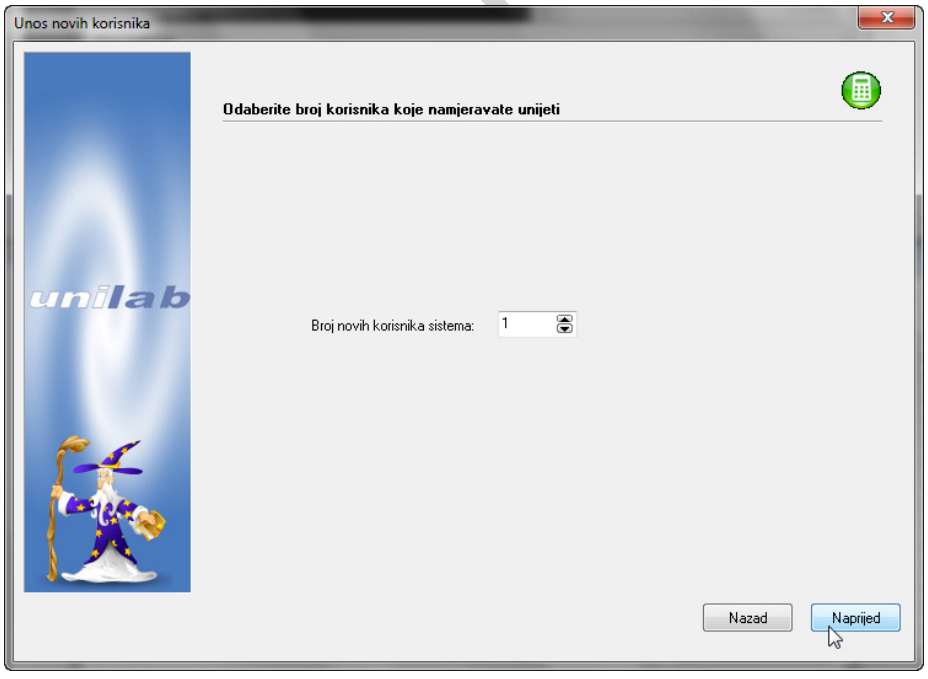
Prije nego što pređemo na razmatranje procesa unosa novih korisnika reći ćemo da "Ključ pretrage" se koristi za brzo pronalaženje željenog korisnika. Naime, dovoljno je napisati dio imena ili prezimena korisnika pa da program pronađe sve one koji ispunjavaju traženi uslov. Da bi smo prikazali sve prijavljene korisnike sistema dovoljno je za ključ pretrage iskoristiti znak %.

Kada su u pitanju novi korisnici, potrebno je kliknuti na istoimeno dugme, čime će biti prikazan slijedeći "Wizard".



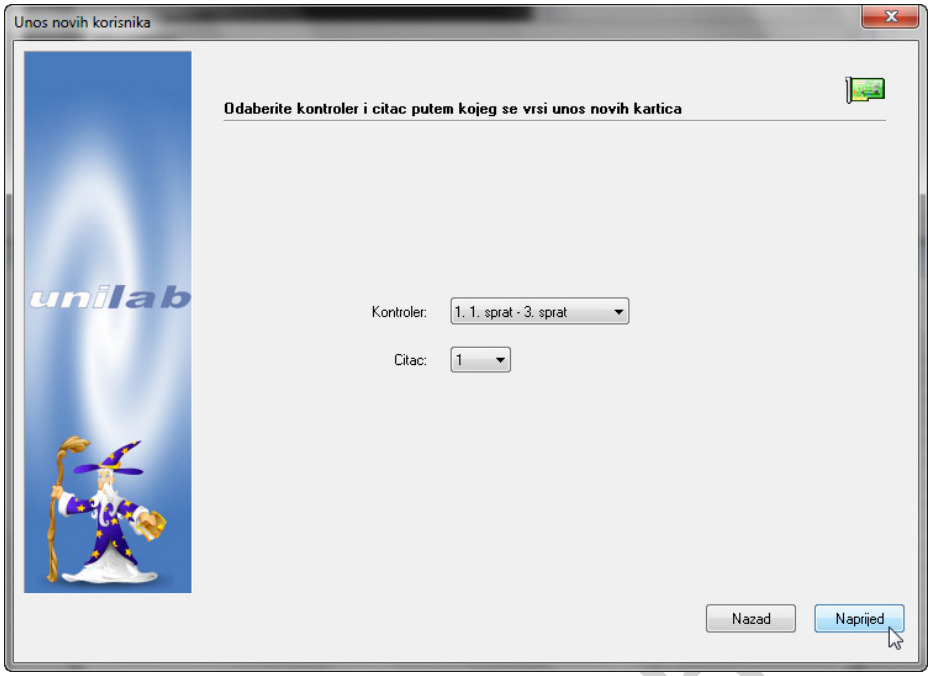
Slika 20. Wizard unosa novih korisnika

Proces unosa novih korisnika od operatera zahtjeva veći broj informacija, koje se traže kretanjem kroz pomenuti wizard. U prvom koraku od operatera se zahtjeva saopštavanje broja novih korisnika što prikazuje slijedeća slika:



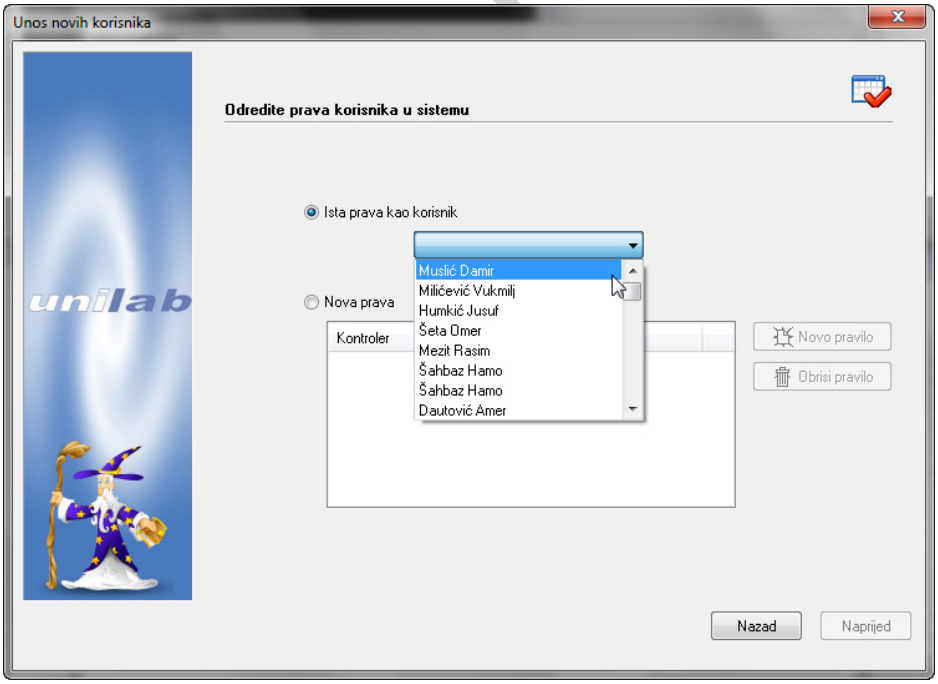
Slika 21. Unos broja novih korisnika

Nakon što smo odredili broj novih korisnika, potrebno je odrediti kontroler koji će izvršiti očitanje novih kartica. Napomenimo da u slučaju terminala radnog vremena čitač broj 1 je integrisan u sam terminal, dok je čitač 2 uvijek realiziran kao eksterni čitač.



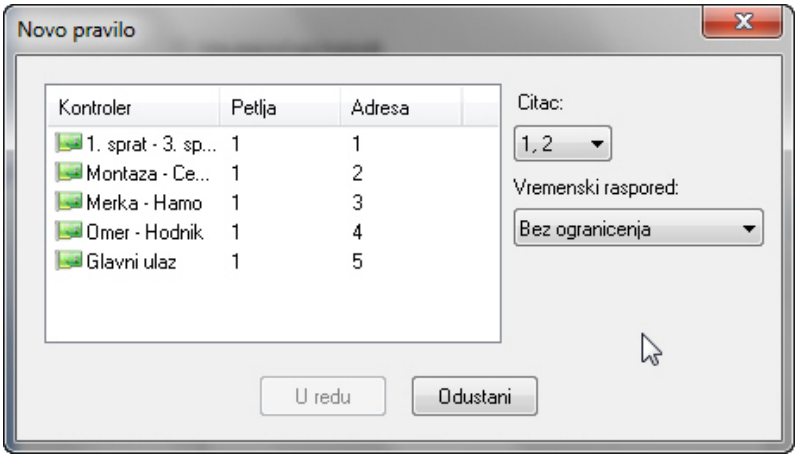
Slika 22. Odabir kontrolera koji vrši očitanje novih kartica

Treći korak u unosu kartica se odnosi na određivanje prava koje će nove kartice imati u sistemu. Operatoru se nudi mogućnost da nove kartice naslijede prava neke od prethodno-unešenih kartica ili da odredi potpuno nova prava.



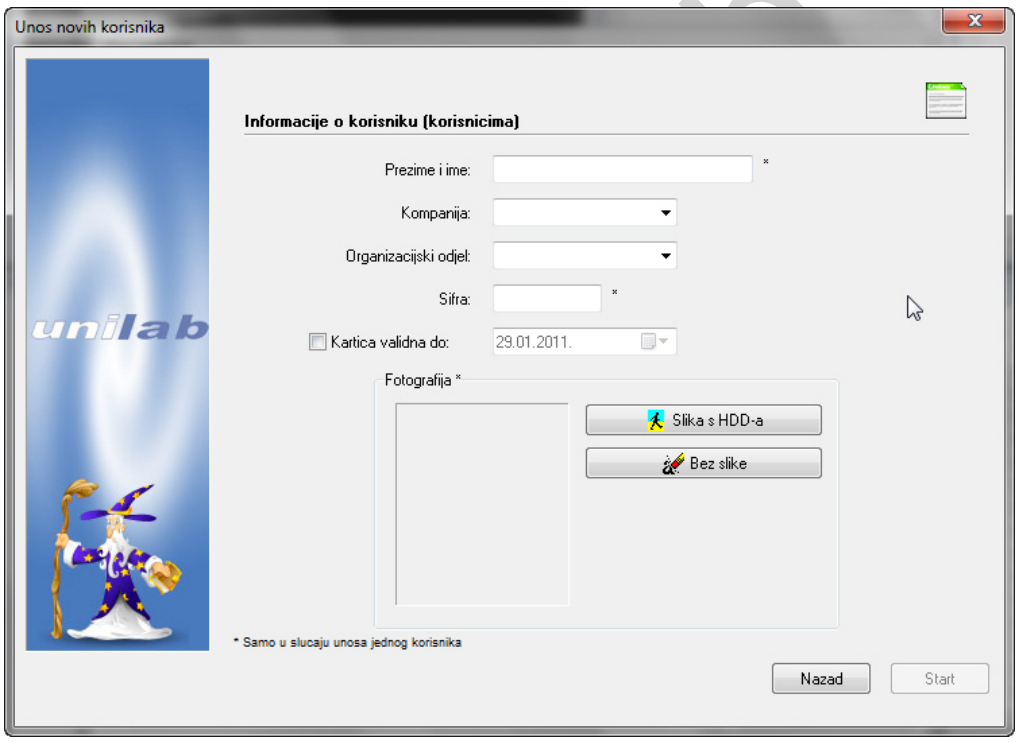
Slika 23. Nasljeđivanje prava od postojećeg korisnika

U slučaju potrebe definisanje novih prava potrebno je najprije označiti ovaj metod, a potom kliknuti na dugme sa nazivom "Novo pravilo". Ovim će biti prikazan slijedeći dialog.



Slika 24. Definisanje novih prava korisnika

Putem ovog dialoga je potrebno označiti kontrolere, vremenski raspored, kao i čitače na kojima želimo da damo prava korištenja novim karticama. Posljednji korak u unosu korisnika je vezan za unos nekih detalja o korisnicima, kao što to prikazuje slijedeća slika.

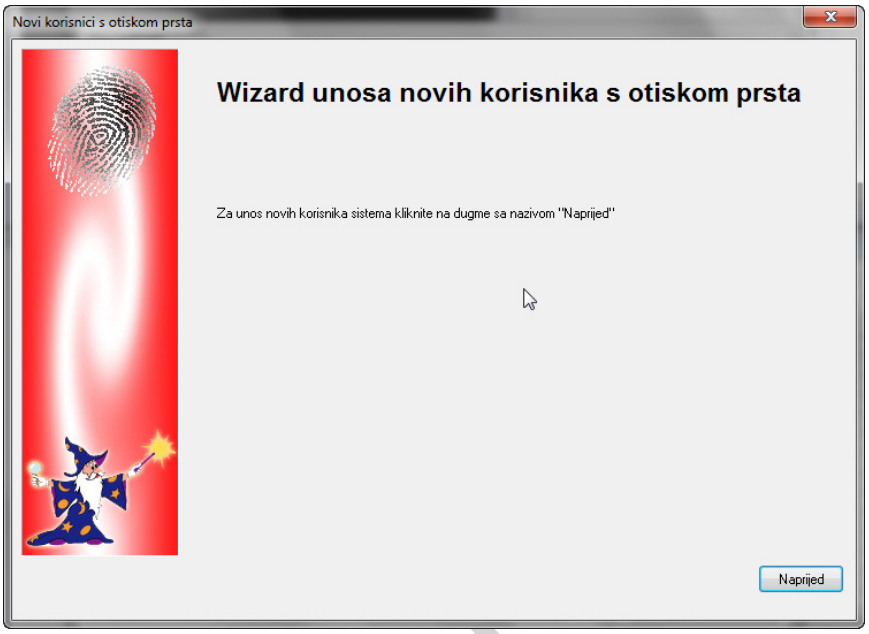


Slika 25. Detalji o novim korisnicima sistema

Napomenimo da neka od polja prikazana na prethodnoj slici imaju smisla isključivo pri unosu jednog korisnika. Ova polja su označena sa *. Za početak unosa novih korisnika potrebno je kliknuti na dugme "Start", a potom je nove kartice potrebno odnijeti do čitača definisanog 2. korakom ovog wizarda te izvršiti njihovo očitanje.

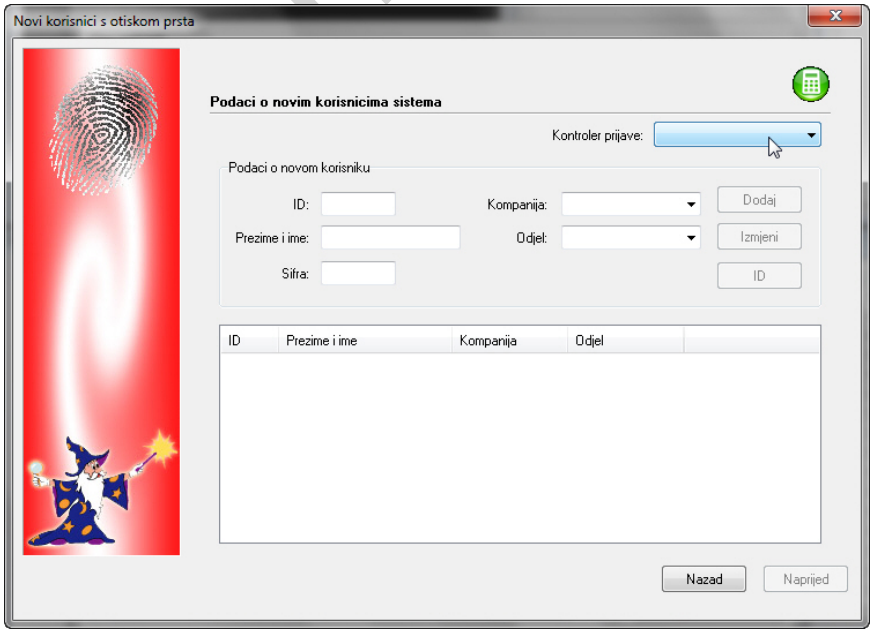
4.2 NOVI OTISCI

Unilab Access Control System uključuje podršku za rad sa IDTECK FINGER007 kontrolerom. Radi se o kontroleru koji pri autentikaciji može zahtjevati od korisnika skeniranje otiska prsta. Unos novih otisaka se obavlja putem posebnog dialoga, a koji se aktivira klikom na dugme "Novi otisci" (pogledati sliku 19).



Slika 26. Wizar unosa novih korisnika sa otiskom prsta

Slično kao i sa unosom korisnika kartica i ovaj unos korisnika uključuje poseban wizard. Prvi korak ovog wizarda prikazuje slijedeća slika.



Slika 27. Podaci o novim korisnicima

Na predthodnoj slici je bitno pojasniti značenje dvaju polja. Prvo od njih se odnosi na kontroler prijave. Radi se o kontroleru u koji su pohranjeni novi otisci prstiju. Naime, procesu unosa korisnika u software prethodi unos otisaka u kontroler. Tokom ovog postupka vrsi se skeniranje otisaka korisnika i dodjela jedinstenog ID svakom od korisnika. Pomenuti ID je drugo veoma važno polje.

Nakon što kreiramo listu novih korisnika sa otiscima prsta, program će klikom na dugme "Naprijed" (slika 27) započeti proces preuzimanja binarne interpretacije otisaka za svakog od novih korisnika.

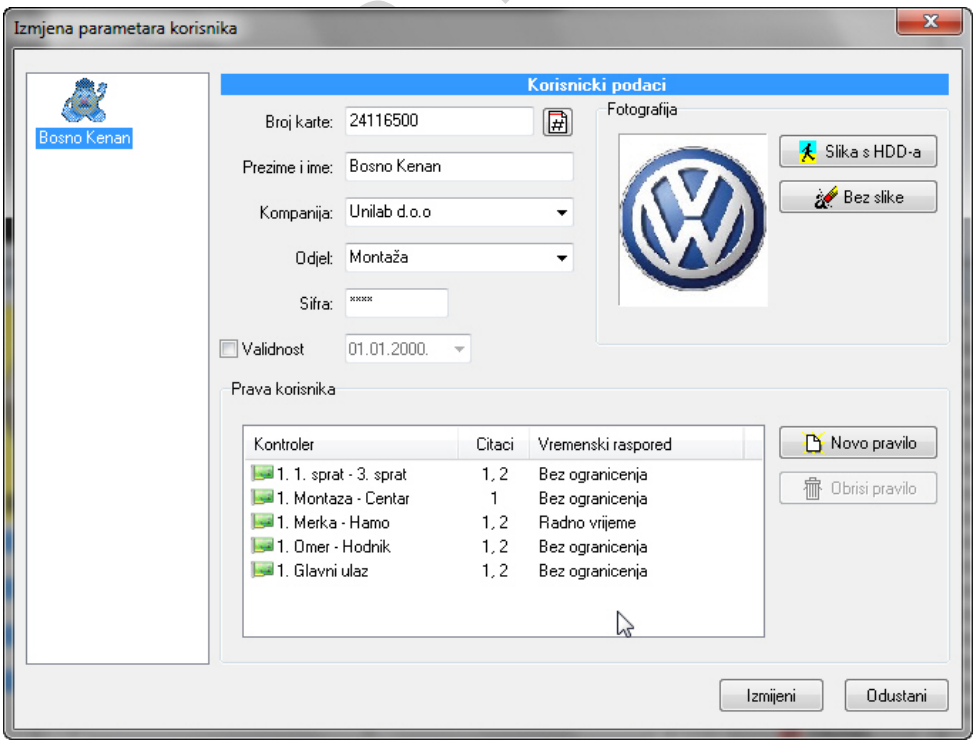
Proces unosa novih korisnika se nastavlja određivanjem prava, koja će novi korisnici imati u sistemu. Radi se o identičnom koraku kao i u slučaju prijave korisnika kartica (slika 23).

4.3 BRISANJE KORISNIKA

Brisanje korisnika iz sistema je jedan od najjednostavnijih postupaka. Potrebno je označiti korisnike koje želimo obrisati (slika 19), te potom kliknuti na dugme sa nazivom "Obriši korisnike". Program će od operatora zatražiti i završnu potvrdu radnje brisanje, nakon koje će u slučaju potvrdnog odgovora, označeni korisnici biti obrisani iz sistema.

4.4 IZMJENA PARAMETARA KORISNIKA

Izmjena podataka vezanih za korisnike, kao što su ime i prezime, organizacijski odjel, prava korisnika i sl. obavlja se putem posebnog dialoga. Naime, potrebno je označiti korisnike, čije parametre želimo mijenjati, a potom kliknuti na dugme sa nazivom "Izmjena parametara" (slika 19). Ovim će biti prikazan dialog kojeg prikazuje slijedeća slika.



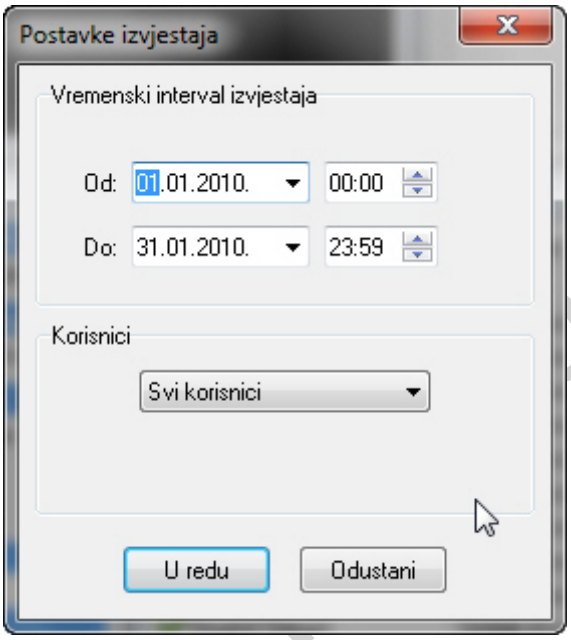
Slika 28. Izmjena parametara korisnika

Sa prethodne slike ćemo pojasniti značenje potencijalno manje razumljivih polja. Polje "Broj karte" sadrži vrijednost koja je upisana u karticu dodjeljenu korisniku. Pored ovog polja pojavljuje se i polje "Šifra", koje ima značaj u slučaju korištenja čitača sa integrisanom tastaturom i RF+PW načinom rada kontrolera (pogledati dio koji se odnosi na programiranje kontrolera). Napomenut ćemo da šifra nema značenje PIN-a. Ukoliko je važenje kartice nekog korisnika potrebno vremenski ograničiti, potrebno je označiti opciju "Validnost" i definisati krajnji datum važenja kartice. Napomenut ćemo da je ova opcija upotpunosti software-ski realizirana. Na kraju pomenimo i dio koji se odnosi na prava korisnika. Radi se o listi koja definiše čitače, kontrolere i vrijeme kada neki korisnik može koristiti svoju karticu. Pogledamo li sliku 28 možemo vidjeti da korisnik svoju karticu može koristiti samo na čitaču 1, u slučaju kontrolera nazvanog "Montaza-Centar" i to u periodu definisanim vremenskim rasporedom sa nazivom "Radno vrijeme".

5. GENERISANJE IZVJEŠTAJA

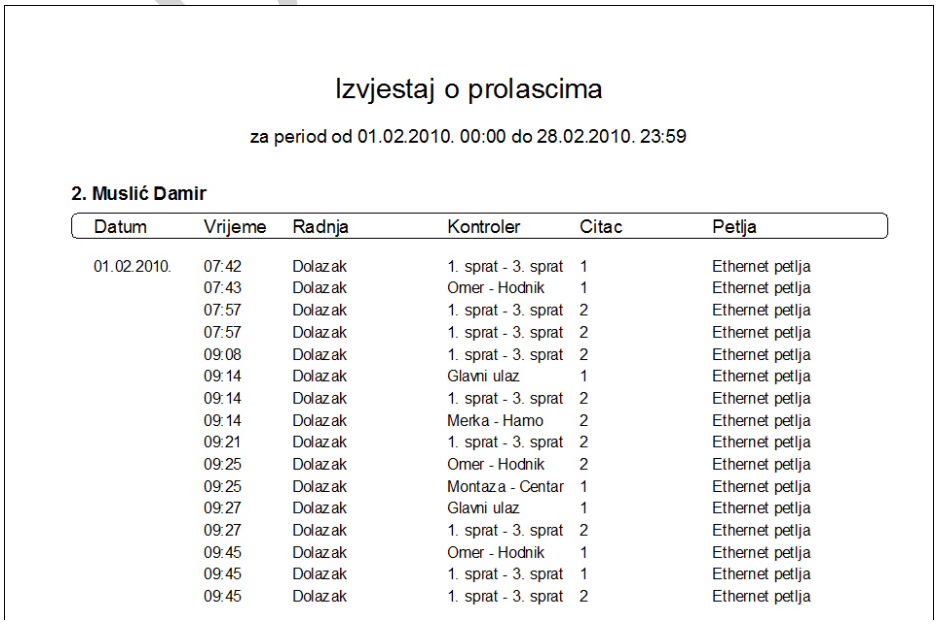
5.1 IZVJEŠTAJ O KORIŠTENJU KARTICA

U sistemima kontrole prolaza čest zahtjev je generisanje izvještaja na osnovu kojeg je moguće utvrditi kada i gdje su korisnici sistema koristili svoje kartice. Ovakav izvještaj je moguće kreirati odabirom stavke „Ulasci/Izlasci“, locirane u „Izvjestaji“ meniju (slika 1).



Slika 29. Kreiranje izvjestaja o kretanju korisnika u sistemu kontrole prolaza

Za razmatrani izvještaj važno je odrediti vremenski interval na koji se izvještaj odnosi, kao i korisnike, za koje se izvještaj kreira. Na slijedećoj slici je dat prikaz razmatranog izvještaja.



Izvjestaj o prolascima

za period od 01.02.2010. 00:00 do 28.02.2010. 23:59

2. Muslić Damir

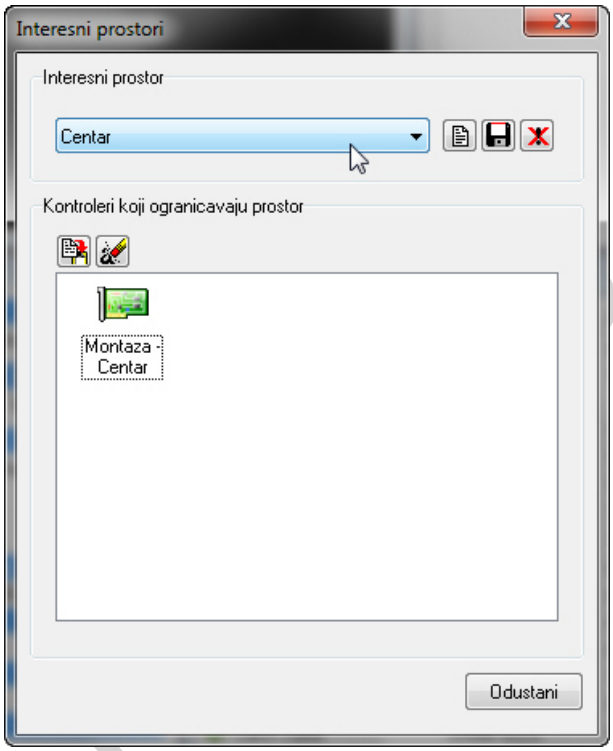
Datum	Vrijeme	Radnja	Kontroler	Citac	Petlja
01.02.2010.	07:42	Dolazak	1. sprat - 3. sprat	1	Ethernet petlja
	07:43	Dolazak	Omer - Hodnik	1	Ethernet petlja
	07:57	Dolazak	1. sprat - 3. sprat	2	Ethernet petlja
	07:57	Dolazak	1. sprat - 3. sprat	2	Ethernet petlja
	09:08	Dolazak	1. sprat - 3. sprat	2	Ethernet petlja
	09:14	Dolazak	Glavni ulaz	1	Ethernet petlja
	09:14	Dolazak	1. sprat - 3. sprat	2	Ethernet petlja
	09:14	Dolazak	Merka - Hamo	2	Ethernet petlja
	09:21	Dolazak	1. sprat - 3. sprat	2	Ethernet petlja
	09:25	Dolazak	Omer - Hodnik	2	Ethernet petlja
	09:25	Dolazak	Montaza - Centar	1	Ethernet petlja
	09:27	Dolazak	Glavni ulaz	1	Ethernet petlja
	09:27	Dolazak	1. sprat - 3. sprat	2	Ethernet petlja
	09:45	Dolazak	Omer - Hodnik	1	Ethernet petlja
	09:45	Dolazak	1. sprat - 3. sprat	1	Ethernet petlja
	09:45	Dolazak	1. sprat - 3. sprat	2	Ethernet petlja

Slika 30. Prikaz izvještaja o kretanju korisnika sistema

5.2 IZVJEŠTAJ O PRISUTNOSTI

Prisutnost odnosno odsutnost korisnika u štićenim prostorima je često vrlo značajna informacija. Da bi smo kreirali izvještaj, koji govori o prisutnim odnosno odsutnim korisnicima u štićenim prostorima, potrebno je najprije izvršiti definisanje „granica“ pojedinih prostora. U slučaju Unilab Access Control Systema granice štićenih prostora određuju čitači kartica, putem kojih se ulazi i eventualno izlazi iz ovih prostora.

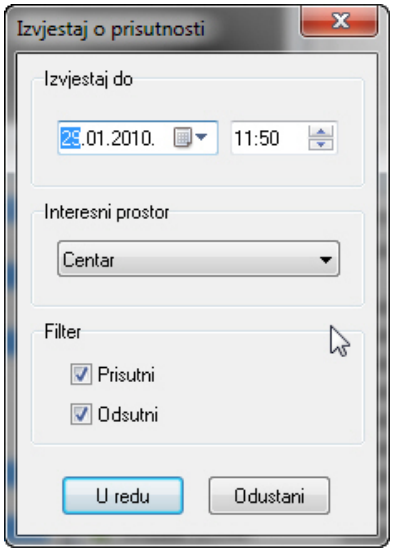
Za definisanje pomenutih granica potrebno je odabrati stavku „Interesni prostori“ smještene u „Izvještaji“ meniju (slika 1).



Slika 31. Definisanje interesnih prostora

Pri definisanju novog interesnog prostora od operatera se zahtjeva unos naziva novog prostora kao i čitači putem kojih se ulazi i izlazi iz tog prostora. Na prethodnoj slici uočavamo dvije cjeline. U prvoj cjelini, koja je označena sa „Interesni prostor“, nalaze se ukupno tri dugmeta, koji imaju funkcije kreiranja novog interesnog prostora, snimanja načinjenih izmjena na postojećem interesnom prostoru te brisanje interesnog prostora, sukcesivno. Drugu cjelinu čini lista čitača koji ograničavaju prostor, kao i dva dugmeta za dodavanje novog i brisanje postojećeg čitača.

Nakon što smo kreirali interesne prostore otvara se mogućnost kreirana izvještaja o prisutnosti korisnika sistema u pojedinim prostorima. Kreiranje ovog izvještaja se obavlja odabirom stavke „Izvještaj o prisutnosti“ smještene u „Izvještaji“ meniju. Na slijedećoj slici je prikazan dialog putem kojeg se konfigurišu parametri izvještaja o prisutnosti korisnika.



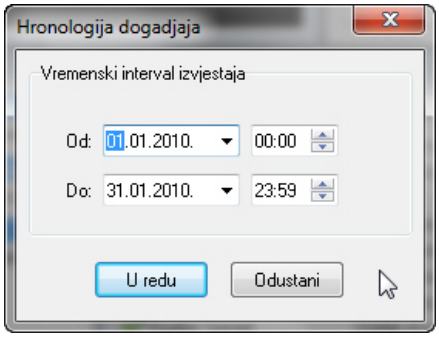
Slika 32. Konfigurisanje izvještaja o prisutnosti korisnika

Za kreiranje izvještaja operater treba definisati vremenski trenutak do kojeg je potrebno provjeriti koji uposlenici su bili u nekom od interesnih prostora, označiti prostor od interesa, te odrediti za koje korisnike se izvještaj odnosi. Na slijedećoj slici je dat prikaz izvještaja o prisutnosti korisnika.

Slika 33. Prikaz izvještaja o prisutnosti korisnika

5.3 HRONOLOGIJA DOGAĐAJA

Ovaj izvještaj, kao što i sam naziv upućuje, daje hronološki popis radnji korisnika sisteama. U slučaju ovog izvještaja od operatora se samo zahtjeva definisanje vremenskog intervala na koji se izvještaj odnosi. Na slijedećoj slici je dat prikaz konfiguracionog dialoga razmatranog izvještaja.



Slika 34. Konfigurisanje izvještaja o hronološkom popisu radnji korisnika

Hronologija dogadjaja

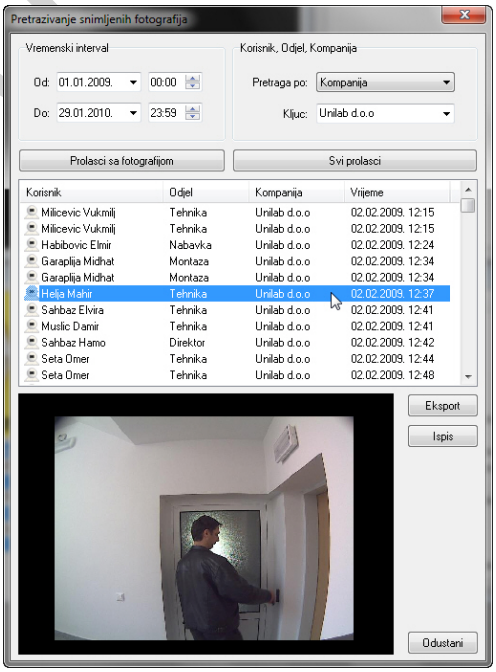
za period od 01.02.2010. 00:00 do 28.02.2010. 23:59

Korisnik	Datum	Vrijeme	Radnja	Kontroler	Citac	Petlja
Šeta Omer	01.02.2010.	05:58	Dolazak	1. sprat - 3. sprat	1	Ethernet petlja
Šeta Omer		05:59	Dolazak	Omer - Hodnik	1	Ethernet petlja
Kadrić Alden		06:48	Dolazak	1. sprat - 3. sprat	1	Ethernet petlja
Edis		07:05	Dolazak	1. sprat - 3. sprat	1	Ethernet petlja
Turulja Muhamed		07:06	Dolazak	1. sprat - 3. sprat	1	Ethernet petlja
Huskić Senad		07:07	Dolazak	1. sprat - 3. sprat	1	Ethernet petlja
Sakić Samir		07:13	Dolazak	1. sprat - 3. sprat	1	Ethernet petlja
Damjanović Saša		07:18	Dolazak	1. sprat - 3. sprat	1	Ethernet petlja
Alić Elvedin		07:19	Dolazak	Montaza - Centar	1	Ethernet petlja
Alić Elvedin		07:26	Dolazak	1. sprat - 3. sprat	1	Ethernet petlja
Kadrić Alden		07:27	Dolazak	1. sprat - 3. sprat	1	Ethernet petlja
Huskić Senad		07:32	Dolazak	Montaza - Centar	1	Ethernet petlja
Huskić Senad		07:32	Dolazak	1. sprat - 3. sprat	1	Ethernet petlja
Huskić Senad		07:33	Dolazak	Montaza - Centar	1	Ethernet petlja
Huskić Senad		07:38	Dolazak	Omer - Hodnik	1	Ethernet petlja
Huskić Senad		07:38	Dolazak	1. sprat - 3. sprat	1	Ethernet petlja
Muslić Damir		07:42	Dolazak	1. sprat - 3. sprat	1	Ethernet petlja
Muslić Damir		07:43	Dolazak	Omer - Hodnik	1	Ethernet petlja

Slika 35. Hronološki popis radnji korisnika sistema kontrole prolaza

5.4 PRETRAŽIVANJE SNIMLJENIH FOTOGRAFIJA

Tokom razmatranja problematike podešavanja hardware-skih komponenata sistema kontrole prolaza, spomenuli smo da Unilab Access Control System podržava rad sa mrežnim kamerama (poglavlje 3.11). Pretraživanje fotografija nastalih korištenjem ovih kamera se obavlja putem zasebnog dialoga, a koji se poziva stavkom „Pretrazivanje fotografija“ u meniju sa nazivom „Ostalo“ (pogledati sliku 1).

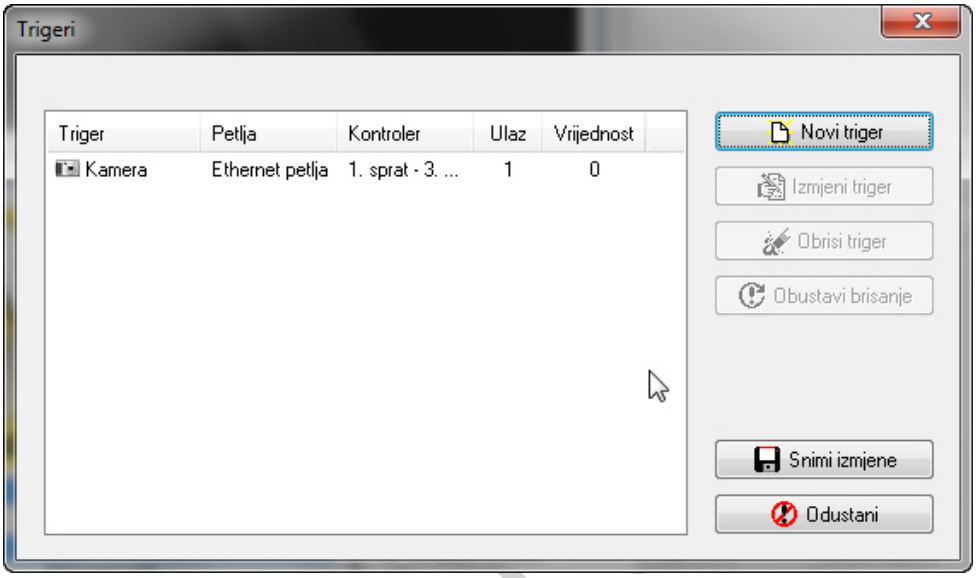


Slika 36. Pretraživanje fotografija uzetih sa mrežnih kamera

Sa prethodne slike možemo vidjeti da se od operatera zahtjeva podešavanje vremenskog intervala u kojem su fotografije nastale, kao i odabir korisnika za koje se fotografije vezuju. Kada su određena ova dva parametra, potrebno je kliknuti na dugme „Prolasci sa fotografijama“ i ovim će sistem prikazati one prolaske koji ispunjavaju zahtjevane kriterije. Pored ovog dugmeta važno je istaći da ispis trenutne fotografije (i njoj pripadajućih podataka) se obavlja klikom na dugme „Ispis“, dok se označena fotografija putem dugmeta „Eksport“ pohranjuje na željeni medij.

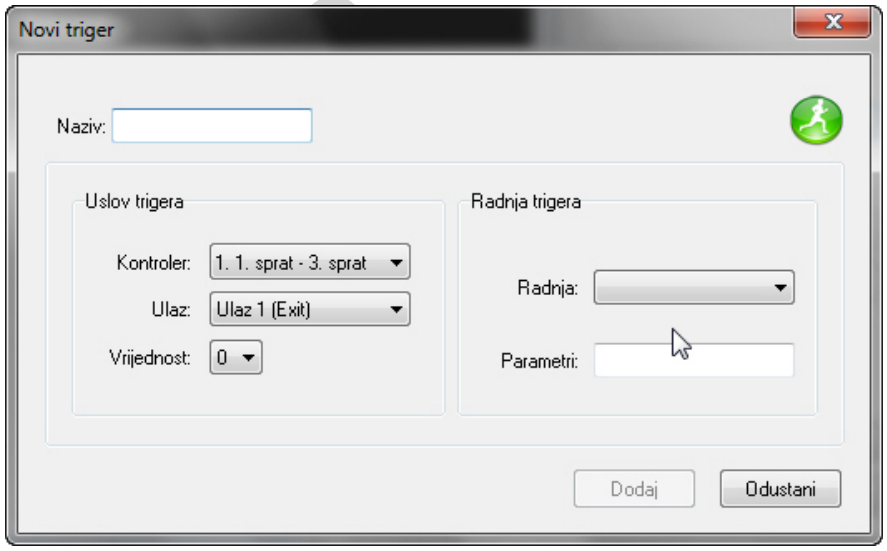
6. TRIGERI, PRISTUP MYSQL SERVERU I OSTALO

Pod trigerima podrazumijevamo mehanizme koji obezbijeđuju reakciju programa na vanjsku pobudu. Tako npr. da bi smo konfigurisali program da snima fotografije, pri ovlaštenom korištenju kartica na nekim čitačima, potrebno je da kreiramo trigger. Kreiranje triggera se obavlja putem dialog, koji biva prikazan odabirom stavke „Trigeri“ u meniju nazvanom „Ostalo“ (pogledati sliku 1).



Slika 37. Ažuriranje liste trigger-a

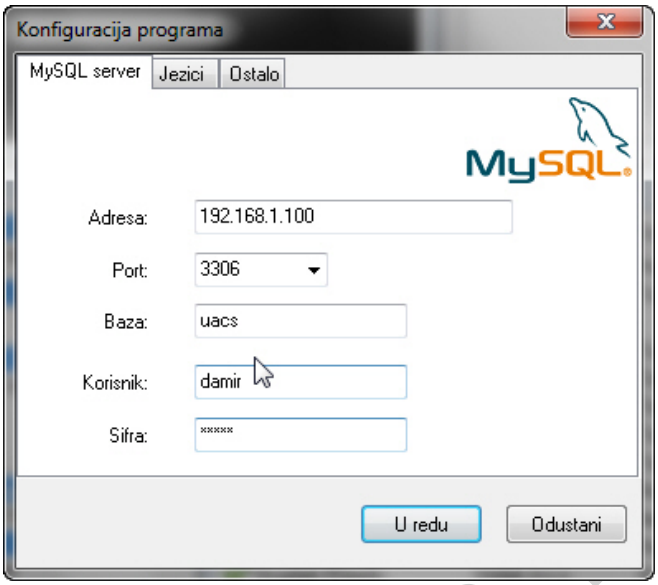
Za dodavanje novog trigera potrebno je kliknuti na dugme „Novi triger“. Ovim će biti prikazan dialog:



Slika 38. Definisanje novog trigera

Vidimo da novom trigeru je potrebno dati određeni naziv, odrediti uslove izvršavanja trigera, te radnju koju triger pri izvršavanju treba obaviti. Triger može biti uslovljen nekom od radnji definisanih listom nazvanom „Ulaz“, dok za radnju koju će triger obaviti možemo koristiti „Aktivni monitoring“ te „Snimanje fotografije“. Obadvije radnje kao parametar očekuju IP adresu kamere sa kojom operišu.

Na početku ovog dokumenta pomenuto je da program koristi MySQL server za skladištenje svih važnih informacija. Parametre pristupa programa serveru, kao i neke druge opcije, možemo podešavati putem dialoga „Konfiguracija programa“, a koji se poziva putem istoimene stavke smještene u meniju nazvanom „Opcije“ (pogledati sliku 1).



Slika 39. Podešavanje pristupa MySQL serveru

A. SISTEMSKI ZAHTJEVI

A.1 HARDWARE-ski ZAHTJEVI

- 2GHz ili brži x86 procesor
- 1GB RAM memorije ili više (zavisno od odabranog OS-a)
- 1GB slobodnog prostora na HDD-u
- 1 RS232 ili Ethernet (10/100Mbps) komunikacioni port

A.2 ZAHTJEVI ZA OPERATIVNIM SISTEMOM

- Window 2000
- Windows XP (32-bit)
- Windows Vista (32-bit)
- Windows 7 (32-bit)

B. MJPEG URI

B.1 AXIS

http://IP_add_or_DN/axis-cgi/mjpg/video.cgi,

pri čemu IP_add_or_DN podrazumijeva IP adresu kamere ili njeno domain ime.

B.2 SONY

http://IP_add_or_DN/image

B.3 PLANET

http://IP_add_or_DN/mjpg/video.mjpg

B.4 TRENDNET

http://IP_add_or_DN/video.cgi