



AVG 9 Anti-Virus sa zaštitnim zidom

Priručnik za korisnike

Revizija dokumenta 90.21 (3.2.2010)

Copyright AVG Technologies CZ, s.r.o. Sva prava zadržana.
Svi ostali žigovi su vlasništvo njihovih doticnih vlasnika.

Ovaj proizvod koristi RSA Data Security, Inc. MD5 Message-Digest algoritam, Copyright (C) 1991-2, RSA Data Security, Inc., kreirano 1991. godine.

Ovaj proizvod koristi kôd iz C-SaCzech biblioteke, Copyright (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz).

Ovaj proizvod koristi biblioteku kompresije zlib, Copyright (c) 1995-2002 Jean-loup Gailly i Mark Adler.

Ovaj proizvod koristi biblioteku kompresije libbzip2, Copyright (c) 1996-2002 Julian R. Seward.

Sadržaj

1. Uvod	7
2. Zahtevi za instalaciju programa AVG	8
2.1 Podržani operativni sistemi	8
2.2 Minimalni i preporučeni hardverski zahtevi	8
3. Opcije za instalaciju programa AVG	9
4. AVG alatka za upravljanje preuzimanjem	10
4.1 Izbor jezika	10
4.2 Provera veze	11
4.3 Podešavanja proxy servera	12
4.4 Preuzmi datoteke za instalaciju	13
5. Proces instalacije programa AVG	14
5.1 Pokretanje instalacije	14
5.2 Ugovor o licenciranju	15
5.3 Provera statusa sistema	15
5.4 Izbor tipa instalacije	16
5.5 Aktivirate svoju AVG licencu	16
5.6 Prilagodena instalacija - Odredišna fascikla	18
5.7 Prilagodena instalacija - Izbor komponenti	19
5.8 AVG bezbednosna traka sa alatkama	20
5.9 Zatvaranje otvorenih aplikacija	21
5.10 Instalacija programa AVG	22
5.11 Planiranje redovnog skeniranja i ažuriranja	23
5.12 Izbor nacina upotrebe racunara	23
5.13 Internet veza na vašem racunaru	24
5.14 Konfigurisanje AVG zaštite je završeno	25
6. Nakon instalacije	26
6.1 Optimizacija skeniranja	26
6.2 Registracija proizvoda	26
6.3 Pristupanje korisničkom interfejsu	26
6.4 Skeniranje celog racunara	27
6.5 Eicar test	27

6.6 Podrazumevana konfiguracija programa AVG	28
7. AVG korisnicki interfejs	29
7.1 Sistemski meni	30
7.1.1 Datoteka	30
7.1.2 Komponente	30
7.1.3 Istorija	30
7.1.4 Alatke	30
7.1.5 Pomoc	30
7.2 Informacije o bezbednosnom statusu	33
7.3 Brze veze	34
7.4 Pregled komponenti	35
7.5 Statistika	36
7.6 Ikona sistemske palete	36
8. Komponente programa AVG	38
8.1 Antivirusni program	38
8.1.1 Antivirusni program Principi	38
8.1.2 Anti-Virus Interfejs	38
8.2 Antispajver	40
8.2.1 Antispajver Principi	40
8.2.2 Interfejs komponente Antispajver	40
8.3 Anti-Rootkit	42
8.4 Zaštitni zid	42
8.4.1 Principi funkcionisanja zaštitnog zida	42
8.4.2 Profili zaštitnog zida	42
8.4.3 Interfejs zaštitnog zida	42
8.5 Skener e-pošte	47
8.5.1 Principi skeniranja e-pošte	47
8.5.2 Interfejs komponente Skener e-pošte	47
8.5.3 Detekcija od strane skenera e-pošte	47
8.6 Licenca	51
8.7 Skener linkova	52
8.7.1 Principi skeniranja linkova	52
8.7.2 Interfejs komponente Skener linkova	52
8.7.3 AVG štit za pretraživanje	52
8.7.4 AVG štit za aktivno pregledanje Interneta	52
8.8 Online Shield	56

8.8.1	Princip rada komponente Online Shield	56
8.8.2	Interfejs komponente Online Shield	56
8.8.3	Detekcija komponente Online Shield	56
8.9	Stalni štit	62
8.9.1	Stalni štit Principi	62
8.9.2	Interfejs komponente Stalni štit	62
8.9.3	Detekcija od strane Stalnog štita	62
8.10	Upravljanje ažuriranjem	66
8.10.1	Principi upravljanja ažuriranjem	66
8.10.2	Interfejs komponente Upravljanje ažuriranjem	66
9.	AVG bezbednosna traka sa alatkama	69
9.1	Interfejs AVG bezbednosne trake sa alatkama	69
9.2	Opcije AVG bezbednosne trake sa alatkama	71
9.2.1	Kartica „Opšte“	71
9.2.2	Kartica „Korisna dugmad“	71
9.2.3	Kartica „Bezbednost“	71
9.2.4	Kartica „Napredne opcije“	71
10.	AVG napredna podešavanja	76
10.1	Izgled	76
10.2	Zvuci	78
10.3	Zanemarivanje stanja sa greškom	80
10.4	Skladište za viruse	81
10.5	Izuzeci od potencijalno neželjenih programa	82
10.6	Online Shield	84
10.6.1	Zaštita na Webu	84
10.6.2	Razmena hitnih poruka	84
10.7	Skener linkova	88
10.8	Skeniranje	89
10.8.1	Skeniraj ceo racunar	89
10.8.2	Shell Extension skeniranje	89
10.8.3	Skeniraj odredene datoteke ili fascikle	89
10.8.4	Skeniranje prenosnog uredaja	89
10.9	Planovi	96
10.9.1	Planirano skeniranje	96
10.9.2	Plan ažuriranja baze podataka o virusima	96
10.10	Skener e-pošte	106

10.10.1	Sertifikacija	106
10.10.2	Filtriranje pošte	106
10.10.3	Datoteke evidencije i rezultati	106
10.10.4	Serveri	106
10.11	Stalni štit	116
10.11.1	Napredna podešavanja	116
10.11.2	Izuzeti direktorijumi	116
10.11.3	Izuzete datoteke	116
10.12	Keš server	121
10.13	Anti-Rootkit	122
10.14	Ažuriranje	123
10.14.1	Proxy	123
10.14.2	Pozivna veza	123
10.14.3	URL adresa	123
10.14.4	Upravljanje	123
10.15	Daljinska administracija	130
11.	Podešavanja zaštitnog zida	132
11.1	Opšte postavke	132
11.2	Bezbednost	133
11.3	Profili za oblasti i mrežne kartice	134
11.4	Datoteke evidencije	135
11.5	Profili	137
11.5.1	Informacije o profilu	137
11.5.2	Definisane mreže	137
11.5.3	Aplikacije	137
11.5.4	Sistemske usluge	137
12.	Skeniranje programom AVG	149
12.1	Interfejs za skeniranje	149
12.2	Unapred definisana skeniranja	150
12.2.1	Skeniraj ceo racunar	150
12.2.2	Skeniraj odredene datoteke ili fascikle	150
12.3	Skeniranje u programu Windows Explorer	158
12.4	Skeniranje komandne linije	159
12.4.1	Parametri za skeniranje iz komandne linije	159
12.5	Planiranje skeniranja	161
12.5.1	Postavke planiranja	161

12.5.2	<i>Kako skenirati</i>	161
12.5.3	<i>Šta skenirati</i>	161
12.6	Pregled rezultata skeniranja	172
12.7	Detalji rezultata skeniranja	173
12.7.1	<i>Kartica Pregled rezultata</i>	173
12.7.2	<i>Kartica Zaraze</i>	173
12.7.3	<i>Kartica Špijunski softver</i>	173
12.7.4	<i>Kartica Upozorenja</i>	173
12.7.5	<i>Kartica Rootkit programi</i>	173
12.7.6	<i>Kartica Informacije</i>	173
12.8	Skladište za viruse	182
13.	Ažuriranje programa AVG	184
13.1	Nivoi ažuriranja	184
13.2	Tipovi ispravki	184
13.3	Proces ažuriranja	185
14.	Istorija događaja	186
15.	Najčešća pitanja i tehnička podrška	188



1. Uvod

Ovo korisnicko uputstvo sadrži sveobuhvatnu dokumentaciju za **AVG 9 Anti-Virus sa zaštitnim zidom**.

Cestitamo vam na kupovini programa AVG 9 Anti-Virus sa zaštitnim zidom!

AVG 9 Anti-Virus sa zaštitnim zidom predstavlja deo asortimana nagradivanih AVG proizvoda, osmišljenih da bi ste vi mogli da budete bezbrižni, znajući da je vaš racunar potpuno zašticen. Kao i svi AVG proizvodi, **AVG 9 Anti-Virus sa zaštitnim zidom** je redizajniran od samog temelja, kako bi se cuvena AVG zaštita obezbedivala na nov, jednostavniji i efikasniji nacin.

Vaš novi **AVG 9 Anti-Virus sa zaštitnim zidom** proizvod odlikuje se svedenim interfejsom u kombinaciji sa agresivnijim i bržim skeniranjem. Radi vece prakticnosti, automatizovano je još nekoliko bezbednosnih funkcija, a dodate su i nove inteligentne korisnicke opcije kako biste bezbednosne funkcije mogli da prilagodite svom nacinu života. Nema više kompromisa po pitanju bezbednosti kako bi se pojednostavilo korišćenje!

Program AVG je osmišljen i razvijen kako bi zaštitio vaše racunarske i mrežne aktivnosti. Uživajte u potpunoj zaštiti koju nudi AVG.



2. Zahtevi za instalaciju programa AVG

2.1. Podržani operativni sistemi

AVG 9 Anti-Virus sa zaštitnim zidom je namenjen zaštiti radnih stanica na kojima se koriste sledeći operativni sistemi:

- Windows 2000 Professional SP4 + zbirne ispravke 1
- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 i x64, sva izdanja)
- Windows 7 (x86 i x64, sva izdanja)

(i eventualno noviji servisni paketi za određene operativne sisteme)

2.2. Minimalni i preporučeni hardverski zahtevi

Minimalni hardverski zahtevi za **AVG 9 Anti-Virus sa zaštitnim zidom**:

- Intel Pentium CPU 1,5 GHz
- 512 MB RAM memorije
- 390 MB slobodnog prostora na cvrstom disku (za instalaciju)

Preporučeni hardverski zahtevi za **AVG 9 Anti-Virus sa zaštitnim zidom**:

- Intel Pentium CPU 1,8 GHz
- 512 MB RAM memorije
- 510 MB slobodnog prostora na cvrstom disku (za instalaciju)



3. Opcije za instalaciju programa AVG

AVG se može instalirati putem instalacione datoteke koja se nalazi na instalacionom CD-u ili tako što ćete preuzeti najnoviju instalacionu datoteku sa AVG Web lokacije (<http://www.avg.com/>).

Pre nego što počnete da instalirate AVG, preporučujemo vam da posetite AVG Web lokaciju (<http://www.avg.com/>) da biste proverili da li postoji nova instalaciona datoteka. Na taj način ćete biti sigurni da ćete instalirati najnoviju verziju programa AVG 9 Anti-Virus sa zaštitnim zidom.

Preporučujemo vam da isprobate novu alatku [AVG alatka za upravljanje preuzimanjem](#) koja će vam pomoći da podesite instalacionu datoteku na jeziku koji izaberete!

Tokom procesa instalacije bićete upitani za broj licence/prodajni broj. Pre nego što započnete instalaciju, uverite se da je taj broj dostupan. Prodajni broj možete pronaći na pakovanju CD-a. Ako ste svoj primerak AVG programa kupili na mreži, broj licence dostavljen vam je e-poštom.

4. AVG alatka za upravljanje preuzimanjem

AVG alatka za upravljanje preuzimanjem je jednostavna alatka koja vam pomaže da izaberete odgovarajuću instalacionu datoteku za probnu verziju vašeg AVG proizvoda. Na osnovu unetih podataka, upravljač će izabrati određeni proizvod, tip licence, željene komponente i jezik. Na kraju, **AVG alatka za upravljanje preuzimanjem** će preuzeti i pokrenuti odgovarajući [instalacioni proces](#).

Upozorenje: Imajte u vidu da AVG alatka za upravljanje preuzimanjem nije pogodna za preuzimanje mrežnih ili SBS izdanja i podržani su samo sledeći operativni sistemi: Windows 2000 (SP4 + SRP), Windows XP, Windows Vista i Windows 7.

AVG alatka za upravljanje preuzimanjem se može preuzeti sa Web lokacije kompanije AVG (<http://www.avg.com/>). Sledi kratak opis koraka koje je potrebno da preduzmete u okviru alatke **AVG alatka za upravljanje preuzimanjem**:

4.1. Izbor jezika



Kao prvi korak u programu **AVG alatka za upravljanje preuzimanjem**, u padajućem meniju izaberite jezik instalacije. Imajte u vidu da se jezik koji ovde izaberete odnosi samo na proces instalacije; nakon instalacije, mogli biste da promenite jezik direktno iz podešavanja programa. Zatim kliknite na dugme **Sledeće** da biste nastavili.

4.2. Provera veze

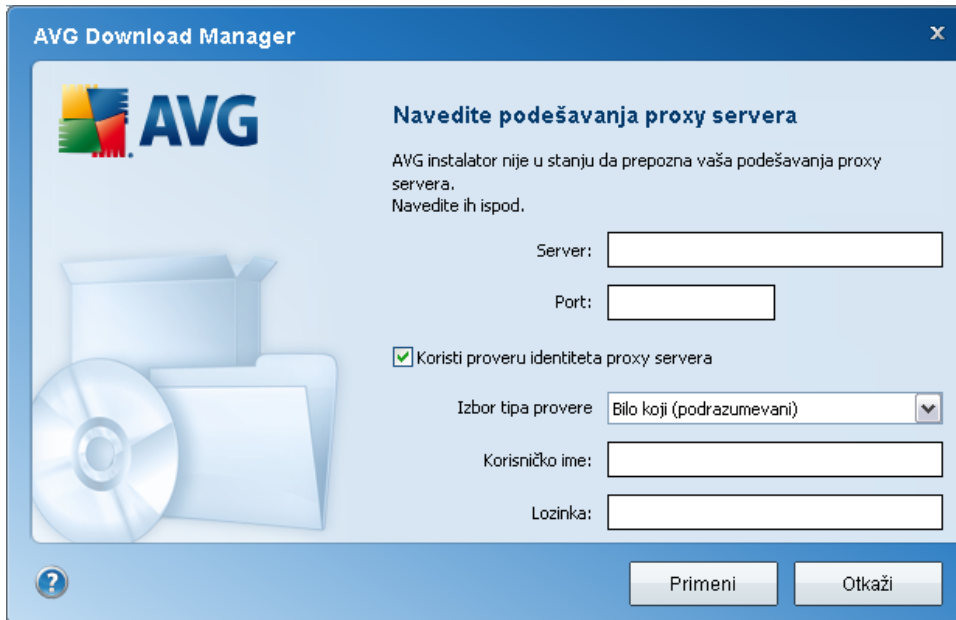
U sledecem koraku, **AVG alatka za upravljanje preuzimanjem** ce pokušati da uspostavi vezu sa Internetom kako bi mogao da pronade ispravke. Necete moci da zapocnete proces preuzimanja sve dok **AVG alatka za upravljanje preuzimanjem** ne završi sa testiranjem veze.

- Ako se testom ne detektuje dostupna veza, proverite da li ste zaista povezani sa Internetom. Zatim kliknite na dugme **Pokušaj ponovo**.



- Ako koristite vezu sa Internetom preko proxy servera, kliknite na dugme **Podešavanja proxy servera** da biste uneli [informacije u vezi sa proxy serverom](#):
- Ako provera uspe, pritisnite dugme **Sledece** da biste nastavili.

4.3. Podešavanja proxy servera



The screenshot shows a dialog box titled "AVG Download Manager" with a close button (X) in the top right corner. On the left side, there is the AVG logo and an illustration of a CD, a folder, and a document. The main text reads: "Navedite podešavanja proxy servera" (Specify proxy server settings). Below this, it says: "AVG instalator nije u stanju da prepozna vaša podešavanja proxy servera. Navedite ih ispod." (The AVG installer is unable to recognize your proxy server settings. Specify them below). The form contains the following fields and options:

- Server: [text input field]
- Port: [text input field]
- Koristi proveru identiteta proxy servera (Use proxy server identity verification)
- Izbor tipa provere: [dropdown menu with "Bilo koji (podrazumevani)" selected]
- Korisničko ime: [text input field]
- Lozinka: [text input field]

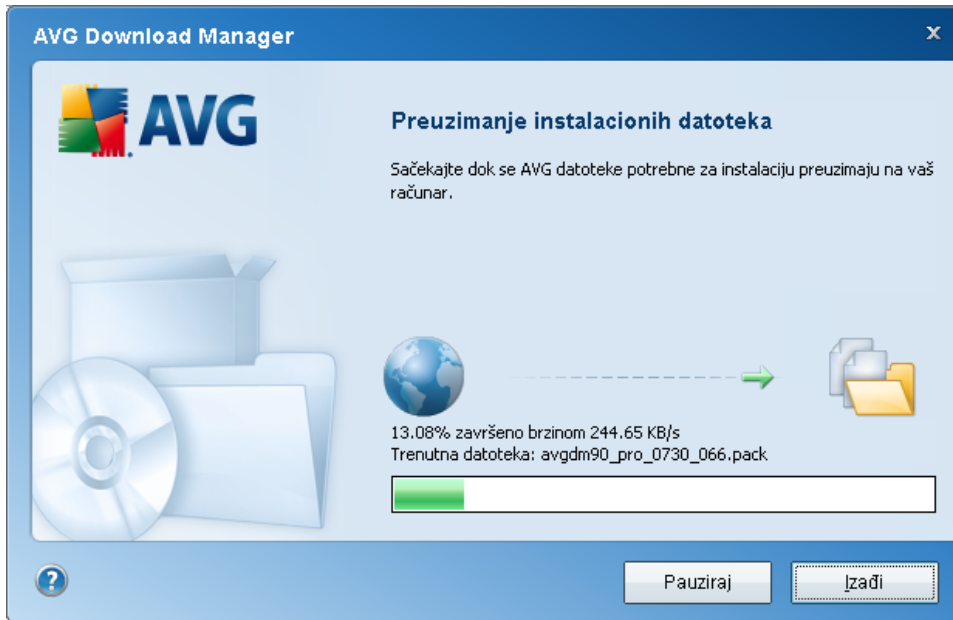
At the bottom right, there are two buttons: "Primeni" (Apply) and "Otkazi" (Cancel). A help icon (?) is located at the bottom left.

Ako **AVG alatka za upravljanje preuzimanjem** nije mogao da prepozna podešavanja proxy servera, moracete da ih unesete rucno. Unesite sledece podatke:

- **Server** - unesite važece ime proxy servera ili IP adresu
- **Port** - unesite broj odgovarajućeg porta
- **Koristi proveru identiteta proxy servera** - ako vaš proxy server zahteva proveru identiteta, označite ovo polje za potvrdu.
- **Izbor provere identiteta** - sa padajućeg menija izaberite tip provere identiteta. Preporučujemo da zadržite podrazumevanu vrednost (*proxy server ce vam zatim automatski preneti svoje zahteve*). Medutim, ako ste iskusan korisnik, može izabrati i opciju Osnovni (*koju zahtevaju neki serveri*) ili NTLM (*koju zahtevaju svi ISA serveri*). Zatim unesite važece **Korisničko ime** i **Lozinku** (opcionally).

Potvrdite podešavanja tako što cete kliknuti na dugme **Primeni** da biste prešli na sledeci korak u programu **AVG alatka za upravljanje preuzimanjem**.

4.4. Preuzmi datoteke za instalaciju



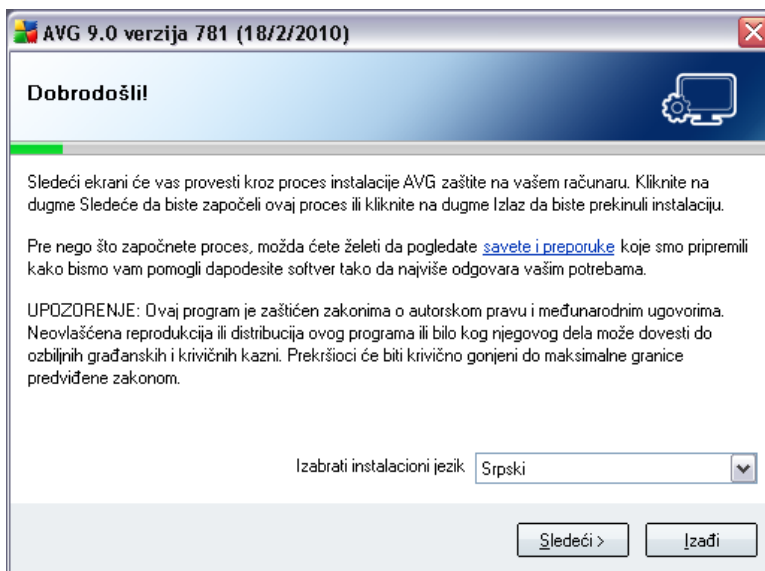
Sada ste uneli sve informacije koje su potrebne da **AVG alatka za upravljanje preuzimanjem** počne sa preuzimanjem instalacionog paketa i pokrene proces instalacije. Predite na [Proces instalacije programa AVG](#).

5. Proces instalacije programa AVG

Da biste instalirali **AVG 9 Anti-Virus sa zaštitnim zidom** na svoj računar, potrebna vam je najnovija instalaciona datoteka. Možete da upotrebite instalacionu datoteku sa CD-a iz kompleta, ali postoji mogućnost da je zastarela. Zato vam preporučujemo da preuzmete najnoviju instalacionu datoteku sa mreže. Datoteku možete da preuzmete sa Web lokacije kompanije AVG (<http://www.avg.com/>), odeljak [Centar za podršku / Preuzimanje](#). Možete da iskoristite i našu novu [AVG alatku za upravljanje preuzimanjem](#) koja vam pomaže da kreirate i preuzmete potrebni instalacioni paket i pokrenete proces instalacije.

Instalaciju čini niz dijaloga sa kratkim opisom radnji koje bi trebalo da preduzmete u tom koraku. U nastavku teksta nalaze se objašnjenja svih dijaloga:

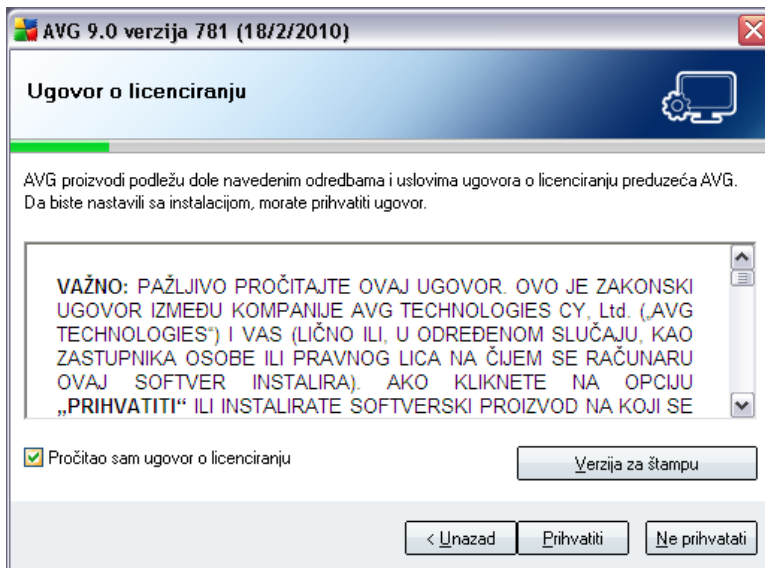
5.1. Pokretanje instalacije



Proces instalacije počinje ekranom **Dobro došli u program za AVG instalaciju**. U njemu možete izabrati jezik instalacije. U donjem delu prozora dijaloga pronađite stavku **Izaberite jezik instalacije** i u padajućem meniju izaberite željeni jezik. Zatim pritisnite dugme **Sledeće** da potvrdite i pređete na sledeći dijalog.

Pažnja: Ovde je potrebno da izaberete jezik za sam proces instalacije. Nije u pitanju izbor jezika na kojem će se prikazivati aplikacija AVG - njega možete definisati kasnije, u toku procesa instalacije!

5.2. Ugovor o licenciranju



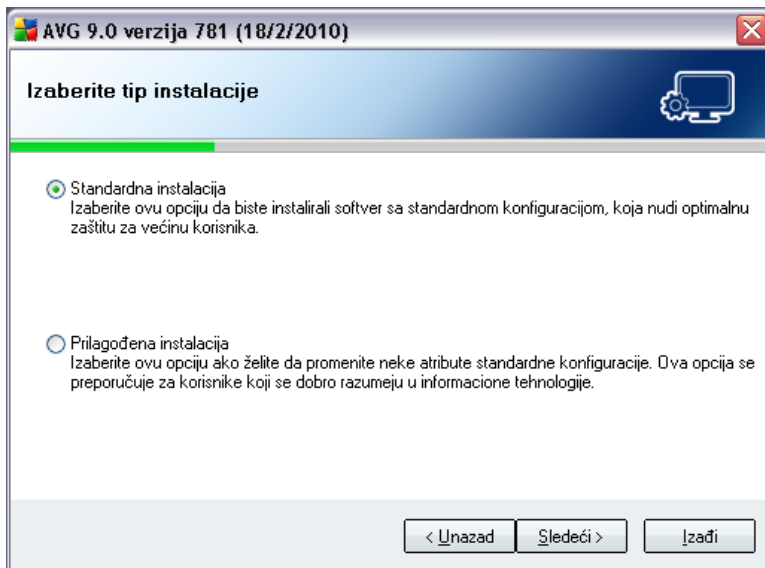
Dijalog **Ugovor o licenciranju** sadrži ceo tekst AVG ugovora o licenciranju. Pročitajte ga pažljivo i potvrdite da ste pročitali, razumeli i prihvatili ugovor tako što ćete potvrditi izbor u polju za potvrdu **Pročitao sam ugovor o licenciranju** i kliknuti na dugme **Prihvatam**.

Ako se ne slažete sa uslovima ugovora o licenciranju kliknite na dugme **Ne prihvatam**, čime ćete odmah prekinuti proces instalacije.

5.3. Provera statusa sistema

Nakon što prihvatite ugovor o licenciranju, bićete preusmereni na dijalog **Provera statusa sistema**. Ovaj dijalog ne zahteva angažovanje korisnika; u pitanju je provera sistema pre pokretanja instalacije programa AVG. Sacekajte da se ovaj proces završi, a zatim ćete automatski nastaviti na sledeći dijalog.

5.4. Izbor tipa instalacije



U dijalogu **Izbor tipa instalacije** možete izabrati jednu od dve opcije instalacije: **standardnu** ili **prilagođenu** instalaciju.

Vecini korisnika se preporučuje da se drže **standardne instalacije**, kojom ce se program AVG instalirati u potpuno automatskom režimu sa postavkama koje je unapred definisao proizvođač softvera. Ova konfiguracija obezbeđuje maksimalnu bezbednost i optimalnu zauzetost resursa. Ako kasnije bude potrebno da promenite konfiguraciju, to cete uvek moći da uradite direktno u aplikaciji AVG.

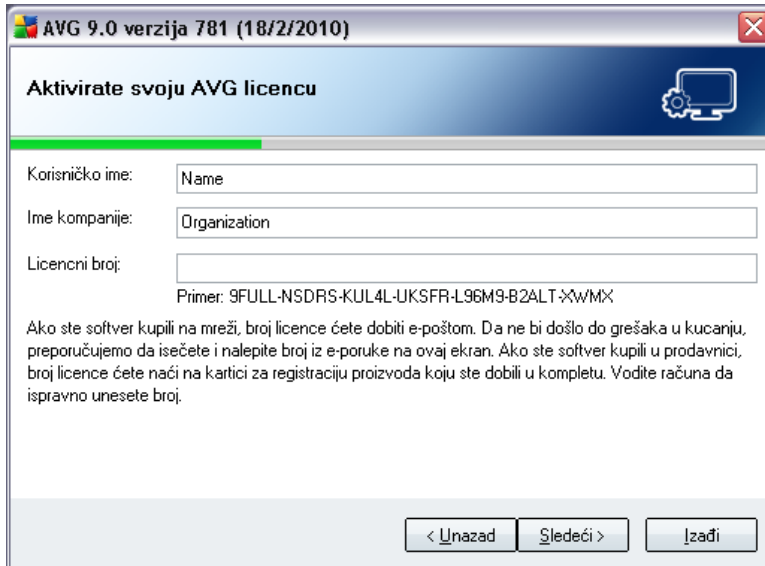
Prilagođenu instalaciju smeju da koriste isključivo iskusni korisnici koji imaju dobar razlog da program AVG instaliraju sa nestandardnim postavkama, npr. u skladu sa specijalnim zahtevima sistema.

5.5. Aktivirate svoju AVG licencu

U dijalogu **Aktivirajte vašu AVG licencu** morate uneti podatke za registraciju. Unesite svoje ime (polje **Korisnicko ime**) i ime vaše organizacije (polje **Ime preduzeća**).

Zatim unesite broj licence/prodajni broj u polje za tekst **Broj licence**. Prodajni broj se nalazi na pakovanju CD-a u kutiji programa **AVG 9 Anti-Virus sa zaštitnim zidom**. Broj licence ce se nalaziti u potvrdnoj e-poruci koju ste dobili nakon kupovine programa **AVG 9 Anti-Virus sa zaštitnim zidom** na Internetu. Morate uneti broj tacno onako kao što je prikazan. Ako je broj licence dostupan u digitalnom obliku (u e-

poruci), preporučujemo da ga umetnete metodom kopiranja i nalepljivanja.



AVG 9.0 verzija 781 (18/2/2010)

Aktivirate svoju AVG licencu

Korisničko ime:

Ime kompanije:

Licencni broj:

Primer: 9FULL-NSDRS-KUL4L-UKSFR-L96M9-B2<-?wMX

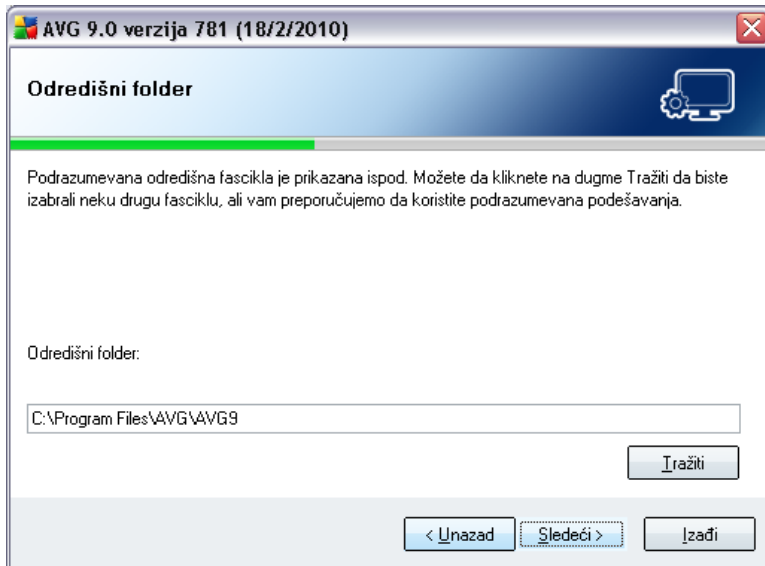
Ako ste softver kupili na mreži, broj licence ćete dobiti e-poštom. Da ne bi došlo do grešaka u kucanju, preporučujemo da isečete i nalepите broj iz e-poruke na ovaj ekran. Ako ste softver kupili u prodavnici, broj licence ćete naći na kartici za registraciju proizvoda koju ste dobili u kompletu. Vodite računa da ispravno unesete broj.

< Unazad Sledeći > Izađi

Pritisnite dugme **Sledece** da biste nastavili sa procesom instalacije.

Ako ste u prethodnom koraku izabrali standardnu instalaciju, bicete preusmereni direktno na dijalog **AVG bezbednosna traka sa alatkama**. Ako ste izabrali prilagodenu instalaciju, nastaviceće dijalogom **Odredišna fascikla**.

5.6. Prilagodena instalacija - Odredišna fascikla

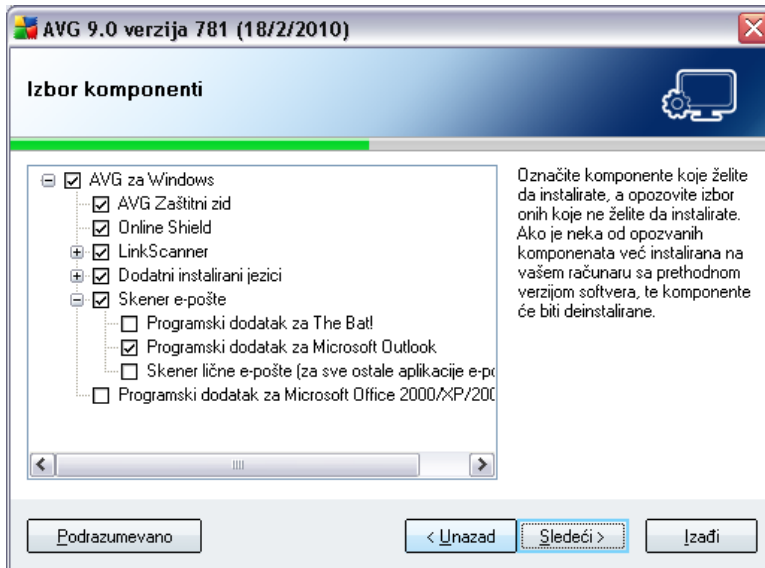


U dijalogu **Odredišna fascikla** možete da navedete lokaciju na kojoj želite da instalirate **AVG 9 Anti-Virus sa zaštitnim zidom**. Podrazumevano, AVG se instalira u fasciklu Programske datoteke na jedinici diska C:- Ukoliko ta fascikla još ne postoji, od vas ce se tražiti da u novom dijalogu potvrdite da želite da AVG odmah kreira tu fasciklu.

Ako želite da promenite ovu lokaciju, kliknite na dugme **Potraži** da biste videli strukturu disk jedinice i izaberite odgovarajuću fasciklu.

Kliknite na dugme **Sledeće** da biste potvrdili.

5.7. Prilagodena instalacija - Izbor komponenti



U dijalogu **Izbor komponenti** se prikazuje pregled svih **AVG 9 Anti-Virus sa zaštitnim zidom** komponenti koje se mogu instalirati. Ako vam podrazumevane postavke ne odgovaraju, možete ukloniti/dodati određene komponente.

Međutim, možete izabrati samo neku od komponenata koje se nalaze u izdanju programa AVG koje ste kupili. U dijalogu Izbor komponenti bice ponudena instalacija samo tih komponenti!

- **Izbor jezika**

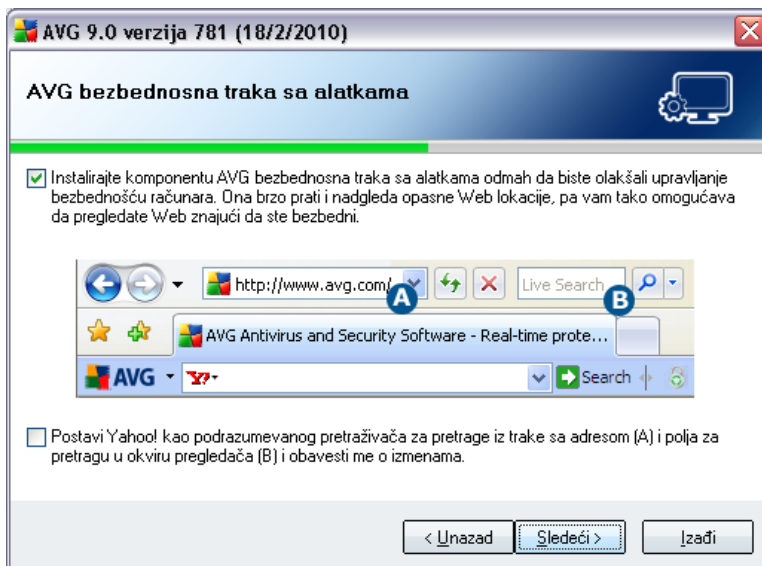
U okviru liste komponenata koje ce se instalirati, možete definisati na kom jeziku (jezicima) ce se instalirati AVG. Potvrdite izbor u polju za potvrdu **Dodatni instalirani jezici**, a zatim izaberite željeni jezik u odgovarajućem meniju.

- **Dodatne komponente za skener e-pošte**

Kliknite na stavku **Skener e-pošte** da biste je otvorili i odredili koja ce se dodatna komponenta instalirati kako bi se zagarantovala bezbedna upotreba e-pošte. Podrazumevano, instalira se **Dodatna komponenta za Microsoft Outlook**. Druga specifična opcija je **Dodatna komponenta za The Bat!** Ako koristite neki drugi klijent za e-poštu (*MS Exchange, Qualcomm Eudora, ...*), izaberite opciju **Skener lične e-pošte** da biste automatski obezbedili komunikaciju preko e-pošte, bez obzira na to koji program za e-poštu koristite.

Zatim pritisnite dugme **Sledece** .

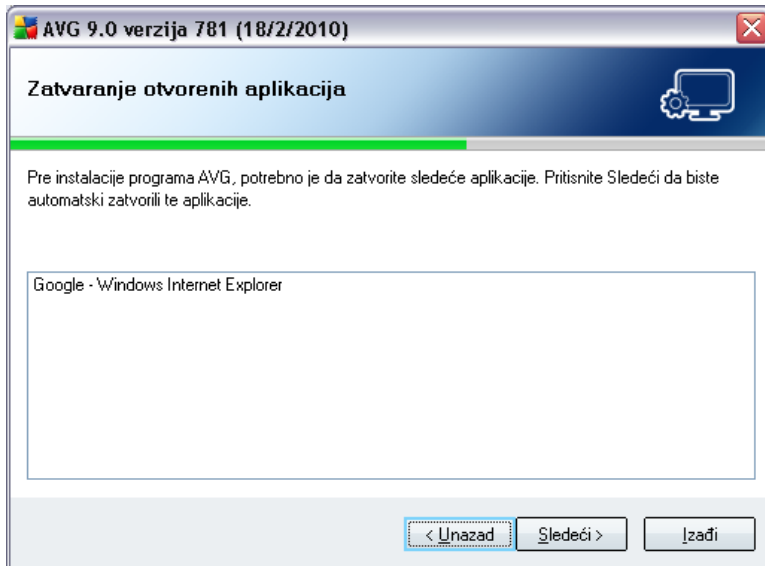
5.8. AVG bezbednosna traka sa alatkama



U dijalogu **AVG bezbednosna traka sa alatkama** , odlucite da li želite da instalirate **AVG bezbednosnu traku sa alatkama** (provera rezultata pretrage podržanim Internet pretraživačima). Ako ne promenite podrazumevana podešavanja, ova komponenta ce biti automatski instalirana u vaš Internet pregledac (trenutno su podržani sledeci pregledaci: Microsoft Internet Explorer v. 6.0 ili novija verzija i Mozilla Firefox v. 2.0 ili novija verzija) kako bi vam pružila sveobihvatnu zaštitu dok pregledate Internet.

Takode cete moci da izaberete da li želite da koristite Yahoo! kao podrazumevani pretraživac. Ako želite, potvrdite izbor u odgovarajucem polju za potvrdu.

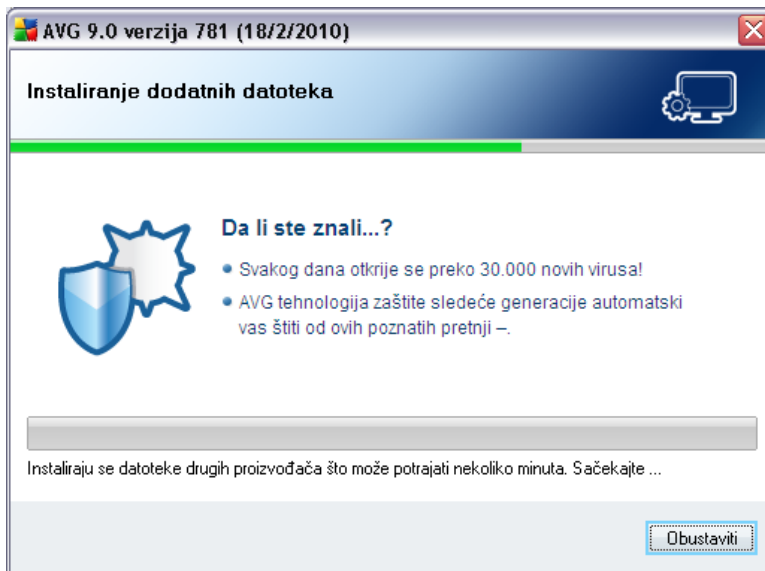
5.9. Zatvaranje otvorenih aplikacija



Dijalog **Zatvaranje otvorenih aplikacija** ce se pojaviti tokom procesa instalacije samo ukoliko su u tom trenutku na racunaru aktivni programi koji mogu da izazovu konflikte. Potom ce se prikazati lista programa koje je potrebno da zatvorite kako bi se proces instalacije uspešno završio. Kliknite na dugme **Dalje** da biste potvrdili da želite da zatvorite odgovarajuće aplikacije i da biste prešli na sledeci korak.

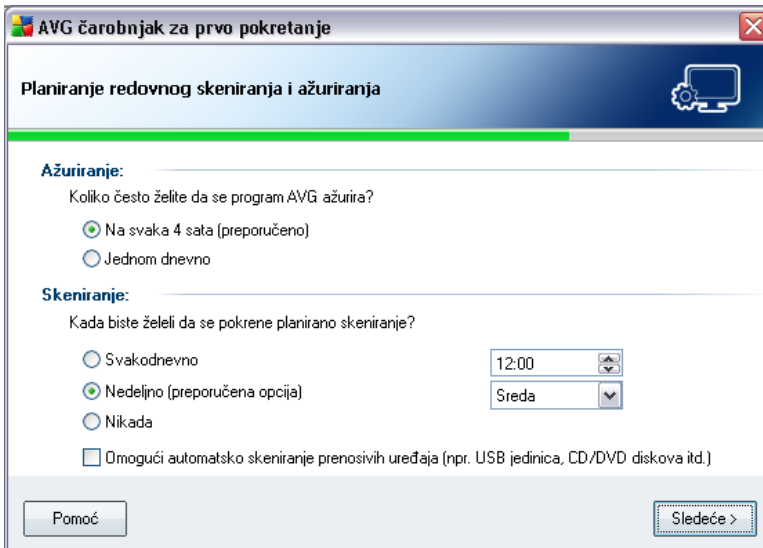
5.10. Instalacija programa AVG

Dijalog **Instalacija programa AVG** prikazuje tok instalacionog procesa i ne zahteva angažovanje korisnika:



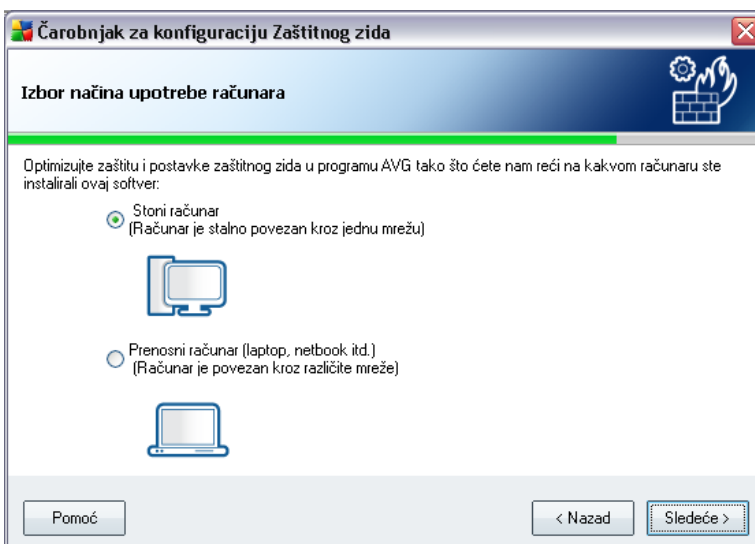
Kada je proces instalacije završen, automatski cete biti preusmereni na sledeci dijalog.

5.1.1. Planiranje redovnog skeniranja i ažuriranja



U dijalogu **Planiranje redovnog skeniranja i ažuriranja** možete podesiti interval u kojem će se proveravati da li postoje nove datoteke za ažuriranje i definisati vreme pokretanja [planiranog skeniranja](#). Preporučujemo da zadržite podrazumevane vrednosti. Kliknite na dugme **Sledeće** da biste nastavili.

5.1.2. Izbor načina upotrebe računara



U ovom dijalogu, **čarobnjak za konfigurisanje zaštitnog zida** pitace vas koji tip računara koristite. Na primer, vaš notebook računar koji se povezuje sa Internetom sa mnogo različitih lokacija (*aerodromi, hotelske sobe itd.*) zahteva bezbednosna pravila koja su strožija od onih za računar u domenu (*mreža preduzeća itd.*). U zavisnosti od izabranog tipa korišćenja računara, podrazumevana pravila komponente **Zaštitni zid** bice definisana sa razlicitim bezbednosnim nivoom.

Možete izabrati jednu od dve opcije:

- **Stoni računar**
- **Prenosni računar**

Potvrdite svoj izbor tako što cete kliknuti na dugme **Sledeće** i preci na sledeci dijalog.

5.13. Internet veza na vašem računaru



U ovom dijalogu, **Čarobnjak za konfiguraciju zaštitnog zida** pita vas na koji se način računar povezuje sa Internetom. U zavisnosti od izabranog tipa veze, podrazumevana pravila komponente **Zaštitni zid** bice definisana sa razlicitim nivoom bezbednosti.

Možete izabrati jednu od tri opcije:

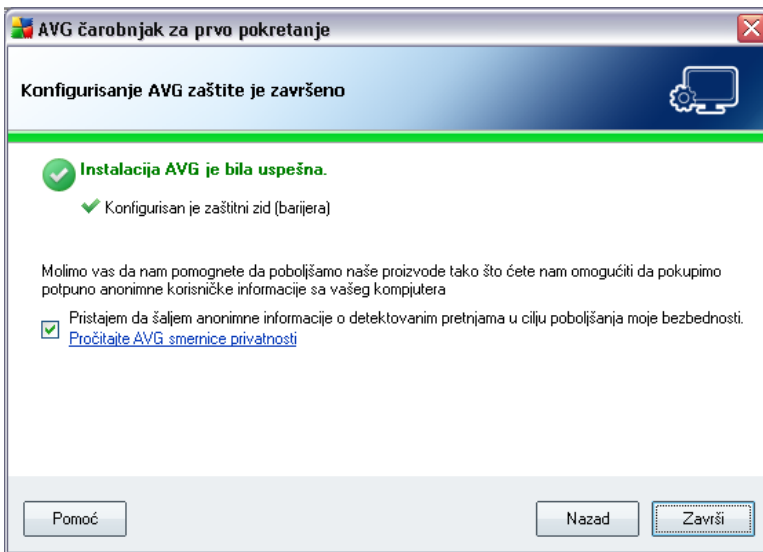
- **Direktno putem modema**
- **Direktno putem žičnog ili bežičnog rutera**

- **Vaš racunar je deo domena**

Izaberite tip veze koji najbolje opisuje nacin povezivanja vašeg racunara sa Internetom.

Potvrdite svoj izbor tako što cete kliknuti na dugme **Sledece** i preci na sledeci dijalog.

5.14. Konfigurisanje AVG zaštite je završeno



Sada je **AVG 9 Anti-Virus sa zaštitnim zidom** konfigurisan.

U ovom dijalogu možete da odlucite da li želite da aktivirate opciju anonimnog izveštavanja o „exploit“ pretnjama i opasnim Web lokacijama AVG laboratoriji virusa. Ako želite, izaberite opciju **Pristajem da šaljem ANONIMNE informacije o otkrivenim pretnjama u cilju poboljšanja moje bezbednosti** .

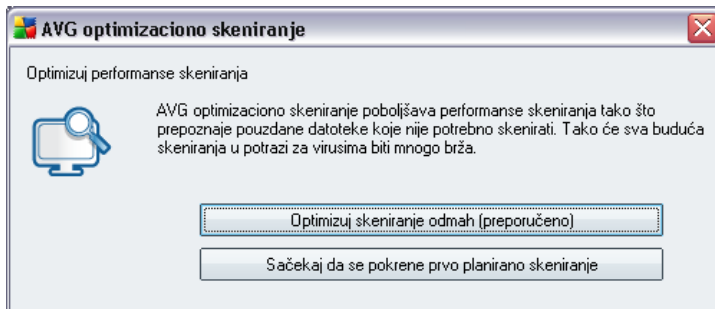
Na kraju kliknite na dugme **Završi**. Možda ce biti potrebno da ponovo pokrenete racunar kako biste mogli da pocnete da radite sa programom AVG.

6. Nakon instalacije

6.1. Optimizacija skeniranja

Funkcija za optimizaciju skeniranja pretražuje fascikle u operativnom sistemu *Windows* i fascikle *programskih datoteka* u kojima detektuje odgovarajuće datoteke (*u ovom trenutku to su sledeće datoteke: *.exe, *.dll i *.sys*) i čuva informacije o tim datotekama. Kada se sledeći put bude pristupalo tim datotekama, one se neće ponovo skenirati, čime se značajno skraćuje vreme skeniranja.

Kada je proces instalacije završen, od vas će se tražiti da putem novog dijaloga optimizujete skeniranje:



Preporučujemo vam da koristite ovu opciju i da pokrenete proces optimizacije skeniranja tako što ćete kliknuti na dugme **Optimizuj skeniranje odmah**.

6.2. Registracija proizvoda

Kada završite instalaciju programa **AVG 9 Anti-Virus sa zaštitnim zidom**, registrujte svoj proizvod na Web lokaciji kompanije AVG (<http://www.avg.com/>), stranica **Registracija** (*sledite uputstva koja se nalaze na stranici*). Nakon registracije, imaćete pun pristup AVG korisničkom nalogu, AVG informativnom biltenu i drugim uslugama koje su dostupne isključivo registrovanim korisnicima.

6.3. Pristupanje korisničkom interfejsu

AVG korisničkom interfejsu možete pristupiti na nekoliko načina:

- dvaput kliknite na AVG ikonu u sistemskoj paleti
- dvaput kliknite na AVG ikonu na radnoj površini

- iz menija **Start/Programi/AVG 9.0/AVG korisnicki interfejs**

6.4. Skeniranje celog racunara

Postoji potencijalni rizik da je vaš racunar zaražen virusom pre instalacije programa **AVG 9 Anti-Virus sa zaštitnim zidom**. Zato je potrebno da pokrenete **Skeniranje celog racunara**, kako biste bili sigurni da racunar nije zaražen.

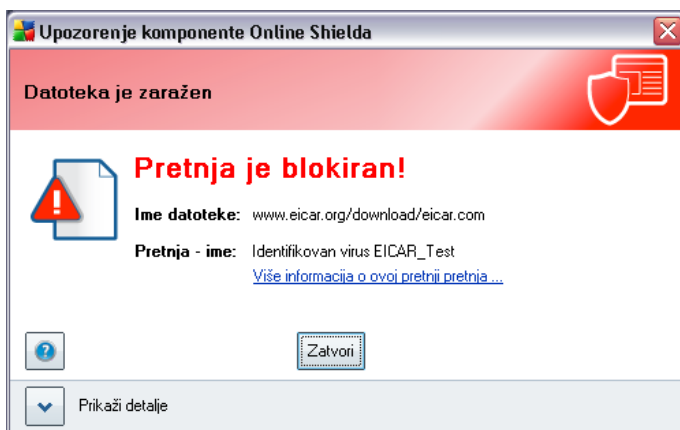
Uputstva za **Skeniranje celog racunara** potražite u poglavlju **Skeniranje programom AVG**.

6.5. Eicar test

Da biste potvrdili da je **AVG 9 Anti-Virus sa zaštitnim zidom** pravilno instaliran, možete obaviti EICAR test.

EICAR test je standardan i potpuno bezbedan metod koji se koristi za testiranje funkcionisanja antivirusnog sistema. Bezbedno ga je širiti zato što nije pravi virus i ne sadrži nijedan deo virusnog koda. Vecina proizvođa reaguje na njega kao na virus (*jako najčešće izveštavaju o njemu sa ociglednim imenom, kao što je „EICAR-AV-Test“*). Virus EICAR možete da preuzmete sa EICAR Web lokacije na adresi www.eicar.com gde takode možete pronaci sve neophodne informacije o EICAR testu.

Pokušajte da preuzmete datoteku ***eicar.com*** i sacuvajte je na lokalnom disku. Cim potvrdite preuzimanje datoteke za testiranje, **Online Shield** ce reagovati upozorenjem. Ovo obaveštenje pokazuje da je AVG ispravno instaliran na racunaru.



Na Web lokaciji <http://www.eicar.com> takode možete da preuzmete komprimovanu verziju EICAR „virusa“ (npr. u obliku *eicar_com.zip*). **Online Shield** vam omogućava da



preuzmete ovu datoteku i da je sacuvate na lokalnom disku, ali ce u tom slucaju **[Stalni štit](#)** detektovati „virus“ kada pokušate da je otpakujete. **Ako AVG ne identifikuje probnu datoteku EICAR kao virus, trebalo bi da ponovo proverite konfiguraciju programa!**

6.6. Podrazumevana konfiguracija programa AVG

Podrazumevanu konfiguraciju (*tj. nacin na koji je aplikacija podešena odmah nakon instalacije*) programa **AVG 9 Anti-Virus sa zaštitnim zidom** podesio je proizvođač softvera kako bi sve komponente i funkcije bile podešene tako da se postignu optimalne performanse.

Nemojte menjati AVG konfiguraciju ukoliko nemate dobar razlog za to! Podešavanja bi trebalo da menjaju samo iskusni korisnici.

Manje izmene [AVG komponenti](#) mogu se obavljati direktno iz korisnickog interfejsa te komponente. Ako bude potrebno da prilagodite konfiguraciju programa AVG svojim potrebama, idite na [AVG napredna podešavanja](#): izaberite stavku iz sistemskog menija **Alatke/Napredna podešavanja** i uredite konfiguraciju programa AVG u dijalogu [AVG napredna podešavanja](#) koji ce se otvoriti.

7. AVG korisnicki interfejs

AVG 9 Anti-Virus sa zaštitnim zidom se otvara sa glavnim prozorom:



Glavni prozor je podeljen na nekoliko odeljaka:

- **Sistemski meni** (gornja sistemska linija u prozoru) je standardni element za navigaciju koji vam omogućava da pristupite svim AVG komponentama, uslugama i funkcijama - [detalji>>](#)
- **Informacije o bezbednosnom statusu** (gornji deo prozora) sadrži informacije o trenutnom statusu programa AVG - [detalji>>](#)
- **Brze veze** (leva strana prozora) omogućavaju vam da brzo pristupite najvažnijim AVG zadacima i onima koji se najčešće koriste - [detalji>>](#)
- **Pregled komponenti** (središnji deo prozora) sadrži pregled instaliranih AVG

komponenata - [detalji>>](#)

- **Statistika** (*donji levi deo prozora*) sadrži sve statističke podatke u vezi sa radom programa - [detalji>>](#)
- **Ikona sistemske palete** (*donji desni ugao ekrana, na sistemskoj paleti*) označava trenutni status programa AVG - [detalji>>](#)

7.1. Sistemski meni

Sistemski meni je standardni oblik navigacije koji se koristi u svim Windows aplikacijama. Postavljen je horizontalno, na samom vrhu glavnog prozora programa **AVG 9 Anti-Virus sa zaštitnim zidom**. Pomocu sistemskog menija možete pristupiti određenim AVG komponentama, funkcijama i uslugama.

Sistemski meni ima pet glavnih odeljaka:

7.1.1. Datoteka

- **Izadi** - zatvaranje **AVG 9 Anti-Virus sa zaštitnim zidom** korisničkog interfejsa. Međutim, aplikacija AVG će i dalje raditi u pozadini, pa će vaš računar biti zaštićen!

7.1.2. Komponente

Stavka **Komponente** u sistemskom meniju sadrži veze ka svim instaliranim AVG komponentama koje služe za otvaranje podrazumevanih dijaloga u korisničkom interfejsu:

- **Pregled sistema** - predite na podrazumevani dijalog korisničkog interfejsa sa [pregledom svih instaliranih komponenti i njihovim statusom](#)
- **Antivirus** - služi za otvaranje podrazumevane stranice komponente [Antivirus](#)
- **Anti-Rootkit** - služi za otvaranje podrazumevane stranice komponente [Anti-Rootkit](#)
- **Antispajver** - služi za otvaranje podrazumevane stranice komponente [Antispajver](#)
- **Zaštitni zid** - služi za otvaranje podrazumevane stranice komponente [Zaštitni zid](#)
- **Skener linkova** - služi za otvaranje podrazumevane stranice komponente [Skener linkova](#)

- **Skener e-pošte** - služi za otvaranje podrazumevane stranice komponente [Skener e-pošte](#)
- **Licenca** služi za otvaranje podrazumevane stranice komponente [Licenca](#)
- **Online Shield** - služi za otvaranje podrazumevane stranice komponente [Online Shield](#)
- **Stalni štiti** - služi za otvaranje podrazumevane stranice komponente [Stalni štiti](#)
- **Upravljanje ažuriranjem** - služi za otvaranje podrazumevane stranice komponente [Upravljanje ažuriranjem](#)

7.1.3. Istorija

- [Rezultati skeniranja](#) - prelazak u AVG interfejs za testiranje, tj. u dijalog [Pregled rezultata skeniranja](#)
- [Detekcija od strane stalnog štita](#) - otvaranje dijaloga sa pregledom pretnji koje je detektovala komponenta [Stalni štiti](#)
- [Detekcija od strane skenera e-pošte](#) - otvaranje dijaloga sa pregledom priloga e-poruka koje je kao opasne detektovala komponenta [Skener e-pošte](#)
- [Stavke koje je pronašao Online Shield](#) - otvaranje dijaloga sa pregledom pretnji koje je detektovao [Online Shield](#)
- [Skladište za viruse](#) - otvaranje interfejsa karantina ([Skladište za viruse](#)) u koji AVG premešta sve detektovane slucajeve zaraze koji se iz nekog razloga ne mogu automatski izleciti. Zaražene datoteke su izolovane u karantinu, pa je bezbednost vašeg racunara zagarantovana; istovremeno, zaražene datoteke se cuvaju radi potencijalnog oporavka u buducnosti.
- [Evidencija istorije dogadaja](#) - otvaranje interfejsa evidencije istorije sa pregledom svih evidentiranih **AVG 9 Anti-Virus sa zaštitnim zidom** radnji.
- [Zaštitni zid](#) - otvara interfejs za podešavanje zaštitnog zida na kartici [Datoteke evidencije](#) sa detaljnim pregledom svih radnji komponente Zaštitni zid.

7.1.4. Alatke

- **Skeniraj racunar** - prelazak u [AVG interfejs za skeniranje](#) i pokretanje skeniranja celog racunara
- **Skeniraj izabranu fasciklu** - prelazak u [AVG interfejs za skeniranje](#), nakon cega sa prikaza vašeg racunara u obliku stabla možete izabrati datoteke i fascikle koje želite da skenirate
- **Skeniraj datoteku** – omogućava vam da pokrenete test pojedinačne datoteke na zahtev tako što ćete je izabrati sa prikaza vaše disk jedinice u obliku stabla
- **Ažuriranje** – automatsko pokretanje procesa ažuriranja za **AVG 9 Anti-Virus sa zaštitnim zidom**
- **Ažuriranje iz direktorijuma** - pokretanje procesa ažuriranja na osnovu datoteka za ažuriranje koje se nalaze u navedenoj fascikli na lokalnom disku. Međutim, korišćenje ove opcije preporučuje se isključivo u hitnim slučajevima, npr. ako nije dostupna veza sa Internetom (*na primer, vaš racunar je zaražen i nije povezan sa Internetom; vaš racunar je povezan na mrežu koja nema pristup Internetu, itd.*). U prozoru koji će se otvoriti, izaberite fasciklu u koju ste prethodno smestili datoteku za ažuriranje, pa pokrenite proces ažuriranja.
- **Napredna podešavanja** – otvaranje dijaloga **AVG napredna podešavanja** u kojem možete urediti **AVG 9 Anti-Virus sa zaštitnim zidom** konfiguraciju. Uglavnom se preporučuje da zadržite podrazumevana podešavanja ove aplikacije koje je definisao proizvođač softvera.
- **Podešavanja zaštitnog zida** - otvaranje samostalnog dijaloga za napredno konfigurisanje komponente **Zaštitni zid**

7.1.5. Pomoc

- **Sadržaj** - otvaranje AVG datoteka pomoci
- **Pronadite pomoc na mreži** - otvaranje AVG Web lokacije (<http://www.avg.com/>) na stranici centra za korisničku podršku
- **Vaš AVG Web** - otvaranje AVG Web lokacije (<http://www.avg.com/>)
- **Više informacija o virusima i pretnjama** - otvaranje **Enciklopedije virusa** na mreži u kojoj možete pronaći detaljne informacije o identifikovanom virusu
- **Ponovo aktiviraj** – otvaranje dijaloga **Aktivacija AVG programa** sa podacima koje ste uneli u dijalogu **Prilagodavanje programa AVG** u toku **procesa**

[instalacije](#). U ovom dijalogu možete uneti svoj broj licence kako biste zamenili prodajni broj (*broj sa kojim ste instalirali AVG*) ili zamenili stari broj licence (*npr. prilikom nadogradnje na nov AVG proizvod*).

- **[Registrujte odmah](#)** - povezivanje sa stranicom za registraciju na AVG Web lokaciji (<http://www.avg.com/>). Unesite registracione podatke; besplatnu tehnicku podršku mogu dobiti samo korisnici koji registruju svoj AVG proizvod.

Napomena: *Ako koristite probnu verziju programa **AVG 9 Anti-Virus sa zaštitnim zidom**, poslednje dve stavke su **Kupite odmah** i **Aktivacija** i omogućavaju vam da odmah kupite punu verziju programa. Ako je **AVG 9 Anti-Virus sa zaštitnim zidom** instaliran sa prodajnim brojem, prikazuju se stavke **Registracija** i **Aktivacija**. Više informacija potražite u odeljku [Licenca](#) u ovoj dokumentaciji.*

- **O programu AVG** - otvaranje dijaloga **Informacije** koji sadrži pet kartica sa podacima o imenu programa, verziji programa i baze podataka o virusima, sistemskim informacijama, ugovorom o licenciranju i kontakt podacima kompanije **AVG Technologies CZ**.

7.2. Informacije o bezbednosnom statusu

Odeljak **Informacije o bezbednosnom statusu** nalazi se u gornjem delu glavnog prozora programa AVG. U ovom odeljku uvek možete pronaci informacije o trenutnom bezbednosnom statusu programa **AVG 9 Anti-Virus sa zaštitnim zidom**. Pogledajte opise ikona iz ovog odeljka i njihovo znacenje:



Zelena ikona ukazuje na to da AVG potpuno funkcionalan. Racunar je u potpunosti zašticen i ažuriran, a sve instalirane komponente ispravno rade.



Narandžasta ikona upozorava na to da su neke komponente nepravilno konfigurisane i da bi trebalo da obratite pažnju na njihova svojstva/podešavanja. Nema kritičnih problema u programu AVG, a verovatno ste odlucili da isključite neku komponentu. I dalje ste zaštriceni pomocu programa AVG. Medutim, obratite pažnju na podešavanja problematicne komponente! Njeno ime ce biti prikazano u odeljku **Informacije o bezbednosnom statusu**.

Ova ikona se takode pojavljuje i ako ste iz nekog razloga odlucili da [zanemarite status greške komponente](#) (opcija „Zanemari stanje komponente“ je dostupna u kontekstualnom meniju koji se otvara tako što cete kliknuti desnim tasterom miša iznad odgovarajuće ikone komponente u pregledu komponente u glavnom

prozoru programa AVG). Možda ćete morati da koristite ovu opciju u određenoj situaciji, ali preporučujemo da isključite opciju „**Zanemari stanje komponente**“ što pre.



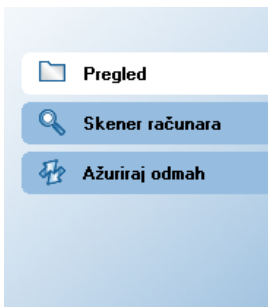
Crvena ikona ukazuje na to da je status programa AVG kritičan! Neke komponente ne rade ispravno pa AVG ne može da zaštiti vaš računar. Odmah pokušajte da rešite prijavljeni problem. Ako ne možete sami da rešite problem, obratite se [AVG timu za tehničku podršku](#).

Preporučuje se da obratite pažnju na Informacije o bezbednosnom statusu, a u slučaju da izveštaj ukazuje na neki problem, odmah pokušajte da ga rešite. U suprotnom vaš računar će biti izložen riziku!

Napomena: Informacije o statusu programa AVG možete dobiti u bilo kojem trenutku i pomoću [ikone u sistemskoj traci poslova](#).

7.3. Brze veze

Brze veze (u odeljku sa leve strane u [AVG korisničkom interfejsu](#)) omogućavaju trenutni pristup najvažnijim i najčešće korišćenim funkcijama programa AVG:



- **Pregled** - ovu vezu koristite da biste sa bilo kojeg otvorenog AVG interfejsa prešli na podrazumevani, sa pregledom svih instaliranih komponenti - pogledajte poglavlje [Pregled komponenti >>](#)
- **Skener računara** - ovu vezu koristite da biste otvorili AVG interfejs za skeniranje iz kojeg možete direktno pokretati testove, planirati skeniranje ili uređivati parametre - pogledajte poglavlje [AVG skeniranje >>](#)
- **Ažuriraj odmah** - pomoću ove veze otvara se interfejs za ažuriranje i trenutno se pokrene proces ažuriranja AVG softvera - pogledajte poglavlje [AVG ažuriranje >>](#)

Te veze su uvek dostupne iz korisnickog interfejsa. Kada upotrebite brzu vezu za pokretanje određenog procesa, otvorice se novi dijalog u korisnickom interfejsu, ali ce brze veze i dalje biti dostupne. Osim toga, aktivni proces prikazan je graficki..

7.4. Pregled komponenti

Odeljak **Pregled komponenta** nalazi se u centralnom delu [AVG korisnickog interfejsa](#). Ovaj odeljak ima dva dela:

- Pregled svih instaliranih komponenti koji se sastoji od panela sa ikonom komponente i informacije o tome da li je ta komponenta aktivna ili ne
- Opis izabrane komponente

U okviru programa **AVG 9 Anti-Virus sa zaštitnim zidom**, odeljak **Pregled komponenti** sadrži informacije o sledecim komponentama:

- **Antivirusni program** obezbeduje zaštitu vašeg racunara od virusa koji pokušavaju da prodru u njega - [detalji >>](#)
- **Antispajver** skenira vaše aplikacije u pozadini dok ih pokrecete - [detalji >>](#)
- **Zaštitni zid** kontroliše nacin na koji racunar razmenjuje podatke sa drugim racunarima na Internetu ili lokalnoj mreži - [detalji >>](#)
- **Skener linkova** proverava rezultate pretrage koji se prikazuju u pregledacu Interneta - [detalji >>](#)
- **Anti-Rootkit** detektuje programe i tehnologije ciji je cilj da kamufliraju zlonamerni softver - [detalji >>](#)
- **Skener e-pošte** proverava dolaznu i odlaznu poštu u potrazi za virusima - [detalji >>](#)
- U odeljku **Licenca** se prikazuje broj licence, tip licence i datum njenog isteka - [detalji >>](#)
- **Online Shield** skenira sve podatke koje preuzima pregledac Weba - [detalji >>](#)
- **Stalni štit** radi u pozadini i skenira datoteke prilikom njihovog kopiranja, otvaranja ili cuvanja - [detalji >>](#)
- **Upravljanje ažuriranjem** upravlja ažuriranjem programa AVG - [detalji >>](#)

Kliknite na ikonu određene komponente da biste je označili u pregledu komponenti. Opis osnovnih funkcija komponente istovremeno će se pojaviti u donjem delu korisničkog interfejsa. Dvaput kliknite na ikonu da biste otvorili interfejs izabrane komponente sa listom osnovnih statističkih podataka.

Kliknite desnim tasterom miša iznad ikone komponente da biste otvorili kontekstualni meni. Osim otvaranja grafičkog interfejsa komponente možete izabrati i opciju **Zanemari stanje komponente**. Izaberite ovu opciju da biste naveli da ste svesni [stanja greške komponente](#), ali da iz nekog razloga želite da se AVG ponaša na ovakav način i ne želite da vas obaveštava putem sive ikone na [sistemskej paleti](#).


7.5. Statistika


Odeljak **Statistika** nalazi se u levom donjem uglu [AVG korisničkog interfejsa](#). On sadrži informacije o radu programa:

- **Poslednje skeniranje** - datum poslednjeg obavljenog skeniranja
- **Poslednje ažuriranje** - datum poslednjeg pokrenutog ažuriranja
- **Baza podataka o virusima** - informiše vas o tome koja je verzija baze podataka o virusima trenutno instalirana
- **AVG verzija** - informiše vas o tome koja je verzija programa AVG (*broj ima oblik 9.0.xx, gde 9.0 označava broj linije proizvoda, a xx predstavlja broj verzije*)
- **Licenca istice** - datum isteka vaše AVG licence

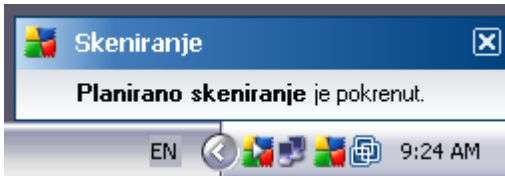
7.6. Ikona sistemske palete

Ikona sistemske palete (na Windows traci zadataka) pokazuje trenutni status programa **AVG 9 Anti-Virus sa zaštitnim zidom**. Stalno je vidljiva u sistemskej paleti, bez obzira na to da li je glavni prozor programa AVG otvoren ili zatvoren.

Ukoliko je u boji  **ikona sistemske palete** ukazuje na to da su sve AVG komponente aktivne i potpuno funkcionalne. Takođe, AVG ikona na sistemskej paleti može se prikazivati u boji i kada je AVG u stanju greške, ali ste potpuno svesni situacije i namerno odlucite da [zanemarite stanje komponente](#).

Ikona sa znakom uzvika  ukazuje na problem (*neaktivna komponenta, greška, itd.*). Dvaput kliknite na **ikonu u sistemskej paleti** da biste otvorili glavni prozor i uredili neku komponentu.

Ikona sistemske palete vas obaveštava i o trenutnim aktivnostima programa AVG i mogućim promenama statusa programa (*npr. automatsko pokretanje planiranog skeniranja ili ažuriranja, promena profila zaštitnog zida, promena statusa komponente, greška, ...*) putem iskacuceg prozora koji se otvara iznad AVG ikone u sistemoj paleti:



Ikona u sistenskoj paleti može se koristiti i kao brza veza za pristup glavnom prozoru programa AVG u bilo kojem trenutku - dvaput kliknite na ikonu. Ako desnim tasterom miša kliknete na **ikonu u sistenskoj paleti** otvorice se kratak kontekstualni meni koji sadrži sledece opcije:

- **Otvori AVG korisnicki interfejs** - kliknite da biste otvorili [AVG korisnicki interfejs](#)
- **Ažuriraj** - odmah se pokrece [ažuriranje](#)



8. Komponente programa AVG

8.1. Antivirusni program

8.1.1. Antivirusni program Principi

Mašina za skeniranje u okviru antivirusnog programa skenira sve datoteke i njihove aktivnosti (otvaranje/zatvaranje datoteka itd.) kako bi se proverilo da li sadrže poznate viruse. Detektovani virusi bice blokirani tako da ne mogu da preduzmu nikakvu akciju, a zatim ce biti izbrisani ili smešteni u karantin. Vecina antivirusnih softvera koristi i heuristicko skeniranje, kod kojeg se u datotekama traže tipicne karakteristike virusa, takozvani viralni potpisi. To znaci da ce antivirusni softver biti u stanju da detektuje nov, nepoznat virus ako taj virus ima neke od tipicnih karakteristika postojecih virusa.

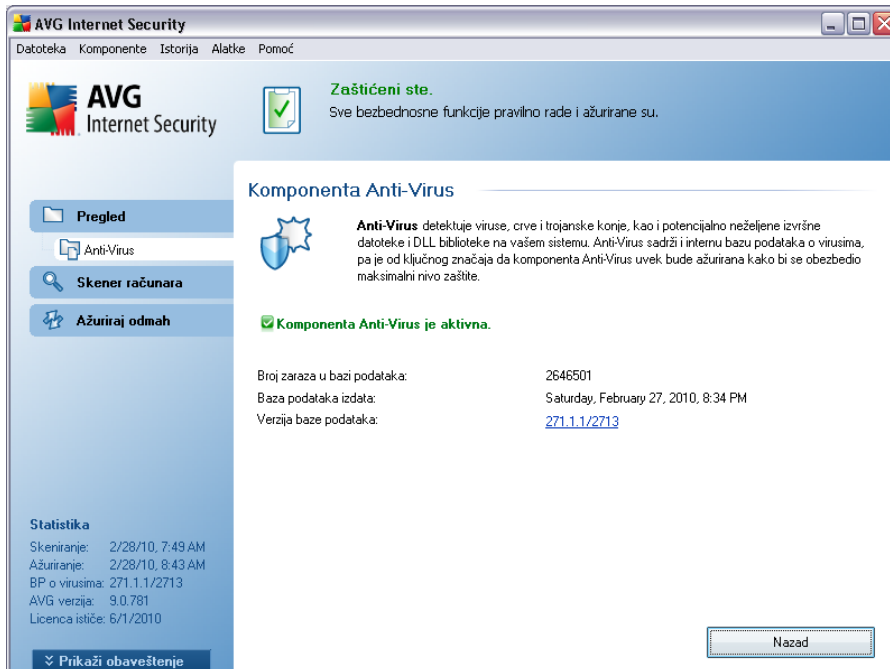
Važna funkcija aktivirusne zaštite jeste to da se nijedan poznat virus ne može pokrenuti na racunaru!

Pošto samo jedna tehnologija može biti nedovoljna za otkrivanje ili identifikaciju virusa, ***Antivirusni program*** kombinuje nekoliko tehnologija da bi obezbedio zaštitu racunara:

- Skeniranje - traženje niski znakova koje su karakteristicne za dati virus
- Heuristicka analiza - dinamička emulacija uputstava skeniranog objekta u virtuelnom racunarskom okruženju
- Genericko otkrivanje - otkrivanje uputstava karakteristicnih za dati virus/grupu virusa

AVG takode može da analizira i otkrije izvršne aplikacije ili DLL biblioteke koje mogu da budu potencijalno neželjene u okviru sistema. Te pretnje nazivamo potencijalno neželjenim programima (razne vrste špijunskog softvera, advera itd.) Osim toga, AVG skenira sistemski registrator u potrazi za sumnjivim stavkama, privremenim Internet datotekama i kolacicima za pracenje i dozvoljava da sve potencijalno štetne stavke tretirate na isti nacin kao i bilo koju drugu zarazu.

8.1.2. Anti-Virus Interfejs



Interfejs komponente **Antivirus** pruža kratak pregled njenih funkcija, informacije o trenutnom statusu komponente (*Komponenta Antivirus je aktivna.*), kao i kratak pregled statistike komponente **Antivirus** :

- **Definicije zaraza** - broj označava količinu virusa u najnovijoj verziji baze podataka virusa
- **Najnovija verzija baze podataka** - navodi datum i vreme poslednjeg ažuriranja baze podataka virusa
- **Verzija baze podataka** - definiše broj najnovije baze podataka virusa; taj broj se uvećava nakon svakog ažuriranja baze podataka virusa

U interfejsu ove komponente dostupno je samo jedno dugme (**Nazad**) - kliknite na ovo dugme da biste se vratili u podrazumevani [AVG korisnički interfejs](#) (pregled komponenti).

Imajte u vidu sledeće: *Proizvodac softvera je podesio sve AVG komponente tako da se postignu optimalne performanse. Nemojte menjati AVG konfiguraciju ukoliko nemate dobar razlog za to. Podešavanja smeju da menjaju samo iskusni korisnici. Ako je potrebno da promenite konfiguraciju programa AVG, u sistemskom meniju izaberite*



stavku **Alatke / Napredna podešavanja**, a zatim uredite AVG konfiguraciju u novootvorenom dijalogu [AVG napredna podešavanja](#).

8.2. Antispajver

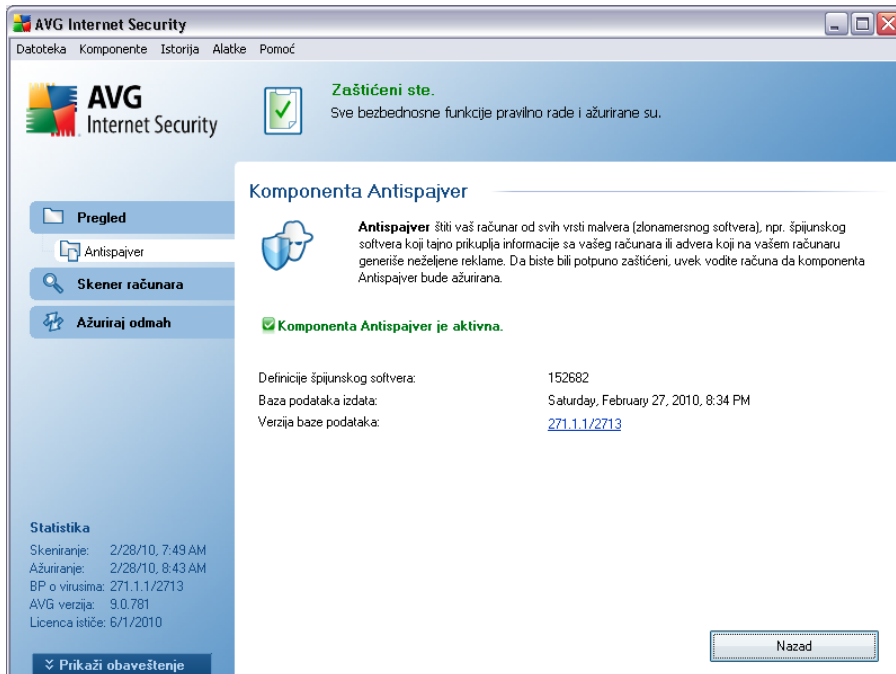
8.2.1. Antispajver Principi

Špijunski softver se obično definiše kao tip malvera, tj. softver koji prikuplja informacije sa računara korisnika bez njegovog znanja ili odobrenja. Neke špijunske aplikacije mogu biti namerno instalirane i često sadrže reklame, iskacuce prozore ili različite vrste neugodnog softvera.

Trenutno, najčešći izvor zaraze su Web lokacije sa potencijalno opasnim sadržajem. Rasprostranjene su i druge metode prenosa, npr. putem e-pošte ili prenos crvima i virusima. Najvažnija zaštita jeste da koristite uvek uključeni skener u pozadini, kao što je **Antispajver** komponenta koja radi kao stalni štit i skenira aplikacije u pozadini dok ih pokrecete.

Postoji i potencijalni rizik da je malver prenet na racunar pre instalacije programa AVG ili da niste ažurirali program **AVG 9 Anti-Virus sa zaštitnim zidom** najnovijim [ispravkama za bazu podataka i program](#). Zato vam AVG omogućava da u potpunosti skenirate racunar u potrazi za malverom/špijunskim softverom koristeći funkciju skeniranja. Ona takode otkriva i malver koji je u stanju spavanja i neaktivan je, tj. malver koji je preuzet, ali još nije aktiviran.

8.2.2. Interfejs komponente Antispajver



Interfejs komponente **Antispajver** pruža kratak pregled njenih funkcija, informacije o trenutnom statusu komponente (*Komponenta Antispajver je aktivna.*), kao i neke **Antispajver** statistike:

- **Definicije špijunskog softvera** - broj označava količinu uzoraka špijunskog softvera u najnovijoj verziji baze podataka špijunskog softvera
- **Najnovija verzija baze podataka** - navodi datum i vreme poslednjeg ažuriranja baze podataka špijunskog softvera
- **Verzija baze podataka** - definiše broj najnovije baze podataka špijunskog softvera; taj broj se uvećava nakon svakog ažuriranja baze podataka virusa

U interfejsu ove komponente dostupno je samo jedno dugme (**Nazad**) - kliknite na ovo dugme da biste se vratili u podrazumevani [AVG korisnički interfejs](#) (pregled komponenti).

Napomena: proizvođač softvera je podesio sve AVG komponente tako da se postignu optimalne performanse. Nemojte menjati AVG konfiguraciju ukoliko nemate dobar razlog za to. Podešavanja smeju da menjaju samo iskusni korisnici. Ako je potrebno da promenite konfiguraciju programa AVG, u sistemskom meniju izaberite stavku

Alatke / Napredna podešavanja, a zatim uredite AVG konfiguraciju u novootvorenom dijalogu [AVG napredna podešavanja](#).

8.3. Anti-Rootkit

Rootkit je program osmišljen da preuzme potpunu kontrolu nad računarskim sistemom bez dozvole vlasnika sistema i administratora kojima je dozvoljen pristup. Pristup hardveru nije potreban jer je cilj rootkit programa da preuzme kontrolu nad operativnim sistemom koji je instaliran na hardveru. Rootkit programi najčešće prikrivaju svoje prisustvo na sistemu pomocu subverzije ili izbegavanja standardnih mehanizama za zaštitu operativnog sistema. Ti programi najčešće spadaju u red trojanskih konja, pa su u stanju da prevare korisnike kako bi poverovali da ih mogu bezbedno pokrenuti na sistemu. Tehnike kojima se to postiže obuhvataju prikrivanje aktivnih procesa kako ih ne bi videli programi za nadgledanje ili sakrivanje datoteka ili sistemskih podataka od operativnog sistema.

8.4. Zaštitni zid

Zaštitni zid je sistem koji nameće smernice za kontrolu pristupa između dve ili više mreža tako što blokira/dozvoljava saobraćaj. Zaštitni zid sadrži skup pravila koja štite unutrašnju mrežu od napada koji dolaze spolja (obično sa Interneta) i kontrolišu komunikaciju na svakom mrežnom portu. Komunikacija se procenjuje u skladu sa definisanim pravilima, a zatim se dozvoljava ili zabranjuje. Ako zaštitni zid prepozna pokušaj napada, on „blokira“ pokušaj i ne dopušta da uljez pristupi računaru.

Zaštitni zid je konfigurisan da omogući ili odbije unutrašnju/spoljnu komunikaciju (obosmernu, ka unutra ili ka spolja) kroz definisane portove, kao i za definisane softverske aplikacije. Na primer, zaštitni zid se može konfigurisati tako da dozvoljava da podaci sa Interneta mogu da ulaze i izlaze samo kroz Microsoft Explorer. Svaki pokušaj prenosa podataka kroz neki drugi pregledac biće blokiran.

Zaštitni zid štiti vaše lične informacije od slanja sa računara bez vaše dozvole. On kontroliše način na koji računar razmenjuje podatke sa drugim računarima na Internetu ili lokalnoj mreži. U okviru organizacije, Zaštitni zid takode štiti pojedinačne računare od napada unutrašnjih korisnika drugih računara u mreži.

Preporuka: ne preporučuje se upotreba više zaštitnih zidova na jednom računaru. Bezbednost računara se ne poboljšava ako instalirate više zaštitnih zidova. Verovatno će doći do neusaglašenosti između ove dve aplikacije. Zbog toga vam preporučujemo da koristite samo jedan zaštitni zid na računaru i da deaktivirate ostale cime cete eliminisati rizik od mogućih neusaglašenosti i problema.

8.4.1. Principi funkcionisanja zaštitnog zida

U okviru sistema AVG, komponenta **Zaštitni zid** kontroliše celokupan saobraćaj na svim mrežnim portovima na racunaru. Na osnovu definisanih pravila **Zaštitni zid** procenjuje aplikacije koje su pokrenute na racunaru i (i koje žele da se povežu sa Internetom/ lokalnom mrežom) ili aplikacije koje spolja pristupaju racunaru pokušavajući da se povežu sa njim. **Zaštitni zid** zatim dozvoljava ili zabranjuje komunikaciju na mrežnim portovima za svaku od tih aplikacija. Podrazumevano, ako je aplikacija nepoznata (tj. za nju nije definisano pravilo **Zaštitnog zida**), **Zaštitni zid** će vas pitati da li želite da dozvolite ili blokirate taj pokušaj komunikacije.

Napomena: AVG Zaštitni zid nije predviđen za serverske platforme!

Mogućnosti koje nudi AVG zaštitni zid:

- Dozvoljavanje ili blokiranje pokušaja komunikacije poznatih [aplikacija](#) automatski ili uz vašu potvrdu
- Korišćenje citavih [profila](#) sa unapred definisanim pravilima u skladu sa vašim potrebama
- [Menjanje profila](#) automatski prilikom povezivanja na različite mreže ili upotrebe različitih mrežnih adaptera

8.4.2. Profili zaštitnog zida

Zaštitni zid vam omogućava da definišete određena bezbednosna pravila na osnovu toga da li se vaš racunar nalazi u domenu, da li je u pitanju samostalan racunar ili prenosni racunar.*** Svaka od tih opcija zahteva različit nivo zaštite, a te nivoe pokrivaju odgovarajući profili. Dakle, profil **Zaštitnog zida** je određena konfiguracija komponente **Zaštitni zid**, a možete koristiti nekoliko unapred definisanih konfiguracija.

Dostupni profili

- **Dozvoli sve** –sistemski profil komponente **Zaštitni zid**, unapred podešen od strane proizvođača i uvek dostupan. Kada se ovaj profil aktivira, svaki vid komunikacije preko mreže je dozvoljen, a ne primenjuju se nikakve bezbednosne smernice, kao da je **Zaštitni zid** isključen (tj. sve aplikacije su dozvoljene, ali se paketi ipak proveravaju - da bi se filtriranje u potpunosti onemogućilo, potrebno je da onemogućite Zaštitni zid). Ovaj sistemski profil ne može se kopirati niti brisati, a njegove postavke se ne mogu menjati.

- **Blokiraj sve**– sistemski profil komponente **Zaštitni zid**, unapred podešen od strane proizvođača i uvek dostupan. Kada je ovaj profil aktiviran, svaki oblik komunikacije preko mreže je blokiran, pa je pristup računaru sa spoljnih mreža onemogućen, a ni računar ne može da komunicira sa spoljnim svetom. Ovaj sistemski profil ne može se kopirati niti brisati, a njegove postavke se ne mogu menjati.
- **Prilagodeni profili:**
 - **Direktna veza sa Internetom**– pogodno za standardne stacionarne kućne računare koji su direktno povezani sa Internetom ili notebook računare koji se povezuju sa Internetom izvan bezbedne mreže preduzeća. Izaberite ovu opciju ako se povezujete od kuće ili ako ste u okviru male mreže preduzeća bez centralne kontrole. Ovu opciju izaberite i ako putujete i pristupate Internetu sa notebook računara na nepoznatim i potencijalno opasnim mestima (*internet kafej, hotelska soba itd.*). Kreirace se restriktivnija pravila jer se pretpostavlja da ovi računari nemaju dodatnu zaštitu i zato zahtevaju maksimalnu zaštitu.
 - **Racunar u domenu** – prikladno za računare na lokalnoj mreži, npr. u školskoj ili korporativnoj mreži. Pretpostavlja se da mreža ima dodatne mere zaštite, pa bezbednosni nivo može biti niži nego na samostalnom računaru.
 - **Mala kućna ili kancelarijska mreža** – prikladno za računare u maloj mreži, npr. kod kuće ili u malom preduzeću, gde je najčešće povezano samo nekoliko računara, bez „centralnog“ administratora.

Zamena profila

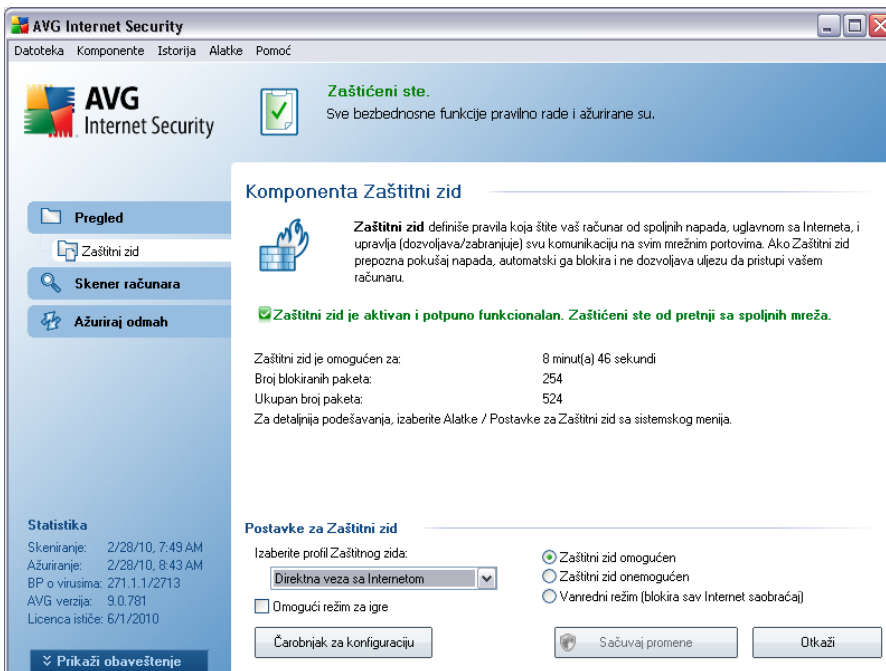
Funkcija zamene profila **Zaštitnom zidu** omogućava da se automatski prebaci na definisani profil prilikom korišćenja određenog mrežnog adaptera ili prilikom povezivanja sa određenim tipom mreže. Ako nekoj mrežnoj oblasti još nije dodeljen profil, prilikom sledećeg povezivanja sa tom oblašću, **Zaštitni zid** će prikazati dijalog kojim se od vas traži da joj dodelite profil.

Možete dodeliti profile svim lokalnim mrežnim interfejsima, a dodatne postavke možete podesiti u dijalogu **Profili za oblasti i mrežne kartice**, u kojem možete i onemogućiti ovu funkciju ako ne želite da je koristite (*u tom slučaju, podrazumevani profil ce se koristiti za sve veze*).

Ova funkcija je uglavnom korisna za korisnike prenosnog računara koji koriste različite tipove veza. Ako imate stacionarni računar, a koristite samo jedan tip veze (npr. *kablovsku*

vezu sa Internetom), ne morate da podešavate funkciju zamene profila jer vam verovatno nikada neće biti potrebna.

8.4.3. Interfejs zaštitnog zida



Interfejs komponente **Zaštitni zid** sadrži osnovne informacije o funkcijama komponente i kratak pregled statistike za **Zaštitni zid** :

- **Zaštitni zid je omogućen u trajanju od** - vremenski period od kako je Zaštitni zid poslednji put pokrenut
- **Blokirani paketi** - broj blokiranih paketa u odnosu na sve proverene pakete
- **Ukupan broj paketa** - broj svih proverenih paketa u toku rada komponente Zaštitni zid

Osnovna konfiguracija komponente

- **Izbor profila zaštitnog zida** - iz padajućeg menija izaberite jedan od definisanih profila - dva profila su uvek dostupna (*podrazumevani profili po imenu **Dozvoli sve** i **Blokiraj sve***), ostali profili su dodati ručno uređivanjem profila u dijalogu **Profili** u okviru stavke **Postavke zaštitnog zida**.

- **Omoguci režim za igre** – Izaberite ovu opciju da biste bili sigurni da se tokom prikazivanja sadržaja preko celog ekrana (igre, PowerPoint prezentacije itd.) neće pojavljivati dijalozi u kojima vas [zaštitni zid](#) pita da li želite da dozvolite ili blokirate komunikaciju sa nepoznatim aplikacijama. Ako za to vreme nepoznata aplikacija pokušava da komunicira preko mreže, [zaštitni zid](#) će automatski dozvoliti ili blokirati pokušaj na osnovu postavki trenutnog profila.
- **Status zaštitnog zida:**
 - **Zaštitni zid omogucen** – izaberite ovu opciju da biste omogucili komunikaciju aplikacijama koje su označene kao „dozvoljene“ u skupu pravila definisanih za izabrani profil [zaštitnog zida](#)
 - **Zaštitni zid onemogucen** – ova opcija potpuno isključuje [zaštitni zid](#), pa je sav mrežni saobraćaj dozvoljen, ali se ne proverava!
 - **Vanredni režim (blokira sav Internet saobraćaj)** - izaberite ovu opciju da biste blokirali sav saobraćaj na svim mrežnim portovima; [Zaštitni zid](#) je i dalje pokrenut, ali je sav mrežni saobraćaj obustavljen

Imajte u vidu sledeće: *Proizvođač softvera je podesio sve AVG komponente tako da se postignu optimalne performanse. Nemojte menjati AVG konfiguraciju ukoliko nemate dobar razlog za to. Postavke smeju da menjaju samo iskusni korisnici. Ako je potrebno da promenite konfiguraciju zaštitnog zida, iz sistemskog menija izaberite stavku **Alatke / Postavke zaštitnog zida**, pa u dijalogu [Postavke zaštitnog zida](#) uredite konfiguraciju zaštitnog zida.*

Kontrolna dugmad

- **[Carobnjak za konfiguraciju](#)** - kliknite na dugme da biste otvorili odgovarajući dijalog (koji se koristi tokom procesa instalacije) pod imenom **[Izbor nacina upotrebe racunara](#)** u kojem možete da podesite konfiguraciju komponente [Zaštitni zid](#)
- **Sacuvaj promene** - kliknite na ovo dugme da biste sacuvali i primenili promene koje ste napravili u ovom dijalogu
- **Otkazi**- kliknite na ovo dugme da biste se vratili u podrazumevani [AVG korisnicki interfejs](#) (*pregled komponenta*)

8.5. Skener e-pošte

E-pošta predstavlja jedan od najčešćih izvora virusa i trojanskih konja. Phishing i bezvredna pošta čine e-poštu još većim izvorom rizika. Besplatni nalozi za e-poštu češće dobijaju takve zlonamerne e-poruke (*pošto najčešće ne primenjuju tehnologiju za zaštitu od neželjene pošte*), a kućni korisnici u velikoj meri koriste takve naloge. Izloženost kućnih korisnika napadima preko e-pošte dodatno povećava pregledanje nepoznatih Web lokacija i unošenje ličnih podataka u obrasce na mreži (*kao što je e-adresa*). Preduzeca obično koriste korporativne naloge za e-poštu i primenjuju filtere za odbranu od bezvredne pošte kako bi se smanjio rizik.

8.5.1. Principi skeniranja e-pošte

Komponenta **Skener e-pošte** automatski skenira dolaznu/odlaznu e-poštu. Možete je koristiti sa klijentima e-pošte koji nemaju sopstvenu dodatnu komponentu za program AVG (*npr. Outlook Express, Mozilla, Incredimail, itd.*).

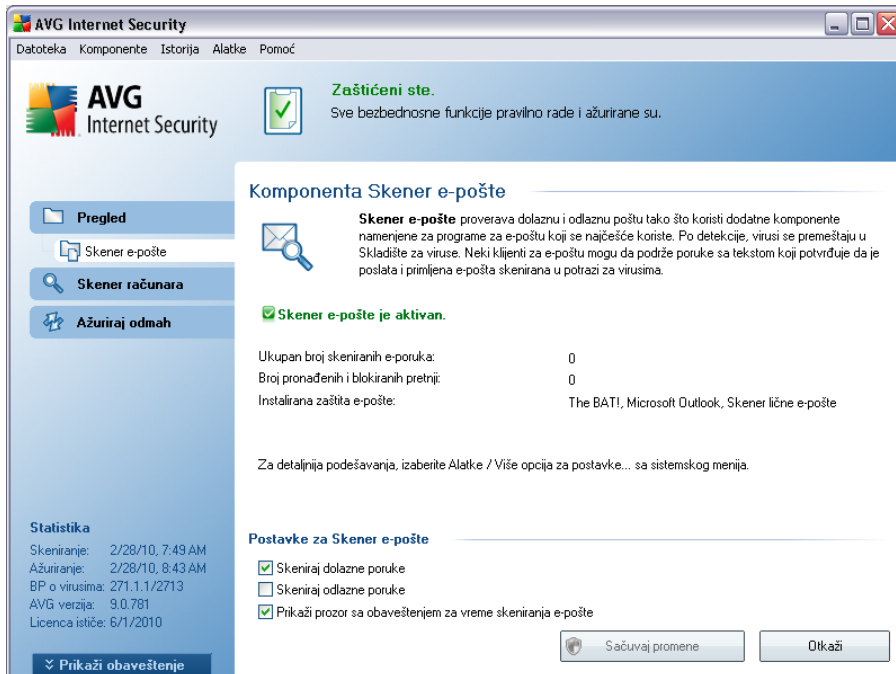
Tokom instalacije programa AVG [***](#) AVG kreiraju se automatski serveri za kontrolu e-pošte: jedan za proveravanje dolazne, a drugi za proveravanje odlazne e-pošte. Upotrebom ova dva servera e-pošta se automatski proverava na portovima 110 i 25 (*standardni portovi za slanje/primanje e-pošte*).

Skener e-pošte funkcioniše kao interfejs između klijenta e-pošte i servera e-pošte na Internetu.

- **Dolazna pošta:** kada primete e-poruke sa servera, komponenta **Skener e-pošte** ih testira na viruse, uklanja zaražene priloge i dodaje certifikate. Nakon detekcije, virusi se odmah smeštaju u [Skladište za viruse](#). Poruka se zatim prosleđuje do klijenta e-pošte.
- **Odlazna pošta:** poruka se šalje od klijenta e-pošte do skenera e-pošte; on proverava da li se u poruci i njenim priložima nalaze virusi, a zatim je šalje na SMTP server (*skeniranje odlazne pošte je podrazumevano onemogućeno i može se ručno podesiti*).

Napomena: AVG skener e-pošte nije predviđen za serverske platforme!

8.5.2. Interfejs komponente Skener e-pošte



U dijalogu komponente **Skener e-pošte** nalazi se kratak tekst koji opisuje funkcije ove komponente, informacije o njenom trenutnom statusu (*Skener e-pošte je aktivan.*), kao i sledeće statističke podatke:

- **Ukupan broj skeniranih e-poruka** - broj skeniranih e-poruka od poslednjeg pokretanja komponente **Skener e-pošte** (*ova vrednost se po potrebi može poništiti; npr. u statističke svrhe - Poništi vrednost*)
- **Broj pronadenih i blokiranih pretnji** - broj detektovanih slučajeva zaraze u e-porukama od poslednjeg pokretanja komponente **Skener e-pošte**
- **Instalirana zaštita e-pošte** - informacije o određenoj dodatnoj komponenti za zaštitu e-pošte koja se odnosi na vaš podrazumevani instalirani klijent za e-poštu.

Osnovna konfiguracija komponente

U donjem delu dijaloga nalazi se odeljak po imenu **Podešavanja skenera e-pošte** u kojem možete urediti neke od osnovnih funkcija ove komponente:

- **Skeniraj dolazne poruke** - izaberite ovu opciju ako želite da se sve e-poruke koje stižu na vaš nalog skeniraju kako bi se proverilo da li sadrže viruse. Ova opcija je podrazumevano uključena i ne preporučuje se da je menjate!
- **Skeniraj odlazne poruke** - izaberite ovu opciju ako želite da se sve e-poruke koje se šalju sa vašeg naloga skeniraju kako bi se proverilo da li sadrže viruse. Ova opcija je podrazumevano isključena.
- **Prikaži ikonu obaveštenja u toku skeniranja e-pošte** - izaberite ovu opciju ako želite da budete obaveštavani putem dijaloga za obaveštavanje koji se prikazuje iznad AVG ikone na sistemskoj paleti tokom skeniranja e-pošte pomoću komponente [Skener e-pošte](#). Ova opcija je podrazumevano uključena i ne preporučuje se da je menjate!

Napredna konfiguracija komponente **Skener e-pošte** dostupna je ako otvorite stavku sistemskog menija **Alatke/Napredna podešavanja**; međutim, napredno konfigurisanje trebalo bi da obavljaju samo iskusni korisnici!

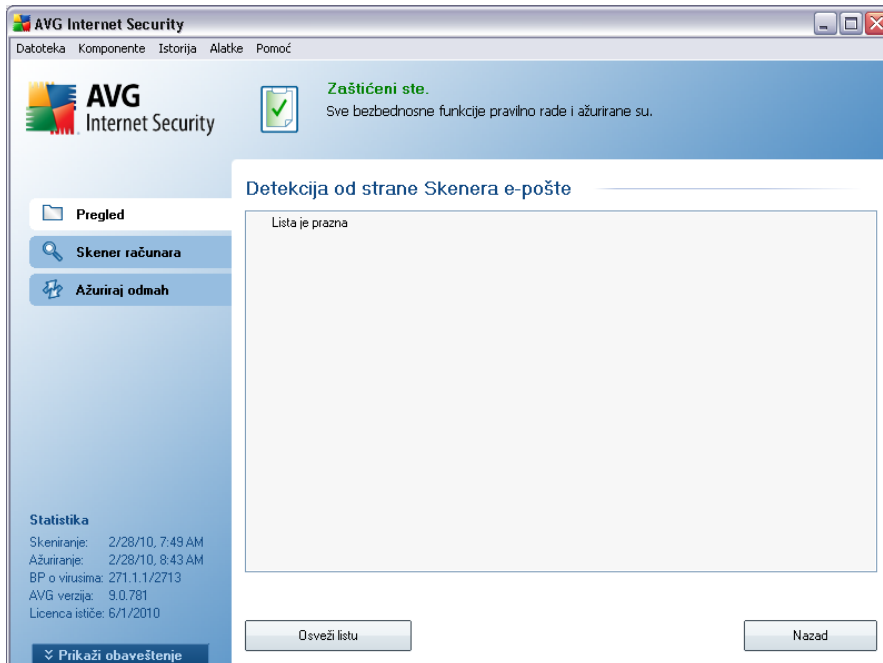
Imajte u vidu sledeće: *Proizvodac softvera je podesio sve AVG komponente tako da se postignu optimalne performanse. Nemojte menjati AVG konfiguraciju ukoliko nemate dobar razlog za to. Podešavanja smeju da menjaju samo iskusni korisnici. Ako je potrebno da promenite konfiguraciju programa AVG, u sistemskom meniju izaberite stavku **Alatke / Napredna podešavanja**, a zatim uredite AVG konfiguraciju u novootvorenom dijalogu [AVG napredna podešavanja](#).*

Kontrolna dugmad

U interfejsu komponente **Skener e-pošte** dostupna su sledeća kontrolna dugmad:

- **Sacuvaj promene** - kliknite na ovo dugme da biste sacuvali i primenili promene koje ste napravili u ovom dijalogu
- **Otkazi** - pritisnite ovo dugme za povratak na podrazumevani [AVG korisnicki interfejs](#) (pregled komponenata)

8.5.3. Detekcija od strane skenera e-pošte



U dijalogu **Detekcija od strane skenera e-pošte** (kojem možete pristupiti pomoću opcije iz sistemskog menija *Istorija / Detekcija od strane skenera e-pošte*) moći ćete da vidite listu svih pretnji koje je detektovala komponenta **Skener e-pošte**. Za svaki detektovan objekat, date su sledeće informacije:

- **Infekcija**- opis (a moguće i ime) otkrivenog objekta
- **Objekat** - lokacija objekta
- **Rezultat** - radnja obavljena nad detektovanim objektom
- **Vreme otkrivanja** - datum i vreme otkrivanja sumnjivog objekta
- **Tip objekta** - tip detektovanog objekta

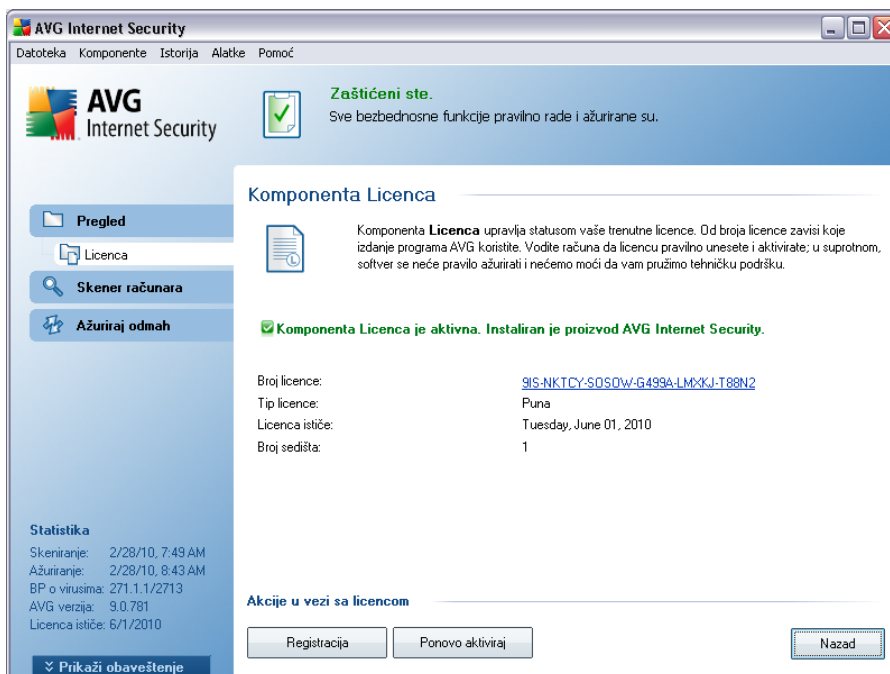
U donjem delu dijaloga, ispod liste, pronaci ćete informacije o ukupnom broju gore navedenih detektovanih objekata. Osim toga, možete izvesti celu listu detektovanih objekata u datoteku (**Izvezi listu u datoteku**) i izbrisati sve stavke o detektovanim objektima (**Isprazni listu**).

Kontrolna dugmad

U interfejsu za **detekciju od strane skenera e-pošte** dostupna su sledeca kontrolna dugmad:

- **Osveži listu** - ažuriranje liste otkrivenih pretnji
- **Nazad** - vraća vas nazad u podrazumevani [AVG korisnicki interfejs](#) (pregled komponenti)

8.6. Licenca



U interfejsu komponente **Licenca** nalazi se kratak tekst koji opisuje funkcije ove komponente, informacije o njenom trenutnom statusu (*Komponenta Licenca je aktivna.*), kao i sledece informacije:

- **Broj licence** - sadrži tačan oblik vašeg broja licence. Pri unošenju vašeg broja licence, morate biti potpuno precizni i uneti je kao što je prikazano. Zbog toga vam preporučujemo da pri svakom unošenju broja licence koristite metod „kopiraj i nalepi“.

- **Tip licence** - određuje tip instaliranog proizvoda.
- **Licenca istice** - ovaj datum određuje period važenja vaše licence. Ako želite da nastavite da koristite **AVG 9 Anti-Virus sa zaštitnim zidom** nakon tog datuma, morate obnoviti licencu. Obnavljanje licence [možete obaviti na mreži](http://www.avg.com/) na AVG Web lokaciji (<http://www.avg.com/>).
- **Broj sedišta** - broj radnih stanica na kojima imate pravo da instalirate **AVG 9 Anti-Virus sa zaštitnim zidom**.

Kontrolna dugmad

- **Registracija** - povezivanje sa stranicom za registraciju na AVG Web lokaciji (<http://www.avg.com/>). Unesite registracione podatke; besplatnu tehnicku podršku mogu dobiti samo korisnici koji registruju svoj AVG proizvod.
- **Ponovo aktiviraj** - otvaranje dijaloga **Aktivacija AVG programa** sa podacima koje ste uneli u dijalogu **Prilagodavanje programa AVG** u toku [procesa instalacije](#). U ovom dijalogu možete uneti svoj broj licence kako biste zamenili prodajni broj (*broj sa kojim ste instalirali AVG*) ili zamenili stari broj licence (*npr. prilikom nadogradnje na nov AVG proizvod*).

Napomena: Ako koristite probnu verziju programa **AVG 9 Anti-Virus sa zaštitnim zidom**, na dugmadima se prikazuje tekst **Kupite odmah i Aktivacija**, i ona vam omogućavaju da odmah kupite punu verziju programa. Ako je **AVG 9 Anti-Virus sa zaštitnim zidom** instaliran sa prodajnim brojem, na dugmadima se prikazuje tekst **Registracija i Aktivacija**.

- **Nazad** - pritisnite ovo dugme da biste se vratili u podrazumevani [AVG korisnicki interfejs](#) (pregled komponenti).

8.7. Skener linkova

8.7.1. Principi skeniranja linkova

Komponenta **Skener linkova** pruža zaštitu od Web lokacija koje su osmišljene tako da instaliraju malver na vaš racunar putem Web pregledaca ili njegovih dodatnih komponenti. Tehnologija **Skener linkova** sastoji se iz dve funkcije, [AVG štit za pretraživanje](#) i [AVG štit za aktivno pregledanje Interneta](#):

- [AVG štit za pretraživanje](#) sadrži listu Web lokacija (*URL adresa*) za koje se zna

da su opasne. Kada pretražujete koristeći Google, Yahoo!, Bing, Baidu, Altavista ili Yandex, svi rezultati pretrage se proveravaju u skladu sa ovom listom i prikazuje se ikona sa ocenom (za Yahoo! rezultate pretrage prikazuju se samo ikone sa ocenom „opasna Web lokacija“). Ako upišete neku adresu direktno u pregledac, kliknete na link na nekoj Web lokaciji ili u e-poruci, on se automatski proverava i blokira ako je to potrebno.

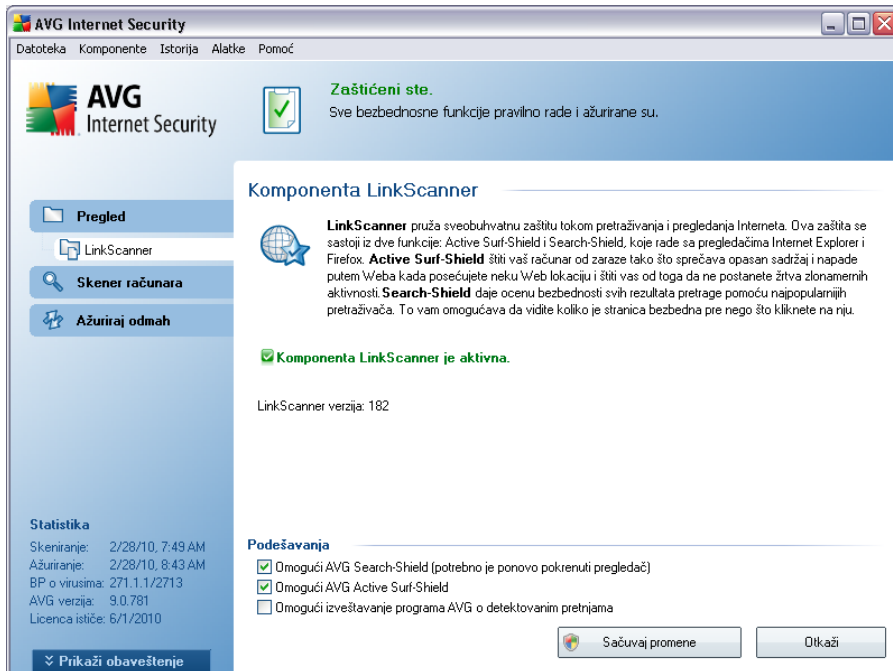
- **AVG štit za aktivno pregledanje Interneta** skenira sadržaj Web lokacija koje posećujete bez obzira na njihovu adresu. Čak i ako **AVG štit za pretraživanje** ne otkrije pojedine Web lokacije (npr. ako se kreira nova zlonamerna Web lokacija ili ako prethodno bezbedna Web lokacija sada sadrži malver), njih će otkriti i blokirati **AVG štit za aktivno pregledanje Interneta** kada pokušate da ih posetite.

Napomena: AVG skener linkova nije predviđen za serverske platforme!

8.7.2. Interfejs komponente Skener linkova

Komponenta **Skener linkova** sastoji se iz dva dela koja možete uključiti/isključiti u interfejsu **komponente Skener linkova** :

Interfejs komponente **Skener linkova** sadrži kratak opis funkcija komponente i informacije o njenom trenutnom statusu (Komponenta „Skener linkova“ je aktivna.). Osim toga, možete videti informacije o najnovijoj verziji baze podataka komponente **Skener linkova** (|Verzija komponente „Skener linkova“).








U donjem delu dijaloga možete urediti nekoliko opcija:

- **Omogući AVG štit za pretraživanje** - (*podrazumevano je uključeno*): ikone obaveštenja koje daju savete o rezultatima pretrage pomoću pretraživača Google, Yahoo!, Bing, Baidu, Yandex ili Altavista, nakon provere sadržaja Web lokacija koje je ponudio pretraživač.
- **Omogući AVG štit za aktivno pregledanje Interneta** - (*podrazumevano uključeno*): aktivna zaštita (*u realnom vremenu*) od zlonamernih Web lokacija u trenutku kada im se pristupa. Poznate zlonamerne Web lokacije i njihov opasan sadržaj se blokiraju dok im korisnik pristupa pomoću Web pregledaca (*ili neke druge aplikacije koja koristi HTTP*).
- **Omogući izveštavanje o otkrivenim pretnjama kompaniji AVG** - izaberite ovu opciju ako želite da omogućite izveštavanje o „exploit“ programima i opasnim Web lokacijama koje korisnik otkrije pomoću funkcije **Bezbedno pregledanje** ili **Bezbedna pretraga** kako biste dodali ove informacije u bazu podataka o zlonamernim aktivnostima na Internetu.

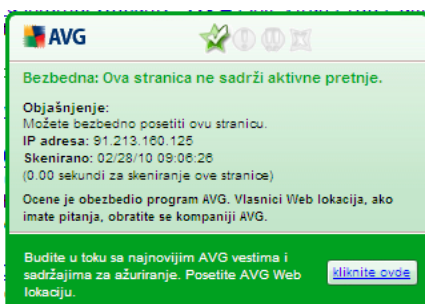
8.7.3. AVG štit za pretraživanje

Kada pretražujete Internet dok je funkcija **AVG štit za pretraživanje** uključena, svi rezultati pretrage pomoću najpopularnijih pretraživača, kao što su Yahoo!, Google, MSN itd. bice procenjeni kako bi se proverilo da li sadrže opasne ili sumnjive linkove. Nakon što proverite linkove i oznaci one opasne, **AVG skener linkova** vas upozorava pre nego što kliknete na opasan ili sumnjiv link, kako biste bili sigurni da ćete posjećivati isključivo bezbedne lokacije.

Dok se link proverava na stranici sa rezultatima pretrage, pored linka će se prikazivati ikona koja označava da je provera linka u toku. Po završetku procene, pojaviće se odgovarajuća informativna ikona:

-  Stranica na koju link upućuje je bezbedna (ako koristite Yahoo! pretragu preko [AVG bezbednosne trake sa alatkama](#) ova ikona se ne prikazuje!).
-  Stranica na koju link upućuje ne sadrži pretnje, ali je donekle sumnjiva (nesigurnog porekla ili motiva, zbog čega se ne preporučuje za kupovinu na mreži itd.).
-  Stranica na koju link upućuje je bezbedna, ali sadrži linkove ka stranicama koje su definitivno opasne, ili je njen kôd sumnjiv iako trenutno ne predstavlja pretnju.
-  Stranica na koju link upućuje sadrži aktivne pretnje! Radi vaše sopstvene bezbednosti, neće vam biti dozvoljeno da posetite ovu stranicu.
-  Stranica na koju link upućuje nije pristupacna, pa se ne može skenirati.

Ako postavite pokazivač iznad pojedinačnih ikona ocene, prikazaće se više informacija o tom linku. Informacije sadrže dodatne detalje o pretnji (ako ih ima), IP adresu linka i kada je stranicu skenirao program AVG:

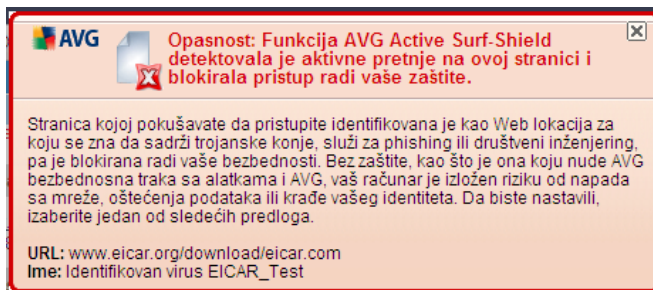


The screenshot shows a green-bordered notification box from AVG. At the top left is the AVG logo. To its right are four small icons: a green star, a yellow warning icon, a red X icon, and a question mark icon. The main text in the box reads: "Bezbedna: Ova stranica ne sadrži aktivne pretnje." Below this, it says "Objašnjenje:" followed by "Možete bezbedno posetiti ovu stranicu.", "IP adresa: 91.213.180.125", "Skenirano: 02/28/10 09:08:28 (0.00 sekundi za skeniranje ove stranice)", and "Ocene je obezbedio program AVG. Vlasnici Web lokacija, ako imate pitanja, obratite se kompaniji AVG." At the bottom left, there is a small text: "Budite u toku sa najnovijim AVG vestima i sadržajima za ažuriranje. Posetite AVG Web lokaciju." To the right of this text is a small blue button with the text "Kliknite ovde".

8.7.4. AVG štit za aktivno pregledanje Interneta

Ovaj snažan vid zaštite blokirace sve zlonamerne sadržaje na stranici koju pokušate da otvorite i sprecice njegovo preuzimanje na racunar. Ako je ova funkcija omogucena, a vi kliknete na link ili unesete URL adresu opasne lokacije, njeno otvaranje bice automatski blokirano kako biste bili zašticeni od slucajne zaraze. Važno je imati u vidu da je dovoljno da posetite opasnu Web lokaciju da bi došlo do zaraze racunara. Zato **AVG skener linkova** neće dozvoliti pregledacu da prikaže opasnu Web stranicu sa „exploit“ programima i drugim opasnim pretnjama kada pokušate da joj pristupite.

Ako naidete na zlonamernu Web lokaciju, **AVG Link Scanner** će prikazati ekran upozorenja u Web pregledacu nalik sledecem:



Ulazak na ovakvu Web lokaciju je veoma rizican i ne preporučuje se!

8.8. Online Shield

8.8.1. Princip rada komponente Online Shield

Online Shield predstavlja vrstu stalne zaštite u realnom vremenu; on skenira sadržaj Web stranica koje posećujete (i potencijalne datoteke koje se na njima nalaze) pre nego što se prikažu u vašem Web pregledacu ili preuzmu na vaš racunar.

Online Shield detektuje ako stranica koju želite da posetite sadrži opasan javascript i sprecava prikazivanje stranice. Takode, on prepoznaje malver koji se nalazi na stranici i odmah prekida njegovo preuzimanje kako ne bi dospeo na vaš racunar.

Napomena: AVG Online Shield nije namenjen za serverske platforme!

8.8.2. Interfejs komponente Online Shield

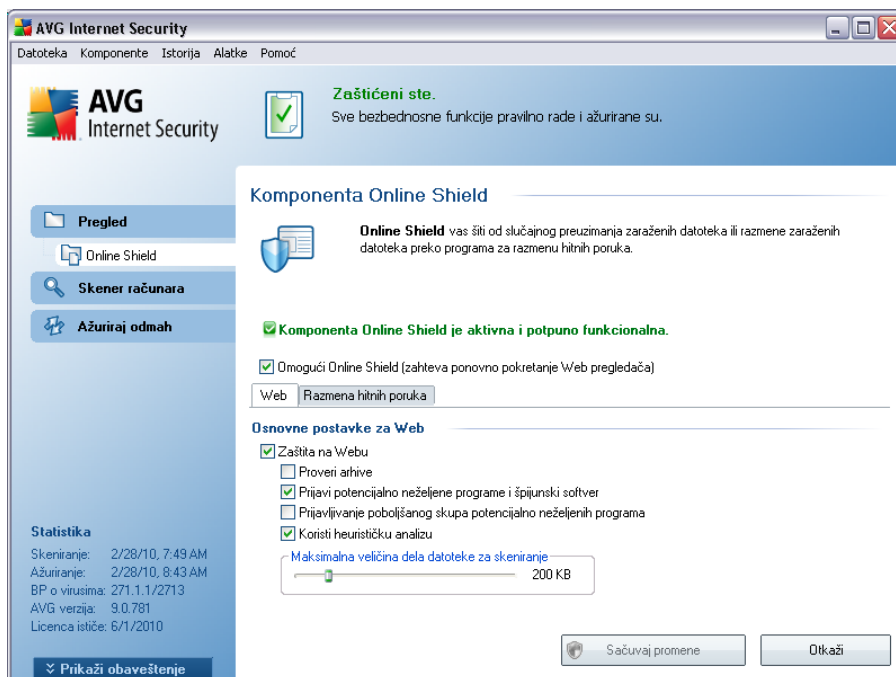
Interfejs komponente **Online Shield** opisuje ponašanje ove vrste zaštite. Tu se nalaze i informacije o trenutnom statusu ove komponente (*Online Shield je aktivan i potpuno funkcionalan.*). U donjem delu ekrana nalaze se osnovne opcije za uređivanje funkcija

ove komponente.

Osnovna konfiguracija komponente

Kao prvo, na raspolaganju vam je opcija da istog trenutka uključite/isključite komponentu **Online Shield** tako što ćete označiti stavku **Omogući Online Shield**. Ova opcija je podrazumevano omogućena, pa je i komponenta **Online Shield**. Osim ako nemate dobar razlog da menjate ove postavke, preporučujemo da ova komponenta ostane aktivna. Ako je ova stavka označena i ako je komponenta **Online Shield** pokrenuta, dostupno je još opcija za konfiguraciju koje se mogu uređivati na dve kartice:

- **Web** - možete uređivati konfiguraciju komponente u vezi sa skeniranjem sadržaja Web lokacija. Interfejs za uređivanje omogućava vam da konfigurirate sledeće osnovne opcije:

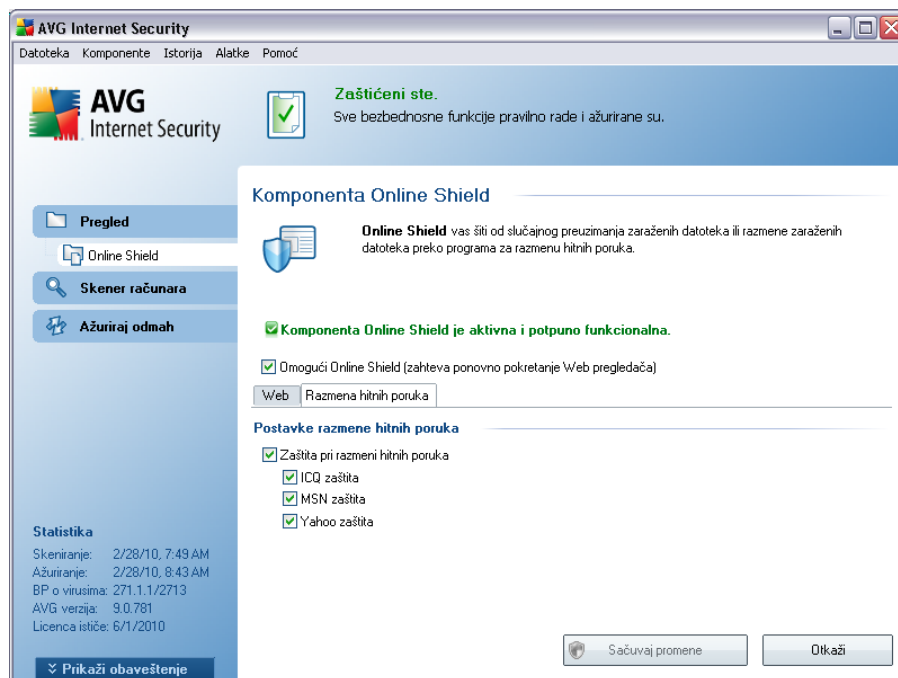


- **Zaštita na Webu** - ova opcija potvrđuje da **Online Shield** treba da obavlja skeniranje sadržaja www stranica. Ako je ova opcija uključena (podrazumevano), možete uključiti/isključiti sledeće stavke:

➤ **Proveri archive** - skeniranje sadržaja arhiva koje se potencijalno

nalaze na www stranici koja se prikazuje

- **Prijavi potencijalno neželjene programe i špijunski softver** - (*podrazumevano je uključeno*): potvrdite izbor u ovom polju za potvrdu da biste aktivirali **Antispajver** mehanizam i obavili skeniranje u potrazi za špijunskim programima i virusima. **Špijunski softver** se ne može sa sigurnošću svrstati u kategoriju malvera: Iako obično predstavlja bezbednosni rizik, neki od ovih programa mogu se bezbedno instalirati na računar. Preporučujemo vam da ova funkcija bude uključena jer povećava bezbednost računara
- **Prijavi poboljšani skup potencijalno neželjenih programa** – ako je prethodna opcija aktivirana, takođe možete da potvrdite izbor u ovom polju za potvrdu kako bi se detektovao poboljšani skup **špijunskih programa**: programi koji su potpuno bezbedni kada ih kupite od proizvođača, ali koji se kasnije mogu iskoristiti u zlonamerne svrhe. Ovo je dodatna mera kojom se bezbednost računara poboljšava još više. Međutim, zbog toga što postoji mogućnost blokiranja legalnih programa, ova opcija je podrazumevano isključena.
- **Koristi heuristicku analizu** - skeniranje sadržaja stranice koja se prikazuje pomoću metoda heurističke analize, tj. simulacija i procena instrukcija skeniranog objekta u virtualnom računarskom okruženju. Zbog toga se ovom analizom može otkriti zlonamerni kôd koji još uvek nije opisan u bazi podataka o virusima (*pogledajte odeljak [Principi zaštite od virusa](#)*).
- **Maksimalna velicina datoteke za skeniranje** - ako se na prikazanoj stranici nalaze datoteke, možete skenirati njihov sadržaj pre nego što se preuzmu na vaš računar. Međutim, skeniranje velikih datoteka može potrajati i, samim tim, znatno usporiti učitavanje Web stranice. Možete da koristite klizac da biste naveli maksimalnu veličinu datoteke za skeniranje komponentom **Online Shield**. Čak i u slučaju da je preuzeta datoteka veća nego što je predviđeno, pa je **Online Shield** neće skenirati, ipak ćete biti zaštićeni: ako je datoteka zaražena, **Stalni štit** će je odmah detektovati.
- **Razmena hitnih poruka** - omogućava uređivanje postavki komponente koje se tiku skeniranja razmene hitnih poruka (*npr. ICQ, MSN Messenger, Yahoo ...*).



- Zaštita pri razmeni hitnih poruka - označite ovu stavku ako želite da Online Shield proverava da li komunikacija na mreži sadrži viruse. Ako je ova opcija uključena, možete definisati koju aplikaciju za razmenu trenutnih poruka želite da pratite - trenutno **AVG 9 Anti-Virus sa zaštitnim zidom**su podržane aplikacije ICQ, MSN i Yahoo.

Napomena: proizvođač softvera je podesio sve AVG komponente tako da se postignu optimalne performanse. Nemojte menjati AVG konfiguraciju ukoliko nemate dobar razlog za to. Podešavanja smeju da menjaju samo iskusni korisnici. Ako je potrebno da promenite konfiguraciju programa AVG, u sistemskom meniju izaberite stavku **Alatke / Napredna podešavanja**, a zatim uredite AVG konfiguraciju u novootvorenom dijalogu [AVG napredna podešavanja](#).

Kontrolna dugmad

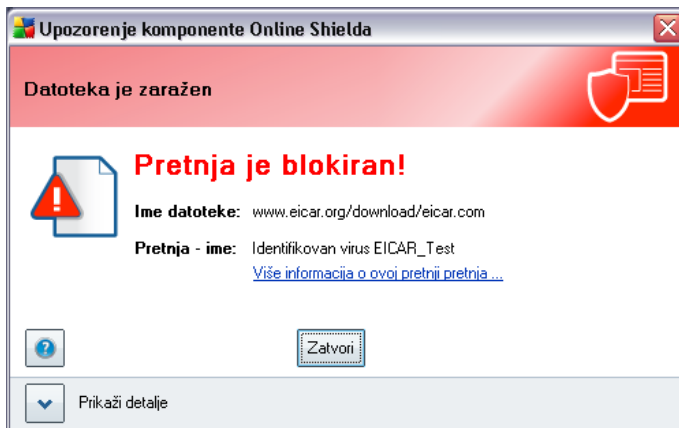
U interfejsu komponente **Online Shield** dostupna su sledeća kontrolna dugmad:

- **Sacuvaj promene** - kliknite na ovo dugme da biste sacuvali i primenili promene koje ste napravili u ovom dijalogu
- **Otkazi**- kliknite na ovo dugme da biste se vratili u podrazumevani [AVG](#)

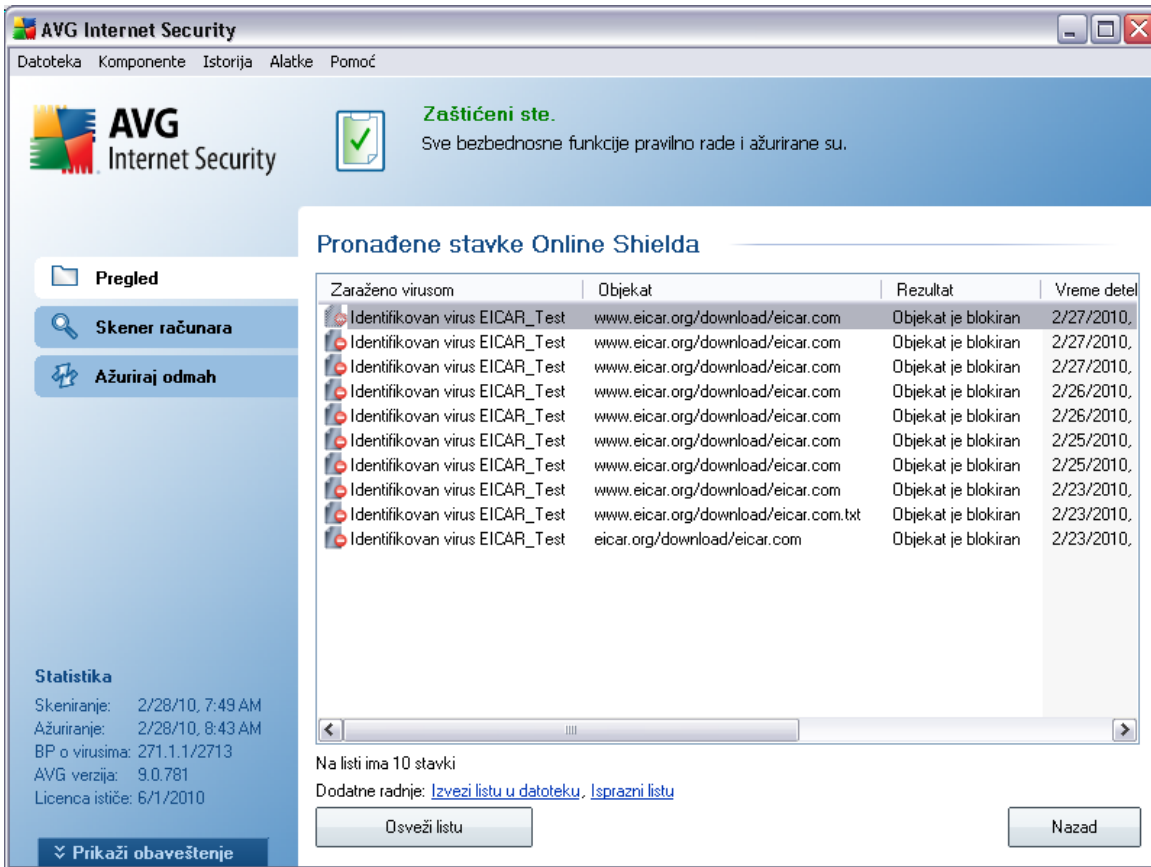
[korisnicki interfejs](#) (pregled komponenta)

8.8.3. Detekcija komponente Online Shield

Online Shield skenira sadržaj Web stranica koje posećujete i potencijalne datoteke koje se na njima nalaze pre nego što se prikažu u vašem Web pregledacu ili preuzmu na vaš racunar. Ako se detektuje pretnja, o tome cete odmah biti obavješteni sledecim dijalogom:



Sumnjiva Web stranica neće biti otvorena, a otkrivena pretnja biće evidentirana na listi **Detekcije komponente Online Shield** - ovom pregledu otkrivenih pretnji možete da pristupite putem sistemskog menija [Istorija / Detekcije komponente Online Shield](#).



AVG Internet Security

Datoteka Komponente Istorija Alatke Pomoć

Zaštićeni ste.
Sve bezbednosne funkcije pravilno rade i ažurirane su.

Pronađene stavke Online Shielda

Zaraženo virusom	Objekat	Rezultat	Vreme detek
Identifikovan virus EICAR_Test	www.eicar.org/download/eicar.com	Objekat je blokiran	2/27/2010,
Identifikovan virus EICAR_Test	www.eicar.org/download/eicar.com	Objekat je blokiran	2/27/2010,
Identifikovan virus EICAR_Test	www.eicar.org/download/eicar.com	Objekat je blokiran	2/27/2010,
Identifikovan virus EICAR_Test	www.eicar.org/download/eicar.com	Objekat je blokiran	2/26/2010,
Identifikovan virus EICAR_Test	www.eicar.org/download/eicar.com	Objekat je blokiran	2/26/2010,
Identifikovan virus EICAR_Test	www.eicar.org/download/eicar.com	Objekat je blokiran	2/25/2010,
Identifikovan virus EICAR_Test	www.eicar.org/download/eicar.com	Objekat je blokiran	2/25/2010,
Identifikovan virus EICAR_Test	www.eicar.org/download/eicar.com	Objekat je blokiran	2/23/2010,
Identifikovan virus EICAR_Test	www.eicar.org/download/eicar.com.txt	Objekat je blokiran	2/23/2010,
Identifikovan virus EICAR_Test	eicar.org/download/eicar.com	Objekat je blokiran	2/23/2010,

Na listi ima 10 stavki
 Dodatne radnje: [Izvezi listu u datoteku.](#) [Isprazni listu](#)

Osveži listu Nazad

Statistika
 Skeniranje: 2/28/10, 7:49 AM
 Ažuriranje: 2/28/10, 8:43 AM
 BP o virusima: 271.1.1/2713
 AVG verzija: 9.0.781
 Licenca ističe: 6/1/2010

▼ Prikaži obaveštenje

Za svaki detektovan objekat, date su sledece informacije:

- **Infekcija**- opis (*a moguće i ime*) otkrivenog objekta
- **Objekat** - izvor objekta (*Web stranica*)
- **Rezultat** - radnja obavljena nad detektovanim objektom
- **Vreme otkrivanja** - datum i vreme otkrivanja i blokiranja pretnje
- **Tip objekta** - tip detektovanog objekta
- **Proces** - radnja koja je obavljena da bi potencijalno opasan objekat mogao da se detektuje

U donjem delu dijaloga, ispod liste, pronaci ćete informacije o ukupnom broju gore navedenih detektovanih objekata. Osim toga, možete izvesti celu listu detektovanih

objekata u datoteku (***Izvezi listu u datoteku***) i izbrisati sve stavke o detektovanim objektima (***Isprazni listu***). Dugme ***Osveži listu*** će ažurirati listu pretnji koje je pronašao ***Online Shield***. Dugme ***Nazad*** vratice vas u podrazumevani ***AVG korisnicki interfejs*** (pregled komponentata).

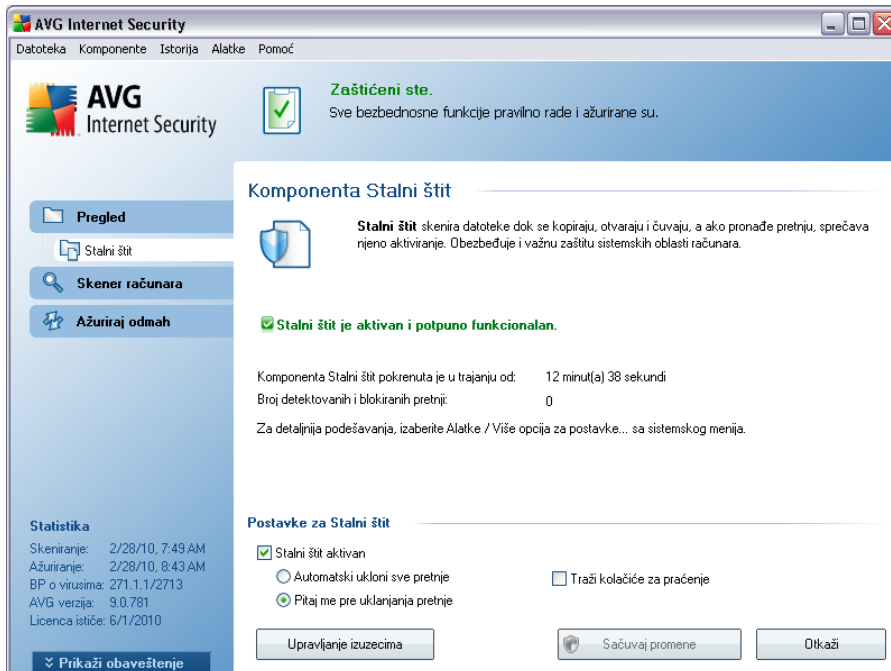
8.9. Stalni štiti

8.9.1. Stalni štiti Principi

Komponenta ***Stalni štiti*** obezbeđuje neprekidnu zaštitu računara. Ona skenira svaku datoteku koju otvarate, čuvate ili kopirate i štiti sistemske oblasti računara. Kada ***Stalni štiti*** otkrije virus u datoteci kojoj se pristupa, on zaustavlja operaciju koja se u tom trenutku izvršava i ne dozvoljava da se virus aktivira. U normalnim okolnostima, ovaj proces se obavlja neprimetno jer se odvija „u pozadini“ i bicete obavješteni samo kada se otkriju pretnje; ***Stalni štiti*** istovremeno sprečava aktiviranje pretnje i uklanja je. ***Stalni štiti*** se učitava u memoriju računara tokom pokretanja sistema.

Upozorenje: stalni štiti se učitava u memoriju računara tokom pokretanja sistema i izuzetno je važno da uvek bude uključen!

8.9.2. Interfejs komponente Stalni štiti



Pored pregleda najvažnijih statističkih podataka i informacija o trenutnom statusu komponente (*Stalni štít je aktivan i potpuno funkcionalan*), interfejs komponente **Stalni štít** sadrži i osnovne opcije za njeno podešavanje. Statistički podaci su sledeci:

- **Stalni štít je aktivan** - vremenski period od kako je ova komponenta poslednji put pokrenuta
- **Detektovane i blokirane pretnje** - broj detektovanih infekcija cije pokretanje/otvaranje je sprečeno (*ova vrednost se po potrebi može poništiti; npr. u statističke svrhe - Poništi vrednost*)

Osnovna konfiguracija komponente

U donjem delu dijaloga nalazi se odeljak **Stalni štít - postavke** u kojem možete urediti osnovne postavke komponente (*detaljnije konfigurisanje, kao i kod ostalih komponenata, dostupno je ako otvorite stavku Alatke/Napredna podešavanja iz sistemskog menija*).

Opcija **Stalni štít je aktivan** omogućava vam da jednostavno uključite/isključite stalnu zaštitu. Ova funkcija je podrazumevano uključena. Ako je stalna zaštita uključena, možete odluciti kako će se postupati sa eventualnim detektovanim zarazama (nacin uklanjanja):

- automatski (**Automatski ukloni sve pretnje**)
- ili tek nakon dozvole korisnika (**Pitaj me pre uklanjanja pretnje**)

Ovaj izbor ne utice na nivo bezbednosti, vec samo zavisi od vaših želja.

U oba slucaja, možete da izaberete da li želite da uključite opciju **Traži kolacice za pracenje**. U određenim slucajevima, možete uključiti ovu opciju da biste postigli najviši nivo bezbednosti, ali je ona podrazumevano isključena. (*kolacici = paketi teksta koje server šalje Web pregledacu, a zatim mu ih pregledac nepromenjene šalje pri svakom sledecem pristupanju serveru. HTTP kolacici služe za proveru identiteta, pracenje i održavanje određenih informacija o korisnicima, kao što su željene opcije za lokaciju ili sadržaj elektronskih kolica za kupovinu*).

Napomena: proizvođač softvera je podesio sve AVG komponente tako da se postignu optimalne performanse. Nemojte menjati AVG konfiguraciju ukoliko nemate dobar razlog za to. Podešavanja smeju da menjaju samo iskusni korisnici. Ako je potrebno da promenite konfiguraciju programa AVG, u sistemskom meniju izaberite stavku **Alatke / Napredna podešavanja**, a zatim uredite AVG konfiguraciju u novootvorenom dijalogu [AVG napredna podešavanja](#).

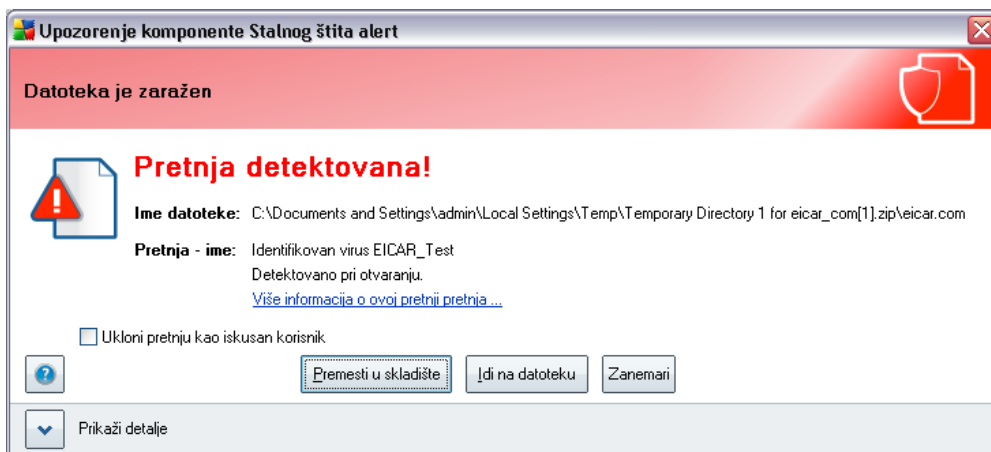
Kontrolna dugmad

U interfejsu komponente **Stalni štiti** dostupna su sledeca kontrolna dugmad:

- **Upravljanje izuzecima** - otvaranje dijaloga [Stalni štiti - izuzimanje direktorijuma](#) u kojem možete definisati koje ce fascikle biti izuzete iz skeniranja pomocu komponente [Stalni štiti](#)
- **Sacuvaj promene** - kliknite na ovo dugme da biste sacuvali i primenili promene koje ste napravili u ovom dijalogu
- **Otkazi** - pritisnite ovu dugme za povratak na podrazumevani [AVG korisnicki interfejs](#) (pregled komponenata)

8.9.3. Detekcija od strane Stalnog štita

Stalni štiti skenira datoteke prilikom njihovog kopiranja, otvaranja ili cuvanja. Kad bude detektovan virus ili bilo kakva pretnja, o tome ce vas odmah upozoriti sledeci dijalog.



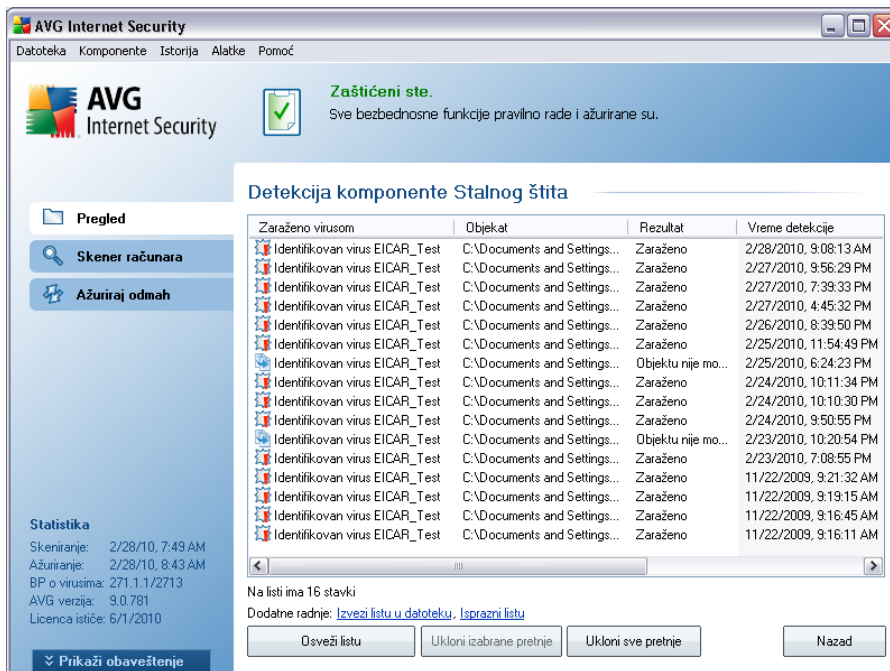
Dijalog sadrži informacije o detektovanoj pretnji i traži od vas da odlucite koja ce se radnja preduzeti:

- **Izleci** - ako je lecenje moguće, AVG ce automatski izleciti zaraženu datoteku; ova opcija se preporucuje
- **Premesti u Skladište** - virus ce biti premešten u AVG [Skladište za viruse](#)
- **Idi do datoteke** - ova opcija vas preusmerava do tacne lokacije sumnjivog objekta (

otvara novi prozor programa Windows Explorer)

- **Zanemari** - savetujemo vam da NE koristite ovu opciju ako za to nemate dobar razlog!

Celokupan pregled pretnji koje je otkrio **Stalni štit** možete videti u dijalogu **Detekcija od strane stalnog štita**, kojem možete pristupiti iz sistemskog menija izborom opcije **Istorija / Pronadene stavke komponente „Stalni štit“**:



Detekcija od strane stalnog štita sadrži pregled objekata koje je detektovala komponenta **Stalni štit**, ocenila ih kao opasne i izlucila ili premestila u fasciklu **Skladište za viruse**. Za svaki detektovan objekat, date su sledece informacije:

- **Infekcija** - opis (a moguće i ime) otkrivenog objekta
- **Objekat** - lokacija objekta
- **Rezultat** - radnja obavljena nad detektovanim objektom
- **Vreme otkrivanja** - datum i vreme otkrivanja objekta
- **Tip objekta** - tip detektovanog objekta

- **Proces** - radnja koja je obavljena da bi potencijalno opasan objekat mogao da se detektuje

U donjem delu dijaloga, ispod liste, pronaci cete informacije o ukupnom broju gore navedenih detektovanih objekata. Osim toga, možete izvesti celu listu detektovanih objekata u datoteku (***Izvezi listu u datoteku***) i izbrisati sve stavke o detektovanim objektima (***Isprazni listu***). Dugme ***Osveži listu*** ažurirace listu pretnji koje je pronašao ***Stalni štit***. Dugme ***Nazad*** vratice vas u podrazumevani ***AVG korisnicki interfejs*** (pregled komponenata).

8.10. Upravljanje ažuriranjem

8.10.1. Principi upravljanja ažuriranjem

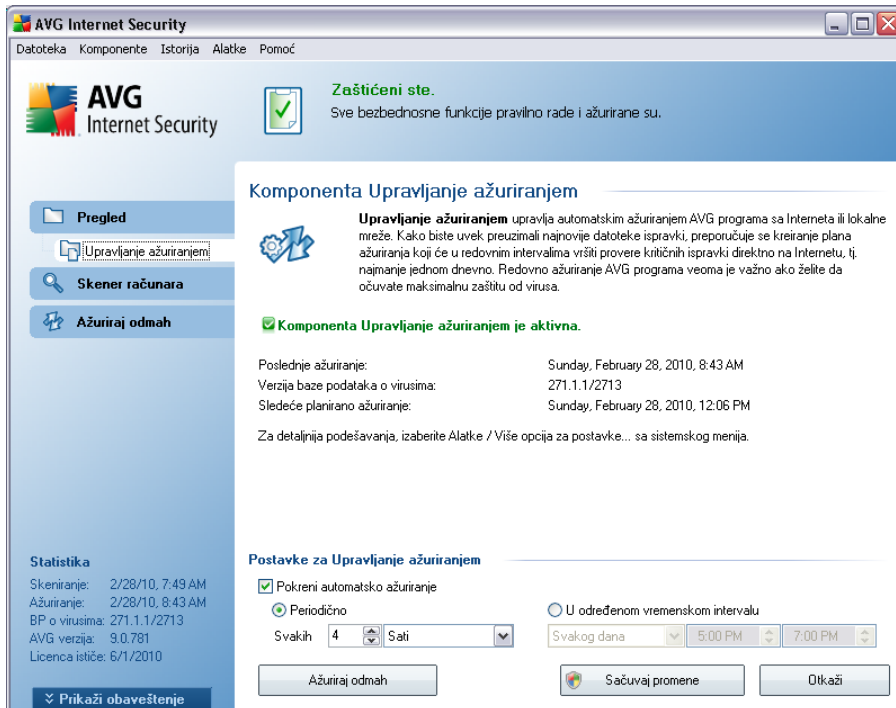
Nijedan bezbednosni softver ne može garantovati pouzdanu zaštitu od raznih vrsta pretnji ako se redovno ne ažurira! Kreatori virusa stalno traže nove propuste u softveru i operativnim sistemima koje mogu da iskoriste. Svakodnevno se pojavljuju novi virusi, nov malver, novi napadi sa mreže. Zato proizvođači softvera redovno izdaju sadržaje za ažuriranje i bezbednosne zakrpe za ispravljanje otkrivenih propusta u bezbednosti.

Od ključnog je značaja da redovno ažurirate program AVG!

Komponenta ***Upravljanje ažuriranjem*** pomaže vam da upravljate redovnim ažuriranjem. U okviru ove komponente, možete zakazati automatsko preuzimanje datoteka za ažuriranje sa Interneta ili lokalne mreže. Ažuriranje osnovnih definicija virusa trebalo bi da se obavlja svakodnevno, ako je moguće. Manje hitno ažuriranje programa može se obavljati jednom nedeljno.

Napomena: Obratite pažnju na poglavlje [Ažuriranje programa AVG](#) za više informacija o vrstama i nivoima ažuriranja!

8.10.2. Interfejs komponente Upravljanje ažuriranjem



Interfejs komponente **Upravljanje ažuriranjem** prikazuje informacije o funkcionalnosti komponente i o njenom trenutnom statusu (*Upravljanje ažuriranjem je aktivno.*), a obezbeđuje i odgovarajuće statističke podatke:

- **Najnovija ispravka** - navodi datum i vreme poslednjeg ažuriranja baze podataka
- **Verzija baze podataka virusa** - definiše broj najnovije baze podataka virusa; taj broj se uvecava nakon svakog ažuriranja baze podataka virusa
- **Sledeće planirano ažuriranje** - oznacava datum i vreme ponovnog ažuriranja baze podataka

Osnovna konfiguracija komponente

U donjem delu dijaloga pronaci cete odeljak **Postavke upravljanja ažuriranjem** gde možete praviti promene pravila za pokretanje ažuriranja. Možete definisati da li želite da se datoteke za ažuriranje automatski preuzimaju (**Automatski zapocni ažuriranje**)

ili samo na zahtev. Opcija **Automatski zapocni ažuriranje** podrazumevano je uključena i preporučuje se da to ne menjate! Redovno preuzimanje datoteka za ažuriranje ključno je za ispravan rad bilo kojeg bezbednosnog softvera!

Takode možete definisati vreme pokretanja ažuriranja:

- **Periodicno** - definišite vremenski interval
- **U određeno vreme** - definišite tačan dan i vreme

Podrazumevano je da se ažuriranje obavlja svaka četiri sata. Preporučuje se da ne menjate ovo podešavanje ukoliko nemate ozbiljan razlog za to!

Napomena: *proizvodac softvera je podesio sve AVG komponente tako da se postignu optimalne performanse. Nemojte menjati AVG konfiguraciju ukoliko nemate dobar razlog za to. Podešavanja smeju da menjaju samo iskusni korisnici. Ako je potrebno da promenite konfiguraciju programa AVG, u sistemskom meniju izaberite stavku **Alatke / Napredna podešavanja**, a zatim uredite AVG konfiguraciju u novootvorenom dijalogu [AVG napredna podešavanja](#).*

Kontrolna dugmad

U interfejsu komponente **Upravljanje ažuriranjem** dostupna su sledeća kontrolna dugmad:

- **Ažuriraj odmah** - pokrece [trenutno ažuriranje](#) na zahtev
- **Sacuvaj promene** - kliknite na ovo dugme da biste sacuvali i primenili promene koje ste napravili u ovom dijalogu
- **Otkazi** - pritisnite ovu dugme za povratak na podrazumevani [AVG korisnicki interfejs](#) (pregled komponentata)

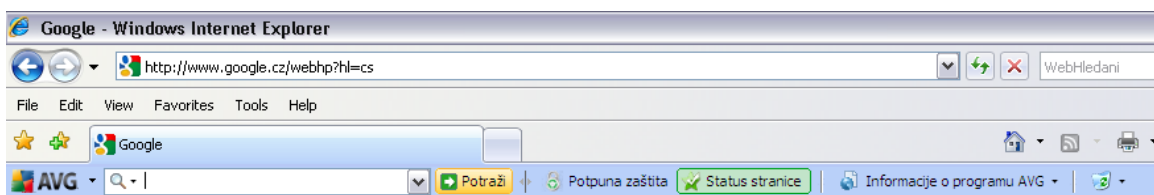
9. AVG bezbednosna traka sa alatkama

AVG bezbednosna traka sa alatkama je nova alatka koja radi zajedno sa komponentom **AVG skener linkova** i proverava rezultate pretrage podržanih Internet pretraživaca (*Yahoo!*, *Google*, *MSN*, *Baidu*). **AVG bezbednosna traka sa alatkama** se može koristiti za kontrolu funkcija komponente **AVG skener linkova** i za podešavanje njenog ponašanja.

Ako odlucite da instalirate traku sa alatkama tokom instalacije programa **AVG 9 Anti-Virus sa zaštitnim zidom**, ona ce biti automatski dodata u vaš Web pregledac. Ako koristite neki alternativni pregledac Interneta (*npr. Avant Browser*), može doci do neocekivanog ponašanja.

9.1. Interfejs AVG bezbednosne trake sa alatkama

AVG bezbednosna traka sa alatkama je osmišljena tako da radi sa programima **MS Internet Explorer** (verzija 6.0 ili novija) i **Mozilla Firefox** (verzija 2.0 ili novija). Kada odlucite da instalirate **AVG bezbednosnu traku sa alatkama** (tokom [procesa instalacije programa AVG](#) od vas se tražilo da odlucite da li želite ili ne želite da instalirate komponentu), komponenta ce se nalaziti u vašem Web pregledacu odmah ispod trake za adresu:



Napomena: AVG bezbednosna traka sa alatkama nije predvidena za serverske platforme!

AVG bezbednosna traka sa alatkama sastoji se od sledecih elemenata:

- **AVG logotip** - pruža pristup opštim stavkama na traci sa alatkama. Kliknite na dugme sa logotipom da biste bili preusmereni na AVG Web lokaciju (<http://www.avg.com/>). Ako kliknete na pokazivac pored AVG ikone, otvorice se sledece:
 - **Informacije o traci sa alatkama** - link ka maticnoj stranici **AVG bezbednosne trake sa alatkama koja sadrži detaljne informacije o zaštiti koju pruža traka sa alatkama**
 - **Pokreni AVG 9 Anti-Virus sa zaštitnim zidom** - otvara korisnicki

interfejs programa **AVG 9 Anti-Virus sa zaštitnim zidom**

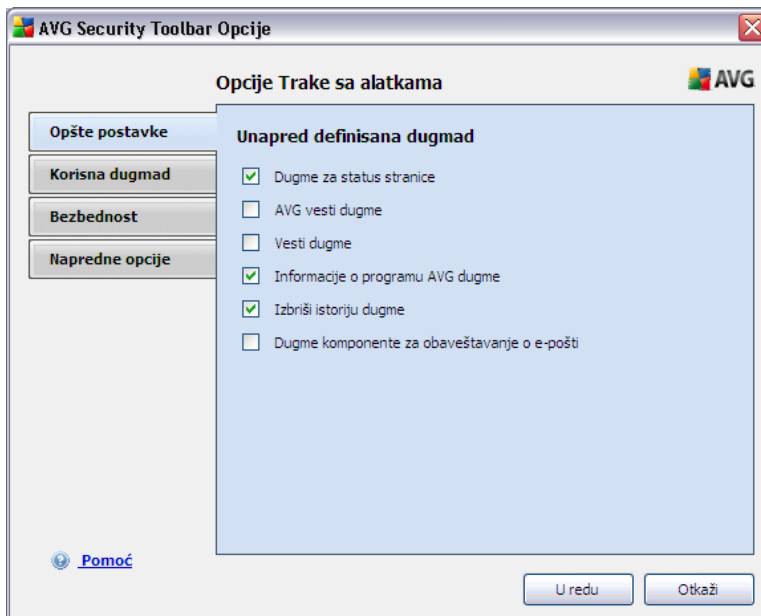
- **Opcije** - otvaranje dijaloga za konfigurisanje u kojem možete da prilagodite postavke **AVG bezbednosne trake sa alatkama** kako bi ona odgovarala vašim potrebama - pogledajte sledece poglavlje [**Opcije AVG bezbednosne trake sa alatkama**](#)
- **Izbriši istoriju** - omogućava vam da *izbrišete celu istoriju AVG bezbednosne trake sa alatkama* ili da *izbrišete istoriju pretrage, istoriju pregledaca, istoriju preuzimanja* i da *izbrišete kolacice*.
- **Ažuriranje** - proveravanje da li postoje novi sadržaji za ažuriranje **AVG bezbednosne trake sa alatkama**
- **Pomoc** - nudi opcije za otvaranje datoteke pomoci, slanje povratnih informacija o proizvodu ili prikazivanje detalja o trenutnoj verziji trake sa alatkama
- **Polje za pretragu** - Upišite rec ili frazu u polje za pretragu. Kliknite na dugme **Pretraži** da biste zapoceli pretragu pomocu izabranog pretraživaca (*željeni pretraživac možete da izaberete u okviru [naprednih podešavanja AVG bezbednosne trake sa alatkama](#) i možete da izaberete Yahoo!, Wikipedia, Baidu, WebHledani ili Yandex*), bez obzira na stranicu koja se trenutno prikazuje. U polju za pretragu prikazuje se i vaša istorija pretraživanja. Pretraživanje pomocu polja za pretragu analizira komponenta [**AVG štit za pretraživanje**](#).
- **Potpuna zaštita** - ovo dugme se pojavljuje opcionalno sa nekim od sledecih natpisa: **Potpuna zaštita / Ogranicena zaštita / Bez zaštite**, u zavisnosti od **AVG 9 Anti-Virus sa zaštitnim zidom** konfiguracije
- **Status stranice** - kada kliknete na ovo dugme, na traci sa alatkama se prikazuje procena trenutno otpremljene Web stranice na osnovu kriterijuma komponente [**AVG štit za pretraživanje**](#) (*stranica može biti bezbedna / sumnjiva / opasna / može sadržati pretnje / nije moguće skenirati stranicu*). Kliknite na ovo dugme da biste otvorili informativni prozor u kojem se nalaze detaljni podaci o određenoj Web stranici.
- **AVG informacije** - sadrži linkove ka najvažnijim bezbednosnim informacijama na Web lokaciji kompanije AVG (<http://www.avg.com/>).
- **Informacije o traci sa alatkama** - link ka matičnoj stranici **AVG bezbednosne trake sa alatkama koja sadrži detaljne informacije o zaštiti koju pruža traka sa alatkama**

- **Više informacija o pretnjama** - otvaranje Web stranice kompanije AVG na kojoj se nalaze informacije o aktuelnim virusima i pretnjama sa Interneta
- **AVG vesti** – otvaranje Web stranice na kojoj se nalaze najnovija saopštenja za štampu u vezi sa programom AVG
- **Trenutni nivo pretnje** – otvaranje Web stranice laboratorije virusa sa grafickim prikazom trenutnog nivoa pretnje na Webu
- **Enciklopedija virusa** – otvaranje stranice enciklopedije virusa na kojoj možete da potražite određene viruse po imenu i dobijete detaljne informacije o svakom od njih

9.2. Opcije AVG bezbednosne trake sa alatkama

Svim parametrima za podešavanje **AVG bezbednosne trake sa alatkama** možete da pristupite direktno iz okna **AVG bezbednosne trake sa alatkama**. Interfejs za uređivanje se otvara putem menija **AVG / Opcije** na traci sa alatkama kao novi dijalog **Opcije trake sa alatkama** koji je podeljen na cetiri dela:

9.2.1. Kartica „Opšte“



Na ovoj kartici možete da odredite koja ce se kontrolna dugmad trake sa alatkama

prikazivati ili ne na **AVG bezbednosnoj traci sa alatkama** . Izaberite odgovarajucu opciju ako želite da prikažete neko dugme. U nastavku je naveden opis funkcije svakog dugmeta na traci sa alatkama:

- Δυγμα **AVG vesti** - ovo dugme otvara Web stranicu na kojoj se nalaze najnovija sopštenja za štampu u vezi sa programom AVG
- Δυγμα **Vesti** - kada kliknete na ovo dugme, prikazuje se strukturalni pregled aktuelnih vesti iz dnevne štampe
- Δυγμα **AVG informacije** - ovo dugme pruža informacije o AVG traci sa alatkama, aktuelnim pretnjama i nivoima pretnji sa Interneta, otvara enciklopediju virusa i obezbeđuje vesti o drugim AVG proizvodima
- **Dugme „Izbriši istoriju“** - ovo dugme vam omogućava da izbrišete celu istoriju, ili da izbrišete istoriju pretrage, istoriju pregledaca, istoriju preuzimanjaili da izbrišete kolacice direktno iz okna AVG bezbednosne trake sa alatkama.

9.2.2. Kartica „Korisna dugmad“








Kartica **Korisna dugmad** vam omogućava da sa liste izaberete aplikacije i da njihove ikone prikažete u interfejsu trake sa alatkama. Ikona služi kao brzi link i omogućava vam da odmah pokrenete odgovarajucu aplikaciju.

9.2.3. Kartica „Bezbednost“



Kartica **Bezbednost** podeljena je na dva dela, **AVG bezbednost pregledaca** i **Ocene**, i omogućava vam da potvrdite izbor u odgovarajucim poljima za potvrdu kako biste **AVG bezbednosnoj traci sa alatka** dodelili željenu funkciju:

- **AVG bezbednost pregledaca** - izaberite ovu opciju kako biste aktivirali ili isključili **AVG štit za pretraživanje** i/ili uslugu **AVG štit za aktivno pregledanje Interneta**
- **Ocene** - izaberite željene graficke simbole koje ce za ocenjivanje rezultata pretrage koristiti komponenta **AVG štit za pretraživanje**
 -  stranica je bezbedna
 -  stranica je donekle sumnjiva
 -  stranica sadrži linkove ka stranicama koje su sigurno opasne
 -  stranica sadrži aktivne pretnje
 -  stranici se ne može pristupiti i zato se ne može skenirati

Oznacite odgovarajuću opciju kako biste potvrdili da želite da budete obavješćavani o ovom određenom nivou pretnje. Međutim, prikazivanje crvenog znaka na stranicama koje sadrže aktivne i opasne pretnje nije moguće isključiti. **Preporučuje se da ne menjate podrazumevanu konfiguraciju koju je podesio prodavac programa osim ako nemate dobar razlog za to.**

9.2.4. Kartica „Napredne opcije“



Na kartici **Napredne opcije** najpre izaberite pretraživač koji želite da se podrazumevano koristi. Možete da izaberete *Yahoo!*, *Baidu*, *WebHledani* i *Yandex*. Kada izaberete podrazumevani pretraživač, ponovo pokrenite Internet pregledac kako bi promena stupila na snagu.

Takođe možete da aktivirate ili da isključite određena podešavanja **AVG bezbednosne trake sa alatkama**:

- **Postavi i zadrži Yahoo! kao pretraživač u traci sa adresom** - (podrazumevano je uključeno) - ako je izabrana, ova opcija vam omogućava da ključnu reč za pretragu upišete direktno u traku za adresu vašeg Internet pregledaca i Yahoo! usluga će se automatski koristiti za pretraživanje relevantnih Web lokacija.
- **Neka AVG daje predloge u slučaju greške u navigaciji pregledaca (404/DNS)** - (podrazumevano je uključeno) - ako prilikom pretraživanja Web



naidete na stranicu koja ne postoji ili stranicu koja se ne može prikazati (greška 404), bicete automatski preusmereni na Web stranicu na kojoj cete moci da izaberete alternativne stranice sa slicnom temom.

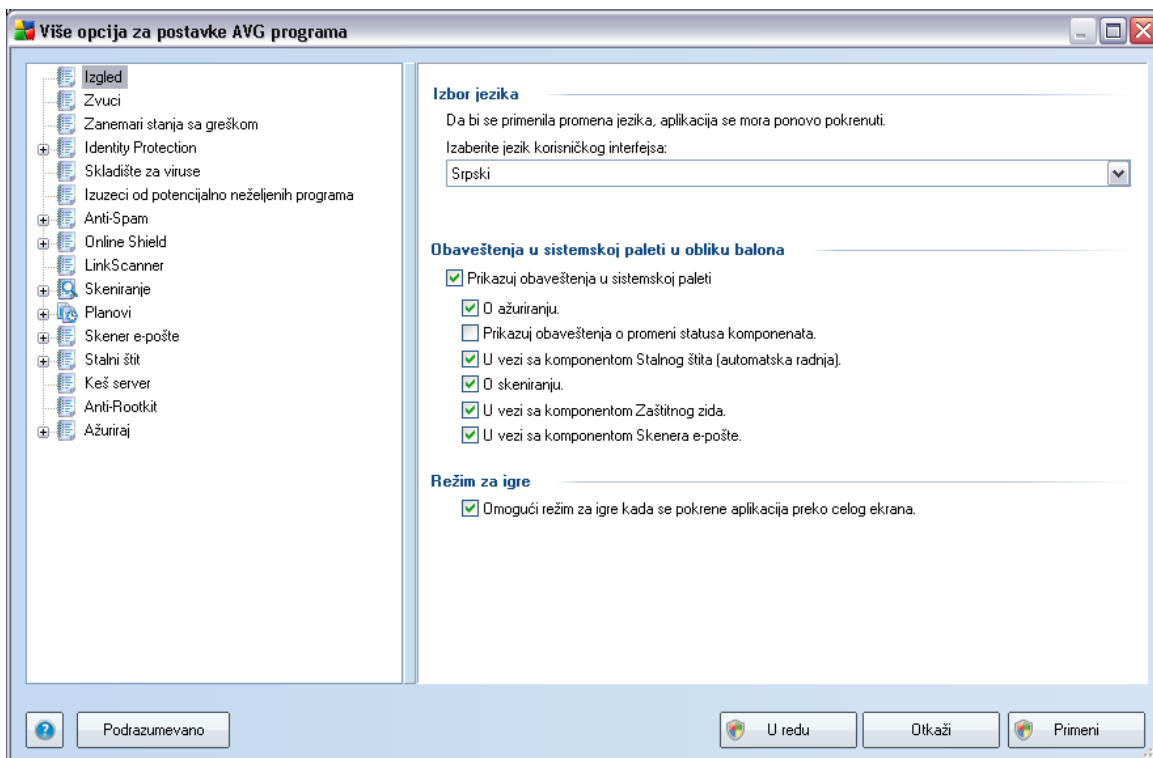
- **Postavi i zadrži Yahoo! kao pretraživac za vaš pregledac** - (*podrazumevano je iskluceno*) - Yahoo! je podrazumevani pretraživac za pretragu u okviru AVG bezbednosne trake sa alatkama, a aktiviranjem ove opcije takode može postati podrazumevani pretraživac u vašem Web pregledacu.
- **Ponovo prikaži AVG bezbednosnu traku sa alatkama kada je skrivena (nedeljno)** - (*podrazumevano je ukluceno*) - ova opcija je podrazumevano aktivirana i kada vaša **AVG bezbednosna traka sa alatkama** slucajno postane skrivena, ovom opcijom ponovo ce se prikazivati u periodu od jedne nedelje.

10. AVG napredna podešavanja

Dijalog za napredna podešavanja programa **AVG 9 Anti-Virus sa zaštitnim zidom** se otvara u novom prozoru **Napredna podešavanja AVG programa**. Ovaj prozor je podeljen u dva odeljka: sa leve strane se nalazi stablo za navigaciju po opcijama za konfigurisanje programa. Izaberite komponentu čiju konfiguraciju želite da izmenite (*ili nekog njenog dela*), kako bi se sa desne strane otvorio dijalog za uređivanje.

10.1. Izgled

Prva stavka navigacionog stabla, **Izgled**, odnosi se na opšta podešavanja [AVG korisničkog interfejsa](#), kao i nekoliko osnovnih opcija ponašanja aplikacije:

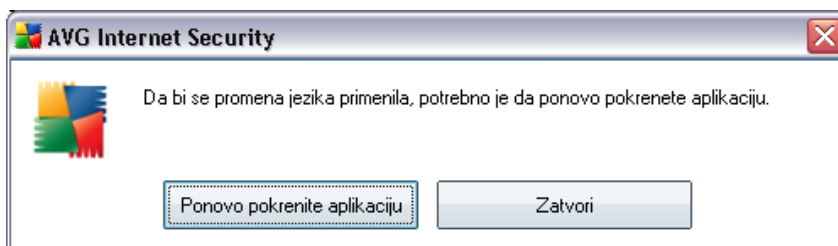


Izbor jezika

U odeljku **Izbor jezika**, možete izabrati željeni jezik sa padajućeg menija; izabrani jezik će se koristiti za citavi [AVG korisnički interfejs](#). U padajućem meniju navedeni su samo oni jezici koje ste izabrali u toku [procesa instalacije](#) (vidi poglavlje [Prilagodena instalacija - Izbor komponenata](#)). Međutim, da biste završili prebacivanje aplikacije na

drugi jezik, potrebno je da ponovo pokrenete korisnicki interfejs; pratite sledece korake:

- Izaberite željeni jezik za aplikaciju i potvrdite izbor pritiskom na dugme **Primeni** (u donjem desnom uglu)
- Kliknite na dugme **U redu** da biste potvrdili
- Pojavice se novi dijalog koji vas obaveštava da promena jezika AVG korisnickog interfejsa zahteva ponovno pokretanje aplikacije:



Obaveštenja u sistemskoj paleti u obliku balona

U ovom odeljku možete izabrati da se ne prikazuju obaveštenja u sistemskoj paleti u obliku balona koja vas informišu o statusu aplikacije. Obaveštenja u obliku balona se podrazumevano prikazuju i preporučuje se da ovu opciju ostavite ukljucenom! Obaveštenja u obliku balona obicno vas informišu o promeni statusa neke AVG komponente, na šta je potrebno da obratite pažnju!

Medutim, ako iz nekog razloga odlucite da ne želite da se prikazuju ova obaveštenja, ili biste želeli da se prikazuju samo odredena obaveštenja (vezana za odredenu AVG komponentu), možete definisati i navesti željene opcije tako što cete oznaciti/poništi izbor sledecih opcija:

- **Prikazuj obaveštenja u sistemskoj paleti** - podrazumevano, ova stavka je izabrana (*ukljucena*), pa se obaveštenja prikazuju. Opozovite izbor ove stavke da biste potpuno iskljucili sva obaveštenja u obliku balona. Ako je ova stavka ukljucena, možete dodatno definisati koja ce se obaveštenja prikazivati:
 - **Prikazuj obaveštenja u sistemskoj paleti o ažuriranju programa** - odlucite da li ce se prikazivati informacije o pokretanju, toku i završetku ažuriranja programa AVG;
 - **Prikazuj obaveštenja o promeni statusa komponenata** - odlucite da li ce se prikazivati informacije o aktivnosti/neaktivnosti komponenata ili

potencijalnim problemima u okviru komponente. Prilikom prijavljivanja stanja greške komponente, ova opcija je jednaka informativnoj funkciji [ikone sistemske palete](#) (promeni boje) koja prijavljuje probleme u AVG komponentama;

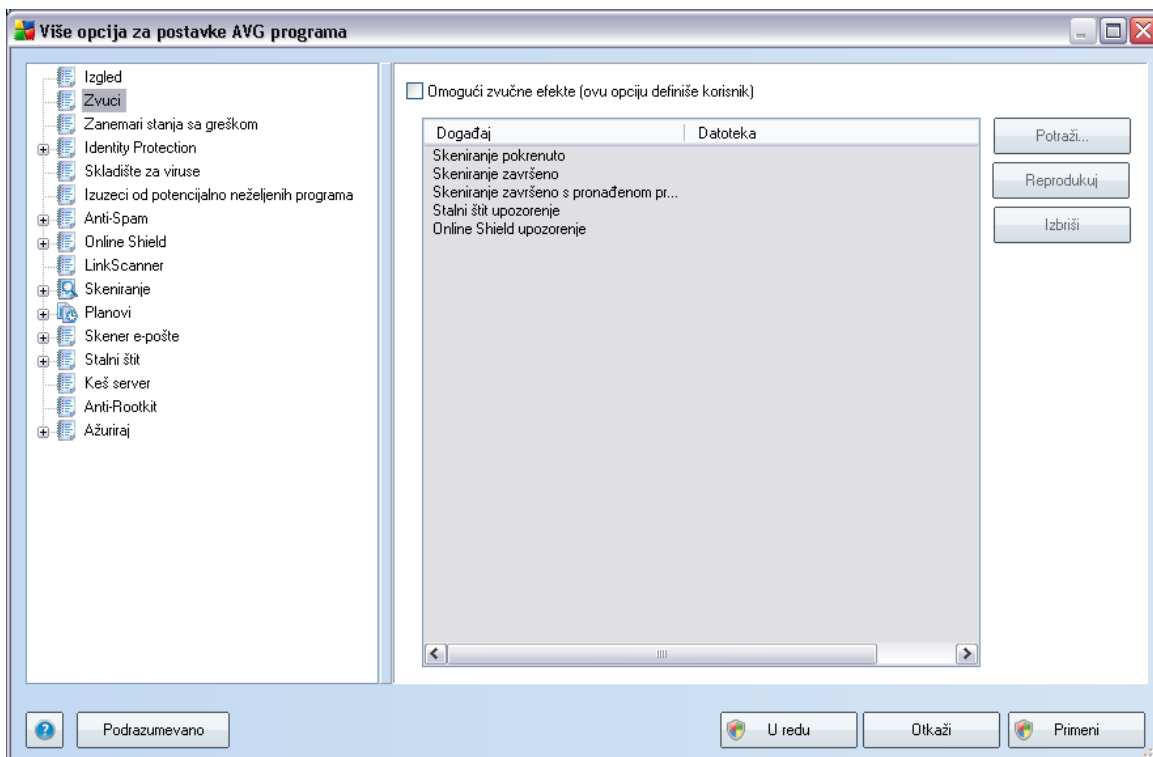
- **Prikazuj obaveštenja u vezi sa [stalnim štitom](#) u sistemskoj paleti** - izaberite da li želite da se informacije u vezi sa cuvanjem, kopiranjem i otvaranjem datoteke prikazuju ili ne (*ova konfiguracija pokazuje da li je opcija stalnog štita [Automatsko lecenje](#) ukljucena*);
- **Prikazuj obaveštenja u sistemskoj paleti o [skeniranju](#)** - odlucite da li ce se prikazivati informacije o automatskom pokretanju planiranog skeniranja, njegovom toku i rezultatima;
- **Prikazuj obaveštenja u sistemskoj paleti u vezi sa [zaštitnim zidom](#)** - odlucite da li ce se obaveštenja u vezi sa statusom i procesima zaštitnog zida, npr. upozorenja o aktiviranju/deaktiviranju ove komponente, mogucem blokiranju saobracaja itd. prikazivati ili ne;
- **Prikazuj obaveštenja u sistemskoj paleti u vezi sa komponentom [Skener e-pošte](#)** - odlucite da li ce se prikazivati informacije o skeniranju sve dolazne i odlazne pošte.

Režim za igre

Ova AVG funkcija je namenjena aplikacijama koje se prikazuju preko celog ekrana i gde bi baloncici sa AVG informacijama (*npr. koji se prikazuju kada se pokrene planirano skeniranje*) mogli da vas ometaju (*oni mogu da umanje aplikaciju ili da naruše njen graficki prikaz*). Da biste izbegli ovakvu situaciju, nemojte opozivati izbor u polju za potvrdu **Omoguci režim za igre kada se prikazuje sadržaj preko celog ekrana** (*podrazumevana postavka*).

10.2. Zvuci

U dijalogu **Zvukovi** možete izabrati da li želite da budete obaveštavani o određenim AVG radnjama putem zvučnog obaveštenja. Ako želite, izaberite opciju **Omoguci zvučne efekte** (*podrazumevano je isključena*) da biste aktivirali listu AVG radnji:

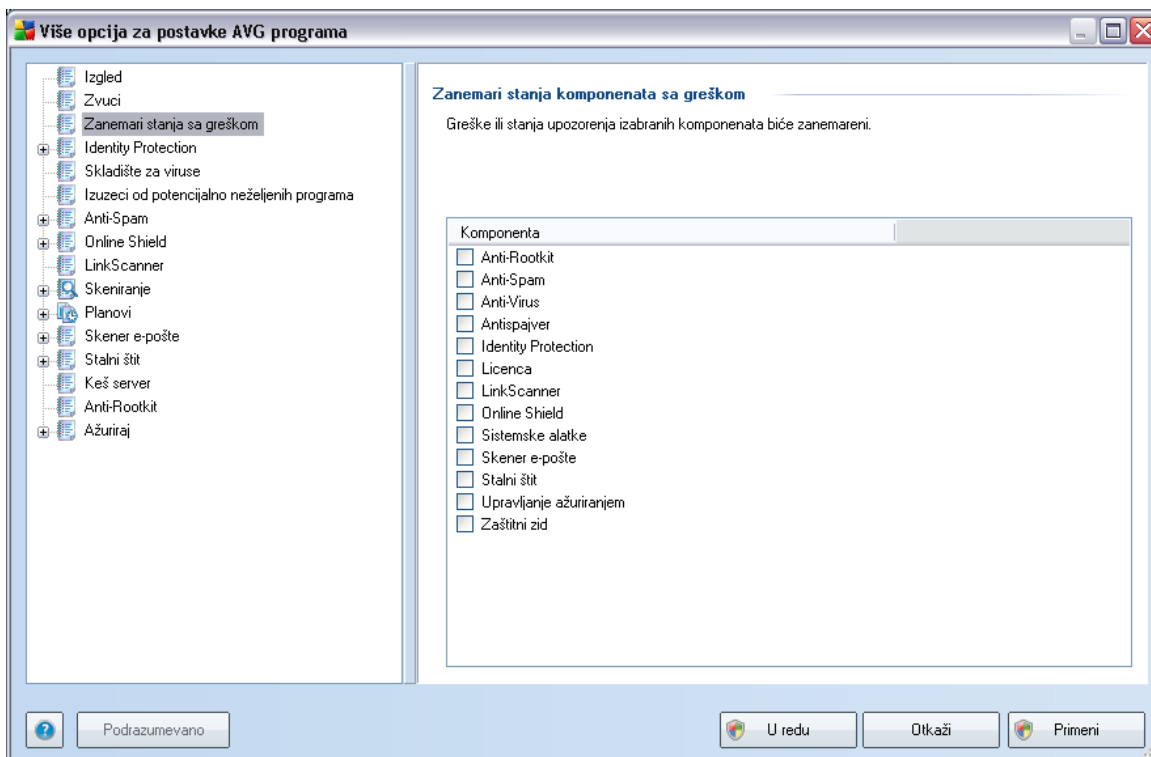


Potom sa liste izaberite odgovarajući događaj i pronađite (**Potraži**) na disku odgovarajući zvuk koji želite da dodelite ovom događaju. Da biste poslušali izabrani zvuk, označite događaj na listi događaja i kliknite na dugme **Reprodukuj**. Kliknite na dugme **Izbriši** da biste uklonili zvuk dodeljen određenom događaju.

Napomena: podržani su samo zvukovi u *.wav formatu!

10.3. Zanemarivanje stanja sa greškom

U dijalogu **Zanemari stanje komponenti sa greškom** možete izabrati one komponente za koje ne želite da dobijate obaveštenja:



Podrazumevano, na listi nije izabrana nijedna komponenta. To znaci da ako se neka komponenta nade u stanju greške, bicete odmah obavešteni putem:

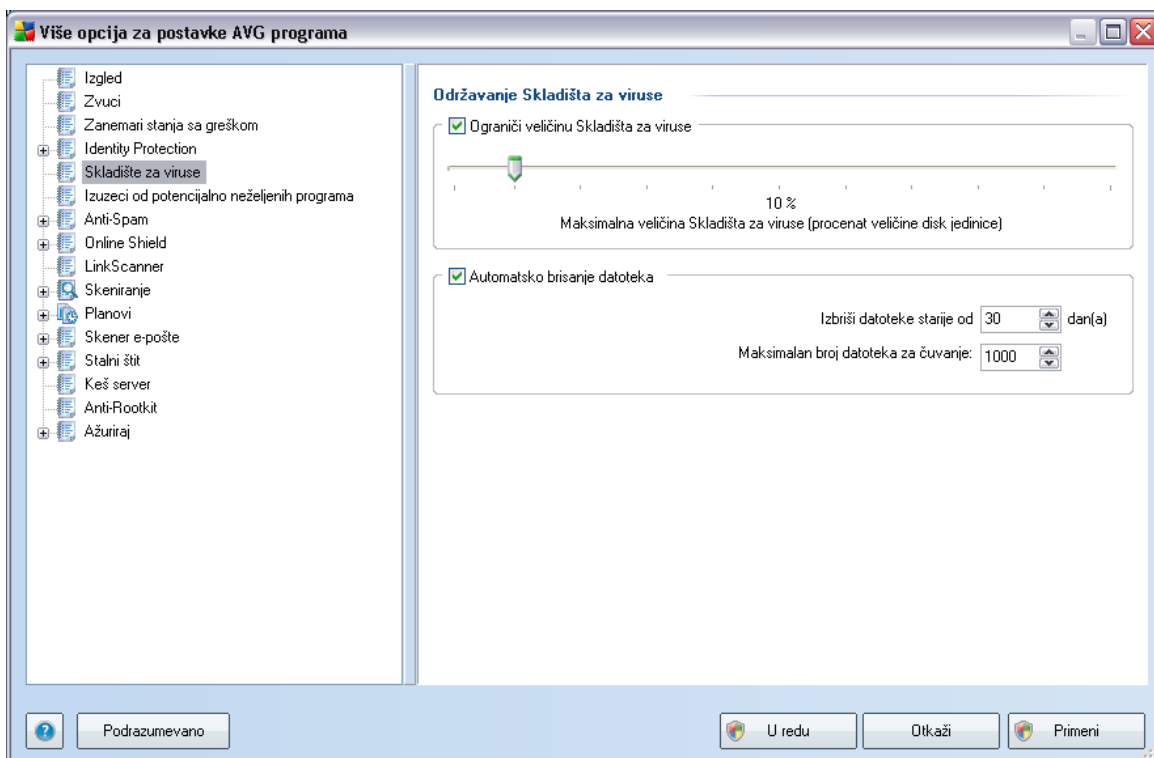
- **ikone na sistemskoj paleti** – kada sve komponente programa AVG rade ispravno, ikona se prikazuje u cetiri boje. Medutim, ako dode do greške, ikona se prikazuje sa žutim znakom uzvika,
- tekstualnog opisa postojećeg problema u odeljku **Informacije o bezbednosnom statusu** u glavnom prozoru programa AVG

Možda ce biti potrebno da u nekoj situaciji iz nekog razloga privremeno isključite komponentu (*to se ne preporučuje, trebalo bi da sve komponente stalno budu uključene i u podrazumevanoj konfiguraciji, ali postoji mogućnost da ih isključite*). U tom slucaju, ikona na sistemskoj paleti vas automatski obaveštava o statusu greške komponente. Medutim, u ovom konkretnom slucaju ne može se govoriti o stvarnoj

grešci jer ste je namerno izazvali i svesni ste moguceg rizika. Kada ikona postane siva, necete dobijati obavještenja o mogujoj drugoj grešci koja se javila.

U tom slucaju, u gore navedenom dijalogu možete izabrati komponente koje mogu biti u stanju greške (*ili isključene*) i za koje ne želite da dobijate obavještenja. Ista opcija za **zanemarivanje stanja komponente** je takode dostupna za određene komponente direktno iz [pregleda komponente u glavnom prozoru programa AVG](#).

10.4. Skladište za viruse



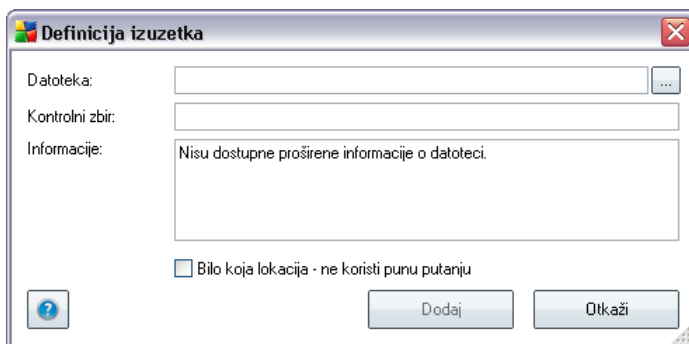
U dijalogu **Održavanje Skladišta za viruse** možete definisati nekoliko parametara u vezi sa administracijom objekata koji se čuvaju u **Skladištu za viruse**:

- **Ograniči veličinu skladišta za viruse** - pomoću klizaca podesite maksimalnu veličinu **skladišta za viruse**. Veličina se definiše kao procenat velicine lokalnog diska.
- **Automatsko brisanje datoteka** - u ovom odeljku možete definisati maksimalni vremenski interval za čuvanje objekata u **Skladištu za viruse** (**Izbriši datoteke starije od ... dana**), kao i maksimalni broj datoteka za čuvanje u

- **Kontrolni zbir** - prikazuje jedinstveni „potpis“ izabrane datoteke. Kontrolni zbir je automatski generisana niska znakova koja dozvoljava AVG programu da nedvosmisleno razlikuje odabranu datoteku od drugih datoteka. Kontrolni zbir se generiše i prikazuje nakon uspešnog dodavanja datoteke.

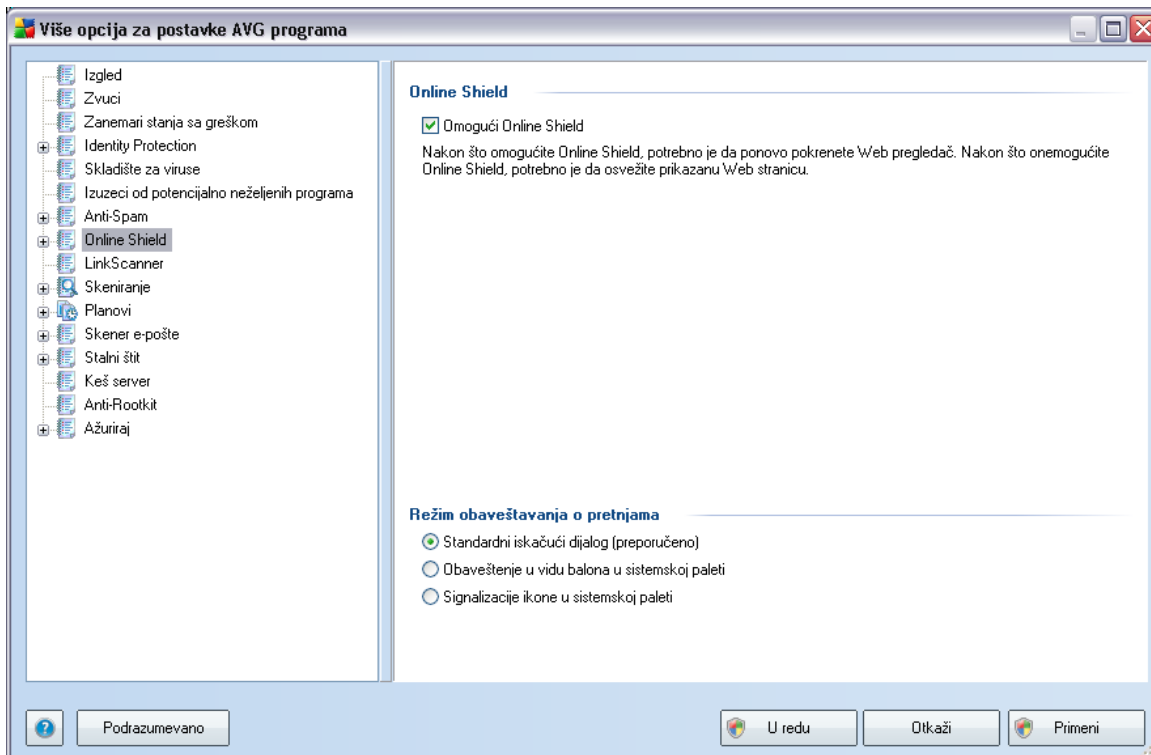
Kontrolna dugmad

- **Uredi** – otvaranje dijaloga za uređivanje (*isti je kao dijalog za definisanje novog izuzetka, pogledajte ispod*) nekog od već definisanih izuzetaka u kojem možete promeniti parametre izuzetka
- **Ukloni** - brisanje izabrane stavke sa liste izuzetaka
- **Dodaj izuzetak** – otvaranje dijaloga za uređivanje u kojem možete definisati parametre novog izuzetka koji će biti kreiran:



- **Datoteka** - unesite punu putanju do datoteke koju želite da označite kao izuzetak
- **Kontrolni zbir** - prikazuje jedinstveni „potpis“ izabrane datoteke. Kontrolni zbir je automatski generisana niska znakova koja dozvoljava AVG programu da nedvosmisleno razlikuje odabranu datoteku od drugih datoteka. Kontrolni zbir se generiše i prikazuje nakon uspešnog dodavanja datoteke.
- **Informacije o datoteci** - prikazivanje postojećih dodatnih informacija o izabranoj datoteci (*informacije o licenci/verziji itd.*)
- **Bilo koja lokacija - ne koristi punu putanju** - ako želite da ovu datoteku označite kao izuzetak samo ako se nalazi na određenoj lokaciji, nemojte izabrati ovo polje.

10.6. Online Shield



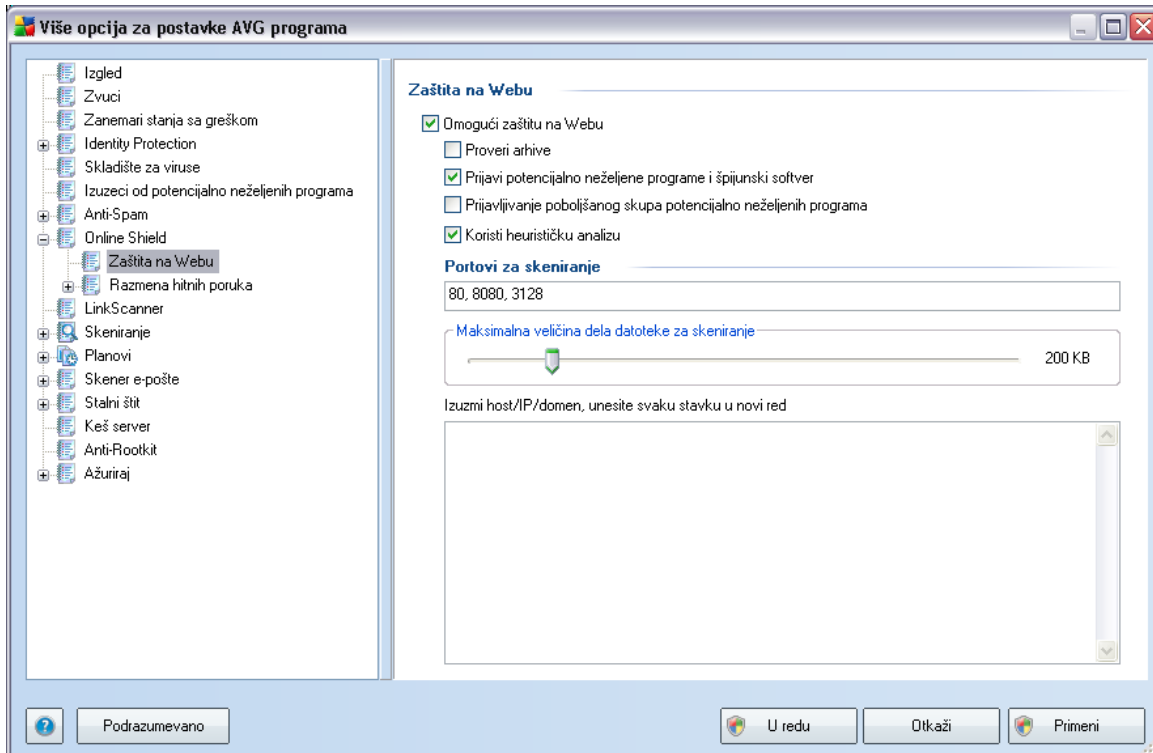
Dijalog **Zaštita na Webu** vam omogućava da aktivirate/deaktivirate celu komponentu **Online Shield** putem opcije **Omogući Online Shield** (*aktivirana je podrazumevano*). Za napredna podešavanja ove komponente, otvorite naredne dijaloge na stablu za navigaciju:

- [Zaštita na Webu](#)
- [Razmena hitnih poruka](#)

Režim obaveštavanja o pretnji

U donjem odeljku ovog dijaloga, izaberite način na koji želite da budete obavestavani o mogućoj otkrivenoj pretnji: putem standardnog iskacuceg dijaloga, obavestjenja u sistemskoj paleti u obliku baloncica ili pomocu signalizacije ikone u sistemskoj paleti.

10.6.1. Zaštita na Webu



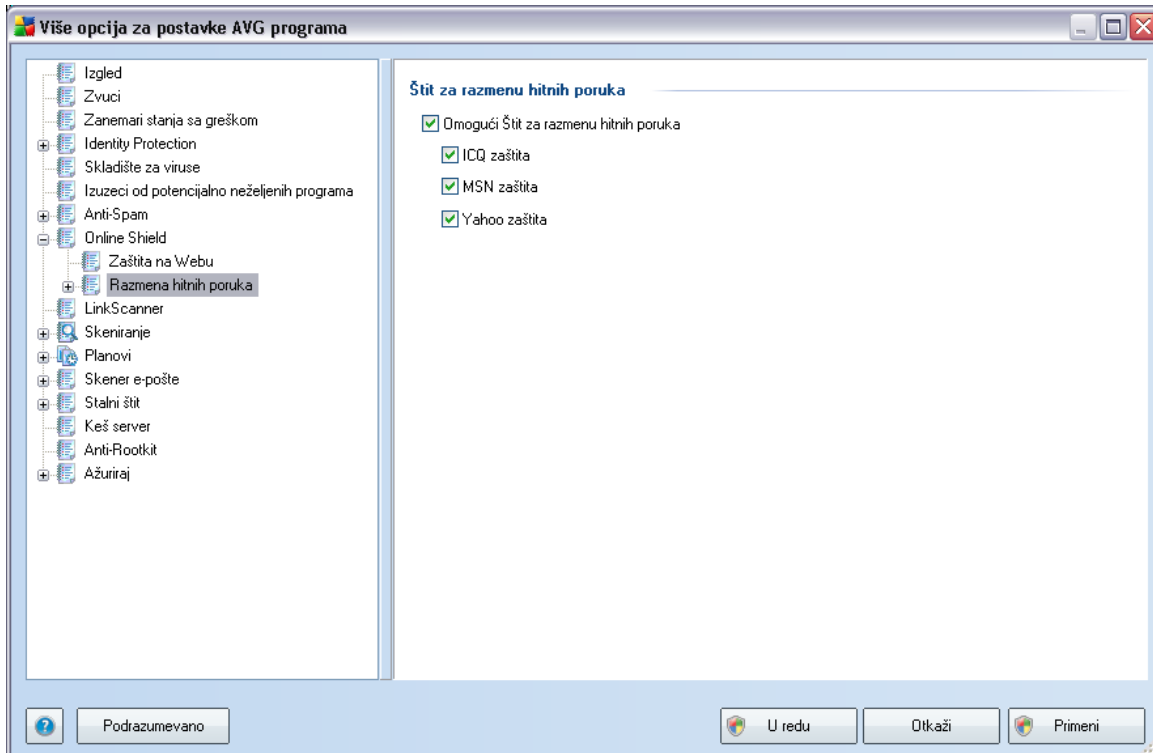
U dijalogu **Zaštita na Webu** možete urediti konfiguraciju komponente u vezi sa skeniranjem sadržaja Web lokacija. Interfejs za uređivanje omogućava vam da konfigurišete sledeće osnovne opcije:

- **Omogući zaštitu na Webu** - ovom opcijom se potvrđuje da **Online Shield** treba da obavlja skeniranje sadržaja www stranica. Ako je ova opcija uključena (*podrazumevano*), možete uključiti/isključiti sledeće stavke:
 - **Proveri arhive** - skeniranje sadržaja arhiva koje se potencijalno nalaze na www stranici koja se prikazuje.
 - **Prijavi potencijalno neželjene programe i špijunski softver** - (*podrazumevano je uključeno*): potvrdite izbor u ovom polju za potvrdu da biste aktivirali **Antispajver** mehanizam i obavili skeniranje u potrazi za špijunskim programima i virusima. **Špijunski softver** se ne može sa sigurnošću svrstati u kategoriju malvera: Iako obično predstavlja bezbednosni rizik, neki od ovih programa mogu se bezbedno instalirati na računar. Preporučujemo vam da ova funkcija bude uključena jer povećava

bezbednost racunara.

- **Prijavi poboljšani skup potencijalno neželjenih programa** – ako je prethodna opcija aktivirana, takode možete da potvrdite izbor u ovom polju za potvrdu kako bi se detektovao poboljšani skup [špijunskih programa](#): programi koji su potpuno bezbedni kada ih kupite od proizvođača, ali koji se kasnije mogu iskoristiti u zlonamerne svrhe. Ovo je dodatna mera kojom se bezbednost racunara poboljšava još više. Medutim, zbog toga što postoji mogućnost blokiranja legalnih programa, ova opcija je podrazumevano isključena.
- **Koristi heuristicku analizu** - skeniranje sadržaja stranice koja se prikazuje pomocu metoda [heuristicke analize](#) (*dinamicke emulacije upustava skeniranog objekta u virtualnom racunarskom okruženju*).
- **Portovi za skeniranje** - ovo polje sadrži listu standardnih portova za http komunikaciju. Ako se konfiguracija vašeg racunara razlikuje, možete promeniti brojeve portova.
- **Maksimalna velicina datoteke za skeniranje** - ako se na prikazanoj stranici nalaze datoteke, možete skenirati njihov sadržaj pre nego što ih preuzmete na vaš racunar. Medutim, skeniranje velikih datoteka može potrajati i, samim tim, znatno usporiti učitavanje Web stranice. Možete da koristite klizac da biste naveli maksimalnu velicinu datoteke za skeniranje komponentom [Online Shield](#). Čak i u slučaju da je preuzeta datoteka veća nego što je predviđeno, pa je Online Shield neće skenirati, ipak ćete biti zaštićeni: ako je datoteka zaražena, [Online Shield](#) će je odmah detektovati.
- **Izuzmi host/IP/domen** - u polje za tekst možete upisati tačno ime servera (*host, IP adresu, IP adresu sa maskom ili URL adresu*) ili domen koji ne bi trebalo da skenira [Online Shield](#). Zbog toga izuzmite samo hostove za koje ste sigurni da ne sadrže Web lokacije sa opasnim sadržajem.

10.6.2. Razmena hitnih poruka

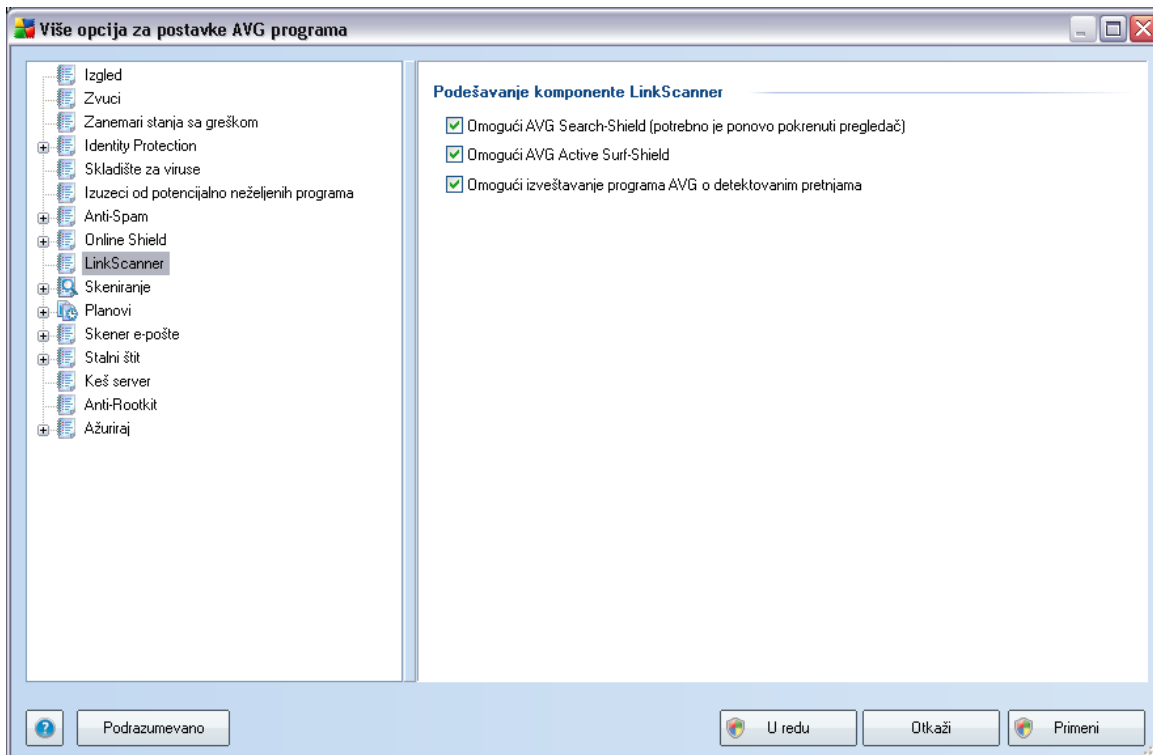


U dijalogu **Štit za razmenu hitnih poruka**, možete urediti podešavanja komponente **Online Shield** koja se odnose na skeniranje hitnih poruka. Trenutno su podržana tri programa za razmenu hitnih poruka: **ICQ**, **MSN** i **Yahoo** - potvrdite izbor u odgovarajućem polju za potvrdu pored svake stavke ako želite da **Online Shield** proverava da li se komunikacija na mreži odvija bez virusa.

Za detaljno podešavanje dozvoljenih/blokiranih korisnika, možete otvoriti i urediti odgovarajući dijalog (**Napredna podešavanja za ICQ**, **Napredna podešavanja za MSN**, **Napredna podešavanja za Yahoo**) i definisati **belu listu** (lista korisnika kojima je dozvoljeno da komuniciraju sa vama) i **crnu listu** (korisnici koje treba blokirati).

10.7. Skener linkova

Dijalog **Postavke skenera linkova** vam omogućava da uključite/isključite osnovne funkcije komponente **Skener linkova**:



- **Omogući AVG štit za pretraživanje** - (*podrazumevano je uključeno*): ikone obaveštenja koje daju savete o rezultatima pretrage pomoću pretraživača Google, Yahoo, Bing, Yandex, Altavista ili Baidu, nakon prethodnog proveravanja sadržaja Web lokacija koje je ponudio pretraživač.
- **Omogući AVG štit za aktivno pregledanje Interneta** - (*podrazumevano uključeno*): aktivna zaštita (*u realnom vremenu*) od zlonamernih Web lokacija u trenutku kada im se pristupa. Poznate zlonamerne Web lokacije i njihov opasan sadržaj se blokiraju dok im korisnik pristupa pomoću Web pregledača (*ili neke druge aplikacije koja koristi HTTP*).
- **Omogući izveštavanje o otkrivenim pretnjama kompaniji AVG** - (*podrazumevano je uključeno*): izaberite ovu opciju da biste omogućili povratno izveštavanje o „exploit“ programima i opasnim Web lokacijama koje korisnik otkrije pomoću funkcije **AVG štit za aktivno pregledanje Interneta** ili **AVG**

Štit za pretraživanje kako biste dodali ove informacije u bazu podataka o zlonamernim aktivnostima na Internetu.

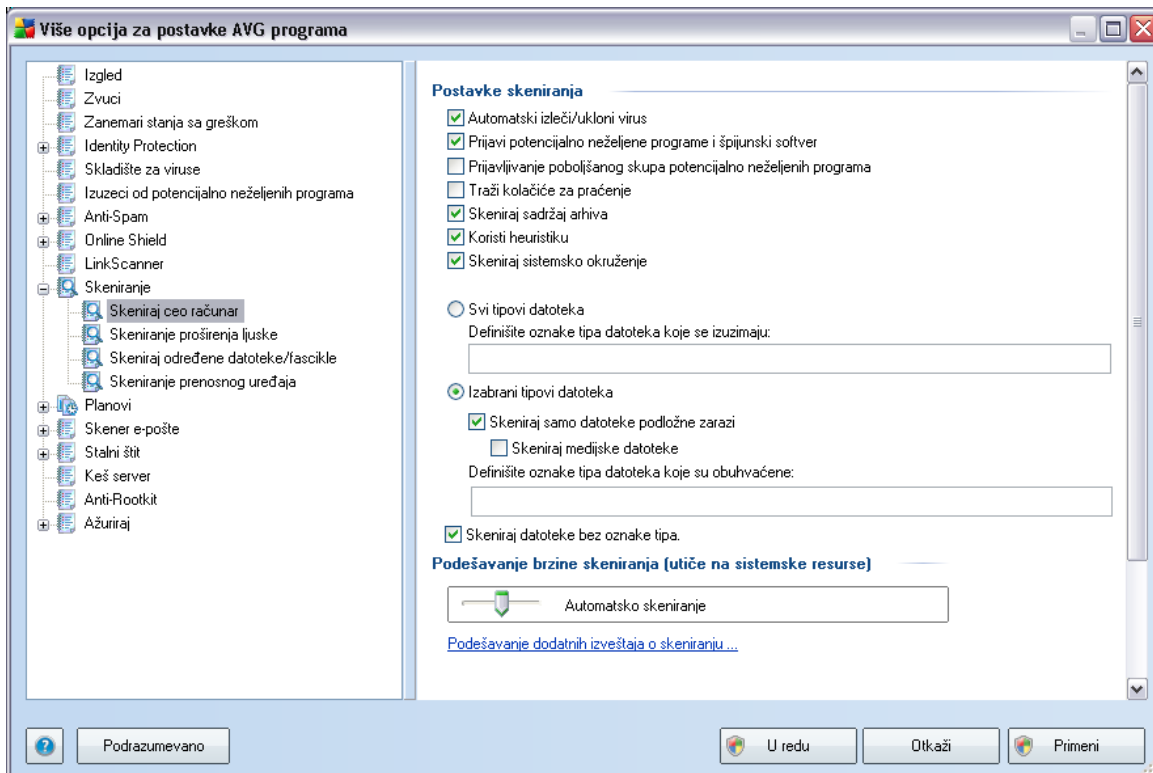
10.8. Skeniranje

Napredna podešavanja skeniranja podijeljena su na tri kategorije koje se odnose na određene tipove skeniranja, definisane od strane proizvođača softvera:

- **Skeniraj ceo racunar** - standardno unapred definisano skeniranje celog racunara
- **Shell Extension skeniranje** - posebno skeniranje izabranog objekta direktno iz programa Windows Explorer
- **Skeniraj odredene datoteke i fascikle** - standardno unapred definisano skeniranje izabranih oblasti racunara
- **Skeniranje prenosnog uredaja** - posebno skeniranje prenosnih uredaja povezanih na racunar

10.8.1. Skeniraj ceo racunar

Opcija **Skeniraj ceo racunar** omogućava uređivanje parametara unapred definisanog skeniranja od strane proizvođača softvera, [Skeniraj ceo racunar](#):



Podešavanja skeniranja

U odeljku **Podešavanja skeniranja** pronaci ćete listu parametara za skeniranje koje je moguće opcionalno uključiti ili isključiti.

- **Automatski izleći/ukloni infekciju** - ako tokom skeniranja bude otkriven virus, moguće ga je automatski ukloniti, ukoliko je dostupan lek. Ukoliko zaraženu datoteku nije moguće automatski izluciti, ona će biti premeštena u [Skladište za viruse](#).
- **Prijavi potencijalno neželjene programe i špijunski softver** - (podrazumevano je uključeno): potvrdite izbor u ovom polju za potvrdu da biste aktivirali [Antispajver](#) mehanizam i obavili skeniranje u potrazi za špijunskim

programima i virusima. [Špijunski softver](#) se ne može sa sigurnošću svrstati u kategoriju malvera: Iako obično predstavlja bezbednosni rizik, neki od ovih programa mogu se bezbedno instalirati na računar. Preporučujemo vam da ova funkcija bude uključena jer povećava bezbednost računara.

- **Prijavi poboljšani skup potencijalno neželjenih programa** – ako je prethodna opcija aktivirana, takođe možete da potvrdite izbor u ovom polju za potvrdu kako bi se detektovao poboljšani skup [špijunskih programa](#): programi koji su potpuno bezbedni kada ih kupite od proizvođača, ali koji se kasnije mogu iskoristiti u zlonamerne svrhe. Ovo je dodatna mera kojom se bezbednost računara poboljšava još više. Međutim, zbog toga što postoji mogućnost blokiranja legalnih programa, ova opcija je podrazumevano isključena.
- **Traži kolacice za pracenje** - ovaj parametar komponente [Antispajver](#) definiše da bi tokom skeniranja trebalo otkrivati kolacice (*HTTP kolacici služe za proveru identiteta, pracenje i održavanje određenih informacija o korisnicima, kao što su željene opcije lokacije ili sadržaj elektronskih korpa za kupovinu*)
- **Skeniraj sadržaj arhiva** - ovaj parametar definiše da bi tokom skeniranja trebalo proveravati sve datoteke, pa čak i one koje se nalaze unutar arhiva, npr. ZIP, RAR, ...
- **Koristi heuristiku** - heuristička analiza (*dinamička emulacija instrukcija skeniranih objekata u virtuelnom računarskom okruženju*) bice jedna od metoda koja će se koristiti za otkrivanje virusa tokom skeniranja;
- **Skeniraj sistemsko okruženje** - skeniranjem će biti obuhvacene i sistemske oblasti računara.

Trebalo bi i da odlucite da li želite da skenirate

- **Sve tipove datoteka** sa mogućnošću definisanja izuzetaka tako što ćete uneti listu oznaka tipa datoteka razdvojenih zarezima koje ne bi trebalo skenirati (*kada sacuvate listu, zarezi se pretvaraju u tacku i zarez*);
- **Izabrane tipove datoteka** - možete izabrati da skenirate samo datoteke za koje postoji mogućnost da su zaražene (*datoteke koje ne mogu biti zaražene neće se skenirati, na primer tekstualne datoteke ili neke druge datoteke koje nisu izvršne*), uključujući medijske datoteke (*video audio datoteke - ako ne potvrdite izbor u ovom polju za potvrdu, vreme skeniranja će se dodatno skratiti jer su datoteke ovog tipa obično velike i malo je verovatno da su zaražene virusom*). Izborom oznake tipa datoteka možete označiti datoteke koje treba uvek skenirati.
- Možete i da izaberete opciju **Skeniraj datoteke bez oznake tipa datoteke** -

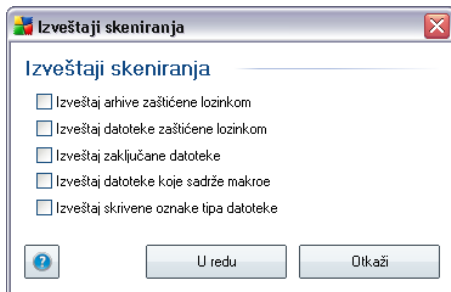
ova opcija je podrazumevano uključena i preporučuje se da je ne isključujete osim ako nemate dobar razlog za to. Datoteke bez oznake tipa datoteke su sumnjive i treba ih uvek skenirati.

Prioritet procesa skeniranja

U odeljku **Prioritet procesa skeniranja** možete dodatno odrediti željenu brzinu skeniranja u zavisnosti od stepena iskorišćenosti sistemskih resursa. Podrazumevana podešavanja za ovu opciju je srednji nivo automatske upotrebe resursa. Ako želite da se skeniranje obavlja brže, bice potrebno manje vremena, ali ce se iskorišćenost sistemskih resursa znacajno povećati tokom skeniranja, a to ce usporiti ostale aktivnosti na racunaru (*ovu opciju možete koristiti kada je racunar ukljucen, ali niko ne radi na njemu*). Sa druge strane, iskorišćenost sistemskih resursa možete smanjiti tako što cete produžiti trajanje skeniranja.

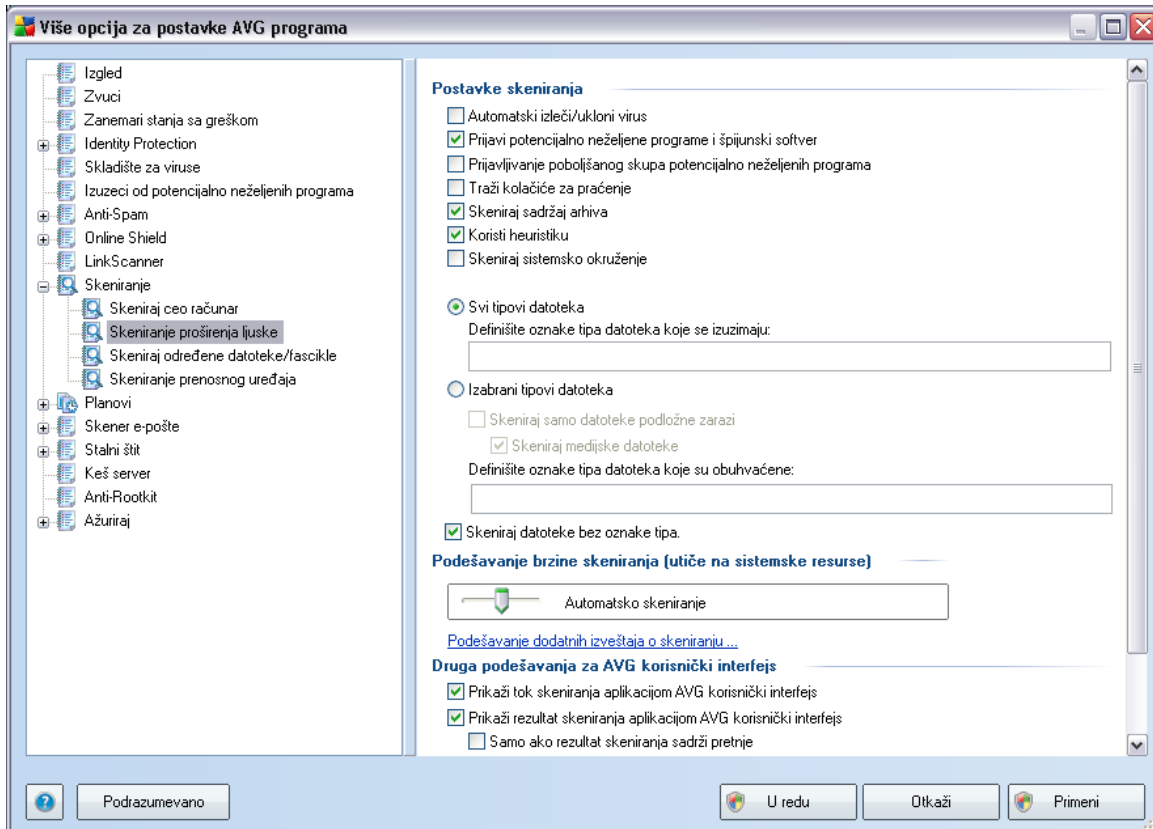
Podešavanje dodatnih izveštaja o skeniranju ...

Kliknite na link **Podešavanje dodatnih izveštaja o skeniranju ...** da biste otvorili samostalan dijalog po imenu **Izveštaji skeniranja** u kojem možete označiti nekoliko stavki kako biste definisali koji ce se rezultati prijavljivati:



10.8.2. Shell Extension skeniranje

Slicno kao i prethodna stavka [Skeniraj ceo racunar](#), stavka **Shell extension skeniranje** takode nudi nekoliko opcija za uređivanje skeniranja koje je unapred definisano od strane proizvođača softvera. Ovog puta konfiguracija se odnosi na [skeniranje određenih objekata koji se pokrecu direktno iz programa Windows Explorer \(shell extension\)](#), pogledajte poglavlje [Skeniranje u programu Windows Explorer](#):

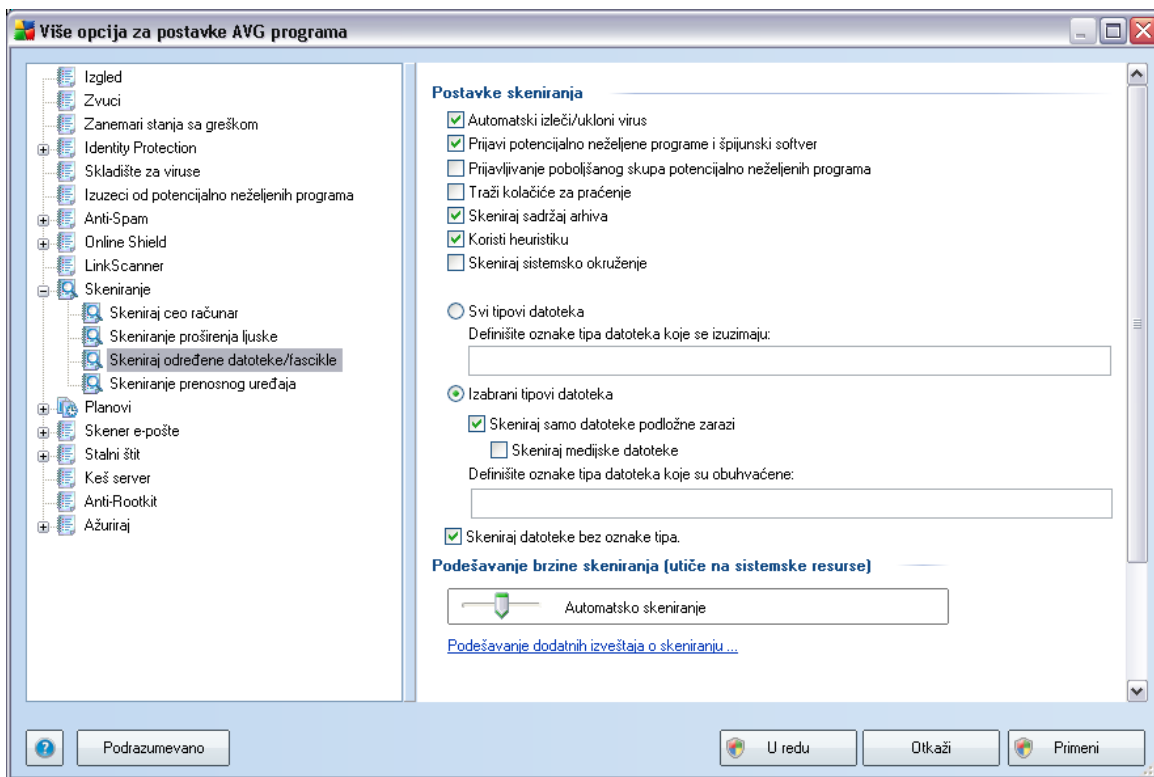


Lista parametara identična je listi koja je dostupna za opciju **[Skeniranje celog racunara](#)**. Međutim, podrazumevane postavke se razlikuju: za opciju **[Skeniranje celog racunara](#)** izabrana je većina parametara, a za opciju **[Shell extension skeniranje \(Skeniranje u programu Windows Explorer\)](#)** uključeni su samo određeni parametri.

Napomena: Opis pojedinačnih parametara potražite u poglavlju **[AVG napredna podešavanja / Skeniranje / Skeniraj ceo racunar](#)**.

10.8.3. Skeniraj određene datoteke ili fascikle

Interfejs za uređivanje opcije **[Skeniraj određene datoteke ili fascikle](#)** isti je kao dijalog za uređivanje opcije **[Skeniraj ceo racunar](#)**. Sve opcije za konfigurisanje su iste, ali su podrazumevane postavke strožije za **[Skeniranje celog racunara](#)**:

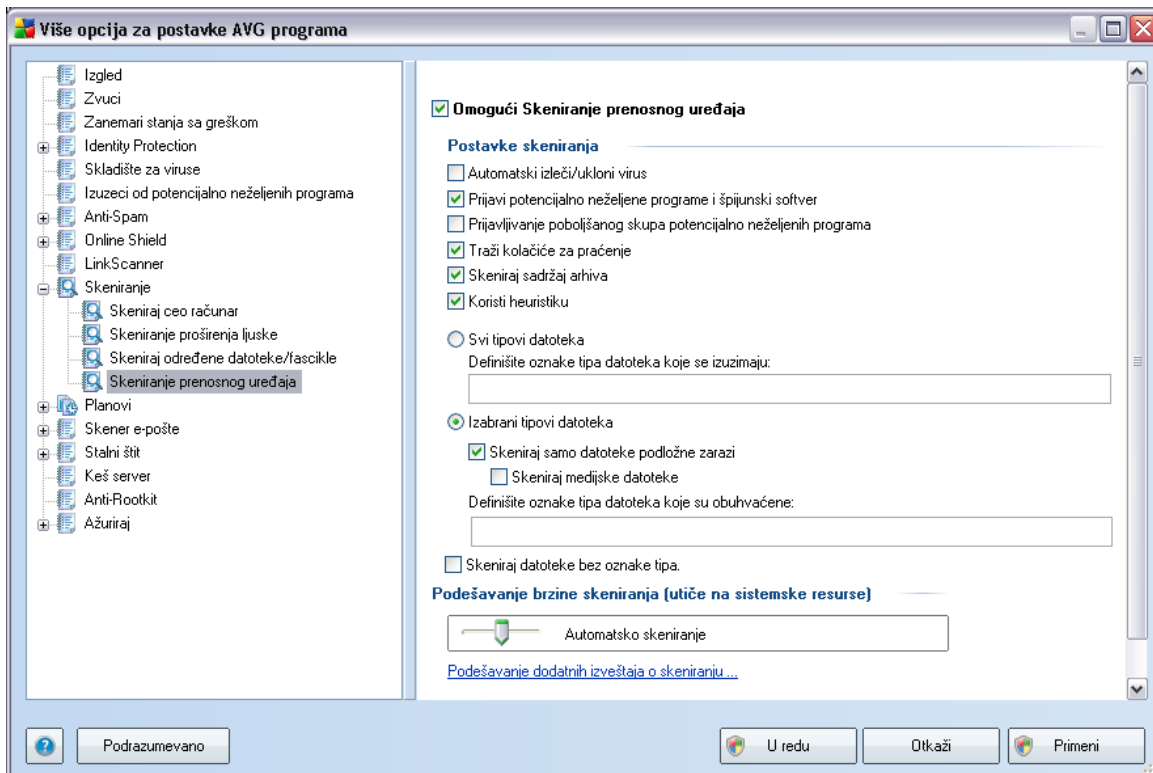


Svi parametri koji su definisani u ovom dijalogu za konfiguraciju odnose se samo na oblasti koje će se skenirati postavkom **Skeniraj određene datoteke ili fascikle**!

Napomena: Opis pojedinačnih parametara potražite u poglavlju **AVG napredna podešavanja / Skeniranje / Skeniraj ceo racunar**.

10.8.4. Skeniranje prenosnog uređaja

Interfejs za uređivanje funkcije **Skeniranje prenosnog uređaja** takode je veoma sličan dijalogu za uređivanje funkcije **Skeniraj ceo racunar**:



Funkcija **Skeniranje prenosnog uređaja** pokrece se automatski kada na racunar povežete bilo koji prenosni uređaj. Podrazumevano, ovaj vid skeniranja je iskljucen. Medutim, od kljucne je važnosti da se prenosni uređaji skeniraju u potrazi za pretnjama pošto oni predstavljaju jedan od najčešćih izvora zaraze. Da bi ovaj vid skeniranja bio u stanju pripravnosti i automatski se pokretao po potrebi, označite opciju **Skeniranje prenosnog uređaja**.

Napomena: Opis pojedinačnih parametara potražite u poglavlju **AVG napredna podešavanja / Skeniranje / Skeniraj ceo racunar**.

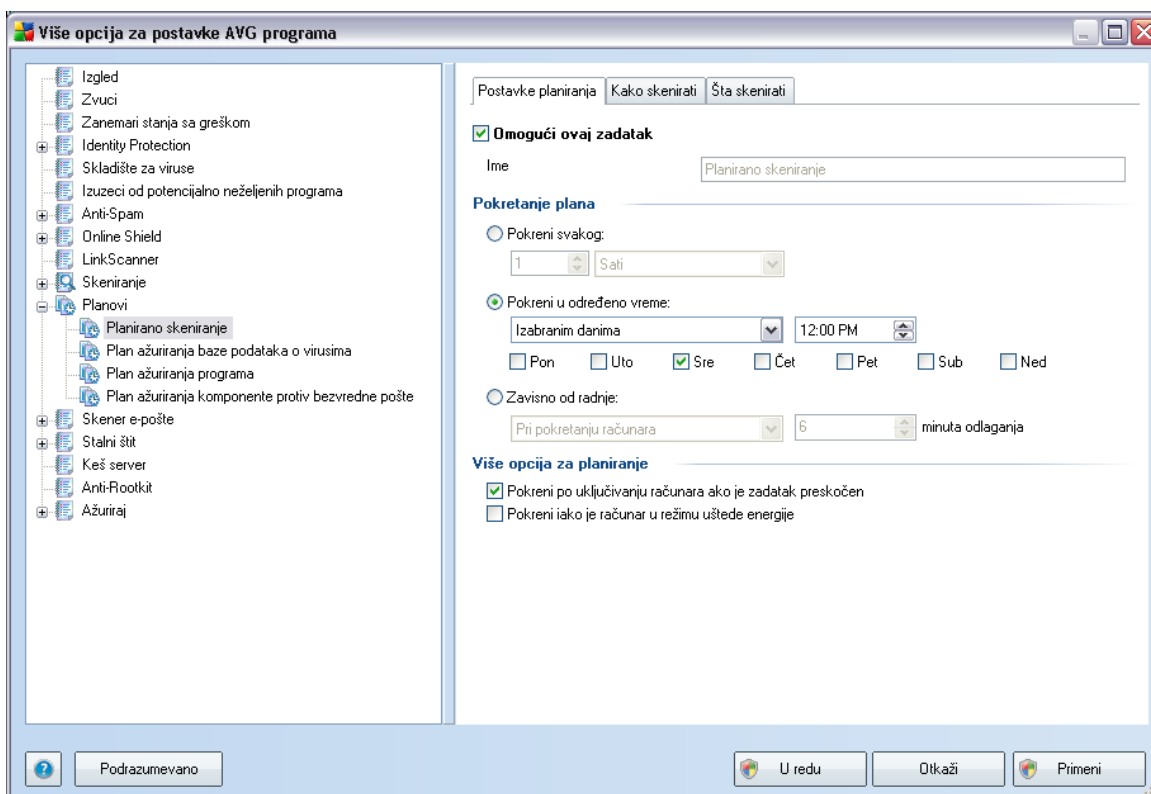
10.9. Planovi

U odeljku **Planovi** možete urediti podrazumevane postavke za:

- [Plan skeniranja celog racunara](#)
- [Plan ažuriranja baze podataka o virusima](#)
- [Plan ažuriranja programa](#)

10.9.1. Planirano skeniranje

Parametri planiranog skeniranja mogu se urediti (*ili se može kreirati novi plan*) na tri kartice:



Na kartici **Podešavanja planiranja** možete prvo oznaciti/poništiti izbor stavke **Omogući ovaj zadatak** da biste jednostavno deaktivirali zakazani test, a kasnije ga

možete uključiti po potrebi.

U tekstualnom polju **Ime** (deaktivirano za sve podrazumevane planove) nalazi se ime koje je prodavac programa dodelio ovom planu. Ukoliko se radi o planovima koje ste naknadno dodali (novi plan možete dodati tako što ćete kliknuti desnim tasterom miša iznad stavke **Planirano skeniranje** u levom stablu za navigaciju), možete da definišete sopstveno ime i u tom slučaju tekstualno polje je moguće urediti. Koristite kratka, opisna i prikladna imena za skeniranja da biste ih kasnije lakše razlikovali.

Primer: Nije dobro nazvati skeniranje „Novo skeniranje“ ili „Moje skeniranje“, pošto ta imena ne opisuju ono što se tim skeniranjem proverava. S druge strane, primer dobrog opisnog imena bio bi „Skeniranje sistemskih oblasti“ itd. Takođe, nije obavezno da u imenu skeniranja navedete da li je u pitanju skeniranje celog računara ili samo određenih datoteka ili fascikli - vaši načini skeniranja uvek će predstavljati određenu verziju [skeniranja određenih datoteka ili fascikli](#).

U ovom dijalogu možete definisati sledeće parametre skeniranja:

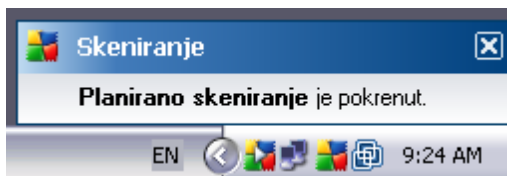
Pokretanje plana

Ovde možete da navedete vremenske intervale za pokretanje novog planiranog skeniranja. Vremenski interval je moguće definisati uzastopnim pokretanjem skeniranja nakon određenog vremenskog perioda (**Pokreni svakih ...**), definisanjem tačnog datuma i vremena (**Pokreni u određeno vreme ...**) ili definisanjem događaja sa kojim bi trebalo povezati pokretanje skeniranja (**Radnja zasnovana na pokretanju računara**).

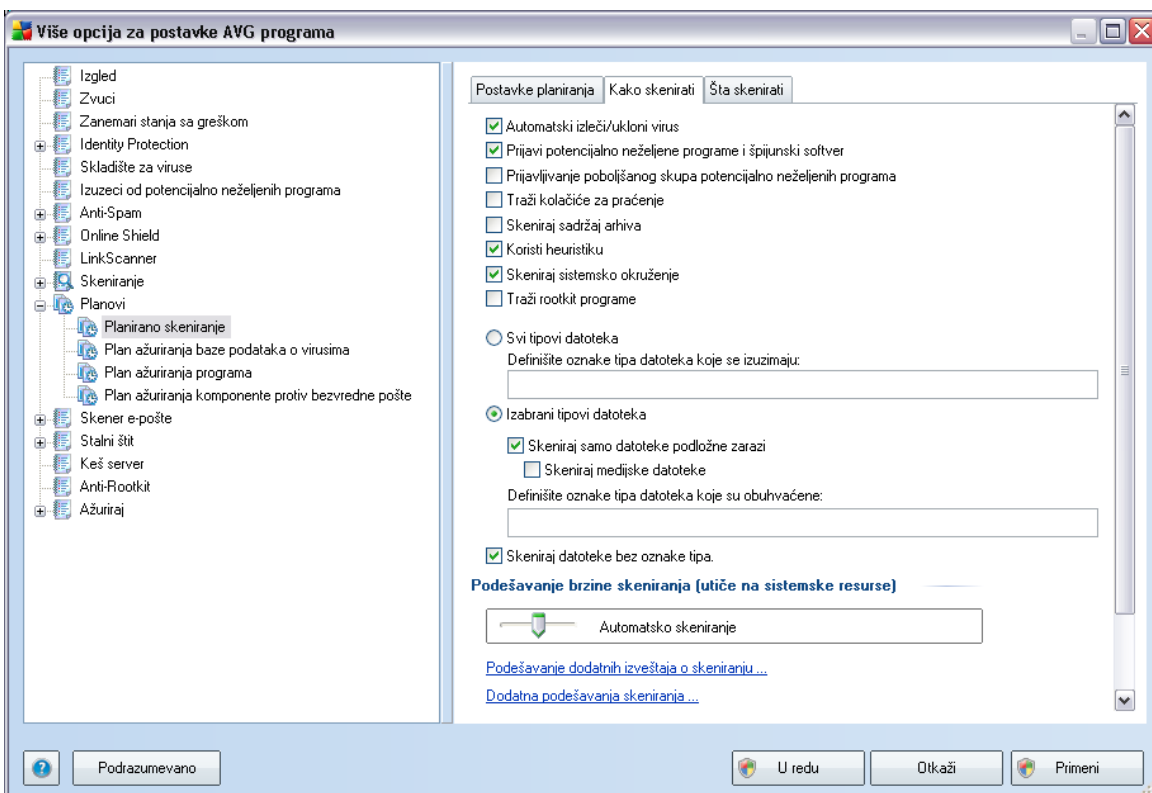
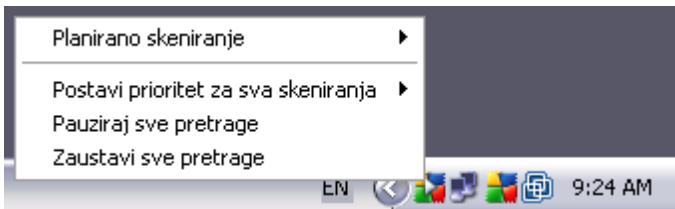
Više opcija za planiranje

U ovom odeljku možete definisati pod kojim se okolnostima skeniranje pokreće/ne pokreće ako je računar u režimu niske potrošnje energije ili je potpuno isključen.

Kada se pokrene planirano skeniranje u navedenom vremenskom periodu, bićete obavješteni putem iskacućeg prozora koji se otvorio iznad [AVG ikone na sistemskoj paleti](#):



Potom se pojavljuje nova [AVG ikona na sistemskoj paleti](#) (u boji sa belom strelicom – pogledajte sliku iznad) koja vas obaveštava da je planirano skeniranje u toku. Kliknite desnim tasterom miša na AVG ikonu koja oznacava da je skeniranje u toku da biste otvorili kontekstualni meni u kojem možete pauzirati ili zaustaviti skeniranje:



Na kartici **Kako skenirati** pronaci cete listu parametara za skeniranje koje je moguće opcionalno uključiti ili isključiti. Vecina parametara je podrazumevano uključena i primenjivace se tokom skeniranja. Ukoliko nemate određen razlog da promenite ta podešavanja, preporučuje se da zadržite unapred definisanu konfiguraciju:

- **Automatski izleci/ukloni infekciju** - ako tokom skeniranja bude otkriven virus, moguće ga je automatski ukloniti, ukoliko je dostupan lek. Ukoliko zaraženu datoteku nije moguće automatski izluciti, ona će biti premeštena u [Skladište za viruse](#).
- **Prijavi potencijalno neželjene programe i špijunski softver** - (*podrazumevano je uključeno*): potvrdite izbor u ovom polju za potvrdu da biste aktivirali [Antispajver](#) mehanizam i obavili skeniranje u potrazi za špijunskim programima i virusima. [Špijunski softver](#) se ne može sa sigurnošću svrstati u kategoriju malvera: Tako obično predstavlja bezbednosni rizik, neki od ovih programa mogu se bezbedno instalirati na računaru. Preporučujemo vam da ova funkcija bude uključena jer povećava bezbednost računara.
- **Prijavi poboljšani skup potencijalno neželjenih programa** - ako je prethodna opcija aktivirana, takođe možete da potvrdite izbor u ovom polju za potvrdu kako bi se detektovao poboljšani skup [špijunskih programa](#): programi koji su potpuno bezbedni kada ih kupite od proizvođača, ali koji se kasnije mogu iskoristiti u zlonamerne svrhe. Ovo je dodatna mera kojom se bezbednost računara poboljšava još više. Međutim, zbog toga što postoji mogućnost blokiranja legalnih programa, ova opcija je podrazumevano isključena.
- **Traži kolacice za pracenje** - (*podrazumevano je uključeno*): ovaj parametar komponente [Antispajver](#) definiše da bi tokom skeniranja trebalo tražiti kolacice (*HTTP kolacici služe za proveru identiteta, pracenje i održavanje određenih informacija o korisnicima, kao što su željene opcije za lokaciju ili sadržaj elektronskih kolica za kupovinu*)
- **Skeniraj unutar arhiva** - (*podrazumevano je uključeno*): ovim parametrom se definiše da bi skeniranje trebalo da obuhvati sve datoteke, čak i ako se one nalaze unutar arhive, npr. ZIP, RAR itd.
- **Koristi heuristiku** - (*podrazumevano je uključeno*): heuristička analiza (*dinamička emulacija instrukcija skeniranih objekata u virtuelnom računarskom okruženju*) bice jedna od metoda koja će se koristiti za otkrivanje virusa tokom skeniranja;
- **Skeniraj sistemsko okruženje** - (*podrazumevano je uključeno*): skeniranje će obuhvatiti i sistemske oblasti na računaru;
- **Traži rootkit programe** - označite ovu stavku ako želite da prilikom skeniranja celog računara obavija i detekcija rootkit programa. Detekcija rootkit programa dostupna je i samostalno, u okviru [Anti-Rootkit](#) komponente;

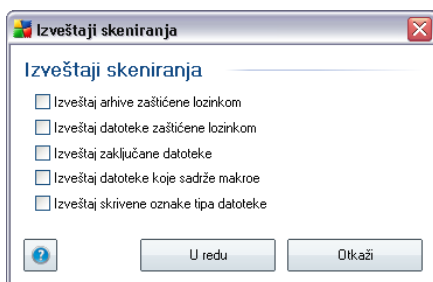
Trebalo bi i da odlucite da li želite da skenirate

- **Sve tipove datoteka** sa mogućnošću definisanja izuzetaka tako što ćete uneti listu oznaka tipa datoteka razdvojenih zarezima koje ne bi trebalo skenirati (*kada sacuvate listu, zarezi se pretvaraju u tacku i zarez*);
- **Izabrane tipove datoteka** - možete izabrati da skenirate samo datoteke za koje postoji mogućnost da su zaražene (*datoteke koje ne mogu biti zaražene neće se skenirati, na primer tekstualne datoteke ili neke druge datoteke koje nisu izvršne*), uključujući medijske datoteke (*video audio datoteke - ako ne potvrdite izbor u ovom polju za potvrdu, vreme skeniranja će se dodatno skratiti jer su datoteke ovog tipa obično velike i malo je verovatno da su zaražene virusom*). Izborom oznake tipa datoteke možete označiti datoteke koje treba uvek skenirati.
- Možete i da izaberete opciju **Skeniraj datoteke bez oznake tipa datoteke** - ova opcija je podrazumevano uključena i preporučuje se da je ne isključujete osim ako nemate dobar razlog za to. Datoteke bez oznake tipa datoteke su sumnjive i treba ih uvek skenirati.

Prioritet procesa skeniranja

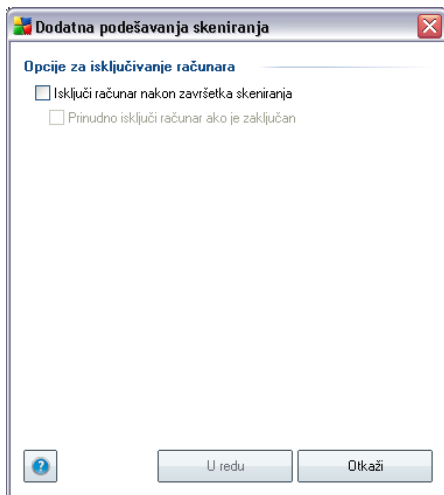
U odeljku **Prioritet procesa skeniranja** možete dodatno odrediti željenu brzinu skeniranja u zavisnosti od stepena iskorišćenosti sistemskih resursa. Podrazumevano podešavanje za ovu opciju je srednji nivo automatske upotrebe resursa. Ako želite da se skeniranje obavlja brže, biće potrebno manje vremena, ali će se iskorišćenost sistemskih resursa značajno povećati tokom skeniranja, a to će usporiti ostale aktivnosti na računaru (*ovu opciju možete koristiti kada je računar uključen, ali niko ne radi na njemu*). Sa druge strane, iskorišćenost sistemskih resursa možete smanjiti tako što ćete produžiti trajanje skeniranja.

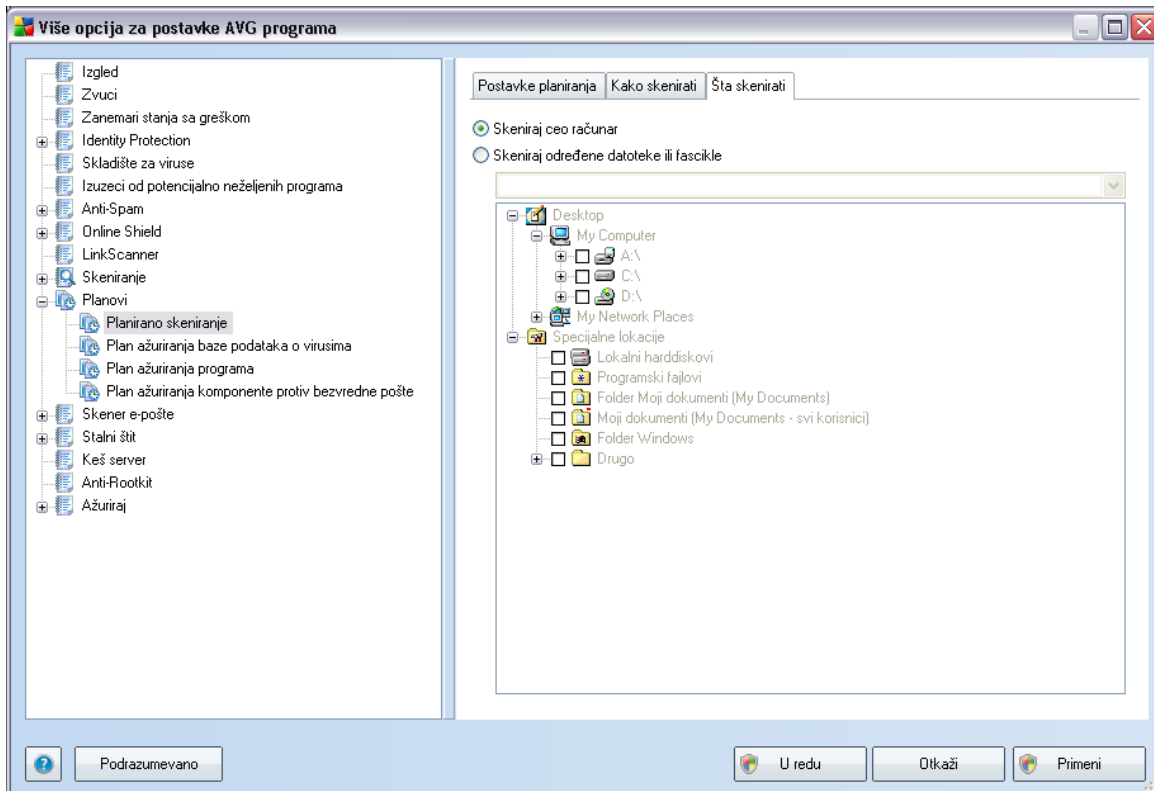
Kliknite na link **Podešavanje dodatnih izveštaja o skeniranju ...** da biste otvorili samostalan dijalog po imenu **Izveštaji skeniranja** u kojem možete označiti nekoliko stavki kako biste definisali koji će se rezultati prijavljivati:



Kliknite na **Dodatna podešavanja skeniranja ...** da biste otvorili novi dijalog **Opcije**

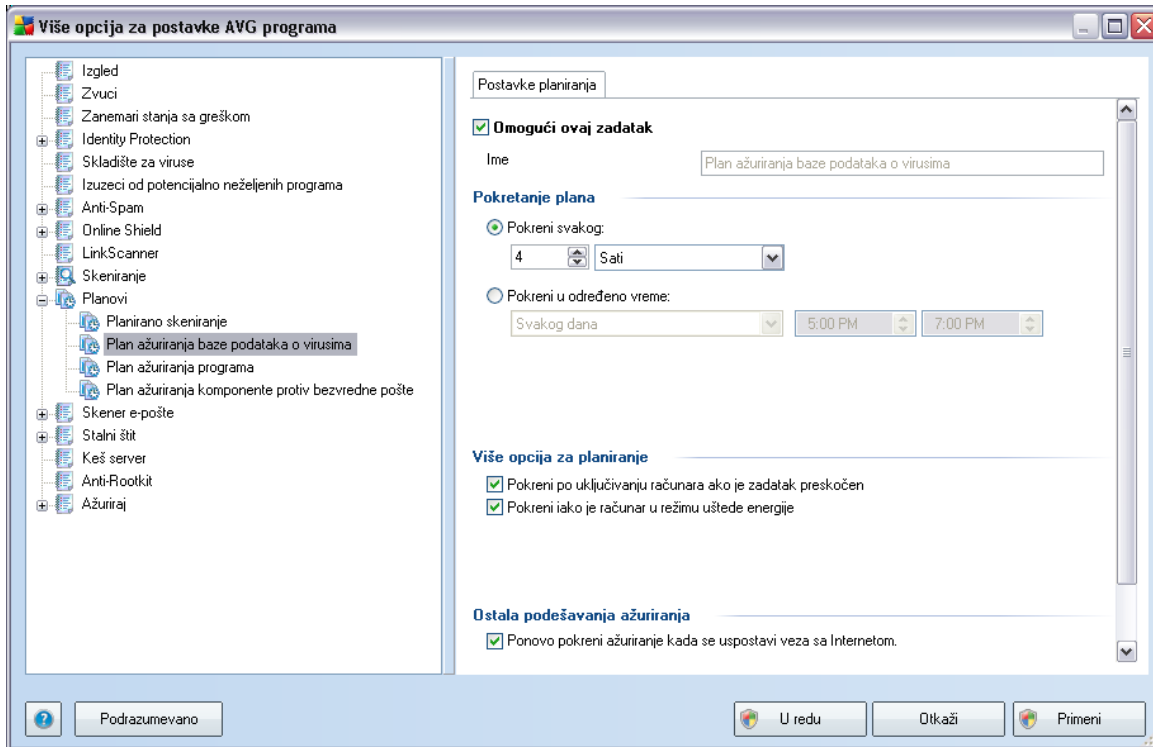
za isključivanje računara u kojem možete izabrati da li će se računar automatski isključiti nakon što se pokrenuto skeniranje završi. Ako potvrdite ovu opciju (**Isključi računar nakon završetka skeniranja**), aktivirace se nova opcija koja omogućava da se računar isključi čak i ako je trenutno zaključan (**Prinudno isključi računar ako je zaključan**).





Na kartici **Šta skenirati**, možete definisati da li želite da zakažete [skeniranje celog računara](#) ili [skeniranje određenih datoteka ili fascikli](#). Ako izaberete skeniranje određenih datoteka ili fascikli, aktivirace se struktura stabla u donjem delu dijaloga, pa možete navesti koje fascikle želite da skenirate.

10.9.2. Plan ažuriranja baze podataka o virusima



Na kartici **Podešavanja planiranja** možete prvo oznaciti/poništi izbor stavke **Omogući ovaj zadatak** da biste jednostavno deaktivirali zakazano ažuriranje baze podataka o virusima, a kasnije ga možete uključiti po potrebi. Osnovno planiranje ažuriranja baze podataka o virusima moguće je obaviti unutar komponente **Upravljanje ažuriranjem**. U ovom dijalogu možete podesiti neke detaljne parametre planiranja ažuriranja baze podataka o virusima. U tekstualnom polju **Ime** (*deaktivirano za sve podrazumevane planove*) nalazi se ime koje je prodavac programa dodelio ovom planu.

Pokretanje plana

U ovom odeljku navedite vremenski interval za pokretanje novog planiranog ažuriranja baze podataka o virusima. Tajming je moguće definisati uzastopnim pokretanjem ažuriranja nakon određenog vremenskog perioda (**Pokreni svakih ...**) ili definisanjem tačnog datuma i vremena (**Pokreni u određeno vreme ...**).

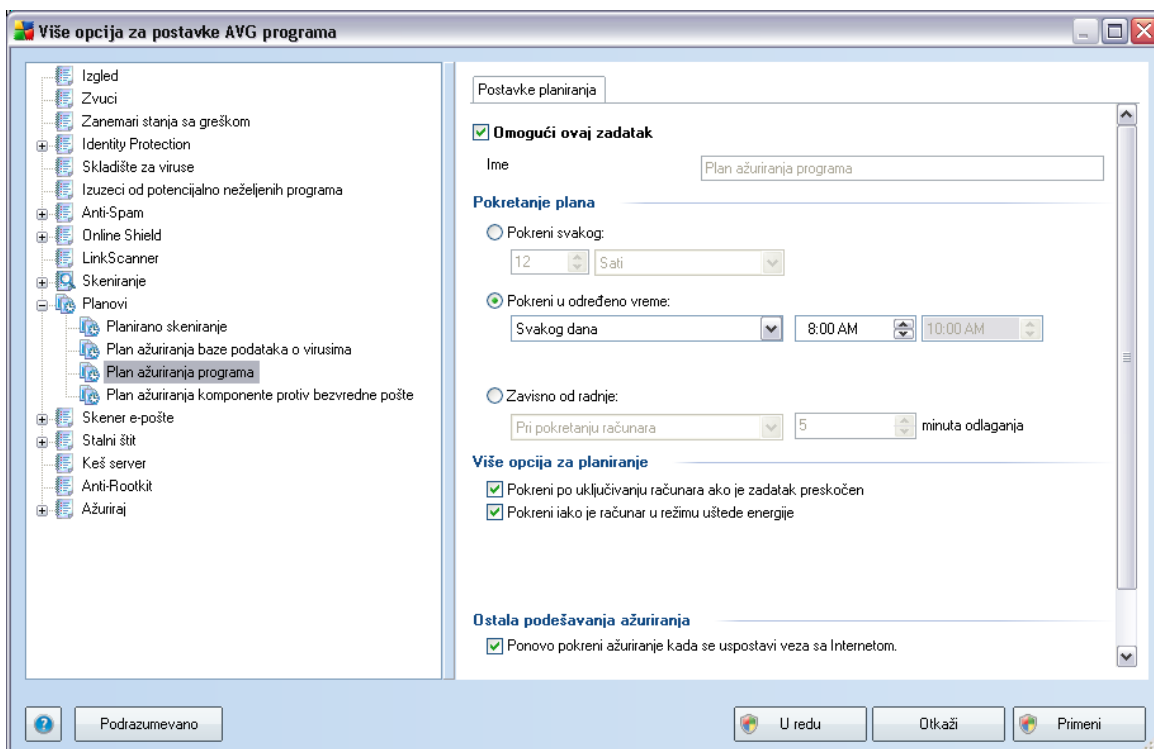
Više opcija za planiranje

U ovom odeljku možete da definišete pod kojim se okolnostima pokrece/ne pokrece ažuriranje baze podataka o virusima ako je racunar u režimu niske potrošnje energije ili je potpuno iskljucen.

Ostala podešavanja ažuriranja

Na kraju proverite opciju **Ponovo pokreni ažuriranje cim se uspostavi veza sa Internetom** da biste bili sigurni da ce, ako dode do prekida procesa ažuriranja usled prekida veze sa Internetom, taj proces biti odmah ponovo pokrenut nakon ponovnog uspostavljanja veze sa Internetom.

Kada se pokrene planirano skeniranje u navedenom vremenskom periodu, bicete obavешteni putem iskacuceg prozora koji se otvorio iznad [AVG ikone na sistemskoj paleti](#)(pod uslovom da niste menjali podrazumevanu konfiguraciju u dijalogu [Napredna podešavanja/Izgled](#)).



Na kartici **Podešavanja planiranja** možete prvo oznaciti/ponišiti izbor stavke



Omoguci ovaj zadatak da biste jednostavno deaktivirali zakazano ažuriranje programa, a kasnije ga možete uključiti po potrebi. U tekstualnom polju **Ime** (*deaktivirano za sve podrazumevane planove*) nalazi se ime koje je prodavac programa dodelio ovom planu.

Pokretanje plana

Ovde navedite vremenski interval za pokretanje novog planiranog ažuriranja programa. Vremenski interval je moguće definisati uzastopnim pokretanjem skeniranja nakon određenog vremenskog perioda (***Pokreni svakih ...***), definisanjem tačnog datuma i vremena (***Pokreni u određeno vreme ...***) ili definisanjem događaja sa kojim bi trebalo povezati pokretanje skeniranja (***Radnja zasnovana na pokretanju računara***).

Više opcija za planiranje

U ovom odeljku možete da definišete pod kojim se okolnostima pokrece/ne pokrece ažuriranje programa ako je računar u režimu niske potrošnje energije ili je potpuno isključen.

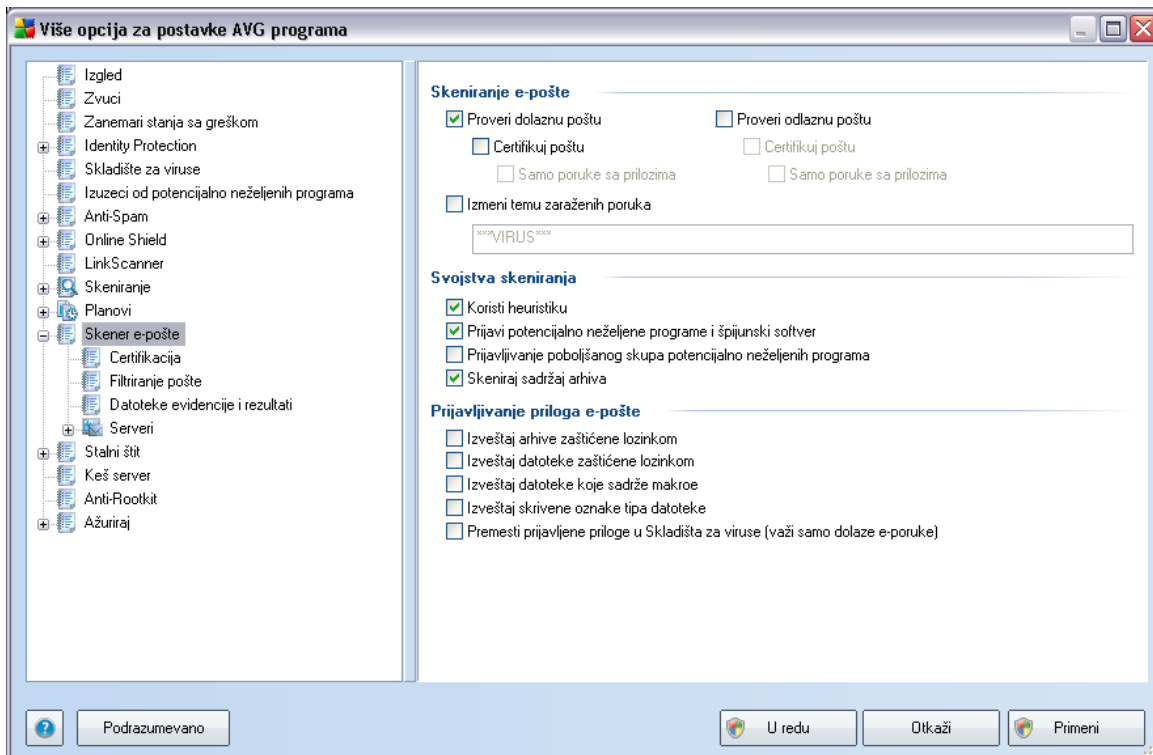
Ostala podešavanja ažuriranja

Izaberite opciju ***Ponovo pokreni ažuriranje čim se uspostavi veza sa Internetom*** da biste bili sigurni da će, ako dođe do prekida procesa ažuriranja usled prekida veze sa Internetom, taj proces biti odmah ponovo pokrenut nakon ponovnog uspostavljanja veze sa Internetom.

Kada se pokrene planirano skeniranje u navedenom vremenskom periodu, bićete obavešteni putem iskacuceg prozora koji se otvorio iznad [AVG ikone na sistemskoj paleti](#) (pod uslovom da niste menjali podrazumevanu konfiguraciju u dijalogu [Napredna podešavanja/Izgled](#)).

Napomena: *Ako dođe do podudaranja u vremenu planiranog ažuriranja programa i planiranog skeniranja, proces ažuriranja ima veći prioritet pa će skeniranje biti prekinuto.*

10.10. Skener e-pošte



Dijalog **Skener e-pošte** podeljen je na tri odeljka:

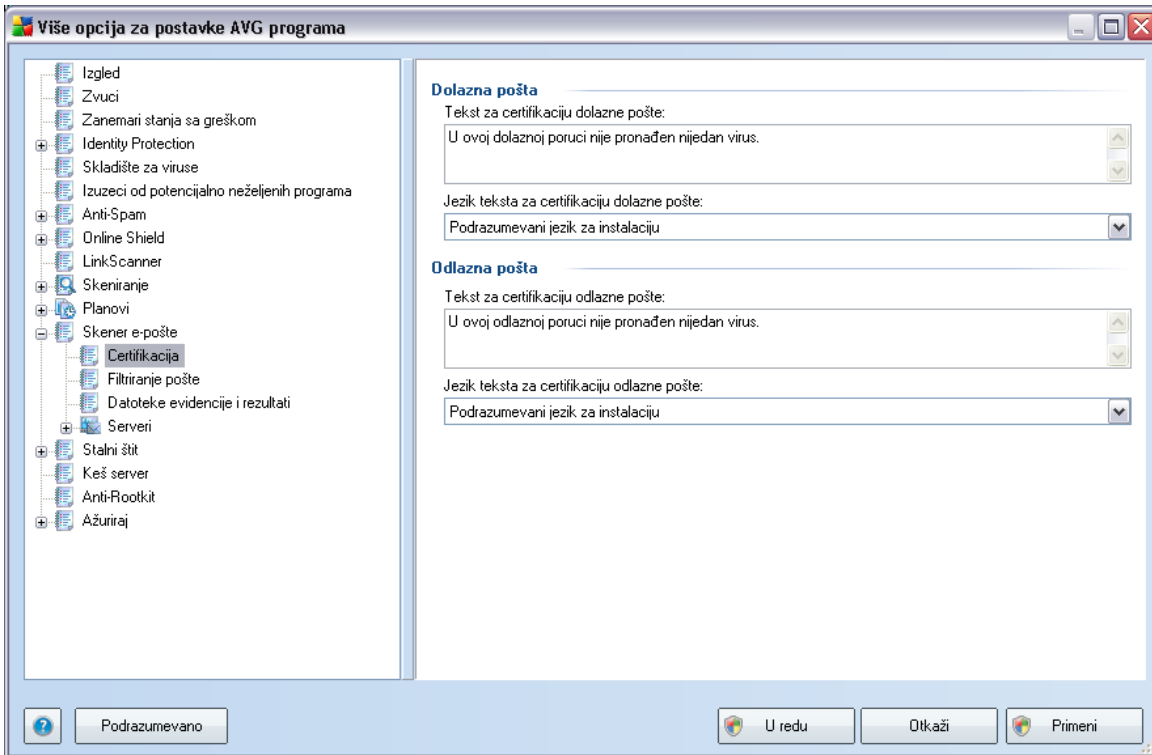
- **Skeniranje e-pošte** - u ovom odeljku možete da podesite osnovne opcije za dolazne i/ili odlazne e-poruke:
 - Da li ce se e-poruke skenirati kako bi se proverilo da li sadrže viruse.
 - Da li ce se na kraju svake poruke nalaziti tekst za certifikaciju kojim se potvrđuje da u poruci nema virusa. Tekst možete da prilagodite u dijalogu [Certifikacija](#).
 - Da li ce se tekst za certifikaciju dodavati samo porukama koje sadrže priloge.

Da biste **Izmenili temu zaraženih poruka**, izaberite ovo polje i unesite željenu vrednost u tekstualno polje. Uneti tekst ce se dodavati u polje za temu svake zaražene e-poruke radi lakše identifikacije i filtriranja. Podrazumevana vrednost je *****VIRUS*****, a mi vam preporučujemo da je ne menjate.

- **Svojstva skeniranja** - u ovom odeljku možete da odredite način skeniranja e-poruka:
 - **Koristi heuristiku** – potvrdite izbor u ovom polju za potvrdu [da biste koristili metod detekcije putem heuristicke analize](#) tokom skeniranja e-poruka. Ako je ova opcija uključena, priloge e-poruka možete filtrirati ne samo po oznaci tipa, već i po stvarnom sadržaju priloga. Filtriranje se može podesiti u dijalogu [Filtriranje pošte](#).
 - **Prijavi potencijalno neželjene programe i špijunski softver** - (*podrazumevano je uključeno*): potvrdite izbor u ovom polju za potvrdu da biste aktivirali **Antispajver** mehanizam i obavili skeniranje u potrazi za špijunskim programima i virusima. [Špijunski softver](#) se ne može sa sigurnošću svrstati u kategoriju malvera: Iako obično predstavlja bezbednosni rizik, neki od ovih programa mogu se bezbedno instalirati na računar. Preporučujemo vam da ova funkcija bude uključena jer povećava bezbednost računara.
 - **Prijavi poboljšani skup potencijalno neželjenih programa** – ako je prethodna opcija aktivirana, takođe možete da potvrdite izbor u ovom polju za potvrdu kako bi se detektovao poboljšani skup [špijunskih programa](#): programi koji su potpuno bezbedni kada ih kupite od proizvođača, ali koji se kasnije mogu iskoristiti u zlonamerne svrhe. Ovo je dodatna mera kojom se bezbednost računara poboljšava još više. Međutim, zbog toga što postoji mogućnost blokiranja legalnih programa, ova opcija je podrazumevano isključena.
 - **Skeniraj unutar arhiva** – potvrdite izbor u polju za potvrdu ako želite da skenirate sadržaj arhiva priloženih e-porukama.
- **Prijavlivanje priloga e-pošte** - u ovom odeljku možete podesiti opcije za kreiranje dodatnih izveštaja o potencijalno opasnim ili sumnjivim datotekama. Imajte u vidu da se neće prikazati dijalog sa upozorenjem, već će na kraju poruke samo biti dodat tekst za certifikaciju, a svi izveštaji te vrste biće navedeni na listi u dijalogu [Detekcija od strane skenera e-pošte](#):
 - **Prijavi archive zaštićene lozinkom** – archive (ZIP, RAR itd.) zaštićene lozinkom ne mogu se skenirati da bi se proverilo da li sadrže viruse; označite ovo polje da bi ih program prijavljivao kao potencijalno opasne.
 - **Prijavi dokumente zaštićene lozinkom** - dokumenti zaštićeni lozinkom ne mogu se skenirati da bi se proverilo da li sadrže viruse; označite ovo polje da bi ih program prijavljivao kao potencijalno opasne.

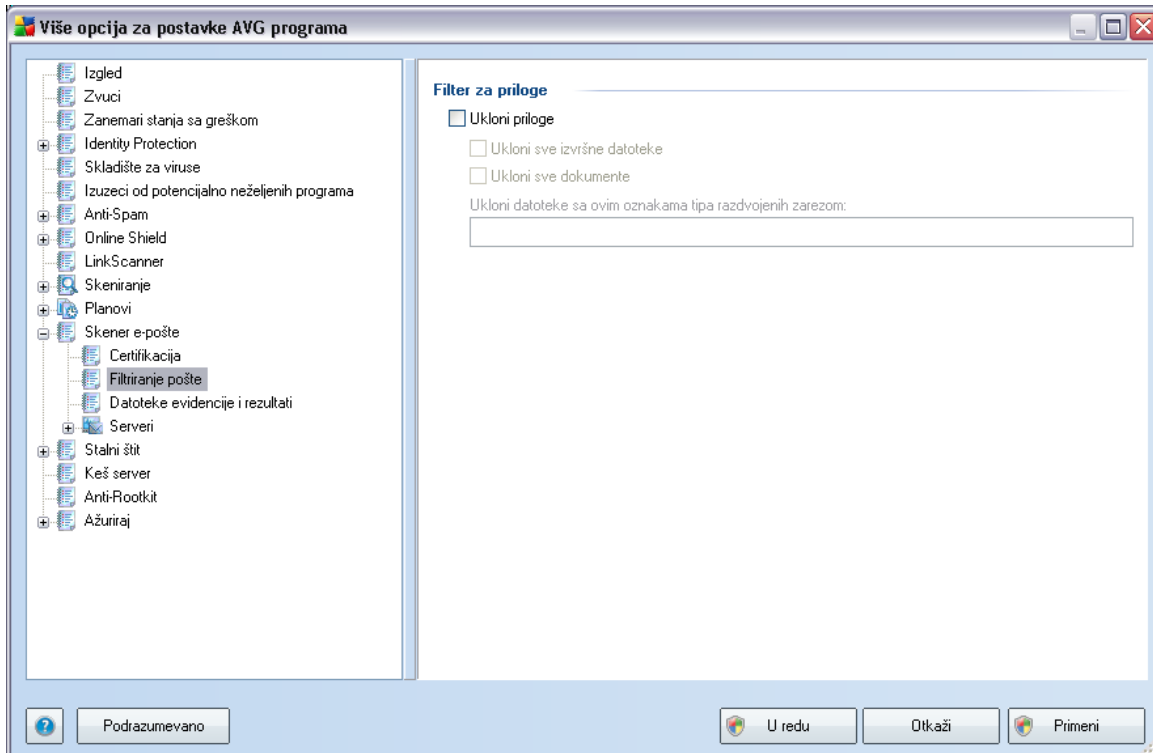
- **Prijavi datoteke koje sadrže makroe** - makro je unapred definisan niz koraka za lakše obavljanje određenih zadataka od strane korisnika (poznati su makroi iz programa MS Word). Kao takvi, makroi mogu sadržati potencijalno opasne instrukcije, pa ćete možda želeći da označite ovo polje kako biste bili sigurni da će datoteke sa makroima biti prijavljene kao sumnjive.
- **Prijavi skrivene oznake tipa datoteke** – skrivene oznake tipa mogu učiniti da npr. sumnjiva izvršna datoteka „nešto.txt.exe“ izgleda kao neškodljiva datoteka u formatu čistog teksta „nešto.txt“; označite ovo polje da bi ih program prijavljivao kao potencijalno opasne.
- **Premesti prijavljene priloge u skladište za viruset** - navedite da li želite da dobijate obaveštenja putem e-pošte o arhivama i dokumentima koji su zaštićeni lozinkom, makroima koji sadrže datoteke i/ili datotekama sa skrivenim oznakama tipa koje su otkrivene u prilogu skenirane e-poruke. Ako takva poruka bude otkrivena tokom skeniranja, definišite da li želite da li želite da premestite takav zaraženi objekat u [Skladište za viruse](#).

10.10.1. Sertifikacija



U dijalogu **Sertifikacija** možete navesti tekst i jezik sertifikacione poruke. Ova stavka se odvojeno podešava za **Dolaznu poštu** i **Odlaznu poštu**.

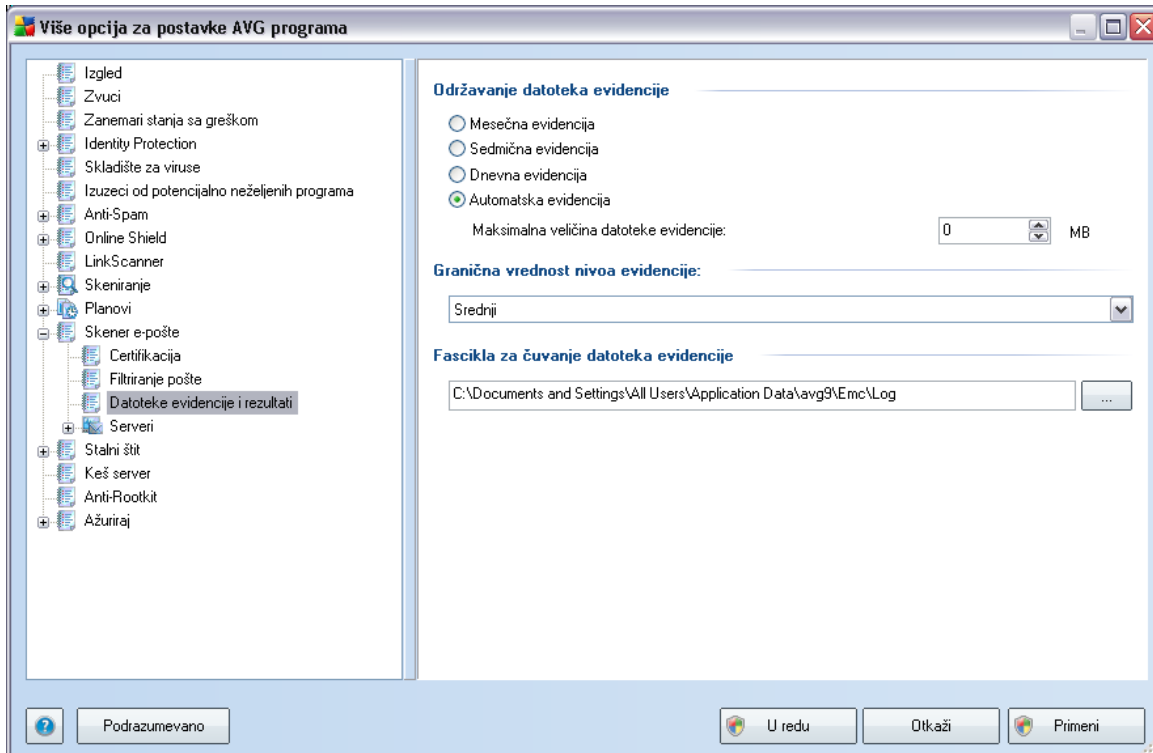
10.10.2. Filtriranje pošte



Dijalog **Filter za priloge** omogućava vam da podesite parametre za skeniranje priloga e-poruka. Podrazumevano, opcija **Ukloni priloge** je isključena. Ako odlucite da je aktivirate, svi prilozi e-poruka koji se prepoznaju kao zarazni ili potencijalno opasni bice automatski uklonjeni. Ako želite da definišete koji ce se tip priloga uklanjati, izaberite željenu opciju:

- **Ukloni sve izvršne datoteke** - sve *.exe datoteke se brišu
- **Ukloni sve dokumente** - bice izbrisane sve datoteke tipa *.doc, *.docx, *.xls, *.xlsx
- **Ukloni datoteke sa sledecim oznakama tipa datoteke razdvojenih zarezima** - uklanjanje svih datoteka sa definisanim oznakama tipa datoteke

10.10.3. Datoteke evidencije i rezultati

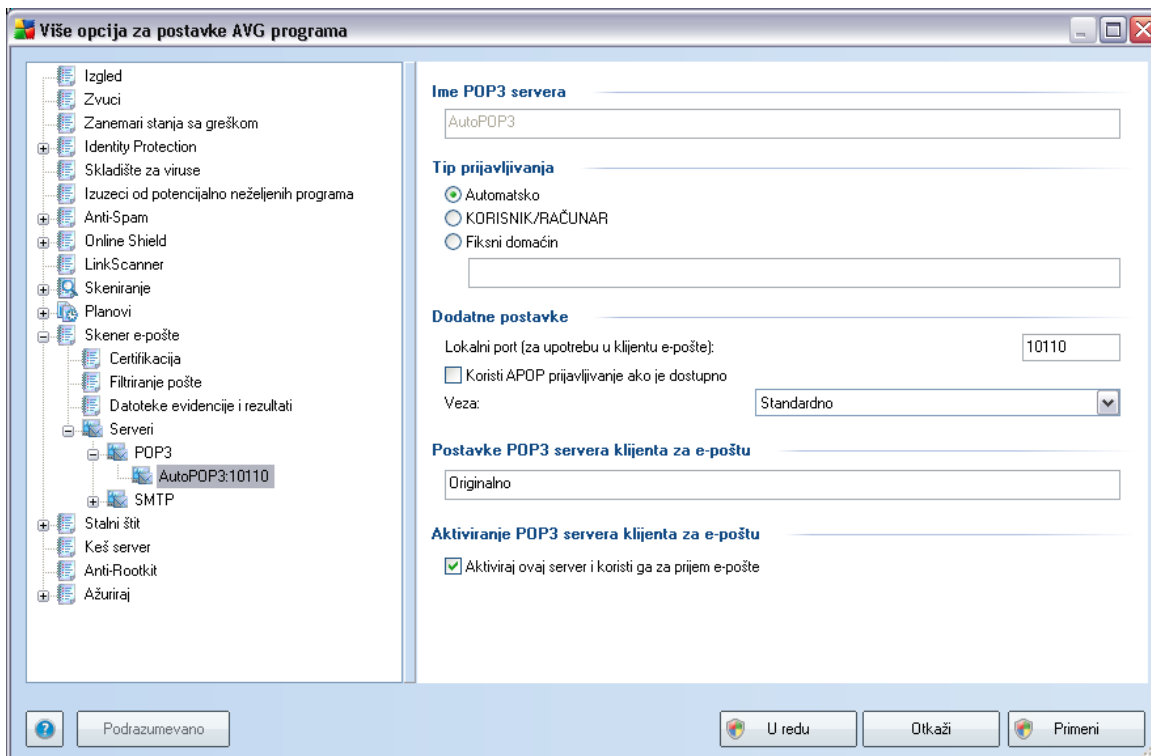


Dijalog koji se otvara ako kliknete na stavku za navigaciju **Datoteke evidencije i rezultati** omogućava vam da definišete parametre za održavanje rezultata skeniranja e-pošte. Ovaj dijalog je podeljen na nekoliko odeljaka:

- **Održavanje datoteka evidencije** - definišete da li želite da se informacije o skeniranju e-pošte evidentiraju svakodnevno, jednom nedeljno, jednom mesечно, ... ; možete definisati i maksimalnu veličinu datoteke evidencije (*u MB*)
- **Granična vrednost nivoa evidencije** - podrazumevano je izabran srednji nivo - možete izabrati niži nivo (*evidentiranje osnovnih informacija o vezi*) ili viši nivo (*evidentiranje svog saobraćaja*)
- **Fascikla za čuvanje datoteka evidencije** - definišete lokaciju datoteke evidencije

10.10.4. Serveri

U odeljku **Serveri** možete urediti parametre servera komponente **Skener e-pošte**, a možete podesiti i novi server pomocu dugmeta **Dodaj novi server**.

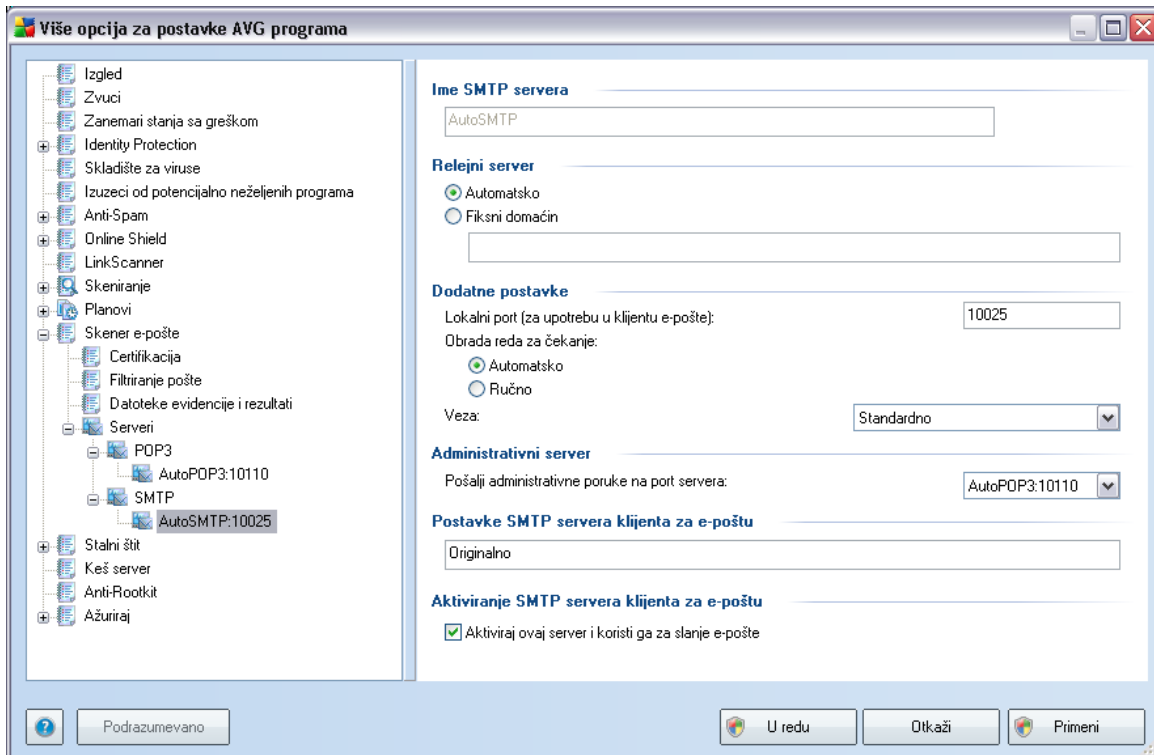


U ovom dijalogu (koji se otvara preko stavke **Serveri / POP3**) možete podesiti nov server za **Skener e-pošte** pomocu POP3 protokola za dolaznu e-poštu:

- **Ime POP3 servera** - unesite ime servera ili zadržite podrazumevano AutoPOP3 ime
- **Tip prijavljivanja** - definiše način određivanja servera za poštu koji se koristi za dolazne e-poruke:
 - **Automatski** - prijavljivanje se obavlja automatski u skladu sa podešavanjima klijenta e-pošte.
 - **KORISNIK/RACUNAR** - najjednostavniji i najčešći metod za utvrđivanje određiškog servera pošte jeste proxy metod. Da biste koristili ovaj metod,

navedite ime ili adresu (ili i port) kao deo korisnickog imena za prijavljivanje za dati server pošte, razdvajajući ih znakom /. Na primer, za nalog korisnik1 na serveru pop.acme.com i portu 8200 koristice korisnik1/pop.acme.com:8200 kao ime za prijavljivanje.

- **Fiksni host** - u ovom slucaju, program ce uvek koristiti server koji je ovde naveden. Navedite adresu ili ime svog servera za poštu. Korisnicko ime ostaje nepromenjeno. Kao ime možete da koristite ime domena (na primer, pop.acme.com), kao i IP adresu (na primer, 123.45.67.89). Ako server za poštu koristi port koji nije standardan, možete da navedete ovaj port iza imena servera koristeći dvotacku kao znak za razgranicavanje (na primer, pop.acme.com:8200). Standardni port za POP3 komunikaciju jeste 110.
- **Dodatna podešavanja** - definisanje dodatnih parametara:
 - **Lokalni port** - određuje port na kojem treba očekivati komunikaciju aplikacije za e-poštu. Zatim morate da u aplikaciji za poštu navedete ovaj port kao port za POP3 komunikaciju.
 - **Koristi APOP kada je dostupno** - ova opcija obezbeduje bezbednije prijavljivanje na server za poštu. Ovo osigurava da **Skener e-pošte** koristi alternativni metod prosledivanja lozinke korisnickog naloga za prijavljivanje, šaljući lozinku serveru ne u otvorenom, vec u šifrovanom obliku koristeći promenljivi lanac dobijen od servera. Naravno, ova funkcija je dostupna samo ako je odredišni server za poštu podržava.
 - **Veza** - u padajucem meniju možete da izaberete vrstu veze koju želite da koristite (standardna/SSL/SSL podrazumevana). Ako odaberete SSL vezu, podaci koji se šalju bice šifrovani bez rizika da ih neko drugi može pratiti ili nadgledati. Ova funkcija je takode dostupna samo ako je odredišni server za poštu podržava.
- **Postavke POP3 servera klijenta e-pošte** - sadrži kratke informacije o postavkama za konfiguraciju koje su potrebne za ispravno konfigurisanje klijenta e-pošte (tako da **skener e-pošte** proverava svu dolaznu poštu). Ovo je rezime zasnovan na odgovarajucim parametrima navedenim u ovom dijalogu i drugim srodnim dijalozima.
- **Aktiviranje POP 3 servera klijenta e-pošte** - potvrdite/opozovite izbor u ovom polju za potvrdu da biste aktivirali ili deaktivirali izabrani POP3 server



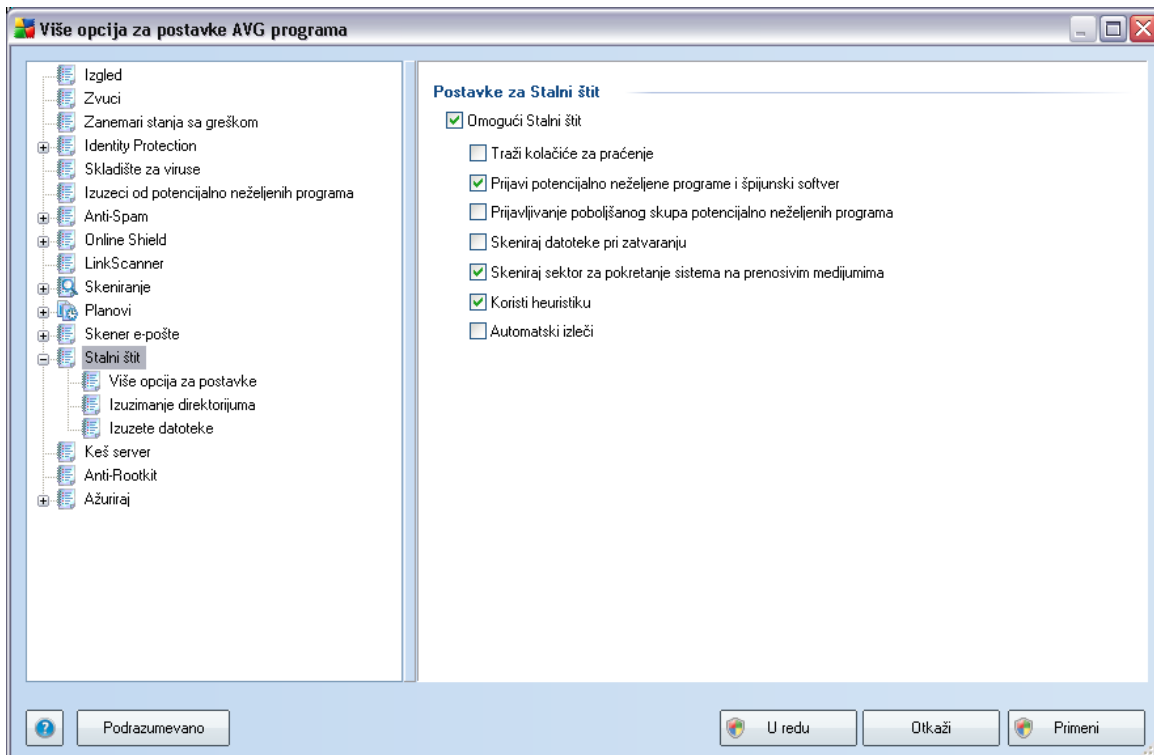
U ovom dijalogu (koji otvarate preko stavke **Serveri / SMTP**) možete podesiti novi server za **Skener e-pošte** pomoću SMTP protokola za odlaznu poštu:

- **Ime SMTP servera** – unesite ime servera ili zadržite podrazumevano AutoSMTP ime
- **Relejni server**– definiše način određivanja servera za e-poštu koji će se koristiti za odlaznu poštu:
 - **Automatski** - prijavljivanje se obavlja automatski, u skladu sa postavkama klijenta e-pošte
 - **Fiksni host** - u ovom slučaju, program će uvek koristiti server koji je ovde naveden. Navedite adresu ili ime svog servera za poštu. Kao ime možete da koristite ime domena (na primer, smtp.acme.com), kao i IP adresu (na primer, 123.45.67.89). Ako server za poštu koristi port koji nije standardan, možete da unesete ovaj port iza imena servera, koristeći dvotacku kao znak za razgranicavanje (na primer, smtp.acme.com:8200). Standardni port za SMTP komunikaciju je 25.

- **Dodatna podešavanja** - definisanje dodatnih parametara:
 - **Lokalni port** - određuje port na kojem treba očekivati komunikaciju aplikacije za e-poštu. Zatim morate da u aplikaciji za poštu navedete ovaj port kao port za komunikaciju.
 - **Obrada reda za cekanje** - određuje ponašanje komponente **Skener e-pošte** prilikom obrade uslova za slanje e-poruka:
 - Automatski - odlazna pošta se odmah isporučuje (šalje) određenom serveru za poštu
 - Rucno - poruka se umeće u red za cekanje odlaznih poruka i šalje se kasnije
 - **Veza** - u ovom padajućem meniju možete da izaberete vrstu veze koju želite da koristite (standardna/SSL/SSL podrazumevana). Ako odaberete SSL vezu, podaci koji se šalju bice šifrovani bez rizika da ih neko drugi može pratiti ili nadgledati. Ova funkcija je dostupna samo ako je određeni server za poštu podržava.
- **Administrativni server** - prikazuje broj porta servera koji ce se koristiti za inverznu isporuku administrativnih izveštaja. Na primer, ove poruke se generišu kada određeni server za poštu odbije odlaznu poruku ili kada taj server za poštu nije dostupan.
- **Podešavanja SMTP servera klijenta e-pošte** - sadrži informacije o tome kako se konfigurise klijentska aplikacija za poštu tako da se odlazne poruke proveravaju pomocu trenutno izmenjenog servera za proveru odlazne pošte. Ovo je rezime zasnovan na odgovarajucim parametrima navedenim u ovom dijalogu i drugim srodnim dijalogima.
- **Aktivacija SMTP servera klijenta e-pošte** - potvrdite/opozovite izbor u ovom polju za potvrdu da biste aktivirali/deaktivirali gore navedeni SMTP server

10.11. Stalni štít

Komponenta **Stalni štít** aktivno štiti datoteke i fascikle od virusa, špijuskog softvera i drugog zlonamernog softvera.



U dijalogu **Podešavanja stalnog štita** možete aktivirati ili deaktivirati **Stalni štít** tako što ćete potvrditi/opozvati izbor u polju za potvrdu **Omogući Stalni štít** (*ova opcija je podrazumevano uključena*). Takođe, možete izabrati funkcije **Stalnog štita** koje bi trebalo aktivirati:

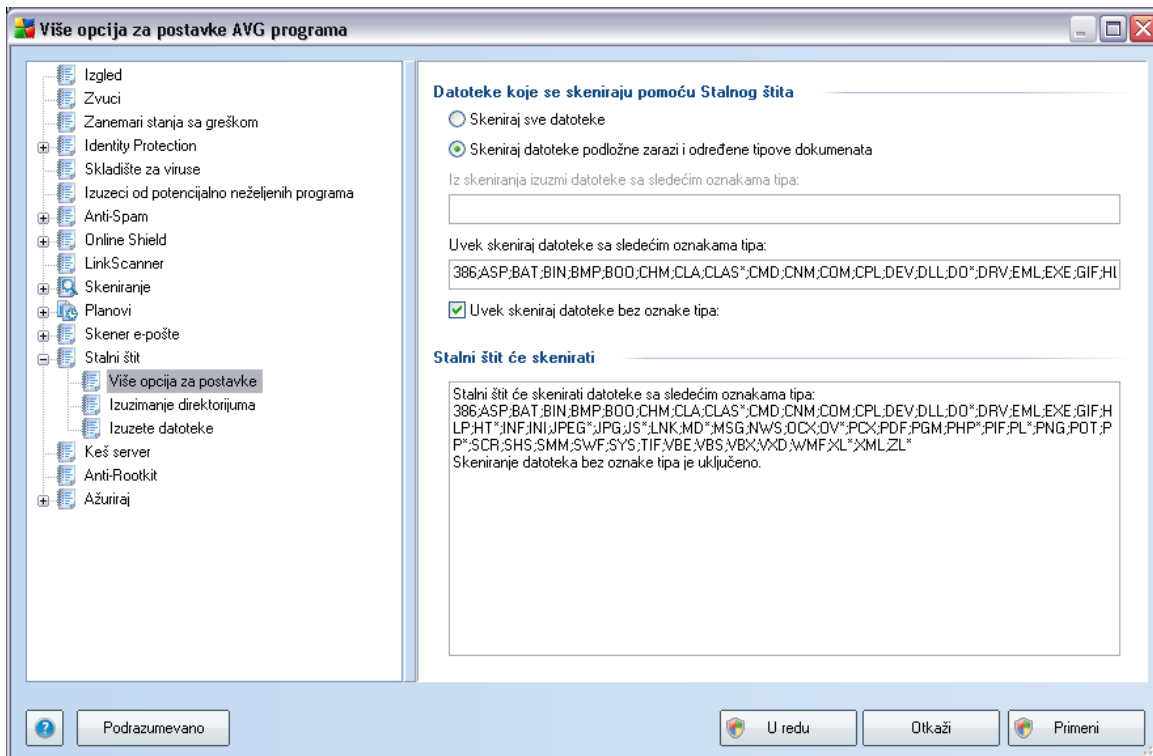
- **Traži kolacice za praćenje** - pomoću ovog parametra definiše se da bi tokom skeniranja trebalo otkrivati kolacice. (*HTTP kolacici služe za proveru identiteta, praćenje i održavanje određenih informacija o korisnicima, kao što su željene opcije za lokaciju ili sadržaj elektronskih kolica za kupovinu*)
- **Prijavi potencijalno neželjene programe i špijunski softver** - (*podrazumevano je uključeno*): potvrdite izbor u ovom polju za potvrdu da biste aktivirali **Antispajver** mehanizam i obavili skeniranje u potrazi za špijunskim programima i virusima. **Špijunski softver** se ne može sa sigurnošću svrstati u kategoriju malvera: Iako obično predstavlja bezbednosni rizik, neki od ovih

programa mogu se bezbedno instalirati na racunar. Preporucujemo vam da ova funkcija bude ukljucena jer povecava bezbednost racunara.

- **Prijavi poboljšani skup potencijalno neželjenih programa** – ako je prethodna opcija aktivirana, takode možete da potvrdite izbor u ovom polju za potvrdu kako bi se detektovao poboljšani skup [špijunskih programa](#): programi koji su potpuno bezbedni kada ih kupite od proizvodaca, ali koji se kasnije mogu iskoristiti u zlonamerne svrhe. Ovo je dodatna mera kojom se bezbednost racunara poboljšava još više. Medutim, zbog toga što postoji mogucnost blokiranja legalnih programa, ova opcija je podrazumevano iskljucena.
- **Skeniraj datoteke pri zatvaranju** - skeniranje po zatvaranju omogucava AVG softveru da skenira aktivne objekte (npr. aplikacije, dokumente ...) pri otvaranju i pri zatvaranju; ova funkcija pomaže u zaštiti racunara od nekih tipova složenih virusa
- **Skeniraj sektor za pokretanje sistema na prenosivim medijumima** - (*podrazumevano je ukljuceno*)
- **Koristi heuristiku** - (*podrazumevano je ukljuceno*) [heuristicka analiza](#) koristice se za otkrivanje (*dinamicke emulacije instrukcija skeniranih objekata' u virtuelnom racunarskom okruženju*)
- **Automatski izleci** - otkrivene zaraze automatski ce se lečiti ako postoji dostupan lek

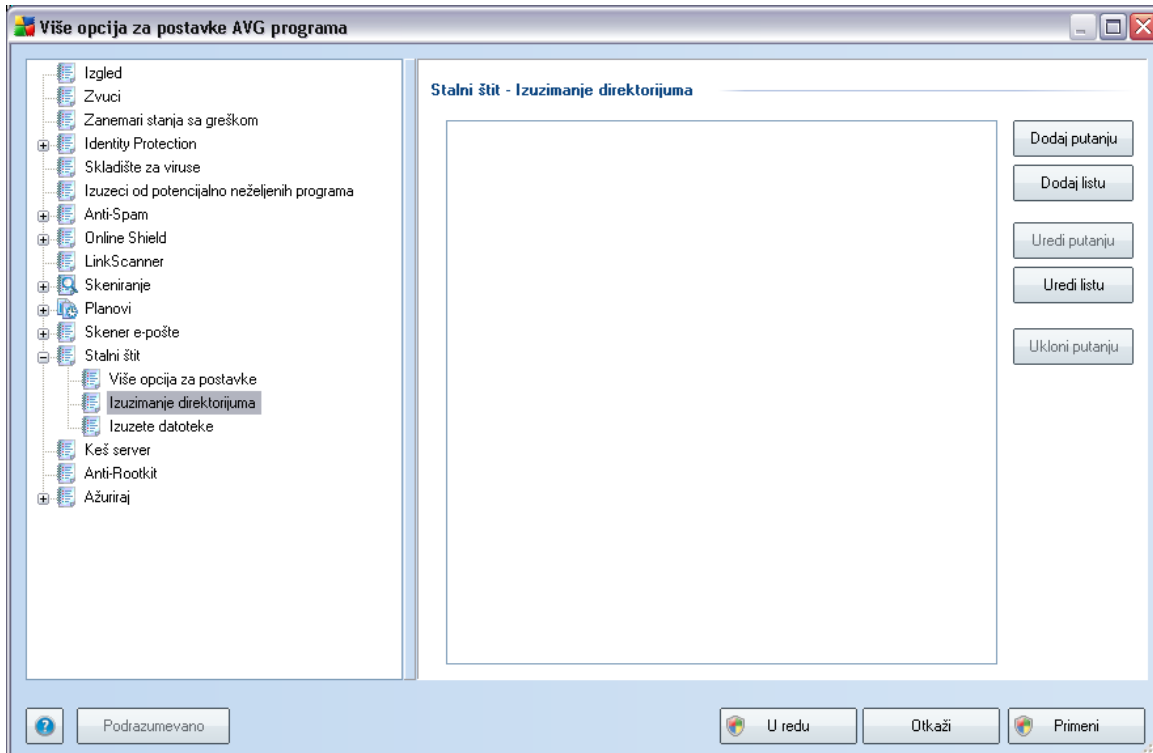
10.11.1. Napredna podešavanja

U dijalogu **Datoteke koje se skeniraju pomoću Stalnog štita** možete konfigurirati koje će se datoteke skenirati (na osnovu njihove oznake tipa):



Odlucite da li želite da se skeniraju sve datoteke ili samo datoteke podložne zarazi - dalje možete definisati listu oznaka tipa datoteke koje se neće skenirati, kao i listu oznaka tipa datoteke koje se obavezno moraju skenirati.

10.11.2. Izuzeti direktorijumi



Dijalog **Stalni štit - Izuzimanje direktorijuma** omogućava vam da definišete fascikle koje će biti izuzete iz skeniranja komponentom **Stalni štit**.

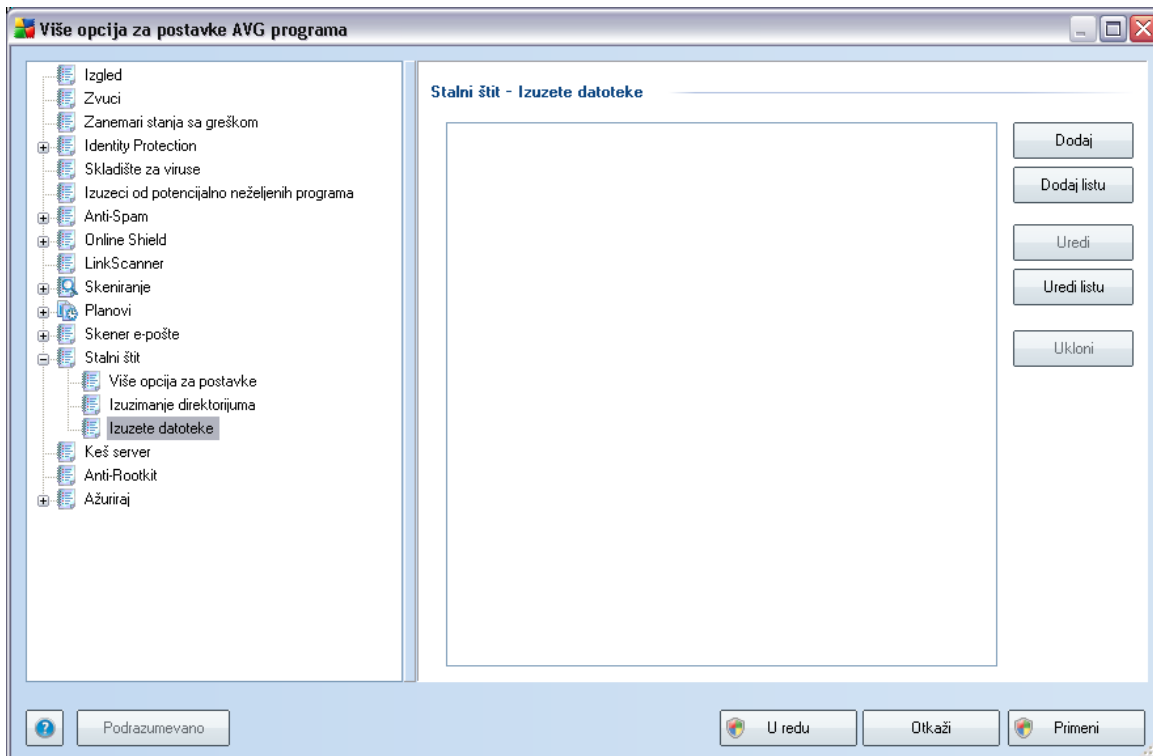
Ako nije neophodno, preporučujemo da ne izuzimate nijedan direktorijum!

Ovaj dijalog sadrži sledeću kontrolnu dugmad:

- **Dodaj putanju**– navedite direktorijume koji će biti izuzeti iz skeniranja tako što ćete sa navigacionog stabla lokalnog diska izabrati jedan po jedan direktorijum
- **Dodaj listu** – omogućava vam da unesete celu listu direktorijuma koji će biti izuzeti iz skeniranja koje vrši **Stalni štit**
- **Uredi putanju**– omogućava vam da uređujete navedenu putanju do izabrane fascikle
- **Uredi listu**–omogućava vam da uređujete listu fascikli

- **Ukloni putanju** – omogućava vam da sa liste izbrisate putanju do izabrane fascikle

10.11.3. Izuzete datoteke



Dijalog **Stalni štit - izuzete datoteke** funkcioniše na isti način kao i prethodno opisani dijalog **Stalni štit - izuzeti direktorijumi** samo što umesto fascikli sada možete definisati određene datoteke koje bi trebalo izuzeti iz skeniranja komponentom **Stalni štit**.

Preporučujemo vam da ne izuzimate nijednu datoteku ako to nije neophodno!

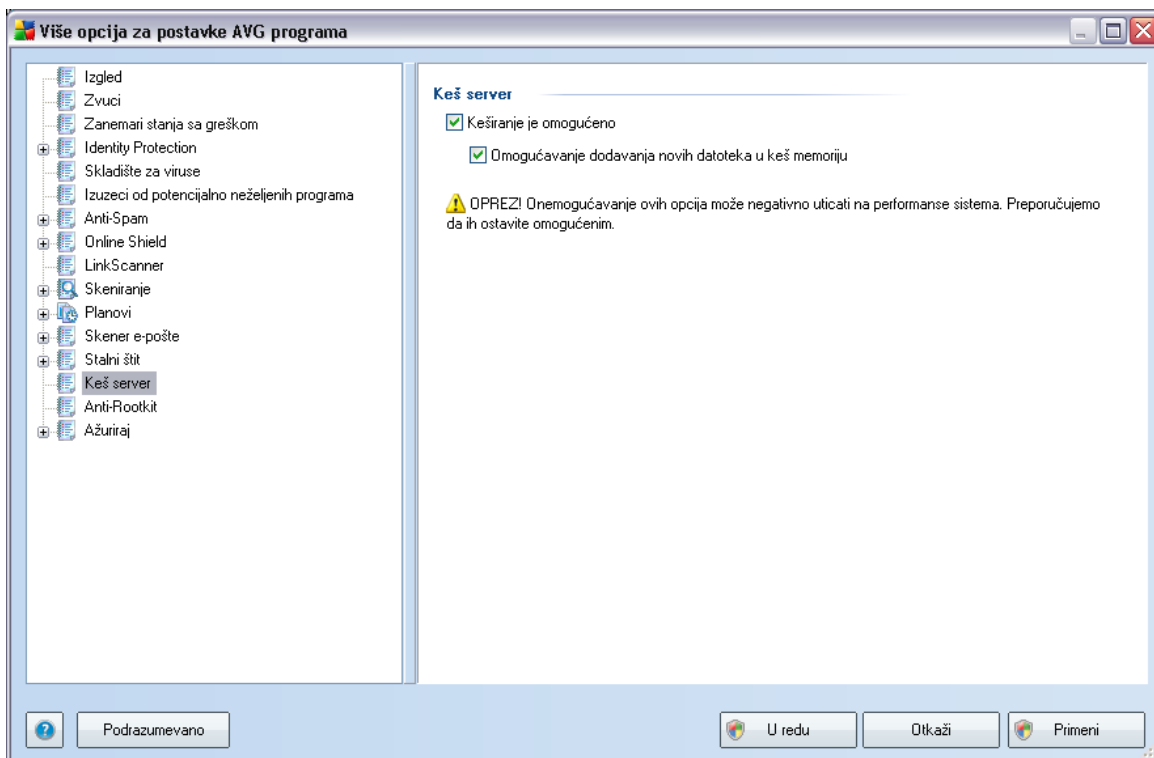
Ovaj dijalog sadrži sledeću kontrolnu dugmad:

- **Dodaj** – navedite datoteke koje će biti izuzete iz skeniranja tako što ćete sa navigacionog stabla lokalnog diska izabrati jednu po jednu datoteku
- **Dodaj listu** – omogućava vam da unesete celu listu datoteka koje će biti izuzete iz skeniranja **Stalnim štitom**

- **Uredi** – omogućava vam da uredite putanju do izabrane datoteke
- **Uredi listu** – omogućava vam da uredite listu datoteka
- **Ukloni** – omogućava vam da sa liste izbrišete putanju do izabrane datoteke

10.12. Keš server

Keš server je proces osmišljen tako da ubrza različite vrste skeniranja (*skeniranje na zahtev, planirano skeniranje celog racunara, skeniranje komponentom Stalni štit*). On prikuplja i čuva informacije o pouzdanim datotekama (*sistemskim datotekama sa digitalnim potpisom itd.*): Te datoteke se smatraju bezbednim i preskacu se tokom skeniranja.



U dijalogu za podešavanje na raspolaganju imate dve opcije:

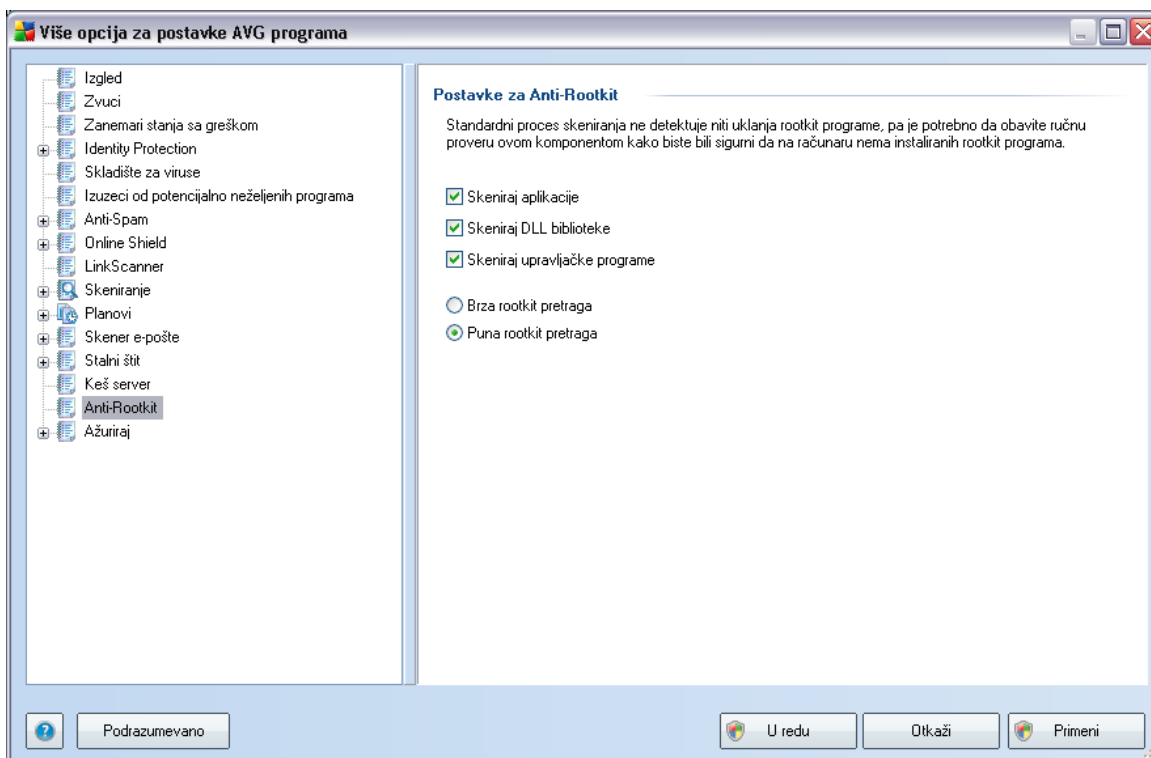
- **Keširanje je omogućeno** (*podrazumevano je uključeno*) - opozovite izbor u ovom polju za potvrdu da biste isključili **Keš server** i ispraznili keš memoriju. Imajte u vidu da će se skeniranje možda usporiti i da može doći do pada ukupnih performansi racunara jer će se svaka datoteka skenirati u potrazi za

virusima i špijunskim programima.

- **Omoguci dodavanje novih datoteka u keš memoriju** (podrazumevano je uključeno) - opozovite izbor u ovom polju za potvrdu da biste zaustavili dodavanje datoteka u keš memoriju. Datoteke koje se već nalaze u keš memoriji koriste se sve dok potpuno ne isključite keširanje ili do sledećeg ažuriranja baze podataka o virusima.

10.13. Anti-Rootkit

U ovom dijalogu možete urediti konfiguraciju komponente **Anti-Rootkit**:



Uređivanje svih funkcija komponente **Anti-Rootkit** navedenih u ovom dijalogu moguće je i direktno iz **interfejsa komponente Anti-Rootkit**.

Potvrdite izbor u odgovarajućim poljima za potvrdu da biste označili objekte koje treba skenirati:

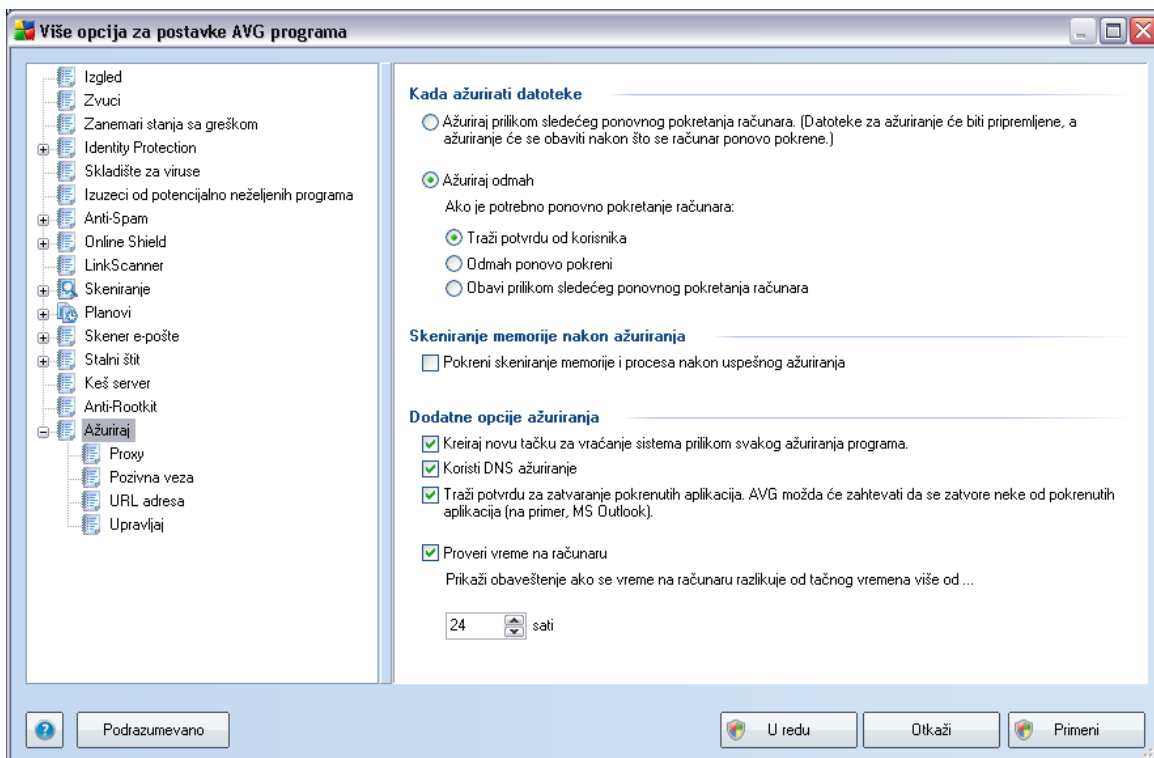
- **Skeniraj aplikacije**

- **Skeniraj DLL biblioteke**
- **Skeniraj upravljacke programe**

Zatim možete izabrati režim rootkit skeniranja:

- **Brzo rootkit skeniranje** - skeniranje svih aktivnih procesa, ucitanih upravljackih programa i sistemske fascikle (*obicno c:\Windows*)
- **Potpuno rootkit skeniranje** - skeniranje svih aktivnih procesa, ucitanih upravljackih programa, sistemske fascikle (*obicno c:\Windows*), kao i svih lokalnih diskova (*ukljucujuci fleš disk, ali izuzimajuci disketnu/CD jedinicu*)

10.14. Ažuriranje



Stavka za navigaciju **Ažuriraj** otvara novi dijalog u kojem možete definisati opšte parametre u vezi sa [ažuriranjem programa AVG](#) :

Kada ažurirati datoteke

U ovom odeljku možete izabrati jednu od dve opcije: [ažuriranje](#) se može zakazati za sledeće pokretanje racunara ili možete odmah pokrenuti [ažuriranje](#). Podrazumevano je izabrana opcija trenutnog ažuriranja pošto na taj način AVG može obezbediti maksimalan nivo bezbednosti. Odlaganje ažuriranja do sledećeg pokretanja racunara može se preporučiti samo ako ste sigurni da se racunar redovno ponovo pokrece, i to najmanje jednom dnevno.

Ako odlucite da zadržite podrazumevanu konfiguraciju i odmah pokrenete proces ažuriranja, možete definisati okolnosti pod kojim ce racunar smeti ponovo da se pokrene, ako je potrebno:

- **Traži potvrdu od korisnika** - od vas ce se tražiti da odobrite ponovno pokretanje racunara koje je potrebno da bi se [proces ažuriranja dovršio](#)
- **Odmah ponovo pokreni** - racunar ce se automatski ponovo pokrenuti nakon završetka [procesa ažuriranja](#), a vaše odobrenje neće biti potrebno
- **Obavi prilikom sledećeg ponovnog pokretanja racunara** - finalizacija procesa [ažuriranja](#) bice odložena do sledećeg pokretanja racunara - ponavljamo, imajte u vidu da se ova opcija preporučuje samo ako ste sigurni da se racunar redovno ponovo pokrece, najmanje jednom dnevno

Skeniranje memorije nakon ažuriranja

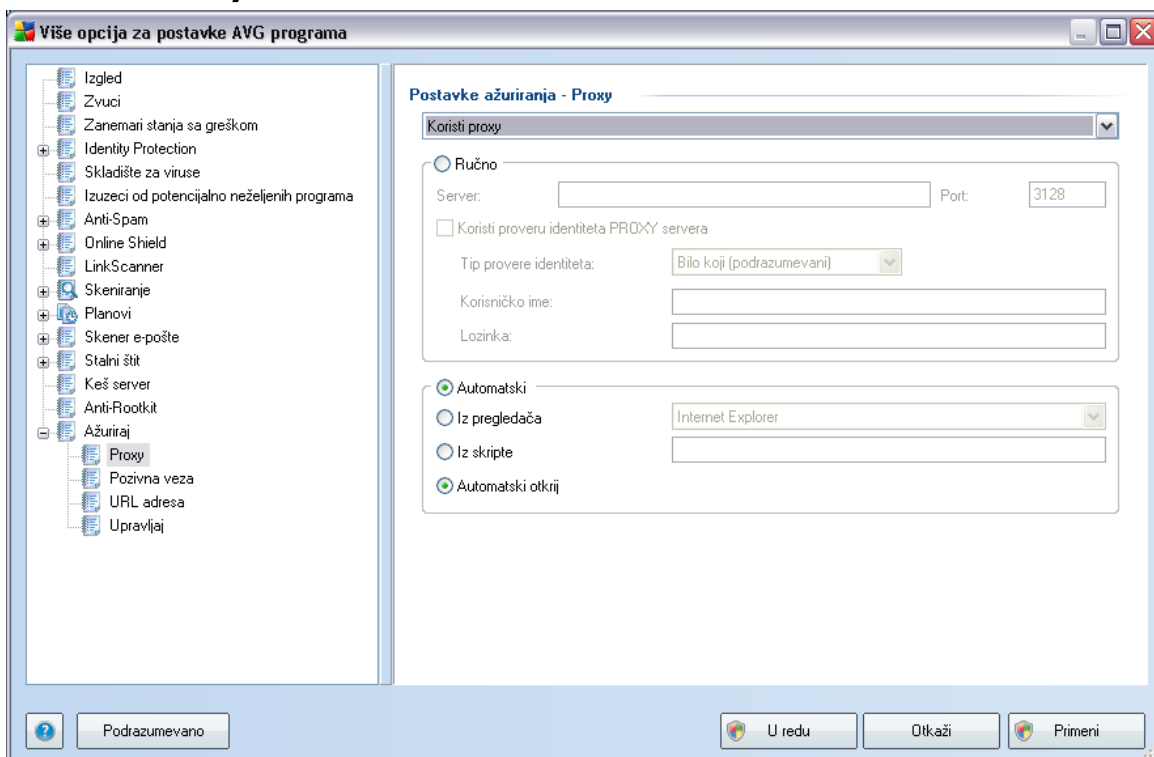
Potvrdite izbor u ovom polju za potvrdu ako želite da se novo skeniranje memorije pokrece nakon svakog uspešnog ažuriranja. Najnovija preuzeta ispravka možda sadrži nove definicije virusa i one se mogu odmah primeniti tokom skeniranja.

Dodatne opcije ažuriranja

- **Kreiraj novu tacku za vraćanje sistema nakon svakog ažuriranja** - pre svakog pokretanja ažuriranja programa AVG, kreira se tacka za vraćanje sistema. Ako proces ažuriranja ne uspe i dode do pada operativnog sistema, možete ga uvek vratiti u stanje prvobitne konfiguracije. Ovoj opciji možete pristupiti ako kliknete na Start / Svi programi / Pribor / Sistemske alatke / Oporavak sistema, ali se ne preporučuje da unosite izmene, osim ako niste iskusan korisnik! Neka ovo polje za potvrdu ostane oznaceno ako želite da koristite ovu funkciju.
- **Koristi DNS ažuriranje** - oznacite ovo polje za potvrdu da biste potvrdili da želite da koristite način detekcije datoteka za ažuriranje koji eliminiše kolicinu podataka koja se prenosi između servera za ažuriranje i AVG klijenta.

- **Traži potvrdu za zatvaranje pokrenutih aplikacija** (podrazumevano je uključeno) - izborom ove opcije bicete sigurni da AVG neće bez vašeg odobrenja zatvarati trenutno pokrenute aplikacije - ako je to potrebno da bi se završio proces ažuriranja;
- **Proveri vreme na racunaru** - oznacite ovu opciju ako želite da se prikazuje obaveštenje ako se vreme podešeno na racunaru razlikuje od tacnog vremena za više od podešenog broja sati.

10.14.1. Proxy



Proxy server je samostalni server ili usluga koja radi na racunarima i garantuje bezbedniju vezu sa Internetom. U skladu sa navedenim mrežnim pravilima, možete da pristupite Internetu direktno ili preko proxy servera. Obe mogućnosti takode mogu da budu istovremeno dozvoljene. Zatim u prvoj stavki u dijalogu **Podešavanja ažuriranja - Proxy** iz padajućeg menija morate da izaberete jednu od sledećih opcija:

- **Koristi proxy**
- **Ne koristi proxy server** - podrazumevano podešavanje

- **Pokušaj da uspostaviš vezu pomocu proxy servera. U slucaju neuspeha, uspostavi vezu direktno**

Ako izaberete neku opciju koja podrazumeva upotrebu proxy servera, moracete da unesete dodatne podatke. Podešavanje servera moguće je podesiti ručno ili automatski.

Ručno podešavanje

Ako izaberete ručno podešavanje (uključite opciju **Ručno da biste aktivirali odgovarajući odeljak dijaloga**) morate podesiti sledeće stavke:

- **Server** – navedite IP adresu servera ili ime servera
- **Port**– navedite broj porta koji omogućava pristup Internetu (*po podrazumevanoj vrednosti, ovaj broj je podešen na 3128, ali se može drugačije postaviti– obratite se administratoru mreže ako niste sigurni*)

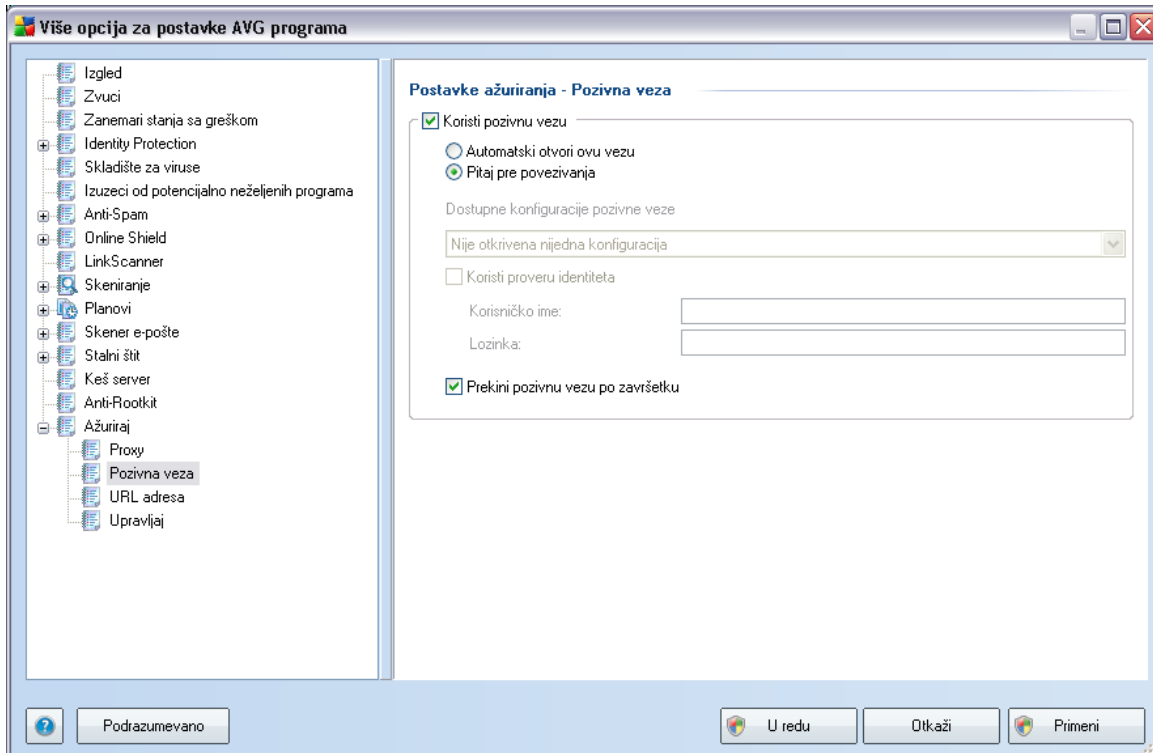
Proxy server takode može da ima konfigurisana određena pravila za svakog korisnika. Ako je vaš proxy server podešen na ovaj način, uključite opciju **Koristi proveru identiteta PROXY servera** da biste proverili da li su vaše korisničko ime i lozinka važeći za povezivanje na Internet pomocu proxy servera.

Automatsko podešavanje

Ako izaberete automatsko podešavanje (*uključite opciju **Automatski da biste aktivirali odgovarajući odeljak dijaloga***), a zatim izaberite odakle bi trebalo preuzeti konfiguraciju proxy servera:

- **Iz pregledaca** - konfiguracija će biti preuzeta iz podrazumevanog Internet pregledaca
- **Iz skripte** - konfiguracija će biti preuzeta iz preuzete skripte koja sadrži funkciju davanja adrese proxy servera
- **Automatski otkrij** - konfiguracija će biti automatski otkrivena direktno sa proxy servera

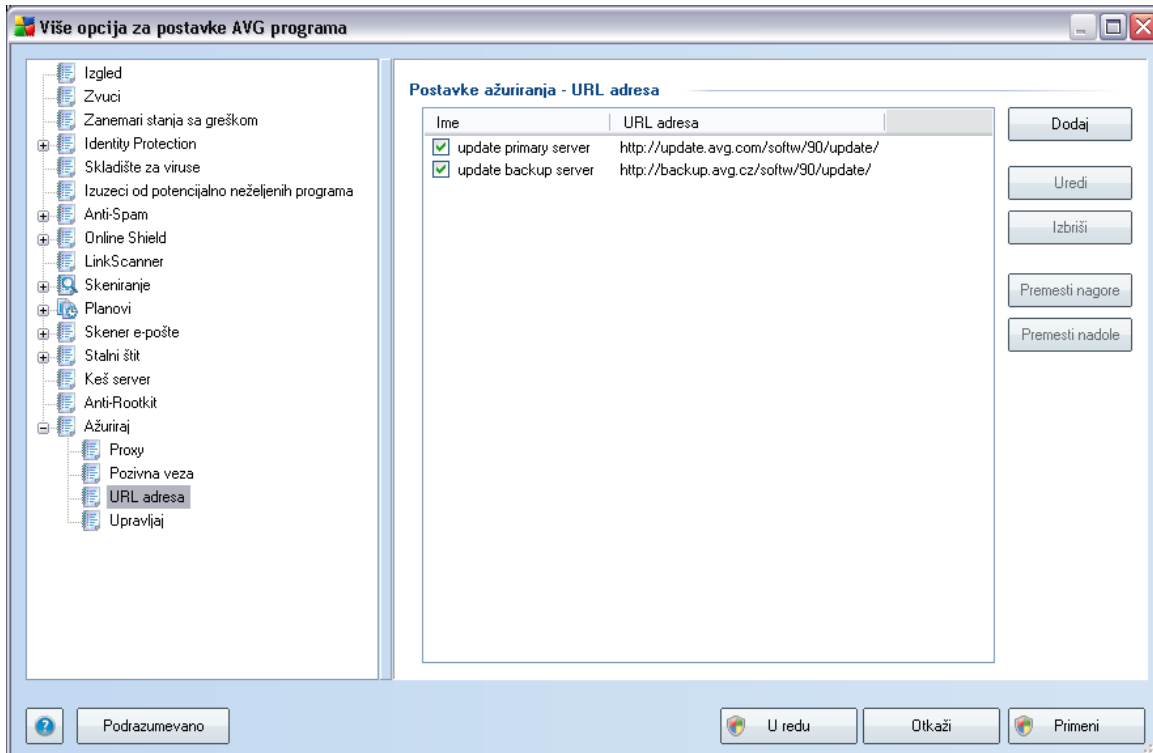
10.14.2. Pozivna veza



Svi parametri koji su opcionalno definisani u dijalogu **Postavke ažuriranja - Pozivna veza** odnose se na pozivnu vezu sa Internetom. Polja na kartici nisu aktivna dok ne označite opciju **Koristi pozivne veze** koja aktivira polja.

Navedite da li želite da se automatski povežete sa Internetom (**Automatski otvori ovu vezu**) ili želite da svaki put ručno potvrdite vezu (**Pitaj pre povezivanja**). Kod automatskog povezivanja, potrebno je još da izaberete da li će se veza prekidati nakon završetka ažuriranja (**Prekini pozivnu vezu po završetku**).

10.14.3. URL adresa

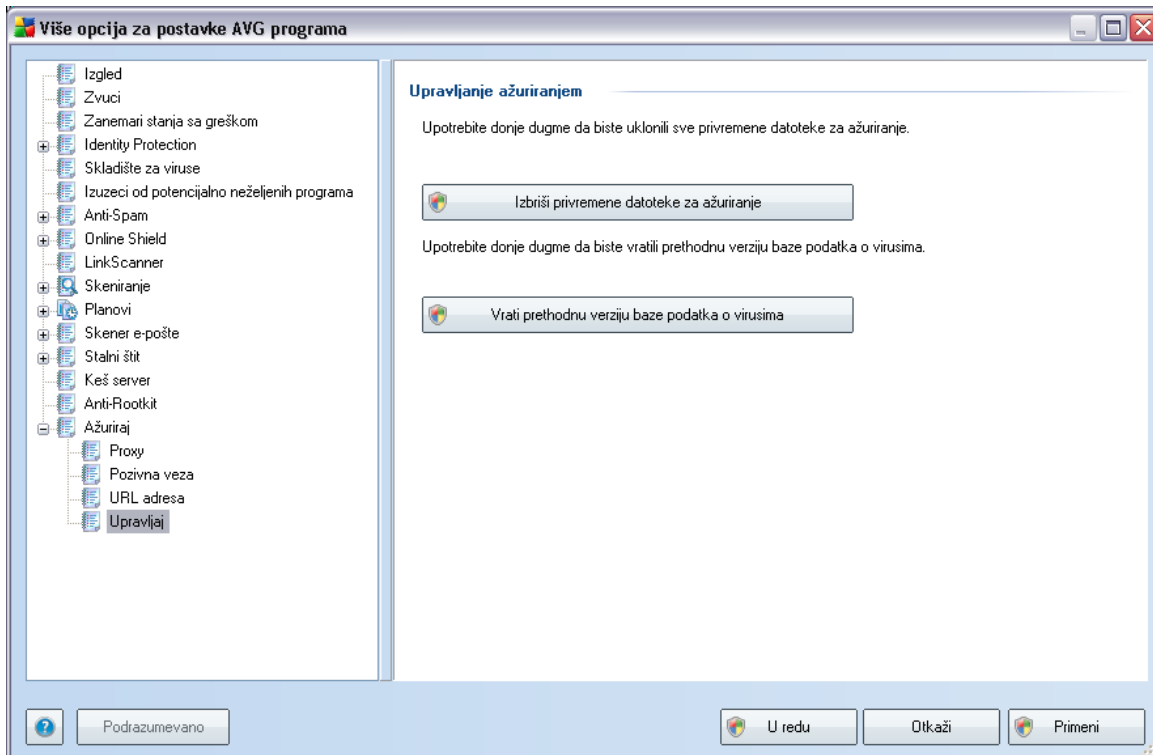


Dijalog **URL adresa** nudi listu Internet adresa sa kojih možete da preuzmete datoteke ispravki. Ova lista i njene stavke mogu se izmeniti pomocu sledece kontrolne dugmadi:

- **Dodaj**– otvara dijalog u kojem možete da navedete novu URL adresu koja ce biti dodata na listu
- **Uredi** - otvara dijalog u kojem možete da uredite izabrane parametre URL adrese
- **Izbriši** – briše izabranu URL adresu sa liste
- **Premesti nagore**– premešta izabranu URL adresu nagore za jedno mesto na listi
- **Premesti nadole** – premešta izabranu URL adresu nadole za jedno mesto na listi

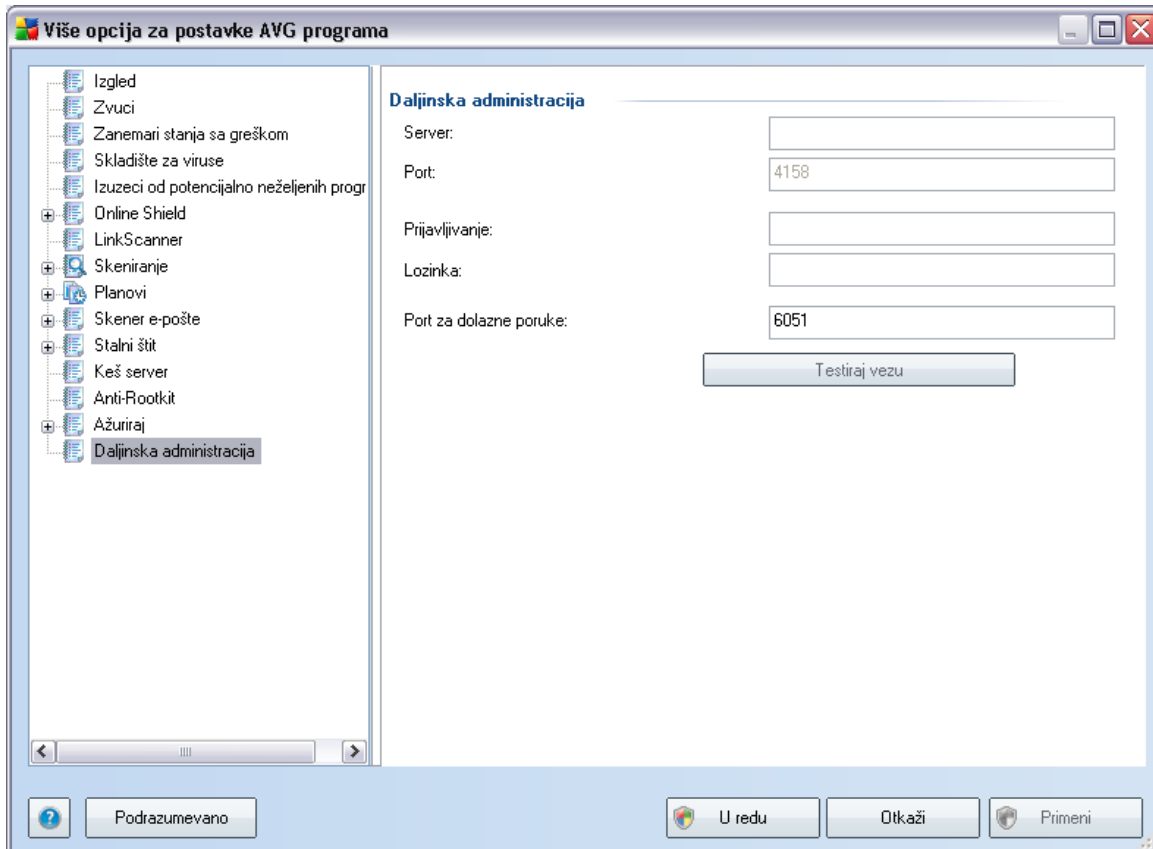
10.14.4. Upravljanje

Dijalog **Upravljač** nudi dve opcije kojima se pristupa pomocu dva dugmeta.



- **Izbriši privremene datoteke za ažuriranje** - pritisnite ovo dugme da biste izbrisali sve nepotrebne datoteke za ažuriranje sa cvrstog diska (*podrazumevano, te datoteke se cuvaju 30 dana*)
- **Vrati prethodnu verziju baze podataka o virusima** – kliknite na ovo dugme da biste izbrisali najnoviju verziju baze podataka o virusima sa cvrstog diska i da biste se vratili na prethodno sacuvanu verziju (*nova verzija baze podatka o virusima preuzece se prilikom sledeceg ažuriranja*)

10.15. Daljinska administracija



Podešavanja **Daljinska administracija** odnose se na povezivanje klijentske AVG stanice sa sistemom za daljinsku administraciju. Ako planirate da stanicu povežete sa daljinskom administracijom, definišite sledeće parametre:

- **Server** - ime servera (ili IP adresa servera) na kojem je instaliran AVG server za administraciju
- **Port** - unesite ime porta na kojem AVG klijent komunicira sa AVG serverom za administraciju (*broj porta 4158 je podrazumevan - ako koristite taj broj porta, ne morate eksplicitno da ga navodite*)
- **Prijavlivanje** - ako se komunikacija između AVG klijenta i AVG servera za administraciju definiše kao bezbedna, unesite svoje korisničko ime ...
- **Lozinka** - ...i svoju lozinku.



- **Port za dolazne poruke** - broj porta na kojem AVG klijent prihvata dolazne poruke od AVG servera za administraciju

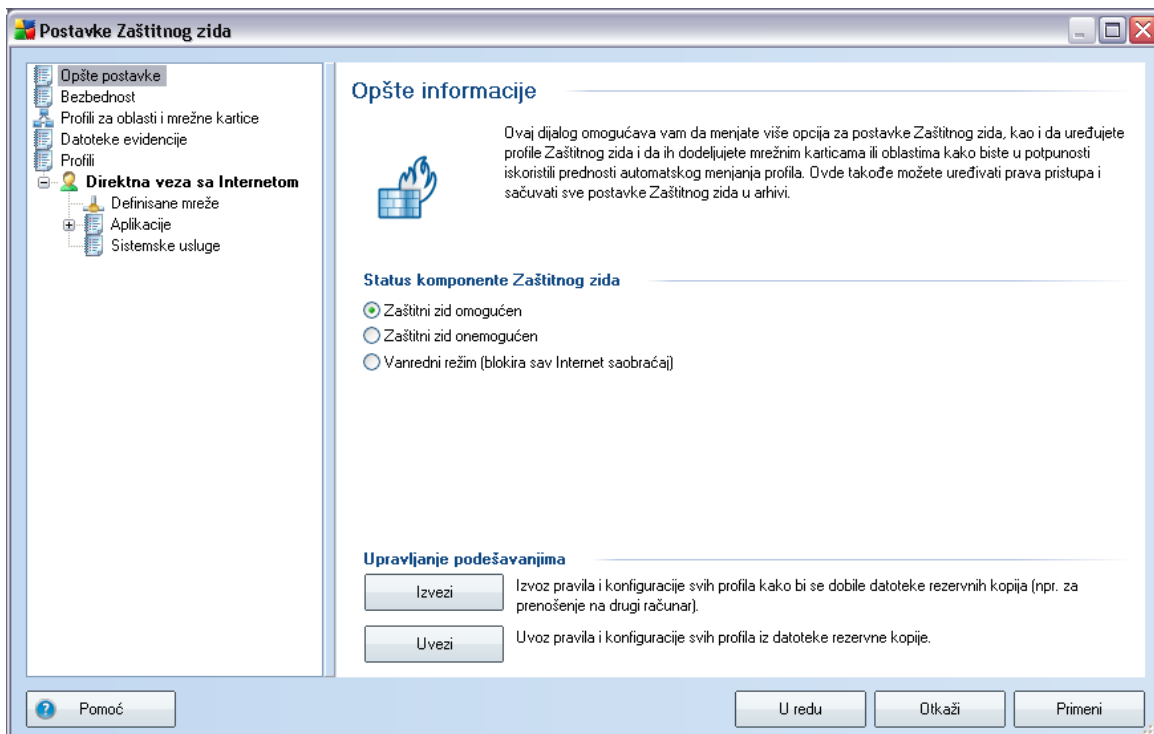
Dugme **Testiraj vezu** vam pomaže da proverite da li su svi gore navedeni podaci važeci i može se koristiti za uspešno povezivanje sa centrom za podatke.

Napomena: *Detaljan opis daljinske administracije potražite u dokumentaciji mrežnog izdanja programa AVG.*

11. Podešavanja zaštitnog zida

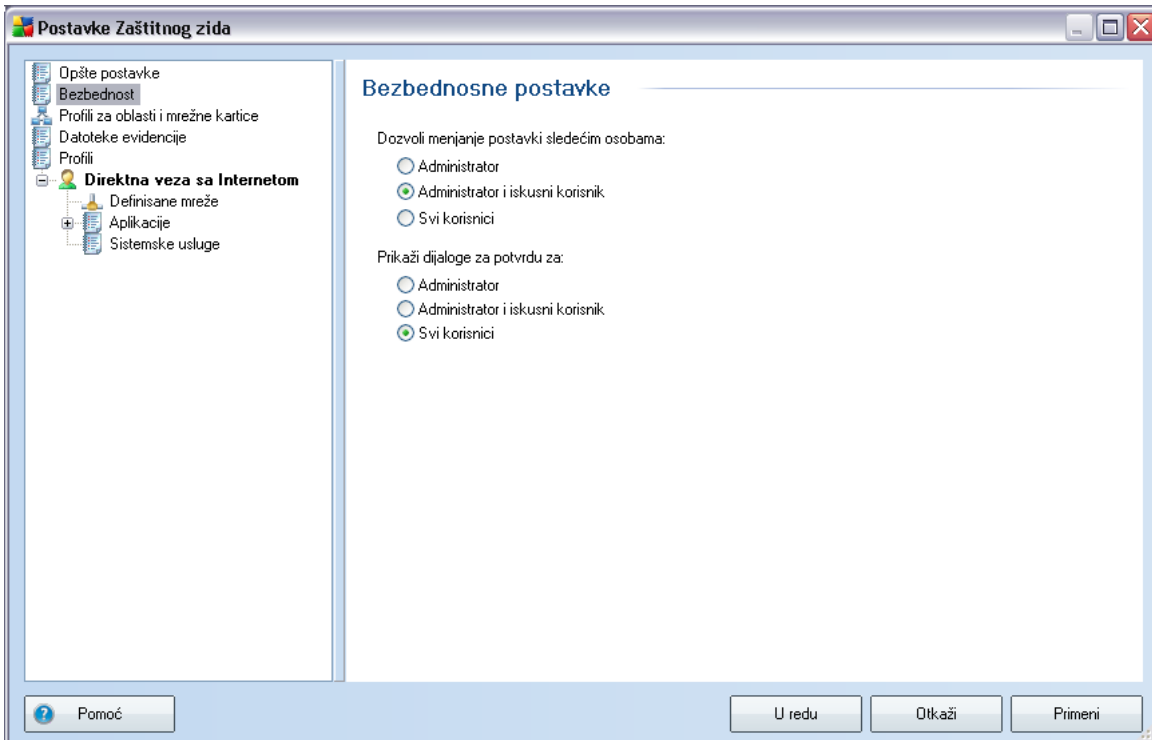
Konfiguracija komponente **Zaštitni zid** otvara se u novom prozoru, a na raspolaganju vam je nekoliko dijaloga za podešavanje veoma naprednih parametara ove komponente. **Medutim, uređivanje naprednih podešavanja namenjeno je isključivo stručnjacima i iskusnim korisnicima.**

11.1. Opšte postavke



U dijalogu **Opšte informacije** možete da **izvezete / uvezete** podešavanja komponente **Zaštitni zid**; tj. da izvezete definisana pravila i postavke komponente **Zaštitni zid** u datoteke rezervne kopije ili da uvezete celu datoteku rezervne kopije.

11.2. Bezbednost



U dijalogu **Bezbednosne postavke** možete definisati opšta pravila ponašanja komponente **Zaštitni zid**, bez obzira na to koji je profil izabran:

- **Dozvoli menjanje postavki sledećim osobama** - navedite kome je dozvoljeno da menja konfiguraciju komponente **Zaštitni zid**.
- **Prikaži dijalog za potvrdu za** - navedite kome ce se prikazivati dijalozi za potvrdu (*dijalozi koji od vas traže da odlucite ako situacija nije pokrivena pravilima komponente **Zaštitni zid***)

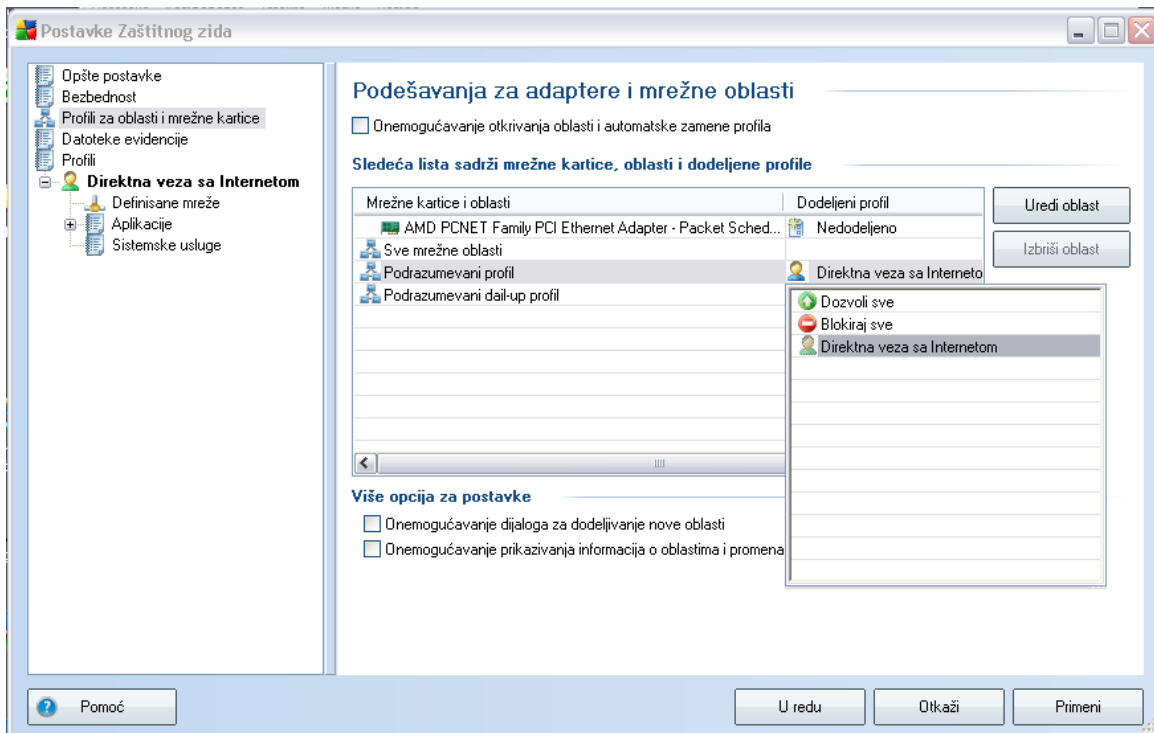
U oba slucaja, određeno pravo možete dodeliti nekoj od sledećih korisnickih grupa:

- **Administrator** – u potpunosti kontroliše racunar i ima pravo da svakog korisnika dodeli grupi sa posebno definisanim ovlašćenjima
- **Administrator i iskusni korisnik** – administrator može svakog korisnika da dodeli određenoj grupi (*iskusni korisnik*), kao i da definiše ovlašćenja

clanova grupe

- o **Svi korisnici** – ostali korisnici koji nisu dodeljeni nijednoj određenoj grupi

11.3. Profili za oblasti i mrežne kartice



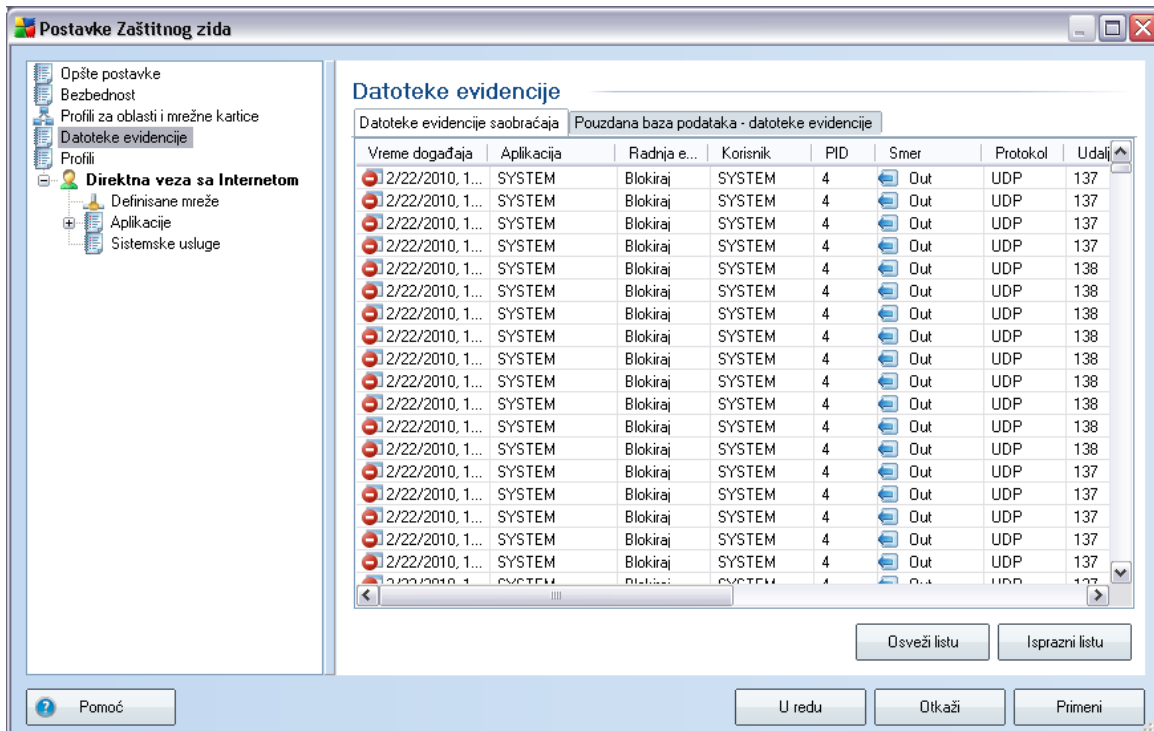
U dijalogu **Postavke za adaptere i mrežne oblasti** možete urediti postavke koje se ticu dodeljivanja definisanih profila određenim adapterima i mrežama:

- **Onemogući otkrivanje oblasti i automatsku zamenu profila** - neki od definisanih profila se može dodeliti svakom tipu mrežnog interfejsa, odnosno svakoj oblasti. Ako ne želite da definišete određene profile, koristice se jedan zajednicki profil definisan na osnovu izabranog [nacina upotrebe racunara](#) i [nacina umrežavanja racunara](#) tokom [procesa instalacije](#). Medutim, ako želite da definišete profile i da ih dodelite određenim adapterima i oblastima, a kasnije iz nekog razloga poželite da privremeno promenite ove postavke, izaberite opciju **Onemogući otkrivanje oblasti i automatsku zamenu profila**.
- **Lista adaptera, oblasti i dodeljenih profila** - na ovoj listi se nalazi pregled detektovanih adaptera i oblasti. Svakoju od ovih stavki možete dodeliti određeni

profil iz menija definisanih profila. Da biste otvorili ovaj meni, kliknite na odgovarajucu stavku sa liste adaptera i izaberite željeni profil.

- **Napredna podešavanja** - ako oznacite odgovarajucu opciju, deaktiviracete funkciju prikazivanja informativne poruke.

11.4. Datoteke evidencije



U dijalogu **Evidencija** možete da pregledate listu svih evidentiranih radnji i događaja komponente **Zaštitni zid** sa detaljnim opisom relevantnih parametara (*vreme događaja, ime aplikacije, odgovarajuca radnja evidencije, korisnicko ime, PID, smer saobracaja, tip protokola, broj udaljenih i lokalnih portova itd.*) na dve kartice:

- **Evidencija saobracaja** - sadrži informacije o aktivnostima svih aplikacija koje su pokušale da se povežu sa mrežom.
- **Evidencija pouzdane baze podataka** - *Pouzdana baza podataka* je interna AVG baza podataka u kojoj se prikupljaju informacije o certifikovanim i pouzdanim aplikacijama kojima se uvek može dozvoliti komunikacija na mreži. Kada aplikacija pokuša prvi put da se poveže sa mrežom (*tj. kada za tu*

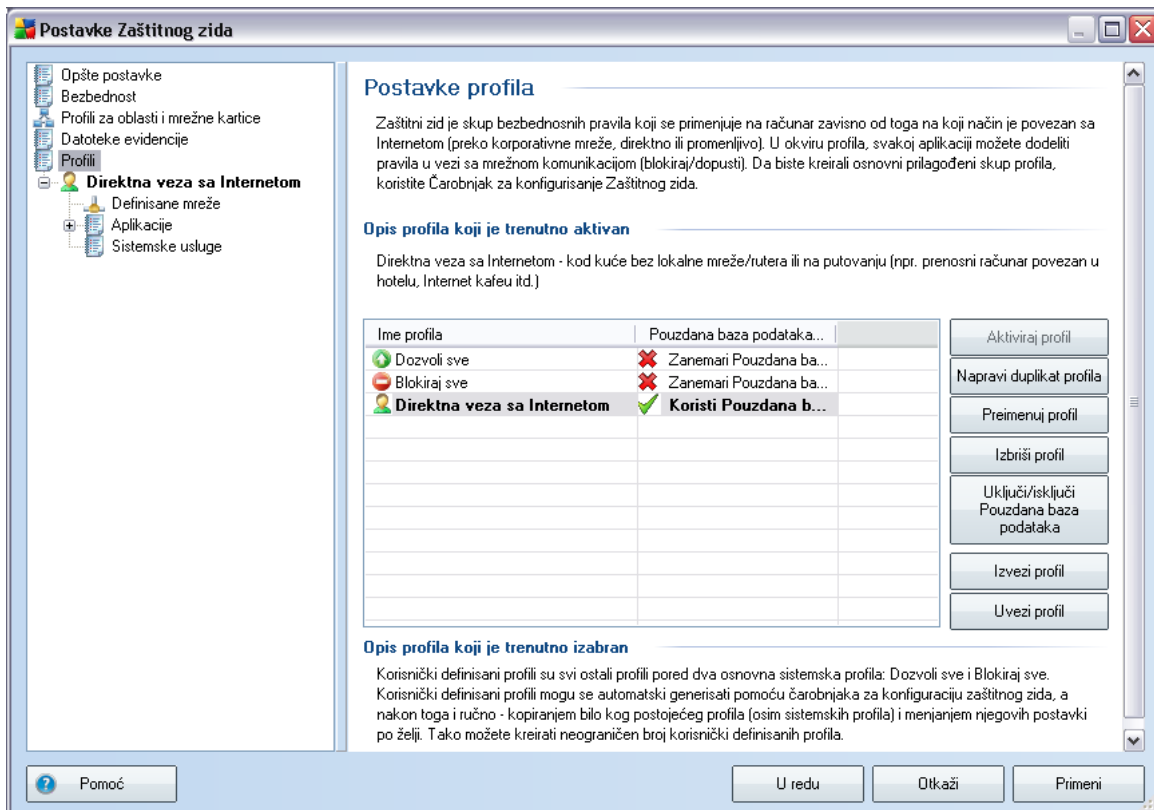
aplikaciju još nije definisano pravilo zaštitnog zida), neophodno je da saznate da li toj aplikaciji treba dozvoliti mrežnu komunikaciju. AVG najpre pretražuje *pouzdanu bazu podataka* i ako se aplikacija nalazi u njoj, automatski će joj biti odobren pristup mreži. Tek nakon toga, pod uslovom da se u bazi podataka ne nalaze informacije o aplikaciji, od vas će se tražiti da u posebnom dijalogu odlucite da li želite da toj aplikaciji dozvolite pristup mreži.

Kontrolna dugmad

- **Pomoc** – otvaranje datoteka pomoci u vezi sa dijalogom.
- **Osveži listu** – svi evidentirani parametri mogu se rasporediti prema izabranom atributu: hronološki (*datum*) ili po abecednom redosledu (*ostale kolone*) – dovoljno je da kliknete na zaglavlje odgovarajuće kolone. Upotrebite dugme **Osveži listu** da biste ažurirali informacije koje se trenutno prikazuju.
- **Isprazni listu** – brisanje svih stavki na grafikonu.

11.5. Profili

U dijalogu **Podešavanja profila** nalazi se lista svih dostupnih profila.



Ostale [profile](#), osim sistemskih, možete urediti direktno u ovom dijalogu pomoću sledeće kontrolne dugmadi:

- **Aktiviraj profil** - ovo dugme postavlja izabrani profil za aktivan, što znači da će konfiguraciju izabranog profila **Zaštitni zid** koristiti za kontrolu mrežnog saobraćaja.
- **Napravi duplikat profila** - kreiranje identične kopije izabranog profila, koju zatim možete urediti i preimenoovati kako biste kreirali novi profil zasnovan na duplikatu originalnog.
- **Preimenuj profil** - omogućava vam da definišete novo ime izabranog profila.
- **Izbriši profil** - briše izabrani profil sa liste

- **Ukljuci/iskljuci pouzdanu bazu podataka** - za izabrani profil možete da koristite informacije *pouzdanu bazu podataka* (*Pouzdana baza podataka je interna AVG baza podataka u kojoj se prikupljaju podaci o pouzdanim i sertifikovanim aplikacijama kojima uvek možete dozvoliti komunikaciju na mreži.*)
- **Izvezi profil** - upisuje konfiguraciju izabranog profila u datoteku koja se zatim cuva za potencijalnu buducu upotrebu
- **Uvezi profil** - konfigurisanje podešavanja izabranog profila na osnovu podataka izvezenih iz rezervne kopije datoteke za konfiguraciju
- **Pomoc** - otvaranje datoteke pomoci u vezi sa ovim dijalogom

U donjem delu dijaloga nalazi se opis profila koji je trenutno izabran na gornjoj listi.

U zavisnosti od broja definisanih profila na listi u dijalogu **Profil**, menjace se i struktura levog navigacionog menija. Za svaki definisani profil kreira se zasebna grana u okviru stavke **Profil**. Pojedinačne profile zatim možete uređivati u sledecim dijalozima (*koji su isti za sve profile*):

11.5.1. Informacije o profilu



Dijalog **Informacije o profilu** je prvi dijalog odeljka u kojem možete urediti konfiguraciju svakog profila u zasebnim dijalozima za svaki parametar profila.

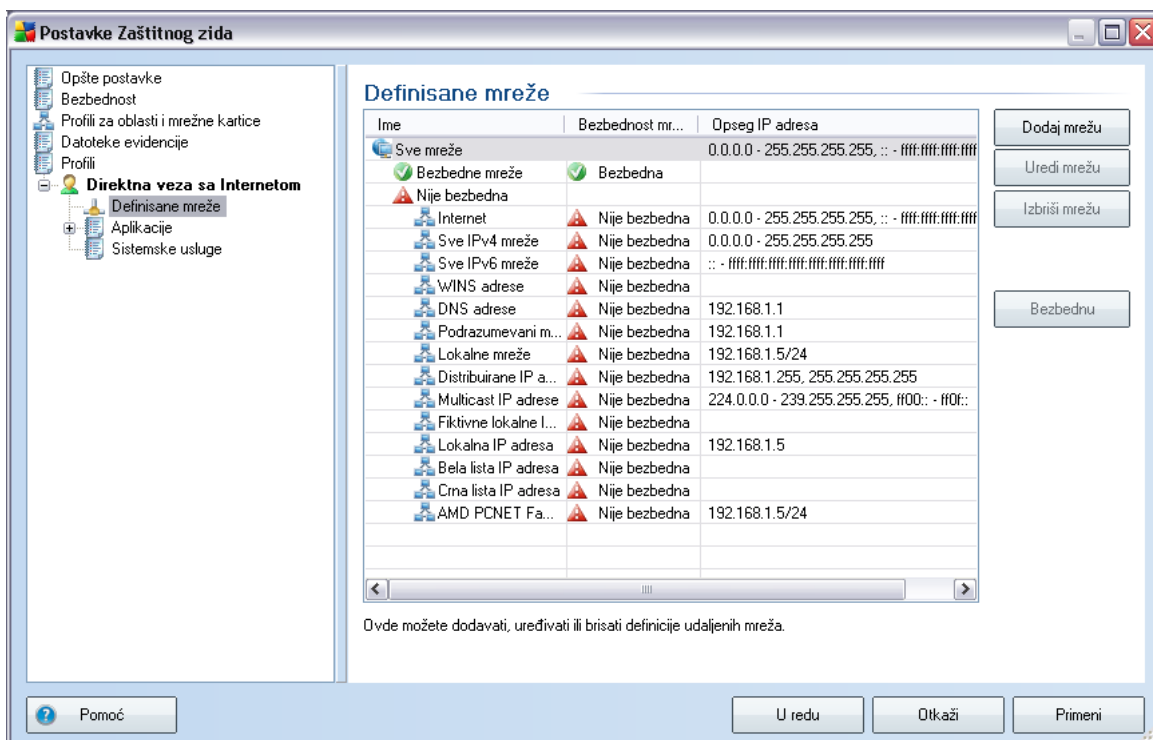
- **Koristi pouzdanu bazu podataka za ovaj profil** - (*podrazumevano je ukljuceno*) izaberite ovu opciju da biste aktivirali *pouzdanu bazu podataka* (tj. *internu AVG bazu podataka u kojoj se prikupljaju informacije o pouzdanim i sertifikovanim aplikacijama koje komuniciraju na mreži. Ako za odredenu aplikaciju još nije navedeno pravilo, neophodno je da saznate da li je toj aplikaciji moguće dozvoliti pristup mreži. AVG najpre pretražuje pouzdanu bazu podataka i ako se aplikacija nalazi u njoj, smatraće se bezbednom i bice joj dozvoljena komunikacija putem mreže. U suprotnom, od vas ce se tražiti da odlucite da li aplikaciji treba dozvoliti komunikaciju putem mreže*) za odgovarajući profil
- **Omoguci premošćeno umrežavanje virtuelnih mašina** - (*podrazumevano je iskljuceno*) izaberite ovu opciju da biste dozvolili VMware virtuelnim mašinama da se direktno povezuju sa mrežom

Postavke režima za igre

U odeljku **Postavke režima za igre** možete izabrati i potvrditi označavanjem odgovarajuće stavke da li želite da komponenta **Zaštitni zid** prikazuje informativne poruke čak i dok su na računaru pokrenute aplikacije preko celog ekrana (*uglavnom igre, ali važi za sve aplikacije preko celog ekrana, npr. PPT prezentacije*). Pošto informativne poruke mogu malo da smetaju.

Ako izaberete opciju **Onemogućeni obaveštenja zaštitnog zida tokom igranja igara**, u padajućem meniju izaberite radnju koju treba preduzeti u slučaju da nova aplikacija za koju još nisu definisana pravila pokuša da komunicira putem mreže (*aplikacije za koje bi se obično pojavio upitni dijalog*), svim ovim aplikacijama može se dozvoliti ili blokirati pristup mreži.

11.5.2. Definisane mreže

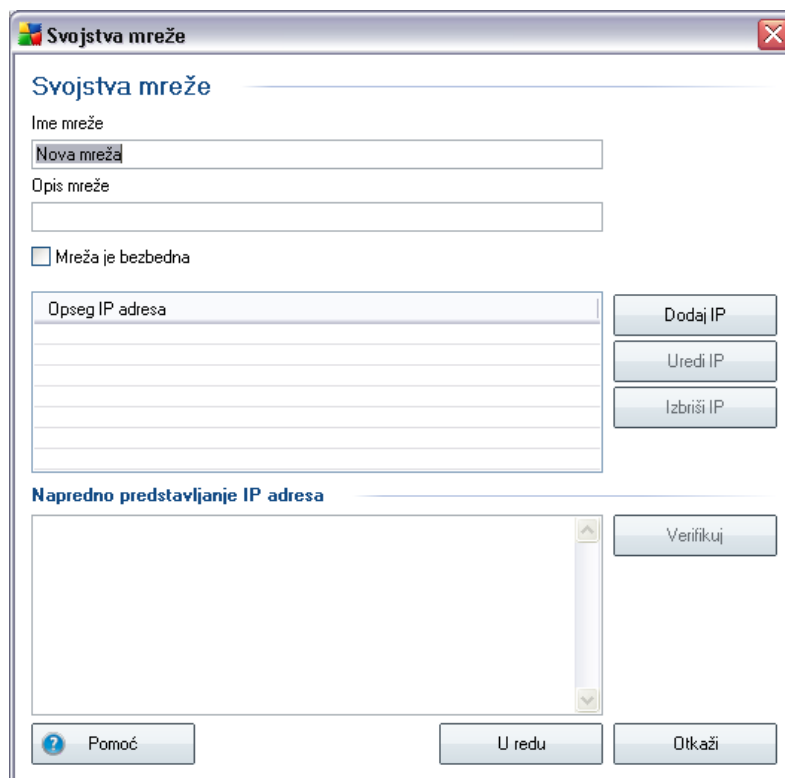


Dijalog **Definisane mreže** sadrži listu svih mreža na koje je povezan vaš računar. Za svaku detektovanu mrežu date su sledeće informacije:

- **Mreže** - lista imena svih mreža na koje je povezan racunar.
- **Bezbednost mreže** - podrazumevano, sve mreže se smatraju nebezbednim, pa mreže oznacavajte kao bezbedne samo ako imate potpuno poverenje u njih (kliknite na stavku sa liste koja se odnosi na željenu mrežu i izaberite opciju „Bezbedna“ u kontekstualnom meniju) - sve bezbedne mreže bice ukljucene u grupu mreža sa kojima aplikacija može da komunicira sa pravilom za aplikacije postavljenim na opciju „Dozvoli kao bezbedno“
- **Opseg IP adresa** - mreže se detektuju automatski i navode u obliku opsega IP adresa

Kontrolna dugmad

- **Dodaj mrežu** - otvaranje dijaloga **Svojstva mreže** u kojem možete urediti parametre nove mreže.



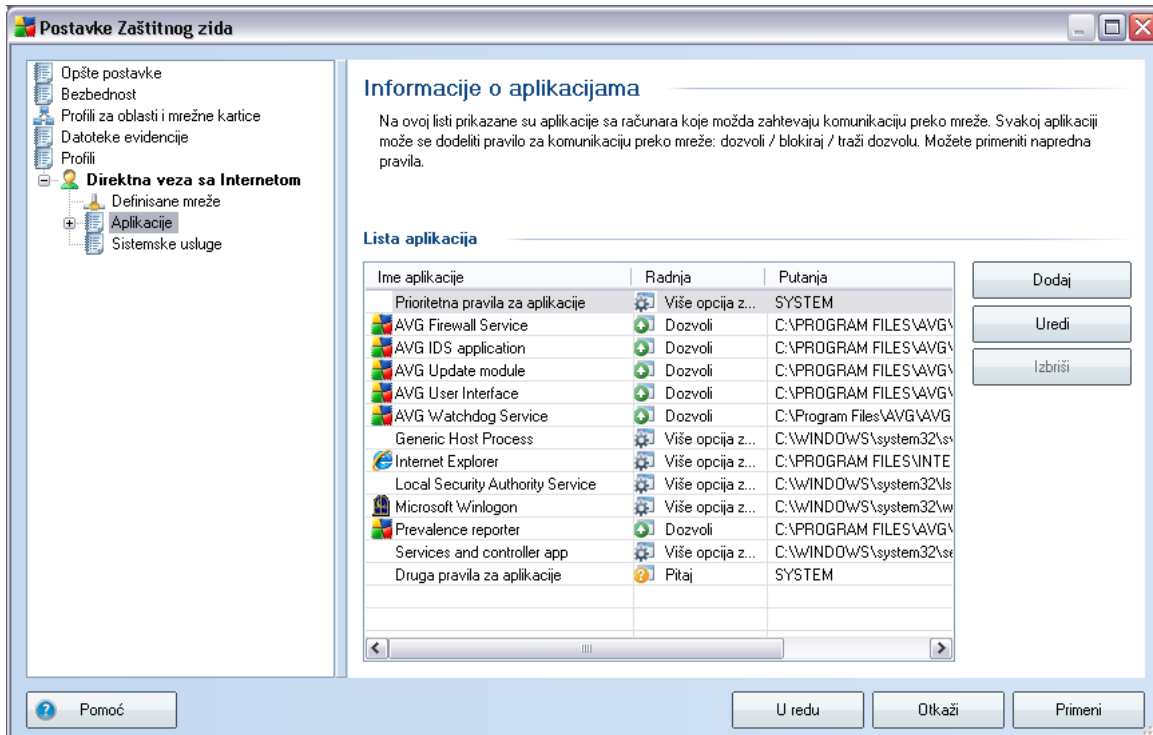
U ovom dijalogu možete navesti **Ime mreže**, uneti **Opis mreže** i

eventualno je oznaciti kao bezbednu. Novu mrežu možete definisati ručno u samostalnom dijalogu koji se otvara ako kliknete na dugme **Dodaj IP** (takode, **Uredi IP / Izbriši IP**); iz tog dijaloga možete navesti mrežu unošenjem njenog opsega IP adresa ili maske.






Ako je potrebno definisati veliki broj mreža kao deo nove mreže, možete upotrebiti opciju **Napredno predstavljanje IP adresa** : unesite listu svih adresa u odgovarajuće polje za tekst (*podržani su svi standardni formati*) i pritisnite dugme **Verifikuj** da biste bili sigurni da je format prepoznat. Zatim pritisnite dugme **U redu** da biste potvrdili i sačuvali podatke.

- **Uredi mrežu** - otvaranje dijaloga **Svojstva mreže** (*vidi iznad*) u kojem možete urediti parametre mreža koje ste već definisali (*ovaj dijalog je isti kao dijalog za dodavanje nove mreže, pogledajte opis u prethodnom pasusu*)
- **Izbriši mrežu** - uklanjanje informacija o izabranoj mreži sa liste mreža.
- **Oznaci kao bezbednu** - podrazumevano, sve mreže se smatraju nebezbednim, pa mreže oznacavajte kao bezbedne pomoću ovog dugmeta samo ako imate potpuno poverenje u njih (*i obrnuto, kada mrežu oznacite kao bezbednu, tekst na dugmetu se menja u „Oznaci kao nebezbednu“*).
- **Pomoc** - otvaranje datoteke pomoci u vezi sa ovim dijalogom

11.5.3. Aplikacije



U dijalogu **Informacije o aplikaciji** navedene su sve instalirane aplikacije kojima može biti potrebna komunikacija preko mreže, zajedno sa ikonama za dodeljenu radnju:

-  Dozvoli komunikaciju sa svim mrežama
-  Dozvoli komunikaciju samo sa mrežama koje su definisane kao Bezbedne
-  Blokiraj komunikaciju
-  Prikaži upitni dijalog (*korisnik ce u ovom trenutku moci da odluci da li želi da dozvoli ili blokira komunikaciju*)
-  Definisana napredna podešavanja

Aplikacije na listi su detektovane na vašem racunaru (*dodeljenje su im odredene radnje*) tokom pretrage pomocu [carobnjaka za konfiguraciju zaštitnog zida](#) ili kasnije, u slučaju nepoznate ili tek instalirane aplikacije.

Napomena: Imajte u vidu da se detektuju samo aplikacije koje su već instalirane, pa ćete, ako kasnije instalirate novu aplikaciju, morati da definišete pravila zaštitnog zida za nju. Kada nova aplikacija prvi put pokuša da se poveže putem mreže, Zaštitni zid će podrazumevano automatski kreirati pravilo za tu aplikaciju u skladu sa Pouzdanom bazom podataka ili će vas pitati da li želite da dozvolite ili blokirate komunikaciju. Ukoliko se radi o drugom slučaju, moći ćete da sacuvate svoj odgovor kao trajno pravilo (koje će biti navedeno u ovom dijalogu).

Naravno, pravila za novu aplikaciju možete i odmah definisati – u ovom dijalogu, pritisnite dugme **Dodaj** i unesite detalje o aplikaciji.

Osim aplikacija, na listi se nalaze i dve specijalne stavke:

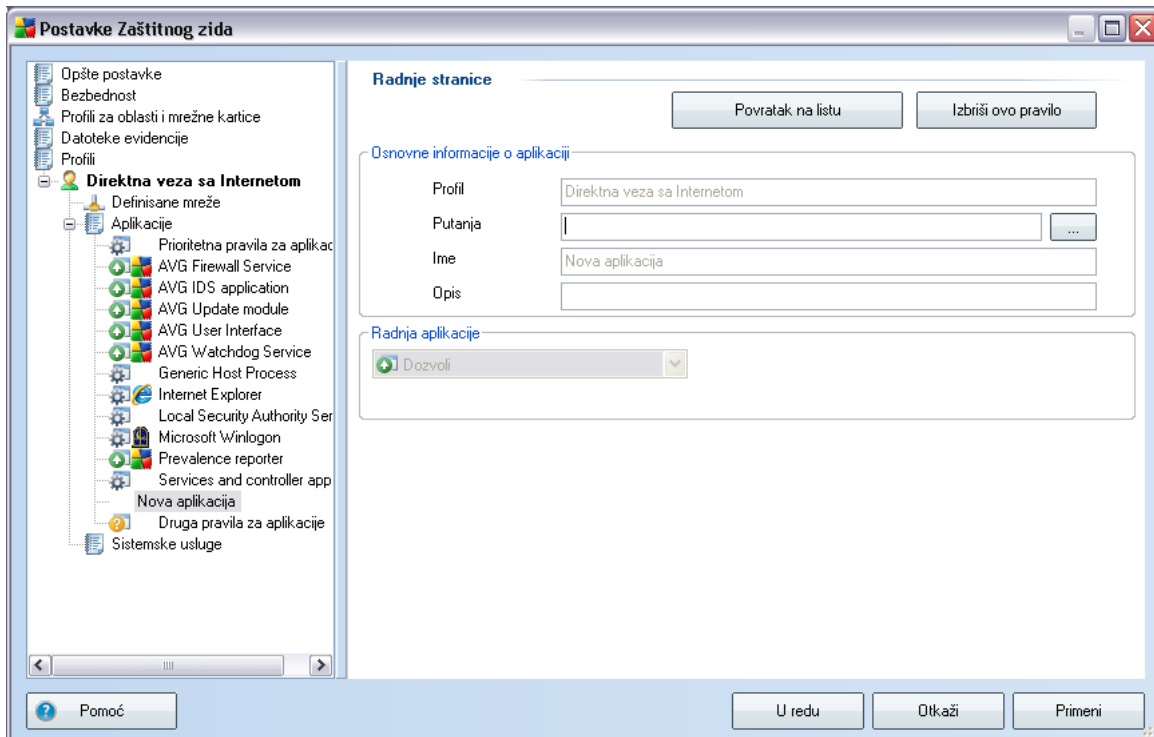
- **Prioritetna pravila za aplikacije** (na vrhu liste) imaju prioritet i uvek se primenjuju pre pravila za pojedinačne aplikacije.
- **Druga pravila za aplikacije** (na dnu liste) koriste se kao „poslednja instanca“ ako ne važe pravila za pojedinačne aplikacije, npr. za nepoznatu i nedefinisanu aplikaciju.

Ove stavke se podešavaju drugacije od ostalih aplikacija, a namenjene su isključivo za iskusne korisnike. Preporučujemo vam da ne menjate ova podešavanja

Kontrolna dugmad

Listu možete urediti pomoću sledeće kontrolne dugmadi:

- **Dodaj** - otvara se prazan dijalog [Radnje na stranici](#) za definisanje novih pravila za aplikaciju
- **Uredi** - otvara se isti dijalog [Radnje na stranici](#) u kojem se nalaze podaci za uređivanje postojećeg skupa pravila za aplikaciju
- **Izbriši** - briše izabranu aplikaciju sa liste
- **Pomoc** - otvaranje datoteke pomoci u vezi sa ovim dijalogom



U ovom dijalogu možete detaljno definisati podešavanja za pojedinačne aplikacije.

Radnje na stranici






- Kada kliknete na dugme **Nazad na listu**, prikazace se pregled svih definisanih pravila za aplikacije.
- Kada kliknete na dugme **Izbriši ovo pravilo**, izbrisace se trenutno prikazano pravilo za aplikaciju. Imajte u vidu da ovu radnju nije moguće opozvati!

Osnovne informacije o aplikaciji

U ovom odeljku unesite **Ime** aplikacije, a opcionalno možete da unesete **Opis** (*kratak komentar o informacijama koje ste uneli*). U polje **Putanja** unesite punu putanju do aplikacije (*izvršne datoteke*) na disku. Umesto toga, aplikaciju možete jednostavno da pronađete u strukturi stabla tako što ćete kliknuti na dugme "...".

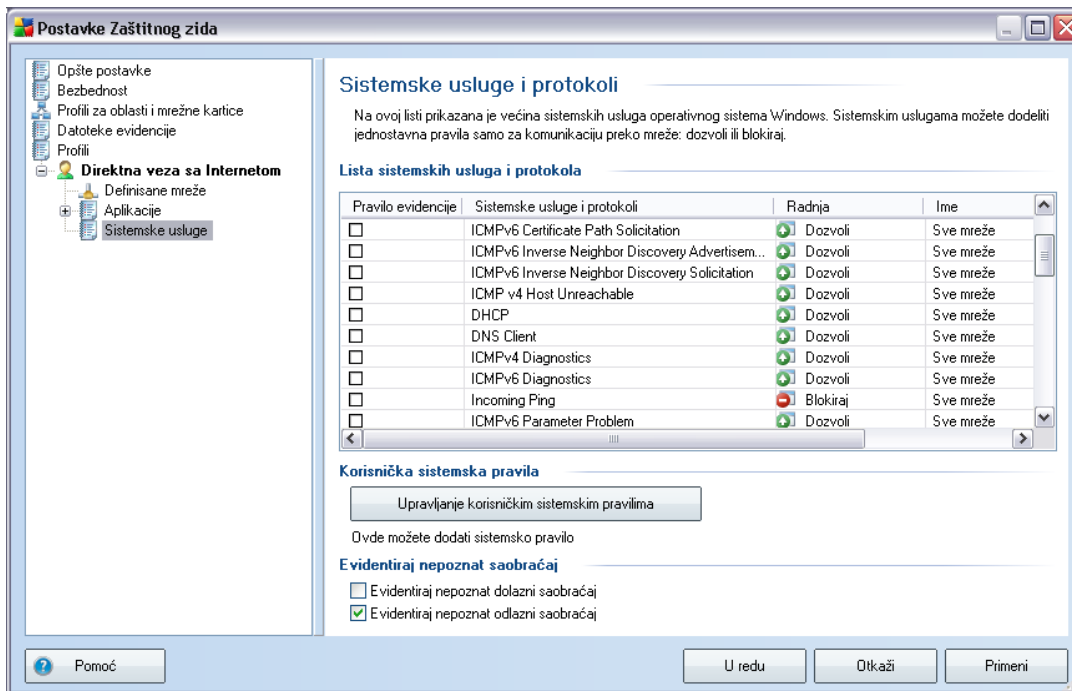
Radnja aplikacije

U padajućem meniju možete izabrati pravilo zaštitnog zida za aplikaciju, tj. šta bi zaštitni zid trebalo da preduzme kada aplikacija pokuša da komunicira preko mreže.

-  **Dozvoli sve** omogućava aplikaciji da komunicira preko svih definisanih mreža i adaptera, bez ikakvih ograničenja.
-  **Dozvoli za bezbedne** omogućava aplikaciji da komunicira samo preko onih mreža koje ste definisali kao Bezbedne (pouz dane).
-  **Blokiraj** automatski zabranjuje komunikaciju; aplikaciji neće biti dozvoljeno da se poveže ni sa jednom mrežom.
-  **Pitaj** prikazuje dijalog koji vam omogućava da odlucite da li želite da dozvolite ili blokirate trenutni pokušaj komunikacije.
-  Καθα κλικνετε να θυμε **Napredna podešavanja**, prikazace se opcije za detaljna podešavanja u donjem delu dijaloga u odeljku **Detaljna pravila za aplikaciju**. Detalji ce se primenjivati prema redosledu na listi tako da cete moći da koristite opcije **Premesti nagore** ili **Premesti nadole** da biste raspodelili pravila na listi po prioritetu. Nakon što kliknete na određeno pravilo sa liste, pregled detalja pravila prikazace se u donjem delu dijaloga. Svaka vrednost koja je podvucena plavom bojom može se promeniti tako što cete kliknuti na odgovarajuci dijalog za podešavanje. Da biste izbrisali istaknuto pravilo, pritisnite dugme **Ukloni**. Da biste definisali novo pravilo, upotrebite dugme **Dodaj** da biste otvorili dijalog **Promeni detalje pravila** u kojem možete definisati sve potrebne detalje.


11.5.4. Sistemske usluge

Uređivanje postavki u dijalogu „Sistemske usluge i protokoli“ preporučuje se SAMO iskusnim korisnicima!



U dijalogu **Sistemske usluge i protokoli** su navedene standardne Windows sistemske usluge i protokoli koji možda zahtevaju komunikaciju putem mreže. Grafikon se sastoji iz sledećih kolona:

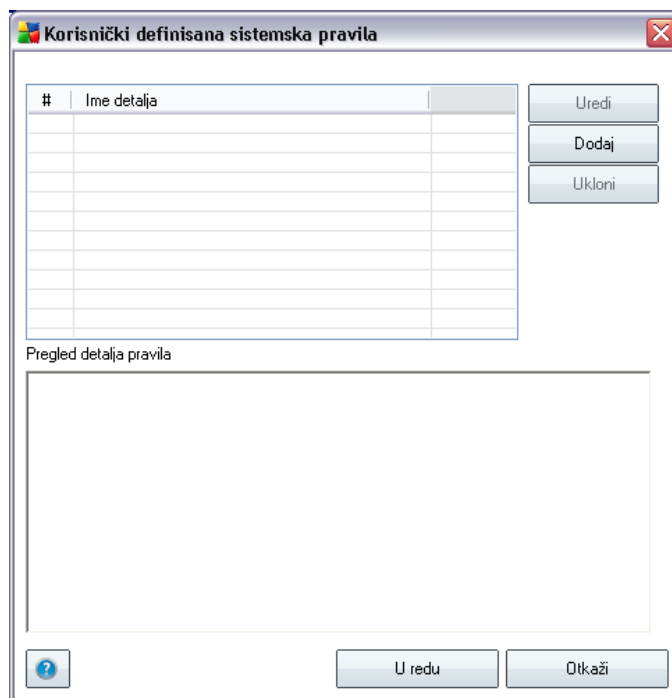
- **Evidentiraj radnju pravila** - ova opcija vam omogućava da uključite evidentiranje primene svakog pravila u datotekama evidencije.
- **Sistemske usluge i protokoli** - u ovoj koloni se prikazuje ime odgovarajuće sistemske usluge.
- **Radnja** - u ovoj koloni se prikazuje ikona za dodeljenu radnju:
 - Dozvoli komunikaciju sa svim mrežama
 - Dozvoli komunikaciju samo sa mrežama koje su definisane kao Bezbedne

o  Blokiraj komunikaciju

- **Mreže** - u ovoj koloni je navedena mreža na koju se primenjuje sistemsko pravilo.

Listu (*uključujući i dodeljene radnje*) možete da uredite pomoću sledećih dugmadi:

- Da biste uredili postavke bilo koje stavke na listi (*uključujući dodeljene radnje*), kliknite desnim tasterom miša na stavku i izaberite opciju **Uredi**.
- Da biste otvorili novi dijalog za definisanje sopstvenog sistemskog pravila (*pogledajte sliku ispod*), kliknite na dugme **Upravljanje korisničkim sistemskim pravilima**. U gornjem delu dijaloga **Korisnički definisana sistemsko pravilo** se prikazuje pregled svih detalja trenutno izmenjenog sistemskog pravila, a u donjem delu se prikazuje izabrani detalj. Korisnički definisana pravila mogu se uređivati, dodavati ili brisati pomoću odgovarajućeg dugmeta. Pravila koje je definisao proizvođač mogu se samo urediti:



Upozorenje: Imajte u vidu da su detaljna podešavanja pravila prevashodno namenjena administratorima mreže koji moraju imati punu kontrolu nad

konfiguracijom zaštitnog zida. Ako niste upoznati sa tipovima protokola za komunikaciju, brojevima mrežnih portova, definicijama IP adresa itd., ne menjajte ove postavke! Ukoliko je zaista potrebno da promenite konfiguraciju, pogledajte datoteke pomoci u odgovarajućem dijalogu da biste saznali više informacija.

Evidentiraj nepoznat saobraćaj

- **Evidentiraj nepoznat dolazni saobraćaj** – potvrdite izbor u polju za potvrdu ako želite da se u fascikli Datoteke evidencije beleži svaki nepoznati pokušaj povezivanja sa racunarom sa spoljne mreže.
- **Evidentiraj nepoznat odlazni sadržaj** – potvrdite izbor u polju za potvrdu ako želite da se u fasciklu Datoteke evidencije beleži svaki nepoznat pokušaj povezivanja sa spoljnom mrežom sa vašeg racunara.

12. Skeniranje programom AVG

Skeniranje je ključni deo funkcionalnosti programa **AVG 9 Anti-Virus sa zaštitnim zidom**. Možete da pokrenete testove na zahtev ili da [planirate da se periodično pokreću](#) u vreme koje vam odgovara.

12.1. Interfejs za skeniranje



AVG interfejsu za skeniranje možete pristupiti preko brze veze ***Skener računara******. Kliknite na ovu vezu da biste prešli na dijalog ***Skeniraj u potrazi za pretnjama***. U tom dijalogu nalaze se sledeći elementi:

- pregled [unapred definisanih skeniranja](#) - tri vrste skeniranja koje je definisao prodavac softvera mogu se koristiti odmah, na zahtev ili planirano:
 - [Skeniraj ceo računara](#)
 - [Skeniraj određene datoteke ili fascikle](#)
 - **Anti-Rootkit skeniranje**
- [odeljak planiranje skeniranja](#) - u kojem možete definisati nove testove i po

potrebi kreirati nove planove.

Kontrolna dugmad

U interfejsu za testiranje dostupna su sledeca kontrolna dugmad:

- **Istorija skeniranja** - prikazuje dijalog [Pregled rezultata skeniranja](#) sa celokupnom istorijom skeniranja
- **Prikaži Skladište za viruse** - otvara novi prozor u kojem se nalazi [Skladište za viruse](#) - karantin za detektovane zaraze.

12.2. Unapred definisana skeniranja

Jedna od glavnih funkcija programa **AVG 9 Anti-Virus sa zaštitnim zidom** je skeniranje na zahtev. Testovi na zahtev su dizajnirani da skeniraju razlicite delove racunara uvek kada postoji sumnja da je moglo doći do zaraze virusom. U svakom slucaju se preporucuje da se testovi redovno izvršavaju cak i kada mislite da nema virusa na racunaru.

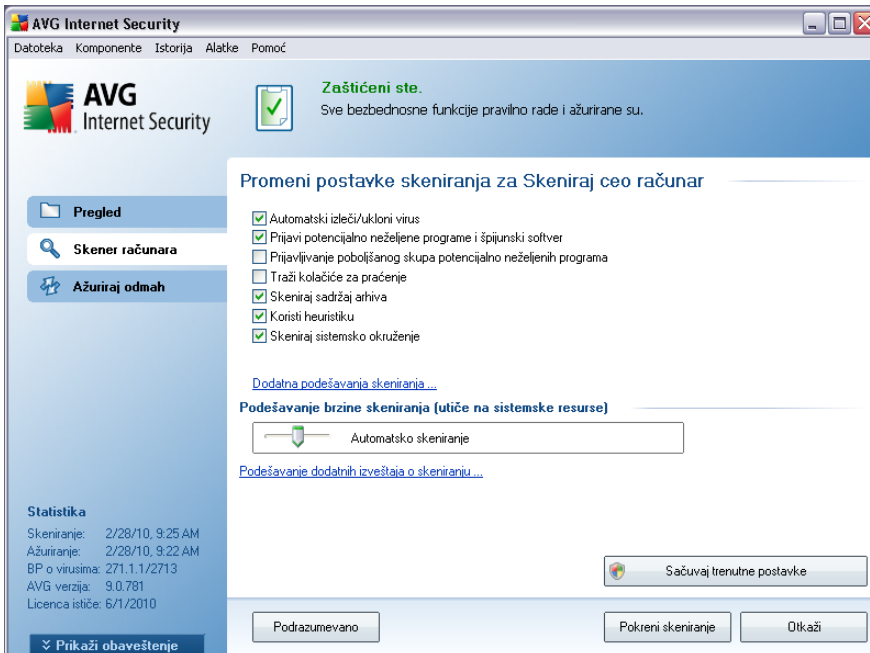
U programu **AVG 9 Anti-Virus sa zaštitnim zidom** postoje dve vrste skeniranja koje je unapred definisao prodavac softvera:

12.2.1. Skeniraj ceo racunar

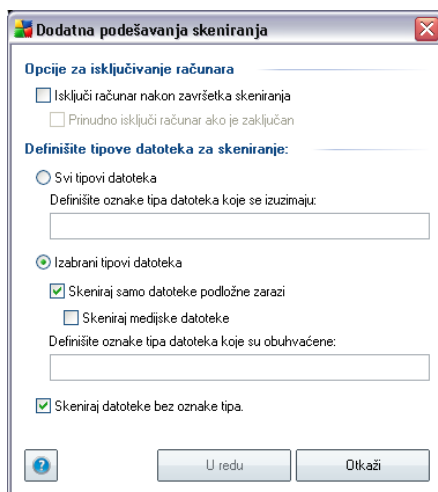
Skeniraj ceo racunar- skeniranje celog racunara kako bi se proverilo da li sadrži viruse i/ili potencijalno neželjene programe. Ovaj test ce skenirati sve cvrste diskove na racunaru, detektovati i oporaviti sve pronadene viruse ili ukloniti zaraženu datoteku i premestiti je u [Skladište za viruse](#). Skeniranje celog racunara trebalo bi da se zakaže na radnoj stanici barem jednom nedeljno.

Pokretanje skeniranja

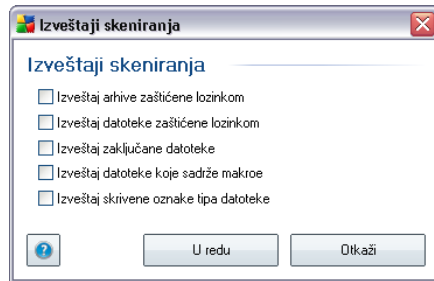
Skeniranje celog racunara može se pokrenuti neposredno iz [interfejsa za skeniranje](#) tako što cete kliknuti na ikonu tog vida skeniranja. Za ovaj tip skeniranja nije potrebno konfigurisati dodatne postavke, a skeniranje ce odmah poceti u okviru dijaloga **Skeniranje je u toku** (pogledajte snimak ekrana). Skeniranje se može privremeno prekinuti (**Pauziraj**) ili otkazati (**Zaustavi**) ako je potrebno.



- **Parametri skeniranja** - na listi parametara za skeniranje po potrebi možete uključiti/isključiti pojedinačne parametre. Podrazumevano, većina parametara je uključena, pa će se automatski koristiti u toku skeniranja.
- **Dodatne postavke skeniranja** - ovaj link otvara novi dijalog **Dodatne postavke skeniranja** u kojem možete da navedete sledeće parametre:



- **Opcije za isključivanje računara** - odlucite da li želite da se racunar automatski iskljuci kada se pokrenuto skeniranje završi. Ako potvrdite ovu opciju (**Iskljuci racunar nakon završetka skeniranja**), aktivirace se nova opcija koja omogućava da se racunar iskljuci cak i ako je trenutno zakljucan (**Prinudno iskljuci racunar ako je zakljucan**).
- **Definišite tipove datoteka za skeniranje** - odlucite da li želite da skenirate:
 - **Sve tipove datoteka** sa mogućnošću definisanja izuzetaka koji se neće skenirati tako što ćete navesti listu oznaka tipa datoteke razdvojenih zarezima koje ne treba skenirati;
 - **Izabrane tipove datoteka** - možete izabrati da skenirate samo datoteke za koje postoji mogućnost da su zaražene (*datoteke koje ne mogu biti zaražene neće se skenirati, na primer tekstualne datoteke ili neke druge datoteke koje nisu izvršne*), uključujući medijske datoteke (*video audio datoteke - ako ne potvrdite izbor u ovom polju za potvrdu, vreme skeniranja će se dodatno skratiti jer su datoteke ovog tipa obično velike i malo je verovatno da su zaražene virusom*). Izborom oznake tipa datoteke možete označiti datoteke koje treba uvek skenirati.
 - Možete i da izaberete opciju **Skeniraj datoteke bez oznake tipa datoteke** - ova opcija je podrazumevano uključena i preporučuje se da je ne isključujete osim ako nemate dobar razlog za to. Datoteke bez oznake tipa datoteke su sumnjive i treba ih uvek skenirati.
- **Prioritet procesa skeniranja** - pomoću klizaca možete promeniti prioritet procesa skeniranja. Podrazumevano, prioritet je podešen na srednji nivo (*Automatsko skeniranje*), što optimizuje brzinu procesa skeniranja i zauzetost sistemskih resursa. Takođe, proces skeniranja možete usporiti, što znači da će zauzetost sistemskih resursa biti manja (*korisno ako morate da radite na računaru, a nije vam važno koliko će skeniranje trajati*), a možete ga i ubrzati, što zahteva više sistemskih resursa (*npr. kada se privremeno udaljite od računara*).
- **Podešavanje dodatnih izveštaja o skeniranju** - ovaj link otvara novi dijalog **Izveštaji skeniranja** u kojem možete da izaberete koji tip pronađenog sadržaja će se prijavljivati:



Upozorenje: Ova podešavanja skeniranja ista su kao parametri najnovijeg definisanog skeniranja - kao što je opisano u poglavlju [AVG skeniranje / Planiranje skeniranja / Kako skenirati](#). Ako odlucite da promenite podrazumevanu konfiguraciju opcije **Skeniraj ceo racunar**, nove postavke možete sacuvati kao podrazumevanu konfiguraciju koja ce se koristiti za svako buduće skeniranje celog racunara.

12.2.2. Skeniraj određene datoteke ili fascikle

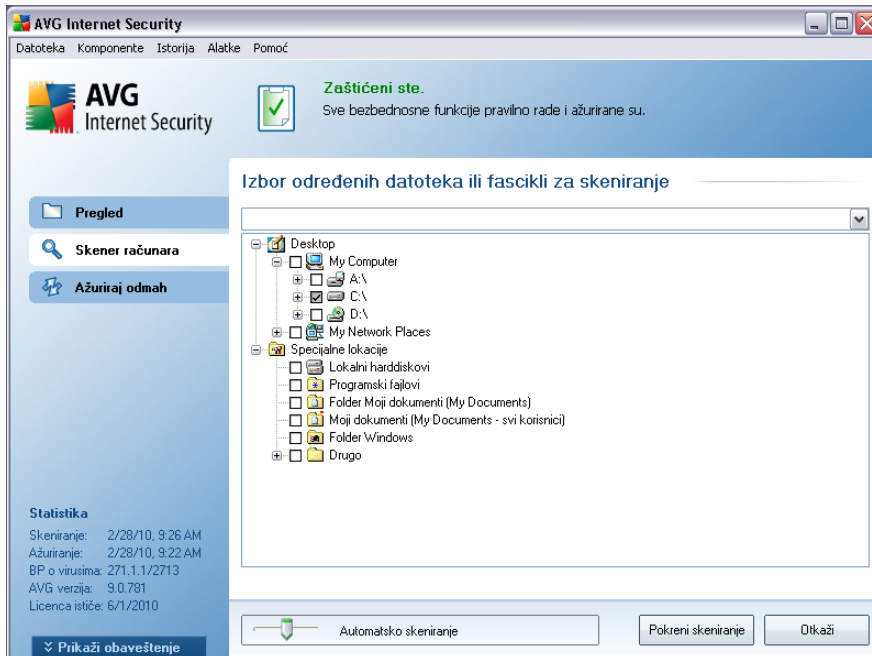
Skeniraj određene datoteke ili fascikle - skeniranje samo onih oblasti racunara koje ste izabrali za skeniranje (*izabrane fascikle, cvrsti diskovi, diskete, kompakt diskovi itd.*). Tok skeniranja u slucaju detekcije virusa i tretiranje virusa isti su kao kod skeniranja celog racunara : pronadeni virusi se uklanjaju iz datoteke ili premeštaju u [Skladište za viruse](#). Skeniranje određenih datoteka ili fascikli možete koristiti da biste kreirali sopstvene testove i planove skeniranja u skladu sa vašim potrebama.

Pokretanje skeniranja

Skeniranje određenih datoteka ili fascikli može se pokrenuti neposredno iz [interfejsa za skeniranje](#) tako što cete kliknuti na ikonu tog vida skeniranja. Otvorice se nov dijalog po imenu **Izbor određenih datoteka ili fascikli za skeniranje**. U prikazu stabla racunara možete izabrati fascikle koje želite da skenirate. Putanja do izabranih fascikli automatski ce se generisati i pojave se u polju za tekst u gornjem delu ovog dijaloga.

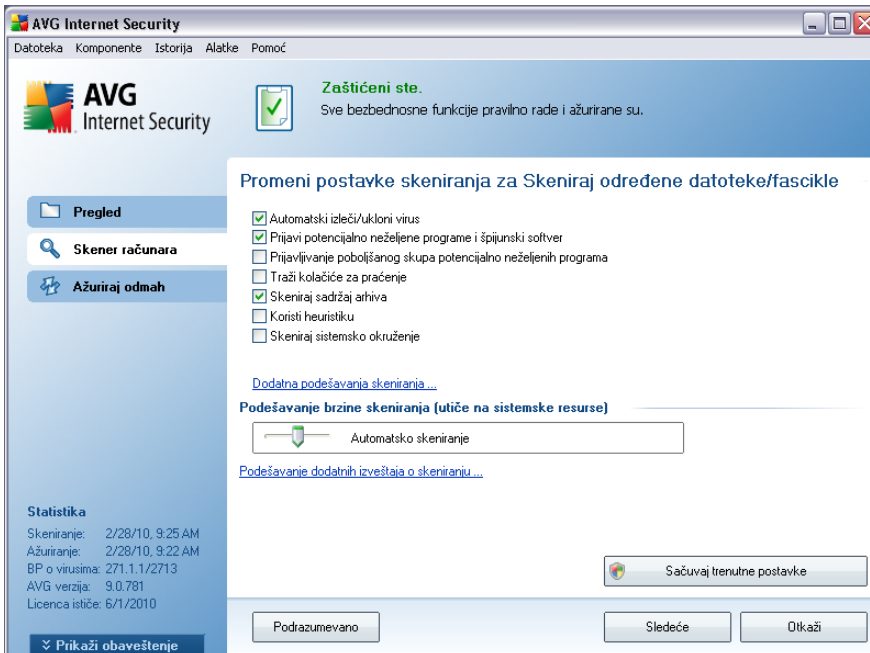
Takode postoji mogucnost skeniranja određene fascikle, ali ne i njenih podfascikli; da biste to ucinili, unesite znak minus „-“ ispred automatski generisane putanje (*vidi snimak ekrana*). Da biste celu fasciklu izuzeli iz skeniranja, koristite „!“ parametar.

Konacno, da biste pokrenuli skeniranje, pritisnite dugme **Pokreni skeniranje** ; sam proces skeniranja je u suštini isti kao [skeniranje celog racunara](#).

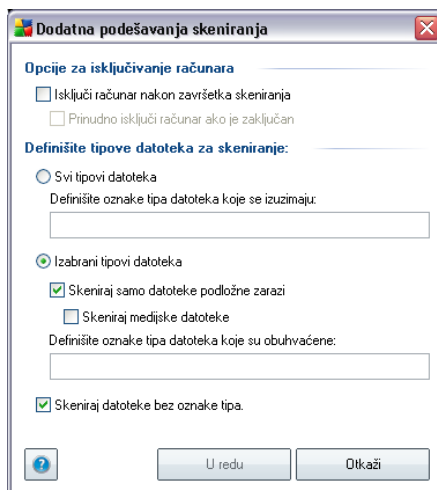


Uređivanje konfiguracije skeniranja

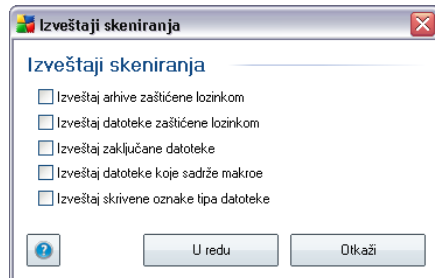
Imate mogućnost uređivanja unapred definisanih podešavanja za **Skeniranje određenih datoteka ili fascikli**. Pritisnite link **Promeni podešavanja skeniranja** da biste otvorili dijalog **Promeni podešavanja skeniranja za Skeniranje određenih datoteka ili fascikli**. **Preporučuje se da zadržite podrazumevana podešavanja, osim ako nemate dobar razlog da ih menjate!**



- **Parametri skeniranja** - na listi parametara za skeniranje po potrebi možete uključiti/isključiti određene parametre (*detaljan opis ovih postavki potražite u poglavlju [AVG napredna podešavanja / Skeniranje / Skeniranje određenih datoteka ili fascikli](#)*).
- **Dodatne postavke skeniranja** - ovaj link otvara novi dijalog Dodatne postavke skeniranja u kojem možete da navedete sledeće parametre:



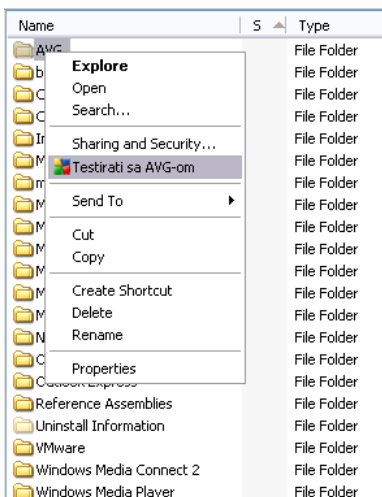
- **Opcije za isključivanje računara** - odlucite da li želite da se računar automatski iskljuci kada se pokrenuto skeniranje završi. Ako potvrdite ovu opciju (**Iskljuci računar nakon završetka skeniranja**), aktivirace se nova opcija koja omogućava da se računar iskljuci čak i ako je trenutno zaključan (**Prinudno iskljuci računar ako je zaključan**).
- **Definišite tipove datoteka za skeniranje** - odlucite da li želite da skenirate:
 - **Sve tipove datoteka** sa mogućnošću definisanja izuzetaka koji se neće skenirati tako što ćete navesti listu oznaka tipa datoteke razdvojenih zarezima koje ne treba skenirati;
 - **Izabrane tipove datoteka** - možete izabrati da skenirate samo datoteke za koje postoji mogućnost da su zaražene (*datoteke koje ne mogu biti zaražene neće se skenirati, na primer tekstualne datoteke ili neke druge datoteke koje nisu izvršne*), uključujući medijske datoteke (*video audio datoteke - ako ne potvrdite izbor u ovom polju za potvrdu, vreme skeniranja će se dodatno skratiti jer su datoteke ovog tipa obično velike i malo je verovatno da su zaražene virusom*). Izborom oznake tipa datoteke možete označiti datoteke koje treba uvek skenirati.
 - Možete i da izaberete opciju **Skeniraj datoteke bez oznake tipa datoteke** - ova opcija je podrazumevano uključena i preporučuje se da je ne isključujete osim ako nemate dobar razlog za to. Datoteke bez oznake tipa datoteke su sumnjive i treba ih uvek skenirati.
- **Prioritet procesa skeniranja** - pomoću klizaca možete promeniti prioritet procesa skeniranja. Podrazumevano, prioritet je podešen na srednji nivo (*Automatsko skeniranje*), što optimizuje brzinu procesa skeniranja i zauzetost sistemskih resursa. Takođe, proces skeniranja možete usporiti, što znači da će zauzetost sistemskih resursa biti manja (*korisno ako morate da radite na računaru, a nije vam važno koliko će skeniranje trajati*), a možete ga i ubrzati, što zahteva više sistemskih resursa (*npr. kada se privremeno udaljite od računara*).
- **Podešavanje dodatnih izveštaja o skeniranju** - ovaj link otvara dijalog **Izveštaji skeniranja** u kojem možete izabrati koji tip pronađenog sadržaja će se prijavljivati:



Upozorenje: Ova podešavanja skeniranja ista su kao parametri najnovijeg definisanog skeniranja - kao što je opisano u poglavlju [AVG skeniranje / Planiranje skeniranja / Kako skenirati](#). Ako odlucite da izmenite podrazumevanu konfiguraciju opcije **Skeniraj određene datoteke ili fascikle**, nova podešavanja možete sacuvati kao podrazumevanu konfiguraciju koja ce se koristiti za svako buduće skeniranje određenih datoteka ili fascikli. Takode, ova konfiguracija ce se koristiti kao predložak za sva nova planirana skeniranja ([sva prilagodena skeniranja zasnivaju se na trenutnoj konfiguraciji opcije Skeniranje određenih datoteka ili fascikli](#)).

12.3. Skeniranje u programu Windows Explorer

Pored unapred definisanog skeniranja celog racunara ili izabраниh oblasti na njemu, **AVG 9 Anti-Virus sa zaštitnim zidom** nudi i opciju brzog skeniranja određenog objekta direktno iz programa Windows Explorer. Ako želite da otvorite nepoznatu datoteku, a niste sigurni u njen sadržaj, možda cete želeti da je skenirate na zahtev. Pratite sledeće korake:



- U programu Windows Explorer označite datoteku (ili fasciklu) koju želite da

skenirate

- Desnim tasterom miša kliknite na taj objekat da bi se otvorio kontekstualni meni
- Izaberite opciju **Skeniraj programom AVG** da bi program AVG skenirao željenu datoteku

12.4. Skeniranje komandne linije

U programu **AVG 9 Anti-Virus sa zaštitnim zidom** postoji opcija za pokretanje skeniranja iz komandne linije. Ovu opciju možete koristiti npr. na serverima ili pri kreiranju grupne skripte koja će se automatski pokretati zajedno sa racunarom. Iz komandne linije možete pokrenuti skeniranje sa vecinom parametara koji su ponudeni u AVG grafickom korisnickom interfejsu.

Da biste pokrenuli AVG skeniranje iz komandne linije, pokrenite sledecu komandu u fascikli u kojoj je instaliran program AVG:

- **avgscanx** za 32-bitne operativne sisteme
- **avgscana** za 64-bitne operativne sisteme

Sintaksa komande

Sintaksa komandi je sledeca:

- **avgscanx /parametar** ... npr. **avgscanx /comp** za skeniranje celog racunara
- **avgscanx /parametar /parametar** .. ako se koristi više parametara koji se redaju jedan za drugim, a odvojeni su razmakom i kosom crtom
- ako je potrebno uneti odredenu vrednost za parametar (npr. parametar **/scan** koji zahteva informacije o tome koje će se oblasti racunara skenirati, pa je potrebno da unesete tacnu putanju do izabranog odeljka), vrednosti su odvojene tackom i zarezom, npr.: **avgscanx /scan=C:\;D:**

Parametri skeniranja

Za prikazivanje celog pregleda dostupnih parametara otkucajte odgovarajucu komandu zajedno sa parametrom **/?** ili **/HELP** (npr. **avgscanx /?**). Jedini obavezni parametar je **/SCAN** kojim se određuju oblasti racunara koje se skeniraju. Za detaljnije objašnjenje opcija pogledajte [pregled parametara komandne linije](#).

Da biste pokrenuli skeniranje, pritisnite taster **Enter**. U toku skeniranja, proces možete zaustaviti ako pritisnete kombinaciju tastera **Ctrl+C** ili **Ctrl+Pause**.

Pokretanje skeniranja iz komandne linije pomocu grafickog interfejsa

Kada pokrenete racunar u Windows bezbednom režimu, postoji i mogucnost pokretanja skeniranja iz komandne linije pomocu grafickog interfejsa. Sâmo skeniranje se pokrece iz komandne linije, a dijalog **Sastavljač komandne linije** vam omogucava da navedete vecinu parametara za skeniranje u komfornom grafickom okruženju.

Buduci da je ovaj dijalog dostupan samo u Windows bezbednom režimu, njegovo detaljno objašnjenje potražite u datoteci pomoci koja se otvara direktno iz dijaloga.

12.4.1. Parametri za skeniranje iz komandne linije

Sledi lista svih dostupnih parametara za skeniranje iz komandne linije:

- **/SCAN** [Skeniranje određenih datoteka ili fascikli](#) /SCAN=putanja;
putanja (npr. /SCAN=C:\;D:\)
- **/COMP** [Skeniraj ceo racunar](#)
- **/HEUR** Koristi heuristicku analizu***
- **/EXCLUDE** Izuzmi putanju ili datoteke iz skeniranja
- **/@** Komandna datoteka /ime datoteke/
- **/EXT** Skeniraj ove oznake tipa /na primer, EXT=EXE,DLL/
- **/NOEXT** Ne skeniraj ove oznake /na primer, NOEXT=JPG/
- **/ARC** Skeniraj arhive
- **/CLEAN** Automatski ocisti
- **/TRASH** Premesti zaražene datoteke u Skladište za viruse***
- **/QT** Brzi test
- **/MACROW** Prijavi makroe
- **/PWDW** Prijavi datoteke zašticene lozinkom

- **/IGNLOCKED** Zanemari zaključane datoteke
- **/REPORT** Izveštaj upiši u datoteku /ime datoteke/
- **/REPAPPEND** Dodaj u datoteku izveštaja
- **/REPOK** Prijavi da su datoteke koje nisu zaražene u redu
- **/NOBREAK** Onemogući prekidanje pomoću tastera CTRL-BREAK
- **/BOOT** Omogući MBR/BOOT proveru
- **/PROC** Skeniraj aktivne procese
- **/PUP** Izveštavanje o „[Potencijalno neželjenim programima](#)“
- **/REG** Skeniraj registrator
- **/COO** Skeniraj kolacice
- **/?** Prikaži pomoć za ovu temu
- **/HELP** Prikaži pomoć za ovu temu
- **/PRIORITY** Podešavanje prioriteta skeniranja /Nizak, automatski, visok/ (pogledajte [Napredna podešavanja / Skeniranje](#))
- **/SHUTDOWN** Isključi računar nakon završetka skeniranja
- **/FORCESHUTDOWN** Prinudno isključi računar nakon završetka skeniranja
- **/ADS** Skeniraj alternativne tokove podataka (samo u NTFS sistemu)

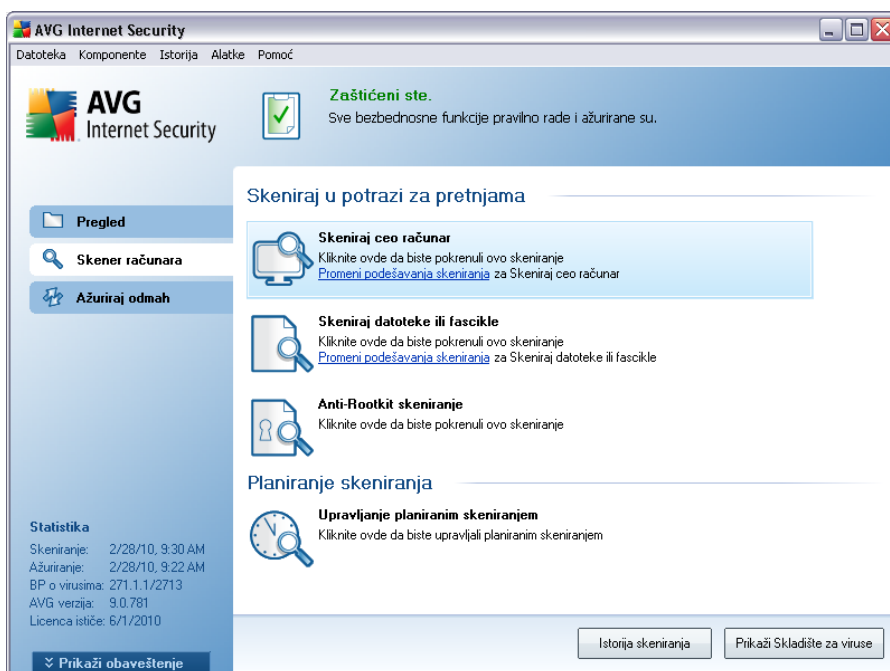
12.5. Planiranje skeniranja

Program **AVG 9 Anti-Virus sa zaštitnim zidom** vam omogućava da pokrenete skeniranje na zahtev (na primer, kada sumnjate da je infekcija prenesena na vaš računar) ili na osnovu plana. Preporučuje se da skeniranje obavljate po planu: na taj način možete biti sigurni da će vaš računar biti zaštićen od mogućnosti zaraze, a nećete morati da brinete ni o tome da li je potrebno pokrenuti skeniranje i kada.

Trebalo bi redovno da koristite opciju **[Skeniraj ceo računar](#)**, bar jednom sedmično. Međutim, ako je moguće, pokrenite skeniranje celog računara jednom dnevno - kao što

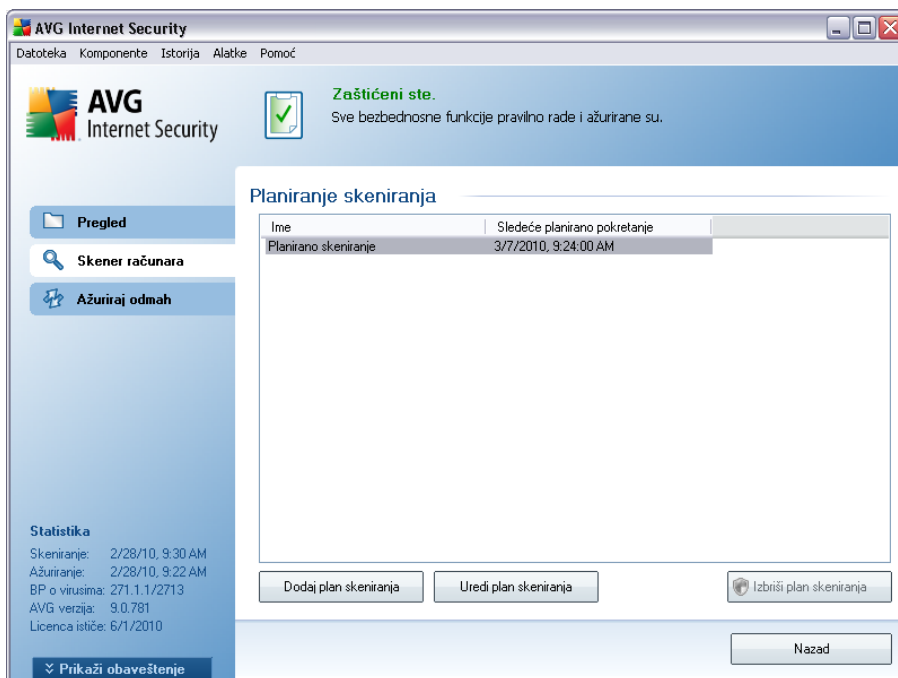
je podešeno u podrazumevanoj konfiguraciji plana za skeniranje. Ako racunar držite stalno ukljucen, možete napraviti plan za skeniranje van radnih sati. Ako ponekad isključujete racunar, zakažite skeniranje [po pokretanju racunara, nakon propuštenog zadatka skeniranja](#).

Da biste kreirali novi plan skeniranja, pogledajte [AVG interfejs za skeniranje](#) pa u donjem delu pronadite odeljak **Plan skeniranja**:



Planiranje skeniranja

Kliknite na graficku ikonu u odeljku **Planiranje skeniranja** da biste otvorili dijalog **Planiranje skeniranja** u kojem možete da vidite spisak svih trenutno planiranih skeniranja:

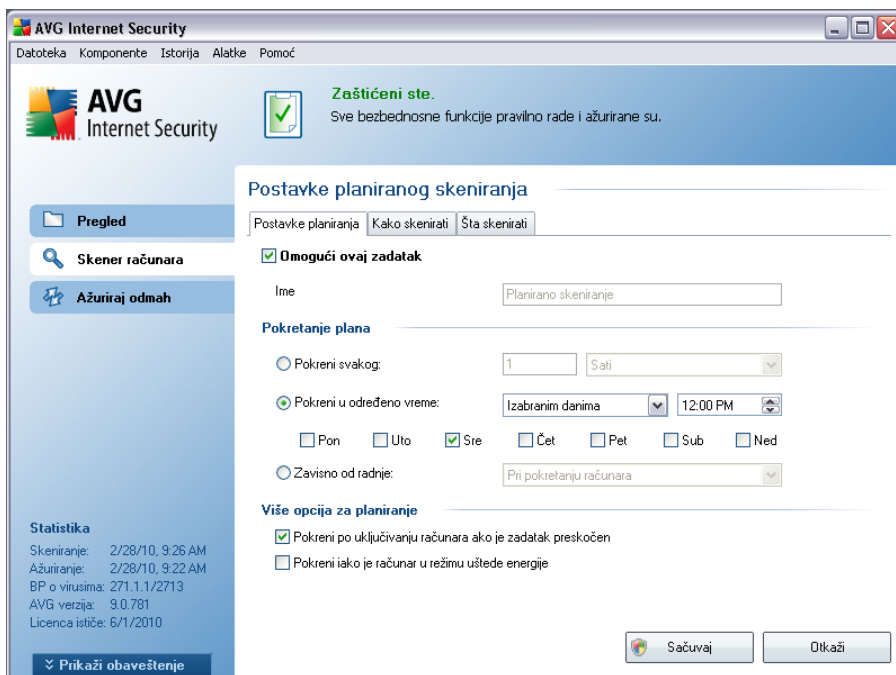


Možete da uredite / dodate skeniranja pomocu sledecih kontrolnih dugmadi:

- **Dodaj plan skeniranja** - služi za otvaranje kartice **Podešavanja planiranja** u dijalogu [Podešavanja za planiranje skeniranja](#) . U ovom dijalogu možete navesti parametre za novodefinisani test.
- **Uredi plan skeniranja** - ovo dugme možete koristiti samo ako ste prethodno izabrali postojeći test iz liste planiranih testova. U tom slučaju dugme će biti aktivno i moći ćete da kliknete na njega da biste prešli na karticu [Schedule settings](#) u dijalogu **Podešavanja za planiranje skeniranja** . Parametri izabranog testa već su navedeni i moguće ih je urediti.
- **Izbriši plan skeniranja** - ovo dugme možete koristiti samo ako ste prethodno izabrali postojeći test iz liste planiranih testova. Ovaj test je moguće izbrisati iz liste tako što ćete kliknuti na kontrolno dugme. Međutim, možete uklanjati samo sopstvene testove; nije moguće izbrisati unapred definisani **Plan skeniranja celog računara** iz podrazumevanih podešavanja.
- **Nazad** - povratak u [AVG interfejs za skeniranje](#)

12.5.1. Postavke planiranja

Ako želite da isplanirate novi test i njegovo redovno pokretanje, otvorite dijalog **Postavke planiranog testa** (kliknite na dugme **Dodaj plan skeniranja** u dijalogu **Planiranje skeniranja**). Dijalog je podjeljen na tri kartice: **Podešavanja planiranja** - pogledajte sliku ispod (podrazumevana kartica koja će se automatski otvoriti), [Kako skenirati](#) i [Šta skenirati](#).



Na kartici **Podešavanja planiranja** možete prvo označiti/poništiti izbor stavke **Omogući ovaj zadatak** da biste jednostavno deaktivirali zakazani test, a kasnije ga možete uključiti po potrebi.

Zatim imenujte način skeniranja koji kreirate i zakazujete. Unesite željeno ime u polje za tekst pored stavke **Ime**. Nastojte da koristite kratka, opisna i prikladna imena za načine skeniranja, kako biste kasnije lakše mogli da ih razlikujete jedne od drugih.

Primer: Nije dobro nazvati skeniranje „Novo skeniranje“ ili „Moje skeniranje“, pošto ta imena ne opisuju ono što se tim skeniranjem proverava. S druge strane, primer dobrog opisanog imena bio bi „Skeniranje sistemskih oblasti“ itd. Takode, nije obavezno da u imenu skeniranja navedete da li je u pitanju skeniranje celog računara ili samo određenih datoteka ili fascikli - vaši načini skeniranja uvek će predstavljati određenu verziju [skeniranja određenih datoteka ili fascikli](#).

U ovom dijalogu možete definisati sledece parametre skeniranja:

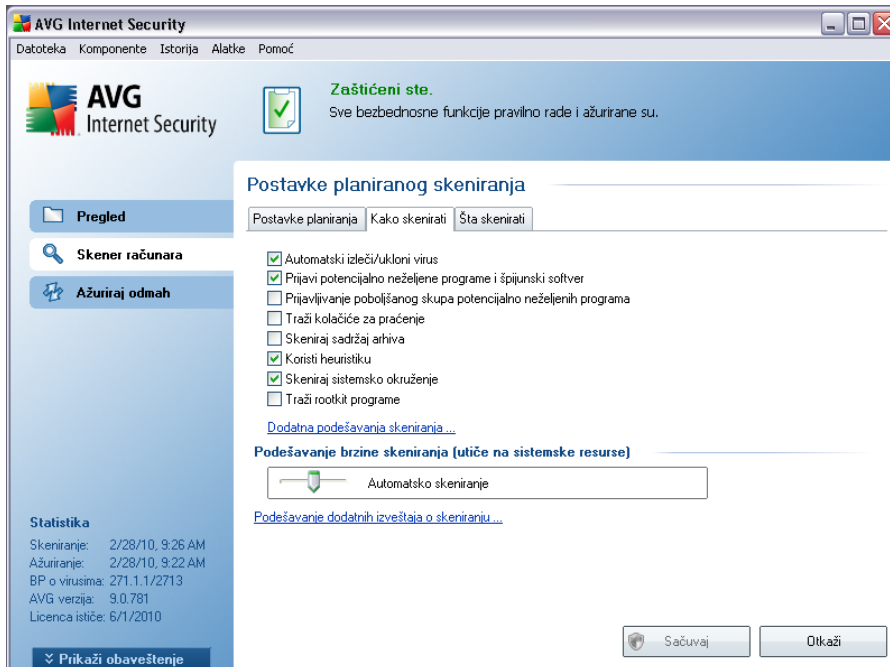
- **Pokretanje plana** - navedite vremenske intervale za pokretanje novog plana skeniranja. Vremenski interval je moguće definisati uzastopnim pokretanjem skeniranja nakon određenog vremenskog perioda (**Pokreni svakih ...**), definisanjem tačnog datuma i vremena (**Pokreni u određeno vreme ...**) ili definisanjem događaja sa kojim bi trebalo povezati pokretanje skeniranja (**Radnja zasnovana na pokretanju računara**).
- **Napredne opcije za planiranje** - u ovom odeljku možete definisati pod kojim se okolnostima skeniranje pokreće/ne pokreće ako je računar u režimu niske potrošnje energije ili je potpuno isključen.

Kontrolna dugmad u dijalogu Podešavanja za planirano skeniranje

Dva kontrolna dugmeta dostupna su na svakoj od tri kartice u dijalogu **Podešavanje planiranog skeniranja** (**Podešavanje planiranja**, [Kako skenirati](#) i [Šta skenirati](#)), a funkcionalnost im je ista bez obzira na to na kojoj se kartici trenutno nalazite:

- **Sacuvaj** - čuva sve promene koje ste napravili na ovoj kartici ili na bilo kojoj drugoj kartici u ovom dijalogu i vraća vas na [podrazumevani dijalog AVG interfejsa za skeniranje](#). Stoga, ako želite da konfigurišete parametre testiranja na svim karticama, pritisnite ovo dugme da ih sacuvate tako nakon što ste uneli sve željene postavke.
- **Otkazi** - otkazivanje svih izmena koje ste uneli na ovoj kartici ili bilo kojoj kartici ovog dijaloga i povratak na [podrazumevani dijalog AVG interfejsa za skeniranje](#)..

12.5.2. Kako skenirati



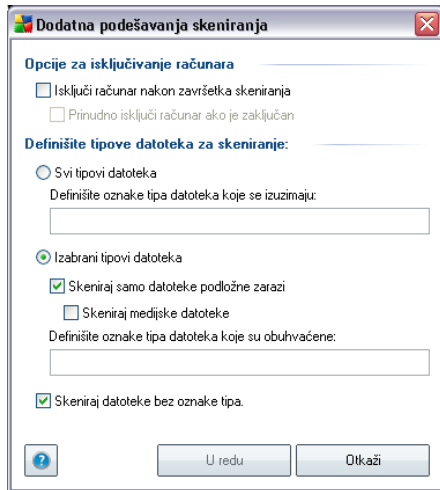
Na kartici **Kako skenirati** pronaci cete listu parametara za skeniranje koje je moguće opcionalno uključiti ili isključiti. Većina parametara je podrazumevano uključena i primenjivace se tokom skeniranja. Ukoliko nemate određen razlog da promenite te postavke, preporučuje se da zadržite unapred definisanu konfiguraciju:

- **Automatski izleći/ukloni infekciju** - (podrazumevano je uključeno): ako tokom skeniranja bude otkriven virus, moguće ga je automatski ukloniti, ukoliko je dostupan lek. U slučaju da zaraženu datoteku nije moguće automatski izluciti ili ako odlucite da isključite ovu opciju, nakon otkrivanja virusa doćete obavještenje, pa cete morati da odlucite šta želite da uradite sa tom datotekom. Preporučena radnja je da zaraženu datoteku premestite u [Skladište za viruse](#).
- **Prijavi potencijalno neželjene programe i špijunski softver** - (podrazumevano je uključeno): potvrdite izbor u ovom polju za potvrdu da biste aktivirali [Antispajver](#) mehanizam i obavili skeniranje u potrazi za špijunskim programima i virusima. [Špijunski softver](#) se ne može sa sigurnošću svrstati u kategoriju malvera: Iako obično predstavlja bezbednosni rizik, neki od ovih programa mogu se bezbedno instalirati na racunar. Preporučujemo vam da ova funkcija bude uključena jer povećava bezbednost racunara

- **Prijavi poboljšani skup potencijalno neželjenih programa** – ako je prethodna opcija aktivirana, takode možete da potvrdite izbor u ovom polju za potvrdu kako bi se detektovao poboljšani skup [špijunskih programa](#): programi koji su potpuno bezbedni kada ih kupite od proizvođača, ali koji se kasnije mogu iskoristiti u zlonamernim svrham. Ovo je dodatna mera kojom se bezbednost računara poboljšava još više. Međutim, zbog toga što postoji mogućnost blokiranja legalnih programa, ova opcija je podrazumevano isključena.
- **Skeniraj kolacice za pracenje** - (podrazumevano je uključeno): ovaj parametar komponente [Antispajver](#) definiše da bi tokom skeniranja trebalo otkrivati kolacice (*HTTP kolacici služe za proveru identiteta, pracenje i održavanje određenih informacija o korisnicima, kao što su željene opcije za lokaciju ili sadržaj elektronskih kolica za kupovinu*);
- **Skeniraj unutar arhiva** - (podrazumevano je uključeno): ovim parametrom se definiše da bi skeniranje trebalo da obuhvati sve datoteke, čak i ako se one nalaze u nekom tipu arhive, npr. ZIP, RAR itd.
- **Koristi heuristiku** - (podrazumevano je uključeno): heuristička analiza (*dinamička emulacija instrukcija skeniranih objekata u virtuelnom računarskom okruženju*) bice jedna od metoda koja ce se koristiti za otkrivanje virusa tokom skeniranja;
- **Skeniraj sistemsko okruženje** - (podrazumevano je uključeno): skeniranje ce obuhvatiti i sistemske oblasti na računaru;

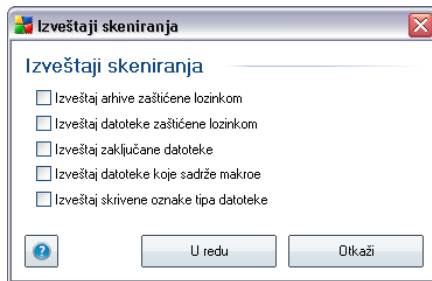
Potom možete da promenite konfiguraciju skeniranja na sledeci način:

- **Dodatne postavke skeniranja** - ovaj link otvara novi dijalog **Dodatne postavke skeniranja** u kojem možete da navedete sledece parametre:



- **Opcije za isključivanje računara** - odlucite da li želite da se racunar automatski iskljuci kada se pokrenuto skeniranje završi. Ako potvrdite ovu opciju (**Iskljuci racunar nakon završetka skeniranja**), aktivirace se nova opcija koja omogucava da se racunar iskljuci cak i ako je trenutno zakljucan (**Prinudno iskljuci racunar ako je zakljucan**).
- **Definišite tipove datoteka za skeniranje** - odlucite da li želite da skenirate:
 - **Sve tipove datoteka** sa mogucnošcu definisanja izuzetaka koji se nece skenirati tako što cete navesti listu oznaka tipa datoteke razdvojenih zarezima koje ne treba skenirati;
 - **Izabrane tipove datoteka** - možete izabrati da skenirate samo datoteke za koje postoji mogucnost da su zaražene (*datoteke koje ne mogu biti zaražene nece se skenirati, na primer tekstualne datoteke ili neke druge datoteke koje nisu izvršne*), ukljucujuci medijske datoteke (*video audio datoteke - ako ne potvrdite izbor u ovom polju za potvrdu, vreme skeniranja ce se dodatno skratiti jer su datoteke ovog tipa obicno velike i malo je verovatno da su zaražene virusom*). Izborom oznake tipa datoteke možete oznaciti datoteke koje treba uvek skenirati.
 - Možete i da izaberete opciju **Skeniraj datoteke bez oznake tipa datoteke** - ova opcija je podrazumevano ukljucena i preporucuje se da je ne iskljucujete osim ako nemate dobar razlog za to. Datoteke bez oznake tipa datoteke su sumnjive i treba ih uvek skenirati.

- **Prioritet procesa skeniranja** - pomocu klizaca možete promeniti prioritet procesa skeniranja. Podrazumevano, prioritet je podešen na srednji nivo (*Automatsko skeniranje*), što optimizuje brzinu procesa skeniranja i zauzetost sistemskih resursa. Takode, proces skeniranja možete usporiti, što znaci da ce zauzetost sistemskih resursa biti manja (*korisno ako morate da radite na racunaru, a nije vam važno koliko ce skeniranje trajati*), a možete ga i ubrzati, što zahteva više sistemskih resursa (*npr. kada se privremeno udaljite od racunara*).
- **Podešavanje dodatnih izveštaja o skeniranju** - ovaj link otvara novi dijalog **Izveštaji skeniranja** u kojem možete da izaberete koji tip pronadenog sadržaja ce se prijavljivati:



Napomena: Podrazumevana podešavanja za konfiguraciju skeniranja su optimalne performanse. Ukoliko nemate određen razlog za menjanje podešavanja skeniranja, preporučuje se da ne menjate unapred definisanu konfiguraciju. Sve promene konfiguracije trebalo bi da obavljaju samo napredni korisnici. Više opcija za konfiguraciju skeniranja potražite u dijalogu **Napredna podešavanja** koji je dostupan pomocu sistemskog menija **Datoteka / Napredna podešavanja** .

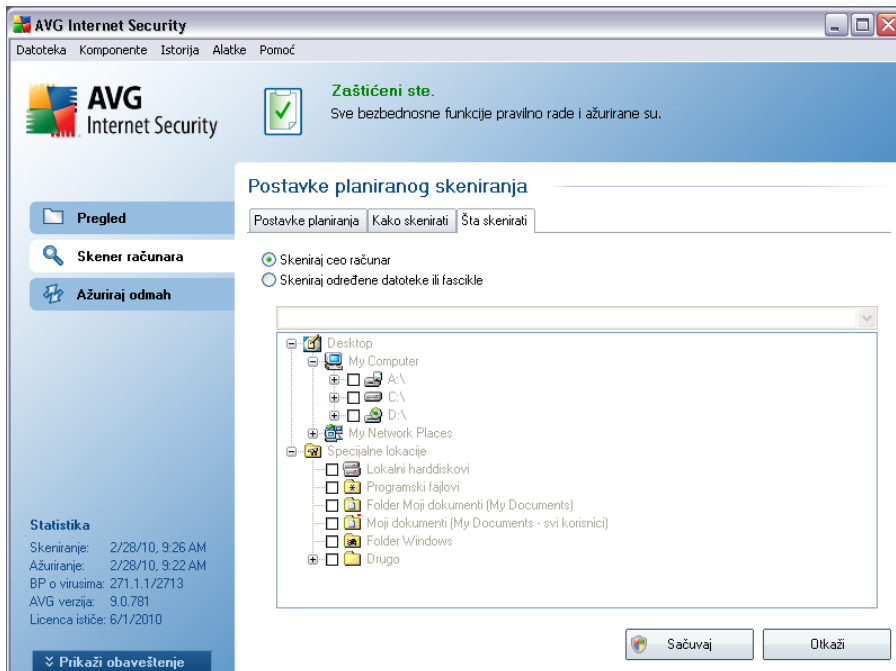
Kontrolna dugmad

Postoje dva kontrolna dugmeta na sve tri kartice u dijalogu **Podešavanja za planirano skeniranje** (**Postavke planiranja**, **Kako skenirati** i **Šta skenirati**), a imaju istu funkcionalnost, bez obzira na to na kojoj kartici se nalazete:

- **Sacuvaj** - cuva sve promene koje ste napravili na ovoj kartici ili na bilo kojoj drugoj kartici u ovom dijalogu i vraća vas na [podrazumevani dijalog AVG interfejsa za skeniranje](#). Stoga, ako želite da konfigurišete parametre testiranja na svim karticama, pritisnite ovo dugme da ih sacuvate tako nakon što ste uneli sve željene postavke.
- **Otkazi** - otkazivanje svih izmena koje ste uneli na ovoj kartici ili bilo kojoj kartici ovog dijaloga i povratak na [podrazumevani dijalog AVG interfejsa za](#)

[skeniranje..](#)

12.5.3. Šta skenirati



Na kartici **Šta skenirati**, možete definisati da li želite da zakažete [skeniranje celog računara](#) ili [skeniranje određenih datoteka ili fascikli](#).

Ukoliko izaberete da želite da skenirate određene datoteke ili fascikle, u donjem delu ovog dijaloga prikazace se prikaz strukture u obliku stabla u kome možete da izaberete fascikle koje želite da skenirate (*proširujte stavke tako što ćete kliknuti na znak sve dok ne pronađete fasciklu koju želite da skenirate*). Možete izabrati više fascikli tako što ćete oznaciti odgovarajuća polja. Izabrane fascikle pojavice se u polju za tekst na vrhu dijaloga, a istorija izabranog skeniranja bice sacuvana u padajucem meniju za buducu upotrebu. Umesto toga, možete rucno uneti punu putanju do željene fascikle (*ako unesete više putanja, morate ih razdvojiti tackom i zarezom, bez dodatnog razmaka između*).

U prikazu strukture u obliku stabla takode možete da vidite granu **Posebne lokacije**. U nastavku sledi lista lokacija koje ce se skenirati kada potvrdite izbor u odgovarajucem polju za potvrdu:

- **Lokalni cvrsti diskovi** - svi cvrsti diskovi na vašem racunaru

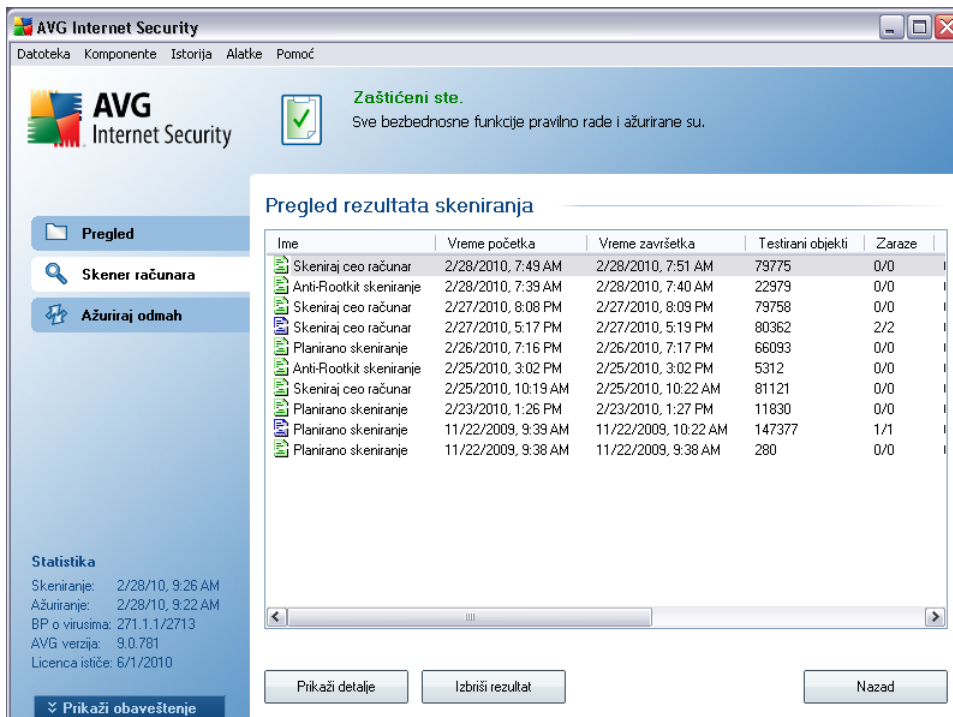
- **Programske datoteke** - C:\Program Files\
 - **Fascikla „Moji dokumenti“** - C:\Documents and Settings\User\My Documents\
 - **Deljeni dokumenti** - C:\Documents and Settings\All Users\Documents\
 - **Fascikla Windows** - C:\Windows\
 - **Drugo**
 - *Sistemska disk jedinica* - cvrsti disk na kojem je instaliran operativni sistem (obicno C:)
 - *Sistemska fascikla* - Windows/System32
 - *Fascikla „Privremene datoteke“* - Documents and Settings/User/Local Settings/Temp
 - *Privremene Internet datoteke* - Documents and Settings/User/Local Settings/Temporary Internet Files











Kontrolna dugmad u dijalogu Podešavanja za planirano skeniranje

Dva kontrolna dugmeta dostupna su na svakoj od tri kartice u dijalogu **Podešavanje planiranog skeniranja** (**Podešavanje planiranja**, **Kako skenirati** i **Šta skenirati**), a funkcionalnost im je ista bez obzira na to na kojoj se kartici trenutno nalazite:

- **Sacuvaj** - cuva sve promene koje ste napravili na ovoj kartici ili na bilo kojoj drugoj kartici u ovom dijalogu i vraća vas na [podrazumevani dijalog AVG interfejsa za skeniranje](#). Stoga, ako želite da konfigurirate parametre testiranja na svim karticama, pritisnite ovo dugme da ih sacuvate tako nakon što ste uneli sve željene postavke.
- **Otkazi** - otkazivanje svih izmena koje ste uneli na ovoj kartici ili bilo kojoj kartici ovog dijaloga i povratak na [podrazumevani dijalog AVG interfejsa za skeniranje](#)..


12.6. Pregled rezultata skeniranja





Ime	Vreme početka	Vreme završetka	Testirani objekti	Zaraze
 Skeniraj ceo računar	2/28/2010, 7:49 AM	2/28/2010, 7:51 AM	79775	0/0
 Anti-Rootkit skeniranje	2/28/2010, 7:39 AM	2/28/2010, 7:40 AM	22979	0/0
 Skeniraj ceo računar	2/27/2010, 8:08 PM	2/27/2010, 8:09 PM	79758	0/0
 Skeniraj ceo računar	2/27/2010, 5:17 PM	2/27/2010, 5:19 PM	80362	2/2
 Planirano skeniranje	2/26/2010, 7:16 PM	2/26/2010, 7:17 PM	66093	0/0
 Anti-Rootkit skeniranje	2/25/2010, 3:02 PM	2/25/2010, 3:02 PM	5312	0/0
 Skeniraj ceo računar	2/25/2010, 10:19 AM	2/25/2010, 10:22 AM	81121	0/0
 Planirano skeniranje	2/23/2010, 1:26 PM	2/23/2010, 1:27 PM	11830	0/0
 Planirano skeniranje	11/22/2009, 9:39 AM	11/22/2009, 10:22 AM	147377	1/1
 Planirano skeniranje	11/22/2009, 9:38 AM	11/22/2009, 9:38 AM	280	0/0

Dijalogu **Pregled rezultata skeniranja** moguće je pristupiti iz [AVG interfejsa za skeniranje](#) pomoću dugmeta **Istorija skeniranja**. Dijalog sadrži listu svih prethodno pokrenutih skeniranja i informacije o njihovim rezultatima:

- **Ime** - određite za skeniranje; to može biti ime nekog od [unapred definisanih skeniranja](#) ili ime koje ste dodelili sopstvenom [planiranom skeniranju](#). Svako ime sadrži i ikonu koja ukazuje na rezultat skeniranja:

 - zelena ikona ukazuje na to da tokom skeniranja nije otkrivena infekcija

 - plava ikona ukazuje na to da je tokom skeniranja otkrivena infekcija, ali je zaraženi objekat automatski uklonjen

 - crvena ikona upozorava na to da je tokom skeniranja otkrivena infekcija i da je nije bilo moguće ukloniti!

Svaka ikona može biti prikazana u celosti ili presečena na pola - ikone koje su predstavljene u celosti predstavljaju skeniranja koja su ispravno

dovršena; presećena ikona ukazuje na to da je skeniranje otkazano ili prekinuto.

Napomena: Detaljne informacije o svakom skeniranju potražite u dijalogu [Rezultati skeniranja](#) kojem možete pristupiti pomoću dugmeta **Prikaži detalje** (u donjem delu ovog dijaloga).

- **Vreme pocetka** - datum i vreme pokretanja skeniranja
- **Vreme završetka** - datum i vreme završetka skeniranja
- **Testirani objekti** - broj objekata koji su pregledani tokom skeniranja
- **Zaraze** - broj otkrivenih/uklonjenih [virusa](#)
- **Špijunski softver** - broj otkrivenih/uklonjenih [špijunskih programa](#)
- **Upozorenja** - broj detektovanih [sumnjivih objekata](#)
- **Rootkit programi** - broj detektovanih [rootkit programa](#)
 - **Informacije o evidenciji skeniranja** - informacije u vezi sa tokom skeniranja i rezultatima (uobicajeno po završetku ili po prekidanju)

Kontrolna dugmad

Kontrolna dugmad za dijalog **Pregled rezultata skeniranja** su:

- **Prikaži detalje** - kliknite na ovo dugme da biste se prebacili u dijalog [Rezultati skeniranja](#) i videli detaljne podatke o izabranom skeniranju
- **Izbriši rezultat** - kliknite na ovo dugme da biste uklonili izabranu stavku iz pregleda rezultata skeniranja
- **Nazad** - služi za vraćanje na podrazumevani dijalog [AVG interfejsa za skeniranje](#)

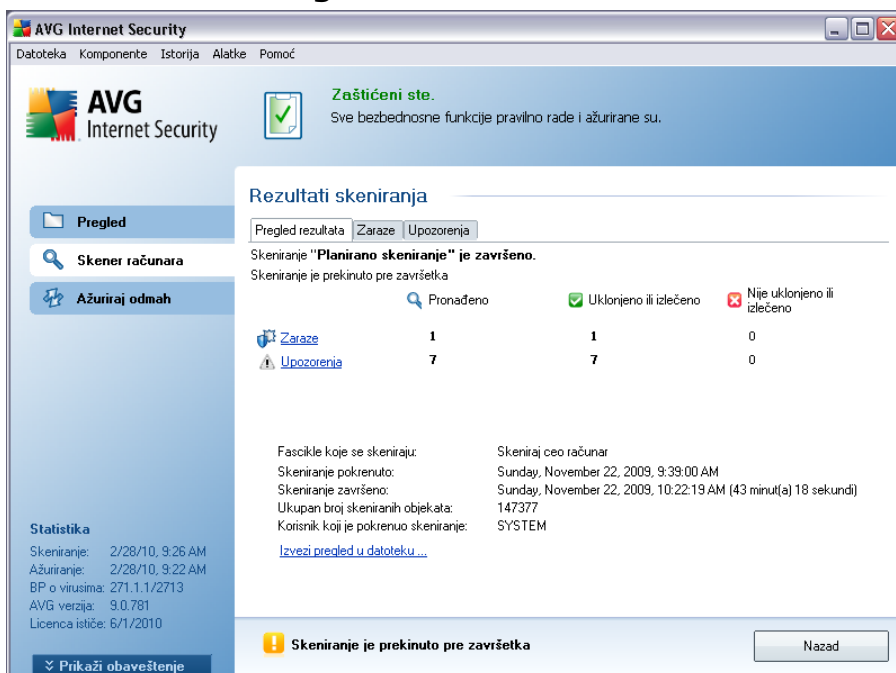
12.7. Detalji rezultata skeniranja

Ako u dijalogu [Pregled rezultata skeniranja](#) izaberite određeni način skeniranja, moći ćete da kliknete na dugme **Prikaži detalje** kako biste prešli u dijalog **Rezultati skeniranja** koji sadrži detaljne informacije o toku i rezultatu izabranog načina skeniranja.

Ovaj dijalog je podeljen na nekoliko kartica:

- **Pregled rezultata** - ova kartica se sve vreme prikazuje, a sadrži statističke podatke o toku skeniranja
- **Zaraze** - ova kartica se prikazuje samo ako je u toku skeniranja detektovana [zaraza virusom](#)
- **Špijunski softver** - ova kartica se prikazuje samo ako je u toku skeniranja detektovan [špijunski softver](#)
- **Upozorenja** - ova kartica se prikazuje ako su, na primer, tokom skeniranja otkriveni kolacici
- **Informacije** - ova kartica se prikazuje samo ako su detektovane određene potencijalne pretnje koje ne spadaju u gornje kategorije; ova kartica sadrži poruku upozorenja u vezi sa pronađenom datotekom. Ovde ćete takode videti informacije o objektima koje nije bilo moguće skenirati (npr. arhivama koje su zaštićene lozinkom).

12.7.1. Kartica Pregled rezultata



AVG Internet Security

Zaštićeni ste.
Sve bezbednosne funkcije pravilno rade i ažurirane su.

Rezultati skeniranja

Pregled rezultata | Zaraze | Upozorenja

Skeniranje "Planirano skeniranje" je završeno.
Skeniranje je prekinuto pre završetka

	Pronađeno	Uklonjeno ili izlečeno	Nije uklonjeno ili izlečeno
Zaraze	1	1	0
Upozorenja	7	7	0

Fascikle koje se skeniraju: Skeniraj ceo računar
 Skeniranje pokrenuto: Sunday, November 22, 2009, 9:39:00 AM
 Skeniranje završeno: Sunday, November 22, 2009, 10:22:19 AM (43 minut(a) 18 sekund)

Ukupan broj skeniranih objekata: 147377
 Korisnik koji je pokrenuo skeniranje: SYSTEM

[Izvezi pregled u datoteku ...](#)

Statistika
 Skeniranje: 2/28/10, 9:26 AM
 Ažuriranje: 2/28/10, 9:22 AM
 BP o virusima: 271.1.1/2713
 AVG verzija: 9.0.781
 Licenca ističe: 6/1/2010

⚠ Skeniranje je prekinuto pre završetka

Nazad

Na kartici **Rezultati skeniranja** nalaze se detaljni statistički podaci o:

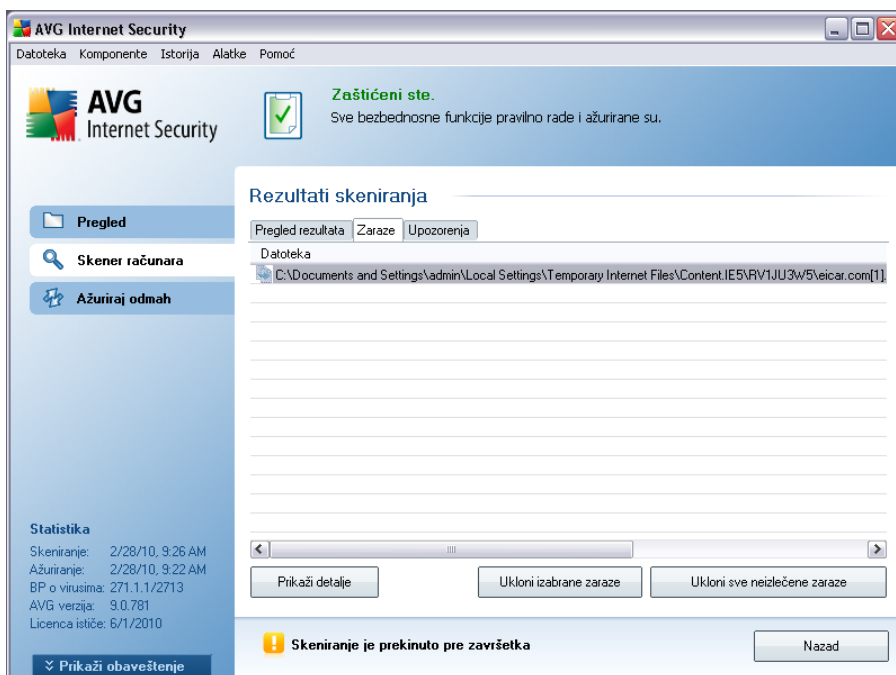
- detektovanim [zarazama virusom](#) / [špijunskim softverom](#)
- uklonjenim [zarazama virusom](#) / [špijunskim softverom](#)
- broju [zaraza virusom](#) / [špijunskim softverom](#) koji se ne mogu ukloniti ili oporaviti

Osim toga, tu su i informacije o datumu i tačnom vremenu pokretanja skeniranja, ukupnom broju skeniranih objekata, trajanju skeniranja i broju grešaka koje su se javile u toku skeniranja.

Kontrolna dugmad

U ovom dijalogu nalazi se samo jedno kontrolno dugme: Dugme **Zatvori** služi za povratak u dijalog [Pregled rezultata skeniranja](#).

12.7.2. Kartica Zaraze



Kartica **Zaraze** prikazuje se u dijalogu **Rezultati skeniranja** samo ako je [zaraza virusom](#) detektovana u toku skeniranja. Kartica je podeljena na tri odeljka i pruža sledeće informacije:

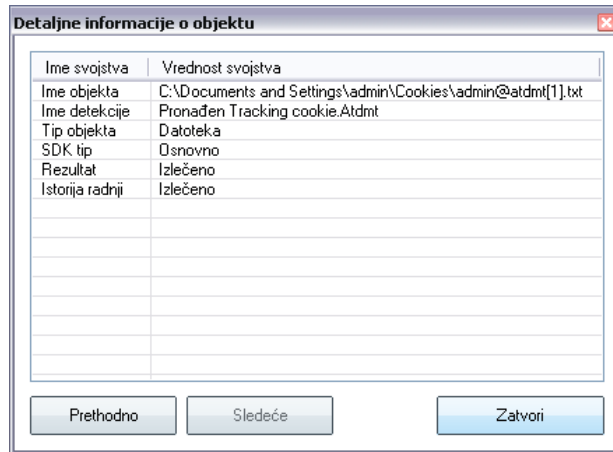
- **Datoteka** - potpuna putanja do originalne lokacije zaraženog objekta

- **Zaraze** - ime detektovanog [virusa](#) (*detaljne informacije o konkretnim virusima potražite u [Enciklopediji virusa](#) na mreži*)
- **Rezultat** - definiše trenutni status zaraženog objekta koji je detektovan u toku skeniranja:
 - **Zaraženo** - zaraženi objekat je detektovan i ostavljen na originalnoj lokaciji (*na primer, ako ste [isključili opciju automatskog oporavka](#) u posebnim podešavanjima skeniranja*)
 - **Izlečeno** - zaraženi objekat je automatski izlečen i ostavljen je na originalnoj lokaciji
 - **Premešteno u skladište virusa** - zaraženi objekat je premešten u [Skladište virusa](#)
 - **Izbrisano** - zaraženi objekat je izbrisan
 - **Dodato u PUP izuzetke** - pronadeni objekat je prepoznat kao izuzetak i dodat na listu Izuzeci od potencijalno neželjenih programa (*koju ste podesili u dijalogu [Izuzeci od potencijalno neželjenih programa](#) u okviru naprednih podešavanja*)
 - **Zaključana datoteka - nije testirano** - pronadeni objekat je zaključan, pa ga AVG ne može skenirati
 - **Potencijalno opasan objekat** - objekat je prepoznat kao potencijalno opasan, ali ne i zaražen (*npr. možda sadrži makroe*); ovu informaciju treba shvatiti samo kao upozorenje
 - **Da bi se operacija dovršila, potrebno je da ponovo pokrenete racunar** - nije moguće ukloniti zaraženi objekat, morate da ponovo pokrenete racunar da biste ga uklonili

Kontrolna dugmad

U ovom dijalogu dostupna su tri kontrolna dugmeta:

- **Prikaži detalje** - služi za otvaranje novog dijaloga pod nazivom **Informacije o rezultatu detaljnog skeniranja**:



U ovom dijalogu možete pronaći informacije o otkrivenom zaraženom objektu (**Ime svojstva**). Pomocu dugmadi **Prethodno** / **Sledeće** možete prikazati informacije o željenim rezultatima. Pomocu dugmeta **Zatvori** možete zatvoriti dijalog.

- **Ukloni izabrane zaraze** - pomocu ovog dugmeta izabrani rezultat možete premestiti u [Skladište virusa](#)
- **Ukloni sve neizlecene zaraze** - pomocu ovog dugmeta možete izbrisati sve rezultate koje nije moguće izlečiti ili ih premestiti u [Skladište virusa](#)
- **Zatvori rezultate** - služi za zatvaranje pregleda detaljnih informacija i vraćanje u dijalog [Pregled rezultata skeniranja](#)

12.7.3. Kartica Špijunski softver

Kartica **Špijunski softver** prikazuje se u dijalogu **Rezultati skeniranja** samo ako je tokom skeniranja otkriven [špijunski softver](#). Kartica je podeljena na tri odeljka i pruža sledeće informacije:

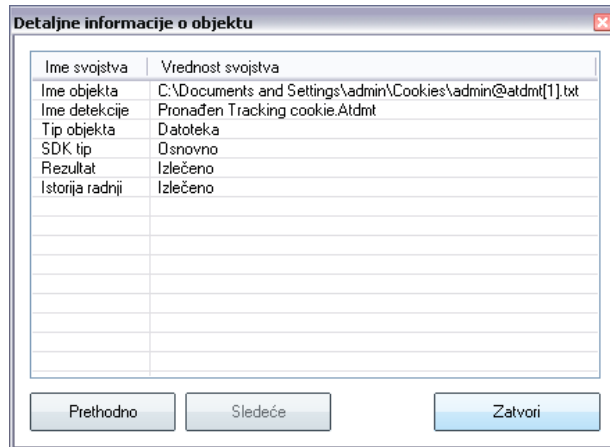
- **Datoteka** - potpuna putanja do originalne lokacije zaraženog objekta
- **Zaraze** - ime otkrivenog [špijunskog softvera](#) (detalje o određenim virusima potražite u [Enciklopediji virusa na mreži](#))
- **Rezultat** - definiše trenutni status objekta koji je otkriven tokom skeniranja:
 - **Zaraženo** - zaraženi objekat je detektovan i ostavljen na originalnoj lokaciji (na primer, ako ste [isključili opciju automatskog oporavka](#) u posebnim podešavanjima skeniranja)

- **Izlečno** - zaraženi objekat je automatski izlečen i ostavljen je na originalnoj lokaciji
- **Premešteno u skladište virusa** - zaraženi objekat je premešten u [Skladište virusa](#)
- **Izbrisano** - zaraženi objekat je izbrisan
- **Dodato u PUP izuzetke** - pronađeni objekat je prepoznat kao izuzetak i dodat na listu izuzetaka od potencijalno neželjenih programa (*koju ste podesili u dijalogu [Izuzeci od potencijalno neželjenih programa](#) u okviru naprednih podešavanja*)
- **Zaključana datoteka - nije testirano** - objekat je zaključan pa AVG ne može da ga skenira
- **Potencijalno opasan objekat** - objekat je označen kao potencijalno opasan, ali nije zaražen (na primer, možda sadrži makroe); ovo je samo upozorenje
- **Da bi se operacija dovršila, potrebno je da ponovo pokrenete racunar** - nije moguće ukloniti zaraženi objekat, morate da ponovo pokrenete racunar da biste ga uklonili

Kontrolna dugmad

U ovom dijalogu dostupna su tri kontrolna dugmeta:

- **Prikaži detalje** - služi za otvaranje novog dijaloga pod nazivom **Informacije o rezultatu detaljnog skeniranja**:

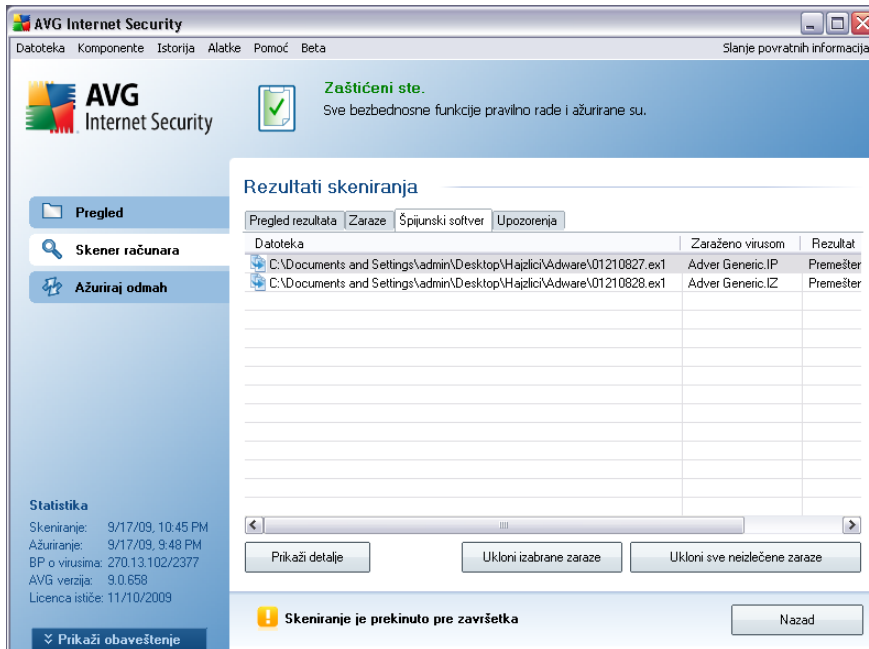


U ovom dijalogu možete pronaći informacije o otkrivenom zaraženom objektu (**Ime svojstva**). Pomocu dugmadi **Prethodno** / **Sledeće** možete prikazati informacije o željenim rezultatima. Pomocu dugmeta **Zatvori** možete zatvoriti ovaj dijalog.

- **Ukloni izabrane zaraze** - pomocu ovog dugmeta izabrani rezultat možete premestiti u [Skladište virusa](#)
- **Ukloni sve neizlečene zaraze** - pomocu ovog dugmeta možete izbrisati sve rezultate koje nije moguće izlečiti ili ih premestiti u [Skladište virusa](#)
- **Zatvori rezultate** - služi za zatvaranje pregleda detaljnih informacija i vraćanje u dijalog [Pregled rezultata skeniranja](#)

12.7.4. Kartica Upozorenja

Na kartici **Upozorenja** prikazane su informacije o „sumnjivim“ objektima (*najčešće datotekama*) koji su detektovani u toku skeniranja. Nakon detekcije komponentom [Stalni štit](#), pristup tim datotekama je blokiran. Najčešći primer za te objekte su: skrivene datoteke, kolacici, sumnjivi ključevi registratora, dokumenti ili arhive zaštićeni lozinkom itd. Te datoteke ne predstavljaju direktnu pretnju po vaš racunar ili bezbednost. Informacije o tim datotekama obično su korisne ako se na racunaru otkrije adware ili špijunski softver. Ukoliko se AVG testom otkriju samo upozorenja, nije potrebno preduzeti nikakvu radnju.



Ovo je kratak opis najčešćih primera takvih objekata:

- **Skrivene datoteke** - skrivene datoteke podrazumevano nisu vidljive u Windowsu i neki virusi ili druge pretnje mogu pokušati da izbegnu otkrivanje tako što se smeštaju u datoteke sa ovim atributom. Ako AVG prijavi skrivenu datoteku za koju sumnjate da je zlonamerna, možete je premestiti u [AVG skladište za viruse](#).
- **Kolacici** - kolacici su datoteke u formatu čistog teksta koje koriste Web lokacije za skladištenje specifičnih informacija o korisniku koje se kasnije koriste za učitavanje prilagođenog rasporeda Web lokacije, automatsko popunjavanje korisničkog imena itd.
- **Sumnjivi ključevi registratora** - određeni tipovi malvera skladište svoje informacije u registrator operativnog sistema Windows kako bi se one učitale prilikom pokretanja sistema ili kako bi proširili svoj efekat na operativni sistem.

12.7.5. Kartica Rootkit programi

Na kartici **Rootkit programi** prikazuju se informacije o rootkit programima otkrivenim tokom skeniranja ukoliko ste pokrenuli **Anti-Rootkit skeniranje** ili ručno dodali opciju za anti-rootkit skeniranje u opciji **Skeniranje celog računara** (ova opcija je podrazumevano isključena).

Rootkit je program osmišljen da preuzme potpunu kontrolu nad računarskim sistemom bez dozvole vlasnika sistema i administratora kojima je dozvoljen pristup. Pristup hardveru nije potreban jer je cilj rootkit programa da preuzme kontrolu nad operativnim sistemom koji je instaliran na hardveru. Rootkit programi najčešće prikrivaju svoje prisustvo na sistemu pomocu subverzije ili izbegavanja standardnih mehanizama za zaštitu operativnog sistema. Ti programi najčešće spadaju u red trojanskih konja, pa su u stanju da prevare korisnike kako bi poverovali da ih mogu bezbedno pokrenuti na sistemu. Tehnike kojima se to postiže obuhvataju prikrivanje aktivnih procesa kako ih ne bi videli programi za nadgledanje ili sakrivanje datoteka ili sistemskih podataka od operativnog sistema.

U osnovi ova kartica izgleda isto kao kartica [Zaraze](#) ili kartica [Špijunski softver](#).

12.7.6. Kartica Informacije

Na kartici **Informacije** nalaze se podaci o pronadenim objektima koji se ne mogu definisati kao zaraze virusom, špijunski softver itd. Ne mogu se obeležiti kao definitivno opasne, ali je potrebno da obratite pažnju na njih. AVG skeniranjem mogu da se otkriju datoteke koje nisu zaražene, ali su sumnjive. Za takve datoteke prikazuje se [Upozorenje](#) ili **Informacija**.

Ozbiljnost na nivou **Informacije** prijavljuje se iz nekog od sledećih razloga:

- **Zapakovan za izvršavanje** - datoteka je zapakovana jednim od manje uobicajenih programa za zapakivanje što može ukazati na pokušaj da se spreči skeniranje ovakve datoteke. Medutim, ne ukazuje svako otkrivanje ovakve datoteke na virus.
- **Rekurzivno zapakovan za izvršavanje** - slicno kao gore navedeno samo što se manje sreće kod uobicajenog softvera. Takve datoteke su sumnjive i trebalo bi da razmislite o njihovom uklanjanju ili slanju na analizu.
- **Arhiva ili dokument zaštićen lozinkom** - AVG ne može da skenira datoteke zaštićene lozinkom (*kao ni bilo koji drugi program za zaštitu od malvera*).
- **Dokument sa makroima** - otkriveni dokument sadrži makroe koji mogu biti zlonamerni.
- **Skrivene oznake tipa datoteke** - datoteke sa skrivenim oznakama tipa datoteke mogu npr. izgledati kao datoteka slike, ali su u stvari izvršne datoteke (*npr. slika.jpg.exe*). Druga oznaka tipa datoteke nije podrazumevano vidljiva u Windowsu, a AVG ce vas obavestiti o ovakvim datotekama kako ih ne biste slučajno otvorili.
- **Neodgovarajuća putanja datoteke** - ako se neka važna sistemska datoteka

pokrece sa putanje koja nije podrazumevana (*npr. winlogon.exe se pokrece iz fascikle koja nije Windows fascikla*), AVG ce prijaviti to neslaganje. U nekim slucajevima, virusi koriste imena standardnih sistemskih procesa kako bi sakrili svoje prisustvo u sistemu.

- **Zakljucana datoteka** - prijavljena datoteka je zakljucana i AVG je ne može skenirati. To obicno znaci da neku datoteku neprekidno koristi sistem (*npr. datoteka virtuelne memorije*).

12.8. Skladište za viruse



Kartica Skladište za viruse predstavlja bezbedno okruženje za upravljanje sumnjivim/zaraženim objektima koji su otkriveni tokom AVG testova. Ako se tokom skeniranja pronade zaraženi objekat, a AVG program ne može automatski da ga oporavi, od vas ce se tražiti da odlucite šta cete uraditi sa sumnjivim objektom. Preporuceno rešenje jeste da premestite objekat u **Skladište za viruse** radi njegovog daljeg tretiranja. Osnovna svrha **Skladišta za viruse** je cuvanje izbrisanih datoteka odredeni vremenski period vreme, kako biste bili sigurni da vam više nece biti potrebne na prvobitnoj lokaciji. Ukoliko primetite da odsutstvo datoteke izaziva probleme, možete poslati tu datoteku na analizu ili možete da je vratite na prvobitnu lokaciju.

Interfejs komponente **Skladište za viruse** otvara se u novom prozoru i sadrži pregled informacija o zaraženim objektima koji su stavljeni u karantin.

- **Ozbiljnost** - informacije o tipu zaraze (*na osnovu njene zarazne moci, objekti na listi mogu biti zaraženi ili potencijalno zaraženi*)
- **Ime virusa** - navodi ime detektovane zaraze na osnovu [Enciklopedije virusa](#) (na mreži)
- **Putanja do datoteke** - puna putanja do originalne lokacije detektovane zarazne datoteke
- **Originalno ime objekta** – svi detektovani objekti navedeni na grafikonu oznaceni su standardnim imenom koje im daje AVG tokom procesa skeniranja. Ukoliko je objekat imao neko odredeno originalno ime koje je poznato (*npr. ime priloga e-poruke koje ne odgovara stvarnom sadržaju priloga*), ono ce biti navedeno u ovoj koloni.
- **Datum skladištenja** - datum i vreme kada je sumnjiva datoteka detektovana i premeštena u **Skladište za viruse**

Kontrolna dugmad

U interfejsu komponente **Skladište za viruse** dostupna su sledeca kontrolna dugmad:

- **Vrati u prethodno stanje** - vraća zaraženu datoteku na originalnu lokaciju na disku
- **Vrati kao** – kliknite na ovo dugme ukoliko odlucite da premestite detektovani zaraženi objekat iz **skladišta za viruse** u izabranu fasciklu. Sumnjivi i detektovani objekat bice sacuvan sa originalnim imenom. Ako je originalno ime nepoznato, koristice se standardno ime.
- **Detalji** – ovo dugme se odnosi samo na pretnje koje je otkrila komponenta **Zaštita identiteta**. Kada kliknete na njega, prikazuje se pregled detalja o pretnji (*datoteke/procesi koji su ugroženi, karakteristike procesa itd.*). Imajte u vidu da je ovo dugme aktivno samo za stavke koje je otkrila komponenta „Zaštita identiteta“!
- **Izbriši** - potpuno i nepovratno uklanjanje zaražene datoteke iz **Skladišta za viruse**
- **Isprazni skladište za viruse** - uklanja iz **Skladišta za viruse** sadržaj kompletno. Kada uklonite datoteke iz skladišta za viruse, one su nepovratno uklonjenje sa diska (nisu premeštene u korpu za otpatke).

13. Ažuriranje programa AVG

Ažuriranje programa AVG je izuzetno bitno kako bi novi virusi mogli da se otkriju što pre.

Tokom [procesa instalacije programa AVG](#) od vas se tražilo da navedete koliko često želite da ažurirate AVG. Na raspolaganju imate sledeće opcije: **Svaka 4 sata** ili **Svaki dan** (pogledajte dijalog [Planiranje redovnog skeniranja i ažuriranja](#)). Buduci da se ispravke za AVG ne objavljuju po nekom određenom rasporedu već pre kao odgovor na kolicinu i ozbiljnost novih pretnji, preporučuje se da barem jednom dnevno proveravate da li postoje nove ispravke. Provera na svaka 4 sata garantuje da će **AVG 9 Anti-Virus sa zaštitnim zidom** biti ažuriran i tokom dana.

13.1. Nivoi ažuriranja

AVG nudi dva nivoa ispravki koje možete izabrati

- **Ažurirane definicije** sadrže promene neophodne za pouzdanu zaštitu od virusa. Ono obično ne sadrži promene kôda i ažurira samo bazu podataka definicija. Ovu ispravku bi trebalo primeniti čim postane dostupna.
- **Ažuriranje programa** sadrži različite promene, ispravke i poboljšanja za program.

Kada [pravite plan za ažuriranje](#), moguće je izabrati nivo prioriteta koji treba da bude preuzet i primenjen.

Napomena: *Ako dode do podudaranja u vremenu planiranog ažuriranja programa i planiranog skeniranja, prosek ažuriranja ima veći prioritet pa će skeniranje biti prekinuto.*

13.2. Tipovi ispravki

Razlikuju se dva tipa ažuriranja:

- **Ažuriranje na zahtev** je trenutno ažuriranje programa AVG koje se može izvršiti uvek kada postoji potreba za time.
- **Planirano ažuriranje** - u programu AVG možete i [unapred podesiti plan ažuriranja](#). Planirano ažuriranje se zatim obavlja periodično u skladu sa konfiguracijom instalacije. Kada se na navedenoj lokaciji pojave nove datoteke ispravki, one se preuzimaju direktno sa Interneta ili iz mrežnog direktorijuma. Kada nema dostupnih novijih ispravki, ništa se ne dešava.

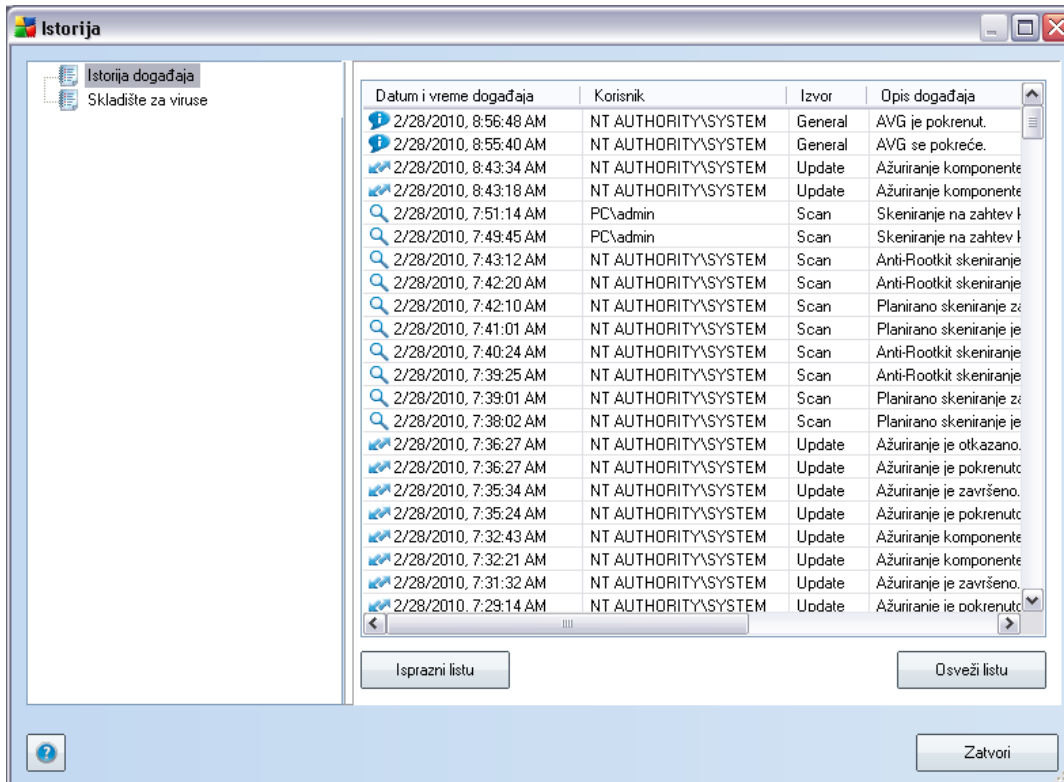
13.3. Proces ažuriranja

Proces ažuriranja moguće je pokrenuti odmah pomoću brze veze **[Ažuriraj odmah***](#)**. Ova veza dostupna je u svakom trenutku iz bilo kojeg dijaloga u [AVG korisničkom interfejsu](#). Međutim, preporučuje se da redovno obavljate ažuriranje, kao što je navedeno u planu ažuriranja koji je moguće urediti pomoću komponente [Upravljanje ažuriranjem](#).

Kada pokrenete ažuriranje, AVG će prvo proveriti da li su dostupne nove datoteke za ažuriranje. Ako jesu, AVG će započeti njihovo preuzimanje i sam proces ažuriranja. Tokom procesa ažuriranja bićete preusmereni na interfejs za **Ažuriranje** gde možete videti grafički prikaz toka procesa, kao i pregled odgovarajućih statističkih parametara (*velicina datoteke za ažuriranje, preuzeti podaci, brzina preuzimanja, proteklo vreme, ...*).

Napomena: pre pokretanja ažuriranja programa AVG, kreira se tačka za vraćanje sistema u prethodno stanje. Ako proces ažuriranja ne uspe i dođe do pada operativnog sistema, možete ga uvek vratiti u stanje prvobitne konfiguracije. Toj opciji možete da pristupite ako kliknete na *Start / Svi programi / Pribor / System tools / Oporavak sistema*. Preporučuje se samo iskusnim korisnicima!

14. Istorija događaja



Dijalogu **Istorija događaja** možete pristupiti iz [sistemskog menija](#), preko stavke **Istorija događaja/Evidencija istorije događaja**. U ovom dijalogu se nalazi rezime važnih događaja do kojih je došlo tokom rada programa **AVG 9 Anti-Virus sa zaštitnim zidom**. **Evidencija istorije događaja** zapisuje sledeće tipove događaja:

- Informacije o ispravkama za AVG aplikaciju
- Pocetak, završetak ili zaustavljanje (uključujući automatski izvršene testove)
- Događaje koji su povezani sa otkrivanjem virusa (pomocu komponente [Stalni štiti](#) ili [skeniranjem](#)), uključujući lokaciju događaja
- Druge važne događaje

Kontrolna dugmad



- **Isprazni listu** - brisanje svih stavki sa liste događaja
- **Osveži listu** - ažuriranje svih stavki sa liste događaja



15. Najčešća pitanja i tehnička podrška

Ukoliko imate poslovnih ili tehničkih problema sa programom AVG, pogledajte odeljak [Najčešća pitanja](http://www.avg.com/) na AVG Web lokaciji (<http://www.avg.com/>).

Ako na taj način ne uspete da pronađete odgovarajuću pomoć, obratite se odeljenju tehničke podrške e-poštom. Upotrebite obrazac za kontakt kojem možete pristupiti iz sistemskog menija izborom stavke **Pomoć / Pomoć na mreži**.